Helyesbítés (érvényes 2013. szeptembertől):

VIZSGÁZNI CSAK AZ JÖHET, AKINEK MEGVAN A GYAKORLATJEGYE ÉS AZ LEGALÁBB ELÉGSÉGES !

Az a későbbi oldalakon gyakran ismétlődő lábjegyzet, amely szerint "a vizsga feltétele 20 pont a gyakorlaton", már **nem érvényes**. A vizsgával kapcsolatos tudnivalók **is változtak.**

Helyesbítés (érvényes 2013. szeptembertől):

VIZSGÁZNI CSAK AZ JÖHET, AKINEK MEGVAN A GYAKORLATJEGYE ÉS AZ LEGALÁBB ELÉGSÉGES !

Az a későbbi oldalakon gyakran ismétlődő lábjegyzet, amely szerint "a vizsga feltétele 20 pont a gyakorlaton", már **nem érvényes**. A vizsgával kapcsolatos tudnivalók **is változtak.**

Helyesbítés (érvényes 2013. szeptembertől):

VIZSGÁZNI <u>CSAK</u> AZ JÖHET, AKINEK MEGVAN A GYAKORLATJEGYE ÉS AZ LEGALÁBB ELÉGSÉGES !

Az a későbbi oldalakon gyakran ismétlődő lábjegyzet, amely szerint "a vizsga feltétele 20 pont a gyakorlaton", már **nem érvényes**. A vizsgával kapcsolatos tudnivalók **is változtak.**

Helyesbítés (érvényes 2013. szeptembertől):

VIZSGÁZNI <u>CSAK</u> AZ JÖHET, AKINEK MEGVAN A GYAKORLATJEGYE ÉS AZ LEGALÁBB ELÉGSÉGES !

Az a későbbi oldalakon gyakran ismétlődő lábjegyzet, amely szerint "a vizsga feltétele 20 pont a gyakorlaton", már **nem érvényes**. A vizsgával kapcsolatos tudnivalók **is változtak.**

Helyesbítés (érvényes 2013. szeptembertől):

VIZSGÁZNI <u>CSAK</u> AZ JÖHET, AKINEK MEGVAN A GYAKORLATJEGYE ÉS AZ LEGALÁBB ELÉGSÉGES !

Az a későbbi oldalakon gyakran ismétlődő lábjegyzet, amely szerint ”a vizsga feltétele 20 pont a gyakorlaton”, már **nem érvényes**. A vizsgával kapcsolatos tudnivalók **is változtak.**

Helyesbítés (érvényes 2013. szeptembertől):

VIZSGÁZNI CSAK AZ JÖHET, AKINEK MEGVAN A GYAKORLATJEGYE ÉS AZ LEGALÁBB ELÉGSÉGES !

Az a későbbi oldalakon gyakran ismétlődő lábjegyzet, amely szerint ”a vizsga feltétele 20 pont a gyakorlaton”, már **nem érvényes**. A vizsgával kapcsolatos tudnivalók **is változtak.**

Tudnivalók

http://www.math.u-szeged.hu/~czedli/

A jelen fájl a félév tervezett anyagát tartalmazza, de apróbb változtatások, hibajavítások várhatók menet közben és/vagy az utolsó tanítási héten.

Kötelező-e előadásra járni?

Kötelező-e előadásra járni? Mivel erről a TVSZ nem rendelkezik, ez a kérdés a Tanszék és az előadó döntési jogkörébe tartozik.

Kötelező-e előadásra járni? Mivel erről a TVSZ nem rendelkezik, ez a kérdés a Tanszék és az előadó döntési jogkörébe tartozik.

Nem teszem kötelezővé — de senki nem hivatkozhat arra, hogy nem volt jelen. (Ez a fájl csak részben —bár túlnyomó részben— tartalmazza a tananyagot.) Az előadáson nagyszámú konkrét feladat megoldását ismertetem (kb. annyit, amennyi a sajnos kis óraszámú gyakorlatokon elhangzik).

Kötelező-e előadásra járni? Mivel erről a TVSZ nem rendelkezik, ez a kérdés a Tanszék és az előadó döntési jogkörébe tartozik.

Nem teszem kötelezővé — de senki nem hivatkozhat arra, hogy nem volt jelen. (Ez a fájl csak részben —bár túlnyomó részben— tartalmazza a tananyagot.) Az előadáson nagyszámú konkrét feladat megoldását ismertetem (kb. annyit, amennyi a sajnos kis óraszámú gyakorlatokon elhangzik).

Kellő számú feladat megoldása nélkül a tananyag nem sajátítható el!

Kötelező-e előadásra járni? Mivel erről a TVSZ nem rendelkezik, ez a kérdés a Tanszék és az előadó döntési jogkörébe tartozik.

Nem teszem kötelezővé — de senki nem hivatkozhat arra, hogy nem volt jelen. (Ez a fájl csak részben —bár túlnyomó részben— tartalmazza a tananyagot.) Az előadáson nagyszámú konkrét feladat megoldását ismertetem (kb. annyit, amennyi a sajnos kis óraszámú gyakorlatokon elhangzik).

Kellő számú feladat megoldása nélkül a tananyag nem sajátítható el! A gyakorlaton való részvétel kevés!

Irodalom:

Szendrei Ágnes: Diszkrét matematika, Polygon, 1994, 1996, 1998, 2000, 2002.

Irodalom:

Szendrei Ágnes: Diszkrét matematika, Polygon, 1994, 1996, 1998, 2000, 2002.

Kalmárné Németh Márta, Katonáné Horváth Eszter, Kámán Tamás: Diszkrét matematikai feladatok, Polygon, Szeged, 2003.

Irodalom:

Szendrei Ágnes: Diszkrét matematika, Polygon, 1994, 1996, 1998, 2000, 2002.

Kalmárné Németh Márta, Katonáné Horváth Eszter, Kámán Tamás: Diszkrét matematikai feladatok, Polygon, Szeged, 2003.

N. J. Vilenkin: Kombinatorika

(Már

Irodalom:

Szendrei Ágnes: Diszkrét matematika, Polygon, 1994, 1996, 1998, 2000, 2002.

Kalmárné Németh Márta, Katonáné Horváth Eszter, Kámán Tamás: Diszkrét matematikai feladatok, Polygon, Szeged, 2003.

N. J. Vilenkin: Kombinatorika

(Már az első két könyv is jóval többet tartalmaz, mint a jelen tantárgy anyaga.)

A gyakorlatra külön kredit és érdemjegy nincs. A gyakorlatokon maximum **50** pontot lehet szerezni.

A gyakorlatra külön kredit és érdemjegy nincs. A gyakorlatokon maximum **50** pontot lehet szerezni. (A részleteket a gyakorlat-vezetők ismertetik.) A félévközi dolgozatok esetén a szorgalmi időszakon **BELÜL pótlásnak helye nincs**.

A gyakorlatra külön kredit és érdemjegy nincs. A gyakorlatokon maximum **50** pontot lehet szerezni. (A részleteket a gyakorlat-vezetők ismertetik.) A félévközi dolgozatok esetén a szorgalmi időszakon **BELÜL pótlásnak helye nincs**. (Igazolt betegség vagy más méltányos indok esetén sem!)

A gyakorlatra külön kredit és érdemjegy nincs. A gyakorlatokon maximum **50** pontot lehet szerezni. (A részleteket a gyakorlatvezetők ismertetik.) A félévközi dolgozatok esetén a szorgalmi időszakon **BELÜL pótlásnak helye nincs**. (Igazolt betegség vagy más méltányos indok esetén sem!)

A gyakorlaton szerzett pontot hozza a hallgató a vizsgára, de aki a gyakorlaton nem ér el legalább 20 pontot, **az nulla pontot hoz**!

A gyakorlatra külön kredit és érdemjegy nincs. A gyakorlatokon maximum **50** pontot lehet szerezni. (A részleteket a gyakorlat-vezetők ismertetik.) A félévközi dolgozatok esetén a szorgalmi időszakon **BELÜL pótlásnak helye nincs**. (Igazolt betegség vagy más méltányos indok esetén sem!)

A gyakorlaton szerzett pontot hozza a hallgató a vizsgára, de aki a gyakorlaton nem ér el legalább 20 pontot, **az nulla pontot hoz**! A vizsga írásbeli, amelyen maximum 60 pontot lehet szerezni. A tantárgyi érdemjegyet a gyakorlaton és a vizsgán szerzett összpontszám határozza meg:

$1 \in [0,\ 49]$,

$1 \in [0,\ 49]$, $2 \in [50,\ 62]$,

$1 \in [0,\ 49]$, $2 \in [50,\ 62]$, $3 \in [63\ 75]$,

$1 \in [0,\ 49]$, $2 \in [50,\ 62]$, $3 \in [63\ 75]$, $4 \in [76,\ 89]$,

$1 \in [0,\ 49]$, $2 \in [50,\ 62]$, $3 \in [63\ 75]$, $4 \in [76,\ 89]$, $5 \in [90,\ 110]$.

$1 \in [0,\ 49]$, $2 \in [50,\ 62]$, $3 \in [63\ 75]$, $4 \in [76,\ 89]$, $5 \in [90,\ 110]$.

Ha valaki a gyakorlaton nem szerzi meg a 20 pontot (és ezért 0 pontot hoz), egyetlen további lehetősége lesz:

$1 \in [0,\ 49]$, $2 \in [50,\ 62]$, $3 \in [63\ 75]$, $4 \in [76,\ 89]$, $5 \in [90,\ 110]$.

Ha valaki a gyakorlaton nem szerzi meg a 20 pontot (és ezért 0 pontot hoz), egyetlen további lehetősége lesz:

($*$) A vizsgaidőszak első hetében egy ún. gyakorlati javítóvizsga-tesztlapon 0 vagy 20 pontot szerezhet. A gyakorlati javítóvizsga-tesztlap **könnyebb**, mint a szokásos vizsgateszt!

A fenti ($*$) lehetőség nem számít vizsgának, az ETR-ben nem kell sőt nem is szabad jelentkezni rá! (Aki mégis jelentkezik, az rosszabbul jár, mert nem vizsgázhat, és ”nem jelent meg” bejegyzést kap.)

A fenti $(*)$ lehetőség nem számít vizsgának, az ETR-ben nem kell sőt nem is szabad jelentkezni rá! (Aki mégis jelentkezik, az rosszabbul jár, mert nem vizsgázhat, és "nem jelent meg" bejegyzést kap.)

Aki sikeres vizsga után újabb vizsgát tesz, a vizsgalap tetején kérheti, hogy ne az eddigi hozott pontszámát, hanem ahelyett az **előző vizsgán elért mínusz 10 pontot** tekintsük hozott pontszámnak.

A tantárggyal kapcsolatos tudnivalók (az eddig elmondottak is) a honlapomon elérhetők:

A tantárggyal kapcsolatos tudnivalók (az eddig elmondottak is) a honlapomon elérhetők:

Az idén is **lila** szín jelzi az ilyen-olyan kiegészítéseket, érdekességeket, amelyeket a vizsgán nem kérek számon. Ezen lila megjegyzések egy része nagyban könnyíti a „normál szöveg” megértését.

Pl. most az első alkalommal érdekes kérdés lehet, hogy miről szól ez a tantárgy.

Pl. most az első alkalommal érdekes kérdés lehet, hogy miről szól ez a tantárgy. A tematika az alábbi:

Pl. most az első alkalommal érdekes kérdés lehet, hogy miről szól ez a tantárgy. A tematika az alábbi: Összeszámlálási alapfeladatok, szitaformula, binomiális tétel.

Pl. most az első alkalommal érdekes kérdés lehet, hogy miről szól ez a tantárgy. A tematika az alábbi: Összeszámlálási alapfeladatok, szitaformula, binomiális tétel. Számelmélet: oszthatóság, euklideszi algoritmus, prímfelbontás, lineáris diofantoszi egyenletek, kongruenciák, Euler és Fermat tételei.

Pl. most az első alkalommal érdekes kérdés lehet, hogy miről szól ez a tantárgy. A tematika az alábbi: Összeszámlálási alapfeladatok, szitaformula, binomiális tétel. Számelmélet: oszthatóság, euklideszi algoritmus, prímfelbontás, lineáris diofantoszi egyenletek, kongruenciák, Euler és Fermat tételei. Gráfok: fák, páros gráfok; a gráfelmélet elemei.

Pl. most az első alkalommal érdekes kérdés lehet, hogy miről szól ez a tantárgy. A tematika az alábbi: Összeszámlálási alapfeladatok, szitaformula, binomiális tétel. Számelmélet: oszthatóság, euklideszi algoritmus, prímfelbontás, lineáris diofantoszi egyenletek, kongruenciák, Euler és Fermat tételei. Gráfok: fák, páros gráfok; a gráfelmélet elemei. Absztrakt algebrai alapfogalmak: algebrai struktúrák és konstrukciók, homomorfiatétel. Félcsoport, csoport, Lagrange-tétel.

Elemi kombinatorika
(összeszámlálási feladatok)

Mielőtt bármilyen számítógépes programot készítünk, érdemes megsaccolni, hogy a programozásra kerülő algoritmus esetén mennyi idő alatt fut majd le.

Elemi kombinatorika

(összeszámlálási feladatok)

Mielőtt bármilyen számítógépes programot készítünk, érdemes megsaccolni, hogy a programozásra kerülő algoritmus esetén mennyi idő alatt fut majd le. Ez elsősorban a végrehajtandó lépések számától függ, azaz — végsősoron — attól, hogy bizonyos esetekből hány darab van, azaz bizonyos véges halmaznak mekkora az elemszáma.

Elemi kombinatorika
(összeszámlálási feladatok)

Mielőtt bármilyen számítógépes programot készítünk, érdemes megsaccolni, hogy a programozásra kerülő algoritmus esetén mennyi idő alatt fut majd le. Ez elsősorban a végrehajtandó lépések számától függ, azaz — végsősoron — attól, hogy bizonyos esetekből hány darab van, azaz bizonyos véges halmaznak mekkora az elemszáma. A kombinatorika célja bizonyos adott véges halmazok elemszámának meghatározása.

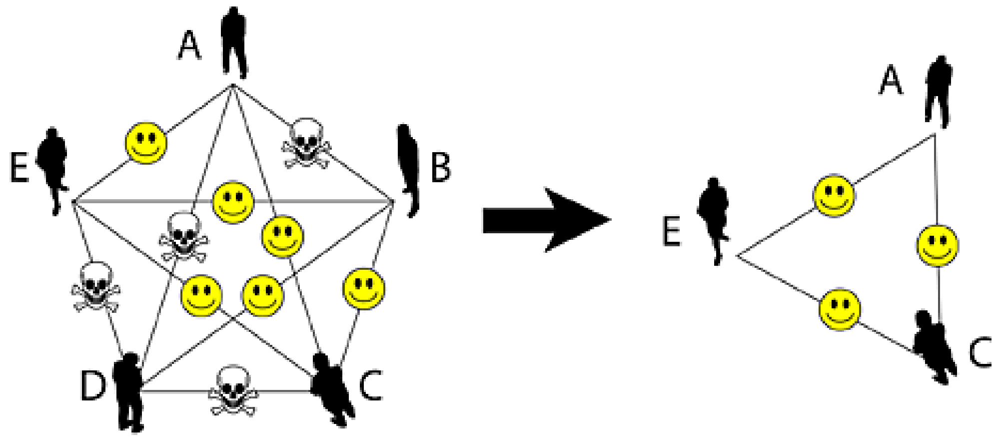
1, példa: PARTISZERVEZÉS:

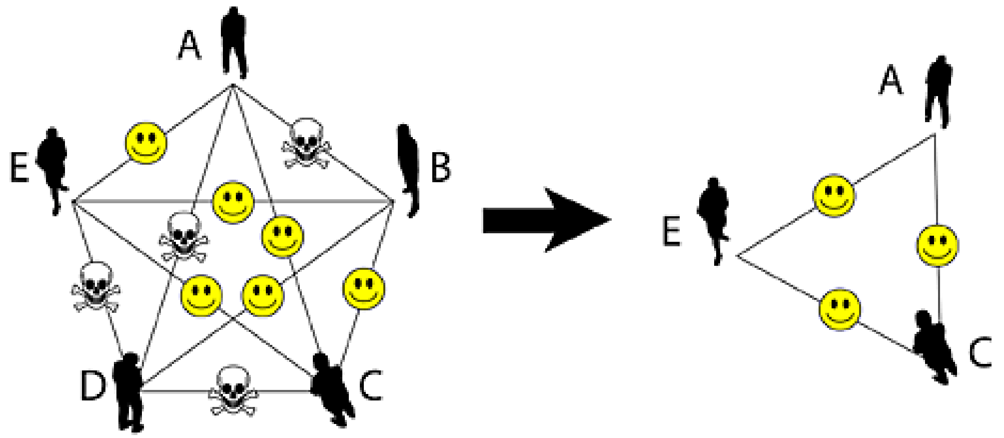
1, példa: PARTISZERVEZÉS: A — mondjuk — 300-fős informatikus évfolyam egyik tagja bejelenti: estélyt ad, amelyre 150 évfolyamtársát hívja meg (mert csak ennyien férnek el).

1, példa: PARTISZERVEZÉS: A — mondjuk — 300-fős informatikus évfolyam egyik tagja bejelenti: estélyt ad, amelyre 150 évfolyamtársát hívja meg (mert csak ennyien férnek el). Hogy jó legyen a hangulat, csak olyanokat hív meg, akik egymással jó viszonyban vannak.

1, példa: PARTISZERVEZÉS: A — mondjuk — 300-fős informatikus évfolyam egyik tagja bejelenti: estélyt ad, amelyre 150 évfolyamtársát hívja meg (mert csak ennyien férnek el). Hogy jó legyen a hangulat, csak olyanokat hív meg, akik egymással jó viszonyban vannak. Ezért felméri, hogy ki kivel van jó viszonyban, azaz meghatározza a „jó viszonyban van” szimmetrikus relációt.

1, példa: PARTISZERVEZÉS: A — mondjuk — 300-fős informatikus évfolyam egyik tagja bejelenti: estélyt ad, amelyre 150 évfolyamtársát hívja meg (mert csak ennyien férnek el). Hogy jó legyen a hangulat, csak olyanokat hív meg, akik egymással jó viszonyban vannak. Ezért felméri, hogy ki kivel van jó viszonyban, azaz meghatározza a „jó viszonyban van" szimmetrikus relációt. Íme egy illusztráció (ahol persze 300 helyett 5, 150 helyett pedig 3 szerepel):


A
B
C
D
E
A
E
C



Majd — a terv szerint — egy programra bízza a meghívandók listájának összellítását. Helyes ez a terv?

Ez attól függ, hogy

Ez attól függ, hogy

(1) van-a valamiféle jó algoritmusunk a probléma megoldására,

Ez attól függ, hogy

(1) van-a valamiféle jó algoritmusunk a probléma megoldására,

és ha nincs, akkor

Ez attól függ, hogy

(1) van-a valamiféle jó algoritmusunk a probléma megoldására,

és ha nincs, akkor

(2) Hányféleképpen lehet kiválasztani 150 évfolyamtársat, azaz hány esetet kell — természetesen programmal — végigvizsgálni.

(

Ez attól függ, hogy

(1) van-a valamiféle jó algoritmusunk a probléma megoldására,

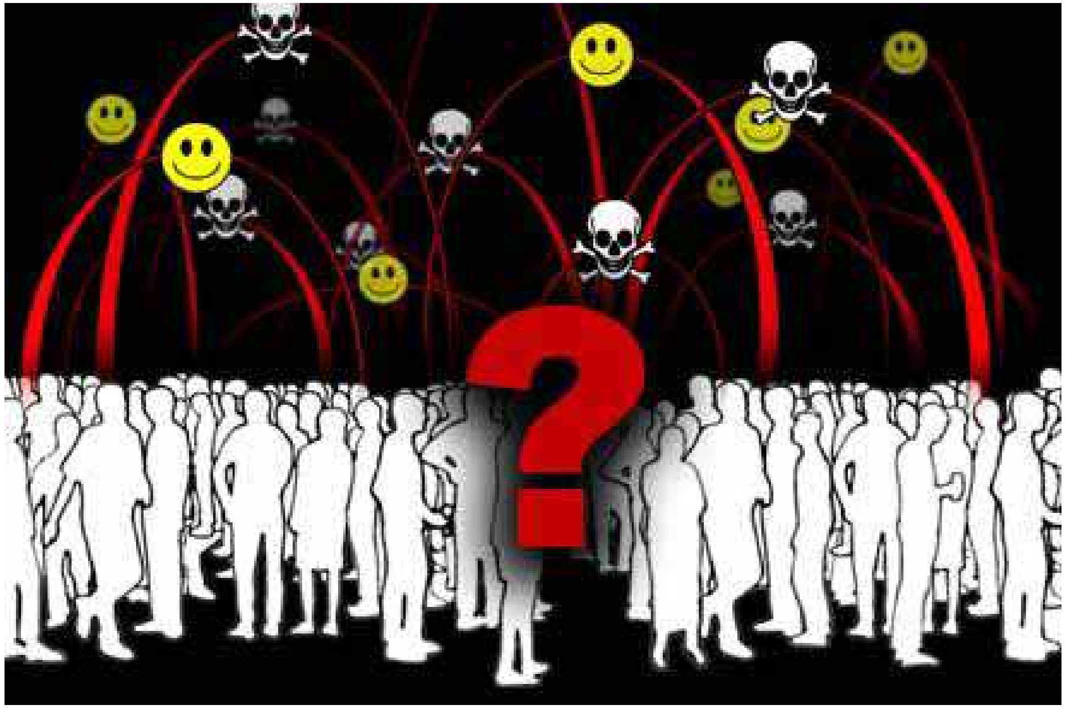
és ha nincs, akkor

(2) Hányféleképpen lehet kiválasztani 150 évfolyamtársat, azaz hány esetet kell — természetesen programmal — végigvizsgálni.

(Kissé előreszaladva az anyagban:

$$93759702772827452793193754439064084879232655700081358920472352712975170021839591675861424 \approx$$

$\approx 9 \cdot 10^{88}$ eset van.)



2. példa: RENDEZÉS: Az adatok begyűjtése után a 300-fős évfolyamot rendezzük az „anyja neve” mező szerint. Itt (az anyagban szintén előreszaladva, továbbá feltéve, hogy a mondott mezők páronként különböznek) a lehetséges esetek száma $3,06057512216440636035370461297 2 \cdot 10^{614}$, tehát jóval több, mint az előző példában.

Ennek ellenére a második példa esetén semmi gond, hiszen

2. példa: RENDEZÉS: Az adatok begyűjtése után a 300-fős évfolyamot rendezzük az „anyja neve” mező szerint. Itt (az anyagban szintén előreszaladva, továbbá feltéve, hogy a mondott mezők páronként különböznek) a lehetséges esetek száma $3,0605751221644063603537046129 72 \cdot 10^{614}$, tehát jóval több, mint az előző példában.

Ennek ellenére a második példa esetén semmi gond, hiszen ismeretes, hogy van jó rendezési algoritmus, amelyik - n adat esetén konst $\cdot\, n \cdot \ln n$ idő alatt lefut. Mivel most $300 \cdot \ln 300 \approx 1711$, egy másodperc se kell a probléma megoldásához.

Bár a partiszervezésnél az esetek száma jóval kevesebb — csupán $9 \cdot 10^{88}$ szemben a $3 \cdot 10^{614}$-vel —, Bár a partiszervezésnél az esetek száma jóval kevesebb — csupán $9 \cdot 10^{88}$ szemben a $3 \cdot 10^{614}$-vel —, jó algoritmust nem ismerünk. A $9 \cdot 10^{88}$ se kevés, ennyi esetet egy mai számítógéppel a Naprendszer élettartama alatt sem lehetne felsorolni, Bár a partiszervezésnél az esetek száma jóval kevesebb — csupán $9 \cdot 10^{88}$ szemben a $3 \cdot 10^{614}$-vel —, jó algoritmust nem ismerünk. A $9 \cdot 10^{88}$ se kevés, ennyi esetet egy mai számítógéppel a Naprendszer élettartama alatt sem lehetne felsorolni, ezért korai lenne a program megírásába belefogni.

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

http://plus.maths.org/issue24/features/budd/

(A „Problem 1: P versus NP" majd a „The party problem" sorig kell legördíteni.)

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

http://plus.maths.org/issue24/features/budd/

(A „Problem 1: P versus NP” majd a „The party problem” sorig kell legördíteni.) Itt jegyzem meg, hogy aki meg tudja válaszolni azt a kérdést, hogy van-e alkalmas program a partiszervezésre, annak a fent említett honlap (tehát nem én!)

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

http://plus.maths.org/issue24/features/budd/

(A „Problem 1: P versus NP” majd a „The party problem” sorig kell legördíteni.) Itt jegyzem meg, hogy aki meg tudja válaszolni azt a kérdést, hogy van-e alkalmas program a partiszervezésre, annak a fent említett honlap (tehát nem én!)

egymillió

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

http://plus.maths.org/issue24/features/budd/

(A „Problem 1: P versus NP" majd a „The party problem" sorig kell legördíteni.) Itt jegyzem meg, hogy aki meg tudja válaszolni azt a kérdést, hogy van-e alkalmas program a partiszervezésre, annak a fent említett honlap (tehát nem én!)

egymillió dollár

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

http://plus.maths.org/issue24/features/budd/

(A „Problem 1: P versus NP” majd a „The party problem” sorig kell legördíteni.) Itt jegyzem meg, hogy aki meg tudja válaszolni azt a kérdést, hogy van-e alkalmas program a partiszervezésre, annak a fent említett honlap (tehát nem én!)

egymillió dollár

jutalmat ígér (Clay Institute).

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

http://plus.maths.org/issue24/features/budd/

(A „Problem 1: P versus NP” majd a „The party problem” sorig kell legördíteni.) Itt jegyzem meg, hogy aki meg tudja válaszolni azt a kérdést, hogy van-e alkalmas program a partiszervezésre, annak a fent említett honlap (tehát nem én!)

egymillió dollár

jutalmat ígér (Clay Institute). A $P = NP$? a matematika és informatika híres megoldatlan problémája —

Láttuk, hogy az esetek megszámolásának szoros köze van az informatikához, a programtervezéshez. A partiszervezős példát az alábbi honlapon találtam:

http://plus.maths.org/issue24/features/budd/

(A „Problem 1: P versus NP" majd a „The party problem" sorig kell legördíteni.) Itt jegyzem meg, hogy aki meg tudja válaszolni azt a kérdést, hogy van-e alkalmas program a partiszervezésre, annak a fent említett honlap (tehát nem én!)

egymillió dollár

jutalmat ígér (Clay Institute). A $P = NP$? a matematika és informatika híres megoldatlan problémája — az érdeklődőknek az említett honlapot vagy valamely későbbi, ezzel részletesen foglalkozó tantárgyat ajánlom.

Megjegyzendő, hogy számos valószínűségszámítási kérdés is lényegében kombinatorikai kérdés. Például

Megjegyzendő, hogy számos valószínűségszámítási kérdés is lényegében kombinatorikai kérdés. Például érdemes-e egy az egyben arra fogadni, hogy az autóbusz

Megjegyzendő, hogy számos valószínűségszámítási kérdés is lényegében kombinatorikai kérdés. Például érdemes-e egy az egyben arra fogadni, hogy az autóbusz 30 (ismeretlen) utasa között van két olyan, akinek az év azonos hónapja azonos napján van a születésnapja; illetve ha egy az egyben nem érdemes, akkor milyen arányban érdemes?

A kombinatorikai feladat gyakran úgy kezdődik, hogy hányféleképpen lehet valamiket valahonnan kiválasztani, hány eset van, hány lehetőség, hány „variáns van” .

A kombinatorikai feladat gyakran úgy kezdődik, hogy hányféleképpen lehet valamiket valahonnan kiválasztani, hány eset van, hány lehetőség, hány „variáns van”. Pl. hányféleképpen lehet az ötös lottót kitölteni, stb.

A kombinatorikai feladat gyakran úgy kezdődik, hogy hányféleképpen lehet valamiket valahonnan kiválasztani, hány eset van, hány lehetőség, hány „variáns van”. Pl. hányféleképpen lehet az ötös lottót kitölteni, stb. Persze fogalmazhatunk absztraktabbul, a halmazok nyelvén, és akkor a feladat úgy szól, hogy hány eleme van egy valahogyan megadott véges halmaznak.

A kombinatorikai feladat gyakran úgy kezdődik, hogy hányféleképpen lehet valamiket valahonnan kiválasztani, hány eset van, hány lehetőség, hány „variáns van". Pl. hányféleképpen lehet az ötös lottót kitölteni, stb. Persze fogalmazhatunk absztraktabbul, a halmazok nyelvén, és akkor a feladat úgy szól, hogy hány eleme van egy valahogyan megadott véges halmaznak. Az ötös lottó (ahol 90 számból kell ötöt eltalálni) esetén az említett feladat így is fogalmazható: hány ötelemű részhalmaza van az $\{1, 2, \ldots, 90\}$ halmaznak.

A kombinatorikai feladat gyakran úgy kezdődik, hogy hányféleképpen lehet valamiket valahonnan kiválasztani, hány eset van, hány lehetőség, hány „variáns van". Pl. hányféleképpen lehet az ötös lottót kitölteni, stb. Persze fogalmazhatunk absztraktabbul, a halmazok nyelvén, és akkor a feladat úgy szól, hogy hány eleme van egy valahogyan megadott véges halmaznak. Az ötös lottó (ahol 90 számból kell ötöt eltalálni) esetén az említett feladat így is fogalmazható: hány ötelemű részhalmaza van az $\{1, 2, \ldots, 90\}$ halmaznak.

Számos kombinatorikai feladat megoldható az

A kombinatorikai feladat gyakran úgy kezdődik, hogy hányféleképpen lehet valamiket valahonnan kiválasztani, hány eset van, hány lehetőség, hány „variáns van”. Pl. hányféleképpen lehet az ötös lottót kitölteni, stb. Persze fogalmazhatunk absztraktabbul, a halmazok nyelvén, és akkor a feladat úgy szól, hogy hány eleme van egy valahogyan megadott véges halmaznak. Az ötös lottó (ahol 90 számból kell ötöt eltalálni) esetén az említett feladat így is fogalmazható: hány ötelemű részhalmaza van az $\{1, 2, \ldots, 90\}$ halmaznak.

Számos kombinatorikai feladat megoldható az **összegezési szabály** és a **szorzási szabály** felhasználásával, azaz elméleti tudás nélkül, a „józan eszünkre” támaszkodva.

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$.

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$. Azaz ha a megszámolandó esetek halmazát két diszjunkt halmaz uniójára tudjuk bontani, akkor elég ezen két halmaz elemeit megszámolni, és a kapott két számot összeadni. (Pl.

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$. Azaz ha a megszámolandó esetek halmazát két diszjunkt halmaz uniójára tudjuk bontani, akkor elég ezen két halmaz elemeit megszámolni, és a kapott két számot összeadni. (Pl. a tanteremben levő emberek száma

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$. Azaz ha a megszámolandó esetek halmazát két diszjunkt halmaz uniójára tudjuk bontani, akkor elég ezen két halmaz elemeit megszámolni, és a kapott két számot összeadni. (Pl. a tanteremben levő emberek száma = a tanteremben levő férfiak száma + a tanteremben levő nők száma.)

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$. Azaz ha a megszámolandó esetek halmazát két diszjunkt halmaz uniójára tudjuk bontani, akkor elég ezen két halmaz elemeit megszámolni, és a kapott két számot összeadni. (Pl. a tanteremben levő emberek száma = a tanteremben levő férfiak száma + a tanteremben levő nők száma.)

Az összadási szabály meglehetősen triviális észrevétel.

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$. Azaz ha a megszámolandó esetek halmazát két diszjunkt halmaz uniójára tudjuk bontani, akkor elég ezen két halmaz elemeit megszámolni, és a kapott két számot összeadni. (Pl. a tanteremben levő emberek száma = a tanteremben levő férfiak száma + a tanteremben levő nők száma.)

Az összadási szabály meglehetősen triviális észrevétel. Nyilván több tagú összegre is érvényes:

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$. Azaz ha a megszámolandó esetek halmazát két diszjunkt halmaz uniójára tudjuk bontani, akkor elég ezen két halmaz elemeit megszámolni, és a kapott két számot összeadni. (Pl. a tanteremben levő emberek száma = a tanteremben levő férfiak száma + a tanteremben levő nők száma.)

Az összadási szabály meglehetősen triviális észrevétel. Nyilván több tagú összegre is érvényes: ha $\mathcal{C}$ osztályozás egy véges A halmazon, akkor

$$|A| =$$

Az **összegzési szabály** annak felel meg, hogy $A \cap B = \emptyset$ esetén $|A \cup B| = |A| + |B|$. Azaz ha a megszámolandó esetek halmazát két diszjunkt halmaz uniójára tudjuk bontani, akkor elég ezen két halmaz elemeit megszámolni, és a kapott két számot összeadni. (Pl. a tanteremben levő emberek száma = a tanteremben levő férfiak száma + a tanteremben levő nők száma.)

Az összadási szabály meglehetősen triviális észrevétel. Nyilván több tagú összegre is érvényes: ha $\mathcal{C}$ osztályozás egy véges A halmazon, akkor

$$|A| = \sum_{X \in \mathcal{C}} |X|.$$

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy**

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.)

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki.

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. B

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. Bá

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. Bár

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. Bárhogy is választottuk, a második betű 26 féleképpen választható.

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. Bárhogy is választottuk, a második betű 26 féleképpen választható. Tehát a lehetőségek száma, azaz a kétbetűs szavak száma

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. Bárhogy is választottuk, a második betű 26 féleképpen választható. Tehát a lehetőségek száma, azaz a kétbetűs szavak száma $26 \cdot 26 = 26^2$.

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. Bárhogy is választottuk, a második betű 26 féleképpen választható. Tehát a lehetőségek száma, azaz a kétbetűs szavak száma $26 \cdot 26 = 26^2$.

A fenti példa túlságosan speciális, hiszen a második betűt az első betűtől függetlenül választjuk.

A **szorzási szabály** akkor alkalmazható, ha (a, b) elempárokat kell kiválasztanunk (valahonnan), és **bárhogy** is választottuk ki az a-t, ugyanannyiféleképpen választhatjuk ki a b-t az a mellé.

Példa: hány kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből?

A kétbetűs szavak felfoghatók a két betűből alkotott rendezett párnak. (Vagy kéttagú sorozatnak.) Az első betűt (azaz az pár első tagját) 26-féleképpen választhatjuk ki. Bárhogy is választottuk, a második betű 26 féleképpen választható. Tehát a lehetőségek száma, azaz a kétbetűs szavak száma $26 \cdot 26 = 26^2$.

A fenti példa túlságosan speciális, hiszen a második betűt az első betűtől függetlenül választjuk. Nézzünk egy tanulságosabbat.

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk.

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **f**

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **fü**

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **füg**

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ**

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ** az első betűtől!

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ** az első betűtől! Ha „a” az első betű, akkor folytathatjuk „b”-vel, de ha

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ** az első betűtől! Ha „a” az első betű, akkor folytathatjuk „b”-vel, de ha „b” az első betű, akkor nem folytathatjuk „b”-vel! De ennek ellenére a szorzási szabály alkalmazható, hiszen

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ** az első betűtől! Ha „a” az első betű, akkor folytathatjuk „b”-vel, de ha „b” az első betű, akkor nem folytathatjuk „b”-vel! De ennek ellenére a szorzási szabály alkalmazható, hiszen nem az a feltétel, hogy a második betű (második komponens) ne függjön az elsőtől,

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ** az első betűtől! Ha „a” az első betű, akkor folytathatjuk „b”-vel, de ha „b” az első betű, akkor nem folytathatjuk „b”-vel! De ennek ellenére a szorzási szabály alkalmazható, hiszen nem az a feltétel, hogy a második betű (második komponens) ne függjön az elsőtől, hanem csak azt követeljük meg, hogy a második komponensre adódó választási lehetőségek

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ** az első betűtől! Ha „a” az első betű, akkor folytathatjuk „b”-vel, de ha „b” az első betű, akkor nem folytathatjuk „b”-vel! De ennek ellenére a szorzási szabály alkalmazható, hiszen nem az a feltétel, hogy a második betű (második komponens) ne függjön az elsőtől, hanem csak azt követeljük meg, hogy a második komponensre adódó választási lehetőségek **száma**

Példa: hány olyan kétbetűs szó készíthető a (huszonhat betűs) angol ábécéből, amelyik két *különböző* betűből áll?

Az első betűt 26-féleképpen választhatjuk. A második betű választása **függ** az első betűtől! Ha „a” az első betű, akkor folytathatjuk „b”-vel, de ha „b” az első betű, akkor nem folytathatjuk „b”-vel! De ennek ellenére a szorzási szabály alkalmazható, hiszen nem az a feltétel, hogy a második betű (második komponens) ne függjön az elsőtől, hanem csak azt követeljük meg, hogy a második komponensre adódó választási lehetőségek **száma** **ne függjön** attól, hogy hogyan választottuk ki az elsőt.

Esetünkben — bármi is az első betű — a másodikat 25-féleképpen választhatjuk. Ezért az esetek száma, azaz a két különböző betűből álló szavak száma

Esetünkben — bármi is az első betű — a másodikat 25-féleképpen választhatjuk. Ezért az esetek száma, azaz a két különböző betűből álló szavak száma $26 \cdot 25$.

Esetünkben — bármi is az első betű — a másodikat 25-féleképpen választhatjuk. Ezért az esetek száma, azaz a két különböző betűből álló szavak száma $26 \cdot 25$.

Bármilyen triviálisnak is tűnnek a fentiek, azért időzünk az összadás és a szorzás kérdésénél annyit, mert a kombinatorikai feladatoknál az egyik fő kérdés (és a hibázás egyik lehetősége) az, hogy mikor kell összeadni és mikor kell összeszorozni a részeredményeket.

A két különböző betűből álló szavak az alábbi módon is megszámolhatók.

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

$$B_{\mathsf{a}} = \{\text{a-val kezdődő } A\text{-beli szavak}\},$$

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

$$B_{\mathsf{a}} = \{\text{a-val kezdődő } A\text{-beli szavak}\},$$
$$B_{\mathsf{b}} = \{\text{b-vel kezdődő } A\text{-beli szavak}\},$$

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

$$B_{\mathsf{a}} = \{\text{a-val kezdődő } A\text{-beli szavak}\},$$
$$B_{\mathsf{b}} = \{\text{b-vel kezdődő } A\text{-beli szavak}\},$$
$$\dots$$
$$B_{\mathsf{z}} = \{\text{z-vel kezdődő } A\text{-beli szavak}\}.$$

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

$$B_{\mathsf{a}} = \{\text{a-val kezdődő } A\text{-beli szavak}\},$$
$$B_{\mathsf{b}} = \{\text{b-vel kezdődő } A\text{-beli szavak}\},$$
$$\dots$$
$$B_{\mathsf{z}} = \{\text{z-vel kezdődő } A\text{-beli szavak}\}.$$

Ekkor $\mathcal{C} = \{B_{\mathsf{a}}, \dots, B_{\mathsf{z}}\}$ osztályozás az A halmazon,

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

$$B_{\mathsf{a}} = \{\text{a-val kezdődő } A\text{-beli szavak}\},$$
$$B_{\mathsf{b}} = \{\text{b-vel kezdődő } A\text{-beli szavak}\},$$
$$\dots$$
$$B_{\mathsf{z}} = \{\text{z-vel kezdődő } A\text{-beli szavak}\}.$$

Ekkor $\mathcal{C} = \{B_{\mathsf{a}}, \dots, B_{\mathsf{z}}\}$ osztályozás az A halmazon, ezért a többtagú (esetünkben 26-tagú) összegezési szabály szerint

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

$$B_{\mathsf{a}} = \{\text{a-val kezdődő } A\text{-beli szavak}\},$$
$$B_{\mathsf{b}} = \{\text{b-vel kezdődő } A\text{-beli szavak}\},$$
$$\dots$$
$$B_{\mathsf{z}} = \{\text{z-vel kezdődő } A\text{-beli szavak}\}.$$

Ekkor $\mathcal{C} = \{B_{\mathsf{a}}, \dots, B_{\mathsf{z}}\}$ osztályozás az A halmazon, ezért a többtagú (esetünkben 26-tagú) összegezési szabály szerint

$$|A| = |B_{\mathsf{a}}| + \cdots + |B_{\mathsf{z}}|.$$

Mármost $|B_{\mathsf{a}}| = |\{\text{„ab”}, \text{„ac”}, \dots, \text{„az”}\}| = 25$, és az összeg többi tagja is 25-elemű,

A két különböző betűből álló szavak az alábbi módon is megszámolhatók. A kétbetűs szavak A-val jelölt halmaza esetén tekintsük az alábbi részhalmazokat:

$$B_{\mathsf{a}} = \{\text{a-val kezdődő } A\text{-beli szavak}\},$$
$$B_{\mathsf{b}} = \{\text{b-vel kezdődő } A\text{-beli szavak}\},$$
$$\dots$$
$$B_{\mathsf{z}} = \{\text{z-vel kezdődő } A\text{-beli szavak}\}.$$

Ekkor $\mathcal{C} = \{B_{\mathsf{a}}, \dots, B_{\mathsf{z}}\}$ osztályozás az A halmazon, ezért a többtagú (esetünkben 26-tagú) összegezési szabály szerint

$$|A| = |B_{\mathsf{a}}| + \cdots + |B_{\mathsf{z}}|.$$

Mármost $|B_{\mathsf{a}}| = |\{\text{„ab”}, \text{„ac”}, \dots, \text{„az”}\}| = 25$, és az összeg többi tagja is 25-elemű, tehát az összeg értéke $26 \cdot 25$.

Feladat: Hányféleképpen lehet a dominókészletből két (különböző) dominót kiválasztani? (A dominókészletben 45 dominó van.

Feladat: Hányféleképpen lehet a dominókészletből két (különböző) dominót kiválasztani? (A dominókészletben 45 dominó van.)

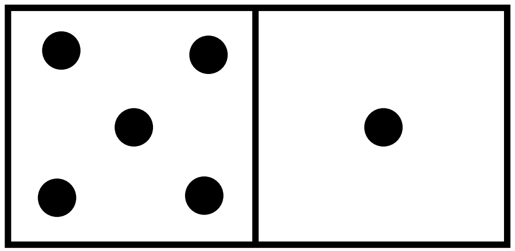
Megoldás: Mindenekelőtt pontosítani kell a feladatot, mert a jelen megfogalmazás **nem világos**.

Feladat: Hányféleképpen lehet a dominókészletből két (különböző) dominót kiválasztani? (A dominókészletben 45 dominó van.)

Megoldás: Mindenekelőtt pontosítani kell a feladatot, mert a jelen megfogalmazás **nem világos**. Kérdéses, hogy mit értünk két dominó kiválasztásán, **számít-e a sorrend?** Oldjuk meg a feladatot így is és úgy is!

Feladat: Hányféleképpen lehet a dominókészletből két (különböző) dominót kiválasztani? (A dominókészletben 45 dominó van.)

Megoldás: Mindenekelőtt pontosítani kell a feladatot, mert a jelen megfogalmazás **nem világos**. Kérdéses, hogy mit értünk két dominó kiválasztásán, **számít-e a sorrend?** Oldjuk meg a feladatot így is és úgy is! A dominókat 00, 88, 51 (ld. alábbi ábra), stb. jelöli.



Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével'' dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért:

Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével” dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért: ha az (időrendi) sorrend számít, akkor a két különböző dominót $45 \cdot 44$ féleképpen választhatjuk ki.

Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével'' dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért: ha az (időrendi) sorrend számít, akkor a két különböző dominót $45 \cdot 44$ féleképpen választhatjuk ki.

Ha a sorrend nem számít:

Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével" dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért: ha az (időrendi) sorrend számít, akkor a két különböző dominót $45 \cdot 44$ féleképpen választhatjuk ki.

Ha a sorrend nem számít: ez az előzőre vezethető vissza.

Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével” dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért: ha az (időrendi) sorrend számít, akkor a két különböző dominót $45 \cdot 44$ féleképpen választhatjuk ki.

Ha a sorrend nem számít: ez az előzőre vezethető vissza. Most bármely dominóválasztás, mondjuk a $\{00, 62\}$ választása — ha a sorrend számítana — kétféleképpen is történhetne:

Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével” dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért: ha az (időrendi) sorrend számít, akkor a két különböző dominót $45 \cdot 44$ féleképpen választhatjuk ki.

Ha a sorrend nem számít: ez az előzőre vezethető vissza. Most bármely dominóválasztás, mondjuk a $\{00, 62\}$ választása — ha a sorrend számítana — kétféleképpen is történhetne: a 00, 62 sorrendben is és a 62, 00 sorrendben is.

Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével" dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért: ha az (időrendi) sorrend számít, akkor a két különböző dominót $45 \cdot 44$ féleképpen választhatjuk ki.

Ha a sorrend nem számít: ez az előzőre vezethető vissza. Most bármely dominóválasztás, mondjuk a $\{00, 62\}$ választása — ha a sorrend számítana — kétféleképpen is történhetne: a 00, 62 sorrendben is és a 62, 00 sorrendben is. Ezért az előbb kapott eredményt meg kell feleznünk, Ha a sorrend számít, akkor a feladat lényegében azonos az előzővel, csak most nem 26-, hanem 45-betűs „ábécével'' dolgozunk. Az első dominót 45 féleképpen választhatjuk ki. Bárhogy is választottuk ki az elsőt, a második választására 44 lehetőség van. Ezért: ha az (időrendi) sorrend számít, akkor a két különböző dominót $45 \cdot 44$ féleképpen választhatjuk ki.

Ha a sorrend nem számít: ez az előzőre vezethető vissza. Most bármely dominóválasztás, mondjuk a $\{00, 62\}$ választása — ha a sorrend számítana — kétféleképpen is történhetne: a 00, 62 sorrendben is és a 62, 00 sorrendben is. Ezért az előbb kapott eredményt meg kell feleznünk, azaz most $\frac{45 \cdot 44}{2} = 990$ az eredmény.

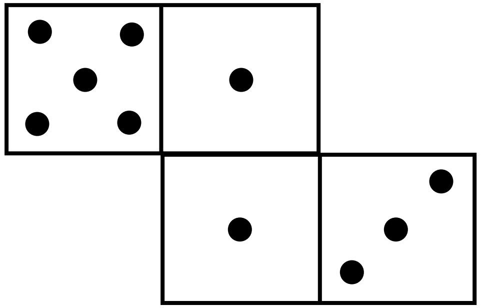
Most lássunk egy olyan feladatot, ahol az összegezési szabály is és a szorzási szabály is szerepet játszik.

Most lássunk egy olyan feladatot, ahol az összegezési szabály is és a szorzási szabály is szerepet játszik.

Feladat: Hányféleképpen húzhatunk ki a dominókészletből két **illeszkedő** dominót, ha sorrendjük nem számít?

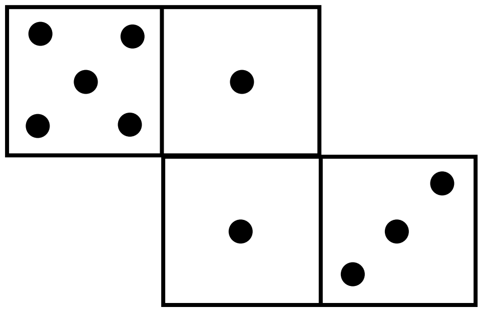
Most lássunk egy olyan feladatot, ahol az összegezési szabály is és a szorzási szabály is szerepet játszik.

Feladat: Hányféleképpen húzhatunk ki a dominókészletből két **illeszkedő** dominót, ha sorrendjük nem számít?



Most lássunk egy olyan feladatot, ahol az összegezési szabály is és a szorzási szabály is szerepet játszik.

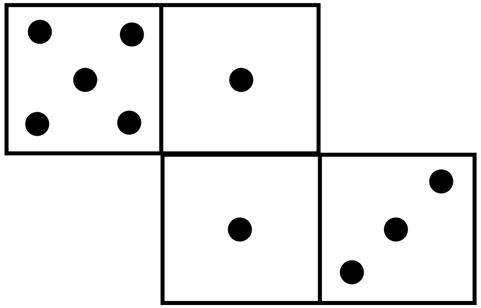
Feladat: Hányféleképpen húzhatunk ki a dominókészletből két **illeszkedő** dominót, ha sorrendjük nem számít?



Megoldás:

Most lássunk egy olyan feladatot, ahol az összegezési szabály is és a szorzási szabály is szerepet játszik.

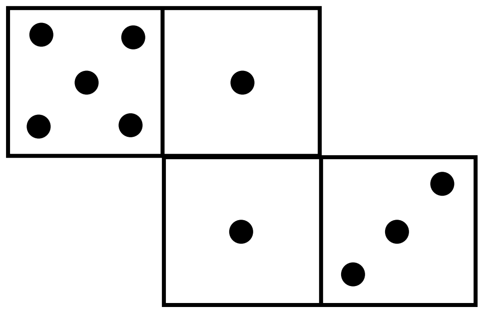
Feladat: Hányféleképpen húzhatunk ki a dominókészletből két **illeszkedő** dominót, ha sorrendjük nem számít?



Megoldás: Két dominót, mondjuk az ab és a cd dominót (ahol $a, b, c, d \in \{0, 1, \ldots, 8\}$) akkor mondunk illeszkedőnek,

Most lássunk egy olyan feladatot, ahol az összegezési szabály is és a szorzási szabály is szerepet játszik.

Feladat: Hányféleképpen húzhatunk ki a dominókészletből két **illeszkedő** dominót, ha sorrendjük nem számít?



Megoldás: Két dominót, mondjuk az ab és a cd dominót (ahol $a, b, c, d \in \{0, 1, \ldots, 8\}$) akkor mondunk illeszkedőnek, ha $\{a, b\} \cap \{c, d\} \neq \emptyset$. Pl. az ábrán látható 51 és 31 dominók illeszkedők.

A vizsga feltétele: 20 pont a gyakorlaton!

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük,

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük, majd az így kapott eredményt elosztjuk 2-vel.

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük, majd az így kapott eredményt elosztjuk 2-vel.

A készletben 45 dominó van. Az elsőt 45 féleképpen választhatjuk ki.

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük, majd az így kapott eredményt elosztjuk 2-vel.

A készletben 45 dominó van. Az elsőt 45 féleképpen választhatjuk ki. De az, hogy hányféleképpen választhatunk egy hozzá illeszkedő másodikat,

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük, majd az így kapott ereményt elosztjuk 2-vel.

A készletben 45 dominó van. Az elsőt 45 féleképpen választhatjuk ki. De az, hogy hányféleképpen választhatunk egy hozzá illeszkedő másodikat, nyilván

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük, majd az így kapott ereményt elosztjuk 2-vel.

A készletben 45 dominó van. Az elsőt 45 féleképpen választhatjuk ki. De az, hogy hányféleképpen választhatunk egy hozzá illeszkedő másodikat, nyilván **füg**

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük, majd az így kapott ereményt elosztjuk 2-vel.

A készletben 45 dominó van. Az elsőt 45 féleképpen választhatjuk ki. De az, hogy hányféleképpen választhatunk egy hozzá illeszkedő másodikat, nyilván **függ**

Mivel két adott dominó kétféleképpen rakható sorba, ezért — az előző feladathoz hasonlóan — most is úgy célszerű a feladatot megoldanunk, hogy először a sorrendet is figyelembe vesszük, majd az így kapott ereményt elosztjuk 2-vel.

A készletben 45 dominó van. Az elsőt 45 féleképpen választhatjuk ki. De az, hogy hányféleképpen választhatunk egy hozzá illeszkedő másodikat, nyilván **függ** az elsőnek kiválasztottól, hiszen a „dupla" dominóhoz kevesebb dominó illeszkedik, mint a nem duplához.

Állapodjunk meg abban, hogy az ab dominó esetén $a \geq b$ (tehát a nagyobb számot írjuk előre).

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó.

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik.

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Második eset: elsőre nem dupla dominót húzunk

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Második eset: elsőre nem dupla dominót húzunk — ezt $45 - 9 =$ 36-féleképpen tehetjük meg.

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, ..., 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, ..., 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Második eset: elsőre nem dupla dominót húzunk — ezt $45 - 9 =$ 36-féleképpen tehetjük meg. Ha mondjuk az 10 dominót húztuk, akkor a hozzá illeszkedő dominók: 00, 20, 30, ..., 80, továbbá

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Második eset: elsőre nem dupla dominót húzunk — ezt $45 - 9 = 36$-féleképpen tehetjük meg. Ha mondjuk az 10 dominót húztuk, akkor a hozzá illeszkedő dominók: 00, 20, 30, . . . , 80, továbbá 11, 21, . . . , 81,

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Második eset: elsőre nem dupla dominót húzunk — ezt $45 - 9 = 36$-féleképpen tehetjük meg. Ha mondjuk az 10 dominót húztuk, akkor a hozzá illeszkedő dominók: 00, 20, 30, . . . , 80, továbbá 11, 21, . . . , 81, tehát 16 darab dominó.

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, ..., 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, ..., 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Második eset: elsőre nem dupla dominót húzunk — ezt $45 - 9 = 36$-féleképpen tehetjük meg. Ha mondjuk az 10 dominót húztuk, akkor a hozzá illeszkedő dominók: 00, 20, 30, ..., 80, továbbá 11, 21, ..., 81, tehát 16 darab dominó. Nyilván más nem dupla dominóhoz is 16 dominó illeszkedik.

Első eset: az elsőnek húzott dominó dupla, pl. a 00 dominó. Ehhez csakis az 10, 20, . . . , 80 dominó illeszkedik, tehát nyolc darab. Ehhez hasonlóan más dupla dominóhoz is nyolc dominó illeszkedik. Tehát ha dupla dominóval kezdünk, akkor az első dominót kilencféleképpen választhatjuk (ugyanis ennyi a 00, 11, . . . , 88 dupladominók száma), és bárhogy választottuk az elsőt, hozzá nyolcféleképpen választhatjuk a másodikat. Tehát az első esetben a lehetőségek száma a szorzási szabály szerint $9 \cdot 8 = 72$.

Második eset: elsőre nem dupla dominót húzunk — ezt $45 - 9 = 36$-féleképpen tehetjük meg. Ha mondjuk az 10 dominót húztuk, akkor a hozzá illeszkedő dominók: 00, 20, 30, . . . , 80, továbbá 11, 21, . . . , 81, tehát 16 darab dominó. Nyilván más nem dupla dominóhoz is 16 dominó illeszkedik. A szorzási szabály szerint a második esethez $36 \cdot 16 = 576$ lehetőség tartozik.

Mivel minden lehetőség a fenti két eset közül pontosan az egyikhez tartozik, Mivel minden lehetőség a fenti két eset közül pontosan az egyikhez tartozik, az összegezési szabály szerint a kapott két számot össze kell adni:

Mivel minden lehetőség a fenti két eset közül pontosan az egyikhez tartozik, az összegezési szabály szerint a kapott két számot össze kell adni: $72 + 576 = 648$-féleképpen lehet két illeszkedő dominót kiválasztani, ha a sorrend számít.

Mivel minden lehetőség a fenti két eset közül pontosan az egyikhez tartozik, az összegezési szabály szerint a kapott két számot össze kell adni: $72 + 576 = 648$-féleképpen lehet két illeszkedő dominót kiválasztani, ha a sorrend számít. De most a sorrend nem számít, tehát az eredménye $648/2 = 324$.

Mivel minden lehetőség a fenti két eset közül pontosan az egyikhez tartozik, az összegezési szabály szerint a kapott két számot össze kell adni: $72 + 576 = 648$-féleképpen lehet két illeszkedő dominót kiválasztani, ha a sorrend számít. De most a sorrend nem számít, tehát az eredménye $648/2 = 324$.

Ha nincs túl sok eset, a lehetőségek szisztematikus végiggondolása akkor is segíthet. Erre két példát fogunk nézni.

Mivel minden lehetőség a fenti két eset közül pontosan az egyikhez tartozik, az összegezési szabály szerint a kapott két számot össze kell adni: $72 + 576 = 648$-féleképpen lehet két illeszkedő dominót kiválasztani, ha a sorrend számít. De most a sorrend nem számít, tehát az eredménye $648/2 = 324$.

Ha nincs túl sok eset, a lehetőségek szisztematikus végigondolása akkor is segíthet. Erre két példát fogunk nézni. Ezek nem igényelnek semmiféle új ismeretet, de az új ismeretek előtt célszerű foglalkozni velük.

Feladat: A háromszemélyes űrhajó kapitányi posztjára három jelentkező van: a_1, a_2, a_3.

Feladat: A háromszemélyes űrhajó kapitányi posztjára három jelentkező van: a_1, a_2, a_3. Fedélzeti mérnöknek ketten jelentkeznek: b_1, b_2,

Feladat: A háromszemélyes űrhajó kapitányi posztjára három jelentkező van: a_1, a_2, a_3. Fedélzeti mérnöknek ketten jelentkeznek: b_1, b_2, hajóorvosnak pedig hárman: c_1, c_2, c_3.

Feladat: A háromszemélyes űrhajó kapitányi posztjára három jelentkező van: a_1, a_2, a_3. Fedélzeti mérnöknek ketten jelentkeznek: b_1, b_2, hajóorvosnak pedig hárman: c_1, c_2, c_3. Tudjuk, hogy az alábbi párok ki nem állhatják egymást:

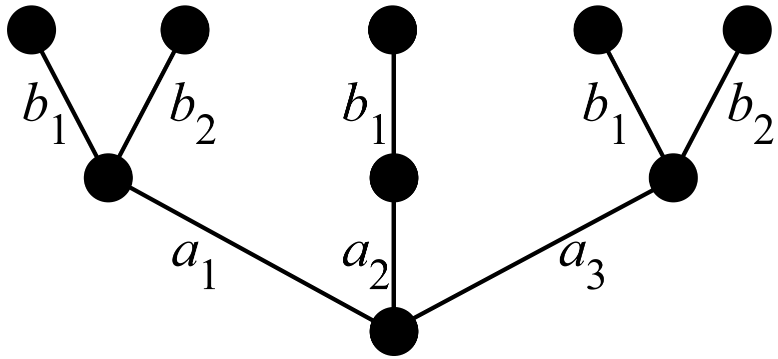
Feladat: A háromszemélyes űrhajó kapitányi posztjára három jelentkező van: a_1, a_2, a_3. Fedélzeti mérnöknek ketten jelentkeznek: b_1, b_2, hajóorvosnak pedig hárman: c_1, c_2, c_3. Tudjuk, hogy az alábbi párok ki nem állhatják egymást: (a_2, b_2), (a_1, c_3), (a_3, c_1), (b_2, c_3). Hányféleképpen állíthatjuk össze az űrhajó egy kapitányból, egy fedélzeti mérnökből és egy hajóorvosból álló legénységét, ha el akarjuk kerülni az előre látható súrlódásokat?

Feladat: A háromszemélyes űrhajó kapitányi posztjára három jelentkező van: a_1, a_2, a_3. Fedélzeti mérnöknek ketten jelentkeznek: b_1, b_2, hajóorvosnak pedig hárman: c_1, c_2, c_3. Tudjuk, hogy az alábbi párok ki nem állhatják egymást: (a_2, b_2), (a_1, c_3), (a_3, c_1), (b_2, c_3). Hányféleképpen állíthatjuk össze az űrhajó egy kapitányból, egy fedélzeti mérnökből és egy hajóorvosból álló legénységét, ha el akarjuk kerülni az előre látható súrlódásokat?

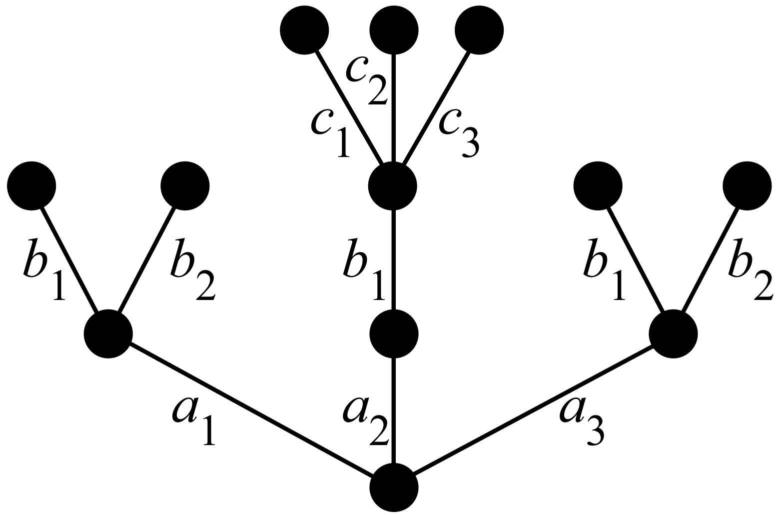
Megoldás: A lehetséges (a_i, b_j, c_k) elemhármasokat kell megszámolnunk.

Feladat: A háromszemélyes űrhajó kapitányi posztjára három jelentkező van: a_1, a_2, a_3. Fedélzeti mérnöknek ketten jelentkeznek: b_1, b_2, hajóorvosnak pedig hárman: c_1, c_2, c_3. Tudjuk, hogy az alábbi párok ki nem állhatják egymást: (a_2, b_2), (a_1, c_3), (a_3, c_1), (b_2, c_3). Hányféleképpen állíthatjuk össze az űrhajó egy kapitányból, egy fedélzeti mérnökből és egy hajóorvosból álló legénységét, ha el akarjuk kerülni az előre látható súrlódásokat?

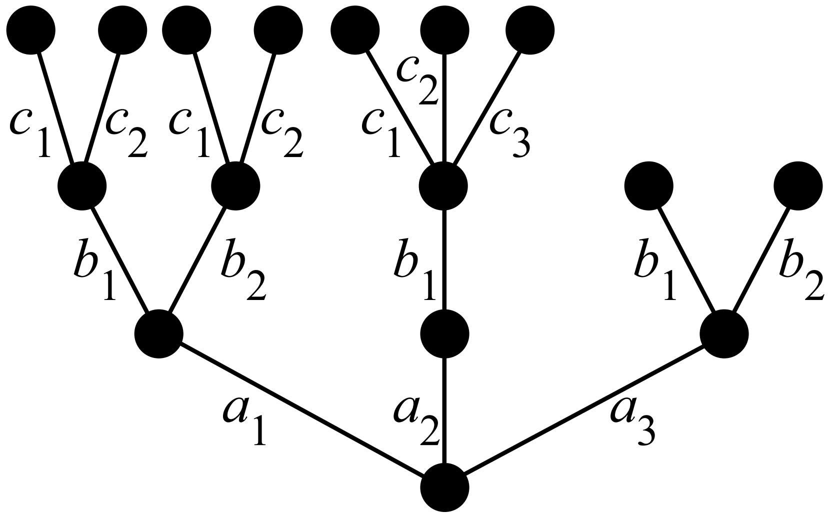
Megoldás: A lehetséges (a_i, b_j, c_k) elemhármasokat kell megszámolnunk. A lehetőségeket az alábbi ábra segítségével tekintjük át.



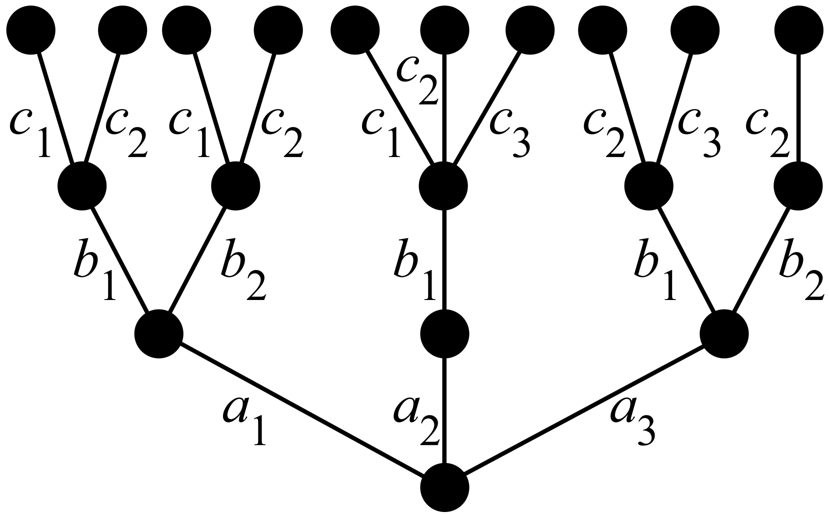
Kizárt párok: $\boxed{(a_2, b_2)}$, (a_1, c_3), (a_3, c_1), (b_2, c_3).



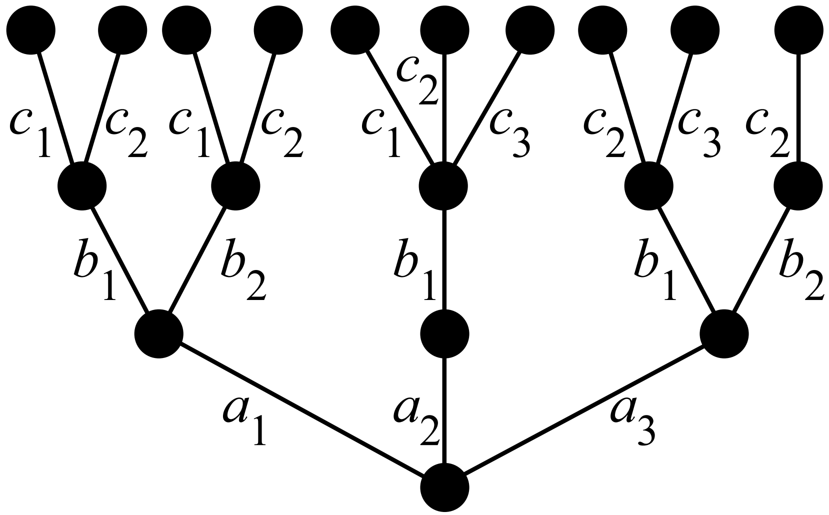
Kizárt párok: (a_2, b_2), (a_1, c_3), (a_3, c_1), (b_2, c_3).



Kizárt párok: (a_2, b_2), (a_1, c_3), (a_3, c_1), (b_2, c_3).



Kizárt párok: (a_2, b_2), (a_1, c_3), (a_3, c_1), (b_2, c_3).



Kizárt párok: (a_2, b_2), (a_1, c_3), $\boxed{(a_3, c_1)}$, $\boxed{(b_2, c_3)}$.

Innen leolvasható, hogy a lehetőségek száma = a felső sorban levő szögpontok („levelek") száma, azaz **tíz**. (Az egyes lehetőségeket a „gyökértől" a levelekig vezető utak adják.)

Mi tagadás, egy ilyenfajta megoldás nem sokkal jobb, mint az összes eset felsorolása, ez esetünkben $3 \cdot 2 \cdot 3 = 18$, majd ezen esetek egyenként történő vizsgálata után a rossz esetek elhagyása, és a visszamaradók megszámolása.

Mi tagadás, egy ilyenfajta megoldás nem sokkal jobb, mint az összes eset felsorolása, ez esetünkben $3 \cdot 2 \cdot 3 = 18$, majd ezen esetek egyenként történő vizsgálata után a rossz esetek elhagyása, és a visszamaradók megszámolása. De nincs minden feladatra elegáns megoldás.

Feladat: Hány ekvivalencia(reláció) van egy négyelemű halmazon?

Feladat: Hány ekvivalencia(reláció) van egy négyelemű halmazon?

Megoldás: Mivel az ekvivalenciák és az osztályozások „lényegében azonosak” (azaz bijekció van az adott halmaz ekvivalenciái és osztályozásai között),

Feladat: Hány ekvivalencia(reláció) van egy négyelemű halmazon?

Megoldás: Mivel az ekvivalenciák és az osztályozások „lényegében azonosak'' (azaz bijekció van az adott halmaz ekvivalenciái és osztályozásai között), elegendő az utóbbit megszámolnunk.

Feladat: Hány ekvivalencia(reláció) van egy négyelemű halmazon?

Megoldás: Mivel az ekvivalenciák és az osztályozások „lényegében azonosak" (azaz bijekció van az adott halmaz ekvivalenciái és osztályozásai között), elegendő az utóbbit megszámolnunk. Rendre megszámoljuk a különféle „típusú" osztályozásokat, majd a kapott számokat (az összegezési szabály szerint) összeadjuk. „Típuson" az osztályozást alkotó osztályok elemszámainak rendszerét fogjuk érteni, tehát pl. $2 + 1 + 1$ típusról beszélünk, amikor egy kételemű és két egyelemű osztály van.

Feladat: Hány ekvivalencia(reláció) van egy négyelemű halmazon?

Megoldás: Mivel az ekvivalenciák és az osztályozások „lényegében azonosak” (azaz bijekció van az adott halmaz ekvivalenciái és osztályozásai között), elegendő az utóbbit megszámolnunk. Rendre megszámoljuk a különféle „típusú” osztályozásokat, majd a kapott számokat (az összegezési szabály szerint) összeadjuk. „Típuson” az osztályozást alkotó osztályok elemszámainak rendszerét fogjuk érteni, tehát pl. $2+1+1$ típusról beszélünk, amikor egy kételemű és két egyelemű osztály van. Legyen $A = \{a, b, c, d\}$ a négyelemű halmaz.

Hogy egyiket se felejtsük ki, a típusokat nagyság szerint soroljuk fel, kezdve a legnagyobb elemszámú osztályt tartalmazóval.

Hogy egyiket se felejtsük ki, a típusokat nagyság szerint soroljuk fel, kezdve a legnagyobb elemszámú osztályt tartalmazóval.

4-típusú: ekkor egyetlen 4-elemű osztály van, az egész A, ilyenből **1** van.

Hogy egyiket se felejtsük ki, a típusokat nagyság szerint soroljuk fel, kezdve a legnagyobb elemszámú osztályt tartalmazóval.

4-típusú: ekkor egyetlen 4-elemű osztály van, az egész A, ilyenből **1** van.

$3+1$ típusú: van egy háromelemű osztály és egy egyelemű. Az osztályozást a „magányos elem” meghatározza, azt négyféleképpen választhatjuk ki. Tehát **4** ilyen osztályozás van.

$2 + 2$ típusú: az osztályozást az határozza meg, hogy a

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen ha mondjuk c-vel, akkor a másik osztály $\{b, d\}$.) Az

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen ha mondjuk c-vel, akkor a másik osztály $\{b, d\}$.) Az a párja háromféleképpen választható ki, tehát ilyen osztályozásból **3** van.

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen ha mondjuk c-vel, akkor a másik osztály $\{b, d\}$.) Az a párja háromféleképpen választható ki, tehát ilyen osztályozásból **3** van.

$2+1+1$ típusú: itt az a kérdés, hogy hányféleképpen lehet két különböző elemet kiválasztani (amelyek egy osztályban lesznek)

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen ha mondjuk c-vel, akkor a másik osztály $\{b, d\}$.) Az a párja háromféleképpen választható ki, tehát ilyen osztályozásból **3** van.

$2+1+1$ típusú: itt az a kérdés, hogy hányféleképpen lehet két különböző elemet kiválasztani (amelyek egy osztályban lesznek) — a sorrend persze nem számít.

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen ha mondjuk c-vel, akkor a másik osztály $\{b, d\}$.) Az a párja háromféleképpen választható ki, tehát ilyen osztályozásból **3** van.

$2+1+1$ típusú: itt az a kérdés, hogy hányféleképpen lehet két különböző elemet kiválasztani (amelyek egy osztályban lesznek) — a sorrend persze nem számít. Ha a sorrend számítana, akkor (a korábbi feladatok mintájára) az elsőt 4-, a másodikat 3-féleképpen, tehát (a szorzási szabály szerint) $4 \cdot 3 = 12$-féleképpen,

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen ha mondjuk c-vel, akkor a másik osztály $\{b, d\}$.) Az a párja háromféleképpen választható ki, tehát ilyen osztályozásból **3** van.

$2+1+1$ típusú: itt az a kérdés, hogy hányféleképpen lehet két különböző elemet kiválasztani (amelyek egy osztályban lesznek) — a sorrend persze nem számít. Ha a sorrend számítana, akkor (a korábbi feladatok mintájára) az elsőt 4-, a másodikat 3-féleképpen, tehát (a szorzási szabály szerint) $4 \cdot 3 = 12$-féleképpen, de ezt meg kell felezni, hiszen a sorrend nem számít. Tehát ezen típus esetén

$2+2$ típusú: az osztályozást az határozza meg, hogy a a b, c, d elemek közül melyikkel van egy osztályban. (Hiszen ha mondjuk c-vel, akkor a másik osztály $\{b, d\}$.) Az a párja háromféleképpen választható ki, tehát ilyen osztályozásból **3** van.

$2+1+1$ típusú: itt az a kérdés, hogy hányféleképpen lehet két különböző elemet kiválasztani (amelyek egy osztályban lesznek) — a sorrend persze nem számít. Ha a sorrend számítana, akkor (a korábbi feladatok mintájára) az elsőt 4-, a másodikat 3-féleképpen, tehát (a szorzási szabály szerint) $4 \cdot 3 = 12$-féleképpen, de ezt meg kell felezni, hiszen a sorrend nem számít. Tehát ezen típus esetén **6** osztályozás van.

$1+1+1+1$ típusú: minden elem „magányos”, ilyen osztályozás **1** van.

$1+1+1+1$ típusú: minden elem „magányos”, ilyen osztályozás **1** van.

Végül az eredmény: a kapott számokat összeadva $1+4+3+6+1 =$ 15 osztályozás van a négyelemű halmazon.

Típushibák: van, hogy valamelyik típusról megfeledkezünk (ez ritka). Gyakori viszont, amikor valaki úgy számolja össze a $2+2$ típusúakat, hogy hányféleképpen lehet kiválasztani két elemet (sorrend nem számít). Nos, hatféleképpen (amint a $2+1+1$ vizsgálatánál láttuk), de ennek ellenére ez nem adja meg a $2+2$ típusú osztályozások számát, hiszen pl. az $\{a, d\}$-t kiválasztva ugyanazon osztályozáshoz jutunk, mint a $\{b, c\}$-t kiválasztva.

Az eddigi feladatokban gyakran ismétlődő gondolatokat fedezhetünk fel. Hatékonyságunkat nagyban növeli, ha ezeket külön névvel látjuk el és külön tételben foglalkozunk velük. Ezek lesznek az ún. **kombinatorikai alapfeladatok**.

Az egyes kombinatorikai alapfeladatokat az alábbiak szerint csoportosítjuk, és felismerésükhöz az alábbiakat kell majd megkérdeznünk magunktól (ezt most még nem kell pontosan érteni, de majd érdemes lesz ide visszalapozni):

Sorba rakjuk-e az összeset ($\Longrightarrow$ permutáció) vagy kiválasztunk-e bizonyosakat ($\Longrightarrow$ variáció vagy kombináció)?

Sorba rakjuk-e az összeset ($\Longrightarrow$ permutáció) vagy kiválasztunk-e bizonyosakat ($\Longrightarrow$ variáció vagy kombináció)?

Sorba rakjuk-e az összeset ($\Longrightarrow$ permutáció) vagy kiválasztunk-e bizonyosakat ($\Longrightarrow$ variáció vagy kombináció)?

Az elemek különbözők-e ($\Longrightarrow$ „ismétlés nélküli") vagy lehetnek közöttük azonosak ($\Longrightarrow$ „ismétléses")?

Sorba rakjuk-e az összeset ($\Longrightarrow$ permutáció) vagy kiválasztunk-e bizonyosakat ($\Longrightarrow$ variáció vagy kombináció)?

Az elemek különbözők-e ($\Longrightarrow$ „ismétlés nélküli") vagy lehetnek közöttük azonosak ($\Longrightarrow$ „ismétléses")?

Bizonyosak kiválasztásánál számít-e a sorrend ($\Longrightarrow$ variáció) vagy nem ($\Longrightarrow$ kombináció)?

Variációk

Definíció Egy n-elemű halmaz elemeiből képezhető k-tagú (ismétlődést megengedő) sorozatot az n elem k-adosztályú (vagy k-tagú) **ismétléses variációjának** nevezzük. A kérdés pedig az, hogy hány ilyen van.

Variációk

Definíció Egy n-elemű halmaz elemeiből képezhető k-tagú (ismétlődést megengedő) sorozatot az n elem k-adosztályú (vagy k-tagú) **ismétléses variációjának** nevezzük. A kérdés pedig az, hogy hány ilyen van.

Megjegyzések: A sorozatban természetesen számít a sorrend.

Variációk

Definíció Egy n-elemű halmaz elemeiből képezhető k-tagú (ismétlődést megengedő) sorozatot az n elem k-adosztályú (vagy k-tagú) **ismétléses variációjának** nevezzük. A kérdés pedig az, hogy hány ilyen van.

Megjegyzések: A sorozatban természetesen számít a sorrend. Ha $n = 3$ és a halmaz $\{0, 1, x\}$, továbbá $k = 13 + 1$, akkor az ismétléses variáció a totószelvény kitöltésének felel meg.

Variációk

Definíció Egy n-elemű halmaz elemeiből képezhető k-tagú (ismétlődést megengedő) sorozatot az n elem k-adosztályú (vagy k-tagú) **ismétléses variációjának** nevezzük. A kérdés pedig az, hogy hány ilyen van.

Megjegyzések: A sorozatban természetesen számít a sorrend. Ha $n = 3$ és a halmaz $\{0, 1, x\}$, továbbá $k = 13 + 1$, akkor az ismétléses variáció a totószelvény kitöltésének felel meg. (A totózókat is érinti a variációk száma — különösen akkor, ha bizonyos meccsek eredményét biztosra veszik.)

Az n-elemű A halmazból képezett k-tagú sorozatok felfoghatók $\{1, 2, \ldots, k\} \to A$ leképezéseknek is. Valóban, Az n-elemű A halmazból képezett k-tagú sorozatok felfoghatók $\{1,2,\ldots,k\} \to A$ leképezéseknek is. Valóban, egy $(a_1,\ldots,a_k)$ sorozat megadása az $1 \mapsto a_1$, ..., $k \mapsto a_k$ leképezés megadásával ekvivalens. Ezért egyes forrásmunkák a variációkat mint leképezéseket definiálják.

1. Tétel. *Legyen $n,k \in \mathbb{N}$. n elem k-adosztályú ismétléses variációinak száma n^k.*

Megjegyzés:

Az n-elemű A halmazból képezett k-tagú sorozatok felfoghatók $\{1, 2, \ldots, k\} \to A$ leképezéseknek is. Valóban, egy $(a_1, \ldots, a_k)$ sorozat megadása az $1 \mapsto a_1$, ..., $k \mapsto a_k$ leképezés megadásával ekvivalens. Ezért egyes forrásmunkák a variációkat mint leképezéseket definiálják.

1. Tétel. *Legyen $n, k \in \mathbb{N}$. n elem k-adosztályú ismétléses variációinak száma n^k.*

Megjegyzés: A tétel $n, k \in \mathbb{N}_0$ esetén is érvényes, de ha k vagy n nulla, akkor triviális (és ezért nem túl érdekes).

Bizonyítás (a célhoz igazított precizitással) A

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki.

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki. A második elem nem függ az elsőtől, tehát azt is n-féleképpen.

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki. A második elem nem függ az elsőtől, tehát azt is n-féleképpen. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n \cdot n = n^2$-féleképpen.

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki. A második elem nem függ az elsőtől, tehát azt is n-féleképpen. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n \cdot n = n^2$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet is n-féleképpen választhatjuk. Tehát

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki. A második elem nem függ az elsőtől, tehát azt is n-féleképpen. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n \cdot n = n^2$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet is n-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n^2 \cdot n = n^3$-féleképpen.

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki. A második elem nem függ az elsőtől, tehát azt is n-féleképpen. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n \cdot n = n^2$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet is n-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n^2 \cdot n = n^3$-féleképpen. És így tovább.

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki. A második elem nem függ az elsőtől, tehát azt is n-féleképpen. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n \cdot n = n^2$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet is n-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n^2 \cdot n = n^3$-féleképpen. És így tovább. Tehát a k-tagú sorozatot n^k-féleképpen választhatjuk ki.

Bizonyítás (a célhoz igazított precizitással) A sorozat első elemét n-féleképpen választhatjuk ki. A második elem nem függ az elsőtől, tehát azt is n-féleképpen. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n \cdot n = n^2$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet is n-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n^2 \cdot n = n^3$-féleképpen. És így tovább. Tehát a k-tagú sorozatot n^k-féleképpen választhatjuk ki. Q.e.d.

A bizonyítások ismertetése nem öncélú:

A bizonyítások ismertetése nem öncélú: ez jó felkészülés a feladatokra; továbbá a képlet megjegyzését is megkönnyíti.

A bizonyítások ismertetése nem öncélú: ez jó felkészülés a feladatokra; továbbá a képlet megjegyzését is megkönnyíti. A vizsgatesztlapok azt mutatják, hogy — konkrét feladat kapcsán, ahol a vizsgázó dolga, hogy eldöntse, melyik a k és melyik az n — nagyon gyakori, A bizonyítások ismertetése nem öncélú: ez jó felkészülés a feladatokra; továbbá a képlet megjegyzését is megkönnyíti. A vizsgatesztlapok azt mutatják, hogy — konkrét feladat kapcsán, ahol a vizsgázó dolga, hogy eldöntse, melyik a k és melyik az n — nagyon gyakori, hogy n^k helyett a rossz k^n képletet alkalmazza valaki. Ez nem fordulhat elő azzal, aki a képlet helyett inkább a fenti — roppant könnyű — bizonyítást jegyzi meg.

A bizonyítások ismertetése nem öncélú: ez jó felkészülés a feladatokra; továbbá a képlet megjegyzését is megkönnyíti. A vizsgatesztlapok azt mutatják, hogy — konkrét feladat kapcsán, ahol a vizsgázó dolga, hogy eldöntse, melyik a k és melyik az n — nagyon gyakori, hogy n^k helyett a rossz k^n képletet alkalmazza valaki. Ez nem fordulhat elő azzal, aki a képlet helyett inkább a fenti — roppant könnyű — bizonyítást jegyzi meg. A fenti bizonyítás teljesen precíz változata n szerinti teljes indukció lenne.

Definíció Egy n-elemű A halmaz elemiből képezhető k-tagú ismétlés nélküli sorozatot az n elem k-adosztályú (vagy k-tagú) **ismétlés nélküli variációjának** nevezzük. Ilyen csak akkor létezik, ha $k \leq n$. A kérdés most is az, hogy hány ilyen van.

Definíció Egy n-elemű A halmaz elemiből képezhető k-tagú ismétlés nélküli sorozatot az n elem k-adosztályú (vagy k-tagú) **ismétlés nélküli variációjának** nevezzük. Ilyen csak akkor létezik, ha $k \leq n$. A kérdés most is az, hogy hány ilyen van.

Definíció Egy n-elemű A halmaz elemiből képezhető k-tagú ismétlés nélküli sorozatot az n elem k-adosztályú (vagy k-tagú) **ismétlés nélküli variációjának** nevezzük. Ilyen csak akkor létezik, ha $k \leq n$. A kérdés most is az, hogy hány ilyen van.

Megjegyzés: Lehetne az ismétlés nélküli variációt **injektív** $\{1, \ldots, k\} \to A$ leképezésként is definiálni.

2. Tétel. *Legyen* $n, k \in \mathbf{N}$ *és* $k \leq n$. n *elem* k*-adosztályú ismétlés nélküli variációinak száma*

$$n(n-1)(n-2)\ldots(n-k+1)$$

(

2. Tétel. *Legyen* $n, k \in \mathbf{N}$ *és* $k \leq n$. n *elem* k*-adosztályú ismétlés nélküli variációinak száma*

$$n(n-1)(n-2)\dots(n-k+1)$$

(tehát egy k*-tényezős szorzat egyre kisebb tényezőkkel).*

2. Tétel. *Legyen* $n, k \in \mathbf{N}$ *és* $k \leq n$. n *elem* k*-adosztályú ismétlés nélküli variációinak száma*

$$n(n-1)(n-2)\ldots(n-k+1)$$

(tehát egy k*-tényezős szorzat egyre kisebb tényezőkkel).*

Megjegyzés:

2. Tétel. *Legyen $n, k \in \mathbf{N}$ és $k \leq n$. n elem k-adosztályú ismétlés nélküli variációinak száma*

$$n(n-1)(n-2)\dots(n-k+1)$$

(tehát egy k-tényezős szorzat egyre kisebb tényezőkkel).

Megjegyzés: A tétel $n, k \in \mathbf{N}_0$ esetén is is érvényes (hiszen az üresszorzat megállapodás szerint 1). A tételből a $k \leq n$ kikötés elhagyható (hiszen $k > n$ esetén a szorzat értéke nulla).

Bizonyítás A

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki.

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki. A második elem függ az elsőtől, tudniillik nem lehet egyenlő vele, tehát azt $(n-1)$-féleképpen választhatjuk ki.

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki. A második elem függ az elsőtől, tudniillik nem lehet egyenlő vele, tehát azt $(n-1)$-féleképpen választhatjuk ki. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n(n-1)$-féleképpen.

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki. A második elem függ az elsőtől, tudniillik nem lehet egyenlő vele, tehát azt $(n-1)$-féleképpen választhatjuk ki. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n(n-1)$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet — mivel az a kiválasztottak egyike sem lehet — csak $n-2$-féleképpen választhatjuk. Tehát

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki. A második elem függ az elsőtől, tudniillik nem lehet egyenlő vele, tehát azt $(n-1)$-féleképpen választhatjuk ki. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n(n-1)$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet — mivel az a kiválasztottak egyike sem lehet — csak $n-2$-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n(n-1)(n-2)$-féleképpen.

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki. A második elem függ az elsőtől, tudniillik nem lehet egyenlő vele, tehát azt $(n-1)$-féleképpen választhatjuk ki. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n(n-1)$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet — mivel az a kiválasztottak egyike sem lehet — csak $n-2$-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n(n-1)(n-2)$-féleképpen. És így tovább.

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki. A második elem függ az elsőtől, tudniillik nem lehet egyenlő vele, tehát azt $(n-1)$-féleképpen választhatjuk ki. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n(n-1)$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet — mivel az a kiválasztottak egyike sem lehet — csak $n-2$-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n(n-1)(n-2)$-féleképpen. És így tovább. Tehát a k-tagú sorozatot $n(n-1)(n-2)\ldots(n-k+1)$-féleképpen választhatjuk ki.

Bizonyítás A sorozat első elemét n-féleképpen választhatjuk ki. A második elem függ az elsőtől, tudniillik nem lehet egyenlő vele, tehát azt $(n-1)$-féleképpen választhatjuk ki. A szorzási szabály szerint az első két elemet (azaz az első két elemből álló sorozatot) $n(n-1)$-féleképpen. Miután két elemet kiválasztottunk, a harmadik elemet — mivel az a kiválasztottak egyike sem lehet — csak $n-2$-féleképpen választhatjuk. Tehát — megint a szorzási szabály szerint — az első három elemet (azaz háromtagú sorozatot) $n(n-1)(n-2)$-féleképpen. És így tovább. Tehát a k-tagú sorozatot $n(n-1)(n-2)\ldots(n-k+1)$-féleképpen választhatjuk ki. Q.e.d.

Permutációk

Definíció Adott n különböző elem esetén az elemek valamilyen sorba (sorozatba) rendezését az n elem **(ismétlés nélküli) permutációjának** nevezzük.

Permutációk

Definíció Adott n különböző elem esetén az elemek valamilyen sorba (sorozatba) rendezését az n elem **(ismétlés nélküli) permutációjának** nevezzük.

Tehát az (ism. nélküli) permutáció nem más, mint n elem n-edosztályú ism. nélküli variációja. (

Permutációk

Definíció Adott n különböző elem esetén az elemek valamilyen sorba (sorozatba) rendezését az n elem **(ismétlés nélküli)** **permutációjának** nevezzük.

Tehát az (ism. nélküli) permutáció nem más, mint n elem n-edosztályú ism. nélküli variációja. (Az ism. nélküli variáció speciális esete, amikor $n = k$.)

Más megfogalmazásban: amikor n elem (ism. nélküli) permutációit megszámoljuk, akkor

Más megfogalmazásban: amikor n elem (ism. nélküli) permutációit megszámoljuk, akkor arra a kérdésre adunk választ, hogy hányféleképpen lehet n elemet sorbarendezni, Más megfogalmazásban: amikor n elem (ism. nélküli) permutációit megszámoljuk, akkor arra a kérdésre adunk választ, hogy hányféleképpen lehet n elemet sorbarendezni, azaz hány **rendezési reláció** van egy n-elemű halmazon, vagy

Más megfogalmazásban: amikor n elem (ism. nélküli) permutációit megszámoljuk, akkor arra a kérdésre adunk választ, hogy hányféleképpen lehet n elemet sorbarendezni, azaz hány **rendezési reláció** van egy n-elemű halmazon, vagy — a sorozatok és leképezések már említett kapcsolatára gondolva — hány önmagára történő **bijekciója** van egy n-elemű halmaznak.

Mellesleg az $\{1, 2, \ldots, n\}$ halmaz önmagára történő bijektív leképezéseit is permutációknak nevezik, és pl. így jelölik: $\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$. Ezen mátrix alsó sorára tekintve jól látszik a permutáció mint leképezés és a permutáció mint sorbarendezés közötti kapcsolat.

Mivel az ism. nélküli permutáció az ism. nélküli variáció speciális esete, azonnal adódik az alábbi

3. Tétel. *Legyen* $n \in \mathbf{N}_0$. n *elem ismétlés nélküli permutációinak száma*

$$1 \cdot 2 \cdot 3 \cdots n = n!$$

Itt $n!$ **(kiolvasva: n faktoriális)** az első n pozitív egész szám szorzatát jelöli. (Megállapodás szerint $0! = 1! = 1$.)

Mivel az ism. nélküli permutáció az ism. nélküli variáció speciális esete, azonnal adódik az alábbi

3. Tétel. *Legyen* $n \in \mathbf{N}_0$. n *elem ismétlés nélküli permutációinak száma*

$$1 \cdot 2 \cdot 3 \cdots n = n!$$

Itt $n!$ **(kiolvasva: n faktoriális)** az első n pozitív egész szám szorzatát jelöli. (Megállapodás szerint $0! = 1! = 1$.) Mivel $n(n-1)\cdots(n-k+1)$ egyenlő

Mivel az ism. nélküli permutáció az ism. nélküli variáció speciális esete, azonnal adódik az alábbi

3. Tétel. *Legyen* $n \in \mathbf{N}_0$. n *elem ismétlés nélküli permutációinak száma*

$$1 \cdot 2 \cdot 3 \cdots n = n!$$

Itt $n!$ **(kiolvasva: n faktoriális)** az első n pozitív egész szám szorzatát jelöli. (Megállapodás szerint $0! = 1! = 1$.) Mivel $n(n-1)\cdots(n-k+1)$ egyenlő $\frac{n!}{(n-k)!}$-sal

Mivel az ism. nélküli permutáció az ism. nélküli variáció speciális esete, azonnal adódik az alábbi

3. Tétel. *Legyen* $n \in \mathbb{N}_0$. n *elem ismétlés nélküli permutációinak száma*

$$1 \cdot 2 \cdot 3 \cdots n = n!$$

Itt $n!$ **(kiolvasva: n faktoriális)** az első n pozitív egész szám szorzatát jelöli. (Megállapodás szerint $0! = 1! = 1$.) Mivel $n(n-1)\cdots(n-k+1)$ egyenlő $\dfrac{n!}{(n-k)!}$-sal — ez a tört leegyszerűsítése után látszik — ezért kapjuk:

1. Következmény. n *elem* k*-adosztályú ismétlés nélküli variációinak száma* $\dfrac{n!}{(n-k)!}$.

Feladat: Ha a nagy- és kisbetűket nem különböztetjük meg és csak ékezet nélküli betűket és számjegyeket használhatunk (összesen 36 karakter), akkor hány nyolcbetűs jelszó készíthető, ha

(A) a jelszóban páronként csupa különböző karaktereknek kell lenniük,

(B) lehetnek azonos karakterek is.

Feladat: Ha a nagy- és kisbetűket nem különböztetjük meg és csak ékezet nélküli betűket és számjegyeket használhatunk (összesen 36 karakter), akkor hány nyolcbetűs jelszó készíthető, ha

(A) a jelszóban páronként csupa különböző karaktereknek kell lenniük,

(B) lehetnek azonos karakterek is.

Megoldás:

Feladat: Ha a nagy- és kisbetűket nem különböztetjük meg és csak ékezet nélküli betűket és számjegyeket használhatunk (összesen 36 karakter), akkor hány nyolcbetűs jelszó készíthető, ha

(A) a jelszóban páronként csupa különböző karaktereknek kell lenniük,

(B) lehetnek azonos karakterek is.

Megoldás: Kiválasztunk és sorrend számít

Feladat: Ha a nagy- és kisbetűket nem különböztetjük meg és csak ékezet nélküli betűket és számjegyeket használhatunk (összesen 36 karakter), akkor hány nyolcbetűs jelszó készíthető, ha

(A) a jelszóban páronként csupa különböző karaktereknek kell lenniük,

(B) lehetnek azonos karakterek is.

Megoldás: Kiválasztunk és sorrend számít $\Longrightarrow$ variáció!

Feladat: Ha a nagy- és kisbetűket nem különböztetjük meg és csak ékezet nélküli betűket és számjegyeket használhatunk (összesen 36 karakter), akkor hány nyolcbetűs jelszó készíthető, ha

(A) a jelszóban páronként csupa különböző karaktereknek kell lenniük,

(B) lehetnek azonos karakterek is.

Megoldás: Kiválasztunk és sorrend számít $\Longrightarrow$ variáció! Az (A) esetben ismétlés nélküli, tehát az eredmény

Feladat: Ha a nagy- és kisbetűket nem különböztetjük meg és csak ékezet nélküli betűket és számjegyeket használhatunk (összesen 36 karakter), akkor hány nyolcbetűs jelszó készíthető, ha

(A) a jelszóban páronként csupa különböző karaktereknek kell lenniük,

(B) lehetnek azonos karakterek is.

Megoldás: Kiválasztunk és sorrend számít $\Longrightarrow$ variáció! Az (A) esetben ismétlés nélküli, tehát az eredmény $36 \cdot 35 \cdots 29 = 220\,096\,908\,800$.

Feladat: Ha a nagy- és kisbetűket nem különböztetjük meg és csak ékezet nélküli betűket és számjegyeket használhatunk (összesen 36 karakter), akkor hány nyolcbetűs jelszó készíthető, ha

(A) a jelszóban páronként csupa különböző karaktereknek kell lenniük,

(B) lehetnek azonos karakterek is.

Megoldás: Kiválasztunk és sorrend számít $\Longrightarrow$ variáció! Az (A) esetben ismétlés nélküli, tehát az eredmény $36 \cdot 35 \cdots 29 = 220\,096\,908\,800$. A (B) esetben ismétléses, tehát az eredmény: $36^8 = 2\,821\,109\,907\,456$.

Megjegyzés: az ismertetett megoldás során alkalmaztuk a variációk számára vonatkozó tételt.

Megjegyzés: az ismertetett megoldás során alkalmaztuk a variációk számára vonatkozó tételt. De felfoghatjuk a megoldást úgy is, hogy a szorzási szabályt alkalmaztuk: a jelszó első karakterét 36-féleképpen választhatjuk, a másodikat (az (A) esetben) 35-féleképpen, stb., és ezeket össze kell szorozni.

Megjegyzés: az ismertetett megoldás során alkalmaztuk a variációk számára vonatkozó tételt. De felfoghatjuk a megoldást úgy is, hogy a szorzási szabályt alkalmaztuk: a jelszó első karakterét 36-féleképpen választhatjuk, a másodikat (az (A) esetben) 35-féleképpen, stb., és ezeket össze kell szorozni.

Feladat:
Hányféleképpen (pontosabban: hányféle „eredménnyel”) lehet a (32-lapos) kártyapaklit megkeverni?

Megjegyzés: az ismertetett megoldás során alkalmaztuk a variációk számára vonatkozó tételt. De felfoghatjuk a megoldást úgy is, hogy a szorzási szabályt alkalmaztuk: a jelszó első karakterét 36-féleképpen választhatjuk, a másodikat (az (A) esetben) 35-féleképpen, stb., és ezeket össze kell szorozni.

Feladat:
Hányféleképpen (pontosabban: hányféle „eredménnyel") lehet a (32-lapos) kártyapaklit megkeverni?

Megoldás: Ahányféleképpen a 32 különböző kártyalapot sorba lehet rendezni,

Megjegyzés: az ismertetett megoldás során alkalmaztuk a variációk számára vonatkozó tételt. De felfoghatjuk a megoldást úgy is, hogy a szorzási szabályt alkalmaztuk: a jelszó első karakterét 36-féleképpen választhatjuk, a másodikat (az (A) esetben) 35-féleképpen, stb., és ezeket össze kell szorozni.

Feladat:
Hányféleképpen (pontosabban: hányféle „eredménnyel") lehet a (32-lapos) kártyapaklit megkeverni?

Megoldás: Ahányféleképpen a 32 különböző kártyalapot sorba lehet rendezni, azaz permutálni, tehát

Megjegyzés: az ismertetett megoldás során alkalmaztuk a variációk számára vonatkozó tételt. De felfoghatjuk a megoldást úgy is, hogy a szorzási szabályt alkalmaztuk: a jelszó első karakterét 36-féleképpen választhatjuk, a másodikat (az (A) esetben) 35-féleképpen, stb., és ezeket össze kell szorozni.

Feladat:
Hányféleképpen (pontosabban: hányféle „eredménnyel") lehet a (32-lapos) kártyapaklit megkeverni?

Megoldás: Ahányféleképpen a 32 különböző kártyalapot sorba lehet rendezni, azaz permutálni, tehát

$$32! =$$

Megjegyzés: az ismertetett megoldás során alkalmaztuk a variációk számára vonatkozó tételt. De felfoghatjuk a megoldást úgy is, hogy a szorzási szabályt alkalmaztuk: a jelszó első karakterét 36-féleképpen választhatjuk, a másodikat (az (A) esetben) 35-féleképpen, stb., és ezeket össze kell szorozni.

Feladat:
Hányféleképpen (pontosabban: hányféle „eredménnyel") lehet a (32-lapos) kártyapaklit megkeverni?

Megoldás: Ahányféleképpen a 32 különböző kártyalapot sorba lehet rendezni, azaz permutálni, tehát

$$32! = 263\,130\,836\,933\,693\,530\,167\,218\,012\,160\,000\,000$$

azaz kb. $2,63 \cdot 10^{35}$-féleképpen.

Kombinációk

Van amikor a sorrend nem számít. Pl. ha három különböző süteményt rendelünk az étteremben, amelyet a pincér egyszerre hoz ki.

Kombinációk

Van amikor a sorrend nem számít. Pl. ha három különböző süteményt rendelünk az étteremben, amelyet a pincér egyszerre hoz ki.

Definíció:

Kombinációk

Van amikor a sorrend nem számít. Pl. ha három különböző süteményt rendelünk az étteremben, amelyet a pincér egyszerre hoz ki.

Definíció: Egy n-elemű halmaz k-elemű részhalmazait a kombinatorikában n elem k-adosztályú **ismétlés nélküli kombinációinak** nevezzük. Az alapfeladat ezek számának meghatározása.

Kombinációk

Van amikor a sorrend nem számít. Pl. ha három különböző süteményt rendelünk az étteremben, amelyet a pincér egyszerre hoz ki.

Definíció: Egy n-elemű halmaz k-elemű részhalmazait a kombinatorikában n elem k-adosztályú **ismétlés nélküli kombinációinak** nevezzük. Az alapfeladat ezek számának meghatározása. Más szóval: n elem közül k különbözőt választunk ki, a **sorrend nem számít**!

4. Tétel. *Legyen* $k \leq n$.

4. Tétel. *Legyen* $k \leq n$. n *elem* k*-adosztályú (ismétlés nélküli) kombinációinak száma,*

4. Tétel. *Legyen $k \leq n$. n elem k-adosztályú (ismétlés nélküli) kombinációinak száma, más szóval egy n-elemű halmaz k-elemű részhalmazainak száma*

$$\frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k} =$$

4. Tétel. *Legyen $k \leq n$. n elem k-adosztályú (ismétlés nélküli) kombinációinak száma, más szóval egy n-elemű halmaz k-elemű részhalmazainak száma*

$$\frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k} = \frac{n!}{k!(n-k)!} =$$

4. Tétel. *Legyen $k \leq n$. n elem k-adosztályú (ismétlés nélküli) kombinációinak száma, más szóval egy n-elemű halmaz k-elemű részhalmazainak száma*

$$\frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k} = \frac{n!}{k!(n-k)!} = \boxed{\binom{n}{k}}.$$

4. Tétel. *Legyen $k \leq n$. n elem k-adosztályú (ismétlés nélküli) kombinációinak száma, más szóval egy n-elemű halmaz k-elemű részhalmazainak száma*

$$\frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k} = \frac{n!}{k!(n-k)!} = \boxed{\binom{n}{k}}.$$

A tételben szereplő (az előtte levő kifejezéssel definiált) $\binom{n}{k}$ szimbólumot úgy olvassuk, hogy „n alatt a k", és **binomiális együtthatónak** nevezzük. (Az elnevezés eredét később tárgyaljuk.)

Körülbelül itt kezdődik a kombinatorikának azon része, ahol már ugyancsak ajánlatos formulákat és tételeket használni a józan eszünk és a szorzási- és összegzési szabály mellett.

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**.

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.)

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon:

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz válasszunk ki egy k-elemű részhalmazt. Ezt megtehetjük x-féleképpen. (

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz válasszunk ki egy k-elemű részhalmazt. Ezt megtehetjük x-féleképpen. (Egyelőre x ismeretlen.) Majd a kiválasztott k elemből készítsünk egy sorozatot, azaz rakjuk őket sorba (

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz válasszunk ki egy k-elemű részhalmazt. Ezt megtehetjük x-féleképpen. (Egyelőre x ismeretlen.) Majd a kiválasztott k elemből készítsünk egy sorozatot, azaz rakjuk őket sorba (permutáció!), ezt megtehetjük $k!$-féleképpen. Mivel ez a $k!$ nem függ a kiválasztott részhalmaztól,

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz válasszunk ki egy k-elemű részhalmazt. Ezt megtehetjük x-féleképpen. (Egyelőre x ismeretlen.) Majd a kiválasztott k elemből készítsünk egy sorozatot, azaz rakjuk őket sorba (permutáció!), ezt megtehetjük $k!$-féleképpen. Mivel ez a $k!$ nem függ a kiválasztott részhalmaztól, a szorzási szabály szerint $x \cdot k!$ sorozat készíthető.

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz válasszunk ki egy k-elemű részhalmazt. Ezt megtehetjük x-féleképpen. (Egyelőre x ismeretlen.) Majd a kiválasztott k elemből készítsünk egy sorozatot, azaz rakjuk őket sorba (permutáció!), ezt megtehetjük $k!$-féleképpen. Mivel ez a $k!$ nem függ a kiválasztott részhalmaztól, a szorzási szabály szerint $x \cdot k!$ sorozat készíthető. De — az ismétlés nélküli variációkra vonatkozó tétel szerint — a kérdéses sorozatok száma $\frac{n!}{(n-k)!}$.

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz válasszunk ki egy k-elemű részhalmazt. Ezt megtehetjük x-féleképpen. (Egyelőre x ismeretlen.) Majd a kiválasztott k elemből készítsünk egy sorozatot, azaz rakjuk őket sorba (permutáció!), ezt megtehetjük $k!$-féleképpen. Mivel ez a $k!$ nem függ a kiválasztott részhalmaztól, a szorzási szabály szerint $x \cdot k!$ sorozat készíthető. De — az ismétlés nélküli variációkra vonatkozó tétel szerint — a kérdéses sorozatok száma $\frac{n!}{(n-k)!}$. Tehát $x \cdot k! = \frac{n!}{(n-k)!}$, és innen $x = \frac{n!}{k!(n-k)!} =$

Bizonyítás: Tegyük fel, hogy n elemből k elemet szeretnénk kiválasztani és a sorrend **számít**. (Nem elírás.) Tegyük ezt a következő módon: először válasszunk ki k elemet sorrendre való tekintet nélkül, azaz válasszunk ki egy k-elemű részhalmazt. Ezt megtehetjük x-féleképpen. (Egyelőre x ismeretlen.) Majd a kiválasztott k elemből készítsünk egy sorozatot, azaz rakjuk őket sorba (permutáció!), ezt megtehetjük $k!$-féleképpen. Mivel ez a $k!$ nem függ a kiválasztott részhalmaztól, a szorzási szabály szerint $x \cdot k!$ sorozat készíthető. De — az ismétlés nélküli variációkra vonatkozó tétel szerint — a kérdéses sorozatok száma $\frac{n!}{(n-k)!}$. Tehát $x \cdot k! = \frac{n!}{(n-k)!}$, és innen $x = \frac{n!}{k!(n-k)!} = \binom{n}{k}$. Q.e.d.

Feladat: Az étlapon tízféle sütemény szerepel (és mind kapható). Hányféleképpen lehet egyszerre négy különböző süteményt rendelni? (A rendelés sorrendje nem számít.)

Megoldás:

Feladat: Az étlapon tízféle sütemény szerepel (és mind kapható). Hányféleképpen lehet egyszerre négy különböző süteményt rendelni? (A rendelés sorrendje nem számít.)

Megoldás: A sorrend nem számít, ezért kombináció,

Feladat: Az étlapon tízféle sütemény szerepel (és mind kapható). Hányféleképpen lehet egyszerre négy különböző süteményt rendelni? (A rendelés sorrendje nem számít.)

Megoldás: A sorrend nem számít, ezért kombináció, és persze ismétlés nélküli. Az eredmény $\binom{10}{4} = \frac{10!}{4! \cdot 6!}$, amit természetesen úgy célszerű kiszámítani, hogy 6!-sal egyszerűsítünk:

$$\binom{10}{4} =$$

Feladat: Az étlapon tízféle sütemény szerepel (és mind kapható). Hányféleképpen lehet egyszerre négy különböző süteményt rendelni? (A rendelés sorrendje nem számít.)

Megoldás: A sorrend nem számít, ezért kombináció, és persze ismétlés nélküli. Az eredmény $\binom{10}{4} = \frac{10!}{4! \cdot 6!}$, amit természetesen úgy célszerű kiszámítani, hogy 6!-sal egyszerűsítünk:

$$\binom{10}{4} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3 \cdot 4} = 10 \cdot 3 \cdot 7 = \underline{210}.$$

Feladat: Az étlapon tízféle sütemény szerepel (és mind kapható). Hányféleképpen lehet egyszerre négy különböző süteményt rendelni? (A rendelés sorrendje nem számít.)

Megoldás: A sorrend nem számít, ezért kombináció, és persze ismétlés nélküli. Az eredmény $\binom{10}{4} = \frac{10!}{4! \cdot 6!}$, amit természetesen úgy célszerű kiszámítani, hogy 6!-sal egyszerűsítünk:

$$\binom{10}{4} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{1 \cdot 2 \cdot 3 \cdot 4} = 10 \cdot 3 \cdot 7 = \underline{210}.$$

Feladat: Az ötöslottó esetén (ahol kilencven számból ötöt kell eltalálni) legalább hány szelvényt kell ahhoz vásárolnunk, hogy biztosan legyen telitalálatunk?

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket,

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket, azaz ahányféleképpen a szelvényre nyomtatott számok 90-elemű halmazából ki lehet választani egy ötelemű részhalmazt, tehát az alábbi számút:

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket, azaz ahányféleképpen a szelvényre nyomtatott számok 90-elemű halmazából ki lehet választani egy ötelemű részhalmazt, tehát az alábbi számút:

$$\binom{90}{5} =$$

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket, azaz ahányféleképpen a szelvényre nyomtatott számok 90-elemű halmazából ki lehet választani egy ötelemű részhalmazt, tehát az alábbi számút:

$$\binom{90}{5} = 43\,949\,268.$$

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket, azaz ahányféleképpen a szelvényre nyomtatott számok 90-elemű halmazából ki lehet választani egy ötelemű részhalmazt, tehát az alábbi számút:

$$\binom{90}{5} = 43\ 949\ 268.$$

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket, azaz ahányféleképpen a szelvényre nyomtatott számok 90-elemű halmazából ki lehet választani egy ötelemű részhalmazt, tehát az alábbi számút:

$$\binom{90}{5} = 43\ 949\ 268.$$

Új téma.

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket, azaz ahányféleképpen a szelvényre nyomtatott számok 90-elemű halmazából ki lehet választani egy ötelemű részhalmazt, tehát az alábbi számút:

$$\binom{90}{5} = 43\,949\,268.$$

Új téma. Mi van, ha — korábbi példánkra utalva — annyira szeretjük a fatörzset, hogy amikor tíz sütemény közül négyet rendelünk, egynél több fatörzsre vágyunk?

Megoldás: Annyit, ahányféleképpen ki lehet tölteni a szelvényeket, azaz ahányféleképpen a szelvényre nyomtatott számok 90-elemű halmazából ki lehet választani egy ötelemű részhalmazt, tehát az alábbi számút:

$$\binom{90}{5} = 43\,949\,268.$$

Új téma. Mi van, ha — korábbi példánkra utalva — annyira szeretjük a fatörzset, hogy amikor tíz sütemény közül négyet rendelünk, egynél több fatörzsre vágyunk? Erre ad választ az alábbi fejezet.

Ismétléses kombinációk

Ismétléses kombinációk

Amint azt vektorrendszerekkel

Ismétléses kombinációk

Amint azt vektorrendszerekkel kapcsolatban tanultuk, a **rendszer** csak annyiban különbözik a halmaztól, hogy nemcsak az számít, hogy mik az elemeik, hanem az is, hogy melyik elem **hányszoros** eleme az összességnek, azaz

Ismétléses kombinációk

Amint azt vektorrendszerekkel kapcsolatban tanultuk, a **rendszer** csak annyiban különbözik a halmaztól, hogy nemcsak az számít, hogy mik az elemeik, hanem az is, hogy melyik elem **hányszoros** eleme az összességnek, azaz mennyi a **multiplicitása**.

Ismétléses kombinációk

Amint azt vektorrendszerekkel kapcsolatban tanultuk, a **rendszer** csak annyiban különbözik a halmaztól, hogy nemcsak az számít, hogy mik az elemeik, hanem az is, hogy melyik elem **hányszoros** eleme az összességnek, azaz mennyi a **multiplicitása**. A rendszer elemszáma az elemei multiplicitásainak összege. Rendszer esetén **az elemek sorrendje nem számít**.

Definíció: n elem k-adosztályú ismétléses kombinácóin az n elemből álló halmaz k-elemű rész

Definíció: n elem k-adosztályú ismétléses kombinácóin az n elemből álló halmaz k-elemű rész**rendszereit** értjük. Tehát k elemet kiválasztunk, egyet

Definíció: n elem k-adosztályú ismétléses kombinácóin az n elemből álló halmaz k-elemű rész**rendszereit** értjük. Tehát k elemet kiválasztunk, egyet **többször is** választhatunk,

Definíció: n elem k-adosztályú ismétléses kombinácóin az n elemből álló halmaz k-elemű rész**rendszereit** értjük. Tehát k elemet kiválasztunk, egyet **többször is** választhatunk, de a sorrend lényegtelen.

5. Tétel. *n elem k-adosztályú ismétléses kombinációinak a száma*

$$\binom{n+k-1}{k}$$

A tétel bizonyítását későbbre halasztjuk, most csak annyit jegyezzünk meg, hogy

Definíció: n elem k-adosztályú ismétléses kombinácóin az n elemből álló halmaz k-elemű rész**rendszereit** értjük. Tehát k elemet kiválasztunk, egyet **többször is** választhatunk, de a sorrend lényegtelen.

5. Tétel. *n elem k-adosztályú ismétléses kombinációinak a száma*

$$\binom{n+k-1}{k}$$

A tétel bizonyítását későbbre halasztjuk, most csak annyit jegyezzünk meg, hogy $k > n$ is lehet.

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit,

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít,

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció.

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció. Ismétléses. Tehát az eredmény:

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció. Ismétléses. Tehát az eredmény:

$$\Big(^{\text{tízből}}$$

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció. Ismétléses. Tehát az eredmény:

$$\Bigg(^{\text{tízből} + \text{négyet}}$$

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció. Ismétléses. Tehát az eredmény:

$$\Bigg(\text{tízből} + \text{négyet} - 1$$

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció. Ismétléses. Tehát az eredmény:

$$\binom{\text{tízből} + \text{négyet} - 1}{\text{négyet}}$$

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció. Ismétléses. Tehát az eredmény:

$$\binom{\text{tízből} + \text{négyet} - 1}{\text{négyet}} = \binom{10 + 4 - 1}{4} =$$

Feladat: Az étlapon tízféle sütemény szerepel (és mindből bőven van a hűtőben). Hányféleképpen lehet egyszerre négy süteményt rendelni? (A rendelés sorrendje nem számít, egy fajtából több is rendelhető.)

Megoldás: Kiválasztunk valamennyit, tehát kombináció vagy variáció (és nem permutáció). Sorrend nem számít, ezért kombináció. Ismétléses. Tehát az eredmény:

$$\binom{\text{tízből} + \text{négyet} - 1}{\text{négyet}} = \binom{10+4-1}{4} = \binom{13}{4} = \frac{13 \cdot 12 \cdot 11 \cdot 10}{1 \cdot 2 \cdot 3 \cdot 4} = \boxed{715}$$

Ismétléses permutációk

Az alapkérdés az, hogy hányféleképpen rakhatók sorba egy n-elemű **rendszer** elemei — egy ilyen sorbarakást (vagy sorozatba rendezést) az n elem egy **ismétléses permutációjának** nevezzük.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek;

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek; mindegyik annyiszor, amennyi a multiplicitása.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek; mindegyik annyiszor, amennyi a multiplicitása.

6. Tétel. *A fenti jelölések mellett az ismétléses permutációk száma*

$$\frac{n!}{k_1! \ldots k_r!}.$$

A

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek; mindegyik annyiszor, amennyi a multiplicitása.

6. Tétel. *A fenti jelölések mellett az ismétléses permutációk száma*

$$\frac{n!}{k_1! \ldots k_r!}.$$

A bizonyítást későbbre halasztjuk. Most lássunk egy feladatot.

A folyóiratok kora előtt a tudósoknak különféle furfanghoz kellett folyamodniuk, hogy mások ne vitassák el az elsőbbségüket. Például miután felfedezésük lényegét pár szóban leírták, a kapott szöveget átrendezték, és ezt küldték el a kollégáiknak. Az ilyen átrendezett szövegeket nevezzük *anagrammáknak*. Pl. a „romok”, a „komor” és a „mokor” egymás angrammái.

Persze a módszer korántsem tökéletes. Amikor

Persze a módszer korántsem tökéletes. Amikor Huygens (1629–1695) felfedezte a Titánt, a Szaturnusz elsőnek felfedezett holdját, akkor felfedezését ilyen anagramma formájában közölte kortársaival.

Persze a módszer korántsem tökéletes. Amikor Huygens (1629–1695) felfedezte a Titánt, a Szaturnusz elsőnek felfedezett holdját, akkor felfedezését ilyen anagramma formájában közölte kortársaival. Ámde Wallis, a kor kitűnő titkosírás-szakértője megfejtette ezt, csinált egy másik anagrammát, és azt visszaküldte Huygensnek. Később, a megfejtések közlésekor az a látszat alakult ki, hogy Huygensnek osztoznia kell az elsőbbségben. Később Wallis beismerte a tréfát, de Huygens soha nem bocsátotta meg neki.

Persze a módszer korántsem tökéletes. Amikor Huygens (1629–1695) felfedezte a Titánt, a Szaturnusz elsőnek felfedezett holdját, akkor felfedezését ilyen anagramma formájában közölte kortársaival. Ámde Wallis, a kor kitűnő titkosírás-szakértője megfejtette ezt, csinált egy másik anagrammát, és azt visszaküldte Huygensnek. Később, a megfejtések közlésekor az a látszat alakult ki, hogy Huygensnek osztoznia kell az elsőbbségben. Később Wallis beismerte a tréfát, de Huygens soha nem bocsátotta meg neki. Tanulság: aki megfelelő titkosírást akar használni, majd vegye fel a megfelelő választható tárgyat.

Persze a módszer korántsem tökéletes. Amikor Huygens (1629–1695) felfedezte a Titánt, a Szaturnusz elsőnek felfedezett holdját, akkor felfedezését ilyen anagramma formájában közölte kortársaival. Ámde Wallis, a kor kitűnő titkosírás-szakértője megfejtette ezt, csinált egy másik anagrammát, és azt visszaküldte Huygensnek. Később, a megfejtések közlésekor az a látszat alakult ki, hogy Huygensnek osztoznia kell az elsőbbségben. Később Wallis beismerte a tréfát, de Huygens soha nem bocsátotta meg neki. Tanulság: aki megfelelő titkosírást akar használni, majd vegye fel a megfelelő választható tárgyat.

Feladat Hányféleképpen keverhetők össze a „MISSISSIPPI” betűi (másként fogalmazva: hány anagrammája van a „MISSISSIPPI” szónak?

Megoldás: Az adott elemeket sorba kell rakni

Feladat Hányféleképpen keverhetők össze a „MISSISSIPPI” betűi (másként fogalmazva: hány anagrammája van a „MISSISSIPPI” szónak?

Megoldás: Az adott elemeket sorba kell rakni $\Longrightarrow$ permutáció, és az adott elemek nem mind különbözők

Feladat Hányféleképpen keverhetők össze a „MISSISSIPPI” betűi (másként fogalmazva: hány anagrammája van a „MISSISSIPPI” szónak?

Megoldás: Az adott elemeket sorba kell rakni $\Longrightarrow$ permutáció, és az adott elemek nem mind különbözők $\Longrightarrow$ ismétléses. Az egyes betűk száma:

Feladat Hányféleképpen keverhetők össze a „MISSISSIPPI” betűi (másként fogalmazva: hány anagrammája van a „MISSISSIPPI” szónak?

Megoldás: Az adott elemeket sorba kell rakni $\Longrightarrow$ permutáció, és az adott elemek nem mind különbözők $\Longrightarrow$ ismétléses. Az egyes betűk száma: $n_M = 1$, $n_I = 4$, $n_S = 4$, $n_P = 2$,

Feladat Hányféleképpen keverhetők össze a „MISSISSIPPI” betűi (másként fogalmazva: hány anagrammája van a „MISSISSIPPI” szónak?

Megoldás: Az adott elemeket sorba kell rakni $\Longrightarrow$ permutáció, és az adott elemek nem mind különbözők $\Longrightarrow$ ismétléses. Az egyes betűk száma: $n_M = 1$, $n_I = 4$, $n_S = 4$, $n_P = 2$, és a betűk száma összesen $n_M + n_I + n_S + n_P = 1 + 4 + 4 + 2 = 11$.

Feladat Hányféleképpen keverhetők össze a „MISSISSIPPI” betűi (másként fogalmazva: hány anagrammája van a „MISSISSIPPI” szónak?

Megoldás: Az adott elemeket sorba kell rakni $\Longrightarrow$ permutáció, és az adott elemek nem mind különbözők $\Longrightarrow$ ismétléses. Az egyes betűk száma: $n_M = 1$, $n_I = 4$, $n_S = 4$, $n_P = 2$, és a betűk száma összesen $n_M + n_I + n_S + n_P = 1 + 4 + 4 + 2 = 11$. Tehát tizenegy betűt (tizenegyelemű rendszert) kell permutálnunk, amelynél az egyes multiplicitások rendre $1, 4, 4, 2$. Az előző tétel szerint az eredmény:

$$\frac{11!}{1! \cdot 4! \cdot 4! \cdot 2!} =$$

Feladat Hányféleképpen keverhetők össze a „MISSISSIPPI” betűi (másként fogalmazva: hány anagrammája van a „MISSISSIPPI” szónak?

Megoldás: Az adott elemeket sorba kell rakni $\Longrightarrow$ permutáció, és az adott elemek nem mind különbözők $\Longrightarrow$ ismétléses. Az egyes betűk száma: $n_M = 1$, $n_I = 4$, $n_S = 4$, $n_P = 2$, és a betűk száma összesen $n_M + n_I + n_S + n_P = 1+4+4+2 = 11$. Tehát tizenegy betűt (tizenegyelemű rendszert) kell permutálnunk, amelynél az egyes multiplicitások rendre $1, 4, 4, 2$. Az előző tétel szerint az eredmény:

$$\frac{11!}{1! \cdot 4! \cdot 4! \cdot 2!} = 34650.$$

Most bebizonyítjuk az ismétléses kombinációk számára vonatkozó tételünket:

7. Tétel. *Legyen* $k, n \in \mathbb{N}$*. Ekkor*

Most bebizonyítjuk az ismétléses kombinációk számára vonatkozó tételünket:

7. Tétel. *Legyen* $k, n \in \mathbf{N}$. *Ekkor* n *elem* k*-adosztályú ismétléses kombinációinak száma,*

Most bebizonyítjuk az ismétléses kombinációk számára vonatkozó tételünket:

7. Tétel. *Legyen* $k, n \in \mathbb{N}$*. Ekkor* n *elem* k*-adosztályú ismétléses kombinációinak száma, más szóval egy* n*-elemű halmaz* k*-elemű részrendszereinek száma*

Most bebizonyítjuk az ismétléses kombinációk számára vonatkozó tételünket:

7. Tétel. *Legyen* $k, n \in \mathbf{N}$. *Ekkor* n *elem* k*-adosztályú ismétléses kombinációinak száma, más szóval egy* n*-elemű halmaz* k*-elemű részrendszereinek száma*

$$\binom{n+k-1}{k}.$$

Az egyszerűség kedvéért legyen $k = 4$

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló).

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz.

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is,

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal;

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal; ehhez csak az kell, hogy a részhalmaz elemeit növekvő sorrendben felírjuk.

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal; ehhez csak az kell, hogy a részhalmaz elemeit növekvő sorrendben felírjuk. Pl. az $\{5, 2, 3, 6\}$ részhalmaz a

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal; ehhez csak az kell, hogy a részhalmaz elemeit növekvő sorrendben felírjuk. Pl. az $\{5, 2, 3, 6\}$ részhalmaz a $(2, 3, 5, 6)$ sorozattal azonosítható.

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n+3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal; ehhez csak az kell, hogy a részhalmaz elemeit növekvő sorrendben felírjuk. Pl. az $\{5, 2, 3, 6\}$ részhalmaz a $(2, 3, 5, 6)$ sorozattal azonosítható. Ezért, ha

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal; ehhez csak az kell, hogy a részhalmaz elemeit növekvő sorrendben felírjuk. Pl. az $\{5, 2, 3, 6\}$ részhalmaz a $(2, 3, 5, 6)$ sorozattal azonosítható. Ezért, ha $S_4(B)$ jelöli a B elemeiből képezhető **S**zigorúan monoton sorozatok halmazát, akkor $|S_4(B)|$ elemszáma

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal; ehhez csak az kell, hogy a részhalmaz elemeit növekvő sorrendben felírjuk. Pl. az $\{5, 2, 3, 6\}$ részhalmaz a $(2, 3, 5, 6)$ sorozattal azonosítható. Ezért, ha $S_4(B)$ jelöli a B elemeiből képezhető **s**zigorúan monoton sorozatok halmazát, akkor $|S_4(B)|$ elemszáma azonos a négyelemű részhalmazok számával, azaz

Az egyszerűség kedvéért legyen $k = 4$ (az általános eset is hasonló). Nyilván az is feltehető, hogy az n-elemű halmaz éppen az $A := \{1, 2, \ldots, n\}$ halmaz. Tekintsük a $B = \{1, \ldots, n + 3\}$ halmazt is, amelynek elemszáma $n + k - 1 = n + 3$.

A B négyelemű részhalmazai azonosíthatók az B elemeiből képezett négyelemű **szigorúan** monoton nővő sorozatokkal; ehhez csak az kell, hogy a részhalmaz elemeit növekvő sorrendben felírjuk. Pl. az $\{5, 2, 3, 6\}$ részhalmaz a $(2, 3, 5, 6)$ sorozattal azonosítható. Ezért, ha $S_4(B)$ jelöli a B elemeiből képezhető **S**zigorúan monoton sorozatok halmazát, akkor $|S_4(B)|$ elemszáma azonos a négyelemű részhalmazok számával, azaz $|S_4(B)| = \binom{n+3}{4} = \binom{n+k-1}{k}$.

Az A négyelemű **résszrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal;

Az A négyelemű **részrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$;

Az A négyelemű **részrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$; ehhez csak az kell, hogy a részrendszer elemeit növekvő sorrendben írjuk fel.

Az A négyelemű **részrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$; ehhez csak az kell, hogy a részrendszer elemeit növekvő sorrendben írjuk fel. Pl. az $\{5, 2, 5, 6\}$ részrendszer a

Az A négyelemű **részrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$; ehhez csak az kell, hogy a részrendszer elemeit növekvő sorrendben írjuk fel. Pl. az $\{5, 2, 5, 6\}$ részrendszer a $(2, 5, 5, 6)$ sorozattal azonosítható.

Az A négyelemű **részrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$; ehhez csak az kell, hogy a részrendszer elemeit növekvő sorrendben írjuk fel. Pl. az $\{5, 2, 5, 6\}$ részrendszer a $(2, 5, 5, 6)$ sorozattal azonosítható. Következésképpen az A négyelemű részrendszereinek (azaz

Az A négyelemű **részrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$; ehhez csak az kell, hogy a részrendszer elemeit növekvő sorrendben írjuk fel. Pl. az $\{5, 2, 5, 6\}$ részrendszer a $(2, 5, 5, 6)$ sorozattal azonosítható. Következésképpen az A négyelemű részrendszereinek (azaz az ismétléses kombinációknak) a száma

Az A négyelemű **résszrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$; ehhez csak az kell, hogy a részrendszer elemeit növekvő sorrendben írjuk fel. Pl. az $\{5, 2, 5, 6\}$ részrendszer a $(2, 5, 5, 6)$ sorozattal azonosítható. Következésképpen az A négyelemű részrendszereinek (azaz az ismétléses kombinációknak) a száma éppen $|T_4(A)|$.

Az A négyelemű **részrendszerei** pedig azonosíthatók az A-ból képezhető négyelemű **t**ágabb értelemben monoton növő részsorozatokkal; az utóbbiak halmazát jelölje $T_4(A)$; ehhez csak az kell, hogy a részrendszer elemeit növekvő sorrendben írjuk fel. Pl. az $\{5, 2, 5, 6\}$ részrendszer a $(2, 5, 5, 6)$ sorozattal azonosítható. Következésképpen az A négyelemű részrendszereinek (azaz az ismétléses kombinációknak) a száma éppen $|T_4(A)|$.

Az eddigiek fényében csak azt kell belátnunk, hogy $|T_4(A)| = |S_4(B)|$. Ezt úgy látjuk be, hogy megadunk egy $\varphi : T_4(A) \to S_4(B)$ bijekciót!

Legyen

$$\varphi : T_4(A) \to S_4(B), \qquad (a_1, a_2, a_3, a_4) \mapsto (a_1, a_2 + 1, a_3 + 2, a_4 + 3).$$

Legyen

$$\varphi : T_4(A) \to S_4(B), \qquad (a_1, a_2, a_3, a_4) \mapsto (a_1, a_2 + 1, a_3 + 2, a_4 + 3).$$

Valóban, ez jó lesz:

Legyen

$$\varphi : T_4(A) \to S_4(B), \quad (a_1, a_2, a_3, a_4) \mapsto (a_1, a_2 + 1, a_3 + 2, a_4 + 3).$$

Valóban, ez jó lesz: mivel $i \in \{1, 2, 3, 4\}$-re $1 \leq a_i \leq n$-ből

$$1 \leq a_i + (i - 1) \leq n + 4 - 1 = n + 3$$

következik, ezért φ A-beli sorozatokhoz B-beli sorozatokat rendel.

Legyen

$$\varphi : T_4(A) \to S_4(B), \quad (a_1, a_2, a_3, a_4) \mapsto (a_1, a_2 + 1, a_3 + 2, a_4 + 3).$$

Valóban, ez jó lesz: mivel $i \in \{1, 2, 3, 4\}$-re $1 \le a_i \le n$-ből

$$1 \le a_i + (i - 1) \le n + 4 - 1 = n + 3$$

következik, ezért φ A-beli sorozatokhoz B-beli sorozatokat rendel. Mivel $a_1 \le a_2 \le a_3 \le a_4$-ből

$$a_1 < a_2 + 1 < a_3 + 2 < a_4 + 3$$

következik, tágabb értelemben monoton sorozatokhoz szigorúan monoton sorozatokat rendel.

Legyen

$$\varphi : T_4(A) \to S_4(B), \quad (a_1, a_2, a_3, a_4) \mapsto (a_1, a_2 + 1, a_3 + 2, a_4 + 3).$$

Valóban, ez jó lesz: mivel $i \in \{1, 2, 3, 4\}$-re $1 \leq a_i \leq n$-ből

$$1 \leq a_i + (i - 1) \leq n + 4 - 1 = n + 3$$

következik, ezért φ A-beli sorozatokhoz B-beli sorozatokat rendel. Mivel $a_1 \leq a_2 \leq a_3 \leq a_4$-ből

$$a_1 < a_2 + 1 < a_3 + 2 < a_4 + 3$$

következik, tágabb értelemben monoton sorozatokhoz szigorúan monoton sorozatokat rendel. Tehát φ csakugyan egy $T_4(A) \to S_4(B)$ leképezés.

Legyen

$$\varphi : T_4(A) \to S_4(B), \quad (a_1, a_2, a_3, a_4) \mapsto (a_1, a_2 + 1, a_3 + 2, a_4 + 3).$$

Valóban, ez jó lesz: mivel $i \in \{1, 2, 3, 4\}$-re $1 \le a_i \le n$-ből

$$1 \le a_i + (i - 1) \le n + 4 - 1 = n + 3$$

következik, ezért φ A-beli sorozatokhoz B-beli sorozatokat rendel. Mivel $a_1 \le a_2 \le a_3 \le a_4$-ből

$$a_1 < a_2 + 1 < a_3 + 2 < a_4 + 3$$

következik, tágabb értelemben monoton sorozatokhoz szigorúan monoton sorozatokat rendel. Tehát φ csakugyan egy $T_4(A) \to S_4(B)$ leképezés. Mivel $(a_1, a_2 + 1, a_3 + 2, a_4 + 3)$ nyilván meghatározza (a_1, a_2, a_3, a_4)-et, ezért φ injektív.

A szürjektivitás igazolásához legyen $(b_1, b_2, b_3, b_4) \in S_4(B)$.

A szürjektivitás igazolásához legyen $(b_1, b_2, b_3, b_4) \in S_4(B)$. Azaz $1 \leq b_1 < b_2 < b_3 < b_4 \leq n + 3$.

A szürjektivitás igazolásához legyen $(b_1, b_2, b_3, b_4) \in S_4(B)$. Azaz $1 \le b_1 < b_2 < b_3 < b_4 \le n + 3$. Mivel egész számokról van szó, A szürjektivitás igazolásához legyen $(b_1, b_2, b_3, b_4) \in S_4(B)$. Azaz $1 \leq b_1 < b_2 < b_3 < b_4 \leq n + 3$. Mivel egész számokról van szó, $1 \leq b_1 \leq b_2 - 1 \leq b_3 - 2 \leq b_4 - 3 \leq n + 3 - 3 = n$.

A szürjektivitás igazolásához legyen $(b_1, b_2, b_3, b_4) \in S_4(B)$. Azaz $1 \leq b_1 < b_2 < b_3 < b_4 \leq n + 3$. Mivel egész számokról van szó, $1 \leq b_1 \leq b_2 - 1 \leq b_3 - 2 \leq b_4 - 3 \leq n + 3 - 3 = n$. Ezért a $(b_1, b_2 - 1, b_3 - 2, b_4 - 3)$ sorozat $T_4(A)$-beli, A szürjektivitás igazolásához legyen $(b_1, b_2, b_3, b_4) \in S_4(B)$. Azaz $1 \leq b_1 < b_2 < b_3 < b_4 \leq n + 3$. Mivel egész számokról van szó, $1 \leq b_1 \leq b_2 - 1 \leq b_3 - 2 \leq b_4 - 3 \leq n + 3 - 3 = n$. Ezért a $(b_1, b_2 - 1, b_3 - 2, b_4 - 3)$ sorozat $T_4(A)$-beli, és nyilván őse a (b_1, b_2, b_3, b_4) sorozatnak.

A szürjektivitás igazolásához legyen $(b_1, b_2, b_3, b_4) \in S_4(B)$. Azaz $1 \le b_1 < b_2 < b_3 < b_4 \le n + 3$. Mivel egész számokról van szó, $1 \le b_1 \le b_2 - 1 \le b_3 - 2 \le b_4 - 3 \le n + 3 - 3 = n$. Ezért a $(b_1, b_2 - 1, b_3 - 2, b_4 - 3)$ sorozat $T_4(A)$-beli, és nyilván őse a (b_1, b_2, b_3, b_4) sorozatnak. Q.e.d.

Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \to V$ bijekciót, és a V halmaz elemeit számoljuk meg (

Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \longrightarrow V$ bijekciót, és a V halmaz elemeit számoljuk meg (hiszen ekkor $|U| = |V|$).

Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \to V$ bijekciót, és a V halmaz elemeit számoljuk meg (hiszen ekkor $|U| = |V|$). A bijekció egyik (implicit) formája és szintén nagyon gyakori kombinatorikai fogás az, Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \to V$ bijekciót, és a V halmaz elemeit számoljuk meg (hiszen ekkor $|U| = |V|$). A bijekció egyik (implicit) formája és szintén nagyon gyakori kombinatorikai fogás az, amikor valamit valami másnak tekintünk.

Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \to V$ bijekciót, és a V halmaz elemeit számoljuk meg (hiszen ekkor $|U| = |V|$). A bijekció egyik (implicit) formája és szintén nagyon gyakori kombinatorikai fogás az, amikor valamit valami másnak tekintünk. Pl. az előző megfontolásban a részhalmazt szigorúan monoton sorozatnak tekintettük — ha

Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \to V$ bijekciót, és a V halmaz elemeit számoljuk meg (hiszen ekkor $|U| = |V|$). A bijekció egyik (implicit) formája és szintén nagyon gyakori kombinatorikai fogás az, amikor valamit valami másnak tekintünk. Pl. az előző megfontolásban a részhalmazt szigorúan monoton sorozatnak tekintettük — ha még precízebben akartunk volna fogalmazni (— de

Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \to V$ bijekciót, és a V halmaz elemeit számoljuk meg (hiszen ekkor $|U| = |V|$). A bijekció egyik (implicit) formája és szintén nagyon gyakori kombinatorikai fogás az, amikor valamit valami másnak tekintünk. Pl. az előző megfontolásban a részhalmazt szigorúan monoton sorozatnak tekintettük — ha még precízebben akartunk volna fogalmazni (— de didaktikai okokból nem akartunk —), akkor

Gyakori fogás a kombinatorikában, hogy amikor egy U halmaz elemeit akarjuk megszámolni, akkor tekintünk egy $U \to V$ bijekciót, és a V halmaz elemeit számoljuk meg (hiszen ekkor $|U| = |V|$). A bijekció egyik (implicit) formája és szintén nagyon gyakori kombinatorikai fogás az, amikor valamit valami másnak tekintünk. Pl. az előző megfontolásban a részhalmazt szigorúan monoton sorozatnak tekintettük — ha még precízebben akartunk volna fogalmazni (— de didaktikai okokból nem akartunk —), akkor azt mondtuk volna, hogy egy bijekciót tekintünk a négyelemű részhalmazok halmaza és a négyelemű szigorúan monoton sorozatok halmaza között.

Most az alábbi, korábban már megfogalmazott tételt fogjuk bizonyítani:

Most az alábbi, korábban már megfogalmazott tételt fogjuk bizonyítani:

Az alapkérdés az, hogy hányféleképpen rakhatók sorba egy n-elemű **rendszer** elemei — egy ilyen sorbarakást (vagy sorozatba rendezést) az n elem egy **ismétléses permutációjának** nevezzük.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek;

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek; mindegyik annyiszor, amennyi a multiplicitása.

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek; mindegyik annyiszor, amennyi a multiplicitása.

8. Tétel. *Ha $k_1 + \cdots + k_r = n$, akkor egy n-elemű, r különböző elemből álló rendszer esetén ha ez egyes elemek multiplicitása k_1, ..., k_r, akkor a rendszer elemei*

Pontosabban: Adott $n, r \in \mathbf{N}$ és $k_1, \ldots, k_r \in \mathbf{N}$ úgy, hogy $k_1 + \cdots + k_r = n$. Tekintsünk egy n-elemű H rendszert, amelyben pontosan r különböző elem van, és az egyes elemek multiplicitása rendre $k_1, \ldots, k_r$. Ismétléses permutációnak nevezünk egy olyan n-tagú sorozatot, amelyben pontosan a H elemei szerepelnek; mindegyik annyiszor, amennyi a multiplicitása.

8. Tétel. *Ha $k_1 + \cdots + k_r = n$, akkor egy n-elemű, r különböző elemből álló rendszer esetén ha ez egyes elemek multiplicitása k_1, ..., k_r, akkor a rendszer elemei*

$$\frac{n!}{k_1! \ldots k_r!}$$

féleképpen rakhatók sorba.

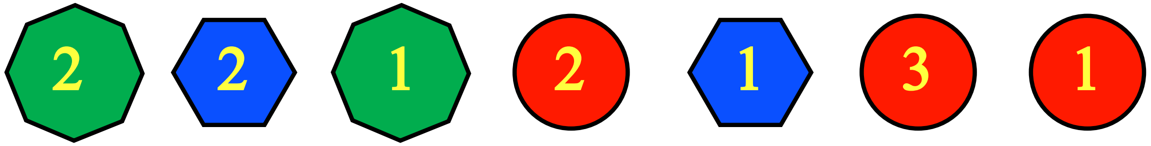
Bizonyítás: Legyen az áttekinthetőség kedvéért $n = 7$, $r = 3$, $k_1 = 3$, $k_2 = 2$ és $k_3 = 2$

Bizonyítás: Legyen az áttekinthetőség kedvéért $n = 7$, $r = 3$, $k_1 = 3$, $k_2 = 2$ és $k_3 = 2$

Tegyük fel, vannak golyóink $r = 3$-féle színben: $k_1 = 3$ darab (kerek) piros, $k_2 = 2$ darab (hatszögletű) kék és $k_3 = 2$ darab (nyolcszögletű) zöld.

Bizonyítás: Legyen az áttekinthetőség kedvéért $n = 7$, $r = 3$, $k_1 = 3$, $k_2 = 2$ és $k_3 = 2$

Tegyük fel, vannak golyóink $r = 3$-féle színben: $k_1 = 3$ darab (kerek) piros, $k_2 = 2$ darab (hatszögletű) kék és $k_3 = 2$ darab (nyolcszögletű) zöld. (Mivel a színek nem biztos, hogy jól láthatók, eltérő formákat alkalmazunk). Az azonos színű golyókat sorszámok különböztetik meg egymástól:



Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót.

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk,

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

De most máshogy is számoljuk meg.

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

De most máshogy is számoljuk meg. Töröljük le a számokat a golyókról, így már nem lesznek mind különbözők,

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

De most máshogy is számoljuk meg. Töröljük le a számokat a golyókról, így már nem lesznek mind különbözők, csak a szín különbözteti meg őket.

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

De most máshogy is számoljuk meg. Töröljük le a számokat a golyókról, így már nem lesznek mind különbözők, csak a szín különbözteti meg őket. Tehát van hét golyó, de rendre 3, 2 és 2 egyforma.

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

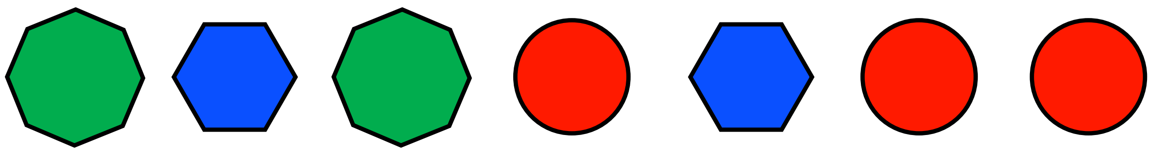
De most máshogy is számoljuk meg. Töröljük le a számokat a golyókról, így már nem lesznek mind különbözők, csak a szín különbözteti meg őket. Tehát van hét golyó, de rendre 3, 2 és 2 egyforma. Ezeket x-féleképpen tudjuk sorbarakni. (x ismeretlen, a cél az, hogy meghatározzuk.) Mármost úgy rakjuk sorba a számozott golyókat, hogy előbb —

Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

De most máshogy is számoljuk meg. Töröljük le a számokat a golyókról, így már nem lesznek mind különbözők, csak a szín különbözteti meg őket. Tehát van hét golyó, de rendre 3, 2 és 2 egyforma. Ezeket x-féleképpen tudjuk sorbarakni. (x ismeretlen, a cél az, hogy meghatározzuk.) Mármost úgy rakjuk sorba a számozott golyókat, hogy előbb —az összes lehetséges módon, azaz x féleképpen —

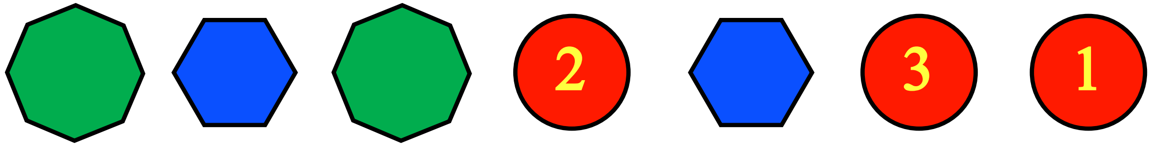
Számoljuk meg, hogy hányféleképpen rakhatjuk sorba ezt a hét **különböző** golyót. Egyrészt tudjuk, hogy 7!-féleképpen.

De most máshogy is számoljuk meg. Töröljük le a számokat a golyókról, így már nem lesznek mind különbözők, csak a szín különbözteti meg őket. Tehát van hét golyó, de rendre 3, 2 és 2 egyforma. Ezeket x-féleképpen tudjuk sorbarakni. (x ismeretlen, a cél az, hogy meghatározzuk.) Mármost úgy rakjuk sorba a számozott golyókat, hogy előbb —az összes lehetséges módon, azaz x féleképpen — sorbarakjuk a számozatlan golyókat:

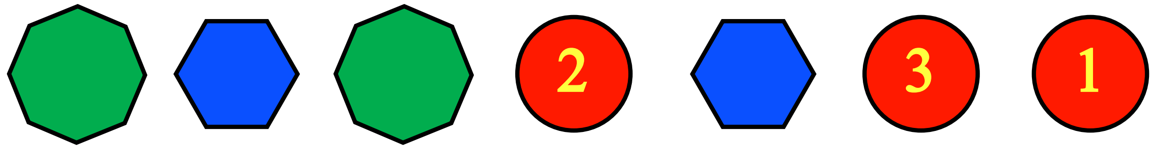


Ezt követően számozzuk be a három piros golyót:

Ezt követően számozzuk be a három piros golyót:

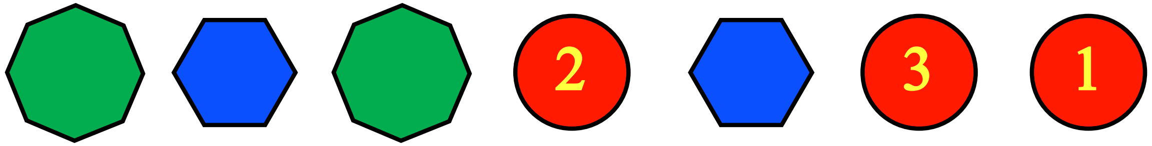


Ezt követően számozzuk be a három piros golyót:



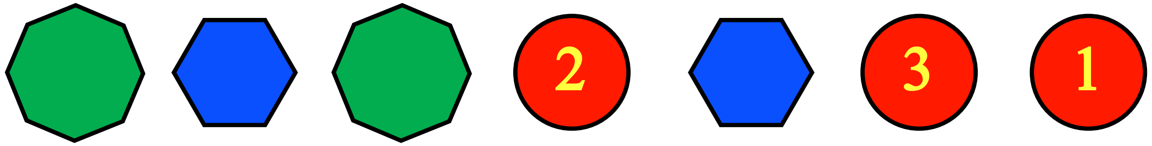
Ez

Ezt követően számozzuk be a három piros golyót:



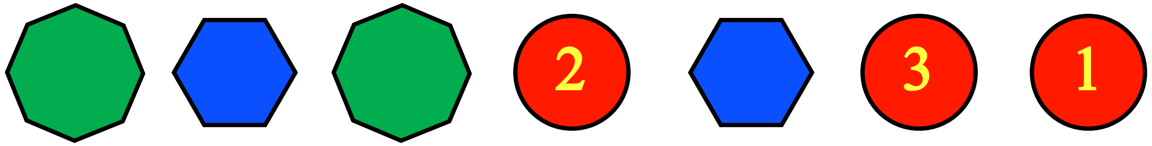
Ez 3!-féleképpen tehető,

Ezt követően számozzuk be a három piros golyót:



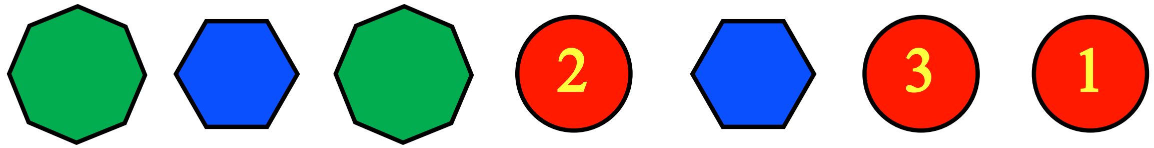
Ez 3!-féleképpen tehető, függetlenül attól, hogy milyen sorrendben vannak a számozatlan golyók. (Azért

Ezt követően számozzuk be a három piros golyót:



Ez 3!-féleképpen tehető, függetlenül attól, hogy milyen sorrendben vannak a számozatlan golyók. (Azért 3!-féleképpen, mert az 1, 2, 3 sorszámokat a rögzített helyzetű piros golyók között ennyiféleképpen permutálhatjuk.)

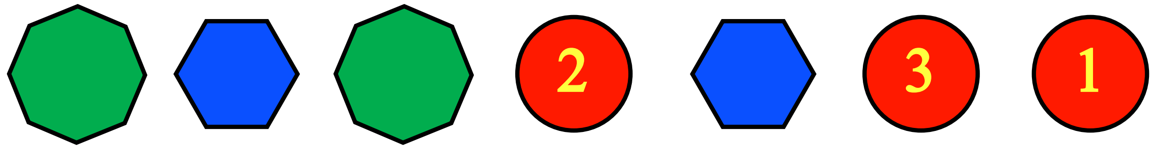
Ezt követően számozzuk be a három piros golyót:



Ez 3!-féleképpen tehető, függetlenül attól, hogy milyen sorrendben vannak a számozatlan golyók. (Azért 3!-féleképpen, mert az 1, 2, 3 sorszámokat a rögzített helyzetű piros golyók között ennyiféleképpen permutálhatjuk.)

A szorzási szabály szerint így

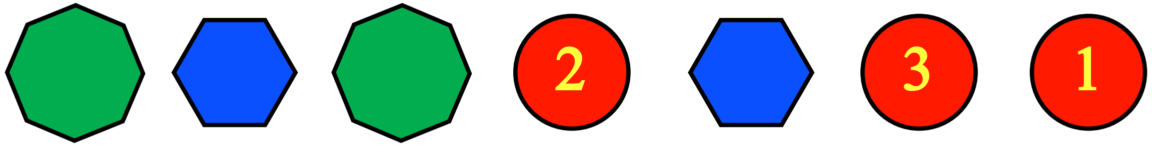
Ezt követően számozzuk be a három piros golyót:



Ez 3!-féleképpen tehető, függetlenül attól, hogy milyen sorrendben vannak a számozatlan golyók. (Azért 3!-féleképpen, mert az 1, 2, 3 sorszámokat a rögzített helyzetű piros golyók között ennyiféleképpen permutálhatjuk.)

A szorzási szabály szerint így a számozott piros és a számozatlan többi golyónak összesen $3! \cdot x$ sorrendje van.

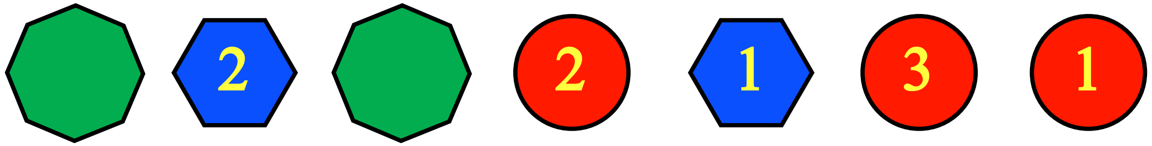
Ezt követően számozzuk be a három piros golyót:

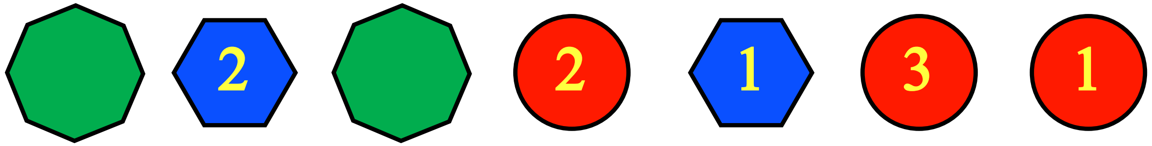


Ez 3!-féleképpen tehető, függetlenül attól, hogy milyen sorrendben vannak a számozatlan golyók. (Azért 3!-féleképpen, mert az 1, 2, 3 sorszámokat a rögzített helyzetű piros golyók között ennyiféleképpen permutálhatjuk.)

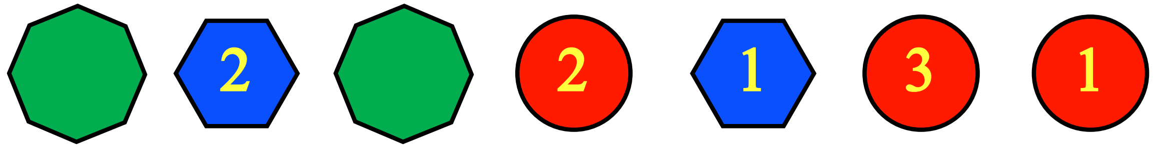
A szorzási szabály szerint így a számozott piros és a számozatlan többi golyónak összesen $3! \cdot x$ sorrendje van.

Most — bármi is az eddigi sorrend — számozzuk be a két darab kék golyót:

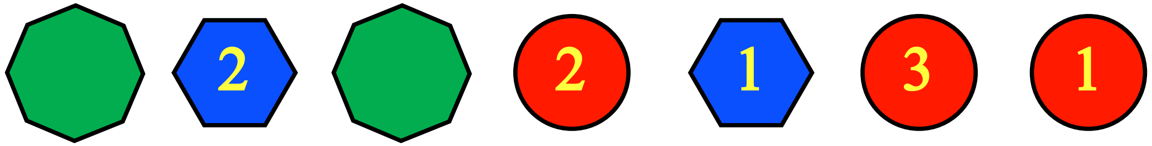

2
2
1
3
1



ez minden esetben 2!-féleképpen tehető.



ez minden esetben 2!-féleképpen tehető. Tehát — újból a szorzási szabályt alkalmazva —



ez minden esetben 2!-féleképpen tehető. Tehát — újból a szorzási szabályt alkalmazva — a számozott piros, számozott kék és számozatlan zöld golyók $2! \cdot 3! \cdot x$-féleképpen rakhatók sorba.

Bárhogy is juttottunk el az eddigi sorrendhez, a két zöld golyó 2!-féleképpen számozható be.

Bárhogy is juttottunk el az eddigi sorrendhez, a két zöld golyó 2!-féleképpen számozható be. Tehát — a szorzási szabály szerint — amikor már minden golyót beszámoztunk, akkor

Bárhogy is juttottunk el az eddigi sorrendhez, a két zöld golyó 2!-féleképpen számozható be. Tehát — a szorzási szabály szerint — amikor már minden golyót beszámoztunk, akkor $2! \cdot 2! \cdot 3! \cdot x$-féle sorrend van.

Bárhogy is juttottunk el az eddigi sorrendhez, a két zöld golyó 2!-féleképpen számozható be. Tehát — a szorzási szabály szerint — amikor már minden golyót beszámoztunk, akkor $2! \cdot 2! \cdot 3! \cdot x$-féle sorrend van. De tudjuk, hogy ekkor (hét különböző golyó lévén) 7! sorrend van. Innen

Bárhogy is juttottunk el az eddigi sorrendhez, a két zöld golyó 2!-féleképpen számozható be. Tehát — a szorzási szabály szerint — amikor már minden golyót beszámoztunk, akkor $2! \cdot 2! \cdot 3! \cdot x$-féle sorrend van. De tudjuk, hogy ekkor (hét különböző golyó lévén) 7! sorrend van. Innen x kifejezhető:

$$x = \frac{7!}{3! \cdot 2! \cdot 2!} = \frac{n!}{k_1! \ldots k_r!}$$

Bárhogy is juttottunk el az eddigi sorrendhez, a két zöld golyó 2!-féleképpen számozható be. Tehát — a szorzási szabály szerint — amikor már minden golyót beszámoztunk, akkor $2! \cdot 2! \cdot 3! \cdot x$-féle sorrend van. De tudjuk, hogy ekkor (hét különböző golyó lévén) 7! sorrend van. Innen x kifejezhető:

$$x = \frac{7!}{3! \cdot 2! \cdot 2!} = \frac{n!}{k_1! \ldots k_r!}$$

, és éppen ez a tétel állítása ezen speciális adatok esetén. (

Bárhogy is juttottunk el az eddigi sorrendhez, a két zöld golyó 2!-féleképpen számozható be. Tehát — a szorzási szabály szerint — amikor már minden golyót beszámoztunk, akkor $2! \cdot 2! \cdot 3! \cdot x$-féle sorrend van. De tudjuk, hogy ekkor (hét különböző golyó lévén) 7! sorrend van. Innen x kifejezhető:

$$x = \frac{7!}{3! \cdot 2! \cdot 2!} = \frac{n!}{k_1! \dots k_r!}$$

, és éppen ez a tétel állítása ezen speciális adatok esetén. (Az általános eset teljesen hasonló.) Q.e.d.

Feladat: Hófehérke huszonnégy **különböző** süteményt sütött a hét törpének.

Feladat: Hófehérke huszonnégy **különböző** süteményt sütött a hét törpének. Hányféleképpen oszthatja szét közöttük a süteményeket, ha

Feladat: Hófehérke huszonnégy **különböző** süteményt sütött a hét törpének. Hányféleképpen oszthatja szét közöttük a süteményeket, ha H**A**pci öt, Szun**D**i négy, a többiek pedig fejenként három süteményt kapnak?

Feladat: Hófehérke huszonnégy **különböző** süteményt sütött a hét törpének. Hányféleképpen oszthatja szét közöttük a süteményeket, ha H**A**pci öt, Szun**D**i négy, a többiek pedig fejenként három süteményt kapnak?

Megoldás: Legyen — a rövidség kedvéért —

Feladat: Hófehérke huszonnégy **különböző** süteményt sütött a hét törpének. Hányféleképpen oszthatja szét közöttük a süteményeket, ha H**A**pci öt, Szun**D**i négy, a többiek pedig fejenként három süteményt kapnak?

Megoldás: Legyen — a rövidség kedvéért — A, B, C, D, E, F, G a törpék betűjele ($A =$ H**A**pci, $D =$ Szun**D**i)).

A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, hogy ezen osztályoknak nevük

A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, hogy ezen osztályoknak nevük (vagy ami ezzel ekvivalens, A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, hogy ezen osztályoknak nevük (vagy ami ezzel ekvivalens, rögzített sorrendjük van), és az egyes

A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, hogy ezen osztályoknak nevük (vagy ami ezzel ekvivalens, rögzített sorrendjük van), és az egyes osztályok elemszáma is meg van mondva (az A osztály elemszáma 5, A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, hogy ezen osztályoknak nevük (vagy ami ezzel ekvivalens, rögzített sorrendjük van), és az egyes osztályok elemszáma is meg van mondva (az A osztály elemszáma 5, a D osztály elemszáma 4, A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, hogy ezen osztályoknak nevük (vagy ami ezzel ekvivalens, rögzített sorrendjük van), és az egyes osztályok elemszáma is meg van mondva (az A osztály elemszáma 5, a D osztály elemszáma 4, a többi osztály elemszáma pedig 3.)

A feladat tulajdonképpen az, hogy hányféleképpen sorolhatjuk a 24 süteményt hét osztályba oly módon, hogy ezen osztályoknak nevük (vagy ami ezzel ekvivalens, rögzített sorrendjük van), és az egyes osztályok elemszáma is meg van mondva (az A osztály elemszáma 5, a D osztály elemszáma 4, a többi osztály elemszáma pedig 3.) Az ilyen fajta osztályozást szokás $(5, 3, 3, 4, 3, 3, 3)$ típusú **rendezett osztályozásnak** nevezni. Ezek számára is van egy tétel a könyvben, ezen tétel használata elkerülhető, ha már az ismétléses permutációkat ismerjük. Ezt példázza a jelen feladat is.

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**.

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**. A jelen esetben: Hófehérke egy fix sorrendben lerakja a 24 süteményt az asztalra.

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**. A jelen esetben: Hófehérke egy fix sorrendben lerakja a 24 süteményt az asztalra. Majd felír öt darab A, négy darab D és három-három darab B, C, E, F, G betűt egy-egy cédulára.

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**. A jelen esetben: Hófehérke egy fix sorrendben lerakja a 24 süteményt az asztalra. Majd felír öt darab A, négy darab D és három-három darab B, C, E, F, G betűt egy-egy cédulára. Így kap 24 cédulát.

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**. A jelen esetben: Hófehérke egy fix sorrendben lerakja a 24 süteményt az asztalra. Majd felír öt darab A, négy darab D és három-három darab B, C, E, F, G betűt egy-egy cédulára. Így kap 24 cédulát. Minden süteményen elhelyez egy cédulát,

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**. A jelen esetben: Hófehérke egy fix sorrendben lerakja a 24 süteményt az asztalra. Majd felír öt darab A, négy darab D és három-három darab B, C, E, F, G betűt egy-egy cédulára. Így kap 24 cédulát. Minden süteményen elhelyez egy cédulát, és a törpék a betűjelüknek megfelelő süteményt kapják.

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**. A jelen esetben: Hófehérke egy fix sorrendben lerakja a 24 süteményt az asztalra. Majd felír öt darab A, négy darab D és három-három darab B, C, E, F, G betűt egy-egy cédulára. Így kap 24 cédulát. Minden süteményen elhelyez egy cédulát, és a törpék a betűjelüknek megfelelő süteményt kapják. Annyiféleképpen helyezheti el a cédulákat, ahányféleképpen a tekintett betűk sorbarakhatók, azaz

$$\frac{24!}{5! \cdot 4! \cdot (3!)^5}$$

Tipikus fogás a kombinatorikában: nem a tárgyakat osztjuk ki az embereknek, hanem **fordítva**. A jelen esetben: Hófehérke egy fix sorrendben lerakja a 24 süteményt az asztalra. Majd felír öt darab A, négy darab D és három-három darab B, C, E, F, G betűt egy-egy cédulára. Így kap 24 cédulát. Minden süteményen elhelyez egy cédulát, és a törpék a betűjelüknek megfelelő süteményt kapják. Annyiféleképpen helyezheti el a cédulákat, ahányféleképpen a tekintett betűk sorbarakhatók, azaz

$$\frac{24!}{5! \cdot 4! \cdot (3!)^5} = 27\,704\,921\,916\,672\,000.$$

Természetesen vizsgán nem kell nagy számokkal számolni.

Binomiális tétel

Binomiális tétel

Most kiderül, honnan ered a „binomiális együttható” elnevezés.

9. Tétel. *Ha* $n \in \mathbb{N}$*, továbbá* a *és* b *valós számokat vagy valós határozatlanokat jelöl, akkor*

Binomiális tétel

Most kiderül, honnan ered a „binomiális együttható” elnevezés.

9. Tétel. *Ha* $n \in \mathbf{N}$, *továbbá* a *és* b *valós számokat vagy valós határozatlanokat jelöl, akkor*

$$(a+b)^n =$$

Binomiális tétel

Most kiderül, honnan ered a „binomiális együttható” elnevezés.

9. Tétel. *Ha $n \in \mathbf{N}$, továbbá a és b valós számokat vagy valós határozatlanokat jelöl, akkor*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i =$$

Binomiális tétel

Most kiderül, honnan ered a „binomiális együttható” elnevezés.

9. Tétel. *Ha $n \in \mathbb{N}$, továbbá a és b valós számokat vagy valós határozatlanokat jelöl, akkor*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i =$$

$$\binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n.$$

A „binom" jelentése: „kéttag

A „binom" jelentése: „kéttag(ú)",

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek:

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 =$$

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 +$$

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 +$$

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 =$

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = \binom{3}{0}a^3 +$$

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+$$

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+$$

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

A „binom" jelentése: „kéttag(ú)", a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás:

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.)

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.) Pl.

$(a_1 + a_2 + a_3) \cdot (b_1 + b_2) =$

A „binom'' jelentése: „kéttag(ú)'', a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.) Pl.

$(a_1 + a_2 + a_3) \cdot (b_1 + b_2) = a_1b_1 +$

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.) Pl.

$$(a_1 + a_2 + a_3) \cdot (b_1 + b_2) = a_1b_1 + a_1b_2 +$$

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.) Pl.

$(a_1 + a_2 + a_3) \cdot (b_1 + b_2) = a_1b_1 + a_1b_2 + a_2b_1 +$

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.) Pl.

$$(a_1+a_2+a_3)\cdot(b_1+b_2) = a_1b_1+a_1b_2+a_2b_1+a_2b_2+$$

A „binom" jelentése: „kéttag(ú)", a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.) Pl.

$$(a_1 + a_2 + a_3) \cdot (b_1 + b_2) = a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2 + a_3b_1 +$$

A „binom” jelentése: „kéttag(ú)”, a binomiális tétel pedig a kéttagú összeg hatványaira vonatkozik. Speciális esetei már a középiskolában is jól ismertek: két tag összegének négyzete és köbe:

$$(a+b)^2 = a^2 + 2ab + b^2 = \binom{2}{0}a^2 + \binom{2}{1}a^1b^1 + \binom{2}{2}b^2,$$

$$(a+b)^3 = a^3+3a^2b+3ab^2+b^3 = \binom{3}{0}a^3+\binom{3}{1}a^2b^1+\binom{3}{2}a^1b^2+\binom{3}{3}b^3.$$

Bizonyítás: Amikor több tagot több taggal szorzunk, akkor minden tagot minden tagot szorzunk, és a kapott szorzatokat összeadjuk. (Így bontjuk fel a zárójeleket, és ezt azért tehetjük, mert a szorzás disztributív az összeadásra nézve.) Pl.

$$(a_1+a_2+a_3)\cdot(b_1+b_2) = a_1b_1+a_1b_2+a_2b_1+a_2b_2+a_3b_1+a_3b_2$$

vagy — az előbbi ismételt alkalmazásával —

$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) =$

vagy — az előbbi ismételt alkalmazásával —

$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+$

vagy — az előbbi ismételt alkalmazásával —

$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+$

vagy — az előbbi ismételt alkalmazásával —

$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$
$$a_1b_3c_1 +$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$
$$a_1b_3c_1 + a_1b_3c_2 +$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$
$$a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 +$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$
$$a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 +$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+ \\ a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 + a_2b_2c_1+$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$
$$a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 + a_2b_2c_1+$$
$$a_2b_2c_2 +$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$
$$a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 + a_2b_2c_1+$$
$$a_2b_2c_2 + a_2b_3c_1 +$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+ a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 + a_2b_2c_1+ a_2b_2c_2 + a_2b_3c_1 + a_2b_3c_2.$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+ \\ a_1b_3c_1+a_1b_3c_2+a_2b_1c_1+a_2b_1c_2+a_2b_2c_1+ \\ a_2b_2c_2+a_2b_3c_1+a_2b_3c_2.$$

Látható, hogy az összeg tagjai olyan szorzatok, amelyek mindegyik zárójelezett összegből pontosan egy tagot tartalmaznak tényezőként,

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+ a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 + a_2b_2c_1+ a_2b_2c_2 + a_2b_3c_1 + a_2b_3c_2.$$

Látható, hogy az összeg tagjai olyan szorzatok, amelyek mindegyik zárójelezett összegből pontosan egy tagot tartalmaznak tényezőként, és annyi tagja van az összegnek, ahányféleképpen az egyes összegekből

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+ a_1b_3c_1+a_1b_3c_2+a_2b_1c_1+a_2b_1c_2+a_2b_2c_1+ a_2b_2c_2+a_2b_3c_1+a_2b_3c_2.$$

Látható, hogy az összeg tagjai olyan szorzatok, amelyek mindegyik zárójelezett összegből pontosan egy tagot tartalmaznak tényezőként, és annyi tagja van az összegnek, ahányféleképpen az egyes összegekből egy-egy tagot ki lehet választani. A fenti példa esetén $2\cdot 3\cdot 2 = 12$-tagú az összeg.

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+$$
$$a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 + a_2b_2c_1+$$
$$a_2b_2c_2 + a_2b_3c_1 + a_2b_3c_2.$$

Látható, hogy az összeg tagjai olyan szorzatok, amelyek mindegyik zárójelezett összegből pontosan egy tagot tartalmaznak tényezőként, és annyi tagja van az összegnek, ahányféleképpen az egyes összegekből egy-egy tagot ki lehet választani. A fenti példa esetén $2 \cdot 3 \cdot 2 = 12$-tagú az összeg. Az eddigiek szerint az

$$(a+b)^n =$$

vagy — az előbbi ismételt alkalmazásával —

$$(a_1+a_2)\cdot(b_1+b_2+b_3)\cdot(c_1+c_2) = a_1b_1c_1+a_1b_1c_2+a_1b_2c_1+a_1b_2c_2+ \\ a_1b_3c_1 + a_1b_3c_2 + a_2b_1c_1 + a_2b_1c_2 + a_2b_2c_1+ \\ a_2b_2c_2 + a_2b_3c_1 + a_2b_3c_2.$$

Látható, hogy az összeg tagjai olyan szorzatok, amelyek mindegyik zárójelezett összegből pontosan egy tagot tartalmaznak tényezőként, és annyi tagja van az összegnek, ahányféleképpen az egyes összegekből egy-egy tagot ki lehet választani. A fenti példa esetén $2 \cdot 3 \cdot 2 = 12$-tagú az összeg. Az eddigiek szerint az

$$(a+b)^n = (a+b)\dots(a+b)$$

egy 2^n-tagú összeg lesz, hiszen mindegyik kéttagú összegből kétféleképpen választhatunk:

egy 2^n-tagú összeg lesz, hiszen mindegyik kéttagú összegből kétféleképpen választhatunk: a-t vagy b-t.

egy 2^n-tagú összeg lesz, hiszen mindegyik kéttagú összegből kétféleképpen választhatunk: a-t vagy b-t. Azonban az így kapott soktagú összegben bizonyos tagok csak a tényezők sorrendjében térnek el, egy 2^n-tagú összeg lesz, hiszen mindegyik kéttagú összegből kétféleképpen választhatunk: a-t vagy b-t. Azonban az így kapott soktagú összegben bizonyos tagok csak a tényezők sorrendjében térnek el, ezek tehát összevonhatók.

egy 2^n-tagú összeg lesz, hiszen mindegyik kéttagú összegből kétféleképpen választhatunk: a-t vagy b-t. Azonban az így kapott soktagú összegben bizonyos tagok csak a tényezők sorrendjében térnek el, ezek tehát összevonhatók. Pl. amikor $n = 6$, akkor az $aabbbb$, $abbbba$ és $bababb$ tagok (és továbbiak is) mindegyike a^2b^4-nel egyenlő.

egy 2^n-tagú összeg lesz, hiszen mindegyik kéttagú összegből kétféleképpen választhatunk: a-t vagy b-t. Azonban az így kapott soktagú összegben bizonyos tagok csak a tényezők sorrendjében térnek el, ezek tehát összevonhatók. Pl. amikor $n = 6$, akkor az $aabbbb$, $abbbba$ és $bababb$ tagok (és továbbiak is) mindegyike a^2b^4-nel egyenlő. Hány tag egyenlő a^2b^4-nel?

egy 2^n-tagú összeg lesz, hiszen mindegyik kéttagú összegből kétféleképpen választhatunk: a-t vagy b-t. Azonban az így kapott soktagú összegben bizonyos tagok csak a tényezők sorrendjében térnek el, ezek tehát összevonhatók. Pl. amikor $n = 6$, akkor az $aabbbb$, $abbbba$ és $bababb$ tagok (és továbbiak is) mindegyike a^2b^4-nel egyenlő. Hány tag egyenlő a^2b^4-nel? Annyi, ahányféleképpen sorba tudunk két a betűt és négy b betűt. Ezt a számot az ismétléses permutációk számára vonatkozó tétel adja:

$$\frac{6!}{2! \cdot 4!}$$

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0, 1, \ldots, n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0, 1, \ldots, n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen $\binom{n}{i}$. Ezért

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0, 1, \ldots, n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen $\binom{n}{i}$. Ezért $(a+b)^n =$

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0, 1, \ldots, n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen $\binom{n}{i}$. Ezért $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i$.

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0, 1, \ldots, n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen $\binom{n}{i}$. Ezért $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$. Q.e.d.

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0, 1, \ldots, n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen $\binom{n}{i}$. Ezért $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i$. Q.e.d.

A fenti megfontolásban a binomiális együtthatók csak a legvégén jöttek be.

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0, 1, \ldots, n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen $\binom{n}{i}$. Ezért $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$. Q.e.d.

A fenti megfontolásban a binomiális együtthatók csak a legvégén jöttek be. Ha nem két, hanem többtagú összeget hatványozunk, akkor — teljesen hasonló gondolatmenet miatt — érvényes az alábbi

Az általános esetben, amikor az $(a+b)^n$ hatványt számoljuk ki, adott $i \in \{0,1,\ldots,n\}$ esetén az $a^{n-i}b^i$ annyiszor lép fel, ahányféleképpen $n-i$ darab a betűt és i darab b betűt sorba tudunk rakni, azaz

$$\frac{n!}{i! \cdot (n-i)!}$$

féleképpen. Ez a szám azonban éppen $\binom{n}{i}$. Ezért $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$. Q.e.d.

A fenti megfontolásban a binomiális együtthatók csak a legvégén jöttek be. Ha nem két, hanem többtagú összeget hatványozunk, akkor — teljesen hasonló gondolatmenet miatt — érvényes az alábbi

10. Tétel. (**Polinomiális tétel**)

$$(a_1 + \cdots + a_k)^n = \sum_{\substack{(i_1, \ldots, i_k) \in \mathbf{N}_0 \\ i_1 + \cdots + i_k = n}} \frac{n!}{i_1! \cdots i_k!} \, a_1^{i_1} a_2^{i_2} \ldots a_k^{i_k}.$$

Megjegyzés: Érdemes a binomiális együtthatókat egy táblázatba foglalni:

$$\binom{0}{0}$$

Megjegyzés: Érdemes a binomiális együtthatókat egy táblázatba foglalni:

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

Megjegyzés: Érdemes a binomiális együtthatókat egy táblázatba foglalni:

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

Megjegyzés: Érdemes a binomiális együtthatókat egy táblázatba foglalni:

$$\begin{matrix}
 & & & \binom{0}{0} & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3}
\end{matrix}$$

Megjegyzés: Érdemes a binomiális együtthatókat egy táblázatba foglalni:

$$\binom{0}{0}$$
$$\binom{1}{0} \quad \binom{1}{1}$$
$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$
$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$
$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

Megjegyzés: Érdemes a binomiális együtthatókat egy táblázatba foglalni:

$$
\begin{array}{ccccccccccc}
 & & & & & \binom{0}{0} & & & & & \\
 & & & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5}
\end{array}
$$

Megjegyzés: Érdemes a binomiális együtthatókat egy táblázatba foglalni:

$$\binom{0}{0}$$
$$\binom{1}{0} \quad \binom{1}{1}$$
$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$
$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$
$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$
$$\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5}$$
$$\ldots$$

Ezt a háromszög alakú táblázatot **Pascal-háromszögnek** nevezik. Az n-edik sor i-edik eleme éppen az $\binom{n}{i}$ binomiális együtthatót adja meg (ha a számolást nullától kezdjük). A konkrét értékeket kiszámítva:

1

1 1

1

1 1

1 2 1

1

1 1

1 2 1

1 3 3 1

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

. . .

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad \boxed{4} \quad \boxed{6} \quad 4 \quad 1 \\
1 \quad 5 \quad \boxed{10} \quad 10 \quad 5 \quad 1 \\
\ldots
\end{array}
$$

Látható, hogy a táblázat szélén 1-esek vannak,

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad \boxed{4} \quad \boxed{6} \quad 4 \quad 1 \\
1 \quad 5 \quad \boxed{10} \quad 10 \quad 5 \quad 1 \\
\ldots
\end{array}
$$

Látható, hogy a táblázat szélén 1-esek vannak, a táblázat függőleges tengelyre szimmetrikus,

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad \boxed{4} \quad \boxed{6} \quad 4 \quad 1 \\
1 \quad 5 \quad \boxed{10} \quad 10 \quad 5 \quad 1 \\
\ldots
\end{array}
$$

Látható, hogy a táblázat szélén 1-esek vannak, a táblázat függőleges tengelyre szimmetrikus, és minden nem a szélén álló elem

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

...

Látható, hogy a táblázat szélén 1-esek vannak, a táblázat függőleges tengelyre szimmetrikus, és minden nem a szélén álló elem a felette levő két elem összege.

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad \boxed{4} \quad \boxed{6} \quad 4 \quad 1 \\
1 \quad 5 \quad \boxed{10} \quad 10 \quad 5 \quad 1 \\
\cdots
\end{array}
$$

Látható, hogy a táblázat szélén 1-esek vannak, a táblázat függőleges tengelyre szimmetrikus, és minden nem a szélén álló elem a felette levő két elem összege. Pontosan ezen megállapításunkat fogalmazzuk meg az alábbi tételben.

11. Tétel. *(***A Pascal-háromszög alaptulajdonságai***)* *Legyen* $0 \le k \le n \in \mathbf{N}_0$*. Ekkor*

11. Tétel. *(***A Pascal-háromszög alaptulajdonságai)** *Legyen* $0 \leq k \leq n \in \mathbf{N}_0$*. Ekkor*

(1) $\binom{n}{0} = \binom{n}{n} = 1$*. (*

11. Tétel. *(**A Pascal-háromszög alaptulajdonságai**)* *Legyen* $0 \le k \le n \in \mathbf{N}_0$. *Ekkor*

(1) $\binom{n}{0} = \binom{n}{n} = 1$. *(„A szélén 1-esek állnak”.)*

11. Tétel. *(***A Pascal-háromszög alaptulajdonságai)** *Legyen* $0 \le k \le n \in \mathbf{N}_0$*. Ekkor*

(1) $\binom{n}{0} = \binom{n}{n} = 1$*. („A szélén 1-esek állnak”.)*

(2) $\binom{n}{k} = \binom{n}{n-k}$*. (*

11. Tétel. *(***A Pascal-háromszög alaptulajdonságai***)* *Legyen* $0 \leq k \leq n \in \mathbb{N}_0$*. Ekkor*

(1) $\binom{n}{0} = \binom{n}{n} = 1$*. („A szélén 1-esek állnak”.)*

(2) $\binom{n}{k} = \binom{n}{n-k}$*. („Függőleges tengelyre szimmetrikus”.)*

11. Tétel. *(***A Pascal-háromszög alaptulajdonságai)** *Legyen* $0 \le k \le n \in \mathbb{N}_0$*. Ekkor*

(1) $\binom{n}{0} = \binom{n}{n} = 1$*. („A szélén 1-esek állnak".)*

(2) $\binom{n}{k} = \binom{n}{n-k}$*. („Függőleges tengelyre szimmetrikus".)*

(3) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$*, ha* $0 < k < n$*. (*

11. Tétel. *(**A Pascal-háromszög alaptulajdonságai**) Legyen $0 \leq k \leq n \in \mathbb{N}_0$. Ekkor*

(1) $\binom{n}{0} = \binom{n}{n} = 1$. *(„A szélén 1-esek állnak".)*

(2) $\binom{n}{k} = \binom{n}{n-k}$. *(„Függőleges tengelyre szimmetrikus".)*

(3) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, *ha* $0 < k < n$. *(„Belső elem a felette levő két elem összege".)*

11. Tétel. *(**A Pascal-háromszög alaptulajdonságai)*** *Legyen* $0 \leq k \leq n \in \mathbb{N}_0$*. Ekkor*

(1) $\binom{n}{0} = \binom{n}{n} = 1$*. („A szélén 1-esek állnak”.)*

(2) $\binom{n}{k} = \binom{n}{n-k}$*. („Függőleges tengelyre szimmetrikus”.)*

(3) $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$*, ha* $0 < k < n$*. („Belső elem a felette levő két elem összege”.)*

Bizonyítás: A tétel mindhárom állítására adható kombinatorikai bizonyítás is, továbbá a binomiális együttható képletén alapuló bizonyítás is; mi csak az egyiket mutatjuk meg, de hol ezt, hol azt.

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van,

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van, az üreshalmaz, ezért $\binom{n}{0} = 1$.

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van, az üreshalmaz, ezért $\binom{n}{0} = 1$. Mivel egyetlen n-elemű részhalmaza van,

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van, az üreshalmaz, ezért $\binom{n}{0} = 1$. Mivel egyetlen n-elemű részhalmaza van, önmaga, ezért

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van, az üreshalmaz, ezért $\binom{n}{0} = 1$. Mivel egyetlen n-elemű részhalmaza van, önmaga, ezért $\binom{n}{n} = 1$.

(2)

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van, az üreshalmaz, ezért $\binom{n}{0} = 1$. Mivel egyetlen n-elemű részhalmaza van, önmaga, ezért $\binom{n}{n} = 1$.

(2) A képlet szerint $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ és

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van, az üreshalmaz, ezért $\binom{n}{0} = 1$. Mivel egyetlen n-elemű részhalmaza van, önmaga, ezért $\binom{n}{n} = 1$.

(2) A képlet szerint $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ és $\binom{n}{n-k} = \frac{n!}{(n-k)!\,(n-(n-k))!}$.

(1) Mivel egy n-elemű halmaznak egyetlen 0-elemű részhalmaza van, az üreshalmaz, ezért $\binom{n}{0} = 1$. Mivel egyetlen n-elemű részhalmaza van, önmaga, ezért $\binom{n}{n} = 1$.

(2) A képlet szerint $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ és $\binom{n}{n-k} = \dfrac{n!}{(n-k)!\,(n-(n-k))!}$. Látszik, hogy a kettő egyenlő.

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák.

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai,

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai, tehát ezek száma

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai, tehát ezek száma $\binom{n-1}{k}$.

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai, tehát ezek száma $\binom{n-1}{k}$.

Másrészt a b-t tartalmazók.

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai, tehát ezek száma $\binom{n-1}{k}$.

Másrészt a b-t tartalmazók. Ezek a b elemen kívül az $A \setminus \{b\}$-nek még további $k-1$ elemét tartalmazzák, amelyek

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai, tehát ezek száma $\binom{n-1}{k}$.

Másrészt a b-t tartalmazók. Ezek a b elemen kívül az $A \setminus \{b\}$-nek még további $k-1$ elemét tartalmazzák, amelyek $\binom{n-1}{k-1}$-féleképpen választhatók ki.

Az összegezési szabály szerint A k-elemű részhalmazainak száma $\binom{n-1}{k-1}+\binom{n-1}{k}$.

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai, tehát ezek száma $\binom{n-1}{k}$.

Másrészt a b-t tartalmazók. Ezek a b elemen kívül az $A \setminus \{b\}$-nek még további $k-1$ elemét tartalmazzák, amelyek $\binom{n-1}{k-1}$-féleképpen választhatók ki.

Az összegezési szabály szerint A k-elemű részhalmazainak száma $\binom{n-1}{k-1}+\binom{n-1}{k}$. Ugyanakkor ezen részhalmazok száma $\binom{n}{k}$.

(3) Legyen A egy n-elemű halmaz, és $b \in A$ egy rögzített elem. Ekkor az A k-elemű részhalmazai kétfélék:

egyrészt azok, amelyek b-t nem tartalmazzák. Ezek éppen az $(n-1)$-elemű $A \setminus \{b\}$ halmaz k-elemű részhalmazai, tehát ezek száma $\binom{n-1}{k}$.

Másrészt a b-t tartalmazók. Ezek a b elemen kívül az $A \setminus \{b\}$-nek még további $k-1$ elemét tartalmazzák, amelyek $\binom{n-1}{k-1}$-féleképpen választhatók ki.

Az összegezési szabály szerint A k-elemű részhalmazainak száma $\binom{n-1}{k-1}+\binom{n-1}{k}$. Ugyanakkor ezen részhalmazok száma $\binom{n}{k}$. Q.e.d.

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$1$$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1
\end{array}
$$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \end{array}$$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \end{array}$$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \end{array}$$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1
\end{array}
$$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\ \ldots \end{array}$$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
\ldots
\end{array}
$$

pl. $(a+b)^4 =$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ 1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\ \cdots \end{array}$$

pl. $(a+b)^4 = a^4$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
\ldots
\end{array}
$$

pl. $(a+b)^4 = a^4 + 4a^3b$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
\cdots
\end{array}
$$

pl. $(a+b)^4 = a^4+4a^3b+6a^2b^2$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
\cdots
\end{array}
$$

pl. $(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+$

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
\ldots
\end{array}
$$

pl. $(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$.

A Pascal háromszög n-edik sora a binomiális tétel szerint az $(a+b)^n$ kifejtéséhez szükséges együtthatókat tartalmazza:

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
\ldots
\end{array}
$$

pl. $(a+b)^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$. A Pascal-háromszögnek további — az előző tételben nem érintett — tulajdonságai is vannak.

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

$$\sum_{i=0}^{n} \binom{n}{i} = ?$$

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

$$\sum_{i=0}^{n} \binom{n}{i} = ?$$

Az 1. megoldás egy ötleten alapul.

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

$$\sum_{i=0}^{n} \binom{n}{i} = ?$$

Az 1. megoldás egy ötleten alapul. (Mi tagadás, erre nem könnyű rájönni.)

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

$$\sum_{i=0}^{n} \binom{n}{i} =?$$

Az 1. megoldás egy ötleten alapul. (Mi tagadás, erre nem könnyű rájönni.) A binomiális tétel szerint

$$\sum_{i=0}^{n} \binom{n}{i} =$$

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

$$\sum_{i=0}^{n} \binom{n}{i} = ?$$

Az 1. megoldás egy ötleten alapul. (Mi tagadás, erre nem könnyű rájönni.) A binomiális tétel szerint

$$\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} 1^{i} =$$

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

$$\sum_{i=0}^{n} \binom{n}{i} = ?$$

Az 1. megoldás egy ötleten alapul. (Mi tagadás, erre nem könnyű rájönni.) A binomiális tétel szerint

$$\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} 1^{i} = (1+1)^{n} =$$

Feladat: Mennyi a Pascal-háromszög n-edik sorában levő elemek összege, azaz

$$\sum_{i=0}^{n} \binom{n}{i} = ?$$

Az 1. megoldás egy ötleten alapul. (Mi tagadás, erre nem könnyű rájönni.) A binomiális tétel szerint

$$\sum_{i=0}^{n} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} 1^{i} = (1+1)^{n} = \boxed{2^{n}}.$$

A 2. megoldás egyéb szempontból is tanulságos:

A 2. **megoldás** egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek.

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint,

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben.

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben. Ily módon kapunk egy n-hosszúságú sorozatot a $\{0, 1\}$ halmaz elemeiből, amelyik meghatározza az S részhalmazt. (

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben. Ily módon kapunk egy n-hosszúságú sorozatot a $\{0, 1\}$ halmaz elemeiből, amelyik meghatározza az S részhalmazt. (Látható, hogy a részhalmazok és az ilyen sorozatok halmaza között bijekció van.)

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben. Ily módon kapunk egy n-hosszúságú sorozatot a $\{0, 1\}$ halmaz elemeiből, amelyik meghatározza az S részhalmazt. (Látható, hogy a részhalmazok és az ilyen sorozatok halmaza között bijekció van.) Ezek szerint pontosan annyi részhalmaza van A-nak,

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben. Ily módon kapunk egy n-hosszúságú sorozatot a $\{0, 1\}$ halmaz elemeiből, amelyik meghatározza az S részhalmazt. (Látható, hogy a részhalmazok és az ilyen sorozatok halmaza között bijekció van.) Ezek szerint pontosan annyi részhalmaza van A-nak, ahány ilyen sorozat,

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben. Ily módon kapunk egy n-hosszúságú sorozatot a $\{0, 1\}$ halmaz elemeiből, amelyik meghatározza az S részhalmazt. (Látható, hogy a részhalmazok és az ilyen sorozatok halmaza között bijekció van.) Ezek szerint pontosan annyi részhalmaza van A-nak, ahány ilyen sorozat, azaz ahány

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben. Ily módon kapunk egy n-hosszúságú sorozatot a $\{0, 1\}$ halmaz elemeiből, amelyik meghatározza az S részhalmazt. (Látható, hogy a részhalmazok és az ilyen sorozatok halmaza között bijekció van.) Ezek szerint pontosan annyi részhalmaza van A-nak, ahány ilyen sorozat, azaz ahány n-edosztályú ismétléses variációja van két elemnek, azaz 2^n.

A 2. megoldás egyéb szempontból is tanulságos: **Hány részhalmaza van egy n-elemű halmaznak?**

Egyrészt legyenek a halmaz elemei az $a_1, \ldots, a_n$ elemek. Tekintsünk egy tetszőleges S részhalmazt. Az $a_1, \ldots, a_n$ elemek mindegyike alá írjunk 1-et vagy 0-t aszerint, hogy benne van-e vagy nincs benne S-ben. Ily módon kapunk egy n-hosszúságú sorozatot a $\{0, 1\}$ halmaz elemeiből, amelyik meghatározza az S részhalmazt. (Látható, hogy a részhalmazok és az ilyen sorozatok halmaza között bijekció van.) Ezek szerint pontosan annyi részhalmaza van A-nak, ahány ilyen sorozat, azaz ahány n-edosztályú ismétléses variációja van két elemnek, azaz 2^n.

Láttuk, hogy ha $|A| = n$, akkor $P(A)$ elemszáma 2^n, tehát egy hatvány. Innen ered a hatványhalmaz elnevezés.

Másrészt — az összegezési szabály szerint —

Másrészt — az összegezési szabály szerint — a részhalmazok száma $=$

Másrészt — az összegezési szabály szerint — a részhalmazok száma $= \sum_{i=0}^{n}$ i-elemű részhalmazok száma $= \sum_{i=0}^{n} \binom{n}{i}$.

Tehát

Másrészt — az összegezési szabály szerint — a részhalmazok száma $= \sum_{i=0}^{n}$ i-elemű részhalmazok száma $= \sum_{i=0}^{n} \binom{n}{i}$.

Tehát $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

Másrészt — az összegezési szabály szerint — a részhalmazok száma $= \sum_{i=0}^{n}$ i-elemű részhalmazok száma $= \sum_{i=0}^{n} \binom{n}{i}$.

Tehát $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

A 3. megoldást nem részletezzük: azon alapul, hogy (néhány kisebb n értéket megvizsgálva)

Másrészt — az összegezési szabály szerint — a részhalmazok száma $= \sum_{i=0}^{n}$ i-elemű részhalmazok száma $= \sum_{i=0}^{n} \binom{n}{i}$.

Tehát $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

A 3. megoldást nem részletezzük: azon alapul, hogy (néhány kisebb n értéket megvizsgálva) megsejtjük, hogy a megoldás 2^n,

Másrészt — az összegezési szabály szerint — a részhalmazok száma $= \sum_{i=0}^{n}$ i-elemű részhalmazok száma $= \sum_{i=0}^{n} \binom{n}{i}$.

Tehát $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

A 3. megoldást nem részletezzük: azon alapul, hogy (néhány kisebb n értéket megvizsgálva) megsejtjük, hogy a megoldás 2^n, majd teljes indukcióval bebizonyítjuk annak felhasználásával, hogy minden belső elem a felette levő két elem összege.

Feladat: Mi az $x^3y^4z^2$ együtthatója, ha kifejtjük az $(x+y+z)^9$ hatványt?

Megoldás: A polinomiális tétel szerint

Feladat: Mi az $x^3y^4z^2$ együtthatója, ha kifejtjük az $(x+y+z)^9$ hatványt?

Megoldás: A polinomiális tétel szerint

$$\frac{9!}{3! \cdot 4! \cdot 2!} =$$

Feladat: Mi az $x^3y^4z^2$ együtthatója, ha kifejtjük az $(x+y+z)^9$ hatványt?

Megoldás: A polinomiális tétel szerint

$$\frac{9!}{3! \cdot 4! \cdot 2!} = 1260.$$

A

Feladat: Mi az $x^3y^4z^2$ együtthatója, ha kifejtjük az $(x+y+z)^9$ hatványt?

Megoldás: A polinomiális tétel szerint

$$\frac{9!}{3! \cdot 4! \cdot 2!} = 1260.$$

A feladat a polinomiális tétel ismerete nélkül is megoldható (de akkor lényegében annak a bizonyítását követjük): a kilenctényezős

Feladat: Mi az $x^3y^4z^2$ együtthatója, ha kifejtjük az $(x+y+z)^9$ hatványt?

Megoldás: A polinomiális tétel szerint

$$\frac{9!}{3! \cdot 4! \cdot 2!} = 1260.$$

A feladat a polinomiális tétel ismerete nélkül is megoldható (de akkor lényegében annak a bizonyítását követjük): a kilenctényezős

$$(x+y+z)(x+y+z)\dots(x+y+z)$$

kifejtésekor kapott $xyzxxyyyz$, $yyxxxzzyy$, stb.

Feladat: Mi az $x^3y^4z^2$ együtthatója, ha kifejtjük az $(x+y+z)^9$ hatványt?

Megoldás: A polinomiális tétel szerint

$$\frac{9!}{3! \cdot 4! \cdot 2!} = 1260.$$

A feladat a polinomiális tétel ismerete nélkül is megoldható (de akkor lényegében annak a bizonyítását követjük): a kilenctényezős

$$(x+y+z)(x+y+z)\ldots(x+y+z)$$

kifejtésekor kapott $xyzxxyyyz$, $yyxxxzzyy$, stb. tagokat kell összeszámolni, azaz azt, hogy három x, négy y és kettő z hányféleképpen rakható sorba,

Feladat: Mi az $x^3y^4z^2$ együtthatója, ha kifejtjük az $(x+y+z)^9$ hatványt?

Megoldás: A polinomiális tétel szerint

$$\frac{9!}{3! \cdot 4! \cdot 2!} = 1260.$$

A feladat a polinomiális tétel ismerete nélkül is megoldható (de akkor lényegében annak a bizonyítását követjük): a kilenctényezős

$$(x+y+z)(x+y+z)\ldots(x+y+z)$$

kifejtésekor kapott $xyzxxyyyz$, $yyxxxzzyy$, stb. tagokat kell összeszámolni, azaz azt, hogy három x, négy y és kettő z hányféleképpen rakható sorba, és erre az ismétléses permutáció képlete alkalmazható.

Gyakran a kombinatorikai feladat nem a hat alapfeladat egyike, hanem összetettebb. Az eddig látott és az ezután bemutatandó fogások sok más esetben is eredményesek.

Feladat: Hányféleképpen helyezkedhet el a tíz férőhelyes körhintán tíz ember? (Két elhelyezkedést akkor tekintünk azonosnak, ha mindenki előtt és után ugyanazon személyek ülnek. Azaz, ha az egyik elhelyezkedés a körhinta elfordításával a másikba átvihető.)

Feladat: Hányféleképpen helyezkedhet el a tíz férőhelyes körhintán tíz ember? (Két elhelyezkedést akkor tekintünk azonosnak, ha mindenki előtt és után ugyanazon személyek ülnek. Azaz, ha az egyik elhelyezkedés a körhinta elfordításával a másikba átvihető.)

Megoldás: Rögzítsük az egyik személyt — az lényegtelen, hogy ő hova ül.

Megoldás: Rögzítsük az egyik személyt — az lényegtelen, hogy ő hova ül. A rögzített személy viszont egyértelműen meghatároz kilenc helyet — függetlenül attól, hogy most éppen hová fordult a körhinta:

Megoldás: Rögzítsük az egyik személyt — az lényegtelen, hogy ő hova ül. A rögzített személy viszont egyértelműen meghatároz kilenc helyet — függetlenül attól, hogy most éppen hová fordult a körhinta: tudniillik a mögötte levő helyet, a mögötte levő hely mögötti helyet, stb.

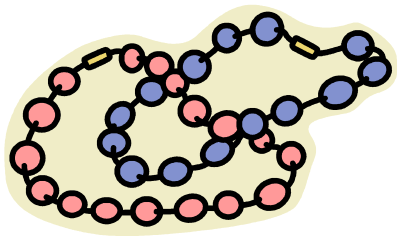
Megoldás: Rögzítsük az egyik személyt — az lényegtelen, hogy ő hova ül. A rögzített személy viszont egyértelműen meghatároz kilenc helyet — függetlenül attól, hogy most éppen hová fordult a körhinta: tudniillik a mögötte levő helyet, a mögötte levő hely mögötti helyet, stb. Az ily módon meghatározott kilenc helyre a maradék kilenc személy

Megoldás: Rögzítsük az egyik személyt — az lényegtelen, hogy ő hova ül. A rögzített személy viszont egyértelműen meghatároz kilenc helyet — függetlenül attól, hogy most éppen hová fordult a körhinta: tudniillik a mögötte levő helyet, a mögötte levő hely mögötti helyet, stb. Az ily módon meghatározott kilenc helyre a maradék kilenc személy 9!-féleképpen permutálható.

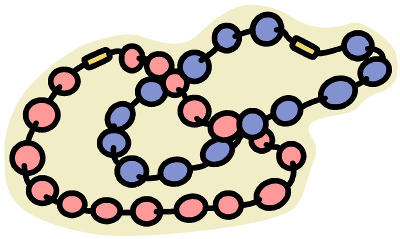
Megoldás: Rögzítsük az egyik személyt — az lényegtelen, hogy ő hova ül. A rögzített személy viszont egyértelműen meghatároz kilenc helyet — függetlenül attól, hogy most éppen hová fordult a körhinta: tudniillik a mögötte levő helyet, a mögötte levő hely mögötti helyet, stb. Az ily módon meghatározott kilenc helyre a maradék kilenc személy 9!-féleképpen permutálható. Tehát az eredmény

$$9! = 362880.$$

Feladat: Hányféleképpen készíthetünk tíz különböző színű gyöngy felfűzésével nyakéket? (A nyakéken nincsen csat, két elrendezést azonosnak tekintünk, ha az egyik a másikba elmozdítható).

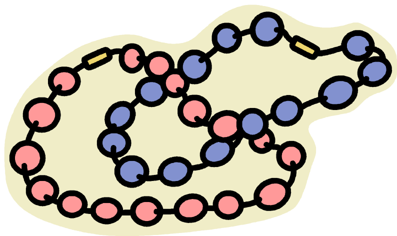


Feladat: Hányféleképpen készíthetünk tíz különböző színű gyöngy felfűzésével nyakéket? (A nyakéken nincsen csat, két elrendezést azonosnak tekintünk, ha az egyik a másikba elmozdítható).



Az ábra inkább azt mutatja, hogy milyen **ne** legyen a nyakék,

Feladat: Hányféleképpen készíthetünk tíz különböző színű gyöngy felfűzésével nyakéket? (A nyakéken nincsen csat, két elrendezést azonosnak tekintünk, ha az egyik a másikba elmozdítható).



Az ábra inkább azt mutatja, hogy milyen **ne** legyen a nyakék, hiszen az ábrán azonos színű gyöngyök vannak, és csat is van, amelyhez a gyöngyök helyzetét viszonyítani lehet.

Megoldás: Legyen A az egyik gyöngy.

Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből

Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből az A szomszédjait

Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből az A szomszédjait $\binom{9}{2}$ $=$

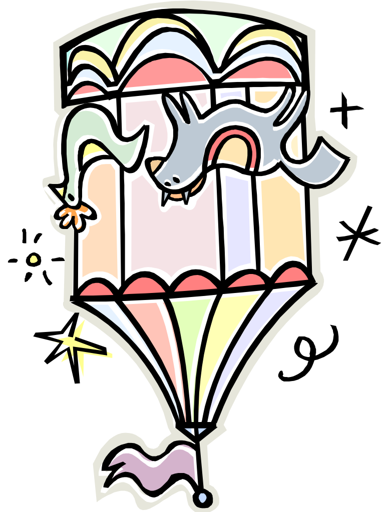
Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből az A szomszédjait $\binom{9}{2} = \frac{9 \cdot 8}{1 \cdot 2} =$

Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből az A szomszédjait $\binom{9}{2} = \dfrac{9 \cdot 8}{1 \cdot 2} = 36$-féleképpen választhatjuk ki. Ugyanis az

Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből az A szomszédjait $\binom{9}{2} = \dfrac{9 \cdot 8}{1 \cdot 2} = 36$-féleképpen választhatjuk ki. Ugyanis az A két szomszédjának a sorrendje nem számít,

Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből az A szomszédjait $\binom{9}{2} = \frac{9 \cdot 8}{1 \cdot 2} = 36$-féleképpen választhatjuk ki. Ugyanis az A két szomszédjának a sorrendje nem számít, hiszen a nyakéket meg is fordíthatjuk.

Megoldás: Legyen A az egyik gyöngy. A maradék kilenc gyöngyből az A szomszédjait $\binom{9}{2} = \frac{9 \cdot 8}{1 \cdot 2} = 36$-féleképpen választhatjuk ki. Ugyanis az A két szomszédjának a sorrendje nem számít, hiszen a nyakéket meg is fordíthatjuk.



Itt tér el a feladat az előző,

Itt tér el a feladat az előző, körhintás feladattól:

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel!

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja.

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott:

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott: ugyanis A-ból B irányába indulva van

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott: ugyanis A-ból B irányába indulva van első, második, ..., hetedik további hely.

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott: ugyanis A-ból B irányába indulva van első, második, $\ldots$, hetedik további hely. Ezekre a maradék hét különböző gyöngyöt

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott: ugyanis A-ból B irányába indulva van első, második, . . . , hetedik további hely. Ezekre a maradék hét különböző gyöngyöt 7!-féleképpen permutálhatjuk.

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott: ugyanis A-ból B irányába indulva van első, második, . . . , hetedik további hely. Ezekre a maradék hét különböző gyöngyöt 7!-féleképpen permutálhatjuk. A szorzási szabály szerint az eredmény

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott: ugyanis A-ból B irányába indulva van első, második, ..., hetedik további hely. Ezekre a maradék hét különböző gyöngyöt 7!-féleképpen permutálhatjuk. A szorzási szabály szerint az eredmény

$$36 \cdot 7! =$$

Itt tér el a feladat az előző, körhintás feladattól: a körhintát (ellentétben az ábrával) nem fordíthatjuk meg, ezért a körhintán A bal- és jobbszomszédja nem cserélhető fel! Legyen B és C az A két szomszédja. Minden további hely már egyértelműen meghatározott: ugyanis A-ból B irányába indulva van első, második, ..., hetedik további hely. Ezekre a maradék hét különböző gyöngyöt 7!-féleképpen permutálhatjuk. A szorzási szabály szerint az eredmény

$$36 \cdot 7! = \underline{181\ 440}.$$

Feladat: Hányféleképpen rakhatjuk sorba a „KOPPAN” szó betűit, ha a két „P” betű nem kerülhet egymás mellé?

Feladat: Hányféleképpen rakhatjuk sorba a „KOPPAN” szó betűit, ha a két „P” betű nem kerülhet egymás mellé?

Megoldás: Ha nem törődünk a „P” betűkre vonatkozó kikötéssel, akkor — az ismétléses permutációkra vonatkozó képlet szerint

Feladat: Hányféleképpen rakhatjuk sorba a „KOPPAN” szó betűit, ha a két „P” betű nem kerülhet egymás mellé?

Megoldás: Ha nem törődünk a „P” betűkre vonatkozó kikötéssel, akkor — az ismétléses permutációkra vonatkozó képlet szerint (Az $1! = 1$ tényezőket ki sem írva) $\frac{6!}{2!} =$

Feladat: Hányféleképpen rakhatjuk sorba a „KOPPAN'' szó betűit, ha a két „P'' betű nem kerülhet egymás mellé?

Megoldás: Ha nem törődünk a „P'' betűkre vonatkozó kikötéssel, akkor — az ismétléses permutációkra vonatkozó képlet szerint (Az $1! = 1$ tényezőket ki sem írva) $\frac{6!}{2!} = 3 \cdot 5! = 360$-féle sorrend van.

Most nézzük meg, hány olyan eset van, amikor a két „P” betű egymás mellett van.

Most nézzük meg, hány olyan eset van, amikor a két „P” betű egymás mellett van. Ekkor felfoghatjuk a feladatot úgy, hogy csak öt betűt, amelyek egyike a „PP” kettősbetű, Most nézzük meg, hány olyan eset van, amikor a két „P” betű egymás mellett van. Ekkor felfoghatjuk a feladatot úgy, hogy csak öt betűt, amelyek egyike a „PP” kettősbetű, kell permutálnunk.

Most nézzük meg, hány olyan eset van, amikor a két „P” betű egymás mellett van. Ekkor felfoghatjuk a feladatot úgy, hogy csak öt betűt, amelyek egyike a „PP” kettősbetű, kell permutálnunk. Ezt $5! = 120$-féleképpen tehetjük.

Most nézzük meg, hány olyan eset van, amikor a két „P” betű egymás mellett van. Ekkor felfoghatjuk a feladatot úgy, hogy csak öt betűt, amelyek egyike a „PP” kettősbetű, kell permutálnunk. Ezt $5! = 120$-féleképpen tehetjük. Végül az eredmény a két részeredmény különbsége: $3 \cdot 5! - 5! = 360 - 120 = \underline{240}$.

Most nézzük meg, hány olyan eset van, amikor a két „P” betű egymás mellett van. Ekkor felfoghatjuk a feladatot úgy, hogy csak öt betűt, amelyek egyike a „PP” kettősbetű, kell permutálnunk. Ezt $5! = 120$-féleképpen tehetjük. Végül az eredmény a két részeredmény különbsége: $3 \cdot 5! - 5! = 360 - 120 = \underline{240}$.

Tanulság: **Kedvező esetek száma = összes eset száma − kedvezőtlen esetek száma.**

Most nézzük meg, hány olyan eset van, amikor a két „P” betű egymás mellett van. Ekkor felfoghatjuk a feladatot úgy, hogy csak öt betűt, amelyek egyike a „PP” kettősbetű, kell permutálnunk. Ezt $5! = 120$-féleképpen tehetjük. Végül az eredmény a két részeredmény különbsége: $3 \cdot 5! - 5! = 360 - 120 = \underline{240}$.

Tanulság: **Kedvező esetek száma = összes eset száma − kedvezőtlen esetek száma.** (Persze csak olyankor hasznos, amikor az egyenlőség jobboldalát könnyebb kiszámolni.)

Feladat: Hányféleképpen rakhatjuk sorba a „KÖRHINTA” szó betűit, ha két magánhangzó nem kerülhet egymás mellé?

Megoldás:

Feladat: Hányféleképpen rakhatjuk sorba a „KÖRHINTA” szó betűit, ha két magánhangzó nem kerülhet egymás mellé?

Megoldás: Először azt vegyük észre, hogy itt az előző ötlet — a kedvezőtlen esetek megszámolása — roppant nehéz lenne:

Feladat: Hányféleképpen rakhatjuk sorba a „KÖRHINTA” szó betűit, ha két magánhangzó nem kerülhet egymás mellé?

Megoldás: Először azt vegyük észre, hogy itt az előző ötlet — a kedvezőtlen esetek megszámolása — roppant nehéz lenne: az „ÖI”, „IA”, stb. mellett a harmadik magánhangzó lehet tőlük távolabb, de lehet közvetlenül mellettük

Feladat: Hányféleképpen rakhatjuk sorba a „KÖRHINTA” szó betűit, ha két magánhangzó nem kerülhet egymás mellé?

Megoldás: Először azt vegyük észre, hogy itt az előző ötlet — a kedvezőtlen esetek megszámolása — roppant nehéz lenne: az „ÖI”, „IA”, stb. mellett a harmadik magánhangzó lehet tőlük távolabb, de lehet közvetlenül mellettük — azaz mindhárom egymás mellett, amit többször is számolnánk, tehát korrigálni kellene, stb. —

Feladat: Hányféleképpen rakhatjuk sorba a „KÖRHINTA” szó betűit, ha két magánhangzó nem kerülhet egymás mellé?

Megoldás: Először azt vegyük észre, hogy itt az előző ötlet — a kedvezőtlen esetek megszámolása — roppant nehéz lenne: az „ÖI”, „IA”, stb. mellett a harmadik magánhangzó lehet tőlük távolabb, de lehet közvetlenül mellettük — azaz mindhárom egymás mellett, amit többször is számolnánk, tehát korrigálni kellene, stb. — csak hogy érzékeltessük a nehézségeket.

Feladat: Hányféleképpen rakhatjuk sorba a „KÖRHINTA" szó betűit, ha két magánhangzó nem kerülhet egymás mellé?

Megoldás: Először azt vegyük észre, hogy itt az előző ötlet — a kedvezőtlen esetek megszámolása — roppant nehéz lenne: az „ÖI", „IA", stb. mellett a harmadik magánhangzó lehet tőlük távolabb, de lehet közvetlenül mellettük — azaz mindhárom egymás mellett, amit többször is számolnánk, tehát korrigálni kellene, stb. — csak hogy érzékeltessük a nehézségeket. Érdemes más módszert keresnünk.

Először rakjuk sorba a mássalhangzókat!

Feladat: Hányféleképpen rakhatjuk sorba a „KÖRHINTA” szó betűit, ha két magánhangzó nem kerülhet egymás mellé?

Megoldás: Először azt vegyük észre, hogy itt az előző ötlet — a kedvezőtlen esetek megszámolása — roppant nehéz lenne: az „ÖI”, „IA”, stb. mellett a harmadik magánhangzó lehet tőlük távolabb, de lehet közvetlenül mellettük — azaz mindhárom egymás mellett, amit többször is számolnánk, tehát korrigálni kellene, stb. — csak hogy érzékeltessük a nehézségeket. Érdemes más módszert keresnünk.

Először rakjuk sorba a mássalhangzókat! Van öt különböző mássalhangzó, ezeknek $5! = 120$ sorrendje lehet.

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le „szellősen”, tehát úgy, hogy bármelyik kettő közé még beférjen egy további betű.

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le „szellősen”, tehát úgy, hogy bármelyik kettő közé még beférjen egy további betű. Pl. így:

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le „szellősen”, tehát úgy, hogy bármelyik kettő közé még beférjen egy további betű. Pl. így:

$$K \quad R \quad H \quad N \quad T$$

Ekkor

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le „szellősen”, tehát úgy, hogy bármelyik kettő közé még beférjen egy további betű. Pl. így:

$$K \quad R \quad H \quad N \quad T$$

Ekkor keletkezik

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le „szellősen”, tehát úgy, hogy bármelyik kettő közé még beférjen egy további betű. Pl. így:

$$K \quad R \quad H \quad N \quad T$$

Ekkor keletkezik hat szabad hely, mindegyik mássalhangzó után és az első előtt, ezeket most most ♠ jelöli:

$$\spadesuit K \spadesuit R \spadesuit H \spadesuit N \spadesuit T \spadesuit$$

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le „szellősen”, tehát úgy, hogy bármelyik kettő közé még beférjen egy további betű. Pl. így:

$$K \quad R \quad H \quad N \quad T$$

Ekkor keletkezik hat szabad hely, mindegyik mássalhangzó után és az első előtt, ezeket most most ♠ jelöli:

$$\spadesuit K \spadesuit R \spadesuit H \spadesuit N \spadesuit T \spadesuit$$

A három magánhangzót ezen hat helyre kell tennünk, de mindegyik ♠ helyére legfeljebb egyet tehetünk (

Bárhogy is raktuk sorba az öt mássalhangzót, írjuk ezeket le „szellősen”, tehát úgy, hogy bármelyik kettő közé még beférjen egy további betű. Pl. így:

$$K \quad R \quad H \quad N \quad T$$

Ekkor keletkezik hat szabad hely, mindegyik mássalhangzó után és az első előtt, ezeket most most $\spadesuit$ jelöli:

$$\spadesuit K \spadesuit R \spadesuit H \spadesuit N \spadesuit T \spadesuit$$

A három magánhangzót ezen hat helyre kell tennünk, de mindegyik $\spadesuit$ helyére legfeljebb egyet tehetünk (nehogy kettő magánhangzó egymás mellé kerüljön).

Egyik folytatás: az „Ö”-t hat helyre tehetjük, utána az „I”-t már csak öt, az „A”-t már csak négy helyre, és így

Egyik folytatás: az „Ö”-t hat helyre tehetjük, utána az „I”-t már csak öt, az „A”-t már csak négy helyre, és így a szorzási szabály szerint $6 \cdot 5 \cdot 4 = 120$-féleképpen rakhatók le a magánhangzók.

Egyik folytatás: az „Ö”-t hat helyre tehetjük, utána az „I”-t már csak öt, az „A”-t már csak négy helyre, és így a szorzási szabály szerint $6 \cdot 5 \cdot 4 = 120$-féleképpen rakhatók le a magánhangzók.

Másik folytatás: Gyakori kombinatorikai fogás: nem a huszár választ lovat, hanem a ló huszárt.

Egyik folytatás: az „Ö”-t hat helyre tehetjük, utána az „I”-t már csak öt, az „A”-t már csak négy helyre, és így a szorzási szabály szerint $6 \cdot 5 \cdot 4 = 120$-féleképpen rakhatók le a magánhangzók.

Másik folytatás: Gyakori kombinatorikai fogás: nem a huszár választ lovat, hanem a ló huszárt. A hat szabad hely (♠) közül kiválasztunk hármat, és

Egyik folytatás: az „Ö”-t hat helyre tehetjük, utána az „I”-t már csak öt, az „A”-t már csak négy helyre, és így a szorzási szabály szerint $6 \cdot 5 \cdot 4 = 120$-féleképpen rakhatók le a magánhangzók.

Másik folytatás: Gyakori kombinatorikai fogás: nem a huszár választ lovat, hanem a ló huszárt. A hat szabad hely ($\spadesuit$) közül kiválasztunk hármat, és amilyen sorrendben kiválasztottuk azt a hármat,

Egyik folytatás: az „Ö”-t hat helyre tehetjük, utána az „I”-t már csak öt, az „A”-t már csak négy helyre, és így a szorzási szabály szerint $6 \cdot 5 \cdot 4 = 120$-féleképpen rakhatók le a magánhangzók.

Másik folytatás: Gyakori kombinatorikai fogás: nem a huszár választ lovat, hanem a ló huszárt. A hat szabad hely (♠) közül kiválasztunk hármat, és amilyen sorrendben kiválasztottuk azt a hármat, a magánhangzókat névsor szerint pakoljuk oda. Az ismétlés nélküli variációkra vonatkozó tétel szerint ezt $6 \cdot 5 \cdot 4 = 120$-féleképpen tehetjük meg.

Harmadik folytatás: Előbb a hat szabad hely (♠) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet

Harmadik folytatás: Előbb a hat szabad hely ($\spadesuit$) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít)

Harmadik folytatás: Előbb a hat szabad hely (♠) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít) $\binom{6}{3}$-féleképpen választhatjuk ki.

Harmadik folytatás: Előbb a hat szabad hely (♠) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít) $\binom{6}{3}$-féleképpen választhatjuk ki. Most hogy már megvan a három hely, oda a három magánhangzót

Harmadik folytatás: Előbb a hat szabad hely (♠) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít) $\binom{6}{3}$-féleképpen választhatjuk ki. Most hogy már megvan a három hely, oda a három magánhangzót $3!$-féleképpen permutálhatjuk.

Harmadik folytatás: Előbb a hat szabad hely ($\spadesuit$) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít) $\binom{6}{3}$-féleképpen választhatjuk ki. Most hogy már megvan a három hely, oda a három magánhangzót 3!-féleképpen permutálhatjuk. A szorzási szabály szerint tehát a magánhangzókat

Harmadik folytatás: Előbb a hat szabad hely (♠) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít) $\binom{6}{3}$-féleképpen választhatjuk ki. Most hogy már megvan a három hely, oda a három magánhangzót 3!-féleképpen permutálhatjuk. A szorzási szabály szerint tehát a magánhangzókat

$$\binom{6}{3} \cdot 3! =$$

Harmadik folytatás: Előbb a hat szabad hely (♠) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít) $\binom{6}{3}$-féleképpen választhatjuk ki. Most hogy már megvan a három hely, oda a három magánhangzót 3!-féleképpen permutálhatjuk. A szorzási szabály szerint tehát a magánhangzókat

$$\binom{6}{3} \cdot 3! = \frac{6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3} \cdot 3! =$$

Harmadik folytatás: Előbb a hat szabad hely (♠) közül kiválasztjuk azt a hármat, ahová magánhangzót akarunk rakni. A három helyet (sorrend nem számít) $\binom{6}{3}$-féleképpen választhatjuk ki. Most hogy már megvan a három hely, oda a három magánhangzót 3!-féleképpen permutálhatjuk. A szorzási szabály szerint tehát a magánhangzókat

$$\binom{6}{3} \cdot 3! = \frac{6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3} \cdot 3! = 6 \cdot 5 \cdot 4 = 120$$

féleképpen helyezhetjük el.

Végezetül: a mássalhangzókat $5! = 120$, ezt követően a magánhangzókat 120-féleképpen lehet elhelyezni

Végezetül: a mássalhangzókat $5! = 120$, ezt követően a magánhangzókat 120-féleképpen lehet elhelyezni (a két szám egyenlősége csak véletlen!)

Végezetül: a mássalhangzókat $5! = 120$, ezt követően a magánhangzókat 120-féleképpen lehet elhelyezni (a két szám egyenlősége csak véletlen!) ezért az eredmény a szorzási szabály szerint $120 \cdot 120 = \underline{14\,400}$.

Végezetül: a mássalhangzókat $5! = 120$, ezt követően a magánhangzókat 120-féleképpen lehet elhelyezni (a két szám egyenlősége csak véletlen!) ezért az eredmény a szorzási szabály szerint $120 \cdot 120 = \underline{14\,400}$.

A megoldás azt is mutatja, hogy egy kombinatorikai (rész)probléma megoldására gyakran több jó lehetőség is van!

Feladat: Hányféleképpen rakhatjuk sorba a

„KOMBINATORIKA”

szó betűit úgy, hogy két magánhangzó ne kerüljön egymás mellé?

Megoldás:

Feladat: Hányféleképpen rakhatjuk sorba a

„KOMBINATORIKA”

szó betűit úgy, hogy két magánhangzó ne kerüljön egymás mellé?

Megoldás: A feladat csak annyiban különbözik az előzőtől, hogy a betűk nem mind különböznek. A megoldás elején ez nem jelent lényeges különbséget,

Feladat: Hányféleképpen rakhatjuk sorba a

„KOMBINATORIKA”

szó betűit úgy, hogy két magánhangzó ne kerüljön egymás mellé?

Megoldás: A feladat csak annyiban különbözik az előzőtől, hogy a betűk nem mind különböznek. A megoldás elején ez nem jelent lényeges különbséget, később pedig profitálhatunk abból, hogy az előbb három változatot is kidolgoztunk (mert az egyik könnyen alkalmazható a jelen szituációban is).

Előbb a „KMBNTRK" betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (

Előbb a „KMBNTRK” betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció).

Előbb a „KMBNTRK" betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció). A hét mássalhangzó nyolc szabad helyet határoz meg (az első előtt, és mindegyik után egyet). A nyolc hely közül válasszuk ki azt a hatot, ahova a hat magánhangzó kerül, ezt $\binom{8}{6}$-féleképpen tehetjük.

Előbb a „KMBNTRK” betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció). A hét mássalhangzó nyolc szabad helyet határoz meg (az első előtt, és mindegyik után egyet). A nyolc hely közül válasszuk ki azt a hatot, ahova a hat magánhangzó kerül, ezt $\binom{8}{6}$-féleképpen tehetjük. Eddig —

Előbb a „KMBNTRK'' betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció). A hét mássalhangzó nyolc szabad helyet határoz meg (az első előtt, és mindegyik után egyet). A nyolc hely közül válasszuk ki azt a hatot, ahova a hat magánhangzó kerül, ezt $\binom{8}{6}$-féleképpen tehetjük. Eddig — a szorzási szabály szerint — ezt $\frac{7!}{2!}\binom{8}{6}$ lehetőség.

Előbb a „KMBNTRK" betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció). A hét mássalhangzó nyolc szabad helyet határoz meg (az első előtt, és mindegyik után egyet). A nyolc hely közül válasszuk ki azt a hatot, ahova a hat magánhangzó kerül, ezt $\binom{8}{6}$-féleképpen tehetjük. Eddig — a szorzási szabály szerint — ezt $\frac{7!}{2!}\binom{8}{6}$ lehetőség. Most, hogy már megvan, hogy az „OIAOIA" magánhangzókat hova kell elhelyezni, ezeket a helyeikre

Előbb a „KMBNTRK” betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció). A hét mássalhangzó nyolc szabad helyet határoz meg (az első előtt, és mindegyik után egyet). A nyolc hely közül válasszuk ki azt a hatot, ahova a hat magánhangzó kerül, ezt $\binom{8}{6}$-féleképpen tehetjük. Eddig — a szorzási szabály szerint — ezt $\frac{7!}{2!}\binom{8}{6}$ lehetőség. Most, hogy már megvan, hogy az „OIAOIA” magánhangzókat hova kell elhelyezni, ezeket a helyeikre — ismétléses permutáció — $\frac{6!}{2!\cdot 2!\cdot 2!}$-féleképpen permutálhatjuk.

Előbb a „KMBNTRK” betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció). A hét mássalhangzó nyolc szabad helyet határoz meg (az első előtt, és mindegyik után egyet). A nyolc hely közül válasszuk ki azt a hatot, ahova a hat magánhangzó kerül, ezt $\binom{8}{6}$-féleképpen tehetjük. Eddig — a szorzási szabály szerint — ezt $\frac{7!}{2!}\binom{8}{6}$ lehetőség. Most, hogy már megvan, hogy az „OIAOIA” magánhangzókat hova kell elhelyezni, ezeket a helyeikre — ismétléses permutáció — $\frac{6!}{2!\cdot 2!\cdot 2!}$-féleképpen permutálhatjuk. A végeredmény a szorzási szabály alapján adódik:

$$\frac{7!}{2!}\binom{8}{6}\frac{6!}{2!\cdot 2!\cdot 2!} =$$

Előbb a „KMBNTRK” betűit, azaz a mássalhangzókat rakjuk sorba, ezt $\frac{7!}{2!}$-féleképpen tehetjük (ismétléses permutáció). A hét mássalhangzó nyolc szabad helyet határoz meg (az első előtt, és mindegyik után egyet). A nyolc hely közül válasszuk ki azt a hatot, ahova a hat magánhangzó kerül, ezt $\binom{8}{6}$-féleképpen tehetjük. Eddig — a szorzási szabály szerint — ezt $\frac{7!}{2!}\binom{8}{6}$ lehetőség. Most, hogy már megvan, hogy az „OIAOIA” magánhangzókat hova kell elhelyezni, ezeket a helyeikre — ismétléses permutáció — $\frac{6!}{2!\cdot 2!\cdot 2!}$-féleképpen permutálhatjuk. A végeredmény a szorzási szabály alapján adódik:

$$\frac{7!}{2!}\binom{8}{6}\frac{6!}{2!\cdot 2!\cdot 2!} = \underline{6\ 350\ 400}.$$

Feladat: A gáz árának növekedése

Feladat: A gáz árának növekedése miatt a gazda úgy határoz, hogy a telkét az utcától elhatároló kerítés 100 függőleges deszkája közül harmincat

Feladat: A gáz árának növekedése miatt a gazda úgy határoz, hogy a telkét az utcától elhatároló kerítés 100 függőleges deszkája közül harmincat felaprít és az így nyert fával fűt be a kályhába.

Feladat: A gáz árának növekedése miatt a gazda úgy határoz, hogy a telkét az utcától elhatároló kerítés 100 függőleges deszkája közül harmincat felaprít és az így nyert fával fűt be a kályhába. Hányféleképpen veheti ki a harminc deszkát a kerítésből úgy,

Feladat: A gáz árának növekedése miatt a gazda úgy határoz, hogy a telkét az utcától elhatároló kerítés 100 függőleges deszkája közül harmincat felaprít és az így nyert fával fűt be a kályhába. Hányféleképpen veheti ki a harminc deszkát a kerítésből úgy, hogy egymás mellettieket ne válasszon? (

Feladat: A gáz árának növekedése miatt a gazda úgy határoz, hogy a telkét az utcától elhatároló kerítés 100 függőleges deszkája közül harmincat felaprít és az így nyert fával fűt be a kályhába. Hányféleképpen veheti ki a harminc deszkát a kerítésből úgy, hogy egymás mellettieket ne válasszon? (Ha egymás melletieket venne ki, akkor túl nagy nyílás keletkezne, amit el akar kerülni.)

Feladat: A gáz árának növekedése miatt a gazda úgy határoz, hogy a telkét az utcától elhatároló kerítés 100 függőleges deszkája közül harmincat felaprít és az így nyert fával fűt be a kályhába. Hányféleképpen veheti ki a harminc deszkát a kerítésből úgy, hogy egymás mellettieket ne válasszon? (Ha egymás melletieket venne ki, akkor túl nagy nyílás keletkezne, amit el akar kerülni.) A sorrend nem számít, hanem csak az, hogy hogy néz majd ki a „foghíjas” kerítés.

Megoldás: A korábbi feladatok után ez sem túl nehéz.

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási” tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk.

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási” tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk,

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási” tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási'' tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási'' tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és két E betű nem lehet egymás mellett.

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási” tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és két E betű nem lehet egymás mellett. Nyilván az adja a választ, hogy hány ilyen szó van.

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási” tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és két E betű nem lehet egymás mellett. Nyilván az adja a választ, hogy hány ilyen szó van. A hetven M betűt (mivel ezek azonosak) egyféleképpen írhatjuk le (köztük persze hézagokat hagyva).

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási” tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és két E betű nem lehet egymás mellett. Nyilván az adja a választ, hogy hány ilyen szó van. A hetven M betűt (mivel ezek azonosak) egyféleképpen írhatjuk le (köztük persze hézagokat hagyva). Ezek meghatároznak 71 helyet (

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási" tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és két E betű nem lehet egymás mellett. Nyilván az adja a választ, hogy hány ilyen szó van. A hetven M betűt (mivel ezek azonosak) egyféleképpen írhatjuk le (köztük persze hézagokat hagyva). Ezek meghatároznak 71 helyet (az első előtti helyet, és minden M betű után egy helyet). Ezen 71 hely közül kell kiválasztani azt a 30-at, ahova az E betűket beírjuk.

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási” tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és két E betű nem lehet egymás mellett. Nyilván az adja a választ, hogy hány ilyen szó van. A hetven M betűt (mivel ezek azonosak) egyféleképpen írhatjuk le (köztük persze hézagokat hagyva). Ezek meghatároznak 71 helyet (az első előtti helyet, és minden M betű után egy helyet). Ezen 71 hely közül kell kiválasztani azt a 30-at, ahova az E betűket beírjuk. (Mivel az E betűk mind egyformák, a sorrendjük most csak egyféle lehet.)

Megoldás: A korábbi feladatok után ez sem túl nehéz. Képzeljük el a „kerítésritkítási'' tervet úgy, hogy a megmaradó deszkákra M, az eltávolítandó deszkákra pedig E betűt írunk. Ekkor — ha a kerítésre írt betűket egybeolvassuk, keletkezik egy szó, amelyikben hetven M és 30 E betű van, és két E betű nem lehet egymás mellett. Nyilván az adja a választ, hogy hány ilyen szó van. A hetven M betűt (mivel ezek azonosak) egyféleképpen írhatjuk le (köztük persze hézagokat hagyva). Ezek meghatároznak 71 helyet (az első előtti helyet, és minden M betű után egy helyet). Ezen 71 hely közül kell kiválasztani azt a 30-at, ahova az E betűket beírjuk. (Mivel az E betűk mind egyformák, a sorrendjük most csak egyféle lehet.) Az eddigiek szerint az eredmény

$$\binom{71}{30} =$$

$$\binom{71}{30} = 95\,846\,086\,442\,150\,951\,368\,.$$

Az alábbi feladat a szitaformulát készíti elő.

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája.

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek,

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek,

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek, franciából 20-nak,

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek, franciából 20-nak, angolból is és németből is 23-nak,

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek, franciából 20-nak, angolból is és németből is 23-nak, angolból is és franciából is 12-nek,

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek, franciából 20-nak, angolból is és németből is 23-nak, angolból is és franciából is 12-nek, németből is és franciából is 11-nek,

Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek, franciából 20-nak, angolból is és németből is 23-nak, angolból is és franciából is 12-nek, németből is és franciából is 11-nek, és mindhárom nyelvből 5-nek.

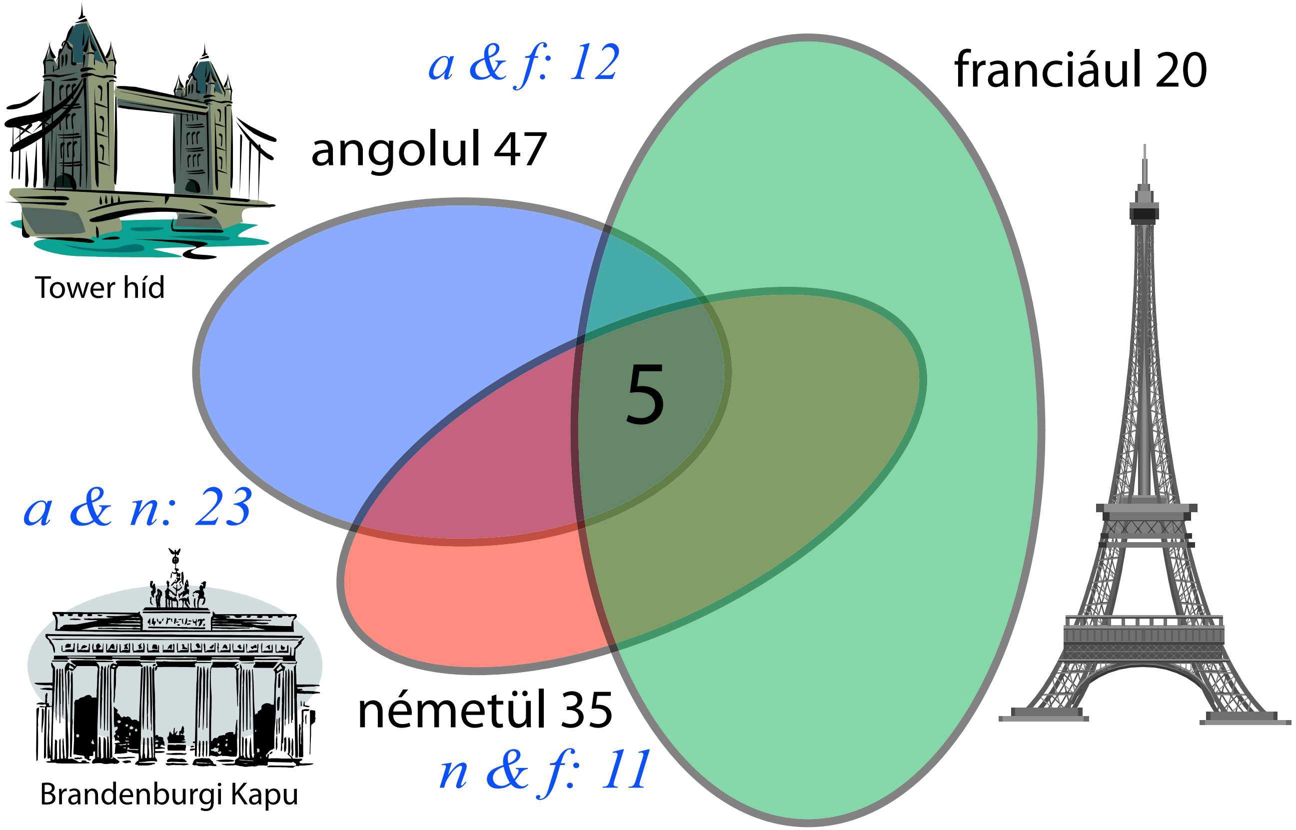
Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek, franciából 20-nak, angolból is és németből is 23-nak, angolból is és franciából is 12-nek, németből is és franciából is 11-nek, és mindhárom nyelvből 5-nek. Hány olyan hallgató van az évfolyamon, akinek nincs nyelvvizsgája?

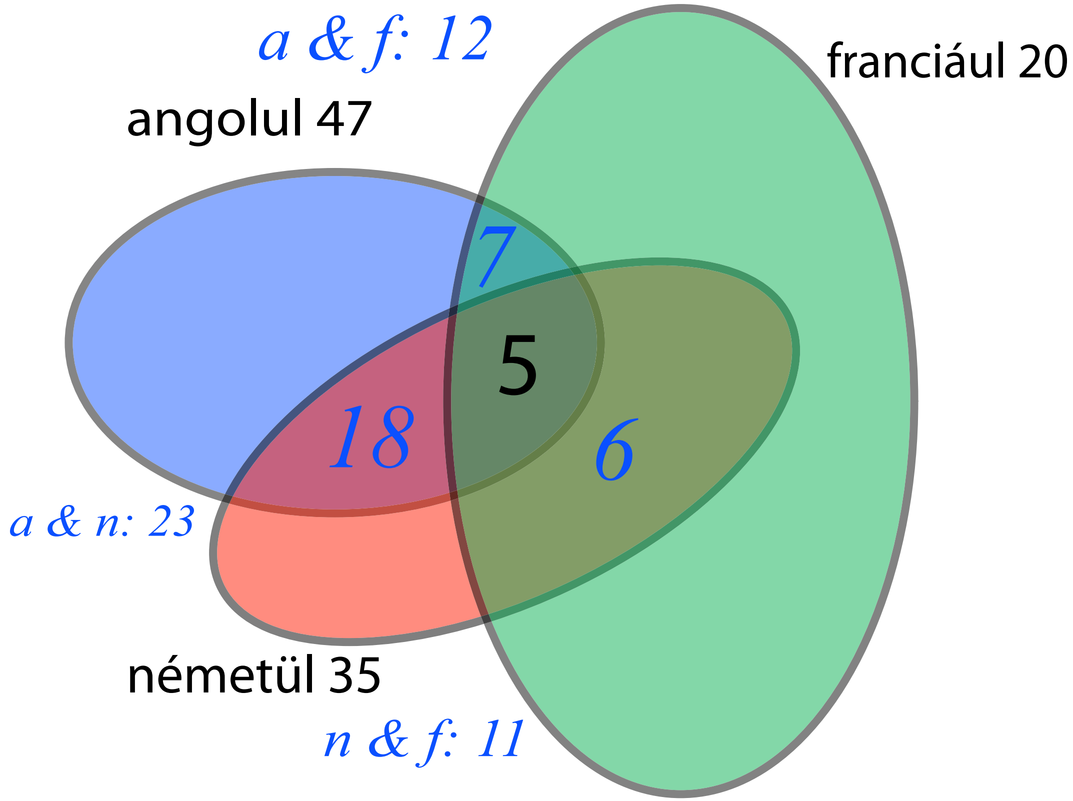
Az alábbi feladat a szitaformulát készíti elő.

Feladat: Egy 67 fős évfolyam hallgatóinak csak angol, német és francia nyelvből van (középfokú) nyelvvizsgája. Angolból 47-nek, németből 35-nek, franciából 20-nak, angolból is és németből is 23-nak, angolból is és franciából is 12-nek, németből is és franciából is 11-nek, és mindhárom nyelvből 5-nek. Hány olyan hallgató van az évfolyamon, akinek nincs nyelvvizsgája?

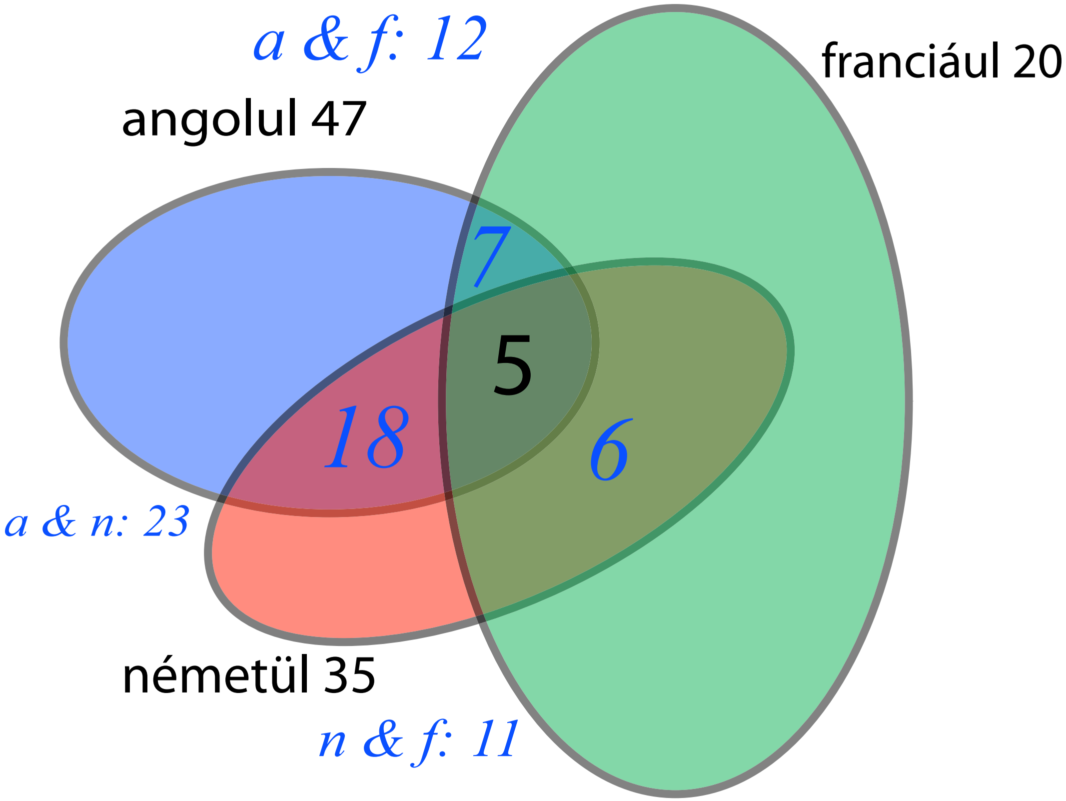
Az alábbi diagrammon ábrázolhatjuk az adatokat:



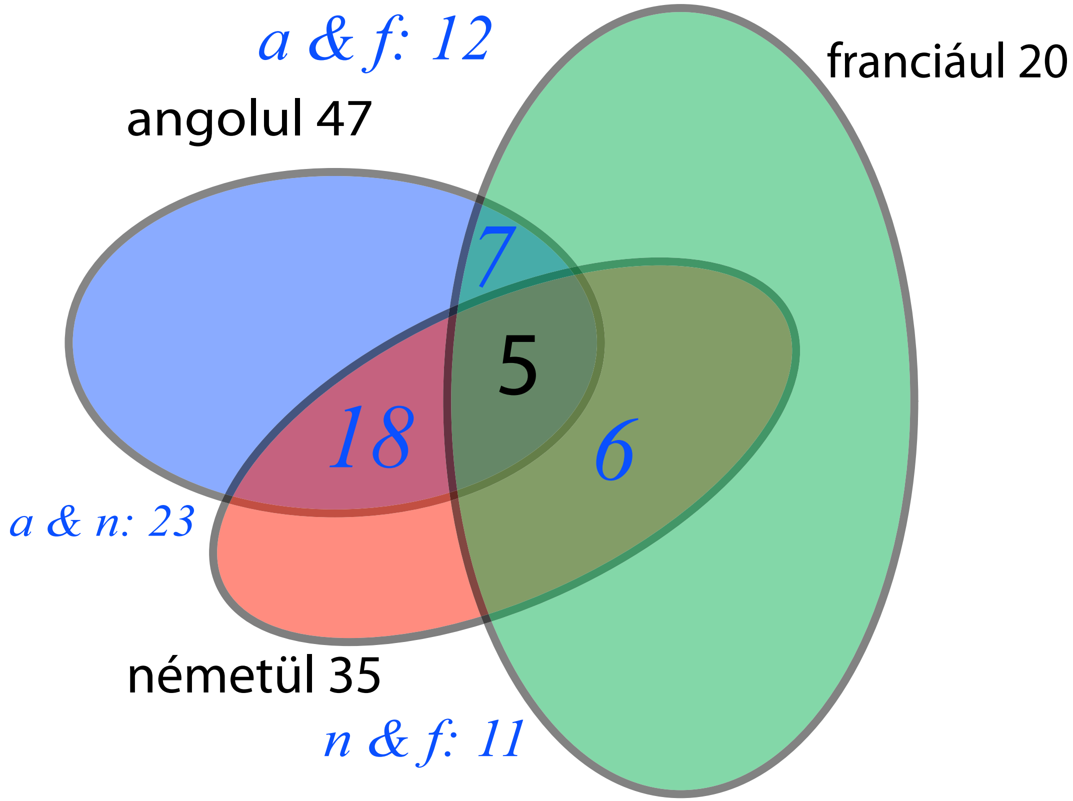
A vizsga feltétele: 20 pont a gyakorlaton!


a & f: 12
franciául 20
angolul 47
7
5
18
6
a & n: 23
németül 35
n & f: 11

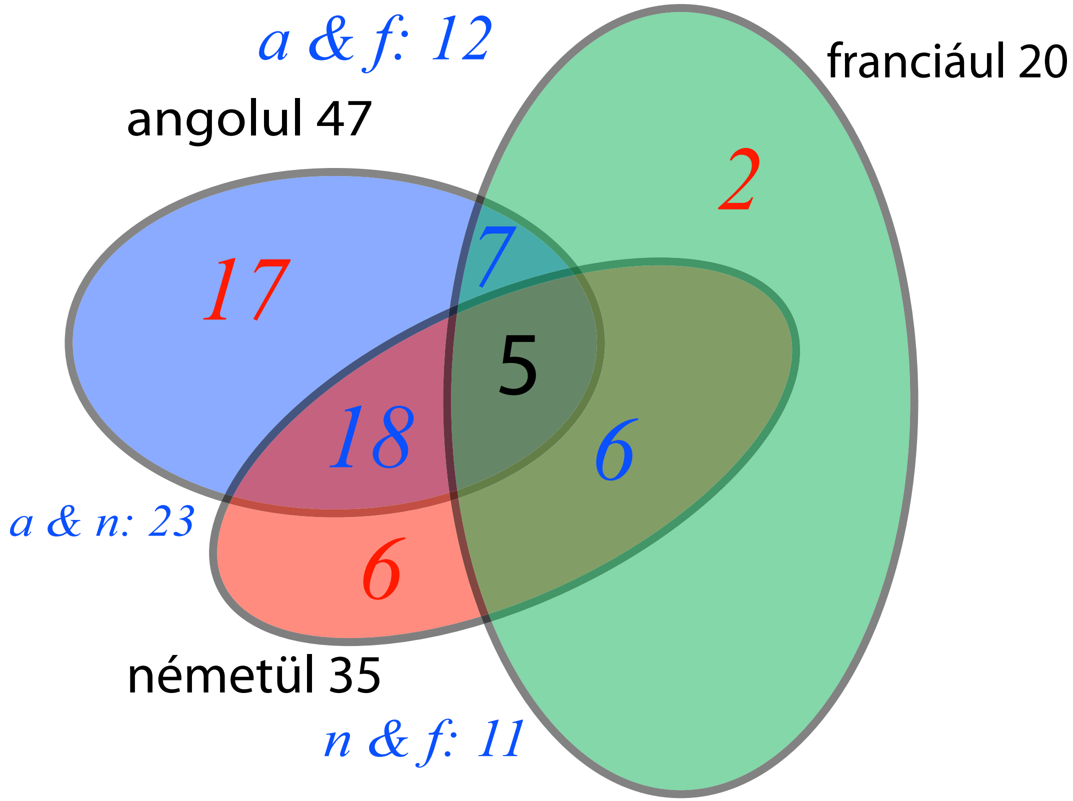
(



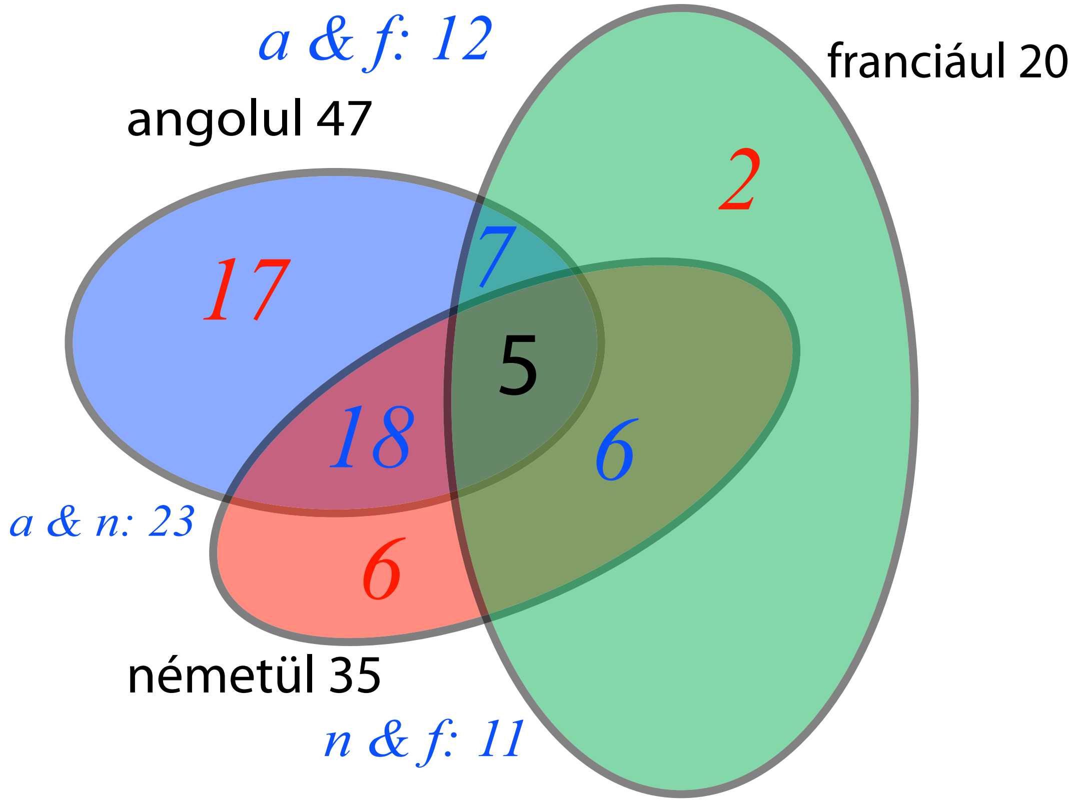
(Pl. a 18 így jött ki:



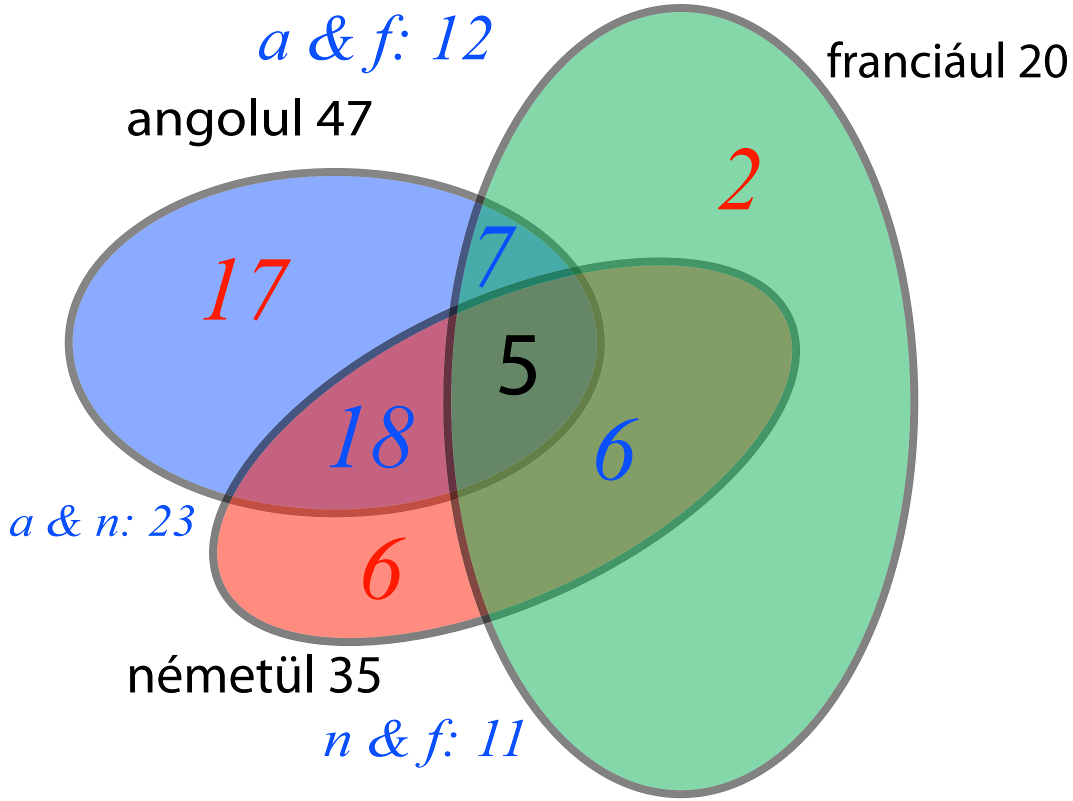
(Pl. a 18 így jött ki: angolul és németül összesen 23-an tudnak, és $18 = 23 - 5$.)


a & f: 12
franciául 20
angolul 47
2
17
7
5
18
6
a & n: 23
6
németül 35
n & f: 11

(



(Pl. a 17 így jött ki: $47 - (18 + 5 + 7)$.)



A beírt számok összege: $5 + 6 + 7 + 18 + 2 + 6 + 17 = 61$.

Ezért a 67-fős évfolyamból $67-61=6$ főnek nincs nyelvvizsgája.

Ezért a 67-fős évfolyamból $67 - 61 = 6$ főnek nincs nyelvvizsgája.

A feladat másként is megvilágítható: legyen rendre A, N és F az angol, német, illetve francia nyelvvizsgával rendelkezők halmaza.

Ezért a 67-fős évfolyamból $67 - 61 = 6$ főnek nincs nyelvvizsgája.

A feladat másként is megvilágítható: legyen rendre A, N és F az angol, német, illetve francia nyelvvizsgával rendelkezők halmaza. Ezek az U évfolyam (mint univerzum) részhalmazai.

Ezért a 67-fős évfolyamból $67-61=6$ főnek nincs nyelvvizsgája.

A feladat másként is megvilágítható: legyen rendre A, N és F az angol, német, illetve francia nyelvvizsgával rendelkezők halmaza. Ezek az U évfolyam (mint univerzum) részhalmazai. Keressük az $U\setminus(A\cup N\cup F)$ halmaz, azaz

Ezért a 67-fős évfolyamból $67-61=6$ főnek nincs nyelvvizsgája.

A feladat másként is megvilágítható: legyen rendre A, N és F az angol, német, illetve francia nyelvvizsgával rendelkezők halmaza. Ezek az U évfolyam (mint univerzum) részhalmazai. Keressük az $U\setminus(A\cup N\cup F)$ halmaz, azaz az $\overline{A\cup N\cup F}$ halmaz elemszámát.

Ezért a 67-fős évfolyamból $67-61=6$ főnek nincs nyelvvizsgája.

A feladat másként is megvilágítható: legyen rendre A, N és F az angol, német, illetve francia nyelvvizsgával rendelkezők halmaza. Ezek az U évfolyam (mint univerzum) részhalmazai. Keressük az $U \setminus (A \cup N \cup F)$ halmaz, azaz az $\overline{A \cup N \cup F}$ halmaz elemszámát. Ezt megkapjuk, ha $|U|$-ból levonjuk az $|A \cup N \cup F|$ elemszámát.

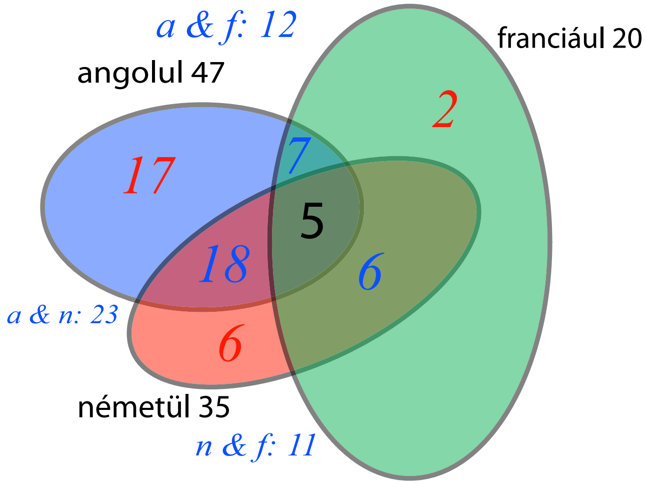
Ezért a 67-fős évfolyamból $67 - 61 = 6$ főnek nincs nyelvvizsgája.

A feladat másként is megvilágítható: legyen rendre A, N és F az angol, német, illetve francia nyelvvizsgával rendelkezők halmaza. Ezek az U évfolyam (mint univerzum) részhalmazai. Keressük az $U \setminus (A \cup N \cup F)$ halmaz, azaz az $\overline{A \cup N \cup F}$ halmaz elemszámát. Ezt megkapjuk, ha $|U|$-ból levonjuk az $|A \cup N \cup F|$ elemszámát. De mennyi az utóbbi?

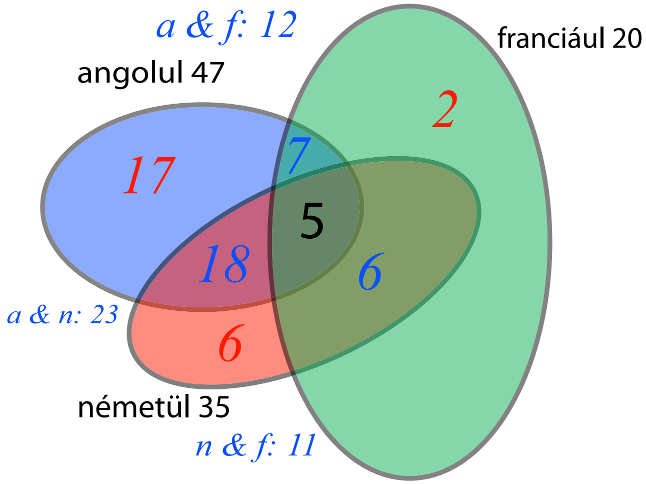
Ezért a 67-fős évfolyamból $67-61=6$ főnek nincs nyelvvizsgája.

A feladat másként is megvilágítható: legyen rendre A, N és F az angol, német, illetve francia nyelvvizsgával rendelkezők halmaza. Ezek az U évfolyam (mint univerzum) részhalmazai. Keressük az $U\setminus(A\cup N\cup F)$ halmaz, azaz az $\overline{A\cup N\cup F}$ halmaz elemszámát. Ezt megkapjuk, ha $|U|$-ból levonjuk az $|A\cup N\cup F|$ elemszámát. De mennyi az utóbbi?

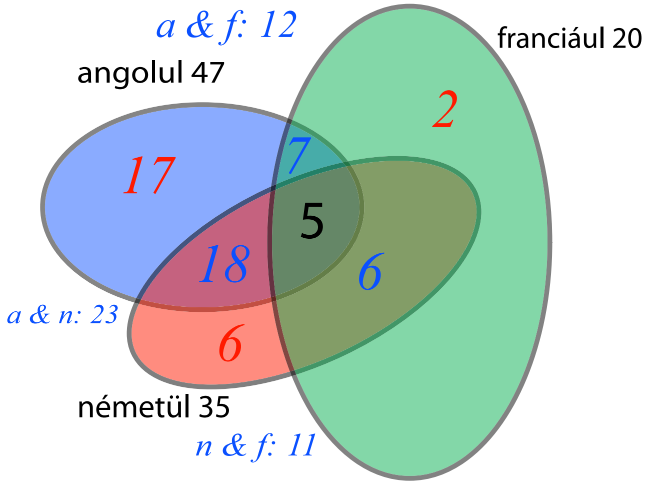
Első közelítésben $|A|+|N|+|F|$.



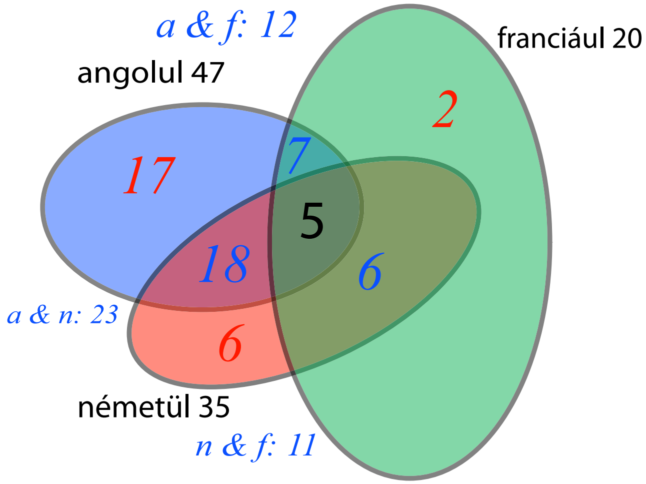
a & f: 12
franciául 20
angolul 47
2
17
7
5
18
6
a & n: 23
6
németül 35
n & f: 11



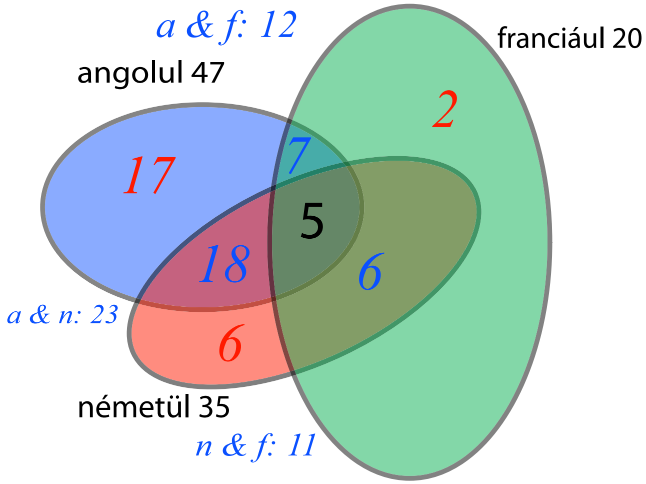
De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni:



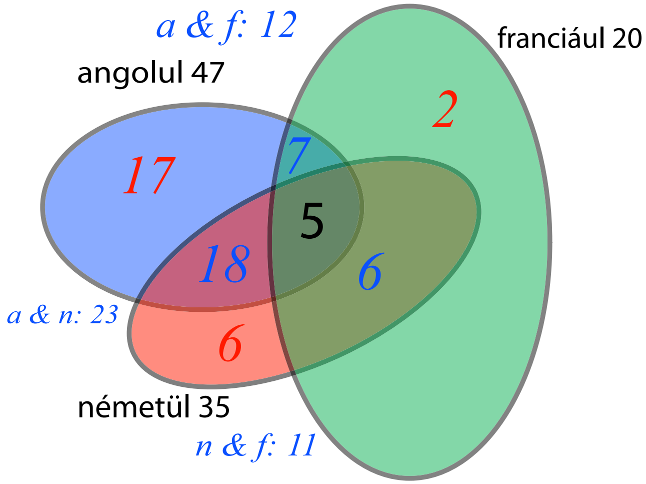
De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)$.



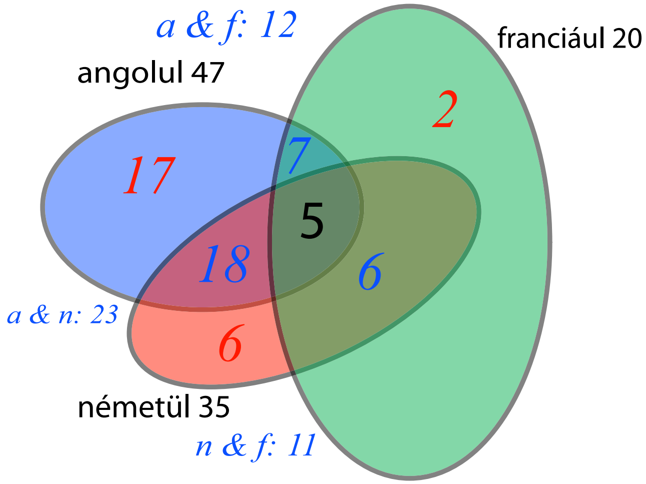
De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)$. Igen ám, de ekkor a mindhárom nyelven tudókat háromszor hozzászámoltuk,



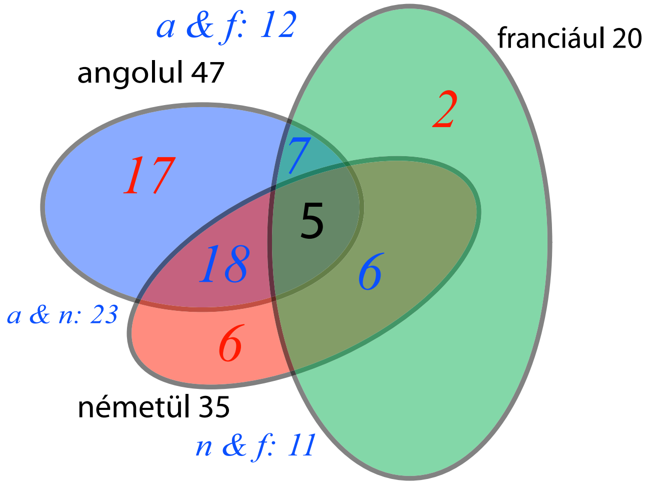
De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)$. Igen ám, de ekkor a mindhárom nyelven tudókat háromszor hozzászámoltuk, háromszor levontuk, ezért ezeket még hozzá kell adni:



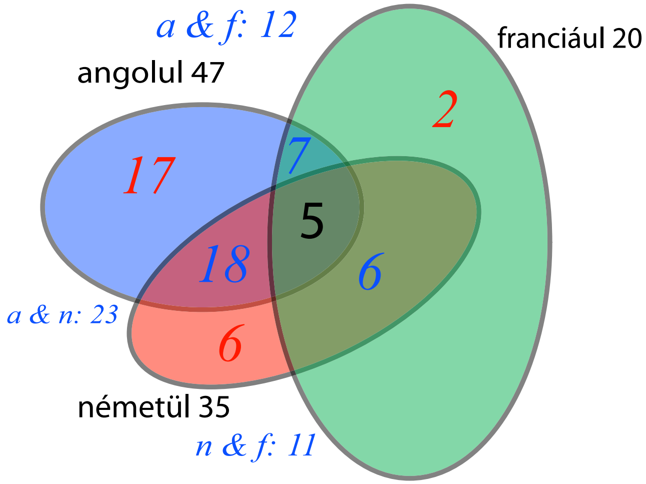
De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)$. Igen ám, de ekkor a mindhárom nyelven tudókat háromszor hozzászámoltuk, háromszor levontuk, ezért ezeket még hozzá kell adni: $|A|+|N|+|F|-$



De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)$. Igen ám, de ekkor a mindhárom nyelven tudókat háromszor hozzászámoltuk, háromszor levontuk, ezért ezeket még hozzá kell adni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)+$



De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)$. Igen ám, de ekkor a mindhárom nyelven tudókat háromszor hozzászámoltuk, háromszor levontuk, ezért ezeket még hozzá kell adni: $|A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)+|A\cap N\cap F|$.



De akkor a két nyelven is tudókat duplán számoltuk, azok számát le kell vonni: $|A|+|N|+|F|-(|A \cap N|+|A \cap F|+|N \cap F|)$. Igen ám, de ekkor a mindhárom nyelven tudókat háromszor hozzászámoltuk, háromszor levontuk, ezért ezeket még hozzá kell adni: $|A|+|N|+|F|-(|A \cap N|+|A \cap F|+|N \cap F|)+|A \cap N \cap F|$. Tehát:

$$|A \cup N \cup F| =$$

$$|A \cup N \cup F| = |A| + |N| + |F| -$$

$$|A \cup N \cup F| = |A| + |N| + |F| - (|A \cap N| + |A \cap F| + |N \cap F|) +$$

$$|A\cup N\cup F| = |A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)+|A\cap N\cap F|.$$

$$|A \cup N \cup F| = |A| + |N| + |F| - (|A \cap N| + |A \cap F| + |N \cap F|) + |A \cap N \cap F|.$$

Innen

$$|\overline{A \cup N \cup F}| =$$

$$|A \cup N \cup F| = |A| + |N| + |F| - (|A \cap N| + |A \cap F| + |N \cap F|) + |A \cap N \cap F|.$$

Innen

$$|\overline{A \cup N \cup F}| =$$

$|U| -$

$$|A \cup N \cup F| = |A| + |N| + |F| - (|A \cap N| + |A \cap F| + |N \cap F|) + |A \cap N \cap F|.$$

Innen

$$|\overline{A \cup N \cup F}| =$$

$$|U| - (|A| + |N| + |F|) +$$

$$|A \cup N \cup F| = |A| + |N| + |F| - (|A \cap N| + |A \cap F| + |N \cap F|) + |A \cap N \cap F|.$$

Innen

$$|\overline{A \cup N \cup F}| =$$

$$|U| - (|A| + |N| + |F|) + (|A \cap N| + |A \cap F| + |N \cap F|) -$$

$$|A \cup N \cup F| = |A| + |N| + |F| - (|A \cap N| + |A \cap F| + |N \cap F|) + |A \cap N \cap F|.$$

Innen

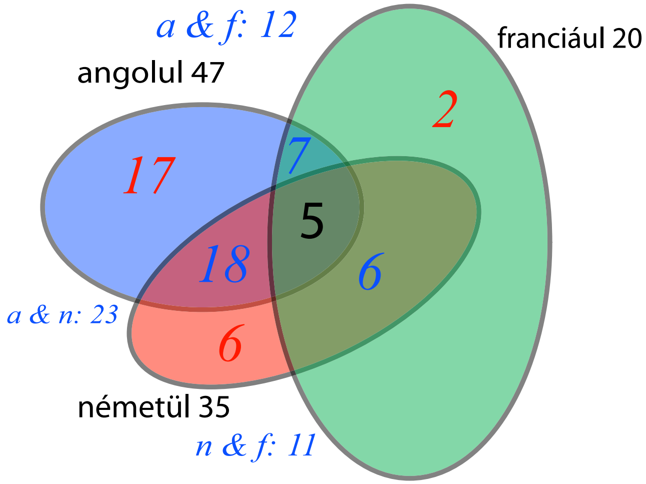
$$|\overline{A \cup N \cup F}| =$$
$$|U| - (|A| + |N| + |F|) + (|A \cap N| + |A \cap F| + |N \cap F|) - |A \cap N \cap F|.$$

$$|A\cup N\cup F| = |A|+|N|+|F|-(|A\cap N|+|A\cap F|+|N\cap F|)+|A\cap N\cap F|.$$

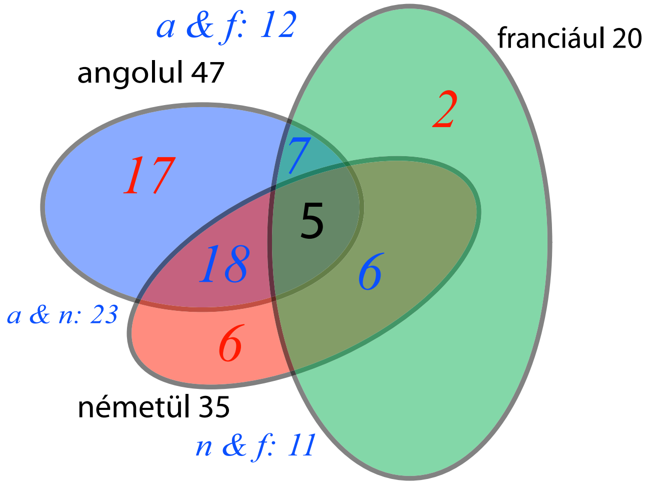
Innen

$$|\overline{A\cup N\cup F}| =$$
$$|U|-(|A|+|N|+|F|)+(|A\cap N|+|A\cap F|+|N\cap F|)-|A\cap N\cap F|.$$

A jelen adatokkal:



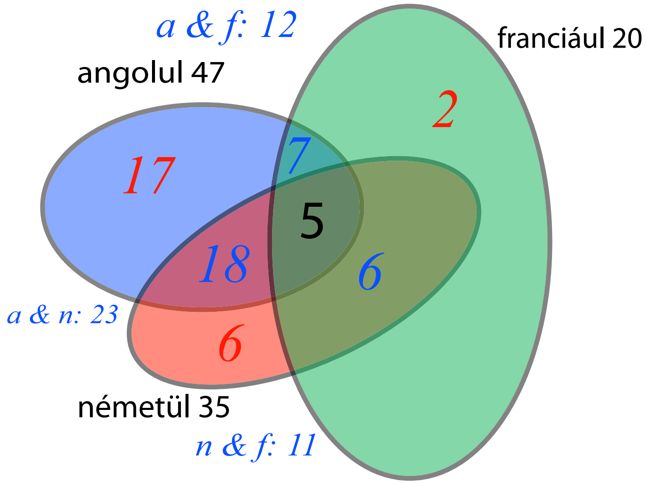
$$|\overline{A \cup N \cup F}| =$$



$$|\overline{A \cup N \cup F}| =$$

$$|U| - (|A| + |N| + |F|) + (|A \cap N| + |A \cap F| + |N \cap F|) - |A \cap N \cap F|.$$

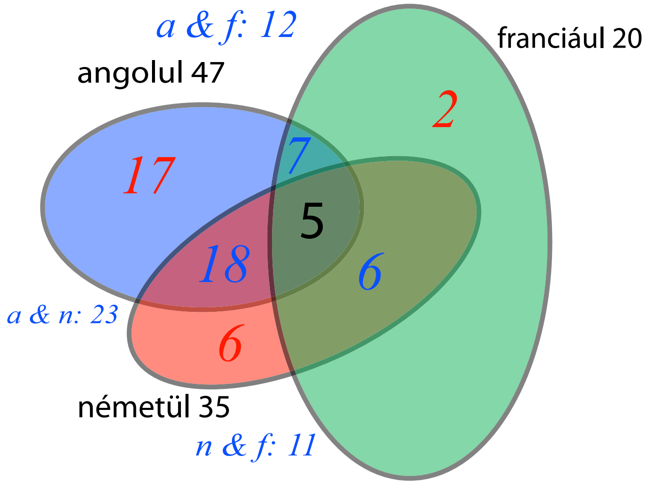
$67 -$



$$|\overline{A \cup N \cup F}| =$$

$$|U| - (|A| + |N| + |F|) + (|A \cap N| + |A \cap F| + |N \cap F|) - |A \cap N \cap F|.$$

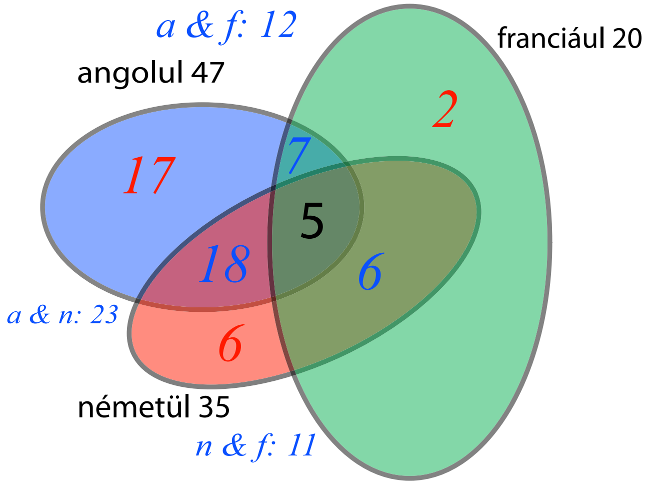
$$67 - (47 + 35 + 20) +$$



$$|\overline{A \cup N \cup F}| =$$

$$|U| - (|A| + |N| + |F|) + (|A \cap N| + |A \cap F| + |N \cap F|) - |A \cap N \cap F|.$$

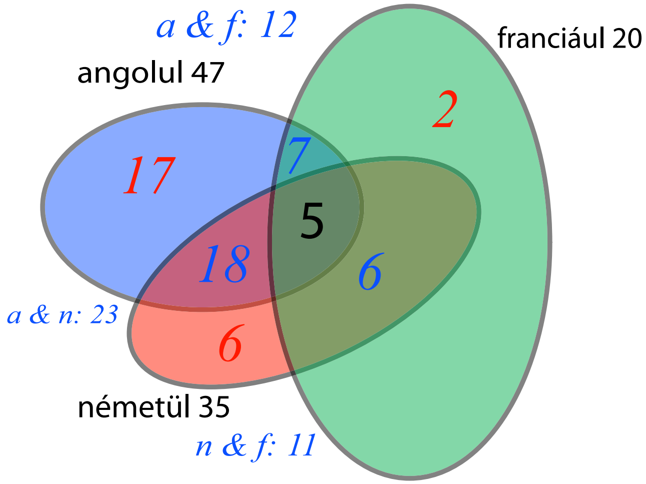
$$67 - (47 + 35 + 20) + (23 + 12 + 11) -$$



$$|\overline{A \cup N \cup F}| =$$

$$|U| - (|A| + |N| + |F|) + (|A \cap N| + |A \cap F| + |N \cap F|) - |A \cap N \cap F|.$$

$$67 - (47 + 35 + 20) + (23 + 12 + 11) - 5 =$$



$$|\overline{A \cup N \cup F}| =$$

$$|U| - (|A| + |N| + |F|) + (|A \cap N| + |A \cap F| + |N \cap F|) - |A \cap N \cap F|.$$

$$67 - (47 + 35 + 20) + (23 + 12 + 11) - 5 = 6.$$

Amit most láttunk, az az úgynevezett logikai szitaformula.

Amit most láttunk, az az úgynevezett logikai szitaformula. Nemcsak három halmaz esetén érvényes.

Amit most láttunk, az az úgynevezett logikai szitaformula. Nemcsak három halmaz esetén érvényes. A szitaformula arra ad választ, hogy adott véges halmazok uniójának komplementere hány elemű.

Amit most láttunk, az az úgynevezett logikai szitaformula. Nemcsak három halmaz esetén érvényes. A szitaformula arra ad választ, hogy adott véges halmazok uniójának komplementere hány elemű. (Az unió elemszámára vonatkozó összefüggést is szokás szitaformulának nevezni.)

Amit most láttunk, az az úgynevezett logikai szitaformula. Nemcsak három halmaz esetén érvényes. A szitaformula arra ad választ, hogy adott véges halmazok uniójának komplementere hány elemű. (Az unió elemszámára vonatkozó összefüggést is szokás szitaformulának nevezni.)

Fogalmazzuk meg a tételt precízen:

12. Tétel. *(A)*

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| =$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n}$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1}$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\{i_1, \ldots, i_r\}}$$

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}}$$

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}}$$

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,n\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:**

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha* $A_1, \ldots, A_n$ *a véges* U *univerzum (alaphalmaz) részhalmazai, akkor*

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| =$$

12. Tétel. *(A) Legyenek* $A_1, \ldots, A_n$ *véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha* $A_1, \ldots, A_n$ *a véges* U *univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| +$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| + \sum_{r=1}^{n}$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| + \sum_{r=1}^{n} (-1)^r$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| + \sum_{r=1}^{n} (-1)^r \sum_{(i_1, \ldots, i_r)}$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| + \sum_{r=1}^{n} (-1)^{r} \sum_{(i_1, \ldots, i_r) \in \{1, \ldots, n\}^r}$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| + \sum_{r=1}^{n} (-1)^{r} \sum_{\substack{(i_1, \ldots, i_r) \in \{1, \ldots, n\}^r \\ 1 \leq i_1 < \cdots < i_r \leq n}}$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| + \sum_{r=1}^{n} (-1)^{r} \sum_{\substack{(i_1, \ldots, i_r) \in \{1, \ldots, n\}^r \\ 1 \leq i_1 < \cdots < i_r \leq n}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

12. Tétel. *(A) Legyenek $A_1, \ldots, A_n$ véges halmazok. Ekkor*

$$|A_1 \cup \cdots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,n\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

(B) **Szitaformula:** *ha $A_1, \ldots, A_n$ a véges U univerzum (alaphalmaz) részhalmazai, akkor*

$$|\overline{A_1} \cap \cdots \cap \overline{A_n}| = |\overline{A_1 \cup \cdots \cup A_n}| =$$

$$|U| + \sum_{r=1}^{n} (-1)^{r} \sum_{\substack{(i_1,\ldots,i_r) \in \{1,\ldots,n\}^r \\ 1 \le i_1 < \cdots < i_r \le n}} |A_{i_1} \cap \cdots \cap A_{i_r}|.$$

Többnyire a „hány olyan . . . van, amelyre se nem . . . , se nem . . . , . . . ” típusú feladatoknál használjuk.

Többnyire a „hány olyan . . . van, amelyre se nem . . . , se nem . . . , . . . ” típusú feladatoknál használjuk. Érdemes megfigyelni, hogy a két szummajel alá írt indextartomány ugyanaz.

Többnyire a „hány olyan . . . van, amelyre se nem . . . , se nem . . . , . . . ” típusú feladatoknál használjuk. Érdemes megfigyelni, hogy a két szummajel alá írt indextartomány ugyanaz. De a formulánál sokkal fontosabb azt megjegyezni, hogy ahogy az egyre nagyobb tényezőszámú metszetek elemszámát vesszük, úgy váltakozik az előjel.

Többnyire a „hány olyan . . . van, amelyre se nem . . . , se nem . . . , . . . ” típusú feladatoknál használjuk. Érdemes megfigyelni, hogy a két szummajel alá írt indextartomány ugyanaz. De a formulánál sokkal fontosabb azt megjegyezni, hogy ahogy az egyre nagyobb tényezőszámú metszetek elemszámát vesszük, úgy váltakozik az előjel.

Speciális esetek (hogy könnyebben érthető legyen):

Többnyire a „hány olyan . . . van, amelyre se nem . . . , se nem . . . , . . . ” típusú feladatoknál használjuk. Érdemes megfigyelni, hogy a két szummajel alá írt indextartomány ugyanaz. De a formulánál sokkal fontosabb azt megjegyezni, hogy ahogy az egyre nagyobb tényezőszámú metszetek elemszámát vesszük, úgy váltakozik az előjel.

Speciális esetek (hogy könnyebben érthető legyen):

$n = 2$:

Többnyire a „hány olyan . . . van, amelyre se nem . . . , se nem . . . , . . . ” típusú feladatoknál használjuk. Érdemes megfigyelni, hogy a két szummajel alá írt indextartomány ugyanaz. De a formulánál sokkal fontosabb azt megjegyezni, hogy ahogy az egyre nagyobb tényezőszámú metszetek elemszámát vesszük, úgy váltakozik az előjel.

Speciális esetek (hogy könnyebben érthető legyen):

$n = 2$: $|A \cup B| = |A| + |B| - |A \cap B|$.

Többnyire a „hány olyan . . . van, amelyre se nem . . . , se nem . . . , . . . ” típusú feladatoknál használjuk. Érdemes megfigyelni, hogy a két szummajel alá írt indextartomány ugyanaz. De a formulánál sokkal fontosabb azt megjegyezni, hogy ahogy az egyre nagyobb tényezőszámú metszetek elemszámát vesszük, úgy váltakozik az előjel.

Speciális esetek (hogy könnyebben érthető legyen):

$n = 2$: $|A \cup B| = |A| + |B| - |A \cap B|$.

$|\overline{A \cup B}| = |U| - (|A| + |B|) + |A \cap B|$.

$n = 3$:

$n = 3$: $|A \cup B \cup C| =$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) -$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) +$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$.

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| =$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| -$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) +$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) -$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| =$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U|$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|)$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$

$(|A$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$

$(|A \cap$

$n=3$: $|A\cup B\cup C| = (|A|+|B|+|C|) - (|A\cap B| + |A\cap C| + |B\cap C|) + |A\cap B\cap C|$. $\quad |\overline{A\cup B\cup C}| = |U| - (|A|+|B|+|C|) + (|A\cap B| + |A\cap C| + |B\cap C|) - |A\cap B\cap C|$.

$n=4$:

$$|\overline{A\cup B\cup C\cup D}| = |U| - (|A|+|B|+|C|+|D|) +$$

$(|A\cap B| + |A$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$

$(|A \cap B| + |A \cap$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$

$$(|A \cap B| + |A \cap C| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$

$$(|A \cap B| + |A \cap C| + |A \cap D| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| + |A \cap B \cap D| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| +$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|)$$

$n=3$: $|A\cup B\cup C| = (|A|+|B|+|C|) - (|A\cap B| + |A\cap C| + |B\cap C|) + |A\cap B\cap C|$. $|\overline{A\cup B\cup C}| = |U| - (|A|+|B|+|C|) + (|A\cap B| + |A\cap C| + |B\cap C|) - |A\cap B\cap C|$.

$n=4$:

$$|\overline{A\cup B\cup C\cup D}| = |U| - (|A|+|B|+|C|+|D|)+$$
$$(|A\cap B| + |A\cap C| + |A\cap D| + |B\cap C| + |B\cap D| + |C\cap D|)$$
$$-(|A\cap B\cap C| + |A\cap B\cap D| + |A\cap C\cap D| + |B\cap C\cap D|) + |A$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|) + |A \cap$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $|\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|) + |A \cap B \cap$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|) + |A \cap B \cap C \cap$$

$n = 3$: $|A \cup B \cup C| = (|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$. $\quad |\overline{A \cup B \cup C}| = |U| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|$.

$n = 4$:

$$|\overline{A \cup B \cup C \cup D}| = |U| - (|A| + |B| + |C| + |D|) +$$
$$(|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|)$$
$$-(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|) + |A \cap B \cap C \cap D|.$$

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$,

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza.

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza. A feladat azt kérdezi, hogy mennyi $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza. A feladat azt kérdezi, hogy mennyi $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$ (a komplementerképzést az U halmazra vonatkoztatva).

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza. A feladat azt kérdezi, hogy mennyi $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$ (a komplementerképzést az U halmazra vonatkoztatva).

A szokásos módon jelölje $[x]$ az x valós szám egészrészét, azaz a legnagyobb olyan $z \in \mathbf{Z}$ számot, amelyre $z \leq x$.

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza. A feladat azt kérdezi, hogy mennyi $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$ (a komplementerképzést az U halmazra vonatkoztatva).

A szokásos módon jelölje $[x]$ az x valós szám egészrészét, azaz a legnagyobb olyan $z \in \mathbf{Z}$ számot, amelyre $z \leq x$. Például $[\sqrt{2}] = 1$,

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza. A feladat azt kérdezi, hogy mennyi $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$ (a komplementerképzést az U halmazra vonatkoztatva).

A szokásos módon jelölje $[x]$ az x valós szám egészrészét, azaz a legnagyobb olyan $z \in \mathbf{Z}$ számot, amelyre $z \leq x$. Például $[\sqrt{2}] = 1$, $[-\sqrt{2}] = -2$,

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza. A feladat azt kérdezi, hogy mennyi $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$ (a komplementerképzést az U halmazra vonatkoztatva).

A szokásos módon jelölje $[x]$ az x valós szám egészrészét, azaz a legnagyobb olyan $z \in \mathbf{Z}$ számot, amelyre $z \leq x$. Például $[\sqrt{2}] = 1$, $[-\sqrt{2}] = -2$, $[3] = 3$,

Feladat: Hány olyan száznál kisebb pozitív egész szám van, amelyik sem 2-vel, sem 3-mal, sem 5-tel nem osztható?

Megoldás: Legyen $U = \{1, 2, \ldots, 99\}$, továbbá A_2, A_3 és A_5 legyen rendre a kettővel, hárommal, illetve öttel osztható U-beli számok halmaza. A feladat azt kérdezi, hogy mennyi $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$ (a komplementerképzést az U halmazra vonatkoztatva).

A szokásos módon jelölje $[x]$ az x valós szám egészrészét, azaz a legnagyobb olyan $z \in \mathbf{Z}$ számot, amelyre $z \leq x$. Például $[\sqrt{2}] = 1$, $[-\sqrt{2}] = -2$, $[3] = 3$, $[-3] = -3$.

Először arra válaszoljunk, hogy adott d pozitív egész szám esetén hány U-beli szám osztható d-vel?

Először arra válaszoljunk, hogy adott d pozitív egész szám esetén hány U-beli szám osztható d-vel? 1-től 99-ig minden d-edik, tehát $[\frac{99}{d}]$ darab.

Először arra válaszoljunk, hogy adott d pozitív egész szám esetén hány U-beli szám osztható d-vel? 1-től 99-ig minden d-edik, tehát $[\frac{99}{d}]$ darab.

Pl. $d = 30$ esetén $[\frac{99}{30}] = 3$ darab U-beli szám osztható harminccal

Először arra válaszoljunk, hogy adott d pozitív egész szám esetén hány U-beli szám osztható d-vel? 1-től 99-ig minden d-edik, tehát $[\frac{99}{d}]$ darab.

Pl. $d = 30$ esetén $[\frac{99}{30}] = 3$ darab U-beli szám osztható harminccal (ezek éppen a 30, 60, 90 számok).

Először arra válaszoljunk, hogy adott d pozitív egész szám esetén hány U-beli szám osztható d-vel? 1-től 99-ig minden d-edik, tehát $[\frac{99}{d}]$ darab.

Pl. $d = 30$ esetén $[\frac{99}{30}] = 3$ darab U-beli szám osztható harminccal (ezek éppen a 30, 60, 90 számok).

Ha A_d jelöli a d-vel osztható U-beli számok halmazát, akkor az eddigiek szerint $|A_d| =$

Először arra válaszoljunk, hogy adott d pozitív egész szám esetén hány U-beli szám osztható d-vel? 1-től 99-ig minden d-edik, tehát $[\frac{99}{d}]$ darab.

Pl. $d = 30$ esetén $[\frac{99}{30}] = 3$ darab U-beli szám osztható harminccal (ezek éppen a 30, 60, 90 számok).

Ha A_d jelöli a d-vel osztható U-beli számok halmazát, akkor az eddigiek szerint $|A_d| = [\frac{99}{d}]$.

Először arra válaszoljunk, hogy adott d pozitív egész szám esetén hány U-beli szám osztható d-vel? 1-től 99-ig minden d-edik, tehát $[\frac{99}{d}]$ darab.

Pl. $d = 30$ esetén $[\frac{99}{30}] = 3$ darab U-beli szám osztható harminccal (ezek éppen a 30, 60, 90 számok).

Ha A_d jelöli a d-vel osztható U-beli számok halmazát, akkor az eddigiek szerint $|A_d| = [\frac{99}{d}]$. Világos az is, hogy pl. $A_3 \cap A_5 = A_{15}$, stb. Ezért a szitaformulát alkalmazva

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2| + |A_3| + |A_5|)$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| -$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|)$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2| + |A_3| + |A_5|) + (|A_2 \cap A_3| + |A_2 \cap A_5| + |A_3 \cap A_5|) - |A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + ($$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6|$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| +$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|)$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) -$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$99 -$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2\cap A_3|+|A_2\cap A_5|+|A_3\cap A_5|)-|A_2\cap A_3\cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}]$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] +$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}])$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2\cap A_3|+|A_2\cap A_5|+|A_3\cap A_5|)-|A_2\cap A_3\cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$
$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}]$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] +$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}])$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 -$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 - ($$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 - (49$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 - (49 + 33$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2| + |A_3| + |A_5|) + (|A_2 \cap A_3| + |A_2 \cap A_5| + |A_3 \cap A_5|) - |A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 - (49 + 33 + 19)$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 - (49 + 33 + 19) + ($$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$
$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$
$$99 - (49 + 33 + 19) + (16 +$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 - (49 + 33 + 19) + (16 + 9 +$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$

$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$

$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$

$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$

$$99 - (49 + 33 + 19) + (16 + 9 + 6) -$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2\cap A_3|+|A_2\cap A_5|+|A_3\cap A_5|)-|A_2\cap A_3\cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$
$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$
$$99 - (49 + 33 + 19) + (16 + 9 + 6) - 3 =$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$
$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$
$$99 - (49 + 33 + 19) + (16 + 9 + 6) - 3 = 26.$$

$$|\overline{A_2 \cup A_3 \cup A_5}| = |U| -$$
$$(|A_2|+|A_3|+|A_5|)+(|A_2 \cap A_3|+|A_2 \cap A_5|+|A_3 \cap A_5|)-|A_2 \cap A_3 \cap A_5| =$$
$$|U| - (|A_2| + |A_3| + |A_5|) + (|A_6| + |A_{10}| + |A_{15}|) - |A_{30}| =$$
$$99 - ([\frac{99}{2}] + [\frac{99}{3}] + [\frac{99}{5}]) + ([\frac{99}{6}] + [\frac{99}{10}] + [\frac{99}{15}]) - [\frac{99}{30}] =$$
$$99 - (49 + 33 + 19) + (16 + 9 + 6) - 3 = 26.$$

A következő feladat a szitaformula egy speciális esetének alkalmazását kívánja.

Feladat: (A) Hányféleképpen lehet n különböző képeslapot

Feladat: (A) Hányféleképpen lehet n különböző képeslapot egy k-tagú család tagjainak kiosztani, hogy mindenkinek legalább egy képeslap jusson?

Feladat: (A) Hányféleképpen lehet n különböző képeslapot egy k-tagú család tagjainak kiosztani, hogy mindenkinek legalább egy képeslap jusson? (A kiosztás sorrendje nem számít, csak az, hogy ki mit kap. Feltesszük, hogy $k \leq n$.)

Feladat: (A) Hányféleképpen lehet n különböző képeslapot egy k-tagú család tagjainak kiosztani, hogy mindenkinek legalább egy képeslap jusson? (A kiosztás sorrendje nem számít, csak az, hogy ki mit kap. Feltesszük, hogy $k \leq n$.)

(B) Egy n-elemű halmaznak hány szürjektív leképezése van egy k elemű halmazra?

Feladat: (A) Hányféleképpen lehet n különböző képeslapot egy k-tagú család tagjainak kiosztani, hogy mindenkinek legalább egy képeslap jusson? (A kiosztás sorrendje nem számít, csak az, hogy ki mit kap. Feltesszük, hogy $k \leq n$.)

(B) Egy n-elemű halmaznak hány szürjektív leképezése van egy k elemű halmazra?

Nyilván a két kérdésre ugyanaz a válasz, hiszen a kiosztás nem más mint egy leképezés (a képeslapot arra családtagra képezi le, aki a képeslapot kapja), és a szürjektivitás éppen azt jelenti, hogy mindenkinek jut képeslap.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap).

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai. Nyilván egy leképezés (avagy kiosztás) pontosan akkor szürjektív, ha egyetlen C_i-ben sincs benne.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai. Nyilván egy leképezés (avagy kiosztás) pontosan akkor szürjektív, ha egyetlen C_i-ben sincs benne. Tehát a szürjektív $A \to B$ leképezések halmaza $\overline{C_1} \cap \cdots \cap \overline{C_k}$.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai. Nyilván egy leképezés (avagy kiosztás) pontosan akkor szürjektív, ha egyetlen C_i-ben sincs benne. Tehát a szürjektív $A \to B$ leképezések halmaza $\overline{C_1} \cap \cdots \cap \overline{C_k}$. Ennek az elemszámát kell meghatároznunk.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai. Nyilván egy leképezés (avagy kiosztás) pontosan akkor szürjektív, ha egyetlen C_i-ben sincs benne. Tehát a szürjektív $A \to B$ leképezések halmaza $\overline{C_1} \cap \cdots \cap \overline{C_k}$. Ennek az elemszámát kell meghatároznunk.

Emlékeztető: egy n-elemű halmaznak egy t-elemű halmazba t^n leképezése van.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai. Nyilván egy leképezés (avagy kiosztás) pontosan akkor szürjektív, ha egyetlen C_i-ben sincs benne. Tehát a szürjektív $A \to B$ leképezések halmaza $\overline{C_1} \cap \cdots \cap \overline{C_k}$. Ennek az elemszámát kell meghatároznunk.

Emlékeztető: egy n-elemű halmaznak egy t-elemű halmazba t^n leképezése van. Ezt az ismétléses variációknál láttuk.

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai. Nyilván egy leképezés (avagy kiosztás) pontosan akkor szürjektív, ha egyetlen C_i-ben sincs benne. Tehát a szürjektív $A \to B$ leképezések halmaza $\overline{C_1} \cap \cdots \cap \overline{C_k}$. Ennek az elemszámát kell meghatároznunk.

Emlékeztető: egy n-elemű halmaznak egy t-elemű halmazba t^n leképezése van. Ezt az ismétléses variációknál láttuk. (Vagy most is könnyen kijön: az első elemnek t képe lehet, a másodiknak is, stb., az n-ediknek is,

Legyen $A = \{1, \ldots, n\}$ a képeslapok, $B = \{1, \ldots, k\}$ a családtagok halmaza. Jelölje C_i az olyan $A \to B$ leképezések halmazát, amelyeknél az i nem képelem (azaz az i családtagnak nem jut képeslap). Itt $i = 1, \ldots, k$. Legyen U az összes $A \to B$ leképezés halmaza. Ez lesz az univerzum, amelynek a C_i-k részhalmazai. Nyilván egy leképezés (avagy kiosztás) pontosan akkor szürjektív, ha egyetlen C_i-ben sincs benne. Tehát a szürjektív $A \to B$ leképezések halmaza $\overline{C_1} \cap \cdots \cap \overline{C_k}$. Ennek az elemszámát kell meghatároznunk.

Emlékeztető: egy n-elemű halmaznak egy t-elemű halmazba t^n leképezése van. Ezt az ismétléses variációknál láttuk. (Vagy most is könnyen kijön: az első elemnek t képe lehet, a másodiknak is, stb., az n-ediknek is, tehát a szorzási szabály szerint t^n leképezés van.)

Ezért $|U| = k^n$. Mivel C_i

Ezért $|U| = k^n$. Mivel C_i éppen az $A \longrightarrow B \setminus \{i\}$ leképezések halmaza, Ezért $|U| = k^n$. Mivel C_i éppen az $A \to B \setminus \{i\}$ leképezések halmaza, $|C_i| = (k-1)^n$.

Ezért $|U| = k^n$. Mivel C_i éppen az $A \to B \setminus \{i\}$ leképezések halmaza, $|C_i| = (k-1)^n$. Mivel $i \neq j$-re $C_i \cap C_j$

Ezért $|U| = k^n$. Mivel C_i éppen az $A \to B \setminus \{i\}$ leképezések halmaza, $|C_i| = (k-1)^n$. Mivel $i \neq j$-re $C_i \cap C_j$ éppen az

Ezért $|U| = k^n$. Mivel C_i éppen az $A \to B \setminus \{i\}$ leképezések halmaza, $|C_i| = (k-1)^n$. Mivel $i \neq j$-re $C_i \cap C_j$ éppen az $A \to B \setminus \{i, j\}$ leképezések halmaza, Ezért $|U| = k^n$. Mivel C_i éppen az $A \to B \setminus \{i\}$ leképezések halmaza, $|C_i| = (k-1)^n$. Mivel $i \neq j$-re $C_i \cap C_j$ éppen az $A \to B \setminus \{i, j\}$ leképezések halmaza, $|C_i \cap C_j| = (k-2)^n$.

Ha $\{i_1, \ldots, i_r\}$ egy r-elemű részhalmaza B-nek, akkor $C_{i_1} \cap \cdots \cap C_{i_r}$ éppen az $A \to B \setminus \{i_1, \ldots, i_r\}$ leképezések halmaza, tehát $(k-r)^n$ eleme van.

Ezért $|U| = k^n$. Mivel C_i éppen az $A \to B \setminus \{i\}$ leképezések halmaza, $|C_i| = (k-1)^n$. Mivel $i \neq j$-re $C_i \cap C_j$ éppen az $A \to B \setminus \{i,j\}$ leképezések halmaza, $|C_i \cap C_j| = (k-2)^n$.

Ha $\{i_1, \ldots, i_r\}$ egy r-elemű részhalmaza B-nek, akkor $C_{i_1} \cap \cdots \cap C_{i_r}$ éppen az $A \to B \setminus \{i_1, \ldots, i_r\}$ leképezések halmaza, tehát $(k-r)^n$ eleme van. Ez független attól, hogy melyik $\{i_1, \ldots, i_r\} \subseteq B$ részhalmazról van szó, csak attól függ, hogy ez a részhalmaz r-elemű.

Ezért $|U| = k^n$. Mivel C_i éppen az $A \to B \setminus \{i\}$ leképezések halmaza, $|C_i| = (k-1)^n$. Mivel $i \neq j$-re $C_i \cap C_j$ éppen az $A \to B \setminus \{i,j\}$ leképezések halmaza, $|C_i \cap C_j| = (k-2)^n$.

Ha $\{i_1, \ldots, i_r\}$ egy r-elemű részhalmaza B-nek, akkor $C_{i_1} \cap \cdots \cap C_{i_r}$ éppen az $A \to B \setminus \{i_1, \ldots, i_r\}$ leképezések halmaza, tehát $(k-r)^n$ eleme van. Ez független attól, hogy melyik $\{i_1, \ldots, i_r\} \subseteq B$ részhalmazról van szó, csak attól függ, hogy ez a részhalmaz r-elemű.

Ezért a szitaformulában szereplő

Ezért a szitaformulában szereplő

$$\sum_{\{i_1,\ldots,i_r\}}$$

Ezért a szitaformulában szereplő

$$\sum_{\{i_1,...,i_r\} \subseteq \{1,...,k\}}$$

Ezért a szitaformulában szereplő

$$\sum_{\substack{\{i_1,\ldots,i_r\}\subseteq\{1,\ldots,k\}\\ |\{i_1,\ldots,,i_r\}|=r}}$$

Ezért a szitaformulában szereplő

$$\sum_{\substack{\{i_1,\ldots,i_r\}\subseteq\{1,\ldots,k\}\\ |\{i_1,\ldots,,i_r\}|=r}} |C_{i_1}\cap\cdots\cap C_{i_r}|$$

részösszeg

Ezért a szitaformulában szereplő

$$\sum_{\substack{\{i_1,\ldots,i_r\}\subseteq\{1,\ldots,k\}\\ |\{i_1,\ldots,,i_r\}|=r}} |C_{i_1}\cap\cdots\cap C_{i_r}|$$

részösszeg minden tagja $(k-r)^n$. Ezen részösszeg tagjainak száma,

Ezért a szitaformulában szereplő

$$\sum_{\substack{\{i_1,\ldots,i_r\}\subseteq\{1,\ldots,k\}\\ |\{i_1,\ldots,,i_r\}|=r}} |C_{i_1}\cap\cdots\cap C_{i_r}|$$

részösszeg minden tagja $(k-r)^n$. Ezen részösszeg tagjainak száma, azaz az r-elemű részhalmazok száma

Ezért a szitaformulában szereplő

$$\sum_{\substack{\{i_1,\ldots,i_r\}\subseteq\{1,\ldots,k\}\\ |\{i_1,\ldots,,i_r\}|=r}} |C_{i_1}\cap\cdots\cap C_{i_r}|$$

részösszeg minden tagja $(k-r)^n$. Ezen részösszeg tagjainak száma, azaz az r-elemű részhalmazok száma $\binom{k}{r}$. Tehát ezen részösszeg értéke $\binom{k}{r}(k-r)^n$.

Ezért a szitaformulában szereplő

$$\sum_{\substack{\{i_1,\ldots,i_r\}\subseteq\{1,\ldots,k\}\\ |\{i_1,\ldots,,i_r\}|=r}} |C_{i_1}\cap\cdots\cap C_{i_r}|$$

részösszeg minden tagja $(k-r)^n$. Ezen részösszeg tagjainak száma, azaz az r-elemű részhalmazok száma $\binom{k}{r}$. Tehát ezen részösszeg értéke $\binom{k}{r}(k-r)^n$. Az eddigiek szerint

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| +$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k}$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \sum_{\{i_1, \ldots, i_r\}}$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \sum_{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, k\}}$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, k\} \\ |\{i_1, \ldots, , i_r\}| = r}}$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, k\} \\ |\{i_1, \ldots, , i_r\}| = r}} |C_{i_1} \cap \cdots \cap C_{i_r}| =$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, k\} \\ |\{i_1, \ldots, , i_r\}| = r}} |C_{i_1} \cap \cdots \cap C_{i_r}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \binom{k}{r} (k-r)^n =$$

$$|\overline{C_1} \cap \cdots \cap \overline{C_k}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,k\} \\ |\{i_1,\ldots,,i_r\}| = r}} |C_{i_1} \cap \cdots \cap C_{i_r}| =$$

$$|U| + \sum_{r=1}^{k} (-1)^r \binom{k}{r} (k-r)^n = \sum_{r=0}^{k} (-1)^r \binom{k}{r} (k-r)^n$$

a szürjektív leképezések száma. Q.e.d.

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás:

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen:

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők,

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő.

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki,

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat.

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat. A szorzási szabály szerint $\binom{8}{i} \cdot \binom{7}{6-i}$ féle módon lehet a ketrecet i darab oroszlánnal és $6-i$ darab leopárddal benépesíteni.

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat. A szorzási szabály szerint $\binom{8}{i} \cdot \binom{7}{6-i}$ féle módon lehet a ketrecet i darab oroszlánnal és $6-i$ darab leopárddal benépesíteni. Végül az eredményt az összeadási szabály adja:

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat. A szorzási szabály szerint $\binom{8}{i} \cdot \binom{7}{6-i}$ féle módon lehet a ketrecet i darab oroszlánnal és $6-i$ darab leopárddal benépesíteni. Végül az eredményt az összeadási szabály adja:

$$\binom{8}{0} \cdot \binom{7}{6}$$

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat. A szorzási szabály szerint $\binom{8}{i} \cdot \binom{7}{6-i}$ féle módon lehet a ketrecet i darab oroszlánnal és $6-i$ darab leopárddal benépesíteni. Végül az eredményt az összeadási szabály adja:

$$\binom{8}{0} \cdot \binom{7}{6} + \binom{8}{1} \cdot \binom{7}{5} +$$

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat. A szorzási szabály szerint $\binom{8}{i} \cdot \binom{7}{6-i}$ féle módon lehet a ketrecet i darab oroszlánnal és $6-i$ darab leopárddal benépesíteni. Végül az eredményt az összeadási szabály adja:

$$\binom{8}{0} \cdot \binom{7}{6} + \binom{8}{1} \cdot \binom{7}{5} + \binom{8}{2} \cdot \binom{7}{4} =$$

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat. A szorzási szabály szerint $\binom{8}{i} \cdot \binom{7}{6-i}$ féle módon lehet a ketrecet i darab oroszlánnal és $6-i$ darab leopárddal benépesíteni. Végül az eredményt az összeadási szabály adja:

$$\binom{8}{0} \cdot \binom{7}{6} + \binom{8}{1} \cdot \binom{7}{5} + \binom{8}{2} \cdot \binom{7}{4} = \dots$$

Feladat: A tágas ketrecbe nyolc oroszlán és hét leopárd közül összesen hat állatot szeretnénk elhelyezni úgy, hogy legalább kétszer annyi leopárd legyen a ketrecben, mint oroszlán.

Megoldás: Értelemszerűen: az állatok különbözők, a sorrend nem számít. Az oroszlánok száma lehet nulla, egy vagy kettő. Ha i darab oroszlánt választunk ki, tehetjük $\binom{8}{i}$ féleképpen, akkor a rögzített kiválasztott oroszlánok mellé $\binom{7}{6-i}$ féleképpen választhatunk leopárdokat. A szorzási szabály szerint $\binom{8}{i} \cdot \binom{7}{6-i}$ féle módon lehet a ketrecet i darab oroszlánnal és $6-i$ darab leopárddal benépesíteni. Végül az eredményt az összeadási szabály adja:

$$\binom{8}{0} \cdot \binom{7}{6} + \binom{8}{1} \cdot \binom{7}{5} + \binom{8}{2} \cdot \binom{7}{4} = \ldots = 1155.$$

Feladat: Az állatidomár libasorban vezeti be állatait, kilenc tigrist és öt medvét, a porondra. Hányféleképpen teheti ezt (hányféleképpen rakhatja sorba az állatokat), ha két medve nem kerülhet egymás mellé, továbbá Balu nem kerülhet Sir Kán mellé?

Feladat: Az állatidomár libasorban vezeti be állatait, kilenc tigrist és öt medvét, a porondra. Hányféleképpen teheti ezt (hányféleképpen rakhatja sorba az állatokat), ha két medve nem kerülhet egymás mellé, továbbá Balu nem kerülhet Sir Kán mellé? (Balu az egyik medve, Sir Kán pedig az egyik tigris.)

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal.

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.)

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba,

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára:

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára: mindegyik tigris előtt, illetve az utolsó tigris után.

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára: mindegyik tigris előtt, illetve az utolsó tigris után. A tíz hely mindegyikére legfeljebb egy medve rakható.

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára: mindegyik tigris előtt, illetve az utolsó tigris után. A tíz hely mindegyikére legfeljebb egy medve rakható. Az első medvét 10,

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára: mindegyik tigris előtt, illetve az utolsó tigris után. A tíz hely mindegyikére legfeljebb egy medve rakható. Az első medvét 10, a másodikat 9,

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára: mindegyik tigris előtt, illetve az utolsó tigris után. A tíz hely mindegyikére legfeljebb egy medve rakható. Az első medvét 10, a másodikat 9, ..., helyre rakhatjuk, tehát a medvék $10 \cdot 9 \ldots \cdot 6$-féleképpen rakhatók sorba. Tehát az

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára: mindegyik tigris előtt, illetve az utolsó tigris után. A tíz hely mindegyikére legfeljebb egy medve rakható. Az első medvét 10, a másodikat 9, ..., helyre rakhatjuk, tehát a medvék $10 \cdot 9 \ldots \cdot 6$-féleképpen rakhatók sorba. Tehát az összes eset:

Megoldás: Először ne törődjünk a Sir Kán — Balu tilalommal. A kilenc tigris 9!-féleképpen rakható sorba. (De tágasan, maradjon köztük hely.) Bárhogy is raktuk őket sorba, tíz hely kínálkozik a medvék számára: mindegyik tigris előtt, illetve az utolsó tigris után. A tíz hely mindegyikére legfeljebb egy medve rakható. Az első medvét 10, a másodikat 9, . . . , helyre rakhatjuk, tehát a medvék $10 \cdot 9 \ldots \cdot 6$-féleképpen rakhatók sorba. Tehát az összes eset:

$$9! \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6.$$

Most nézzük a rossz eseteket.

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X.

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük.

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük. A négy további medvét a kimaradó helyekre rakhatjuk (ez 10 hely), Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük. A négy további medvét a kimaradó helyekre rakhatjuk (ez 10 hely), kivéve az X előtti helyet.

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük. A négy további medvét a kimaradó helyekre rakhatjuk (ez 10 hely), kivéve az X előtti helyet. Az X előtti hely akkor is kivétel, ha X a sor elején vagy végén áll. Tehát csak kilenc hely marad a négy további medvének.

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük. A négy további medvét a kimaradó helyekre rakhatjuk (ez 10 hely), kivéve az X előtti helyet. Az X előtti hely akkor is kivétel, ha X a sor elején vagy végén áll. Tehát csak kilenc hely marad a négy további medvének. Az elsőt 9, a másodikat 8, stb.

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük. A négy további medvét a kimaradó helyekre rakhatjuk (ez 10 hely), kivéve az X előtti helyet. Az X előtti hely akkor is kivétel, ha X a sor elején vagy végén áll. Tehát csak kilenc hely marad a négy további medvének. Az elsőt 9, a másodikat 8, stb. helyre tehetjük, azaz $9 \cdot 8 \cdot 7 \cdot 6$-féleképpen helyezhetjük el a medvéket.

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük. A négy további medvét a kimaradó helyekre rakhatjuk (ez 10 hely), kivéve az X előtti helyet. Az X előtti hely akkor is kivétel, ha X a sor elején vagy végén áll. Tehát csak kilenc hely marad a négy további medvének. Az elsőt 9, a másodikat 8, stb. helyre tehetjük, azaz $9 \cdot 8 \cdot 7 \cdot 6$-féleképpen helyezhetjük el a medvéket. A szorzási szabály szerint ha Balu közvetlenül Sir Kán előtt van, az

Most nézzük a rossz eseteket. Ha B(alu) és S(ir Kán) egymás mellé kerül, mondjuk BS sorrendben, akkor ők ketten egyetlen állatnak tekinthetők, ezt az állatot jelölje X. Előbb helyezzük el X-et és a további 8 tigrist, ezt 9!-féleképpen tehetjük. A négy további medvét a kimaradó helyekre rakhatjuk (ez 10 hely), kivéve az X előtti helyet. Az X előtti hely akkor is kivétel, ha X a sor elején vagy végén áll. Tehát csak kilenc hely marad a négy további medvének. Az elsőt 9, a másodikat 8, stb. helyre tehetjük, azaz $9 \cdot 8 \cdot 7 \cdot 6$-féleképpen helyezhetjük el a medvéket. A szorzási szabály szerint ha Balu közvetlenül Sir Kán előtt van, az $9! \cdot 9 \cdot 8 \cdot 7 \cdot 6$-féleképpen lehetséges.

Nyilván ugyanez jön ki akkor is, ha Sir Kán van közvetlenül Balu előtt

Nyilván ugyanez jön ki akkor is, ha Sir Kán van közvetlenül Balu előtt (a különbség csak annyi, hogy nem az X előtti, hanem az X utáni hely tiltott a medvék számára).

Nyilván ugyanez jön ki akkor is, ha Sir Kán van közvetlenül Balu előtt (a különbség csak annyi, hogy nem az X előtti, hanem az X utáni hely tiltott a medvék számára). Tehát a rossz esetek száma $2 \cdot 9! \cdot 9 \cdot 8 \cdot 7 \cdot 6$.

Nyilván ugyanez jön ki akkor is, ha Sir Kán van közvetlenül Balu előtt (a különbség csak annyi, hogy nem az X előtti, hanem az X utáni hely tiltott a medvék számára). Tehát a rossz esetek száma $2 \cdot 9! \cdot 9 \cdot 8 \cdot 7 \cdot 6$.

Ezek után az eredmény

$$9! \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 - 2 \cdot 9! \cdot 9 \cdot 8 \cdot 7 \cdot 6 =$$

Nyilván ugyanez jön ki akkor is, ha Sir Kán van közvetlenül Balu előtt (a különbség csak annyi, hogy nem az X előtti, hanem az X utáni hely tiltott a medvék számára). Tehát a rossz esetek száma $2 \cdot 9! \cdot 9 \cdot 8 \cdot 7 \cdot 6$.

Ezek után az eredmény

$$9! \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 - 2 \cdot 9! \cdot 9 \cdot 8 \cdot 7 \cdot 6 = \underline{8\,778\,792\,960}.$$

Feladat: Öt házaspár hányféleképpen táncolhat úgy, hogy egyik férj sem a saját feleségével táncol?

Feladat: Öt házaspár hányféleképpen táncolhat úgy, hogy egyik férj sem a saját feleségével táncol? (Nyilván a sorrend nem számít, csak az, hogy ki kivel táncol.)

Megoldás: A feladat azzal ekvivalens, hogy

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj,

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5,

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön.

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát,

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!.

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4, 5, 2, 3, 1) \in U$.)

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol).

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2$

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2 \cap A_3$. Mi az $\overline{A_1} \cap \cdots \cap \overline{A_5}$ elemszámát keressük.

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2 \cap A_3$. Mi az $\overline{A_1} \cap \cdots \cap \overline{A_5}$ elemszámát keressük. Vegyük észre, hogy $|A_1| = 4! = 24$ (

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2 \cap A_3$. Mi az $\overline{A_1} \cap \cdots \cap \overline{A_5}$ elemszámát keressük. Vegyük észre, hogy $|A_1| = 4! = 24$ (mert az 1 helyben marad és csak a további négy elemet kell permutálni),

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2 \cap A_3$. Mi az $\overline{A_1} \cap \cdots \cap \overline{A_5}$ elemszámát keressük. Vegyük észre, hogy $|A_1| = 4! = 24$ (mert az 1 helyben marad és csak a további négy elemet kell permutálni), $|A_1 \cap A_2| = 3! = 6$

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2 \cap A_3$. Mi az $\overline{A_1} \cap \cdots \cap \overline{A_5}$ elemszámát keressük. Vegyük észre, hogy $|A_1| = 4! = 24$ (mert az 1 helyben marad és csak a további négy elemet kell permutálni), $|A_1 \cap A_2| = 3! = 6$ (mert az 1 és a 2 helyben marad, és csak a további három elemet kell permutálni), stb. Ezért,

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2 \cap A_3$. Mi az $\overline{A_1} \cap \cdots \cap \overline{A_5}$ elemszámát keressük. Vegyük észre, hogy $|A_1| = 4! = 24$ (mert az 1 helyben marad és csak a további négy elemet kell permutálni), $|A_1 \cap A_2| = 3! = 6$ (mert az 1 és a 2 helyben marad, és csak a további három elemet kell permutálni), stb. Ezért, a szitaformulát használva

Megoldás: A feladat azzal ekvivalens, hogy hányféleképpen permutálható az öt férj, mondjuk az 1,2,3,4,5, hogy egyik se a saját helyére kerüljön. Jelölje U az 1,2,3,4,5 összes permutációjának halmazát, ennek elemszáma 5!. Például 45231 $\in U$, 52134 $\in U$, stb. (Persze írhatnánk így is: $(4,5,2,3,1) \in U$.) Legyen A_i azon permutációk halmaza, amelyeknél az i-edik helyen i van (azaz, ahol i a saját feleségével táncol). Pl. 52314 $\in A_2 \cap A_3$. Mi az $\overline{A_1} \cap \cdots \cap \overline{A_5}$ elemszámát keressük. Vegyük észre, hogy $|A_1| = 4! = 24$ (mert az 1 helyben marad és csak a további négy elemet kell permutálni), $|A_1 \cap A_2| = 3! = 6$ (mert az 1 és a 2 helyben marad, és csak a további három elemet kell permutálni), stb. Ezért, a szitaformulát használva

$$|\overline{A_1 \cup \cdots \cup A_5}|$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| +$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5}$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\{i_1,\ldots,i_r\}}$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, 5\}}$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}}$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}}$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, 5\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, 5\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 -$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, 5\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! +$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3!$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, 5\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! +$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! -$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! =$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, 5\} \\ |\{i_1, \ldots, i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! =$$

$$120 - 120 +$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! =$$

$$120 - 120 + 60 -$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! =$$

$$120 - 120 + 60 - 20 +$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! =$$

$$120 - 120 + 60 - 20 + 5 -$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! =$$

$$120 - 120 + 60 - 20 + 5 - 1 =$$

$$|\overline{A_1 \cup \cdots \cup A_5}| \overset{\text{de Morgan}}{=} |\overline{A_1} \cap \cdots \cap \overline{A_5}|$$

$$|U| + \sum_{r=1}^{5} (-1)^r \sum_{\substack{\{i_1,\ldots,i_r\} \subseteq \{1,\ldots,5\} \\ |\{i_1,\ldots,i_r\}| = r}} |A_{i_1} \cap \cdots \cap A_{i_r}| =$$

$$5! + \sum_{r=1}^{5} (-1)^r \binom{5}{r} (5-r)! =$$

$$120 - \binom{5}{1} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! =$$

$$120 - 120 + 60 - 20 + 5 - 1 = \underline{44}$$

-féleképpen.

Feladat: Hányféleképpen lehet az 52-lapos franciakártya-pakliból valakinek öt lapot kiosztani úgy, hogy az illetőnek több mint kétszer annyi ásza legyen, mint kettese? (

Feladat: Hányféleképpen lehet az 52-lapos franciakártya-pakliból valakinek öt lapot kiosztani úgy, hogy az illetőnek több mint kétszer annyi ásza legyen, mint kettese? (Az 52-lapos franciakártyában négy szín van, $\clubsuit$, $\spadesuit$, $\diamondsuit$, $\heartsuit$, és minden színből 13 érték. Sorrend nem számít.)

Feladat: Hányféleképpen lehet az 52-lapos franciakártya-pakliból valakinek öt lapot kiosztani úgy, hogy az illetőnek több mint kétszer annyi ásza legyen, mint kettese? (Az 52-lapos franciakártyában négy szín van, ♣, ♠, ♢, ♡, és minden színből 13 érték. Sorrend nem számít.)

Megoldás:

Feladat: Hányféleképpen lehet az 52-lapos franciakártya-pakliból valakinek öt lapot kiosztani úgy, hogy az illetőnek több mint kétszer annyi ásza legyen, mint kettese? (Az 52-lapos franciakártyában négy szín van, ♣, ♠, ♢, ♡, és minden színből 13 érték. Sorrend nem számít.)

Megoldás: Több esetet különböztetünk meg aszerint, hogy hány kettes (k) és hány

Feladat: Hányféleképpen lehet az 52-lapos franciakártya-pakliból valakinek öt lapot kiosztani úgy, hogy az illetőnek több mint kétszer annyi ásza legyen, mint kettese? (Az 52-lapos franciakártyában négy szín van, $\clubsuit$, $\spadesuit$, $\diamondsuit$, $\heartsuit$, és minden színből 13 érték. Sorrend nem számít.)

Megoldás: Több esetet különböztetünk meg aszerint, hogy hány kettes (k) és hány ász (a) van.

A lehetséges (k, a) típusok: $(0, 1)$, $(0, 2)$, $(0, 3)$, $(0, 4)$, $(1, 3)$, $(1, 4)$. A

A lehetséges (k, a) típusok: $(0,1)$, $(0,2)$, $(0,3)$, $(0,4)$, $(1,3)$, $(1,4)$. A (k, a) pár esetén: a ketteseket $\binom{4}{k}$ féleképpen, az ászokat $\binom{4}{a}$ féleképpen, és a további lapokat $\binom{44}{5-k-a}$-féleképpen választhatjuk ki.

A lehetséges (k, a) típusok: $(0,1)$, $(0,2)$, $(0,3)$, $(0,4)$, $(1,3)$, $(1,4)$. A (k, a) pár esetén: a ketteseket $\binom{4}{k}$ féleképpen, az ászokat $\binom{4}{a}$ féleképpen, és a további lapokat $\binom{44}{5-k-a}$-féleképpen választhatjuk ki. A szorzási szabály szerint a (k, a) típus $\binom{4}{k} \cdot \binom{4}{a} \cdot \binom{44}{5-k-a}$ esetet jelent. Az

A lehetséges (k,a) típusok: $(0,1)$, $(0,2)$, $(0,3)$, $(0,4)$, $(1,3)$, $(1,4)$. A (k,a) pár esetén: a ketteseket $\binom{4}{k}$ féleképpen, az ászokat $\binom{4}{a}$ féleképpen, és a további lapokat $\binom{44}{5-k-a}$-féleképpen választhatjuk ki. A szorzási szabály szerint a (k,a) típus $\binom{4}{k}\cdot\binom{4}{a}\cdot\binom{44}{5-k-a}$ esetet jelent. Az összegezési szabály szerint a végeredmény

$$\sum_{(k,a)\in\{(0,1),(0,2),(0,3),(0,4),(1,3),(1,4)\}} \binom{4}{k}\cdot\binom{4}{a}\cdot\binom{44}{5-k-a}$$

$$=$$

A lehetséges (k,a) típusok: $(0,1)$, $(0,2)$, $(0,3)$, $(0,4)$, $(1,3)$, $(1,4)$. A (k,a) pár esetén: a ketteseket $\binom{4}{k}$ féleképpen, az ászokat $\binom{4}{a}$ féleképpen, és a további lapokat $\binom{44}{5-k-a}$-féleképpen választhatjuk ki. A szorzási szabály szerint a (k,a) típus $\binom{4}{k}\cdot\binom{4}{a}\cdot\binom{44}{5-k-a}$ esetet jelent. Az összegezési szabály szerint a végeredmény

$$\sum_{(k,a)\in\{(0,1),(0,2),(0,3),(0,4),(1,3),(1,4)\}} \binom{4}{k}\cdot\binom{4}{a}\cdot\binom{44}{5-k-a}$$

$$= \cdots$$

A lehetséges (k,a) típusok: $(0,1)$, $(0,2)$, $(0,3)$, $(0,4)$, $(1,3)$, $(1,4)$. A (k,a) pár esetén: a ketteseket $\binom{4}{k}$ féleképpen, az ászokat $\binom{4}{a}$ féleképpen, és a további lapokat $\binom{44}{5-k-a}$-féleképpen választhatjuk ki. A szorzási szabály szerint a (k,a) típus $\binom{4}{k}\cdot\binom{4}{a}\cdot\binom{44}{5-k-a}$ esetet jelent. Az összegezési szabály szerint a végeredmény

$$\sum_{(k,a)\in\{(0,1),(0,2),(0,3),(0,4),(1,3),(1,4)\}} \binom{4}{k}\cdot\binom{4}{a}\cdot\binom{44}{5-k-a}$$

$$= \cdots = \underline{627\ 004}.$$

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben?

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Megoldás: Legyenek az oktatók A, B, C.

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Megoldás: Legyenek az oktatók A, B, C. Rakjuk az 1200 hallgatót sorba (pl. névsorba). Ekkor m

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Megoldás: Legyenek az oktatók A, B, C. Rakjuk az 1200 hallgatót sorba (pl. névsorba). Ekkor minden eset megfelel egy, az A, B, C betűkből képezhető olyan sorozatnak (azaz szónak),

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Megoldás: Legyenek az oktatók A, B, C. Rakjuk az 1200 hallgatót sorba (pl. névsorba). Ekkor minden eset megfelel egy, az A, B, C betűkből képezhető olyan sorozatnak (azaz szónak), amelyben 200 A, 320 B és 680 C betű van. Ezek száma

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Megoldás: Legyenek az oktatók A, B, C. Rakjuk az 1200 hallgatót sorba (pl. névsorba). Ekkor minden eset megfelel egy, az A, B, C betűkből képezhető olyan sorozatnak (azaz szónak), amelyben 200 A, 320 B és 680 C betű van. Ezek száma az ismétléses permutációra vonatkozó képlet szerint

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Megoldás: Legyenek az oktatók A, B, C. Rakjuk az 1200 hallgatót sorba (pl. névsorba). Ekkor minden eset megfelel egy, az A, B, C betűkből képezhető olyan sorozatnak (azaz szónak), amelyben 200 A, 320 B és 680 C betű van. Ezek száma az ismétléses permutációra vonatkozó képlet szerint

$$\frac{1200!}{200! \cdot 320! \cdot 680!}$$

Feladat: Egy minden egyetemista által szabadon választható kurzust egyidőben három oktató is tart, rendre 200, 320 és 680-férőhelyes teremben. (Ezek a számok egyúttal az ETR-ben is meg vannak létszámkorlátként adva.) A kurzus iránt pontosan $1200 = 200 + 320 + 680$ hallgató érdeklődik. Hányféleképpen vehetik fel az ETR-ben? (A sorrend nem számít, hanem csak az, hogy ki melyik oktatónál veszi fel a kurzust.)

Megoldás: Legyenek az oktatók A, B, C. Rakjuk az 1200 hallgatót sorba (pl. névsorba). Ekkor minden eset megfelel egy, az A, B, C betűkből képezhető olyan sorozatnak (azaz szónak), amelyben 200 A, 320 B és 680 C betű van. Ezek száma az ismétléses permutációra vonatkozó képlet szerint

$$\frac{1200!}{200! \cdot 320! \cdot 680!} \approx 9,53 \cdot 10^{503}.$$

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges?

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás:

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás: Elkezdeni

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás: Elkezdeni nem nehéz: mindenkinek adjunk 10 eurót, és

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás: Elkezdeni nem nehéz: mindenkinek adjunk 10 eurót, és csak a maradék 230-at kell 20 ember között elosztani.

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás: Elkezdeni nem nehéz: mindenkinek adjunk 10 eurót, és csak a maradék 230-at kell 20 ember között elosztani. **Kombinatorikai ötlettárunk gyarapítása:**

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás: Elkezdeni nem nehéz: mindenkinek adjunk 10 eurót, és csak a maradék 230-at kell 20 ember között elosztani. **Kombinatorikai ötlettárunk gyarapítása:** próbáljuk másként interpretálni a jelenséget!

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás: Elkezdeni nem nehéz: mindenkinek adjunk 10 eurót, és csak a maradék 230-at kell 20 ember között elosztani. **Kombinatorikai ötlettárunk gyarapítása:** próbáljuk másként interpretálni a jelenséget! Erre eddig is láttunk példát: nem a törpék kapták a süteményt, hanem a sütemények a törpéket, nem a kerítésléceket választottuk ki, hanem egy szó betűit permutáltuk. Most újabb példát látunk.

Feladat A TTK HÖK 430 euró jutalmat oszt ki a diákköri konferencián helyezést elért 20 hallgatónak. Mindenkinek legalább 10 eurót, és mindenkinek egész értéket. Ezen feltételek mellett hányféle pénzosztás lehetséges? (A sorrend nem számít, csak az, hogy ki mennyit kap.)

Megoldás: Elkezdeni nem nehéz: mindenkinek adjunk 10 eurót, és csak a maradék 230-at kell 20 ember között elosztani. **Kombinatorikai ötlettárunk gyarapítása:** próbáljuk másként interpretálni a jelenséget! Erre eddig is láttunk példát: nem a törpék kapták a süteményt, hanem a sütemények a törpéket, nem a kerítésléceket választottuk ki, hanem egy szó betűit permutáltuk. Most újabb példát látunk.

Legyen a húsz hallgató A, B, C, . . . (azaz rakjuk őket névsorba), és a 230 euró kiosztását a következő módon vitelezzük ki:

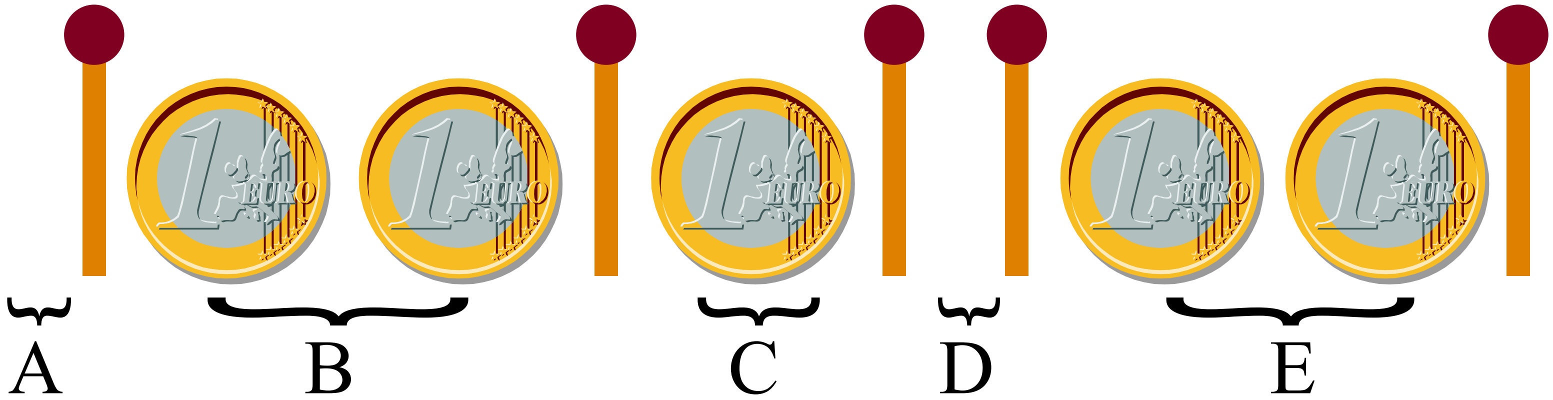
Legyen a húsz hallgató A, B, C, ... (azaz rakjuk őket névsorba), és a 230 euró kiosztását a következő módon vitelezzük ki: Vegyünk $20 - 1 = 19$ egyforma gyufaszálat és 230 egyeurós érmét.

Legyen a húsz hallgató A, B, C, ... (azaz rakjuk őket névsorba), és a 230 euró kiosztását a következő módon vitelezzük ki: Vegyünk $20 - 1 = 19$ egyforma gyufaszálat és 230 egyeurós érmét. Tetszés szerint rakjuk sorba az érméket és a gyufákat! Az ábrán — terjedelmi okból — az így kapott sornak csak az eleje látszik:

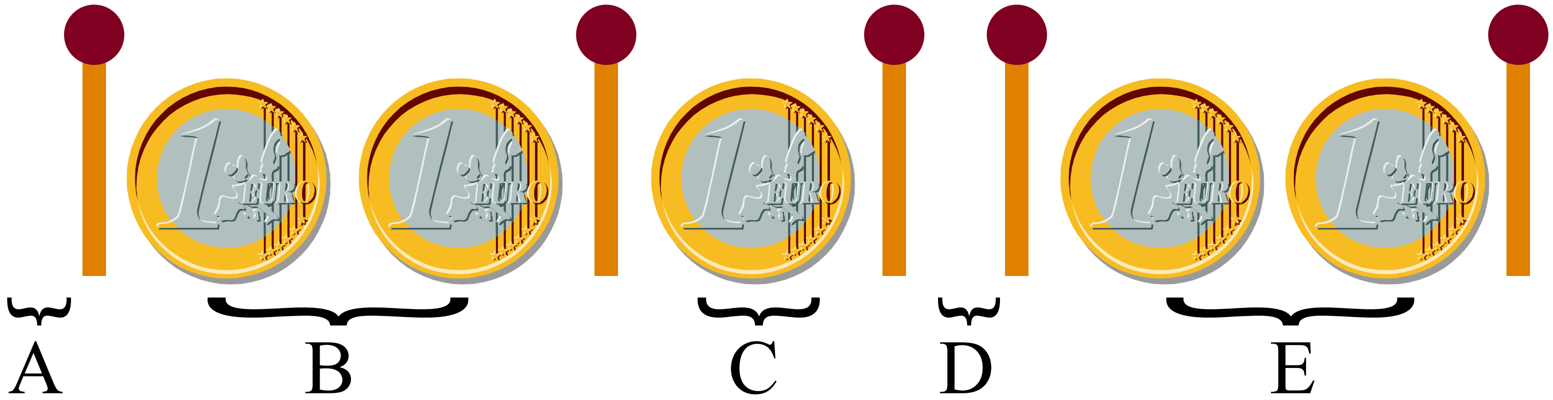
Legyen a húsz hallgató A, B, C, ... (azaz rakjuk őket névsorba), és a 230 euró kiosztását a következő módon vitelezzük ki: Vegyünk $20 - 1 = 19$ egyforma gyufaszálat és 230 egyeurós érmét. Tetszés szerint rakjuk sorba az érméket és a gyufákat! Az ábrán — terjedelmi okból — az így kapott sornak csak az eleje látszik:

Ezt követően az első gyufa előtt eurókat kapja A, az első hallgató, Ezt követően az első gyufa előtt eurókat kapja A, az első hallgató, az első és a második gyufa közötti eurókat kapja a második hallgató, Ezt követően az első gyufa előtt eurókat kapja A, az első hallgató, az első és a második gyufa közötti eurókat kapja a második hallgató, a második és harmadik gyufa közötti eurókat a harmadik hallgató, . . . , Ezt követően az első gyufa előtt eurókat kapja A, az első hallgató, az első és a második gyufa közötti eurókat kapja a második hallgató, a második és harmadik gyufa közötti eurókat a harmadik hallgató, . . . , a tizennyolcadik és tizenkilencedik gyufa közöttieket a tizenkilencedik hallgató, és végül a tizenkilencedik gyufa utániakat a huszadik hallgató.

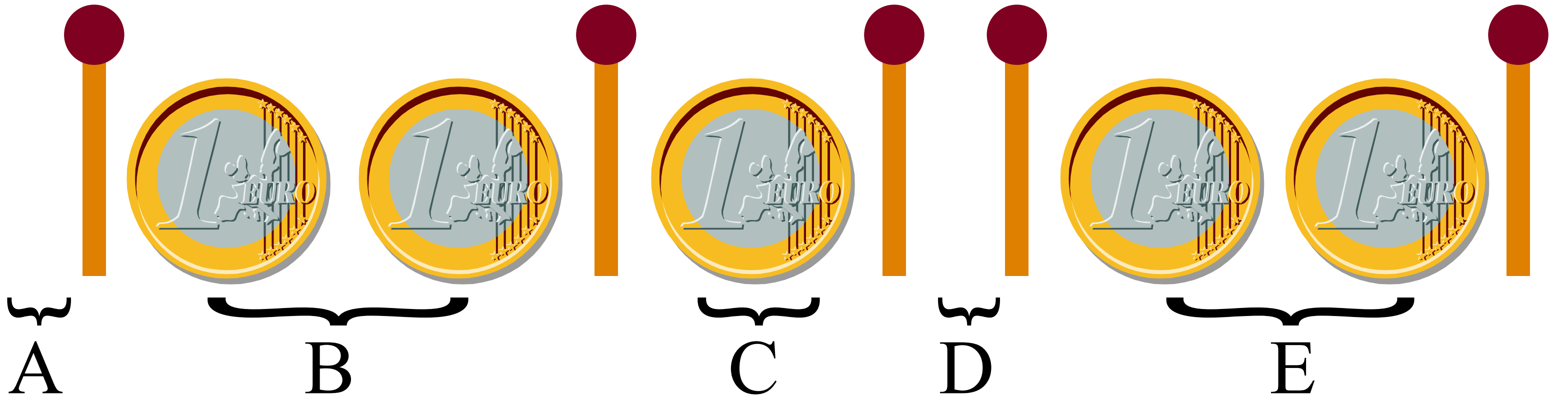
Ezt követően az első gyufa előtt eurókat kapja A, az első hallgató, az első és a második gyufa közötti eurókat kapja a második hallgató, a második és harmadik gyufa közötti eurókat a harmadik hallgató, . . . , a tizennyolcadik és tizenkilencedik gyufa közöttieket a tizenkilencedik hallgató, és végül a tizenkilencedik gyufa utániakat a huszadik hallgató. Megeshet, hogy egy-egy hallgató semmit sem kap, Ezt követően az első gyufa előtt eurókat kapja A, az első hallgató, az első és a második gyufa közötti eurókat kapja a második hallgató, a második és harmadik gyufa közötti eurókat a harmadik hallgató, . . . , a tizennyolcadik és tizenkilencedik gyufa közöttieket a tizenkilencedik hallgató, és végül a tizenkilencedik gyufa utániakat a huszadik hallgató. Megeshet, hogy egy-egy hallgató semmit sem kap, így jár az ábrán az első (A) és a negyedik (D) hallgató.



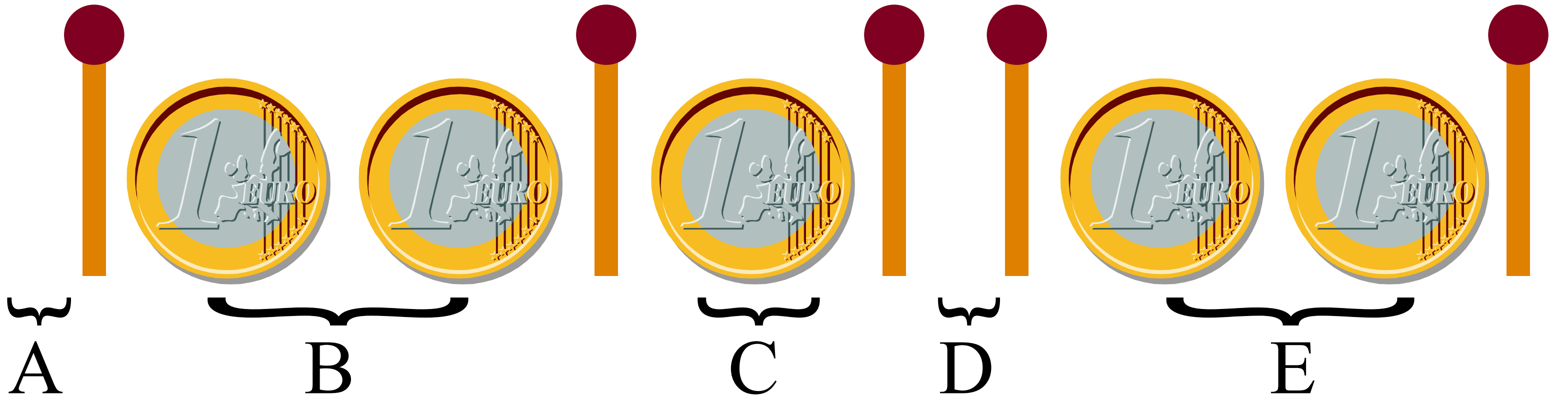
Nyilván az érmék és gyufák lerakása egyértelműen meghatározza a pénzosztást,



Nyilván az érmék és gyufák lerakása egyértelműen meghatározza a pénzosztást, minden lehetséges pénzosztás megkapható ily módon,



Nyilván az érmék és gyufák lerakása egyértelműen meghatározza a pénzosztást, minden lehetséges pénzosztás megkapható ily módon, és két különböző érme-gyufa sorrendhez különböző pénzosztás tartozik.



Nyilván az érmék és gyufák lerakása egyértelműen meghatározza a pénzosztást, minden lehetséges pénzosztás megkapható ily módon, és két különböző érme-gyufa sorrendhez különböző pénzosztás tartozik. (Másként fogalmazva: az érme-gyufa sorrendek halmaza és a pénzkiosztások halmaza között bijekció van.)

Az érme-gyufa permutációk számát az ismétléses permutációra vonatkozó képlet adja, és az egyúttal a feladat végeredménye:

$$\frac{249!}{230! \cdot 19!}$$

Az érme-gyufa permutációk számát az ismétléses permutációra vonatkozó képlet adja, és az egyúttal a feladat végeredménye:

$$\frac{249!}{230! \cdot 19!}$$

$$= 13\,701\,531\,519\,608\,330\,239\,173\,255\,924$$

Az érme-gyufa permutációk számát az ismétléses permutációra vonatkozó képlet adja, és az egyúttal a feladat végeredménye:

$$\frac{249!}{230! \cdot 19!}$$

$$= 13\ 701\ 531\ 519\ 608\ 330\ 239\ 173\ 255\ 924 \approx 1,37 \cdot 10^{28}.$$

Az érme-gyufa permutációk számát az ismétléses permutációra vonatkozó képlet adja, és az egyúttal a feladat végeredménye:

$$\frac{249!}{230! \cdot 19!}$$

$$= 13\,701\,531\,519\,608\,330\,239\,173\,255\,924 \approx 1,37 \cdot 10^{28}.$$

Megjegyzendő, hogy $\frac{249!}{230! \cdot 19!} = \binom{249}{19}$, ami

Az érme-gyufa permutációk számát az ismétléses permutációra vonatkozó képlet adja, és az egyúttal a feladat végeredménye:

$$\frac{249!}{230! \cdot 19!}$$

$$= 13\ 701\ 531\ 519\ 608\ 330\ 239\ 173\ 255\ 924 \approx 1,37 \cdot 10^{28}.$$

Megjegyzendő, hogy $\frac{249!}{230! \cdot 19!} = \binom{249}{19}$, ami annak felel meg, hogy a lehetséges permutációkat az határozza meg, hogy a 249 hely közül hányféleképpen választhatjuk ki a tizenkilenc gyufa helyét.

Feladat: Hányféleképpen húzhatunk fel nyolc különböző gyűrűt a balkezünkre, ha a hüvelykujjunkra nem kerülhet gyűrű?

Feladat: Hányféleképpen húzhatunk fel nyolc különböző gyűrűt a balkezünkre, ha a hüvelykujjunkra nem kerülhet gyűrű? Az is számít, hogy egy-egy ujjunkon milyen sorrendben vannak a gyűrűk.

Feladat: Hányféleképpen húzhatunk fel nyolc különböző gyűrűt a balkezünkre, ha a hüvelykujjunkra nem kerülhet gyűrű? Az is számít, hogy egy-egy ujjunkon milyen sorrendben vannak a gyűrűk. Feltesszük, hogy az ujjaink kb. „egyforma vastagok" (azaz, hogy bármelyik gyűrű bármelyik ujjunkra felhúzható).

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít.

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát!

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel:

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel: az első gyufa előtti gyűrűket az adott sorrendben a mutató ujjunkra húzzuk, A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel: az első gyufa előtti gyűrűket az adott sorrendben a mutató ujjunkra húzzuk, az első és második gyufa közöttieket (az adott sorrendben) a középső ujjunkra, A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel: az első gyufa előtti gyűrűket az adott sorrendben a mutató ujjunkra húzzuk, az első és második gyufa közöttieket (az adott sorrendben) a középső ujjunkra, a második és harmadik gyufa közöttieket a gyűrűsujjunkra, A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel: az első gyufa előtti gyűrűket az adott sorrendben a mutató ujjunkra húzzuk, az első és második gyufa közöttieket (az adott sorrendben) a középső ujjunkra, a második és harmadik gyufa közöttieket a gyűrűsujjunkra, és végül a harmadik gyufa utániakat a kisujjunkra.

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel: az első gyufa előtti gyűrűket az adott sorrendben a mutató ujjunkra húzzuk, az első és második gyufa közöttieket (az adott sorrendben) a középső ujjunkra, a második és harmadik gyufa közöttieket a gyűrűsujjunkra, és végül a harmadik gyufa utániakat a kisujjunkra. Az ismétléses permutációkra vonatkozó képlet szerint a végeredmény:

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel: az első gyufa előtti gyűrűket az adott sorrendben a mutató ujjunkra húzzuk, az első és második gyufa közöttieket (az adott sorrendben) a középső ujjunkra, a második és harmadik gyufa közöttieket a gyűrűsujjunkra, és végül a harmadik gyufa utániakat a kisujjunkra. Az ismétléses permutációkra vonatkozó képlet szerint a végeredmény:

$$\frac{11!}{3!} =$$

A feladat hasonlít a pénzosztási feladatra, de itt most a sorrend számít. Vegyünk három egyforma gyufát! A nyolc különböző gyűrű és a három egyforma gyufa permutációi lényegében azonosak a gyűrűelhelyezésekkel: az első gyufa előtti gyűrűket az adott sorrendben a mutató ujjunkra húzzuk, az első és második gyufa közöttieket (az adott sorrendben) a középső ujjunkra, a második és harmadik gyufa közöttieket a gyűrűsujjunkra, és végül a harmadik gyufa utániakat a kisujjunkra. Az ismétléses permutációkra vonatkozó képlet szerint a végeredmény:

$$\frac{11!}{3!} = 6\,652\,800.$$

Feladat: Újabb gyűrűket vettünk, és immár tizenöt különböző gyűrűnk van. Ezért azt a kikötést tesszük, hogy a balkezünk mind a négy ujjára legalább kettő gyűrű jusson. Ekkor hányféleképpen húzhatjuk fel a tizenöt gyűrűt a balkezünk négy ujjára?

Feladat: Újabb gyűrűket vettünk, és immár tizenöt különböző gyűrűnk van. Ezért azt a kikötést tesszük, hogy a balkezünk mind a négy ujjára legalább kettő gyűrű jusson. Ekkor hányféleképpen húzhatjuk fel a tizenöt gyűrűt a balkezünk négy ujjára?

Megoldás:

Feladat: Újabb gyűrűket vettünk, és immár tizenöt különböző gyűrűnk van. Ezért azt a kikötést tesszük, hogy a balkezünk mind a négy ujjára legalább kettő gyűrű jusson. Ekkor hányféleképpen húzhatjuk fel a tizenöt gyűrűt a balkezünk négy ujjára?

Megoldás: A legalsó (azaz a csuklónkhoz legközelebbi) nyolc (tehát ujjanként kettő) gyűrűt

Feladat: Újabb gyűrűket vettünk, és immár tizenöt különböző gyűrűnk van. Ezért azt a kikötést tesszük, hogy a balkezünk mind a négy ujjára legalább kettő gyűrű jusson. Ekkor hányféleképpen húzhatjuk fel a tizenöt gyűrűt a balkezünk négy ujjára?

Megoldás: A legalsó (azaz a csuklónkhoz legközelebbi) nyolc (tehát ujjanként kettő) gyűrűt (ismétlés nélküli variáció) hányféleképpen választhatjuk ki?

Feladat: Újabb gyűrűket vettünk, és immár tizenöt különböző gyűrűnk van. Ezért azt a kikötést tesszük, hogy a balkezünk mind a négy ujjára legalább kettő gyűrű jusson. Ekkor hányféleképpen húzhatjuk fel a tizenöt gyűrűt a balkezünk négy ujjára?

Megoldás: A legalsó (azaz a csuklónkhoz legközelebbi) nyolc (tehát ujjanként kettő) gyűrűt (ismétlés nélküli variáció) hányféleképpen választhatjuk ki?

A mutatóujj legalsó gyűrűjét 15-féleképpen,

Feladat: Újabb gyűrűket vettünk, és immár tizenöt különböző gyűrűnk van. Ezért azt a kikötést tesszük, hogy a balkezünk mind a négy ujjára legalább kettő gyűrű jusson. Ekkor hányféleképpen húzhatjuk fel a tizenöt gyűrűt a balkezünk négy ujjára?

Megoldás: A legalsó (azaz a csuklónkhoz legközelebbi) nyolc (tehát ujjanként kettő) gyűrűt (ismétlés nélküli variáció) hányféleképpen választhatjuk ki?

A mutatóujj legalsó gyűrűjét 15-féleképpen, a mutatóujj második gyűrűjét 14-féleképpen, a középső ujj legalsó gyűrűjét 13-féleképpen, stb.,

Feladat: Újabb gyűrűket vettünk, és immár tizenöt különböző gyűrűnk van. Ezért azt a kikötést tesszük, hogy a balkezünk mind a négy ujjára legalább kettő gyűrű jusson. Ekkor hányféleképpen húzhatjuk fel a tizenöt gyűrűt a balkezünk négy ujjára?

Megoldás: A legalsó (azaz a csuklónkhoz legközelebbi) nyolc (tehát ujjanként kettő) gyűrűt (ismétlés nélküli variáció) hányféleképpen választhatjuk ki?

A mutatóujj legalsó gyűrűjét 15-féleképpen, a mutatóujj második gyűrűjét 14-féleképpen, a középső ujj legalsó gyűrűjét 13-féleképpen, stb., tehát a szorzási szabály szerint összesen $15 \cdot 14 \cdot \dots \cdot 8 = \frac{15!}{7!}$-féleképpen.

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa)

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük.

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

$$\frac{15!}{7!} \cdot \frac{10!}{3!} =$$

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

$$\frac{15!}{7!} \cdot \frac{10!}{3!} = 156\ 920\ 924\ 160\ 000.$$

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

$$\frac{15!}{7!} \cdot \frac{10!}{3!} = 156\,920\,924\,160\,000.$$

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

$$\frac{15!}{7!} \cdot \frac{10!}{3!} = 156\ 920\ 924\ 160\ 000.$$

Megjegyzés:

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

$$\frac{15!}{7!} \cdot \frac{10!}{3!} = 156\ 920\ 924\ 160\ 000.$$

Megjegyzés: Érdekes, hogy az eredmény éppen $15! \cdot \binom{10}{3}$. Vajon mi lehet ennek az oka?

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

$$\frac{15!}{7!} \cdot \frac{10!}{3!} = 156\ 920\ 924\ 160\ 000.$$

Megjegyzés: Érdekes, hogy az eredmény éppen $15! \cdot \binom{10}{3}$. Vajon mi lehet ennek az oka? Van talán egy másik gondolatmenet, amelyből éppen ez adódik?

Bárhogy is választottuk ki a legalsó nyolc gyűrűt, a maradék hét gyűrűt már minden további megkötés nélkül húzhatjuk föl, ezt az előző feladat mintájára (hét különböző gyűrű és három egyforma gyufa) $\frac{10!}{3!}$-féleképpen tehetjük. A szorzási szabály szerint a végeredmény:

$$\frac{15!}{7!} \cdot \frac{10!}{3!} = 156\,920\,924\,160\,000.$$

Megjegyzés: Érdekes, hogy az eredmény éppen $15! \cdot \binom{10}{3}$. Vajon mi lehet ennek az oka? Van talán egy másik gondolatmenet, amelyből éppen ez adódik? **Igen!** Erre a következő feladat megoldása után adunk választ.

Feladat: Hányféleképpen lehet az $n \in \mathbf{N}$ számot $k \in \mathbf{N}$ darab nemnegatív egész szám összegére bontani, ha az összeg tagjainak sorrendje is számít?

Feladat: Hányféleképpen lehet az $n \in \mathbf{N}$ számot $k \in \mathbf{N}$ darab nemnegatív egész szám összegére bontani, ha az összeg tagjainak sorrendje is számít?

Megoldás:

Megoldás: Minden ilyen összeg,

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$,

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1)$$

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) +$$

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1)$$

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)$$

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) +$$

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + ()$$

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)$$

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + () + (1 + 1 + 1 + 1) + \cdots,$$

ahol az () üres összeg a nullát jelöli.

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + () + (1 + 1 + 1 + 1) + \cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + () + (1 + 1 + 1 + 1) + \cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

111

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + () + (1 + 1 + 1 + 1) + \cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111 + 11$$

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111+11+1$$

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111+11+1+$$

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111+11+1+\ +1111+\ldots\ .$$

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111+11+1+\ +1111+\ldots\ .$$

Ez egy

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + () + (1 + 1 + 1 + 1) + \cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111 + 11 + 1 + \ + 1111 + \ldots\ .$$

Ez egy n darab 1-ből és $k - 1$

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111+11+1+\ +1111+\ldots\ .$$

Ez egy n darab 1-ből és $k-1$ darab $+$ jelből álló, $n+k-1$-elemű sorozat.

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + () + (1 + 1 + 1 + 1) + \cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111 + 11 + 1 + \; + 1111 + \ldots \; .$$

Ez egy n darab 1-ből és $k-1$ darab $+$ jelből álló, $n+k-1$-elemű sorozat. Az összegek keresett száma éppen az ilyen sorozatok száma, amelyet kétféleképpen is megkaphatunk:

Megoldás: Minden ilyen összeg, pl. a $3 + 2 + 1 + 0 + 4 + \cdots$, felfogható így is:

$$(1 + 1 + 1) + (1 + 1) + (1) + () + (1 + 1 + 1 + 1) + \cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111 + 11 + 1 + \ + 1111 + \ldots \ .$$

Ez egy n darab 1-ből és $k-1$ darab + jelből álló, $n+k-1$-elemű sorozat. Az összegek keresett száma éppen az ilyen sorozatok száma, amelyet kétféleképpen is megkaphatunk: ismétléses permutációk számaként,

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111+11+1+\ +1111+\ldots\ .$$

Ez egy n darab 1-ből és $k-1$ darab $+$ jelből álló, $n+k-1$-elemű sorozat. Az összegek keresett száma éppen az ilyen sorozatok száma, amelyet kétféleképpen is megkaphatunk: ismétléses permutációk számaként, illetve $n+k-1$ hely közül $(k-1)$-et a $+$ jeleknek kiválasztva.

Megoldás: Minden ilyen összeg, pl. a $3+2+1+0+4+\cdots$, felfogható így is:

$$(1+1+1)+(1+1)+(1)+()+(1+1+1+1)+\cdots,$$

ahol az () üres összeg a nullát jelöli. Ha megállapodunk abban, hogy a zárójelen belüli összeadást egymás mellé írással jelöljük és a zárójeleket elhagyjuk, akkor a fenti összeg ilyen alakú lesz:

$$111+11+1+\ +1111+\ldots\ .$$

Ez egy n darab 1-ből és $k-1$ darab $+$ jelből álló, $n+k-1$-elemű sorozat. Az összegek keresett száma éppen az ilyen sorozatok száma, amelyet kétféleképpen is megkaphatunk: ismétléses permutációk számaként, illetve $n+k-1$ hely közül $(k-1)$-et a $+$ jeleknek kiválasztva. Tehát a végeredmény:

$$\frac{(n+k-1)!}{n!\cdot(k-1)!} =$$

$$\frac{(n+k-1)!}{n! \cdot (k-1)!} = \binom{n+k-1}{k-1}.$$

A 15 gyűrűs feladatra visszatérve:

$$\frac{(n+k-1)!}{n! \cdot (k-1)!} = \binom{n+k-1}{k-1}.$$

A 15 gyűrűs feladatra visszatérve: hányféleképpen lehet a tizenötöt négy egynél nagyobb egész szám összegére bontani, ha a tagok sorrendje is számít?

$$\frac{(n+k-1)!}{n!\cdot(k-1)!}=\binom{n+k-1}{k-1}.$$

A 15 gyűrűs feladatra visszatérve: hányféleképpen lehet a tizenötöt négy egynél nagyobb egész szám összegére bontani, ha a tagok sorrendje is számít? Nyilván annyiféleképpen, ahányféleképpen a $15-8=7$-et négy nemegatív egész szám összegére,

$$\frac{(n+k-1)!}{n!\cdot(k-1)!}=\binom{n+k-1}{k-1}.$$

A 15 gyűrűs feladatra visszatérve: hányféleképpen lehet a tizenötöt négy egynél nagyobb egész szám összegére bontani, ha a tagok sorrendje is számít? Nyilván annyiféleképpen, ahányféleképpen a $15-8=7$-et négy nemegatív egész szám összegére, hiszen az utóbbi összeg tagjaihoz kettőt hozzáadva az előbbi összeget kapjuk.

$$\frac{(n+k-1)!}{n!\cdot(k-1)!}=\binom{n+k-1}{k-1}.$$

A 15 gyűrűs feladatra visszatérve: hányféleképpen lehet a tizenötöt négy egynél nagyobb egész szám összegére bontani, ha a tagok sorrendje is számít? Nyilván annyiféleképpen, ahányféleképpen a $15-8=7$-et négy nemegatív egész szám összegére, hiszen az utóbbi összeg tagjaihoz kettőt hozzáadva az előbbi összeget kapjuk. Tehát, a most megoldott feladat szerint,

$$\frac{(n+k-1)!}{n!\cdot(k-1)!}=\binom{n+k-1}{k-1}.$$

A 15 gyűrűs feladatra visszatérve: hányféleképpen lehet a tizenötöt négy egynél nagyobb egész szám összegére bontani, ha a tagok sorrendje is számít? Nyilván annyiféleképpen, ahányféleképpen a $15-8=7$-et négy nemegatív egész szám összegére, hiszen az utóbbi összeg tagjaihoz kettőt hozzáadva az előbbi összeget kapjuk. Tehát, a most megoldott feladat szerint, $\binom{7+4-1}{4-1}$

$$\frac{(n+k-1)!}{n!\cdot(k-1)!}=\binom{n+k-1}{k-1}.$$

A 15 gyűrűs feladatra visszatérve: hányféleképpen lehet a tizenötöt négy egynél nagyobb egész szám összegére bontani, ha a tagok sorrendje is számít? Nyilván annyiféleképpen, ahányféleképpen a $15-8=7$-et négy nemegatív egész szám összegére, hiszen az utóbbi összeg tagjaihoz kettőt hozzáadva az előbbi összeget kapjuk. Tehát, a most megoldott feladat szerint, $\binom{7+4-1}{4-1}=\binom{10}{3}$-féleképpen.

Mármost rakjuk sorba a gyűrűket:

Mármost rakjuk sorba a gyűrűket: 15!.

Ármost rakjuk sorba a gyűrűket: 15!. Minden ilyen sorrend esetén bontsuk fel a tizenötöt négy darab egynél nagyobb egész szám összegére:

Mármost rakjuk sorba a gyűrűket: 15!. Minden ilyen sorrend esetén bontsuk fel a tizenötöt négy darab egynél nagyobb egész szám összegére: ezt $\binom{10}{3}$-féleképpen tehetjük.

Mármost rakjuk sorba a gyűrűket: $15!$. Minden ilyen sorrend esetén bontsuk fel a tizenötöt négy darab egynél nagyobb egész szám összegére: ezt $\binom{10}{3}$-féleképpen tehetjük. A szorzási szabály szerint eddig $15! \cdot \binom{10}{3}$-féleképpen járhattunk el.

Mármost rakjuk sorba a gyűrűket: $15!$. Minden ilyen sorrend esetén bontsuk fel a tizenötöt négy darab egynél nagyobb egész szám összegére: ezt $\binom{10}{3}$-féleképpen tehetjük. A szorzási szabály szerint eddig $15! \cdot \binom{10}{3}$-féleképpen járhattunk el. Az eddigiek viszont egyértelműen meghatározzák a gyűrűviselést:

Ármost rakjuk sorba a gyűrűket: 15!. Minden ilyen sorrend esetén bontsuk fel a tizenötöt négy darab egynél nagyobb egész szám összegére: ezt $\binom{10}{3}$-féleképpen tehetjük. A szorzási szabály szerint eddig $15! \cdot \binom{10}{3}$-féleképpen járhattunk el. Az eddigiek viszont egyértelműen meghatározzák a gyűrűviselést: ahogy a gyűrűk jönnek sorba, az összeg

Mármost rakjuk sorba a gyűrűket: $15!$. Minden ilyen sorrend esetén bontsuk fel a tizenötöt négy darab egynél nagyobb egész szám összegére: ezt $\binom{10}{3}$-féleképpen tehetjük. A szorzási szabály szerint eddig $15! \cdot \binom{10}{3}$-féleképpen járhattunk el. Az eddigiek viszont egyértelműen meghatározzák a gyűrűviselést: ahogy a gyűrűk jönnek sorba, az összeg első tagjával egyenlő darabot húzunk a mutatóujjunkra, az összeg második tagjával egyenlő darabot, a középső ujjunkra, stb.

Ármost rakjuk sorba a gyűrűket: 15!. Minden ilyen sorrend esetén bontsuk fel a tizenötöt négy darab egynél nagyobb egész szám összegére: ezt $\binom{10}{3}$-féleképpen tehetjük. A szorzási szabály szerint eddig $15! \cdot \binom{10}{3}$-féleképpen járhattunk el. Az eddigiek viszont egyértelműen meghatározzák a gyűrűviselést: ahogy a gyűrűk jönnek sorba, az összeg első tagjával egyenlő darabot húzunk a mutatóujjunkra, az összeg második tagjával egyenlő darabot, a középső ujjunkra, stb. Ezzel kombinatorikai magyarázatot — és egyúttal más megoldást — adtunk arra, hogy miért $15! \cdot \binom{10}{3}$ a végeredmény.

Feladat: Csoportterápia céljából egy pszichológus a száznegyven páciensét két harmincfős, három húszfős és két tízfős csoportba osztja be. Hányféleképpen teheti ezt, ha az azonos létszámú csoportok között nem tesz különbséget (azaz ugyanazt a programot valósítja meg)?

Feladat: Csoportterápia céljából egy pszichológus a száznegyven páciensét két harmincfős, három húszfős és két tízfős csoportba osztja be. Hányféleképpen teheti ezt, ha az azonos létszámú csoportok között nem tesz különbséget (azaz ugyanazt a programot valósítja meg)? Tehát a csoportokon belül a sorrend nem számít.

Feladat: Csoportterápia céljából egy pszichológus a száznegyven páciensét két harmincfős, három húszfős és két tízfős csoportba osztja be. Hányféleképpen teheti ezt, ha az azonos létszámú csoportok között nem tesz különbséget (azaz ugyanazt a programot valósítja meg)? Tehát a csoportokon belül a sorrend nem számít. Két beosztást akkor tekintünk azonosnak, ha mindenkinek pontosan ugyanazok a csoporttársai.

Megoldás

Megoldás Az biztos számít, hogy ki az a hatvan ember, aki harmincfős csoportba kerül.

Megoldás Az biztos számít, hogy ki az a hatvan ember, aki harmincfős csoportba kerül. Ezeket $\binom{140}{60}$ féleképpen választhatjuk ki.

Megoldás Az biztos számít, hogy ki az a hatvan ember, aki harmincfős csoportba kerül. Ezeket $\binom{140}{60}$ féleképpen választhatjuk ki.

Legyen X a kiválasztottak egyike.

Megoldás Az biztos számít, hogy ki az a hatvan ember, aki harmincfős csoportba kerül. Ezeket $\binom{140}{60}$ féleképpen választhatjuk ki.

Legyen X a kiválasztottak egyike. Az eddigi 60 fő felosztását az határozza meg, hogy ki az a 29 fő a további 59-ből, aki X-szel egy csoportba kerül,

Megoldás Az biztos számít, hogy ki az a hatvan ember, aki harmincfős csoportba kerül. Ezeket $\binom{140}{60}$ féleképpen választhatjuk ki.

Legyen X a kiválasztottak egyike. Az eddigi 60 fő felosztását az határozza meg, hogy ki az a 29 fő a további 59-ből, aki X-szel egy csoportba kerül, tehát ez $\binom{59}{29}$ lehetőség.

Megoldás Az biztos számít, hogy ki az a hatvan ember, aki harmincfős csoportba kerül. Ezeket $\binom{140}{60}$ féleképpen választhatjuk ki.

Legyen X a kiválasztottak egyike. Az eddigi 60 fő felosztását az határozza meg, hogy ki az a 29 fő a további 59-ből, aki X-szel egy csoportba kerül, tehát ez $\binom{59}{29}$ lehetőség. Tehát —

Megoldás Az biztos számít, hogy ki az a hatvan ember, aki harmincfős csoportba kerül. Ezeket $\binom{140}{60}$ féleképpen választhatjuk ki.

Legyen X a kiválasztottak egyike. Az eddigi 60 fő felosztását az határozza meg, hogy ki az a 29 fő a további 59-ből, aki X-szel egy csoportba kerül, tehát ez $\binom{59}{29}$ lehetőség. Tehát — a szorzási szabály szerint — a harmincfős csoportokat

$$\binom{140}{60} \cdot \binom{59}{29}$$

féleképpen jelölhetjük ki.

Az eddigiekhez teljesen hasonlóan, a maradék 80 emberből a tízfős csoportokba kerülőket

Az eddigiekhez teljesen hasonlóan, a maradék 80 emberből a tízfős csoportokba kerülőket $\binom{80}{20}$-féleképpen választhatjuk ki, majd a kiválasztottakat $\binom{19}{9}$-féleképpen oszthatjuk két tízfős csoportba.

Az eddigiekhez teljesen hasonlóan, a maradék 80 emberből a tízfős csoportokba kerülőket $\binom{80}{20}$-féleképpen választhatjuk ki, majd a kiválasztottakat $\binom{19}{9}$-féleképpen oszthatjuk két tízfős csoportba. Ezért a harmincfős és a tízfős csoportok kialakítása — a szorzási szabály szerint —

Az eddigiekhez teljesen hasonlóan, a maradék 80 emberből a tízfős csoportokba kerülőket $\binom{80}{20}$-féleképpen választhatjuk ki, majd a kiválasztottakat $\binom{19}{9}$-féleképpen oszthatjuk két tízfős csoportba. Ezért a harmincfős és a tízfős csoportok kialakítása — a szorzási szabály szerint —

$$\binom{140}{60} \cdot \binom{59}{29} \cdot \binom{80}{20} \cdot \binom{19}{9}$$

féleképpen történhet.

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg.

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az ő csoporttársait $\binom{59}{19}$-féleképpen választhatjuk ki.

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az ő csoporttársait $\binom{59}{19}$-féleképpen választhatjuk ki. (Az biztos „számít, hogy kik az Y csoporttársai" — ha két csoportokra bontás esetén Y-nak nem ugyanazok a csoporttársai, akkor az a két csoportfelbontás különböző a mi szempontunkból.)

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az ő csoporttársait $\binom{59}{19}$-féleképpen választhatjuk ki. (Az biztos „számít, hogy kik az Y csoporttársai” — ha két csoportokra bontás esetén Y-nak nem ugyanazok a csoporttársai, akkor az a két csoportfelbontás különböző a mi szempontunkból.) Miután Y csoportját kialakítottuk, legyen Z egy rögzített személy a maradék negyvenből.

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az ő csoporttársait $\binom{59}{19}$-féleképpen választhatjuk ki. (Az biztos „számít, hogy kik az Y csoporttársai" — ha két csoportokra bontás esetén Y-nak nem ugyanazok a csoporttársai, akkor az a két csoportfelbontás különböző a mi szempontunkból.) Miután Y csoportját kialakítottuk, legyen Z egy rögzített személy a maradék negyvenből. Z csoporttársait $\binom{39}{19}$-féleképpen választhatjuk ki —

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az ő csoporttársait $\binom{59}{19}$-féleképpen választhatjuk ki. (Az biztos „számít, hogy kik az Y csoporttársai" — ha két csoportokra bontás esetén Y-nak nem ugyanazok a csoporttársai, akkor az a két csoportfelbontás különböző a mi szempontunkból.) Miután Y csoportját kialakítottuk, legyen Z egy rögzített személy a maradék negyvenből. Z csoporttársait $\binom{39}{19}$-féleképpen választhatjuk ki — és ez is biztos „számít".

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az ő csoporttársait $\binom{59}{19}$-féleképpen választhatjuk ki. (Az biztos „számít, hogy kik az Y csoporttársai" — ha két csoportokra bontás esetén Y-nak nem ugyanazok a csoporttársai, akkor az a két csoportfelbontás különböző a mi szempontunkból.) Miután Y csoportját kialakítottuk, legyen Z egy rögzített személy a maradék negyvenből. Z csoporttársait $\binom{39}{19}$-féleképpen választhatjuk ki — és ez is biztos „számít". A maradék húsz emberrel nincs dolgunk, azok egy csoportot alkotnak.

Most már csak az a kérdés, hogy a maradék hatvan embert hogyan lehet három húszfős csoportra osztani, ha az egyes csoportokat nem különböztetjük meg. Legyen Y az egyik személy, az ő csoporttársait $\binom{59}{19}$-féleképpen választhatjuk ki. (Az biztos „számít, hogy kik az Y csoporttársai" — ha két csoportokra bontás esetén Y-nak nem ugyanazok a csoporttársai, akkor az a két csoportfelbontás különböző a mi szempontunkból.) Miután Y csoportját kialakítottuk, legyen Z egy rögzített személy a maradék negyvenből. Z csoporttársait $\binom{39}{19}$-féleképpen választhatjuk ki — és ez is biztos „számít". A maradék húsz emberrel nincs dolgunk, azok egy csoportot alkotnak. A szorzási szabály szerint a húszfős csoportok kialakítása $\binom{59}{19} \cdot \binom{39}{19}$-féleképpen történhet.

A szorzási szabály szerint a végeredmény:

$$\binom{140}{60} \cdot \binom{59}{29} \cdot \binom{80}{20} \cdot \binom{19}{9} \cdot \binom{59}{19} \cdot \binom{39}{19}$$

A szorzási szabály szerint a végeredmény:

$$\binom{140}{60} \cdot \binom{59}{29} \cdot \binom{80}{20} \cdot \binom{19}{9} \cdot \binom{59}{19} \cdot \binom{39}{19} =$$

A szorzási szabály szerint a végeredmény:

$$\binom{140}{60} \cdot \binom{59}{29} \cdot \binom{80}{20} \cdot \binom{19}{9} \cdot \binom{59}{19} \cdot \binom{39}{19} =$$

$$4204154626348497299650185178370476444241178782532788411750571767581048083488851804239549505213372932864 0000$$

A szorzási szabály szerint a végeredmény:

$$\binom{140}{60}\cdot\binom{59}{29}\cdot\binom{80}{20}\cdot\binom{19}{9}\cdot\binom{59}{19}\cdot\binom{39}{19} =$$

$$4204154626348497299650185178370476444241178782532788411750571767581048083488851804239549505213372932864000$$
$$\approx 4,204\cdot 10^{106}\,.$$

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az ö

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az öszegezési szabály szerint aszerint különböztetünk meg eseteket, hogy a három **európai** (azaz nem Ford) autó szétosztása milyen.

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az öszegezési szabály szerint aszerint különböztetünk meg eseteket, hogy a három **európai** (azaz nem Ford) autó szétosztása milyen.

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az öszegezési szabály szerint aszerint különböztetünk meg eseteket, hogy a három **európai** (azaz nem Ford) autó szétosztása milyen.

3-as típus: egy minisztérium kapja mind a hármat:

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az öszegezési szabály szerint aszerint különböztetünk meg eseteket, hogy a három **európai** (azaz nem Ford) autó szétosztása milyen.

3-as típus: egy minisztérium kapja mind a hármat: ez

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az öszegezési szabály szerint aszerint különböztetünk meg eseteket, hogy a három **európai** (azaz nem Ford) autó szétosztása milyen.

3-as típus: egy minisztérium kapja mind a hármat: ez 5 eset (

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az öszegezési szabály szerint aszerint különböztetünk meg eseteket, hogy a három **európai** (azaz nem Ford) autó szétosztása milyen.

3-as típus: egy minisztérium kapja mind a hármat: ez 5 eset (hiszen ennyiféleképpen választhatjuk ki azt az egy minisztériumot, és

Feladat: Hányféleképpen lehet tizenhét egyforma Ford, egy Renault, egy Skoda és egy Opel személygépkocsit öt minisztérium között szétosztani úgy, hogy az öt közül mindegyik minisztérium négy gépkocsit kapjon? A sorrend nem számít: a személygépkocsik egyidőben kerülnek átadásra.

Megoldás: Az öszegezési szabály szerint aszerint különböztetünk meg eseteket, hogy a három **európai** (azaz nem Ford) autó szétosztása milyen.

3-as típus: egy minisztérium kapja mind a hármat: ez 5 eset (hiszen ennyiféleképpen választhatjuk ki azt az egy minisztériumot, és annak kiválasztása már meghatározza az elosztást).

$2 + 1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap:

$2+1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap: A két európait kapó minisztérium kiválasztható ötféleképpen,

$2+1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap: A két európait kapó minisztérium kiválasztható ötféleképpen, ezt követően az egyet kapó 4-féleképpen.

$2+1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap: A két európait kapó minisztérium kiválasztható ötféleképpen, ezt követően az egyet kapó 4-féleképpen. Már csak az a kérdés, hányféleképpen választhatjuk ki azt az európai autót, amelyet az egy ilyet kapó minisztériumnak szánunk:

$2+1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap: A két európait kapó minisztérium kiválasztható ötféleképpen, ezt követően az egyet kapó 4-féleképpen. Már csak az a kérdés, hányféleképpen választhatjuk ki azt az európai autót, amelyet az egy ilyet kapó minisztériumnak szánunk: 3-féleképpen. Ez $5 \cdot 4 \cdot 3 = 60$ eset.

$2+1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap: A két európait kapó minisztérium kiválasztható ötféleképpen, ezt követően az egyet kapó 4-féleképpen. Már csak az a kérdés, hányféleképpen választhatjuk ki azt az európai autót, amelyet az egy ilyet kapó minisztériumnak szánunk: 3-féleképpen. Ez $5 \cdot 4 \cdot 3 = 60$ eset.

$1+1+1$ típus: a három európai autó három különböző minisztériumhoz kerül. A Renault 5 helyre, a Skoda már csak 4 helyre, az Opel pedig 3 helyre adható, ez összesen $5 \cdot 4 \cdot 3 = 60$ eset.

$2+1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap: A két európait kapó minisztérium kiválasztható ötféleképpen, ezt követően az egyet kapó 4-féleképpen. Már csak az a kérdés, hányféleképpen választhatjuk ki azt az európai autót, amelyet az egy ilyet kapó minisztériumnak szánunk: 3-féleképpen. Ez $5 \cdot 4 \cdot 3 = 60$ eset.

$1+1+1$ típus: a három európai autó három különböző minisztériumhoz kerül. A Renault 5 helyre, a Skoda már csak 4 helyre, az Opel pedig 3 helyre adható, ez összesen $5 \cdot 4 \cdot 3 = 60$ eset.

A végeredmény a fenti részeredmények összege:

$$5 + 60 + 60 =$$

$2+1$ típus: az egyik minisztérium kettőt, egy másik pedig egyet kap: A két európait kapó minisztérium kiválasztható ötféleképpen, ezt követően az egyet kapó 4-féleképpen. Már csak az a kérdés, hányféleképpen választhatjuk ki azt az európai autót, amelyet az egy ilyet kapó minisztériumnak szánunk: 3-féleképpen. Ez $5 \cdot 4 \cdot 3 = 60$ eset.

$1+1+1$ típus: a három európai autó három különböző minisztériumhoz kerül. A Renault 5 helyre, a Skoda már csak 4 helyre, az Opel pedig 3 helyre adható, ez összesen $5 \cdot 4 \cdot 3 = 60$ eset.

A végeredmény a fenti részeredmények összege:

$$5 + 60 + 60 = 125.$$

Számelméle

Számelmélet

Számelmélet

„Kellett nekem számelmélet,

Számelmélet

„Kellett nekem számelmélet,

minden jó komám elszéledt.”

Számelmélet

„Kellett nekem számelmélet,

minden jó komám elszéledt.”

—

Számelmélet

„Kellett nekem számelmélet,

minden jó komám elszéledt.”

—— Ez a mottó most nem érvényes, hiszen csupa fontos és érdekes dologgal fogunk foglalkozni.

Definíció:

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval,

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak,

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $a \mid b$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $\boxed{a \mid b}$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$,

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $\boxed{a \mid b}$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $a \mid b$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re $1 \mid x$,

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $a \mid b$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re $1 \mid x$, $x \mid x$

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $\boxed{a \mid b}$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re $1 \mid x$, $x \mid x$ és $x \mid 0$, ha $0 \mid x$ akkor $x = 0$. De pl. $7 \nmid 20$.

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $a \mid b$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re $1 \mid x$, $x \mid x$ és $x \mid 0$, ha $0 \mid x$ akkor $x = 0$. De pl. $7 \nmid 20$.

Mivel $x \mid y \iff |x| \mid |y|$, a továbbiakban gyakran csak $\mathbf{N}_0$-ra szorítkozunk.

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $\boxed{a \mid b}$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re $1 \mid x$, $x \mid x$ és $x \mid 0$, ha $0 \mid x$ akkor $x = 0$. De pl. $7 \nmid 20$.

Mivel $x \mid y \iff |x| \mid |y|$, a továbbiakban gyakran csak $\mathbf{N}_0$-ra szorítkozunk. Ez esetben $a \mid b \iff (\exists c \in \mathbf{N}_0)(ac = b)$,

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $\boxed{a \mid b}$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re $1 \mid x$, $x \mid x$ és $x \mid 0$, ha $0 \mid x$ akkor $x = 0$. De pl. $7 \nmid 20$.

Mivel $x \mid y \iff |x| \mid |y|$, a továbbiakban gyakran csak $\mathbf{N}_0$-ra szorítkozunk. Ez esetben $a \mid b \iff (\exists c \in \mathbf{N}_0)(ac = b)$, de itt nyilván $c \in \mathbf{Z}$ -t is írhatnánk,

Definíció: Legyen $a, b \in \mathbf{Z}$. Akkor mondjuk, hogy a **osztja** b-t, más szóval, b **osztható** a-val, más szóval, b **többszöröse** a-nak, jelöléssel $a \mid b$, ha létezik olyan $c \in \mathbf{Z}$, hogy $ac = b$.

Példák: $3 \mid 15$, $-10 \mid 20$, bármely $x \in \mathbf{Z}$-re $1 \mid x$, $x \mid x$ és $x \mid 0$, ha $0 \mid x$ akkor $x = 0$. De pl. $7 \nmid 20$.

Mivel $x \mid y \iff |x| \mid |y|$, a továbbiakban gyakran csak $\mathbf{N}_0$-ra szorítkozunk. Ez esetben $a \mid b \iff (\exists c \in \mathbf{N}_0)(ac = b)$, de itt nyilván $c \in \mathbf{Z}$ -t is írhatnánk, tehát nemnegatív egész számok esetében az oszthatóság fogalma nem függ attól, hogy $\mathbf{Z}$-t vagy $\mathbf{N}_0$-at tekintjük.

Viszont pl. $\mathbf{Q}$ vagy $\mathbf{R}$ esetén nem szokás oszthatósági kérdésekkel foglalkozni, hiszen — leszámítva azt, hogy a 0 csak önmagát osztja — a fentivel analóg definíció szerint bármely két racionális, illetve valós szám osztja egymást.

Viszont pl. $\mathbf{Q}$ vagy $\mathbf{R}$ esetén nem szokás oszthatósági kérdésekkel foglalkozni, hiszen — leszámítva azt, hogy a 0 csak önmagát osztja — a fentivel analóg definíció szerint bármely két racionális, illetve valós szám osztja egymást.Másrészt viszont pl. a valós vagy racionális együtthatós polinomok körében az oszthatóság érdekes — és a Diszkrét matematika III. során tanulmányozandó kérdés; most csak annyit említünk, Viszont pl. $\mathbf{Q}$ vagy $\mathbf{R}$ esetén nem szokás oszthatósági kérdésekkel foglalkozni, hiszen — leszámítva azt, hogy a 0 csak önmagát osztja — a fentivel analóg definíció szerint bármely két racionális, illetve valós szám osztja egymást.Másrészt viszont pl. a valós vagy racionális együtthatós polinomok körében az oszthatóság érdekes — és a Diszkrét matematika III. során tanulmányozandó kérdés; most csak annyit említünk, hogy $x+1 \mid x^2+2x+1$, $x+1 \nmid x^2+2x+2$, és a számelmélet alaptétele — a fogalmak alkalmas értelmezése mellett — ott is érvényes lesz.

13. Tétel. *(***Az oszthatóság elemi tulajdonságai***)*
Legyen $a, b, c, d \in \mathbf{N}_0$ *tetszőleges. Ekkor*

13. Tétel. *(**Az oszthatóság elemi tulajdonságai**)*
Legyen $a, b, c, d \in \mathbb{N}_0$ *tetszőleges. Ekkor*

(1) Az oszthatósági reláció az $\mathbb{N}_0$ *halmazon* **részben-rendezés***, azaz*

13. Tétel. *(***Az oszthatóság elemi tulajdonságai***)*
Legyen $a, b, c, d \in \mathbf{N}_0$ *tetszőleges. Ekkor*

(1) Az oszthatósági reláció az $\mathbf{N}_0$ *halmazon* **részben-rendezés***, azaz reflexív* ($a \mid a$)*, antiszimmetrikus*

13. Tétel. *(***Az oszthatóság elemi tulajdonságai***)*
Legyen $a, b, c, d \in \mathbf{N}_0$ *tetszőleges. Ekkor*

(1) Az oszthatósági reláció az $\mathbf{N}_0$ *halmazon* **részben-rendezés***, azaz reflexív (*$a \mid a$*), antiszimmetrikus (ha* $a \mid b$ *és* $b \mid a$*, akkor* $a = b$*) és tranzitív*

13. Tétel. *(***Az oszthatóság elemi tulajdonságai***)*
Legyen $a, b, c, d \in \mathbf{N}_0$ *tetszőleges. Ekkor*

(1) Az oszthatósági reláció az $\mathbf{N}_0$ *halmazon* **részben-rendezés***, azaz reflexív (*$a \mid a$*), antiszimmetrikus (ha* $a \mid b$ *és* $b \mid a$*, akkor* $a = b$*) és tranzitív (ha* $a \mid b$ *és* $b \mid c$*, akkor* $a \mid c$*).*

13. Tétel. *(**Az oszthatóság elemi tulajdonságai**)*
Legyen $a, b, c, d \in \mathbf{N}_0$ tetszőleges. Ekkor

(1) Az oszthatósági reláció az $\mathbf{N}_0$ halmazon ***részbenrendezés**, azaz reflexív ($a \mid a$), antiszimmetrikus (ha $a \mid b$ és $b \mid a$, akkor $a = b$) és tranzitív (ha $a \mid b$ és $b \mid c$, akkor $a \mid c$).*

(2) Ha $a \mid b$ és $a \mid c$, akkor

13. Tétel. *(**Az oszthatóság elemi tulajdonságai**) Legyen $a, b, c, d \in \mathbf{N}_0$ tetszőleges. Ekkor*

*(1) Az oszthatósági reláció az $\mathbf{N}_0$ halmazon **részbenrendezés**, azaz reflexív ($a \mid a$), antiszimmetrikus (ha $a \mid b$ és $b \mid a$, akkor $a = b$) és tranzitív (ha $a \mid b$ és $b \mid c$, akkor $a \mid c$).*

(2) Ha $a \mid b$ és $a \mid c$, akkor $a \mid bc$, $a \mid b + c$ és $a \mid b - c$.

(3) Ha $ac \mid bc$ és $c \neq 0$, akkor $a \mid b$. (Lehet $c \neq 0$-val egyszerűsíteni.)

Bizonyítás:

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei,

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk.

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$.

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$. Ekkor létezik $b_1, c_1 \in \mathbf{N}_0$, hogy $ab_1 = b$ és $ac_1 = c$. Ezért $a(b_1 + c_1) = ab_1 + ac_1 = b + c$, azaz

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$. Ekkor létezik $b_1, c_1 \in \mathbf{N}_0$, hogy $ab_1 = b$ és $ac_1 = c$. Ezért $a(b_1 + c_1) = ab_1 + ac_1 = b + c$, azaz $a \mid b + c$. Q.e.d

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$. Ekkor létezik $b_1, c_1 \in \mathbf{N}_0$, hogy $ab_1 = b$ és $ac_1 = c$. Ezért $a(b_1 + c_1) = ab_1 + ac_1 = b + c$, azaz $a \mid b + c$. Q.e.d

Megjegyzések: Az antiszimmetriát (és ezért a részbenrendezést) leszámítva a tétel állításai $\mathbf{Z}$-ben is érvényesek.

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$. Ekkor létezik $b_1, c_1 \in \mathbf{N}_0$, hogy $ab_1 = b$ és $ac_1 = c$. Ezért $a(b_1 + c_1) = ab_1 + ac_1 = b + c$, azaz $a \mid b + c$. Q.e.d

Megjegyzések: Az antiszimmetriát (és ezért a részbenrendezést) leszámítva a tétel állításai $\mathbf{Z}$-ben is érvényesek. Hamarosan azt is látni fogjuk, hogy $(\mathbf{N}_0, |)$ nemcsak részbenrendezett halmaz, hanem háló is, amelynek

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$. Ekkor létezik $b_1, c_1 \in \mathbf{N}_0$, hogy $ab_1 = b$ és $ac_1 = c$. Ezért $a(b_1 + c_1) = ab_1 + ac_1 = b + c$, azaz $a \mid b + c$. Q.e.d

Megjegyzések: Az antiszimmetriát (és ezért a részbenrendezést) leszámítva a tétel állításai $\mathbf{Z}$-ben is érvényesek. Hamarosan azt is látni fogjuk, hogy $(\mathbf{N}_0, \mid)$ nemcsak részbenrendezett halmaz, hanem háló is, amelynek — ellentétben a részbenrendezéseknél szokásos jelölésekkel — az 1 a legkisebb eleme (

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$. Ekkor létezik $b_1, c_1 \in \mathbf{N}_0$, hogy $ab_1 = b$ és $ac_1 = c$. Ezért $a(b_1 + c_1) = ab_1 + ac_1 = b + c$, azaz $a \mid b + c$. Q.e.d

Megjegyzések: Az antiszimmetriát (és ezért a részbenrendezést) leszámítva a tétel állításai $\mathbf{Z}$-ben is érvényesek. Hamarosan azt is látni fogjuk, hogy $(\mathbf{N}_0, |)$ nemcsak részbenrendezett halmaz, hanem háló is, amelynek — ellentétben a részbenrendezéseknél szokásos jelölésekkel — az 1 a legkisebb eleme (mert mindent oszt) és a 0 a legnagyobb eleme
(

Bizonyítás: A tétel állításai a definíció közvetlen — és többnyire közismert — következményei, ezért ízelítőként csak az egyiket igazoljuk. Tegyük fel, hogy $a \mid b$ és $a \mid c$. Ekkor létezik $b_1, c_1 \in \mathbf{N}_0$, hogy $ab_1 = b$ és $ac_1 = c$. Ezért $a(b_1 + c_1) = ab_1 + ac_1 = b + c$, azaz $a \mid b + c$. Q.e.d

Megjegyzések: Az antiszimmetriát (és ezért a részbenrendezést) leszámítva a tétel állításai $\mathbf{Z}$-ben is érvényesek. Hamarosan azt is látni fogjuk, hogy $(\mathbf{N}_0, |)$ nemcsak részbenrendezett halmaz, hanem háló is, amelynek — ellentétben a részbenrendezéseknél szokásos jelölésekkel — az 1 a legkisebb eleme (mert mindent oszt) és a 0 a legnagyobb eleme (mert őt minden osztja).

Most definiáljuk a legnagyobb közös osztó és a legkisebb közös többszörös fogalmát $\mathbf{Z}$-ben. Ezek természetesen a középiskolában megszokott jelentéssel bírnak.

Most definiáljuk a legnagyobb közös osztó és a legkisebb közös többszörös fogalmát $\mathbf{Z}$-ben. Ezek természetesen a középiskolában megszokott jelentéssel bírnak. Azonban definíciónk az ott megszokottól eltérő lesz, Most definiáljuk a legnagyobb közös osztó és a legkisebb közös többszörös fogalmát $\mathbf{Z}$-ben. Ezek természetesen a középiskolában megszokott jelentéssel bírnak. Azonban definíciónk az ott megszokottól eltérő lesz, — egyrészt azért, mert az itt szereplő definíció könnyedén átvihető majd polinomokra (a Diszkrét matematika III tantárgyban), másrészt mert így azonnal látható lesz, hogy $(\mathbf{N}_0, |)$ háló.

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **leg-nagyobb közös osztója**, ha

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **leg-nagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Hasonlítsuk ezt össze az alábbi, korábban tanult definícióval.

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Hasonlítsuk ezt össze az alábbi, korábban tanult definícióval.

Definíció: Legyen $(A; \leq)$ részbenrendezett halmaz.

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Hasonlítsuk ezt össze az alábbi, korábban tanult definícióval.

Definíció: Legyen $(A; \leq)$ részbenrendezett halmaz. Akkor mondjuk, hogy $c \in A$ az $a, b \in A$ elemek infimuma (más szóval: metszete, legnagyobb alsó korlátja),

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Hasonlítsuk ezt össze az alábbi, korábban tanult definícióval.

Definíció: Legyen $(A; \leq)$ részbenrendezett halmaz. Akkor mondjuk, hogy $c \in A$ az $a, b \in A$ elemek infimuma (más szóval: metszete, legnagyobb alsó korlátja), ha egyrészt $c \leq a$ és $c \leq b$ (azaz

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Hasonlítsuk ezt össze az alábbi, korábban tanult definícióval.

Definíció: Legyen $(A; \leq)$ részbenrendezett halmaz. Akkor mondjuk, hogy $c \in A$ az $a, b \in A$ elemek infimuma (más szóval: metszete, legnagyobb alsó korlátja), ha egyrészt $c \leq a$ és $c \leq b$ (azaz c alsó korlát), és

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Hasonlítsuk ezt össze az alábbi, korábban tanult definícióval.

Definíció: Legyen $(A; \leq)$ részbenrendezett halmaz. Akkor mondjuk, hogy $c \in A$ az $a, b \in A$ elemek infimuma (más szóval: metszete, legnagyobb alsó korlátja), ha egyrészt $c \leq a$ és $c \leq b$ (azaz c alsó korlát), és másrészt bármely $d \in A$ esetén ha $d \leq a$ és $d \leq b$, akkor $d \leq c$ (azaz c-nél mindegyik alsó korlát kisebb vagy egyenlő).

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legnagyobb közös osztója**, ha egyrészt $c \mid a$ és $c \mid b$ (azaz c közös osztó), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $d \mid a$ és $d \mid b$, akkor $d \mid c$ (azaz c-t mindegyik közös osztó osztja).

Hasonlítsuk ezt össze az alábbi, korábban tanult definícióval.

Definíció: Legyen $(A; \leq)$ részbenrendezett halmaz. Akkor mondjuk, hogy $c \in A$ az $a, b \in A$ elemek infimuma (más szóval: metszete, legnagyobb alsó korlátja), ha egyrészt $c \leq a$ és $c \leq b$ (azaz c alsó korlát), és másrészt bármely $d \in A$ esetén ha $d \leq a$ és $d \leq b$, akkor $d \leq c$ (azaz c-nél mindegyik alsó korlát kisebb vagy egyenlő).

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus.

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z};|)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0;|)$ már részbenrendezett halmazt, Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z};|)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0;|)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója , pontosabban a legnagyobb közös osztói

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója , pontosabban a legnagyobb közös osztói a 2 és a -2.

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója , pontosabban a legnagyobb közös osztói a 2 és a -2. Ugyanis a közös osztók halmaza

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z};|)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0;|)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója , pontosabban a legnagyobb közös osztói a 2 és a -2. Ugyanis a közös osztók halmaza $\{1, -1, 2, -2\}$, és ezen közös osztók mindegyike osztja a 2-t,

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z};|)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0;|)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója , pontosabban a legnagyobb közös osztói a 2 és a -2. Ugyanis a közös osztók halmaza $\{1, -1, 2, -2\}$, és ezen közös osztók mindegyike osztja a 2-t, és persze a -2-t is.

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója , pontosabban a legnagyobb közös osztói a 2 és a -2. Ugyanis a közös osztók halmaza $\{1, -1, 2, -2\}$, és ezen közös osztók mindegyike osztja a 2-t, és persze a -2-t is. Az 50 és a -15 legnagyobb közös osztói:

Az előbbi összehasonlítás kapcsán fontos megjegyeznünk, hogy $(\mathbf{Z}; |)$ **nem** részbenrendezett halmaz, hiszen pl. $-1 \mid 1$ és $1 \mid -1$ miatt a reláció nem antiszimmetrikus. Viszont $(\mathbf{N}_0; |)$ már részbenrendezett halmazt, és az előző két definíció összehasonlítása alapján látható, hogy a legnagyobb közös osztó éppen a legnagyobb alsó korlát (azaz infimum).

Példák: $\mathbf{Z}$-ben a -4 és -6 legnagyobb közös osztója , pontosabban a legnagyobb közös osztói a 2 és a -2. Ugyanis a közös osztók halmaza $\{1, -1, 2, -2\}$, és ezen közös osztók mindegyike osztja a 2-t, és persze a -2-t is. Az 50 és a -15 legnagyobb közös osztói: 5 és -5.

Feladat: Legyen $a = 0$ és $b = 0$. Mi a és b legnagyobb közös osztója $\mathbf{Z}$-ben?

Feladat: Legyen $a = 0$ és $b = 0$. Mi a és b legnagyobb közös osztója $\mathbf{Z}$-ben?

Megoldás: A közös osztók halmaza most

Feladat: Legyen $a = 0$ és $b = 0$. Mi a és b legnagyobb közös osztója $\mathbf{Z}$-ben?

Megoldás: A közös osztók halmaza most $\mathbf{Z}$. Van-e ezek között olyan d, amelyiket az összes többi osztja?

Feladat: Legyen $a = 0$ és $b = 0$. Mi a és b legnagyobb közös osztója $\mathbf{Z}$-ben?

Megoldás: A közös osztók halmaza most $\mathbf{Z}$. Van-e ezek között olyan d, amelyiket az összes többi osztja? Igen,

Feladat: Legyen $a = 0$ és $b = 0$. Mi a és b legnagyobb közös osztója $\mathbf{Z}$-ben?

Megoldás: A közös osztók halmaza most $\mathbf{Z}$. Van-e ezek között olyan d, amelyiket az összes többi osztja? Igen, $d = 0$! (Más ilyen d nincs, mert d-nek többek között a nullával is oszthatónak kell lennie.)

Feladat: Legyen $a = 0$ és $b = 0$. Mi a és b legnagyobb közös osztója $\mathbf{Z}$-ben?

Megoldás: A közös osztók halmaza most $\mathbf{Z}$. Van-e ezek között olyan d, amelyiket az összes többi osztja? Igen, $d = 0$! (Más ilyen d nincs, mert d-nek többek között a nullával is oszthatónak kell lennie.)

Látható, hogy a nulla jelenléte esetén definíciónk eltér a középiskolaitól, hiszen a „legnagyobb" hétköznapi értelmében a 0 nem a legnagyobb egész szám.

Definíciónk azért nem a „legnagyobb” hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, Definíciónk azért nem a „legnagyobb” hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl.

Definíciónk azért nem a „legnagyobb'' hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl. nem tudjuk megmondani, hogy az x^2+1 és a 100

Definíciónk azért nem a „legnagyobb” hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl. nem tudjuk megmondani, hogy az x^2+1 és a 100^{100}

Definíciónk azért nem a „legnagyobb'' hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl. nem tudjuk megmondani, hogy az x^2+1 és a $100^{100^{100}}$

Definíciónk azért nem a „legnagyobb” hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl. nem tudjuk megmondani, hogy az x^2+1 és a $100^{100^{100}}x+$

Definíciónk azért nem a „legnagyobb'' hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl. nem tudjuk megmondani, hogy az x^2+1 és a $100^{100^{100}}x+10$

Definíciónk azért nem a „legnagyobb” hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl. nem tudjuk megmondani, hogy az x^2+1 és a $100^{100^{100}}x+10^{10^{10}}$ polinomok közül melyik a nagyobb.

Definíciónk azért nem a „legnagyobb” hétköznapi jelentésére támaszkodik, hogy polinomokra könnyen átvihető legyen, ugyanis a polinomok halmaza nem rendeztt; pl. nem tudjuk megmondani, hogy az x^2+1 és a $100^{100^{100}}x+10^{10^{10}}$ polinomok közül melyik a nagyobb.

A legkisebb közös többszöröst a legkisebb felső korlát mintájára definiáljuk.

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha egyrészt $a \mid c$ és $b \mid c$ (azaz

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha egyrészt $a \mid c$ és $b \mid c$ (azaz c közös többszörös), és

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha egyrészt $a \mid c$ és $b \mid c$ (azaz c közös többszörös), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $a \mid d$ és $b \mid d$, akkor $c \mid d$ (azaz c-nek mindegyik közös többszörös többszöröse).

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha egyrészt $a \mid c$ és $b \mid c$ (azaz c közös többszörös), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $a \mid d$ és $b \mid d$, akkor $c \mid d$ (azaz c-nek mindegyik közös többszörös többszöröse).

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha egyrészt $a \mid c$ és $b \mid c$ (azaz c közös többszörös), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $a \mid d$ és $b \mid d$, akkor $c \mid d$ (azaz c-nek mindegyik közös többszörös többszöröse).

Közismert, hogy $\mathbf{Z}$-ben a legnagyobb közös osztó is és a legkisebb közös többszörös is

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha egyrészt $a \mid c$ és $b \mid c$ (azaz c közös többszörös), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $a \mid d$ és $b \mid d$, akkor $c \mid d$ (azaz c-nek mindegyik közös többszörös többszöröse).

Közismert, hogy $\mathbf{Z}$-ben a legnagyobb közös osztó is és a legkisebb közös többszörös is létezik, és

Definíció: Akkor mondjuk, hogy $c \in \mathbf{Z}$ az $a, b \in \mathbf{Z}$ számok **legkisebb közös többszöröse**, ha egyrészt $a \mid c$ és $b \mid c$ (azaz c közös többszörös), és másrészt bármely $d \in \mathbf{Z}$ esetén ha $a \mid d$ és $b \mid d$, akkor $c \mid d$ (azaz c-nek mindegyik közös többszörös többszöröse).

Közismert, hogy $\mathbf{Z}$-ben a legnagyobb közös osztó is és a legkisebb közös többszörös is létezik, és előjel erejéig egyértelműen meg van határozva.

Ami az egyértelműséget illeti, az

Ami az egyértelműséget illeti, az triviális: ha

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös.

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják.

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú.

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért $c = c_1 d_1 c$, ahonnan

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért $c = c_1 d_1 c$, ahonnan — ha $c \neq 0$ — $c_1 d_1 = 1$, tehát $c_1, d_1 \in \{1, -1\}$, azaz

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért $c = c_1 d_1 c$, ahonnan — ha $c \neq 0$ — $c_1 d_1 = 1$, tehát $c_1, d_1 \in \{1, -1\}$, azaz c és d csak előjelben tér el.

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért $c = c_1 d_1 c$, ahonnan — ha $c \neq 0$ — $c_1 d_1 = 1$, tehát $c_1, d_1 \in \{1, -1\}$, azaz c és d csak előjelben tér el. Ez akkor is igaz, ha $c = 0$, hiszen akkor $d = d_1 c = 0$.

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért $c = c_1 d_1 c$, ahonnan — ha $c \neq 0$ — $c_1 d_1 = 1$, tehát $c_1, d_1 \in \{1, -1\}$, azaz c és d csak előjelben tér el. Ez akkor is igaz, ha $c = 0$, hiszen akkor $d = d_1 c = 0$.

Az már sokkal kevésbé nyilvánvaló, hogy bármely két egész számnak létezik legnagyobb közös osztója és legkisebb közös többszöröse.

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért $c = c_1 d_1 c$, ahonnan — ha $c \neq 0$ — $c_1 d_1 = 1$, tehát $c_1, d_1 \in \{1, -1\}$, azaz c és d csak előjelben tér el. Ez akkor is igaz, ha $c = 0$, hiszen akkor $d = d_1 c = 0$.

Az már sokkal kevésbé nyilvánvaló, hogy bármely két egész számnak létezik legnagyobb közös osztója és legkisebb közös többszöröse. Ezt hamarosan be fogjuk bizonyítani —

Ami az egyértelműséget illeti, az triviális: ha c is és d is az a, b egész számok legkisebb közös többszöröse, akkor $c \mid d$, hiszen c a legkisebb, d pedig egy másik közös többszörös, de $d \mid c$ is teljesül, hiszen d a legkisebb, c pedig egy másik közös többszörös. Tehát c és d egymást kölcsönösen osztják. Így $c = c_1 d$, $d = d_1 c$ alakú. Ezért $c = c_1 d_1 c$, ahonnan — ha $c \neq 0$ — $c_1 d_1 = 1$, tehát $c_1, d_1 \in \{1, -1\}$, azaz c és d csak előjelben tér el. Ez akkor is igaz, ha $c = 0$, hiszen akkor $d = d_1 c = 0$.

Az már sokkal kevésbé nyilvánvaló, hogy bármely két egész számnak létezik legnagyobb közös osztója és legkisebb közös többszöröse. Ezt hamarosan be fogjuk bizonyítani — elsősorban azért, mert a bizonyítás egy jó algoritmust szolgáltat az ln.k.o. és az lk.k.t. kiszámításához.

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése.

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése.
Tekintsük a páros egész számok halmazát: A.

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése. Tekintsük a páros egész számok halmazát: A. A-ban is definiálhatjuk az oszthatóságot: $a, b \in A$ esetén $a \mid b$ jelentse azt, hogy van olyan $c \in A$, amelyre $ac = b$.

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése. Tekintsük a páros egész számok halmazát: A. A-ban is definiálhatjuk az oszthatóságot: $a, b \in A$ esetén $a \mid b$ jelentse azt, hogy van olyan $c \in A$, amelyre $ac = b$. Mármost a 6-nak és a 8-nak egyáltalán nincs közös osztója A-ban — hiszen a 6 semmivel sem osztható A-ban!

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése. Tekintsük a páros egész számok halmazát: A. A-ban is definiálhatjuk az oszthatóságot: $a, b \in A$ esetén $a \mid b$ jelentse azt, hogy van olyan $c \in A$, amelyre $ac = b$. Mármost a 6-nak és a 8-nak egyáltalán nincs közös osztója A-ban — hiszen a 6 semmivel sem osztható A-ban!

Definíció: Egy 1-nél nagyobb p egész számot **irreducibilis** számnak (más szóval **törzsszámnak**) nevezünk, ha $\mathbf{N}_0$-ban p csak 1-gyel és önmagával osztható.

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése. Tekintsük a páros egész számok halmazát: A. A-ban is definiálhatjuk az oszthatóságot: $a, b \in A$ esetén $a \mid b$ jelentse azt, hogy van olyan $c \in A$, amelyre $ac = b$. Mármost a 6-nak és a 8-nak egyáltalán nincs közös osztója A-ban — hiszen a 6 semmivel sem osztható A-ban!

Definíció: Egy 1-nél nagyobb p egész számot **irreducibilis** számnak (más szóval **törzsszámnak**) nevezünk, ha $\mathbf{N}_0$-ban p csak 1-gyel és önmagával osztható. Példák: a 2, 3, 5, 7, 11 törzsszámok, de a 6 nem.

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése. Tekintsük a páros egész számok halmazát: A. A-ban is definiálhatjuk az oszthatóságot: $a, b \in A$ esetén $a \mid b$ jelentse azt, hogy van olyan $c \in A$, amelyre $ac = b$. Mármost a 6-nak és a 8-nak egyáltalán nincs közös osztója A-ban — hiszen a 6 semmivel sem osztható A-ban!

Definíció: Egy 1-nél nagyobb p egész számot **irreducibilis** számnak (más szóval **törzsszámnak**) nevezünk, ha $\mathbf{N}_0$-ban p csak 1-gyel és önmagával osztható. Példák: a 2, 3, 5, 7, 11 törzsszámok, de a 6 nem. Egy 1-nél nagyobb p egész számot **prímszámnak** nevezünk, ha bármely $a, b \in \mathbf{N}_0$ esetén ha $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$.

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése. Tekintsük a páros egész számok halmazát: A. A-ban is definiálhatjuk az oszthatóságot: $a, b \in A$ esetén $a \mid b$ jelentse azt, hogy van olyan $c \in A$, amelyre $ac = b$. Mármost a 6-nak és a 8-nak egyáltalán nincs közös osztója A-ban — hiszen a 6 semmivel sem osztható A-ban!

Definíció: Egy 1-nél nagyobb p egész számot **irreducibilis** számnak (más szóval **törzsszámnak**) nevezünk, ha $\mathbf{N}_0$-ban p csak 1-gyel és önmagával osztható. Példák: a 2, 3, 5, 7, 11 törzsszámok, de a 6 nem. Egy 1-nél nagyobb p egész számot **prímszámnak** nevezünk, ha bármely $a, b \in \mathbf{N}_0$ esetén ha $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$. (Azaz ha p oszt egy szorzatot, akkor osztja annak az egyik tényezőjét.)

Íme egy példa, hogy miért is nem triviális az ln.k.o. létezése. Tekintsük a páros egész számok halmazát: A. A-ban is definiálhatjuk az oszthatóságot: $a, b \in A$ esetén $a \mid b$ jelentse azt, hogy van olyan $c \in A$, amelyre $ac = b$. Mármost a 6-nak és a 8-nak egyáltalán nincs közös osztója A-ban — hiszen a 6 semmivel sem osztható A-ban!

Definíció: Egy 1-nél nagyobb p egész számot **irreducibilis** számnak (más szóval **törzsszámnak**) nevezünk, ha $\mathbf{N}_0$-ban p csak 1-gyel és önmagával osztható. Példák: a 2, 3, 5, 7, 11 törzsszámok, de a 6 nem. Egy 1-nél nagyobb p egész számot **prímszámnak** nevezünk, ha bármely $a, b \in \mathbf{N}_0$ esetén ha $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$. (Azaz ha p oszt egy szorzatot, akkor osztja annak az egyik tényezőjét.) Példák: a 2, 3, 5, 7, 11 prímszámok, de a 6 nem.

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában a 6 irreducibilis — hiszen nem áll elő két páros szám szorzataként.

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában a 6 irreducibilis — hiszen nem áll elő két páros szám szorzataként. De nem prím, hiszen pl. $6 \mid 18 \cdot 30$

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában a 6 irreducibilis — hiszen nem áll elő két páros szám szorzataként. De nem prím, hiszen pl. $6 \mid 18 \cdot 30 = 540 =$

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában a 6 irreducibilis — hiszen nem áll elő két páros szám szorzataként. De nem prím, hiszen pl. $6 \mid 18 \cdot 30 = 540 = 6 \cdot 90$, de $6 \not| \ 18$ és $6 \not| \ 30$.

14. Tétel. *$\mathbf{Z}$-ben mindig elvégezhető a maradékos osztás. Azaz*

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában a 6 irreducibilis — hiszen nem áll elő két páros szám szorzataként. De nem prím, hiszen pl. $6 \mid 18 \cdot 30 = 540 = 6 \cdot 90$, de $6 \nmid 18$ és $6 \nmid 30$.

14. Tétel. *$\mathbf{Z}$-ben mindig elvégezhető a maradékos osztás. Azaz bármely $a \in \mathbf{Z}$ és $b \in \mathbf{Z} \setminus \{0\}$ esetén létezik olyan $q, r \in \mathbf{Z}$, hogy $0 \leq r < |b|$ és $a = bq + r$.*

A

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában a 6 irreducibilis — hiszen nem áll elő két páros szám szorzataként. De nem prím, hiszen pl. $6 \mid 18 \cdot 30 = 540 = 6 \cdot 90$, de $6 \nmid 18$ és $6 \nmid 30$.

14. Tétel. *$\mathbf{Z}$-ben mindig elvégezhető a maradékos osztás. Azaz bármely $a \in \mathbf{Z}$ és $b \in \mathbf{Z} \setminus \{0\}$ esetén létezik olyan $q, r \in \mathbf{Z}$, hogy $0 \leq r < |b|$ és $a = bq + r$.*

A tételbeli a-t **osztandónak**, b-t **osztónak**, q-t **hányadosnak** és r-et **maradéknak** nevezik.

Néha hasznos negatív maradékot is megengedni,

Hamarosan látni fogjuk, hogy az irreducibilis számok ugyanazok, mint a prímszámok. Ez azonban távolról sem triviális. Például a már említett páros számok A halmazában a 6 irreducibilis — hiszen nem áll elő két páros szám szorzataként. De nem prím, hiszen pl. $6 \mid 18 \cdot 30 = 540 = 6 \cdot 90$, de $6 \nmid 18$ és $6 \nmid 30$.

14. Tétel. *$\mathbf{Z}$-ben mindig elvégezhető a maradékos osztás. Azaz bármely $a \in \mathbf{Z}$ és $b \in \mathbf{Z} \setminus \{0\}$ esetén létezik olyan $q, r \in \mathbf{Z}$, hogy $0 \leq r < |b|$ és $a = bq + r$.*

A tételbeli a-t **osztandónak**, b-t **osztónak**, q-t **hányadosnak** és r-et **maradéknak** nevezik.

Néha hasznos negatív maradékot is megengedni, ekkor $|r| \leq |b|/2$-t kötjük ki.

Bizonyítás (vázlat): Csak

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk.

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt.

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának.

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0.

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0. Ekkor alkalmas $q_0 \in \mathbf{Z}$-re $r_0 = a - bq_0$. Ha $r_0 \geq b$ lenne, akkor

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0. Ekkor alkalmas $q_0 \in \mathbf{Z}$-re $r_0 = a - bq_0$. Ha $r_0 \geq b$ lenne, akkor $0 \leq r_0 - b = a - bq_0 - b =$

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0. Ekkor alkalmas $q_0 \in \mathbf{Z}$-re $r_0 = a - bq_0$. Ha $r_0 \geq b$ lenne, akkor $0 \leq r_0 - b = a - bq_0 - b = a - b(q_0 + 1)$ is M-beli lenne, ami $r_0 - b < r_0$ miatt ellentmondana

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0. Ekkor alkalmas $q_0 \in \mathbf{Z}$-re $r_0 = a - bq_0$. Ha $r_0 \geq b$ lenne, akkor $0 \leq r_0 - b = a - bq_0 - b = a - b(q_0 + 1)$ is M-beli lenne, ami $r_0 - b < r_0$ miatt ellentmondana r_0 minimalitásának.

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0. Ekkor alkalmas $q_0 \in \mathbf{Z}$-re $r_0 = a - bq_0$. Ha $r_0 \geq b$ lenne, akkor $0 \leq r_0 - b = a - bq_0 - b = a - b(q_0 + 1)$ is M-beli lenne, ami $r_0 - b < r_0$ miatt ellentmondana r_0 minimalitásának. Tehát $r_0 < b$, és

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0. Ekkor alkalmas $q_0 \in \mathbf{Z}$-re $r_0 = a - bq_0$. Ha $r_0 \geq b$ lenne, akkor $0 \leq r_0 - b = a - bq_0 - b = a - b(q_0 + 1)$ is M-beli lenne, ami $r_0 - b < r_0$ miatt ellentmondana r_0 minimalitásának. Tehát $r_0 < b$, és — az $r_0 = a - bq_0$ egyenlőséget átrendeze — $a = bq_0 + r_0$.

Bizonyítás (vázlat): Csak pozitív a-val és b-vel foglalkozunk. Tekintsük az $M = \{a - bq \in \mathbf{N}_0 : q \in \mathbf{Z}\}$ halmazt. Ez nem üres, hiszen q választható nullának. Mint $\mathbf{N}_0$ bármely nemüres részhalmazának, M-nek is van legkisebb eleme, jelölje azt r_0. Ekkor alkalmas $q_0 \in \mathbf{Z}$-re $r_0 = a - bq_0$. Ha $r_0 \geq b$ lenne, akkor $0 \leq r_0 - b = a - bq_0 - b = a - b(q_0 + 1)$ is M-beli lenne, ami $r_0 - b < r_0$ miatt ellentmondana r_0 minimalitásának. Tehát $r_0 < b$, és — az $r_0 = a - bq_0$ egyenlőséget átrendeze — $a = bq_0 + r_0$. Q.e.d.

Hogyan határozhatjuk meg két szám legnagyobb közös osztóját?

Hogyan határozhatjuk meg két szám legnagyobb közös osztóját?
„Kis” számok esetében a prímfelbontás segít.

Hogyan határozhatjuk meg két szám legnagyobb közös osztóját? „Kis” számok esetében a prímfelbontás segít. Ez azonban nem alkalmazható nagy számoknál, hiszen egy nagy szám prímtényezőkre bontását nem ismerjük. Tekintsük például az alábbi, háromszáz jegyű számot:

$$
\begin{aligned}
c = {} & 19980539999978399999999969659178600992799881392 2\\
& 999999309685999420818231006059999989978403690 03\\
& 451608719005891999760000629995487300013117020 48\\
& 349650696701565548639774189497713188181873231 10\\
& 461649614481329992978266091406012999999298158 95\\
& 097752115629221614873000000234057796594380058 01\\
& 815330791283814831
\end{aligned}
$$

$$
\begin{gathered}
c = 1998053999997839999999999696591786009927998813922 \\
9999993096859994208182310060599999899784036900 3 \\
4516087190058919997600006299954873000131170204 8 \\
3496506967015655486397741894977131881818732311 0 \\
4616496144813299929782660914060129999992981589 5 \\
0977521156292216148730000002340577965943800580 1 \\
815330791283814831
\end{gathered}
$$

Annyit elárulok, hogy c-nek mindössze két prímtényezője van.

$$
\begin{aligned}
c = {} & 19980539999978399999999969659178600992799881392 2\\
& 999999309685999420818231006059999989978403690 03\\
& 4516087190058919997600006299954873000131170204 8\\
& 3496506967015655486397741894977131881818732311 0\\
& 4616496144813299929782660914060129999992981589 5\\
& 0977521156292216148730000002340577965943800580 1\\
& 815330791283814831
\end{aligned}
$$

Annyit elárulok, hogy c-nek mindössze két prímtényezője van. Jeles vizsgajegyet ajánlok annak, aki elsőként meghatározza c prímtényezős felbontását.

$$
\begin{aligned}
c = {} & 1998053999978399999999696591786009927998813922 \\
& 99999930968599942081823100605999998997840369003 \\
& 45160871900589199976000062999548730001311702048 \\
& 34965069670156554863977418949771318818187323110 \\
& 46164961448132999297826609140601299999929815895 \\
& 09775211562922161487300000023405779659438005801 \\
& 8153307912838 14831
\end{aligned}
$$

Annyit elárulok, hogy c-nek mindössze két prímtényezője van. Jeles vizsgajegyet ajánlok annak, aki elsőként meghatározza c prímtényezős felbontását. Mindenféle segédeszköz használható.

A

A m

A ma

A matematika jelen tudása szerint egy véletlenül előállított ilyen szám tényezőkre bontásához a naprendszer élettartama akkor sem lenne elegendő, ha minden létező számítógép ezen dolgozna.

A matematika jelen tudása szerint egy véletlenül előállított ilyen szám tényezőkre bontásához a naprendszer élettartama akkor sem lenne elegendő, ha minden létező számítógép ezen dolgozna. c-t — számítógéppel, a Maple V programmal — úgy állítottam elő, hogy két nagy **majdnem** véletlenül választott prímszámot összeszoroztam, ez — gépeléssel együtt — csupán néhány percet igényelt.

A matematika jelen tudása szerint egy véletlenül előállított ilyen szám tényezőkre bontásához a naprendszer élettartama akkor sem lenne elegendő, ha minden létező számítógép ezen dolgozna. c-t — számítógéppel, a Maple V programmal — úgy állítottam elő, hogy két nagy **majdnem** véletlenül választott prímszámot összeszoroztam, ez — gépeléssel együtt — csupán néhány percet igényelt. A nyilvános kulcsú titkosírások egy része, pl. a legkinkább közismert RSA, A matematika jelen tudása szerint egy véletlenül előállított ilyen szám tényezőkre bontásához a naprendszer élettartama akkor sem lenne elegendő, ha minden létező számítógép ezen dolgozna. c-t — számítógéppel, a Maple V programmal — úgy állítottam elő, hogy két nagy **majdnem** véletlenül választott prímszámot összeszoroztam, ez — gépeléssel együtt — csupán néhány percet igényelt. A nyilvános kulcsú titkosírások egy része, pl. a legkinkább közismert RSA, azon alapul, hogy a nagy számokat roppant nehéz tényezők szorzatára bontani.

A matematika jelen tudása szerint egy véletlenül előállított ilyen szám tényezőkre bontásához a naprendszer élettartama akkor sem lenne elegendő, ha minden létező számítógép ezen dolgozna. c-t — számítógéppel, a Maple V programmal — úgy állítottam elő, hogy két nagy **majdnem** véletlenül választott prímszámot összeszoroztam, ez — gépeléssel együtt — csupán néhány percet igényelt. A nyilvános kulcsú titkosírások egy része, pl. a legkinkább közismert RSA, azon alapul, hogy a nagy számokat roppant nehéz tényezők szorzatára bontani.

A legnagyobb közös osztó meghatározására vonatkozó alábbi módszert a fentiek fényében kell értékelni.

15. Tétel. *(***Euklideszi algoritmus***)* *Legyen* $a, b \in \mathbb{N}$,

15. Tétel. (Euklideszi algoritmus) *Legyen* $a, b \in \mathbb{N}$*, és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

15. Tétel. (**Euklideszi algoritmus**) *Legyen* $a, b \in \mathbb{N}$*, és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$a = bq_1 + r_1,$$

15. Tétel. (**Euklideszi algoritmus**) *Legyen* $a, b \in \mathbb{N}$*, és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$a = bq_1 + r_1,$$
$$b = r_1q_2 + r_2,$$

15. Tétel. (Euklideszi algoritmus) *Legyen* $a, b \in \mathbb{N}$*, és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$a = bq_1 + r_1,$$
$$b = r_1 q_2 + r_2,$$
$$r_1 = r_2 q_3 + r_3,$$

15. Tétel. (Euklideszi algoritmus) *Legyen* $a, b \in \mathbb{N}$*, és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\dots \end{aligned}$$

15. Tétel. (Euklideszi algoritmus) *Legyen* $a, b \in \mathbb{N}$*, és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n,
\end{aligned}
$$

15. Tétel. (Euklideszi algoritmus) *Legyen* $a, b \in \mathbb{N}$*, és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}
$$

15. Tétel. (Euklideszi algoritmus) *Legyen* $a, b \in \mathbb{N}$, *és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$
\begin{aligned}
a &= bq_1 + r_1,\\
b &= r_1q_2 + r_2,\\
r_1 &= r_2q_3 + r_3,\\
&\dots\\
r_{n-2} &= r_{n-1}q_n + r_n,\\
r_{n-1} &= r_nq_{n+1}
\end{aligned}
$$

Tehát mindig az előző osztóból lesz az osztandó, és az előző maradékból az osztó.

Mivel $b > r_1 > r_2 > \cdots$, *véges számú, mondjuk* n, *lépésben eljutunk addig, hogy a maradék 0 lesz, és akkor megállunk.*

15. Tétel. (Euklideszi algoritmus) *Legyen* $a, b \in \mathbb{N}$, *és tekintsük az alábbi maradékos osztásokat (mindig* q_i *jelenti a hányadost,* r_i *pedig a maradékot):*

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\cdots \\
r_{n-2} &= r_{n-1} q_n + r_n, \\
r_{n-1} &= r_n q_{n+1}
\end{aligned}
$$

Tehát mindig az előző osztóból lesz az osztandó, és az előző maradékból az osztó.

Mivel $b > r_1 > r_2 > \cdots$, *véges számú, mondjuk* n, *lépésben eljutunk addig, hogy a maradék 0 lesz, és akkor megállunk.*

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot 4 +$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot 4 + 12,$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$\begin{aligned} 72 &= 15 \cdot 4 + 12, \\ 15 &= \end{aligned}$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot 4 + 12,$$
$$15 = 12 \cdot$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot 4 + 12,$$
$$15 = 12 \cdot 1 +$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot 4 + 12,$$
$$15 = 12 \cdot 1 + 3,$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$\begin{aligned}
72 &= 15 \cdot 4 + 12, \\
15 &= 12 \cdot 1 + 3, \\
12 &=
\end{aligned}$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$\begin{aligned}72 &= 15 \cdot 4 + 12,\\ 15 &= 12 \cdot 1 + 3,\\ 12 &= 3 \cdot 4 +\end{aligned}$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot 4 + 12,$$
$$15 = 12 \cdot 1 + 3,$$
$$12 = 3 \cdot 4 + 0.$$

Ekkor r_n, azaz az utolsó nemzérus maradék, éppen az a és b számok legnagyobb közös osztója.

Példa: Számítsuk ki a 72 és a 15 legnagyobb közös osztóját!

$$72 = 15 \cdot 4 + 12,$$
$$15 = 12 \cdot 1 + 3,$$
$$12 = 3 \cdot 4 + 0.$$

Tehát az utolsó nemzérus maradék a 3, és ez a keresett ln.k.o.

Bizonyítás: a lényeg az alábbi (konkrét feladatokban is kamatoztatható) állítás. (A legnagyobb közös osztót a továbbiakban ln.k.o. fogja jelölni —

Bizonyítás: a lényeg az alábbi (konkrét feladatokban is kamatoztatható) állítás. (A legnagyobb közös osztót a továbbiakban ln.k.o. fogja jelölni — tehát ln.k.o.$(a, b) \in \mathbf{N}_0$.)

1. Állítás. *Tetszőleges $a, b, q \in \mathbf{Z}$ esetén*

$$\textit{ln.k.o.}(a, b) = \textit{ln.k.o.}(a - bq, b).$$

1. Állítás. *Tetszőleges* $a, b, q \in \mathbf{Z}$ *esetén*

$$\textit{ln.k.o.}(a, b) = \textit{ln.k.o.}(a - bq, b).$$

Valóban, ha $d \mid a$ és $d \mid b$, akkor $d \mid a - bq$.

1. Állítás. *Tetszőleges* $a, b, q \in \mathbf{Z}$ *esetén*

$$\text{\textit{ln.k.o.}}(a, b) = \text{\textit{ln.k.o.}}(a - bq, b).$$

Valóban, ha $d \mid a$ és $d \mid b$, akkor $d \mid a - bq$. Speciálisan , d helyére ln.k.o.(a, b)-t írva kapjuk, hogy

1. Állítás. *Tetszőleges* $a, b, q \in \mathbf{Z}$ *esetén*

$$\textit{ln.k.o.}(a, b) = \textit{ln.k.o.}(a - bq, b).$$

Valóban, ha $d \mid a$ és $d \mid b$, akkor $d \mid a - bq$. Speciálisan , d helyére ln.k.o.(a, b)-t írva kapjuk, hogy ln.k.o.$(a, b) \mid a - bq$

1. Állítás. *Tetszőleges $a, b, q \in \mathbf{Z}$ esetén*

$$\textit{ln.k.o.}(a, b) = \textit{ln.k.o.}(a - bq, b).$$

Valóban, ha $d \mid a$ és $d \mid b$, akkor $d \mid a - bq$. Speciálisan , d helyére ln.k.o.(a, b)-t írva kapjuk, hogy ln.k.o.$(a, b) \mid a - bq$ és persze ln.k.o.$(a, b) \mid b$ is. Ezért

1. Állítás. *Tetszőleges $a, b, q \in \mathbf{Z}$ esetén*

$$\textit{ln.k.o.}(a, b) = \textit{ln.k.o.}(a - bq, b).$$

Valóban, ha $d \mid a$ és $d \mid b$, akkor $d \mid a - bq$. Speciálisan , d helyére ln.k.o.(a, b)-t írva kapjuk, hogy ln.k.o.$(a, b) \mid a - bq$ és persze ln.k.o.$(a, b) \mid b$ is. Ezért ln.k.o.$(a, b) \mid$ ln.k.o.$(a - bq, b)$,

1. Állítás. *Tetszőleges* $a, b, q \in \mathbf{Z}$ *esetén*

$$\textit{ln.k.o.}(a,b) = \textit{ln.k.o.}(a-bq,b).$$

Valóban, ha $d \mid a$ és $d \mid b$, akkor $d \mid a - bq$. Speciálisan , d helyére ln.k.o.(a,b)-t írva kapjuk, hogy ln.k.o.$(a,b) \mid a - bq$ és persze ln.k.o.$(a,b) \mid b$ is. Ezért ln.k.o.$(a,b) \mid$ ln.k.o.$(a-bq,b)$, **tetszőleges** q-ra.

1. Állítás. *Tetszőleges* $a, b, q \in \mathbf{Z}$ *esetén*

$$\textit{ln.k.o.}(a, b) = \textit{ln.k.o.}(a - bq, b).$$

Valóban, ha $d \mid a$ és $d \mid b$, akkor $d \mid a - bq$. Speciálisan , d helyére ln.k.o.(a, b)-t írva kapjuk, hogy ln.k.o.$(a, b) \mid a - bq$ és persze ln.k.o.$(a, b) \mid b$ is. Ezért ln.k.o.$(a, b) \mid$ ln.k.o.$(a - bq, b)$, **tetszőleges** q-ra. Tehát q nem csak a hányados lehet!

Vegyük észre, hogy

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val)

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a =$

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) =$

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$.

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll:

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a - bq, b)$ | ln.k.o.(a, b).

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a - bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a - bq, b)$.

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a - bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a - bq, b)$.

Az állítás birtokában a tétel könnyen következik, Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a-bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a-bq, b)$.

Az állítás birtokában a tétel könnyen következik, ugyanis ha q az osztás hányadosát jelöli, akkor $a-pq = r$ éppen a maradék. Tehát az $a = bq + r$ maradékos osztás esetén ln.k.o.$(a, b) =$ ln.k.o.(b, r).

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a - bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a - bq, b)$.

Az állítás birtokában a tétel könnyen következik, ugyanis ha q az osztás hányadosát jelöli, akkor $a - pq = r$ éppen a maradék. Tehát az $a = bq + r$ maradékos osztás esetén ln.k.o.$(a, b) =$ ln.k.o.(b, r). Ezt a formulát balról jobbra alkalmazva:

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a-bq, b)$ | ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a-bq, b)$.

Az állítás birtokában a tétel könnyen következik, ugyanis ha q az osztás hányadosát jelöli, akkor $a - pq = r$ éppen a maradék. Tehát az $a = bq + r$ maradékos osztás esetén ln.k.o.$(a, b) =$ ln.k.o.(b, r). Ezt a formulát balról jobbra alkalmazva: az (osztandó, osztó) pár helyét átveszi az (osztó, maradék) pár, Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a-bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a-bq, b)$.

Az állítás birtokában a tétel könnyen következik, ugyanis ha q az osztás hányadosát jelöli, akkor $a-pq = r$ éppen a maradék. Tehát az $a = bq + r$ maradékos osztás esetén ln.k.o.$(a, b) =$ ln.k.o.(b, r). Ezt a formulát balról jobbra alkalmazva: az (osztandó, osztó) pár helyét átveszi az (osztó, maradék) pár, és a tétel szerint ezt a lépést kell ismételgetni.

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a - bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a - bq, b)$.

Az állítás birtokában a tétel könnyen következik, ugyanis ha q az osztás hányadosát jelöli, akkor $a - pq = r$ éppen a maradék. Tehát az $a = bq + r$ maradékos osztás esetén ln.k.o.$(a, b) =$ ln.k.o.(b, r). Ezt a formulát balról jobbra alkalmazva: az (osztandó, osztó) pár helyét átveszi az (osztó, maradék) pár, és a tétel szerint ezt a lépést kell ismételgetni. Mivel ln.k.o.$(x, 0) = x$,

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a - bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a - bq, b)$.

Az állítás birtokában a tétel könnyen következik, ugyanis ha q az osztás hányadosát jelöli, akkor $a - pq = r$ éppen a maradék. Tehát az $a = bq + r$ maradékos osztás esetén ln.k.o.$(a, b) =$ ln.k.o.(b, r). Ezt a formulát balról jobbra alkalmazva: az (osztandó, osztó) pár helyét átveszi az (osztó, maradék) pár, és a tétel szerint ezt a lépést kell ismételgetni. Mivel ln.k.o.$(x, 0) = x$, látható, hogy a legutolsó osztó,

Vegyük észre, hogy amilyen módon az $(a', b') := (a - bq, b)$ párt kaptuk az (a, b) párból, ugyanolyan módon (csak ellentétes előjelű q-val) adódik az (a, b) pár az (a', b') párból, hiszen $a = (a - bq) - b(-q) = a' - b'(-q)$. Ezért a fentiek szerint a fordított oszthatóság is fennáll: ln.k.o.$(a - bq, b) \mid$ ln.k.o.(a, b). De az oszthatóság az $\mathbf{N}_0$ halmazon antiszimmetrikus, és így ln.k.o.$(a, b) =$ ln.k.o.$(a - bq, b)$.

Az állítás birtokában a tétel könnyen következik, ugyanis ha q az osztás hányadosát jelöli, akkor $a - pq = r$ éppen a maradék. Tehát az $a = bq + r$ maradékos osztás esetén ln.k.o.$(a, b) =$ ln.k.o.(b, r). Ezt a formulát balról jobbra alkalmazva: az (osztandó, osztó) pár helyét átveszi az (osztó, maradék) pár, és a tétel szerint ezt a lépést kell ismételgetni. Mivel ln.k.o.$(x, 0) = x$, látható, hogy a legutolsó osztó, ami éppen az utolsó nemzérus maradék, a keresett legnagyobb közös osztó. Q.e.d.

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke.

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \leq r < b$, hanem azt, hogy $|r| \leq b/2$.

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \leq r < b$, hanem azt, hogy $|r| \leq b/2$. Azt is felhasználhatjuk, hogy a legnagyobb közös osztó

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \leq r < b$, hanem azt, hogy $|r| \leq b/2$. Azt is felhasználhatjuk, hogy a legnagyobb közös osztó „érzéketlen az előjelre”, azaz $\text{ln.k.o.}(x, y) = \text{ln.k.o.}(x, -y)$, tehát a

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \leq r < b$, hanem azt, hogy $|r| \leq b/2$. Azt is felhasználhatjuk, hogy a legnagyobb közös osztó „érzéketlen az előjelre”, azaz $\text{ln.k.o.}(x, y) = \text{ln.k.o.}(x, -y)$, tehát a maradék helyett (

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \leq r < b$, hanem azt, hogy $|r| \leq b/2$. Azt is felhasználhatjuk, hogy a legnagyobb közös osztó „érzéketlen az előjelre”, azaz ln.k.o.$(x, y) =$ ln.k.o.$(x, -y)$, tehát a maradék helyett (ha az negatív) az

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \le r < b$, hanem azt, hogy $|r| \le b/2$. Azt is felhasználhatjuk, hogy a legnagyobb közös osztó „érzéketlen az előjelre", azaz ln.k.o.$(x, y) =$ ln.k.o.$(x, -y)$, tehát a maradék helyett (ha az negatív) az abszolút értékét is vehetjük.

A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \leq r < b$, hanem azt, hogy $|r| \leq b/2$. Azt is felhasználhatjuk, hogy a legnagyobb közös osztó „érzéketlen az előjelre", azaz ln.k.o.$(x, y) =$ ln.k.o.$(x, -y)$, tehát a maradék helyett (ha az negatív) az abszolút értékét is vehetjük. Ha ezt az utat követjük, A bizonyítás közben megfogalmazott állításból könnyen látható, hogy az euklideszi algoritmus **gyorsítható** oly módon, hogy az osztás során negatív maradékot is megengedünk annak érdekében, hogy minél kisebb legyen a maradék abszolút értéke. Ilyenkor nem azt követeljük meg, hogy $0 \leq r < b$, hanem azt, hogy $|r| \leq b/2$. Azt is felhasználhatjuk, hogy a legnagyobb közös osztó „érzéketlen az előjelre”, azaz ln.k.o.$(x, y) =$ ln.k.o.$(x, -y)$, tehát a maradék helyett (ha az negatív) az abszolút értékét is vehetjük. Ha ezt az utat követjük, általában hamarabb megkapjuk a legnagyobb közös osztót.

Példa: Számítsuk ki az $a = 12209$ és a $b = 6264$ legnagyobb közös osztóját az (eredeti) euklideszi algoritmussal, továbbá annak gyorsított változatával is!

Az euklideszi algoritmussal:

$$12209 = 6264$$

Az euklideszi algoritmussal:

$$12209 = 6264 \cdot 1 +$$

Az euklideszi algoritmussal:

$$12209 = 6264 \cdot 1 + 5945,$$
$$6264 = 5945$$

Az euklideszi algoritmussal:

$$12209 = 6264 \cdot 1 + 5945,$$
$$6264 = 5945 \cdot 1 +$$

Az euklideszi algoritmussal:

$$\begin{aligned} 12209 &= 6264 \cdot 1 + 5945, \\ 6264 &= 5945 \cdot 1 + 319, \\ 5945 &= 319 \end{aligned}$$

Az euklideszi algoritmussal:

$$\begin{aligned} 12209 &= 6264 \cdot 1 + 5945, \\ 6264 &= 5945 \cdot 1 + 319, \\ 5945 &= 319 \cdot 18 + \end{aligned}$$

Az euklideszi algoritmussal:

$$\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203
\end{aligned}$$

Az euklideszi algoritmussal:

$$
\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203 \cdot 1 +
\end{aligned}
$$

Az euklideszi algoritmussal:

$$\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203 \cdot 1 + 116, \\
203 &= 116
\end{aligned}$$

Az euklideszi algoritmussal:

$$
\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203 \cdot 1 + 116, \\
203 &= 116 \cdot 1 +
\end{aligned}
$$

Az euklideszi algoritmussal:

$$\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203 \cdot 1 + 116, \\
203 &= 116 \cdot 1 + 87, \\
116 &= 87
\end{aligned}$$

Az euklideszi algoritmussal:

$$12209 = 6264 \cdot 1 + 5945,$$
$$6264 = 5945 \cdot 1 + 319,$$
$$5945 = 319 \cdot 18 + 203,$$
$$319 = 203 \cdot 1 + 116,$$
$$203 = 116 \cdot 1 + 87,$$
$$116 = 87 \cdot 1 +$$

Az euklideszi algoritmussal:

$$\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203 \cdot 1 + 116, \\
203 &= 116 \cdot 1 + 87, \\
116 &= 87 \cdot 1 + 29, \\
87 &= 29
\end{aligned}$$

Az euklideszi algoritmussal:

$$
\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203 \cdot 1 + 116, \\
203 &= 116 \cdot 1 + 87, \\
116 &= 87 \cdot 1 + 29, \\
87 &= 29 \cdot 3
\end{aligned}
$$

Az euklideszi algoritmussal:

$$\begin{aligned}
12209 &= 6264 \cdot 1 + 5945, \\
6264 &= 5945 \cdot 1 + 319, \\
5945 &= 319 \cdot 18 + 203, \\
319 &= 203 \cdot 1 + 116, \\
203 &= 116 \cdot 1 + 87, \\
116 &= 87 \cdot 1 + 29, \\
87 &= 29 \cdot 3.
\end{aligned}$$

Az euklideszi algoritmussal:

$$\begin{aligned}12209 &= 6264 \cdot 1 + 5945,\\ 6264 &= 5945 \cdot 1 + 319,\\ 5945 &= 319 \cdot 18 + 203,\\ 319 &= 203 \cdot 1 + 116,\\ 203 &= 116 \cdot 1 + 87,\\ 116 &= 87 \cdot 1 + 29,\\ 87 &= 29 \cdot 3.\end{aligned}$$

Tehát a hetedik lépésben megtudtuk, hogy ln.k.o.$(a, b) = 29$.

A gyorsított euklideszi algoritmussal:

$$12209 = 6264$$

A gyorsított euklideszi algoritmussal:

$$12209 = 6264 \cdot 2 -$$

A gyorsított euklideszi algoritmussal:

$$12209 = 6264 \cdot 2 - 319,$$
$$6264 = 319$$

A gyorsított euklideszi algoritmussal:

$$\begin{aligned}12209 &= 6264 \cdot 2 - 319,\\ 6264 &= 319 \cdot 20\end{aligned}$$

A gyorsított euklideszi algoritmussal:

$$
\begin{aligned}
12209 &= 6264 \cdot 2 - 319,\\
6264 &= 319 \cdot 20 - 116,\\
319 &= 116
\end{aligned}
$$

A gyorsított euklideszi algoritmussal:

$$\begin{aligned} 12209 &= 6264 \cdot 2 - 319, \\ 6264 &= 319 \cdot 20 - 116, \\ 319 &= 116 \cdot 3 - \end{aligned}$$

A gyorsított euklideszi algoritmussal:

$$
\begin{aligned}
12209 &= 6264 \cdot 2 - 319, \\
6264 &= 319 \cdot 20 - 116, \\
319 &= 116 \cdot 3 - 29, \\
116 &= 29
\end{aligned}
$$

A gyorsított euklideszi algoritmussal:

$$12209 = 6264 \cdot 2 - 319,$$
$$6264 = 319 \cdot 20 - 116,$$
$$319 = 116 \cdot 3 - 29,$$
$$116 = 29 \cdot 4$$

A gyorsított euklideszi algoritmussal:

$$12209 = 6264 \cdot 2 - 319,$$
$$6264 = 319 \cdot 20 - 116,$$
$$319 = 116 \cdot 3 - 29,$$
$$116 = 29 \cdot 4.$$

M

A gyorsított euklideszi algoritmussal:

$$12209 = 6264 \cdot 2 - 319,$$
$$6264 = 319 \cdot 20 - 116,$$
$$319 = 116 \cdot 3 - 29,$$
$$116 = 29 \cdot 4.$$

Most négy lépésben kaptuk, hogy ln.k.o.$(a, b) = 29$.

Mennyire gyors a gyorsított euklideszi algoritmus?

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken.

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b, \ \ldots,$

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \le b/2 = 2^{-1}b$, $r_2 \le r_1/2 \le 2^{-2}b$, ..., $r_n \le r_{n-1}/2 \le 2^{-(n-1)}b/2 = 2^{-n}b$.

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \le b/2 = 2^{-1}b$, $r_2 \le r_1/2 \le 2^{-2}b$, $\ldots$, $r_n \le r_{n-1}/2 \le 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő'' osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, ..., $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, ..., $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő" osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, ..., $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (lelogaritmizálva) $n > \log_2 b$, Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, $\ldots$, $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (lelogaritmizálva) $n > \log_2 b$, akkor $r_n < 1$, azaz

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, ..., $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (lelogaritmizálva) $n > \log_2 b$, akkor $r_n < 1$, azaz $r_n = 0$. Tehát a gyorsított algoritmus legkésőbb $[\log_2 b] + 1$ lépésben véget ér!

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő" osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, ..., $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (lelogaritmizálva) $n > \log_2 b$, akkor $r_n < 1$, azaz $r_n = 0$. Tehát a gyorsított algoritmus legkésőbb $[\log_2 b] + 1$ lépésben véget ér!

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, ..., $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (lelogaritmizálva) $n > \log_2 b$, akkor $r_n < 1$, azaz $r_n = 0$. Tehát a gyorsított algoritmus legkésőbb $[\log_2 b] + 1$ lépésben véget ér!

A gyorsított algoritmus sebességének érzékeltetésére megemlítjük, hogy ha

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b$, ..., $r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (lelogaritmizálva) $n > \log_2 b$, akkor $r_n < 1$, azaz $r_n = 0$. Tehát a gyorsított algoritmus legkésőbb $[\log_2 b] + 1$ lépésben véget ér!

A gyorsított algoritmus sebességének érzékeltetésére megemlítjük, hogy ha a és b közül a kisebbik szám háromszáz számjegyű —

Mennyire gyors a gyorsított euklideszi algoritmus? Mivel mindig a maradék „lép elő” osztóvá, az osztó (a két kezdeti szám közül a nem nagyobbik) abszolút értéke minden lépésben a felére, vagy még annál is kisebbre csökken. Tehát $r_1 \leq b/2 = 2^{-1}b$, $r_2 \leq r_1/2 \leq 2^{-2}b, \ldots, r_n \leq r_{n-1}/2 \leq 2^{-(n-1)}b/2 = 2^{-n}b$. De ugyanakkor r_n egész szám, tehát ha $2^{-n}b < 1$, azaz ha $2^n > b$, azaz ha (lelogaritmizálva) $n > \log_2 b$, akkor $r_n < 1$, azaz $r_n = 0$. Tehát a gyorsított algoritmus legkésőbb $[\log_2 b] + 1$ lépésben véget ér!

A gyorsított algoritmus sebességének érzékeltetésére megemlítjük, hogy ha a és b közül a kisebbik szám háromszáz számjegyű — pl. a korábban felírt szám —, akkor a gyorsított algoritmus legfeljebb

$$1 + \log_2 10^{300} =$$

$$1 + \log_2 10^{300} = 1 + 300 \log_2 10 \approx 1 + 300 \cdot 3,321928095 \approx 998$$

lépésben lefut.

$$1 + \log_2 10^{300} = 1 + 300 \log_2 10 \approx 1 + 300 \cdot 3,321928095 \approx 998$$

lépésben lefut. Ennek fényében nem meglepő, hogy a Maple V (egy átlagos mai számítógépen) egy háromszáz- és egy négyszázjegyű szám legnagyobb közös osztóját egy másodpercen belül kiszámítja,

$$1 + \log_2 10^{300} = 1 + 300 \log_2 10 \approx 1 + 300 \cdot 3,321928095 \approx 998$$

lépésben lefut. Ennek fényében nem meglepő, hogy a Maple V (egy átlagos mai számítógépen) egy háromszáz- és egy négyszázjegyű szám legnagyobb közös osztóját egy másodpercen belül kiszámítja, annak ellenére, hogy évmilliárdok alatt sem tudná az adott számokat prímtényezőkre bontani.

$$1+\log_2 10^{300} = 1+300\log_2 10 \approx 1+300\cdot 3,321928095 \approx 998$$

lépésben lefut. Ennek fényében nem meglepő, hogy a Maple V (egy átlagos mai számítógépen) egy háromszáz- és egy négyszázjegyű szám legnagyobb közös osztóját egy másodpercen belül kiszámítja, annak ellenére, hogy évmilliárdok alatt sem tudná az adott számokat prímtényezőkre bontani.

A fentieknek is köze van a nyilvános kulcsú titkosírások elméletéhez.

A következő tétel első két állítása az euklideszi algoritmus következménye.

16. Tétel. *(A) Bármely két egész számnak van legnagyobb közös osztója.*

16. Tétel. *(A) Bármely két egész számnak van legnagyobb közös osztója.*

(B) Ha $a, b \in \mathbf{Z}$, akkor van olyan $u, v \in \mathbf{Z}$, hogy

$$\textit{ln.k.o.}(a, b) = ua + vb.$$

16. Tétel. *(A) Bármely két egész számnak van legnagyobb közös osztója.*

(B) Ha $a, b \in \mathbf{Z}$*, akkor van olyan* $u, v \in \mathbf{Z}$*, hogy*

$$\textit{ln.k.o.}(a, b) = ua + vb.$$

(C) Ha $a, b, c \in \mathbf{Z}$*, akkor* $\textit{ln.k.o.}(ca, cb) = |c|\textit{ln.k.o.}(a, b)$*,*

16. Tétel. *(A) Bármely két egész számnak van legnagyobb közös osztója.*

(B) Ha $a, b \in \mathbf{Z}$*, akkor van olyan* $u, v \in \mathbf{Z}$*, hogy*

$$\textit{ln.k.o.}(a, b) = ua + vb.$$

(C) Ha $a, b, c \in \mathbf{Z}$*, akkor* $\textit{ln.k.o.}(ca, cb) = |c|\textit{ln.k.o.}(a, b)$*, azaz a legnagyobb közös osztó képzésekor a közös tényező kiemelhető.*

16. Tétel. *(A) Bármely két egész számnak van legnagyobb közös osztója.*

(B) Ha $a, b \in \mathbf{Z}$*, akkor van olyan* $u, v \in \mathbf{Z}$*, hogy*

$$\textit{ln.k.o.}(a, b) = ua + vb.$$

(C) Ha $a, b, c \in \mathbf{Z}$*, akkor* $\textit{ln.k.o.}(ca, cb) = |c|\textit{ln.k.o.}(a, b)$*, azaz a legnagyobb közös osztó képzésekor a közös tényező kiemelhető.*

(D) Ha $a, b \in \mathbf{Z}$ *és* $\{a, b\} \neq \{0\}$*, akkor*

$$\textit{ln.k.o.}\Big(\frac{a}{\textit{ln.k.o.}(a, b)}, \ \frac{b}{\textit{ln.k.o.}(a, b)}\Big) = 1.$$

Egészen pontatlanul fogalmazva a (B) részt: két szám legnagyobb közös osztója előáll a két szám „lineáris kombinációjaként”.

Egészen pontatlanul fogalmazva a (B) részt: két szám legnagyobb közös osztója előáll a két szám „lineáris kombinációjaként”. Ez a megfogalmazás azért helytelen, mert lineáris kombinációról csak vektorterek esetében beszélhetünk, itt

Egészen pontatlanul fogalmazva a (B) részt: két szám legnagyobb közös osztója előáll a két szám „lineáris kombinációjaként”. Ez a megfogalmazás azért helytelen, mert lineáris kombinációról csak vektorterek esetében beszélhetünk, itt pedig nincs vektortér. A (B) rész bizonyítására később, a diofantoszi egyenlet megoldásánál is szükségünk lesz.

Bizonyítás: Az (A) rész az euklideszi algoritmus kivitelezhetőségéből következik.

Egészen pontatlanul fogalmazva a (B) részt: két szám legnagyobb közös osztója előáll a két szám „lineáris kombinációjaként”. Ez a megfogalmazás azért helytelen, mert lineáris kombinációról csak vektorterek esetében beszélhetünk, itt pedig nincs vektortér. A (B) rész bizonyítására később, a diofantoszi egyenlet megoldásánál is szükségünk lesz.

Bizonyítás: Az (A) rész az euklideszi algoritmus kivitelezhetőségéből következik. A (B) rész bizonyításához idézzük fel, hogy az euklideszi algoritmus végén éppen r_n a legnagyobb közös osztó, majd vegyük észre, hogy az r_1, r_2, r_3, ... maradékok rendre kifejezhetők az a és b „lineáris kombinációjaként”:

$$a = bq_1 + r_1,$$

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2,
\end{aligned}
$$

$$a = bq_1 + r_1,$$
$$b = r_1 q_2 + r_2,$$
$$r_1 = r_2 q_3 + r_3,$$

$$
\begin{gathered}
a = bq_1 + r_1, \\
b = r_1 q_2 + r_2, \\
r_1 = r_2 q_3 + r_3, \\
\cdots
\end{gathered}
$$

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\cdots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen

$$
\begin{aligned}
a &= bq_1 + r_1,\\
b &= r_1 q_2 + r_2,\\
r_1 &= r_2 q_3 + r_3,\\
&\cdots\\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (

$$
\begin{aligned}
a &= bq_1 + r_1,\\
b &= r_1 q_2 + r_2,\\
r_1 &= r_2 q_3 + r_3,\\
&\dots\\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$).

$$
\begin{aligned}
a &= bq_1 + r_1,\\
b &= r_1 q_2 + r_2,\\
r_1 &= r_2 q_3 + r_3,\\
&\dots\\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\dots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 =$

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\dots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) =$

$$a = bq_1 + r_1,$$
$$b = r_1 q_2 + r_2,$$
$$r_1 = r_2 q_3 + r_3,$$
$$\dots$$
$$r_{i-2} = r_{i-1} q_i + r_i,$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú.

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\dots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\dots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből

$$a = bq_1 + r_1,$$
$$b = r_1 q_2 + r_2,$$
$$r_1 = r_2 q_3 + r_3,$$
$$\dots$$
$$r_{i-2} = r_{i-1} q_i + r_i,$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből $r_i = r_{i-2} - q_i r_{i-1} =$

$$
\begin{aligned}
a &= bq_1 + r_1,\\
b &= r_1 q_2 + r_2,\\
r_1 &= r_2 q_3 + r_3,\\
&\dots\\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből $r_i = r_{i-2} - q_i r_{i-1} = u_{i-2}a + v_{i-2}b - q_i(u_{i-1}a + v_{i-1}b) =$

$$a = bq_1 + r_1,$$
$$b = r_1 q_2 + r_2,$$
$$r_1 = r_2 q_3 + r_3,$$
$$\dots$$
$$r_{i-2} = r_{i-1} q_i + r_i,$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből $r_i = r_{i-2} - q_i r_{i-1} = u_{i-2} a + v_{i-2} b - q_i(u_{i-1} a + v_{i-1} b) = (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b$

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\dots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből $r_i = r_{i-2} - q_i r_{i-1} = u_{i-2} a + v_{i-2} b - q_i(u_{i-1} a + v_{i-1} b) = (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b$ alakú, azaz $u_i a + v_i b$ alakú.

$$
\begin{aligned}
a &= bq_1 + r_1,\\
b &= r_1 q_2 + r_2,\\
r_1 &= r_2 q_3 + r_3,\\
&\dots\\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből $r_i = r_{i-2} - q_i r_{i-1} = u_{i-2}a + v_{i-2}b - q_i(u_{i-1}a + v_{i-1}b) = (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b$ alakú, azaz $u_i a + v_i b$ alakú. Ez az utolsó

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\dots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből $r_i = r_{i-2} - q_i r_{i-1} = u_{i-2} a + v_{i-2} b - q_i(u_{i-1} a + v_{i-1} b) = (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b$ alakú, azaz $u_i a + v_i b$ alakú. Ez az utolsó nemzérus maradékra,

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1 q_2 + r_2, \\
r_1 &= r_2 q_3 + r_3, \\
&\dots \\
r_{i-2} &= r_{i-1} q_i + r_i,
\end{aligned}
$$

Innen $r_1 = 1 \cdot a - q_1 b$, azaz $r_1 = u_1 a + v_1 b$ alakú (ahol $u_1 = 1$, $v_1 = -q_1$). A második egyenlőségből $r_2 = b - q_2 r_1 = b - q_2(u_1 a + v_1 b) = (-q_2 u_1)a + (1 - v_1 q_2)b = u_2 a + v_2 b$ alakú. És így tovább. Ha már tudjuk, hogy $j < i$-re $r_j = u_j a + v_j b$ alakú, akkor az i-edik egyenlőségből $r_i = r_{i-2} - q_i r_{i-1} = u_{i-2}a + v_{i-2}b - q_i(u_{i-1}a + v_{i-1}b) = (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b$ alakú, azaz $u_i a + v_i b$ alakú. Ez az utolsó nemzérus maradékra, azaz a legnagyobb közös osztóra is érvényes.

(C) Jelölje ln.k.o.(a, b)-t d.

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d =$

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú.

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető.

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua+vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$.

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek,

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua+vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor — mivel az összeg mindkét tagját osztja —

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua+vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor — mivel az összeg mindkét tagját osztja — $g \mid u(ca) + v(cb) =$

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua+vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor — mivel az összeg mindkét tagját osztja — $g \mid u(ca) + v(cb) = c(ua + vb) =$

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua+vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor — mivel az összeg mindkét tagját osztja — $g \mid u(ca) + v(cb) = c(ua + vb) = cd$.

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor — mivel az összeg mindkét tagját osztja — $g \mid u(ca) + v(cb) = c(ua + vb) = cd$. Ezért ca és cb legnagyobb közös osztója $cd = c$ln.k.o.(a, b),

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua + vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor — mivel az összeg mindkét tagját osztja — $g \mid u(ca) + v(cb) = c(ua + vb) = cd$. Ezért ca és cb legnagyobb közös osztója $cd = c$ln.k.o.(a, b), azaz (C) teljesül.

(C) Jelölje ln.k.o.(a, b)-t d. Tudjuk, hogy $d = ua+vb$ alakú. Mivel az előjel oszthatósági kérdéseknél lényegtelen, $c > 0$ feltehető. Mivel $d \mid a$ és $d \mid b$, ezért $cd \mid ca$ és $cd \mid cb$. Azaz, cd közös osztója ca-nak és cb-nek.

Ha g is közös osztója ca-nak és cb-nek, akkor — mivel az összeg mindkét tagját osztja — $g \mid u(ca) + v(cb) = c(ua + vb) = cd$. Ezért ca és cb legnagyobb közös osztója $cd = c$ln.k.o.(a, b), azaz (C) teljesül.

(D) Legyen $d = \text{ln.k.o.}(a, b)$,

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0.

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \dfrac{a}{d}$,

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$.

(D) Legyen $d =$ ln.k.o.(a, b), ez nyilván nem 0. $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$.
Ezen jelölések mellett azt kell belátnunk, hogy

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$.
Ezen jelölések mellett azt kell belátnunk, hogy $\text{ln.k.o.}(a_1, b_1) = 1$.

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$.
Ezen jelölések mellett azt kell belátnunk, hogy $\text{ln.k.o.}(a_1, b_1) = 1$.
A már igazolt

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$.
Ezen jelölések mellett azt kell belátnunk, hogy $\text{ln.k.o.}(a_1, b_1) = 1$.
A már igazolt (C) szerint

$$d = \text{ln.k.o.}(a, b) =$$

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$.
Ezen jelölések mellett azt kell belátnunk, hogy $\text{ln.k.o.}(a_1, b_1) = 1$.
A már igazolt (C) szerint

$$d = \text{ln.k.o.}(a, b) = \text{ln.k.o.}(da_1, db_1) = d \cdot \text{ln.k.o.}(a_1, b_1).$$

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$.
Ezen jelölések mellett azt kell belátnunk, hogy $\text{ln.k.o.}(a_1, b_1) = 1$.
A már igazolt (C) szerint

$$d = \text{ln.k.o.}(a, b) = \text{ln.k.o.}(da_1, db_1) = d \cdot \text{ln.k.o.}(a_1, b_1).$$

d-vel egyszerűsítve a kívánt

$$1 = \text{ln.k.o.}(a_1, b_1) = \text{ln.k.o.}\left(\frac{a}{\text{ln.k.o.}(a, b)}, \frac{b}{\text{ln.k.o.}(a, b)}\right)$$

adódik.

(D) Legyen $d = \text{ln.k.o.}(a, b)$, ez nyilván nem 0. $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$.
Ezen jelölések mellett azt kell belátnunk, hogy $\text{ln.k.o.}(a_1, b_1) = 1$.
A már igazolt (C) szerint

$$d = \text{ln.k.o.}(a, b) = \text{ln.k.o.}(da_1, db_1) = d \cdot \text{ln.k.o.}(a_1, b_1).$$

d-vel egyszerűsítve a kívánt

$$1 = \text{ln.k.o.}(a_1, b_1) = \text{ln.k.o.}\left(\frac{a}{\text{ln.k.o.}(a, b)}, \frac{b}{\text{ln.k.o.}(a, b)}\right)$$

adódik. Q.e.d.

2. Következmény. *Tegyük fel, hogy* $a, b \in \mathbf{Z}$ **relatív prímek**,

2. Következmény. *Tegyük fel, hogy* $a, b \in \mathbf{Z}$ **relatív prímek**, *azaz olyan egész számok, hogy* ln.k.o.$(a, b) = 1$. *Ekkor tetszőleges* $c \in \mathbf{Z}$*-re*

2. Következmény. *Tegyük fel, hogy* $a, b \in \mathbf{Z}$ **relatív prímek**, *azaz olyan egész számok, hogy ln.k.o.*$(a, b) = 1$. *Ekkor tetszőleges* $c \in \mathbf{Z}$*-re*

(A) Ha $a \mid bc$*, akkor* $a \mid c$*;*

2. Következmény. *Tegyük fel, hogy* $a, b \in \mathbf{Z}$ **relatív prímek**, *azaz olyan egész számok, hogy* ln.k.o.$(a, b) = 1$. *Ekkor tetszőleges* $c \in \mathbf{Z}$*-re*

(A) Ha $a \mid bc$, *akkor* $a \mid c$;

(B) Ha $a \mid c$ *és* $b \mid c$, *akkor* $ab \mid c$.

A középiskolai ismeretek —

2. Következmény. *Tegyük fel, hogy* $a, b \in \mathbf{Z}$ **relatív prímek**, *azaz olyan egész számok, hogy* ln.k.o.$(a, b) = 1$. *Ekkor tetszőleges* $c \in \mathbf{Z}$*-re*

(A) Ha $a \mid bc$, *akkor* $a \mid c$;

(B) Ha $a \mid c$ *és* $b \mid c$, *akkor* $ab \mid c$.

A középiskolai ismeretek — nevezetesen a prímtényezős felbontás —

2. Következmény. *Tegyük fel, hogy* $a, b \in \mathbf{Z}$ **relatív prímek**, *azaz olyan egész számok, hogy ln.k.o.*$(a, b) = 1$. *Ekkor tetszőleges* $c \in \mathbf{Z}$*-re*

(A) Ha $a \mid bc$, *akkor* $a \mid c$;

(B) Ha $a \mid c$ *és* $b \mid c$, *akkor* $ab \mid c$.

A középiskolai ismeretek — nevezetesen a prímtényezős felbontás — alapján mindez nyilvánvaló, az viszont

2. Következmény. *Tegyük fel, hogy* $a, b \in \mathbf{Z}$ **relatív prímek**, *azaz olyan egész számok, hogy* ln.k.o.$(a, b) = 1$. *Ekkor tetszőleges* $c \in \mathbf{Z}$*-re*

(A) Ha $a \mid bc$*, akkor* $a \mid c$*;*

(B) Ha $a \mid c$ *és* $b \mid c$*, akkor* $ab \mid c$*.*

A középiskolai ismeretek — nevezetesen a prímtényezős felbontás — alapján mindez nyilvánvaló, az viszont távolról sem nyilvánvaló, hogy a prímtényezős felbontás rendelkezik a megszokott tulajdonságokkal.

Bizonyítás:

Bizonyítás: Az előző tétel szerint vannak olyan

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A):

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c =$

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c =$

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c = (ua + vb)c =$

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$.

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val,

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c = (ua + vb)c = a(uc) + (bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is.

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c = (ua + vb)c = a(uc) + (bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua + vb)c = a(uc) + (bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$.

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$.

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$. Ezért (

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb =$ ln.k.o.$(a, b) = 1$.

(A): $c = 1 \cdot c = (ua + vb)c = a(uc) + (bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$. Ezért (mivel mindkét tag osztható lesz ab-vel)

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$. Ezért (mivel mindkét tag osztható lesz ab-vel) $ab \mid uac +$

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$. Ezért (mivel mindkét tag osztható lesz ab-vel) $ab \mid uac + vbc =$

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua + vb)c = a(uc) + (bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$. Ezért (mivel mindkét tag osztható lesz ab-vel) $ab \mid uac + vbc = (ua + vb)c =$

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua+vb)c = a(uc)+(bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$. Ezért (mivel mindkét tag osztható lesz ab-vel) $ab \mid uac + vbc = (ua + vb)c = 1 \cdot c = c$,

Bizonyítás: Az előző tétel szerint vannak olyan u, v egészek, hogy $ua + vb = \text{ln.k.o.}(a, b) = 1$.

(A): $c = 1 \cdot c = (ua + vb)c = a(uc) + (bc)v$. Mivel az összeg mindkét tagja esetén az első tényező osztható a-val, ezért a összeg is. Tehát $a \mid c$.

(B) A feltevés szerint $a \mid c$, és innen $ab \mid bc$. Hasonlóan, a $b \mid c$ feltevésből $ab \mid ac$. Ezért (mivel mindkét tag osztható lesz ab-vel) $ab \mid uac + vbc = (ua + vb)c = 1 \cdot c = c$, valóban. Q.e.d.

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\textit{ln.k.o.}(a,b) \cdot \textit{lk.k.t.}(ab) = |ab|$$

összefüggés.

17. Tétel. $\mathbf{Z}$*-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha* $a, b \in \mathbf{Z}$*, akkor érvényes az*

$$\textit{ln.k.o.}(a, b) \cdot \textit{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\textit{ln.k.o.}(a, b) \cdot \textit{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\textit{ln.k.o.}(a, b) \cdot \textit{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

Bizonyítás: Ha $a = 0$, akkor

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\textit{ln.k.o.}(a,b) \cdot \textit{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

Bizonyítás: Ha $a = 0$, akkor a egyetlen többszöröse a 0,

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\textit{ln.k.o.}(a, b) \cdot \textit{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

Bizonyítás: Ha $a = 0$, akkor a egyetlen többszöröse a 0, így az a legkisebb közös többszörös is,

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse**. *Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\text{ln.k.o.}(a, b) \cdot \text{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

Bizonyítás: Ha $a = 0$, akkor a egyetlen többszöröse a 0, így az a legkisebb közös többszörös is, és egyúttal $|ab|$ is.

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\textit{ln.k.o.}(a,b) \cdot \textit{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

Bizonyítás: Ha $a = 0$, akkor a egyetlen többszöröse a 0, így az a legkisebb közös többszörös is, és egyúttal $|ab|$ is. Hasonló a helyzet akkor is, ha $b = 0$.

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse***. Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\text{ln.k.o.}(a, b) \cdot \text{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

Bizonyítás: Ha $a = 0$, akkor a egyetlen többszöröse a 0, így az a legkisebb közös többszörös is, és egyúttal $|ab|$ is. Hasonló a helyzet akkor is, ha $b = 0$. Ezért a továbbiakban feltesszük, hogy $ab \neq 0$. Mivel

17. Tétel. *$\mathbf{Z}$-ben bármely két számnak van* **legkisebb közös többszöröse**. *Ha $a, b \in \mathbf{Z}$, akkor érvényes az*

$$\text{ln.k.o.}(a,b) \cdot \text{lk.k.t.}(ab) = |ab|$$

összefüggés. Szavakban: két egész szám legnagyobb közös osztójának és legkisebb közös többszörösének szorzata a két szám szorzatának abszolút értéke.

Bizonyítás: Ha $a = 0$, akkor a egyetlen többszöröse a 0, így az a legkisebb közös többszörös is, és egyútal $|ab|$ is. Hasonló a helyzet akkor is, ha $b = 0$. Ezért a továbbiakban feltesszük, hogy $ab \neq 0$. Mivel az előjel a többszörösök szempontjából érdektelen, $a, b \in \mathbf{N}$-et is feltesszük.

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$.

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$. Legyen

t

A $d = \text{ln.k.o.}(a,b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a,b)} =$$

A $d = \text{ln.k.o.}(a,b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a,b)} = \frac{a_1 d \cdot b_1 d}{d} =$$

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1$

A $d = \text{ln.k.o.}(a,b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a,b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1 (b_1 d) = a_1 b$ többszöröse b-nek is,

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1 (b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1 (b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

Legyen most h egy tetszőleges közös többszörös.

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1 (b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

Legyen most h egy tetszőleges közös többszörös. Ekkor $a_1 d = a \mid h$ miatt

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1 (b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

Legyen most h egy tetszőleges közös többszörös. Ekkor $a_1 d = a \mid h$ miatt $a_1 \mid \frac{h}{d}$ (

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1 (b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

Legyen most h egy tetszőleges közös többszörös. Ekkor $a_1 d = a \mid h$ miatt $a_1 \mid \dfrac{h}{d}$ (ami egész szám), és

A $d = \text{ln.k.o.}(a, b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a, b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1 (b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

Legyen most h egy tetszőleges közös többszörös. Ekkor $a_1 d = a \mid h$ miatt $a_1 \mid \dfrac{h}{d}$ (ami egész szám), és ugyanígy $b_1 \mid \dfrac{h}{d}$.

A $d = \text{ln.k.o.}(a,b)$ jelöléssel legyen $a_1 = \dfrac{a}{d}$, $b_1 = \dfrac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a,b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1(b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

Legyen most h egy tetszőleges közös többszörös. Ekkor $a_1 d = a \mid h$ miatt $a_1 \mid \dfrac{h}{d}$ (ami egész szám), és ugyanígy $b_1 \mid \dfrac{h}{d}$. Korábbi tételeink szerint $\text{ln.k.o.}(a_1, b_1) = 1$ és ezért $a_1 b_1 \mid \dfrac{h}{d}$.

A $d = \text{ln.k.o.}(a,b)$ jelöléssel legyen $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Legyen

$$t = \frac{ab}{\text{ln.k.o.}(a,b)} = \frac{a_1 d \cdot b_1 d}{d} = a_1 b_1 d$$

Ki fogjuk mutatni, hogy t a legkisebb közös többszörös.

Az világos, hogy $t = (a_1 d) b_1 = a b_1$ többszöröse a-nak és $t = a_1(b_1 d) = a_1 b$ többszöröse b-nek is, tehát t közös többszörös.

Legyen most h egy tetszőleges közös többszörös. Ekkor $a_1 d = a \mid h$ miatt $a_1 \mid \frac{h}{d}$ (ami egész szám), és ugyanígy $b_1 \mid \frac{h}{d}$. Korábbi tételeink szerint $\text{ln.k.o.}(a_1, b_1) = 1$ és ezért $a_1 b_1 \mid \frac{h}{d}$. Innen

$a_1 b_1 d \mid h,$ azaz

$a_1b_1d \mid h$, azaz $t \mid h$.

$a_1 b_1 d \mid h$, azaz $t \mid h$. Tehát t a legkisebb közös többszörös.

$a_1 b_1 d \mid h$, azaz $t \mid h$. Tehát t a legkisebb közös többszörös. Q.e.d.

Az eddigiek birtokában egyszerűen kapjuk az alábbi (de nem nyilvánvaló) tényt:

3. Következmény. *A törzsszámok ugyanazok, mint a prímszámok.*

Az eddigiek birtokában egyszerűen kapjuk az alábbi (de nem nyilvánvaló) tényt:

3. Következmény. *A törzsszámok ugyanazok, mint a prímszámok.*

Emlékeztetünk arra, hogy törzsszámnak vagy irreducibilis számnak nevezzük azt az 1-nél nagyobb számot, amelynek $\mathbf{N}$-ben csak triviális osztói vannak: az 1 és önmaga.

Az eddigiek birtokában egyszerűen kapjuk az alábbi (de nem nyilvánvaló) tényt:

3. Következmény. *A törzsszámok ugyanazok, mint a prímszámok.*

Emlékeztetünk arra, hogy törzsszámnak vagy irreducibilis számnak nevezzük azt az 1-nél nagyobb számot, amelynek $\mathbf{N}$-ben csak triviális osztói vannak: az 1 és önmaga. Prímszámnak meg az olyan 1-nél nagyobb p számot nevezzük, amely ha

Az eddigiek birtokában egyszerűen kapjuk az alábbi (de nem nyilvánvaló) tényt:

3. Következmény. *A törzsszámok ugyanazok, mint a prímszámok.*

Emlékeztetünk arra, hogy törzsszámnak vagy irreducibilis számnak nevezzük azt az 1-nél nagyobb számot, amelynek $\mathbf{N}$-ben csak triviális osztói vannak: az 1 és önmaga. Prímszámnak meg az olyan 1-nél nagyobb p számot nevezzük, amely ha oszt egy szorzatot, akkor szükségképpen osztja a szorzat egyik tényezőjét.

Bizonyítás (vázlat) Legyen t törzsszám, és tegyük fel, hogy $t \mid ab$.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \ a$, akkor —

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \ a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja,

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \, a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \, a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \nmid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \, a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \nmid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$.

Bizonyítás (vázlat) Legyen t törzsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \nmid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a,t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b =$

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \ a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b =$

Bizonyítás (vázlat) Legyen t törzsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \; a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b =$

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not\mid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt

Bizonyítás (vázlat) Legyen t törzsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \; a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt $t \mid b$.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not\mid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt $t \mid b$.

Legyen most p prímszám.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \nmid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\boxed{ab} + v\boxed{t}b$ miatt $t \mid b$.

Legyen most p prímszám. Ekkor $p > 1$. Ha

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not| \ a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt $t \mid b$.

Legyen most p prímszám. Ekkor $p > 1$. Ha nem lenne törzsszám (azaz irreducibilis), akkor $p = ab$ alakú lenne, ahol

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \not\mid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a,t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt $t \mid b$.

Legyen most p prímszám. Ekkor $p > 1$. Ha nem lenne törzsszám (azaz irreducibilis), akkor $p = ab$ alakú lenne, ahol $\{a,b\} \cap \{1,p\} = \emptyset$.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \nmid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt $t \mid b$.

Legyen most p prímszám. Ekkor $p > 1$. Ha nem lenne törzsszám (azaz irreducibilis), akkor $p = ab$ alakú lenne, ahol $\{a, b\} \cap \{1, p\} = \emptyset$. Ekkor $1 < a < p$ és $1 < b < p$. Mivel p prím, $p \mid a$ vagy $p \mid b$,

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \nmid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a, t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt $t \mid b$.

Legyen most p prímszám. Ekkor $p > 1$. Ha nem lenne törzsszám (azaz irreducibilis), akkor $p = ab$ alakú lenne, ahol $\{a, b\} \cap \{1, p\} = \emptyset$. Ekkor $1 < a < p$ és $1 < b < p$. Mivel p prím, $p \mid a$ vagy $p \mid b$, de ekkor $p \le a$ vagy $p \le b$, ami ellentmondás.

Bizonyítás (vázlat) Legyen t tözsszám, és tegyük fel, hogy $t \mid ab$. Be kell látni, hogy $t \mid a$ vagy $t \mid b$. Ha $t \mid a$, akkor nincs mit bizonyítani. Ha $t \nmid a$, akkor — tekintettel arra, hogy $\mathbf{N}$-ben t-t csak az 1 és t osztja, a t és az a egyetlen közös osztója az 1. Ezért ln.k.o.$(a,t) = 1$. Így alkalmas u, v egészekre $1 = ua + vt$. Ezért $b = 1 \cdot b = (ua + vt)b = u\,ab + v\,t\,b$ miatt $t \mid b$.

Legyen most p prímszám. Ekkor $p > 1$. Ha nem lenne törzsszám (azaz irreducibilis), akkor $p = ab$ alakú lenne, ahol $\{a, b\} \cap \{1, p\} = \emptyset$. Ekkor $1 < a < p$ és $1 < b < p$. Mivel p prím, $p \mid a$ vagy $p \mid b$, de ekkor $p \leq a$ vagy $p \leq b$, ami ellentmondás. Q.e.d.

18. Tétel. *(***A számelmélet alaptétele***) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún.* **prímtényezős felbontás***) a tényezők sorrendjétől eltekintve* **egyértelmű***.*

18. Tétel. *(**A számelmélet alaptétele**) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún. **prímtényezős felbontás**) a tényezők sorrendjétől eltekintve **egyértelmű**.*

Bizonyítás (vázlat): Mivel

18. Tétel. *(**A számelmélet alaptétele**) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún. **prímtényezős felbontás**) a tényezők sorrendjétől eltekintve **egyértelmű**.*

Bizonyítás (vázlat): Mivel a prímszámok ugyanazok, mint az irreducibilis számok (törzsszámok),

18. Tétel. *(***A számelmélet alaptétele***) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún.* **prímtényezős felbontás***) a tényezők sorrendjétől eltekintve* **egyértelmű***.*

Bizonyítás (vázlat): Mivel a prímszámok ugyanazok, mint az irreducibilis számok (törzsszámok), az szinte triviális, hogy a mondott felbontás létezik.

18. Tétel. *(***A számelmélet alaptétele***) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún.* **prímtényezős felbontás***) a tényezők sorrendjétől eltekintve* **egyértelmű***.*

Bizonyítás (vázlat): Mivel a prímszámok ugyanazok, mint az irreducibilis számok (törzsszámok), az szinte triviális, hogy a mondott felbontás létezik. Ezt n, a felbontandó szám szerinti teljes indukcióval kapjuk.

18. Tétel. *(***A számelmélet alaptétele***) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún.* **prímtényezős felbontás***) a tényezők sorrendjétől eltekintve* **egyértelmű***.*

Bizonyítás (vázlat): Mivel a prímszámok ugyanazok, mint az irreducibilis számok (törzsszámok), az szinte triviális, hogy a mondott felbontás létezik. Ezt n, a felbontandó szám szerinti teljes indukcióval kapjuk. Ha $n = 1$, akkor az

18. Tétel. *(***A számelmélet alaptétele***) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún.* **prímtényezős felbontás***) a tényezők sorrendjétől eltekintve* **egyértelmű***.*

Bizonyítás (vázlat): Mivel a prímszámok ugyanazok, mint az irreducibilis számok (törzsszámok), az szinte triviális, hogy a mondott felbontás létezik. Ezt n, a felbontandó szám szerinti teljes indukcióval kapjuk. Ha $n = 1$, akkor az üresszorzat adja a kívánt felbontást.

18. Tétel. *(**A számelmélet alaptétele**) Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás (az ún. **prímtényezős felbontás**) a tényezők sorrendjétől eltekintve **egyértelmű**.*

Bizonyítás (vázlat): Mivel a prímszámok ugyanazok, mint az irreducibilis számok (törzsszámok), az szinte triviális, hogy a mondott felbontás létezik. Ezt n, a felbontandó szám szerinti teljes indukcióval kapjuk. Ha $n = 1$, akkor az üresszorzat adja a kívánt felbontást. Az indukciós lépéshez tegyük fel, hogy $n > 1$ és az n-nél kisebb számok már mind felbonthatók prímszámok szorzatára.

Ha n prímszám, akkor nyilván felbontható (

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata.

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata. Az indukciós hipotézis szerint ezen tényezők felbonthatók prímszámok szorzatára,

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata. Az indukciós hipotézis szerint ezen tényezők felbonthatók prímszámok szorzatára, ezért n is felbontható.

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata. Az indukciós hipotézis szerint ezen tényezők felbonthatók prímszámok szorzatára, ezért n is felbontható.

Az egyértelműséget szintén n szerinti teljes indukcióval látjuk be.

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata. Az indukciós hipotézis szerint ezen tényezők felbonthatók prímszámok szorzatára, ezért n is felbontható.

Az egyértelműséget szintén n szerinti teljes indukcióval látjuk be. Ha $n = 1$, akkor csak az üresszorzat állítja elő, és az egyértelműség teljesül.

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata. Az indukciós hipotézis szerint ezen tényezők felbonthatók prímszámok szorzatára, ezért n is felbontható.

Az egyértelműséget szintén n szerinti teljes indukcióval látjuk be. Ha $n = 1$, akkor csak az üresszorzat állítja elő, és az egyértelműség teljesül. Tegyük most fel, hogy $n > 1$, de a nála kisebb számok esetében az egyértelmű prímfelbontást már igazoltuk.

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata. Az indukciós hipotézis szerint ezen tényezők felbonthatók prímszámok szorzatára, ezért n is felbontható.

Az egyértelműséget szintén n szerinti teljes indukcióval látjuk be. Ha $n = 1$, akkor csak az üresszorzat állítja elő, és az egyértelműség teljesül. Tegyük most fel, hogy $n > 1$, de a nála kisebb számok esetében az egyértelmű prímfelbontást már igazoltuk. Tegyük fel, hogy

Ha n prímszám, akkor nyilván felbontható (mint egytényezős szorzat). Ha n nem prímszám, akkor nem irreducibilis, tehát két nála kisebb tényező szorzata. Az indukciós hipotézis szerint ezen tényezők felbonthatók prímszámok szorzatára, ezért n is felbontható.

Az egyértelműséget szintén n szerinti teljes indukcióval látjuk be. Ha $n = 1$, akkor csak az üresszorzat állítja elő, és az egyértelműség teljesül. Tegyük most fel, hogy $n > 1$, de a nála kisebb számok esetében az egyértelmű prímfelbontást már igazoltuk. Tegyük fel, hogy

$$p_1 p_2 \cdots p_k$$

$$p_1 p_2 \ldots p_k = n$$

$$p_1 p_2 \dots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek.

$$p_1p_2\dots p_k = n = q_1q_2\cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is.

$$p_1 p_2 \ldots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért

$$p_1 p_2 \ldots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De

$$p_1 p_2 \dots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható.

$$p_1 p_2 \ldots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható. Ezért $p_1 = q_i$.

$$p_1 p_2 \dots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható. Ezért $p_1 = q_i$. Az egyenlőtlenséget $p_1 = q_i$-vel egyszerűsítve és az

$$p_1 p_2 \dots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható. Ezért $p_1 = q_i$. Az egyenlőtlenséget $p_1 = q_i$-vel egyszerűsítve és az indukciós hipotézist az $\frac{n}{p_1} = \frac{n}{q_i}$ számra alkalmazva kapjuk, hogy a $p_2, \dots, p_k$ prímek sorrendtől

$$p_1 p_2 \ldots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható. Ezért $p_1 = q_i$. Az egyenlőtlenséget $p_1 = q_i$-vel egyszerűsítve és az indukciós hipotézist az $\frac{n}{p_1} = \frac{n}{q_i}$ számra alkalmazva kapjuk, hogy a $p_2, \ldots, p_k$ prímek sorrendtől eltekintve megegyeznek a $q_1, \ldots, q_{i-1}$, $q_{i+1}, \ldots, q_\ell$ prímekkel

$$p_1 p_2 \dots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható. Ezért $p_1 = q_i$. Az egyenlőtlenséget $p_1 = q_i$-vel egyszerűsítve és az indukciós hipotézist az $\frac{n}{p_1} = \frac{n}{q_i}$ számra alkalmazva kapjuk, hogy a $p_2, \dots, p_k$ prímek sorrendtől eltekintve megegyeznek a $q_1, \dots, q_{i-1}$, $q_{i+1}, \dots, q_\ell$ prímekkel (mint rendszer a rendszerrel). Innen kapjuk, hogy a $\{p_1, \dots, p_k\}$ rendszer azonos a $\{q_1, \dots, q_\ell\}$ rendszerrel (

$$p_1p_2\ldots p_k = n = q_1q_2\cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható. Ezért $p_1 = q_i$. Az egyenlőtlenséget $p_1 = q_i$-vel egyszerűsítve és az indukciós hipotézist az $\dfrac{n}{p_1} = \dfrac{n}{q_i}$ számra alkalmazva kapjuk, hogy a $p_2, \ldots, p_k$ prímek sorrendtől eltekintve megegyeznek a $q_1, \ldots, q_{i-1}$, $q_{i+1}, \ldots, q_\ell$ prímekkel (mint rendszer a rendszerrel). Innen kapjuk, hogy a $\{p_1, \ldots, p_k\}$ rendszer azonos a $\{q_1, \ldots, q_\ell\}$ rendszerrel (beleértve természetesen azt is, hogy $k = \ell$).

$$p_1 p_2 \dots p_k = n = q_1 q_2 \cdots q_\ell,$$

ahol a p_i-k és a q_j-k prímek. A baloldal osztható p_1-gyel, ezért a jobboldal is. De p_1 prím, ezért osztja a jobboldal valamelyik tényezőjét, mondjuk q_i-t. De q_i irreducibilis, ezért csak 1-gyel és önmagával osztható. Ezért $p_1 = q_i$. Az egyenlőtlenséget $p_1 = q_i$-vel egyszerűsítve és az indukciós hipotézist az $\frac{n}{p_1} = \frac{n}{q_i}$ számra alkalmazva kapjuk, hogy a $p_2, \dots, p_k$ prímek sorrendtől eltekintve megegyeznek a $q_1, \dots, q_{i-1}$, $q_{i+1}, \dots, q_\ell$ prímekkel (mint rendszer a rendszerrel). Innen kapjuk, hogy a $\{p_1, \dots, p_k\}$ rendszer azonos a $\{q_1, \dots, q_\ell\}$ rendszerrel (beleértve természetesen azt is, hogy $k = \ell$). Q.e.d.

A prímtényezős felbontásban a többször fellépő prímek szorzata helyett prímhatványokat írva

A prímtényezős felbontásban a többször fellépő prímek szorzata helyett prímhatványokat írva kapjuk a **prímhatvány felbontást:**

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

ahol a p_i-k páronként **különböző** prímek, és az α_i kitevők pozitív egész számok.

A prímtényezős felbontásban a többször fellépő prímek szorzata helyett prímhatványokat írva kapjuk a **prímhatvány felbontást:**

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

ahol a p_i-k páronként **különböző** prímek, és az α_i kitevők pozitív egész számok. A számelmélet alaptétele szerint ez a felbontás is egyértelmű. (

A prímtényezős felbontásban a többször fellépő prímek szorzata helyett prímhatványokat írva kapjuk a **prímhatvány felbontást:**

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

ahol a p_i-k páronként **különböző** prímek, és az α_i kitevők pozitív egész számok. A számelmélet alaptétele szerint ez a felbontás is egyértelmű. (A produktumban a tényezők sorrendje nem számít.)

A prímtényezős felbontásban a többször fellépő prímek szorzata helyett prímhatványokat írva kapjuk a **prímhatvány felbontást:**

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

ahol a p_i-k páronként **különböző** prímek, és az α_i kitevők pozitív egész számok. A számelmélet alaptétele szerint ez a felbontás is egyértelmű. (A produktumban a tényezők sorrendje nem számít.)

Néha megengedjük 0-t is kitevőként,

A prímtényezős felbontásban a többször fellépő prímek szorzata helyett prímhatványokat írva kapjuk a **prímhatvány felbontást:**

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

ahol a p_i-k páronként **különböző** prímek, és az α_i kitevők pozitív egész számok. A számelmélet alaptétele szerint ez a felbontás is egyértelmű. (A produktumban a tényezők sorrendje nem számít.)

Néha megengedjük 0-t is kitevőként, hiszen a $p_i^0 = 1$ tényező „nem zavarja" a szorzatot.

A prímtényezős felbontásban a többször fellépő prímek szorzata helyett prímhatványokat írva kapjuk a **prímhatvány felbontást:**

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

ahol a p_i-k páronként **különböző** prímek, és az α_i kitevők pozitív egész számok. A számelmélet alaptétele szerint ez a felbontás is egyértelmű. (A produktumban a tényezők sorrendje nem számít.)

Néha megengedjük 0-t is kitevőként, hiszen a $p_i^0 = 1$ tényező „nem zavarja" a szorzatot. Ennek az az előnye, hogy ily módon bármely két pozitív egész szám **ugyanazon** prímek nemnegatív egész kitevős hatványainak szorzataként írható fel.

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \textit{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$.

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$. *Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\})\,(\alpha_i \leq \beta_i),$$

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{\textit{és}} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$*. Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\})\,(\alpha_i \leq \beta_i),$$

$$\text{\textit{ln.k.o.}}(m, n) =$$

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$*. Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\})\,(\alpha_i \leq \beta_i),$$

$$\text{ln.k.o.}(m, n) = \prod_{i=1}^{k} p$$

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$. *Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\})\,(\alpha_i \leq \beta_i),$$

$$\text{ln.k.o.}(m, n) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)},$$

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \textit{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$. *Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\}) \, (\alpha_i \leq \beta_i),$$

$$\textit{ln.k.o.}(m, n) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)},$$

$$\textit{lk.k.t.}(m, n) =$$

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \textit{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$. *Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\})\,(\alpha_i \le \beta_i),$$

$$\textit{ln.k.o.}(m, n) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)},$$

$$\textit{lk.k.t.}(m, n) = \prod_{i=1}^{k} p$$

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \textit{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$. *Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\})\,(\alpha_i \leq \beta_i),$$

$$\textit{ln.k.o.}(m, n) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)},$$

$$\textit{lk.k.t.}(m, n) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}.$$

19. Tétel. *Legyen*

$$m = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \textit{és} \quad n = \prod_{i=1}^{k} p_i^{\beta_i},$$

ahol $p_1, \ldots, p_k$ *páronként különböző prímek, és* $i = 1, \ldots, k$*-ra* $\alpha_i, \beta_i \in \mathbf{N}_0$. *Ekkor*

$$m \mid n \iff (\forall i \in \{1, \ldots, k\})\,(\alpha_i \leq \beta_i),$$

$$\textit{ln.k.o.}(m,n) = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)},$$

$$\textit{lk.k.t.}(m,n) = \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)}.$$

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

ln.k.o.$(a, b) =$

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

ln.k.o.$(a, b) = 2^3 \cdot 3^2 = 72$ és

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

$$\text{ln.k.o.}(a, b) = 2^3 \cdot 3^2 = 72 \text{ és } \text{lk.k.t.}(a, b) = 2^4 \cdot 3^3 \cdot 5 =$$

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

ln.k.o.$(a, b) = 2^3 \cdot 3^2 = 72$ és lk.k.t.$(a, b) = 2^4 \cdot 3^3 \cdot 5 = 2160$.

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

$$\text{ln.k.o.}(a, b) = 2^3 \cdot 3^2 = 72 \text{ és } \text{lk.k.t.}(a, b) = 2^4 \cdot 3^3 \cdot 5 = 2160.$$

A bizonyítás az előzőekre támaszkodva nem nehéz, de nem tárgyaljuk.

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

$$\text{ln.k.o.}(a,b) = 2^3 \cdot 3^2 = 72 \text{ és } \text{lk.k.t.}(a,b) = 2^4 \cdot 3^3 \cdot 5 = 2160.$$

A bizonyítás az előzőekre támaszkodva nem nehéz, de nem tárgyaljuk. A számelmélet alaptételéből (sőt anélkül is) könnyen adódik az alábbi tétel, amely Eukleidesztől származik (Euklidesz-nek is szokták írni):

20. Tétel.

Példa: Ha $a = 2^4 \cdot 3^2 = 144$ és $b = 2^3 \cdot 3^3 \cdot 5 = 1080$, akkor

$$\text{ln.k.o.}(a, b) = 2^3 \cdot 3^2 = 72 \text{ és } \text{lk.k.t.}(a, b) = 2^4 \cdot 3^3 \cdot 5 = 2160.$$

A bizonyítás az előzőekre támaszkodva nem nehéz, de nem tárgyaljuk. A számelmélet alaptételéből (sőt anélkül is) könnyen adódik az alábbi tétel, amely Eukleidesztől származik (Euklidesz-nek is szokták írni):

20. Tétel.

Végtelen sok prímszám van.

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van;

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$.

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q az $n = p_1 \ldots p_k + 1$ szám egyik prímosztóját.

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q az $n = p_1 \ldots p_k + 1$ szám egyik prímosztóját. Ilyen létezik, hiszen n is prímszámok szorzatára bontható. Ha valamely $i \in \{1, \ldots, k\}$-ra p_i osztaná n-et, akkor az $1 = n - p_1 \ldots p_k$ számot is osztaná,

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q az $n = p_1 \ldots p_k + 1$ szám egyik prímosztóját. Ilyen létezik, hiszen n is prímszámok szorzatára bontható. Ha valamely $i \in \{1, \ldots, k\}$-ra p_i osztaná n-et, akkor az $1 = n - p_1 \ldots p_k$ számot is osztaná, ami lehetetlen.

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q az $n = p_1 \ldots p_k + 1$ szám egyik prímosztóját. Ilyen létezik, hiszen n is prímszámok szorzatára bontható. Ha valamely $i \in \{1, \ldots, k\}$-ra p_i osztaná n-et, akkor az $1 = n - p_1 \ldots p_k$ számot is osztaná, ami lehetetlen. Ezért q a $p_1, \ldots, p_k$ számok (

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q az $n = p_1 \ldots p_k + 1$ szám egyik prímosztóját. Ilyen létezik, hiszen n is prímszámok szorzatára bontható. Ha valamely $i \in \{1, \ldots, k\}$-ra p_i osztaná n-et, akkor az $1 = n - p_1 \ldots p_k$ számot is osztaná, ami lehetetlen. Ezért q a $p_1, \ldots, p_k$ számok (azaz az összes prímszám) mindegyikétől különbözik, ami

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q az $n = p_1 \ldots p_k + 1$ szám egyik prímosztóját. Ilyen létezik, hiszen n is prímszámok szorzatára bontható. Ha valamely $i \in \{1, \ldots, k\}$-ra p_i osztaná n-et, akkor az $1 = n - p_1 \ldots p_k$ számot is osztaná, ami lehetetlen. Ezért q a $p_1, \ldots, p_k$ számok (azaz az összes prímszám) mindegyikétől különbözik, ami ellentmond az indirekt feltevésünknek.

A bizonyítás típuspéldája az indirekt bizonyításnak. Tegyük fel (indirekt módon), hogy csak véges sok prímszám van; legyenek ezek $p_1, \ldots, p_k$. Jelölje q az $n = p_1 \ldots p_k + 1$ szám egyik prímosztóját. Ilyen létezik, hiszen n is prímszámok szorzatára bontható. Ha valamely $i \in \{1, \ldots, k\}$-ra p_i osztaná n-et, akkor az $1 = n - p_1 \ldots p_k$ számot is osztaná, ami lehetetlen. Ezért q a $p_1, \ldots, p_k$ számok (azaz az összes prímszám) mindegyikétől különbözik, ami ellentmond az indirekt feltevésünknek. Q.e.d.

Erősebb állítás is érvényes.

Erősebb állítás is érvényes. A kettőhatványok, azaz az 1, 2, 4, 8, 16, 32, ... számok, továbbá a négyzetszámok is végtelen sokan vannak, de a reciprokaikból alkotott végtelen sor összege véges:

$$\sum_{n=0}^{\infty} \frac{1}{2^n} =$$

Erősebb állítás is érvényes. A kettőhatványok, azaz az 1, 2, 4, 8, 16, 32, ... számok, továbbá a négyzetszámok is végtelen sokan vannak, de a reciprokaikból alkotott végtelen sor összege véges:

$$\sum_{n=0}^{\infty} \frac{1}{2^n} = 2, \qquad \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Ezzel szemben a prímszámok reciprokaiból alkotott sor divergens, azaz

$$\sum_{p \text{ prímszám}} \frac{1}{p} = \infty\,.$$

Erősebb állítás is érvényes. A kettőhatványok, azaz az 1, 2, 4, 8, 16, 32, . . . számok, továbbá a négyzetszámok is végtelen sokan vannak, de a reciprokaikból alkotott végtelen sor összege véges:

$$\sum_{n=0}^{\infty} \frac{1}{2^n} = 2, \qquad \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Ezzel szemben a prímszámok reciprokaiból alkotott sor divergens, azaz

$$\sum_{p \text{ prímszám}} \frac{1}{p} = \infty\,.$$

Persze a kettőhatványok halmaza is, a négyzetszámok halmaza is és a prímszámok halmaza is megszámlálhatóan végtelen, tehát itt csak arról van szó, hogy a prímszámok valamilyen értelemben

Erősebb állítás is érvényes. A kettőhatványok, azaz az 1, 2, 4, 8, 16, 32, ... számok, továbbá a négyzetszámok is végtelen sokan vannak, de a reciprokaikból alkotott végtelen sor összege véges:

$$\sum_{n=0}^{\infty} \frac{1}{2^n} = 2, \qquad \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Ezzel szemben a prímszámok reciprokaiból alkotott sor divergens, azaz

$$\sum_{p \text{ prímszám}} \frac{1}{p} = \infty\,.$$

Persze a kettőhatványok halmaza is, a négyzetszámok halmaza is és a prímszámok halmaza is megszámlálhatóan végtelen, tehát itt csak arról van szó, hogy a prímszámok valamilyen értelemben **sűrűbben** helyezkednek el.

A kettőhatványokkal való összehasonlításnak egy másik aspektusát tárja fel az alábbi:

21. Tétel. *(Csebisev-tétel) Ha* $1 < x \in \mathbf{R}$, *akkor az* $(x, 2x)$ *intervallumban van prímszám.*

A kettőhatványokkal való összehasonlításnak egy másik aspektusát tárja fel az alábbi:

21. Tétel. *(Csebisev-tétel) Ha* $1 < x \in \mathbf{R}$, *akkor az* $(x, 2x)$ *intervallumban van prímszám.*

Pongyolán fogalmazva: bármely szám és kétszerese között van prímszám.

A kettőhatványokkal való összehasonlításnak egy másik aspektusát tárja fel az alábbi:

21. Tétel. *(Csebisev-tétel) Ha* $1 < x \in \mathbf{R}$*, akkor az* $(x, 2x)$ *intervallumban van prímszám.*

Pongyolán fogalmazva: bármely szám és kétszerese között van prímszám. A prímszámok eloszlásáról legtöbbet az alábbi, ún. **nagy prímszámtétel** árul el, amelyet már Gauss is sejtett, de csak

A kettőhatványokkal való összehasonlításnak egy másik aspektusát tárja fel az alábbi:

21. Tétel. *(Csebisev-tétel) Ha* $1 < x \in \mathbf{R}$, *akkor az* $(x, 2x)$ *intervallumban van prímszám.*

Pongyolán fogalmazva: bármely szám és kétszerese között van prímszám. A prímszámok eloszlásáról legtöbbet az alábbi, ún. **nagy prímszámtétel** árul el, amelyet már Gauss is sejtett, de csak 1896-ban bizonyította Hadamard

A kettőhatványokkal való összehasonlításnak egy másik aspektusát tárja fel az alábbi:

21. Tétel. *(Csebisev-tétel) Ha* $1 < x \in \mathbf{R}$*, akkor az* $(x, 2x)$ *intervallumban van prímszám.*

Pongyolán fogalmazva: bármely szám és kétszerese között van prímszám. A prímszámok eloszlásáról legtöbbet az alábbi, ún. **nagy prímszámtétel** árul el, amelyet már Gauss is sejtett, de csak 1896-ban bizonyította Hadamard és de la Vallée-Puossain.

A kettőhatványokkal való összehasonlításnak egy másik aspektusát tárja fel az alábbi:

21. Tétel. *(Csebisev-tétel) Ha* $1 < x \in \mathbf{R}$*, akkor az* $(x, 2x)$ *intervallumban van prímszám.*

Pongyolán fogalmazva: bármely szám és kétszerese között van prímszám. A prímszámok eloszlásáról legtöbbet az alábbi, ún. **nagy prímszámtétel** árul el, amelyet már Gauss is sejtett, de csak 1896-ban bizonyította Hadamard és de la Vallée-Puossain. Jelölje $\pi(n)$ az n-nél nem nagyobb prímszámok számát.

22. Tétel. *(Nagy Prímszámtétel):*

$$\lim_{n\to\infty} \frac{\pi(n)}{\dfrac{n}{\ln n}} = 1$$

22. Tétel. *(Nagy Prímszámtétel):*

$$\lim_{n\to\infty} \frac{\pi(n)}{\dfrac{n}{\ln n}} = 1$$

Ha $x \geq 10^{99}$, akkor a fenti tört már olyan jól megközelíti az 1-et, hogy nem követünk el számottevő hibát, ha ilyen nagy x-ekre úgy számolunk, hogy $\pi(x) \approx \frac{x}{\ln x}$.

22. Tétel. *(Nagy Prímszámtétel):*

$$\lim_{n\to\infty} \frac{\pi(n)}{\dfrac{n}{\ln n}} = 1$$

Ha $x \geq 10^{99}$, akkor a fenti tört már olyan jól megközelíti az 1-et, hogy nem követünk el számottevő hibát, ha ilyen nagy x-ekre úgy számolunk, hogy $\pi(x) \approx \frac{x}{\ln x}$. Ezen képlettel a százjegyű prímszámok

22. Tétel. *(Nagy Prímszámtétel):*

$$\lim_{n\to\infty} \frac{\pi(n)}{\dfrac{n}{\ln n}} = 1$$

Ha $x \geq 10^{99}$, akkor a fenti tört már olyan jól megközelíti az 1-et, hogy nem követünk el számottevő hibát, ha ilyen nagy x-ekre úgy számolunk, hogy $\pi(x) \approx \frac{x}{\ln x}$. Ezen képlettel a százjegyű prímszámok $\pi(10^{100}) - \pi(10^{99})$ számát kiszámolva —

22. Tétel. *(Nagy Prímszámtétel):*

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$

Ha $x \geq 10^{99}$, akkor a fenti tört már olyan jól megközelíti az 1-et, hogy nem követünk el számottevő hibát, ha ilyen nagy x-ekre úgy számolunk, hogy $\pi(x) \approx \frac{x}{\ln x}$. Ezen képlettel a százjegyű prímszámok $\pi(10^{100}) - \pi(10^{99})$ számát kiszámolva — a logaritmus azonosságait alkalmazva —

22. Tétel. *(Nagy Prímszámtétel):*

$$\lim_{n\to\infty} \frac{\pi(n)}{\dfrac{n}{\ln n}} = 1$$

Ha $x \geq 10^{99}$, akkor a fenti tört már olyan jól megközelíti az 1-et, hogy nem követünk el számottevő hibát, ha ilyen nagy x-ekre úgy számolunk, hogy $\pi(x) \approx \frac{x}{\ln x}$. Ezen képlettel a százjegyű prímszámok $\pi(10^{100}) - \pi(10^{99})$ számát kiszámolva — a logaritmus azonosságait alkalmazva — könnyen kapjuk, hogy a

hogy a százjegyű számoknak kb. az

hogy a százjegyű számoknak kb. az $\frac{1}{230}$ -adrésze prímszám!

hogy a százjegyű számoknak kb. az $\dfrac{1}{230}$ -adrésze prímszám! De a 2 kivételével a prímek páratlanok, ezért hogy a százjegyű számoknak kb. az $\frac{1}{230}$ -adrésze prímszám! De a 2 kivételével a prímek páratlanok, ezért a százjegyű páratlan számok $\frac{1}{115}$ -ödrésze prímszám.

hogy a százjegyű számoknak kb. az $\frac{1}{230}$ -adrésze prímszám! De a 2 kivételével a prímek páratlanok, ezért a százjegyű páratlan számok $\frac{1}{115}$ -ödrésze prímszám. Ennek alapján nem meglepő, hogy

hogy a százjegyű számoknak kb. az $\frac{1}{230}$ -adrésze prímszám! De a 2 kivételével a prímek páratlanok, ezért a százjegyű páratlan számok $\frac{1}{115}$ -ödrésze prímszám. Ennek alapján nem meglepő, hogy ha véletlenszerűen — számjegyenként sorsolva — állítunk elő százjegyű páratlan számokat, akkor párszáz próbálkozás után —

hogy a százjegyű számoknak kb. az $\dfrac{1}{230}$ -adrésze prímszám! De a 2 kivételével a prímek páratlanok, ezért a százjegyű páratlan számok $\dfrac{1}{115}$ -ödrésze prímszám. Ennek alapján nem meglepő, hogy ha véletlenszerűen — számjegyenként sorsolva — állítunk elő százjegyű páratlan számokat, akkor párszáz próbálkozás után — számítógépen egy másodperc alatt — találunk százjegyű prímszámot.

hogy a százjegyű számoknak kb. az $\frac{1}{230}$ -adrésze prímszám! De a 2 kivételével a prímek páratlanok, ezért a százjegyű páratlan számok $\frac{1}{115}$ -ödrésze prímszám. Ennek alapján nem meglepő, hogy ha véletlenszerűen — számjegyenként sorsolva — állítunk elő százjegyű páratlan számokat, akkor párszáz próbálkozás után — számítógépen egy másodperc alatt — találunk százjegyű prímszámot. Ennek a ténynek is fontos szerepe van az RSA nyilvános kulcsú titkosírás szempontjából.

Lineáris diofantoszi egyenletek

A diofantoszi jelző arra utal, hogy az ismeretleneket az egész számok körében keressük.

Lineáris diofantoszi egyenletek

A diofantoszi jelző arra utal, hogy az ismeretleneket az egész számok körében keressük. Nem lenne értelme az egyismeretlenes diofantoszi egyenlet vizsgálatának, hiszen azt többnyire egyértelműen meg lehet oldani a valós számok halmazán, és azt követően ellenőrizni lehet, hogy egész számot kaptunk-e.

Lineáris diofantoszi egyenletek

A diofantoszi jelző arra utal, hogy az ismeretleneket az egész számok körében keressük. Nem lenne értelme az egyismeretlenes diofantoszi egyenlet vizsgálatának, hiszen azt többnyire egyértelműen meg lehet oldani a valós számok halmazán, és azt követően ellenőrizni lehet, hogy egész számot kaptunk-e. Ezért mi csak az alábbi típusú lineáris diofantoszi egyenlettel foglalkozunk,

Lineáris diofantoszi egyenletek

A diofantoszi jelző arra utal, hogy az ismeretleneket az egész számok körében keressük. Nem lenne értelme az egyismeretlenes diofantoszi egyenlet vizsgálatának, hiszen azt többnyire egyértelműen meg lehet oldani a valós számok halmazán, és azt követően ellenőrizni lehet, hogy egész számot kaptunk-e. Ezért mi csak az alábbi típusú lineáris diofantoszi egyenlettel foglalkozunk, viszont megemlítjük, hogy az n darab lineáris egyenletből álló egész együtthatós m-ismeretlenes diofantoszi egyenletrendszereknek is van — Frobeniustól származó — szép elmélete.

Definíció: Lineáris diofantoszi egyenleten egy

$$ax + by = c$$

egyenletet értünk, ahol $a, b, c \in \mathbf{Z}$, és az x, y ismeretleneket is $\mathbf{Z}$-ben keressük.

Definíció: Lineáris diofantoszi egyenleten egy

$$ax + by = c$$

egyenletet értünk, ahol $a, b, c \in \mathbf{Z}$, és az x, y ismeretleneket is $\mathbf{Z}$-ben keressük.

23. Tétel. *A fenti diofantoszi egyenlet akkor és csak akkor oldható meg, ha ln.k.o.*$(a, b) \mid c$ *(*

Definíció: Lineáris diofantoszi egyenleten egy

$$ax + by = c$$

egyenletet értünk, ahol $a, b, c \in \mathbf{Z}$, és az x, y ismeretleneket is $\mathbf{Z}$-ben keressük.

23. Tétel. *A fenti diofantoszi egyenlet akkor és csak akkor oldható meg, ha ln.k.o.*$(a, b) \mid c$ *(azaz az együtthatók legnagyobb közös osztója osztja a konstanst).*

Definíció: Lineáris diofantoszi egyenleten egy

$$ax + by = c$$

egyenletet értünk, ahol $a, b, c \in \mathbf{Z}$, és az x, y ismeretleneket is $\mathbf{Z}$-ben keressük.

23. Tétel. *A fenti diofantoszi egyenlet akkor és csak akkor oldható meg, ha ln.k.o.*$(a, b) \mid c$ *(azaz az együtthatók legnagyobb közös osztója osztja a konstanst). Amennyiben az egyenlet megoldható és* (x_0, y_0) *egy rögzített megoldása, akkor*

Definíció: Lineáris diofantoszi egyenleten egy

$$ax + by = c$$

egyenletet értünk, ahol $a, b, c \in \mathbf{Z}$, és az x, y ismeretleneket is $\mathbf{Z}$-ben keressük.

23. Tétel. *A fenti diofantoszi egyenlet akkor és csak akkor oldható meg, ha ln.k.o.$(a, b) \mid c$ (azaz az együtthatók legnagyobb közös osztója osztja a konstanst). Amennyiben az egyenlet megoldható és (x_0, y_0) egy rögzített megoldása, akkor a megoldások halmaza*

$$\{(x_0 + t \cdot \frac{b}{\textit{ln.k.o.}(a,b)},\ y_0 - t \cdot \frac{a}{\textit{ln.k.o.}(a,b)}) : t \in \mathbf{Z}\}\ .$$

A tétel második mondata úgy is fogalmazható, hogy amennyiben (x_0, y_0) egy **partikuláris megoldás**, akkor az egyenlet **általános megoldása**

$$x = x_0 + t \cdot \frac{b}{\text{ln.k.o.}(a,b)}, \quad y = y_0 - t \cdot \frac{a}{\text{ln.k.o.}(a,b)} \qquad (t \in \mathbf{Z}),$$

ahol t paramétert jelöl.

A tétel második mondata úgy is fogalmazható, hogy amennyiben (x_0, y_0) egy **partikuláris megoldás**, akkor az egyenlet **általános megoldása**

$$x = x_0 + t \cdot \frac{b}{\text{ln.k.o.}(a,b)}, \;\; y = y_0 - t \cdot \frac{a}{\text{ln.k.o.}(a,b)} \qquad (t \in \mathbf{Z}),$$

ahol t paramétert jelöl.

A bizonyítás

A tétel második mondata úgy is fogalmazható, hogy amennyiben (x_0, y_0) egy **partikuláris megoldás**, akkor az egyenlet **általános megoldása**

$$x = x_0 + t \cdot \frac{b}{\text{ln.k.o.}(a,b)}, \;\; y = y_0 - t \cdot \frac{a}{\text{ln.k.o.}(a,b)} \qquad (t \in \mathbf{Z}),$$

ahol t paramétert jelöl.

A bizonyítás egyúttal azt is megmutatja, hogy hogyan kell egy ilyen egyenletet megoldani.

A tétel második mondata úgy is fogalmazható, hogy amennyiben (x_0, y_0) egy **partikuláris megoldás**, akkor az egyenlet **általános megoldása**

$$x = x_0 + t \cdot \frac{b}{\text{ln.k.o.}(a,b)}, \quad y = y_0 - t \cdot \frac{a}{\text{ln.k.o.}(a,b)} \qquad (t \in \mathbf{Z}),$$

ahol t paramétert jelöl.

A bizonyítás egyúttal azt is megmutatja, hogy hogyan kell egy ilyen egyenletet megoldani. Vezessük be az alábbi jelöléseket: $d = \text{ln.k.o.}(a,b)$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$.

A tétel második mondata úgy is fogalmazható, hogy amennyiben (x_0, y_0) egy **partikuláris megoldás**, akkor az egyenlet **általános megoldása**

$$x = x_0 + t \cdot \frac{b}{\text{ln.k.o.}(a, b)}, \ \ y = y_0 - t \cdot \frac{a}{\text{ln.k.o.}(a, b)} \qquad (t \in \mathbf{Z}),$$

ahol t paramétert jelöl.

A bizonyítás egyúttal azt is megmutatja, hogy hogyan kell egy ilyen egyenletet megoldani. Vezessük be az alábbi jelöléseket: $d = \text{ln.k.o.}(a, b)$, $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$. Tehát $a = a_1 d$, $b = b_1 d$.

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$,

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is —

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$.

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal:

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} =$

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} = c$. Innen

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} = c$. Innen látható, hogy van megoldás:

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} = c$. Innen látható, hogy van megoldás: az $(u\frac{c}{d}, v\frac{c}{d})$ pár megoldás.

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} = c$. Innen látható, hogy van megoldás: az $(u\frac{c}{d}, v\frac{c}{d})$ pár megoldás. Ezzel a megoldhatóságra vonatkozó kritériumot igazoltuk.

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **egyúttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} = c$. Innen látható, hogy van megoldás: az $(u\frac{c}{d}, v\frac{c}{d})$ pár megoldás. Ezzel a megoldhatóságra vonatkozó kritériumot igazoltuk.

Tegyük fel, hogy az egyenlet megoldható és (x_0, y_0) megoldása. A bevezetett jelöléseinkkel (

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} = c$. Innen látható, hogy van megoldás: az $(u\frac{c}{d}, v\frac{c}{d})$ pár megoldás. Ezzel a megoldhatóságra vonatkozó kritériumot igazoltuk.

Tegyük fel, hogy az egyenlet megoldható és (x_0, y_0) megoldása. A bevezetett jelöléseinkkel (tehát $d =$ ln.k.o.(a, b), $a = a_1 d$, $b = b_1 d$)

Ha megoldható, akkor létezik (x_0, y_0) megoldás. Mivel $d \mid a \mid ax_0$ és $d \mid b \mid by_0$, ezért $d \mid ax_0 + by_0 = c$, valóban.

Ha $d \mid c$, akkor először is — az euklideszi algoritmusnál tanultak szerint (és ez **együttal számolási módszer is!!!**) van olyan $u, v \in \mathbf{Z}$, hogy $ua + vb = d$. Szorozzuk meg mindkét oldalt a $\frac{c}{d}$ **egész** számmal: $au\frac{c}{d} + bv\frac{c}{d} = c$. Innen látható, hogy van megoldás: az $(u\frac{c}{d}, v\frac{c}{d})$ pár megoldás. Ezzel a megoldhatóságra vonatkozó kritériumot igazoltuk.

Tegyük fel, hogy az egyenlet megoldható és (x_0, y_0) megoldása. A bevezetett jelöléseinkkel (tehát $d =$ ln.k.o.(a, b), $a = a_1 d$, $b = b_1 d$) azt kell igazolni, hogy $x_0 + tb_1$, $y = y_0 - ta_1$ $(t \in \mathbf{Z})$ az általános megoldása.

Egyrészt (

Egyrészt (és ez a könnyebb rész), ha

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by =$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1 dx + b_1 dy =$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1 dx + b_1 dy = a_1 d(x_0 + tb_1) + b_1 d(y_0 - ta_1) =$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1dx + b_1dy = a_1d(x_0 + tb_1) + b_1d(y_0 - ta_1) =$$
$$(a_1d)x_0 + (b_1d)y_0 = ax_0 + by_0 = c$$

tehát a t paraméter tetszőleges értékére megoldást ad.

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1dx + b_1dy = a_1d(x_0 + tb_1) + b_1d(y_0 - ta_1) =$$
$$(a_1d)x_0 + (b_1d)y_0 = ax_0 + by_0 = c$$

tehát a t paraméter tetszőleges értékére megoldást ad.

Most tegyük fel, hogy (x, y) megoldás. Ekkor

$$0 =$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1dx + b_1dy = a_1d(x_0 + tb_1) + b_1d(y_0 - ta_1) =$$
$$(a_1d)x_0 + (b_1d)y_0 = ax_0 + by_0 = c$$

tehát a t paraméter tetszőleges értékére megoldást ad.

Most tegyük fel, hogy (x, y) megoldás. Ekkor

$$0 = \frac{c}{d} - \frac{c}{d} =$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1dx + b_1dy = a_1d(x_0 + tb_1) + b_1d(y_0 - ta_1) =$$
$$(a_1d)x_0 + (b_1d)y_0 = ax_0 + by_0 = c$$

tehát a t paraméter tetszőleges értékére megoldást ad.

Most tegyük fel, hogy (x, y) megoldás. Ekkor

$$0 = \frac{c}{d} - \frac{c}{d} = \frac{ax + by}{d} -$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1dx + b_1dy = a_1d(x_0 + tb_1) + b_1d(y_0 - ta_1) =$$
$$(a_1d)x_0 + (b_1d)y_0 = ax_0 + by_0 = c$$

tehát a t paraméter tetszőleges értékére megoldást ad.

Most tegyük fel, hogy (x, y) megoldás. Ekkor

$$0 = \frac{c}{d} - \frac{c}{d} = \frac{ax + by}{d} - \frac{ax_0 + by_0}{d} =$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1dx + b_1dy = a_1d(x_0 + tb_1) + b_1d(y_0 - ta_1) =$$
$$(a_1d)x_0 + (b_1d)y_0 = ax_0 + by_0 = c$$

tehát a t paraméter tetszőleges értékére megoldást ad.

Most tegyük fel, hogy (x, y) megoldás. Ekkor

$$0 = \frac{c}{d} - \frac{c}{d} = \frac{ax + by}{d} - \frac{ax_0 + by_0}{d} =$$
$$(a_1x + b_1y) - (a_1x_0 + b_1y_0) =$$

Egyrészt (és ez a könnyebb rész), ha $t \in \mathbf{Z}$, akkor

$$ax + by = a_1dx + b_1dy = a_1d(x_0 + tb_1) + b_1d(y_0 - ta_1) =$$
$$(a_1d)x_0 + (b_1d)y_0 = ax_0 + by_0 = c$$

tehát a t paraméter tetszőleges értékére megoldást ad.

Most tegyük fel, hogy (x, y) megoldás. Ekkor

$$0 = \frac{c}{d} - \frac{c}{d} = \frac{ax + by}{d} - \frac{ax_0 + by_0}{d} =$$
$$(a_1x + b_1y) - (a_1x_0 + b_1y_0) = a_1(x - x_0) + b_1(y - y_0),$$

azaz

$$a_1(x - x_0) = -b_1(y - y_0).$$

M

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja,

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$.

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$. Ezért alkalmas $t \in \mathbf{Z}$-re

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$. Ezért alkalmas $t \in \mathbf{Z}$-re $x - x_0 = tb_1$, azaz $x = x_0 + tb_1$.

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$. Ezért alkalmas $t \in \mathbf{Z}$-re $x - x_0 = tb_1$, azaz $x = x_0 + tb_1$. Ezt a fenti kivetett képletbe visszahelyettesítve kapjuk, hogy

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$. Ezért alkalmas $t \in \mathbf{Z}$-re $x - x_0 = tb_1$, azaz $x = x_0 + tb_1$. Ezt a fenti kivetett képletbe visszahelyettesítve kapjuk, hogy $a_1 tb_1 = -b_1(y - y_0)$. Miután $-b_1$-gyel egyszerűsítettünk:

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$. Ezért alkalmas $t \in \mathbf{Z}$-re $x - x_0 = tb_1$, azaz $x = x_0 + tb_1$. Ezt a fenti kivetett képletbe visszahelyettesítve kapjuk, hogy $a_1tb_1 = -b_1(y - y_0)$. Miután $-b_1$-gyel egyszerűsítettünk: $-a_1t = y - y_0$,

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$. Ezért alkalmas $t \in \mathbf{Z}$-re $x - x_0 = tb_1$, azaz $x = x_0 + tb_1$. Ezt a fenti kivetett képletbe visszahelyettesítve kapjuk, hogy $a_1 tb_1 = -b_1(y - y_0)$. Miután $-b_1$-gyel egyszerűsítettünk: $-a_1 t = y - y_0$, innen y kifejezhető: $y = y_0 - ta_1$.

$$a_1(x - x_0) = -b_1(y - y_0).$$

Mivel b_1 osztja a jobboldalt, a baloldalt is osztja, de mivel ln.k.o.$(a_1, b_1) = 1$, innen $b_1 \mid x - x_0$. Ezért alkalmas $t \in \mathbf{Z}$-re $x - x_0 = tb_1$, azaz $x = x_0 + tb_1$. Ezt a fenti kivetett képletbe visszahelyettesítve kapjuk, hogy $a_1tb_1 = -b_1(y - y_0)$. Miután $-b_1$-gyel egyszerűsítettünk: $-a_1t = y - y_0$, innen y kifejezhető: $y = y_0 - ta_1$. Q.e.d.

Feladat: Oldjuk meg az alábbi diofantoszi egyenletet:

$$7640x + 234y = 90.$$

1. Megoldás: Először

Feladat: Oldjuk meg az alábbi diofantoszi egyenletet:

$$7640x + 234y = 90.$$

1. Megoldás: Először az együtthatók legnagyobb közös osztóját kell kiszámítani, majd megnézni, hogy osztja-e a

Feladat: Oldjuk meg az alábbi diofantoszi egyenletet:

$$7640x + 234y = 90.$$

1. Megoldás: Először az együtthatók legnagyobb közös osztóját kell kiszámítani, majd megnézni, hogy osztja-e a 90-et. Ha igen,

Feladat: Oldjuk meg az alábbi diofantoszi egyenletet:

$$7640x + 234y = 90.$$

1. Megoldás: Először az együtthatók legnagyobb közös osztóját kell kiszámítani, majd megnézni, hogy osztja-e a 90-et. Ha igen, akkor a következő lépés az,

Feladat: Oldjuk meg az alábbi diofantoszi egyenletet:

$$7640x + 234y = 90.$$

1. Megoldás: Először az együtthatók legnagyobb közös osztóját kell kiszámítani, majd megnézni, hogy osztja-e a 90-et. Ha igen, akkor a következő lépés az, hogy az ln.k.o.-t kifejezzük a két együttható

Feladat: Oldjuk meg az alábbi diofantoszi egyenletet:

$$7640x + 234y = 90.$$

1. Megoldás: Először az együtthatók legnagyobb közös osztóját kell kiszámítani, majd megnézni, hogy osztja-e a 90-et. Ha igen, akkor a következő lépés az, hogy az ln.k.o.-t kifejezzük a két együttható „lineáris kombinációjaként”. Most
(

Feladat: Oldjuk meg az alábbi diofantoszi egyenletet:

$$7640x + 234y = 90.$$

1. Megoldás: Először az együtthatók legnagyobb közös osztóját kell kiszámítani, majd megnézni, hogy osztja-e a 90-et. Ha igen, akkor a következő lépés az, hogy az ln.k.o.-t kifejezzük a két együttható „lineáris kombinációjaként''. Most (kivételesen, mert nyomdatechnikailag nem könnyű) a kézi számoláskor szokásos elrendezést ismertetjük.

7　6

7 6 4

7 6 4 0

7 6 4 0 :

7 6 4 0 : 2

7 6 4 0 : 2 3

7 6 4 0 : 2 3 4

$$7\ 6\ 4\ 0 : 2\ 3\ 4 = 3$$

$$7640 : 234 = 3$$

7 6 4 0 : 2 3 4 = 3

6

7 6 4 0 : 2 3 4 = 3

6 2

$$\begin{array}{ccccccccc} 7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 \\ & 6 & 2 & & & & & & \end{array}$$

7　6

7 6 4

7 6 4 0

7 6 4 0 :

7 6 4 0 : 2

7 6 4 0 : 2 3

7 6 4 0 : 2 3 4

$$7640 : 234 = 3$$

$7640 : 234 = 33$

$7640 : 234 = 33$

6

7 6 4 0 : 2 3 4 = 3 3

6 2

$$7640 : 234 = 33$$

$$620$$

$$
\begin{array}{r}
7640 : 234 = 33 \\
620 \\
-
\end{array}
$$

$$
\begin{array}{llllllllll}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & & & & & & & &
\end{array}
$$

$$\begin{array}{llllllllll} 7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\ & 6 & 2 & 0 & & & & & & \\ - & 7 & 0 & & & & & & & \end{array}$$

$$
\begin{array}{llllllllll}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & &
\end{array}
$$

$$
\begin{array}{llllllllll}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & & & & & & & & &
\end{array}
$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & & & & & & & &
\end{array}
$$

7	6	4	0	:	2	3	4	= 3	3
	6	2	0						
−	7	0	2						
+	6	2							

7	6	4	0	:	2	3	4	= 3	3
	6	2	0						
−	7	0	2						
+	6	2	0						

7	6	4	0	:	2	3	4	= 3	3
	6	2	0						
−	7	0	2						
+	6	2	0						
	−								

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & & & & & & &
\end{array}
$$

$$
\begin{array}{ccccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = & 3 & 3 \\
 & 6 & 2 & 0 & & & & & & & \\
- & 7 & 0 & 2 & & & & & & & \\
+ & 6 & 2 & 0 & & & & & & & \\
 & - & 8 & 2 & & & & & & &
\end{array}
$$

7	6	4	0	:	2	3	4	= 3	3	
	6	2	0							
−	7	0	2							
+	6	2	0							
	−	8	2							82 =

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
  & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
  & - & 8 & 2 & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{ccccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = & 3 & 3 \\
 & 6 & 2 & 0 & & & & & & & \\
- & 7 & 0 & 2 & & & & & & & \\
+ & 6 & 2 & 0 & & & & & & & \\
 & - & 8 & 2 & & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

7	6	4	0	:	2	3	4	= 3	3	
	6	2	0							
$-$	7	0	2							
$+$	6	2	0							
	$-$	8	2							$82 = 33 \cdot 234 - 1 \cdot 7640$
	2									

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & & \\
 & 2 & 3 & & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & & \\
 & 2 & 3 & 4 & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{cccc}
2 & 3 & 4 & :
\end{array}
$$

$$
\begin{array}{cccccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{ccccc}
2 & 3 & 4 & : & 8
\end{array}
$$

$$
\begin{array}{ccccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
\qquad 82 = 33 \cdot 234 - 1 \cdot 7640
$$

$$
\begin{array}{cccccc}
2 & 3 & 4 & : & 8 & 2
\end{array}
$$

$$
\begin{array}{cccccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = & 3 & 3 \\
  & 6 & 2 & 0 \\
- & 7 & 0 & 2 \\
+ & 6 & 2 & 0 \\
  & - & 8 & 2
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{cccccc}
2 & 3 & 4 & : & 8 & 2 & =
\end{array}
$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{cccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = 3 \\
- & & & & & & &
\end{array}
$$

$$\begin{array}{ccccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$\begin{array}{ccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = & 3 \\
- & 2 & & & & & & &
\end{array}$$

$$
\begin{array}{ccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 \quad 3 \\
  & 6 & 2 & 0 & & & & & \\
- & 7 & 0 & 2 & & & & & \\
+ & 6 & 2 & 0 & & & & & \\
  & - & 8 & 2 & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{ccccccc}
  & 2 & 3 & 4 & : & 8 \quad 2 & = \quad 3 \\
- & 2 & 4 & & & &
\end{array}
$$

$$
\begin{array}{cccccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = & 3 & 3 \\
  & 6 & 2 & 0 \\
- & 7 & 0 & 2 \\
+ & 6 & 2 & 0 \\
  & - & 8 & 2
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{ccccccccc}
  & 2 & 3 & 4 & : & 8 & 2 & = & 3 \\
- & 2 & 4 & 6 \\
+ & & &
\end{array}
$$

$$\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$\begin{array}{ccccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = & 3 \\
- & 2 & 4 & 6 & & & & & \\
+ & 2 & & & & & & &
\end{array}$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{ccccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = & 3 \\
- & 2 & 4 & 6 & & & & & \\
+ & 2 & 3 & & & & & &
\end{array}
$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$
\begin{array}{cccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = 3 \\
- & 2 & 4 & 6 & & & & \\
+ & 2 & 3 & 4 & & & &
\end{array}
$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
\qquad 82 = 33 \cdot 234 - 1 \cdot 7640
$$

$$
\begin{array}{cccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = 3 \\
- & 2 & 4 & 6 & & & & \\
+ & 2 & 3 & 4 & & & & \\
 & - & & & & & &
\end{array}
$$

$$
\begin{array}{rrrrcrrrl}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 \quad 3 \\
 & 6 & 2 & 0 & & & & & \\
- & 7 & 0 & 2 & & & & & \\
+ & 6 & 2 & 0 & & & & & \\
 & - & 8 & 2 & & & & &
\end{array}
\qquad 82 = 33 \cdot 234 - 1 \cdot 7640
$$

$$
\begin{array}{rrrrcrrl}
 & 2 & 3 & 4 & : & 8 & 2 & = \quad 3 \\
- & 2 & 4 & 6 & & & & \\
+ & 2 & 3 & 4 & & & & \\
 & - & 1 & & & & &
\end{array}
$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
\qquad 82 = 33 \cdot 234 - 1 \cdot 7640
$$

$$
\begin{array}{cccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = 3 \\
- & 2 & 4 & 6 & & & & \\
+ & 2 & 3 & 4 & & & & \\
 & - & 1 & 2 & & & &
\end{array}
$$

$$
\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}
\qquad 82 = 33 \cdot 234 - 1 \cdot 7640
$$

$$
\begin{array}{cccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = \; 3 \\
- & 2 & 4 & 6 & & & & \\
+ & 2 & 3 & 4 & & & & \\
 & - & 1 & 2 & & & &
\end{array}
\qquad 12 = 3 \cdot 82 - 234
$$

$$\begin{array}{cccccccccc}
7 & 6 & 4 & 0 & : & 2 & 3 & 4 & = 3 & 3 \\
 & 6 & 2 & 0 & & & & & & \\
- & 7 & 0 & 2 & & & & & & \\
+ & 6 & 2 & 0 & & & & & & \\
 & - & 8 & 2 & & & & & &
\end{array}$$

$$82 = 33 \cdot 234 - 1 \cdot 7640$$

$$\begin{array}{ccccccccc}
 & 2 & 3 & 4 & : & 8 & 2 & = & 3 \\
- & 2 & 4 & 6 & & & & & \\
+ & 2 & 3 & 4 & & & & & \\
 & - & 1 & 2 & & & & &
\end{array}$$

$$12 = 3 \cdot 82 - 234$$

$$
\begin{array}{cccccccc}
 & 8 & 2 & : & 1 & 2 & = & 7 \\
- & 8 & 4 & & & & & \\
+ & 8 & 2 & & & & & \\
 & - & 2 & & & & &
\end{array}
$$

$$2 = 7 \cdot 12 - 82$$

$$1 \quad 2 \quad :$$

$$\begin{array}{ccccccc} & 8 & 2 & : & 1 & 2 & = & 7 \\ - & 8 & 4 & & & & & \\ + & 8 & 2 & & & & & \\ & - & 2 & & & & & \end{array}$$

$$2 = 7 \cdot 12 - 82$$

$$1 \quad 2 \quad : \quad 2 \quad =$$

$$\begin{array}{rrrcrrcr}
 & 8 & 2 & : & 1 & 2 & = & 7 \\
- & 8 & 4 & & & & & \\
+ & 8 & 2 & & & & & \\
 & - & 2 & & & & &
\end{array}$$

$$2 = 7 \cdot 12 - 82$$

$$\begin{array}{rrcrcr}
1 & 2 & : & 2 & = & 6 \\
 & 0 & & & &
\end{array}$$

$$
\begin{array}{cccccccc}
 & 8 & 2 & : & 1 & 2 & = & 7 \\
- & 8 & 4 & & & & & \\
+ & 8 & 2 & & & & & \\
 & - & 2 & & & & &
\end{array}
\qquad\qquad 2 = 7 \cdot 12 - 82
$$

$$
\begin{array}{cccccc}
1 & 2 & : & 2 & = & 6 \\
 & 0 & & & &
\end{array}
$$

Az utolsó nemzérus maradék -2, ezért $\mathrm{ln.k.o.}(7640, 234) = 2$.
(

$$
\begin{array}{cccccccc}
 & 8 & 2 & : & 1 & 2 & = & 7 \\
- & 8 & 4 & & & & & \\
+ & 8 & 2 & & & & & \\
 & - & 2 & & & & &
\end{array}
\qquad\qquad 2 = 7 \cdot 12 - 82
$$

$$
\begin{array}{cccccc}
1 & 2 & : & 2 & = & 6 \\
 & 0 & & & &
\end{array}
$$

Az utolsó nemzérus maradék -2, ezért ln.k.o.$(7640, 234) = 2$. (Az előjelet elhagyjuk.) Mivel a 2 osztja a $7640x + 234y = 90$ egyenletben a konstanst,

$$
\begin{array}{cccccccc}
 & 8 & 2 & : & 1 & 2 & = & 7 \\
- & 8 & 4 & & & & & \\
+ & 8 & 2 & & & & & \\
 & - & 2 & & & & &
\end{array}
\qquad\qquad 2 = 7 \cdot 12 - 82
$$

$$
\begin{array}{cccccc}
1 & 2 & : & 2 & = & 6 \\
 & 0 & & & &
\end{array}
$$

Az utolsó nemzérus maradék -2, ezért ln.k.o.$(7640, 234) = 2$. (Az előjelet elhagyjuk.) Mivel a 2 osztja a $7640x + 234y = 90$ egyenletben a konstanst, a diofantoszi egyenlet megoldható.

$$
\begin{array}{cccccccc}
 & 8 & 2 & : & 1 & 2 & = & 7 \\
- & 8 & 4 & & & & & \\
+ & 8 & 2 & & & & & \\
 & - & 2 & & & & &
\end{array}
\qquad\qquad 2 = 7 \cdot 12 - 82
$$

$$
\begin{array}{cccccc}
1 & 2 & : & 2 & = & 6 \\
 & 0 & & & &
\end{array}
$$

Az utolsó nemzérus maradék -2, ezért ln.k.o.$(7640, 234) = 2$. (Az előjelet elhagyjuk.) Mivel a 2 osztja a $7640x + 234y = 90$ egyenletben a konstanst, a diofantoszi egyenlet megoldható. A megoldáshoz szükségünk lesz a jobbszélen kigyűjtött egyenlőségekre:

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 =$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 =$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$
$$20 \cdot 82 - 7 \cdot 234 =$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$

$$20 \cdot 82 - 7 \cdot 234 = 20 \cdot ($$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$
$$20 \cdot 82 - 7 \cdot 234 = 20 \cdot (33 \cdot 234 - 1 \cdot 7640) - 7 \cdot 234 =$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$
$$20 \cdot 82 - 7 \cdot 234 = 20 \cdot (33 \cdot 234 - 1 \cdot 7640) - 7 \cdot 234 =$$
$$-20 \cdot 7640 + 653 \cdot 234 =$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$
$$20 \cdot 82 - 7 \cdot 234 = 20 \cdot (33 \cdot 234 - 1 \cdot 7640) - 7 \cdot 234 =$$
$$-20 \cdot 7640 + 653 \cdot 234 = 7640 \cdot (-20) + 234 \cdot 653.$$

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$
$$20 \cdot 82 - 7 \cdot 234 = 20 \cdot (33 \cdot 234 - 1 \cdot 7640) - 7 \cdot 234 =$$
$$-20 \cdot 7640 + 653 \cdot 234 = 7640 \cdot (-20) + 234 \cdot 653.$$

A fentit $90/2 = 45$-tel átszoroza a $7640x + 234y = 90$ egyenlet egy partikuláris megoldását kapjuk, :

$$82 = 33 \cdot 234 - 1 \cdot 7640, \qquad 12 = 3 \cdot 82 - 234, \qquad 2 = 7 \cdot 12 - 82.$$

A cél a 2 kifejezése a 7640 és a 234 lineáris kombinciójával. A fenti egyenlőségeket fordított sorrendben dolgozzuk fel (hiszen a legutolsó az, amelyik a 2-t valahogy kifejezi.)

$$2 = 7 \cdot 12 - 82 = 7 \cdot (3 \cdot 82 - 234) - 82 =$$
$$20 \cdot 82 - 7 \cdot 234 = 20 \cdot (33 \cdot 234 - 1 \cdot 7640) - 7 \cdot 234 =$$
$$-20 \cdot 7640 + 653 \cdot 234 = 7640 \cdot (-20) + 234 \cdot 653.$$

A fentit $90/2 = 45$-tel átszoroza a $7640x + 234y = 90$ egyenlet egy partikuláris megoldását kapjuk, :

$$7640 \cdot (-900) + 234 \cdot 29385 = 90$$

Tehát

Tehát $(x_0, y_0) = (-900, 29385)$.

Tehát $(x_0, y_0) = (-900, 29385)$. Az $7640x + 234y = 90$ egyenlet általános megoldása

Tehát $(x_0, y_0) = (-900, 29385)$. Az $7640x+234y = 90$ egyenlet általános megoldása $x = -900 + \frac{234}{2} \cdot t$, $y = 29385 - \frac{7640}{2} \cdot t$ $(t \in \mathbf{Z})$, azaz (

Tehát $(x_0, y_0) = (-900, 29385)$. Az $7640x+234y = 90$ egyenlet általános megoldása $x = -900 + \frac{234}{2} \cdot t$, $y = 29385 - \frac{7640}{2} \cdot t$ ($t \in \mathbf{Z}$), azaz (és más terminológiával) a diofantoszi egyenlet megoldásainak halmaza:

$$\{(-900 + 117t, 29385 - 3820t) : t \in \mathbf{Z}\}.$$

2. Megoldás: A $7640x + 234y = 90$ diofantoszi egyenletet „ügyes” helyettesítések sorozatával is megoldhatjuk. (

2. Megoldás: A $7640x + 234y = 90$ diofantoszi egyenletet „ügyes” helyettesítések sorozatával is megoldhatjuk. (De a tényleges numerikus számolás nem tér el az előző megoldástól,

2. Megoldás: A $7640x + 234y = 90$ diofantoszi egyenletet „ügyes'' helyettesítések sorozatával is megoldhatjuk. (De a tényleges numerikus számolás nem tér el az előző megoldástól, tehát programozási szempontból a két algoritmus nem különbözik.

2. Megoldás: A $7640x + 234y = 90$ diofantoszi egyenletet „ügyes” helyettesítések sorozatával is megoldhatjuk. (De a tényleges numerikus számolás nem tér el az előző megoldástól, tehát programozási szempontból a két algoritmus nem különbözik. Az alábbiaknál kevesebbet is elegendő lenne leírni — most csak az előző megoldással való összevethetőség miatt írunk ennyit, és ezzel azt hangsúlyozzuk, hogy nem véletlenszerűen, hanem a maradékos osztásnak „megfelelően” választjuk meg az alkalmazott helyettesítéseket.

2. Megoldás: A $7640x + 234y = 90$ diofantoszi egyenletet „ügyes" helyettesítések sorozatával is megoldhatjuk. (De a tényleges numerikus számolás nem tér el az előző megoldástól, tehát programozási szempontból a két algoritmus nem különbözik. Az alábbiaknál kevesebbet is elegendő lenne leírni — most csak az előző megoldással való összevethetőség miatt írunk ennyit, és ezzel azt hangsúlyozzuk, hogy nem véletlenszerűen, hanem a maradékos osztásnak „megfelelően" választjuk meg az alkalmazott helyettesítéseket. A gyakorlati számolás során elegendő lenne szinte csak az $\underbrace{\qquad}$-lel jelölt helyettesítéseket tartalmazó képleteket leírni —

2. Megoldás: A $7640x + 234y = 90$ diofantoszi egyenletet „ügyes” helyettesítések sorozatával is megoldhatjuk. (De a tényleges numerikus számolás nem tér el az előző megoldástól, tehát programozási szempontból a két algoritmus nem különbözik. Az alábbiaknál kevesebbet is elegendő lenne leírni — most csak az előző megoldással való összevethetőség miatt írunk ennyit, és ezzel azt hangsúlyozzuk, hogy nem véletlenszerűen, hanem a maradékos osztásnak „megfelelően” választjuk meg az alkalmazott helyettesítéseket. A gyakorlati számolás során elegendő lenne szinte csak az $\underbrace{\quad\quad}$-lel jelölt helyettesítéseket tartalmazó képleteket leírni — erre egy későbbi feladat során látunk majd példát.)

$7640x + 234y$

$$7640x+234y = (33\cdot 234-82)x+234y$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x + y}$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x =$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z - 82x =$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z - 82x = (3\cdot 82 - 12)z - 82x$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z - 82x = (3\cdot 82 - 12)z - 82x = 82$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x})$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z-82x = (3\cdot 82-12)z-82x = 82(\underbrace{3z-x}_{u})-12z$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$82u-12z=$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$82u-12z=(7\cdot 12-2)u-12z$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z-82x = (3\cdot 82-12)z-82x = 82(\underbrace{3z-x}_{u})-12z = 90,$$

$$82u-12z = (7\cdot 12-2)u-12z = 12(\underbrace{7u-z}_{v})$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z-82x = (3\cdot 82-12)z-82x = 82(\underbrace{3z-x}_{u})-12z = 90,$$

$$82u-12z = (7\cdot 12-2)u-12z = 12(\underbrace{7u-z}_{v})-2u = 90$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$82u-12z=(7\cdot 12-2)u-12z=12(\underbrace{7u-z}_{v})-2u=90$$

$$12v-2u=$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$82u-12z=(7\cdot 12-2)u-12z=12(\underbrace{7u-z}_{v})-2u=90$$

$$12v-2u=6\cdot 2v-2u$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$82u-12z=(7\cdot 12-2)u-12z=12(\underbrace{7u-z}_{v})-2u=90$$

$$12v-2u=6\cdot 2v-2u=2(\underbrace{6v-u}_{w})$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z - 82x = (3\cdot 82 - 12)z - 82x = 82(\underbrace{3z-x}_{u}) - 12z = 90,$$

$$82u - 12z = (7\cdot 12 - 2)u - 12z = 12(\underbrace{7u-z}_{v}) - 2u = 90$$

$$12v - 2u = 6\cdot 2v - 2u = 2(\underbrace{6v-u}_{w}) = 2w =$$

$$7640x+234y = (33\cdot 234-82)x+234y = 234(\underbrace{33x+y}_{z})-82x = 90,$$

$$234z-82x = (3\cdot 82-12)z-82x = 82(\underbrace{3z-x}_{u})-12z = 90,$$

$$82u-12z = (7\cdot 12-2)u-12z = 12(\underbrace{7u-z}_{v})-2u = 90$$

$$12v-2u = 6\cdot 2v-2u = 2(\underbrace{6v-u}_{w}) = 2w = 90.$$

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$82u-12z=(7\cdot 12-2)u-12z=12(\underbrace{7u-z}_{v})-2u=90$$

$$12v-2u=6\cdot 2v-2u=2(\underbrace{6v-u}_{w})=2w=90.$$

Innen $w=45$.

$$7640x+234y=(33\cdot 234-82)x+234y=234(\underbrace{33x+y}_{z})-82x=90,$$

$$234z-82x=(3\cdot 82-12)z-82x=82(\underbrace{3z-x}_{u})-12z=90,$$

$$82u-12z=(7\cdot 12-2)u-12z=12(\underbrace{7u-z}_{v})-2u=90$$

$$12v-2u=6\cdot 2v-2u=2(\underbrace{6v-u}_{w})=2w=90.$$

Innen $w=45$. Most két lehetőségünk van.

Az egyik lehetőség az, hogy a $6v - u = w = 45$ helyettesítésnél azt mondjuk, hogy legyen $v \in \mathbf{Z}$ tetszőleges, azaz paraméter, Az egyik lehetőség az, hogy a $6v - u = w = 45$ helyettesítésnél azt mondjuk, hogy legyen $v \in \mathbf{Z}$ tetszőleges, azaz paraméter, v függvényében fejezzük ki u-t, és

Az egyik lehetőség az, hogy a $6v - u = w = 45$ helyettesítésnél azt mondjuk, hogy legyen $v \in \mathbf{Z}$ tetszőleges, azaz paraméter, v függvényében fejezzük ki u-t, és haladunk visszafelé a helyettesítések mentén, és az eredményben is benne marad a v paraméter, azaz ily módon az általános megoldást kapjuk. (

Az egyik lehetőség az, hogy a $6v - u = w = 45$ helyettesítésnél azt mondjuk, hogy legyen $v \in \mathbf{Z}$ tetszőleges, azaz paraméter, v függvényében fejezzük ki u-t, és haladunk visszafelé a helyettesítések mentén, és az eredményben is benne marad a v paraméter, azaz ily módon az általános megoldást kapjuk. (Ennél a módszernél nem kell az általános megoldás képletét tudni, viszont a v paraméter cipelgetése kissé növeli a munkát.

Az egyik lehetőség az, hogy a $6v - u = w = 45$ helyettesítésnél azt mondjuk, hogy legyen $v \in \mathbf{Z}$ tetszőleges, azaz paraméter, v függvényében fejezzük ki u-t, és haladunk visszafelé a helyettesítések mentén, és az eredményben is benne marad a v paraméter, azaz ily módon az általános megoldást kapjuk. (Ennél a módszernél nem kell az általános megoldás képletét tudni, viszont a v paraméter cipelgetése kissé növeli a munkát. Nem lehet összetéveszteni, hogy az elején u és v közül melyiket fejezzük ki és melyik legyen a tetszőleges paraméter:

Az egyik lehetőség az, hogy a $6v - u = w = 45$ helyettesítésnél azt mondjuk, hogy legyen $v \in \mathbf{Z}$ tetszőleges, azaz paraméter, v függvényében fejezzük ki u-t, és haladunk visszafelé a helyettesítések mentén, és az eredményben is benne marad a v paraméter, azaz ily módon az általános megoldást kapjuk. (Ennél a módszernél nem kell az általános megoldás képletét tudni, viszont a v paraméter cipelgetése kissé növeli a munkát. Nem lehet összetéveszteni, hogy az elején u és v közül melyiket fejezzük ki és melyik legyen a tetszőleges paraméter: v-t ki se tudnánk fejezni *tetszőleges* u esetén, hiszen nem minden egész szám osztható 6-tal.)

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter,

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v-u = w = 45$-ből
$u =$

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z =$

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v =$

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v = 41v - 315$, A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v = 41v - 315$, $3z - x = u$-ból

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v = 41v - 315$, $3z - x = u$-ból $x =$

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v = 41v - 315$, $3z - x = u$-ból $x = 3z - u =$

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v = 41v - 315$, $3z - x = u$-ból $x = 3z - u = 3(41v - 315) - (6v - 45) = 117v - 900$, A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v-u=w=45$-ből $u=6v-45$, $7u-z=v$-ből $z=7u-v=7(6v-45)-v=41v-315$, $3z-x=u$-ból $x=3z-u=3(41v-315)-(6v-45)=117v-900$, és végül

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v-u = w = 45$-ből $u = 6v-45$, $7u-z = v$-ből $z = 7u-v = 7(6v-45)-v = 41v-315$, $3z-x = u$-ból $x = 3z-u = 3(41v-315)-(6v-45) = 117v-900$, és végül $33x + y = z$-ből

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v = 41v - 315$, $3z - x = u$-ból $x = 3z - u = 3(41v - 315) - (6v - 45) = 117v - 900$, és végül $33x + y = z$-ből $y = z - 33x =$

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v-u = w = 45$-ből $u = 6v-45$, $7u-z = v$-ből $z = 7u-v = 7(6v-45)-v = 41v-315$, $3z-x = u$-ból $x = 3z-u = 3(41v-315)-(6v-45) = 117v-900$, és végül $33x+y = z$-ből $y = z-33x = (41v-315)-33(117v-900) =$

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v - u = w = 45$-ből $u = 6v - 45$, $7u - z = v$-ből $z = 7u - v = 7(6v - 45) - v = 41v - 315$, $3z - x = u$-ból $x = 3z - u = 3(41v - 315) - (6v - 45) = 117v - 900$, és végül $33x + y = z$-ből $y = z - 33x = (41v - 315) - 33(117v - 900) = -3820v + 29385$. Tehát

A jelen esetben: $v \in \mathbf{Z}$ tetszőleges paraméter, $6v-u=w=45$-ből $u=6v-45$, $7u-z=v$-ből $z=7u-v=7(6v-45)-v=41v-315$, $3z-x=u$-ból $x=3z-u=3(41v-315)-(6v-45)=117v-900$, és végül $33x+y=z$-ből $y=z-33x=(41v-315)-33(117v-900)=-3820v+29385$. Tehát az általános megoldás: $x=117v-900$ és $y=-3820v+29385$ $(v \in \mathbf{Z})$.

A másik lehetőség az, hogy csak egy partikuláris megoldást szeretnénk kiszámolni —

A másik lehetőség az, hogy csak egy partikuláris megoldást szeretnénk kiszámolni — és az általános megoldást a képlet alapján írjuk fel. (

A másik lehetőség az, hogy csak egy partikuláris megoldást szeretnénk kiszámolni — és az általános megoldást a képlet alapján írjuk fel. (Ehhez persze ismerni kell az együtthatók legnagyobb közös osztóját!)

A másik lehetőség az, hogy csak egy partikuláris megoldást szeretnénk kiszámolni — és az általános megoldást a képlet alapján írjuk fel. (Ehhez persze ismerni kell az együtthatók legnagyobb közös osztóját!) Ilyenkor v-nek mindjárt az elején egy konkrét értéket adunk (

A másik lehetőség az, hogy csak egy partikuláris megoldást szeretnénk kiszámolni — és az általános megoldást a képlet alapján írjuk fel. (Ehhez persze ismerni kell az együtthatók legnagyobb közös osztóját!) Ilyenkor v-nek mindjárt az elején egy konkrét értéket adunk (arra törekedve, hogy ne lépjenek fel túl nagy abszolút értékű számok).

A másik lehetőség az, hogy csak egy partikuláris megoldást szeretnénk kiszámolni — és az általános megoldást a képlet alapján írjuk fel. (Ehhez persze ismerni kell az együtthatók legnagyobb közös osztóját!) Ilyenkor v-nek mindjárt az elején egy konkrét értéket adunk (arra törekedve, hogy ne lépjenek fel túl nagy abszolút értékű számok). Nézzünk erre is példát —

A másik lehetőség az, hogy csak egy partikuláris megoldást szeretnénk kiszámolni — és az általános megoldást a képlet alapján írjuk fel. (Ehhez persze ismerni kell az együtthatók legnagyobb közös osztóját!) Ilyenkor v-nek mindjárt az elején egy konkrét értéket adunk (arra törekedve, hogy ne lépjenek fel túl nagy abszolút értékű számok). Nézzünk erre is példát — az előző fóliákról másoljuk ide az ott alkalmazott helyettesítéseket (amelyeket majd fordított sorrendben fogunk figyelembe venni):

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg,

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$.

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z =$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v =$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$,

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x =$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u =$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$,

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y =$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x =$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 =$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$.

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás.

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója 2 (

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója 2 (ez nem innen, hanem külön számolás árán derül ki), ezért

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója 2 (ez nem innen, hanem külön számolás árán derül ki), ezért a $7640x + 234y = 90$ diofantoszi egyenlet megoldásainak halmaza az alábbi:

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója 2 (ez nem innen, hanem külön számolás árán derül ki), ezért a $7640x + 234y = 90$ diofantoszi egyenlet megoldásainak halmaza az alábbi:

$$\{(36 + 117t, -1175 - 3820t) : t \in \mathbf{Z}\}.$$

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t választjuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója 2 (ez nem innen, hanem külön számolás árán derül ki), ezért a $7640x + 234y = 90$ diofantoszi egyenlet megoldásainak halmaza az alábbi:

$$\{(36 + 117t, -1175 - 3820t) : t \in \mathbf{Z}\}.$$

Csak első ránézésre különbözik a korábbi megoldástól!

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója 2 (ez nem innen, hanem külön számolás árán derül ki), ezért a $7640x + 234y = 90$ diofantoszi egyenlet megoldásainak halmaza az alábbi:

$$\{(36 + 117t, -1175 - 3820t) : t \in \mathbf{Z}\}.$$

Csak első ránézésre különbözik a korábbi megoldástól! Az általános megoldást vagy a megoldások halmazát bármely partikuláris megoldásból kiindulva fel lehet írni,

$$33x + y = z, \quad 3z - x = u, \quad 7u - z = v, \quad 6v - u = w = 45$$

Először u-t és v-t válasszuk meg, mondjuk $v = 8$, $u = 3$. Ekkor $z = 7u - v = 13$, $x = 3z - u = 36$, $y = z - 33x = 13 - 33 \cdot 36 = -1175$. Tehát $x_0 = 36$, $y_0 = -1175$ egy partikuláris megoldás. Mivel az együtthatók legnagyobb közös osztója 2 (ez nem innen, hanem külön számolás árán derül ki), ezért a $7640x + 234y = 90$ diofantoszi egyenlet megoldásainak halmaza az alábbi:

$$\{(36 + 117t, -1175 - 3820t) : t \in \mathbf{Z}\}.$$

Csak első ránézésre különbözik a korábbi megoldástól! Az általános megoldást vagy a megoldások halmazát bármely partikuláris megoldásból kiindulva fel lehet írni, és a különböző módszerek különböző partikuláris megoldáshoz vezethetnek.

Feladat: A Számítóközpont egy EU pályázatban 102058 eurót nyert nagy teljesítményű szerverek és hozzájuk kapcsolódó terminálok vásárlására.

Feladat: A Számítóközpont egy EU pályázatban 102058 eurót nyert nagy teljesítményű szerverek és hozzájuk kapcsolódó terminálok vásárlására. A szerverek darabja 7640 euró, a termináloké 234 euró,

Feladat: A Számítóközpont egy EU pályázatban 102058 eurót nyert nagy teljesítményű szerverek és hozzájuk kapcsolódó terminálok vásárlására. A szerverek darabja 7640 euró, a terminálok 234 euró, és pontosan 102058 eurót kell elkölteni.

Feladat: A Számítóközpont egy EU pályázatban 102058 eurót nyert nagy teljesítményű szerverek és hozzájuk kapcsolódó terminálok vásárlására. A szerverek darabja 7640 euró, a termináloké 234 euró, és pontosan 102058 eurót kell elkölteni. Hány terminált vásároltak a pályázati pénzből?

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le.

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos,

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik,

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst;

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst; továbbá

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst; továbbá $7640 \cdot (-20) + 234 \cdot 653 = 2$. Beszorozva $\frac{102058}{2} =$

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst; továbbá $7640 \cdot (-20) + 234 \cdot 653 = 2$. Beszorozva $\frac{102058}{2} = 51029$-cel:

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst; továbbá $7640 \cdot (-20) + 234 \cdot 653 = 2$. Beszorozva $\frac{102058}{2} = 51029$-cel:

$$7640 \cdot (-1020580) + 234 \cdot 33321937 = 102058.$$

Tehát

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst; továbbá $7640 \cdot (-20) + 234 \cdot 653 = 2$. Beszorozva $\frac{102058}{2} =$ 51029-cel:

$$7640 \cdot (-1020580) + 234 \cdot 33321937 = 102058.$$

Tehát az $x_0 = -1020580$, $y_0 =$

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst; továbbá $7640 \cdot (-20) + 234 \cdot 653 = 2$. Beszorozva $\frac{102058}{2} = 51029$-cel:

$$7640 \cdot (-1020580) + 234 \cdot 33321937 = 102058.$$

Tehát az $x_0 = -1020580$, $y_0 = 33321937$ egy

Megoldás: A szerverek számát x-szel, a terminálokét pedig y-nal jelölve a problémát a $7640x+234y = 102058$ diofantoszi egyenlet írja le. Ezen egyenlet baloldala az előző egyenlet baloldalával azonos, tehát a korábbi számolással most az adódik, hogy az együtthatók legnagyobb közös osztója 2, ami osztja a konstanst; továbbá $7640 \cdot (-20) + 234 \cdot 653 = 2$. Beszorozva $\frac{102058}{2} = 51029$-cel:

$$7640 \cdot (-1020580) + 234 \cdot 33321937 = 102058.$$

Tehát az $x_0 = -1020580$, $y_0 = 33321937$ egy partikuláris megoldás. Az általános megoldás pedig

$$x = -1020580 + 117t, \qquad y = 33321937 - 3820t \qquad (t \in \mathbf{Z}).$$

Értelemszerűen $x, y \geq 0$, tehát

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0$$

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722,91 \quad \text{és}$$

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722,91 \quad \text{és}$$

$$33321937 - 3820t \geq 0 \Longrightarrow t \leq 8723,02.$$

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722,91 \quad \text{és}$$

$$33321937 - 3820t \geq 0 \Longrightarrow t \leq 8723,02.$$

Az egyetlen olyan t egész szám, amely ezen feltételeknek eleget tesz: a $t = 8723$.

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722,91 \quad \text{és}$$

$$33321937 - 3820t \geq 0 \Longrightarrow t \leq 8723,02.$$

Az egyetlen olyan t egész szám, amely ezen feltételeknek eleget tesz: a $t = 8723$. Ezért

$$x = -1020580 + 117t =$$

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722,91 \quad \text{és}$$

$$33321937 - 3820t \geq 0 \Longrightarrow t \leq 8723,02.$$

Az egyetlen olyan t egész szám, amely ezen feltételeknek eleget tesz: a $t = 8723$. Ezért

$$x = -1020580 + 117t = -1020580 + 117 \cdot 8723 = 11,$$

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722{,}91 \quad \text{és}$$

$$33321937 - 3820t \geq 0 \Longrightarrow t \leq 8723{,}02.$$

Az egyetlen olyan t egész szám, amely ezen feltételeknek eleget tesz: a $t = 8723$. Ezért

$$x = -1020580 + 117t = -1020580 + 117 \cdot 8723 = 11,$$

$$y = 33321937 - 3820t =$$

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722,91 \quad \text{és}$$

$$33321937 - 3820t \geq 0 \Longrightarrow t \leq 8723,02.$$

Az egyetlen olyan t egész szám, amely ezen feltételeknek eleget tesz: a $t = 8723$. Ezért

$$x = -1020580 + 117t = -1020580 + 117 \cdot 8723 = 11,$$
$$y = 33321937 - 3820t = y = 33321937 - 3820 \cdot 8723 = 77.$$

Értelemszerűen $x, y \geq 0$, tehát

$$-1020580 + 117t \geq 0 \Longrightarrow t \geq 8722,91 \quad \text{és}$$

$$33321937 - 3820t \geq 0 \Longrightarrow t \leq 8723,02.$$

Az egyetlen olyan t egész szám, amely ezen feltételeknek eleget tesz: a $t = 8723$. Ezért

$$x = -1020580 + 117t = -1020580 + 117 \cdot 8723 = 11,$$
$$y = 33321937 - 3820t = y = 33321937 - 3820 \cdot 8723 = 77.$$

Tehát 77 terminált vásároltak.

Szemben az előző feladat nagy számaival, a következő feladat a vizsgán is megjelenhetne. (Lesznek hasonlók!)

Feladat: $|\{(x, y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| =?$

Megoldás: Mivel $\text{ln.k.o.}(76, 43) = 1$ (

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}|=?$

Megoldás: Mivel $\text{ln.k.o.}(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

Feladat: $|\{(x, y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| = ?$

Megoldás: Mivel $\text{ln.k.o.}(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 =$$

Feladat: $|\{(x, y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| =?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y =$$

Feladat: $|\{(x,y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z})$$

Feladat: $|\{(x, y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x$$

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}|=?$

Megoldás: Mivel ln.k.o.$(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14=76x-43y=43(\underbrace{2x-y}_{z})-10x=10(\underbrace{4z-x}_{u})+3z$$
$$=$$

Feladat: $|\{(x, y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \le x \le 200\}| =?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x = 10(\underbrace{4z - x}_{u}) + 3z$$
$$= 3(\underbrace{3u + z}_{v}) + u.$$

Feladat: $|\{(x,y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre", hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x = 10(\underbrace{4z - x}_{u}) + 3z$$
$$= 3(\underbrace{3u + z}_{v}) + u.$$

Legyen

Feladat: $|\{(x,y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \le x \le 200\}| =?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x = 10(\underbrace{4z - x}_{u}) + 3z$$
$$= 3(\underbrace{3u + z}_{v}) + u.$$

Legyen $v = 4$,

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| =?$

Megoldás: Mivel ln.k.o.$(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x-43y = 43(\underbrace{2x-y}_{z})-10x = 10(\underbrace{4z-x}_{u})+3z$$
$$= 3(\underbrace{3u+z}_{v})+u.$$

Legyen $v=4$, $u=2$,

Feladat: $|\{(x,y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| =?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x = 10(\underbrace{4z - x}_{u}) + 3z$$
$$= 3(\underbrace{3u + z}_{v}) + u.$$

Legyen $v = 4$, $u = 2$, $z =$

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x-43y = 43(\underbrace{2x-y}_{z}) - 10x = 10(\underbrace{4z-x}_{u}) + 3z$$
$$= 3(\underbrace{3u+z}_{v}) + u.$$

Legyen $v=4$, $u=2$, $z=v-3u=$

Feladat: $|\{(x,y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x = 10(\underbrace{4z - x}_{u}) + 3z$$
$$= 3(\underbrace{3u + z}_{v}) + u.$$

Legyen $v = 4$, $u = 2$, $z = v - 3u = -2$,

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x-43y = 43(\underbrace{2x-y}_{z})-10x = 10(\underbrace{4z-x}_{u})+3z$$
$$= 3(\underbrace{3u+z}_{v})+u.$$

Legyen $v=4$, $u=2$, $z=v-3u=-2$, $x=$

Feladat: $|\{(x,y)\in\mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| =?$

Megoldás: Mivel ln.k.o.$(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14=76x-43y=43(\underbrace{2x-y}_{z})-10x=10(\underbrace{4z-x}_{u})+3z$$
$$=3(\underbrace{3u+z}_{v})+u.$$

Legyen $v=4,\ u=2,\ z=v-3u=\ -2,\ x=4z-u=$

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| = ?$

Megoldás: Mivel $\text{ln.k.o.}(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x-y}_{z}) - 10x = 10(\underbrace{4z-x}_{u}) + 3z$$

$$= 3(\underbrace{3u+z}_{v}) + u.$$

Legyen $v=4$, $u=2$, $z=v-3u=\ -2$, $x=4z-u=\ -10$,

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14$ és $100\le x\le 200\}| =?$

Megoldás: Mivel ln.k.o.$(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14=76x-43y=43(\underbrace{2x-y}_{z})-10x=10(\underbrace{4z-x}_{u})+3z$$
$$=3(\underbrace{3u+z}_{v})+u.$$

Legyen $v=4$, $u=2$, $z=v-3u=\,-2$, $x=4z-u=\,-10$,
(y-ra most nem is lesz szükség, de az sem nehéz: $y=$

Feladat: $|\{(x, y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre", hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x = 10(\underbrace{4z - x}_{u}) + 3z$$
$$= 3(\underbrace{3u + z}_{v}) + u.$$

Legyen $v = 4$, $u = 2$, $z = v - 3u = -2$, $x = 4z - u = -10$,
(y-ra most nem is lesz szükség, de az sem nehéz: $y = 2x - z =$

Feladat: $|\{(x,y) \in \mathbf{Z}^2 : 76x - 43y = 14 \text{ és } 100 \leq x \leq 200\}| = ?$

Megoldás: Mivel ln.k.o.$(76, 43) = 1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x - 43y = 43(\underbrace{2x - y}_{z}) - 10x = 10(\underbrace{4z - x}_{u}) + 3z$$
$$= 3(\underbrace{3u + z}_{v}) + u.$$

Legyen $v = 4$, $u = 2$, $z = v - 3u = -2$, $x = 4z - u = -10$, (y-ra most nem is lesz szükség, de az sem nehéz: $y = 2x - z = -18$.)

Feladat: $|\{(x,y)\in\mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| =?$

Megoldás: Mivel $\text{lnko}(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x-43y = 43(\underbrace{2x-y}_{z})-10x = 10(\underbrace{4z-x}_{u})+3z$$
$$= 3(\underbrace{3u+z}_{v})+u.$$

Legyen $v=4$, $u=2$, $z=v-3u=-2$, $x=4z-u=-10$, (y-ra most nem is lesz szükség, de az sem nehéz: $y=2x-z=-18$.) Az egyenlet általános megoldása:

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| = ?$

Megoldás: Mivel $\text{ln.k.o.}(76,43)=1$ („ránézésre", hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x-43y = 43(\underbrace{2x-y}_{z}) - 10x = 10(\underbrace{4z-x}_{u}) + 3z$$
$$= 3(\underbrace{3u+z}_{v}) + u.$$

Legyen $v=4$, $u=2$, $z=v-3u=-2$, $x=4z-u=-10$, (y-ra most nem is lesz szükség, de az sem nehéz: $y=2x-z=-18$.) Az egyenlet általános megoldása: $x=-10-43t$ és $y=-18-76t$).

Feladat: $|\{(x,y)\in \mathbf{Z}^2 : 76x-43y=14 \text{ és } 100\le x\le 200\}| = ?$

Megoldás: Mivel $\text{ln.k.o.}(76,43)=1$ („ránézésre”, hiszen a 43 prímszám), elég az egyenlet egy partikuláris megoldásást keresni helyettesítgetésekkel:

$$14 = 76x-43y = 43(\underbrace{2x-y}_{z}) - 10x = 10(\underbrace{4z-x}_{u}) + 3z$$
$$= 3(\underbrace{3u+z}_{v}) + u.$$

Legyen $v=4$, $u=2$, $z=v-3u=\ -2$, $x=4z-u=\ -10$, (y-ra most nem is lesz szükség, de az sem nehéz: $y=2x-z=\ -18$.) Az egyenlet általános megoldása: $x=-10-43t$ és $y=-18-76t$). Nézzük most az egyenlőtlenséget:

$$100 \leq x \leq 200$$

$$100 \leq x \leq 200$$
$$100 \leq -10 - 43t \leq 200$$

$$100 \leq x \leq 200$$

$$100 \leq -10 - 43t \leq 200$$

$$-100$$

$$100 \le x \le 200$$
$$100 \le -10 - 43t \le 200$$
$$-100 \ge 10 + 43t \ge -200$$

$$
\begin{aligned}
100 &\leq x \leq 200 \\
100 &\leq -10 - 43t \leq 200 \\
-100 &\geq 10 + 43t \geq -200 \\
-110 &\geq 43t \geq -210
\end{aligned}
$$

$$100 \leq x \leq 200$$
$$100 \leq -10 - 43t \leq 200$$
$$-100 \geq 10 + 43t \geq -200$$
$$-110 \geq 43t \geq -210$$
$$-\frac{110}{43} \geq t \geq -\frac{210}{43}$$

$$100 \leq x \leq 200$$
$$100 \leq -10 - 43t \leq 200$$
$$-100 \geq 10 + 43t \geq -200$$
$$-110 \geq 43t \geq -210$$
$$-\frac{110}{43} \geq t \geq -\frac{210}{43}$$
$$-2,6 \geq t \geq -4,9$$

$$
\begin{gathered}
100 \leq x \leq 200 \\
100 \leq -10 - 43t \leq 200 \\
-100 \geq 10 + 43t \geq -200 \\
-110 \geq 43t \geq -210 \\
-\frac{110}{43} \geq t \geq -\frac{210}{43} \\
-2{,}6 \geq t \geq -4{,}9 \\
t \in \{-4, -3\}.
\end{gathered}
$$

$$100 \leq x \leq 200$$
$$100 \leq -10 - 43t \leq 200$$
$$-100 \geq 10 + 43t \geq -200$$
$$-110 \geq 43t \geq -210$$
$$-\frac{110}{43} \geq t \geq -\frac{210}{43}$$
$$-2,6 \geq t \geq -4,9$$
$$t \in \{-4, -3\}.$$

Ezért az eredmény:

$$
\begin{gathered}
100 \leq x \leq 200 \\
100 \leq -10 - 43t \leq 200 \\
-100 \geq 10 + 43t \geq -200 \\
-110 \geq 43t \geq -210 \\
-\frac{110}{43} \geq t \geq -\frac{210}{43} \\
-2,6 \geq t \geq -4,9 \\
t \in \{-4, -3\}.
\end{gathered}
$$

Ezért az eredmény: a kérdéses halmaz **kételemű**.

Számelméleti kongruenciák

Definíció: Legyen $a, b, m \in \mathbf{Z}$. Akkor mondjuk, hogy a **kongruens** b-vel **modulo** m, jelölésben

$$a \equiv b \pmod{m},$$

ha $m \mid a - b$ (

Számelméleti kongruenciák

Definíció: Legyen $a, b, m \in \mathbf{Z}$. Akkor mondjuk, hogy a **kongruens** b-vel **modulo** m, jelölésben

$$a \equiv b \pmod{m},$$

ha $m \mid a - b$ (vagy, ami ezzel ekvivalens, a és b ugyanazt a maradékot adja m-mel osztva).

Számelméleti kongruenciák

Definíció: Legyen $a, b, m \in \mathbf{Z}$. Akkor mondjuk, hogy a **kongruens** b-vel **modulo** m, jelölésben

$$a \equiv b \pmod{m},$$

ha $m \mid a - b$ (vagy, ami ezzel ekvivalens, a és b ugyanazt a maradékot adja m-mel osztva).

Pl. $12 \equiv 1342 \pmod{10}$,

Számelméleti kongruenciák

Definíció: Legyen $a, b, m \in \mathbf{Z}$. Akkor mondjuk, hogy a **kongruens** b-vel **modulo** m, jelölésben

$$a \equiv b \pmod{m},$$

ha $m \mid a - b$ (vagy, ami ezzel ekvivalens, a és b ugyanazt a maradékot adja m-mel osztva).

Pl. $12 \equiv 1342 \pmod{10}$, $40 \equiv 19 \pmod{3}$, de

Számelméleti kongruenciák

Definíció: Legyen $a, b, m \in \mathbf{Z}$. Akkor mondjuk, hogy a **kongruens** b-vel **modulo** m, jelölésben

$$a \equiv b \pmod{m},$$

ha $m \mid a - b$ (vagy, ami ezzel ekvivalens, a és b ugyanazt a maradékot adja m-mel osztva).

Pl. $12 \equiv 1342 \pmod{10}$, $40 \equiv 19 \pmod{3}$, de $30 \not\equiv 40 \pmod{7}$.

Megjegyzés: Mivel oszthatósági szempontból a **modulus előjele** nem érdekes,

Számelméleti kongruenciák

Definíció: Legyen $a, b, m \in \mathbf{Z}$. Akkor mondjuk, hogy a **kongruens** b-vel **modulo** m, jelölésben

$$a \equiv b \pmod{m},$$

ha $m \mid a - b$ (vagy, ami ezzel ekvivalens, a és b ugyanazt a maradékot adja m-mel osztva).

Pl. $12 \equiv 1342 \pmod{10}$, $40 \equiv 19 \pmod{3}$, de $30 \not\equiv 40 \pmod{7}$.

Megjegyzés: Mivel oszthatósági szempontból a **modulus előjele** nem érdekes, azaz $a \equiv b \pmod{m} \iff a \equiv b \pmod{-m}$, ezért

Számelméleti kongruenciák

Definíció: Legyen $a, b, m \in \mathbf{Z}$. Akkor mondjuk, hogy a **kongruens** b-vel **modulo** m, jelölésben

$$a \equiv b \pmod{m},$$

ha $m \mid a - b$ (vagy, ami ezzel ekvivalens, a és b ugyanazt a maradékot adja m-mel osztva).

Pl. $12 \equiv 1342 \pmod{10}$, $40 \equiv 19 \pmod{3}$, de $30 \not\equiv 40 \pmod{7}$.

Megjegyzés: Mivel oszthatósági szempontból a **modulus előjele** nem érdekes, azaz $a \equiv b \pmod{m} \iff a \equiv b \pmod{-m}$, ezért a továbbiakban feltesszük, hogy $m \geq 0$.

24. Tétel. *Rögzített* $m \in \mathbf{N}_0$ *esetén a modulo* m **számelméleti kongruencia** *(röviden csak kongruencia),*

24. Tétel. *Rögzített* $m \in \mathbf{N}_0$ *esetén a modulo* m **számelméleti kongruencia** *(röviden csak kongruencia), azaz az*

$$\{(a,b) \in \mathbf{Z}^2 : a \equiv b \pmod{m}\} \subseteq \mathbf{Z}^2$$

reláció

24. Tétel. *Rögzített* $m \in \mathbf{N}_0$ *esetén a modulo* m **számelméleti kongruencia** *(röviden csak kongruencia), azaz az*

$$\{(a,b) \in \mathbf{Z}^2 : a \equiv b \pmod{m}\} \subseteq \mathbf{Z}^2$$

reláció ekvivalencia a $\mathbf{Z}$ *halmazon. Továbbá*

24. Tétel. *Rögzített* $m \in \mathbf{N}_0$ *esetén a modulo* m **számelméleti kongruencia** *(röviden csak kongruencia), azaz az*

$$\{(a,b) \in \mathbf{Z}^2 : a \equiv b \pmod{m}\} \subseteq \mathbf{Z}^2$$

reláció ekvivalencia a $\mathbf{Z}$ *halmazon. Továbbá tetszőleges* $a_1, b_1, a_2, b_2 \in \mathbf{Z}$ *esetén*

$$\textit{ha } a_1 \equiv a_2 \pmod{m} \textit{ és } b_1 \equiv b_2 \pmod{m} \textit{ akkor}$$

24. Tétel. *Rögzített* $m \in \mathbf{N}_0$ *esetén a modulo* m **számelméleti kongruencia** *(röviden csak kongruencia), azaz az*

$$\{(a,b) \in \mathbf{Z}^2 : a \equiv b \pmod{m}\} \subseteq \mathbf{Z}^2$$

reláció ekvivalencia a $\mathbf{Z}$ *halmazon. Továbbá tetszőleges* $a_1, b_1, a_2, b_2 \in \mathbf{Z}$ *esetén*

$$\textit{ha } a_1 \equiv a_2 \pmod{m} \textit{ és } b_1 \equiv b_2 \pmod{m} \textit{ akkor}$$
$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \quad \textit{és} \quad a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

A tétel második mondatát szavakban úgy lehetne (pontatlanul) mondani, hogy

A tétel második mondatát szavakban úgy lehetne (pontatlanul) mondani, hogy a kongruenciákat össze szabad adni és szorozni, A tétel második mondatát szavakban úgy lehetne (pontatlanul) mondani, hogy a kongruenciákat össze szabad adni és szorozni, más szavakkal: összeg tagjait velük kongruensekre cserélve az eredetivel kongruens összeget kapunk,

A tétel második mondatát szavakban úgy lehetne (pontatlanul) mondani, hogy a kongruenciákat össze szabad adni és szorozni, más szavakkal: összeg tagjait velük kongruensekre cserélve az eredetivel kongruens összeget kapunk, szorzat tényezőit velük kongruensekre cserélve az eredetivel kongruenset kapunk:

A tétel második mondatát szavakban úgy lehetne (pontatlanul) mondani, hogy a kongruenciákat össze szabad adni és szorozni, más szavakkal: összeg tagjait velük kongruensekre cserélve az eredetivel kongruens összeget kapunk, szorzat tényezőit velük kongruensekre cserélve az eredetivel kongruenset kapunk:

$$\text{ha } a_1 \equiv a_2 \pmod m \text{ és } b_1 \equiv b_2 \pmod m \text{ akkor}$$

A tétel második mondatát szavakban úgy lehetne (pontatlanul) mondani, hogy a kongruenciákat össze szabad adni és szorozni, más szavakkal: összeg tagjait velük kongruensekre cserélve az eredetivel kongruens összeget kapunk, szorzat tényezőit velük kongruensekre cserélve az eredetivel kongruenset kapunk:

$$\text{ha } a_1 \equiv a_2 \pmod{m} \text{ és } b_1 \equiv b_2 \pmod{m} \text{ akkor}$$
$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \quad \text{és} \quad a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

Más szóval: a kongruenciákkal

A tétel második mondatát szavakban úgy lehetne (pontatlanul) mondani, hogy a kongruenciákat össze szabad adni és szorozni, más szavakkal: összeg tagjait velük kongruensekre cserélve az eredetivel kongruens összeget kapunk, szorzat tényezőit velük kongruensekre cserélve az eredetivel kongruenset kapunk:

$$\text{ha } a_1 \equiv a_2 \pmod m \text{ és } b_1 \equiv b_2 \pmod m \text{ akkor}$$
$$a_1 + b_1 \equiv a_2 + b_2 \pmod m \quad \text{és} \quad a_1 b_1 \equiv a_2 b_2 \pmod m.$$

Más szóval: a kongruenciákkal sok (de nem minden!) vonatkozásban úgy számolunk, mint az egyenlőséggel!

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben.

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (azaz *egyenlő marad*) amikor a tényezői helyett velük egyenlőket veszünk, Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (azaz *egyenlő marad*) amikor a tényezői helyett velük egyenlőket veszünk, ugyanúgy a szorzat *kongruens marad*, ha a tényezői helyett velük kongruenseket veszünk. (

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (azaz *egyenlő marad*) amikor a tényezői helyett velük egyenlőket veszünk, ugyanúgy a szorzat *kongruens marad*, ha a tényezői helyett velük kongruenseket veszünk. (A rend kedvéért említjük csak, Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (azaz *egyenlő marad*) amikor a tényezői helyett velük egyenlőket veszünk, ugyanúgy a szorzat *kongruens marad*, ha a tényezői helyett velük kongruenseket veszünk. (A rend kedvéért említjük csak, hogy van olyan — pl. elemszámmal kapcsolatos — formula is, amelyik különbsége tesz a két eset között.)

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (azaz *egyenlő marad*) amikor a tényezői helyett velük egyenlőket veszünk, ugyanúgy a szorzat *kongruens marad*, ha a tényezői helyett velük kongruenseket veszünk. (A rend kedvéért említjük csak, hogy van olyan — pl. elemszámmal kapcsolatos — formula is, amelyik különbséget tesz a két eset között.)

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (azaz *egyenlő marad*) amikor a tényezői helyett velük egyenlőket veszünk, ugyanúgy a szorzat *kongruens marad*, ha a tényezői helyett velük kongruenseket veszünk. (A rend kedvéért említjük csak, hogy van olyan — pl. elemszámmal kapcsolatos — formula is, amelyik különbsége tesz a két eset között.)

Azaz: a modulo m kongruenciával

Lényegében arról van szó, hogy mindegy, hogy a $+, \cdot$ kétváltozós függvényjelek mellett az egyenlőségjelet vagy a modulo m kongruencia jelét vesszül hozzá az elsőrendű nyelvhez, a szokásos $(\mathbf{Z}; +, \cdot)$ interpretáció esetén számos formula egyszerre teljesül mindkét esetben. Pl. ahogy egy szorzat nem változik (azaz *egyenlő marad*) amikor a tényezői helyett velük egyenlőket veszünk, ugyanúgy a szorzat *kongruens marad*, ha a tényezői helyett velük kongruenseket veszünk. (A rend kedvéért említjük csak, hogy van olyan — pl. elemszámmal kapcsolatos — formula is, amelyik különbséget tesz a két eset között.)

Azaz: a modulo m kongruenciával sok (de nem minden) szempontból úgy számolhatunk, mintha egyenlőség lenne.

A modulo m kongruencia igen gyakran fellépő matematikai alapfogalom, még a konkrét programíráshoz is köze van, hiszen pl. a Pascal nyelvben a mod művelet ezt támogatja, A modulo m kongruencia igen gyakran fellépő matematikai alapfogalom, még a konkrét programíráshoz is köze van, hiszen pl. a Pascal nyelvben a mod művelet ezt támogatja, pl. elképzelhető az alábbi:

A modulo m kongruencia igen gyakran fellépő matematikai alapfogalom, még a konkrét programíráshoz is köze van, hiszen pl. a Pascal nyelvben a mod művelet ezt támogatja, pl. elképzelhető az alábbi:

```
for i:= 1 to n do
 case i mod 3 of
    0: begin ... end;
    1: begin ... end;
    2: begin ... end;
end;
```

Bizonyos feladatok

Bizonyos feladatok szinte igénylik a kongruencia fogalmát.

Bizonyos feladatok szinte igénylik a kongruencia fogalmát. Pl. milyen számjegyre

Bizonyos feladatok szinte igénylik a kongruencia fogalmát. Pl. milyen számjegyre végződik egy (képlettel adott) szám.

Bizonyos feladatok szinte igénylik a kongruencia fogalmát. Pl. milyen számjegyre végződik egy (képlettel adott) szám. Vagy pl. ha 2006. február 26-a vasárnapra esik, akkor milyen napra esik február 26-a 2007-ben?

Bizonyos feladatok szinte igénylik a kongruencia fogalmát. Pl. milyen számjegyre végződik egy (képlettel adott) szám. Vagy pl. ha 2006. február 26-a vasárnapra esik, akkor milyen napra esik február 26-a 2007-ben?

Ez utóbbinak a megoldása:

Bizonyos feladatok szinte igénylik a kongruencia fogalmát. Pl. milyen számjegyre végződik egy (képlettel adott) szám. Vagy pl. ha 2006. február 26-a vasárnapra esik, akkor milyen napra esik február 26-a 2007-ben?

Ez utóbbinak a megoldása: Mivel

Bizonyos feladatok szinte igénylik a kongruencia fogalmát. Pl. milyen számjegyre végződik egy (képlettel adott) szám. Vagy pl. ha 2006. február 26-a vasárnapra esik, akkor milyen napra esik február 26-a 2007-ben?

Ez utóbbinak a megoldása: Mivel $365 \equiv 1 \pmod 7$ ezért egy év múlva pontosan olyan nap lesz, mint egy nap múlva, azaz

Bizonyos feladatok szinte igénylik a kongruencia fogalmát. Pl. milyen számjegyre végződik egy (képlettel adott) szám. Vagy pl. ha 2006. február 26-a vasárnapra esik, akkor milyen napra esik február 26-a 2007-ben?

Ez utóbbinak a megoldása: Mivel $365 \equiv 1 \pmod 7$ ezért egy év múlva pontosan olyan nap lesz, mint egy nap múlva, azaz hétfő.

Bizonyítás:

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható.

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük:

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod m$ és $b_1 \equiv b_2 \pmod m$, akkor

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$a_1 b_1 - a_2 b_2$

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$a_1b_1 - a_2b_2 = a_1b_1 -$

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2$$

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 =$$

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod m$ és $b_1 \equiv b_2 \pmod m$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1$$

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2)$$

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$$

is osztható m-mel, azaz $a_1b_1 \equiv a_2b_2 \pmod{m}$.

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2) b_2$$

is osztható m-mel, azaz $a_1 b_1 \equiv a_2 b_2 \pmod{m}$. Q.e.d.

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod m$ és $b_1 \equiv b_2 \pmod m$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2) b_2$$

is osztható m-mel, azaz $a_1 b_1 \equiv a_2 b_2 \pmod m$. Q.e.d.

Megjegyzendő, hogy — a reflexivitás miatt —

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod m$ és $b_1 \equiv b_2 \pmod m$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1 b_1 - a_2 b_2 = a_1 b_1 - a_1 b_2 + a_1 b_2 - a_2 b_2 = a_1(b_1 - b_2) + (a_1 - a_2) b_2$$

is osztható m-mel, azaz $a_1 b_1 \equiv a_2 b_2 \pmod m$. Q.e.d.

Megjegyzendő, hogy — a reflexivitás miatt — a tételből az is adódik, hogy pl. $a \equiv b \pmod m$-ből $ac \equiv bc \pmod m$.

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod m$ és $b_1 \equiv b_2 \pmod m$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$$

is osztható m-mel, azaz $a_1b_1 \equiv a_2b_2 \pmod m$. Q.e.d.

Megjegyzendő, hogy — a reflexivitás miatt — a tételből az is adódik, hogy pl. $a \equiv b \pmod m$-ből $ac \equiv bc \pmod m$. Az is világos, hogy a modulo 0 kongruencia az egyenlőségreláció,

Bizonyítás: A tétel az oszthatóság megismert szabályainak birtokában igen könnyen igazolható. Csak a legnezebb részét ismertetjük: ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor $m \mid a_1 - a_2$ és $m \mid b_1 - b_2$, és ezért

$$a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$$

is osztható m-mel, azaz $a_1b_1 \equiv a_2b_2 \pmod{m}$. Q.e.d.

Megjegyzendő, hogy — a reflexivitás miatt — a tételből az is adódik, hogy pl. $a \equiv b \pmod{m}$-ből $ac \equiv bc \pmod{m}$. Az is világos, hogy a modulo 0 kongruencia az egyenlőségreláció, a modulo 1 kongruencia pedig a teljes reláció (azaz $\mathbf{Z}^2$).

4. Következmény. *(***Néhány oszthatósági szabály***)* *Legyen* $n \in \mathbb{N}$*. Jelölje* s *az* n *(tizes számrendszerbeli) számjegyeinek összegét,* v *pedig a számjegyeinek váltakozó előjellel vett összegét (mindegy, hogy melyik előjellel kezdve).*

(a) $3 \mid n \iff 3 \mid s$.

4. Következmény. *(***Néhány oszthatósági szabály***)* *Legyen* $n \in \mathbb{N}$*. Jelölje* s *az* n *(tizes számrendszerbeli) számjegyeinek összegét,* v *pedig a számjegyeinek váltakozó előjellel vett összegét (mindegy, hogy melyik előjellel kezdve).*

(a) $3 \mid n \iff 3 \mid s$*. Hasonlóan,* $9 \mid n \iff 9 \mid s$*.*

(b) $11 \mid n \iff 11 \mid v$*.*

4. Következmény. *(Néhány oszthatósági szabály)* *Legyen $n \in \mathbb{N}$. Jelölje s az n (tizes számrendszerbeli) számjegyeinek összegét, v pedig a számjegyeinek váltakozó előjellel vett összegét (mindegy, hogy melyik előjellel kezdve).*

(a) $3 \mid n \iff 3 \mid s$. *Hasonlóan,* $9 \mid n \iff 9 \mid s$.

(b) $11 \mid n \iff 11 \mid v$.

Bizonyítás: Legyenek $a_k, a_{k-1}, \ldots, a_0$ az n szám számjegyei.

4. Következmény. *(**Néhány oszthatósági szabály**)* *Legyen $n \in \mathbb{N}$. Jelölje s az n (tizes számrendszerbeli) számjegyeinek összegét, v pedig a számjegyeinek váltakozó előjellel vett összegét (mindegy, hogy melyik előjellel kezdve).*

(a) $3 \mid n \iff 3 \mid s$. *Hasonlóan,* $9 \mid n \iff 9 \mid s$.

(b) $11 \mid n \iff 11 \mid v$.

Bizonyítás: Legyenek $a_k, a_{k-1}, \ldots, a_0$ az n szám számjegyei. (Pl. ha $n = 2006$, akkor $k = 3$, $a_3 = 2$, $a_2 = a_1 = 0$ és $a_0 = 6$, azaz a_i a 10^i helyiértékű számjegy.

4. Következmény. *(Néhány oszthatósági szabály) Legyen $n \in \mathbb{N}$. Jelölje s az n (tizes számrendszerbeli) számjegyeinek összegét, v pedig a számjegyeinek váltakozó előjellel vett összegét (mindegy, hogy melyik előjellel kezdve).*

(a) $3 \mid n \iff 3 \mid s$. *Hasonlóan,* $9 \mid n \iff 9 \mid s$.

(b) $11 \mid n \iff 11 \mid v$.

Bizonyítás: Legyenek $a_k, a_{k-1}, \ldots, a_0$ az n szám számjegyei. (Pl. ha $n = 2006$, akkor $k = 3$, $a_3 = 2$, $a_2 = a_1 = 0$ és $a_0 = 6$, azaz a_i a 10^i helyiértékű számjegy. Ekkor, a kongruenciák tulajdonságai szerint, a $10 \equiv 1 \pmod 3$, $10 \equiv 1 \pmod 9$ és $10 \equiv -1 \pmod{11}$ összefüggésekből kiindulva:

$n =$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

I

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

Innen az állítás már adódik, hiszen $m \in \{3, 9, 11\}$-re (sőt, bármely $m \in \mathbf{Z}$-re is) $m \mid x \iff x \equiv 0 \pmod m$.

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3)$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

Innen az állítás már adódik, hiszen $m \in \{3, 9, 11\}$-re (sőt, bármely $m \in \mathbf{Z}$-re is) $m \mid x \iff x \equiv 0 \pmod m$. Q.e.d.

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3)$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

Innen az állítás már adódik, hiszen $m \in \{3, 9, 11\}$-re (sőt, bármely $m \in \mathbf{Z}$-re is) $m \mid x \iff x \equiv 0 \pmod m$. Q.e.d.

Az is kijött, hogy

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3$$
$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9$$
$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

Innen az állítás már adódik, hiszen $m \in \{3, 9, 11\}$-re (sőt, bármely $m \in \mathbf{Z}$-re is) $m \mid x \iff x \equiv 0 \pmod m$. Q.e.d.

Az is kijött, hogy $n \equiv s \pmod 9$ és

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3)$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

Innen az állítás már adódik, hiszen $m \in \{3, 9, 11\}$-re (sőt, bármely $m \in \mathbf{Z}$-re is) $m \mid x \iff x \equiv 0 \pmod m$. Q.e.d.

Az is kijött, hogy $n \equiv s \pmod 9$ és $n \equiv v \pmod{11}$; az utóbbinál persze lényeges

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3)$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

Innen az állítás már adódik, hiszen $m \in \{3, 9, 11\}$-re (sőt, bármely $m \in \mathbf{Z}$-re is) $m \mid x \iff x \equiv 0 \pmod m$. Q.e.d.

Az is kijött, hogy $n \equiv s \pmod 9$ és $n \equiv v \pmod{11}$; az utóbbinál persze lényeges v előjele:

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 3)$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot 1^i = \sum_{i=0}^{k} a_i = s \pmod 9)$$

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot (-1)^i = v \pmod{11}.$$

Innen az állítás már adódik, hiszen $m \in \{3, 9, 11\}$-re (sőt, bármely $m \in \mathbf{Z}$-re is) $m \mid x \iff x \equiv 0 \pmod{m}$. Q.e.d.

Az is kijött, hogy $n \equiv s \pmod 9$ és $n \equiv v \pmod{11}$; az utóbbinál persze lényeges v előjele: az egyesek (10^0) helyén álló számjegyet kell $+$ -szal venni.

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$.

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni”, azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$?

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni": azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni", azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni”, azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni”, azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni": azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni", azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, míg $a \equiv b \pmod{m}$ pedig lehet hamis is.

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni": azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni", azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, míg $a \equiv b \pmod{m}$ pedig lehet hamis is. Tehát a nullával a kongruenciát éppúgy nem szabad egyszerűsíteni, mint ahogy az egyenlőséget sem. Tehát

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni": azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni", azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, míg $a \equiv b \pmod{m}$ pedig lehet hamis is. Tehát a nullával a kongruenciát éppúgy nem szabad egyszerűsíteni, mint ahogy az egyenlőséget sem. Tehát csak annyi elvárásunk lehet, hogy

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni”, azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, míg $a \equiv b \pmod{m}$ pedig lehet hamis is. Tehát a nullával a kongruenciát éppúgy nem szabad egyszerűsíteni, mint ahogy az egyenlőséget sem. Tehát csak annyi elvárásunk lehet, hogy nemzérus c-vel egyszerűsíteni tudjunk, Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni”, azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, míg $a \equiv b \pmod{m}$ pedig lehet hamis is. Tehát a nullával a kongruenciát éppúgy nem szabad egyszerűsíteni, mint ahogy az egyenlőséget sem. Tehát csak annyi elvárásunk lehet, hogy nemzérus c-vel egyszerűsíteni tudjunk, de még **ez sem igaz**!

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni”, azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, míg $a \equiv b \pmod{m}$ pedig lehet hamis is. Tehát a nullával a kongruenciát éppúgy nem szabad egyszerűsíteni, mint ahogy az egyenlőséget sem. Tehát csak annyi elvárásunk lehet, hogy nemzérus c-vel egyszerűsíteni tudjunk, de még **ez sem igaz**! Például $6 \cdot 2 \equiv 4 \cdot 2 \pmod{4}$, de $6 \not\equiv 4 \pmod{4}$, tehát a 2-vel nem lehet a modulo 4 kongruenciát egyszerűsíteni.

Láttuk, hogy tetszőleges $c \in \mathbf{Z}$ konstanssal „a kongruenciát be lehet szorozni”: azaz ha $a \equiv b \pmod{m}$, akkor $ac \equiv bc \pmod{m}$. A kérdés mármost az, hogy „el lehet-e a kongruenciát c-vel osztani, azaz egyszerűsíteni”, azaz következik-e $ac \equiv bc \pmod{m}$-ből $a \equiv b \pmod{m}$? Nyilván nem, hiszen $a0 \equiv b0 \pmod{m}$ mindig igaz, míg $a \equiv b \pmod{m}$ pedig lehet hamis is. Tehát a nullával a kongruenciát éppúgy nem szabad egyszerűsíteni, mint ahogy az egyenlőséget sem. Tehát csak annyi elvárásunk lehet, hogy nemzérus c-vel egyszerűsíteni tudjunk, de még **ez sem igaz**! Például $6 \cdot 2 \equiv 4 \cdot 2 \pmod{4}$, de $6 \not\equiv 4 \pmod{4}$, tehát a 2-vel nem lehet a modulo 4 kongruenciát egyszerűsíteni. Ennek fényében értékelendő az alábbi tétel:

25. Tétel. *(A) Ha* $ac \equiv bc$ *(mod* m*) és* *ln.k.o.*$(m, c) = 1$*, akkor* $a \equiv b$ *(mod* m*).*

25. Tétel. *(A) Ha* $ac \equiv bc \pmod{m}$ *és lnko*$(m,c) = 1$*, akkor* $a \equiv b \pmod{m}$*. Azaz a kongruencia minden olyan tényezővel egyszerűsíthető, amelyik relatív prím a modulushoz.*

25. Tétel. *(A) Ha* $ac \equiv bc \pmod{m}$ *és* *ln.k.o.*$(m, c) = 1$*, akkor* $a \equiv b \pmod{m}$*. Azaz a kongruencia minden olyan tényezővel egyszerűsíthető, amelyik relatív prím a modulushoz. Ez fordítva is igaz:* $(\forall a)\,(\forall b)\,(ac \equiv bc \pmod{m}) \Longrightarrow a \equiv b \pmod{m}$*, akkor* *ln.k.o.*$(m, c) = 1$*.*

25. Tétel. *(A) Ha* $ac \equiv bc \pmod m$ *és* $\text{ln.k.o.}(m,c) = 1$*, akkor* $a \equiv b \pmod m$*. Azaz a kongruencia minden olyan tényezővel egyszerűsíthető, amelyik relatív prím a modulushoz. Ez fordítva is igaz:* $(\forall a)\,(\forall b)\,(ac \equiv bc \pmod m) \implies a \equiv b \pmod m$*, akkor* $\text{ln.k.o.}(m,c) = 1$*.*

(B) Ha $ac \equiv bc \pmod m$*, akkor* $a \equiv b \pmod{\frac{m}{\text{ln.k.o.}(m,c)}}$*.*

Bizonyítás:

25. Tétel. *(A) Ha* $ac \equiv bc \pmod m$ *és lnko*$(m, c) = 1$*, akkor* $a \equiv b \pmod m$*. Azaz a kongruencia minden olyan tényezővel egyszerűsíthető, amelyik relatív prím a modulushoz. Ez fordítva is igaz:* $(\forall a)\,(\forall b)\,(ac \equiv bc \pmod m) \Longrightarrow a \equiv b \pmod m$*, akkor lnko*$(m, c) = 1$*.*

(B) Ha $ac \equiv bc \pmod m$*, akkor* $a \equiv b \ \left(\bmod \dfrac{m}{\text{lnko}(m, c)}\right)$*.*

Bizonyítás: (A) speciális esete (B)-nek.

25. Tétel. *(A) Ha* $ac \equiv bc \pmod{m}$ *és* $\text{ln.k.o.}(m, c) = 1$, *akkor* $a \equiv b \pmod{m}$. *Azaz a kongruencia minden olyan tényezővel egyszerűsíthető, amelyik relatív prím a modulushoz. Ez fordítva is igaz:* $(\forall a)\,(\forall b)\,(ac \equiv bc \pmod{m}) \Longrightarrow a \equiv b \pmod{m}$, *akkor* $\text{ln.k.o.}(m, c) = 1$.

(B) Ha $ac \equiv bc \pmod{m}$, *akkor* $a \equiv b \left(\bmod \dfrac{m}{\text{ln.k.o.}(m, c)}\right)$.

Bizonyítás: (A) speciális esete (B)-nek. (B) igazolásához legyen $d = \text{ln.k.o.}(m, c)$, $m = m_1 d$ és $c = c_1 d$. Ekkor

25. Tétel. *(A) Ha* $ac \equiv bc \pmod{m}$ *és* ln.k.o.$(m,c) = 1$, *akkor* $a \equiv b \pmod{m}$. *Azaz a kongruencia minden olyan tényezővel egyszerűsíthető, amelyik relatív prím a modulushoz. Ez fordítva is igaz:* $(\forall a)\,(\forall b)\,(ac \equiv bc \pmod{m}) \Longrightarrow a \equiv b \pmod{m}$, *akkor* ln.k.o.$(m,c) = 1$.

(B) Ha $ac \equiv bc \pmod{m}$, *akkor* $a \equiv b \left(\mathrm{mod}\, \dfrac{m}{\text{ln.k.o.}(m,c)}\right)$.

Bizonyítás: (A) speciális esete (B)-nek. (B) igazolásához legyen $d =$ ln.k.o.(m,c), $m = m_1 d$ és $c = c_1 d$. Ekkor

$$m = m_1 d \mid (a-b)c_1 d$$

25. Tétel. *(A) Ha* $ac \equiv bc \pmod{m}$ *és* ln.k.o.$(m, c) = 1$*, akkor* $a \equiv b \pmod{m}$*. Azaz a kongruencia minden olyan tényezővel egyszerűsíthető, amelyik relatív prím a modulushoz. Ez fordítva is igaz:* $(\forall a)\,(\forall b)\,(ac \equiv bc \pmod{m}) \Longrightarrow a \equiv b \pmod{m}$*, akkor* ln.k.o.$(m, c) = 1$*.*

(B) Ha $ac \equiv bc \pmod{m}$*, akkor* $a \equiv b \ \left(\bmod \frac{m}{\text{ln.k.o.}(m,c)}\right)$*.*

Bizonyítás: (A) speciális esete (B)-nek. (B) igazolásához legyen $d = \text{ln.k.o.}(m, c)$, $m = m_1 d$ és $c = c_1 d$. Ekkor

$$m = m_1 d \mid (a - b) c_1 d$$

miatt

$$m_1 \mid (a-b)c_1,$$

de

$$m_1 \mid (a-b)c_1,$$

de mivel ln.k.o.$(m_1, c_1) = 1$, ezért

$$m_1 \mid (a-b)c_1,$$

de mivel ln.k.o.$(m_1, c_1) = 1$, ezért $m_1 \mid a-b$,

$$m_1 \mid (a-b)c_1,$$

de mivel ln.k.o.$(m_1, c_1) = 1$, ezért $m_1 \mid a-b$, azaz $a \equiv b \pmod{m_1}$, valóban.

$$m_1 \mid (a-b)c_1,$$

de mivel ln.k.o.$(m_1, c_1) = 1$, ezért $m_1 \mid a - b$, azaz $a \equiv b \pmod{m_1}$, valóban. Q.e.d.

$$m_1 \mid (a-b)c_1,$$

de mivel $\text{ln.k.o.}(m_1, c_1) = 1$, ezért $m_1 \mid a-b$, azaz $a \equiv b \pmod{m_1}$, valóban. Q.e.d.

Az alábbi szép tétel a kongruenciákra vonatkozó tételek közül az első nemtriviális.

26. Tétel. *(**„kis” Fermat-tétel**) Ha p prímszám és $a \in \mathbf{Z}$ nem osztható p-vel, akkor*

$$a^{p-1} \equiv 1 \pmod{p}.$$

26. Tétel. *(**„kis” Fermat-tétel**) Ha p prímszám és $a \in \mathbf{Z}$ nem osztható p-vel, akkor*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ekvivalens megfogalmazásban:

26. Tétel. *(„kis” **Fermat-tétel**) Ha p prímszám és $a \in \mathbf{Z}$ nem osztható p-vel, akkor*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ekvivalens megfogalmazásban: ha p prím, akkor tetszőleges $a \in \mathbf{Z}$-re

$$a^{p} \equiv a \pmod{p}.$$

Bizonyítás: Ha $p \not| \ a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$.

Bizonyítás: Ha $p \not| \ a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$,

Bizonyítás: Ha $p \not| \ a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$

Bizonyítás: Ha $p \not| \ a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka.

Bizonyítás: Ha $p \not| \; a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy

Bizonyítás: Ha $p \not| \, a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$.

Bizonyítás: Ha $p \not| \ a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ —

Bizonyítás: Ha $p \not| \, a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés,

Bizonyítás: Ha $p \not| \, a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei,

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (

Bizonyítás: Ha $p \not| \ a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám)

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges.

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint —

Bizonyítás: Ha $p \not| \ a$, akkor legyen $B = \{1, 2, \dots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint — $xa \equiv ya \pmod p$.

Bizonyítás: Ha $p \not| \; a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint — $xa \equiv ya \pmod p$. De most $p \not| \; a$ és p prím, ezért

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint — $xa \equiv ya \pmod p$. De most $p \not| a$ és p prím, ezért ln.k.o.$(p, a) =$ 1, és így a kongruencia a-val egszerűsíthető.

Bizonyítás: Ha $p \not| \, a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint — $xa \equiv ya \pmod p$. De most $p \not| \, a$ és p prím, ezért ln.k.o.$(p, a) = 1$, és így a kongruencia a-val egszerűsíthető. Így kapjuk, hogy $x \equiv y \pmod p$.

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint — $xa \equiv ya \pmod p$. De most $p \not| a$ és p prím, ezért ln.k.o.$(p, a) = 1$, és így a kongruencia a-val egszerűsíthető. Így kapjuk, hogy $x \equiv y \pmod p$. Tehát $p \mid x - y$, de

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint — $xa \equiv ya \pmod p$. De most $p \not| a$ és p prím, ezért ln.k.o.$(p, a) =$ 1, és így a kongruencia a-val egszerűsíthető. Így kapjuk, hogy $x \equiv y \pmod p$. Tehát $p \mid x - y$, de mivel $|x - y| \leq p - 2$, ezért ez csak $x = y$ esetén lehetéges.

Bizonyítás: Ha $p \not| a$, akkor legyen $B = \{1, 2, \ldots, p-1\}$. Legyen $\psi : B \to B$, $x \mapsto$ az $xa : p$ osztás maradéka. Más szóval, $x\psi$-t az definiálja, hogy $x\psi \in B$ és $x\psi \equiv xa \pmod p$. ψ — a jelöléssel összhangban — csakugyan leképezés, mert az xa-t p-vel osztva a lehetséges maradékok a $B \cup \{0\}$ elemei, de a 0 nem lehetséges, mert akkor $p \mid xa$ miatt (mivel prímszám) $p \mid a$ vagy $p \mid x \in B$, de egyik sem lehetséges. Tehát ψ leképezés.

Ha $x, y \in B$-re $x\psi = y\psi$, akkor — a kongruencia definíciója szerint — $xa \equiv ya \pmod p$. De most $p \not| a$ és p prím, ezért ln.k.o.$(p, a) = 1$, és így a kongruencia a-val egszerűsíthető. Így kapjuk, hogy $x \equiv y \pmod p$. Tehát $p \mid x - y$, de mivel $|x - y| \le p - 2$, ezért ez csak $x = y$ esetén lehetéges. Ezzel beláttuk, hogy ψ injektív.

Az injektivitás miatt az $1\psi, 2\psi, \ldots, (p-1)\psi$ mind különbözők, Az injektivitás miatt az $1\psi, 2\psi, \ldots, (p-1)\psi$ mind különbözők, és így kimerítik a $(p-1)$-elemű B halmaz elemeit. Azaz

Az injektivitás miatt az $1\psi, 2\psi, \ldots, (p-1)\psi$ mind különbözők, és így kimerítik a $(p-1)$-elemű B halmaz elemeit. Azaz ψ szürjektív is, és

Az injektivitás miatt az $1\psi, 2\psi, \ldots, (p-1)\psi$ mind különbözők, és így kimerítik a $(p-1)$-elemű B halmaz elemeit. Azaz ψ szürjektív is, és $B = \{1\psi, \ldots, (p-1)\psi\}$.

Az injektivitás miatt az $1\psi, 2\psi, \ldots, (p-1)\psi$ mind különbözők, és így kimerítik a $(p-1)$-elemű B halmaz elemeit. Azaz ψ szürjektív is, és $B = \{1\psi, \ldots, (p-1)\psi\}$. Ezért (a ψ jelentése miatt) az $1a$, $2a$, ..., $(p-1)a$ elemek

Az injektivitás miatt az $1\psi, 2\psi, \ldots, (p-1)\psi$ mind különbözők, és így kimerítik a $(p-1)$-elemű B halmaz elemeit. Azaz ψ szürjektív is, és $B = \{1\psi, \ldots, (p-1)\psi\}$. Ezért (a ψ jelentése miatt) az $1a$, $2a$, $\ldots$, $(p-1)a$ elemek *valamilyen sorrendben* éppen az $1, \ldots, p-1$ elemekkel kongruensek modulo p, hiszen az

Az injektivitás miatt az $1\psi, 2\psi, \ldots, (p-1)\psi$ mind különbözők, és így kimerítik a $(p-1)$-elemű B halmaz elemeit. Azaz ψ szürjektív is, és $B = \{1\psi, \ldots, (p-1)\psi\}$. Ezért (a ψ jelentése miatt) az $1a$, $2a$, $\ldots$, $(p-1)a$ elemek *valamilyen sorrendben* éppen az $1, \ldots, p-1$ elemekkel kongruensek modulo p, hiszen az $1a$, $2a$, $\ldots$, $(p-1)a$ elemeket p-vel osztva éppen ezek a maradékok lépnek fel, mindegyik pontosan egyszer.

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)!$$

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)! =$$

$(1a)$

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)! =$$

$(1a)(2a)$

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)! =$$
$$(1a)(2a)\dots((p-1)a) \equiv 1 \cdot 2 \dots \cdot (p-1) = (p-1)! \pmod{p}.$$

Tehát

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesít-hetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)! =$$
$$(1a)(2a)\ldots((p-1)a) \equiv 1 \cdot 2 \ldots \cdot (p-1) = (p-1)! \pmod{p}.$$

Tehát

$$a^{p-1} \cdot (p-1)! \equiv 1 \cdot (p-1)! \pmod{p} .$$

Mivel $p \not| (p-1)!$

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)! =$$
$$(1a)(2a)\ldots((p-1)a) \equiv 1 \cdot 2 \ldots \cdot (p-1) = (p-1)! \pmod{p}.$$

Tehát

$$a^{p-1} \cdot (p-1)! \equiv 1 \cdot (p-1)! \pmod{p} .$$

Mivel $p \not| \ (p-1)!$ (hiszen a $(p-1)!$ szorzat egyik tényezőjét sem osztja) és ezért ln.k.o.$(p,(p-1)!) = 1$, a fenti kongruencia egyszerűsíthető,

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)! =$$
$$(1a)(2a)\ldots((p-1)a) \equiv 1 \cdot 2 \ldots \cdot (p-1) = (p-1)! \pmod{p}.$$

Tehát

$$a^{p-1} \cdot (p-1)! \equiv 1 \cdot (p-1)! \pmod{p} .$$

Mivel $p \not| \ (p-1)!$ (hiszen a $(p-1)!$ szorzat egyik tényezőjét sem osztja) és ezért ln.k.o.$(p,(p-1)!) = 1$, a fenti kongruencia egyszerűsíthető, és kapjuk, hogy valóban:

Felhasználva, hogy a szorzat tényezői kongruensekkel helyettesíthetők és hogy a szorzat nem függ a tényezők sorrendjétől:

$$a^{p-1} \cdot (p-1)! =$$
$$(1a)(2a)\ldots((p-1)a) \equiv 1 \cdot 2 \ldots \cdot (p-1) = (p-1)! \pmod{p}.$$

Tehát

$$a^{p-1} \cdot (p-1)! \equiv 1 \cdot (p-1)! \pmod{p} .$$

Mivel $p \not| \ (p-1)!$ (hiszen a $(p-1)!$ szorzat egyik tényezőjét sem osztja) és ezért ln.k.o.$(p,(p-1)!) = 1$, a fenti kongruencia egyszerűsíthető, és kapjuk, hogy valóban:

$$a^{p-1} \equiv 1 \pmod{p} .$$

Mindkét

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \ a \ ,$$

az pedig

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \ a \ ,$$

az pedig evidens, hogy

$$a^p \equiv a \pmod p \text{ ha } p \mid a \ .$$

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \ a \ ,$$

az pedig evidens, hogy

$$a^p \equiv a \pmod p \text{ ha } p \mid a \ .$$

Q.e.d.

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \; a \; ,$$

az pedig evidens, hogy

$$a^p \equiv a \pmod p \text{ ha } p \mid a \; .$$

Q.e.d.

Arra még nem adtunk választ, hogy a tétel második megfogalmazásásból,

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \ a \ ,$$

az pedig evidens, hogy

$$a^p \equiv a \pmod p \text{ ha } p \mid a \ .$$

Q.e.d.

Arra még nem adtunk választ, hogy a tétel második megfogalmazásásból, azaz $a^p \equiv a \pmod p$ -ből hogyan következik az első, azaz

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \, a \ ,$$

az pedig evidens, hogy

$$a^p \equiv a \pmod p \text{ ha } p \mid a \ .$$

Q.e.d.

Arra még nem adtunk választ, hogy a tétel második megfogalmazásásból, azaz $a^p \equiv a \pmod p$ -ből hogyan következik az első, azaz $p \not| \, a \Longrightarrow a^{p-1} \equiv 1 \pmod p$.

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \; a \ ,$$

az pedig evidens, hogy

$$a^p \equiv a \pmod p \text{ ha } p \mid a \ .$$

Q.e.d.

Arra még nem adtunk választ, hogy a tétel második megfogalmazásásból, azaz $a^p \equiv a \pmod p$ -ből hogyan következik az első, azaz $p \not| \; a \Longrightarrow a^{p-1} \equiv 1 \pmod p$. De ez evidens: $\text{ln.k.o.}(p, a) = 1$ miatt

Mindkét oldalt a-val beszorozva kapjuk, hogy

$$a^p \equiv a \pmod p \text{ ha } p \not| \ a \ ,$$

az pedig evidens, hogy

$$a^p \equiv a \pmod p \text{ ha } p \mid a \ .$$

Q.e.d.

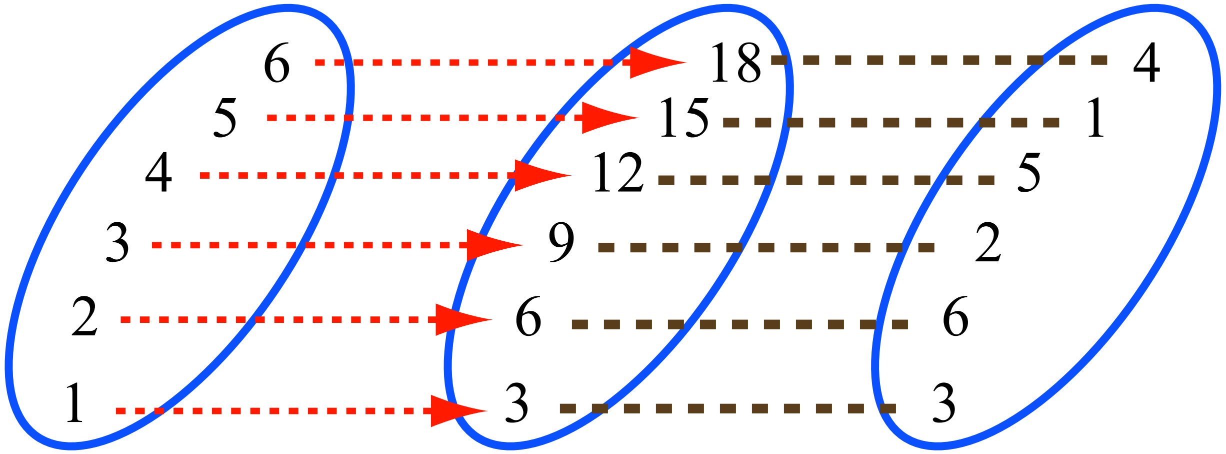
Arra még nem adtunk választ, hogy a tétel második megfogalmazásásból, azaz $a^p \equiv a \pmod p$ -ből hogyan következik az első, azaz $p \not| \ a \Longrightarrow a^{p-1} \equiv 1 \pmod p$. De ez evidens: ln.k.o.$(p, a) = 1$ miatt a $a^p \equiv a \pmod p$ kongruencia egyszerűsíthető a-val.

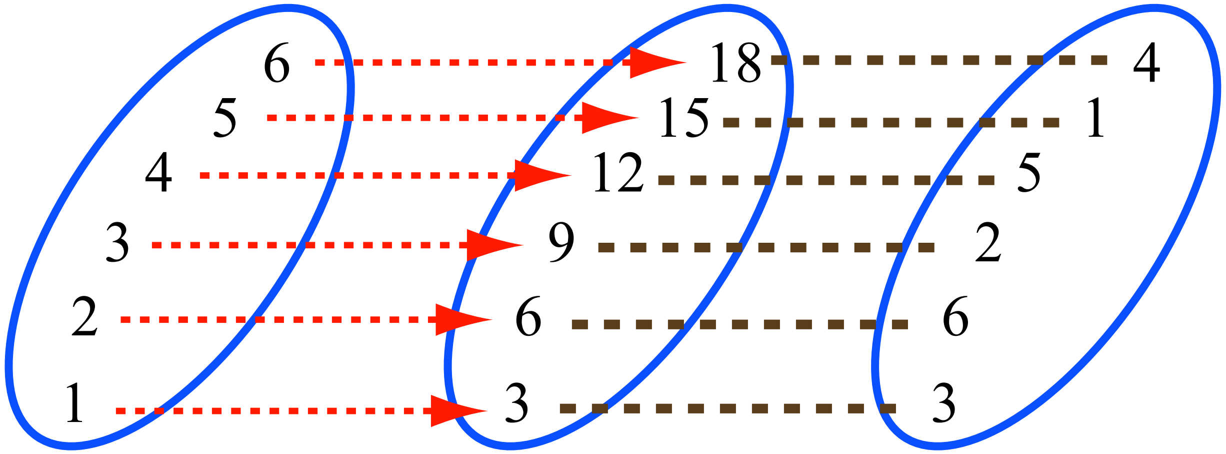
A bizonyítást az alábbi ábra illusztrálja

A bizonyítást az alábbi ábra illusztrálja (a cél $3^6 \equiv 1 \pmod 7$) igazolása).

A bizonyítást az alábbi ábra illusztrálja (a cél $3^6 \equiv 1 \pmod 7$) igazolása). A piros szaggatott nyilak a 3-mal való szorzást, a vastag barna szaggatott vonalak a modulo 7 kongruenciát jelölik.

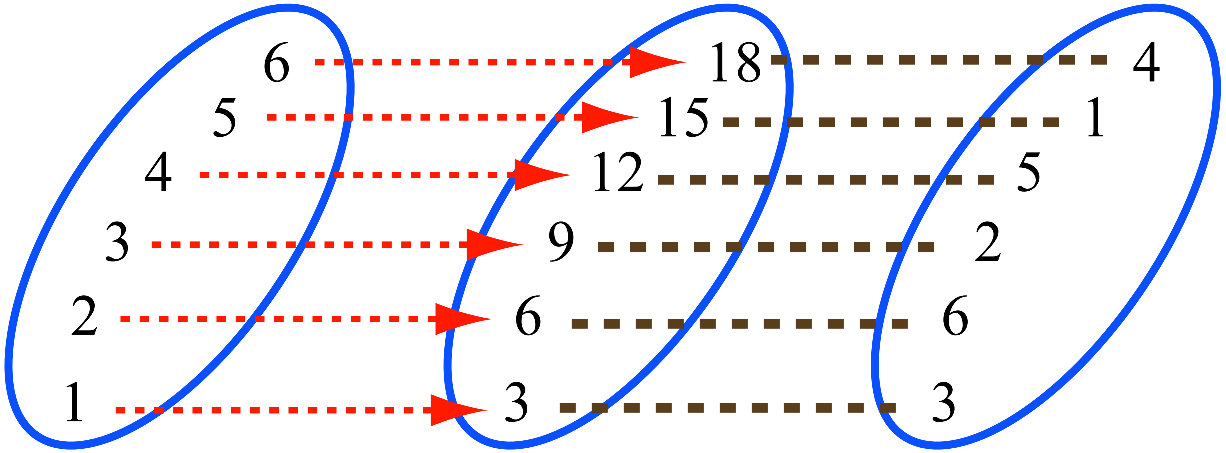
A bizonyítást az alábbi ábra illusztrálja (a cél $3^6 \equiv 1 \pmod 7$) igazolása). A piros szaggatott nyilak a 3-mal való szorzást, a vastag barna szaggatott vonalak a modulo 7 kongruenciát jelölik. (Az illusztráció csak a bizonyítás megértését könnyíti, de nem pótolja a bizonyítást.)


6
5
4
3
2
1
18
15
12
9
6
3
4
1
5
2
6
3



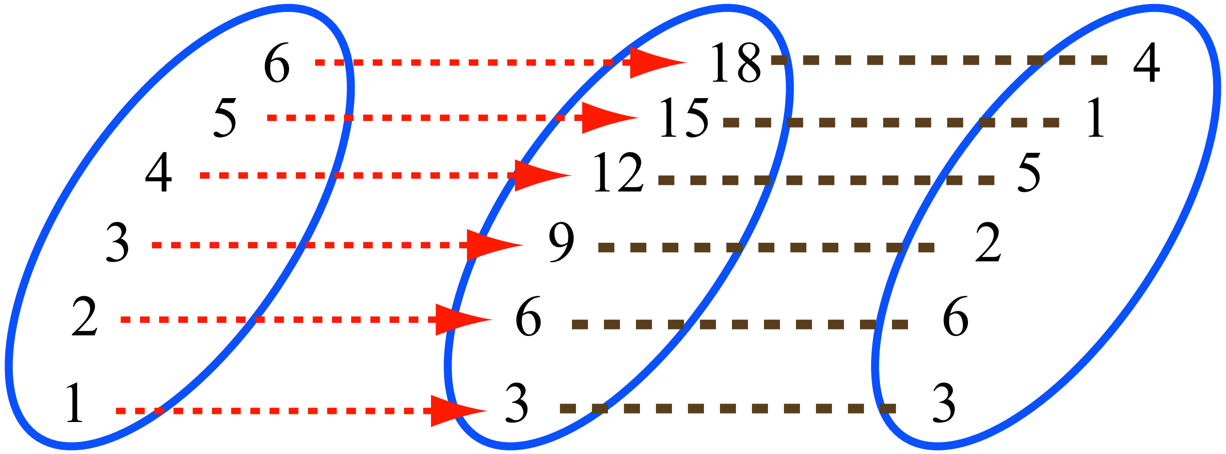
Innen

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 =$$



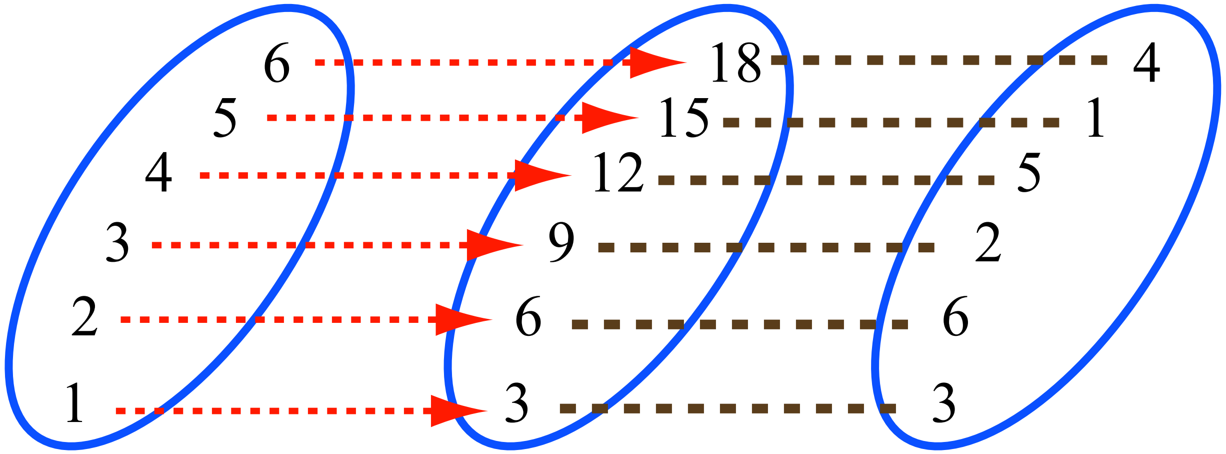
Innen

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4$$



Innen

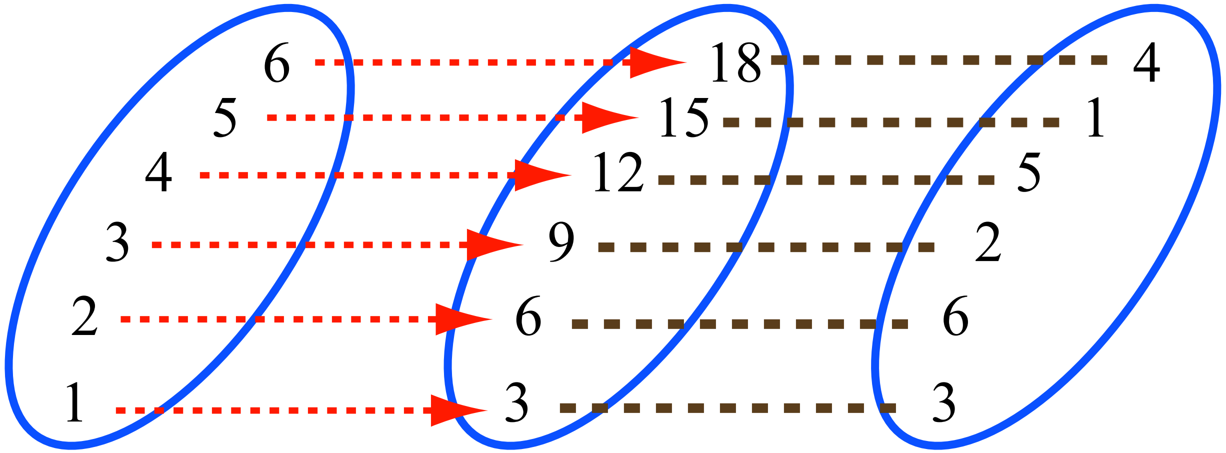
$$1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 = 3\cdot 6\cdot 2\cdot 5\cdot 1\cdot 4 \equiv$$
$$3\cdot 6\cdot 9\cdot 12\cdot 15\cdot 18 = 3^6\cdot(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \pmod 7.$$



Innen

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \equiv$$
$$3 \cdot 6 \cdot 9 \cdot 12 \cdot 15 \cdot 18 = 3^6 \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \pmod 7.$$

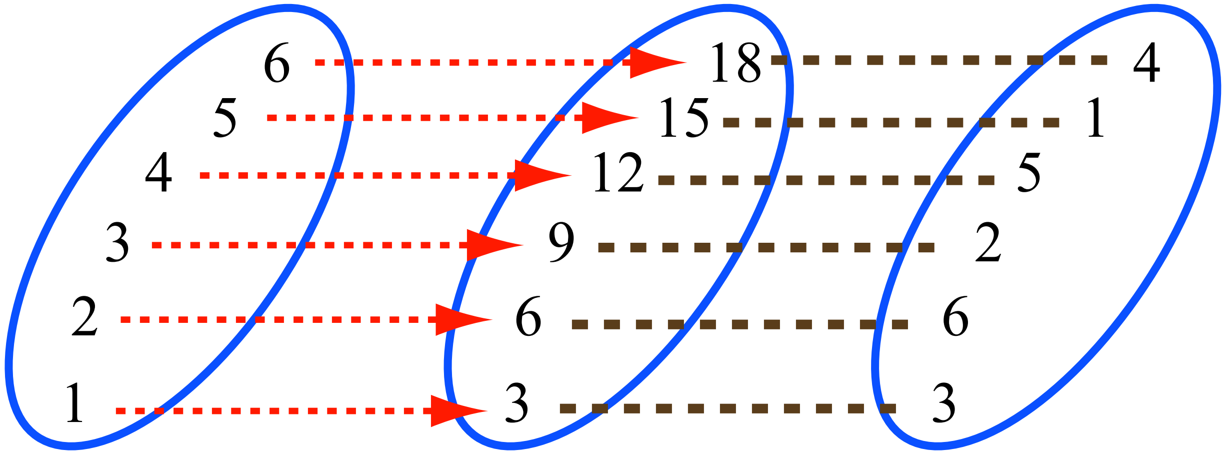
A kongruenciát 6!-sal egyszerűsítve:



Innen

$$1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 = 3\cdot 6\cdot 2\cdot 5\cdot 1\cdot 4 \equiv$$
$$3\cdot 6\cdot 9\cdot 12\cdot 15\cdot 18 = 3^6\cdot(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \pmod 7.$$

A kongruenciát 6!-sal egyszerűsítve: $1 \equiv 3^6 \pmod 7$,



Innen

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \equiv$$
$$3 \cdot 6 \cdot 9 \cdot 12 \cdot 15 \cdot 18 = 3^6 \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \pmod 7.$$

A kongruenciát 6!-sal egyszerűsítve: $1 \equiv 3^6 \pmod 7$, valóban.

A kis Fermat-tétel általánosításáról is hamarosan szó lesz.

Lineáris kongruenciarendszerek

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (amire meg kell oldanunk).

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (amire meg kell oldanunk). Tehát — legalábbis most — a (lineáris) kongruencia a

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (amire meg kell oldanunk). Tehát — legalábbis most — a (lineáris) kongruencia a (lineáris) egyenlettel analóg.

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (amire meg kell oldanunk). Tehát — legalábbis most — a (lineáris) kongruencia a (lineáris) egyenlettel analóg. A kongruenciák tulajdonságai alapján evidens, hogy ha $x_0 \in \mathbf{Z}$ megoldása a fenti kongruenciának és $x_1 \equiv x_0 \pmod{m}$, akkor x_1 is megoldása.

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (amire meg kell oldanunk). Tehát — legalábbis most — a (lineáris) kongruencia a (lineáris) egyenlettel analóg. A kongruenciák tulajdonságai alapján evidens, hogy ha $x_0 \in \mathbf{Z}$ megoldása a fenti kongruenciának és $x_1 \equiv x_0 \pmod{m}$, akkor x_1 is megoldása. (Valóban, ez esetben $ax_1 \equiv ax_0 \equiv b \pmod{m}$.)

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (amire meg kell oldanunk). Tehát — legalábbis most — a (lineáris) kongruencia a (lineáris) egyenlettel analóg. A kongruenciák tulajdonságai alapján evidens, hogy ha $x_0 \in \mathbf{Z}$ megoldása a fenti kongruenciának és $x_1 \equiv x_0 \pmod{m}$, akkor x_1 is megoldása. (Valóban, ez esetben $ax_1 \equiv ax_0 \equiv b \pmod{m}$.) Tehát ha egyáltalán van megoldása a fenti kongruenciának,

Lineáris kongruenciarendszerek

Definíció: **Lineáris kongruencián** egy

$$ax \equiv b \pmod{m}$$

alakú kongruenciát értünk, ahol $m \in \mathbf{N}$ és $a, b \in \mathbf{Z}$ adott, és $x \in \mathbf{Z}$ az ismeretlen (amire meg kell oldanunk). Tehát — legalábbis most — a (lineáris) kongruencia a (lineáris) egyenlettel analóg. A kongruenciák tulajdonságai alapján evidens, hogy ha $x_0 \in \mathbf{Z}$ megoldása a fenti kongruenciának és $x_1 \equiv x_0 \pmod{m}$, akkor x_1 is megoldása. (Valóban, ez esetben $ax_1 \equiv ax_0 \equiv b \pmod{m}$.) Tehát ha egyáltalán van megoldása a fenti kongruenciának, akkor végtelen sok megoldása van:

végtelen sok megoldása van: az $x_0 + tm$ $(t \in \mathbf{Z})$ számok is mind megoldásai.

végtelen sok megoldása van: az $x_0 + tm$ $(t \in \mathbf{Z})$ számok is mind megoldásai. Éppen ezért — amikor a megoldásokat összeszámoljuk — akkor a modulo m kongruens megoldásokat nem célszerű különbözőnek tekinteni.

27. Tétel. *Az* $ax \equiv b \pmod{m}$ *kongruencia akkor és csak akkor oldható meg, ha*

27. Tétel. *Az* $ax \equiv b \pmod{m}$ *kongruencia akkor és csak akkor oldható meg, ha ln.k.o.*$(a, m) \mid b$.

27. Tétel. *Az* $ax \equiv b \pmod m$ *kongruencia akkor és csak akkor oldható meg, ha ln.k.o.*$(a, m) \mid b$*.*

Amennyiben megoldható, akkor egyrészt modulo m *a megoldások száma*

27. Tétel. *Az* $ax \equiv b \pmod{m}$ *kongruencia akkor és csak akkor oldható meg, ha* $\text{ln.k.o.}(a,m) \mid b$.

Amennyiben megoldható, akkor egyrészt modulo m *a megoldások száma* $\text{ln.k.o.}(a,m)$*; másrészt a megoldás modulo* $\dfrac{m}{\text{ln.k.o.}(a,m)}$ *egyértelműen meghatározott, azaz az általános megoldás* $x = x_0 + t \cdot \dfrac{m}{\text{ln.k.o.}(a,m)}$ $(t \in \mathbf{Z})$ *alakú.*

27. Tétel. *Az $ax \equiv b \pmod m$ kongruencia akkor és csak akkor oldható meg, ha ln.k.o.$(a,m) \mid b$.*

Amennyiben megoldható, akkor egyrészt modulo m a megoldások száma ln.k.o.(a,m); másrészt a megoldás modulo $\frac{m}{\text{ln.k.o.}(a,m)}$ egyértelműen meghatározott, azaz az általános megoldás $x = x_0 + t \cdot \frac{m}{\text{ln.k.o.}(a,m)}$ $(t \in \mathbf{Z})$ alakú. Más szóval, ha x_0 az $ax \equiv b \pmod m$ kongruencia egyik partikuláris megoldása, akkor ez a kongruencia ekvivalens az alábbi kongruenciával:

27. Tétel. *Az $ax \equiv b \pmod{m}$ kongruencia akkor és csak akkor oldható meg, ha ln.k.o.$(a, m) \mid b$.*

Amennyiben megoldható, akkor egyrészt modulo m a megoldások száma ln.k.o.(a, m); másrészt a megoldás modulo $\frac{m}{\text{ln.k.o.}(a,m)}$ egyértelműen meghatározott, azaz az általános megoldás $x = x_0 + t \cdot \frac{m}{\text{ln.k.o.}(a,m)}$ $(t \in \mathbf{Z})$ alakú. Más szóval, ha x_0 az $ax \equiv b \pmod{m}$ kongruencia egyik partikuláris megoldása, akkor ez a kongruencia ekvivalens az alábbi kongruenciával:

$$x \equiv x_0 \pmod{\frac{m}{\text{ln.k.o.}(a,m)}}.$$

A bizonyítás együttal megoldási módszert is szolgáltat:

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza.

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy $m \mid ax - b$, azaz

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy $m \mid ax - b$, azaz azzal, hogy van olyan $y \in \mathbf{Z}$, hogy $my = ax - b$, azaz

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy $m \mid ax - b$, azaz azzal, hogy van olyan $y \in \mathbf{Z}$, hogy $my = ax - b$, azaz $ax + (-m)y = b$.

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy $m \mid ax - b$, azaz azzal, hogy van olyan $y \in \mathbf{Z}$, hogy $my = ax - b$, azaz $ax + (-m)y = b$.

Tehát a kiindulási kongruencia megoldhatósága az

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy $m \mid ax - b$, azaz azzal, hogy van olyan $y \in \mathbf{Z}$, hogy $my = ax - b$, azaz $ax + (-m)y = b$.

Tehát a kiindulási kongruencia megoldhatósága az $ax + (-m)y = b$

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy $m \mid ax - b$, azaz azzal, hogy van olyan $y \in \mathbf{Z}$, hogy $my = ax - b$, azaz $ax + (-m)y = b$.

Tehát a kiindulási kongruencia megoldhatósága az $ax + (-m)y = b$ diofantoszi egyenlet megoldhatóságával ekvivalens,

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod{m}$ azzal ekvivalens, hogy $m \mid ax - b$, azaz azzal, hogy van olyan $y \in \mathbf{Z}$, hogy $my = ax - b$, azaz $ax + (-m)y = b$.

Tehát a kiindulási kongruencia megoldhatósága az $ax + (-m)y = b$ diofantoszi egyenlet megoldhatóságával ekvivalens, de ez utóbbiról tudjuk, hogy $\iff$ ln.k.o.$(a, -m) \mid b$, ami

A bizonyítás egyúttal megoldási módszert is szolgáltat: a lineáris kongruenciát lineáris difofantoszi egyenletre vezethetjük vissza. Nyilván — tetszőleges $x \in \mathbf{Z}$ esetén — $ax \equiv b \pmod m$ azzal ekvivalens, hogy $m \mid ax - b$, azaz azzal, hogy van olyan $y \in \mathbf{Z}$, hogy $my = ax - b$, azaz $ax + (-m)y = b$.

Tehát a kiindulási kongruencia megoldhatósága az $ax + (-m)y = b$ diofantoszi egyenlet megoldhatóságával ekvivalens, de ez utóbbiról tudjuk, hogy $\iff$ ln.k.o.$(a, -m) \mid b$, ami ln.k.o.$(a, -m) =$ ln.k.o.(a, m) miatt a tétel első mondatát igazolja.

Ha a kongruencia megoldható, akkor a tekintett diofantoszi egyenlet általános megoldását adó képlet szerint

$$x = x_0 + t \cdot \frac{-m}{\text{ln.k.o.}(a, m)},$$

Ha a kongruencia megoldható, akkor a tekintett diofantoszi egyenlet általános megoldását adó képlet szerint

$$x = x_0 + t \cdot \frac{-\,m}{\text{ln.k.o.}(a,m)},$$

azaz (

Ha a kongruencia megoldható, akkor a tekintett diofantoszi egyenlet általános megoldását adó képlet szerint

$$x = x_0 + t \cdot \frac{-\,m}{\text{ln.k.o.}(a, m)},$$

azaz (t helyett $-t$-t írva)

Ha a kongruencia megoldható, akkor a tekintett diofantoszi egyenlet általános megoldását adó képlet szerint

$$x = x_0 + t \cdot \frac{-\,m}{\text{ln.k.o.}(a, m)},$$

azaz (t helyett $-t$-t írva)

$$x = x_0 + t \cdot \frac{m}{\text{ln.k.o.}(a, m)} \qquad (t \in \mathbf{Z})$$

az x-re adódó általános megoldás.

Ha a kongruencia megoldható, akkor a tekintett diofantoszi egyenlet általános megoldását adó képlet szerint

$$x = x_0 + t \cdot \frac{-m}{\text{ln.k.o.}(a,m)},$$

azaz (t helyett $-t$-t írva)

$$x = x_0 + t \cdot \frac{m}{\text{ln.k.o.}(a,m)} \qquad (t \in \mathbf{Z})$$

az x-re adódó általános megoldás. Tehát a megoldások modulo $\frac{m}{\text{ln.k.o.}(a,m)}$ egyértelműen meghatározottak.

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \ldots d - 1$ értékére páronként inkongruenseket kapunk

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \ldots d - 1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d - 1)m_1 < dm_1 = m$

Legyen $d=$ ln.k.o.(a,m) és $m_1=\dfrac{m}{\text{ln.k.o.}(a,m)}$. Ekkor $m=m_1d$, és a fentiek szerint a kongruencia általános megoldása

$$x=x_0+t\cdot m_1 \qquad (t\in\mathbf{Z}).$$

Ezek közül a paraméter $t=0,1,\ldots d-1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d-1)m_1<dm_1=m$ miatt nem osztható m-mel), viszont

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \dots d - 1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d-1)m_1 < dm_1 = m$ miatt nem osztható m-mel), viszont az összes többi megoldás ezen d darab valamelyikével kongruens.

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \ldots d - 1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d-1)m_1 < dm_1 = m$ miatt nem osztható m-mel), viszont az összes többi megoldás ezen d darab valamelyikével kongruens. Csakugyan, tetszőleges megoldás $x_0 + tm_1$ alakú;

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \ldots d - 1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d - 1)m_1 < dm_1 = m$ miatt nem osztható m-mel), viszont az összes többi megoldás ezen d darab valamelyikével kongruens. Csakugyan, tetszőleges megoldás $x_0 + tm_1$ alakú; osszuk el t-t d-vel maradékosan:

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \ldots d - 1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d-1)m_1 < dm_1 = m$ miatt nem osztható m-mel), viszont az összes többi megoldás ezen d darab valamelyikével kongruens. Csakugyan, tetszőleges megoldás $x_0 + tm_1$ alakú; osszuk el t-t d-vel maradékosan: $t = dq + r$.

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \ldots d - 1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d-1)m_1 < dm_1 = m$ miatt nem osztható m-mel), viszont az összes többi megoldás ezen d darab valamelyikével kongruens. Csakugyan, tetszőleges megoldás $x_0 + tm_1$ alakú; osszuk el t-t d-vel maradékosan: $t = dq + r$. Ekkor $0 \leq r < d$ miatt $x_0 + rm_1$ a felsorolt d darab

Legyen $d = \text{ln.k.o.}(a, m)$ és $m_1 = \dfrac{m}{\text{ln.k.o.}(a, m)}$. Ekkor $m = m_1 d$, és a fentiek szerint a kongruencia általános megoldása

$$x = x_0 + t \cdot m_1 \qquad (t \in \mathbf{Z}).$$

Ezek közül a paraméter $t = 0, 1, \ldots d - 1$ értékére páronként inkongruenseket kapunk (hiszen két ilyen különbsége legfeljebb $(d-1)m_1 < dm_1 = m$ miatt nem osztható m-mel), viszont az összes többi megoldás ezen d darab valamelyikével kongruens. Csakugyan, tetszőleges megoldás $x_0 + tm_1$ alakú; osszuk el t-t d-vel maradékosan: $t = dq + r$. Ekkor $0 \leq r < d$ miatt $x_0 + rm_1$ a felsorolt d darab megoldás egyike, és

$$(x_0 + tm_1) - (x_0 + rm_1) =$$

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 =$$

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 = dqm_1 =$$

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 = dqm_1 = qm$$

miatt $x_0 + tm_1 \equiv x_0 + rm_1 \equiv b \pmod{m}$.

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 = dqm_1 = qm$$

miatt $x_0 + tm_1 \equiv x_0 + rm_1 \equiv b \pmod{m}$. Q.e.d.

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 = dqm_1 = qm$$

miatt $x_0 + tm_1 \equiv x_0 + rm_1 \equiv b \pmod m$. Q.e.d.

Példa: Oldjuk meg a $21x \equiv 15 \pmod{33}$ kongruenciát.

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 = dqm_1 = qm$$

miatt $x_0 + tm_1 \equiv x_0 + rm_1 \equiv b \pmod{m}$. Q.e.d.

Példa: Oldjuk meg a $21x \equiv 15 \pmod{33}$ kongruenciát.

Megoldás: Előbb oldjuk meg a $21x + 33y = 15$ diofantoszi egyenletet!

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 = dqm_1 = qm$$

miatt $x_0 + tm_1 \equiv x_0 + rm_1 \equiv b \pmod{m}$. Q.e.d.

Példa: Oldjuk meg a $21x \equiv 15 \pmod{33}$ kongruenciát.

Megoldás: Előbb oldjuk meg a $21x + 33y = 15$ diofantoszi egyenletet! (Hiszen $33 \mid 15 - 21x$ miatt a

$$(x_0 + tm_1) - (x_0 + rm_1) = (t - r)m_1 = dqm_1 = qm$$

miatt $x_0 + tm_1 \equiv x_0 + rm_1 \equiv b \pmod{m}$. Q.e.d.

Példa: Oldjuk meg a $21x \equiv 15 \pmod{33}$ kongruenciát.

Megoldás: Előbb oldjuk meg a $21x + 33y = 15$ diofantoszi egyenletet! (Hiszen $33 \mid 15 - 21x$ miatt a $15 - 21x$ felírható $33y$ alakban.) A tanult módszerek közül most pl. a helyettesítgetések módszerét alkalmazzuk, hiszen „ránézésre'' látható, hogy $\mathrm{ln.k.o.}(21, 33) = 3$. Mivel $3 \mid 15$, az is látszik, hogy van megoldás.

$15 =$

$$15 = 21x + 33y =$$

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y =$$

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor

$$15 = 21x + 33y = 21(\underbrace{x+y}_{z}) + 12y = 12(\underbrace{2z+y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y =$

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y = u - 2z =$

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y = u - 2z = 3$ és

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y = u - 2z = 3$ és $x =$

$$15 = 21x + 33y = 21(\underbrace{x+y}_{z}) + 12y = 12(\underbrace{2z+y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y = u - 2z = 3$ és $x = z - y =$

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y = u - 2z = 3$ és $x = z - y = -4$.

$$15 = 21x + 33y = 21(\underbrace{x + y}_{z}) + 12y = 12(\underbrace{2z + y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y = u - 2z = 3$ és $x = z - y = \ -4$.

Tehát a $21x \equiv 15 \pmod{33}$ kongruencia egyik partikuláris megoldása a -4. A modulo 33 inkongruens megoldások száma

$$15 = 21x + 33y = 21(\underbrace{x+y}_{z}) + 12y = 12(\underbrace{2z+y}_{u}) - 3z.$$

Hárommal átosztva:

$$5 = 4u - z.$$

Mivel most csak egyetlen megoldás kell, legyen pl. $u = 1$, $z = -1$, ekkor $y = u - 2z = 3$ és $x = z - y = -4$.

Tehát a $21x \equiv 15 \pmod{33}$ kongruencia egyik partikuláris megoldása a -4. A modulo 33 inkongruens megoldások száma három. A kongruencia általános megoldása

$$x \equiv -4 \pmod{11}.$$

Természetesen az eredmény úgy is megadató, hogy

$$x \equiv 7 \pmod{11},$$

vagy pedig úgy is, hogy

Természetesen az eredmény úgy is megadató, hogy

$$x \equiv 7 \pmod{11},$$

vagy pedig úgy is, hogy

$$x = -4 + 11t \quad (t \in \mathbf{Z}).$$

Természetesen az eredmény úgy is megadató, hogy

$$x \equiv 7 \pmod{11},$$

vagy pedig úgy is, hogy

$$x = -4 + 11t \quad (t \in \mathbf{Z}).$$

Másik megoldás: A lineáris kongruencia a kongruenciák tulajdonságai alapján is megoldható.

Természetesen az eredmény úgy is megadató, hogy

$$x \equiv 7 \pmod{11},$$

vagy pedig úgy is, hogy

$$x = -4 + 11t \quad (t \in \mathbf{Z}).$$

Másik megoldás: A lineáris kongruencia a kongruenciák tulajdonságai alapján is megoldható. (Ezt a módszer leginkább kis számok esetén javasolható,

Természetesen az eredmény úgy is megadató, hogy

$$x \equiv 7 \pmod{11},$$

vagy pedig úgy is, hogy

$$x = -4 + 11t \quad (t \in \mathbf{Z}).$$

Másik megoldás: A lineáris kongruencia a kongruenciák tulajdonságai alapján is megoldható. (Ezt a módszer leginkább kis számok esetén javasolható, olyankor viszont gyorsabb, mint a diofantoszi egyenletre való visszavezetés.)

Természetesen az eredmény úgy is megadató, hogy

$$x \equiv 7 \pmod{11},$$

vagy pedig úgy is, hogy

$$x = -4 + 11t \quad (t \in \mathbf{Z}).$$

Másik megoldás: A lineáris kongruencia a kongruenciák tulajdonságai alapján is megoldható. (Ezt a módszer leginkább kis számok esetén javasolható, olyankor viszont gyorsabb, mint a diofantoszi egyenletre való visszavezetés. Nagy számok esetén az alábbiakban alkalmazott trükkök megtalálása — ha programot írnánk rá — lényegében azonos lenne a diofantoszi egyenlethez szükséges számolással.)

$$21x \equiv 15 \pmod{33}$$

$21x \equiv 15 \pmod{33}$: 3

$7x \equiv 5$ (mod

$$21x \equiv 15 \pmod{33}$$: 3

$$7x \equiv 5 \pmod{11}$$

$$\begin{aligned} 21x &\equiv 15 \pmod{33} && : 3 \\ 7x &\equiv 5 \pmod{11} && \cdot (-1) \end{aligned}$$

$$
\begin{aligned}
21x &\equiv 15 \pmod{33} && : 3 \\
7x &\equiv 5 \pmod{11} && \cdot (-1) \\
4x &\equiv
\end{aligned}
$$

$$\begin{aligned} 21x &\equiv 15 \pmod{33} && :3 \\ 7x &\equiv 5 \pmod{11} && \cdot(-1) \\ 4x &\equiv 6 \pmod{11} \end{aligned}$$

$$
\begin{aligned}
21x &\equiv 15 \pmod{33} && : 3 \\
7x &\equiv 5 \pmod{11} && \cdot (-1) \\
4x &\equiv 6 \pmod{11} && : 2
\end{aligned}
$$

$$
\begin{aligned}
21x &\equiv 15 \pmod{33} && : 3 \\
7x &\equiv 5 \pmod{11} && \cdot (-1) \\
4x &\equiv 6 \pmod{11} && : 2 \\
2x &\equiv 3 \ (\mathrm{mod}
\end{aligned}
$$

$$
\begin{aligned}
21x &\equiv 15 \pmod{33} && : 3 \\
7x &\equiv 5 \pmod{11} && \cdot (-1) \\
4x &\equiv 6 \pmod{11} && : 2 \\
2x &\equiv 3 \pmod{11} \\
2x &\equiv
\end{aligned}
$$

$$
\begin{aligned}
21x &\equiv 15 \pmod{33} && : 3 \\
7x &\equiv 5 \pmod{11} && \cdot (-1) \\
4x &\equiv 6 \pmod{11} && : 2 \\
2x &\equiv 3 \pmod{11} \\
2x &\equiv -8 \pmod{11}
\end{aligned}
$$

$$
\begin{aligned}
21x &\equiv 15 \pmod{33} && : 3 \\
7x &\equiv 5 \pmod{11} && \cdot (-1) \\
4x &\equiv 6 \pmod{11} && : 2 \\
2x &\equiv 3 \pmod{11} && \\
2x &\equiv -8 \pmod{11} && : 2 \\
x &\equiv &&
\end{aligned}
$$

$$
\begin{aligned}
21x &\equiv 15 \pmod{33} && : 3 \\
7x &\equiv 5 \pmod{11} && \cdot (-1) \\
4x &\equiv 6 \pmod{11} && : 2 \\
2x &\equiv 3 \pmod{11} && \\
2x &\equiv -8 \pmod{11} && : 2 \\
x &\equiv -4 \pmod{11} \;; && \text{ez az általános megoldás.}
\end{aligned}
$$

Példa: Oldjuk meg a $128x \equiv 26 \pmod{202}$ kongruenciát.

Példa: Oldjuk meg a $128x \equiv 26 \pmod{202}$ kongruenciát.

Megoldás:

Példa: Oldjuk meg a $128x \equiv 26 \pmod{202}$ kongruenciát.

Megoldás: Kettőhatvány - ezt ki lehet használni!

Példa: Oldjuk meg a $128x \equiv 26 \pmod{202}$ kongruenciát.

Megoldás: Kettőhatvány - ezt ki lehet használni! Mivel $\text{ln.k.o.}(128, 202) = 2 \mid 26$, megoldható.

Példa: Oldjuk meg a $128x \equiv 26 \pmod{202}$ kongruenciát.

Megoldás: Kettőhatvány - ezt ki lehet használni! Mivel $\text{lnko}(128, 202) = 2 \mid 26$, megoldható. Érdemes $\text{lnko}(128, 202) = 2$-vel

Példa: Oldjuk meg a $128x \equiv 26 \pmod{202}$ kongruenciát.

Megoldás: Kettőhatvány - ezt ki lehet használni! Mivel $\text{ln.k.o.}(128, 202) = 2 \mid 26$, megoldható. Érdemes $\text{ln.k.o.}(128, 202) = 2$-vel egyszerűsíteni, ekkor (a kis Fermat-tétel előtti tétel (B) része szerint) $64x \equiv 13 \pmod{101}$,

Példa: Oldjuk meg a $128x \equiv 26 \pmod{202}$ kongruenciát.

Megoldás: Kettőhatvány - ezt ki lehet használni! Mivel ln.k.o.$(128, 202) = 2 \mid 26$, megoldható. Érdemes ln.k.o.$(128, 202) =$ 2-vel egyszerűsíteni, ekkor (a kis Fermat-tétel előtti tétel (B) része szerint) $64x \equiv 13 \pmod{101}$, **tehát a modulust is változott!**. A számolás:

$$64x \equiv 13 \pmod{101}$$

$$64x \equiv 13 \pmod{101}$$
$$64x \equiv -88 \pmod{101}$$

$$64x \equiv 13 \pmod{101}$$
$$64x \equiv -88 \pmod{101}$$
$$8x \equiv -11 \pmod{101}$$

$$64x \equiv 13 \pmod{101}$$
$$64x \equiv -88 \pmod{101}$$
$$8x \equiv -11 \pmod{101}$$
$$8x \equiv -112 \pmod{101}$$

$$
\begin{aligned}
64x &\equiv 13 \pmod{101} \\
64x &\equiv -88 \pmod{101} \\
8x &\equiv -11 \pmod{101} \\
8x &\equiv -112 \pmod{101} \\
x &\equiv -14 \pmod{101}
\end{aligned}
$$

$$
\begin{aligned}
64x &\equiv 13 \pmod{101} \\
64x &\equiv -88 \pmod{101} \\
8x &\equiv -11 \pmod{101} \\
8x &\equiv -112 \pmod{101} \\
x &\equiv -14 \pmod{101} \\
x &\equiv 87 \pmod{101} ,
\end{aligned}
$$

$$
\begin{aligned}
64x &\equiv 13 \pmod{101} \\
64x &\equiv -88 \pmod{101} \\
8x &\equiv -11 \pmod{101} \\
8x &\equiv -112 \pmod{101} \\
x &\equiv -14 \pmod{101} \\
x &\equiv 87 \pmod{101} ,
\end{aligned}
$$

és ez a megoldás.

Definíció: **Lineáris kongruenciarendszeren** a

$$\begin{gathered} c_1 x \equiv d_1 \pmod{m_1} \\ \cdots \\ c_k x \equiv d_k \pmod{m_k} \end{gathered}$$

alakú kongruenciarendszereket értjük, ahol $2 \leq k \in \mathbf{N}$, $m_1, \ldots, m_k \in \mathbf{N}$,

Definíció: **Lineáris kongruenciarendszeren** a

$$c_1 x \equiv d_1 \pmod{m_1}$$
$$\dots$$
$$c_k x \equiv d_k \pmod{m_k}$$

alakú kongruenciarendszereket értjük, ahol $2 \leq k \in \mathbf{N}$, $m_1, \dots, m_k \in \mathbf{N}$, $c_1, \dots, c_k, d_1, \dots, d_k \in \mathbf{Z}$ adott számok,

Definíció: **Lineáris kongruenciarendszeren** a

$$c_1 x \equiv d_1 \pmod{m_1}$$
$$\dots$$
$$c_k x \equiv d_k \pmod{m_k}$$

alakú kongruenciarendszereket értjük, ahol $2 \leq k \in \mathbf{N}$, $m_1, \dots, m_k \in \mathbf{N}$, $c_1, \dots, c_k, d_1, \dots, d_k \in \mathbf{Z}$ adott számok, és az $x \in \mathbf{Z}$ ismeretlent keressük.

Definíció: **Lineáris kongruenciarendszeren** a

$$c_1 x \equiv d_1 \pmod{m_1}$$
$$\dots$$
$$c_k x \equiv d_k \pmod{m_k}$$

alakú kongruenciarendszereket értjük, ahol $2 \leq k \in \mathbf{N}$, $m_1, \dots, m_k \in \mathbf{N}$, $c_1, \dots, c_k, d_1, \dots, d_k \in \mathbf{Z}$ adott számok, és az $x \in \mathbf{Z}$ ismeretlent keressük.

Egy ilyen kongruenciarendszer megoldhatóságának

Definíció: **Lineáris kongruenciarendszeren** a

$$c_1 x \equiv d_1 \pmod{m_1}$$
$$\ldots$$
$$c_k x \equiv d_k \pmod{m_k}$$

alakú kongruenciarendszereket értjük, ahol $2 \leq k \in \mathbf{N}$, $m_1, \ldots, m_k \in \mathbf{N}$, $c_1, \ldots, c_k, d_1, \ldots, d_k \in \mathbf{Z}$ adott számok, és az $x \in \mathbf{Z}$ ismeretlent keressük.

Egy ilyen kongruenciarendszer megoldhatóságának szükséges feltétele, hogy az egyes kongruenciák külön-külön megoldhatóak legyenek. Az előző tételből tudjuk, hogy a $c_i x \equiv d_i \pmod{m_i}$ kongruencia — amennyiben megoldható és x_0 egy megoldása — ekvivalens az $x \equiv x_0 \pmod{\frac{m_i}{\text{ln.k.o.}(m_i, c_i)}}$ kongruenciával.

Ezért a fenti kongruenciarendszer megoldásához

Ezért a fenti kongruenciarendszer megoldásához úgy kell hozzáfogni, hogy külön-külön megoldjuk az egyes kongruenciákat, és ily módon (

Ezért a fenti kongruenciarendszer megoldásához úgy kell hozzáfogni, hogy külön-külön megoldjuk az egyes kongruenciákat, és ily módon (ha van megoldás) az eredeti

Ezért a fenti kongruenciarendszer megoldásához úgy kell hozzáfogni, hogy külön-külön megoldjuk az egyes kongruenciákat, és ily módon (ha van megoldás) az eredeti kongruenciarendszert az alábbi alakú kongruenciarendszerre vezetjük vissza:

Ezért a fenti kongruenciarendszer megoldásához úgy kell hozzáfogni, hogy külön-külön megoldjuk az egyes kongruenciákat, és ily módon (ha van megoldás) az eredeti kongruenciarendszert az alábbi alakú kongruenciarendszerre vezetjük vissza:

$$x \equiv a_1 \pmod{m_1}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}.$$

Ezért a fenti kongruenciarendszer megoldásához úgy kell hozzáfogni, hogy külön-külön megoldjuk az egyes kongruenciákat, és ily módon (ha van megoldás) az eredeti kongruenciarendszert az alábbi alakú kongruenciarendszerre vezetjük vissza:

$$x \equiv a_1 \pmod{m_1}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}.$$

Ennél pedig **majd** az lesz a megoldás lényege, hogy két kongruenciát eggyel tudunk helyettesíteni - és ilyen lépések sorozatával jutunk el majd a megoldáshoz.

Ezért a fenti kongruenciarendszer megoldásához úgy kell hozzáfogni, hogy külön-külön megoldjuk az egyes kongruenciákat, és ily módon (ha van megoldás) az eredeti kongruenciarendszert az alábbi alakú kongruenciarendszerre vezetjük vissza:

$$x \equiv a_1 \pmod{m_1}$$
$$\ldots$$
$$x \equiv a_k \pmod{m_k}.$$

Ennél pedig **majd** az lesz a megoldás lényege, hogy két kongruenciát eggyel tudunk helyettesíteni - és ilyen lépések sorozatával jutunk el majd a megoldáshoz. Éppen ezért először a $k = 2$ speciális esettel foglalkozunk.

28. Tétel. *Az*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

kongruenciarendszer akkor és csak akkor oldható meg, ha

28. Tétel. *Az*

$$x \equiv a_1 \ (mod\, m_1)$$
$$x \equiv a_2 \ (mod\, m_2)$$

kongruenciarendszer akkor és csak akkor oldható meg, ha

$$ln.k.o.(m_1, m_2) \mid a_1 - a_2.$$

28. Tétel. *Az*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

kongruenciarendszer akkor és csak akkor oldható meg, ha

$$\text{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.$$

Amennyiben megoldható és x_0 *egy rögzített megoldása, akkor a fenti kongruenciarendszer*

28. Tétel. *Az*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

kongruenciarendszer akkor és csak akkor oldható meg, ha

$$\text{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.$$

Amennyiben megoldható és x_0 *egy rögzített megoldása, akkor a fenti kongruenciarendszer ekvivalens az alábbi kongruenciával:*

$$x \equiv x_0 \pmod{\text{lk.k.t.}(m_1, m_2)}$$

és

28. Tétel. *Az*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

kongruenciarendszer akkor és csak akkor oldható meg, ha

$$\textit{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.$$

Amennyiben megoldható és x_0 *egy rögzített megoldása, akkor a fenti kongruenciarendszer ekvivalens az alábbi kongruenciával:*

$$x \equiv x_0 \pmod{\textit{lk.k.t.}(m_1, m_2)}$$

és ezért az általános megoldása

28. Tétel. *Az*

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

kongruenciarendszer akkor és csak akkor oldható meg, ha

$$\textit{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.$$

Amennyiben megoldható és x_0 egy rögzített megoldása, akkor a fenti kongruenciarendszer ekvivalens az alábbi kongruenciával:

$$x \equiv x_0 \pmod{\textit{lk.k.t.}(m_1, m_2)}$$

és ezért az általános megoldása

$$x = x_0 + t \cdot \textit{lk.k.t.}(m_1, m_2) \quad (t \in \mathbf{Z}).$$

Szavakban a feltétel úgy szól, hogy „a modulusok legnagyobb közös osztójának osztania kell a konstansok különbségét”.

Szavakban a feltétel úgy szól, hogy „a modulusok legnagyobb közös osztójának osztania kell a konstansok különbségét”. A tétel és a bizonyítása egyaránt fontos —

Szavakban a feltétel úgy szól, hogy „a modulusok legnagyobb közös osztójának osztania kell a konstansok különbségét”. A tétel és a bizonyítása egyaránt fontos — az utóbbi azért, mert onnan tudjuk meg, hogyan lehet egy partikuláris megoldást keresni.

Szavakban a feltétel úgy szól, hogy „a modulusok legnagyobb közös osztójának osztania kell a konstansok különbségét". A tétel és a bizonyítása egyaránt fontos — az utóbbi azért, mert onnan tudjuk meg, hogyan lehet egy partikuláris megoldást keresni.

Bizonyítás: a lényege az, hogy

Szavakban a feltétel úgy szól, hogy „a modulusok legnagyobb közös osztójának osztania kell a konstansok különbségét”. A tétel és a bizonyítása egyaránt fontos — az utóbbi azért, mert onnan tudjuk meg, hogyan lehet egy partikuláris megoldást keresni.

Bizonyítás: a lényege az, hogy **diofantoszi egyenletre** vezetjük vissza!

Szavakban a feltétel úgy szól, hogy „a modulusok legnagyobb közös osztójának osztania kell a konstansok különbségét”. A tétel és a bizonyítása egyaránt fontos — az utóbbi azért, mert onnan tudjuk meg, hogyan lehet egy partikuláris megoldást keresni.

Bizonyítás: a lényege az, hogy **diofantoszi egyenletre** vezetjük vissza!

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

pontosan akkor oldható meg, ha

$$(\exists x)(\exists y)(\exists z)$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2)$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2) \iff$$
$$(\exists y)(\exists z)$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2) \iff$$
$$(\exists y)(\exists z)\,(\qquad a_1 + ym_1 =$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2) \iff$$
$$(\exists y)(\exists z)\,(\qquad a_1 + ym_1 = \qquad \underbrace{a_2 + zm_2}$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2) \iff$$
$$(\exists y)(\exists z)\,(\quad a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}}\quad)$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \ \wedge\ x = a_2 + zm_2) \iff$$

$$(\exists y)(\exists z)\,(\quad a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \quad)$$

$$\iff$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2) \iff$$

$$(\exists y)(\exists z)\,(\quad a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \quad)$$

$$\iff m_1 y - m_2 z = a_2 - a_1 \text{ megoldható}$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \ \wedge\ x = a_2 + zm_2) \iff$$

$$(\exists y)(\exists z)\,(\qquad a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \qquad)$$

$$\iff m_1 y - m_2 z = a_2 - a_1 \text{ megoldható}$$

$$\iff \text{ln.k.o.}(m_1, -m_2) \mid a_2 - a_1$$

$$
\begin{aligned}
&(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2) \iff \\
&(\exists y)(\exists z)\,(\quad a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \quad) \\
&\iff m_1 y - m_2 z = a_2 - a_1 \text{ megoldható} \\
&\iff \text{ln.k.o.}(m_1, -m_2) \mid a_2 - a_1 \iff \text{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.
\end{aligned}
$$

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \ \wedge \ x = a_2 + zm_2) \iff$$
$$(\exists y)(\exists z)\,(\qquad a_1 + ym_1 = \qquad \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \qquad)$$
$$\iff m_1 y - m_2 z = a_2 - a_1 \text{ megoldható}$$
$$\iff \text{ln.k.o.}(m_1, -m_2) \mid a_2 - a_1 \iff \text{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.$$

Ezzel a tételnek a megoldhatóságra vonatkozó részét igazoltuk.

$$(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \;\wedge\; x = a_2 + zm_2) \iff$$

$$(\exists y)(\exists z)\,(\qquad a_1 + ym_1 = \qquad \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \qquad)$$

$$\iff m_1 y - m_2 z = a_2 - a_1 \text{ megoldható}$$

$$\iff \text{ln.k.o.}(m_1, -m_2) \mid a_2 - a_1 \iff \text{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.$$

Ezzel a tételnek a megoldhatóságra vonatkozó részét igazoltuk.

Az eddigiek **megmutatják**, hogyan kell a kongruenciarendszert diofantoszi egyenletre visszavezetni.

$$
\begin{gathered}
(\exists x)(\exists y)(\exists z)\,(x = a_1 + ym_1 \ \wedge\ x = a_2 + zm_2) \iff \\
(\exists y)(\exists z)\,(\qquad a_1 + ym_1 = \qquad \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \qquad) \\
\iff m_1 y - m_2 z = a_2 - a_1 \text{ megoldható} \\
\iff \text{ln.k.o.}(m_1, -m_2) \mid a_2 - a_1 \iff \text{ln.k.o.}(m_1, m_2) \mid a_1 - a_2.
\end{gathered}
$$

Ezzel a tételnek a megoldhatóságra vonatkozó részét igazoltuk.

Az eddigiek **megmutatják**, hogyan kell a kongruenciarendszert diofantoszi egyenletre visszavezetni. Az általános megoldásra vonatkozó rész könnyen adódik a diofantoszi egyenletből:

Ha y_0 az

$$a_1 + ym_1 =$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}$$

Ha y_0 az

$$a_1 + y m_1 = \underbrace{a_2 + z m_2}_{x\text{-nek választható}}$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor

Ha y_0 az

$$a_1 + y m_1 = \underbrace{a_2 + z m_2}_{x\text{-nek választható}} \iff m_1 y - m_2 z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk —

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1 y - m_2 z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit),

Ha y_0 az

$$a_1 + y m_1 = \underbrace{a_2 + z m_2}_{x\text{-nek választható}} \iff m_1 y - m_2 z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

$$x = a_1 + ym_1 =$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

$$x = a_1 + ym_1 = a_1 + (y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}) \cdot m_1 =$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

$$x = a_1 + ym_1 = a_1 + (y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}) \cdot m_1 =$$

$$\underbrace{(a_1 + y_0m_1)}$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

$$x = a_1 + ym_1 = a_1 + (y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}) \cdot m_1 =$$

$$\underbrace{(a_1 + y_0m_1)}_{x_0} + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)} \cdot m_1 =$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

$$x = a_1 + ym_1 = a_1 + (y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}) \cdot m_1 =$$

$$\underbrace{(a_1 + y_0m_1)}_{x_0} + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)} \cdot m_1 = x_0 + t \cdot$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1y - m_2z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \dfrac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

$$x = a_1 + ym_1 = a_1 + (y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}) \cdot m_1 =$$

$$\underbrace{(a_1 + y_0m_1)}_{x_0} + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)} \cdot m_1 = x_0 + t \cdot \text{lk.k.t.}(m_1, m_2).$$

Ha y_0 az

$$a_1 + ym_1 = \underbrace{a_2 + zm_2}_{x\text{-nek választható}} \iff m_1 y - m_2 z = a_2 - a_1$$

egyenlet partikuláris megoldása, akkor ezen egyenlet általános megoldása $y = y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}$ (a tanult képletben t helyett $-t$-t írtunk — ezt szabad volt, hiszen $-t$ is befutja $\mathbf{Z}$ elemeit), és így az x-re adódó általános megoldás

$$x = a_1 + ym_1 = a_1 + (y_0 + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)}) \cdot m_1 =$$

$$\underbrace{(a_1 + y_0 m_1)}_{x_0} + t \cdot \frac{m_2}{\text{ln.k.o.}(m_1, m_2)} \cdot m_1 = x_0 + t \cdot \text{lk.k.t.}(m_1, m_2).$$

Q.e.d.

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \ (mod\, m_1)$$
$$\dots$$
$$x \equiv a_k \ (mod\, m_k)$$

„úgy célszerű" megoldani, hogy —

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \pmod{m_1}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}$$

„úgy célszerű” megoldani, hogy — az előző tételnek megfelelően — két kongruenciát eggyel helyettesítünk

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \ \ (\mathit{mod}\, m_1)$$
$$\dots$$
$$x \equiv a_k \ \ (\mathit{mod}\, m_k)$$

„úgy célszerű” megoldani, hogy — az előző tételnek megfelelően — két kongruenciát eggyel helyettesítünk mindaddig, amíg a rendszer egynél több kongruenciából áll.

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \;\; (mod\, m_1)$$
$$\dots$$
$$x \equiv a_k \;\; (mod\, m_k)$$

„úgy célszerű" megoldani, hogy — az előző tételnek megfelelően — két kongruenciát eggyel helyettesítünk mindaddig, amíg a rendszer egynél több kongruenciából áll.

(B) A fenti kongruenciarendszer akkor és csak akkor oldható meg, ha bármely kételemű részrendszere megoldható,

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \ (\mathit{mod}\, m_1)$$
$$\dots$$
$$x \equiv a_k \ (\mathit{mod}\, m_k)$$

„úgy célszerű” megoldani, hogy — az előző tételnek megfelelően — két kongruenciát eggyel helyettesítünk mindaddig, amíg a rendszer egynél több kongruenciából áll.

(B) A fenti kongruenciarendszer akkor és csak akkor oldható meg, ha bármely kételemű részrendszere megoldható, azaz ha bármely $1 \leq i < j \leq k$ *esetén*

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \pmod{m_1}$$
$$\dots$$
$$x \equiv a_k \pmod{m_k}$$

„úgy célszerű" megoldani, hogy — az előző tételnek megfelelően — két kongruenciát eggyel helyettesítünk mindaddig, amíg a rendszer egynél több kongruenciából áll.

(B) A fenti kongruenciarendszer akkor és csak akkor oldható meg, ha bármely kételemű részrendszere megoldható, azaz ha bármely $1 \le i < j \le k$ *esetén ln.k.o.*$(m_i, m_j) \mid a_i - a_j$.

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \ (mod\, m_1)$$
$$\ldots$$
$$x \equiv a_k \ (mod\, m_k)$$

„úgy célszerű" megoldani, hogy — az előző tételnek megfelelően — két kongruenciát eggyel helyettesítünk mindaddig, amíg a rendszer egynél több kongruenciából áll.

(B) A fenti kongruenciarendszer akkor és csak akkor oldható meg, ha bármely kételemű részrendszere megoldható, azaz ha bármely $1 \leq i < j \leq k$ esetén ln.k.o.$(m_i, m_j) \mid a_i - a_j$. Ha megoldható és x_0 egy partikuláris megoldása, akkor az általános megoldása

29. Tétel. *(A) Az alábbi kongruenciarendszert*

$$x \equiv a_1 \ (\textit{mod}\, m_1)$$
$$\dots$$
$$x \equiv a_k \ (\textit{mod}\, m_k)$$

„úgy célszerű" megoldani, hogy — az előző tételnek megfelelően — két kongruenciát eggyel helyettesítünk mindaddig, amíg a rendszer egynél több kongruenciából áll.

(B) A fenti kongruenciarendszer akkor és csak akkor oldható meg, ha bármely kételemű részrendszere megoldható, azaz ha bármely $1 \le i < j \le k$ *esetén ln.k.o.*$(m_i, m_j) \mid a_i - a_j$. *Ha megoldható és* x_0 *egy partikuláris megoldása, akkor az általános megoldása*

$$x \equiv x_0 \ (\textit{mod}\, \textit{lk.k.t.}(m_1, m_2, \dots, m_k)).$$

(C) (**Kínai maradéktétel**) *Ha az* $m_1, \ldots, m_k$ *modulusok páronként relatív prímek,*

(C) **(Kínai maradéktétel)** *Ha az $m_1, \ldots, m_k$ modulusok páronként relatív prímek, akkor a fenti kongruenciarendszer mindig megoldható, és — egy partikuláris megoldását x_0-lal jelölve —*

(C) (**Kínai maradéktétel)** *Ha az* $m_1, \ldots, m_k$ *modulusok páronként relatív prímek, akkor a fenti kongruenciarendszer mindig megoldható, és — egy partikuláris megoldását* x_0*-lal jelölve — az általános megoldása*

$$x = x_0 + t \cdot m_1 \ldots m_k \qquad (t \in \mathbf{Z}).$$

(C) (**Kínai maradéktétel)** *Ha az $m_1, \ldots, m_k$ modulusok páronként relatív prímek, akkor a fenti kongruenciarendszer mindig megoldható, és — egy partikuláris megoldását x_0-lal jelölve — az általános megoldása*

$$x = x_0 + t \cdot m_1 \ldots m_k \qquad (t \in \mathbf{Z}).$$

A tétel (A) része valójában nem is tétel, hiszen az „úgy célszerű megoldani” nem egy matematikai állítás. (

*(C) (**Kínai maradéktétel**) Ha az $m_1, \dots, m_k$ modulusok páronként relatív prímek, akkor a fenti kongruenciarendszer mindig megoldható, és — egy partikuláris megoldását x_0-lal jelölve — az általános megoldása*

$$x = x_0 + t \cdot m_1 \dots m_k \qquad (t \in \mathbf{Z}).$$

A tétel (A) része valójában nem is tétel, hiszen az „úgy célszerű megoldani” nem egy matematikai állítás. (Részben ízlés dolga, hogy ki mit tart célszerűnek, másrészt a jövőben — legalábbis elvileg — egyéb célszerű megoldási módszereket is találhatnak, *(C)* *(***Kínai maradéktétel)** *Ha az* $m_1, \ldots, m_k$ *modulusok páronként relatív prímek, akkor a fenti kongruenciarendszer mindig megoldható, és — egy partikuláris megoldását* x_0*-lal jelölve — az általános megoldása*

$$x = x_0 + t \cdot m_1 \ldots m_k \qquad (t \in \mathbf{Z}).$$

A tétel (A) része valójában nem is tétel, hiszen az „úgy célszerű megoldani" nem egy matematikai állítás. (Részben ízlés dolga, hogy ki mit tart célszerűnek, másrészt a jövőben — legalábbis elvileg — egyéb célszerű megoldási módszereket is találhatnak, tehát — ellentétben a matematikai állításokkal —

*(C) (***Kínai maradéktétel)** *Ha az* $m_1, \ldots, m_k$ *modulusok páronként relatív prímek, akkor a fenti kongruenciarendszer mindig megoldható, és — egy partikuláris megoldását* x_0*-lal jelölve — az általános megoldása*

$$x = x_0 + t \cdot m_1 \ldots m_k \qquad (t \in \mathbf{Z}).$$

A tétel (A) része valójában nem is tétel, hiszen az „úgy célszerű megoldani” nem egy matematikai állítás. (Részben ízlés dolga, hogy ki mit tart célszerűnek, másrészt a jövőben — legalábbis elvileg — egyéb célszerű megoldási módszereket is találhatnak, tehát — ellentétben a matematikai állításokkal — az „úgy célszerű megoldani" kijelentésnek nem tulajdoníthatunk objektív logikai értéket.) Másfelől az (A) rész meglehetősen evidens, így nem bizonyítjuk.

A tétel (B) részének hosszadalmas bizonyításával nem foglalkozunk. (

A tétel (B) részének hosszadalmas bizonyításával nem foglalkozunk. (A $k = 2$ speciális esetet az előző tétel tartalmazza.)

A tétel (B) részének hosszadalmas bizonyításával nem foglalkozunk. (A $k = 2$ speciális esetet az előző tétel tartalmazza.) A (C) rész a (B) rész speciális esete és már az ókori Kínában is imerték (innen ered a neve).

A tétel (B) részének hosszadalmas bizonyításával nem foglalkozunk. (A $k = 2$ speciális esetet az előző tétel tartalmazza.) A (C) rész a (B) rész speciális esete és már az ókori Kínában is imerték (innen ered a neve). Tételeink „erejét” demonstrálja a következő „trükkös”

A tétel (B) részének hosszadalmas bizonyításával nem foglalkozunk. (A $k = 2$ speciális esetet az előző tétel tartalmazza.) A (C) rész a (B) rész speciális esete és már az ókori Kínában is imerték (innen ered a neve). Tételeink „erejét” demonstrálja a következő „trükkös” feladat megoldása:

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás:

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: L

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Lá

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Lát

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 =$

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása,

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása, azaz egy partikuláris megoldás.

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása, azaz egy partikuláris megoldás. A modulusok legkisebb közös többszöröse (

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása, azaz egy partikuláris megoldás. A modulusok legkisebb közös többszöröse (a prímfelbontásuk alapján)

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása, azaz egy partikuláris megoldás. A modulusok legkisebb közös többszöröse (a prímfelbontásuk alapján) $8 \cdot 7 \cdot 3 \cdot 5 =$

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása, azaz egy partikuláris megoldás. A modulusok legkisebb közös többszöröse (a prímfelbontásuk alapján) $8 \cdot 7 \cdot 3 \cdot 5 = 840$. Ezért

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$x \equiv 7 \pmod 8$$
$$x \equiv 6 \pmod 7$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 4 \pmod 5$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása, azaz egy partikuláris megoldás. A modulusok legkisebb közös többszöröse (a prímfelbontásuk alapján) $8 \cdot 7 \cdot 3 \cdot 5 = 840$. Ezért a kongruenciarendszer általános megoldása

Feladat Oldjuk meg az alábbi kongruenciarendszert:

$$\begin{aligned} x &\equiv 7 \pmod 8 \\ x &\equiv 6 \pmod 7 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

Megoldás: Látható, hogy az $x_0 = -1$ mindegyiknek megoldása, azaz egy partikuláris megoldás. A modulusok legkisebb közös többszöröse (a prímfelbontásuk alapján) $8 \cdot 7 \cdot 3 \cdot 5 = 840$. Ezért a kongruenciarendszer általános megoldása

$$x = 840t - 1 \qquad (t \in \mathbf{Z}).$$

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.)

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna.

Feladat: A kirándulócsoport harminchat-, húsz- és tizenöts-zemélyes kibérelhető hajó közül választhatott (de csak az egyi-ket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna. Ha a húszszemélyeset, akkor az utolsó fordulóra tizenkét utas maradt volna.

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna. Ha a húszszemélyeset, akkor az utolsó fordulóra tizenkét utas maradt volna. Végül a harminchat személyeset bérelték ki, és az utolsó fordulóra

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna. Ha a húszszemélyeset, akkor az utolsó fordulóra tizenkét utas maradt volna. Végül a harminchat személyeset bérelték ki, és az utolsó fordulóra tizenvalahány utas maradt.

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna. Ha a húszszemélyeset, akkor az utolsó fordulóra tizenkét utas maradt volna. Végül a harminchat személyeset bérelték ki, és az utolsó fordulóra tizenvalahány utas maradt. Pontosan hányan maradtak az utolsó fordulóra?

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna. Ha a húszszemélyeset, akkor az utolsó fordulóra tizenkét utas maradt volna. Végül a harminchat személyeset bérelték ki, és az utolsó fordulóra tizenvalahány utas maradt. Pontosan hányan maradtak az utolsó fordulóra?

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna. Ha a húszszemélyeset, akkor az utolsó fordulóra tizenkét utas maradt volna. Végül a harminchat személyeset bérelték ki, és az utolsó fordulóra tizenvalahány utas maradt. Pontosan hányan maradtak az utolsó fordulóra?

A megoldás

Feladat: A kirándulócsoport harminchat-, húsz- és tizenötszemélyes kibérelhető hajó közül választhatott (de csak az egyiket több fordulóra), hogy a szigetre utazzon. (A férőhelybe a legénység nem számít bele.) Ha a tizenötszemélyeset bérelték volna ki, akkor az utolsó fordulóra hét utas maradt volna. Ha a húszszemélyeset, akkor az utolsó fordulóra tizenkét utas maradt volna. Végül a harminchat személyeset bérelték ki, és az utolsó fordulóra tizenvalahány utas maradt. Pontosan hányan maradtak az utolsó fordulóra?

A megoldás nyilvánvaló módon adódik a következő feladat megoldásából, ha ott b jelöli az itt keresett számot és x jelöli a kirándulócsoport létszámát.

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$5 = \text{ln.k.o.}(20, 15) \mid 12 - 7$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$5 = \text{ln.k.o.}(20, 15) \mid 12 - 7 \qquad \text{(ez teljesül)},$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$5 = \text{ln.k.o.}(20, 15) \mid 12 - 7 \qquad \text{(ez teljesül)},$$
$$4 = \text{ln.k.o.}(36, 20) \mid b - 12$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$5 = \text{ln.k.o.}(20, 15) \mid 12 - 7 \qquad \text{(ez teljesül)},$$
$$4 = \text{ln.k.o.}(36, 20) \mid b - 12 \iff 4 \mid b$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$5 = \text{ln.k.o.}(20, 15) \mid 12 - 7 \qquad \text{(ez teljesül)},$$
$$4 = \text{ln.k.o.}(36, 20) \mid b - 12 \iff 4 \mid b \qquad \Longrightarrow b \in \{12, 16\},$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$
\begin{aligned}
5 = \text{ln.k.o.}(20, 15) \mid 12 - 7 & \qquad \text{(ez teljesül)}, \\
4 = \text{ln.k.o.}(36, 20) \mid b - 12 \iff 4 \mid b & \qquad \Longrightarrow b \in \{12, 16\}, \\
3 = \text{ln.k.o.}(36, 15) \mid b - 7 &
\end{aligned}
$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$5 = \text{ln.k.o.}(20, 15) \mid 12 - 7 \qquad \text{(ez teljesül)},$$
$$4 = \text{ln.k.o.}(36, 20) \mid b - 12 \iff 4 \mid b \qquad \Longrightarrow b \in \{12, 16\},$$
$$3 = \text{ln.k.o.}(36, 15) \mid b - 7 \Longrightarrow b \in \{10, 13, 16, 19\}.$$

Feladat: Minek kell a $b \in \{10, 11, \ldots, 19\}$ paramétert választani, hogy az alábbi kongruenciarendszernek legyen megoldása?

$$x \equiv b \pmod{36}$$
$$x \equiv 12 \pmod{20}$$
$$x \equiv 7 \pmod{15}$$

Megoldás: A megoldhatóság feltétele:

$$5 = \text{ln.k.o.}(20, 15) \mid 12 - 7 \qquad \text{(ez teljesül)},$$
$$4 = \text{ln.k.o.}(36, 20) \mid b - 12 \iff 4 \mid b \qquad \Longrightarrow b \in \{12, 16\},$$
$$3 = \text{ln.k.o.}(36, 15) \mid b - 7 \Longrightarrow b \in \{10, 13, 16, 19\}.$$

<u>Tehát a megoldás</u>: $b = 16$.

Feladat: Melyik a legkisebb olyan x négyjegyű természetes szám, amelyre

$$26x \equiv 20 \pmod{100}$$
$$36x \equiv 80 \pmod{40}$$
$$18x \equiv 68 \pmod{73}$$

Feladat: Melyik a legkisebb olyan x négyjegyű természetes szám, amelyre

$$26x \equiv 20 \pmod{100}$$
$$36x \equiv 80 \pmod{40}$$
$$18x \equiv 68 \pmod{73}$$

Megoldás:

Feladat: Melyik a legkisebb olyan x négyjegyű természetes szám, amelyre

$$26x \equiv 20 \pmod{100}$$
$$36x \equiv 80 \pmod{40}$$
$$18x \equiv 68 \pmod{73}$$

Megoldás: Először külön-külön kell az egyes kongruenciákat megoldanunk.

$$26x \equiv 20 \pmod{100}$$

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50}$$

$$26x \equiv 20 \pmod{100} \iff$$

$$13x \equiv 10 \pmod{50} \iff$$

$$10 = 13x + 50y =$$

$$26x \equiv 20 \pmod{100} \iff$$

$$13x \equiv 10 \pmod{50} \iff$$

$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y =$$

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük,

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni.

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni.
Legyen mondjuk $t = 4$,

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x+4y}_{z}) - 2y = 2(\underbrace{6z-y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni.

Legyen mondjuk $t = 4$, $z = 2$,

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni.

Legyen mondjuk $t = 4$, $z = 2$, $y =$

$$26x \equiv 20 \pmod{100} \iff$$

$$13x \equiv 10 \pmod{50} \iff$$

$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni.

Legyen mondjuk $t = 4$, $z = 2$, $y = 6z - t = 8$,

$$26x \equiv 20 \pmod{100} \iff$$

$$13x \equiv 10 \pmod{50} \iff$$

$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni.

Legyen mondjuk $t = 4$, $z = 2$, $y = 6z - t = 8$, $x =$

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel $\text{ln.k.o.}(13, 50) = 1$-et ismerjük, elég egy megoldást találni.

Legyen mondjuk $t = 4$, $z = 2$, $y = 6z - t = 8$, $x = z - 4y = -30$.

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni. Legyen mondjuk $t = 4$, $z = 2$, $y = 6z - t = 8$, $x = z - 4y = -30$. Tehát az első kongruencia az alábbival ekvivalens:

$$x \equiv -30 \pmod{50}.$$

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni. Legyen mondjuk $t = 4$, $z = 2$, $y = 6z - t = 8$, $x = z - 4y = -30$. Tehát az első kongruencia az alábbival ekvivalens:

$$x \equiv -30 \pmod{50}.$$

(Célszerű lenne ehelyett a $x \equiv 20 \pmod{50}$-ra áttérni, de tanulságosabb, ha nem tesszük.)

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel $\ln.k.o.(13, 50) = 1$-et ismerjük, elég egy megoldást találni. Legyen mondjuk $t = 4$, $z = 2$, $y = 6z - t = 8$, $x = z - 4y = -30$. Tehát az első kongruencia az alábbival ekvivalens:

$$x \equiv -30 \pmod{50}\,.$$

(Célszerű lenne ehelyett a $x \equiv 20 \pmod{50}$-ra áttérni, de tanulságosabb, ha nem tesszük.)

$$26x \equiv 20 \pmod{100} \iff$$
$$13x \equiv 10 \pmod{50} \iff$$
$$10 = 13x + 50y = 13(\underbrace{x + 4y}_{z}) - 2y = 2(\underbrace{6z - y}_{t}) + z.$$

Mivel ln.k.o.$(13, 50) = 1$-et ismerjük, elég egy megoldást találni. Legyen mondjuk $t = 4$, $z = 2$, $y = 6z - t = 8$, $x = z - 4y = -30$. Tehát az első kongruencia az alábbival ekvivalens:

$$x \equiv -30 \pmod{50}\,.$$

(Célszerű lenne ehelyett a $x \equiv 20 \pmod{50}$-ra áttérni, de tanulságosabb, ha nem tesszük.) Nézzük most a második kongruenciát:

$$36x \equiv 80 \pmod{40}$$

$$36x \equiv 80 \pmod{40} \iff$$

$$36x \equiv 80 \pmod{40} \iff$$
$$9x \equiv 20 \pmod{10}$$

$$36x \equiv 80 \pmod{40} \iff$$
$$9x \equiv 20 \pmod{10} \iff$$

$$36x \equiv 80 \pmod{40} \iff$$
$$9x \equiv 20 \pmod{10} \iff$$
$$9x \equiv 0 \pmod{10}$$

$$36x \equiv 80 \pmod{40} \iff$$

$$9x \equiv 20 \pmod{10} \iff$$

$$9x \equiv 0 \pmod{10} \iff$$

$$
\begin{aligned}
36x \equiv 80 \pmod{40} &\iff \\
9x \equiv 20 \pmod{10} &\iff \\
9x \equiv 0 \pmod{10} &\iff \\
-x \equiv 0 \pmod{10}
\end{aligned}
$$

$$\begin{aligned} 36x \equiv 80 \pmod{40} &\iff \\ 9x \equiv 20 \pmod{10} &\iff \\ 9x \equiv 0 \pmod{10} &\iff \\ -x \equiv 0 \pmod{10} &\iff \end{aligned}$$

$$
\begin{aligned}
36x \equiv 80 \pmod{40} &\iff \\
9x \equiv 20 \pmod{10} &\iff \\
9x \equiv 0 \pmod{10} &\iff \\
-x \equiv 0 \pmod{10} &\iff \\
x \equiv 0 \pmod{10}&.
\end{aligned}
$$

$$
\begin{aligned}
36x \equiv 80 \pmod{40} &\iff \\
9x \equiv 20 \pmod{10} &\iff \\
9x \equiv 0 \pmod{10} &\iff \\
-x \equiv 0 \pmod{10} &\iff \\
x \equiv 0 \pmod{10}\,.
\end{aligned}
$$

Tehát a második kongruencia ekvivalens az alábbival:

$$x \equiv 0 \pmod{10}.$$

$$
\begin{aligned}
36x \equiv 80 \pmod{40} &\iff \\
9x \equiv 20 \pmod{10} &\iff \\
9x \equiv 0 \pmod{10} &\iff \\
-x \equiv 0 \pmod{10} &\iff \\
x \equiv 0 \pmod{10}&.
\end{aligned}
$$

Tehát a második kongruencia ekvivalens az alábbival:

$$x \equiv 0 \pmod{10}.$$

Nézzük a harmadikat:

$$18x \equiv 68 \pmod{73}$$

$$18x \equiv 68 \pmod{73} \iff$$

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73}$$

$$18x \equiv 68 \pmod{73} \iff$$

$$9x \equiv 34 \pmod{73} \iff$$

$$18x \equiv 68 \pmod{73} \iff$$

$$9x \equiv 34 \pmod{73} \iff$$

$34 =$

$$18x \equiv 68 \pmod{73} \iff$$

$$9x \equiv 34 \pmod{73} \iff$$

$$34 = 9x$$

$$18x \equiv 68 \pmod{73} \iff$$

$$9x \equiv 34 \pmod{73} \iff$$

$$34 = 9x + 73y =$$

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73} \iff$$
$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y$$

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73} \iff$$
$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.$$

Legyen mondjuk

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73} \iff$$
$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.$$

Legyen mondjuk $z = 3$,

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73} \iff$$
$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.$$

Legyen mondjuk $z = 3$, $y = 7$,

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73} \iff$$
$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.$$

Legyen mondjuk $z = 3$, $y = 7$, $x =$

$$18x \equiv 68 \pmod{73} \iff$$

$$9x \equiv 34 \pmod{73} \iff$$

$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.$$

Legyen mondjuk $z = 3$, $y = 7$, $x = z - 8y =$

$$
\begin{gathered}
18x \equiv 68 \pmod{73} \iff \\
9x \equiv 34 \pmod{73} \iff \\
34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.
\end{gathered}
$$

Legyen mondjuk $z = 3$, $y = 7$, $x = z - 8y = -53$. Tehát a most vizsgált kongruencia megoldása

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73} \iff$$
$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.$$

Legyen mondjuk $z = 3$, $y = 7$, $x = z - 8y = -53$. Tehát a most vizsgált kongruencia megoldása $x \equiv -53 \pmod{73}$.

$$18x \equiv 68 \pmod{73} \iff$$
$$9x \equiv 34 \pmod{73} \iff$$
$$34 = 9x + 73y = 9(\underbrace{x + 8y}_{z}) + y\,.$$

Legyen mondjuk $z = 3$, $y = 7$, $x = z - 8y = -53$. Tehát a most vizsgált kongruencia megoldása $x \equiv -53 \pmod{73}$. Az eredetivel ekvivalens rendszer az alábbi:

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73} .$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73} .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73}\ .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)

Az első két kongruenciát tekintve

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73}\ .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)

Az első két kongruenciát tekintve a modulusok legkisebb közös többszöröse

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73}\ .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)

Az első két kongruenciát tekintve a modulusok legkisebb közös többszöröse 50.

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73}\ .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)

Az első két kongruenciát tekintve a modulusok legkisebb közös többszöröse 50. Elegendő egy közös partikuláris megoldást keresnünk:

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73}\ .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)
Az első két kongruenciát tekintve a modulusok legkisebb közös többszöröse 50. Elegendő egy közös partikuláris megoldást keresnünk:

$$x = -30 + 50y$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73}\ .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)
Az első két kongruenciát tekintve a modulusok legkisebb közös többszöröse 50. Elegendő egy közös partikuláris megoldást keresnünk:

$$x = -30 + 50y = 0 + 10z \iff$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73}\ .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.)

Az első két kongruenciát tekintve a modulusok legkisebb közös többszöröse 50. Elegendő egy közös partikuláris megoldást keresnünk:

$$x = -30 + 50y = 0 + 10z \iff 50y - 10z = 30 \wedge$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv 0 \pmod{10}$$
$$x \equiv -53 \pmod{73} .$$

(Természetesen egyből látszik, hogy az $x = -30$ közös megoldása az első kettőnek, de a módszer ismertetése érdekében ezt most nem vesszük észre, mint ahogy mást sem korábban.) Az első két kongruenciát tekintve a modulusok legkisebb közös többszöröse 50. Elegendő egy közös partikuláris megoldást keresnünk:

$$x = -30 + 50y = 0 + 10z \iff 50y - 10z = 30 \wedge x = 10z$$

$$5y - z = 3,$$

$5y - z = 3$, legyen mondjuk

$5y - z = 3$, legyen mondjuk $y = 0$, $z = -3$,

$5y - z = 3$, legyen mondjuk $y = 0$, $z = -3$, $x = -30$. Tehát

$5y - z = 3$, legyen mondjuk $y = 0$, $z = -3$, $x = -30$. Tehát az első két kongruenciából álló rendszer ekvivalens az alábbival:

$5y - z = 3$, legyen mondjuk $y = 0$, $z = -3$, $x = -30$. Tehát az első két kongruenciából álló rendszer ekvivalens az alábbival:

$$x \equiv -30 \pmod{50}.$$

$5y - z = 3$, legyen mondjuk $y = 0$, $z = -3$, $x = -30$. Tehát az első két kongruenciából álló rendszer ekvivalens az alábbival:

$$x \equiv -30 \pmod{50}.$$

Így az alábbi kongruenciarendszerrel kell foglalkoznunk:

$$x \equiv -30 \pmod{50}$$

$$
\begin{aligned}
x &\equiv -30 \pmod{50} \\
x &\equiv -53 \pmod{73} \ .
\end{aligned}
$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \land x = -53 + 73z$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z =$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u =$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t-23 =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$,

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff \quad 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73} \ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$,
$z =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z-y}_{u}) + 23z = 23(\underbrace{2u+z}_{v}) + 4u = 4(\underbrace{6v+u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u = -149$,

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u = -149$, $y =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z-y}_{u}) + 23z = 23(\underbrace{2u+z}_{v}) + 4u = 4(\underbrace{6v+u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u = -149$, $y = z - u =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u = -149$, $y = z - u = -218$,

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u = -149$, $y = z - u = -218$, $x = -30 + 50y = -30 + 50 \cdot (-218) =$

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z-y}_{u}) + 23z = 23(\underbrace{2u+z}_{v}) + 4u = 4(\underbrace{6v+u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u = -149$, $y = z - u = -218$, $x = -30 + 50y = -30 + 50 \cdot (-218) = -10930$. Tehát

$$x \equiv -30 \pmod{50}$$
$$x \equiv -53 \pmod{73}\ .$$

Diofantoszi egyenletre vezetjük vissza:

$$x = -30 + 50y \wedge x = -53 + 73z$$
$$\underbrace{-30 + 50y}_{x} = -53 + 73z \iff 23 = 73z - 50y$$
$$23 = 50(\underbrace{z - y}_{u}) + 23z = 23(\underbrace{2u + z}_{v}) + 4u = 4(\underbrace{6v + u}_{t}) - v$$

Legyen mondjuk $t = 3$, ekkor $v = 4t - 23 = -11$, $u = t - 6v = 69$, $z = v - 2u = -149$, $y = z - u = -218$, $x = -30 + 50y = -30 + 50 \cdot (-218) = -10930$. Tehát egy partikuláris megoldás az $x_0 = -10930$.

Mivel $\text{lk.k.t.}(50, 73) = 50 \cdot 73 = 3650$,

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

Mivel lk.k.t.$(50,73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \leq 3650t - 10930 < 10000 \iff$$

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \leq 3650t - 10930 < 10000 \iff 11930 \leq 3650t < 20930$$

Mivel lk.k.t.$(50,73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \le 3650t - 10930 < 10000 \iff 11930 \le 3650t < 20930$$

$$3,27 \approx \frac{11930}{3650} \le t < \frac{20930}{3650} \approx 5,73\ .$$

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \leq 3650t - 10930 < 10000 \iff 11930 \leq 3650t < 20930$$

$$3,27 \approx \frac{11930}{3650} \leq t < \frac{20930}{3650} \approx 5,73 \ .$$

A legkisebb ilyen x-et a legkisebb t adja, azaz

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \le 3650t - 10930 < 10000 \iff 11930 \le 3650t < 20930$$

$$3,27 \approx \frac{11930}{3650} \le t < \frac{20930}{3650} \approx 5,73\ .$$

A legkisebb ilyen x-et a legkisebb t adja, azaz $t = 4$ és $x = 3650 \cdot 4 - 10930 =$

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \le 3650t - 10930 < 10000 \iff 11930 \le 3650t < 20930$$
$$3,27 \approx \frac{11930}{3650} \le t < \frac{20930}{3650} \approx 5,73 \ .$$

A legkisebb ilyen x-et a legkisebb t adja, azaz $t = 4$ és $x = 3650 \cdot 4 - 10930 = 3670$.

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \leq 3650t - 10930 < 10000 \iff 11930 \leq 3650t < 20930$$
$$3,27 \approx \frac{11930}{3650} \leq t < \frac{20930}{3650} \approx 5,73\ .$$

A legkisebb ilyen x-et a legkisebb t adja, azaz $t = 4$ és $x = 3650 \cdot 4 - 10930 = 3670$. <u>Tehát a feladat megoldása</u>:

Mivel lk.k.t.$(50, 73) = 50 \cdot 73 = 3650$, a kiindulási kongruencia-rendszer általános megoldása

$$x \equiv -10930 \pmod{3650}, \quad \text{azaz } x = 3650t - 10930 \quad (t \in \mathbf{Z}).$$

Mármost x pontosan akkor négyjegyű természetes szám, ha

$$1000 \leq 3650t - 10930 < 10000 \iff 11930 \leq 3650t < 20930$$
$$3,27 \approx \frac{11930}{3650} \leq t < \frac{20930}{3650} \approx 5,73\ .$$

A legkisebb ilyen x-et a legkisebb t adja, azaz $t = 4$ és $x = 3650 \cdot 4 - 10930 = 3670$. Tehát a feladat megoldása: $x = 3670$.

Definíció Ha $n \in \mathbf{N}$, akkor az $\{x \in \mathbf{N} : x \leq n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszámát $\varphi(n)$-nel jelöljük, és φ-t az **Euler-féle φ függvénynek** nevezzük.

Definíció Ha $n \in \mathbf{N}$, akkor az $\{x \in \mathbf{N} : x \leq n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszámát $\varphi(n)$-nel jelöljük, és φ-t az **Euler-féle φ függvénynek** nevezzük.

Tehát $\varphi(n)$ az n-nél nem nagyobb, n-hez relatív prím pozitív egész számok számát jelöli.

Definíció Ha $n \in \mathbf{N}$, akkor az $\{x \in \mathbf{N} : x \leq n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszámát $\varphi(n)$-nel jelöljük, és φ-t az **Euler-féle φ függvénynek** nevezzük.

Tehát $\varphi(n)$ az n-nél nem nagyobb, n-hez relatív prím pozitív egész számok számát jelöli. Nyilván $\varphi(1) = 1$.

Definíció Ha $n \in \mathbf{N}$, akkor az $\{x \in \mathbf{N} : x \leq n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszámát $\varphi(n)$-nel jelöljük, és φ-t az **Euler-féle φ függvénynek** nevezzük.

Tehát $\varphi(n)$ az n-nél nem nagyobb, n-hez relatív prím pozitív egész számok számát jelöli. Nyilván $\varphi(1) = 1$. Ha $n > 1$, akkor

Definíció Ha $n \in \mathbf{N}$, akkor az $\{x \in \mathbf{N} : x \leq n$ és $\text{ln.k.o.}(x, n) = 1\}$ halmaz elemszámát $\varphi(n)$-nel jelöljük, és φ-t az **Euler-féle φ függvénynek** nevezzük.

Tehát $\varphi(n)$ az n-nél nem nagyobb, n-hez relatív prím pozitív egész számok számát jelöli. Nyilván $\varphi(1) = 1$. Ha $n > 1$, akkor úgy is fogalmazhatunk, hogy $\varphi(n)$ az n-nél kisebb, n-hez relatív prím pozitív egész számok száma.

Definíció Ha $n \in \mathbf{N}$, akkor az $\{x \in \mathbf{N} : x \leq n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszámát $\varphi(n)$-nel jelöljük, és φ-t az **Euler-féle φ függvénynek** nevezzük.

Tehát $\varphi(n)$ az n-nél nem nagyobb, n-hez relatív prím pozitív egész számok számát jelöli. Nyilván $\varphi(1) = 1$. Ha $n > 1$, akkor úgy is fogalmazhatunk, hogy $\varphi(n)$ az n-nél kisebb, n-hez relatív prím pozitív egész számok száma. Például $\varphi(6) = 2$, $\varphi(7) = 6$, és általában is,

Definíció Ha $n \in \mathbf{N}$, akkor az $\{x \in \mathbf{N} : x \leq n$ és $\text{ln.k.o.}(x, n) = 1\}$ halmaz elemszámát $\varphi(n)$-nel jelöljük, és φ-t az **Euler-féle φ függvénynek** nevezzük.

Tehát $\varphi(n)$ az n-nél nem nagyobb, n-hez relatív prím pozitív egész számok számát jelöli. Nyilván $\varphi(1) = 1$. Ha $n > 1$, akkor úgy is fogalmazhatunk, hogy $\varphi(n)$ az n-nél kisebb, n-hez relatív prím pozitív egész számok száma. Például $\varphi(6) = 2$, $\varphi(7) = 6$, és általában is, ha p prím, akkor $\varphi(p) = p - 1$.

Mivel ln.k.o.$(0, n) = n$, az $n = 1$, illetve $n > 1$ esetet megvizsgálva könnyen látható, hogy

Mivel ln.k.o.$(0, n) = n$, az $n = 1$, illetve $n > 1$ esetet megvizsgálva könnyen látható, hogy

Észrevétel: Ha $n \in \mathbf{N}$, akkor $\varphi(n)$ éppen a

Mivel ln.k.o.$(0, n) = n$, az $n = 1$, illetve $n > 1$ esetet megvizsgálva könnyen látható, hogy

Észrevétel: Ha $n \in \mathbf{N}$, akkor $\varphi(n)$ éppen a $\{x \in \mathbf{N}_0 : x < n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszáma.

Mivel ln.k.o.$(0, n) = n$, az $n = 1$, illetve $n > 1$ esetet megvizsgálva könnyen látható, hogy

Észrevétel: Ha $n \in \mathbf{N}$, akkor $\varphi(n)$ éppen a $\{x \in \mathbf{N}_0 : x < n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszáma.

A későbbi megfontolásaink során gyakran a

$$\varphi(n) = |\{x \in \mathbf{N}_0 : x < n \quad \text{és} \quad \text{ln.k.o.}(x, n) = 1\}|$$

összefüggést fogjuk használni.

Mivel ln.k.o.$(0, n) = n$, az $n = 1$, illetve $n > 1$ esetet megvizsgálva könnyen látható, hogy

Észrevétel: Ha $n \in \mathbf{N}$, akkor $\varphi(n)$ éppen a $\{x \in \mathbf{N}_0 : x < n$ és ln.k.o.$(x, n) = 1\}$ halmaz elemszáma.

A későbbi megfontolásaink során gyakran a

$$\varphi(n) = |\{x \in \mathbf{N}_0 : x < n \quad \text{és} \quad \text{ln.k.o.}(x, n) = 1\}|$$

összefüggést fogjuk használni.

A kongruenciarendszerekről tanultak alapján megmutatjuk, hogyan lehet $\varphi(n)$-et az n prímhatványtényezős felbontása alapján könnyen meghatározni.

30. Tétel. *Ha* $n \in \mathbf{N}$ *prímhatványtényezős alakja*

$$\prod_{i=1}^{t} p_i^{k_i},$$

akkor

30. Tétel. *Ha $n \in \mathbf{N}$ prímhatványtényezős alakja*

$$\prod_{i=1}^{t} p_i^{k_i},$$

akkor

$$\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i - 1}) =$$

30. Tétel. *Ha* $n \in \mathbf{N}$ *prímhatványtényezős alakja*

$$\prod_{i=1}^{t} p_i^{k_i},$$

akkor

$$\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{i=1}^{t} (1 - \frac{1}{p_i}).$$

Az világos, hogy ha $n = p^k$ (prímhatvány), akkor az n-hez

30. Tétel. *Ha $n \in \mathbf{N}$ prímhatványtényezős alakja*

$$\prod_{i=1}^{t} p_i^{k_i},$$

akkor

$$\varphi(n) = \prod_{i=1}^{t}(p_i^{k_i} - p_i^{k_i-1}) = n\prod_{i=1}^{t}(1 - \frac{1}{p_i}).$$

Az világos, hogy ha $n = p^k$ (prímhatvány), akkor az n-hez **nem** relatív prímek éppen a p-vel osztható számok, tehát az $\{1, 2, \ldots, n = p^k\}$ halmazból minden p-edik,

30. Tétel. *Ha $n \in \mathbf{N}$ prímhatványtényezős alakja*

$$\prod_{i=1}^{t} p_i^{k_i},$$

akkor

$$\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{i=1}^{t} (1 - \frac{1}{p_i}).$$

Az világos, hogy ha $n = p^k$ (prímhatvány), akkor az n-hez **nem** relatív prímek éppen a p-vel osztható számok, tehát az $\{1, 2, \ldots, n = p^k\}$ halmazból minden p-edik, ezek száma $\frac{n}{p} = p^{k-1}$,

30. Tétel. *Ha $n \in \mathbf{N}$ prímhatványtényezős alakja*

$$\prod_{i=1}^{t} p_i^{k_i},$$

akkor

$$\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{i=1}^{t} (1 - \frac{1}{p_i}).$$

Az világos, hogy ha $n = p^k$ (prímhatvány), akkor az n-hez **nem** relatív prímek éppen a p-vel osztható számok, tehát az $\{1, 2, \ldots, n = p^k\}$ halmazból minden p-edik, ezek száma $\frac{n}{p} = p^{k-1}$, és pontosan a visszamaradó számok lesznek n-hez relatív prímek, szám szerint $p^k - p^{k-1}$.

30. Tétel. *Ha $n \in \mathbf{N}$ prímhatványtényezős alakja*

$$\prod_{i=1}^{t} p_i^{k_i},$$

akkor

$$\varphi(n) = \prod_{i=1}^{t} (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{i=1}^{t} (1 - \frac{1}{p_i}).$$

Az világos, hogy ha $n = p^k$ (prímhatvány), akkor az n-hez **nem** relatív prímek éppen a p-vel osztható számok, tehát az $\{1, 2, \ldots, n = p^k\}$ halmazból minden p-edik, ezek száma $\frac{n}{p} = p^{k-1}$, és pontosan a visszamaradó számok lesznek n-hez relatív prímek, szám szerint $p^k - p^{k-1}$. Tehát prímhatványra a tétel igaz.

Az is világos (a baloldali szorzat minden egyes tényezőjéből a kisebbítendőt kiemelve), hogy

$$\prod_{i=1}^{t}(p_i^{k_i} - p_i^{k_i-1}) =$$

Az is világos (a baloldali szorzat minden egyes tényezőjéből a kisebbítendőt kiemelve), hogy

$$\prod_{i=1}^{t}(p_i^{k_i} - p_i^{k_i-1}) = n\prod_{i=1}^{t}(1 - \frac{1}{p_i}).$$

Az is világos (a baloldali szorzat minden egyes tényezőjéből a kisebbítendőt kiemelve), hogy

$$\prod_{i=1}^{t}(p_i^{k_i} - p_i^{k_i-1}) = n\prod_{i=1}^{t}(1 - \frac{1}{p_i}).$$

Ezért — az eddigiek figyelembe vételével — a fenti tétel könnyen következik az alábbiból.

31. Tétel. *Ha $m, n \in \mathbf{N}$ relatív prímek, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.*

Az is világos (a baloldali szorzat minden egyes tényezőjéből a kisebbítendőt kiemelve), hogy

$$\prod_{i=1}^{t}(p_i^{k_i} - p_i^{k_i-1}) = n\prod_{i=1}^{t}(1 - \frac{1}{p_i}).$$

Ezért — az eddigiek figyelembe vételével — a fenti tétel könnyen következik az alábbiból.

31. Tétel. *Ha $m, n \in \mathbf{N}$ relatív prímek, akkor $\varphi(mn) = \varphi(m)\varphi(n)$.*

Ha m és n nem relatív prímek, akkor ez nem igaz, pl. $\varphi(3{\cdot}3) = 6$, de $\varphi(3) \cdot \varphi(3) = 4$.

Bizonyítás:

Bizonyítás: Legyen (a könnyebb jelölések érdekében) $k = \varphi(m)$, $\ell = \varphi(n)$.

Bizonyítás: Legyen (a könnyebb jelölések érdekében) $k = \varphi(m)$, $\ell = \varphi(n)$. A $\{0, 1, \ldots, m-1\}$ halmaz m-hez relatív prím elemeit (

Bizonyítás: Legyen (a könnyebb jelölések érdekében) $k = \varphi(m)$, $\ell = \varphi(n)$. A $\{0, 1, \ldots, m-1\}$ halmaz m-hez relatív prím elemeit (számuk pontosan k)

Bizonyítás: Legyen (a könnyebb jelölések érdekében) $k = \varphi(m)$, $\ell = \varphi(n)$. A $\{0, 1, \ldots, m-1\}$ halmaz m-hez relatív prím elemeit (számuk pontosan k) jelölje $a_1, \ldots, a_k$. Hasonlóan, a $\{0, 1, \ldots, n-1\}$ halmaz n-hez relatív prím elemeit (

Bizonyítás: Legyen (a könnyebb jelölések érdekében) $k = \varphi(m)$, $\ell = \varphi(n)$. A $\{0, 1, \ldots, m-1\}$ halmaz m-hez relatív prím elemeit (számuk pontosan k) jelölje $a_1, \ldots, a_k$. Hasonlóan, a $\{0, 1, \ldots, n-1\}$ halmaz n-hez relatív prím elemeit (számuk pontosan ℓ)

Bizonyítás: Legyen (a könnyebb jelölések érdekében) $k = \varphi(m)$, $\ell = \varphi(n)$. A $\{0, 1, \ldots, m-1\}$ halmaz m-hez relatív prím elemeit (számuk pontosan k) jelölje $a_1, \ldots, a_k$. Hasonlóan, a $\{0, 1, \ldots, n-1\}$ halmaz n-hez relatív prím elemeit (számuk pontosan ℓ) pedig jelölje $b_1, \ldots, b_\ell$.

Bizonyítás: Legyen (a könnyebb jelölések érdekében) $k = \varphi(m)$, $\ell = \varphi(n)$. A $\{0, 1, \ldots, m-1\}$ halmaz m-hez relatív prím elemeit (számuk pontosan k) jelölje $a_1, \ldots, a_k$. Hasonlóan, a $\{0, 1, \ldots, n-1\}$ halmaz n-hez relatív prím elemeit (számuk pontosan ℓ) pedig jelölje $b_1, \ldots, b_\ell$.

Minden egyes $i \in \{1, \ldots, k\}$ és $j \in \{1, \ldots, \ell\}$ indexpár esetén jelölje t_{ij} az

$$x \equiv a_i \pmod{m}$$
$$x \equiv b_j \pmod{n}$$

kongruenciarendszernek **azt a** megoldását, amelyik az $\{0, 1, \ldots, mn - 1\}$ halmazban van.

$$x \equiv a_i \pmod{m}$$
$$x \equiv b_j \pmod{n}$$

kongruenciarendszernek **azt a** megoldását, amelyik az $\{0, 1, \ldots, mn - 1\}$ halmazban van. A határozott névelőt használata most helyes, hiszen a kínai maradéktétel szerint a kongruenciarendszernek van megoldása, és a megoldása $x \equiv x_0 \pmod{mn}$ alakú. (

$$x \equiv a_i \pmod{m}$$
$$x \equiv b_j \pmod{n}$$

kongruenciarendszernek **azt a** megoldását, amelyik az $\{0, 1, \ldots, mn - 1\}$ halmazban van. A határozott névelőt használata most helyes, hiszen a kínai maradéktétel szerint a kongruenciarendszernek van megoldása, és a megoldása $x \equiv x_0 \pmod{mn}$ alakú. (Tehát a számegyenesen x_0-ból indulva

$$x \equiv a_i \pmod{m}$$
$$x \equiv b_j \pmod{n}$$

kongruenciarendszernek **azt a** megoldását, amelyik az $\{0, 1, \ldots, mn-1\}$ halmazban van. A határozott névelőt használata most helyes, hiszen a kínai maradéktétel szerint a kongruenciarendszernek van megoldása, és a megoldása $x \equiv x_0 \pmod{mn}$ alakú. (Tehát a számegyenesen x_0-ból indulva mn-es lépésekkel jobbra-balra haladva kapjuk a megoldást, világos, hogy ezen lépésekkel pontosan egyszer „lépünk bele” az mn „szélességű” $\{0, 1, \ldots, mn-1\}$ halmazba.)

Ha $(i_1, j_1), (i_2, j_2)$ olyan indexpárok, hogy $t_{i_1 j_1} = t_{i_2 j_2}$, akkor egyrészt

Ha $(i_1, j_1), (i_2, j_2)$ olyan indexpárok, hogy $t_{i_1 j_1} = t_{i_2 j_2}$, akkor egyrészt

$$a_{i_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv a_{i_2} \pmod{m}$$

miatt $i_1 = i_2$,

Ha $(i_1, j_1), (i_2, j_2)$ olyan indexpárok, hogy $t_{i_1 j_1} = t_{i_2 j_2}$, akkor egyrészt

$$a_{i_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv a_{i_2} \pmod m$$

miatt $i_1 = i_2$, és

$$b_{j_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv b_{j_2} \pmod n$$

miatt $j_1 = j_2$. (

Ha $(i_1, j_1), (i_2, j_2)$ olyan indexpárok, hogy $t_{i_1 j_1} = t_{i_2 j_2}$, akkor egyrészt

$$a_{i_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv a_{i_2} \pmod m$$

miatt $i_1 = i_2$, és

$$b_{j_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv b_{j_2} \pmod n$$

miatt $j_1 = j_2$. (Itt kihasználtuk, hogy pl. mivel $a_{i_1}, a_{i_2} \in \{0, 1, \ldots, m-1\}$ miatt csak úgy lehetnek modulo m kongruensek, ha egyenlők.)

Ha $(i_1, j_1), (i_2, j_2)$ olyan indexpárok, hogy $t_{i_1 j_1} = t_{i_2 j_2}$, akkor egyrészt

$$a_{i_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv a_{i_2} \pmod m$$

miatt $i_1 = i_2$, és

$$b_{j_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv b_{j_2} \pmod n$$

miatt $j_1 = j_2$. (Itt kihasználtuk, hogy pl. mivel $a_{i_1}, a_{i_2} \in \{0, 1, \ldots, m-1\}$ miatt csak úgy lehetnek modulo m kongruensek, ha egyenlők.) Ezért a t_{ij} számok páronként különbözők, és számuk

Ha $(i_1, j_1), (i_2, j_2)$ olyan indexpárok, hogy $t_{i_1 j_1} = t_{i_2 j_2}$, akkor egyrészt

$$a_{i_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv a_{i_2} \pmod m$$

miatt $i_1 = i_2$, és

$$b_{j_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv b_{j_2} \pmod n$$

miatt $j_1 = j_2$. (Itt kihasználtuk, hogy pl. mivel $a_{i_1}, a_{i_2} \in \{0, 1, \ldots, m-1\}$ miatt csak úgy lehetnek modulo m kongruensek, ha egyenlők.) Ezért a t_{ij} számok páronként különbözők, és számuk $k\ell =$

Ha $(i_1, j_1), (i_2, j_2)$ olyan indexpárok, hogy $t_{i_1 j_1} = t_{i_2 j_2}$, akkor egyrészt

$$a_{i_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv a_{i_2} \pmod m$$

miatt $i_1 = i_2$, és

$$b_{j_1} \equiv t_{i_1 j_1} = t_{i_2 j_2} \equiv b_{j_2} \pmod n$$

miatt $j_1 = j_2$. (Itt kihasználtuk, hogy pl. mivel $a_{i_1}, a_{i_2} \in \{0, 1, \ldots, m-1\}$ miatt csak úgy lehetnek modulo m kongruensek, ha egyenlők.) Ezért a t_{ij} számok páronként különbözők, és számuk $k\ell = \varphi(m)\varphi(n)$.

Mindegyik t_{ij} relatív prím az mn-hez.

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod m$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod m$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek,

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike.

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \dots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1.

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1. Az $y = mq + r$ maradékos osztást tekintve

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1. Az $y = mq + r$ maradékos osztást tekintve tudjuk (az euklideszi algoritmusból), hogy

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod m$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1. Az $y = mq + r$ maradékos osztást tekintve tudjuk (az euklideszi algoritmusból), hogy ln.k.o.$(y, m) =$ ln.k.o.(m, r). Tehát r az a_i-k egyike, és $y \equiv r \equiv a_i \pmod m$.

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1. Az $y = mq + r$ maradékos osztást tekintve tudjuk (az euklideszi algoritmusból), hogy ln.k.o.$(y, m) =$ ln.k.o.(m, r). Tehát r az a_i-k egyike, és $y \equiv r \equiv a_i \pmod{m}$. Hasonlóan kapjuk, hogy valamely j-re $y \equiv b_i \pmod{m}$.

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1. Az $y = mq + r$ maradékos osztást tekintve tudjuk (az euklideszi algoritmusból), hogy ln.k.o.$(y, m) =$ ln.k.o.(m, r). Tehát r az a_i-k egyike, és $y \equiv r \equiv a_i \pmod{m}$. Hasonlóan kapjuk, hogy valamely j-re $y \equiv b_i \pmod{m}$. Minthogy ugyanezek a feltételek

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1. Az $y = mq + r$ maradékos osztást tekintve tudjuk (az euklideszi algoritmusból), hogy ln.k.o.$(y, m) =$ ln.k.o.(m, r). Tehát r az a_i-k egyike, és $y \equiv r \equiv a_i \pmod{m}$. Hasonlóan kapjuk, hogy valamely j-re $y \equiv b_i \pmod{m}$. Minthogy ugyanezek a feltételek definiálják (és egyértelműen definiálják) a t_{ij}-t is, $y = t_{ij}$.

Mindegyik t_{ij} relatív prím az mn-hez. Hiszen ellenkező esetben valamely p prímre $p \mid t_{ij}$ és mondjuk $p \mid m$, de ekkor $t_{ij} \equiv a_i \pmod{m}$ miatt $p \mid m \mid a_i - t_{ij}$-ből és $p \mid t_{ij}$-ből $p \mid a_i$ adódik, és így p közös osztója a_i-nek és m-nek, holott ezek relatív prímek.

Már csak azt kell belátni, hogy ha $y \in \{1, \ldots, mn\}$ és ln.k.o.$(y, mn) = 1$, akkor y a t_{ij}-k egyike. Mármost ln.k.o.(y, m) is 1. Az $y = mq + r$ maradékos osztást tekintve tudjuk (az euklideszi algoritmusból), hogy ln.k.o.$(y, m) =$ ln.k.o.(m, r). Tehát r az a_i-k egyike, és $y \equiv r \equiv a_i \pmod{m}$. Hasonlóan kapjuk, hogy valamely j-re $y \equiv b_i \pmod{m}$. Minthogy ugyanezek a feltételek definiálják (és egyértelműen definiálják) a t_{ij}-t is, $y = t_{ij}$. Q.e.d.

Példák:

$$\varphi(10) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$

$$\varphi(100) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2 - 2^1)(5^2 - 5^1) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$

Példák:

$$\begin{aligned}
\varphi(10) &= \varphi(2)\varphi(5) = (2-1)(5-1) = 4, \\
\varphi(100) &= \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40, \\
\varphi(1000) &=
\end{aligned}$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) =$$

Példák:

$$\begin{aligned}
\varphi(10) &= \varphi(2)\varphi(5) = (2-1)(5-1) = 4,\\
\varphi(100) &= \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,\\
\varphi(1000) &= \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) =
\end{aligned}$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) = \varphi(2^3)\varphi(5) =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) = \varphi(2^3)\varphi(5) = 4 \cdot 4 =$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) = \varphi(2^3)\varphi(5) = 4\cdot 4 = 16.$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) = \varphi(2^3)\varphi(5) = 4 \cdot 4 = 16.$$

32. Tétel. *(**Euler-tétele**) Amennyiben $m \in \mathbf{N}$-re és $a \in \mathbf{Z}$-re ln.k.o.$(a, m) = 1$, akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) = \varphi(2^3)\varphi(5) = 4 \cdot 4 = 16.$$

32. Tétel. *(***Euler-tétele***) Amennyiben $m \in \mathbf{N}$-re és $a \in \mathbf{Z}$-re ln.k.o.$(a,m) = 1$, akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Megjegyzés:

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) = \varphi(2^3)\varphi(5) = 4\cdot 4 = 16.$$

32. Tétel. *(**Euler-tétele**) Amennyiben $m \in \mathbf{N}$-re és $a \in \mathbf{Z}$-re ln.k.o.$(a,m) = 1$, akkor*

$$a^{\varphi(m)} \equiv 1 \;(\mathit{mod}\, m)\,.$$

Megjegyzés: A kis Fermat-tétel ennek speciális esete, hiszen ha $m = p$ prím, akkor $\varphi(p) = p-1$ és

Példák:

$$\varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4,$$
$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2^1)(5^2-5^1) = 40,$$
$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = (2^3-2^2)(5^3-5^2) = 400,$$
$$\varphi(40) = \varphi(2^3)\varphi(5) = 4 \cdot 4 = 16.$$

32. Tétel. (**Euler-tétele**) *Amennyiben $m \in \mathbf{N}$-re és $a \in \mathbf{Z}$-re ln.k.o.$(a,m) = 1$, akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Megjegyzés: A kis Fermat-tétel ennek speciális esete, hiszen ha $m = p$ prím, akkor $\varphi(p) = p-1$ és ln.k.o.$(a,p) = 1 \iff p \not| \, a$.

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal.

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és} \quad x < m\}.$$

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és} \quad x < m\}.$$

Ekkor $|A| = \varphi(m)$

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és} \quad x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$,

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és } x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka.

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és } x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció.

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és } x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció. Nyilván $xa \equiv x\tau \pmod{m}$. Ezért

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és } x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció. Nyilván $xa \equiv x\tau \pmod{m}$. Ezért

$$a^{\varphi(m)} \cdot \prod_{x \in A} x$$

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és} \;\; x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció. Nyilván $xa \equiv x\tau \pmod{m}$. Ezért

$$a^{\varphi(m)} \cdot \prod_{x \in A} x = 1 \cdot \prod_{x \in A} xa \equiv$$

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és } x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció. Nyilván $xa \equiv x\tau \pmod m$. Ezért

$$a^{\varphi(m)} \cdot \prod_{x \in A} x = 1 \cdot \prod_{x \in A} xa \equiv 1 \cdot \prod_{x \in A} x\tau =$$

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és } x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció. Nyilván $xa \equiv x\tau \pmod{m}$. Ezért

$$a^{\varphi(m)} \cdot \prod_{x \in A} x = 1 \cdot \prod_{x \in A} xa \equiv 1 \cdot \prod_{x \in A} x\tau = 1 \cdot \prod_{x \in A} x \pmod{m}$$

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és} \ x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció. Nyilván $xa \equiv x\tau \pmod{m}$. Ezért

$$a^{\varphi(m)} \cdot \prod_{x \in A} x = 1 \cdot \prod_{x \in A} xa \equiv 1 \cdot \prod_{x \in A} x\tau = 1 \cdot \prod_{x \in A} x \pmod{m}$$

ahonnan az m-hez relatív prím

A bizonyítás alapgondolata: lényegében azonos a kis Fermat-tételnél látottal. Legyen

$$A = \{x \in \mathbf{N}_0 : \text{ln.k.o.}(x, m) = 1 \quad \text{és } x < m\}.$$

Ekkor $|A| = \varphi(m)$. Legyen $\tau : A \to A$, $x \mapsto$ az $xa : m$ osztás maradéka. Az eddigi ismeretek alapján könnyen kimutatható, hogy τ bijekció. Nyilván $xa \equiv x\tau \pmod m$. Ezért

$$a^{\varphi(m)} \cdot \prod_{x \in A} x = 1 \cdot \prod_{x \in A} xa \equiv 1 \cdot \prod_{x \in A} x\tau = 1 \cdot \prod_{x \in A} x \pmod m$$

ahonnan az m-hez relatív prím $\prod_{x \in A} x$-vel egyszerűsítve adódik az Euler-tétel. Q.e.d.

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$112134723635523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét.

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100.

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$.

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá $\text{ln.k.o.}(23, 100) = 1$.

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$112134723635 23^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt $\varphi(100) =$

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt $\varphi(100) = \varphi(4)\varphi(25) =$

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$112134723635 23^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá $\text{ln.k.o.}(23, 100) = 1$. Másrészt $\varphi(100) = \varphi(4)\varphi(25) = 40$. Tehát $23^{40} \equiv 1 \pmod{100}$.

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$112134723635 23^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt $\varphi(100) = \varphi(4)\varphi(25) = 40$. Tehát $23^{40} \equiv 1 \pmod{100}$. Miután az n kitevőt elosztottuk 40-nel, kapjuk, hogy $n = 40m + 2$ alakú. (

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt $\varphi(100) = \varphi(4)\varphi(25) = 40$. Tehát $23^{40} \equiv 1 \pmod{100}$. Miután az n kitevőt elosztottuk 40-nel, kapjuk, hogy $n = 40m + 2$ alakú. (Ez fejben is látszik, hiszen nekünk csak a maradék kell.) Az eddigiek szerint

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt $\varphi(100) = \varphi(4)\varphi(25) = 40$. Tehát $23^{40} \equiv 1 \pmod{100}$. Miután az n kitevőt elosztottuk 40-nel, kapjuk, hogy $n = 40m + 2$ alakú. (Ez fejben is látszik, hiszen nekünk csak a maradék kell.) Az eddigiek szerint

$$a^n \equiv 23^{40m+2} = (23^{40})^m \cdot 23^2 \equiv 1^m \cdot 23^2 = 529 \equiv 29 \pmod{100}.$$

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$112134723635 23^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt $\varphi(100) = \varphi(4)\varphi(25) = 40$. Tehát $23^{40} \equiv 1 \pmod{100}$. Miután az n kitevőt elosztottuk 40-nel, kapjuk, hogy $n = 40m + 2$ alakú. (Ez fejben is látszik, hiszen nekünk csak a maradék kell.) Az eddigiek szerint

$$a^n \equiv 23^{40m+2} = (23^{40})^m \cdot 23^2 \equiv 1^m \cdot 23^2 = 529 \equiv 29 \pmod{100}.$$

Tehát a megadott szám utolsó két számjegye:

Feladat: Határozzuk meg az alábbi szám utolsó két számjegyét:

$$11213472363523^{4040404042}$$

Megoldás: Jelölje a a hatvány alapját és n a kitevőjét. Azt a legfeljebb kétjegyű nemnegatív számot keressük, amelyel a^n kongruens modulo 100. Világos, hogy $a \equiv 23 \pmod{100}$. Továbbá ln.k.o.$(23, 100) = 1$. Másrészt $\varphi(100) = \varphi(4)\varphi(25) = 40$. Tehát $23^{40} \equiv 1 \pmod{100}$. Miután az n kitevőt elosztottuk 40-nel, kapjuk, hogy $n = 40m + 2$ alakú. (Ez fejben is látszik, hiszen nekünk csak a maradék kell.) Az eddigiek szerint

$$a^n \equiv 23^{40m+2} = (23^{40})^m \cdot 23^2 \equiv 1^m \cdot 23^2 = 529 \equiv 29 \pmod{100}.$$

<u>Tehát a megadott szám utolsó két számjegye: 29</u>.

(Aligha kell ecsetelni a fellépő nehézségeket, ha mindenféle elmélet nélkül fognánk hozzá az előbbi, vagy a következő feladathoz.)

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet:

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1}

Feladat: Határozzuk meg a $2007^{400000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000)$

Feladat: Határozzuk meg a $2007^{4000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000) = 400 \mid n+1$

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000) = 400 \mid n+1$ és $\text{ln.k.o.}(a, 1000) = 1$ miatt

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000) = 400 \mid n+1$ és ln.k.o.$(a, 1000) = 1$ miatt $a^{n+1} \equiv 1 \pmod{1000}$.

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000) = 400 \mid n+1$ és ln.k.o.$(a, 1000) = 1$ miatt $a^{n+1} \equiv 1 \pmod{1000}$.

Keresett az a legf. háromjegyű x, amelyre $a^n \equiv x \pmod{1000}$.

Feladat: Határozzuk meg a $2007^{40000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000) = 400 \mid n+1$ és ln.k.o.$(a, 1000) = 1$ miatt $a^{n+1} \equiv 1 \pmod{1000}$.

Keresett az a legf. háromjegyű x, amelyre $a^n \equiv x \pmod{1000}$.

$7x$

Feladat: Határozzuk meg a $2007^{4000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000) = 400 \mid n+1$ és ln.k.o.$(a, 1000) = 1$ miatt $a^{n+1} \equiv 1 \pmod{1000}$.

Keresett az a legf. háromjegyű x, amelyre $a^n \equiv x \pmod{1000}$.

$$7x \equiv a \cdot a^n = a^{n+1} = (a^{400})^q \equiv 1^q = 1 \pmod{1000}.$$

Feladat: Határozzuk meg a $2007^{400000000000001599}$ szám utolsó három számjegyét!

Megoldás: Alapötlet: a^n helyett a^{n+1} könnyű, hiszen $\varphi(1000) = 400 \mid n+1$ és ln.k.o.$(a, 1000) = 1$ miatt $a^{n+1} \equiv 1 \pmod{1000}$.

Keresett az a legf. háromjegyű x, amelyre $a^n \equiv x \pmod{1000}$.

$$7x \equiv a \cdot a^n = a^{n+1} = (a^{400})^q \equiv 1^q = 1 \pmod{1000}.$$

Tehát x-et megkapjuk, ha megoldjuk a $7x \equiv 1 \pmod{1000}$ lineáris kongruenciát.

$$7x \equiv 1 \pmod{1000}$$

$$7x \equiv 1 \pmod{1000} \qquad / \cdot 143$$

$$7x \equiv 1 \pmod{1000} \qquad / \cdot 143$$

$$1001x \equiv 143 \pmod{1000}$$

$$7x \equiv 1 \pmod{1000} \qquad / \cdot 143$$
$$1001x \equiv 143 \pmod{1000}$$

$$7x \equiv 1 \pmod{1000} \qquad\qquad / \cdot 143$$
$$1001x \equiv 143 \pmod{1000}$$
$$x \equiv 143 \pmod{1000}.$$

$$7x \equiv 1 \pmod{1000} \qquad\qquad / \cdot 143$$
$$1001x \equiv 143 \pmod{1000}$$
$$x \equiv 143 \pmod{1000}.$$

Tehát a kérdéses szám 143-ra végződik.

$$7x \equiv 1 \pmod{1000} \qquad\qquad / \cdot 143$$
$$1001x \equiv 143 \pmod{1000}$$
$$x \equiv 143 \pmod{1000}.$$

Tehát a kérdéses szám 143-ra végződik.

Most nézzünk egy olyan feladatot, amelyben többször is kell az eddig látott trükköket alkalmazni. (Ezt követően a hasonló jellegű feladatok nem okozhatnak nehézséget.)

Feladat: Határozzuk meg az $n = 214503^{640169^{8079}}$ utolsó két számjegyét.

Megoldás: $n = 214503^{640169^{8079}} \equiv$

Megoldás: $n = 214503^{640169^{8079}} \equiv 3^{640169^{8079}} =$

Megoldás: $n = 214503^{640169^{8079}} \equiv 3^{640169^{8079}} = 3^{40q+r} =$

Megoldás: $n = 214503^{640169^{8079}} \equiv 3^{640169^{8079}} = 3^{40q+r} = (3^{40})^q \cdot 3^r \equiv$

Megoldás: $n = 214503^{640169^{8079}} \equiv 3^{640169^{8079}} = 3^{40q+r} = (3^{40})^q \cdot 3^r \equiv 1^q \cdot 3^r = 3^r \pmod{100}$.

Megoldás: $n = 214503^{640169^{8079}} \equiv 3^{640169^{8079}} = 3^{40q+r} = (3^{40})^q \cdot 3^r \equiv 1^q \cdot 3^r = 3^r \pmod{100}$. Ehhez:

$r \equiv 640169^{8079} = 9^{8079} = 9^{\varphi(40)q'+r'} = 9^{16q'+15} = (9^{16})^{q'} . 9^{15} \equiv 1^{q'} . 9^{15} = 9^{15}$

Megoldás: $n = 214503^{640169^{8079}} \equiv 3^{640169^{8079}} = 3^{40q+r} = (3^{40})^q \cdot 3^r \equiv 1^q \cdot 3^r = 3^r \pmod{100}$. Ehhez:

$r \equiv 640169^{8079} = 9^{8079} = 9^{\varphi(40)q'+r'} = 9^{16q'+15} = (9^{16})^{q'}.9^{15} \equiv 1^{q'}.9^{15} = 9^{15} \pmod{40}$. A 9^{15} kiszámítása helyett gyorsabb, ha r ismeretlen, majd $\times 9$, utána $+80$:

$$r \equiv 9^{15} \pmod{40}$$
$$9r \equiv 1 \pmod{40}$$
$$9r \equiv 81 \pmod{40}$$
$$r \equiv 9 \pmod{40}.$$

$n \equiv 3^r = 3^9 = 81 \cdot 343 \equiv 83 \pmod{100}$. Tehát 83-ra végződik.

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} =$$

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16$$

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16$$

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik.

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik. C

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik. Csakhogy ez

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik. Csakhogy ez

elégtelen (1)

azaz [redacted]

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik. Csakhogy ez

elégtelen (1)

azaz **rossz megoldás**!

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik. Csakhogy ez

elégtelen (1)

azaz **rossz megoldás**! Hiszen

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik. Csakhogy ez

elégtelen (1)

azaz **rossz megoldás**! Hiszen ln.k.o.$(16, 100) \neq 1$ miatt az Euler-tétel nem alkalmazható!

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét!

Megoldás Mivel $\varphi(100) = 40$, ezért

$$16^{401} = (16^{40})^{10} \cdot 16 \equiv 1^{10} \cdot 16 \equiv 16 \pmod{100}.$$

Tehát a 16^{401} szám **16**-ra végződik. Csakhogy ez

elégtelen (1)

azaz **rossz megoldás**! Hiszen $\text{ln.k.o.}(16, 100) \neq 1$ miatt az Euler-tétel nem alkalmazható! Pl. ugyanezzel az erővel (az Euler-tételt hibásan alkalmazva) azt is mondhatnánk, hogy

$$16^{400} = (16^{40})^{10} \equiv 1^{10} = 1 \pmod{100}$$

miatt a 16^{400} szám 01-re végződik, ami

$$16^{400} = (16^{40})^{10} \equiv 1^{10} = 1 \pmod{100}$$

miatt a 16^{400} szám 01-re végződik, ami — páros számról lévén szó — **hibás kijelentés**.

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Megoldás: Mivel $a \equiv b \pmod{100}$ azzal ekvivalens, hogy $a \equiv b \pmod{25}$ és $a \equiv b \pmod{4}$ (

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Megoldás: Mivel $a \equiv b \pmod{100}$ azzal ekvivalens, hogy $a \equiv b \pmod{25}$ és $a \equiv b \pmod{4}$ (hiszen $100 \mid a-b \iff 25 \mid a-b$ és $4 \mid a-b$), ezért célszerű a kérdést külön kezelni modulo 25 és modulo 4.

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Megoldás: Mivel $a \equiv b \pmod{100}$ azzal ekvivalens, hogy $a \equiv b \pmod{25}$ és $a \equiv b \pmod{4}$ (hiszen $100 \mid a-b \iff 25 \mid a-b$ és $4 \mid a-b$), ezért célszerű a kérdést külön kezelni modulo 25 és modulo 4.

Mivel $\text{ln.k.o.}(16, 25) = 1$ és

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Megoldás: Mivel $a \equiv b \pmod{100}$ azzal ekvivalens, hogy $a \equiv b \pmod{25}$ és $a \equiv b \pmod{4}$ (hiszen $100 \mid a-b \iff 25 \mid a-b$ és $4 \mid a-b$), ezért célszerű a kérdést külön kezelni modulo 25 és modulo 4.

Mivel $\text{ln.k.o.}(16, 25) = 1$ és $\varphi(25) = 20$,

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Megoldás: Mivel $a \equiv b \pmod{100}$ azzal ekvivalens, hogy $a \equiv b \pmod{25}$ és $a \equiv b \pmod{4}$ (hiszen $100 \mid a - b \iff 25 \mid a - b$ és $4 \mid a - b$), ezért célszerű a kérdést külön kezelni modulo 25 és modulo 4.

Mivel ln.k.o.$(16, 25) = 1$ és $\varphi(25) = 20$, az Euler-tétel szerint

$$x \equiv 16^{401} =$$

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Megoldás: Mivel $a \equiv b \pmod{100}$ azzal ekvivalens, hogy $a \equiv b \pmod{25}$ és $a \equiv b \pmod{4}$ (hiszen $100 \mid a-b \iff 25 \mid a-b$ és $4 \mid a-b$), ezért célszerű a kérdést külön kezelni modulo 25 és modulo 4.

Mivel ln.k.o.$(16, 25) = 1$ és $\varphi(25) = 20$, az Euler-tétel szerint

$$x \equiv 16^{401} = (16^{20})^{20} \cdot 16 \equiv$$

Feladat: Határozzuk meg a 16^{401} utolsó két számjegyét (de most már jól)!

Megoldás: Mivel $a \equiv b \pmod{100}$ azzal ekvivalens, hogy $a \equiv b \pmod{25}$ és $a \equiv b \pmod 4$ (hiszen $100 \mid a - b \iff 25 \mid a - b$ és $4 \mid a - b$), ezért célszerű a kérdést külön kezelni modulo 25 és modulo 4.

Mivel ln.k.o.$(16, 25) = 1$ és $\varphi(25) = 20$, az Euler-tétel szerint

$$x \equiv 16^{401} = (16^{20})^{20} \cdot 16 \equiv 1^{20} \cdot 16 = 16 \pmod{25}.$$

Másrészt nyilván

$$x \equiv 16^{401} \equiv 0^{401} \equiv 0 \equiv 16 \pmod 4.$$

A kapott két kongruenciából $16^{401} \equiv 16 \pmod{100}$, A kapott két kongruenciából $16^{401} \equiv 16 \pmod{100}$, tehát a 16^{401} szám **16-ra végződik**.

Most is ugyanaz jött ki, mint az előbb, de ez nem mentség az előző rossz megoldásra!

Gráfok

Gráfok

A matematikában a **gráfokat** többféleképpen is szokás definiálni, és többféle struktúrát is lehet gráfnak nevezni.

Gráfok

A matematikában a **gráfokat** többféleképpen is szokás definiálni, és többféle struktúrát is lehet gráfnak nevezni. (A későbbiekben — egyéb kitétel híján — vagy mindegy vagy pedig értelemszerű, hogy melyikről lesz szó.)

Definíció (Többszörös élek nélküli) **irányított gráfon** egy $(V; \rho)$ párt értünk, ahol V nemüres halmaz (

Gráfok

A matematikában a **gráfokat** többféleképpen is szokás definiálni, és többféle struktúrát is lehet gráfnak nevezni. (A későbbiekben — egyéb kitétel híján — vagy mindegy vagy pedig értelemszerű, hogy melyikről lesz szó.)

Definíció (Többszörös élek nélküli) **irányított gráfon** egy $(V;\rho)$ párt értünk, ahol V nemüres halmaz (a szögpontok halmaza, „vertex set"), $\rho \subseteq V^2$ pedig tetszőleges reláció (

Gráfok

A matematikában a **gráfokat** többféleképpen is szokás definiálni, és többféle struktúrát is lehet gráfnak nevezni. (A későbbiekben — egyéb kitétel híján — vagy mindegy vagy pedig értelemszerű, hogy melyikről lesz szó.)

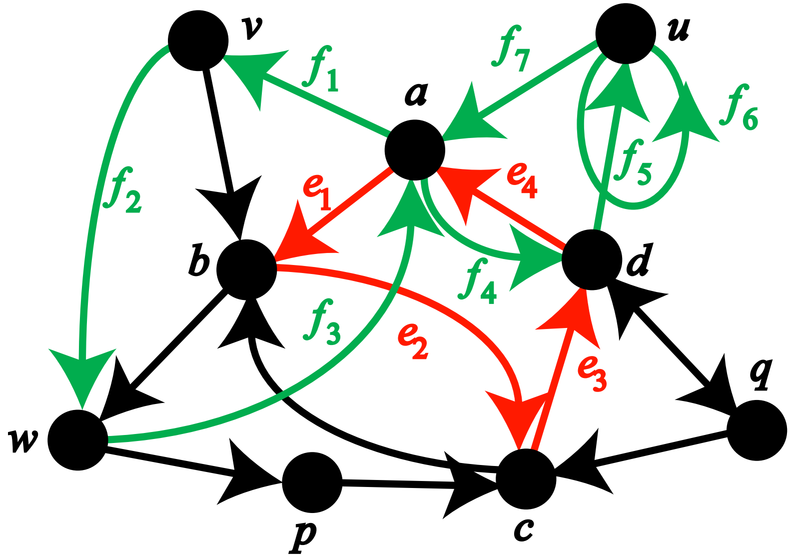
Definíció (Többszörös élek nélküli) **irányított gráfon** egy $(V; \rho)$ párt értünk, ahol V nemüres halmaz (a szögpontok halmaza, „vertex set"), $\rho \subseteq V^2$ pedig tetszőleges reláció (az élek halmaza).

Gráfok

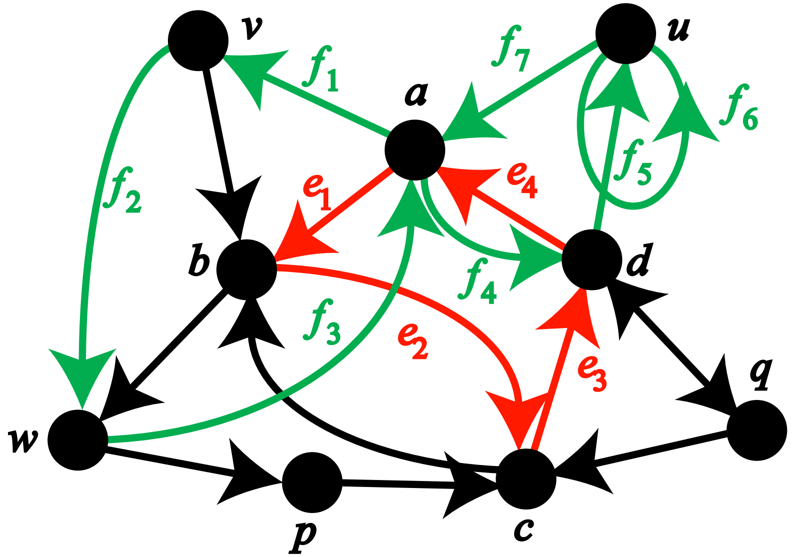
A matematikában a **gráfokat** többféleképpen is szokás definiálni, és többféle struktúrát is lehet gráfnak nevezni. (A későbbiekben — egyéb kitétel híján — vagy mindegy vagy pedig értelemszerű, hogy melyikről lesz szó.)

Definíció (Többszörös élek nélküli) **irányított gráfon** egy $(V;\rho)$ párt értünk, ahol V nemüres halmaz (a szögpontok halmaza, „vertex set"), $\rho \subseteq V^2$ pedig tetszőleges reláció (az élek halmaza).

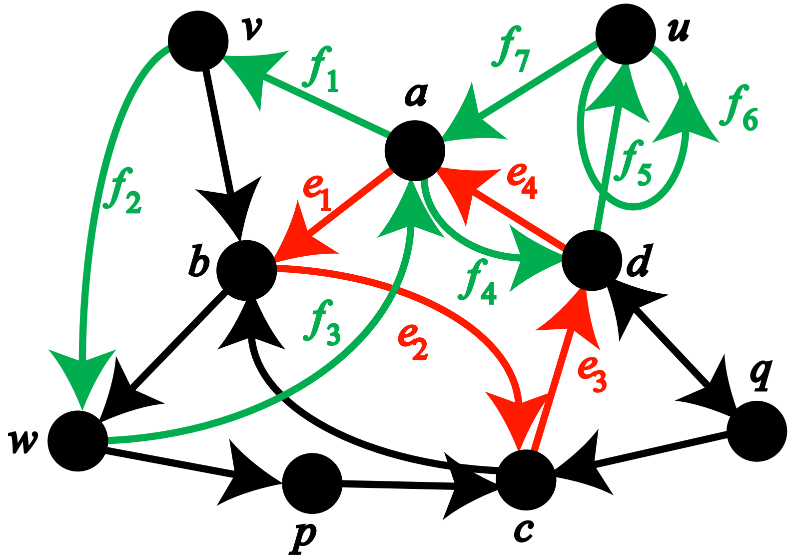
Ha $(a,b) \in \rho$, akkor az ábrán az a szögpontból egy irányított nyilat rajzolunk a b szögpontba:



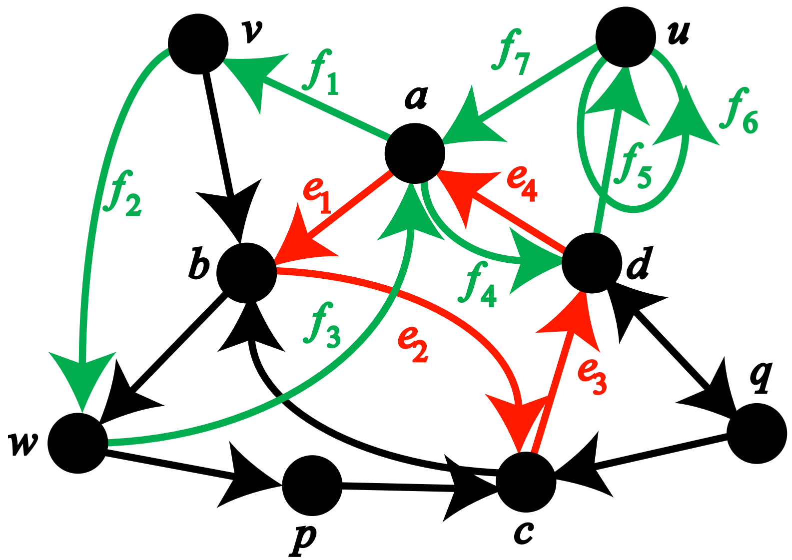
Az ábrán pl. a zöld $f_6 \in \rho$ **hurokél** az $(u, u) \in \rho$-nak felel meg.



Az ábrán pl. a zöld $f_6 \in \rho$ **hurokél** az $(u, u) \in \rho$-nak felel meg. Ha (x, y) is és (y, x) is eleme ρ-nak, akkor ezt jelölhetjük két ellentétesen irányított nyíllal is (



Az ábrán pl. a zöld $f_6 \in \rho$ **hurokél** az $(u, u) \in \rho$-nak felel meg. Ha (x, y) is és (y, x) is eleme ρ-nak, akkor ezt jelölhetjük két ellentétesen irányított nyíllal is (pl. a b és c szögpontok esetén), de



Az ábrán pl. a zöld $f_6 \in \rho$ **hurokél** az $(u, u) \in \rho$-nak felel meg. Ha (x, y) is és (y, x) is eleme ρ-nak, akkor ezt jelölhetjük két ellentétesen irányított nyíllal is (pl. a b és c szögpontok esetén), de választhatjuk a mindkét irányban irányított nyilat is (pl. d és q között).

Egy irányított gráfban **irányított sétának nevezünk** egy $g_1, g_2, \ldots, g_n$ élsorozatot, ha minden értelmes i-re a g_{i-1} végpontja azonos a g_i kezdőpontjával.

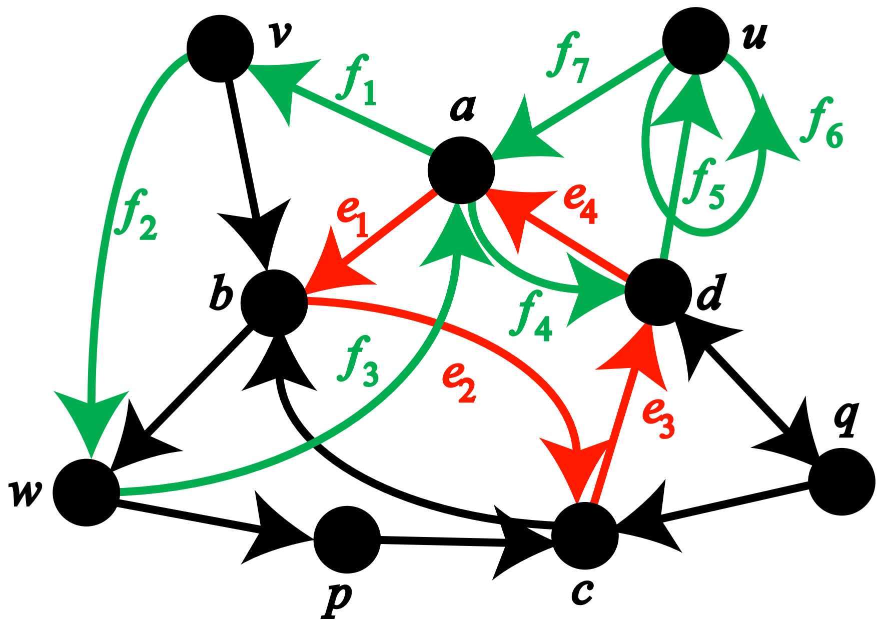
Egy irányított gráfban **irányított sétának nevezünk** egy $g_1, g_2, \ldots, g_n$ élsorozatot, ha minden értelmes i-re a g_{i-1} végpontja azonos a g_i kezdőpontjával. Az irányított séta tehát csatlakozó élek sorozata.

Egy irányított gráfban **irányított sétának nevezünk** egy $g_1, g_2, \ldots, g_n$ élsorozatot, ha minden értelmes i-re a g_{i-1} végpontja azonos a g_i kezdőpontjával. Az irányított séta tehát csatlakozó élek sorozata. Ha az első él kezdőpontja azonos az utolsó él végpontjával, akkor **zárt irányított sétáról**, egyébként pedig **nyitott irányított sétáról** beszélünk.

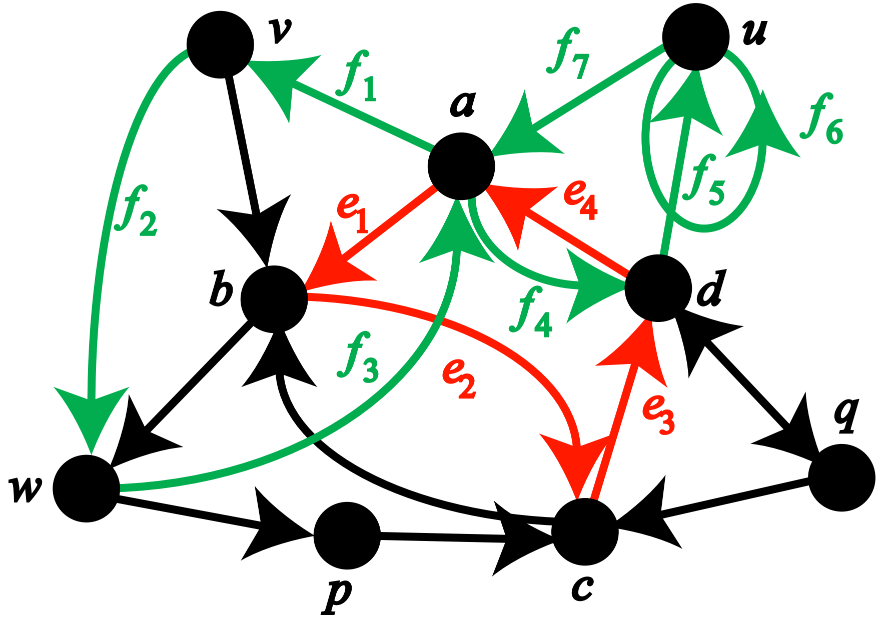
Egy irányított gráfban **irányított sétának nevezünk** egy $g_1, g_2, \ldots, g_n$ élsorozatot, ha minden értelmes i-re a g_{i-1} végpontja azonos a g_i kezdőpontjával. Az irányított séta tehát csatlakozó élek sorozata. Ha az első él kezdőpontja azonos az utolsó él végpontjával, akkor **zárt irányított sétáról**, egyébként pedig **nyitott irányított sétáról** beszélünk. Például a zöld élek egy

$$f_1, f_2, \ldots, f_5, f_6, f_7$$

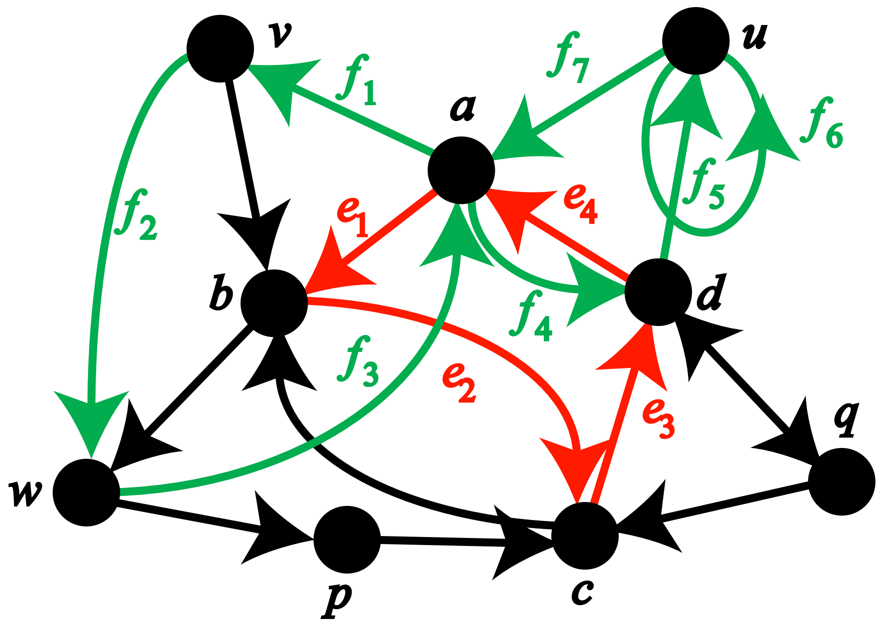
zárt sétát alkotnak.



Természetesen egy séta a **meglátogatott szögpontok** felsorolásával is megadható,

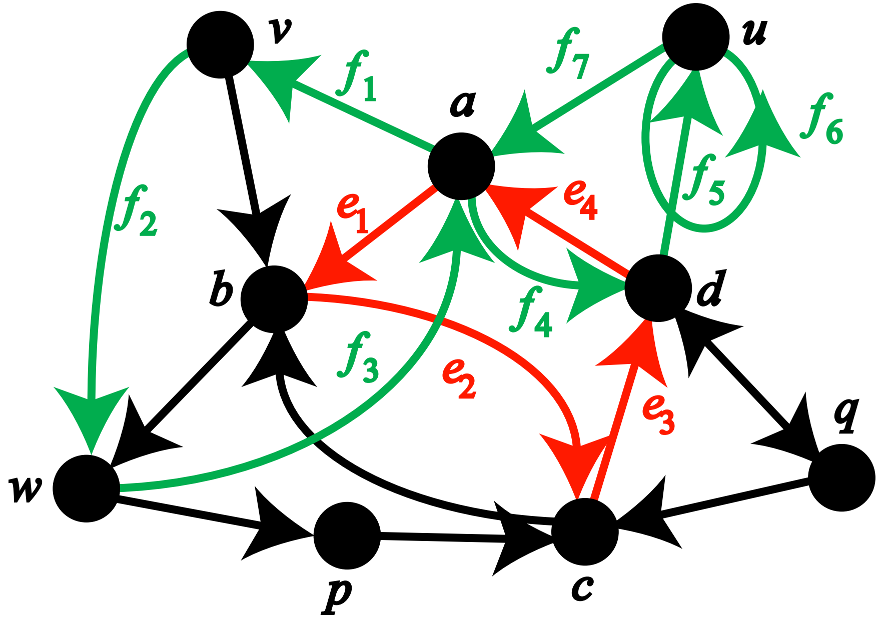


Természetesen egy séta a **meglátogatott szögpontok** felsorolásával is megadható, sőt még azt is megtehetjük, hogy az éleket és szögpontokat együtt soroljuk fel.



Természetesen egy séta a **meglátogatott szögpontok** felsorolásával is megadható, sőt még azt is megtehetjük, hogy az éleket és szögpontokat együtt soroljuk fel. Esetünkben így:

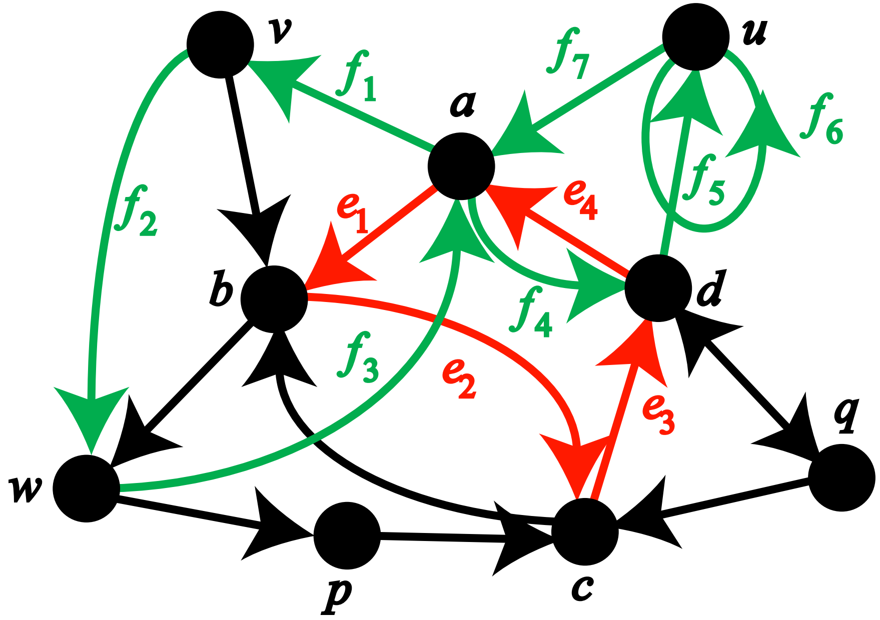
a, v, w, a, d, u, u, a , vagy így:



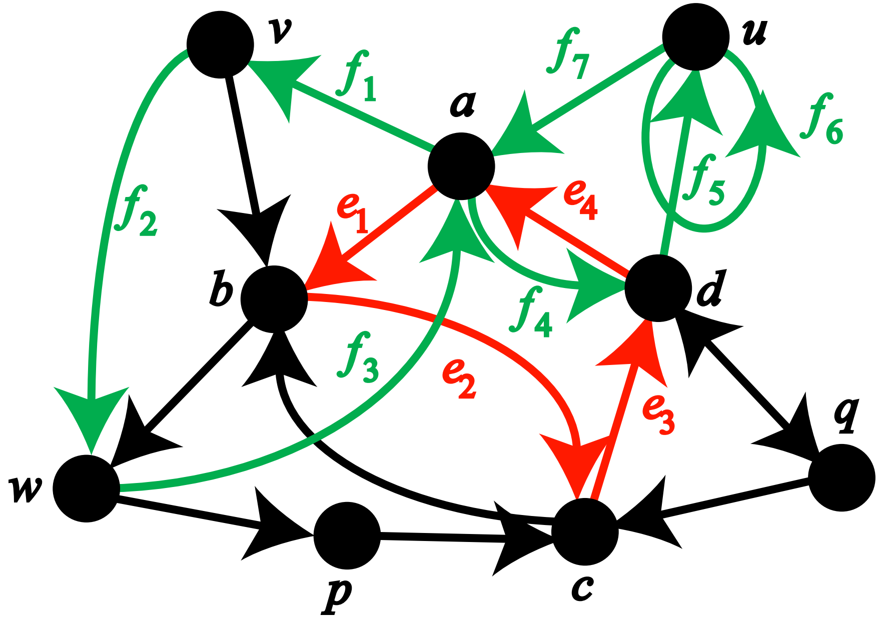
Természetesen egy séta a **meglátogatott szögpontok** felsorolásával is megadható, sőt még azt is megtehetjük, hogy az éleket és szögpontokat együtt soroljuk fel. Esetünkben így:

$$a, v, w, a, d, u, u, a \quad , \qquad \text{vagy így:}$$

$$a, f_1, v, f_2, w, f_3, a, f_4, d, f_5, u, f_6, u, f_7, a.$$



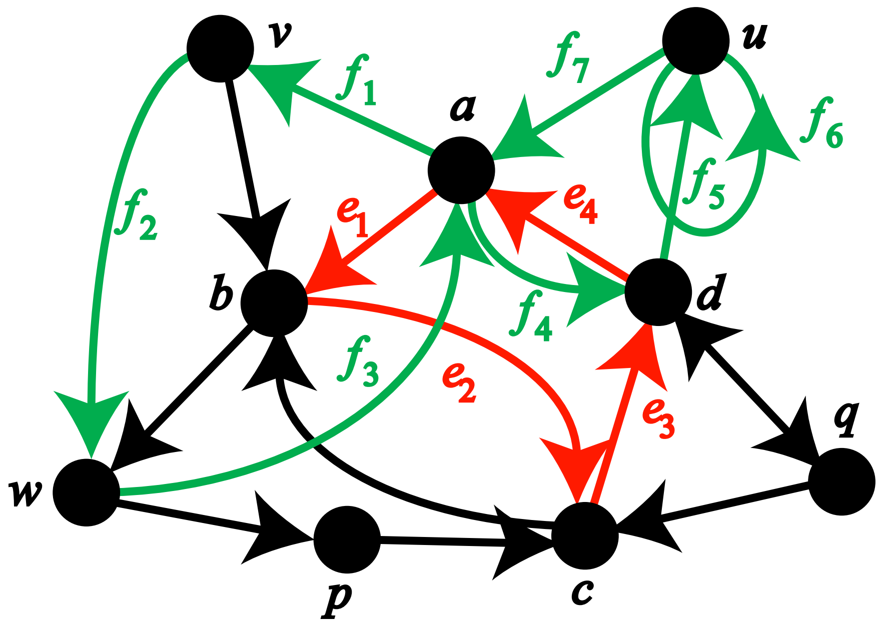
Az irányított séta **hossza** a felsorolt élek száma (a többször fellépő éleket többször számolva),



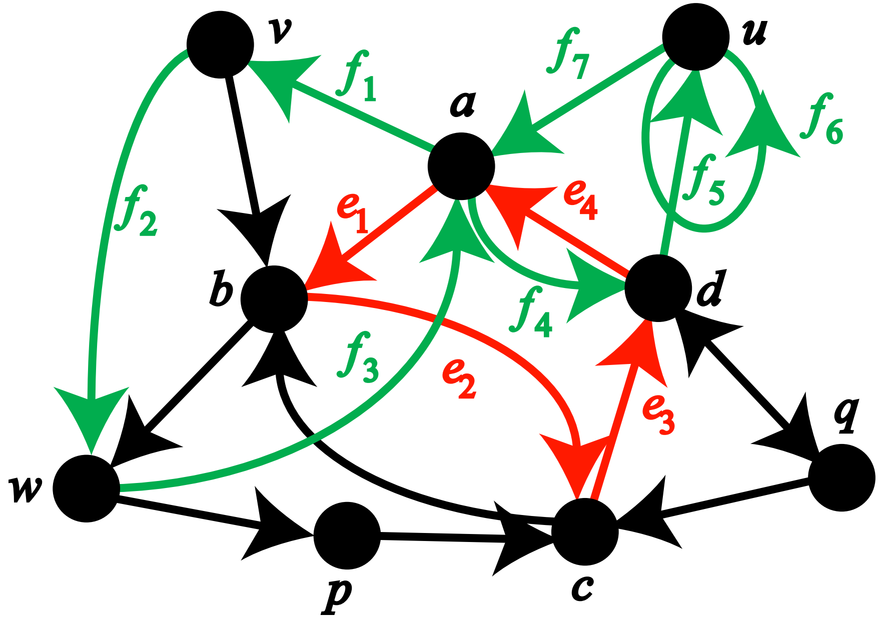
Az irányított séta **hossza** a felsorolt élek száma (a többször fellépő éleket többször számolva), Pl. az előbbi "zöld" séta hossza 7.

Ha — a kezdő- és végpont esetleges megegyezését leszámítva — az irányított séta által meglátogatott szögpontok **páronként különböznek**, Ha — a kezdő- és végpont esetleges megegyezését leszámítva — az irányított séta által meglátogatott szögpontok **páronként különböznek**, akkor (logikusan!) a sétát **irányított útnak** nevezzük.

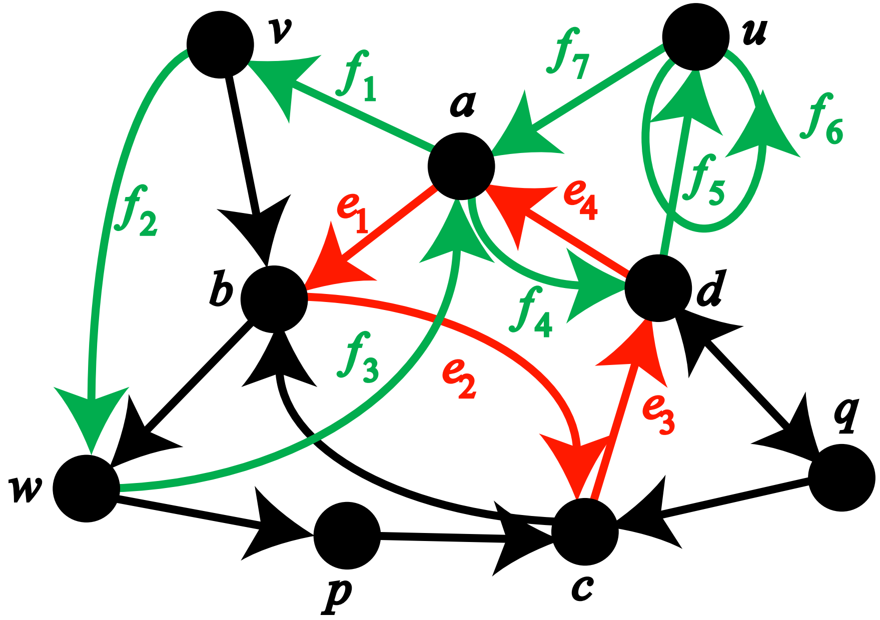
Ha — a kezdő- és végpont esetleges megegyezését leszámítva — az irányított séta által meglátogatott szögpontok **páronként különböznek**, akkor (logikusan!) a sétát **irányított útnak** nevezzük. A zárt, legalább 2 hosszúságú irányított út neve **irányított kör**.



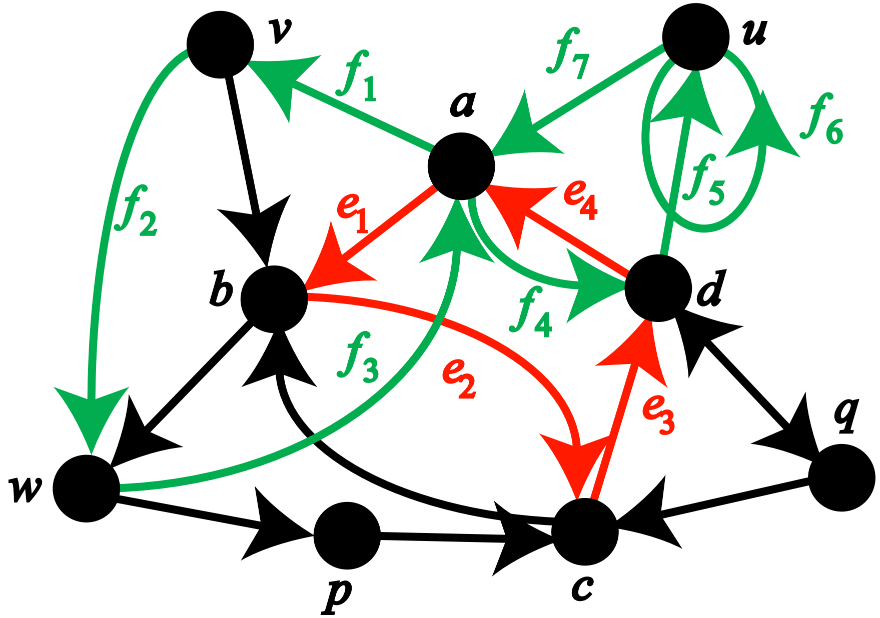
v
u
a
b
d
w
p
c
q
f1
f2
f3
f4
f5
f6
f7
e1
e2
e3
e4



Például a, b, c (vagy más jelöléssel e_1, e_2, megint más jelöléssel a, e_1, b, e_2, c)



Például a, b, c (vagy más jelöléssel e_1, e_2, megint más jelöléssel a, e_1, b, e_2, c) egy kettő hosszúságú irányított út,



Például a, b, c (vagy más jelöléssel e_1, e_2, megint más jelöléssel a, e_1, b, e_2, c) egy kettő hosszúságú irányított út, a, b, c, d, a pedig egy négy hosszúságú irányított kör. Csupán irányított 6 hosszúságú zárt séta de nem kör a következő: a, d, u, a, d, u, a.

Tehát az út (és a kör)

Tehát az út (és a kör) „céltudatos” közlekedés a gráfban, amikor fölöslegesen nem megyünk egy szögpontba kétszer (

Tehát az út (és a kör) „céltudatos” közlekedés a gráfban, amikor fölöslegesen nem megyünk egy szögpontba kétszer (kivéve kör esetén a kezdő- és végpont megegyezését).

Tehát az út (és a kör) „céltudatos” közlekedés a gráfban, amikor fölöslegesen nem megyünk egy szögpontba kétszer (kivéve kör esetén a kezdő- és végpont megegyezését).

Ezzel szemben a

Tehát az út (és a kör) „céltudatos” közlekedés a gráfban, amikor fölöslegesen nem megyünk egy szögpontba kétszer (kivéve kör esetén a kezdő- és végpont megegyezését).

Ezzel szemben a séta „céltalan csámborgás”, nélkülözi a fenti céltudatosságot.

Definíció **(Többszörös élek nélküli, irányítás nélküli)** gráfon egy (V, ρ) párt értünk, ahol V nemüres halmaz (

Tehát az út (és a kör) „céltudatos” közlekedés a gráfban, amikor fölöslegesen nem megyünk egy szögpontba kétszer (kivéve kör esetén a kezdő- és végpont megegyezését).

Ezzel szemben a séta „céltalan csámborgás”, nélkülözi a fenti céltudatosságot.

Definíció **(Többszörös élek nélküli, irányítás nélküli)** gráfon egy (V, ρ) párt értünk, ahol V nemüres halmaz (a szögpontok halmaza), $\rho \subseteq V^2$ pedig tetszőleges **szimmetrikus** reláció (

Tehát az út (és a kör) „céltudatos” közlekedés a gráfban, amikor fölöslegesen nem megyünk egy szögpontba kétszer (kivéve kör esetén a kezdő- és végpont megegyezését).

Ezzel szemben a séta „céltalan csámborgás”, nélkülözi a fenti céltudatosságot.

Definíció **(Többszörös élek nélküli, irányítás nélküli)** gráfon egy (V, ρ) párt értünk, ahol V nemüres halmaz (a szögpontok halmaza), $\rho \subseteq V^2$ pedig tetszőleges **szimmetrikus** reláció (az élek halmaza).

Tehát az út (és a kör) „céltudatos” közlekedés a gráfban, amikor fölöslegesen nem megyünk egy szögpontba kétszer (kivéve kör esetén a kezdő- és végpont megegyezését).

Ezzel szemben a séta „céltalan csámborgás”, nélkülözi a fenti céltudatosságot.

Definíció **(Többszörös élek nélküli, irányítás nélküli)** gráfon egy (V, ρ) párt értünk, ahol V nemüres halmaz (a szögpontok halmaza), $\rho \subseteq V^2$ pedig tetszőleges **szimmetrikus** reláció (az élek halmaza).

Természtesen irányítatlan gráf ábráján nem nyilakat, csak éleket rajzolunk. Ha $(v, v) \in \rho$, akkor ennek egy hurokél felel meg.

Definíció: Azokat az — irányított vagy irányítatlan — gráfokat, amelyekben **sem hurokélek, sem többszörös élek** nincsenek,

Definíció: Azokat az — irányított vagy irányítatlan — gráfokat, amelyekben **sem hurokélek, sem többszörös élek** nincsenek, **egyszerű gráfoknak** nevezzük.

Megjegyzés: Ha nem mondjuk meg, hogy irányított-e egy gráf vagy sem, akkor

Definíció: Azokat az — irányított vagy irányítatlan — gráfokat, amelyekben **sem hurokélek, sem többszörös élek** nincsenek, **egyszerű gráfoknak** nevezzük.

Megjegyzés: Ha nem mondjuk meg, hogy irányított-e egy gráf vagy sem, akkor alapértelmezés szerint irányítás **nélküli** gráfra gondolunk.

Az irányítatlan egyszerű gráfokat másként is szokás definiálni. Jelölje

Az irányítatlan egyszerű gráfokat másként is szokás definiálni. Jelölje $P_2(V)$ a V kételemű részhalmazainak halmazát.

Az irányítatlan egyszerű gráfokat másként is szokás definiálni. Jelölje $P_2(V)$ a V kételemű részhalmazainak halmazát.

Definíció **Egyszerű irányítatlan** gráfon egy (V, E) párt értünk, ahol V nemüres halmaz,

Az irányítatlan egyszerű gráfokat másként is szokás definiálni. Jelölje $P_2(V)$ a V kételemű részhalmazainak halmazát.

Definíció **Egyszerű irányítatlan** gráfon egy (V, E) párt értünk, ahol V nemüres halmaz, E (

Az irányítatlan egyszerű gráfokat másként is szokás definiálni. Jelölje $P_2(V)$ a V kételemű részhalmazainak halmazát.

Definíció **Egyszerű irányítatlan** gráfon egy (V, E) párt értünk, ahol V nemüres halmaz, E (az élek halmaza,

Az irányítatlan egyszerű gráfokat másként is szokás definiálni. Jelölje $P_2(V)$ a V kételemű részhalmazainak halmazát.

Definíció **Egyszerű irányítatlan** gráfon egy (V, E) párt értünk, ahol V nemüres halmaz, E (az élek halmaza, „edge set") pedig tetszőleges részhalmaza $P_2(V)$-nek. (

Az irányítatlan egyszerű gráfokat másként is szokás definiálni. Jelölje $P_2(V)$ a V kételemű részhalmazainak halmazát.

Definíció **Egyszerű irányítatlan** gráfon egy (V, E) párt értünk, ahol V nemüres halmaz, E (az élek halmaza, „edge set”) pedig tetszőleges részhalmaza $P_2(V)$-nek. (Ebben a felfogásban az élt a két végpontjából álló halmazzal azonosítjuk — halmaz esetén a két végpont sorrendje nem számít.)

A (nyitott vagy zárt) séta, az út és a kör fogalma irányítatlan gráfok esetén is ugyanúgy definiálható, mint irányított gráfok esetében.

A (nyitott vagy zárt) séta, az út és a kör fogalma irányítatlan gráfok esetén is ugyanúgy definiálható, mint irányított gráfok esetében.

Ha a **többszörös éleket** sem akarjuk kizárni, akkor a gráfok általánosabb definíciójához folyamodunk:

A (nyitott vagy zárt) séta, az út és a kör fogalma irányítatlan gráfok esetén is ugyanúgy definiálható, mint irányított gráfok esetében.

Ha a **többszörös éleket** sem akarjuk kizárni, akkor a gráfok általánosabb definíciójához folyamodunk:

Definíció: Irányított gráfon egy (V, E, ι) rendezett hármast értünk, ahol

A (nyitott vagy zárt) séta, az út és a kör fogalma irányítatlan gráfok esetén is ugyanúgy definiálható, mint irányított gráfok esetében.

Ha a **többszörös éleket** sem akarjuk kizárni, akkor a gráfok általánosabb definíciójához folyamodunk:

Definíció: Irányított gráfon egy (V, E, ι) rendezett hármast értünk, ahol V tetszőleges nemüres halmaz (a szögpontok halmaza), E tetszőleges halmaz (az élek halmaza), ι

A (nyitott vagy zárt) séta, az út és a kör fogalma irányítatlan gráfok esetén is ugyanúgy definiálható, mint irányított gráfok esetében.

Ha a **többszörös éleket** sem akarjuk kizárni, akkor a gráfok általánosabb definíciójához folyamodunk:

Definíció: Irányított gráfon egy (V, E, ι) rendezett hármast értünk, ahol V tetszőleges nemüres halmaz (a szögpontok halmaza), E tetszőleges halmaz (az élek halmaza), ι (görög ióta) pedig tetszőleges $E \to V \times V$ leképezés. (

A (nyitott vagy zárt) séta, az út és a kör fogalma irányítatlan gráfok esetén is ugyanúgy definiálható, mint irányított gráfok esetében.

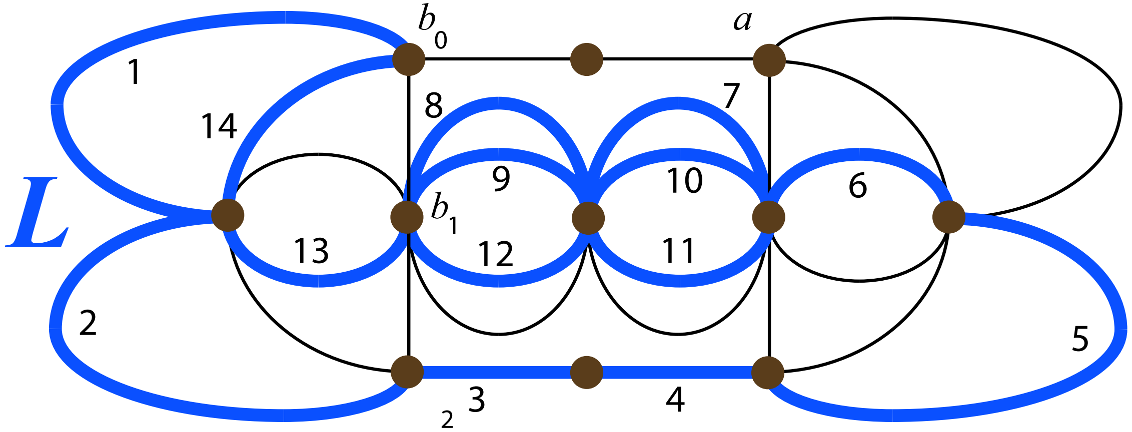
Ha a **többszörös éleket** sem akarjuk kizárni, akkor a gráfok általánosabb definíciójához folyamodunk:

Definíció: Irányított gráfon egy (V, E, ι) rendezett hármast értünk, ahol V tetszőleges nemüres halmaz (a szögpontok halmaza), E tetszőleges halmaz (az élek halmaza), ι (görög ióta) pedig tetszőleges $E \to V \times V$ leképezés. (ι „mondja meg”, hogy egy élnek mi a kezdő- és végpontja.)

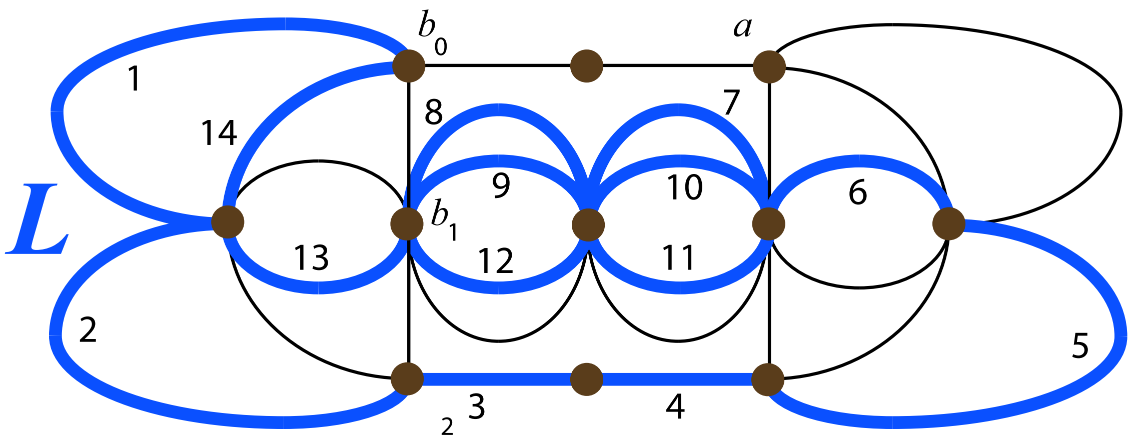
Definíció: Irányítatlan gráfon egy (V, E, ι) rendezett hármast értünk, ahol

Definíció: Irányítatlan gráfon egy (V, E, ι) rendezett hármast értünk, ahol V tetszőleges nemüres halmaz (a szögpontok halmaza), E tetszőleges halmaz (az élek halmaza), ι pedig tetszőleges $E \to P_2(V)$ leképezés.

Definíció: Irányítatlan gráfon egy (V, E, ι) rendezett hármast értünk, ahol V tetszőleges nemüres halmaz (a szögpontok halmaza), E tetszőleges halmaz (az élek halmaza), ι pedig tetszőleges $E \to P_2(V)$ leképezés.



Definíció: Irányítatlan gráfon egy (V, E, ι) rendezett hármast értünk, ahol V tetszőleges nemüres halmaz (a szögpontok halmaza), E tetszőleges halmaz (az élek halmaza), ι pedig tetszőleges $E \to P_2(V)$ leképezés.



Itt egy példa, és benne egy 14 hosszúságú zárt séta (a vastag kék élek).

Ha mindenféle precizitást nélkülözve, laikus szinten akarnánk a gráf fogalmát meghatározni, akkor azt is mondhatnánk, hogy a gráf egy gumilepedőre rajzolt, csomópontokból és bizonyos csomópontok közötti vonalakból álló alakzat; de két ilyen alakzatot nem különböztetünk meg, ha csak a lepedő elmozgatása és ilyen-olyan (helytől függő de szakadást nem okozó) nyújtása különbözteti meg azokat.

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük,

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak ”mindkét vége” az adott szögpontból indul).

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak "mindkét vége" az adott szögpontból indul). Többszörös élek is megengedettek.

33. Tétel. Véges gráf esetén a szögpontok fokainak összege éppen az élek számának kétszerese.

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak "mindkét vége" az adott szögpontból indul). Többszörös élek is megengedettek.

33. Tétel. **Véges gráf esetén a szögpontok fokainak összege éppen az élek számának kétszerese.**

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak ”mindkét vége” az adott szögpontból indul). Többszörös élek is megengedettek.

33. Tétel. Véges gráf esetén a szögpontok fokainak összege éppen az élek számának kétszerese.

Bizonyítás:

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak ”mindkét vége” az adott szögpontból indul). Többszörös élek is megengedettek.

33. Tétel. **Véges gráf esetén a szögpontok fokainak összege éppen az élek számának kétszerese.**

Bizonyítás: Minden él kettővel járul hozzá a mondott összeghez: a hurokélnél

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak "mindkét vége" az adott szögpontból indul). Többszörös élek is megengedettek.

33. Tétel. **Véges gráf esetén a szögpontok fokainak összege éppen az élek számának kétszerese.**

Bizonyítás: Minden él kettővel járul hozzá a mondott összeghez: a hurokélnél így állapodtunk meg, a többi él pedig eleve két szögpontból indul.

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak ”mindkét vége” az adott szögpontból indul). Többszörös élek is megengedettek.

33. Tétel. **Véges gráf esetén a szögpontok fokainak összege éppen az élek számának kétszerese.**

Bizonyítás: Minden él kettővel járul hozzá a mondott összeghez: a hurokélnél így állapodtunk meg, a többi él pedig eleve két szögpontból indul. Q.e.d.

Definíció: Egy **szögpont fokán** a pontból induló élek számát értjük, a hurokéleket duplán számolva (hiszen azoknak "mindkét vége" az adott szögpontból indul). Többszörös élek is megengedettek.

33. Tétel. Véges gráf esetén a szögpontok fokainak összege éppen az élek számának kétszerese.

Bizonyítás: Minden él kettővel járul hozzá a mondott összeghez: a hurokélnél így állapodtunk meg, a többi él pedig eleve két szögpontból indul. Q.e.d.

Teljesen hasonló az alábbi is.

Definíció: Irányított gráf esetén egy szögpont **kifoka** a szögpontból induló élek száma, **befoka** pedig a szögpontba érkező élek száma. (Hurokél indul is és érkezik is.) Nyilván érvényes az alábbi, triviális tétel:

34. Tétel.

Definíció: Irányított gráf esetén egy szögpont **kifoka** a szögpontból induló élek száma, **befoka** pedig a szögpontba érkező élek száma. (Hurokél indul is és érkezik is.) Nyilván érvényes az alábbi, triviális tétel:

34. Tétel.

Véges irányított gráfok esetén a szögpontok kifokainak összege is és a szögpontok befokainak összege is egyenlő az élek számával.

Definíció: Irányított gráf esetén egy szögpont **kifoka** a szögpontból induló élek száma, **befoka** pedig a szögpontba érkező élek száma. (Hurokél indul is és érkezik is.) Nyilván érvényes az alábbi, triviális tétel:

34. Tétel.

Véges irányított gráfok esetén a szögpontok kifokainak összege is és a szögpontok befokainak összege is egyenlő az élek számával.

Definíció: Irányított gráf esetén egy szögpont **kifoka** a szögpontból induló élek száma, **befoka** pedig a szögpontba érkező élek száma. (Hurokél indul is és érkezik is.) Nyilván érvényes az alábbi, triviális tétel:

34. Tétel.

Véges irányított gráfok esetén a szögpontok kifokainak összege is és a szögpontok befokainak összege is egyenlő az élek számával.

Egy városban úgy célszerű az úthálózatot építeni (és egyes utakat egyirányúsítani), hogy bármely két

Definíció: Irányított gráf esetén egy szögpont **kifoka** a szögpontból induló élek száma, **befoka** pedig a szögpontba érkező élek száma. (Hurokél indul is és érkezik is.) Nyilván érvényes az alábbi, triviális tétel:

34. Tétel.

Véges irányított gráfok esetén a szögpontok kifokainak összege is és a szögpontok befokainak összege is egyenlő az élek számával.

Egy városban úgy célszerű az úthálózatot építeni (és egyes utakat egyirányúsítani), hogy bármely két utcasarok (azaz szögpont) esetén az egyikből el lehessen autóval jutni a másikba. Most az ennek megfelelő fogalmat tárgyaljuk gráfok esetén. Ebből a szempontból a többszörös éleknek nincs jelentősége.

Definíció: Akkor mondjuk hogy egy (irányítás nélküli) gráf **összefüggő**, ha bármely két szögpontja között vezet út. (A nulla hosszúságú utat is megengedjük.)

Definíció: Akkor mondjuk hogy egy (irányítás nélküli) gráf **összefüggő**, ha bármely két szögpontja között vezet út. (A nulla hosszúságú utat is megengedjük.)

Úgy is fogalmazhattunk volna, hogy bármely két szögpont esetén létezik olyan séta, amelyik az egyikből indul és a másikba érkezik (hiszen

Definíció: Akkor mondjuk hogy egy (irányítás nélküli) gráf **összefüggő**, ha bármely két szögpontja között vezet út. (A nulla hosszúságú utat is megengedjük.)

Úgy is fogalmazhattunk volna, hogy bármely két szögpont esetén létezik olyan séta, amelyik az egyikből indul és a másikba érkezik (hiszen a séta felesleges „vargabetűit” levágva utat kapunk.)

Definíció: Akkor mondjuk hogy egy irányított gráf **erősen összefüggő**, ha bármely a és b szögpontja esetén létezik irányított út a-ból b-be. (A 0 hosszúságú utat itt is megengedjük.)

Definíció: Akkor mondjuk hogy egy irányított gráf **erősen összefüggő**, ha bármely a és b szögpontja esetén létezik irányított út a-ból b-be. (A 0 hosszúságú utat itt is megengedjük.) Akkor mondjuk hogy egy irányított gráf **gyengén összefüggő**, ha az irányítás „elfelejtésével" keletkező gráf összefüggő.

Definíció: Akkor mondjuk hogy egy irányított gráf **erősen összefüggő**, ha bármely a és b szögpontja esetén létezik irányított út a-ból b-be. (A 0 hosszúságú utat itt is megengedjük.) Akkor mondjuk hogy egy irányított gráf **gyengén összefüggő**, ha az irányítás „elfelejtésével'' keletkező gráf összefüggő. (Az irányítás elfelejtésén azt értjük, hogy az élekről a nyilakat levesszük, azaz az „egyirányú utcákat kétirányúsítjuk''.)

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja,

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja, és másrészt H minden éle G-nek is éle.

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja, és másrészt H minden éle G-nek is éle. Ha emellett még az is igaz, hogy a H bármely a, b szögpontja és a G bármely e éle esetén

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja, és másrészt H minden éle G-nek is éle. Ha emellett még az is igaz, hogy a H bármely a, b szögpontja és a G bármely e éle esetén ha e az a és b szögpontokat köti össze, akkor e a H-nak is éle, akkor H-t a G **feszített részgráfjának** nevezzük.

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja, és másrészt H minden éle G-nek is éle. Ha emellett még az is igaz, hogy a H bármely a, b szögpontja és a G bármely e éle esetén ha e az a és b szögpontokat köti össze, akkor e a H-nak is éle, akkor H-t a G **feszített részgráfjának** nevezzük.

Például a $G =$ Magyarország gráfnak (

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja, és másrészt H minden éle G-nek is éle. Ha emellett még az is igaz, hogy a H bármely a, b szögpontja és a G bármely e éle esetén ha e az a és b szögpontokat köti össze, akkor e a H-nak is éle, akkor H-t a G **feszített részgráfjának** nevezzük.

Például a $G =$ Magyarország gráfnak (szögpontok a települések, élek az utak)

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja, és másrészt H minden éle G-nek is éle. Ha emellett még az is igaz, hogy a H bármely a, b szögpontja és a G bármely e éle esetén ha e az a és b szögpontokat köti össze, akkor e a H-nak is éle, akkor H-t a G **feszített részgráfjának** nevezzük.

Például a $G =$ Magyarország gráfnak (szögpontok a települések, élek az utak) feszített részgráfja a hasonló módon értelmezett H $=$ Csongrád megye gráf.

Definíció: Legyen H és G egy-egy gráf (a legáltalánosabb értelemben). Akkor mondjuk, hogy H **részgráfja** G-nek, ha egyrészt H minden szögpontja G-nek is szögpontja, és másrészt H minden éle G-nek is éle. Ha emellett még az is igaz, hogy a H bármely a, b szögpontja és a G bármely e éle esetén ha e az a és b szögpontokat köti össze, akkor e a H-nak is éle, akkor H-t a G **feszített részgráfjának** nevezzük.

Például a $G =$ Magyarország gráfnak (szögpontok a települések, élek az utak) feszített részgráfja a hasonló módon értelmezett H = Csongrád megye gráf. De ha Csongrád megye néhány útját elhagyjuk H-ból, akkor már csak részgráfja lesz G-nek.

35. Tétel. *Tetszőleges irányítatlan gráf páronként diszjunkt, összefüggő maximális feszített részgráfok egyesítése, és ez a felbontás egyértelmű.*

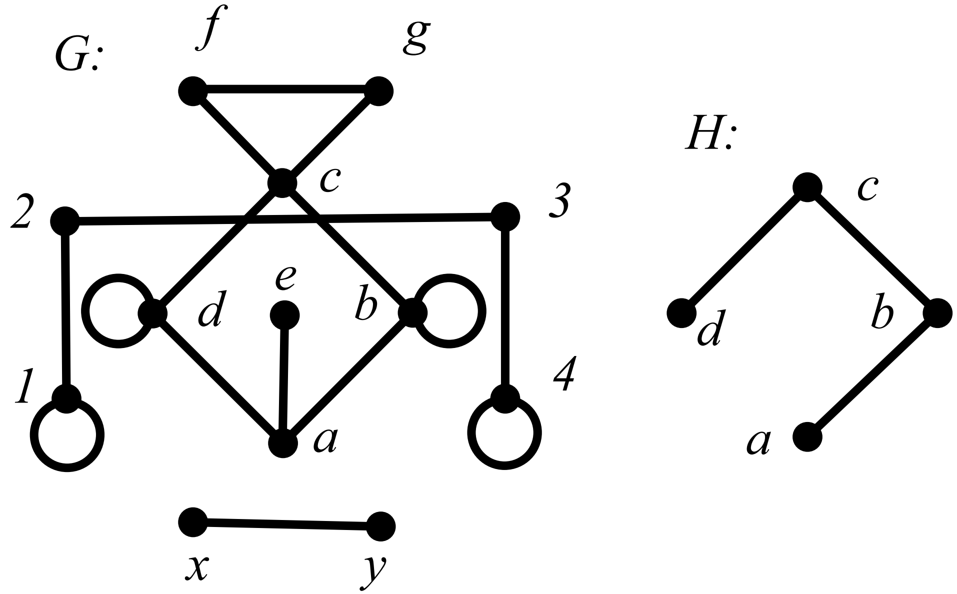
35. Tétel. *Tetszőleges irányítatlan gráf páronként diszjunkt, összefüggő maximális feszített részgráfok egyesítése, és ez a felbontás egyértelmű.*

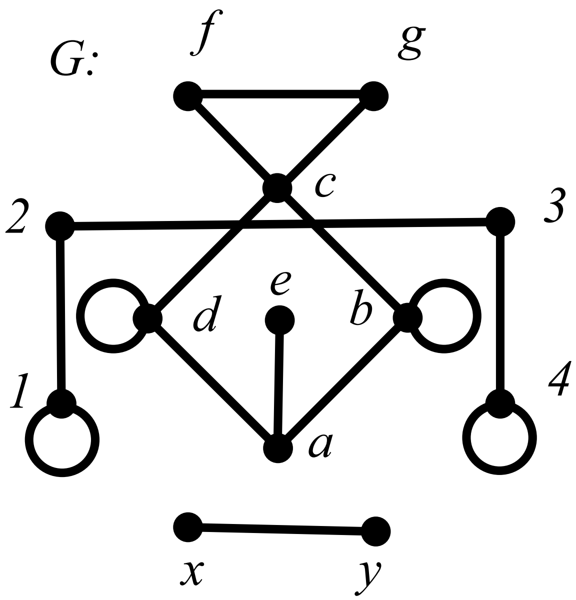
35. Tétel. *Tetszőleges irányítatlan gráf páronként diszjunkt, összefüggő maximális feszített részgráfok egyesítése, és ez a felbontás egyértelmű.*

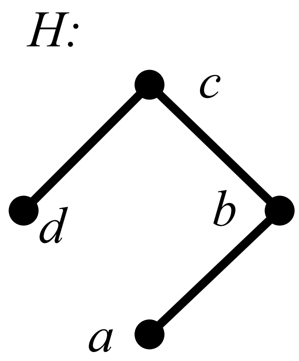
A tételben szereplő maximális feszített részgráfok

35. Tétel. *Tetszőleges irányítatlan gráf páronként diszjunkt, összefüggő maximális feszített részgráfok egyesítése, és ez a felbontás egyértelmű.*

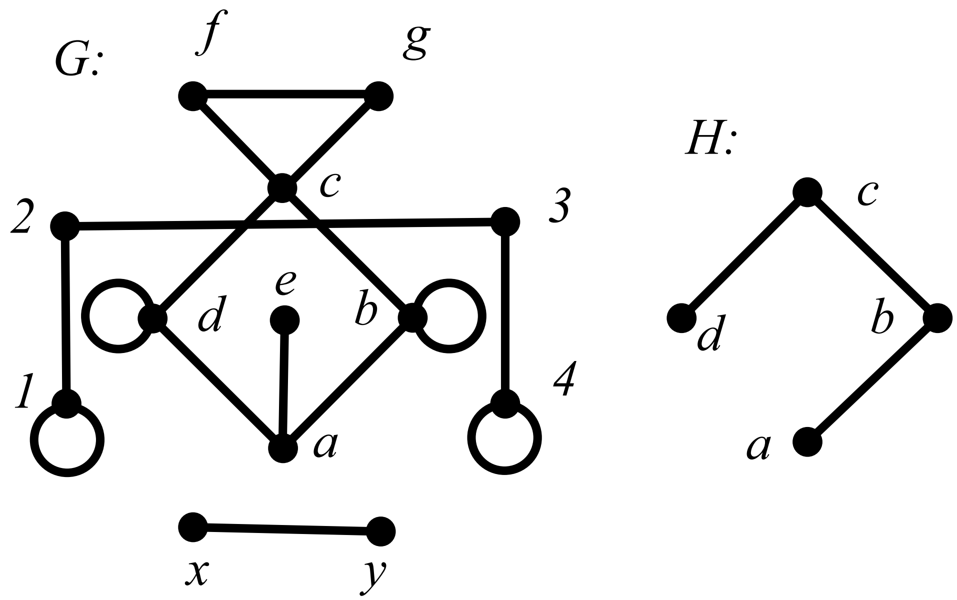
A tételben szereplő maximális feszített részgráfok az úgynevezett **összefüggő komponensek**.


G:
f
g
c
2
3
e
d
b
1
4
a
x
y
H:
c
d
b
a

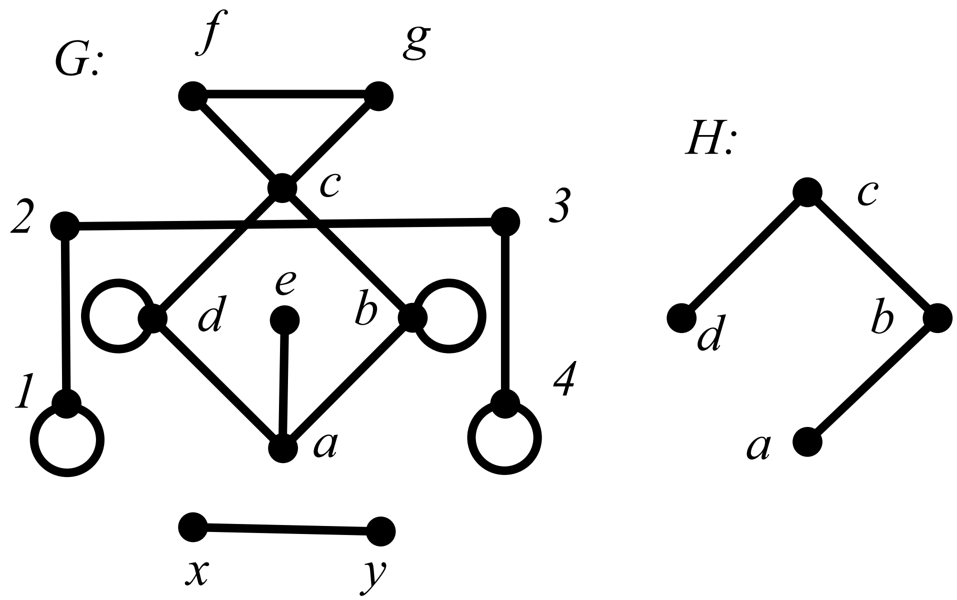




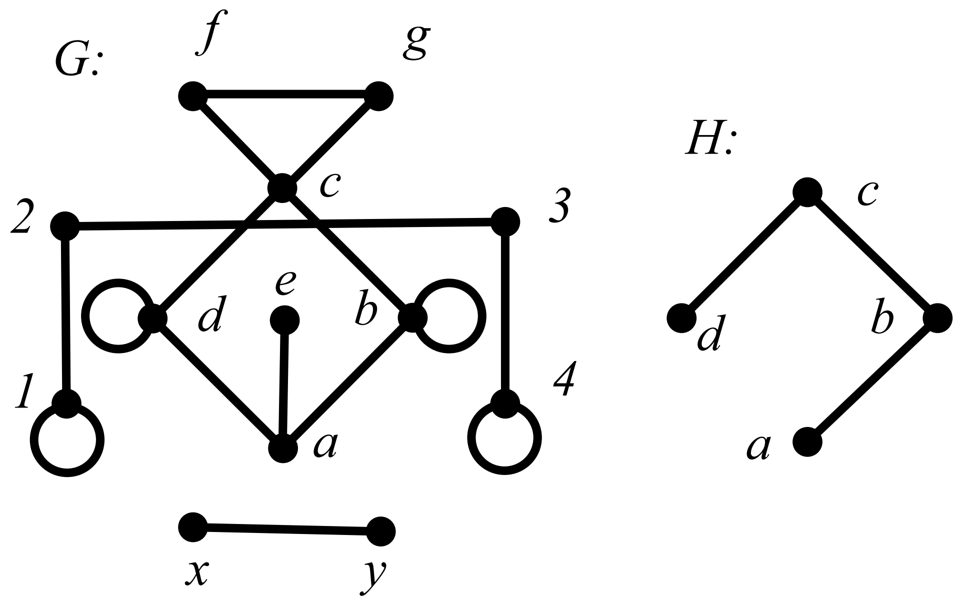
Például az ábrán az összefüggő komponensek:



Például az ábrán az összefüggő komponensek: $\{x, y\}$, $\{1, 2, 3, 4\}$ és $\{a, b, c, d, e, f, g\}$.



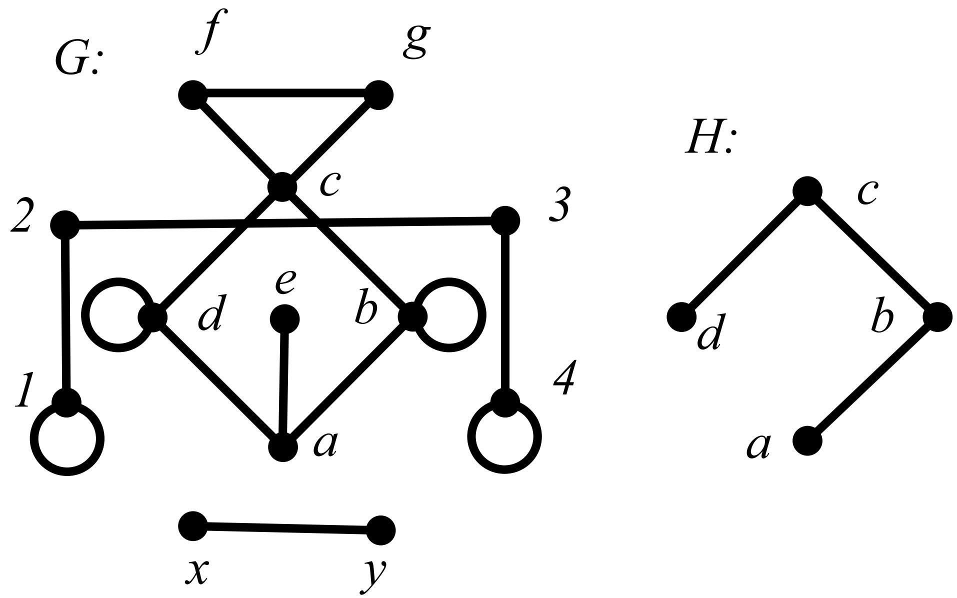
Például az ábrán az összefüggő komponensek:$\{x, y\}$, $\{1, 2, 3, 4\}$ és $\{a, b, c, d, e, f, g\}$. H részgráf (de nem feszített. A tételből a **maximális**



Például az ábrán az összefüggő komponensek:$\{x, y\}$, $\{1, 2, 3, 4\}$ és $\{a, b, c, d, e, f, g\}$. H részgráf (de nem feszített. A tételből a **maximális** jelző nem hagyható el, mert különben a felbontás nem egyértelmű (hiszen pl. egyelemű összefüggő részgráfokra is felbontható).

Nem hagyható el a

Nem hagyható el a *feszített* jelző sem, hiszen egyébként pl. az $\{a, b, c, d, e, f, g\}$ komponensből az "(a, d)-él" elhagyható lenne, és megintcsak oda az egyértelműség.



A bizonyítás alapötlete: Az $\alpha :=$

A bizonyítás alapötlete: Az $\alpha := \{(a, b) \in V^2$: létezik út a-ból b-be$\}$

A bizonyítás alapötlete: Az $\alpha := \{(a, b) \in V^2$: létezik út a-ból b-be$\}$ ekvivalenciareláció szerinti osztályozás blokkjai adják a komponenseket.

A bizonyítás alapötlete: Az $\alpha := \{(a,b) \in V^2$: létezik út a-ból b-be$\}$ ekvivalenciareláció szerinti osztályozás blokkjai adják a komponenseket. (Az evidens részletek az érdeklődő hallgatóságra maradnak.) Q.e.d.

Euler-vonal

Euler-vonal

A legelső gráfelméleti eredményről lesz szó (Euler, 1736).

Euler-vonal

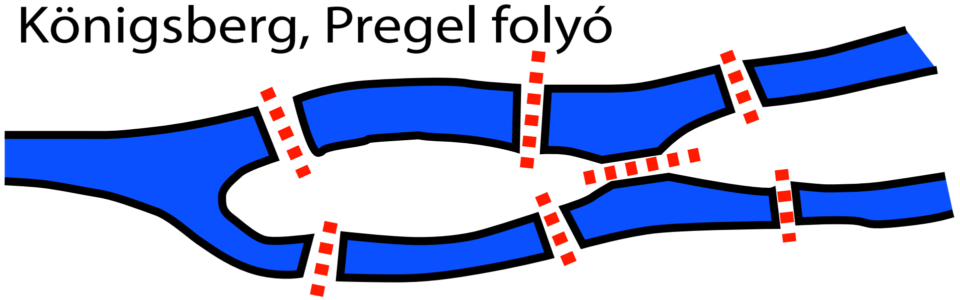
A legelső gráfelméleti eredményről lesz szó (Euler, 1736). Végig lehet-e menni a Pregel-folyó hét hídján úgy,

Euler-vonal

A legelső gráfelméleti eredményről lesz szó (Euler, 1736). Végig lehet-e menni a Pregel-folyó hét hídján úgy, hogy mindegyiken pontosan egyszer megyünk keresztül? (

Euler-vonal

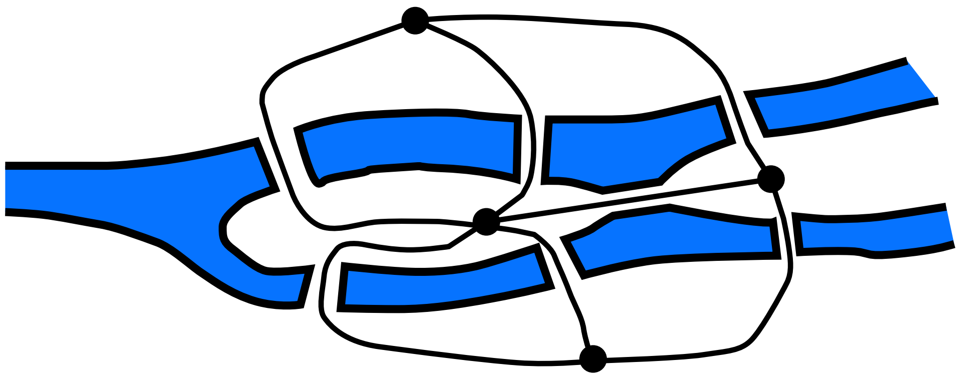
A legelső gráfelméleti eredményről lesz szó (Euler, 1736). Végig lehet-e menni a Pregel-folyó hét hídján úgy, hogy mindegyiken pontosan egyszer megyünk keresztül? (A nagyobbik sziget csak félig látszik az ábrán.)



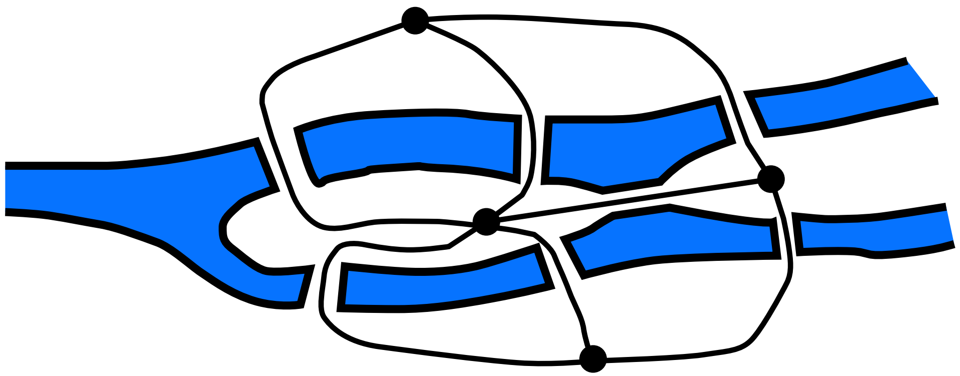
Königsberget a folyó négy részre vágja, ezeket egy gráf szögpontjainak, a hidakat pedig ezen gráf éleinek kinevezve:

Königsberget a folyó négy részre vágja, ezeket egy gráf szögpontjainak, a hidakat pedig ezen gráf éleinek kinevezve: a kérdés az, hogy van-e ebben a gráfban

Königsberget a folyó négy részre vágja, ezeket egy gráf szögpontjainak, a hidakat pedig ezen gráf éleinek kinevezve: a kérdés az, hogy van-e ebben a gráfban olyan séta, amelyik a gráf mindegyik élét pontosan egyszer tartalmazza.

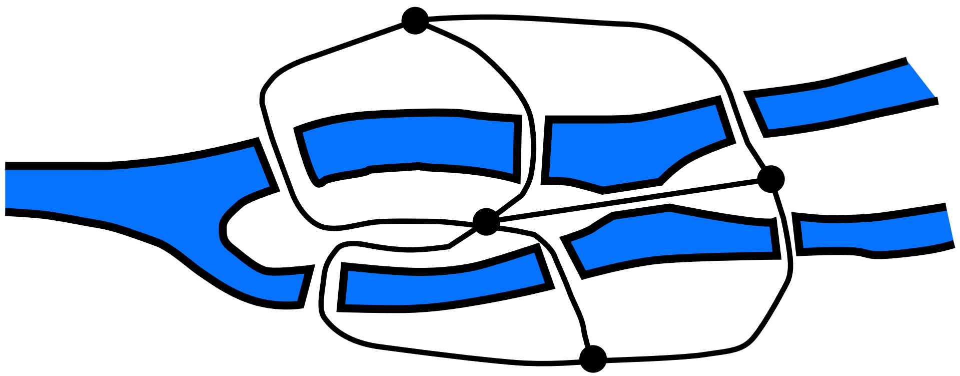


Königsberget a folyó négy részre vágja, ezeket egy gráf szögpontjainak, a hidakat pedig ezen gráf éleinek kinevezve: a kérdés az, hogy van-e ebben a gráfban olyan séta, amelyik a gráf mindegyik élét pontosan egyszer tartalmazza.



Ma — akár mondjuk külön, akár nem — csak véges gráfokat tekintünk.

Königsberget a folyó négy részre vágja, ezeket egy gráf szögpontjainak, a hidakat pedig ezen gráf éleinek kinevezve: a kérdés az, hogy van-e ebben a gráfban olyan séta, amelyik a gráf mindegyik élét pontosan egyszer tartalmazza.



Ma — akár mondjuk külön, akár nem — csak véges gráfokat tekintünk.

Definíció: Egy olyan sétát, amely a gráf minden élét pontosan egyszer tartalmazza, **Euler-vonalnak** nevezünk. Ha emellett a séta zárt

Definíció: Egy olyan sétát, amely a gráf minden élét pontosan egyszer tartalmazza, **Euler-vonalnak** nevezünk. Ha emellett a séta zárt (kezdőpont=végpont), akkor **zárt Euler-vonalnak** nevezzük.

Definíció: Egy olyan sétát, amely a gráf minden élét pontosan egyszer tartalmazza, **Euler-vonalnak** nevezünk. Ha emellett a séta zárt (kezdőpont=végpont), akkor **zárt Euler-vonalnak** nevezzük.

Ha egy G gráfban nincs izolált (

Definíció: Egy olyan sétát, amely a gráf minden élét pontosan egyszer tartalmazza, **Euler-vonalnak** nevezünk. Ha emellett a séta zárt (kezdőpont=végpont), akkor **zárt Euler-vonalnak** nevezzük.

Ha egy G gráfban nincs izolált (=nulladfokú) szögpont és van Euler-vonal, akkor nyilván

Definíció: Egy olyan sétát, amely a gráf minden élét pontosan egyszer tartalmazza, **Euler-vonalnak** nevezünk. Ha emellett a séta zárt (kezdőpont=végpont), akkor **zárt Euler-vonalnak** nevezzük.

Ha egy G gráfban nincs izolált (=nulladfokú) szögpont és van Euler-vonal, akkor nyilván a gráf összefüggő, továbbá

Definíció: Egy olyan sétát, amely a gráf minden élét pontosan egyszer tartalmazza, **Euler-vonalnak** nevezünk. Ha emellett a séta zárt (kezdőpont=végpont), akkor **zárt Euler-vonalnak** nevezzük.

Ha egy G gráfban nincs izolált (=nulladfokú) szögpont és van Euler-vonal, akkor nyilván a gráf összefüggő, továbbá a séta kezdő és végpontját (ha ezek különbözők) leszámítva minden szögpontba bemegyünk és onnak kijövünk, esetleg többször is, és így ezen szögpontok foka páros. Ha zárt Euler-vonal is van

Definíció: Egy olyan sétát, amely a gráf minden élét pontosan egyszer tartalmazza, **Euler-vonalnak** nevezünk. Ha emellett a séta zárt (kezdőpont=végpont), akkor **zárt Euler-vonalnak** nevezzük.

Ha egy G gráfban nincs izolált (=nulladfokú) szögpont és van Euler-vonal, akkor nyilván a gráf összefüggő, továbbá a séta kezdő és végpontját (ha ezek különbözők) leszámítva minden szögpontba bemegyünk és onnak kijövünk, esetleg többször is, és így ezen szögpontok foka páros. Ha zárt Euler-vonal is van (azaz a gráf **Euler-gráf**, akkor minden szögpont foka páros.

Meglepő módon ezen könnyen látható szükséges feltételek elegendőek is! Pontosabban:

Meglepő módon ezen könnyen látható szükséges feltételek elegendőek is! Pontosabban:

36. Tétel. *Legyen* G *egy izolált pont nélküli gráf. (Irányítatlan; többszörös élek megengedettek.) Ekkor*

Meglepő módon ezen könnyen látható szükséges feltételek elegendőek is! Pontosabban:

36. Tétel. *Legyen G egy izolált pont nélküli gráf. (Irányítatlan; többszörös élek megengedettek.) Ekkor*

(1) G Euler-gráf $\iff$ összefüggő és minden szögpont foka páros.

Meglepő módon ezen könnyen látható szükséges feltételek elegendőek is! Pontosabban:

36. Tétel. *Legyen G egy izolált pont nélküli gráf. (Irányítatlan; többszörös élek megengedettek.) Ekkor*

(1) G Euler-gráf $\iff$ összefüggő és minden szögpont foka páros.

(2) G-ben van Euler-vonal $\iff$ G összefügő és legfeljebb kettő páratlan fokú szögpontja van.

A bizonyítás vázlata: (

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros.

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros. Feltehető, hogy nincsenek hurokélek (hiszen azok utólag is hozzávehetők majd a hurokéleitől megfosztott gráf Euler-vonalához).

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros. Feltehető, hogy nincsenek hurokélek (hiszen azok utólag is hozzávehetők majd a hurokéleitől megfosztott gráf Euler-vonalához).

Létezik olyan zárt séta, amelyikben bármely él legfeljebb egyszer fordul elő.

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros. Feltehető, hogy nincsenek hurokélek (hiszen azok utólag is hozzávehetők majd a hurokéleitől megfosztott gráf Euler-vonalához).

Létezik olyan zárt séta, amelyikben bármely él legfeljebb egyszer fordul elő. Ugyanis: engedjük meg a 0 hosszúságú sétát is (0 élből és egyetlen szögpontból áll)!

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros. Feltehető, hogy nincsenek hurokélek (hiszen azok utólag is hozzávehetők majd a hurokéleitől megfosztott gráf Euler-vonalához).

Létezik olyan zárt séta, amelyikben bármely él legfeljebb egyszer fordul elő. Ugyanis: engedjük meg a 0 hosszúságú sétát is (0 élből és egyetlen szögpontból áll)!

Legyen L *maximális*

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros. Feltehető, hogy nincsenek hurokélek (hiszen azok utólag is hozzávehetők majd a hurokéleitől megfosztott gráf Euler-vonalához).

Létezik olyan zárt séta, amelyikben bármely él legfeljebb egyszer fordul elő. Ugyanis: engedjük meg a 0 hosszúságú sétát is (0 élből és egyetlen szögpontból áll)!

Legyen L *maximális* hosszúságú zárt séta, amelyben mindegyik él legfeljebb egyszer lép fel.

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros. Feltehető, hogy nincsenek hurokélek (hiszen azok utólag is hozzávehetők majd a hurokéleitől megfosztott gráf Euler-vonalához).

Létezik olyan zárt séta, amelyikben bármely él legfeljebb egyszer fordul elő. Ugyanis: engedjük meg a 0 hosszúságú sétát is (0 élből és egyetlen szögpontból áll)!

Legyen L *maximális* hosszúságú zárt séta, amelyben mindegyik él legfeljebb egyszer lép fel. Indirekt tegyük fel, hogy L nem tartalmazza az összes élet.

A bizonyítás vázlata: (**Algoritmust is ad!**) Tegyük fel, hogy G öfgő és minden pont foka páros. Feltehető, hogy nincsenek hurokélek (hiszen azok utólag is hozzávehetők majd a hurokéleitől megfosztott gráf Euler-vonalához).

Létezik olyan zárt séta, amelyikben bármely él legfeljebb egyszer fordul elő. Ugyanis: engedjük meg a 0 hosszúságú sétát is (0 élből és egyetlen szögpontból áll)!

Legyen L *maximális* hosszúságú zárt séta, amelyben mindegyik él legfeljebb egyszer lép fel. Indirekt tegyük fel, hogy L nem tartalmazza az összes élet.

Állítjuk, hogy

Állítjuk, hogy létezik egy L-en kívüli e_1 él úgy, hogy ezen élnek (legalább) az egyik végpontja, mondjuk b, L által látogatott.

Állítjuk, hogy létezik egy L-en kívüli e_1 él úgy, hogy ezen élnek (legalább) az egyik végpontja, mondjuk b, L által látogatott. (Azért nem mondom, hogy L-beli, mert a többszörös élek miatt a szögpontok sorozata nem határozza meg az élek sorozatát; tehát itt a séta csakis az élek sorozatával adható meg!)

Állítjuk, hogy létezik egy L-en kívüli e_1 él úgy, hogy ezen élnek (legalább) az egyik végpontja, mondjuk b, L által látogatott. (Azért nem mondom, hogy L-beli, mert a többszörös élek miatt a szögpontok sorozata nem határozza meg az élek sorozatát; tehát itt a séta csakis az élek sorozatával adható meg!)

Ha L mindegyik szögpontot meglátogatja, akkor ez evidens.

Állítjuk, hogy létezik egy L-en kívüli e_1 él úgy, hogy ezen élnek (legalább) az egyik végpontja, mondjuk b, L által látogatott. (Azért nem mondom, hogy L-beli, mert a többszörös élek miatt a szögpontok sorozata nem határozza meg az élek sorozatát; tehát itt a séta csakis az élek sorozatával adható meg!)

Ha L mindegyik szögpontot meglátogatja, akkor ez evidens. Ha nem, akkor tekinsünk egy L által nem látogatott a szögpontot és egy L által látogatott b szögpontot, majd

Állítjuk, hogy létezik egy L-en kívüli e_1 él úgy, hogy ezen élnek (legalább) az egyik végpontja, mondjuk b, L által látogatott. (Azért nem mondom, hogy L-beli, mert a többszörös élek miatt a szögpontok sorozata nem határozza meg az élek sorozatát; tehát itt a séta csakis az élek sorozatával adható meg!)

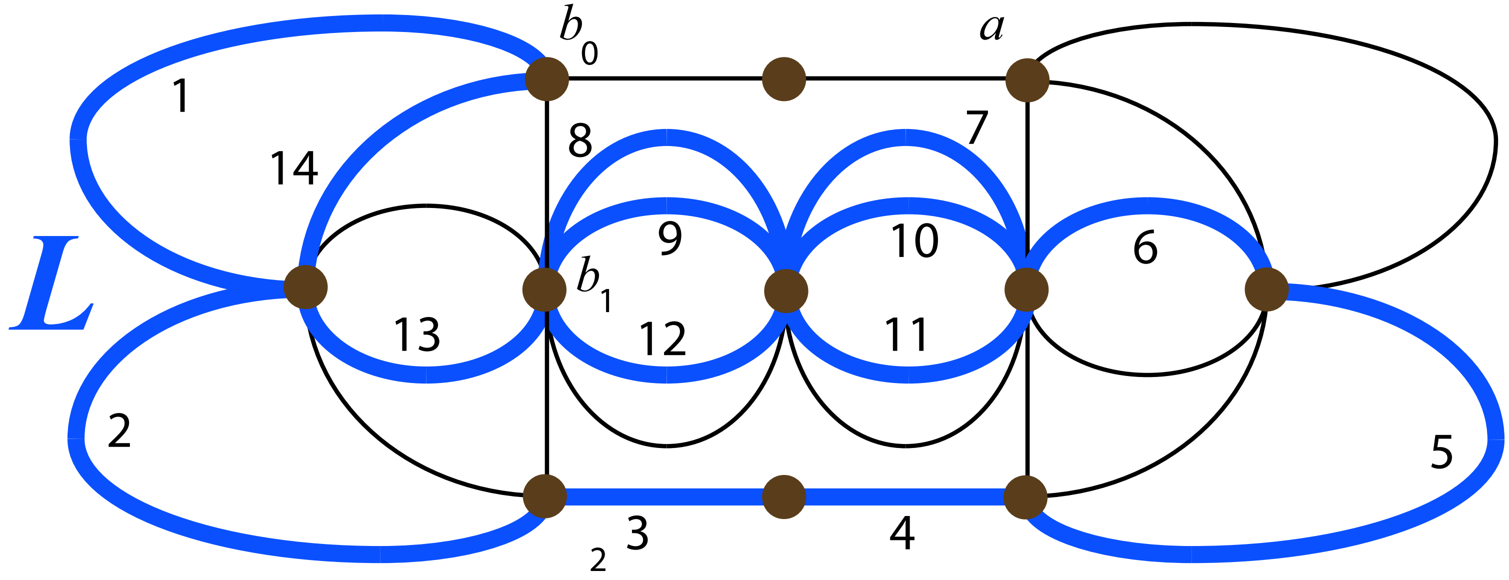
Ha L mindegyik szögpontot meglátogatja, akkor ez evidens. Ha nem, akkor tekinsünk egy L által nem látogatott a szögpontot és egy L által látogatott b szögpontot, majd (G öfgő!) egy utat a-ból b-be

Állítjuk, hogy létezik egy L-en kívüli e_1 él úgy, hogy ezen élnek (legalább) az egyik végpontja, mondjuk b, L által látogatott. (Azért nem mondom, hogy L-beli, mert a többszörös élek miatt a szögpontok sorozata nem határozza meg az élek sorozatát; tehát itt a séta csakis az élek sorozatával adható meg!)

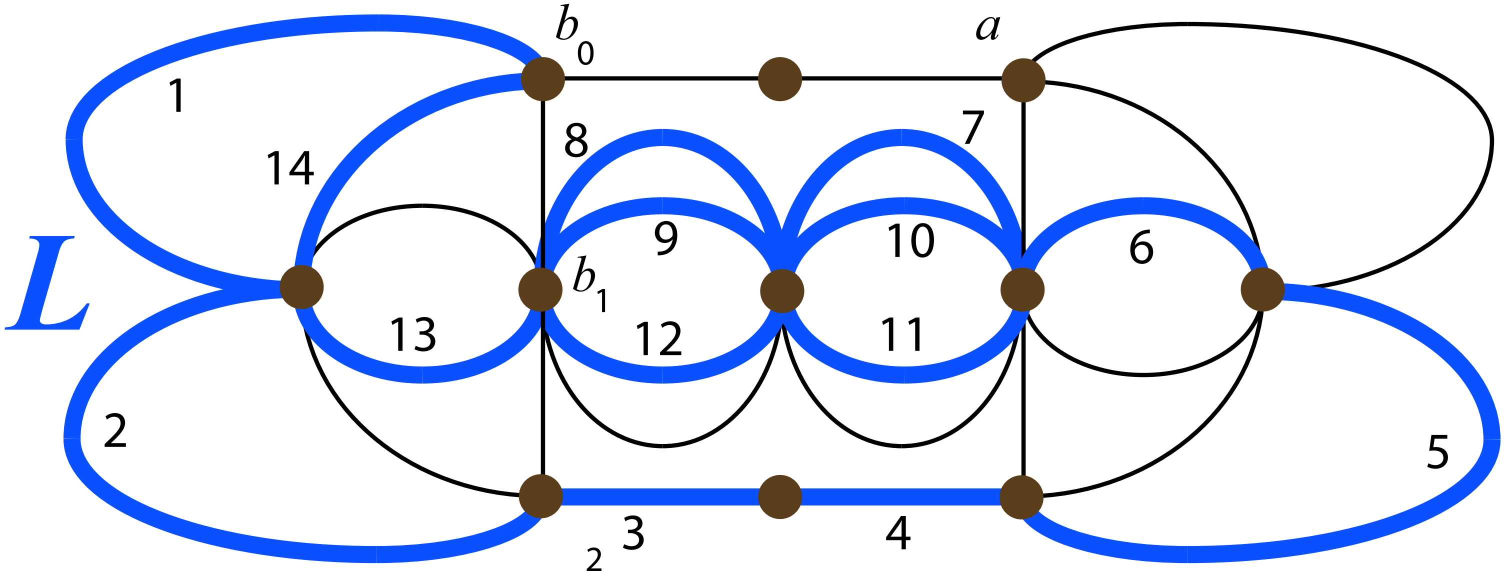
Ha L mindegyik szögpontot meglátogatja, akkor ez evidens. Ha nem, akkor tekinsünk egy L által nem látogatott a szögpontot és egy L által látogatott b szögpontot, majd (G öfgő!) egy utat a-ból b-be — az első olyan él, amelyik nem látogatott szögpontból látogatottba visz, jó lesz.

Állítjuk, hogy létezik egy L-en kívüli e_1 él úgy, hogy ezen élnek (legalább) az egyik végpontja, mondjuk b, L által látogatott. (Azért nem mondom, hogy L-beli, mert a többszörös élek miatt a szögpontok sorozata nem határozza meg az élek sorozatát; tehát itt a séta csakis az élek sorozatával adható meg!)

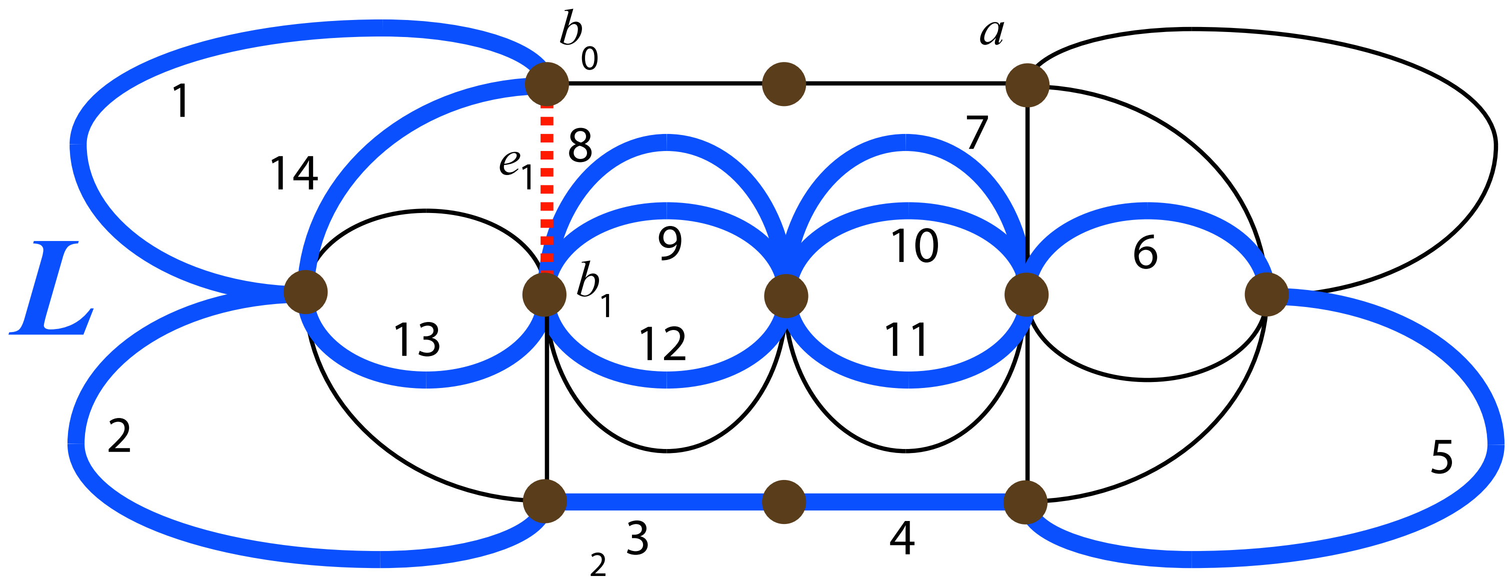
Ha L mindegyik szögpontot meglátogatja, akkor ez evidens. Ha nem, akkor tekinsünk egy L által nem látogatott a szögpontot és egy L által látogatott b szögpontot, majd (G öfgő!) egy utat a-ból b-be — az első olyan él, amelyik nem látogatott szögpontból látogatottba visz, jó lesz. (De mi az ábrán egy másikat tekintjük e_1-nek, mivel az tanulságosabb.)



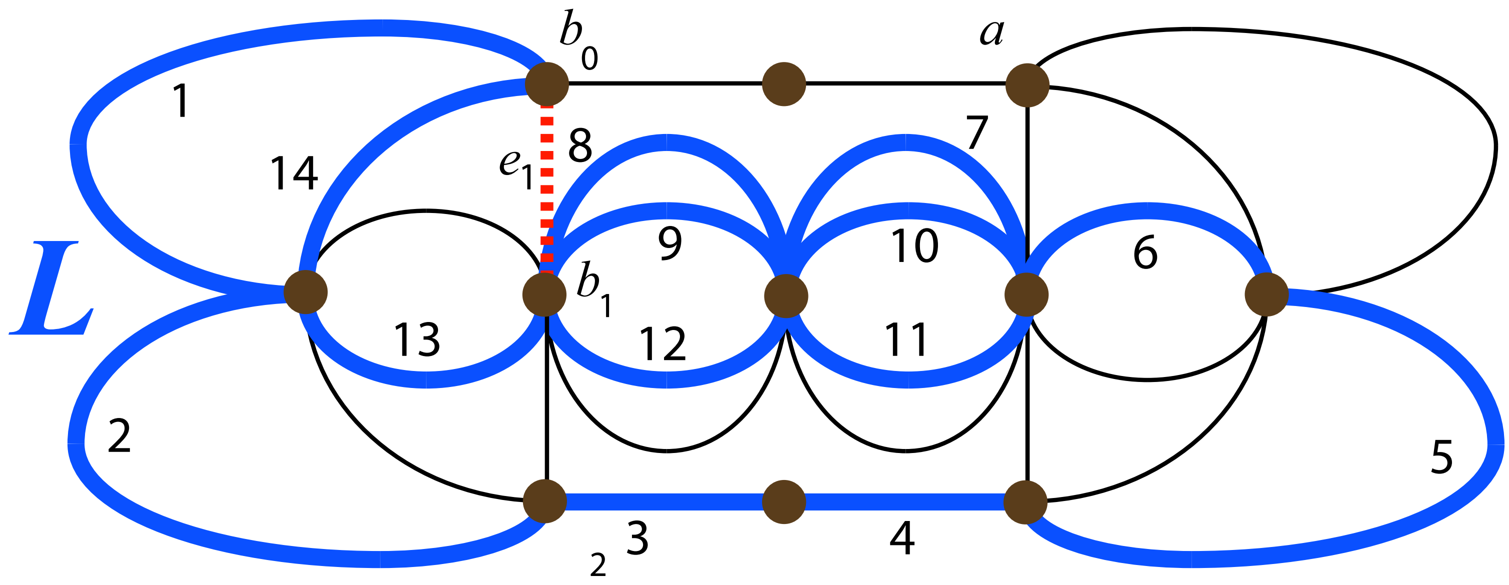
Tehát $\exists b$, amelyet L (vastag kék) látogat, és amelyből L-en kívüli e_1 él indul.



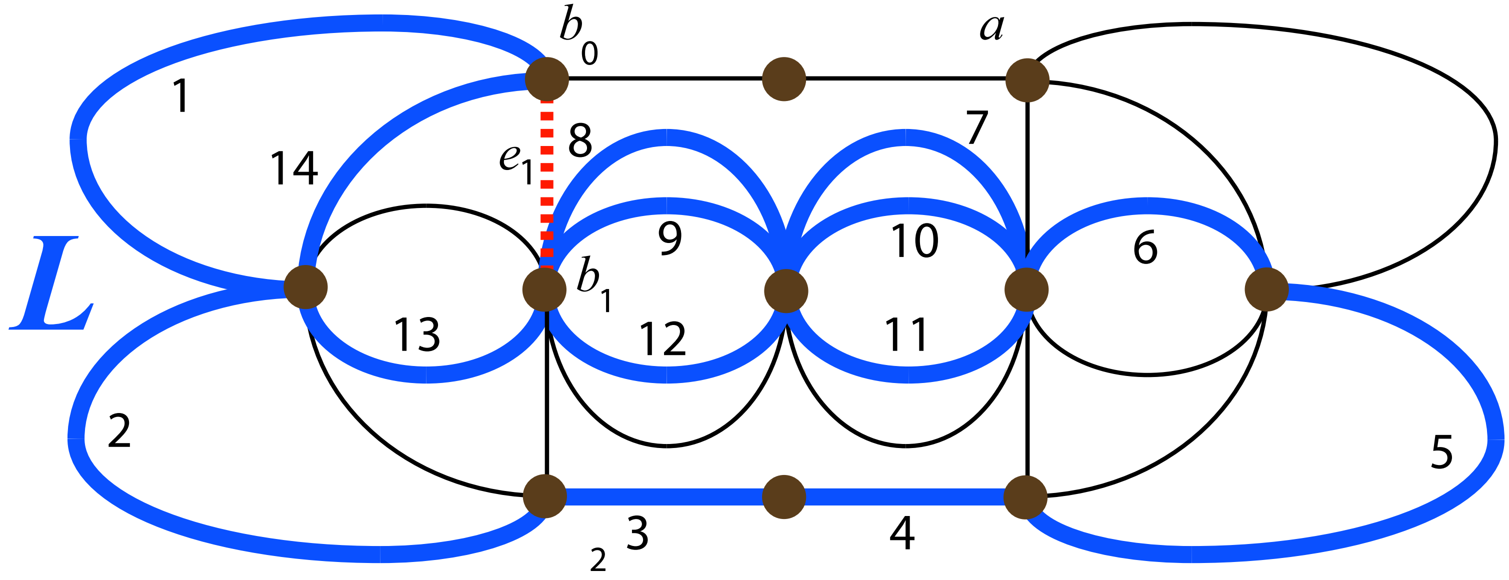
Tehát $\exists b$, amelyet L (vastag kék) látogat, és amelyből L-en kívüli e_1 él indul. Induljunk el egy K sétára (vastag szaggatott piros) $b = b_0$-ból L-en kívüli éleken, éleket nem ismételve.



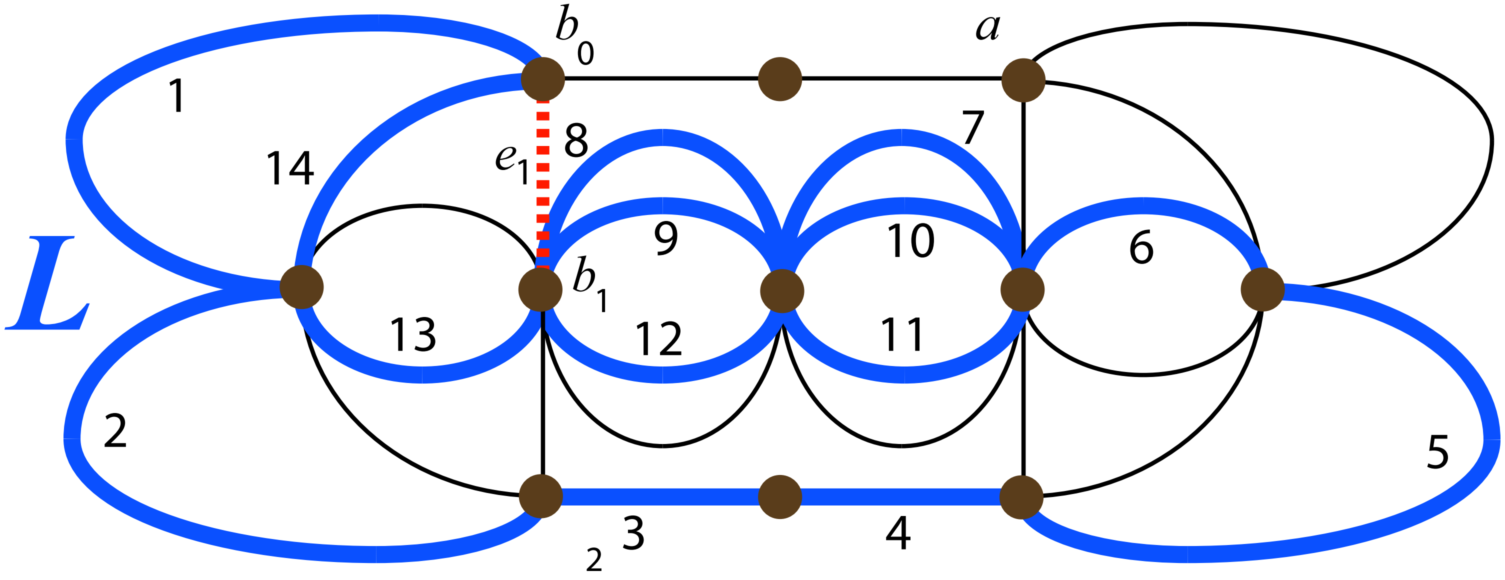
Az e_1 élen eljutunk $b = b_0$-ból egy $b_1 \neq b_0$ pontba.



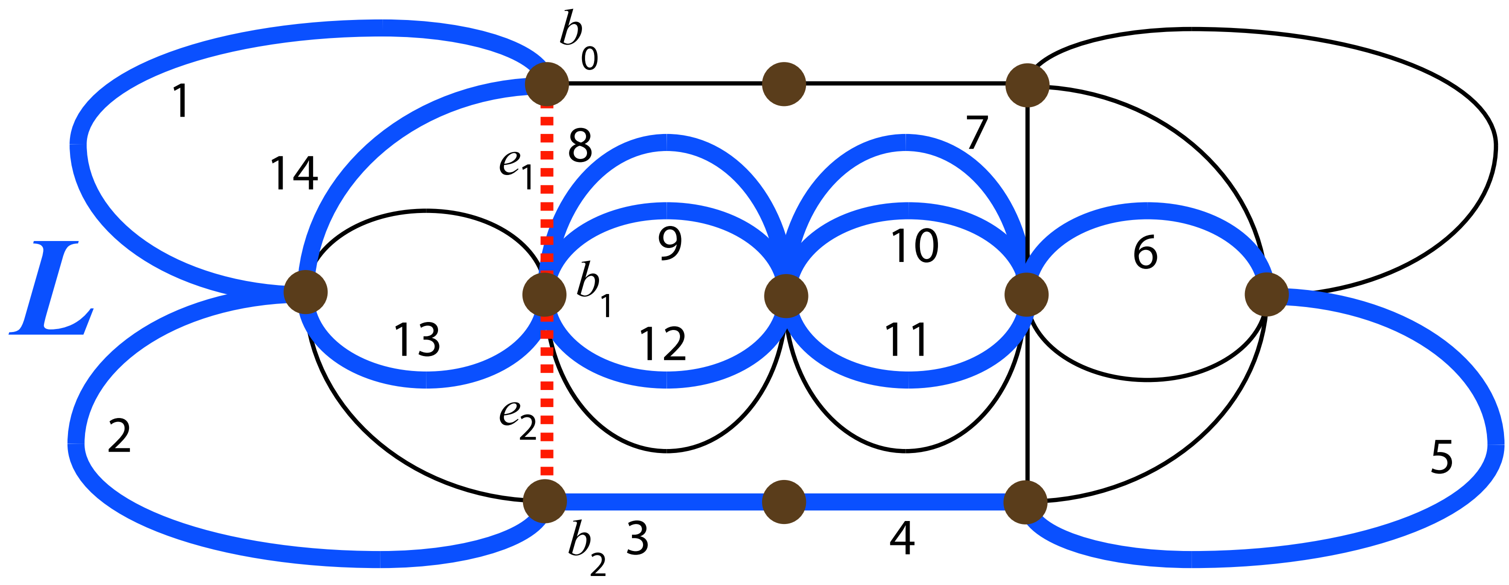
Az e_1 élen eljutunk $b = b_0$-ból egy $b_1 \neq b_0$ pontba. Mivel b_1 "L-foka" (azaz az L-beli élek által alkotott részgráfban — ami nyilván Euler-gráf — tekintett foka) páros, és G-beli foka is páros,



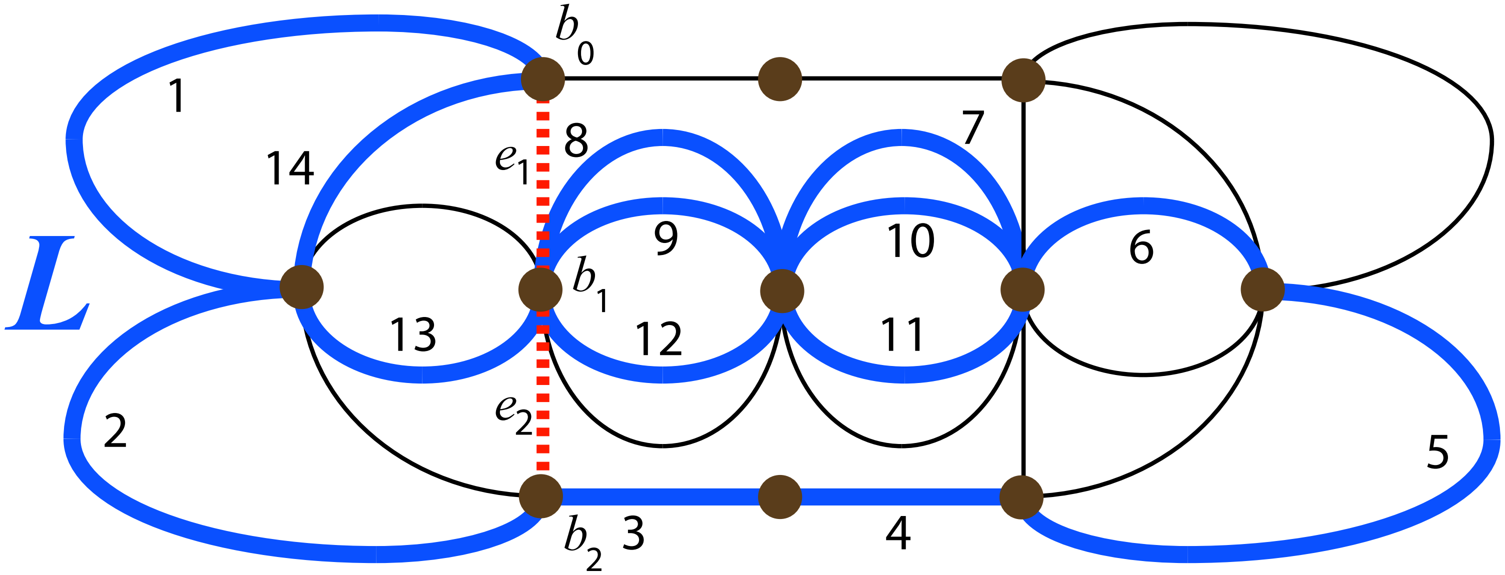
Az e_1 élen eljutunk $b = b_0$-ból egy $b_1 \neq b_0$ pontba. Mivel b_1 "L-foka" (azaz az L-beli élek által alkotott részgráfban — ami nyilván Euler-gráf — tekintett foka) páros, és G-beli foka is páros, van az L-beli éleken és az e_1 élen kívül is L-ből induló további, e_2 él!



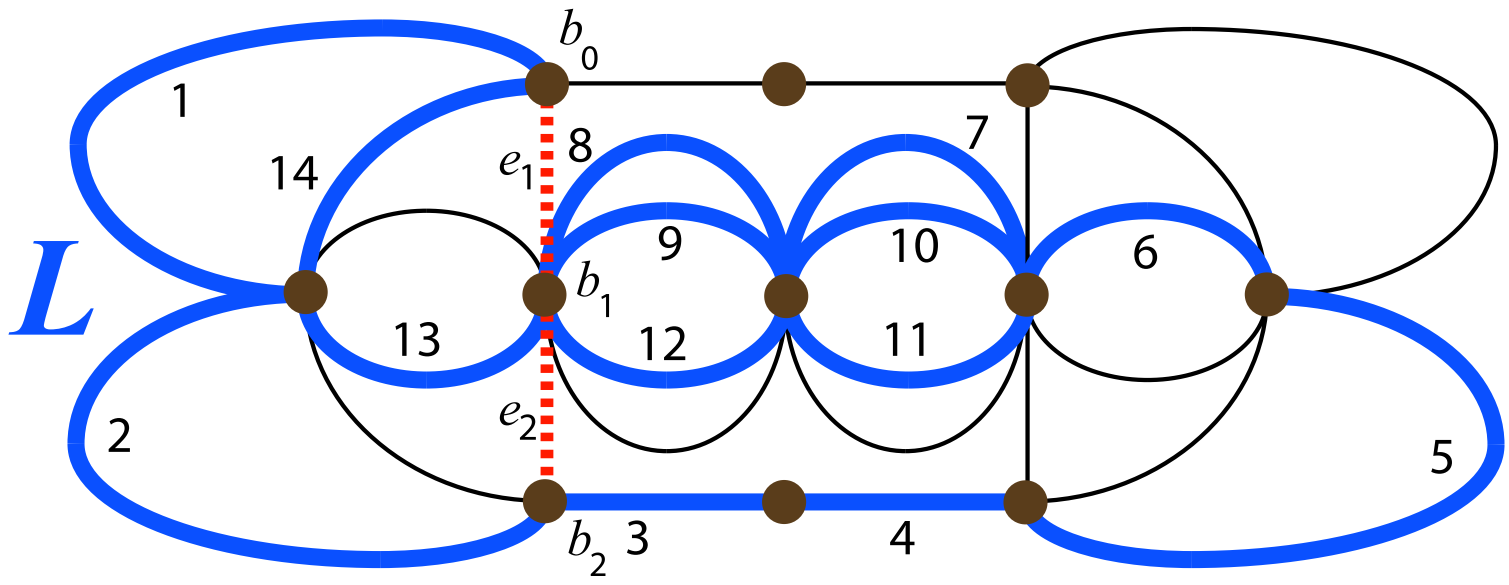
Az e_1 élen eljutunk $b = b_0$-ból egy $b_1 \neq b_0$ pontba. Mivel b_1 "L-foka" (azaz az L-beli élek által alkotott részgráfban — ami nyilván Euler-gráf — tekintett foka) páros, és G-beli foka is páros, van az L-beli éleken és az e_1 élen kívül is L-ből induló további, e_2 él! Azon menjünk tovább egy b_2-vel jelölt szögpontba!



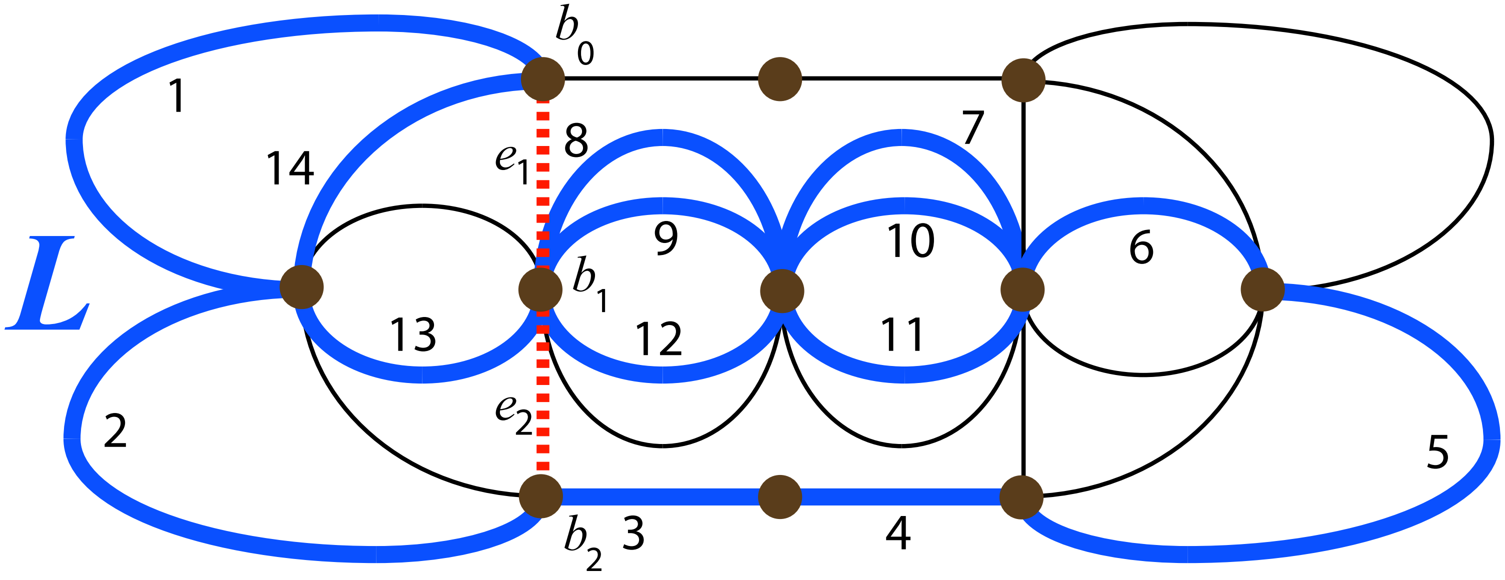
Ha $b_2 \neq b_0$, akkor — mivel az L-foka is és a G-beli foka is páros, létezik b_2-ből induló, eddig még nem szerepelt él, azon menjünk tovább.



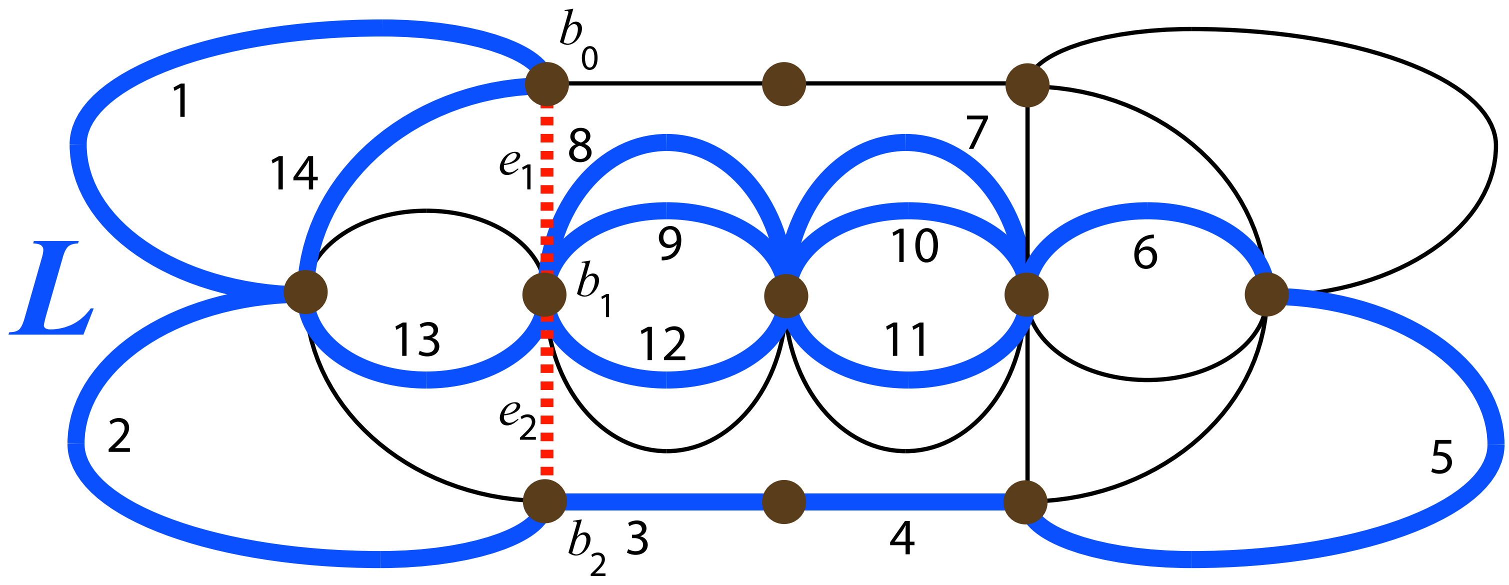
Ha $b_2 \neq b_0$, akkor — mivel az L-foka is és a G-beli foka is páros, létezik b_2-ből induló, eddig még nem szerepelt él, azon menjünk tovább. Stb.



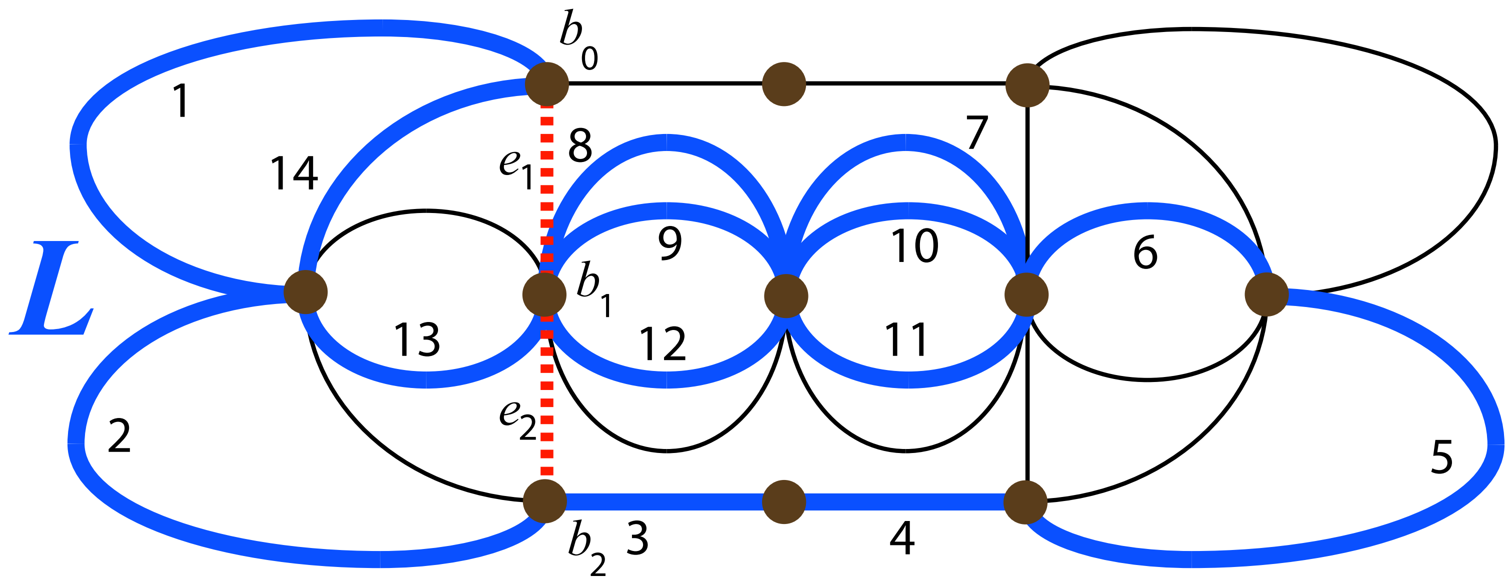
Az se baj, ha visszaérünk egy korábbi, de b_0-tól különböző szögponthoz:



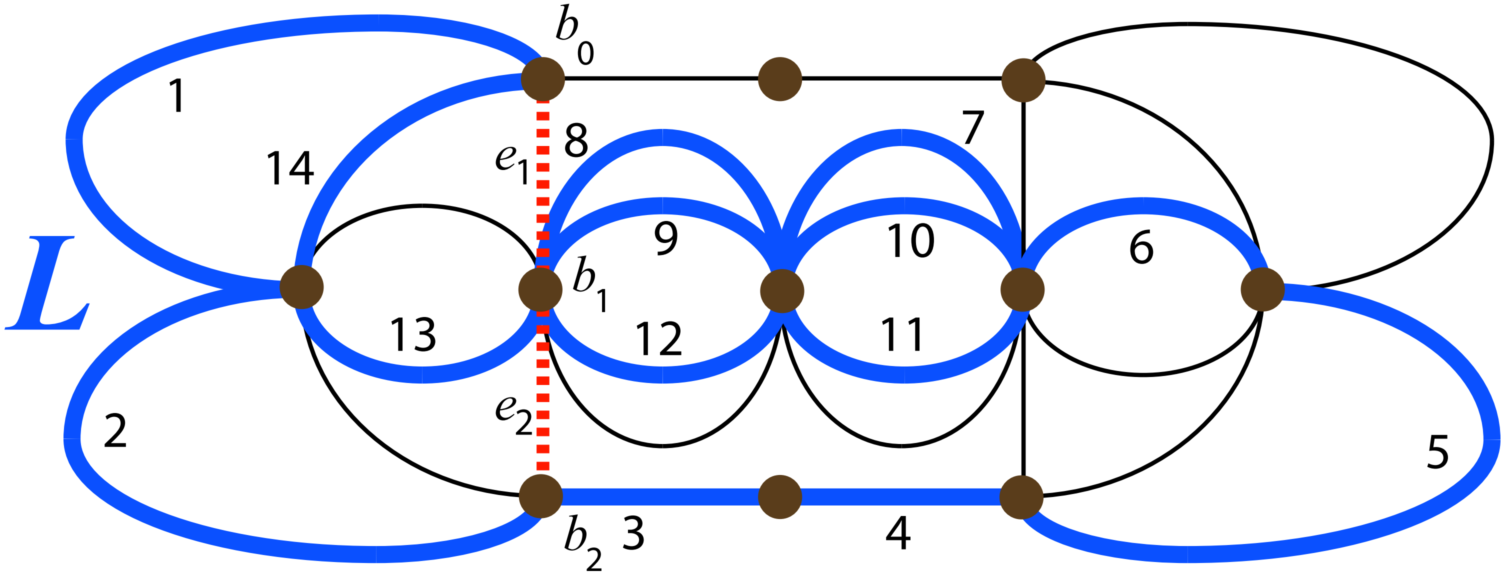
Az se baj, ha visszaérünk egy korábbi, de b_0-tól különböző szögponthoz: L valahányszor bement és ugyanannyiszor kiment (páros sok él),



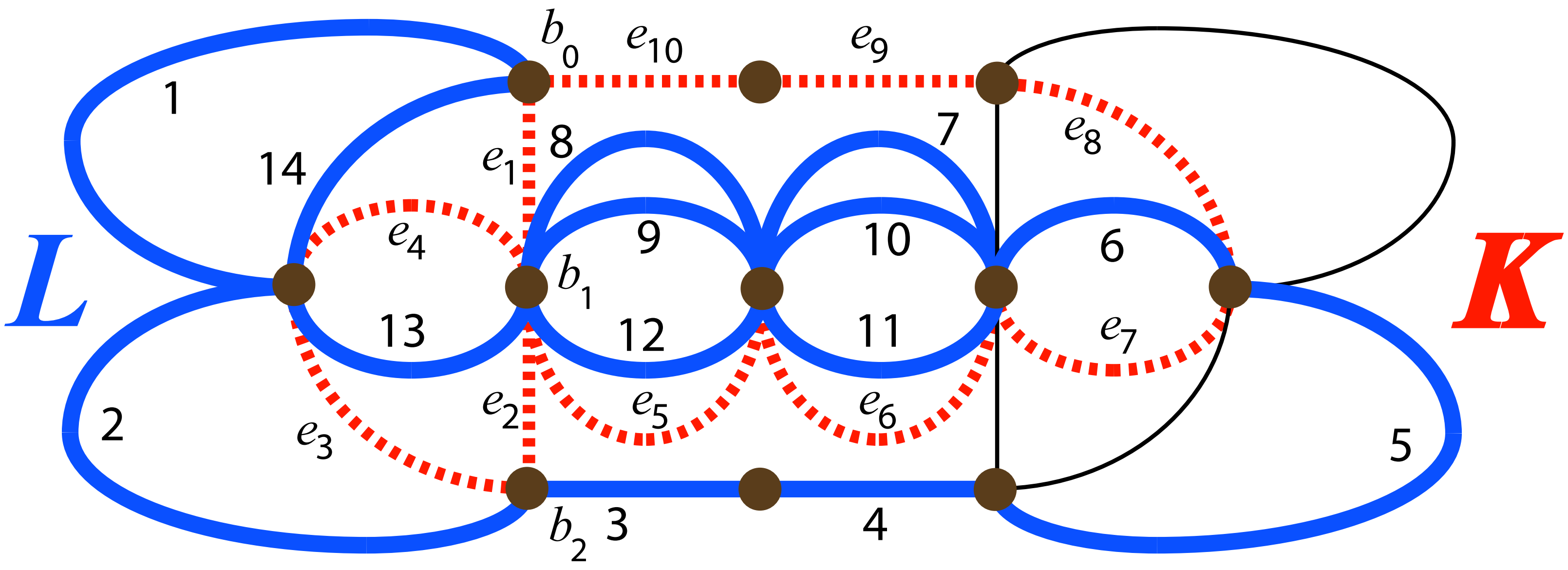
és K eddigi része is korábban valahányszor bement és kiment (páros sok él),



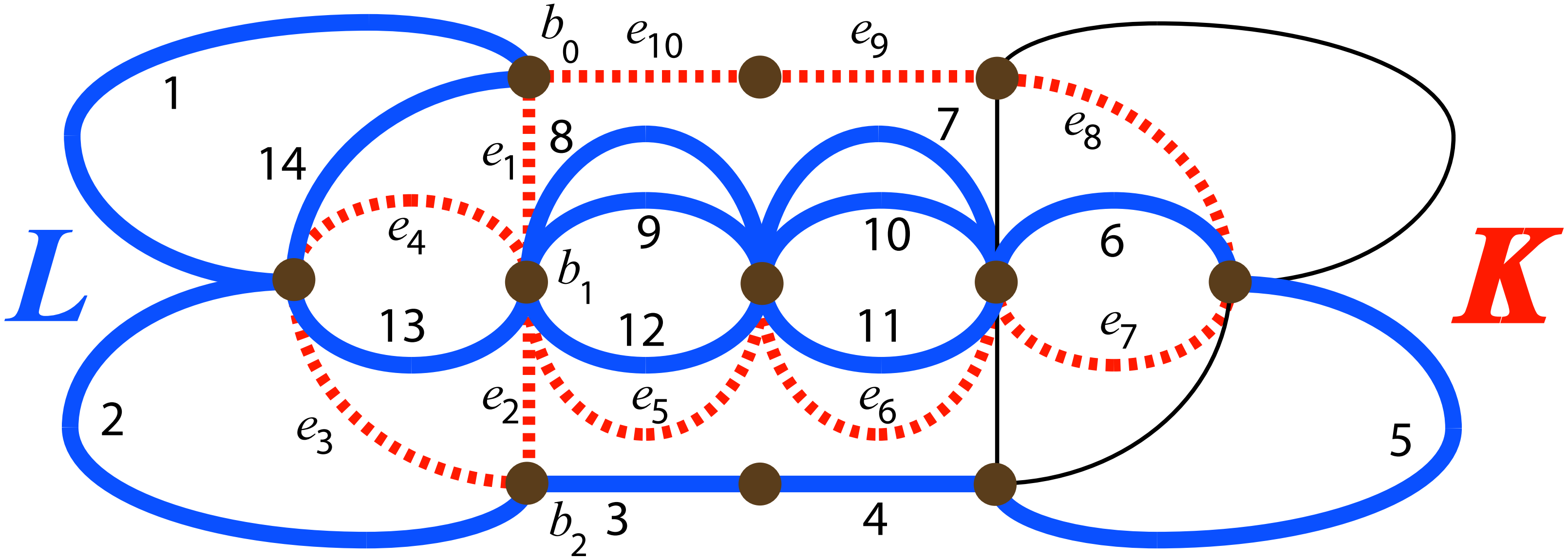
és K eddigi része is korábban valahányszor bement és kiment (páros sok él), most bementünk, (ez eddig páratlan sok él),



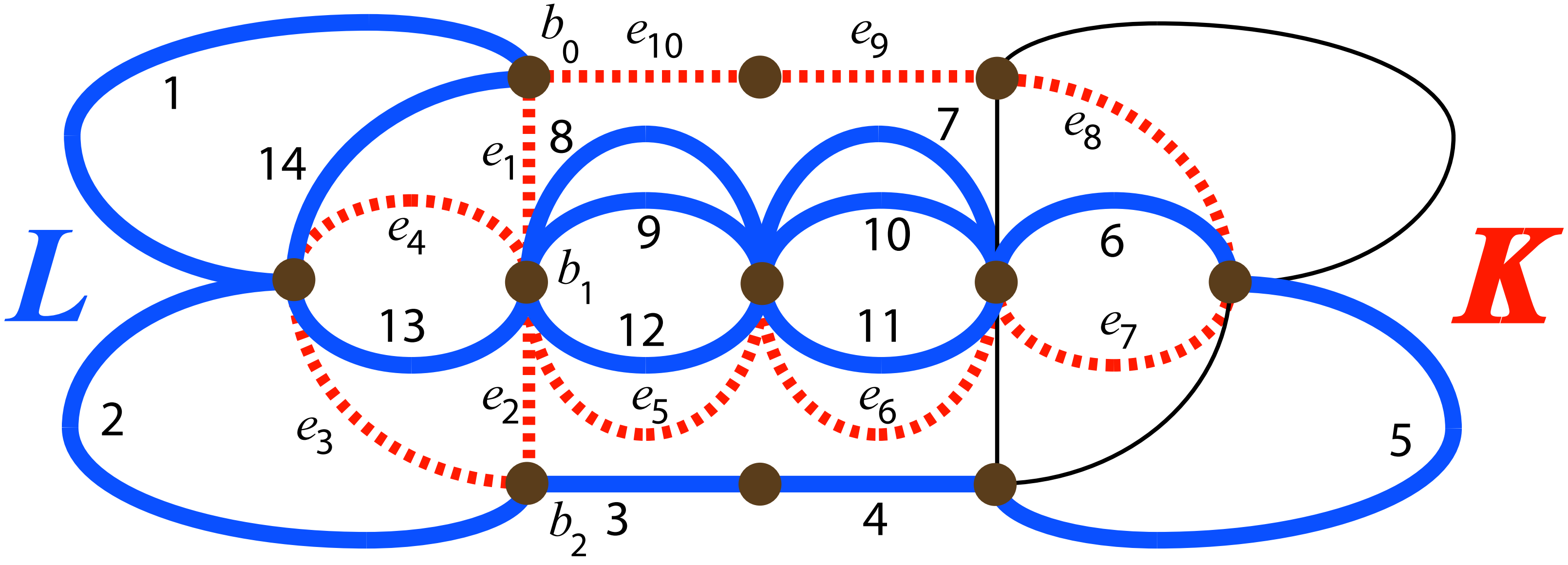
és K eddigi része is korábban valahányszor bement és kiment (páros sok él), most bementünk, (ez eddig páratlan sok él), van tehát eddig nem használt él, amin távozhatunk.



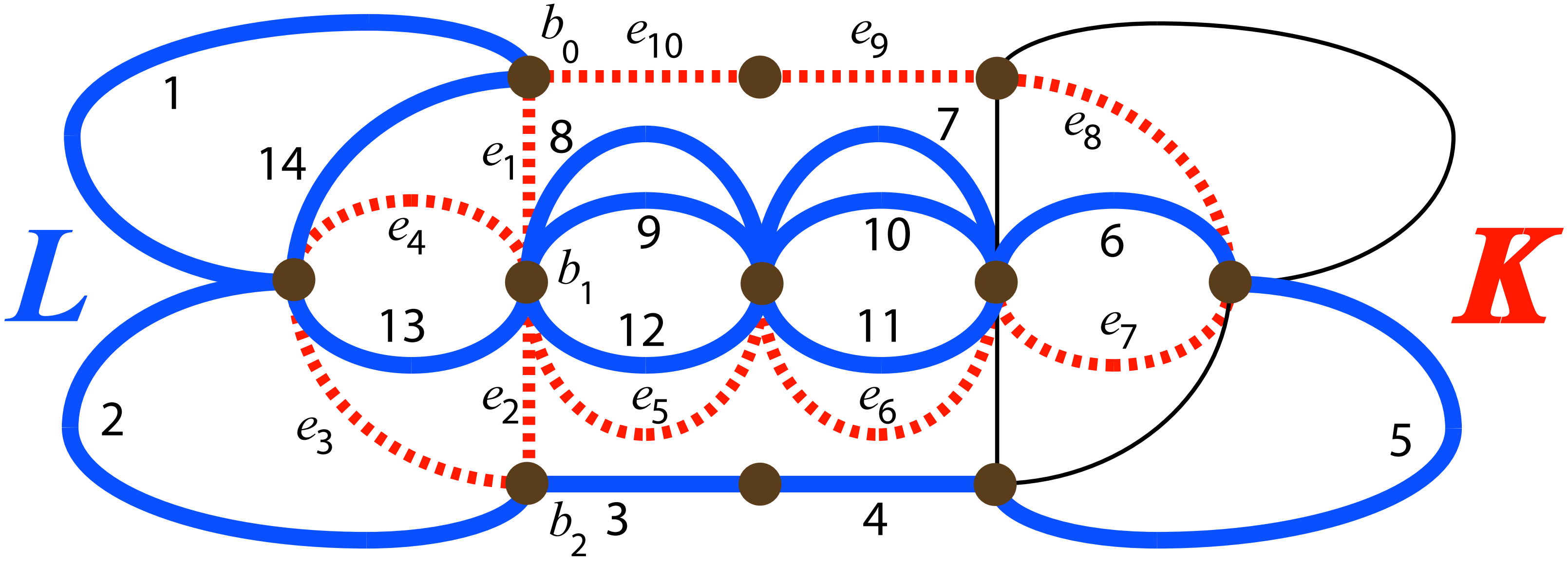
Végtelen sokszor nem találhatunk új élet, tehát



Végtelen sokszor nem találhatunk új élet, tehát — mivel minden más esetben találunk — előbb-utóbb visszaérünk b_0-ba, és ezzel befejeződik a K séta konstrukciója.



b_0
e_{10}
e_9
1
14
e_1
8
7
e_8
e_4
9
10
6
L
b_1
K
13
12
11
e_7
2
e_2
e_5
e_6
e_3
5
b_2
3
4



Mármost ha b_0-ból előbb L majd K mentén sétálunk, akkor zárt sétát kapunk különböző éleken, ami hosszabb L-nél, ellentmondás, q.e.d.

A bizonyítás **algoritmust** szolgáltat zárt Euler-vonal keresésére! (Elég jót, bár van jobb is a könyvben.)

A bizonyítás **algoritmust** szolgáltat zárt Euler-vonal keresésére! (Elég jót, bár van jobb is a könyvben.)

A nem zárt Euler-vonal esete a zárt Euler-vonalra vezethető könnyedén vissza. A tétel szerint legfeljebb két páratlan fokú pont esetén létezik Euler-vonal.

A bizonyítás **algoritmust** szolgáltat zárt Euler-vonal keresésére! (Elég jót, bár van jobb is a könyvben.)

A nem zárt Euler-vonal esete a zárt Euler-vonalra vezethető könnyedén vissza. A tétel szerint legfeljebb két páratlan fokú pont esetén létezik Euler-vonal. Mivel a fokszámok összege páros (kétszerese az élek számának), ezért nem lehet pontosan egy páratlan fokú pont.

A bizonyítás **algoritmust** szolgáltat zárt Euler-vonal keresésére! (Elég jót, bár van jobb is a könyvben.)

A nem zárt Euler-vonal esete a zárt Euler-vonalra vezethető könnyedén vissza. A tétel szerint legfeljebb két páratlan fokú pont esetén létezik Euler-vonal. Mivel a fokszámok összege páros (kétszerese az élek számának), ezért nem lehet pontosan egy páratlan fokú pont. Ha nulla van, akkor zárt Euler-vonal is van (és láttuk, hogyan lehet találni.)

A bizonyítás **algoritmust** szolgáltat zárt Euler-vonal keresésére! (Elég jót, bár van jobb is a könyvben.)

A nem zárt Euler-vonal esete a zárt Euler-vonalra vezethető könnyedén vissza. A tétel szerint legfeljebb két páratlan fokú pont esetén létezik Euler-vonal. Mivel a fokszámok összege páros (kétszerese az élek számának), ezért nem lehet pontosan egy páratlan fokú pont. Ha nulla van, akkor zárt Euler-vonal is van (és láttuk, hogyan lehet találni.) Ha pontosan kettő páratlan fokú pont van, akkor kössük őket össze egy új éllel.

A bizonyítás **algoritmust** szolgáltat zárt Euler-vonal keresésére! (Elég jót, bár van jobb is a könyvben.)

A nem zárt Euler-vonal esete a zárt Euler-vonalra vezethető könnyedén vissza. A tétel szerint legfeljebb két páratlan fokú pont esetén létezik Euler-vonal. Mivel a fokszámok összege páros (kétszerese az élek számának), ezért nem lehet pontosan egy páratlan fokú pont. Ha nulla van, akkor zárt Euler-vonal is van (és láttuk, hogyan lehet találni.) Ha pontosan kettő páratlan fokú pont van, akkor kössük őket össze egy új éllel. Az új gráfban van zárt Euler-vonal, és meg is tudjuk keresni.

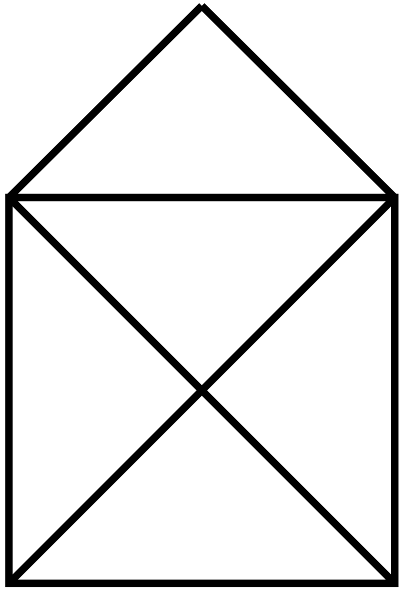
A bizonyítás **algoritmust** szolgáltat zárt Euler-vonal keresésére! (Elég jót, bár van jobb is a könyvben.)

A nem zárt Euler-vonal esete a zárt Euler-vonalra vezethető könnyedén vissza. A tétel szerint legfeljebb két páratlan fokú pont esetén létezik Euler-vonal. Mivel a fokszámok összege páros (kétszerese az élek számának), ezért nem lehet pontosan egy páratlan fokú pont. Ha nulla van, akkor zárt Euler-vonal is van (és láttuk, hogyan lehet találni.) Ha pontosan kettő páratlan fokú pont van, akkor kössük őket össze egy új éllel. Az új gráfban van zárt Euler-vonal, és meg is tudjuk keresni. Ha ebből az új élet elhagyjuk, az eredeti gráf egy nyitott Euler-vonalát kapjuk.

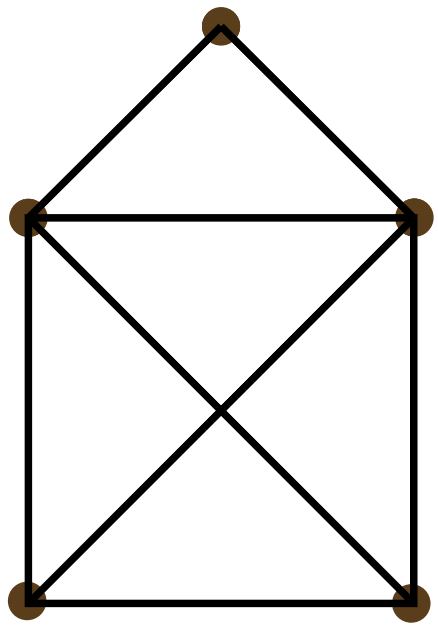
Az előző tétel módszerével könnyen kapjuk az alábbi tételt is (és az előbb látott módszer ott is alkalmas lesz a zárt Euler-vonal megkeresésére).

Az előző tétel módszerével könnyen kapjuk az alábbi tételt is (és az előbb látott módszer ott is alkalmas lesz a zárt Euler-vonal megkeresésére).

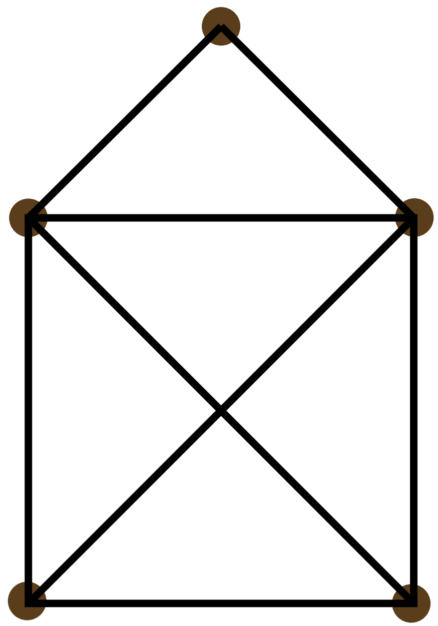
37. Tétel. *Irányított gráfnak pontosan akkor létezik zárt (természetesen irányított) Euler-vonala, ha a gráf gyengén összefüggő és minden pont kifoka azonos a befokával.*



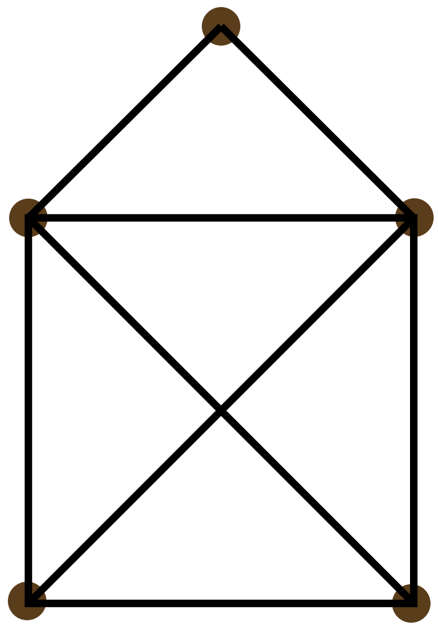
Feladat: Lerajzolható-e az ábrán látható ház anélkül, hogy a ceruzát felemelnénk?



Igen, mert ez a gráf összefüggő, és a páratlan fokú pontok száma 2.



Igen, mert ez a gráf összefüggő, és a páratlan fokú pontok száma 2. (Ugyanez a helyzet akkor is, ha az átlók metszéspontját is szögpontnak tekintjük.



Igen, mert ez a gráf összefüggő, és a páratlan fokú pontok száma 2. (Ugyanez a helyzet akkor is, ha az átlók metszéspontját is szögpontnak tekintjük. Mellesleg az eddig tanultak alapján világos, hogy a keresett Euler-vonal az egyik harmadfokú pontból a másikba megy.)

Hamilton-kör, Hamilton-út

Városnéző sétán többnyire nem az a cél, hogy a hidakon átmenjünk, hanem az, hogy minden nevezetességhez eljussunk pontosan egyszer.

Def: egyszerű (= nincs hurokél, nincs többszörös él) gráf esetén ha egy kör, illetve út minden szögponton átmegy, akkor **Hamilton-körnek**, illetve **Hamilton-útnak** nevezzük.

Megj.: a hurokéleknek, többszörös éleknek nem is jutna szerep, hiszen a kör/út bármely szögponton **csak egyszer** mehet át.

Hamilton-kör, Hamilton-út

Városnéző sétán többnyire nem az a cél, hogy a hidakon átmenjünk, hanem az, hogy minden nevezetességhez eljussunk pontosan egyszer.

Def: egyszerű (= nincs hurokél, nincs többszörös él) gráf esetén ha egy kör, illetve út minden szögponton átmegy, akkor **Hamilton-körnek**, illetve **Hamilton-útnak** nevezzük.

Megj.: a hurokéleknek, többszörös éleknek nem is jutna szerep, hiszen a kör/út bármely szögponton **csak egyszer** mehet át. Ha van Hamilton-kör, akkor Hamilton út is van.

Hamilton-kör, Hamilton-út

Városnéző sétán többnyire nem az a cél, hogy a hidakon átmenjünk, hanem az, hogy minden nevezetességhez eljussunk pontosan egyszer.

Def: egyszerű (= nincs hurokél, nincs többszörös él) gráf esetén ha egy kör, illetve út minden szögponton átmegy, akkor **Hamilton-körnek**, illetve **Hamilton-útnak** nevezzük.

Megj.: a hurokéleknek, többszörös éleknek nem is jutna szerep, hiszen a kör/út bármely szögponton **csak egyszer** mehet át. Ha van Hamilton-kör, akkor Hamilton út is van. Fordítva ez nem áll fenn, pl. a két szögpontú egyetlen élet tartalmazó gráfban (semilyen) kör nincs, de Hamilton-út van.

Jogos a várakozás, hogy a zárt Euler-vonalra vonatkozó könnyű és gyors algoritmus után hasonló szerepeljen a Hamilton-körre is.

Jogos a várakozás, hogy a zárt Euler-vonalra vonatkozó könnyű és gyors algoritmus után hasonló szerepeljen a Hamilton-körre is. Időhiány, Jogos a várakozás, hogy a zárt Euler-vonalra vonatkozó könnyű és gyors algoritmus után hasonló szerepeljen a Hamilton-körre is. Időhiány, és nincs is!

Jogos a várakozás, hogy a zárt Euler-vonalra vonatkozó könnyű és gyors algoritmus után hasonló szerepeljen a Hamilton-körre is. Időhiány, és nincs is! A Hamilton-kör keresése bizonyítottan **NP-teljes** probléma! (Ld. későbbi tanulmányok.

Jogos a várakozás, hogy a zárt Euler-vonalra vonatkozó könnyű és gyors algoritmus után hasonló szerepeljen a Hamilton-körre is. Időhiány, és nincs is! A Hamilton-kör keresése bizonyítottan **NP-teljes** probléma! (Ld. későbbi tanulmányok. P $=^?$ NP ???

Jogos a várakozás, hogy a zárt Euler-vonalra vonatkozó könnyű és gyors algoritmus után hasonló szerepeljen a Hamilton-körre is. Időhiány, és nincs is! A Hamilton-kör keresése bizonyítottan **NP-teljes** probléma! (Ld. későbbi tanulmányok. P $\stackrel{?}{=}$ NP ??? A megoldónak http://plus.maths.org/issue24/features/budd/ egymillió dollárt ígér!)

Jogos a várakozás, hogy a zárt Euler-vonalra vonatkozó könnyű és gyors algoritmus után hasonló szerepeljen a Hamilton-körre is. Időhiány, és nincs is! A Hamilton-kör keresése bizonyítottan **NP-teljes** probléma! (Ld. későbbi tanulmányok. P $=^?$ NP ??? A megoldónak http://plus.maths.org/issue24/features/budd/ egymillió dollárt ígér!) E bonyolult témakörből csak egyetlen tételt ismertetek, bizonyítás nélkül:

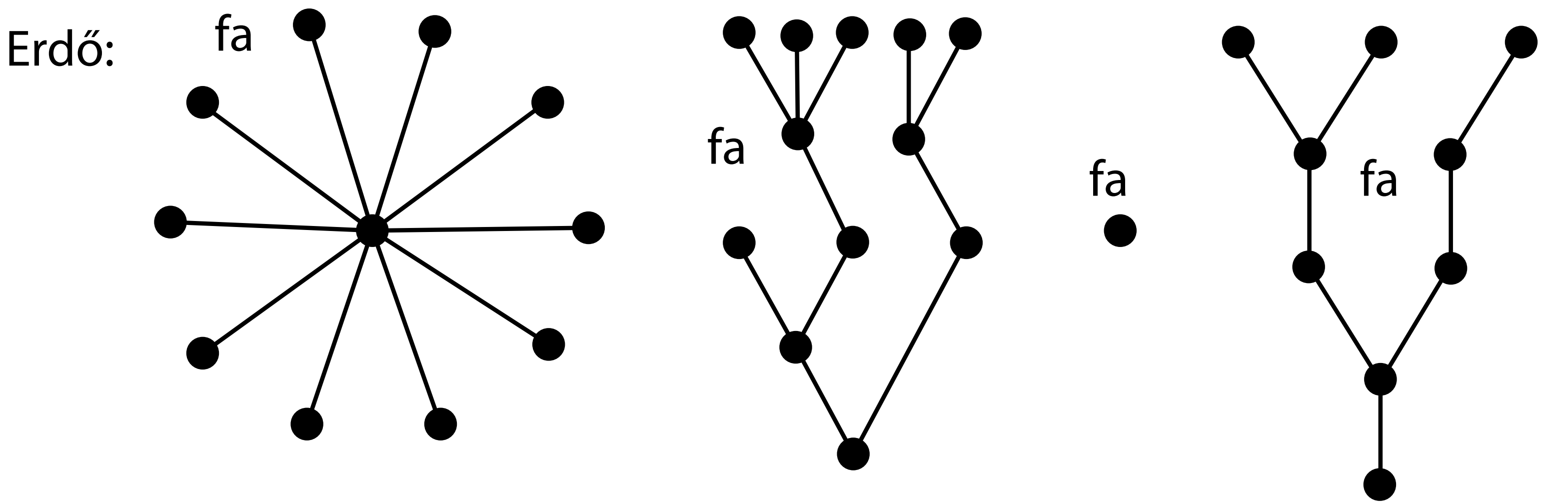
38. Tétel. *Ha a G véges egyszerű gráfban bármely szögpont foka legalább fele a szögpontok számának, akkor G-ben van Hamilton-kör.*

Fák és erdők

Definíció: Az egyszerű körmentes összefüggő gráfokat **fáknak** nevezzük.

Fák és erdők

Definíció: Az egyszerű körmentes összefüggő gráfokat **fáknak** nevezzük. **Erdőnek** nevezzük az olyan gráfokat, amelyeknek összefüggő komponensei fák.



A vizsga feltétele: 20 pont a gyakorlaton!

Egy gráfot **minimális összefüggőnek** nevezünk, ha összefüggő, de bármely élét elhagyva már nem összefüggő.

Egy gráfot **minimális összefüggőnek** nevezünk, ha összefüggő, de bármely élét elhagyva már nem összefüggő. **Maximális körmentesnek** nevezzük, ha nincs benne kör (=zárt út ≥ 2), de bármely új élet hozzávéve lesz benne kör.

Egy gráfot **minimális összefüggőnek** nevezünk, ha összefüggő, de bármely élét elhagyva már nem összefüggő. **Maximális körmentesnek** nevezzük, ha nincs benne kör (=zárt út ≥ 2), de bármely új élet hozzávéve lesz benne kör.

39. Tétel. *Legyen G egy véges, n-szögpontú egyszerű gráf.* **Az alábbi öt feltétel ekvivalens:**

(1) G **fa** *(azaz körmentes és összefüggő).*

39. Tétel. *Legyen G egy véges, n-szögpontú egyszerű gráf.* **Az alábbi öt feltétel ekvivalens:**

(1) G **fa** *(azaz körmentes és összefüggő).*

(2) G **minimális összefüggő gráf.**

39. Tétel. *Legyen G egy véges, n-szögpontú egyszerű gráf.* **Az alábbi öt feltétel ekvivalens:**

(1) G **fa** *(azaz körmentes és összefüggő).*

(2) G **minimális összefüggő gráf.**

(3) G **maximális körmentes gráf.**

39. Tétel. *Legyen G egy véges, n-szögpontú egyszerű gráf.* **Az alábbi öt feltétel ekvivalens:**

(1) G **fa** *(azaz körmentes és összefüggő).*

(2) G **minimális összefüggő gráf.**

(3) G **maximális körmentes gráf.**

(4) G **összefüggő, és eggyel kevesebb éle van, mint csúcsa.**

39. Tétel. *Legyen G egy véges, n-szögpontú egyszerű gráf.* **Az alábbi öt feltétel ekvivalens:**

(1) G **fa** *(azaz körmentes és összefüggő).*

(2) G **minimális összefüggő gráf.**

(3) G **maximális körmentes gráf.**

(4) G **összefüggő, és eggyel kevesebb éle van, mint csúcsa.**

(5) G **körmentes, és eggyel kevesebb éle van, mint csúcsa.**

39. Tétel. *Legyen G egy véges, n-szögpontú egyszerű gráf.* **Az alábbi öt feltétel ekvivalens:**

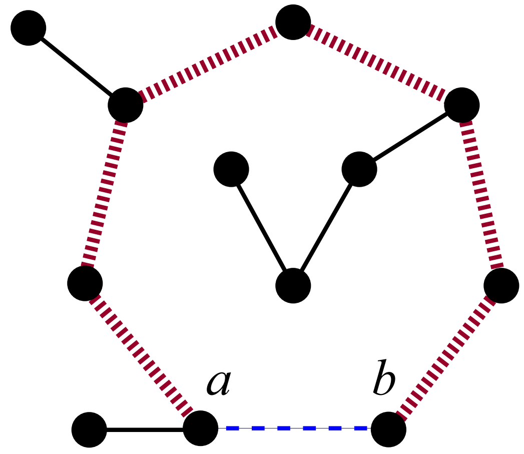
(1) G **fa** *(azaz körmentes és összefüggő).*

(2) G **minimális összefüggő gráf.**

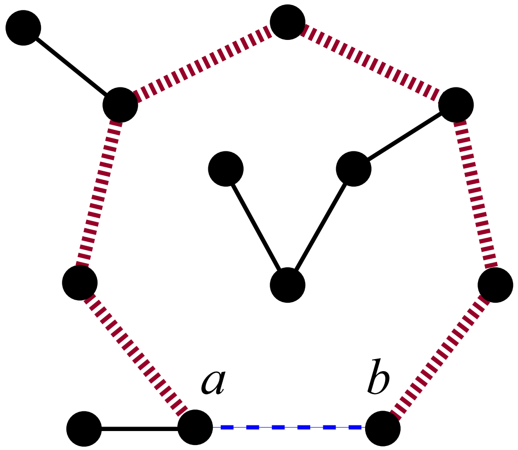
(3) G **maximális körmentes gráf.**

(4) G **összefüggő, és eggyel kevesebb éle van, mint csúcsa.**

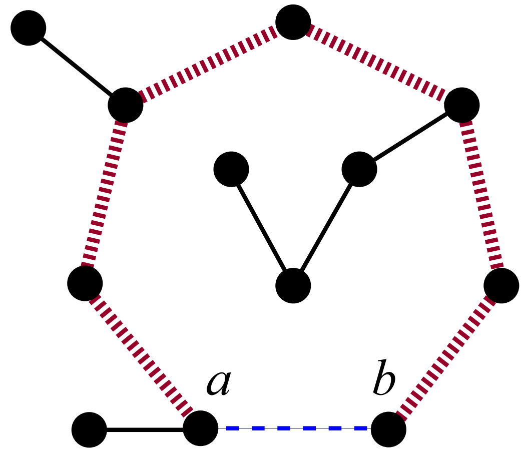
(5) G **körmentes, és eggyel kevesebb éle van, mint csúcsa.**



Bizonyítás: (1: fa) $\Longrightarrow$ (2: min.öfgő): Indirekt.



Bizonyítás: (1: fa) $\Longrightarrow$ (2: min.öfgő): Indirekt. Ekkor G-nek valamely (a, b) élét elhagyva még mindig összefüggő: G'.



Bizonyítás: (1: fa) $\Longrightarrow$ (2: min.öfgő): Indirekt. Ekkor G-nek valamely (a, b) élét elhagyva még mindig összefüggő: G'. G'-ben van út a-ból b-be; ehhez az elhagyott (a, b) élet visszatéve kört kapunk G-ben, ellentmondás.

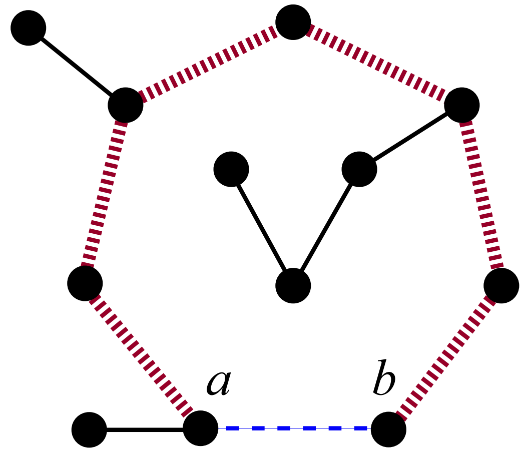
(2: min.öfgő) $\Longrightarrow$ (1: fa):

(2: min.öfgő) $\Longrightarrow$ (1: fa): Indirekt. Ha G nem fa, akkor öfgő és van benne kör.

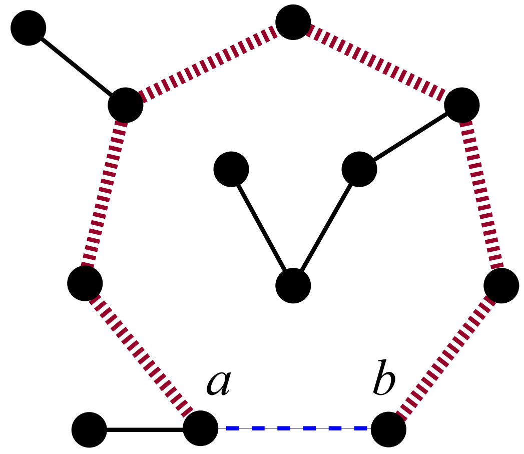
(2: min.öfgő) $\Longrightarrow$ (1: fa): Indirekt. Ha G nem fa, akkor öfgő és van benne kör. A kör tetszőleges (a, b) élét hagyjuk el!

(2: min.öfgő) $\Longrightarrow$ (1: fa): Indirekt. Ha G nem fa, akkor öfgő és van benne kör. A kör tetszőleges (a, b) élét hagyjuk el! Továbbra is öfgő marad, hiszen az eddigi (a, b)-t tartalmazó utak helyett van másik, kerülő út, hiszen a-ból b-be a "kör hosszabbik ívén"

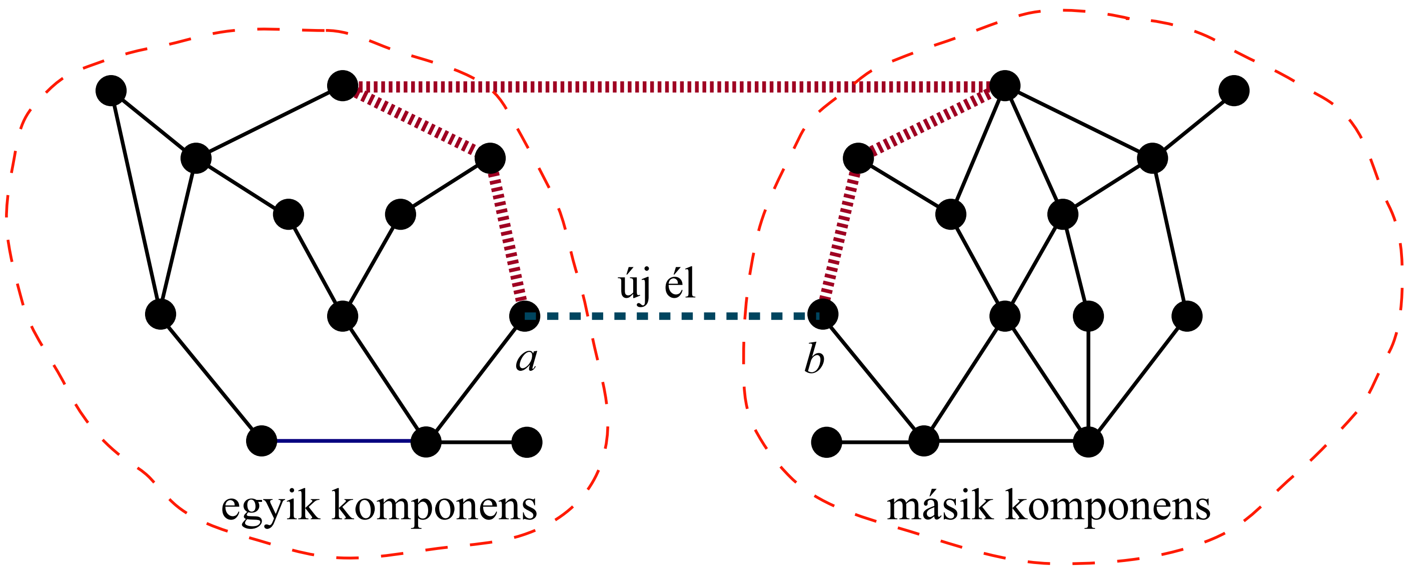
(2: min.öfgő) $\Longrightarrow$ (1: fa): Indirekt. Ha G nem fa, akkor öfgő és van benne kör. A kör tetszőleges (a, b) élét hagyjuk el! Továbbra is öfgő marad, hiszen az eddigi (a, b)-t tartalmazó utak helyett van másik, kerülő út, hiszen a-ból b-be a ''kör hosszabbik ívén'' (azaz $\geq$) is mehetünk. Ez viszont ellentmond annak, hogy *minimális* öfgő. Tehát (1:fa) $\iff$ (2:min.öfgő).



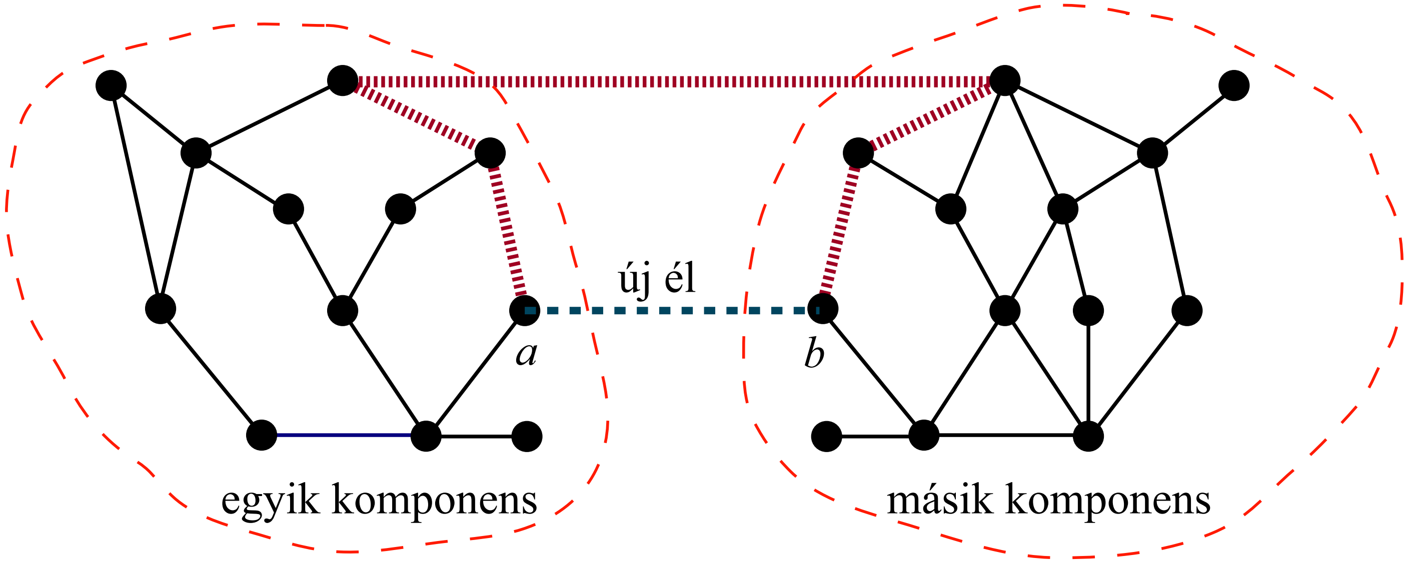
(1:fa) $\Longrightarrow$ (3:max.körm):



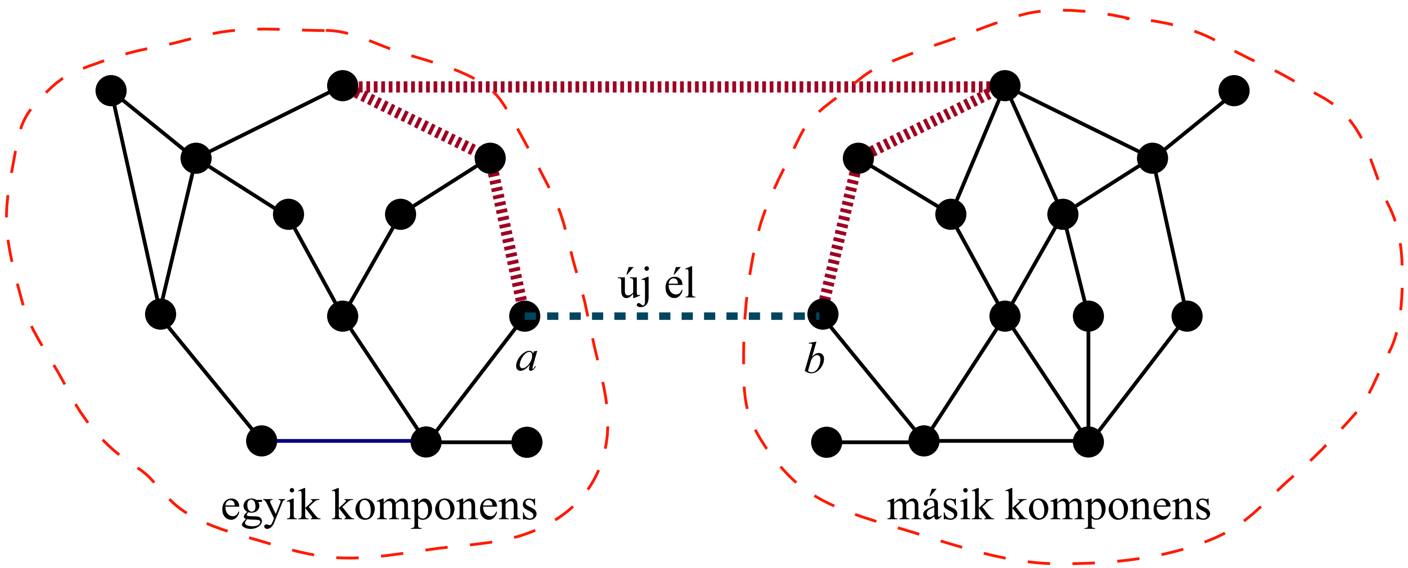
(1:fa) $\Longrightarrow$ (3:max.körm): Tfh. (1). Ekkor G öfgő és körm. Legyen $(a, b) \in A^2 \setminus \rho$ tetszőleges. Ha az (a, b) élet hozzávesszük, akkor lesz kör, hiszen volt út a és b között, amelyet (a, b) körré egészít ki. Ellentmondás. Tehát G max.körm.



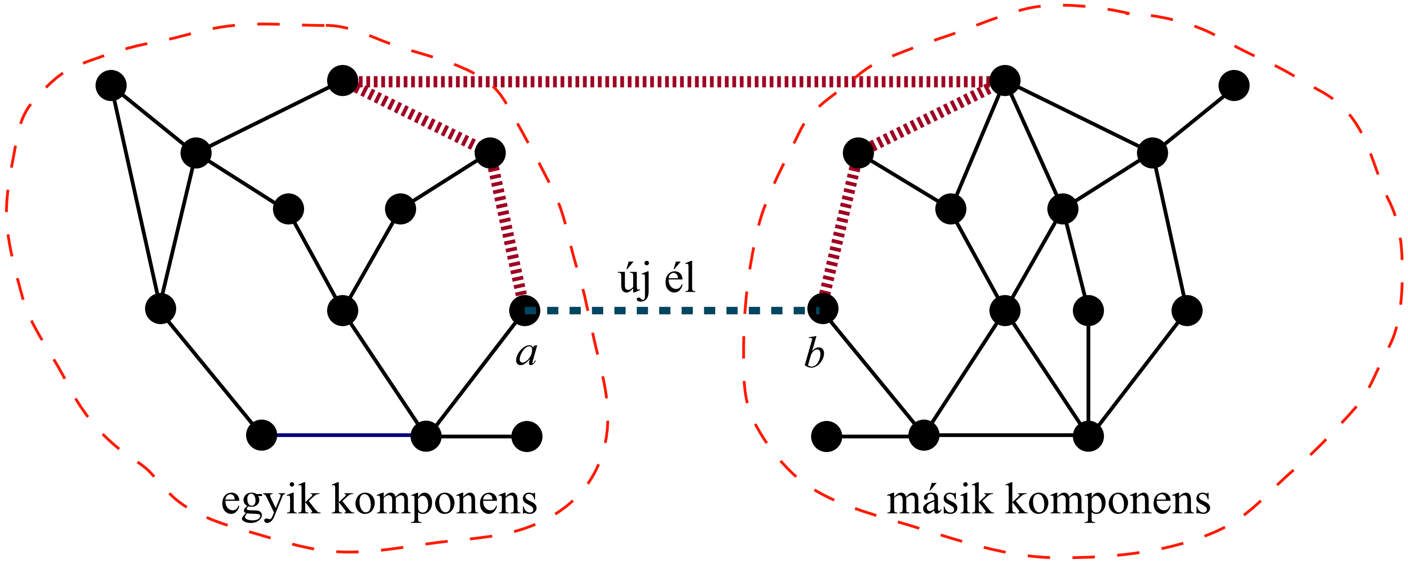
(3:max.körm) $\Longrightarrow$ (1:fa): Tfh. (3). Indirek tfh. $\neg$(3). Ekkor legyen a és b különböző komponensekből. Az



(3:max.körm) $\Longrightarrow$ (1:fa): Tfh. (3). Indirek tfh. $\neg$(3). Ekkor legyen a és b különböző komponensekből. Az (a, b) élet G-hez adva kapjuk G'-t.



(3:max.körm) $\Longrightarrow$ (1:fa): Tfh. (3). Indirek tfh. $\neg$(3). Ekkor legyen a és b különböző komponensekből. Az (a, b) élet G-hez adva kapjuk G'-t. Áll.: G' még mindig körmentes (és ez ellentmondás).



(3:max.körm) $\Longrightarrow$ (1:fa): Tfh. (3). Indirek tfh. $\neg$(3). Ekkor legyen a és b különböző komponensekből. Az (a, b) élet G-hez adva kapjuk G'-t. Áll.: G' még mindig körmentes (és ez ellentmondás). Hiszen ha lenne benne kör, az tartalmazná az új élet, de a kör ezen kívüli íve két különböző komponens között menne, ami lehetetlen (ld. fenti ábra). Tehát (3) $\Longrightarrow$ (1).

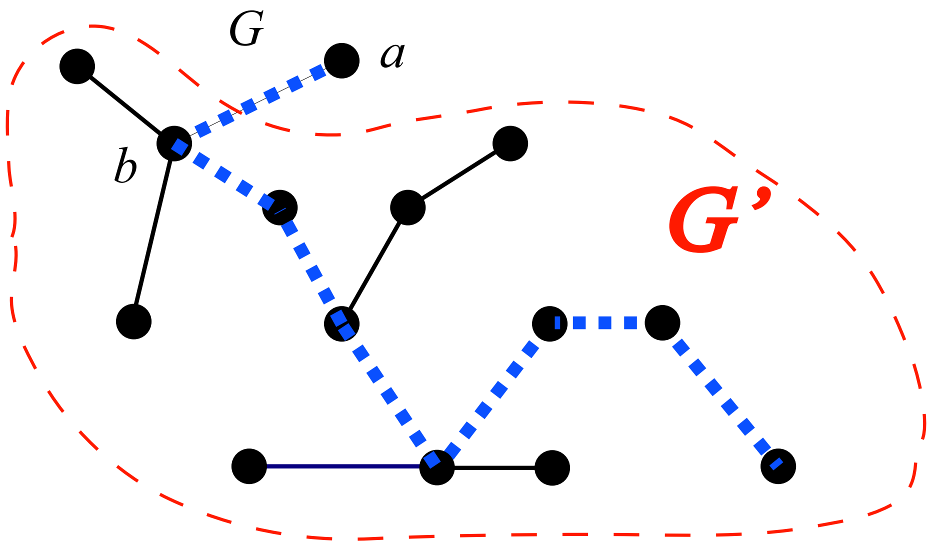
Láttuk, hogy (1:fa) $\iff$ (2:min.öfgő) $\iff$ (3:max.körm.).

Láttuk, hogy (1:fa) $\iff$ (2:min.öfgő) $\iff$ (3:max.körm.).

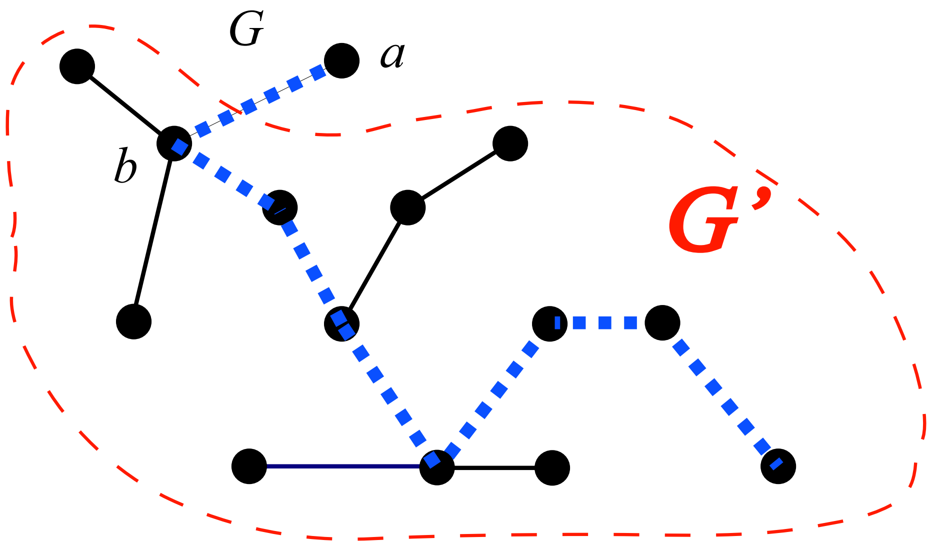
Az (1:fa), (4:öfgő $n-1$) és (5:körm $n-1$) ekvivalenciáját n szerinti teljes indukcióval biz. $n=1$: stimmel.

Láttuk, hogy (1:fa) $\iff$ (2:min.öfgő) $\iff$ (3:max.körm.).

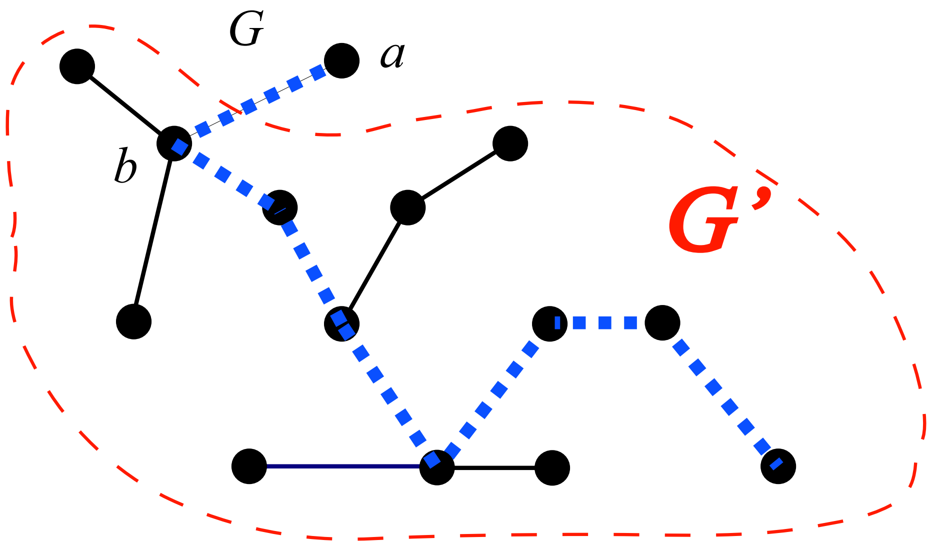
Az (1:fa), (4:öfgő $n-1$) és (5:körm $n-1$) ekvivalenciáját n szerinti teljes indukcióval biz. $n=1$: stimmel. Legyen $n>1$.



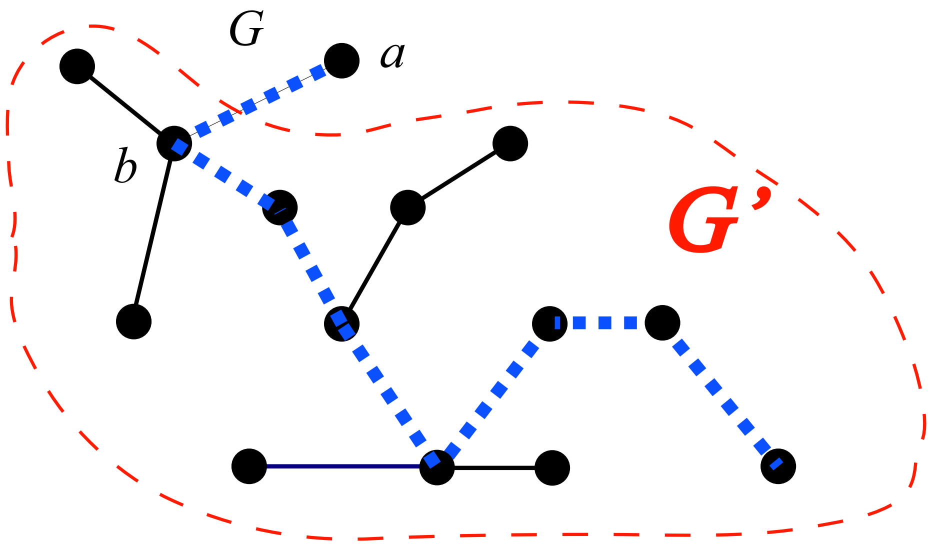
Áll.: (1), (4) és (5) bármelyikét tesszük fel, van (legalább kettő) elsőfokú szögpont.



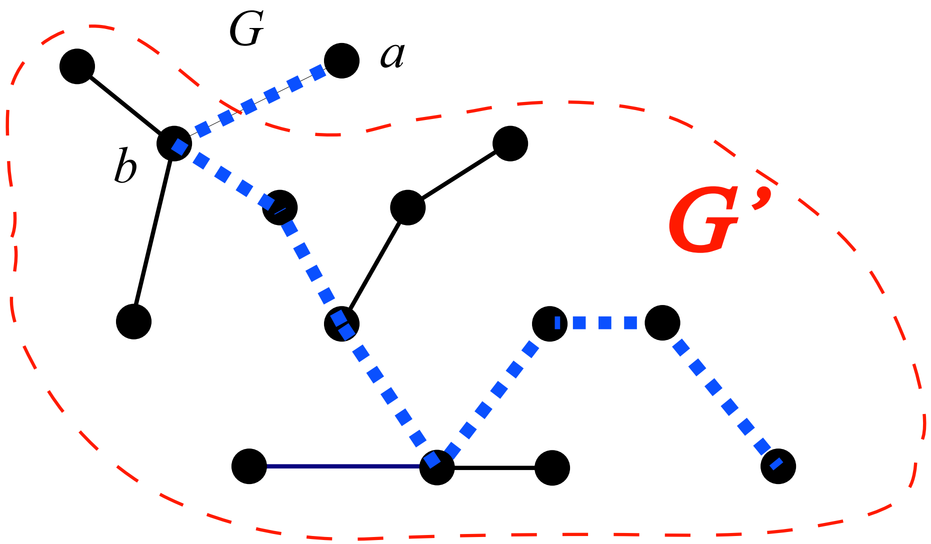
Áll.: (1), (4) és (5) bármelyikét tesszük fel, van (legalább kettő) elsőfokú szögpont. (1:fa) esetén: az (egyik) leghosszabb út végpontja.



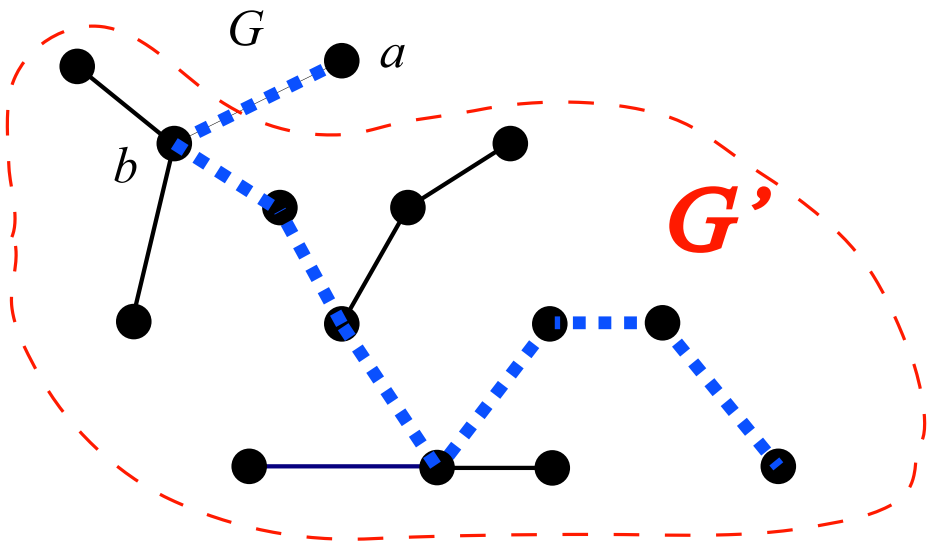
Áll.: (1), (4) és (5) bármelyikét tesszük fel, van (legalább kettő) elsőfokú szögpont. (1:fa) esetén: az (egyik) leghosszabb út végpontja. (4:öfgő $n-1$) vagy (5:körm $n-1$) esetén:



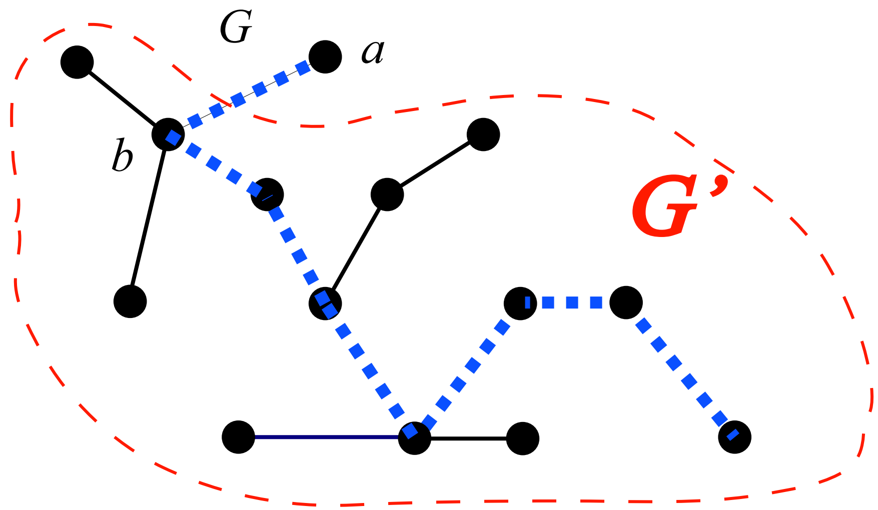
Áll.: (1), (4) és (5) bármelyikét tesszük fel, van (legalább kettő) elsőfokú szögpont. (1:fa) esetén: az (egyik) leghosszabb út végpontja. (4:öfgő $n-1$) vagy (5:körm $n-1$) esetén: ha minden szögpont foka ≥ 2 lenne, akkor



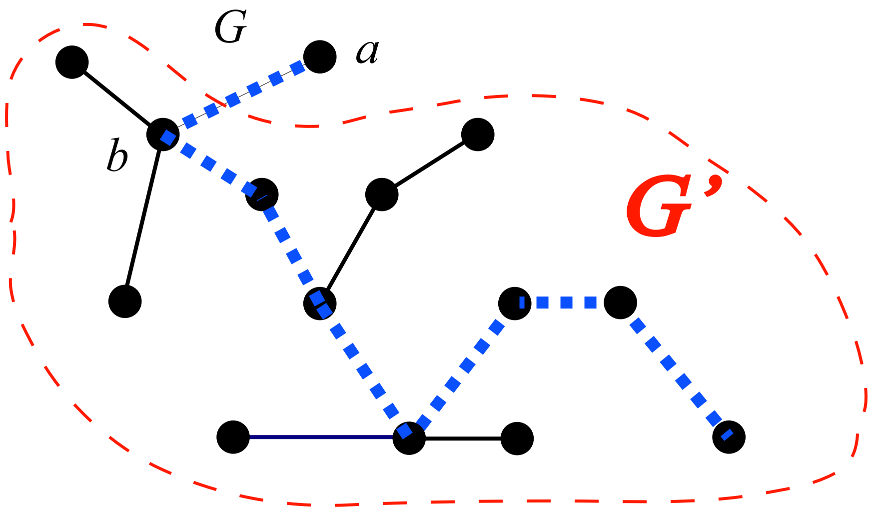
Áll.: (1), (4) és (5) bármelyikét tesszük fel, van (legalább kettő) elsőfokú szögpont. (1:fa) esetén: az (egyik) leghosszabb út végpontja. (4:öfgő $n-1$) vagy (5:körm $n-1$) esetén: ha minden szögpont foka ≥ 2 lenne, akkor a fokok összege $\geq 2n \neq 2(n-1) =$ $2\cdot$ élek száma, ami ellentmondás lenne.



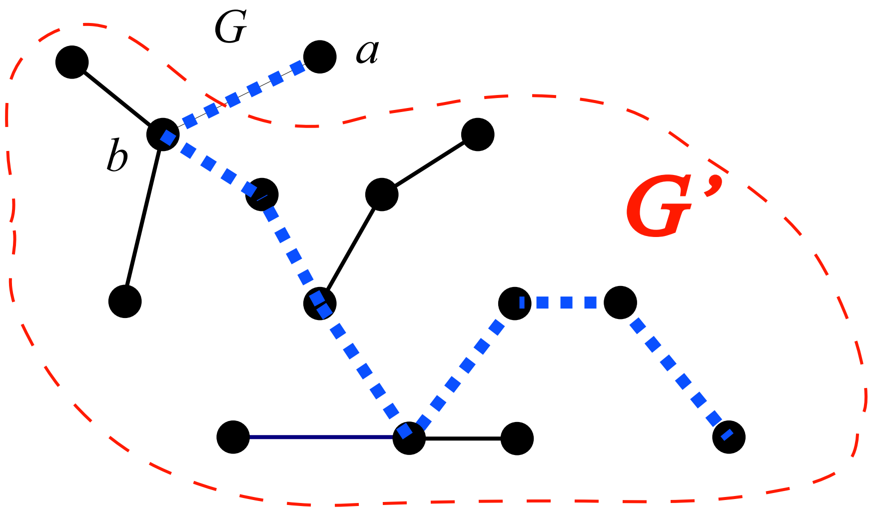
Legyen a egy elsőfokú szögpont! a-t és a belőle induló egyetlen élet elhagyva kapjuk G'-t.



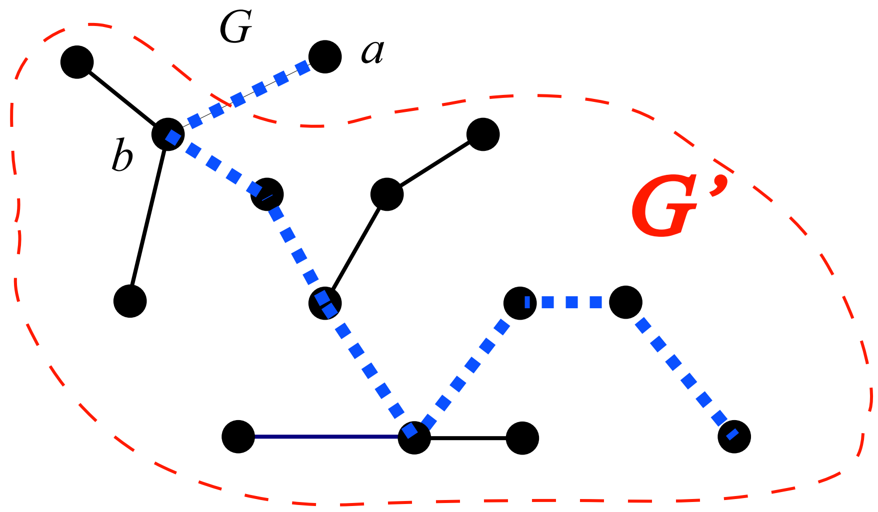
G pontosan akkor fa, ha G' fa! Hiszen egyrészt körmentességük ekvivalens (a-n nem mehet át kör, mert az (a, b) él "zsákutca".)



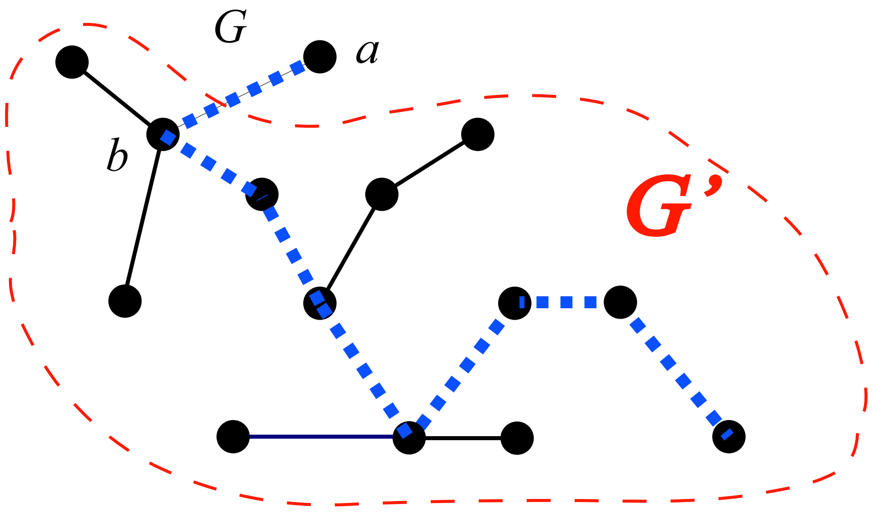
G pontosan akkor fa, ha G' fa! Hiszen egyrészt körmentességük ekvivalens (a-n nem mehet át kör, mert az (a, b) él "zsákutca".) Ha G öfgő, akkor G' is, hiszen ha $c, d \in G'$, akkor közöttük G-ben van út, de az elkerüli az említett zsákutcát, tehát G'-beli út.



G pontosan akkor fa, ha G' fa! Hiszen egyrészt körmentességük ekvivalens (a-n nem mehet át kör, mert az (a, b) él "zsákutca".) Ha G öfgő, akkor G' is, hiszen ha $c, d \in G'$, akkor közöttük G-ben van út, de az elkerüli az említett zsákutcát, tehát G'-beli út. Ha pedig G' összefüggő, akkor nyilván G is.



G-re pontosan akkor teljesül a (4:öfgő és él=csúcs−1) feltétel, ha G'-re teljesül. Hiszen az összefüggőség ekvivalenciáját láttuk. Másrészt az élek száma is és a csúcsok száma is eggyel változik.



G-re pontosan akkor teljesül az (5:körm. és él=csúcs–1) feltétel, ha G'-re teljesül. Ugyanis ha G körmentes, akkor — részgráf lévén — G' is az. Másrészt a-n (elsőfokú lévén) nem mehet át G-beli kör, ha tehát G' körmentes, akkor G is az. Most is az élek száma is és a csúcsok száma is eggyel változik.

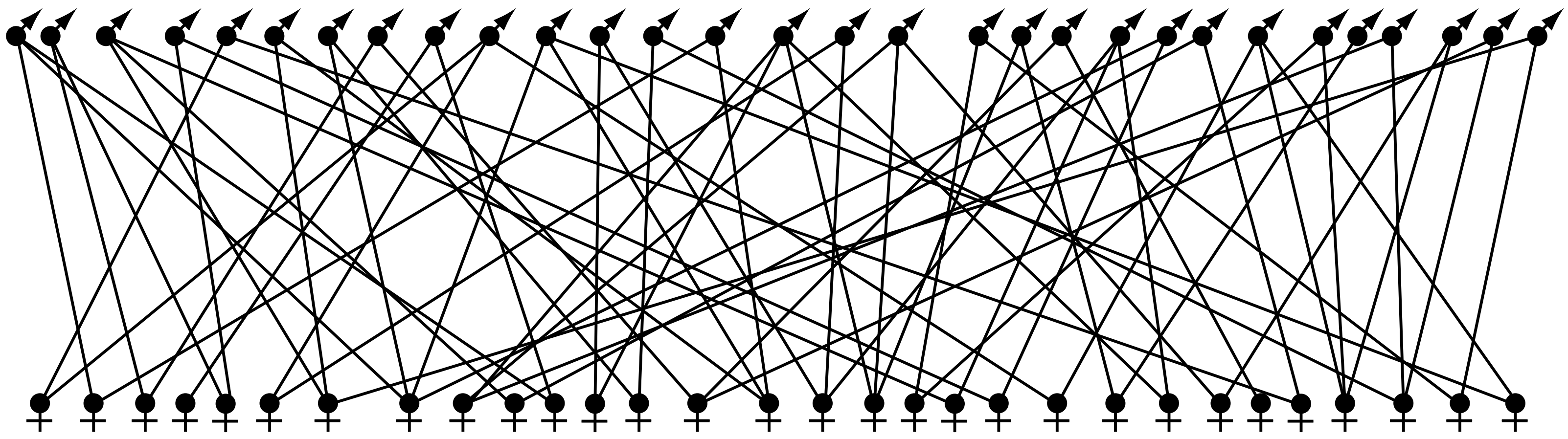
Az eddigiek szerint (1), (4) és (5) ekvivalenciája teljes indukcióval azonnal adódik: $n = 1$-re evidens, és ezen feltételek bármelyike ekvivalens G'-re és G-re; mivel G'-re az ind. hip. szerint egymással ekvivalensek, ezért G-re is egymással ekvivalensek. Q.e.d.

Következmény: **Véges, egynél többelemű fában legalább két elsőfokú pont van.**

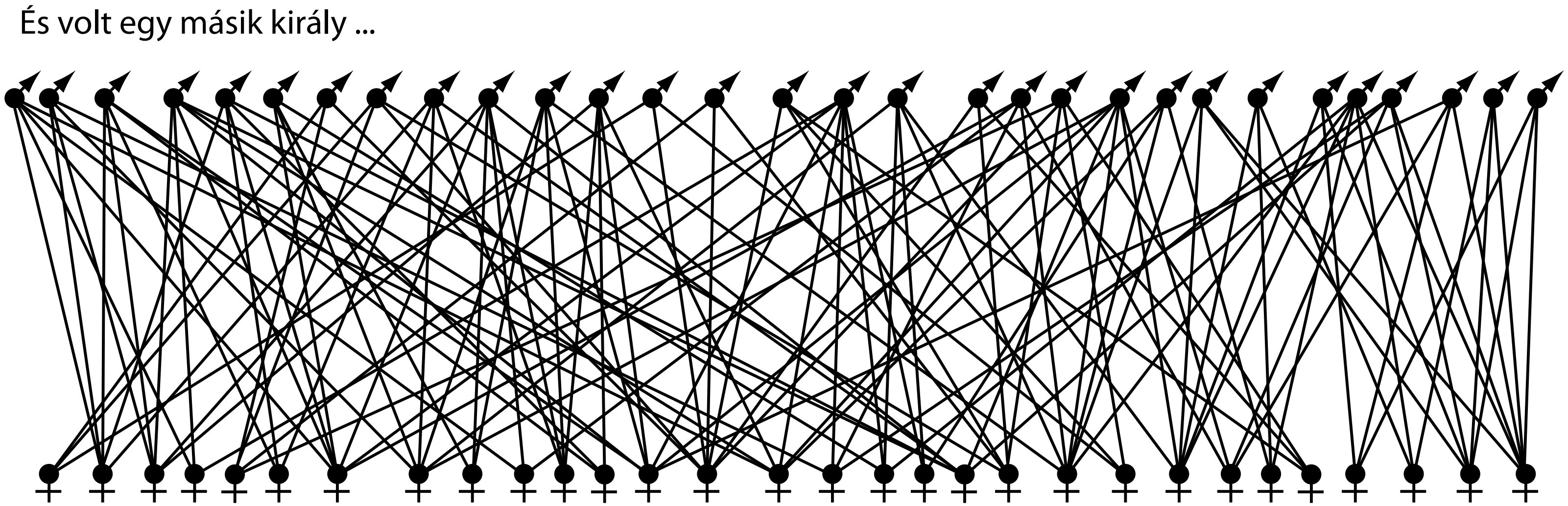
Ezt menet közben láttuk: bármelyik leghosszabb út két végpontja elsőfokú pont.

Páros gráfok

Volt egyszer egy király ...



és az udvarában 30 lovag és 30 udvarhölgy. Közöttük a kölcsönös szimpátiát mint relációt a fenti gráf adja meg. Ezt figyelembe véve akarta a király az udvarhölgyeket, mind a harmicat, a lovagokkal összeházasítani. Sikerülhetett ez?



és a feladat meg a kérdés ugyanaz.

A feladatot — mindkét királyi udvarban — a kancellár kapta. A lehetőségek száma:

$30! = 265252859812191058636308480000000 = 2,65 \cdot 10^{32}$.

Ha másodpercenként 10^9 lehetőséget ellenőrzünk (1 GHz $= 10^9$ művelet/secundum), akkor az összes lehetőség végignézéséhez $8,4 \cdot 10^{15}$ évre lenne szükség. (A Naprendszer $4,5 \cdot 10^9$ éves.)

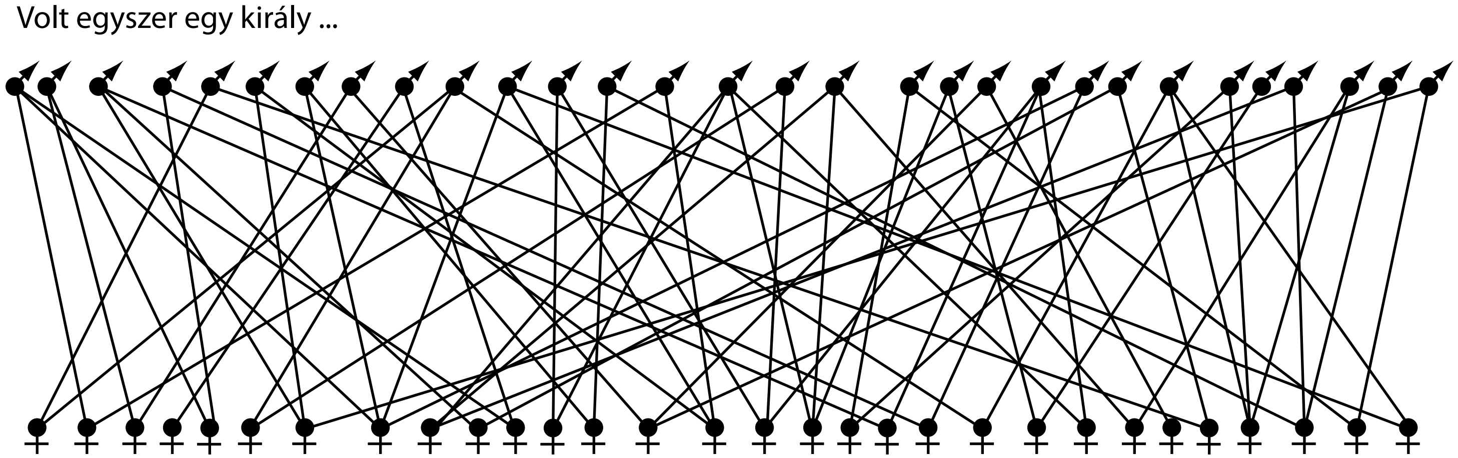
Mindkét kancellár megbukott.

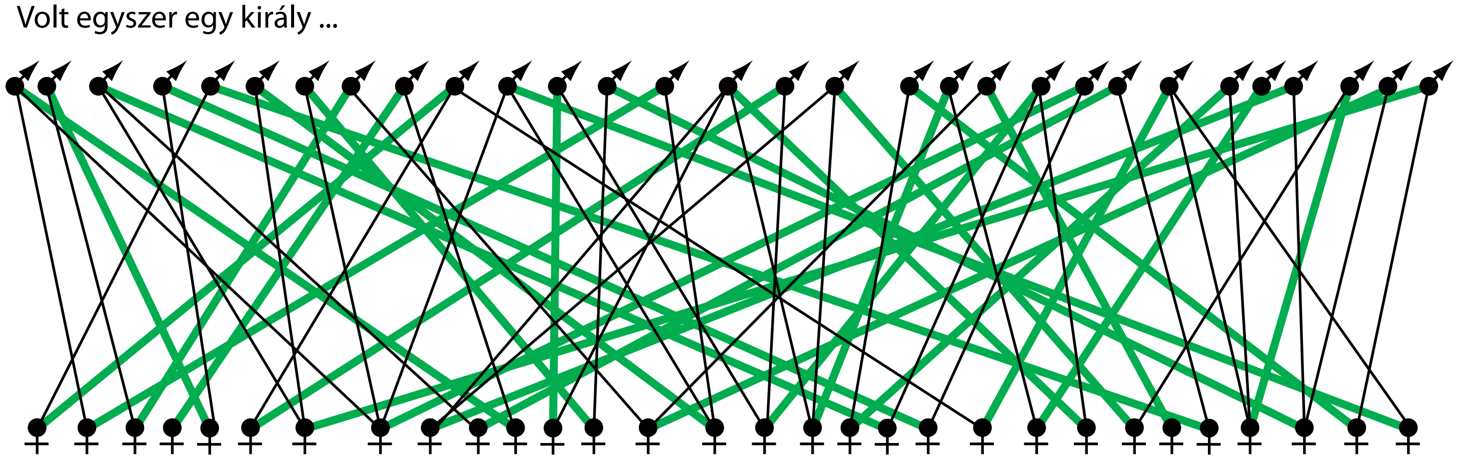
Mindkét kancellár megbukott. Az egyik azért, mert lett volna megoldás (azaz alkalmas párosítás), de idő híján nem találta meg.

Mindkét kancellár megbukott. Az egyik azért, mert lett volna megoldás (azaz alkalmas párosítás), de idő híján nem találta meg. A másik azért, mert — sok-sok számítógéppel — meglepő módon mégiscsak sikerült az összes lehetőséget végignézetnie, de ez nem győzte meg a királyt. De bukásuk fő oka:

Mindkét kancellár megbukott. Az egyik azért, mert lett volna megoldás (azaz alkalmas párosítás), de idő híján nem találta meg. A másik azért, mert — sok-sok számítógéppel — meglepő módon mégiscsak sikerült az összes lehetőséget végignézetnie, de ez nem győzte meg a királyt. De bukásuk fő oka: a diszkrét matematika tudásuk hiányossága!

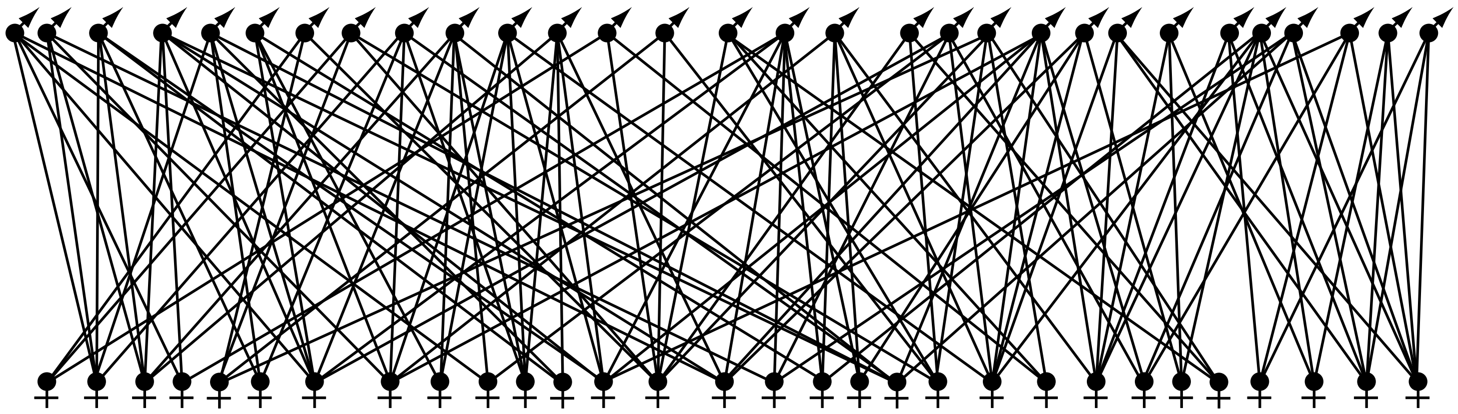
Mindkét kancellár megbukott. Az egyik azért, mert lett volna megoldás (azaz alkalmas párosítás), de idő híján nem találta meg. A másik azért, mert — sok-sok számítógéppel — meglepő módon mégiscsak sikerült az összes lehetőséget végignézetnie, de ez nem győzte meg a királyt. De bukásuk fő oka: a diszkrét matematika tudásuk hiányossága! Lássuk a megoldást (pontosabban szólva: az eredményközlést):



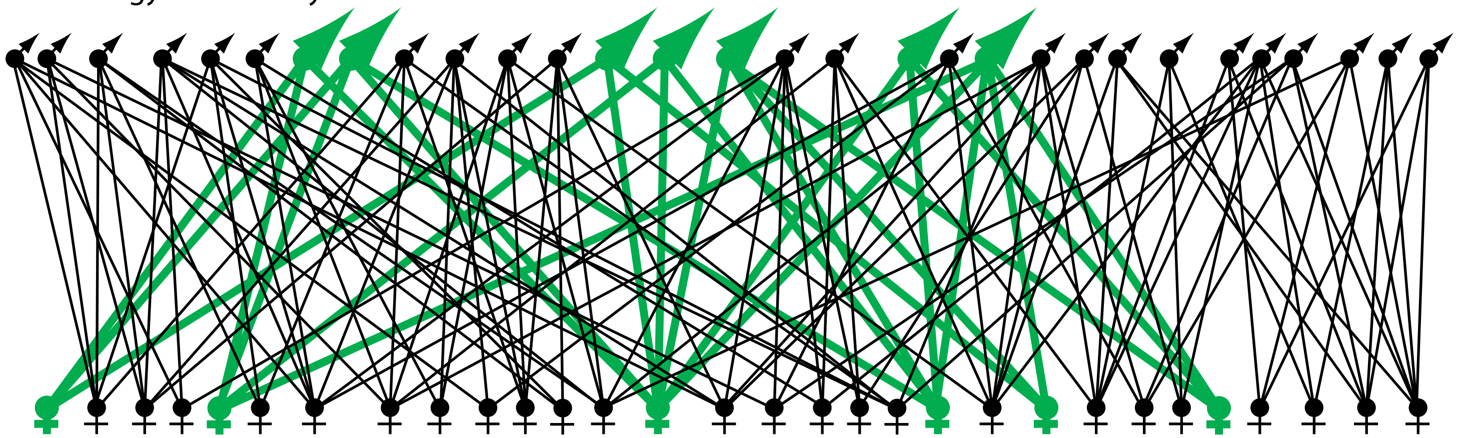


A vizsga feltétele: 20 pont a gyakorlaton!

És volt egy másik király ...



És volt egy másik király ...



A vizsga feltétele: 20 pont a gyakorlaton!

Tehát az első esetben van párosítás (a vastag zöld élek jelölik). A második esetben pedig van hét lovag és hat udvarhölgy (a zöld megnagyobbított szögpontok jelölik ezeket) úgy, hogy a hét lovag mindegyike csakis ezen hat udvarhölgy valamelyikével, és a hat udvarhölgy mindegyike csakis ezen hét lovag valamelyikével házasítható össze, és ez nyilván lehetetlen.

Definíció: Legyen $G = (V, E)$ egy (irányítatlan, hurokélmentes) gráf. Ha V az A és B részhalmazainak diszkjunkt uniója és bármely él egyik végpontja A-ban, a másik pedig B-ben van, akkor azt mondjuk, hogy G **páros gráf** (az A, B pontosztályokkal).

Definíció: Legyen $G = (V, E)$ egy (irányítatlan, hurokélmentes) gráf. Ha V az A és B részhalmazainak diszkjunkt uniója és bármely él egyik végpontja A-ban, a másik pedig B-ben van, akkor azt mondjuk, hogy G **páros gráf** (az A, B pontosztályokkal).

40. Tétel. *Legyen $G = (V, E)$ egy (irányítatlan, hurokélmentes) gráf. G* **páros gráf** $\iff$ *nincs benne* **páratlan** *hosszúságú kör.*

Bizonyítás Ha G páros gráf, akkor — mivel az élek csak A és B között mehetnek — tetszőleges kör szögpontjai

Bizonyítás Ha G páros gráf, akkor — mivel az élek csak A és B között mehetnek — tetszőleges kör szögpontjai **felváltva** A-, illetve B-beliek, ezért

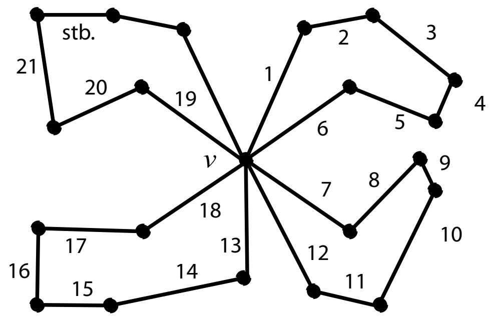
Bizonyítás Ha G páros gráf, akkor — mivel az élek csak A és B között mehetnek — tetszőleges kör szögpontjai **felváltva** A-, illetve B-beliek, ezért csak páros lépesben juthatunk vissza a kiindulási pontba, tehát tetszőleges kör páros hosszúságú.

Bizonyítás Ha G páros gráf, akkor — mivel az élek csak A és B között mehetnek — tetszőleges kör szögpontjai **felváltva** A-, illetve B-beliek, ezért csak páros lépesben juthatunk vissza a kiindulási pontba, tehát tetszőleges kör páros hosszúságú.

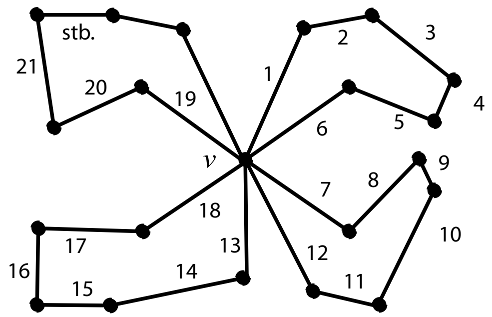
Fordítva, most tegyük fel, hogy tetszőleges G-beli kör páros hosszúságú.

Bizonyítás Ha G páros gráf, akkor — mivel az élek csak A és B között mehetnek — tetszőleges kör szögpontjai **felváltva** A-, illetve B-beliek, ezért csak páros lépesben juthatunk vissza a kiindulási pontba, tehát tetszőleges kör páros hosszúságú.

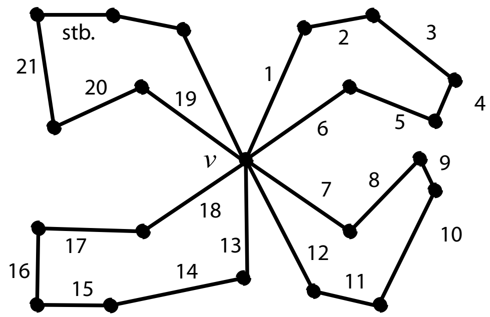
Fordítva, most tegyük fel, hogy tetszőleges G-beli kör páros hosszúságú. Elég belátni, hogy G összefüggő komponensei páros gráfok, mert akkor G is páros gráf. Ezért feltehetjük, hogy G összefüggő.



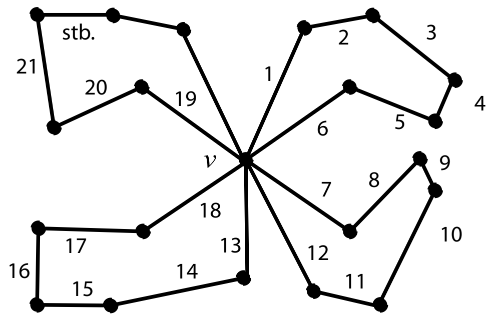
Állítjuk, hogy G-ben minden zárt séta páros hosszúságú.



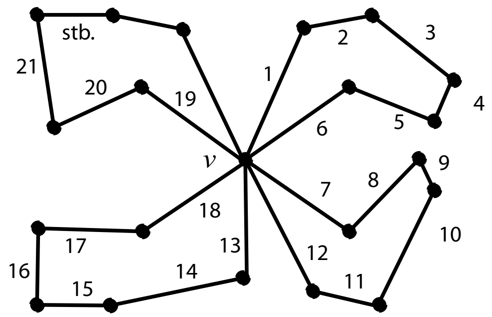
Állítjuk, hogy G-ben minden zárt séta páros hosszúságú. Ellenkező esetben van **legrövidebb** páratlan hosszúságú zárt séta:



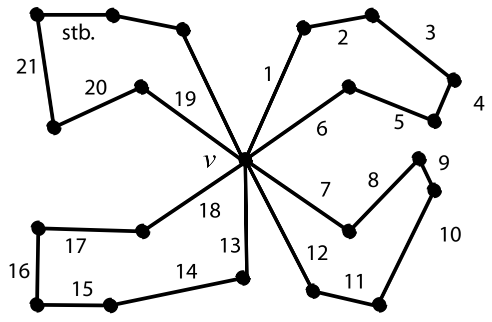
Állítjuk, hogy G-ben minden zárt séta páros hosszúságú. Ellenkező esetben van **legrövidebb** páratlan hosszúságú zárt séta: L.



Állítjuk, hogy G-ben minden zárt séta páros hosszúságú. Ellenkező esetben van **legrövidebb** páratlan hosszúságú zárt séta: L. A feltevés miatt ez nem kör, tehát valamely v szögponton többször is átmegy. A v pont a sétát több (az ábrán pl. négy) rövidebb zárt sétára bontja,



Állítjuk, hogy G-ben minden zárt séta páros hosszúságú. Ellenkező esetben van **legrövidebb** páratlan hosszúságú zárt séta: L. A feltevés miatt ez nem kör, tehát valamely v szögponton többször is átmegy. A v pont a sétát több (az ábrán pl. négy) rövidebb zárt sétára bontja, amelyek L-nél rövidebbek lévén páros hosszúságúak.



Állítjuk, hogy G-ben minden zárt séta páros hosszúságú. Ellenkező esetben van **legrövidebb** páratlan hosszúságú zárt séta: L. A feltevés miatt ez nem kör, tehát valamely v szögponton többször is átmegy. A v pont a sétát több (az ábrán pl. négy) rövidebb zárt sétára bontja, amelyek L-nél rövidebbek lévén páros hosszúságúak. Ezért (páros számok összegeként) L hossza is páros, és ez ellentmond a feltevésnek.

Mármost legyen v egy rögzített szögpont. Legyen A azon szögpontok halmaza, amelyekbe v-ből páros hosszúságú séta vezet, B pedig azon szögpontok halmaza, amelyekbe páratlan hosszúságú sétával juthatunk el v-ből. (Megengedett a 0 hosszúságú séta is, tehát $v \in A$.)

Mármost legyen v egy rögzített szögpont. Legyen A azon szögpontok halmaza, amelyekbe v-ből páros hosszúságú séta vezet, B pedig azon szögpontok halmaza, amelyekbe páratlan hosszúságú sétával juthatunk el v-ből. (Megengedett a 0 hosszúságú séta is, tehát $v \in A$.)

Mivel G összefüggő, $A \cup B = V$. Másrészt

Mármost legyen v egy rögzített szögpont. Legyen A azon szögpontok halmaza, amelyekbe v-ből páros hosszúságú séta vezet, B pedig azon szögpontok halmaza, amelyekbe páratlan hosszúságú sétával juthatunk el v-ből. (Megengedett a 0 hosszúságú séta is, tehát $v \in A$.)

Mivel G összefüggő, $A \cup B = V$. Másrészt $A \cap B = \emptyset$,

Mármost legyen v egy rögzített szögpont. Legyen A azon szögpontok halmaza, amelyekbe v-ből páros hosszúságú séta vezet, B pedig azon szögpontok halmaza, amelyekbe páratlan hosszúságú sétával juthatunk el v-ből. (Megengedett a 0 hosszúságú séta is, tehát $v \in A$.)

Mivel G összefüggő, $A \cup B = V$. Másrészt $A \cap B = \emptyset$, hiszen ha létezne közös elemük, mondjuk $u \in A \cap B$, akkor

Mármost legyen v egy rögzített szögpont. Legyen A azon szögpontok halmaza, amelyekbe v-ből páros hosszúságú séta vezet, B pedig azon szögpontok halmaza, amelyekbe páratlan hosszúságú sétával juthatunk el v-ből. (Megengedett a 0 hosszúságú séta is, tehát $v \in A$.)

Mivel G összefüggő, $A \cup B = V$. Másrészt $A \cap B = \emptyset$, hiszen ha létezne közös elemük, mondjuk $u \in A \cap B$, akkor lenne páros séta is v-ből u-ba, és lenne páratlan is, és a két séta uniója egy páratlan hosszúságú zárt séta lenne, ami ellentmondás. Q.e.d.

Definíció: A továbbiakban **csak véges** gráfokat tekintünk! Legyen $G = (V, E)$ hurokmentes gráf. Ha $M \subseteq E$ és az M-beli élek **idegenek**, azaz bármely két M-beli élnek nincs közös végpontja, akkor az M élhalmazt **párosításnak** nevezzük.

Definíció: A továbbiakban **csak véges** gráfokat tekintünk! Legyen $G = (V, E)$ hurokmentes gráf. Ha $M \subseteq E$ és az M-beli élek **idegenek**, azaz bármely két M-beli élnek nincs közös végpontja, akkor az M élhalmazt **párosításnak** nevezzük. Ha M párosítás és a gráf minden szögpontja valamely M-beli él egyik végpontja, akkor M-et **teljes párosításnak** nevezzük. (Pl.

Definíció: A továbbiakban **csak véges** gráfokat tekintünk! Legyen $G = (V, E)$ hurokmentes gráf. Ha $M \subseteq E$ és az M-beli élek **idegenek**, azaz bármely két M-beli élnek nincs közös végpontja, akkor az M élhalmazt **párosításnak** nevezzük. Ha M párosítás és a gráf minden szögpontja valamely M-beli él egyik végpontja, akkor M-et **teljes párosításnak** nevezzük. (Pl. a lovagok és udvarhölgyek esetén a kérdés az, hogy van-e teljes párosítás, és azt hogy lehet megtalálni.)

Definíció: A továbbiakban **csak véges** gráfokat tekintünk! Legyen $G = (V, E)$ hurokmentes gráf. Ha $M \subseteq E$ és az M-beli élek **idegenek**, azaz bármely két M-beli élnek nincs közös végpontja, akkor az M élhalmazt **párosításnak** nevezzük. Ha M párosítás és a gráf minden szögpontja valamely M-beli él egyik végpontja, akkor M-et **teljes párosításnak** nevezzük. (Pl. a lovagok és udvarhölgyek esetén a kérdés az, hogy van-e teljes párosítás, és azt hogy lehet megtalálni.) Legyen most $S \subseteq V$. Ha minden G-beli élnek legalább az egyik végpontja S-ben van, akkor S-et **lefogó ponthalmaznak** nevezzük.

Definíció: A továbbiakban **csak véges** gráfokat tekintünk! Legyen $G = (V, E)$ hurokmentes gráf. Ha $M \subseteq E$ és az M-beli élek **idegenek**, azaz bármely két M-beli élnek nincs közös végpontja, akkor az M élhalmazt **párosításnak** nevezzük. Ha M párosítás és a gráf minden szögpontja valamely M-beli él egyik végpontja, akkor M-et **teljes párosításnak** nevezzük. (Pl. a lovagok és udvarhölgyek esetén a kérdés az, hogy van-e teljes párosítás, és azt hogy lehet megtalálni.) Legyen most $S \subseteq V$. Ha minden G-beli élnek legalább az egyik végpontja S-ben van, akkor S-et **lefogó ponthalmaznak** nevezzük.

Tétel: Ha a G páros gráfban van teljes párosítás,

Definíció: A továbbiakban **csak véges** gráfokat tekintünk! Legyen $G = (V, E)$ hurokmentes gráf. Ha $M \subseteq E$ és az M-beli élek **idegenek**, azaz bármely két M-beli élnek nincs közös végpontja, akkor az M élhalmazt **párosításnak** nevezzük. Ha M párosítás és a gráf minden szögpontja valamely M-beli él egyik végpontja, akkor M-et **teljes párosításnak** nevezzük. (Pl. a lovagok és udvarhölgyek esetén a kérdés az, hogy van-e teljes párosítás, és azt hogy lehet megtalálni.) Legyen most $S \subseteq V$. Ha minden G-beli élnek legalább az egyik végpontja S-ben van, akkor S-et **lefogó ponthalmaznak** nevezzük.

Tétel: Ha a G páros gráfban van teljes párosítás, akkor a két pontosztály **azonos elemszámú**.

Bizonyítás: A teljes párosítás bijekciót ad a két pontosztály, A és B között. Q.e.d.

Bizonyítás: A teljes párosítás bijekciót ad a két pontosztály, A és B között. Q.e.d.

Jelölje $\nu(G)$ a G-beli párosítások elemszámának maximumát, és

Bizonyítás: A teljes párosítás bijekciót ad a két pontosztály, A és B között. Q.e.d.

Jelölje $\nu(G)$ a G-beli párosítások elemszámának maximumát, és $\tau(G)$ a G-beli lefogó ponthalmazok elemszámának minimuma.

Megjegyzés: párosításnál az "kunszt", ha minél több idegen élet meg tudunk adni, ezért a maximumot tekintjük. Lefogó ponthalmaz esetén az a "nagy kunszt", ha minél kevesebb szögponttal le tudjuk az éleket fogni, ezért a minimumot tekintjük.

41. Tétel. **(Kőnig-tétel)** *Véges páros gráf esetében* $\nu(G) = \tau(G)$.

Bizonyítás (amit jól kell tudni, hiszen ezen alapul majd az algoritmus is). Az evidens, hogy $\nu(G) \leq \tau(G)$:

41. Tétel. (Kőnig-tétel) *Véges páros gráf esetében* $\nu(G) = \tau(G)$.

Bizonyítás (amit jól kell tudni, hiszen ezen alapul majd az algoritmus is). Az evidens, hogy $\nu(G) \leq \tau(G)$: tekintsünk egy $\nu(G)$ elemszámú párosítást, azaz

41. Tétel. (Kőnig-tétel) *Véges páros gráf esetében* $\nu(G) = \tau(G)$.

Bizonyítás (amit jól kell tudni, hiszen ezen alapul majd az algoritmus is). Az evidens, hogy $\nu(G) \leq \tau(G)$: tekintsünk egy $\nu(G)$ elemszámú párosítást, azaz $\nu(G)$ darab egymástól idegen élet. Világos, hogy bármely lefogó ponthalmaz

41. Tétel. **(Kőnig-tétel)** *Véges páros gráf esetében* $\nu(G) = \tau(G)$*.*

Bizonyítás (amit jól kell tudni, hiszen ezen alapul majd az algoritmus is). Az evidens, hogy $\nu(G) \leq \tau(G)$: tekintsünk egy $\nu(G)$ elemszámú párosítást, azaz $\nu(G)$ darab egymástól idegen élet. Világos, hogy bármely lefogó ponthalmaz a tekintett élek bármelyikének legalább az egyik végpontját tartalmazza, tehát legalább

41. Tétel. (Kőnig-tétel) *Véges páros gráf esetében* $\nu(G) = \tau(G)$.

Bizonyítás (amit jól kell tudni, hiszen ezen alapul majd az algoritmus is). Az evidens, hogy $\nu(G) \leq \tau(G)$: tekintsünk egy $\nu(G)$ elemszámú párosítást, azaz $\nu(G)$ darab egymástól idegen élet. Világos, hogy bármely lefogó ponthalmaz a tekintett élek bármelyikének legalább az egyik végpontját tartalmazza, tehát legalább $\nu(G)$ szögpontból áll. Ennélfogva a lefogó ponthalmazok elemszámának minimuma, azaz $\tau(G)$ is legalább $\nu(G)$.

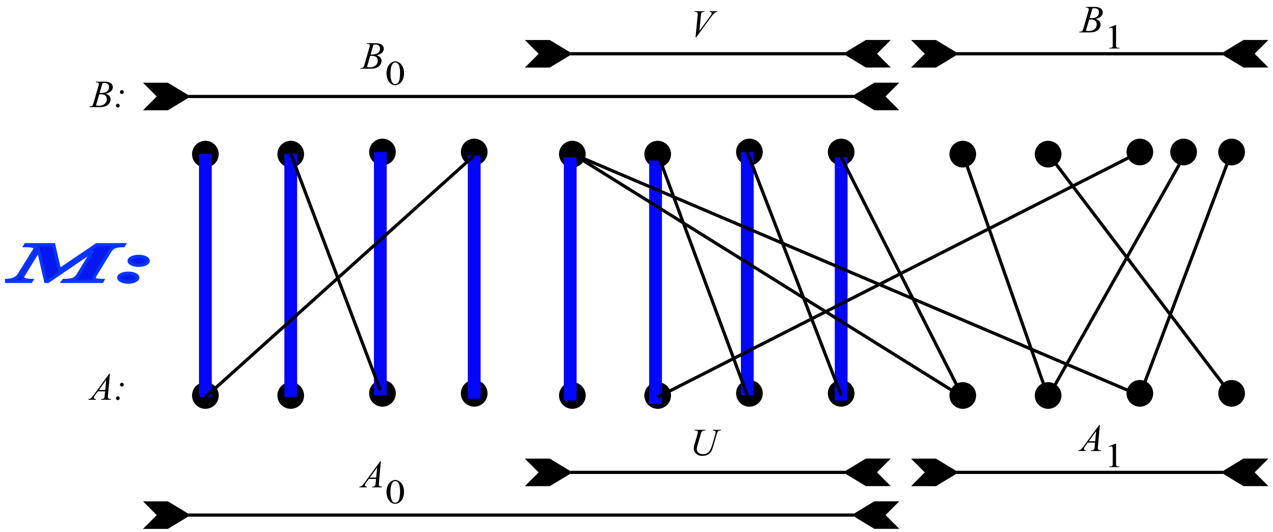
Legyen most M egy tetszőleges párosítás. (M-re vonatkozó) **alternáló útnak** nevezünk egy olyan utat, amelynek élei felváltva M-beliek és nem M-beliek. Pl. minden 1-hosszúságú út ilyen.

Legyen most M egy tetszőleges párosítás. (M-re vonatkozó) **alternáló útnak** nevezünk egy olyan utat, amelynek élei felváltva M-beliek és nem M-beliek. Pl. minden 1-hosszúságú út ilyen.

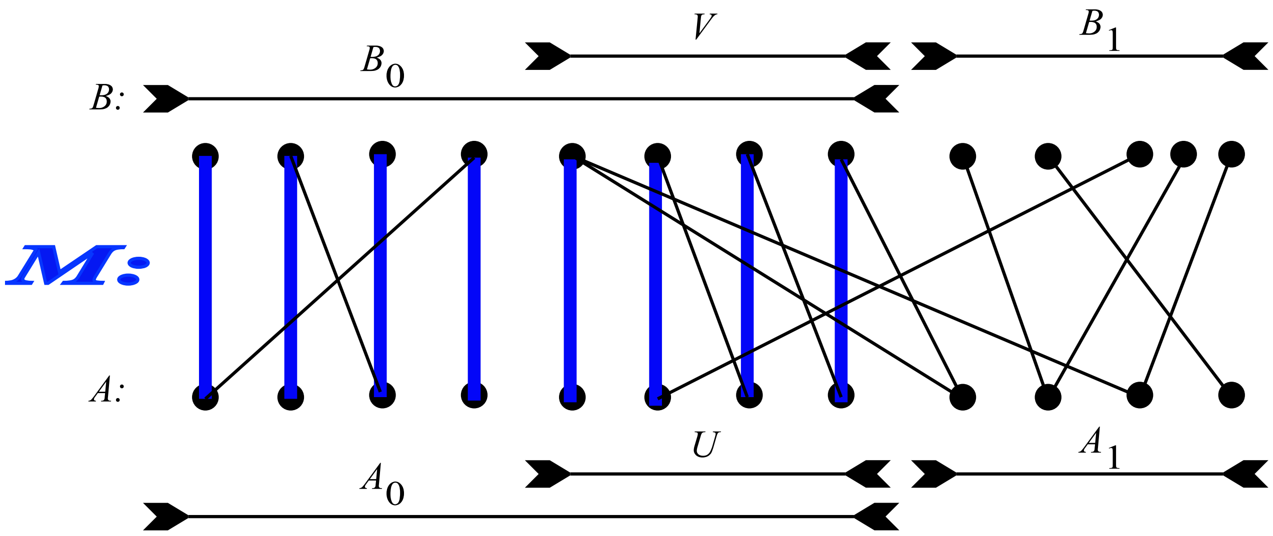
Legyen A_0, illetve B_0 az M párosítás éleinek az A, illetve a B pontosztályba eső végpontjainak halmaza.

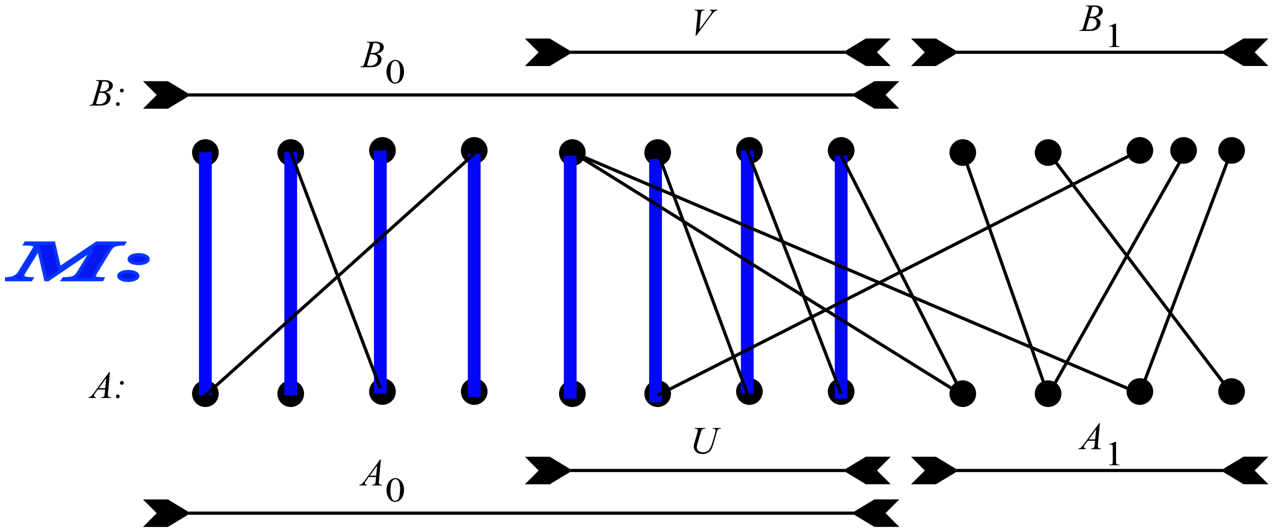
Legyen $A_1 := A \setminus A_0$ és $B_1 := B \setminus B_0$. Legyen

Legyen $A_1 := A \setminus A_0$ és $B_1 := B \setminus B_0$. Legyen U azon A_0-beli pontok halmaza, amelyek A_1-ből alternáló úttal elérhetők, és legyen V az U-ból induló M-beli élek másik (B_0-beli) végpontjainak halmaza. Az eddigi jelöléseket az alábbi ábra illusztrálja:

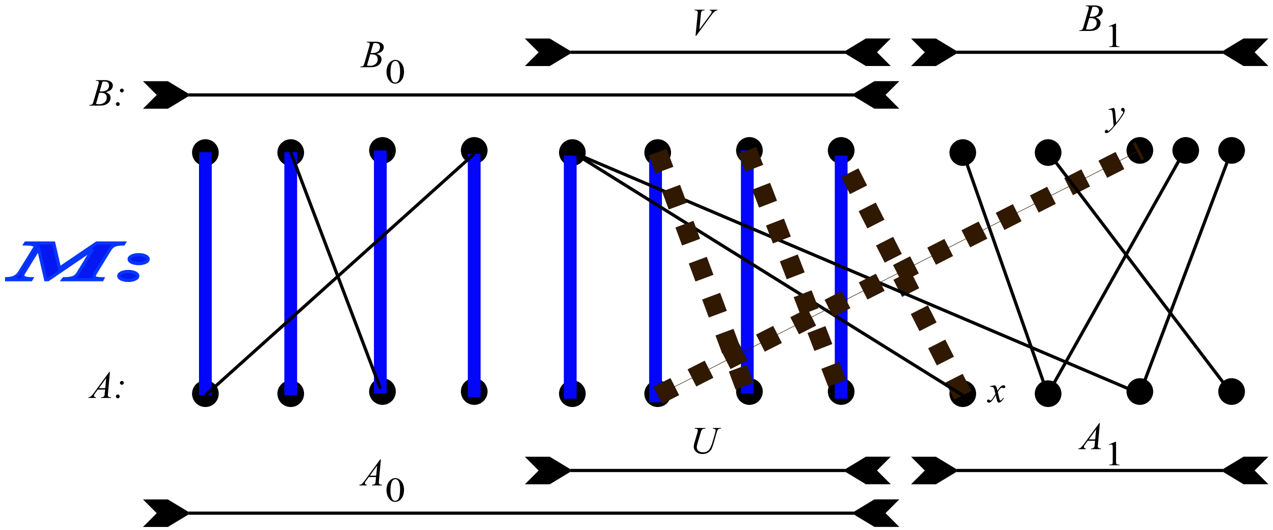


1. Segédtétel Ha **van alternáló út** A_1-ből (azaz valamely A_1-beli szögpontból) B_1-be, akkor M **nem maximális** elemszámú párosítás.

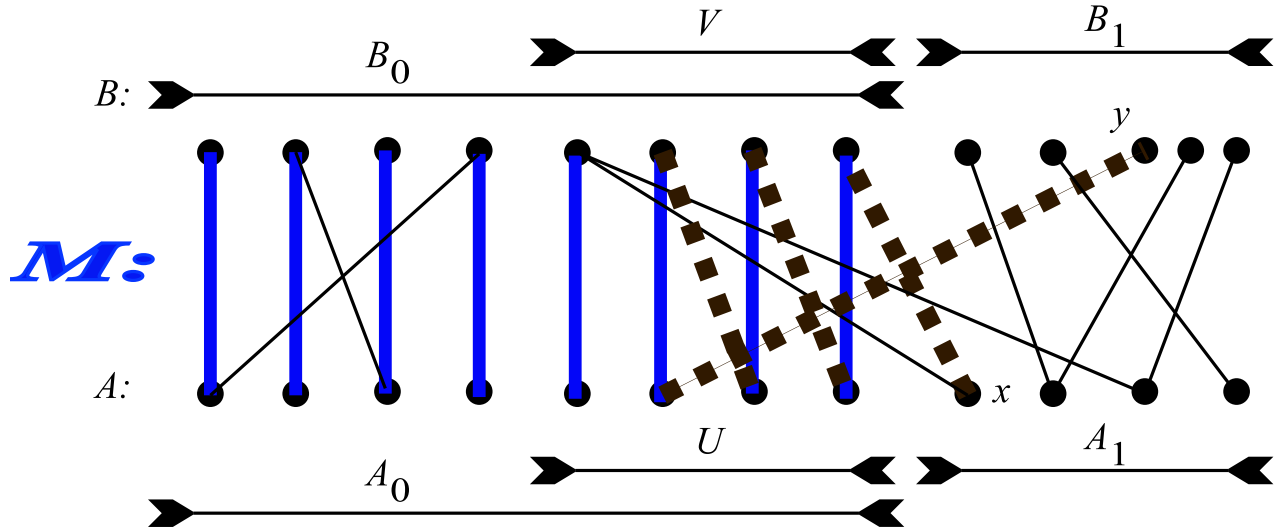




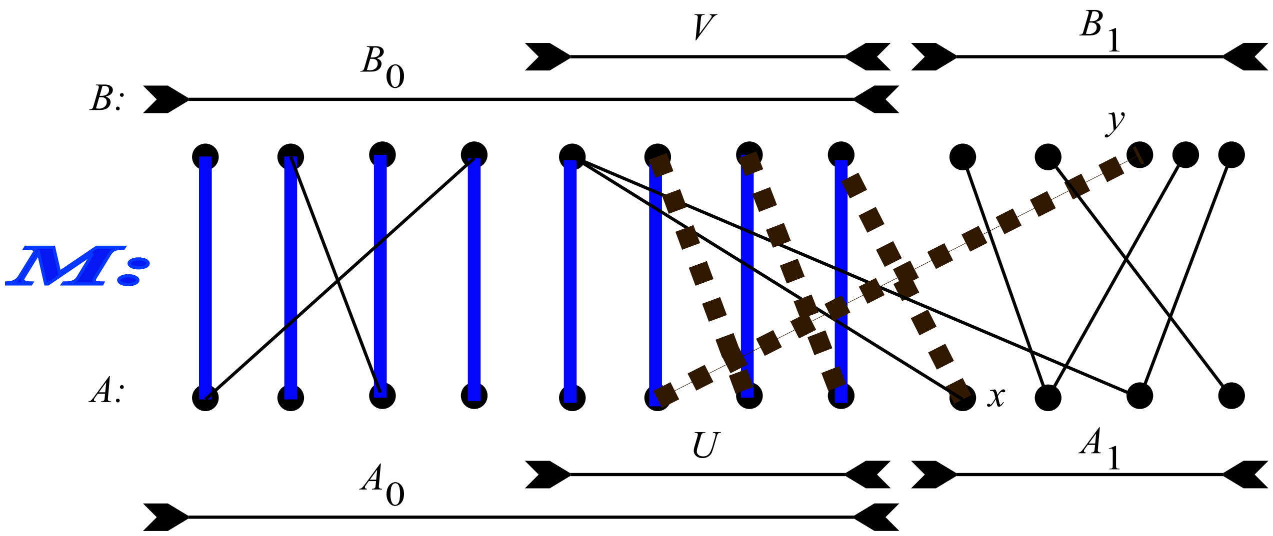
Bizonyítás: a következő két ábra mutatja meg, hogyan kapunk az M párosításból egy eggyel nagyobb elemszámú M' párosítást, ha $x \in A_1$-ből van alternáló út $y \in B_1$-be. Ez igazolja majd a segédtételt.



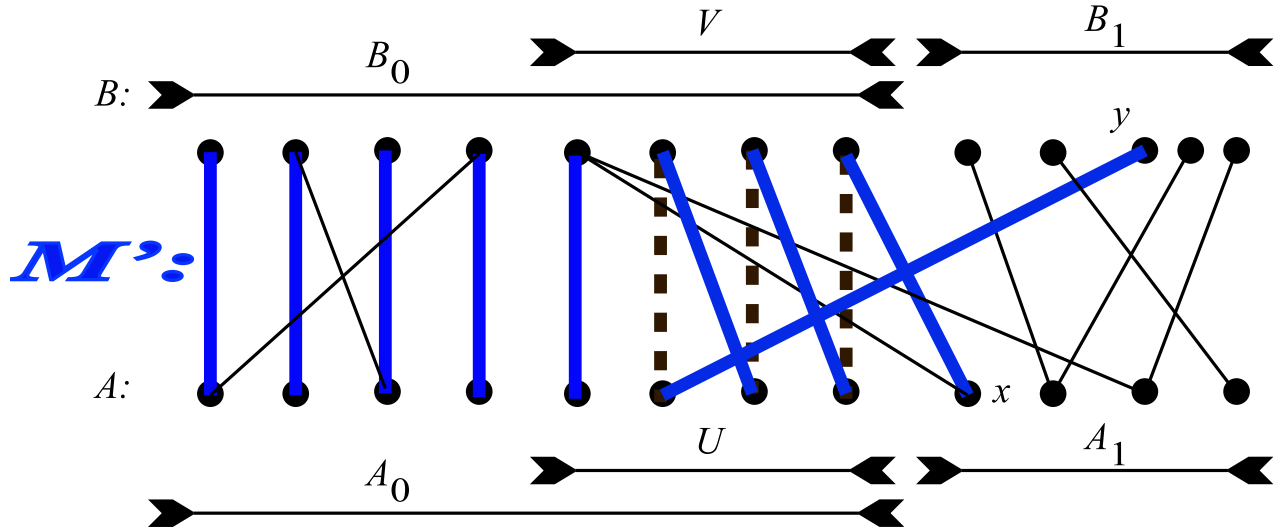
V
B 1
B 0
B:
y
M:
A:
x
U
A 1
A 0



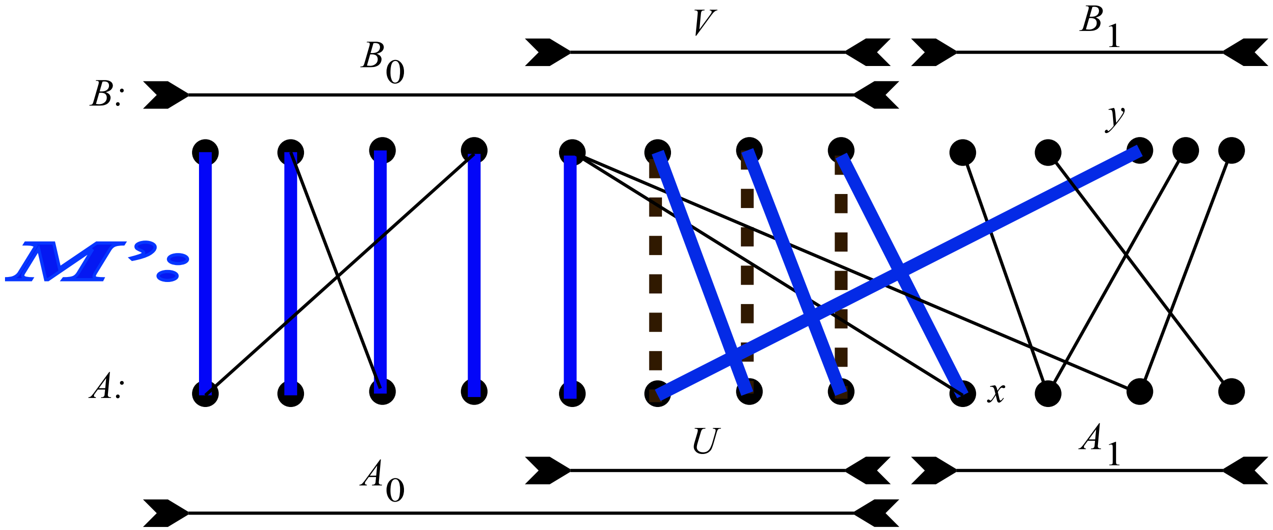
Az alternáló úton cseréljük meg a színeket!



Az alternáló úton cseréljük meg a színeket! Pontosabban: az alternáló út M-beli elemeit dobjuk ki M-ből, viszont az eredetileg M-en kívülieket vegyük be M-be!



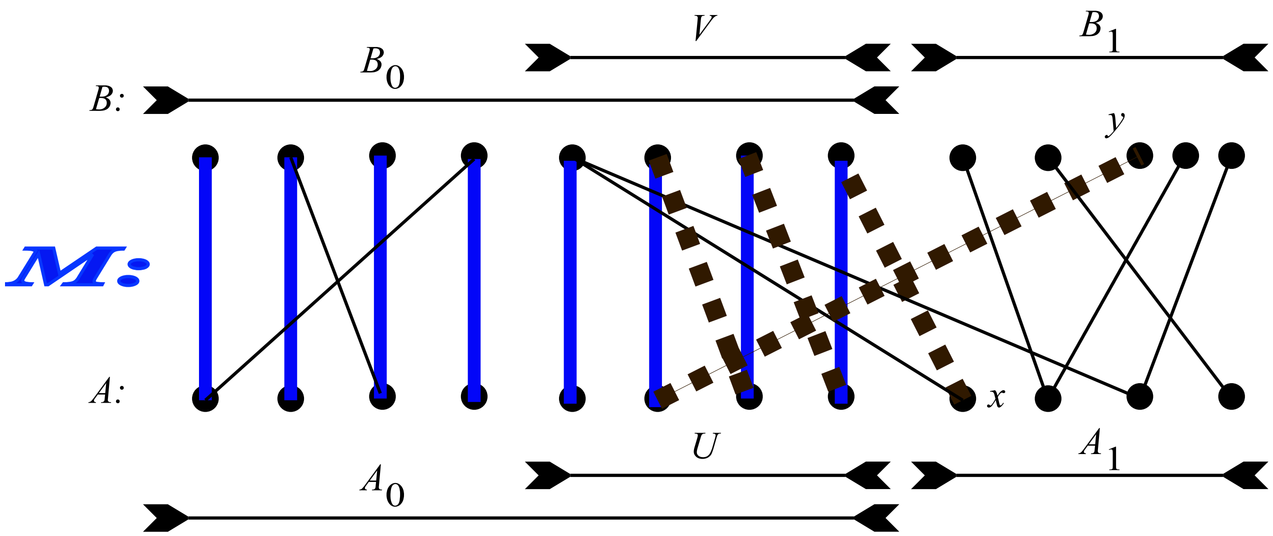
V
B_1
B_0
B:
y
M':
A:
x
U
A_1
A_0



Ezzel a segédtételt igazoltuk.

2. Segédtétel Ha **nincs alternáló út** A_1-ből B_1-be, akkor $(A_0 \setminus U) \cup V$ **lefogó ponthalmaz**. Továbbá

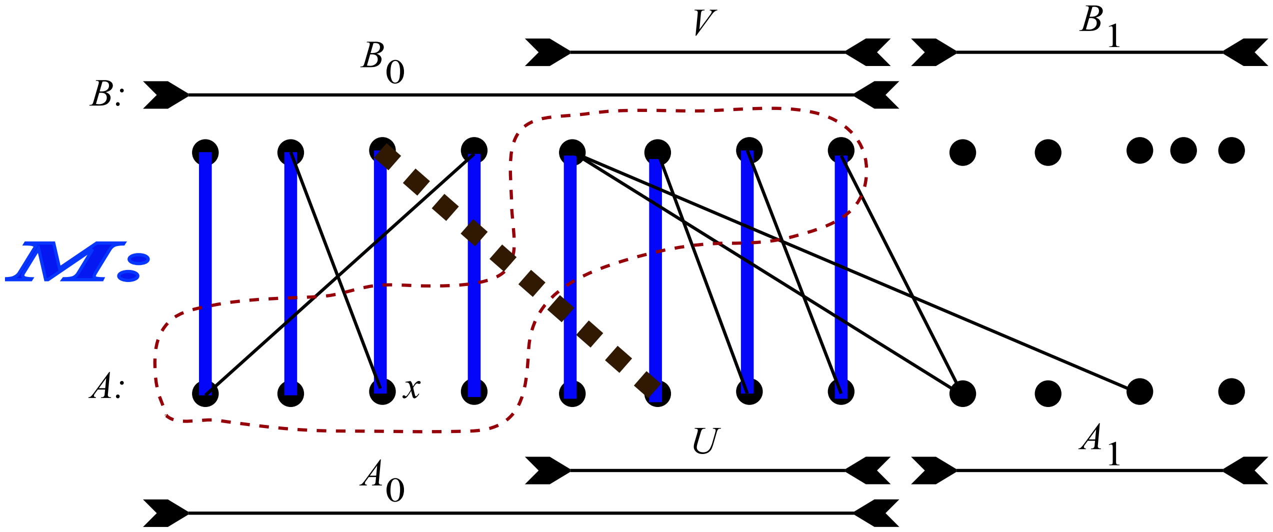
2. Segédtétel Ha **nincs alternáló út** A_1-ből B_1-be, akkor $(A_0 \backslash U) \cup V$ **lefogó ponthalmaz**. Továbbá $|M| = |(A_0 \backslash U) \cup V|$ miatt $\nu(G) \geq \tau(G)$, M maximális elemszámú párosítás, és a tételt igazoltuk.



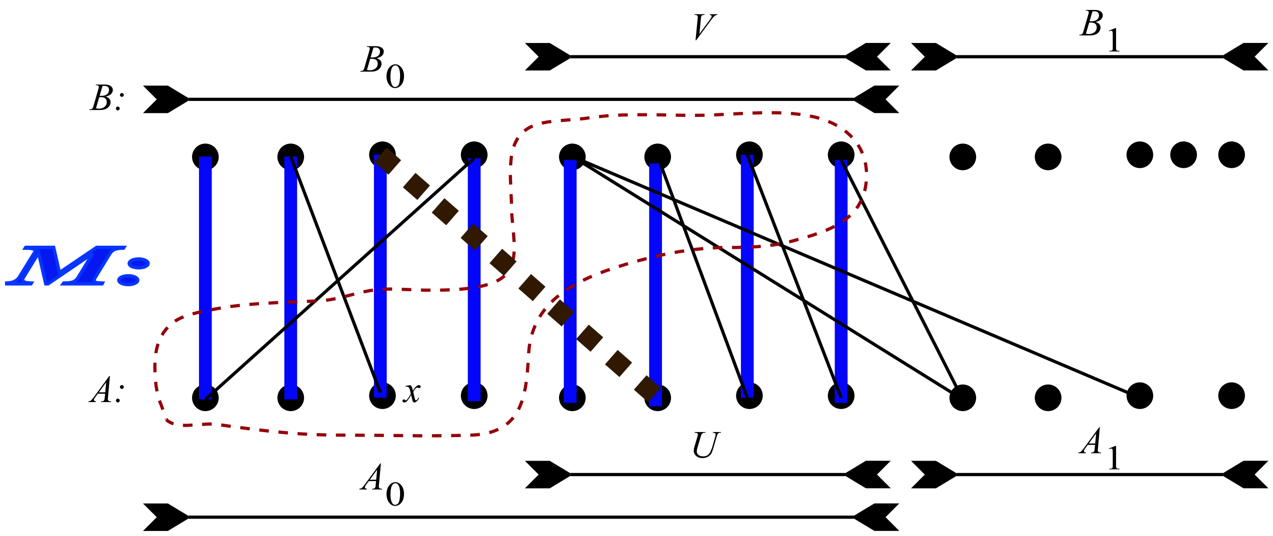
Ennek bizonyítása: A második mondat következik az elsőből, ezért

Ennek bizonyítása: A második mondat következik az elsőből, ezért csak azt kell belátnunk, hogy a mondott $(A_0 \setminus U) \cup V$ halmaz (az ábrákon szaggatott piros vonallal bekarikázva) lefogó, ehhez pedig

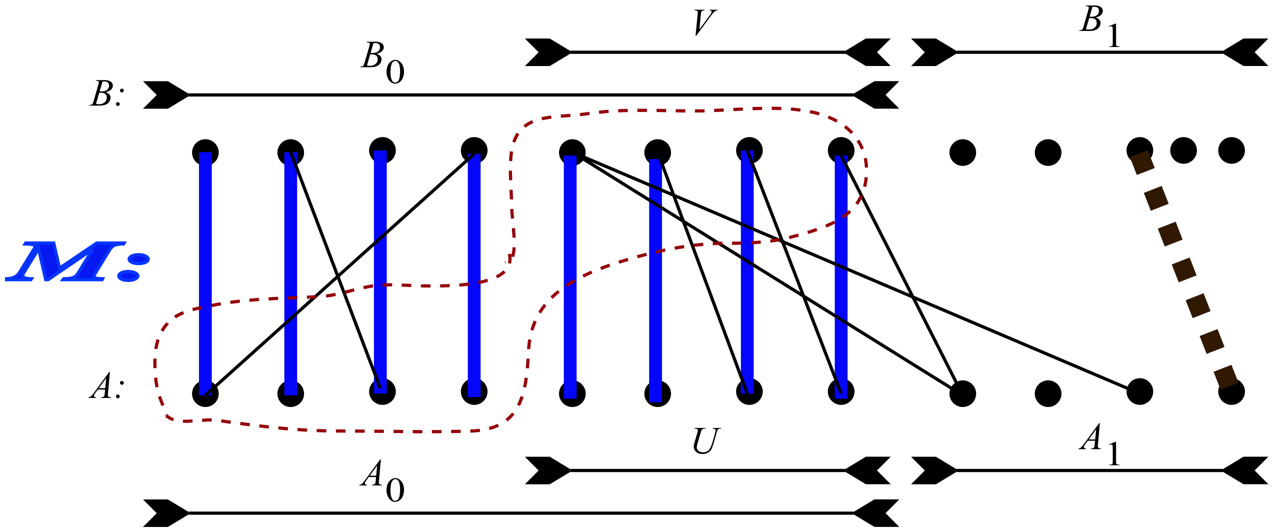
Ennek bizonyítása: A második mondat következik az elsőből, ezért csak azt kell belátnunk, hogy a mondott $(A_0 \setminus U) \cup V$ halmaz (az ábrákon szaggatott piros vonallal bekarikázva) lefogó, ehhez pedig azt kell igazolni, hogy ''rossz helyen'' (azaz a mondott halmaz által le nem fogottan) nem mennek élek. Ezt több esetre bontva indirekt igazoljuk az alábbi ábrák segítségével.



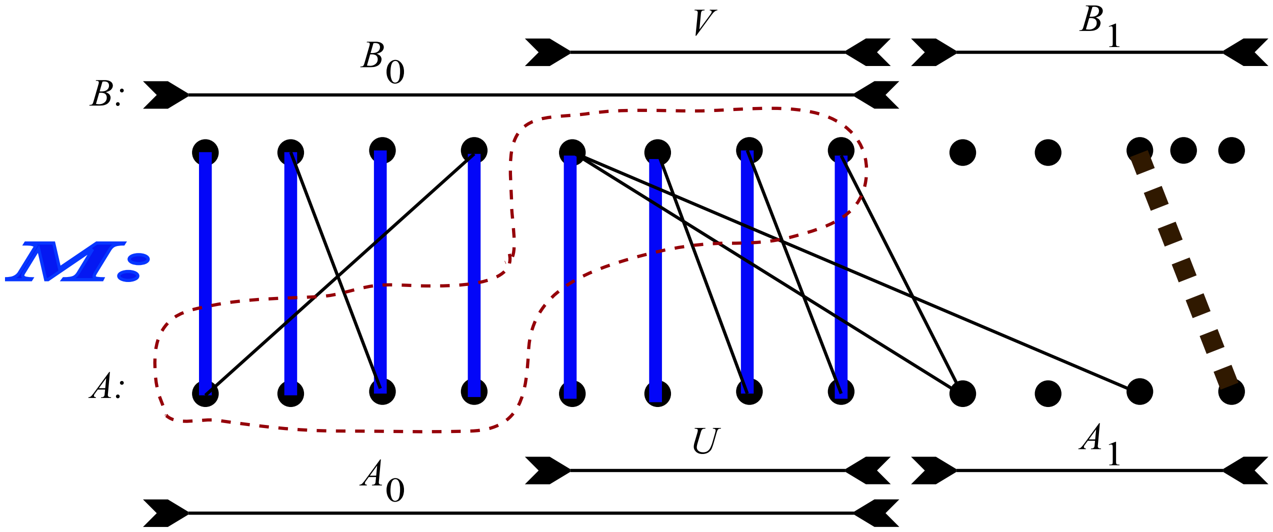
Ha egy $B_0 \setminus V$-ből induló él (az ábrán barna vastag szaggatott) nem A_0-ban landol (azaz nincs lefogva), akkor x-be is vezet alternáló út A_1-ből,



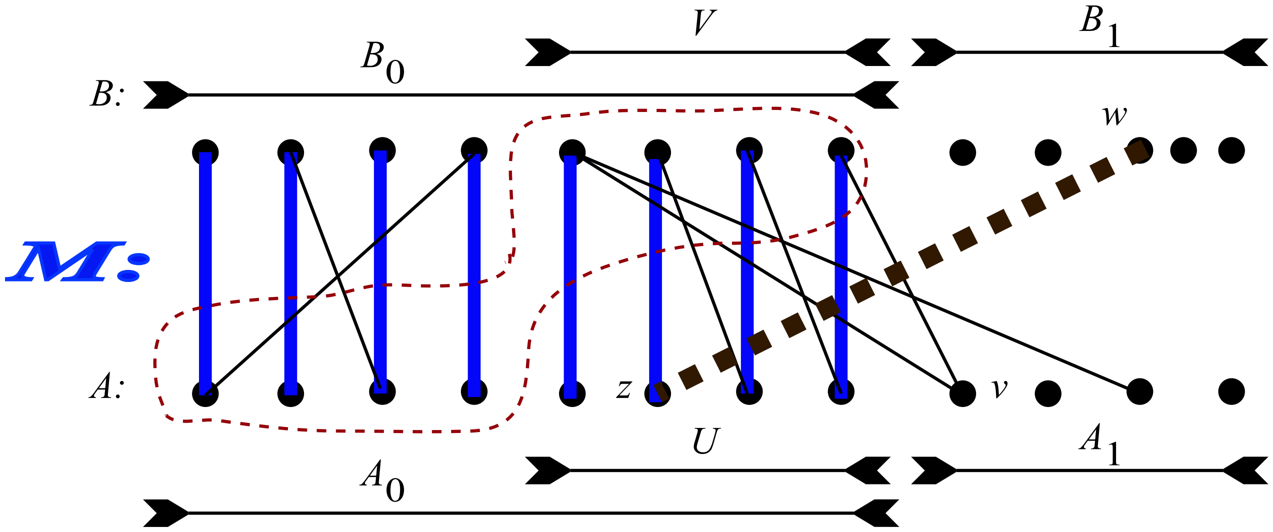
Ha egy $B_0 \setminus V$-ből induló él (az ábrán barna vastag szaggatott) nem A_0-ban landol (azaz nincs lefogva), akkor x-be is vezet alternáló út A_1-ből, így $x \in U$, ellentmondás.



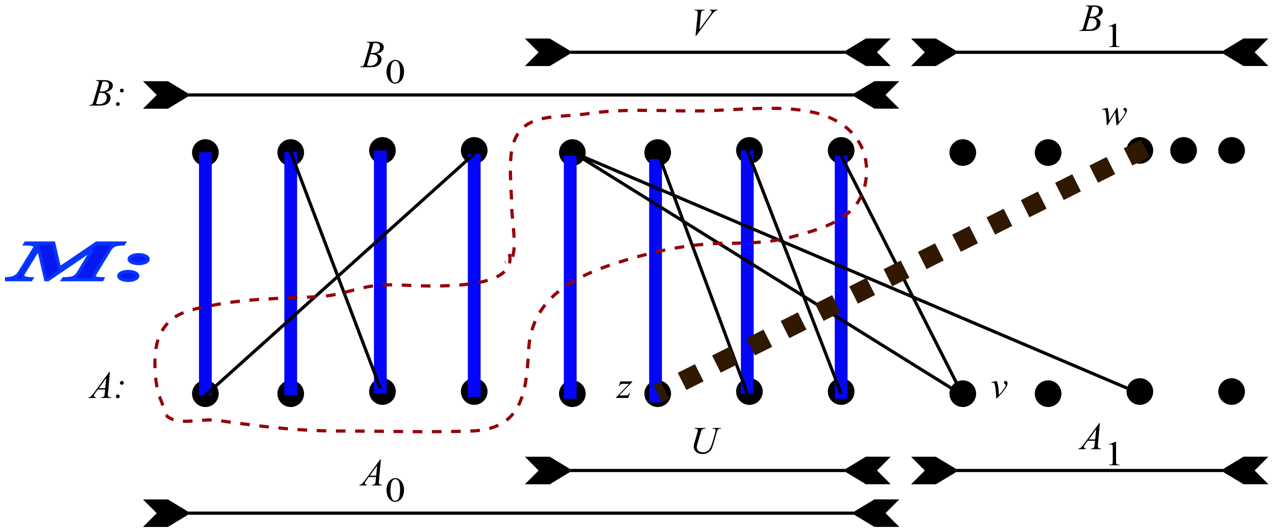
Ha egy B_1-ből induló él nem A_0-ban landol, akkor A_1-ben a feltevés miatt nem landolhat,



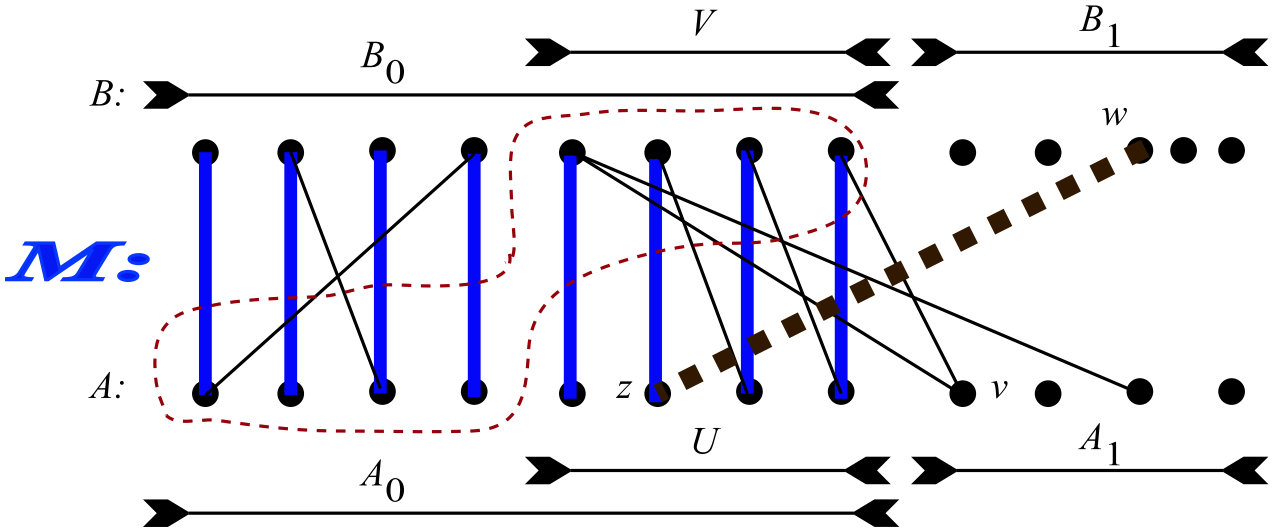
Ha egy B_1-ből induló él nem A_0-ban landol, akkor A_1-ben a feltevés miatt nem landolhat, hiszen akkor lenne 1 hosszúságú alternáló út A_1-ből B_1-be, ami a feltevés szerint lehetetlen. Ha pedig



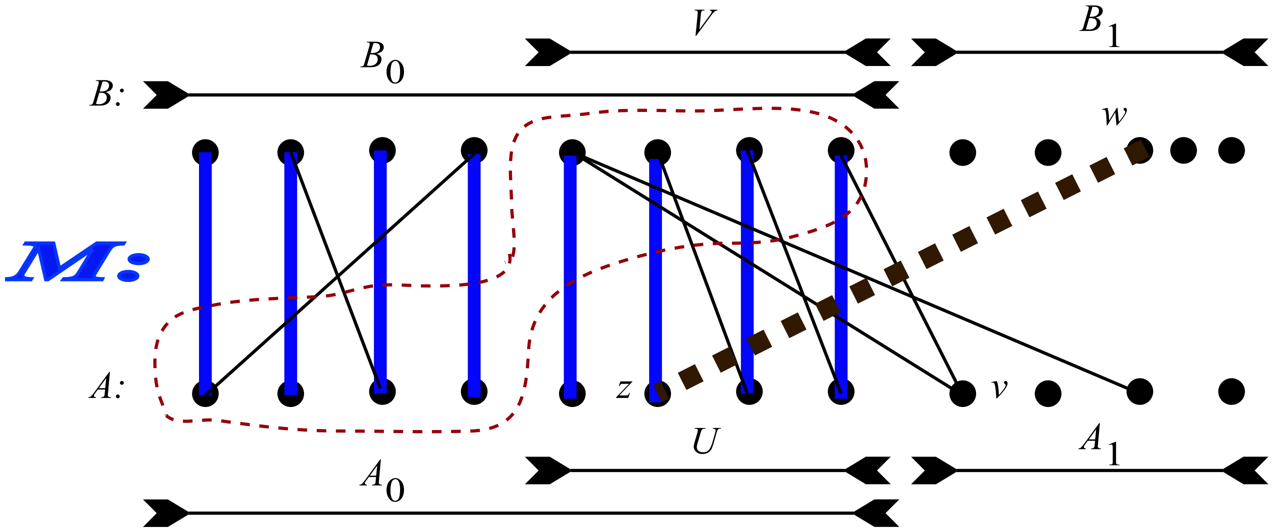
U-ban landol (az ábrán barna vastag szaggatott él):



U-ban landol (az ábrán barna vastag szaggatott él): mivel z elérhető valamely $v \in A_1$-beli pontból alternáló úttal, ezért $w \in B_1$ is,



U-ban landol (az ábrán barna vastag szaggatott él): mivel z elérhető valamely $v \in A_1$-beli pontból alternáló úttal, ezért $w \in B_1$ is, tehát — a feltevéssel ellentétben — van alternáló út A_1-ből B_1-be; ellentmondás.



U-ban landol (az ábrán barna vastag szaggatott él): mivel z elérhető valamely $v \in A_1$-beli pontból alternáló úttal, ezért $w \in B_1$ is, tehát — a feltevéssel ellentétben — van alternáló út A_1-ből B_1-be; ellentmondás. Q.e.d.

Magyar módszer: Adott egy páros gráf. Keresünk egy maximális elemszámú párosítást.

Magyar módszer: Adott egy páros gráf. Keresünk egy maximális elemszámú párosítást. A módszer: elindulunk egy tetszőleges M párosításból. (Lehet üres is, de célszerű annál bővebből indulni.)

Magyar módszer: Adott egy páros gráf. Keresünk egy maximális elemszámú párosítást. A módszer: elindulunk egy tetszőleges M párosításból. (Lehet üres is, de célszerű annál bővebből indulni.) Ezt követően az előző bizonyítást követjük:

Magyar módszer: Adott egy páros gráf. Keresünk egy maximális elemszámú párosítást. A módszer: elindulunk egy tetszőleges M párosításból. (Lehet üres is, de célszerű annál bővebből indulni.) Ezt követően az előző bizonyítást követjük: ha van alternáló út A_1-ből B_1-be, akkor ezen úton az M-beli éleket M-ből kidobva, a nem M-belieket pedig M-hez hozzávéve egy nagyobb elemszámú párosítást kapunk.

Magyar módszer: Adott egy páros gráf. Keresünk egy maximális elemszámú párosítást. A módszer: elindulunk egy tetszőleges M párosításból. (Lehet üres is, de célszerű annál bővebből indulni.) Ezt követően az előző bizonyítást követjük: ha van alternáló út A_1-ből B_1-be, akkor ezen úton az M-beli éleket M-ből kidobva, a nem M-belieket pedig M-hez hozzávéve egy nagyobb elemszámú párosítást kapunk.

Ha pedig nincs, akkor $(A_0 \setminus U) \cup V$ lefogó ponthalmaz.

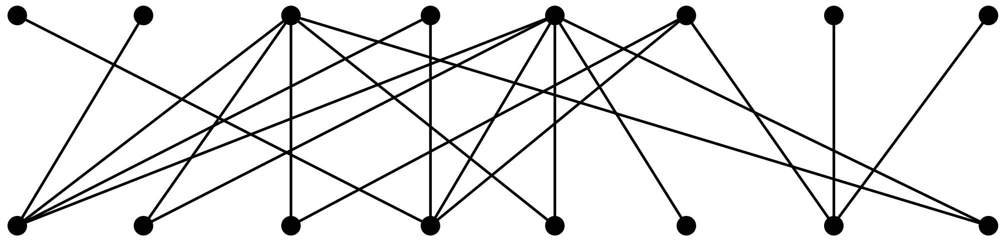
Magyar módszer: Adott egy páros gráf. Keresünk egy maximális elemszámú párosítást. A módszer: elindulunk egy tetszőleges M párosításból. (Lehet üres is, de célszerű annál bővebből indulni.) Ezt követően az előző bizonyítást követjük: ha van alternáló út A_1-ből B_1-be, akkor ezen úton az M-beli éleket M-ből kidobva, a nem M-belieket pedig M-hez hozzávéve egy nagyobb elemszámú párosítást kapunk.

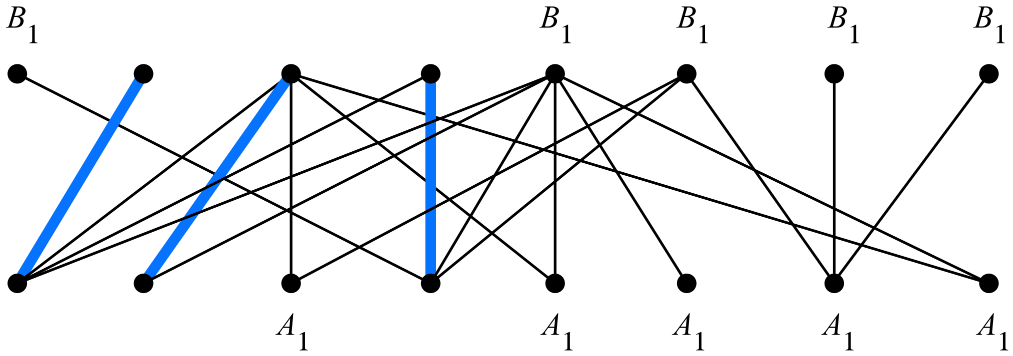
Ha pedig nincs, akkor $(A_0 \setminus U) \cup V$ lefogó ponthalmaz. Érdemes ellenőrizni, hogy tényleg lefogó és tényleg annyi eleme van, mint amennyi a párosításnak (ha nem, akkor valamit elrontottunk: valószínűleg az U-t rosszul határoztuk meg.)

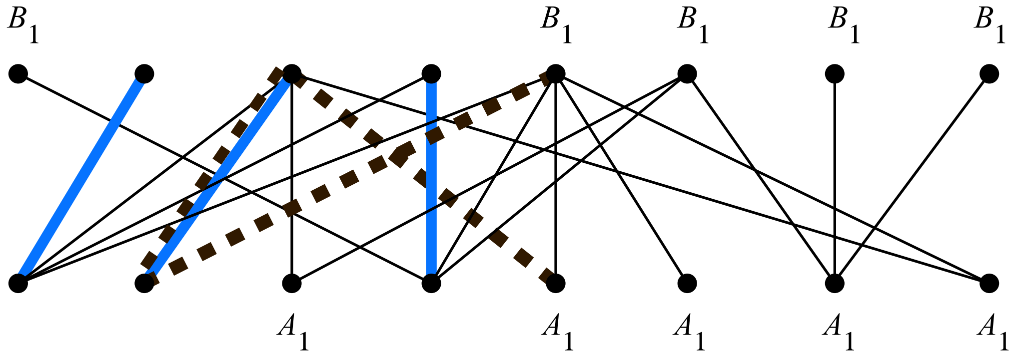
Magyar módszer: Adott egy páros gráf. Keresünk egy maximális elemszámú párosítást. A módszer: elindulunk egy tetszőleges M párosításból. (Lehet üres is, de célszerű annál bővebből indulni.) Ezt követően az előző bizonyítást követjük: ha van alternáló út A_1-ből B_1-be, akkor ezen úton az M-beli éleket M-ből kidobva, a nem M-belieket pedig M-hez hozzávéve egy nagyobb elemszámú párosítást kapunk.

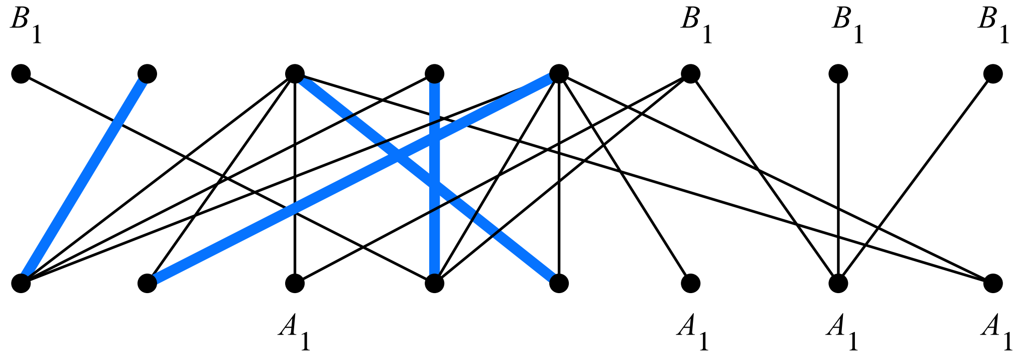
Ha pedig nincs, akkor $(A_0 \setminus U) \cup V$ lefogó ponthalmaz. Érdemes ellenőrizni, hogy tényleg lefogó és tényleg annyi eleme van, mint amennyi a párosításnak (ha nem, akkor valamit elrontottunk: valószínűleg az U-t rosszul határoztuk meg.)

Példa: az alábbi ábrák szerint.

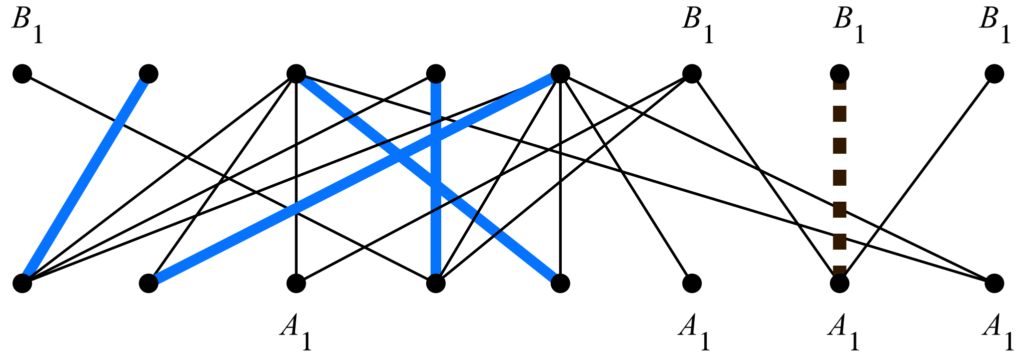



B1
B1
B1
B1
B1
A1
A1
A1
A1
A1

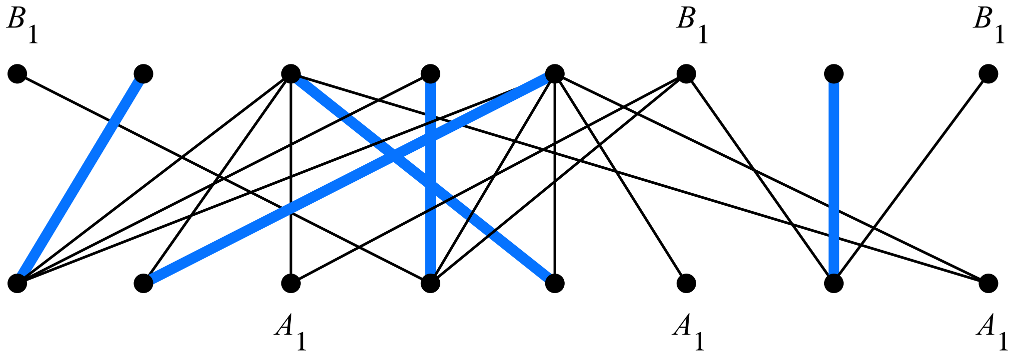

B_1
B_1
B_1
B_1
B_1
A_1
A_1
A_1
A_1
A_1

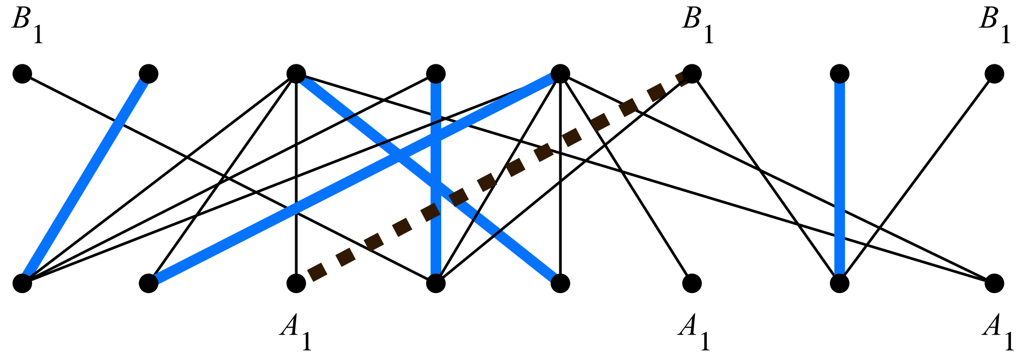


B_1
B_1
B_1
B_1
A_1
A_1
A_1
A_1

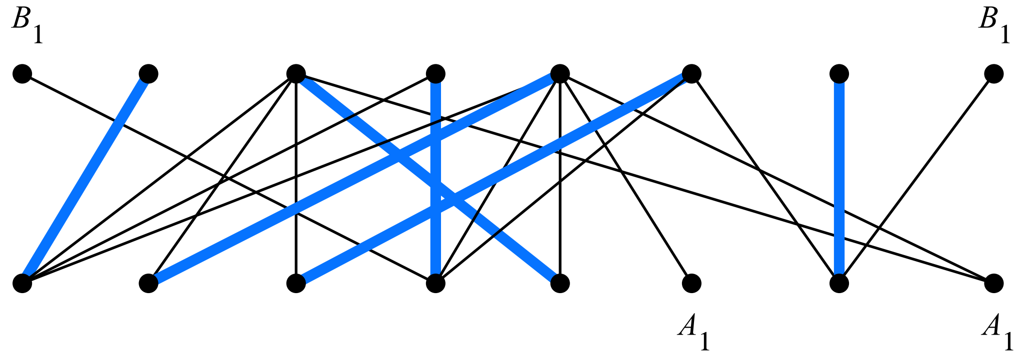


B_1
B_1
B_1
B_1
A_1
A_1
A_1
A_1

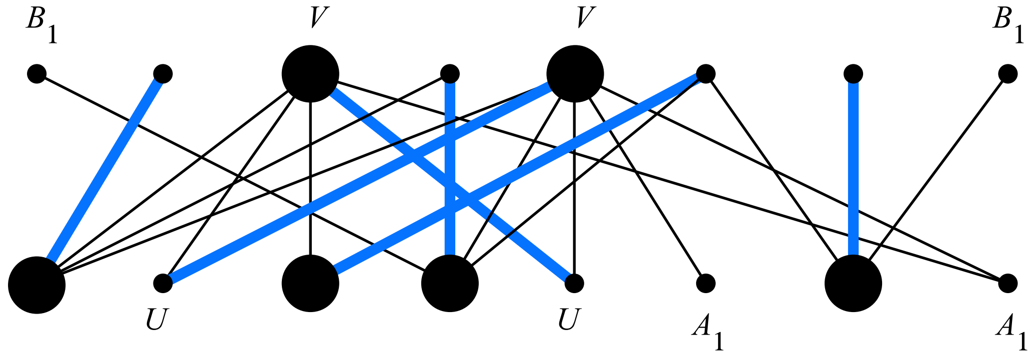

B_1
B_1
B_1
A_1
A_1
A_1

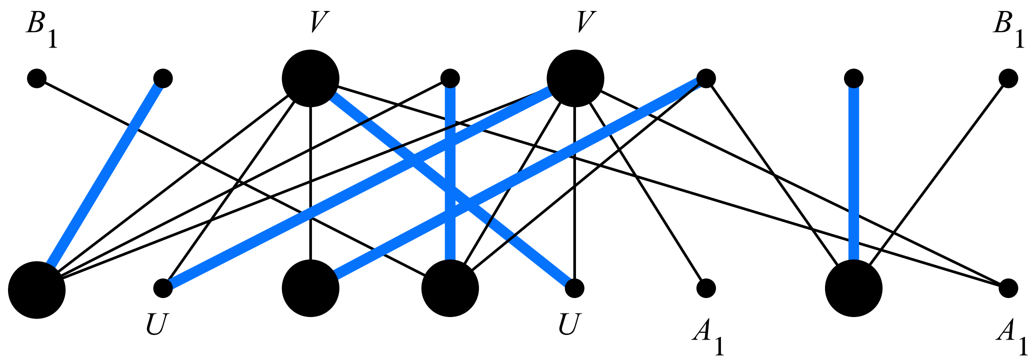


B_1
B_1
B_1
A_1
A_1
A_1



A vizsga feltétele: 20 pont a gyakorlaton!


B_1
V
V
B_1
U
U
A_1
A_1



A nagy ”gombócok” lefogó ponthalmazt alkotnak. Számuk valóban $|M|$. Tehát M maximális elemszámú párosítás.

Megjegyzés: ha M (mindegy, hogyan találtuk) olyan párosítás, hogy létezik $|M|$ elemszámú lefogó ponthalmaz, akkor M maximális elemszámú párosítás (és a kérdéses lefogó ponthalmaz minimális elemszámú).

$X \subseteq V$-re jelölje $\Gamma(X)$ az X-beli szögpontok szomszédainak halmazát. (Azaz azon szögpontok halmazát, amelyek valamely X-beli szögponttal össze vannak kötve éllel.)

$X \subseteq V$-re jelölje $\Gamma(X)$ az X-beli szögpontok szomszédainak halmazát. (Azaz azon szögpontok halmazát, amelyek valamely X-beli szögponttal össze vannak kötve éllel.)

42. Tétel. *Kőnig–Hall-tétel. Legyen G páros gráf az A, B pontosztályokkal. Akkor és csak akkor létezik A-t lefedő párosítás, ha*

$X \subseteq V$-re jelölje $\Gamma(X)$ az X-beli szögpontok szomszédainak halmazát. (Azaz azon szögpontok halmazát, amelyek valamely X-beli szögponttal össze vannak kötve éllel.)

42. Tétel. *Kőnig–Hall-tétel. Legyen G páros gráf az A, B pontosztályokkal. Akkor és csak akkor létezik A-t lefedő párosítás, ha bármely $X \subseteq A$-ra $|\Gamma(X)| \geq |X|$. ("Kőnig–Hall-feltétel".)*

$X \subseteq V$-re jelölje $\Gamma(X)$ az X-beli szögpontok szomszédainak halmazát. (Azaz azon szögpontok halmazát, amelyek valamely X-beli szögponttal össze vannak kötve éllel.)

42. Tétel. *Kőnig–Hall-tétel. Legyen G páros gráf az A, B pontosztályokkal. Akkor és csak akkor létezik A-t lefedő párosítás, ha bármely $X \subseteq A$-ra $|\Gamma(X)| \geq |X|$. ("Kőnig–Hall-feltétel".)*

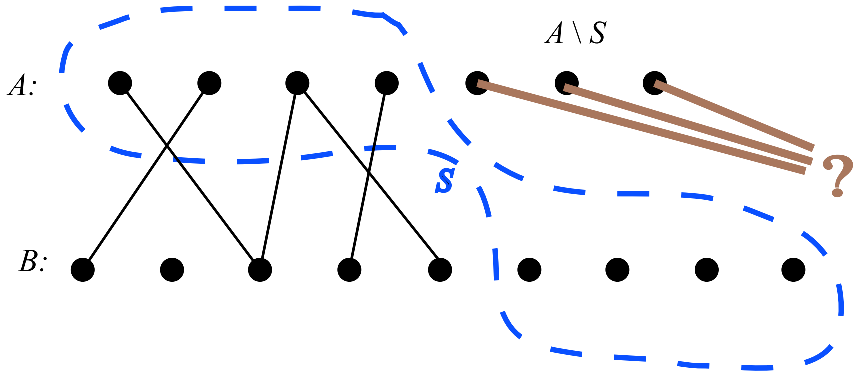
(Nagyon) pongyolán fogalmazva: a feltétel az, hogy A bármely részhalmazának elég sok szomszédja legyen.

Bizonyítás: A feltétel nyilván szükséges. Az elegendőséghez a Kőnig-tétel szerint elegendő azt belátni, hogy

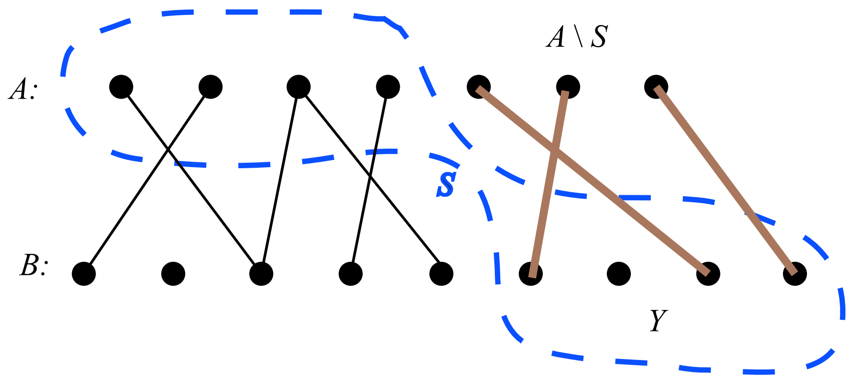
Bizonyítás: A feltétel nyilván szükséges. Az elegendőséghez a Kőnig-tétel szerint elegendő azt belátni, hogy $\tau(G) = |A|$, azaz $\tau(G) \geq |A|$, azaz

Bizonyítás: A feltétel nyilván szükséges. Az elegendőséghez a Kőnig-tétel szerint elegendő azt belátni, hogy $\tau(G) = |A|$, azaz $\tau(G) \geq |A|$, azaz hogy bármely S lefogó szögponthalmaznak legalább $|A|$ eleme van.

Bizonyítás: A feltétel nyilván szükséges. Az elegendőséghez a Kőnig-tétel szerint elegendő azt belátni, hogy $\tau(G) = |A|$, azaz $\tau(G) \geq |A|$, azaz hogy bármely S lefogó szögponthalmaznak legalább $|A|$ eleme van. Az ábra szerint:

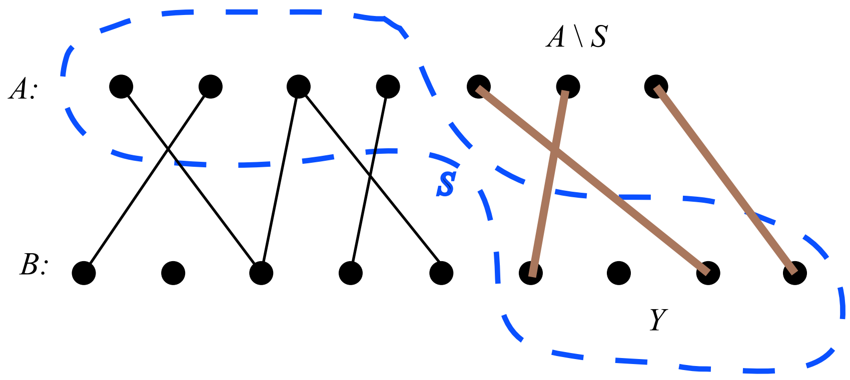


Az $A \setminus S$-ből induló élek (hogy S tényleg "lefogja" őket), csakis



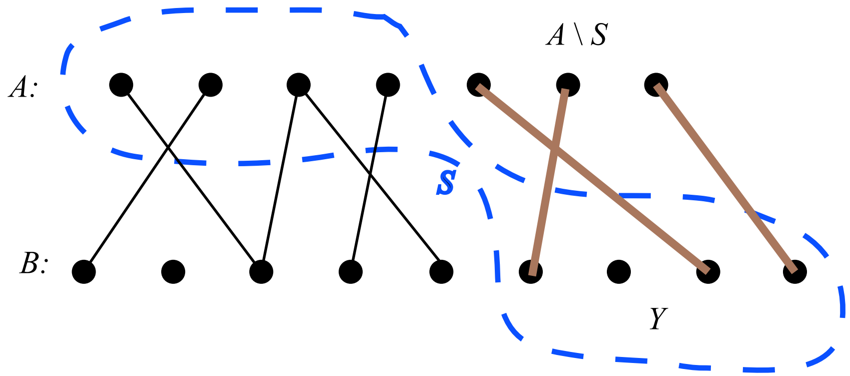
$Y := B \cap S$-ben végződhetnek.

Az $A \setminus S$-ből induló élek (hogy S tényleg ”lefogja” őket), csakis



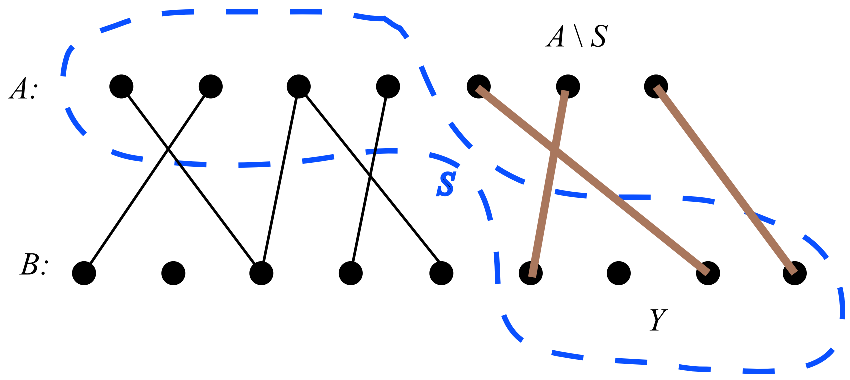
$Y := B \cap S$-ben végződhetnek. Ezért $\Gamma(A \setminus S) \subseteq Y$, így

Az $A \setminus S$-ből induló élek (hogy S tényleg "lefogja" őket), csakis



$Y := B \cap S$-ben végződhetnek. Ezért $\Gamma(A \setminus S) \subseteq Y$, így $|A \setminus S| \leq |\Gamma(A \setminus S)| \leq |Y|$,

Az $A \setminus S$-ből induló élek (hogy S tényleg "lefogja" őket), csakis



$Y := B \cap S$-ben végződhetnek. Ezért $\Gamma(A \setminus S) \subseteq Y$, így $|A \setminus S| \leq |\Gamma(A \setminus S)| \leq |Y|$, és ezért látható, hogy $|A| \leq |S|$. Q.e.d.

Az eddigiek következménye az alábbi:

43. Tétel. *Legyen* G *páros gráf az* A*,* B *pontosztályokkal. Pontosan akkor létezik teljes párosítás, ha*

Az eddigiek következménye az alábbi:

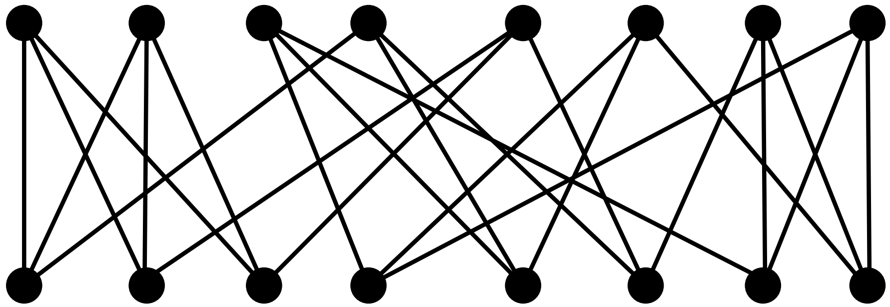
43. Tétel. *Legyen* G *páros gráf az* A*,* B *pontosztályokkal. Pontosan akkor létezik teljes párosítás, ha* $|A| = |B|$ *és (Kőnig–Hall-feltétel:)*

Az eddigiek következménye az alábbi:

43. Tétel. *Legyen* G *páros gráf az* A, B *pontosztályokkal. Pontosan akkor létezik teljes párosítás, ha* $|A| = |B|$ *és (Kőnig–Hall-feltétel:) az* A *bármely* S *részhalmazának legalább* $|S|$ *szomszédja van.*

Egy gráfot k-regulárisnak nevezünk, ha minden pontja k-adfokú.
Regulárisnak, ha

Egy gráfot k-regulárisnak nevezünk, ha minden pontja k-adfokú. Regulárisnak, ha valamely $k \geq 1$-re k-reguláris. Példa:



3-reguláris páros gráf

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be.

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be. Mivel $\Gamma(X)$ egy-egy szögpontjába pontosan k él fut be, ezért $|\Gamma(X)|$ nem lehet

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be. Mivel $\Gamma(X)$ egy-egy szögpontjába pontosan k él fut be, ezért $|\Gamma(X)|$ nem lehet túl kis elemszámú, hogy az X-ből befutó élek landolni tudjanak.

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be. Mivel $\Gamma(X)$ egy-egy szögpontjába pontosan k él fut be, ezért $|\Gamma(X)|$ nem lehet túl kis elemszámú, hogy az X-ből befutó élek landolni tudjanak. Pontosabban: kn él csak úgy landolhat, ha

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be. Mivel $\Gamma(X)$ egy-egy szögpontjába pontosan k él fut be, ezért $|\Gamma(X)|$ nem lehet túl kis elemszámú, hogy az X-ből befutó élek landolni tudjanak. Pontosabban: kn él csak úgy landolhat, ha $|\Gamma(X)| \geq n = |X|$ (Kőnig–Hall-feltétel). Speciálisan:

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be. Mivel $\Gamma(X)$ egy-egy szögpontjába pontosan k él fut be, ezért $|\Gamma(X)|$ nem lehet túl kis elemszámú, hogy az X-ből befutó élek landolni tudjanak. Pontosabban: kn él csak úgy landolhat, ha $|\Gamma(X)| \geq n = |X|$ (Kőnig–Hall-feltétel). Speciálisan: $X = A$ esetén kapjuk, hogy $|A| \leq |\Gamma(A)| \leq |B|$. Szerepcserével:

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be. Mivel $\Gamma(X)$ egy-egy szögpontjába pontosan k él fut be, ezért $|\Gamma(X)|$ nem lehet túl kis elemszámú, hogy az X-ből befutó élek landolni tudjanak. Pontosabban: kn él csak úgy landolhat, ha $|\Gamma(X)| \geq n = |X|$ (Kőnig–Hall-feltétel). Speciálisan: $X = A$ esetén kapjuk, hogy $|A| \leq |\Gamma(A)| \leq |B|$. Szerepcserével: $|B| \leq |A|$.

44. Tétel. *Minden reguláris páros gráfban létezik teljes párosítás.*

Bizonyítás: Legyen $X \subseteq A$, $|X| = n$. Ekkor X-ből kn él indul ki $\Gamma(X)$-be. Mivel $\Gamma(X)$ egy-egy szögpontjába pontosan k él fut be, ezért $|\Gamma(X)|$ nem lehet túl kis elemszámú, hogy az X-ből befutó élek landolni tudjanak. Pontosabban: kn él csak úgy landolhat, ha $|\Gamma(X)| \geq n = |X|$ (Kőnig–Hall-feltétel). Speciálisan: $X = A$ esetén kapjuk, hogy $|A| \leq |\Gamma(A)| \leq |B|$. Szerepcserével: $|B| \leq |A|$. Az előző tétel miatt Q.e.d.

Síkgráfok

Def.

Síkgráfok

Def. Síkgráf: amelyik lerajzolható a síkba úgy, hogy élei csakis szögpontokban találkoznak, de egyenes szakaszok mellett lehetnek görbe vonalak is.

Síkgráfok

Def. Síkgráf: amelyik lerajzolható a síkba úgy, hogy élei csakis szögpontokban találkoznak, de egyenes szakaszok mellett lehetnek görbe vonalak is. (A "görbe vonal" távolról sem precíz!)

A

Síkgráfok

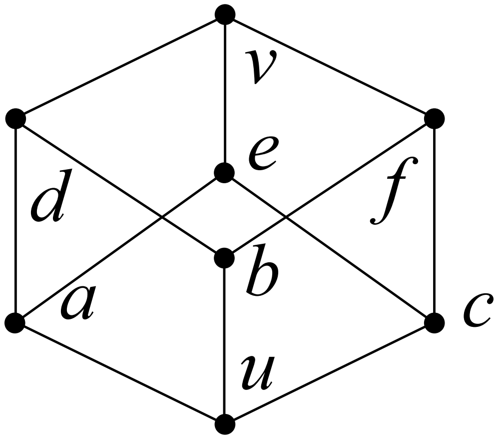
Def. Síkgráf: amelyik lerajzolható a síkba úgy, hogy élei csakis szögpontokban találkoznak, de egyenes szakaszok mellett lehet-nek görbe vonalak is. (A ''görbe vonal'' távolról sem precíz!)

A többszörös- és hurokéleknek itt nincs szerepe, az irányításnak sincs, ezért egyszerű irányítatlan gráfokat tekintünk. T

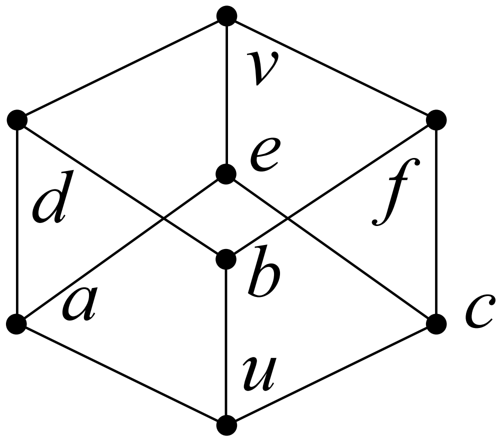
Síkgráfok

Def. Síkgráf: amelyik lerajzolható a síkba úgy, hogy élei csakis szögpontokban találkoznak, de egyenes szakaszok mellett lehetnek görbe vonalak is. (A "görbe vonal" távolról sem precíz!)

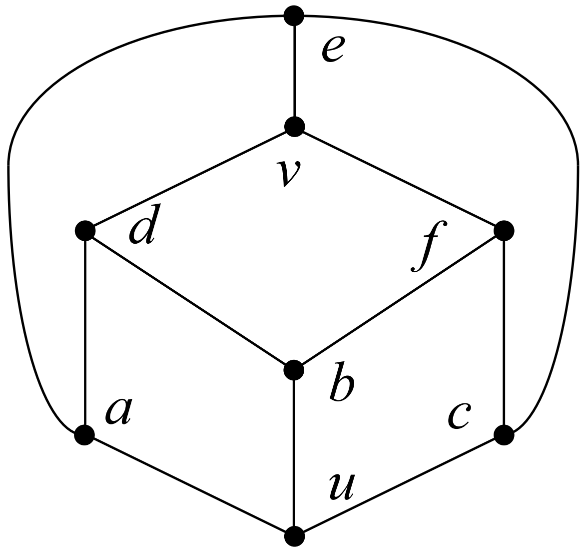
A többszörös- és hurokéleknek itt nincs szerepe, az irányításnak sincs, ezért egyszerű irányítatlan gráfokat tekintünk. Természetesen egy gráf, $G = (V, E)$, többféleképpen is lerajzolható, hiszen az ábra csak szemlélteti, hogy V mely legfeljebb kételemű részhalmazai tartoznak E-hez.

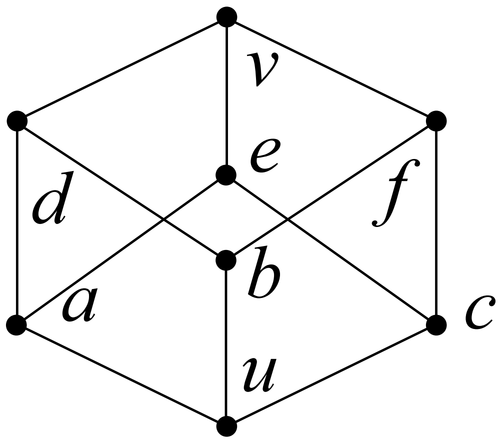


Ez síkgráf?

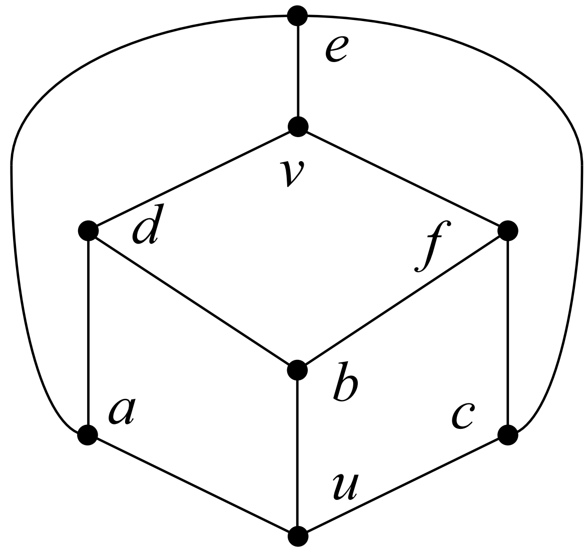


Ez síkgráf?





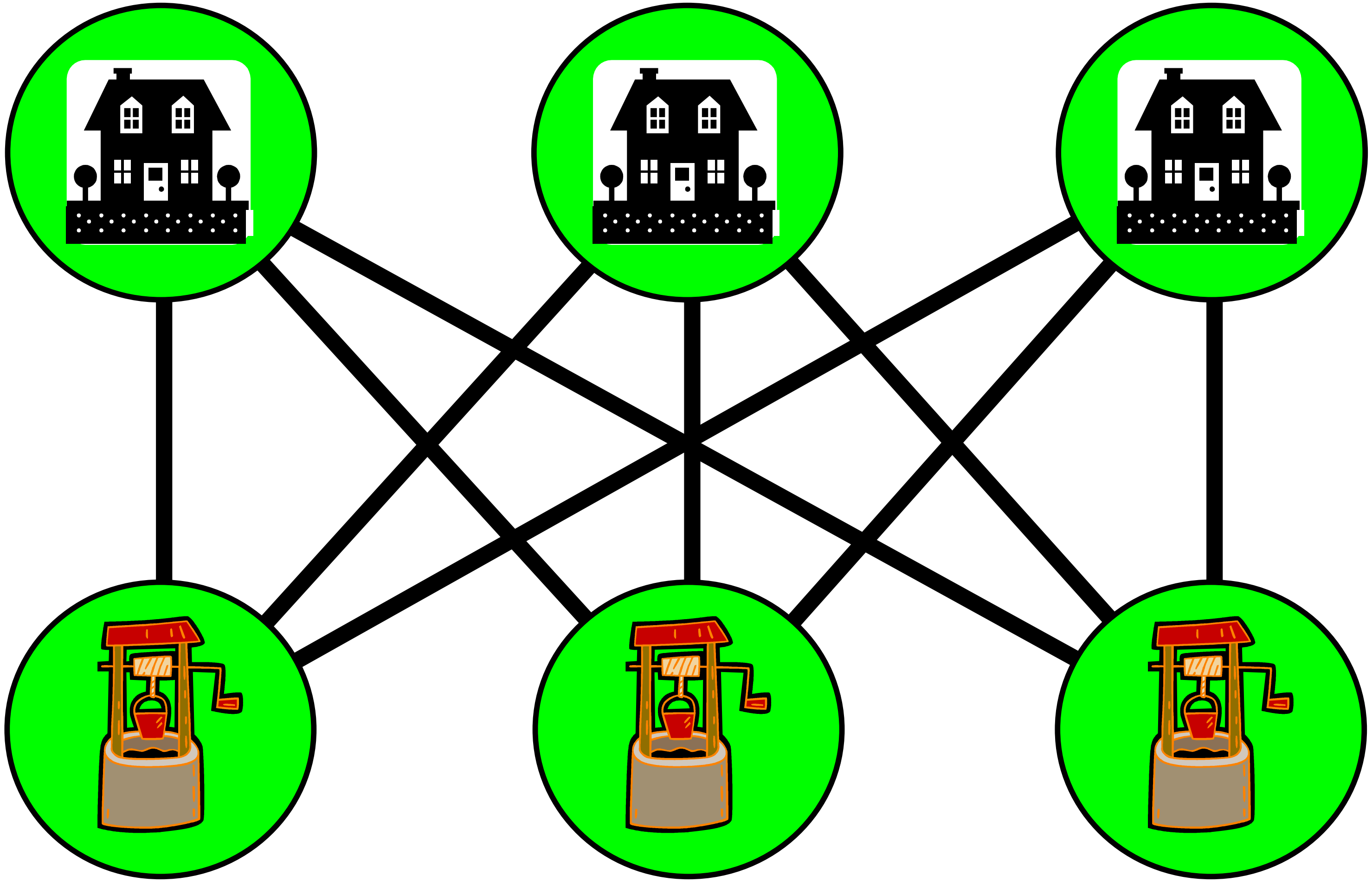
Ez síkgráf?



Igen!

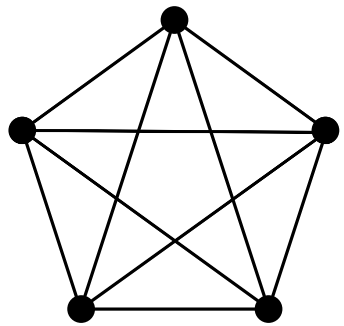
És síkgráf-e az ún. ”három ház — három kút gráf” ?

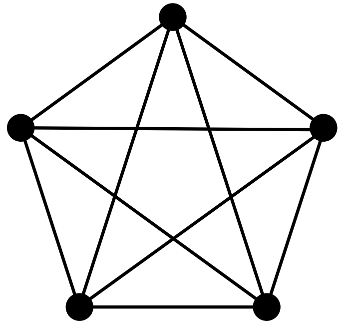
És síkgráf-e az ún. ''három ház — három kút gráf''? A történet: úgy akarnak három ház mindegyikéből mindhárom kúthoz utat építeni, hogy azok ne keresztezzék egymást.



A vizsga feltétele: 20 pont a gyakorlaton!

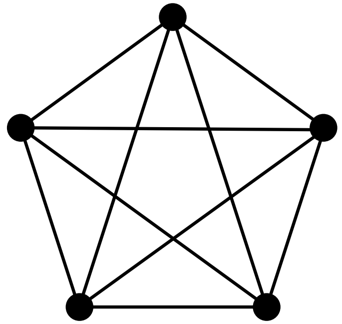
És a ”teljes ötszög”? :

És a "teljes ötszög"? : 

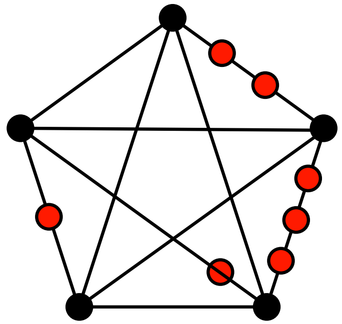
És a ”teljes ötszög”? : 

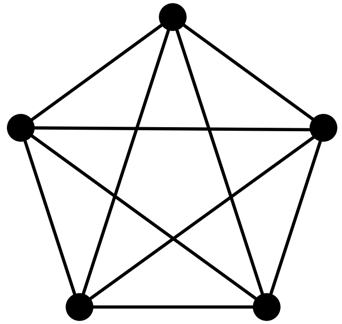
Def.: pontokkal továbbosztott gráf: az élekre további szögpon-

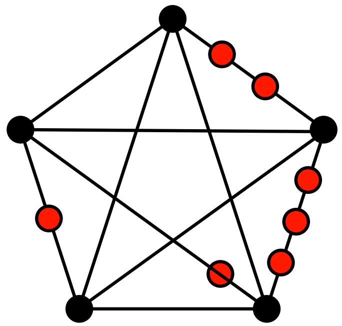
tokat helyezünk el. Pl:

És a "teljes ötszög"? : 

Def.: pontokkal továbbosztott gráf: az élekre további szögpon-

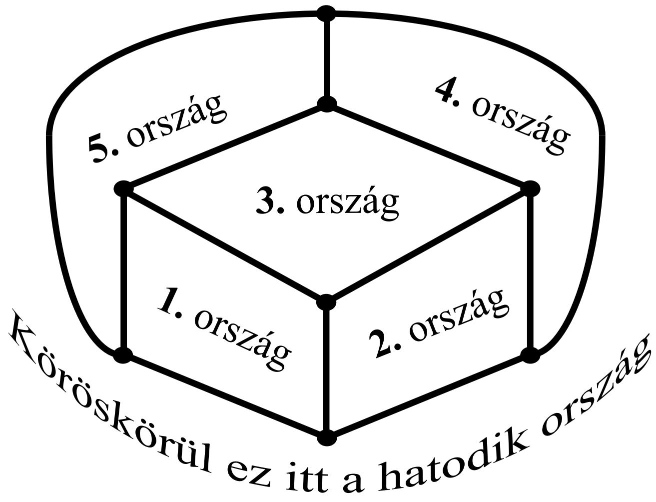
tokat helyezünk el. Pl:  .

És a "teljes ötszög"? : 

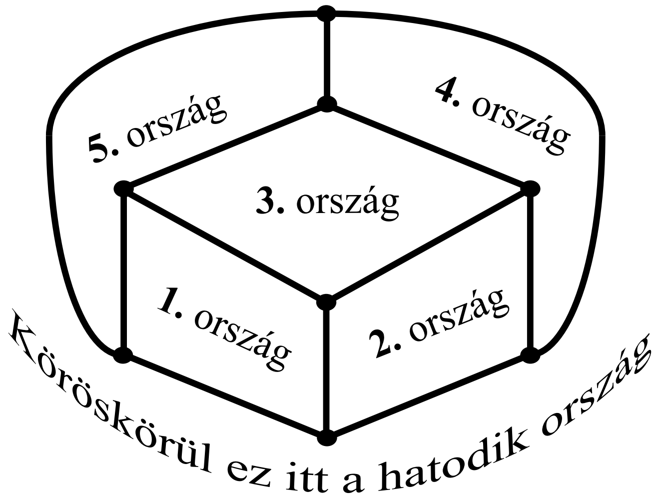
Def.: pontokkal továbbosztott gráf: az élekre további szögpontokat helyezünk el. Pl: . Síkbarajzolhatóság szempontjából az eredetivel azonos módon viselkedik.

Def.: térkép =

Def.: térkép = síkba rajzolt egyszerű gráf.

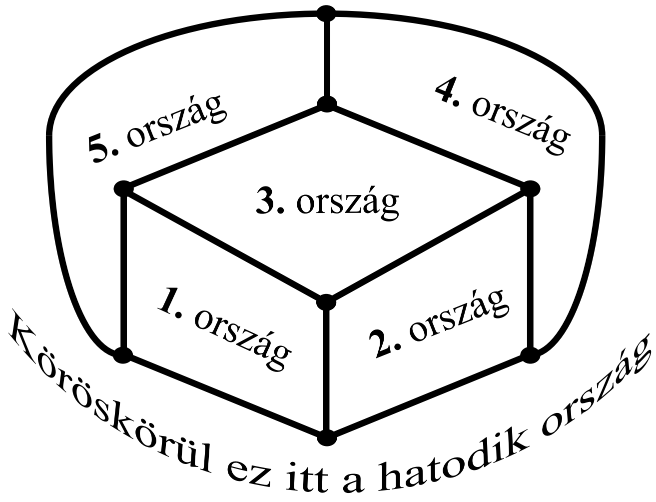


Euler tétele:



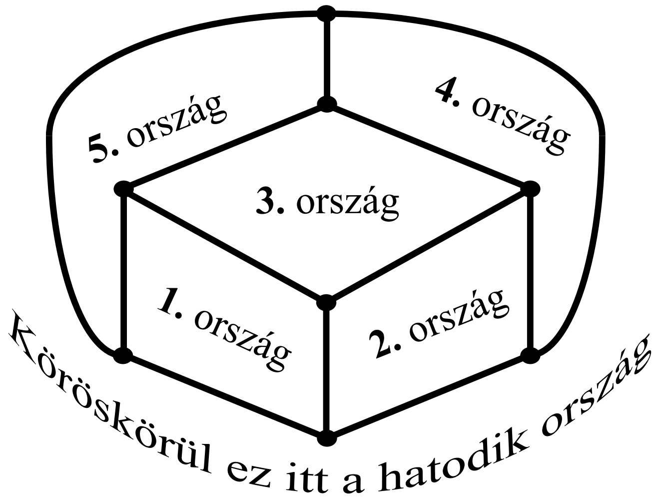
Euler tétele: Tetszőleges térkép esetén **szögpontok (csúcsok) száma** + **országok száma** = **élek száma** + **2**.

Az ábrán



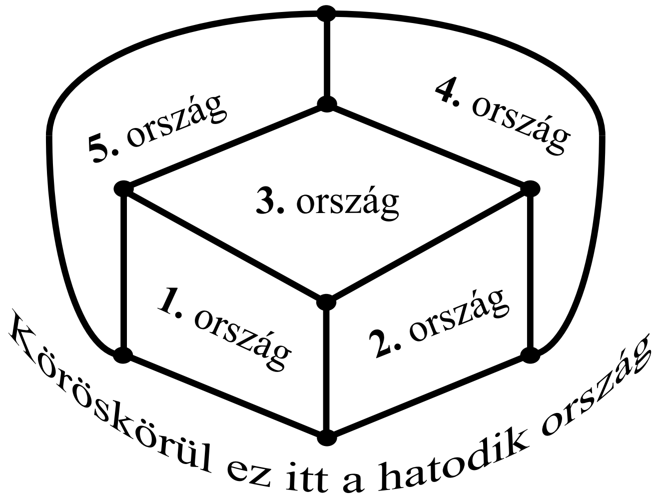
Euler tétele: Tetszőleges térkép esetén **szögpontok (csúcsok) száma** + **országok száma** = **élek száma** + **2**.

Az ábrán : 8 csúcs, 6 ország, 12 él.



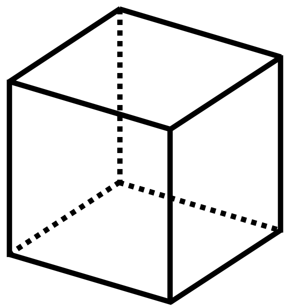
Euler tétele: Tetszőleges térkép esetén **szögpontok (csúcsok) száma** + **országok száma** = **élek száma** + **2**.

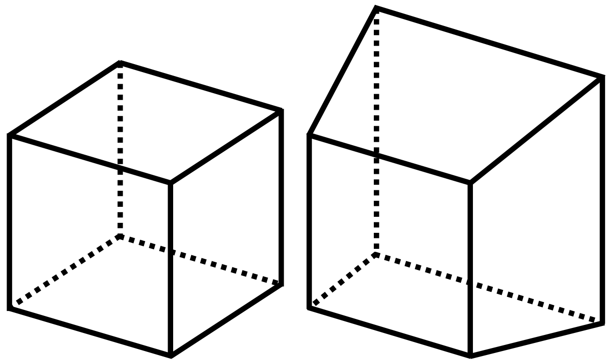
Az ábrán : 8 csúcs, 6 ország, 12 él. Poliéderekre (= síkidomok által határolt testekre, pl. kokcka, oktatéder, stb.) is érvényes, hiszen

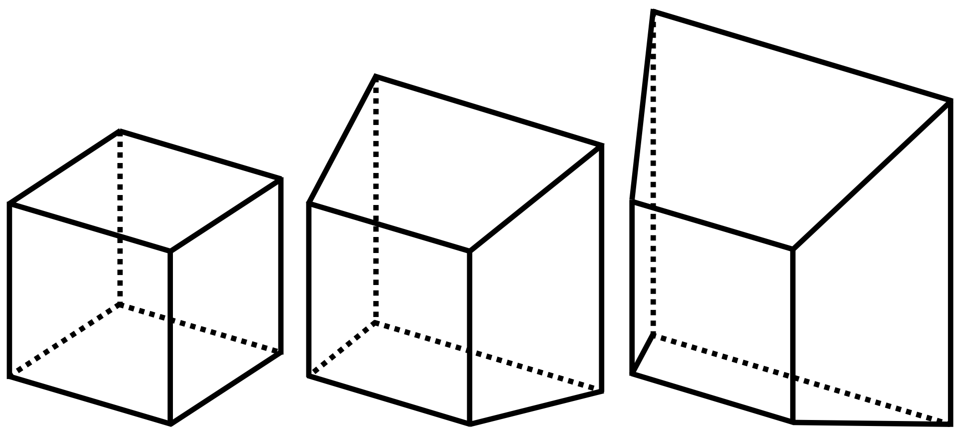


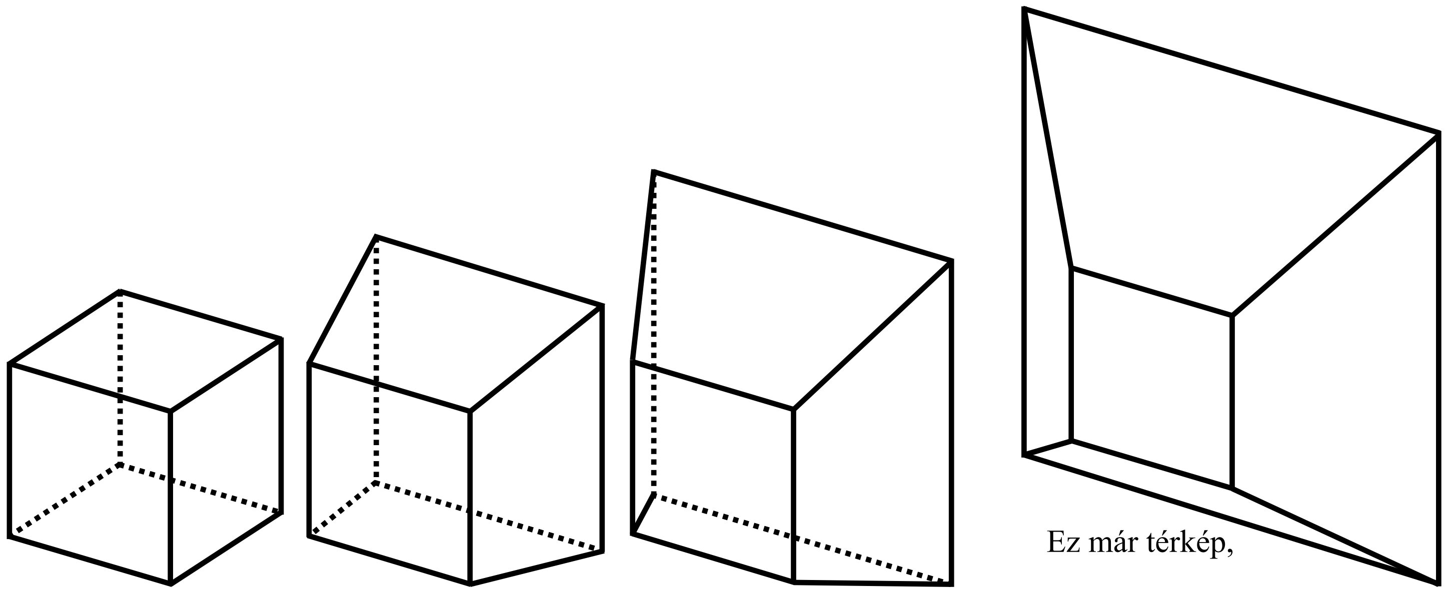
Euler tétele: Tetszőleges térkép esetén **szögpontok (csúcsok) száma** + **országok száma** = **élek száma** + **2**.

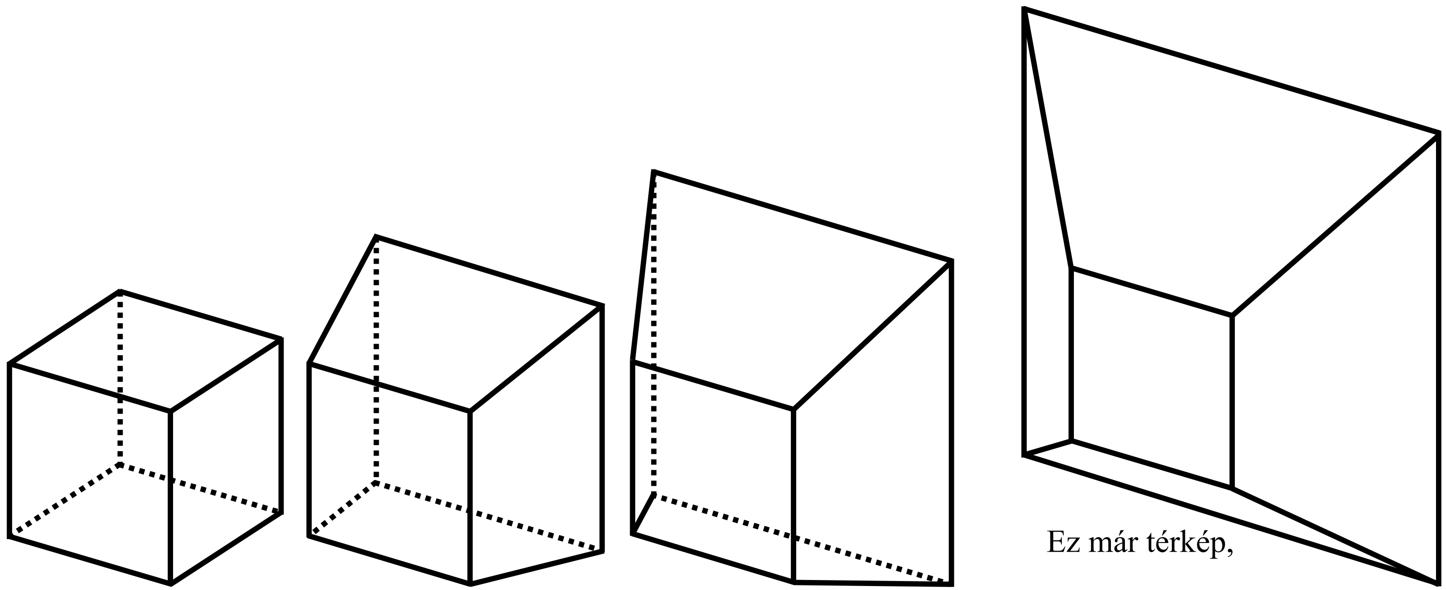
Az ábrán : 8 csúcs, 6 ország, 12 él. Poliéderekre (= síkidomok által határolt testekre, pl. kokcka, oktatéder, stb.) is érvényes, hiszen a gumiból készült poliéder egyik lapját kinyújtva, majd a többit rávasalva síkbeli térképet kapunk; a kinyújtott lap felel meg a ”végtelen országnak”. A a gumiból készült poliéder egyik lapját kinyújtva, majd a többit rávasalva síkbeli térképet kapunk; a kinyújtott lap felel meg a ”végtelen országnak”. A kocka esetén ezt a nyújtást–vasalást így szemléltethetjük:








Ez már térkép,



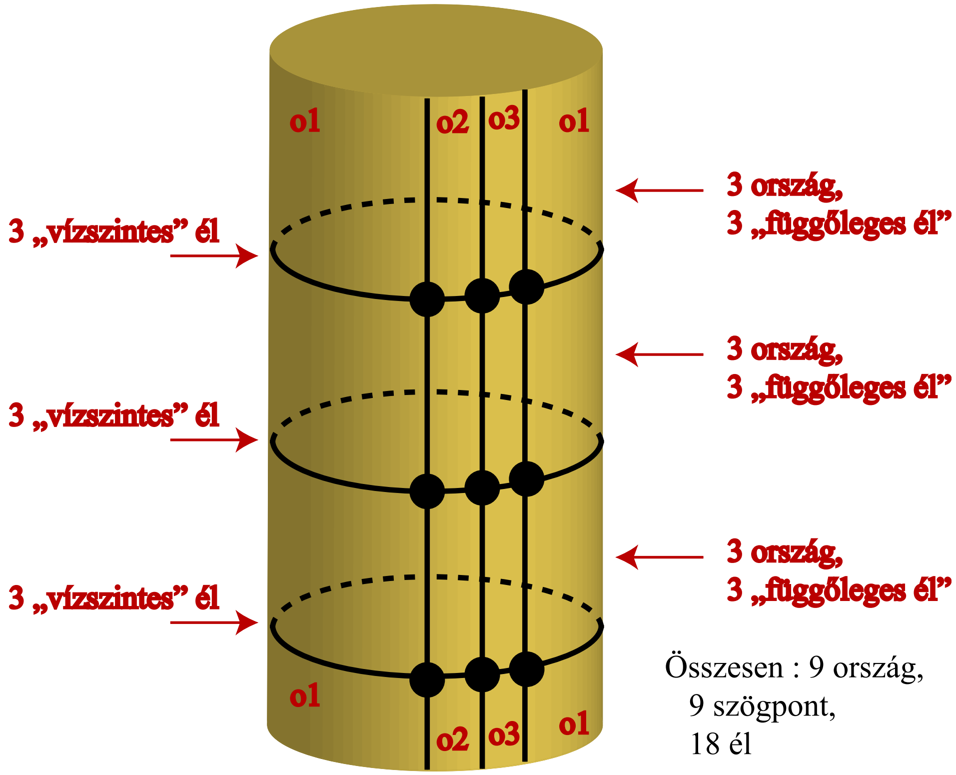
ha az alaplapot elhagyjuk és helyette a külső végtelen országot tekintjük.

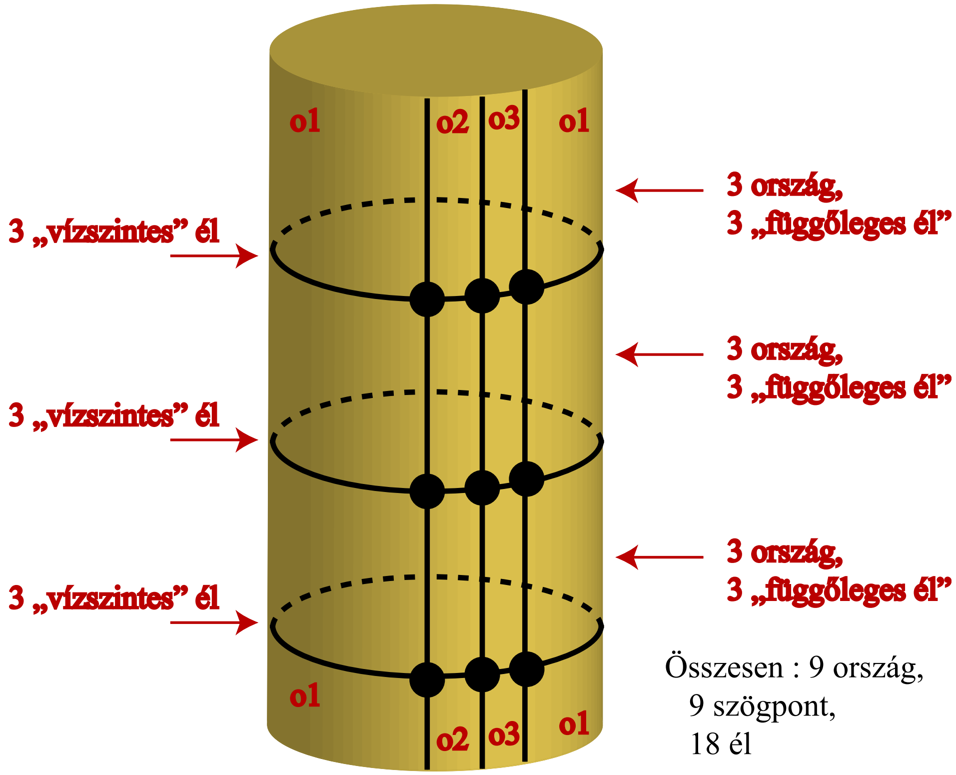
A tételt —

A tételt —hogy melyik kettőt kell összadni — a kockára gondolva lehet megjegyezni, hiszen ott 6 lap, 8 csúcs és 12 él van, tehát az élek száma $+2 =$ lapok (országok) száma $+$ csúcsok száma.

A tételt —hogy melyik kettőt kell összadni — a kockára gondolva lehet megjegyezni, hiszen ott 6 lap, 8 csúcs és 12 él van, tehát az élek száma $+2 =$ lapok (országok) száma $+$ csúcsok száma.

A **tóruszon** az Euler-tételbeli formula (”ország+szögpont $=$ él $+2$”) nem érvényes:


o1
o2
o3
o1
3 ország,
3 „függőleges él"
3 „vízszintes" él
3 ország,
3 „függőleges él"
3 „vízszintes" él
3 ország,
3 „függőleges él"
3 „vízszintes" él
o1
o2
o3
o1
Összesen : 9 ország,
9 szögpont,
18 él



(Függőleges nyújtás után a tetejét az aljával össze kell ragasztani.)

(Az Euler-féle poliéder érvényét vizsgálva a ”kétdimenziós lények” is ki tudják deríteni, hogy gömbön vagy tóruszon élnek.

(Az Euler-féle poliéder érvényét vizsgálva a ”kétdimenziós lények” is ki tudják deríteni, hogy gömbön vagy tóruszon élnek.

45. Tétel. *(***Kuratowski tétele***)*

(Az Euler-féle poliéder érvényét vizsgálva a ”kétdimenziós lények” is ki tudják deríteni, hogy gömbön vagy tóruszon élnek.

45. Tétel. *(***Kuratowski tétele***) Egy egyszerű gráf pontosan akkor síkgráf, ha nincs olyan részgráfja, amelyik a három ház—három kút gráfból vagy a teljes ötszögből keletkezik úgy, hogy annak éleit pontokkal továbbosztjuk.*

Tehát

(Az Euler-féle poliéder érvényét vizsgálva a ”kétdimenziós lények” is ki tudják deríteni, hogy gömbön vagy tóruszon élnek.

45. Tétel. (**Kuratowski tétele**) *Egy egyszerű gráf pontosan akkor síkgráf, ha nincs olyan részgráfja, amelyik a három ház—három kút gráfból vagy a teljes ötszögből keletkezik úgy, hogy annak éleit pontokkal továbbosztjuk.*

Tehát — ezen tétel következtében — a három ház—három kút gráf nem síkgráf, és a teljes ötszög sem.

Def.: Egy egyszerű gráf **kromatikus száma** az a legkisebb olyan $k \in \mathbf{N}$ szám, amelyre a gráf **szögpontjai** kiszínezhetők k színnel úgy, hogy bármely él végpontjai különböző színűek.

Def.: Egy egyszerű gráf **kromatikus száma** az a legkisebb olyan $k \in \mathbb{N}$ szám, amelyre a gráf **szögpontjai** kiszínezhetők k színnel úgy, hogy bármely él végpontjai különböző színűek.

Természetesen minden egyes szögpont pontosan egy színnel színezendő.

46. Tétel. *(***Négyszíntétel***): Bármely egyszerű síkgráf négyszínezhető (*

Def.: Egy egyszerű gráf **kromatikus száma** az a legkisebb olyan $k \in \mathbf{N}$ szám, amelyre a gráf **szögpontjai** kiszínezhetők k színnel úgy, hogy bármely él végpontjai különböző színűek.

Természetesen minden egyes szögpont pontosan egy színnel színezendő.

46. Tétel. *(**Négyszíntétel**): Bármely egyszerű síkgráf négyszínezhető (azaz a kromatikus száma $\leq$ 4.)*

Def.: Egy egyszerű gráf **kromatikus száma** az a legkisebb olyan $k \in \mathbf{N}$ szám, amelyre a gráf **szögpontjai** kiszínezhetők k színnel úgy, hogy bármely él végpontjai különböző színűek.

Természetesen minden egyes szögpont pontosan egy színnel színezendő.

46. Tétel. *(**Négyszíntétel**): Bármely egyszerű síkgráf négyszínezhető (azaz a kromatikus száma $\leq$ 4.)*

Több mint száz évig „négyszínsejtés” néven élt, 1976-ban számítógépet felhasználva bizonyította Appel és Haken. A négyszínsejtést házi feladatként adták fel annak idején angol diákoknak a szünet idejére.

Def.: Egy egyszerű gráf **kromatikus száma** az a legkisebb olyan $k \in \mathbf{N}$ szám, amelyre a gráf **szögpontjai** kiszínezhetők k színnel úgy, hogy bármely él végpontjai különböző színűek.

Természetesen minden egyes szögpont pontosan egy színnel színezendő.

46. Tétel. *(***Négyszíntétel***): Bármely egyszerű síkgráf négyszínezhető (azaz a kromatikus száma* $\leq$ *4.)*

Több mint száz évig „négyszínsejtés” néven élt, 1976-ban számítógépet felhasználva bizonyította Appel és Haken. A négyszínsejtést házi feladatként adták fel annak idején angol diákoknak a szünet idejére.

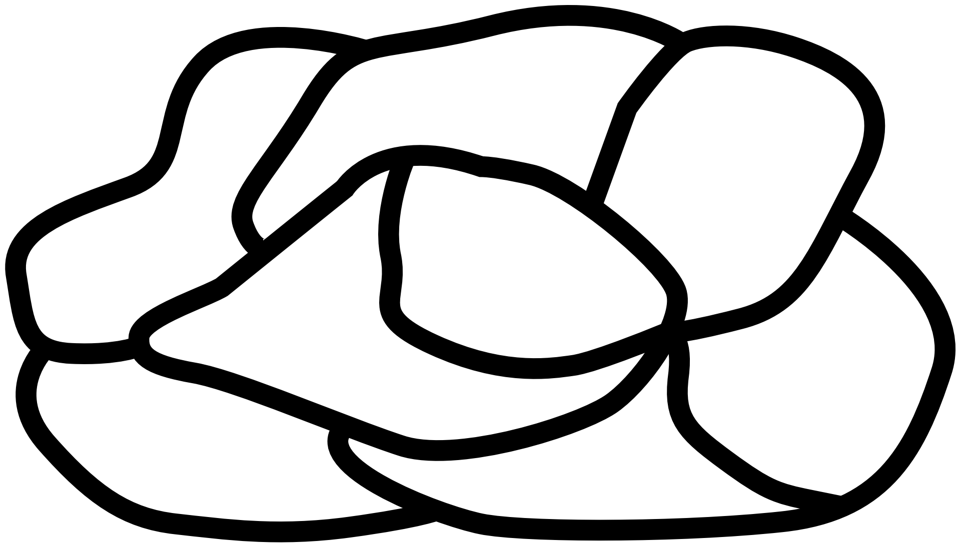
Következmény (A négyszíntétel közismertebb alakja): A síkon minden térkép kiszínezhető legfeljebb négy színnel.

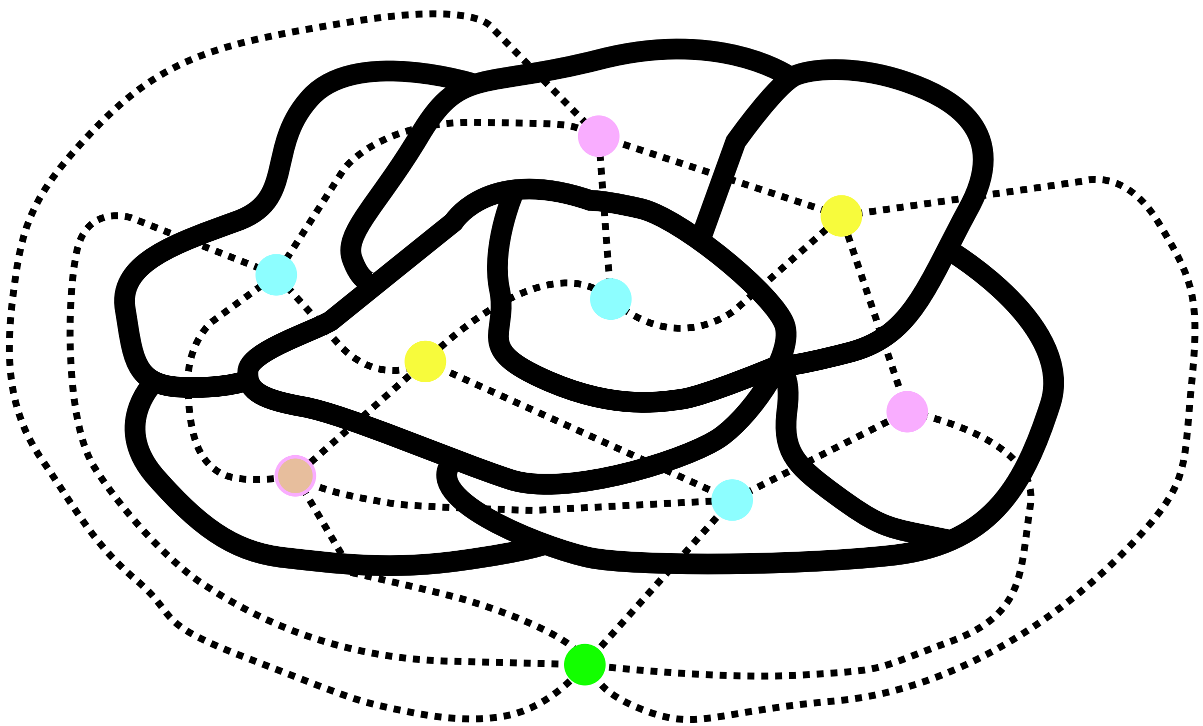
Következmény (A négyszíntétel közismertebb alakja): A síkon minden térkép kiszínezhető legfeljebb négy színnel.

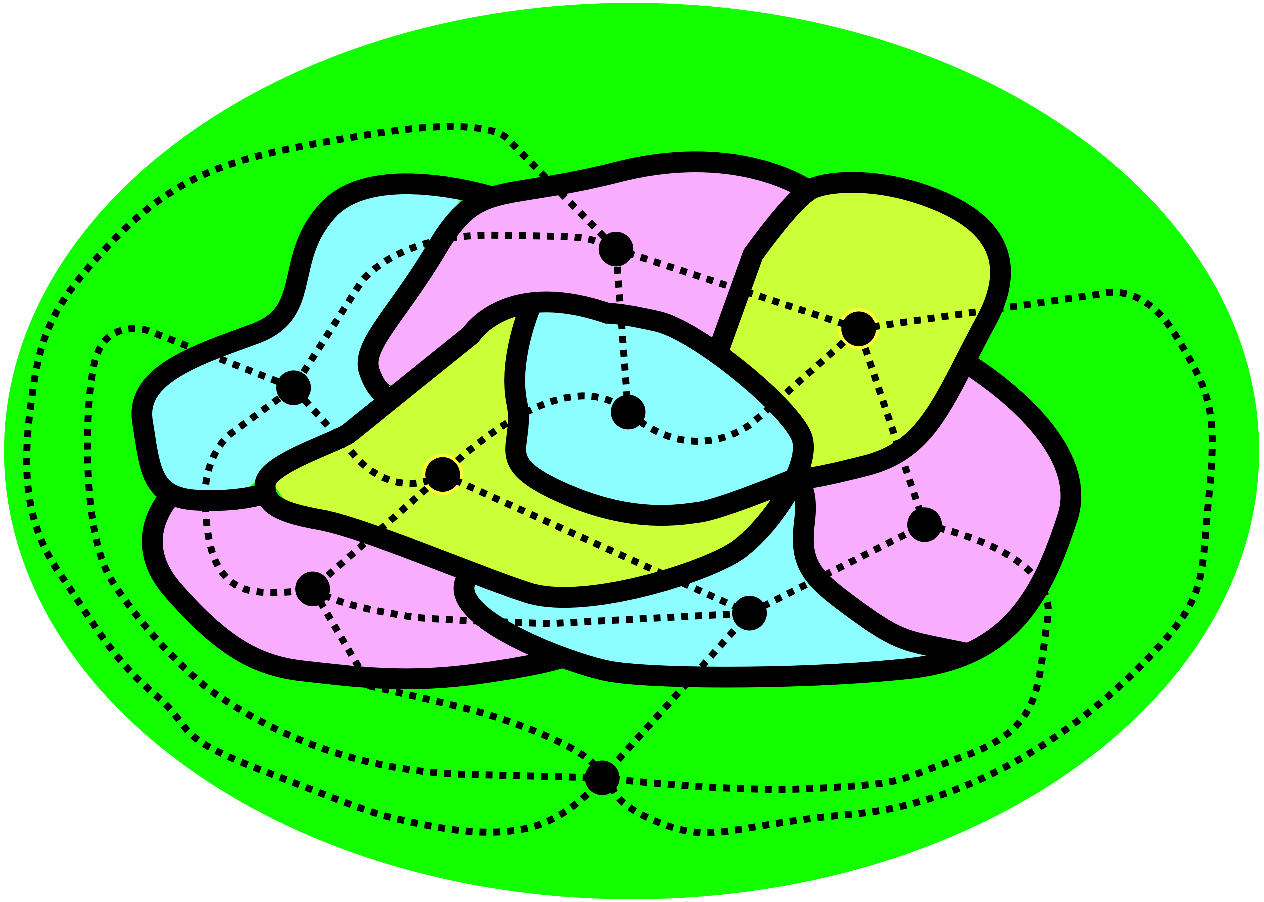
Ugyanis ha az országok fővárosait egy gráf szögpontjainak tekintjük,

Következmény (A négyszíntétel közismertebb alakja): A síkon minden térkép kiszínezhető legfeljebb négy színnel.

Ugyanis ha az országok fővárosait egy gráf szögpontjainak tekintjük, és két fővárost pontosan akkor kötünk össze éllel, ha a két országnak van közös határa (és ez esetben az él a közös határon menjen át), akkor a kapott síkgráf kiszínezése egyúttal a térkép kiszínezését is adja, ld. az alábbi három színes ábrán:







A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

Számos művelettel találkoztunk már az eddigiek során:

A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

Számos művelettel találkoztunk már az eddigiek során: logikai műveletek (pl. konjunkció),

A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

Számos művelettel találkoztunk már az eddigiek során: logikai műveletek (pl. konjunkció), aritmetikai műveletek (pl. összeadás),

A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

Számos művelettel találkoztunk már az eddigiek során: logikai műveletek (pl. konjunkció), aritmetikai műveletek (pl. összeadás), halmazműveletek (pl. szimmetrikus differencia), stb.

A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

Számos művelettel találkoztunk már az eddigiek során: logikai műveletek (pl. konjunkció), aritmetikai műveletek (pl. összeadás), halmazműveletek (pl. szimmetrikus differencia), stb. Sok esetben a műveletek tulajdonságait is tanulmányoztuk (pl. a metszetképzés disztributív az unióra, stb.)

A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

Számos művelettel találkoztunk már az eddigiek során: logikai műveletek (pl. konjunkció), aritmetikai műveletek (pl. összeadás), halmazműveletek (pl. szimmetrikus differencia), stb. Sok esetben a műveletek tulajdonságait is tanulmányoztuk (pl. a metszetképzés disztributív az unióra, stb.) Most az eddigieknél szisztematikusabban tanulmányozzuk a műveleteket **általában**: ily módon egyrészt az ismereteinket rendszerezzük,

A gráf kromatikus számának meghatározása, illetve annak ismeretében a megfelelő színezés megtalálása algoritmus szempontjából nehéz probléma.

Algebrai struktúrák

Számos művelettel találkoztunk már az eddigiek során: logikai műveletek (pl. konjunkció), aritmetikai műveletek (pl. összeadás), halmazműveletek (pl. szimmetrikus differencia), stb. Sok esetben a műveletek tulajdonságait is tanulmányoztuk (pl. a metszetképzés disztributív az unióra, stb.) Most az eddigieknél szisztematikusabban tanulmányozzuk a műveleteket **általában**: ily módon egyrészt az ismereteinket rendszerezzük, és természetesen bővítjük is.

Definíció: Legyen A nemüres halmaz, $n \in \mathbf{N}_0$. Ekkor az $A^n \to A$ leképezéseket A-n értelmezett n-változós **műveleteknek** nevezzük. Az n a művelet **változószáma** (más néven: **aritása**).

Definíció: Legyen A nemüres halmaz, $n \in \mathbf{N}_0$. Ekkor az $A^n \rightarrow A$ leképezéseket A-n értelmezett n-változós **műveleteknek** nevezzük. Az n a művelet **változószáma** (más néven: **aritása**).

A függvénykalkulusban (más néven predikátumkalkulusban) is találkoztunk már a művelet fogalmával: az interpretáció során a függvényjelekhez műveleteket rendeltünk hozzá.

Definíció: Legyen A nemüres halmaz, $n \in \mathbf{N}_0$. Ekkor az $A^n \to A$ leképezéseket A-n értelmezett n-változós **műveleteknek** nevezzük. Az n a művelet **változószáma** (más néven: **aritása**).

A függvénykalkulusban (más néven predikátumkalkulusban) is találkoztunk már a művelet fogalmával: az interpretáció során a függvényjelekhez műveleteket rendeltünk hozzá. A függvényjelnek, más néven műveleti jelnek *az a dolga*, hogy konkrét műveletet jelöljön.)

A műveleteket műveleti jelekkel (más néven függvényjelekkel) jelöljük.

A műveleteket műveleti jelekkel (más néven függvényjelekkel) jelöljük. Ha semmi különöset nem teszünk fel a jelölendő műveletről, akkor latin kisbetűket haszálunk:

A műveleteket műveleti jelekkel (más néven függvényjelekkel) jelöljük. Ha semmi különöset nem teszünk fel a jelölendő műveletről, akkor latin kisbetűket haszálunk:

$$f : A^n \to A, \qquad (x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n).$$

Használható (de az az algebrában kevésbé elterjedt) a lengyel jelölés:

$$f : A^n \to A, \qquad (x_1, \ldots, x_n) \mapsto f x_1 \ldots x_n$$

A műveleteket műveleti jelekkel (más néven függvényjelekkel) jelöljük. Ha semmi különöset nem teszünk fel a jelölendő műveletről, akkor latin kisbetűket haszálunk:

$$f : A^n \to A, \qquad (x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n).$$

Használható (de az az algebrában kevésbé elterjedt) a lengyel jelölés:

$$f : A^n \to A, \qquad (x_1, \ldots, x_n) \mapsto f x_1 \ldots x_n$$

és a a fordított lengyel jelölés:

$$f : A^n \to A, \qquad (x_1, \ldots, x_n) \mapsto x_1 \ldots x_n f$$

A műveleteket műveleti jelekkel (más néven függvényjelekkel) jelöljük. Ha semmi különöset nem teszünk fel a jelölendő műveletről, akkor latin kisbetűket haszálunk:

$$f : A^n \to A, \qquad (x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n).$$

Használható (de az az algebrában kevésbé elterjedt) a lengyel jelölés:

$$f : A^n \to A, \qquad (x_1, \dots, x_n) \mapsto f x_1 \dots x_n$$

és a a fordított lengyel jelölés:

$$f : A^n \to A, \qquad (x_1, \dots, x_n) \mapsto x_1 \dots x_n f$$

is.

Természetesen a hagyományos jólismert műveleteket a szokott módon (is) jelölhetjük.

Természetesen a hagyományos jólismert műveleteket a szokott módon (is) jelölhetjük. Pl. az egész számok halmazán értelmezett összeadási művelet —

Természetesen a hagyományos jólismert műveleteket a szokott módon (is) jelölhetjük. Pl. az egész számok halmazán értelmezett összeadási művelet — amely egy $\mathbf{Z}^2 \to \mathbf{Z}$ leképezés —

Természetesen a hagyományos jólismert műveleteket a szokott módon (is) jelölhetjük. Pl. az egész számok halmazán értelmezett összeadási művelet — amely egy $\mathbf{Z}^2 \to \mathbf{Z}$ leképezés — az (x, y) elempár képét nem $+(x, y)$ hanem $x + y$ jelöli.

Természetesen a hagyományos jólismert műveleteket a szokott módon (is) jelölhetjük. Pl. az egész számok halmazán értelmezett összeadási művelet — amely egy $\mathbf{Z}^2 \to \mathbf{Z}$ leképezés — az (x, y) elempár képét nem $+(x, y)$ hanem $x + y$ jelöli.

A művelet megadásához természetesen az A halmaz megadása is hozzátartozik. Ez többnyire értelemszerű, de ha nem, akkor a művelet jelét az A halmazzal megindexeljük.

Természetesen a hagyományos jólismert műveleteket a szokott módon (is) jelölhetjük. Pl. az egész számok halmazán értelmezett összeadási művelet — amely egy $\mathbf{Z}^2 \to \mathbf{Z}$ leképezés — az (x, y) elempár képét nem $+(x, y)$ hanem $x + y$ jelöli.

A művelet megadásához természetesen az A halmaz megadása is hozzátartozik. Ez többnyire értelemszerű, de ha nem, akkor a művelet jelét az A halmazzal megindexeljük. Tehát pl. az egész számok összadásának műveletét a racionális számok halmazán értelmezett összeadási művelettől szükség esetén úgy különböztetjük meg, hogy az előbbit $+_{\mathbf{Z}}$, az utóbbit pedig $+_{\mathbf{Q}}$ jelöli.

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x, y)$-t felírva):

$$x \wedge y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x, y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x, y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x, y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$

$$x + y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x, y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$

$$x + y, \qquad x - y \qquad , x^y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$

$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x, y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x, y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

A nem közismert kétváltozós műveletek is jelölhetők speciális jelekkel, például (megint csak mindjárt az $f(x, y)$-t felírva):

$$x \circ y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

A nem közismert kétváltozós műveletek is jelölhetők speciális jelekkel, például (megint csak mindjárt az $f(x,y)$-t felírva):

$$x \circ y, \qquad x * y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

A nem közismert kétváltozós műveletek is jelölhetők speciális jelekkel, például (megint csak mindjárt az $f(x,y)$-t felírva):

$$x \circ y, \qquad x * y, \qquad x \bullet y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

A nem közismert kétváltozós műveletek is jelölhetők speciális jelekkel, például (megint csak mindjárt az $f(x,y)$-t felírva):

$$x \circ y, \qquad x * y, \qquad x \bullet y, \qquad x \sqcap y$$
$$x \diamond y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

A nem közismert kétváltozós műveletek is jelölhetők speciális jelekkel, például (megint csak mindjárt az $f(x,y)$-t felírva):

$$x \circ y, \qquad x * y, \qquad x \bullet y, \qquad x \sqcap y$$
$$x \diamond y, \qquad x \oslash y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

A nem közismert kétváltozós műveletek is jelölhetők speciális jelekkel, például (megint csak mindjárt az $f(x,y)$-t felírva):

$$x \circ y, \qquad x * y, \qquad x \bullet y, \qquad x \sqcap y$$
$$x \diamond y, \qquad x \oslash y, \qquad x \uplus y,$$

Néhány tipikus jelölés közismert **kétváltozós** műveletre (mindjárt az $f(x,y)$-t felírva):

$$x \wedge y, \qquad x \leftrightarrow y, \qquad x \cap y, \qquad x \triangle y$$
$$x + y, \qquad x - y \qquad , x^y, \qquad x \cdot y, \qquad xy\,.$$

A nem közismert kétváltozós műveletek is jelölhetők speciális jelekkel, például (megint csak mindjárt az $f(x,y)$-t felírva):

$$x \circ y, \qquad x * y, \qquad x \bullet y, \qquad x \sqcap y$$
$$x \diamond y, \qquad x \oslash y, \qquad x \uplus y, \qquad xy\ .$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.)

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is.

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2,$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1},$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x},$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x}, \qquad -x,$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x}, \qquad -x, \qquad \sin x$$

$$\widehat{x},$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x}, \qquad -x, \qquad \sin x$$

$$\widehat{x}, \qquad \neg x,$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x}, \qquad -x, \qquad \sin x$$

$$\widehat{x}, \qquad \neg x, \qquad \tilde{x},$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x}, \qquad -x, \qquad \sin x$$

$$\widehat{x}, \qquad \neg x, \qquad \tilde{x}, \qquad x',$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x}, \qquad -x, \qquad \sin x$$

$$\widehat{x}, \qquad \neg x, \qquad \tilde{x}, \qquad x', \qquad \sqrt{x},$$

(A lehetőségeknek csak a nyomdatechnika, illetve a fantáziánk szab határt.) Itt jegyzem meg, hogy a **konkatenáció** (azaz egymásmellé írás) nemcsak a számok hagyományos szorzását jelölheti, hanem — amikor ezt külön megmondjuk — más műveletet is. Hasonlóan, a $+$ sem csak a számok hagyományos összeadását jelölheti, hanem más absztrakt műveletet is.

Az A **nemüres** alaphalmazon értelmezett **egyváltozós műveletek** éppen az $A \to A$ leképezések. Néhány példa ezek jelölésére (mindjárt az $x \in A$ képének jelölését megadva):

$$x^2, \qquad x^{-1}, \qquad \frac{1}{x}, \qquad -x, \qquad \sin x$$

$$\widehat{x}, \qquad \neg x, \qquad \widetilde{x}, \qquad x', \qquad \sqrt{x}, \qquad e^x \ .$$

Két megjegyzés kívánkozik ide.

Két megjegyzés kívánkozik ide. Egyrészt a $-$ jelölhet egyváltozós műveletet is (ellentettképzés) és

Két megjegyzés kívánkozik ide. Egyrészt a $-$ jelölhet egyváltozós műveletet is (ellentettképzés) és kétváltozós műveletet is (kivonás). Másrészt a hagyományos jelek (pl. a $-x$) is jelölhet absztrakt műveletet, ha úgy nyilatkozunk.

Véges halmazon műveletet értéktáblázattal is megadhatunk:

Egyváltozós:

$$\begin{array}{c|c} f & \\ \hline \vdots & \vdots \\ a & f(a) \\ \vdots & \vdots \end{array}$$

g	
0	3
1	2
2	1
3	0

Kétváltozós:

$$\begin{array}{c|ccc} \circ & \cdots & b & \cdots \\ \hline \vdots & & & \\ a & & a \circ b & \\ \vdots & & & \end{array}$$

$$\begin{array}{r|c|c|c|c|c|l} & & & & & b= & \\ & \circ & 0 & 1 & 2 & 3 & \\ \hline & 0 & 0 & 0 & 0 & 0 & \\ & 1 & 0 & 1 & 2 & 3 & \\ a= & 2 & 0 & 2 & 0 & 2 & =a \circ b \\ & 3 & 0 & 3 & 2 & 1 & \end{array}$$

Véges halmazon műveletet értéktáblázattal is megadhatunk:

Egyváltozós:

f	
$\vdots$	$\vdots$
a	$f(a)$
$\vdots$	$\vdots$

g	
0	3
1	2
2	1
3	0

Kétváltozós:

$\circ$	$\dots$ b $\dots$
$\vdots$	
a	$a \circ b$
$\vdots$	

$\circ$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Megjegyzés: úgy is lehetne, mint a logikai műveletek esetén (de kétváltozósnál az ritka).

Külön értelmezési nehézséget vet fel a nullaváltozós művelet fogalma. Tetszőleges A nemüres halmaz nulladik hatványa az egyelemű $\{\emptyset\}$ halmaz —

Külön értelmezési nehézséget vet fel a nullaváltozós művelet fogalma. Tetszőleges A nemüres halmaz nulladik hatványa az egyelemű $\{\emptyset\}$ halmaz — annak mintájára, hogy a számok nulladik hatványa 1.

Külön értelmezési nehézséget vet fel a nullaváltozós művelet fogalma. Tetszőleges A nemüres halmaz nulladik hatványa az egyelemű $\{\emptyset\}$ halmaz — annak mintájára, hogy a számok nulladik hatványa 1. Mármost ha a kiindulási A^0 halmaz egyelemű, akkor tetszőleges $A^0 \to A$ művelet megadása nem jelent mást, mint azon egyetlen elem képének a megadását. Ezek után érthető és az előző definícióval összhangban van, hogy a továbbiakban:

Külön értelmezési nehézséget vet fel a nullaváltozós művelet fogalma. Tetszőleges A nemüres halmaz nulladik hatványa az egyelemű $\{\emptyset\}$ halmaz — annak mintájára, hogy a számok nulladik hatványa 1. Mármost ha a kiindulási A^0 halmaz egyelemű, akkor tetszőleges $A^0 \to A$ művelet megadása nem jelent mást, mint azon egyetlen elem képének a megadását. Ezek után érthető és az előző definícióval összhangban van, hogy a továbbiakban:

Definíció: Az A halmazon megadott nullaváltozós művelet nem más, mint az A egy rögzített (konstans) eleme.

Szokás pl. a nullaváltozós műveletet e-vel, 1-gyel, 0-val jelölni.

Algebra

Algebra i struktúra

Algebrai struktúra

Definíció: **Algebrai struktúrán** vagy röviden csak **algebrán**

Algebrai struktúra

Definíció: **Algebrai struktúrán** vagy röviden csak **algebrán** egy (A, F) párt értünk, ahol A **nemüres** halmaz, F pedig A-n értelmezett műveleteknek egy adott halmaza.

Algebrai struktúra

Definíció: **Algebrai struktúrán** vagy röviden csak **algebrán** egy (A, F) párt értünk, ahol A **nemüres** halmaz, F pedig A-n értelmezett műveleteknek egy adott halmaza.

Fontos megjegyeznünk, hogy az algebra nem más, mint egy olyan elsőrendű nyelv modellje (interpretációja), amelyben a függvényjeleken kívül az egyetlen predikátum az egyenlőségjel (és azt a szokásos módon interpretáljuk). F lehet üres is, de az nem túlzottan érdekes eset.

Ha F-nek kevés eleme van, akkor a jelölésben F helyett az elemeit (azaz a műveleteket) is felsorolhatjuk. Pl. $(\mathbf{Z}; \{+, \cdot\})$ és $(\mathbf{Z}; +, \cdot)$ ugyanazt jelenti. Csak olyan jelölést szabad használni, amelynél

Ha F-nek kevés eleme van, akkor a jelölésben F helyett az elemeit (azaz a műveleteket) is felsorolhatjuk. Pl. $(\mathbf{Z}; \{+, \cdot\})$ és $(\mathbf{Z}; +, \cdot)$ ugyanazt jelenti. Csak olyan jelölést szabad használni, amelynél — konvenció vagy előzetes közlés alapján — az olvasó tudja, hogy az egyes műveleti jelek hányváltozós műveletet jelölnek.

Ha F-nek kevés eleme van, akkor a jelölésben F helyett az elemeit (azaz a műveleteket) is felsorolhatjuk. Pl. $(\mathbf{Z}; \{+, \cdot\})$ és $(\mathbf{Z}; +, \cdot)$ ugyanazt jelenti. Csak olyan jelölést szabad használni, amelynél — konvenció vagy előzetes közlés alapján — az olvasó tudja, hogy az egyes műveleti jelek hányváltozós műveletet jelölnek. Tehát pl. önmagában $(\mathbf{Z}; -)$ kevés, mert azt is meg kell mondani, hogy a $-$ jel egy- vagy kétváltozós.

Végtelen sok algebrai struktúra definiálható, még

Végtelen sok algebrai struktúra definiálható, még akkor is, ha az A alaphalmaz egy rögzített véges halmaz.

Végtelen sok algebrai struktúra definiálható, még akkor is, ha az A alaphalmaz egy rögzített véges halmaz. De természetesen nem mindegyik érdekes és hasznos számunkra, ahogy

Végtelen sok algebrai struktúra definiálható, még akkor is, ha az A alaphalmaz egy rögzített véges halmaz. De természetesen nem mindegyik érdekes és hasznos számunkra, ahogy pl. a folytonos valós függvények közül se mindegyik.

Végtelen sok algebrai struktúra definiálható, még akkor is, ha az A alaphalmaz egy rögzített véges halmaz. De természetesen nem mindegyik érdekes és hasznos számunkra, ahogy pl. a folytonos valós függvények közül se mindegyik. Egyes könyvek az algebra és a tartóhalmaza között nem tesznek jelölésbeli különbséget, de mi igen.

Végtelen sok algebrai struktúra definiálható, még akkor is, ha az A alaphalmaz egy rögzített véges halmaz. De természetesen nem mindegyik érdekes és hasznos számunkra, ahogy pl. a folytonos valós függvények közül se mindegyik. Egyes könyvek az algebra és a tartóhalmaza között nem tesznek jelölésbeli különbséget, de mi igen.

A műveleteknek és az algebrai struktúráknak lehetnek speciális jó tulajdonságai. Némelyek elég fontosak és hasznosak ahhoz, hogy elnevezést és tanulmányozást érdemeljenek. (Ez már

Végtelen sok algebrai struktúra definiálható, még akkor is, ha az A alaphalmaz egy rögzített véges halmaz. De természetesen nem mindegyik érdekes és hasznos számunkra, ahogy pl. a folytonos valós függvények közül se mindegyik. Egyes könyvek az algebra és a tartóhalmaza között nem tesznek jelölésbeli különbséget, de mi igen.

A műveleteknek és az algebrai struktúráknak lehetnek speciális jó tulajdonságai. Némelyek elég fontosak és hasznosak ahhoz, hogy elnevezést és tanulmányozást érdemeljenek. (Ez már az ismereteink rendszerezése miatt is megéri, de további haszna is van.)

A matematikából a természettudományokban leginkább az analízis, a geometria és a sztochasztika témakörébe eső elméleteket használják, ilyen pl. a fizika és ilyenek a mérnöki tudományok. Az algebrai struktúrák viszonylag kisebb szerephez jutnak, A matematikából a természettudományokban leginkább az analízis, a geometria és a sztochasztika témakörébe eső elméleteket használják, ilyen pl. a fizika és ilyenek a mérnöki tudományok. Az algebrai struktúrák viszonylag kisebb szerephez jutnak, de pl. a kristálytanban előfordulnak.

Az informatikában viszont az algebrai struktúrák és a műveletek szerepe megnő. A programozási nyelvekben beépített műveletek vannak és továbbiakat is lehet definiálni. A progam is felfogható műveletnek, amely a bemeneti jelekből eredményként az outputot adja. A hibajavító kódolások igen érdekes és fontos — eddig nem tanult — algebrai struktúrákon alapulnak.

Az informatikában viszont az algebrai struktúrák és a műveletek szerepe megnő. A programozási nyelvekben beépített műveletek vannak és továbbiakat is lehet definiálni. A progam is felfogható műveletnek, amely a bemeneti jelekből eredményként az outputot adja. A hibajavító kódolások igen érdekes és fontos — eddig nem tanult — algebrai struktúrákon alapulnak. Ugyancsak hasznosak az algebrai struktúrák a matematikai titkosírások elméletében.

A fokozatosság elvének megfelelően először csak speciális algebrákkal foglalkozunk.

Definíció: Az egyetlen kétváltozós művelettel rendelkező algebrai struktúra neve: **grupoid**.

A fokozatosság elvének megfelelően először csak speciális algebrákkal foglalkozunk.

Definíció: Az egyetlen kétváltozós művelettel rendelkező algebrai struktúra neve: **grupoid**. A grupoid műveletét többnyire szorzás (egymás mellé írás) jelöli, de más jelölés is elképzelhető: azaz

A fokozatosság elvének megfelelően először csak speciális algebrákkal foglalkozunk.

Definíció: Az egyetlen kétváltozós művelettel rendelkező algebrai struktúra neve: **grupoid**. A grupoid műveletét többnyire szorzás (egymás mellé írás) jelöli, de más jelölés is elképzelhető: azaz egy grupoidot nemcsak $(A; \cdot)$ jelölhet (amikoris egymásmellé írás is jelölheti a műveletet), hanem pl.

A fokozatosság elvének megfelelően először csak speciális algebrákkal foglalkozunk.

Definíció: Az egyetlen kétváltozós művelettel rendelkező algebrai struktúra neve: **grupoid**. A grupoid műveletét többnyire szorzás (egymás mellé írás) jelöli, de más jelölés is elképzelhető: azaz egy grupoidot nemcsak $(A;\cdot)$ jelölhet (amikoris egymásmellé írás is jelölheti a műveletet), hanem pl. $(A;\oplus)$ is.

Definíció: Legyen $(A; \cdot)$ egy grupoid. Azt mondjuk, hogy ez a grupoid (vagy a rajta értelmezett művelet)

— **kommutatív** $\overset{\text{def}}{\iff}$ **bármely** $a, b \in A$-ra $ab = ba$,

— **asszociatív** $\overset{\text{def}}{\iff}$ **bármely** $a, b, c \in A$-ra $(ab)c = a(bc)$.

Definíció: Legyen $(A; \cdot)$ egy grupoid. Azt mondjuk, hogy ez a grupoid (vagy a rajta értelmezett művelet)

— **kommutatív** $\overset{\text{def}}{\Longleftrightarrow}$ **bármely** $a, b \in A$-ra $ab = ba$,

— **asszociatív** $\overset{\text{def}}{\Longleftrightarrow}$ **bármely** $a, b, c \in A$-ra $(ab)c = a(bc)$.

Definíció: Legyen $(A; \cdot)$ egy grupoid. Azt mondjuk, hogy ez a grupoid (vagy a rajta értelmezett művelet)

— **kommutatív** $\overset{\text{def}}{\iff}$ **bármely** $a, b \in A$-ra $ab = ba$,

— **asszociatív** $\overset{\text{def}}{\iff}$ **bármely** $a, b, c \in A$-ra $(ab)c = a(bc)$.

Fontos, hogy más jelölésrendszerek esetén is ismerjük a definíciót! Íme néhány példa:

Definíció: Legyen $(A;\cdot)$ egy grupoid. Azt mondjuk, hogy ez a grupoid (vagy a rajta értelmezett művelet)

— **kommutatív** $\overset{\text{def}}{\iff}$ **bármely** $a, b \in A$-ra $ab = ba$,

— **asszociatív** $\overset{\text{def}}{\iff}$ **bármely** $a, b, c \in A$-ra $(ab)c = a(bc)$.

Fontos, hogy más jelölésrendszerek esetén is ismerjük a definíciót! Íme néhány példa:

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\stackrel{\text{def}}{\Longleftrightarrow}$

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\stackrel{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha hatványozás módjára jelöljük a műveletet, akkor

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha hatványozás módjára jelöljük a műveletet, akkor

— a művelet asszociatív $\overset{\text{def}}{\iff}$ bármely

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha hatványozás módjára jelöljük a műveletet, akkor

— a művelet asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $(a^b)^c = a^{(b^c)}$ (a második zárójelpárt el szokás hagyni).

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\overset{\text{def}}{\Longleftrightarrow}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha hatványozás módjára jelöljük a műveletet, akkor

— a művelet asszociatív $\overset{\text{def}}{\Longleftrightarrow}$ bármely $a, b, c \in A$-ra $(a^b)^c = a^{(b^c)}$ (a második zárójelpárt el szokás hagyni).

Ha pedig f-et fordított lengyel jelöléssel alkalmazzuk, akkor

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\overset{\text{def}}{\Longleftrightarrow}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha hatványozás módjára jelöljük a műveletet, akkor

— a művelet asszociatív $\overset{\text{def}}{\Longleftrightarrow}$ bármely $a, b, c \in A$-ra $(a^b)^c = a^{(b^c)}$ (a második zárójelpárt el szokás hagyni).

Ha pedig f-et fordított lengyel jelöléssel alkalmazzuk, akkor

— f asszociatív $\overset{\text{def}}{\Longleftrightarrow}$

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha hatványozás módjára jelöljük a műveletet, akkor

— a művelet asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $(a^b)^c = a^{(b^c)}$ (a második zárójelpárt el szokás hagyni).

Ha pedig f-et fordított lengyel jelöléssel alkalmazzuk, akkor

— f asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $abfcf = abcff$.

Ha f jelöli a műveletet, és az (x, y) képét $f(x, y)$, akkor

— f asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $f(f(a, b), c) = f(a, f(b, c))$.

Ha hatványozás módjára jelöljük a műveletet, akkor

— a művelet asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $(a^b)^c = a^{(b^c)}$ (a második zárójelpárt el szokás hagyni).

Ha pedig f-et fordított lengyel jelöléssel alkalmazzuk, akkor

— f asszociatív $\overset{\text{def}}{\iff}$ bármely $a, b, c \in A$-ra $abfcf = abcff$.

Követelmény: a fenti és későbbi fogalmakat a lehetséges jelölési rendszerek mindegyikében tudni kell!

Követelmény: a fenti és későbbi fogalmakat a lehetséges jelölési rendszerek mindegyikében tudni kell!

$$(ab)c = a(bc)$$

Követelmény: a fenti és későbbi fogalmakat a lehetséges jelölési rendszerek mindegyikében tudni kell!

$$(ab)c = a(bc)$$

Az asszociativitás esetén pl.

Követelmény: a fenti és későbbi fogalmakat a lehetséges jelölési rendszerek mindegyikében tudni kell!

$$(ab)c = a(bc)$$

Az asszociativitás esetén pl. azt is tudni kell, hogy a lényeg:

Követelmény: a fenti és későbbi fogalmakat a lehetséges jelölési rendszerek mindegyikében tudni kell!

$$(ab)c = a(bc)$$

Az asszociativitás esetén pl. azt is tudni kell, hogy a lényeg: adott három elem, rögzített sorrendben. Mindegy, hogy először az első kettőt helyettesítjük a szorzatukkal, és azután végezzük el a második szorzást, vagy pedig

Követelmény: a fenti és későbbi fogalmakat a lehetséges jelölési rendszerek mindegyikében tudni kell!

$$(ab)c = a(bc)$$

Az asszociativitás esetén pl. azt is tudni kell, hogy a lényeg: adott három elem, rögzített sorrendben. Mindegy, hogy először az első kettőt helyettesítjük a szorzatukkal, és azután végezzük el a második szorzást, vagy pedig először az utolsó kettőt helyettesítjük a szorzatukkal, és azután végezzük el a második szorzást.

Definíció: Legyen $(A;\cdot)$ grupoid és $e \in A$. Ha **bármely** $x \in A$-ra $ex = x$ és $xe = x$, akkor

Definíció: Legyen $(A;\cdot)$ grupoid és $e \in A$. Ha **bármely** $x \in A$-ra $ex = x$ és $xe = x$, akkor e-t a grupoid **egységelemének** nevezzük. Ha egy grupoidnak van egységeleme (más szóval: a grupoidban van egységelem), akkor **egységelemes grupoidról** beszélünk.

Definíció: Legyen $(A; \cdot)$ grupoid és $e \in A$. Ha **bármely** $x \in A$-ra $ex = x$ és $xe = x$, akkor e-t a grupoid **egységelemének** nevezzük. Ha egy grupoidnak van egységeleme (más szóval: a grupoidban van egységelem), akkor **egységelemes grupoidról** beszélünk.

2. Állítás. *Egységelemes grupoidnak pontosan egy egységeleme van.*

Bizonyítás

Definíció: Legyen $(A; \cdot)$ grupoid és $e \in A$. Ha **bármely** $x \in A$-ra $ex = x$ és $xe = x$, akkor e-t a grupoid **egységelemének** nevezzük. Ha egy grupoidnak van egységeleme (más szóval: a grupoidban van egységelem), akkor **egységelemes grupoidról** beszélünk.

2. Állítás. *Egységelemes grupoidnak pontosan egy egységeleme van.*

Bizonyítás Ha e_1 is és e_2 is egységelem, akkor

Definíció: Legyen $(A; \cdot)$ grupoid és $e \in A$. Ha **bármely** $x \in A$-ra $ex = x$ és $xe = x$, akkor e-t a grupoid **egységelemének** nevezzük. Ha egy grupoidnak van egységeleme (más szóval: a grupoidban van egységelem), akkor **egységelemes grupoidról** beszélünk.

2. Állítás. *Egységelemes grupoidnak pontosan egy egységeleme van.*

Bizonyítás Ha e_1 is és e_2 is egységelem, akkor $e_1 e_2 = e_2$, mivel e_1 egységelem, továbbá $e_1 e_2 = e_1$, mivel e_2 egységelem,

Definíció: Legyen $(A; \cdot)$ grupoid és $e \in A$. Ha **bármely** $x \in A$-ra $ex = x$ és $xe = x$, akkor e-t a grupoid **egységelemének** nevezzük. Ha egy grupoidnak van egységeleme (más szóval: a grupoidban van egységelem), akkor **egységelemes grupoidról** beszélünk.

2. Állítás. *Egységelemes grupoidnak pontosan egy egységeleme van.*

Bizonyítás Ha e_1 is és e_2 is egységelem, akkor $e_1 e_2 = e_2$, mivel e_1 egységelem, továbbá $e_1 e_2 = e_1$, mivel e_2 egységelem, és innen $e_1 = e_2$. Q.e.d.

Definíció: Legyen $(A; \cdot)$ grupoid és $z \in A$. Ha **bármely** $x \in A$-ra $zx = z$ és $xz = z$, akkor

Definíció: Legyen $(A;\cdot)$ grupoid és $z \in A$. Ha **bármely** $x \in A$-ra $zx = z$ és $xz = z$, akkor z-t a grupoid **zéruselemének** nevezzük. Ha egy grupoidnak van zéruseleme (más szóval: a grupoidban van zéruselem), akkor **zéruselemes grupoidról** beszélünk.

Definíció: Legyen $(A;\cdot)$ grupoid és $z \in A$. Ha **bármely** $x \in A$-ra $zx = z$ és $xz = z$, akkor z-t a grupoid **zéruselemének** nevezzük. Ha egy grupoidnak van zéruseleme (más szóval: a grupoidban van zéruselem), akkor **zéruselemes grupoidról** beszélünk.

3. Állítás. *Zéruselemes grupoidnak pontosan egy zéruseleme van.*

Bizonyítás

Definíció: Legyen $(A; \cdot)$ grupoid és $z \in A$. Ha **bármely** $x \in A$-ra $zx = z$ és $xz = z$, akkor z-t a grupoid **zéruselemének** nevezzük. Ha egy grupoidnak van zéruseleme (más szóval: a grupoidban van zéruselem), akkor **zéruselemes grupoidról** beszélünk.

3. Állítás. *Zéruselemes grupoidnak pontosan egy zéruseleme van.*

Bizonyítás Ha z_1 is és z_2 is zéruselem, akkor

Definíció: Legyen $(A;\cdot)$ grupoid és $z \in A$. Ha **bármely** $x \in A$-ra $zx = z$ és $xz = z$, akkor z-t a grupoid **zéruselemének** nevezzük. Ha egy grupoidnak van zéruseleme (más szóval: a grupoidban van zéruselem), akkor **zéruselemes grupoidról** beszélünk.

3. Állítás. *Zéruselemes grupoidnak pontosan egy zéruseleme van.*

Bizonyítás Ha z_1 is és z_2 is zéruselem, akkor $z_1 z_2 = z_1$, mivel z_1 zéruselem, továbbá $z_1 z_2 = z_2$, mivel z_2 zéruselem,

Definíció: Legyen $(A; \cdot)$ grupoid és $z \in A$. Ha **bármely** $x \in A$-ra $zx = z$ és $xz = z$, akkor z-t a grupoid **zéruselemének** nevezzük. Ha egy grupoidnak van zéruseleme (más szóval: a grupoidban van zéruselem), akkor **zéruselemes grupoidról** beszélünk.

3. Állítás. *Zéruselemes grupoidnak pontosan egy zéruseleme van.*

Bizonyítás Ha z_1 is és z_2 is zéruselem, akkor $z_1 z_2 = z_1$, mivel z_1 zéruselem, továbbá $z_1 z_2 = z_2$, mivel z_2 zéruselem, és innen $z_1 = z_2$. Q.e.d.

Példák: A $(\mathbf{Z}; \cdot)$ grupoidban

Példák: A $(\mathbf{Z};\cdot)$ grupoidban az 1 egységelem, a 0 pedig zéruselem. Innen

Példák: A $(\mathbf{Z};\cdot)$ grupoidban az 1 egységelem, a 0 pedig zéruselem. Innen ered az elnevezés!

Példák: A $(\mathbf{Z};\cdot)$ grupoidban az 1 egységelem, a 0 pedig zéruselem. Innen ered az elnevezés!

A $(\mathbf{Z};+)$ grupoidban viszont

Példák: A $(\mathbf{Z}; \cdot)$ grupoidban az 1 egységelem, a 0 pedig zéruselem. Innen ered az elnevezés!

A $(\mathbf{Z}; +)$ grupoidban viszont a 0 egységelem, és

Példák: A $(\mathbf{Z};\cdot)$ grupoidban az 1 egységelem, a 0 pedig zéruselem. Innen ered az elnevezés!

A $(\mathbf{Z};+)$ grupoidban viszont a 0 egységelem, és nincs zéruselem!

Félcsoport, monoid

Definíció: Félcsoport = asszociatív grupoid

Félcsoport, monoid

Definíció: Félcsoport = asszociatív grupoid

Definíció: Monoid = egységelemes félcsoport = egységelemes asszociatív grupoid

Félcsoport, monoid

Definíció: Félcsoport $=$ asszociatív grupoid

Definíció: Monoid $=$ egységelemes félcsoport $=$ egységelemes asszociatív grupoid

Példák: Egész számok additív félcsoportja: $(\mathbf{Z};+)$, ez

Félcsoport, monoid

Definíció: **Félcsoport $=$ asszociatív grupoid**

Definíció: **Monoid $=$ egységelemes félcsoport $=$ egységelemes asszociatív grupoid**

Példák: Egész számok additív félcsoportja: $(\mathbf{Z};+)$, ez monoid.

Félcsoport, monoid

Definíció: **Félcsoport = asszociatív grupoid**

Definíció: **Monoid = egységelemes félcsoport = egységelemes asszociatív grupoid**

Példák: Egész számok additív félcsoportja: $(\mathbf{Z}; +)$, ez monoid.
Egész számok multiplikatív félcsoportja: $(\mathbf{Z}; \cdot)$, ez

Félcsoport, monoid

Definíció: **Félcsoport = asszociatív grupoid**

Definíció: **Monoid = egységelemes félcsoport = egységelemes asszociatív grupoid**

Példák: Egész számok additív félcsoportja: $(\mathbf{Z};+)$, ez monoid.
Egész számok multiplikatív félcsoportja: $(\mathbf{Z};\cdot)$, ez is monoid.

Feladat: Monoid-e a pozitív egész számok additív grupoidja: $(\mathbb{N}; +)$?

Megoldás:

Feladat: Monoid-e a pozitív egész számok additív grupoidja: $(\mathbf{N};+)$?

Megoldás: Az összeadás valóban művelet, hiszen $(a,b) \in \mathbf{N}^2$-re $a+b \in \mathbf{N}$.

Feladat: Monoid-e a pozitív egész számok additív grupoidja: $(\mathbf{N};+)$?

Megoldás: Az összeadás valóban művelet, hiszen $(a,b) \in \mathbf{N}^2$-re $a+b \in \mathbf{N}$. (Ezzel a megállapítással aligha okoztam nagy meglepetést.

Feladat: Monoid-e a pozitív egész számok additív grupoidja: $(\mathbf{N}; +)$?

Megoldás: Az összeadás valóban művelet, hiszen $(a, b) \in \mathbf{N}^2$-re $a + b \in \mathbf{N}$. (Ezzel a megállapítással aligha okoztam nagy meglepetést. De bármilyen triviális is ezen megállapítás, nem szabad megfeledkezni róla.)

Feladat: Monoid-e a pozitív egész számok additív grupoidja: $(\mathbf{N};+)$?

Megoldás: Az összeadás valóban művelet, hiszen $(a,b) \in \mathbf{N}^2$-re $a+b \in \mathbf{N}$. (Ezzel a megállapítással aligha okoztam nagy meglepetést. De bármilyen triviális is ezen megállapítás, nem szabad megfeledkezni róla.) Ismeretes, hogy a pozitív egész számok (sőt a valós számok) összadása asszociatív. Tehát $(\mathbf{N};+)$-ról máris tudjuk, hogy félcsoport.

Van-e egységeleme? Figyelem, nem az a kérdés, hogy valamilyen korábban megismert egységelem, mondjuk az 1 vagy más esetben a nulla, benne van-e $\mathbb{N}$-ben! Hiszen ami az egyik algebrában egységelem, az nem feltétlenül egységelem egy másikban!

Vizsgálódjunk. Tegyük fel, hogy $e \in \mathbf{N}$ egységeleme a $(\mathbf{N}; +)$ félcsoportnak. Ez — a

Vizsgálódjunk. Tegyük fel, hogy $e \in \mathbf{N}$ egységeleme a $(\mathbf{N}; +)$ félcsoportnak. Ez — a definíció szerint — azt jelenti, hogy $e+x = x = x+e$ <u>minden</u> $x \in \mathbf{N}$-re teljesül.

Vizsgálódjunk. Tegyük fel, hogy $e \in \mathbf{N}$ egységeleme a $(\mathbf{N}; +)$ félcsoportnak. Ez — a definíció szerint — azt jelenti, hogy $e+x = x = x+e$ minden $x \in \mathbf{N}$-re teljesül. Ez azonban lehetetlen:

Vizsgálódjunk. Tegyük fel, hogy $e \in \mathbf{N}$ egységeleme a $(\mathbf{N}; +)$ félcsoportnak. Ez — a definíció szerint — azt jelenti, hogy $e+x = x = x+e$ <u>minden</u> $x \in \mathbf{N}$-re teljesül. Ez azonban lehetetlen: ez <u>egyetlen egy</u> $x \in \mathbf{N}$-re <u>sem</u> teljesül (

Vizsgálódjunk. Tegyük fel, hogy $e \in \mathbf{N}$ egységeleme a $(\mathbf{N}; +)$ félcsoportnak. Ez — a definíció szerint — azt jelenti, hogy $e+x = x = x+e$ minden $x \in \mathbf{N}$-re teljesül. Ez azonban lehetetlen: ez egyetlen egy $x \in \mathbf{N}$-re sem teljesül (hiszen $x < x + e$). Tehát $(\mathbf{N}; +)$ nem monoid (viszont félcsoport).

Példa: Az összetett pozitív egész számok multiplikatív grupoi-dja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez

Példa: Az összetett pozitív egész számok multiplikatív grupoidja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez félcsoport,

Példa: Az összetett pozitív egész számok multiplikatív grupoidja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez félcsoport, de nem monoid!

Példa: Az összetett pozitív egész számok multiplikatív grupoidja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez félcsoport, de nem monoid! (A megfontolás az előzőhöz hasonló).

Példa:

Példa: Az összetett pozitív egész számok multiplikatív grupoidja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez félcsoport, de nem monoid! (A megfontolás az előzőhöz hasonló).

Példa:

A prímszámok multiplikatív félcsoportja: $(\{2, 3, 5, 7, \ldots\}; \cdot)$

Példa: Az összetett pozitív egész számok multiplikatív grupoidja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez félcsoport, de nem monoid! (A megfontolás az előzőhöz hasonló).

Példa:

~~A prímszámok multiplikatív félcsoportja: $(\{2, 3, 5, 7, \ldots\}$~~$; \cdot)$

Példa: Az összetett pozitív egész számok multiplikatív grupoidja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez félcsoport, de nem monoid! (A megfontolás az előzőhöz hasonló).

Példa:

~~A prímszámok multiplikatív félcsoportja:~~ $(\cancel{\{2, 3, 5, 7, \ldots\}}; \cdot)$

Nem! Ez még csak nem is algebrai struktúra!

Példa: Az összetett pozitív egész számok multiplikatív grupoidja: $(\{4, 6, 8, 9, 10, \ldots\}; \cdot)$: ez félcsoport, de nem monoid! (A megfontolás az előzőhöz hasonló).

Példa:

~~A prímszámok multiplikatív félcsoportja: $(\{2, 3, 5, 7, \ldots\}$~~$; \cdot)$

Nem! Ez még csak nem is algebrai struktúra! A szorzás nem is művelet rajta, hiszen két prímszám szorzata nincs benne az alaphalmazban!

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$?

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás:

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z};*)$, ahol $a*b := a+b-ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a,b \in \mathbf{Z}$, akkor $a*b = a+b-ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid.

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z};*)$, ahol $a*b := a+b-ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a,b \in \mathbf{Z}$, akkor $a*b = a+b-ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a,b,c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a, b \in \mathbf{Z}$, akkor $a * b = a + b - ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a, b, c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a * b) * c =$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a, b \in \mathbf{Z}$, akkor $a * b = a + b - ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a, b, c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a * b) * c = (a + b - ab)$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a, b \in \mathbf{Z}$, akkor $a * b = a + b - ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a, b, c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a * b) * c = (a + b - ab) * c =$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z};*)$, ahol $a*b := a+b-ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a,b \in \mathbf{Z}$, akkor $a*b = a+b-ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a,b,c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a*b)*c = (a+b-ab)*c = (a+b-ab)$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z};*)$, ahol $a*b:=a+b-ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a, b \in \mathbf{Z}$, akkor $a*b=a+b-ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a, b, c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a*b)*c=(a+b-ab)*c=(a+b-ab)+c$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a, b \in \mathbf{Z}$, akkor $a * b = a + b - ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a, b, c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z};*)$, ahol $a*b := a+b-ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a,b \in \mathbf{Z}$, akkor $a*b = a+b-ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a,b,c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a*b)*c = (a+b-ab)*c = (a+b-ab)+c-(a+b-ab)c =$$
$$a+b-ab+c-ac-bc+abc,$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a, b \in \mathbf{Z}$, akkor $a * b = a + b - ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a, b, c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b - ab + c - ac - bc + abc,$$
$$a * (b * c) =$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z}; *)$, ahol $a * b := a + b - ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a, b \in \mathbf{Z}$, akkor $a * b = a + b - ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a, b, c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$

$$a + b - ab + c - ac - bc + abc,$$

$$a * (b * c) = a * (b + c - bc) =$$

Feladat: Monoid-e, félcsoport-e, grupoid-e $(\mathbf{Z};*)$, ahol $a*b := a+b-ab$? (Ilyen jellegű feladatok is lesznek a vizsgán.)

Megoldás: Ha $a,b \in \mathbf{Z}$, akkor $a*b = a+b-ab \in \mathbf{Z}$, tehát a művelet jól van definiálva. Ezért grupoid. Legyen $a,b,c \in \mathbf{Z}$ és — az asszociativitás eldöntése érdekében — számoljunk:

$$(a*b)*c = (a+b-ab)*c = (a+b-ab)+c-(a+b-ab)c =$$
$$a+b-ab+c-ac-bc+abc,$$
$$a*(b*c) = a*(b+c-bc) = a+(b+c-bc)-a(b+c-bc) =$$
$$a+b+c-bc-ab-ac+abc\,.$$

A kétféleképpen zárójelezett szorzatra ugyanaz adódott, tehát a művelet asszociatív, azaz $(\mathbf{Z}; *)$ félcsoport.

A kétféleképpen zárójelezett szorzatra ugyanaz adódott, tehát a művelet asszociatív, azaz $(\mathbf{Z};*)$ félcsoport.

Van-e egységeleme? Azaz van-e olyan $e \in \mathbf{Z}$, hogy **bármely** $x \in \mathbf{Z}$-re $e*x = x*e = x$ teljesül? (

A kétféleképpen zárójelezett szorzatra ugyanaz adódott, tehát a művelet asszociatív, azaz $(\mathbf{Z}; *)$ félcsoport.

Van-e egységeleme? Azaz van-e olyan $e \in \mathbf{Z}$, hogy **bármely** $x \in \mathbf{Z}$-re $e*x = x*e = x$ teljesül? (A művelet nyilván kommutatív, tehát elegendő $e * x = x$-szel foglalkozni.

A kétféleképpen zárójelezett szorzatra ugyanaz adódott, tehát a művelet asszociatív, azaz $(\mathbf{Z};*)$ félcsoport.

Van-e egységeleme? Azaz van-e olyan $e \in \mathbf{Z}$, hogy **bármely** $x \in \mathbf{Z}$-re $e*x = x*e = x$ teljesül? (A művelet nyilván kommutatív, tehát elegendő $e * x = x$-szel foglalkozni. Tehát bármely x-re

A kétféleképpen zárójelezett szorzatra ugyanaz adódott, tehát a művelet asszociatív, azaz $(\mathbf{Z}; *)$ félcsoport.

Van-e egységeleme? Azaz van-e olyan $e \in \mathbf{Z}$, hogy **bármely** $x \in \mathbf{Z}$-re $e*x = x*e = x$ teljesül? (A művelet nyilván kommutatív, tehát elegendő $e * x = x$-szel foglalkozni. Tehát bármely x-re $e + x - ex = x$, azaz $e(1 - x) = 0$. Igen, van ilyen e, mégpedig az $e = 0$.

A kétféleképpen zárójelezett szorzatra ugyanaz adódott, tehát a művelet asszociatív, azaz $(\mathbf{Z}; *)$ félcsoport.

Van-e egységeleme? Azaz van-e olyan $e \in \mathbf{Z}$, hogy **bármely** $x \in \mathbf{Z}$-re $e*x = x*e = x$ teljesül? (A művelet nyilván kommutatív, tehát elegendő $e * x = x$-szel foglalkozni. Tehát bármely x-re $e + x - ex = x$, azaz $e(1 - x) = 0$. Igen, van ilyen e, mégpedig az $e = 0$.

Tehát $(\mathbf{Z}; *)$ monoid, egységeleme a 0 szám.

Grupoidban az $a_1a_2 \ldots a_n$ "szorzatnak" általában nincs értelme, mert

Grupoidban az $a_1 a_2 \ldots a_n$ ''szorzatnak'' általában nincs értelme, mert még az sem világos, melyik két elemet kell először összeszorozni. (Már $n = 3$ esetén is eltérő eredményt kaphatunk, ha más sorrendet választunk.) Csak

Grupoidban az $a_1 a_2 \ldots a_n$ ”szorzatnak” általában nincs értelme, mert még az sem világos, melyik két elemet kell először összeszorozni. (Már $n = 3$ esetén is eltérő eredményt kaphatunk, ha más sorrendet választunk.) Csak akkor válik értelmessé, ha zárójelekkel kijelölünk valamilyen sorrendet.

Grupoidban az $a_1 a_2 \ldots a_n$ ”szorzatnak” általában nincs értelme, mert még az sem világos, melyik két elemet kell először összeszorozni. (Már $n = 3$ esetén is eltérő eredményt kaphatunk, ha más sorrendet választunk.) Csak akkor válik értelmessé, ha zárójelekkel kijelölünk valamilyen sorrendet.

47. Tétel. *Általános asszociativitás tétele: félcsoport tetszőleges $a_1, \ldots, a_n$ ($n \geq 1$) elemeire bárhogy zárójelezzük (természetesen szintaktikusan helyesen) az*

$$a_1 a_2 \ldots a_n$$

szorzatot, az eredmény független a zárójelezéstől.

Grupoidban az $a_1a_2\ldots a_n$ ”szorzatnak” általában nincs értelme, mert még az sem világos, melyik két elemet kell először összeszorozni. (Már $n=3$ esetén is eltérő eredményt kaphatunk, ha más sorrendet választunk.) Csak akkor válik értelmessé, ha zárójelekkel kijelölünk valamilyen sorrendet.

47. Tétel. *Általános asszociativitás tétele: félcsoport tetszőleges $a_1,\ldots,a_n$ ($n\geq 1$) elemeire bárhogy zárójelezzük (természetesen szintaktikusan helyesen) az*

$$a_1a_2\ldots a_n$$

szorzatot, az eredmény független a zárójelezéstől.

Mivel úgysem függ a zárójelezéstől a szorzat, a zárójeleket félcsoportban többnyire elhagyjuk.

Mivel úgysem függ a zárójelezéstől a szorzat, a zárójeleket félcsoportban többnyire elhagyjuk.

Definíció: azt mondjuk, hogy egy $(A;\cdot)$ grupoid a, b elemei **felcserélhetők**, ha $ab = ba$.

Megjegyzés:

Mivel úgysem függ a zárójelezéstől a szorzat, a zárójeleket félcsoportban többnyire elhagyjuk.

Definíció: azt mondjuk, hogy egy $(A;\cdot)$ grupoid a, b elemei **felcserélhetők**, ha $ab = ba$.

Megjegyzés: nyilván a grupoid pontosan akkor kommutatív, ha bármely két eleme felcserélhető. Szinte

Mivel úgysem függ a zárójelezéstől a szorzat, a zárójeleket félcsoportban többnyire elhagyjuk.

Definíció: azt mondjuk, hogy egy $(A; \cdot)$ grupoid a, b elemei **felcserélhetők**, ha $ab = ba$.

Megjegyzés: nyilván a grupoid pontosan akkor kommutatív, ha bármely két eleme felcserélhető. Szinte evidens az alábbi tétel.

48. Tétel. *(Általános kommutativitás tétele.)* *(1) Ha egy félcsoport* $a_1, \ldots, a_n$ *elemei páronként felcserélhetők, akkor bármely* $\pi \in S_n$ *permutációra*

$$a_{1\pi} a_{2\pi} \ldots a_{n\pi} = a_1 a_2 \ldots a_n.$$

(2)

48. Tétel. *(Általános kommutativitás tétele.)* *(1) Ha egy félcsoport* $a_1, \ldots, a_n$ *elemei páronként felcserélhetők, akkor bármely* $\pi \in S_n$ *permutációra*

$$a_{1\pi} a_{2\pi} \ldots a_{n\pi} = a_1 a_2 \ldots a_n.$$

(2) Kommutatív félcsoportban a többtényezős szorzatok eredménye független a tényezők sorrendjétől.

Az $(\mathbf{N};+)$ és $(\mathbf{N};\cdot)$ félcsoportok esetén az általános asszociativitás és kommutativitás már az általános iskola alsó tagozatán szinte tudat alatti készséggé válik. Példa

Az $(\mathbb{N};+)$ és $(\mathbb{N};\cdot)$ félcsoportok esetén az általános asszociativitás és kommutativitás már az általános iskola alsó tagozatán szinte tudat alatti készséggé válik. Példa erre az alábbi szorzat kiszámítása:

$$9\cdot 17\cdot 6\cdot 13\cdot 21\cdot 8\cdot 15\cdot 5\cdot 27\cdot 24\cdot 0\cdot 7 =?$$

Hatványozás félcsoportban

$a^n = aa\ldots a$. Grupoidban ez kevés lenne (hogyan zárójelezzük?).

Hatványozás félcsoportban

$a^n = aa \ldots a$. Grupoidban ez kevés lenne (hogyan zárójelezzük?). Ezért feltesszük, hogy a művelet asszociatív, azaz *csak félcsoportban* definiáljuk:

Hatványozás félcsoportban

$a^n = aa \dots a$. Grupoidban ez kevés lenne (hogyan zárójelezzük?). Ezért feltesszük, hogy a művelet asszociatív, azaz *csak félcsoportban* definiáljuk: $a^n = aa \dots a$ (n tényező, $n \geq 1$, $a^1 := a$). M

Hatványozás félcsoportban

$a^n = aa \dots a$. Grupoidban ez kevés lenne (hogyan zárójelezzük?). Ezért feltesszük, hogy a művelet asszociatív, azaz *csak félcsoportban* definiáljuk: $a^n = aa \dots a$ (n tényező, $n \geq 1$, $a^1 := a$). Másként: $a^1 := a$, $a^{n+1} := a^n \cdot a$ (rekurzióval).

49. Tétel. *(Hatványozás azonosságai félcsoportban.)* *Félcsoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{N}$*-re*

49. Tétel. *(Hatványozás azonosságai félcsoportban.)* *Félcsoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{N}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(a*

49. Tétel. *(Hatványozás azonosságai félcsoportban.)* *Félcsoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{N}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása),*

$(a^n)^m = a^{nm}$ *(h*

49. Tétel. *(Hatványozás azonosságai félcsoportban.)* *Félcsoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{N}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása),*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

49. Tétel. *(Hatványozás azonosságai félcsoportban.)* *Félcsoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{N}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása),*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

ha a *és* b *felcserélhető, akkor* $a^n \cdot b^n = (ab)^n$ *(a*

49. Tétel. *(Hatványozás azonosságai félcsoportban.)* *Félcsoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{N}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása),*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

ha a *és* b *felcserélhető, akkor* $a^n \cdot b^n = (ab)^n$ *(azonos kitevőjű hatványok szorzása).*

49. Tétel. *(Hatványozás azonosságai félcsoportban.) Félcsoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{N}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása),*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

ha a *és* b *felcserélhető, akkor* $a^n \cdot b^n = (ab)^n$ *(azonos kitevőjű hatványok szorzása).*

Bizonyítás: Az általános asszociativitás miatt mindegy, hogy az azonos tényezőkből álló szorzatot hogyan zárójelezzük. Ezért

Bizonyítás: Az általános asszociativitás miatt mindegy, hogy az azonos tényezőkből álló szorzatot hogyan zárójelezzük. Ezért a tétel ugyanúgy adódik, ahogy számokra (triviálisan). De

Bizonyítás: Az általános asszociativitás miatt mindegy, hogy az azonos tényezőkből álló szorzatot hogyan zárójelezzük. Ezért a tétel ugyanúgy adódik, ahogy számokra (triviálisan). De teljes indukcióval is lehet bizonyítani.

Bizonyítás: Az általános asszociativitás miatt mindegy, hogy az azonos tényezőkből álló szorzatot hogyan zárójelezzük. Ezért a tétel ugyanúgy adódik, ahogy számokra (triviálisan). De teljes indukcióval is lehet bizonyítani.

Definíció: Legyen $(A, \cdot)$ egységelemes grupoid. Egységelemét jelölje 1.

Bizonyítás: Az általános asszociativitás miatt mindegy, hogy az azonos tényezőkből álló szorzatot hogyan zárójelezzük. Ezért a tétel ugyanúgy adódik, ahogy számokra (triviálisan). De teljes indukcióval is lehet bizonyítani.

Definíció: Legyen $(A, \cdot)$ egységelemes grupoid. Egységelemét jelölje 1. Ha $a, b \in A$ és $ab = ba = 1$, akkor azt mondjuk, hogy b **inverze** a-nak.

Bizonyítás: Az általános asszociativitás miatt mindegy, hogy az azonos tényezőkből álló szorzatot hogyan zárójelezzük. Ezért a tétel ugyanúgy adódik, ahogy számokra (triviálisan). De teljes indukcióval is lehet bizonyítani.

Definíció: Legyen $(A, \cdot)$ egységelemes grupoid. Egységelemét jelölje 1. Ha $a, b \in A$ és $ab = ba = 1$, akkor azt mondjuk, hogy b **inverze** a-nak. (Figyelem: mindkét sorrendben szorozva 1-et kell kapnunk!)

4. Állítás.

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás:

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor $b_1 =$

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor $b_1 = b_1 \cdot 1 =$

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor $b_1 = b_1 \cdot 1 = b_1(ab_2) =$

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor $b_1 = b_1 \cdot 1 = b_1(ab_2) = (b_1a)b_2 =$

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor $b_1 = b_1 \cdot 1 = b_1(ab_2) = (b_1a)b_2 = 1 \cdot b_2 =$

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor $b_1 = b_1 \cdot 1 = b_1(ab_2) = (b_1a)b_2 = 1 \cdot b_2 = b_2$.

4. Állítás.

Monoidban bármely elemnek legfeljebb egy inverze van.

Bizonyítás: Ha b_1 is és b_2 is inverze a-nak, akkor $b_1 = b_1 \cdot 1 = b_1(ab_2) = (b_1a)b_2 = 1 \cdot b_2 = b_2$. Tehát az a bármely két inverze megegyezik, ezért csak egy inverze van. Q.e.d.

Monoidban — ha létezik — az a elem inverzét (amiből csak egy van) a^{-1} jelöli.

Monoidban — ha létezik — az a elem inverzét (amiből csak egy van) a^{-1} jelöli. Ha létezik a^{-1}, akkor

Monoidban — ha létezik — az a elem inverzét (amiből csak egy van) a^{-1} jelöli. Ha létezik a^{-1}, akkor neki is van inverze:

Monoidban — ha létezik — az a elem inverzét (amiből csak egy van) a^{-1} jelöli. Ha létezik a^{-1}, akkor neki is van inverze: a. Azaz $(a^{-1})^{-1} = a$.

Monoidban — ha létezik — az a elem inverzét (amiből csak egy van) a^{-1} jelöli. Ha létezik a^{-1}, akkor neki is van inverze: a. Azaz $(a^{-1})^{-1} = a$.

Példa: $(\mathbf{Z}; \cdot)$ monoid, az 1 szám az egységeleme,

Monoidban — ha létezik — az a elem inverzét (amiből csak egy van) a^{-1} jelöli. Ha létezik a^{-1}, akkor neki is van inverze: a. Azaz $(a^{-1})^{-1} = a$.

Példa: $(\mathbf{Z}; \cdot)$ monoid, az 1 szám az egységeleme, csakis az 1-nek és -1-nek van inverze: önmaguk.

50. Tétel. *Ha egy monoid* $a_1, \ldots, a_n$ *elemeinek van inverze, akkor*

50. Tétel. *Ha egy monoid* $a_1, \ldots, a_n$ *elemeinek van inverze, akkor ezen elemek szorzatának is van és*

50. Tétel. *Ha egy monoid $a_1, \ldots, a_n$ elemeinek van inverze, akkor ezen elemek szorzatának is van és*

$$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

50. Tétel. *Ha egy monoid $a_1, \ldots, a_n$ elemeinek van inverze, akkor ezen elemek szorzatának is van és*

$$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

Azaz: ha a tényezőknek van inverze, akkor

50. Tétel. *Ha egy monoid $a_1, \ldots, a_n$ elemeinek van inverze, akkor ezen elemek szorzatának is van és*

$$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

Azaz: ha a tényezőknek van inverze, akkor a szorzatnak is van, és

50. Tétel. *Ha egy monoid* $a_1, \ldots, a_n$ *elemeinek van inverze, akkor ezen elemek szorzatának is van és*

$$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

Azaz: ha a tényezőknek van inverze, akkor a szorzatnak is van, és a szorzat inverze a

50. Tétel. *Ha egy monoid* $a_1, \ldots, a_n$ *elemeinek van inverze, akkor ezen elemek szorzatának is van és*

$$(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}.$$

Azaz: ha a tényezőknek van inverze, akkor a szorzatnak is van, és a szorzat inverze a tényezők inverzének fordított sorrendben vett szorzata.

Bizonyítás: Szorozzuk össze a kettőt mindkét sorrendben (de csak az egyiket részletezzük):

$$a_1 \dots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1} =$$

$$a_1 \ldots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \ldots a_1^{-1} =$$

$$a_1 \ldots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} \, 1 \, a_{n-1}^{-1} \ldots a_1^{-1} =$$

$$a_1 \dots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1} =$$
$$a_1 \dots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \dots a_1^{-1} =$$
$$a_1 \dots a_{n-1}\, 1\, a_{n-1}^{-1} \dots a_1^{-1} =$$
$$a_1 \dots a_{n-1}\, (1\, a_{n-1}^{-1}) \dots a_1^{-1} =$$

$$a_1 \ldots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} \, 1 \, a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} \, (1 \, a_{n-1}^{-1}) \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} a_{n-1}^{-1} \ldots a_1^{-1} =$$

$$a_1 \dots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1} =$$
$$a_1 \dots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \dots a_1^{-1} =$$
$$a_1 \dots a_{n-1} \, 1 \, a_{n-1}^{-1} \dots a_1^{-1} =$$
$$a_1 \dots a_{n-1} \, (1 \, a_{n-1}^{-1}) \dots a_1^{-1} =$$
$$a_1 \dots a_{n-1} a_{n-1}^{-1} \dots a_1^{-1} =$$
$$\dots$$

$$a_1 \ldots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} \, 1 \, a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} \, (1 \, a_{n-1}^{-1}) \ldots a_1^{-1} =$$
$$a_1 \ldots a_{n-1} a_{n-1}^{-1} \ldots a_1^{-1} =$$
$$\ldots$$
$$a_1 a_1^{-1} =$$

$$
\begin{gathered}
a_1 \ldots a_{n-1} a_n a_n^{-1} a_{n-1}^{-1} \ldots a_1^{-1} = \\
a_1 \ldots a_{n-1} (a_n a_n^{-1}) a_{n-1}^{-1} \ldots a_1^{-1} = \\
a_1 \ldots a_{n-1}\, 1\, a_{n-1}^{-1} \ldots a_1^{-1} = \\
a_1 \ldots a_{n-1}\, (1\, a_{n-1}^{-1}) \ldots a_1^{-1} = \\
a_1 \ldots a_{n-1} a_{n-1}^{-1} \ldots a_1^{-1} = \\
\ldots \\
a_1 a_1^{-1} = 1,
\end{gathered}
$$

valóban. Q.e.d.

A fenti tételnek speciális esete a leképezések szorzásáról a múltl félévben tanult hasonló formula. Ugyanis:

A fenti tételnek speciális esete a leképezések szorzásáról a múltl félévben tanult hasonló formula. Ugyanis:

Példa: Legyen B nemüres halmaz és jelölje T_B a $B \to B$ leképezések halmazát, $\circ$ pedig a leképezésszorzást. Ekkor $(T_B; \circ)$ monoid.

A fenti tételnek speciális esete a leképezések szorzásáról a múltl félévben tanult hasonló formula. Ugyanis:

Példa: Legyen B nemüres halmaz és jelölje T_B a $B \to B$ leképezések halmazát, $\circ$ pedig a leképezésszorzást. Ekkor $(T_B; \circ)$ monoid. Egységeleme az identikus $B \to B$, $x \mapsto x$ leképezés.

A fenti tételnek speciális esete a leképezések szorzásáról a múltl félévben tanult hasonló formula. Ugyanis:

Példa: Legyen B nemüres halmaz és jelölje T_B a $B \longrightarrow B$ leképezések halmazát, $\circ$ pedig a leképezésszorzást. Ekkor $(T_B; \circ)$ monoid. Egységeleme az identikus $B \longrightarrow B$, $x \mapsto x$ leképezés. Ebben a monoidban pontosan a bijektív leképezéseknek van inverzük,

A fenti tételnek speciális esete a leképezések szorzásáról a múltl félévben tanult hasonló formula. Ugyanis:

Példa: Legyen B nemüres halmaz és jelölje T_B a $B \longrightarrow B$ leképezések halmazát, $\circ$ pedig a leképezésszorzást. Ekkor $(T_B; \circ)$ monoid. Egységeleme az identikus $B \longrightarrow B$, $x \longmapsto x$ leképezés. Ebben a monoidban pontosan a bijektív leképezéseknek van inverzük, és bijektív leképezések esetén a szorzat (ami szintén bijektív) inverze a tényezők inverzének fordított sorrendben vett szorzata.

Feladat: (A) Legyen B végtelen halmaz, és jelölje N_B a nemszürjektív $B \to B$ leképezések halmazát. Monoid-e, félcsoport-e $(N_B; \circ)$? ($\circ$ a leképezésszorzást jelöli.)

Feladat: (A) Legyen B végtelen halmaz, és jelölje N_B a nemszürjektív $B \longrightarrow B$ leképezések halmazát. Monoid-e, félcsoport-e $(N_B; \circ)$? ($\circ$ a leképezésszorzást jelöli.)

(B) Ugyanez a kérdés, de B most véges.

Megoldás (A)

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív.

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben,

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben.

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon.

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (sőt tetszőleges leképezések esetén is, ha azok egyáltalán összeszorozhatók) teljesül az asszociativitás, ezért

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (sőt tetszőleges leképezések esetén is, ha azok egyáltalán összeszorozhatók) teljesül az asszociativitás, ezért speciális esetként N_B elemeire is.

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (sőt tetszőleges leképezések esetén is, ha azok egyáltalán összeszorozhatók) teljesül az asszociativitás, ezért speciális esetként N_B elemeire is. Tehát $(N_B; \circ)$ félcsoport.

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (sőt tetszőleges leképezések esetén is, ha azok egyáltalán összeszorozhatók) teljesül az asszociativitás, ezért speciális esetként N_B elemeire is. Tehát $(N_B; \circ)$ félcsoport.

Eddig könnyű volt, de most az a kérdés, hogy $(N_B; \circ)$ monoid-e,

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (sőt tetszőleges leképezések esetén is, ha azok egyáltalán összeszorozhatók) teljesül az asszociativitás, ezért speciális esetként N_B elemeire is. Tehát $(N_B; \circ)$ félcsoport.

Eddig könnyű volt, de most az a kérdés, hogy $(N_B; \circ)$ monoid-e, azaz, hogy van-e egységeleme?

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (sőt tetszőleges leképezések esetén is, ha azok egyáltalán összeszorozhatók) teljesül az asszociativitás, ezért speciális esetként N_B elemeire is. Tehát $(N_B; \circ)$ félcsoport.

Eddig könnyű volt, de most az a kérdés, hogy $(N_B; \circ)$ monoid-e, azaz, hogy van-e egységeleme? Az identikus $\mathrm{id} : B \to B$, $x \mapsto x$ leképezés (szürjektív lévén) nincs benne N_B-ben. Tehát

Megoldás (A) Tanultuk a múlt félévben, hogy ha két leképezés szorzata szürjektív, akkor a második tényező is szürjektív. Ezért ha $f, g \in N_B$ akkor $f \circ g$ azért van N_B-ben, mert ellenkező esetben g szürjektív lenne, és így g nem lehetne N_B-ben. Tehát a $\circ$ tényleg művelet az N_B halmazon. Mivel tetszőleges $B \to B$ leképezések (sőt tetszőleges leképezések esetén is, ha azok egyáltalán összeszorozhatók) teljesül az asszociativitás, ezért speciális esetként N_B elemeire is. Tehát $(N_B; \circ)$ félcsoport.

Eddig könnyű volt, de most az a kérdés, hogy $(N_B; \circ)$ monoid-e, azaz, hogy van-e egységeleme? Az identikus id : $B \to B$, $x \mapsto x$ leképezés (szürjektív lévén) nincs benne N_B-ben. Tehát

a kérdés még nyitott! És nem is olyan könnyű.

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$.
(

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz $(xf)e = xf$. Azaz

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz $(xf)e = xf$. Azaz e szükségképpen identikusan hat az f értékkészletén.

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz $(xf)e = xf$. Azaz e szükségképpen identikusan hat az f értékkészletén. Viszont minden $x \in B$ egy alkalmas $f \in N_B$ értékkészletéhez tartozik (

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz $(xf)e = xf$. Azaz e szükségképpen identikusan hat az f értékkészletén. Viszont minden $x \in B$ egy alkalmas $f \in N_B$ értékkészletéhez tartozik (választhatjuk f-et úgy is, hogy minden elem képe x legyen), ezért minden $x \in B$-re $xe = x$.

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz $(xf)e = xf$. Azaz e szükségképpen identikusan hat az f értékkészletén. Viszont minden $x \in B$ egy alkalmas $f \in N_B$ értékkészletéhez tartozik (választhatjuk f-et úgy is, hogy minden elem képe x legyen), ezért minden $x \in B$-re $xe = x$. Azaz e az identikus leképezés a B halmazon.

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz $(xf)e = xf$. Azaz e szükségképpen identikusan hat az f értékkészletén. Viszont minden $x \in B$ egy alkalmas $f \in N_B$ értékkészletéhez tartozik (választhatjuk f-et úgy is, hogy minden elem képe x legyen), ezért minden $x \in B$-re $xe = x$. Azaz e az identikus leképezés a B halmazon. De az nem szürjektív, azaz $e \notin N_B$, ami ellentmondás.

a kérdés még nyitott! És nem is olyan könnyű. Tegyük fel, hogy $e \in N_B$ egységelem. Ekkor bármely $f \in N_B$-re $f \circ e = f$. (És persze $e \circ f = f$ is, de most az előbbire koncentrálunk.)

Azaz bármely $x \in B$-re $x(f \circ e) = xf$, azaz $(xf)e = xf$. Azaz e szükségképpen identikusan hat az f értékkészletén. Viszont minden $x \in B$ egy alkalmas $f \in N_B$ értékkészletéhez tartozik (választhatjuk f-et úgy is, hogy minden elem képe x legyen), ezért minden $x \in B$-re $xe = x$. Azaz e az identikus leképezés a B halmazon. De az nem szürjektív, azaz $e \notin N_B$, ami ellentmondás.

Tehát most már tudjuk, hogy $(N_B; \circ)$-nek nincs egységeleme, azaz nem monoid.

A (B) esetben B véges.

A (B) esetben B véges. Látszólag könnyen rávágjuk a választ: mivel az előbb nem használtuk ki, hogy B véges-e vagy végtelen, ezért $(N_B; \circ)$ félcsoport de nem monoid. **De ez rossz válasz**; ha az előző megfontolást alaposan átgondoljuk, annyit azért mégiscsak kihasználtunk, hogy B-nek azért van „elég sok'' eleme.

A (B) esetben B véges. Látszólag könnyen rávágjuk a választ: mivel az előbb nem használtuk ki, hogy B véges-e vagy végtelen, ezért $(N_B; \circ)$ félcsoport de nem monoid. **De ez rossz válasz**; ha az előző megfontolást alaposan átgondoljuk, annyit azért mégiscsak kihasználtunk, hogy B-nek azért van „elég sok'' eleme.

Könnyű (az előző gondolatmenet birtokában) meggondolni, hogy ha $|B| < 2$, akkor $N_B = \emptyset$ és ezért $(N_B; \circ)$ nem monoid és nem félcsoport, sőt mégcsak nem is grupoid. (Ugyanis az algebra tartóhalmaza — definíció szerint — nem lehet üres.) Viszont ha $|B| \geq 2$, akkor N_B már nem üres, és a korábbi gondolatmenet alapján $(N_B; \circ)$ félcsoport de nem monoid.

Csoport

Definíció: **csoport** $\overset{\text{def}}{\iff}$ monoid, amelyben minden elemnek van inverze.

Csoport

Definíció: **csoport** $\overset{\text{def}}{\iff}$ monoid, amelyben minden elemnek van inverze. Azaz asszociatív, egységelemes grupoid, amelyben minden elemnek van inverze.

Emlékeztető: Monoidban minden egyes elemenek legfeljebb egy inverze lehet.

J

Jelölések: a csoport egységelemét 1 (

Jelölések: a csoport egységelemét 1 (néha e), az a elem inverzét (amely a fentiek szerint egyértelműen meghatározott)

Jelölések: a csoport egységelemét 1 (néha e), az a elem inverzét (amely a fentiek szerint egyértelműen meghatározott) pedig a^{-1} jelöli.

Definíció: **Abel-csoport** $\overset{\text{def}}{\Longleftrightarrow}$ kommutatív csoport.

Jelölések: a csoport egységelemét 1 (néha e), az a elem inverzét (amely a fentiek szerint egyértelműen meghatározott) pedig a^{-1} jelöli.

Definíció: **Abel-csoport** $\overset{\text{def}}{\Longleftrightarrow}$ kommutatív csoport.

Jelölések: Abel-csoportok esetén kétféle jelölésmód terjedt el. A **multiplikatív** írásmód esetén 1

Jelölések: a csoport egységelemét 1 (néha e), az a elem inverzét (amely a fentiek szerint egyértelműen meghatározott) pedig a^{-1} jelöli.

Definíció: **Abel-csoport** $\overset{\text{def}}{\Longleftrightarrow}$ kommutatív csoport.

Jelölések: Abel-csoportok esetén kétféle jelölésmód terjedt el. A **multiplikatív** írásmód esetén 1 (vagy e) jelöli a csoport egységelemét, szorzásjel (vagy egymásmellé írás) a műveletet, és x^{-1} az x elem inverzét. (Ahogy általában a csoportok esetén.)

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy összeadás jelöli a műveletet, 0 az egységelemet és $-x$ az x elem (additív) inverzét.

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy összeadás jelöli a műveletet, 0 az egységelemet és $-x$ az x elem (additív) inverzét. Ez összhangban van a „megszokott látvánnyal”: $0 + x = x + 0 = x$, $x + (-x) = 0$.

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy összeadás jelöli a műveletet, 0 az egységelemet és $-x$ az x elem (additív) inverzét. Ez összhangban van a „megszokott látvánnyal”: $0 + x = x + 0 = x$, $x + (-x) = 0$.

Példák csoportokra:

$(\mathbf{R} \setminus \{0\}; \cdot)$

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy összeadás jelöli a műveletet, 0 az egységelemet és $-x$ az x elem (additív) inverzét. Ez összhangban van a „megszokott látvánnyal”: $0 + x = x + 0 = x$, $x + (-x) = 0$.

Példák csoportokra:

$(\mathbf{R} \setminus \{0\}; \cdot)$ Abel-csoport, itt az 1 szám az egységelem, és a reciprok az inverz.

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy összeadás jelöli a műveletet, 0 az egységelemet és $-x$ az x elem (additív) inverzét. Ez összhangban van a „megszokott látvánnyal”: $0+x = x+0 = x$, $x+(-x) = 0$.

Példák csoportokra:

$(\mathbf{R}\setminus\{0\};\cdot)$ Abel-csoport, itt az 1 szám az egységelem, és a reciprok az inverz.

$(\mathbf{R};\cdot)$

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy összeadás jelöli a műveletet, 0 az egységelemet és $-x$ az x elem (additív) inverzét. Ez összhangban van a „megszokott látvánnyal”: $0 + x = x + 0 = x$, $x + (-x) = 0$.

Példák csoportokra:

$(\mathbf{R} \setminus \{0\}; \cdot)$ Abel-csoport, itt az 1 szám az egységelem, és a reciprok az inverz.

$(\mathbf{R}; \cdot)$ **nem** csoport, mert a 0-nak nincs inverze.

Ennél gyakoribb (és csak Abel-csoportok esetén), hogy összeadás jelöli a műveletet, 0 az egységelemet és $-x$ az x elem (additív) inverzét. Ez összhangban van a „megszokott látvánnyal": $0 + x = x + 0 = x$, $x + (-x) = 0$.

Példák csoportokra:

$(\mathbf{R} \setminus \{0\}; \cdot)$ Abel-csoport, itt az 1 szám az egységelem, és a reciprok az inverz.

$(\mathbf{R}; \cdot)$ **nem** csoport, mert a 0-nak nincs inverze. Csak kommutatív monoid.

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport.

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport. ?

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport. ? Az 1

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport. ? Az 1 egységelem, hiszen bármely $x \in \mathbf{Z} \setminus \{0\}$ esetén $1x = x1 = x$.

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport. ? Az 1 egységelem, hiszen bármely $x \in \mathbf{Z} \setminus \{0\}$ esetén $1x = x1 = x$. Tehát az 1

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport. ? Az 1 egységelem, hiszen bármely $x \in \mathbf{Z} \setminus \{0\}$ esetén $1x = x1 = x$. Tehát az 1 **az** egységelem.

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport. ? Az 1 egységelem, hiszen bármely $x \in \mathbf{Z} \setminus \{0\}$ esetén $1x = x1 = x$. Tehát az 1 **az** egységelem. Pl. a 2-nek nincs inverze, hiszen nincsen olyan b *egész* szám, amelyre $2b = 1$.

$(\mathbf{Q} \setminus \{0\}; \cdot)$ *multiplikatív* Abel-csoport. A jelző arra utal, hogy a művelet (jelölése) a szorzás.

$(\mathbf{Z} \setminus \{0\}; \cdot)$ **nem** csoport. ? Az 1 egységelem, hiszen bármely $x \in \mathbf{Z}\setminus\{0\}$ esetén $1x = x1 = x$. Tehát az 1 **az** egységelem. Pl. a 2-nek nincs inverze, hiszen nincsen olyan b *egész* szám, amelyre $2b = 1$.

Az előző félév anyagából következik (egyszerű gyakorló feladat a halmazműveletek tulajdonságaira), hogy

$(P(M); \triangle)$, ahol M tetszőleges halmaz,

Az előző félév anyagából következik (egyszerű gyakorló feladat a halmazműveletek tulajdonságaira), hogy

$(P(M);\triangle)$, ahol M tetszőleges halmaz, Abel-csoport. Itt

Az előző félév anyagából következik (egyszerű gyakorló feladat a halmazműveletek tulajdonságaira), hogy

$(P(M); \triangle)$, ahol M tetszőleges halmaz, Abel-csoport. Itt az $\emptyset$ az egységelem, és tetszőleges elem inverze önmaga.

Az előző félév anyagából következik (egyszerű gyakorló feladat a halmazműveletek tulajdonságaira), hogy

$(P(M); \triangle)$, ahol M tetszőleges halmaz, Abel-csoport. Itt az $\emptyset$ az egységelem, és tetszőleges elem inverze önmaga.

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve:

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport.

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport. Itt a művelet a leképezések szorzása, és

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport. Itt a művelet a leképezések szorzása, és az identikus permutáció lesz az egységelem.

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport. Itt a művelet a leképezések szorzása, és az identikus permutáció lesz az egységelem.A csoportbeli inverz pedig nem más, mint a kérdéses permutáció (mint leképezés) inverze.

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport. Itt a művelet a leképezések szorzása, és az identikus permutáció lesz az egységelem.A csoportbeli inverz pedig nem más, mint a kérdéses permutáció (mint leképezés) inverze.

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport. Itt a művelet a leképezések szorzása, és az identikus permutáció lesz az egységelem.A csoportbeli inverz pedig nem más, mint a kérdéses permutáció (mint leképezés) inverze.

Az $(S_n; \circ)$ csoportot **n-edfokú szimmetrikus csoportnak** nevezzük.

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport. Itt a művelet a leképezések szorzása, és az identikus permutáció lesz az egységelem.A csoportbeli inverz pedig nem más, mint a kérdéses permutáció (mint leképezés) inverze.

Az $(S_n; \circ)$ csoportot **n-edfokú szimmetrikus csoportnak** nevezzük. Elemszáma:

Az $\{1, 2, \ldots, n\}$ halmaz permutációinak (azaz önmagára történő bijekcióinak) halmazát S_n-nel jelölve: $(S_n; \circ)$ csoport. Itt a művelet a leképezések szorzása, és az identikus permutáció lesz az egységelem.A csoportbeli inverz pedig nem más, mint a kérdéses permutáció (mint leképezés) inverze.

Az $(S_n; \circ)$ csoportot **n-edfokú szimmetrikus csoportnak** nevezzük. Elemszáma: $n!$.

Az előbbi $(S_n; \circ)$ csoport

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport.

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2 \dots i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\dots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2 \ldots i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, $x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$-ra $x \mapsto x$

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, ..., $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, $x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

Az előbbi $(S_n;\circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2 \dots i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2,\ i_2 \mapsto i_3,\ \dots,\ i_{k-1} \mapsto i_k,\ i_k \mapsto i_1,\ x \in \{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

$$(1\quad 2\quad 3)\,(1\quad 2) =$$

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, $x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

$$(1\quad 2\quad 3)\,(1\quad 2) = (2$$

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2,\ i_2 \mapsto i_3,\ \ldots,\ i_{k-1} \mapsto i_k,\ i_k \mapsto i_1,\ x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

$$(1\quad 2\quad 3)\,(1\quad 2) = (2\quad 3),$$

Az előbbi $(S_n;\circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, $x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

$$(1\quad 2\quad 3)\,(1\quad 2) = (2\quad 3),$$

$$(1\quad 2)\,(1\quad 2\quad 3) =$$

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, $x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

$$(\,1 \quad 2 \quad 3\,)\,(\,1 \quad 2\,) = (\,2 \quad 3\,),$$
$$(\,1 \quad 2\,)\,(\,1 \quad 2 \quad 3\,) = (\,1$$

Az előbbi $(S_n; \circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, ..., $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, $x \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

$$(1\quad 2\quad 3)\,(1\quad 2) = (2\quad 3),$$
$$(1\quad 2)\,(1\quad 2\quad 3) = (1\quad 3),$$

Az előbbi $(S_n;\circ)$ csoport $n \geq 3$ esetén nem Abel-csoport. Csakugyan, ha $(i_1\ i_2\ \ldots\ i_k)$ jelöle azt a permutációt, amelyre $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, $i_k \mapsto i_1$, $x \in \{1,2,\ldots,n\} \setminus \{i_1,i_2,\ldots,i_k\}$-ra $x \mapsto x$ — az ilyen permutációt **ciklusnak** nevezzük — akkor

$$(1\quad 2\quad 3)(1\quad 2) = (2\quad 3),$$
$$(1\quad 2)(1\quad 2\quad 3) = (1\quad 3),$$

tehát a szorzás nem kommutatív.

A sík (vagy tér) egybevágósági transzformációinak halmaza a leképezésszorzásra nézve

A sík (vagy tér) egybevágósági transzformációinak halmaza a leképezésszorzásra nézve csoport, nem Abel.

A sík (vagy tér) egybevágósági transzformációinak halmaza a leképezésszorzásra nézve csoport, nem Abel.

Rögzített (többnyire ”szabályos”) T síkidom vagy térbeli test esetén azon egybevágósági transzformációk halmaza (a leképezésszorzásra nézve), amelyek T-t önmagába viszik —

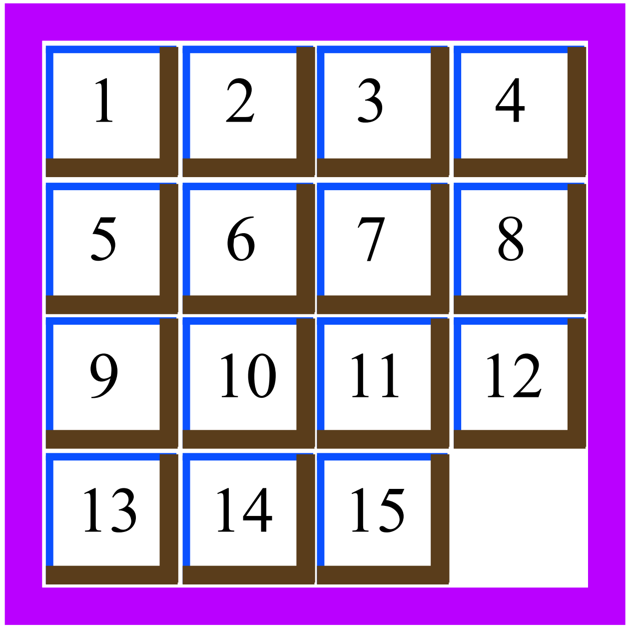
A sík (vagy tér) egybevágósági transzformációinak halmaza a leképezésszorzásra nézve csoport, nem Abel.

Rögzített (többnyire "szabályos") T síkidom vagy térbeli test esetén azon egybevágósági transzformációk halmaza (a leképezésszorzásra nézve), amelyek T-t önmagába viszik — ez csoport. Pl. a kocka egybevágósági csoportja (vagy más néven szimmetriacsoportja), a hatszög egybevágósági (vagy szimmetria-) csoportja, stb.

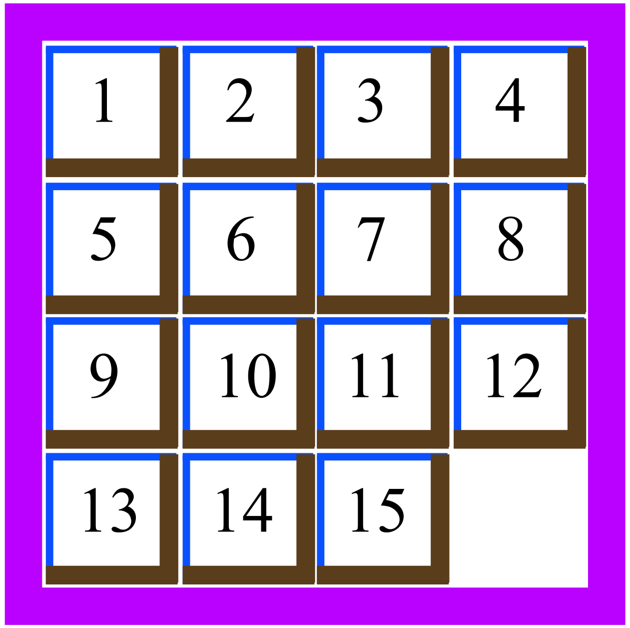
Az előbbi T esetén esetén a sík, ill. tér azon mozgástranszformációinak csoportja, amelyek T-t önmagába viszik —

Az előbbi T esetén esetén a sík, ill. tér azon mozgástranszformációinak csoportja, amelyek T-t önmagába viszik — ez csoport. Pl. a kocka mozgáscsoportja különbözik a kocka egybevágósági csoportjától, mert az előbbiben nincsenek benne (a kocka középpontján átmenő, lappal párhuzamos síkokra való) tükrözések.

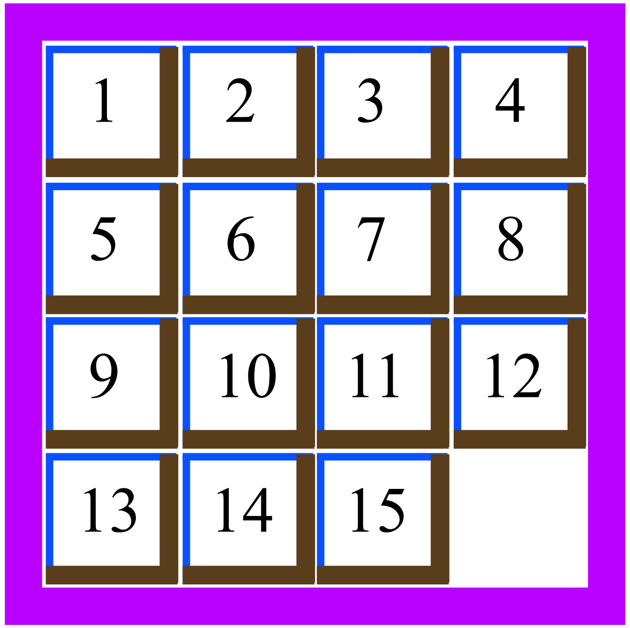
Adott kristályrács szimmetriacsoportja, azaz a rácsot önmagába vivő egybevágósági transzformációk csoportja, Adott kristályrács szimmetriacsoportja, azaz a rácsot önmagába vivő egybevágósági transzformációk csoportja, a kristálytanban kap szerepet.



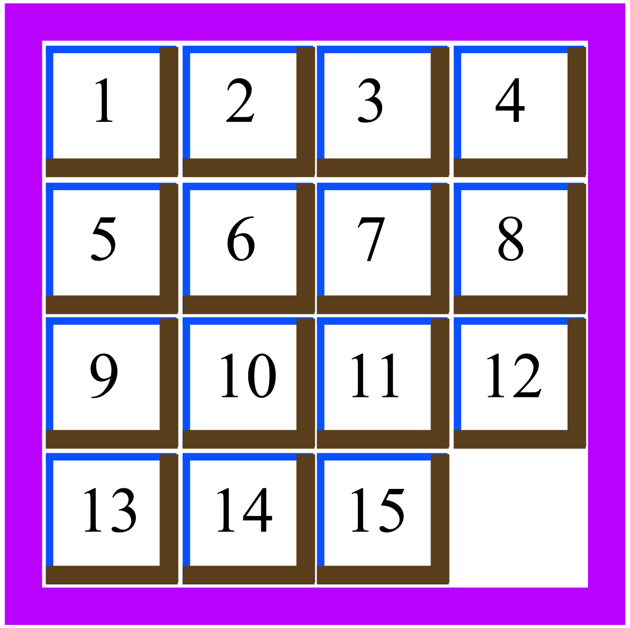
Az $(S_{16}; \circ)$ szimmetrikus csoport minden egyes eleme (tehát minden permutáció) a közismert tizenötös tologatós játék egy-egy pozícióját írja le.



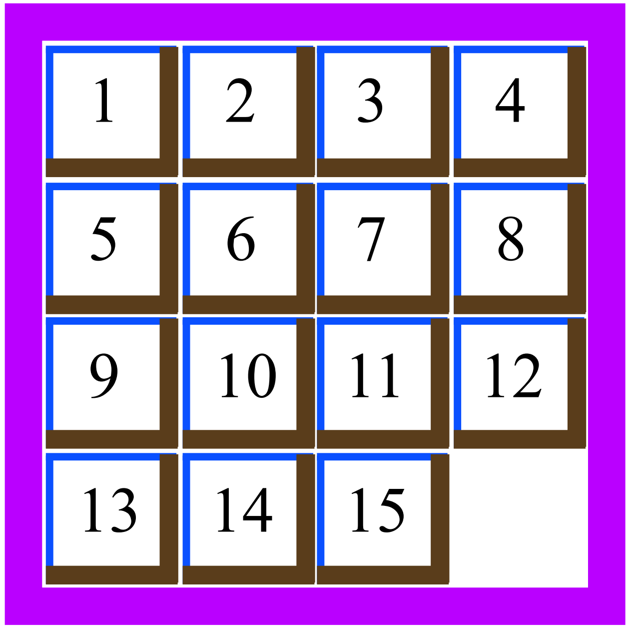
Az $(S_{16};\circ)$ szimmetrikus csoport minden egyes eleme (tehát minden permutáció) a közismert tizenötös tologatós játék egy-egy pozícióját írja le. Itt tizenöt számozott négyzetet kell egy négyszer négyes dobozban tologatni. Személetesen: a „lyukat” tolhatjuk függőlegesen vagy vízszintesen.



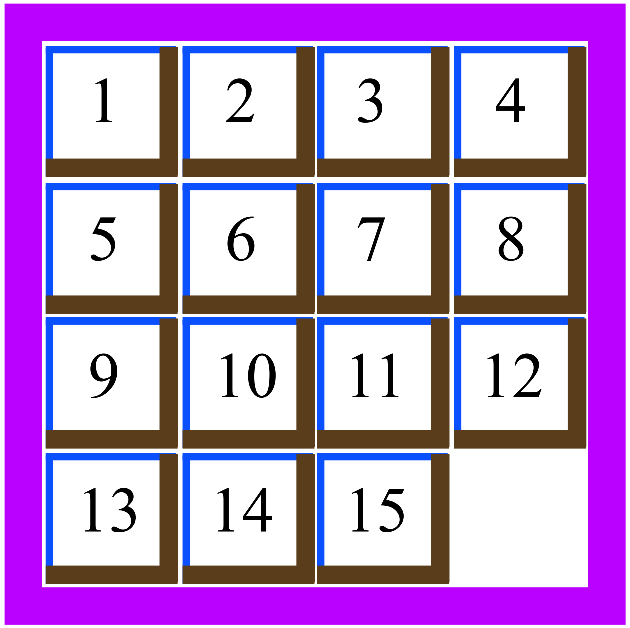
Ha a lyukat — gondolatban — 16-os sorszámmal látjuk el és a számokat sorfolytonosan leolvassuk, akkor az $\{1, 2, \ldots, 16\}$ halmaz egy permutációját kapjuk.



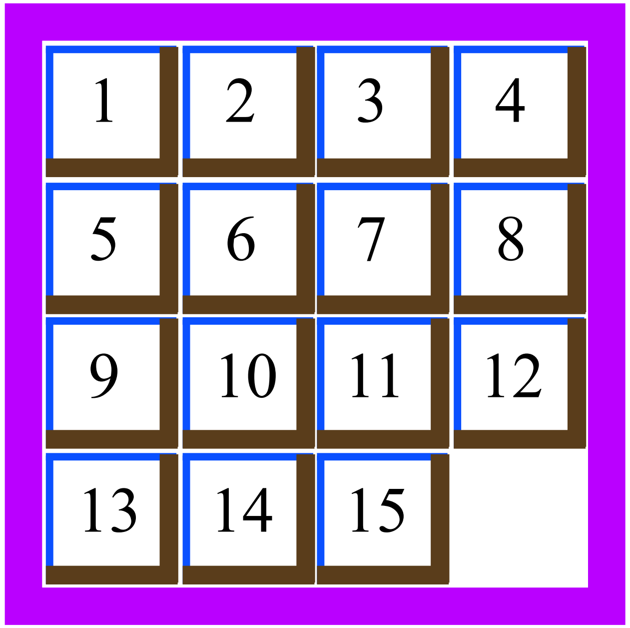
A fenti alapállásból tologatássorozattal nyerhető pozícióknak



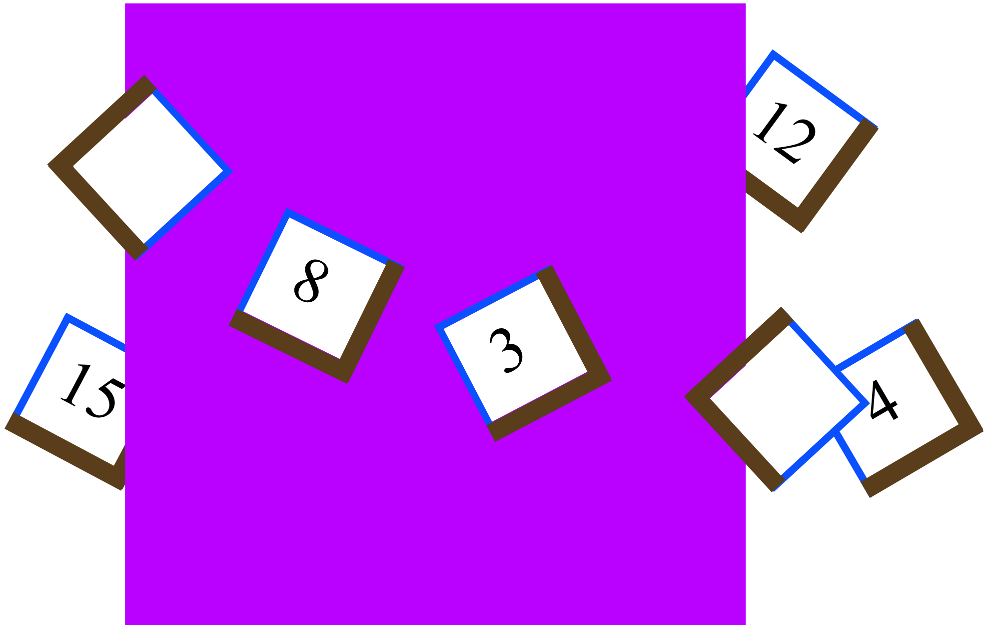
A fenti alapállásból tologatássorozattal nyerhető pozícióknak megfelelő permutációk szintén egy csoportot alkotnak, ahol a művelet az „egymás után végrehajtás”,



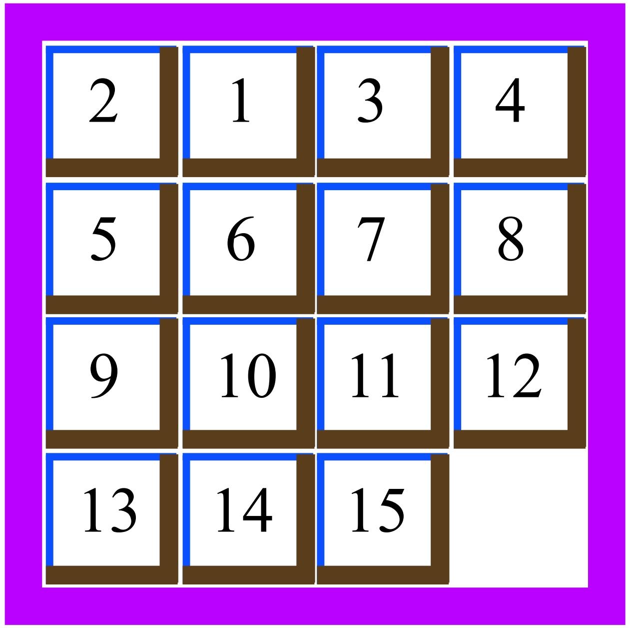
A fenti alapállásból tologatássorozattal nyerhető pozícióknak megfelelő permutációk szintén egy csoportot alkotnak, ahol a művelet az „egymás után végrehajtás”, azaz a leképezésszorzás. Ezt a csoportot a tizenötös játék mozgáscsoportjának nevezzük.



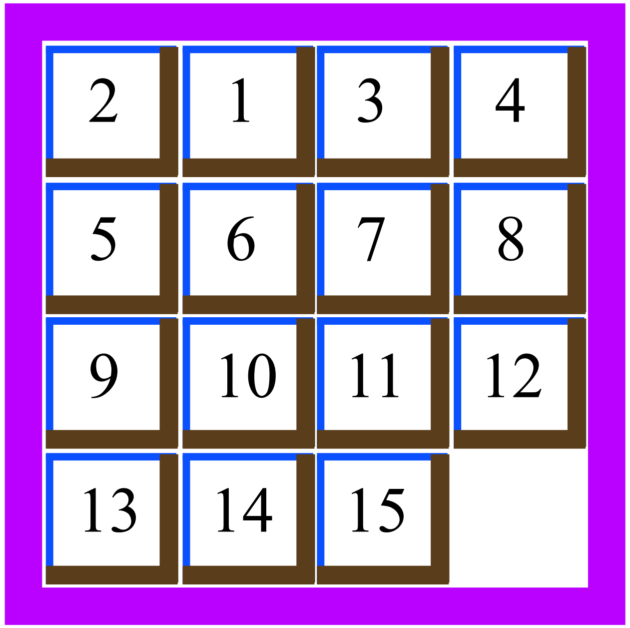
Ezen csoport — mellesleg nem túl bonyolult — tanulmányozásával könnyen választ adhatunk arra a kérdésre, hogy milyen pozíciók tologathatók ki az alapállásból.



Vagy — ami ezzel ekvivalens — ha kiborul a doboz és ezt követően valahogy visszapakoljuk, akkor abból kitologatható-e az alapállás?



Ha például a fenti módon rakjuk vissza, akkor



Ha például a fenti módon rakjuk vissza, akkor NEM!

A Rubik-kocka (bűvös kocka) csoportja:

A Rubik-kocka (bűvös kocka) csoportja: lényegében ez is egy mozgáscsoport (de most nem definiáljuk), amelynek tanulmányozása segít a kocka helyreforgatásában.

A Rubik-kocka (bűvös kocka) csoportja: lényegében ez is egy mozgáscsoport (de most nem definiáljuk), amelynek tanulmányozása segít a kocka helyreforgatásában. Továbbá arra is alkalmas, hogy amennyiben — az előbbi dobozkiborítás példájára — szétszedjük a kockát és máshogy rakjuk össze, akkor a mozgáscsoport ismeretében eldönthető, hogy helyreforgatható-e a kocka.

A Rubik-kocka (bűvös kocka) csoportja: lényegében ez is egy mozgáscsoport (de most nem definiáljuk), amelynek tanulmányozása segít a kocka helyreforgatásában. Továbbá arra is alkalmas, hogy amennyiben — az előbbi dobozkiborítás példájára — szétszedjük a kockát és máshogy rakjuk össze, akkor a mozgáscsoport ismeretében eldönthető, hogy helyreforgatható-e a kocka.

Míg azonban a tizenötös játék mozgáscsoportja olyan egyszerű, hogy a Diszkrét matematika III után egy-két óra alatt el lehet mesélni és az is kijön, hogy tényleg nem tologatható helyre a legutóbbi ábrán látott elrendezés,

A Rubik-kocka (bűvös kocka) csoportja: lényegében ez is egy mozgáscsoport (de most nem definiáljuk), amelynek tanulmányozása segít a kocka helyreforgatásában. Továbbá arra is alkalmas, hogy amennyiben — az előbbi dobozkiborítás példájára — szétszedjük a kockát és máshogy rakjuk össze, akkor a mozgáscsoport ismeretében eldönthető, hogy helyreforgatható-e a kocka.

Míg azonban a tizenötös játék mozgáscsoportja olyan egyszerű, hogy a Diszkrét matematika III után egy-két óra alatt el lehet mesélni és az is kijön, hogy tényleg nem tologatható helyre a legutóbbi ábrán látott elrendezés, a Rubik-kocka mozgáscsoportja lényegesen bonyolultabb.

A **csoport** egyike a matematika igazán szerencsés fogalomalkotásainak:

A **csoport** egyike a matematika igazán szerencsés fogalomalkotásainak: elég általános ahhoz, hogy sok helyen fellépjen és sok alkalmazása legyen,

A **csoport** egyike a matematika igazán szerencsés fogalomalkotásainak: elég általános ahhoz, hogy sok helyen fellépjen és sok alkalmazása legyen, és elég speciális ahhoz, hogy sok szép tulajdonsággal rendelkezzen.

A **csoport** egyike a matematika igazán szerencsés fogalomalkotásainak: elég általános ahhoz, hogy sok helyen fellépjen és sok alkalmazása legyen, és elég speciális ahhoz, hogy sok szép tulajdonsággal rendelkezzen.

Definíció: Elem hatványa csoportban: pozitív kitevőre mint eddig (ismételt szorzás).

A **csoport** egyike a matematika igazán szerencsés fogalomalkotásainak: elég általános ahhoz, hogy sok helyen fellépjen és sok alkalmazása legyen, és elég speciális ahhoz, hogy sok szép tulajdonsággal rendelkezzen.

Definíció: Elem hatványa csoportban: pozitív kitevőre mint eddig (ismételt szorzás). $a^0 := 1$.

A **csoport** egyike a matematika igazán szerencsés fogalomalkotásainak: elég általános ahhoz, hogy sok helyen fellépjen és sok alkalmazása legyen, és elég speciális ahhoz, hogy sok szép tulajdonsággal rendelkezzen.

Definíció: Elem hatványa csoportban: pozitív kitevőre mint eddig (ismételt szorzás). $a^0 := 1$. Ha $k < 0$, akkor $a^k := (a^{-1})^{-k}$.

51. Tétel. *(Hatványozás azonosságai csoportban.) Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

51. Tétel. *(Hatványozás azonosságai csoportban.) Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(a*

51. Tétel. *(Hatványozás azonosságai csoportban.)* *Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása,*

$(a^n)^m = a^{nm}$ *(h*

51. Tétel. *(Hatványozás azonosságai csoportban.)* *Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása,*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

51. Tétel. *(Hatványozás azonosságai csoportban.)* *Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása,*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

ha $ab = ba$ *(más szóval, ha* a *és* b *felcserélhető),*

51. Tétel. *(Hatványozás azonosságai csoportban.)* *Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása,*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

ha $ab = ba$ *(más szóval, ha* a *és* b *felcserélhető), akkor* $a^n \cdot b^n = (ab)^n$ *(a*

51. Tétel. *(Hatványozás azonosságai csoportban.)* *Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása,*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

ha $ab = ba$ *(más szóval, ha* a *és* b *felcserélhető), akkor* $a^n \cdot b^n = (ab)^n$ *(azonos kitevőjű hatványok szorzása).*

51. Tétel. *(Hatványozás azonosságai csoportban.) Csoport tetszőleges* a, b *elemére és* $n, m \in \mathbf{Z}$*-re*

$a^n \cdot a^m = a^{n+m}$ *(azonos alapú hatványok szorzása,*

$(a^n)^m = a^{nm}$ *(hatvány hatványozása),*

ha $ab = ba$ *(más szóval, ha* a *és* b *felcserélhető), akkor* $a^n \cdot b^n = (ab)^n$ *(azonos kitevőjű hatványok szorzása).*

Bizonyítás: Éppúgy, mint 0-tól különböző racionális számok esetén. Q.e.d.

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell!

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi ”táblázat” jelenti a szótárt a multiplikatív és az additív írásmód között:

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi ”táblázat” jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel: $\cdot$ (szorzás)

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi ”táblázat” jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:		

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi ”táblázat” jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi "táblázat" jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:		

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi "táblázat" jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi ”táblázat” jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	$-x$ (ellentett);
Hatvány:		

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi "táblázat" jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	$-x$ (ellentett);
Hatvány:	a^n	

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi ”táblázat” jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	$-x$ (ellentett);
Hatvány:	a^n	na;
Azonos alap. szorz.:		

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi "táblázat" jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	$-x$ (ellentett);
Hatvány:	a^n	na;
Azonos alap. szorz.:	$a^n \cdot a^m = a^{n+m}$	

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi ”táblázat” jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	$-x$ (ellentett);
Hatvány:	a^n	na;
Azonos alap. szorz.:	$a^n \cdot a^m = a^{n+m}$	$na + ma = (n+m)a$;
Hatvány hatványozása:		

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi "táblázat" jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	$-x$ (ellentett);
Hatvány:	a^n	na;
Azonos alap. szorz.:	$a^n \cdot a^m = a^{n+m}$	$na + ma = (n+m)a$;
Hatvány hatványozása:	$(a^n)^m = a^{nm}$	

A fogalmakat más jelölésmód esetén — pl. additív írásmód esetén is — tudni kell! Az alábbi "táblázat" jelenti a szótárt a multiplikatív és az additív írásmód között:

Műveleti jel:	$\cdot$ (szorzás)	$+$;
Egységelem:	1	0;
x elemre:	x^{-1} (inverz)	$-x$ (ellentett);
Hatvány:	a^n	na;
Azonos alap. szorz.:	$a^n \cdot a^m = a^{n+m}$	$na + ma = (n+m)a$;
Hatvány hatványozása:	$(a^n)^m = a^{nm}$	$m(na) = (nm)a$

Definíció: Egy $(A;\cdot)$ félcsoportot **kancellatívnak** (vagy **egyszerűsítésesnek**) nevezünk $\overset{\text{def}}{\iff}$ bármely a, x, y elemeire $ax = ay \implies x = y$ és $xa = ya \implies x = y$.

Definíció: Egy $(A;\cdot)$ félcsoportot **kancellatívnak** (vagy **egyszerűsítésesnek**) nevezünk $\overset{\text{def}}{\iff}$ bármely a, x, y elemeire $ax = ay \implies x = y$ és $xa = ya \implies x = y$. (”cancel” = ”egyszerűsít”)

P

Definíció: Egy $(A; \cdot)$ félcsoportot **kancellatívnak** (vagy **egyszerűsítésesnek**) nevezünk $\stackrel{\text{def}}{\Longleftrightarrow}$ bármely a, x, y elemeire $ax = ay \Longrightarrow x = y$ és $xa = ya \Longrightarrow x = y$. (”cancel” = ”egyszerűsít”)

Példák: $(\mathbf{R}; \cdot)$ monoid de **nem** kancellatív, hiszen

Definíció: Egy $(A; \cdot)$ félcsoportot **kancellatívnak** (vagy **egyszerűsítésesnek**) nevezünk $\overset{\text{def}}{\iff}$ bármely a, x, y elemeire $ax = ay \implies x = y$ és $xa = ya \implies x = y$. ("cancel" = "egyszerűsít")

Példák: $(\mathbf{R}; \cdot)$ monoid de **nem** kancellatív, hiszen a nullával nem lehet egyszerűsíteni.

Definíció: Egy $(A;\cdot)$ félcsoportot **kancellatívnak** (vagy **egyszerűsítésesnek**) nevezünk $\overset{\text{def}}{\Longleftrightarrow}$ bármely a, x, y elemeire $ax = ay \Longrightarrow x = y$ és $xa = ya \Longrightarrow x = y$. (''cancel'' = ''egyszerűsít'')

Példák: $(\mathbf{R};\cdot)$ monoid de **nem** kancellatív, hiszen a nullával nem lehet egyszerűsíteni.

$(\mathbf{R}\setminus\{0\};\cdot)$ is és

Definíció: Egy $(A;\cdot)$ félcsoportot **kancellatívnak** (vagy **egyszerűsítésesnek**) nevezünk $\overset{\text{def}}{\iff}$ bármely a, x, y elemeire $ax = ay \Longrightarrow x = y$ és $xa = ya \Longrightarrow x = y$. ("cancel" = "egyszerűsít")

Példák: $(\mathbf{R};\cdot)$ monoid de **nem** kancellatív, hiszen a nullával nem lehet egyszerűsíteni.

$(\mathbf{R}\setminus\{0\};\cdot)$ is és $(\mathbf{N};\cdot)$ is kancellatív monoid.

52. Tétel. *(1)*

52. Tétel. *(1) Minden csoport kancellatív monoid.*

52. Tétel. *(1) Minden csoport kancellatív monoid.*

(2) Minden **véges** *kancellatív félcsoport csoport.*

52. Tétel. *(1) Minden csoport kancellatív monoid.*

(2) Minden **véges** *kancellatív félcsoport csoport.*

Megjegyzés: még

52. Tétel. *(1) Minden csoport kancellatív monoid.*

(2) Minden **véges** *kancellatív félcsoport csoport.*

Megjegyzés: még az is meglepő, hogy a (2) feltételéből következik az egységelem léte.

Bizonyítás

Bizonyítás (Szép.)

(1) Tfh. $(A;\cdot)$ csoport és $ax = ay$. Ekkor

$x =$

Bizonyítás (Szép.)

(1) Tfh. $(A;\cdot)$ csoport és $ax = ay$. Ekkor

$x = 1x =$

Bizonyítás (Szép.)

(1) Tfh. $(A;\cdot)$ csoport és $ax = ay$. Ekkor

$$x = 1x = (a^{-1}a)x =$$

Bizonyítás (Szép.)

(1) Tfh. $(A;\cdot)$ csoport és $ax = ay$. Ekkor

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) =$$

Bizonyítás (Szép.)

(1) Tfh. $(A; \cdot)$ csoport és $ax = ay$. Ekkor

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) =$$

Bizonyítás (Szép.)

(1) Tfh. $(A; \cdot)$ csoport és $ax = ay$. Ekkor

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y =$$

Bizonyítás (Szép.)

(1) Tfh. $(A; \cdot)$ csoport és $ax = ay$. Ekkor

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1y =$$

Bizonyítás (Szép.)

(1) Tfh. $(A;\cdot)$ csoport és $ax = ay$. Ekkor

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1y = y.$$

Bizonyítás (Szép.)

(1) Tfh. $(A;\cdot)$ csoport és $ax = ay$. Ekkor

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1y = y.$$

A bal és a jobb oldal szerepének felcserélésével adódik, hogy $xa = ya$-ból is következik $x = y$. Ezzel (1)-et beláttuk.

(2) Tfh. $(A;\cdot)$ kancellatív véges félcsoport. Ekkor, amennyiben $a \in A$, az

$$A \longrightarrow A,$$

(2) Tfh. $(A; \cdot)$ kancellatív véges félcsoport. Ekkor, amennyiben $a \in A$, az

$$A \longrightarrow A, \qquad x \longmapsto ax$$

leképezés a kancellativitás miatt

(2) Tfh. $(A; \cdot)$ kancellatív véges félcsoport. Ekkor, amennyiben $a \in A$, az

$$A \longrightarrow A, \qquad x \longmapsto ax$$

leképezés a kancellativitás miatt injektív, így a végesség miatt

(2) Tfh. $(A; \cdot)$ kancellatív véges félcsoport. Ekkor, amennyiben $a \in A$, az

$$A \longrightarrow A, \qquad x \longmapsto ax$$

leképezés a kancellativitás miatt injektív, így a végesség miatt szürjektív is. Tehát

(2) Tfh. $(A;\cdot)$ kancellatív véges félcsoport. Ekkor, amennyiben $a \in A$, az

$$A \longrightarrow A, \qquad x \longmapsto ax$$

leképezés a kancellativitás miatt injektív, így a végesség miatt szürjektív is. Tehát bármely $a, b \in A$ esetén létezik olyan $x \in A$, hogy $ax = b$.

(2) Tfh. $(A;\cdot)$ kancellatív véges félcsoport. Ekkor, amennyiben $a \in A$, az

$$A \longrightarrow A, \qquad x \mapsto ax$$

leképezés a kancellativitás miatt injektív, így a végesség miatt szürjektív is. Tehát bármely $a, b \in A$ esetén létezik olyan $x \in A$, hogy $ax = b$.

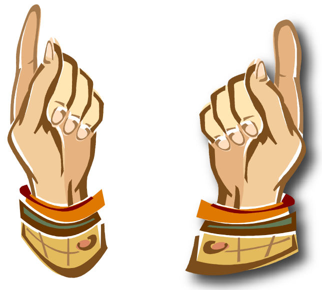
Röviden:

(2) Tfh. $(A;\cdot)$ kancellatív véges félcsoport. Ekkor, amennyiben $a \in A$, az

$$A \to A, \qquad x \mapsto ax$$

leképezés a kancellativitás miatt injektív, így a végesség miatt szürjektív is. Tehát bármely $a, b \in A$ esetén létezik olyan $x \in A$, hogy $ax = b$.

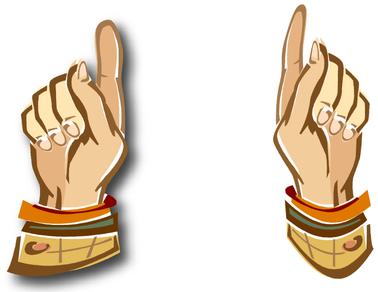
Röviden: *az $ax = b$ egyenletek megoldhatók*!!!



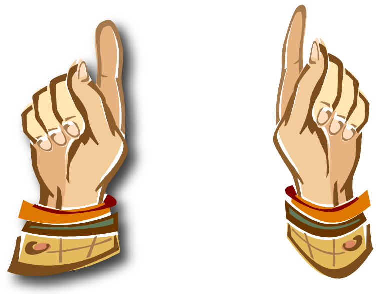
Mármost,

Mármost, ha az $ax = b$ egyenletek megoldhatók, akkor —

Mármost, ha az $ax = b$ egyenletek megoldhatók, akkor — az eddigi megfontolásban a bal és a jobb szerepének felcserélésével —



kapjuk, hogy az $xa = b$ egyenletek is megoldhatók!



kapjuk, hogy az $xa = b$ egyenletek is megoldhatók!

Tehát (a véges kancellatív félcsoportunkban) az $ax = b$ is és az $xa = b$ egyenletek is megoldhatók.

Tehát (a véges kancellatív félcsoportunkban) az $ax = b$ is és az $xa = b$ egyenletek is megoldhatók. Ezt használjuk ki a későbbiekben, amikor valamely adott elem helyett x-szer egy másik adott elemet írunk (a sorrend mindegy).

Rögzítsünk egy $a \in A$ elemet.

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$$eb =$$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$$eb = e(ax) =$$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$$eb = e(ax) = (ea)x =$$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$.

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

B

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\quad \Longrightarrow \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\implies \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\quad \Longrightarrow \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\Longrightarrow f =$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\quad \Longrightarrow \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\Longrightarrow f = ef =$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\quad \Longrightarrow \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\Longrightarrow$ $f = ef = e$. Ezért

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\quad \Longrightarrow \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\Longrightarrow f = ef = e$. Ezért

$(*)$ és $(**)$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\implies \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\implies f = ef = e$. Ezért

$(*)$ és $(**)$ $\implies$

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\implies \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\implies f = ef = e$. Ezért

$(*)$ és $(**)$ $\implies e$ egységelem! Jelöljük 1-gyel!

Van

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\quad\Longrightarrow \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\Longrightarrow f = ef = e$. Ezért

$(*)$ és $(**)$ $\Longrightarrow e$ egységelem! Jelöljük 1-gyel!

Van egységelem, tehát $(A; \cdot)$ monoid! Vajon

Rögzítsünk egy $a \in A$ elemet. Az $xa = a$ egyik megoldását jelölje e. Ekkor tetszőleges b elemre

$eb = e(ax) = (ea)x = ax = b$. Azaz bármely b-re $eb = b$. $(*)$

Bal $\leftrightarrow$ jobb $\implies \exists f \in A$, hogy $\forall b$-re $bf = b$. $(**)$

$(*)$ és $(**)$ $\implies f = ef = e$. Ezért

$(*)$ és $(**)$ $\implies e$ egységelem! Jelöljük 1-gyel!

Van egységelem, tehát $(A; \cdot)$ monoid! Vajon van-e tetszőleges $a \in A$-nak inverze?

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Va-
jon

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$???

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt)

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \;=$$

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

De ez könnyen adódik: $(ab)a =$

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

De ez könnyen adódik: $(ab)a = a(ba) =$

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

De ez könnyen adódik: $(ab)a = a(ba) = a1 =$

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

De ez könnyen adódik: $(ab)a = a(ba) = a1 = a$, csakugyan.

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

De ez könnyen adódik: $(ab)a = a(ba) = a1 = a$, csakugyan.

Tehát b inverze a-nak.

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

De ez könnyen adódik: $(ab)a = a(ba) = a1 = a$, csakugyan.

Tehát b inverze a-nak. Így minden elemnek van inverze, ezért

Az $xa = 1$ egyenletre gondolva van olyan b, hogy $ba = 1$. Vajon inverze-e b az a-nak? Azaz vajon $ab \stackrel{?}{=} 1$??? Ehhez (a kancellativitás miatt) elegendő lenne, hogy

$$(ab)a \stackrel{?}{=} 1a.$$

De ez könnyen adódik: $(ab)a = a(ba) = a1 = a$, csakugyan.

Tehát b inverze a-nak. Így minden elemnek van inverze, ezért $(A; \cdot)$ csakugyan csoport. Q.e.d.

Gyűrűk

Def: Ha $*$ és $\circ$ kétváltozós műveletek egy nemüres A halmazon, akkor $*$ **disztributív** a $\circ$-ra

Gyűrűk

Def: Ha $*$ és $\circ$ kétváltozós műveletek egy nemüres A halmazon, akkor $*$ **disztributív** a $\circ$-ra $\overset{\text{def}}{\iff}$ $\forall a, b, c \in A$-ra

$a * (b \circ c) = (a * b) \circ (a * c)$ **és** $(b \circ c) * a = (b * a) \circ (c * a)$.

Példa (és ez alapján érdemes megjegyezni a fenti formulát): a (számok körében) **a szorzás disztributív az összeadásra**.

Gyűrűk

Def: Ha $*$ és $\circ$ kétváltozós műveletek egy nemüres A halmazon, akkor $*$ **disztributív** a $\circ$-ra $\overset{\text{def}}{\iff}$ $\forall a, b, c \in A$-ra

$a * (b \circ c) = (a * b) \circ (a * c)$ **és** $(b \circ c) * a = (b * a) \circ (c * a)$.

Példa (és ez alapján érdemes megjegyezni a fenti formulát): a (számok körében) **a szorzás disztributív az összeadásra**. (És nem fordítva.)

Példa:

Gyűrűk

Def: Ha $*$ és $\circ$ kétváltozós műveletek egy nemüres A halmazon, akkor $*$ **disztributív** a $\circ$-ra $\overset{\text{def}}{\Longleftrightarrow}$ $\forall a, b, c \in A$-ra

$a * (b \circ c) = (a * b) \circ (a * c)$ **és** $(b \circ c) * a = (b * a) \circ (c * a)$.

Példa (és ez alapján érdemes megjegyezni a fenti formulát): a (számok körében) **a szorzás disztributív az összeadásra**. (És nem fordítva.)

Példa: $\cap$ és $\cup$ egymásra kölcsönösen disztributívak.

Gyűrűk

Def: Ha $*$ és $\circ$ kétváltozós műveletek egy nemüres A halmazon, akkor $*$ **disztributív** a $\circ$-ra $\overset{\text{def}}{\Longleftrightarrow}$ $\forall a, b, c \in A$-ra

$a * (b \circ c) = (a * b) \circ (a * c)$ **és** $(b \circ c) * a = (b * a) \circ (c * a)$.

Példa (és ez alapján érdemes megjegyezni a fenti formulát): a (számok körében) **a szorzás disztributív az összeadásra**. (És nem fordítva.)

Példa: $\cap$ és $\cup$ egymásra kölcsönösen disztributívak. A $\cap$ disztributív a $\triangle$-ra (szimmetrikus differencia).

Feladat: mit jelent az, hogy f disztributív g-re? (Mindkettő kétváltozós.)

Feladat: mit jelent az, hogy f disztributív g-re? (Mindkettő kétváltozós.)

Megoldás:

$$f(a, g(b, c)) = g(f(a, b), f(a, c))$$

Feladat: mit jelent az, hogy f disztributív g-re? (Mindkettő kétváltozós.)

Megoldás:

$f(a, g(b, c)) = g(f(a, b), f(a, c))$ és $f(g(b, c), a) = g(f(b, a), f(c, a))$

tetszőleges A-beli elemekre, mert

Feladat: mit jelent az, hogy f disztributív g-re? (Mindkettő kétváltozós.)

Megoldás:

$f(a, g(b, c)) = g(f(a, b), f(a, c))$ és $f(g(b, c), a) = g(f(b, a), f(c, a))$

tetszőleges A-beli elemekre, mert ide vezet, ha a szorzás helyére f-et, az összeadás helyére g-t írunk az alábbi azonosságban:

Feladat: mit jelent az, hogy f disztributív g-re? (Mindkettő kétváltozós.)

Megoldás:

$f(a, g(b, c)) = g(f(a, b), f(a, c))$ és $f(g(b, c), a) = g(f(b, a), f(c, a))$

tetszőleges A-beli elemekre, mert ide vezet, ha a szorzás helyére f-et, az összeadás helyére g-t írunk az alábbi azonosságban:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ és } (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Definíció: az $(A;+,\cdot)$ algebrai struktúra (ahol $+$ és $\cdot$ kétváltozós) **gyűrű** $\overset{\text{def}}{\Longleftrightarrow}$ $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport és a $\cdot$ disztributív az $+$-ra.

Definíció: az $(A;+,\cdot)$ algebrai struktúra (ahol $+$ és $\cdot$ kétváltozós) **gyűrű** $\overset{\text{def}}{\iff}$ $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport és a $\cdot$ disztributív az $+$-ra.

Tehát

Definíció: az $(A;+,\cdot)$ algebrai struktúra (ahol $+$ és $\cdot$ kétváltozós) **gyűrű** $\overset{\text{def}}{\Longleftrightarrow}$ $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport és a $\cdot$ disztributív az $+$-ra.

Tehát a gyűrű **kétműveletes** algebra, amelynek van egy ún. **additív csoportja**, az $(A;+)$ Abel-csoport, van egy **multiplikatív félcsoportja**, az $(A;\cdot)$ félcsoport, és a szorzás **disztributív** az összeadásra.

Példa: az egész számok gyűrűje.

Definíció: az $(A;+,\cdot)$ algebrai struktúra (ahol $+$ és $\cdot$ kétváltozós) **gyűrű** $\overset{\text{def}}{\Longleftrightarrow}$ $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport és a $\cdot$ disztributív az $+$-ra.

Tehát a gyűrű **kétműveletes** algebra, amelynek van egy ún. **additív csoportja**, az $(A;+)$ Abel-csoport, van egy **multiplikatív félcsoportja**, az $(A;\cdot)$ félcsoport, és a szorzás **disztributív** az összeadásra.

Példa: az egész számok gyűrűje.

A multiplikatív félcsoport jelzői

Definíció: az $(A;+,\cdot)$ algebrai struktúra (ahol $+$ és $\cdot$ kétváltozós) **gyűrű** $\overset{\text{def}}{\Longleftrightarrow}$ $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport és a $\cdot$ disztributív az $+$-ra.

Tehát a gyűrű **kétműveletes** algebra, amelynek van egy ún. **additív csoportja**, az $(A;+)$ Abel-csoport, van egy **multiplikatív félcsoportja**, az $(A;\cdot)$ félcsoport, és a szorzás **disztributív** az összeadásra.

Példa: az egész számok gyűrűje.

A multiplikatív félcsoport jelzői (kommutatív, egységelemes) egyúttal a gyűrű jelzői is.

Definíció: az $(A;+,\cdot)$ algebrai struktúra (ahol $+$ és $\cdot$ kétváltozós) **gyűrű** $\overset{\text{def}}{\iff}$ $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport és a $\cdot$ disztributív az $+$-ra.

Tehát a gyűrű **kétműveletes** algebra, amelynek van egy ún. **additív csoportja**, az $(A;+)$ Abel-csoport, van egy **multiplikatív félcsoportja**, az $(A;\cdot)$ félcsoport, és a szorzás **disztributív** az összeadásra.

Példa: az egész számok gyűrűje.

A multiplikatív félcsoport jelzői (kommutatív, egységelemes) egyúttal a gyűrű jelzői is. (Az összeadás — lévén Abelcsoport-művelet — automatikusan kommutatív és egységelemes.)

Példa: $(\mathbb{Z}; +, \cdot)$

Példa: $(\mathbb{Z}; +, \cdot)$ kommutatív egységelemes gyűrű!

Példa: $(\mathbf{Z};+,\cdot)$ kommutatív egységelemes gyűrű!

Példa:$(\mathbf{R}_{n\times n};+,\cdot)$ (valós $n \times n$ -es mátrixok)

Példa: $(\mathbf{Z};+,\cdot)$ kommutatív egységelemes gyűrű!

Példa:$(\mathbf{R}_{n\times n};+,\cdot)$ (valós $n \times n$ -es mátrixok) egységelemes de $n > 1$ esetén nem kommutatív gyűrű.

Példa: $(\mathbf{Z}; +, \cdot)$ kommutatív egységelemes gyűrű!

Példa:$(\mathbf{R}_{n\times n}; +, \cdot)$ (valós $n \times n$ -es mátrixok) egységelemes de $n > 1$ esetén nem kommutatív gyűrű. Itt a szokásos mátrixműveleteket tekintjük. Az egységmátrix lesz az egységelem.

Példa: $(\mathbf{Z};+,\cdot)$ kommutatív egységelemes gyűrű!

Példa:$(\mathbf{R}_{n\times n};+,\cdot)$ (valós $n\times n$ -es mátrixok) egységelemes de $n>1$ esetén nem kommutatív gyűrű. Itt a szokásos mátrixműveleteket tekintjük. Az egységmátrix lesz az egységelem. (Az ezen kijelentésünket bizonyító azonosságokat a múlt félévben tanultuk.)

Példa:$(\mathbf{Z}_{n\times n};+,\cdot)$ egységelemes, nem kommutatív gyűrű.

Példa: $(\mathbf{Z};+,\cdot)$ kommutatív egységelemes gyűrű!

Példa:$(\mathbf{R}_{n\times n};+,\cdot)$ (valós $n \times n$ -es mátrixok) egységelemes de $n > 1$ esetén nem kommutatív gyűrű. Itt a szokásos mátrixműveleteket tekintjük. Az egységmátrix lesz az egységelem. (Az ezen kijelentésünket bizonyító azonosságokat a múlt félévben tanultuk.)

Példa:$(\mathbf{Z}_{n\times n};+,\cdot)$ egységelemes, nem kommutatív gyűrű. Az előbbi példa fényében ennek igazolására csak annyit kell mondanunk, hogy ha két mátrix egész számokból áll, akkor — a mátrixszorzás formulája miatt — a szorzatuk is,

Példa: $(\mathbf{Z};+,\cdot)$ kommutatív egységelemes gyűrű!

Példa:$(\mathbf{R}_{n\times n};+,\cdot)$ (valós $n\times n$ -es mátrixok) egységelemes de $n>1$ esetén nem kommutatív gyűrű. Itt a szokásos mátrixműveleteket tekintjük. Az egységmátrix lesz az egységelem. (Az ezen kijelentésünket bizonyító azonosságokat a múlt félévben tanultuk.)

Példa:$(\mathbf{Z}_{n\times n};+,\cdot)$ egységelemes, nem kommutatív gyűrű. Az előbbi példa fényében ennek igazolására csak annyit kell mondanunk, hogy ha két mátrix egész számokból áll, akkor — a mátrixszorzás formulája miatt — a szorzatuk is, továbbá az egységmátrix is egész számokból áll.

Példa: Ha U

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű.

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: ({páros

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{\text{páros egész számok}\}; +, \cdot)$

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{\text{páros egész számok}\}; +, \cdot)$ kommutatív

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{\text{páros egész számok}\}; +, \cdot)$ kommutatív de nem egységelemes gyűrű.

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. 0 : $\emptyset$, 1 : U. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{\text{páros egész számok}\}; +, \cdot)$ kommutatív de nem egységelemes gyűrű. Nem

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{\text{páros egész számok}\}; +, \cdot)$ kommutatív de nem egységelemes gyűrű. Nem azért nem egységelemes, mert az 1 páratlan szám lévén nincs benne! Hanem

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{$páros egész számok$\}; +, \cdot)$ kommutatív de nem egységelemes gyűrű. Nem azért nem egységelemes, mert az 1 páratlan szám lévén nincs benne! Hanem mert nincs olyan e páros szám, hogy bármely x páros számra $ex = x$ lenne,

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{\text{páros egész számok}\}; +, \cdot)$ kommutatív de nem egységelemes gyűrű. Nem azért nem egységelemes, mert az 1 páratlan szám lévén nincs benne! Hanem mert nincs olyan e páros szám, hogy bármely x páros számra $ex = x$ lenne, sőt

Példa: Ha U halmaz, akkor $(P(U); \triangle, \cap)$ kommutatív egységelemes gyűrű. $0 : \emptyset$, $1 : U$. (A megfelelő azonosságok — mellesleg nem túl nehéz — igazolása a múlt félévi gyakorlat anyagához tartozik.)

Példa: $(\{\text{páros egész számok}\}; +, \cdot)$ kommutatív de nem egységelemes gyűrű. Nem azért nem egységelemes, mert az 1 páratlan szám lévén nincs benne! Hanem mert nincs olyan e páros szám, hogy bármely x páros számra $ex = x$ lenne, sőt még olyan sincs, hogy mondjuk $e \cdot 2 = 2$ legyen.

Példa: ({páratlan

Példa: $(\{\text{páratlan egész számok}\}; +, \cdot)$

Példa: $(\{\text{páratlan egész számok}\}; +, \cdot)$ **nem** gyűrű, mégcsak nem is algebra(i struktúra).

Példa: $(\{\text{páratlan egész számok}\}; +, \cdot)$ **nem** gyűrű, mégcsak nem is algebra(i struktúra). Bár az azonosságok látszólag OK, a szorzással sincs gond, az összadás **nem művelet**, hiszen két páratlan szám összege nem páratlan! (Ha

Példa: ($\{$páratlan egész számok$\}; +, \cdot$) **nem** gyűrű, mégcsak nem is algebra(i struktúra). Bár az azonosságok látszólag OK, a szorzással sincs gond, az összadás **nem művelet**, hiszen két páratlan szám összege nem páratlan! (Ha mást nem mondunk, mint itt is, a $+$ és $\cdot$ a szokásos jelentésűek.)

Példa: $(\{\text{páratlan egész számok}\}; +, \cdot)$ **nem** gyűrű, mégcsak nem is algebra(i struktúra). Bár az azonosságok látszólag OK, a szorzással sincs gond, az összeadás **nem művelet**, hiszen két páratlan szám összege nem páratlan! (Ha mást nem mondunk, mint itt is, a $+$ és $\cdot$ a szokásos jelentésűek.)

Gyűrűben (ha mást nem mondunk) az additív csoport

Példa: ({páratlan egész számok}; $+, \cdot$) **nem** gyűrű, mégcsak nem is algebra(i struktúra). Bár az azonosságok látszólag OK, a szorzással sincs gond, az összadás **nem művelet**, hiszen két páratlan szám összege nem páratlan! (Ha mást nem mondunk, mint itt is, a $+$ és $\cdot$ a szokásos jelentésűek.)

Gyűrűben (ha mást nem mondunk) az additív csoport egységelemét 0, a multiplikatív félcsoport egységelemét (ha van) 1 jelöli.

Definíció **test** $\overset{\text{def}}{\Longleftrightarrow}$ **kommutatív, legalább kételemű, egységelemes gyűrű**, amelyben **minden nemnulla elemnek van** multiplikatív **inverze**.

A definíciók alapján meggondolható (de most nem tesszük), hogy

5. Állítás. *Egy kommutatív gyűrű akkor és csak akkor test, ha nullától különböző elemei a szorzásra nézve csoportot alkotnak.*

Definíció **test** $\overset{\text{def}}{\Longleftrightarrow}$ **kommutatív, legalább kételemű, egységelemes gyűrű**, amelyben **minden nemnulla elemnek van** multiplikatív **inverze**.

A definíciók alapján meggondolható (de most nem tesszük), hogy

5. Állítás. *Egy kommutatív gyűrű akkor és csak akkor test, ha nullától különböző elemei a szorzásra nézve csoportot alkotnak.*

Példák: a szokásos műveletekkel testek:

Definíció **test** $\overset{\text{def}}{\Longleftrightarrow}$ **kommutatív, legalább kételemű, egységelemes gyűrű**, amelyben **minden nemnulla elemnek van** multiplikatív **inverze**.

A definíciók alapján meggondolható (de most nem tesszük), hogy

5. Állítás. *Egy kommutatív gyűrű akkor és csak akkor test, ha nullától különböző elemei a szorzásra nézve csoportot alkotnak.*

Példák: a szokásos műveletekkel testek: $\mathbf{Q}$ és

Definíció **test** $\overset{\text{def}}{\Longleftrightarrow}$ **kommutatív, legalább kételemű, egységelemes gyűrű**, amelyben **minden nemnulla elemnek van** multiplikatív **inverze**.

A definíciók alapján meggondolható (de most nem tesszük), hogy

5. Állítás. *Egy kommutatív gyűrű akkor és csak akkor test, ha nullától különböző elemei a szorzásra nézve csoportot alkotnak.*

Példák: a szokásos műveletekkel testek: $\mathbf{Q}$ és $\mathbf{R}$. Más megfogalmazásban: a racionális, illetve a valós számok (a szokásos műveletekkel) testet alkotnak.

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A = \{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$.

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A=\{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2} \in A$ és $a_2+b_2\sqrt{2} \in A$ (azaz ha $a_1,b_1,a_2,b_2 \in \mathbf{Q}$), akkor

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b\in\mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A=\{a+b\sqrt{2} : a,b\in\mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2}\in A$ és $a_2+b_2\sqrt{2}\in A$ (azaz ha $a_1,b_1,a_2,b_2\in\mathbf{Q}$), akkor

$$a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2}=$$

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A=\{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2} \in A$ és $a_2+b_2\sqrt{2} \in A$ (azaz ha $a_1,b_1,a_2,b_2 \in \mathbf{Q}$), akkor

$$a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2} = (\underbrace{a_1+a_2}_{\in \mathbf{Q}})+(\underbrace{b_1+b_2}_{\in \mathbf{Q}})\sqrt{2} \in A$$

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A = \{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2} \in A$ és $a_2+b_2\sqrt{2} \in A$ (azaz ha $a_1, b_1, a_2, b_2 \in \mathbf{Q}$), akkor

$$a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2} = (\underbrace{a_1+a_2}_{\in \mathbf{Q}}) + (\underbrace{b_1+b_2}_{\in \mathbf{Q}})\sqrt{2} \in A \text{ és}$$

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) =$$

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A=\{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2} \in A$ és $a_2+b_2\sqrt{2} \in A$ (azaz ha $a_1,b_1,a_2,b_2 \in \mathbf{Q}$), akkor

$$a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2} = (\underbrace{a_1+a_2}_{\in \mathbf{Q}}) + (\underbrace{b_1+b_2}_{\in \mathbf{Q}})\sqrt{2} \in A \text{ és}$$

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = a_1a_2 +$$

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A=\{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2} \in A$ és $a_2+b_2\sqrt{2} \in A$ (azaz ha $a_1,b_1,a_2,b_2 \in \mathbf{Q}$), akkor

$$a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2} = (\underbrace{a_1+a_2}_{\in \mathbf{Q}}) + (\underbrace{b_1+b_2}_{\in \mathbf{Q}})\sqrt{2} \in A \text{ és}$$

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = a_1a_2+a_1b_2\sqrt{2}+$$

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A=\{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2} \in A$ és $a_2+b_2\sqrt{2} \in A$ (azaz ha $a_1,b_1,a_2,b_2 \in \mathbf{Q}$), akkor

$$a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2} = (\underbrace{a_1+a_2}_{\in \mathbf{Q}})+(\underbrace{b_1+b_2}_{\in \mathbf{Q}})\sqrt{2} \in A \text{ és}$$

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = a_1a_2+a_1b_2\sqrt{2}+a_2b_1\sqrt{2}$$

Példa: Az $(\{0,1\};+,\cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1+1=0$.

Feladat: Test-e, gyűrű-e az $(\{a+b\sqrt{2} : a,b \in \mathbf{Q}\};+,\cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A=\{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Ha $a_1+b_1\sqrt{2} \in A$ és $a_2+b_2\sqrt{2} \in A$ (azaz ha $a_1,b_1,a_2,b_2 \in \mathbf{Q}$), akkor

$$a_1+b_1\sqrt{2}+a_2+b_2\sqrt{2} = (\underbrace{a_1+a_2}_{\in \mathbf{Q}})+(\underbrace{b_1+b_2}_{\in \mathbf{Q}})\sqrt{2} \in A \text{ és}$$

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = a_1a_2+a_1b_2\sqrt{2}+a_2b_1\sqrt{2}+2b_1b_2 =$$

Példa: Az $(\{0, 1\}; +, \cdot)$ is test, ha a műveletek jelentése a szokásos, azzal a kivétellel, hogy most $1 + 1 = 0$.

Feladat: Test-e, gyűrű-e az $(\{a + b\sqrt{2} : a, b \in \mathbf{Q}\}; +, \cdot)$, ha a műveletek a valós számok körében szokásos műveleteket jelölik?

Megoldás: Legyen $A = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$. Ha $a_1 + b_1\sqrt{2} \in A$ és $a_2 + b_2\sqrt{2} \in A$ (azaz ha $a_1, b_1, a_2, b_2 \in \mathbf{Q}$), akkor

$$a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} = (\underbrace{a_1 + a_2}_{\in \mathbf{Q}}) + (\underbrace{b_1 + b_2}_{\in \mathbf{Q}})\sqrt{2} \in A \text{ és}$$

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + a_1b_2\sqrt{2} + a_2b_1\sqrt{2} + 2b_1b_2 =$$
$$(\underbrace{a_1a_2 + 2b_1b_2}_{\in \mathbf{Q}}) + (\underbrace{a_1b_2 + a_2b_1}_{\in \mathbf{Q}})\sqrt{2} \in A.$$

Ezért $(A; +, \cdot)$ valóban algebra.

Ezért $(A; +, \cdot)$ valóban algebra. (Ha nem lenne **zárt** a műveletekre, akkor még csak algebra sem lenne!

Ezért $(A;+,\cdot)$ valóban algebra. (Ha nem lenne **zárt** a műveletekre, akkor még csak algebra sem lenne!) Könnyű látni azt is, hogy $0 = 0 + 0 \cdot \sqrt{2} \in A$ és $a + b\sqrt{2} \in A$ esetén $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in A$.

Ezért $(A; +, \cdot)$ valóban algebra. (Ha nem lenne **zárt** a műveletekre, akkor még csak algebra sem lenne!) Könnyű látni azt is, hogy $0 = 0 + 0 \cdot \sqrt{2} \in A$ és $a + b\sqrt{2} \in A$ esetén $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in A$.

Tudjuk, hogy tetszőleges valós számok esetén érvényes a kommutativitás, asszociativitás és disztributivitás, Ezért $(A; +, \cdot)$ valóban algebra. (Ha nem lenne **zárt** a műveletekre, akkor még csak algebra sem lenne!) Könnyű látni azt is, hogy $0 = 0 + 0 \cdot \sqrt{2} \in A$ és $a + b\sqrt{2} \in A$ esetén $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in A$.

Tudjuk, hogy tetszőleges valós számok esetén érvényes a kommutativitás, asszociativitás és disztributivitás, ezért ezek annál inkább érvényesek, ha csak A-beli valós számokra szorítkozunk. (

Ezért $(A;+,\cdot)$ valóban algebra. (Ha nem lenne **zárt** a műveletekre, akkor még csak algebra sem lenne!) Könnyű látni azt is, hogy $0 = 0 + 0 \cdot \sqrt{2} \in A$ és $a + b\sqrt{2} \in A$ esetén $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in A$.

Tudjuk, hogy tetszőleges valós számok esetén érvényes a kommutativitás, asszociativitás és disztributivitás, ezért ezek annál inkább érvényesek, ha csak A-beli valós számokra szorítkozunk. (Más szóval, a műveletek asszociativitása, kommutativitása és disztributivitása „öröklődik" $\mathbf{R}$-ről A-ra.)

Ezért $(A;+,\cdot)$ valóban algebra. (Ha nem lenne **zárt** a műveletekre, akkor még csak algebra sem lenne!) Könnyű látni azt is, hogy $0 = 0 + 0\cdot\sqrt{2} \in A$ és $a + b\sqrt{2} \in A$ esetén $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in A$.

Tudjuk, hogy tetszőleges valós számok esetén érvényes a kommutativitás, asszociativitás és disztributivitás, ezért ezek annál inkább érvényesek, ha csak A-beli valós számokra szorítkozunk. (Más szóval, a műveletek asszociativitása, kommutativitása és disztributivitása „öröklődik" $\mathbf{R}$-ről A-ra.) Az eddigiekből látható, hogy $(A;+,\cdot)$ **gyűrű**.

Ezért $(A;+,\cdot)$ valóban algebra. (Ha nem lenne **zárt** a műveletekre, akkor még csak algebra sem lenne!) Könnyű látni azt is, hogy $0 = 0 + 0 \cdot \sqrt{2} \in A$ és $a + b\sqrt{2} \in A$ esetén $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2} \in A$.

Tudjuk, hogy tetszőleges valós számok esetén érvényes a kommutativitás, asszociativitás és disztributivitás, ezért ezek annál inkább érvényesek, ha csak A-beli valós számokra szorítkozunk. (Más szóval, a műveletek asszociativitása, kommutativitása és disztributivitása „öröklődik" $\mathbf{R}$-ről A-ra.) Az eddigiekből látható, hogy $(A;+,\cdot)$ **gyűrű**.

Ahhoz, hogy test legyen az kell, hogy nemzérus elemeinek legyen multiplikatív inverze (más szóval reciproka) **A-ban**.

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$).

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \dfrac{1}{x}$.

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \dfrac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\dfrac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} =$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \frac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\frac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} =$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \dfrac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\dfrac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} =$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \dfrac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\dfrac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} =$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \frac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\frac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} =$$

$$\underbrace{\frac{a}{a^2 - 2b^2}}$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \frac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\frac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} =$$

$$\underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbf{Q}} +$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \frac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\frac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} =$$

$$\underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbf{Q}} + \underbrace{\frac{-b}{a^2 - 2b^2}}_{\in \mathbf{Q}} \sqrt{2}$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \dfrac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\dfrac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbf{Q}} + \underbrace{\frac{-b}{a^2 - 2b^2}}_{\in \mathbf{Q}} \sqrt{2} \in A\,.$$

Legyen $x = a + b\sqrt{2} \in A \setminus \{0\}$ (tehát $a, b \in \mathbf{Q}$). Ha x-nek A-ban van multiplikatív inverze, mondjuk $y \in A$, akkor $xy = 1$ miatt ($\mathbf{R}$-ben) $y = \frac{1}{x}$. Tehát csak az a kérdés, hogy (az R-beli) $\frac{1}{x}$ eleme-e A-nak. Számoljunk:

$$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} =$$

$$\underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbf{Q}} + \underbrace{\frac{-b}{a^2 - 2b^2}}_{\in \mathbf{Q}} \sqrt{2} \in A\,.$$

Ez azonban még nem teljes értékű, hiszen nem vizsgáltuk, hogy $a - b\sqrt{2}$, amivel a törtet bővítettük, vajon nem nulla-e (amikor is nem szabad vele törtet bővíteni)!

Ha (várakozásunkkal ellentétben)

Ha (várakozásunkkal ellentétben) $a - b\sqrt{2} = 0$, akkor két eset van. Ha $b \neq 0$, akkor $\sqrt{2} = \frac{a}{b} \in \mathbf{Q}$, ami nem lehet. Ha pedig $b = 0$, akkor $a = b\sqrt{2} = 0$ miatt $x = a + b\sqrt{2} = 0$, ami ellentmond korábbi feltevésünknek. Tehát $a - b\sqrt{2} \neq 0$.

Ha (várakozásunkkal ellentétben) $a - b\sqrt{2} = 0$, akkor két eset van. Ha $b \neq 0$, akkor $\sqrt{2} = \frac{a}{b} \in \mathbf{Q}$, ami nem lehet. Ha pedig $b = 0$, akkor $a = b\sqrt{2} = 0$ miatt $x = a + b\sqrt{2} = 0$, ami ellentmond korábbi feltevésünknek. Tehát $a - b\sqrt{2} \neq 0$.

Ezzel beláttuk, hogy a nemzérus elemeknek van multiplikatív inverzük. Tehát $(A; +, \cdot)$ test.

Ha (várakozásunkkal ellentétben) $a - b\sqrt{2} = 0$, akkor két eset van. Ha $b \neq 0$, akkor $\sqrt{2} = \frac{a}{b} \in \mathbf{Q}$, ami nem lehet. Ha pedig $b = 0$, akkor $a = b\sqrt{2} = 0$ miatt $x = a + b\sqrt{2} = 0$, ami ellentmond korábbi feltevésünknek. Tehát $a - b\sqrt{2} \neq 0$.

Ezzel beláttuk, hogy a nemzérus elemeknek van multiplikatív inverzük. Tehát $(A; +, \cdot)$ test.

Az alábbi példák segíthetnek, hogy ne keverjük össze a definíciókat:

természetes számok multiplikatív félcsoportja,

természetes számok multiplikatív félcsoportja,

az $(S_n; \circ)$ **ún. szimmetrikus csoport** vagy a kocka **forgáscsoportja**,

természetes számok multiplikatív félcsoportja,

az $(S_n; \circ)$ **ún. szimmetrikus csoport** vagy a kocka **forgáscsoportja**,

az egész számok gyűrűje,

természetes számok multiplikatív félcsoportja,

az $(S_n; \circ)$ **ún. szimmetrikus csoport** vagy a kocka **forgáscsoportja**,

az egész számok gyűrűje,

a valós számok teste.

természetes számok multiplikatív félcsoportja,

az $(S_n; \circ)$ **ún. szimmetrikus csoport** vagy a kocka **forgáscsoportja**,

az egész számok gyűrűje,

a valós számok teste.

természetes számok multiplikatív félcsoportja,

az $(S_n; \circ)$ **ún. szimmetrikus csoport** vagy a kocka **forgáscsoportja**,

az egész számok gyűrűje,

a valós számok teste.

Jelölés: gyűrű esetén $a - b := a + (-b)$

természetes számok multiplikatív félcsoportja,

az $(S_n; \circ)$ **ún. szimmetrikus csoport** vagy a kocka **forgáscsoportja**,

az egész számok gyűrűje,

a valós számok teste.

Jelölés: gyűrű esetén $a - b := a + (-b)$ (kivonás).

természetes számok multiplikatív félcsoportja,

az $(S_n; \circ)$ **ún. szimmetrikus csoport** vagy a kocka **forgáscsoportja**,

az egész számok gyűrűje,

a valós számok teste.

Jelölés: gyűrű esetén $a - b := a + (-b)$ (kivonás).

A definíciókból levezethető az alábbi tétel:

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.*

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.* $0x = 0$,

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.* $0x = 0$, $a(b - c) = ab - ac$,

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.* $0x = 0$, $a(b-c) = ab - ac$, $-(a+b) = -a-b$,

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.* $0x = 0$, $a(b-c) = ab - ac$, $-(a+b) = -a-b$, $a(-b) = -ab = (-a)b$,

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.* $0x = 0$, $a(b-c) = ab - ac$, $-(a+b) = -a-b$, $a(-b) = -ab = (-a)b$, $(-a)(-b) = ab$,

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.* $0x = 0$, $a(b-c) = ab - ac$, $-(a+b) = -a-b$, $a(-b) = -ab = (-a)b$, $(-a)(-b) = ab$, *általános disztributivitás (több tagú összegek szokásos szorzása):*

$$\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)},$$

ahol F *az összes olyan* f *leképezések halmaza, amelyekre a* $\sum_{f \in F}$ *utáni produktumnak (szorzatnak) értelme van,*

53. Tétel. *Gyűrűkben érvényesek a szokásos (azaz mátrixok, ill. a szorzás kommutativitását leszámítva a számok körében megszokott) számolási szabályok, pl.* $0x = 0$, $a(b-c) = ab - ac$, $-(a+b) = -a-b$, $a(-b) = -ab = (-a)b$, $(-a)(-b) = ab$, *általános disztributivitás (több tagú összegek szokásos szorzása):*

$$\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)},$$

ahol F *az összes olyan* f *leképezések halmaza, amelyekre a* $\sum\limits_{f \in F}$ *utáni produktumnak (szorzatnak) értelme van,*

pontosabban: F *az összes olyan* $f : \{1, \ldots, n\} \to \mathbf{N}$ *leképezések halmaza, amelyekre* $k = 1, \ldots, n$*-re* $1 \leq f(k) \leq m_k$.

Az "ijesztő formula" a "zárójelek szokásos fölbontásának felel meg. A

Az "ijesztő formula" a "zárójelek szokásos fölbontásának felel meg. A

$$\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$$

formulának, persze előnye is van:

Az "ijesztő formula" a "zárójelek szokásos fölbontásának felel meg. A

$$\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$$

formulának, persze előnye is van: szoros analógiát mutat a programozási nyelvekkel (és ezért a hagyományos, $\prod$ és $\sum$ jeleket nem tartalmazó kifejezéseknél könnyebben programozható). Ezt az alábbiakban demonstráljuk.

$$\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij}$$

```
szorzat := 1 ;
for i:= 1 to n do
begin szumma:=0 ;
      for j:=1 to m[i] do szumma:= szumma+a[i,j] ;
      szorzat := szorzat * szumma
end;    {és ekkor a szorzat értéke a kérdéses kifejezés}
```

A $\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

A $\displaystyle\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

A $\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

ha $n = 3$, $m_1 = m_2 = m_3 = 2$, akkor $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} \in F$-re:

A $\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

ha $n = 3$, $m_1 = m_2 = m_3 = 2$, akkor $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} \in F$-re:

$$\prod_{k=1}^{n} a_{k,f(k)} =$$

A $\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

ha $n = 3$, $m_1 = m_2 = m_3 = 2$, akkor $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} \in F$-re:

$$\prod_{k=1}^{n} a_{k,f(k)} = a_{1,f(1)} a_{2,f(2)} a_{3,f(3)} =$$

A $\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

ha $n = 3$, $m_1 = m_2 = m_3 = 2$, akkor $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} \in F$-re:

$$\prod_{k=1}^{n} a_{k,f(k)} = a_{1,f(1)} a_{2,f(2)} a_{3,f(3)} = a_{1,2} a_{2,1} a_{3,2} =$$

A $\prod_{i=1}^{n}\sum_{j=1}^{m_i} a_{ij} = \sum_{f\in F}\prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

ha $n = 3$, $m_1 = m_2 = m_3 = 2$, akkor $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} \in F$-re:

$$\prod_{k=1}^{n} a_{k,f(k)} = a_{1,f(1)}a_{2,f(2)}a_{3,f(3)} = a_{1,2}a_{2,1}a_{3,2} = a_{12}a_{21}a_{32},$$

és az ilyen tagokat (szám szerint $|F| = 8$-at) kell most összeadni:

A $\prod_{i=1}^{n} \sum_{j=1}^{m_i} a_{ij} = \sum_{f \in F} \prod_{k=1}^{n} a_{k,f(k)}$ formula speciális esetben:

ha $n = 3$, $m_1 = m_2 = m_3 = 2$, akkor $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} \in F$-re:

$$\prod_{k=1}^{n} a_{k,f(k)} = a_{1,f(1)} a_{2,f(2)} a_{3,f(3)} = a_{1,2} a_{2,1} a_{3,2} = a_{12} a_{21} a_{32},$$

és az ilyen tagokat (szám szerint $|F| = 8$-at) kell most összeadni:

$$(a_{11} + a_{12})(a_{21} + a_{22})(a_{31} + a_{32}) =$$
$$a_{11}a_{21}a_{31} + a_{11}a_{21}a_{32} + a_{11}a_{22}a_{31} + a_{11}a_{22}a_{32} +$$
$$a_{12}a_{21}a_{31} + a_{12}a_{21}a_{32} + a_{12}a_{22}a_{31} + a_{12}a_{22}a_{32}.$$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása:

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x =$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$$0x = (0 + 0)x =$$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x = (0 + 0)x = 0x + 0x$. Felhasználva ezt, az asszociativitást, és a $0x$ additív inverzének, azaz $-0x$-nek a ”jelentését”, kapjuk, hogy:

$0 =$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x = (0 + 0)x = 0x + 0x$. Felhasználva ezt, az asszociativitást, és a $0x$ additív inverzének, azaz $-0x$-nek a ''jelentését'', kapjuk, hogy:

$0 = 0x + (-0x) =$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x = (0 + 0)x = 0x + 0x$. Felhasználva ezt, az asszociativitást, és a $0x$ additív inverzének, azaz $-0x$-nek a ''jelentését'', kapjuk, hogy:

$0 = 0x + (-0x) = (0x + 0x) + (-0x) =$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x = (0 + 0)x = 0x + 0x$. Felhasználva ezt, az asszociativitást, és a $0x$ additív inverzének, azaz $-0x$-nek a ''jelentését'', kapjuk, hogy:

$0 = 0x + (-0x) = (0x + 0x) + (-0x) = 0x + (0x + (-0x)) =$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x = (0 + 0)x = 0x + 0x$. Felhasználva ezt, az asszociativitást, és a $0x$ additív inverzének, azaz $-0x$-nek a ''jelentését'', kapjuk, hogy:

$0 = 0x + (-0x) = (0x + 0x) + (-0x) = 0x + (0x + (-0x)) = 0x + 0 =$

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x = (0 + 0)x = 0x + 0x$. Felhasználva ezt, az asszociativitást, és a $0x$ additív inverzének, azaz $-0x$-nek a "jelentését", kapjuk, hogy:

$0 = 0x + (-0x) = (0x + 0x) + (-0x) = 0x + (0x + (-0x)) = 0x + 0 = 0x$.

Tehát $0x = 0$, valóban.

Részlet a Tétel bizonyításából: Állítjuk, hogy $0x = 0$, ennek igazolása: $0 + y = y$ bármely y-ra, hiszen a 0 jelöli az additív egységelemet. Speciálisan: $0 + 0 = 0$. Ezt és a disztributivitást felhasználva:

$0x = (0 + 0)x = 0x + 0x$. Felhasználva ezt, az asszociativitást, és a $0x$ additív inverzének, azaz $-0x$-nek a "jelentését", kapjuk, hogy:

$0 = 0x + (-0x) = (0x + 0x) + (-0x) = 0x + (0x + (-0x)) = 0x + 0 = 0x$.

Tehát $0x = 0$, valóban.

Feladatok

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás:

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az ♣ művelet disztributív a ♠ műveletre?

Megoldás: Útmutatás:

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

x

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y$$

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y\spadesuit z) =$$

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y\spadesuit z) = (x\clubsuit y)\spadesuit(x\clubsuit z)$$

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y\spadesuit z) = (x\clubsuit y)\spadesuit(x\clubsuit z) \text{ és } (x\spadesuit y)\clubsuit z =$$

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y\spadesuit z) = (x\clubsuit y)\spadesuit(x\clubsuit z) \text{ és } (x\spadesuit y)\clubsuit z = (x\clubsuit z)\spadesuit(y\clubsuit z).$$

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y\spadesuit z) = (x\clubsuit y)\spadesuit(x\clubsuit z) \text{ és } (x\spadesuit y)\clubsuit z = (x\clubsuit z)\spadesuit(y\clubsuit z).$$

Vigyázat, a (szorzás és összeadás esetével ellentétben) itt a $\clubsuit$-nek nincs precedenciája a $\spadesuit$-kel szemben!

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y\spadesuit z) = (x\clubsuit y)\spadesuit(x\clubsuit z) \text{ és } (x\spadesuit y)\clubsuit z = (x\clubsuit z)\spadesuit(y\clubsuit z).$$

Vigyázat, a (szorzás és összeadás esetével ellentétben) itt a $\clubsuit$-nek nincs precedenciája a $\spadesuit$-kel szemben! Ezt kell fordított lengyel jelölésbe átírni.

1. Feladat. Fordított lengyel jelölés esetén mit jelent, hogy az $\clubsuit$ művelet disztributív a $\spadesuit$ műveletre?

Megoldás: Útmutatás: az $x(y+z) = xy+xz$ és $(x+y)z = xz+yz$ analógiájára

$$x\clubsuit(y\spadesuit z) = (x\clubsuit y)\spadesuit(x\clubsuit z) \text{ és } (x\spadesuit y)\clubsuit z = (x\clubsuit z)\spadesuit(y\clubsuit z).$$

Vigyázat, a (szorzás és összeadás esetével ellentétben) itt a $\clubsuit$-nek nincs precedenciája a $\spadesuit$-kel szemben! Ezt kell fordított lengyel jelölésbe átírni. Azt jelenti, hogy az algebra bármely x, y, z elemére

$$xyz\spadesuit\clubsuit = xy\clubsuit xz\clubsuit\spadesuit \text{ és } xy\spadesuit z\clubsuit = xz\clubsuit yz\clubsuit\spadesuit.$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás:

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$,

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó.

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c =$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab)$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c =$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b + c - ab - ac - bc + abc,$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b + c - ab - ac - bc + abc,$$

$a * (b * c) =$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. <u>Tetszőleges</u> $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b + c - ab - ac - bc + abc,$$

$a * (b * c) = a + (b * c) - a(b * c) =$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b + c - ab - ac - bc + abc,$$
$$a * (b * c) = a + (b * c) - a(b * c) = a + (b + c - bc) - a(b + c - bc) =$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b + c - ab - ac - bc + abc,$$
$$a * (b * c) = a + (b * c) - a(b * c) = a + (b + c - bc) - a(b + c - bc) =$$
$$a + b + c - ab - ac - bc + abc$$

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b + c - ab - ac - bc + abc,$$
$$a * (b * c) = a + (b * c) - a(b * c) = a + (b + c - bc) - a(b + c - bc) =$$
$$a + b + c - ab - ac - bc + abc,$$

tehát a művelet asszociatív.

2. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(\mathbf{Z}; *)$ grupoidot, ahol $a * b := a + b - ab$.

Megoldás: Mivel $a, b \in \mathbf{Z}$-re $a * b := a + b - ab \in \mathbf{Z}$, valóban grupoidról van szó. Tetszőleges $a, b, c \in \mathbf{Z}$-re

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c =$$
$$a + b + c - ab - ac - bc + abc,$$
$$a * (b * c) = a + (b * c) - a(b * c) = a + (b + c - bc) - a(b + c - bc) =$$
$$a + b + c - ab - ac - bc + abc,$$

tehát a művelet asszociatív. Nyilván kommutatív is. Tehát $(\mathbf{Z}; *)$ kommutatív félcsoport.

Van-e egységeleme? Tegyük fel, hogy $e \in \mathbf{Z}$ egységelem, azaz bármely $x \in \mathbf{Z}$-re $e * x = x$ és $x * e = x$. (

Van-e egységeleme? Tegyük fel, hogy $e \in \mathbf{Z}$ egységelem, azaz bármely $x \in \mathbf{Z}$-re $e * x = x$ és $x * e = x$. (A kommutativitás miatt elég az egyikkel foglalkozni.)

Van-e egységeleme? Tegyük fel, hogy $e \in \mathbf{Z}$ egységelem, azaz bármely $x \in \mathbf{Z}$-re $e * x = x$ és $x * e = x$. (A kommutativitás miatt elég az egyikkel foglalkozni.) Számoljunk:

$(\forall x)\,(x = e * x =$

Van-e egységeleme? Tegyük fel, hogy $e \in \mathbf{Z}$ egységelem, azaz bármely $x \in \mathbf{Z}$-re $e * x = x$ és $x * e = x$. (A kommutativitás miatt elég az egyikkel foglalkozni.) Számoljunk:

$$(\forall x)\,(x = e * x = e + x - ex)$$

Van-e egységeleme? Tegyük fel, hogy $e \in \mathbf{Z}$ egységelem, azaz bármely $x \in \mathbf{Z}$-re $e * x = x$ és $x * e = x$. (A kommutativitás miatt elég az egyikkel foglalkozni.) Számoljunk:

$$(\forall x)\,(x = e * x = e + x - ex) \iff (\forall x)\,(e(1 - x) = 0)$$

Van-e egységeleme? Tegyük fel, hogy $e \in \mathbf{Z}$ egységelem, azaz bármely $x \in \mathbf{Z}$-re $e * x = x$ és $x * e = x$. (A kommutativitás miatt elég az egyikkel foglalkozni.) Számoljunk:

$$(\forall x)\,(x = e * x = e + x - ex) \iff (\forall x)\,(e(1 - x) = 0) \iff e = 0.$$

Tehát a 0 egységelem, és így $(\mathbf{Z}; *)$ **monoid**.

Van-e egységeleme? Tegyük fel, hogy $e \in \mathbf{Z}$ egységelem, azaz bármely $x \in \mathbf{Z}$-re $e * x = x$ és $x * e = x$. (A kommutativitás miatt elég az egyikkel foglalkozni.) Számoljunk:

$$(\forall x)\,(x = e * x = e + x - ex) \iff (\forall x)\,(e(1 - x) = 0) \iff e = 0.$$

Tehát a 0 egységelem, és így $(\mathbf{Z}; *)$ **monoid**.

Van-e tetszőleges $a \in \mathbf{Z}$-nek inverze, azaz van-e bármely a-hoz olyan $x \in \mathbf{Z}$, hogy $a * x = 0$? Számoljunk:

$$0 = a * x = a + x - ax = a + x(1 - a).$$

Innen látható, hogy pl. $a = 1$-nek nincs inverze,

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Van-e zéruselem?

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Van-e zéruselem? Ha $z \in \mathbf{Z}$ zéruselem, akkor bármely $x \in \mathbf{Z}$-re

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Van-e zéruselem? Ha $z \in \mathbf{Z}$ zéruselem, akkor bármely $x \in \mathbf{Z}$-re

$$(\forall x)(z = z * x = z + x - zx)$$

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Van-e zéruselem? Ha $z \in \mathbf{Z}$ zéruselem, akkor bármely $x \in \mathbf{Z}$-re

$$(\forall x)(z = z * x = z + x - zx) \iff (\forall x)(0 = x(1 - z)\,)$$

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Van-e zéruselem? Ha $z \in \mathbf{Z}$ zéruselem, akkor bármely $x \in \mathbf{Z}$-re

$$(\forall x)(z = z * x = z + x - zx) \iff (\forall x)(0 = x(1 - z)\,) \iff z = 1.$$

Tehát a monoidnak **van zéruseleme, az 1**.

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Van-e zéruselem? Ha $z \in \mathbf{Z}$ zéruselem, akkor bármely $x \in \mathbf{Z}$-re

$$(\forall x)(z = z * x = z + x - zx) \iff (\forall x)(0 = x(1 - z)\,) \iff z = 1.$$

Tehát a monoidnak **van zéruseleme, az 1**.

Mivel van zéruselem és egynél többelemű a grupoid, ezért <u>nem kancellatív</u>.

Innen látható, hogy pl. $a = 1$-nek nincs inverze, sőt a legtöbb a-nak nincs (hiszen a legtöbb a-ra a nem osztható $1 - a$-val). Tehát $(\mathbf{Z}; *)$ **nem csoport.**

Van-e zéruselem? Ha $z \in \mathbf{Z}$ zéruselem, akkor bármely $x \in \mathbf{Z}$-re

$$(\forall x)(z = z * x = z + x - zx) \iff (\forall x)(0 = x(1 - z)\,) \iff z = 1.$$

Tehát a monoidnak **van zéruseleme, az 1**.

Mivel van zéruselem és egynél többelemű a grupoid, ezért nem kancellatív. Hiszen bármely x, y-t a zéruselemmel szorozva ugyanazt (nevezetesen a zéruselemet) kapjuk, de ebből mégsem következik $x = y$.

3. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(A;*)$ grupoidot, ahol A a páros egész számok halmaza és $a*b := a - b + ab$.

3. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(A; *)$ grupoidot, ahol A a páros egész számok halmaza és $a * b := a - b + ab$.

Megoldás Az világos,

3. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(A; *)$ grupoidot, ahol A a páros egész számok halmaza és $a*b := a - b + ab$.

Megoldás Az világos, hogy $a, b \in A$ esetén $a * b \in A$. Tehát valóban grupoidról van szó.

3. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(A;*)$ grupoidot, ahol A a páros egész számok halmaza és $a*b := a-b+ab$.

Megoldás Az világos, hogy $a,b \in A$ esetén $a*b \in A$. Tehát valóban grupoidról van szó. Mivel $a*b = a-b+ab \neq b-a+ba = b*a$ (kivéve ha $a=b$), ezért $(A;*)$ **nem kommutatív**. Számoljunk:

$$(a * b) * c =$$

$$(a * b) * c = (a - b + ab) * c$$

$$(a * b) * c = (a - b + ab) * c = (a - b + ab) - c + (a - b + ab)c$$

$$(a * b) * c = (a - b + ab) * c = (a - b + ab) - c + (a - b + ab)c =$$
$$a - b - c + ab + ac - bc + abc,$$

$$(a*b)*c = (a-b+ab)*c = (a-b+ab)-c+(a-b+ab)c =$$

$$a-b-c+ab+ac-bc+abc,$$

$$a*(b*c)$$

$$(a*b)*c=(a-b+ab)*c=(a-b+ab)-c+(a-b+ab)c=$$

$$a-b-c+ab+ac-bc+abc,$$

$$a*(b*c)=a*(b-c+bc)$$

$$(a*b)*c=(a-b+ab)*c=(a-b+ab)-c+(a-b+ab)c=$$
$$a-b-c+ab+ac-bc+abc,$$
$$a*(b*c)=a*(b-c+bc)=a-(b-c+bc)+a(b-c+bc)$$

$$(a * b) * c = (a - b + ab) * c = (a - b + ab) - c + (a - b + ab)c =$$
$$a - b - c + ab + ac - bc + abc,$$
$$a * (b * c) = a * (b - c + bc) = a - (b - c + bc) + a(b - c + bc) =$$
$$a - b + c + ab - ac - bc + abc.$$

Innen (

$$(a*b)*c=(a-b+ab)*c=(a-b+ab)-c+(a-b+ab)c=$$
$$a-b-c+ab+ac-bc+abc,$$
$$a*(b*c)=a*(b-c+bc)=a-(b-c+bc)+a(b-c+bc)=$$
$$a-b+c+ab-ac-bc+abc.$$

Innen (sejtve, hogy e kettő általában nem egyenlő):

$$(a*b)*c = (a-b+ab)*c = (a-b+ab)-c+(a-b+ab)c =$$
$$a-b-c+ab+ac-bc+abc,$$
$$a*(b*c) = a*(b-c+bc) = a-(b-c+bc)+a(b-c+bc) =$$
$$a-b+c+ab-ac-bc+abc.$$

Innen (sejtve, hogy e kettő általában nem egyenlő):

$$((a*b)*c)-(a*(b*c)) = 2ac-2c = 2c(a-1),$$

ami (

$$(a*b)*c = (a-b+ab)*c = (a-b+ab)-c+(a-b+ab)c =$$
$$a-b-c+ab+ac-bc+abc,$$
$$a*(b*c) = a*(b-c+bc) = a-(b-c+bc)+a(b-c+bc) =$$
$$a-b+c+ab-ac-bc+abc.$$

Innen (sejtve, hogy e kettő általában nem egyenlő):

$$((a*b)*c)-(a*(b*c)) = 2ac-2c = 2c(a-1),$$

ami (az $a=1$ vagy $c=0$ kivételtől eltekintve) nem zérus. Tehát (a mondott kivételtől eltekintve) $(a*b)*c \neq a*(b*c)$, azaz a művelet nem asszociatív, és így $(A;*)$ **nem félcsoport**.

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex =$$

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x$$

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x$$

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e$$

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen (átrendezve) $2x = 2e$, ami

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen (átrendezve) $2x = 2e$, ami nem teljesülhet bármely $x \in A$-ra. Tehát **nincs egységelem**.

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen (átrendezve) $2x = 2e$, ami nem teljesülhet bármely $x \in A$-ra. Tehát **nincs egységelem**.

Tegyük fel, hogy $z \in A$ zéruselem. Ekkor

$$(\forall x)\,(z - x + zx =$$

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen (átrendezve) $2x = 2e$, ami nem teljesülhet bármely $x \in A$-ra. Tehát **nincs egységelem**.

Tegyük fel, hogy $z \in A$ zéruselem. Ekkor

$$(\forall x)\,(z - x + zx = z * x =$$

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen (átrendezve) $2x = 2e$, ami nem teljesülhet bármely $x \in A$-ra. Tehát **nincs egységelem**.

Tegyük fel, hogy $z \in A$ zéruselem. Ekkor

$$(\forall x)\,(z - x + zx = z * x = z = x * z$$

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen (átrendezve) $2x = 2e$, ami nem teljesülhet bármely $x \in A$-ra. Tehát **nincs egységelem**.

Tegyük fel, hogy $z \in A$ zéruselem. Ekkor

$$(\forall x)\,(z - x + zx = z * x = z = x * z = x - z + xz).$$

Innen

Tegyük fel, hogy $e \in A$ egységelem. Ekkor

$$(\forall x)\,(e - x + ex = e * x = x = x * e = x - e + xe).$$

Innen (átrendezve) $2x = 2e$, ami nem teljesülhet bármely $x \in A$-ra. Tehát **nincs egységelem**.

Tegyük fel, hogy $z \in A$ zéruselem. Ekkor

$$(\forall x)\,(z - x + zx = z * x = z = x * z = x - z + xz).$$

Innen (átrendezve) $2x = 2z$, ami nem teljesülhet bármely $x \in A$-ra. Tehát **nincs zéruselem**.

A kancellativitás lényegében azt jelenti, hogy $a * b := a - b + ab$ és az egyik tényezője egyértelműen meghatározza a másik tényezőt.

A kancellativitás lényegében azt jelenti, hogy $a * b := a - b + ab$ és az egyik tényezője egyértelműen meghatározza a másik tényezőt. Azonban ha $a = 1$, akkor $1 * b =$

A kancellativitás lényegében azt jelenti, hogy $a * b := a - b + ab$ és az egyik tényezője egyértelműen meghatározza a másik tényezőt. Azonban ha $a = 1$, akkor $1 * b = 1 - b + b = 1$ bármely b-re, tehát az 1-gyel nem lehet egyszerűsíteni balról. Ezért a művelet nem kancellatív.

A kancellativitás lényegében azt jelenti, hogy $a * b := a - b + ab$ és az egyik tényezője egyértelműen meghatározza a másik tényezőt. Azonban ha $a = 1$, akkor $1 * b = 1 - b + b = 1$ bármely b-re, tehát az 1-gyel nem lehet egyszerűsíteni balról. Ezért a művelet nem kancellatív. (Mellesleg jobbról sem lehet egyszerűsíteni: ha $b = -1$, akkor $a * (-1) = a - (-1) + a(-1) = 1$ minden a-ra.)

5. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az alábbi grupoidot:

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Megoldás:

5. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az alábbi grupoidot:

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Megoldás: Kommutatív (hiszen a „főátlóra szimmetrikus”).

5. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az alábbi grupoidot:

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Megoldás: Kommutatív (hiszen a „főátlóra szimmetrikus”). **Az 1 egységelem**,

5. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az alábbi grupoidot:

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Megoldás: Kommutatív (hiszen a „főátlóra szimmetrikus"). **Az 1 egységelem**, hiszen sorában, illetve oszlopában a fejléc sor, illetve oszlop ismétlődik meg.

5. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az alábbi grupoidot:

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Megoldás: Kommutatív (hiszen a „főátlóra szimmetrikus"). **Az 1 egységelem**, hiszen sorában, illetve oszlopában a fejléc sor, illetve oszlop ismétlődik meg. **A 2 zéruselem**,

5. Feladat. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az alábbi grupoidot:

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Megoldás: Kommutatív (hiszen a „főátlóra szimmetrikus”). **Az 1 egységelem**, hiszen sorában, illetve oszlopában a fejléc sor, illetve oszlop ismétlődik meg. **A 2 zéruselem**, hiszen sorában is és oszlopában is csak ő van.

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Az asszociativitás eldöntése a művelettáblázat alapján

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Az asszociativitás eldöntése a művelettáblázat alapján *reménytelenül nehéz*,

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Az asszociativitás eldöntése a művelettáblázat alapján *remény-telenül nehéz*, hiszen n-elemű grupod esetén n^3 darab (a, b, c) elemhármast kell megvizsgálni. (Szász Gábor tétele szerint az n^3 vizsgálat egyike sem hagyható el, ha $n \geq 4$.)

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Az asszociativitás eldöntése a művelettáblázat alapján *reménytelenül nehéz*, hiszen n-elemű grupod esetén n^3 darab (a, b, c) elemhármast kell megvizsgálni. (Szász Gábor tétele szerint az n^3 vizsgálat egyike sem hagyható el, ha $n \geq 4$.)

Ha nincs egyéb ötletünk vagy nem számítógéppel dolgozunk, akkor legjobb hozzá sem fogni.

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Az asszociativitás eldöntése a művelettáblázat alapján *remény-telenül nehéz*, hiszen n-elemű grupod esetén n^3 darab (a, b, c) elemhármast kell megvizsgálni. (Szász Gábor tétele szerint az n^3 vizsgálat egyike sem hagyható el, ha $n \geq 4$.)

Ha nincs egyéb ötletünk vagy nem számítógéppel dolgozunk, akkor legjobb hozzá sem fogni. Most viszont van:

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Az asszociativitás eldöntése a művelettáblázat alapján *reménytelenül nehéz*, hiszen n-elemű grupod esetén n^3 darab (a, b, c) elemhármast kell megvizsgálni. (Szász Gábor tétele szerint az n^3 vizsgálat egyike sem hagyható el, ha $n \geq 4$.)

Ha nincs egyéb ötletünk vagy nem számítógéppel dolgozunk, akkor legjobb hozzá sem fogni. Most viszont van: a válasz nyilván nem az elemek jelölésétől függ.

∘	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

∘	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a

∘	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor a művelet éppen a

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor a művelet éppen a minimumképzés!

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor a művelet éppen a minimumképzés! Amely nyilván asszociatív, hiszen bárhogy is zárójelezünk három elemet,

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor a művelet éppen a minimumképzés! Amely nyilván asszociatív, hiszen bárhogy is zárójelezünk három elemet, a végeredmény közülük a legkisebb.

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor a művelet éppen a minimumképzés! Amely nyilván asszociatív, hiszen bárhogy is zárójelezünk három elemet, a végeredmény közülük a legkisebb. Az eddigiek szerint a művelettáblázat **kommutatív monoidot** ad meg.

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor a művelet éppen a minimumképzés! Amely nyilván asszociatív, hiszen bárhogy is zárójelezünk három elemet, a végeredmény közülük a legkisebb. Az eddigiek szerint a művelettáblázat **kommutatív monoidot** ad meg. Ez **nem csoport**, mert a zéruselemnek nincs inverze (

$\circ$	0	1	2
0	0	0	2
1	0	1	2
2	2	2	2

Gondolatban mindenhol írjunk a 2 helyett -1-et! Ekkor a művelet éppen a minimumképzés! Amely nyilván asszociatív, hiszen bárhogy is zárójelezünk három elemet, a végeredmény közülük a legkisebb. Az eddigiek szerint a művelettáblázat **kommutatív monoidot** ad meg. Ez **nem csoport**, mert a zéruselemnek nincs inverze (hiszen nincs olyan elem, amellyel szorozva az egységelemet és nem a zéruselemet kapjuk.). A zéruselem létezése miatt (mivel $|A| > 1$) **nem kancellatív**. (Miért?) Q.e.d.

6 . Feladat. Gyűrű, illetve test-e a következő algebra: $(\{\mathbf{i}, \mathbf{h}\}; \not\leftrightarrow, \wedge)$? (Az ilyen feladatot úgy kell érteni, hogy az elsőnek megadott művelet játsza az összadás, a másik pedig a szorzás szerepét.)

6 . Feladat. Gyűrű, illetve test-e a következő algebra: $(\{\mathbf{i}, \mathbf{h}\}; \not\leftrightarrow, \wedge)$? (Az ilyen feladatot úgy kell érteni, hogy az elsőnek megadott művelet játsza az összadás, a másik pedig a szorzás szerepét.)

Megoldás:

6 . Feladat. Gyűrű, illetve test-e a következő algebra: $(\{\mathbf{i}, \mathbf{h}\}; \not\leftrightarrow, \wedge)$? (Az ilyen feladatot úgy kell érteni, hogy az elsőnek megadott művelet játsza az összadás, a másik pedig a szorzás szerepét.)

Megoldás: (Vázlat.)

6 . Feladat. Gyűrű, illetve test-e a következő algebra: $(\{\mathbf{i}, \mathbf{h}\}; \not\leftrightarrow, \wedge)$? (Az ilyen feladatot úgy kell érteni, hogy az elsőnek megadott művelet játsza az összadás, a másik pedig a szorzás szerepét.)

Megoldás: (Vázlat.) Bár tudjuk, hogy a konjunkció asszociatív, a megfelelő azonosságok (

6 . Feladat. Gyűrű, illetve test-e a következő algebra: $(\{\mathbf{i}, \mathbf{h}\}; \not\leftrightarrow, \wedge)$? (Az ilyen feladatot úgy kell érteni, hogy az elsőnek megadott művelet játsza az összadás, a másik pedig a szorzás szerepét.)

Megoldás: (Vázlat.) Bár tudjuk, hogy a konjunkció asszociatív, a megfelelő azonosságok (azaz tautológiák) ellenőrzése — bár ismert és szokásos teendő — sokáig tartana, ezért nem ismertetjük. (

6 . Feladat. Gyűrű, illetve test-e a következő algebra: $(\{\mathbf{i}, \mathbf{h}\}; \not\leftrightarrow, \wedge)$? (Az ilyen feladatot úgy kell érteni, hogy az elsőnek megadott művelet játsza az összadás, a másik pedig a szorzás szerepét.)

Megoldás: (Vázlat.) Bár tudjuk, hogy a konjunkció asszociatív, a megfelelő azonosságok (azaz tautológiák) ellenőrzése — bár ismert és szokásos teendő — sokáig tartana, ezért nem ismertetjük. (Pl. az $\not\leftrightarrow$ asszociativitásának ellenőrzéséhez egy nyolcsoros igazságtáblázatot kellene felírni, vagy a kifejezések azonos átalakításával kellene dolgozni.)

Ennél ötletesebb és gyorsabb, ha észrevesszük, hogy

Ennél ötletesebb és gyorsabb, ha észrevesszük, hogy ha 0-val, illetve 1-gyel jelöljük a $\mathbf{h}$ (hamis), illetve $\mathbf{i}$ (igaz) logikai értékeket, akkor $\wedge$ éppen a szorzás, $\not\leftrightarrow$ pedig éppen az (

Ennél ötletesebb és gyorsabb, ha észrevesszük, hogy ha 0-val, illetve 1-gyel jelöljük a $\mathbf{h}$ (hamis), illetve $\mathbf{i}$ (igaz) logikai értékeket, akkor $\wedge$ éppen a szorzás, $\not\leftrightarrow$ pedig éppen az (úgynevezett modulo 2) összeadás

Ennél ötletesebb és gyorsabb, ha észrevesszük, hogy ha 0-val, illetve 1-gyel jelöljük a $\mathbf{h}$ (hamis), illetve $\mathbf{i}$ (igaz) logikai értékeket, akkor $\wedge$ éppen a szorzás, $\not\leftrightarrow$ pedig éppen az (úgynevezett modulo 2) összeadás (ami csak annyiban különbözik a szokásostól, hogy $1+1=0$. Erről pedig már említettük, hogy ez test.

Ennél ötletesebb és gyorsabb, ha észrevesszük, hogy ha 0-val, illetve 1-gyel jelöljük a $\mathbf{h}$ (hamis), illetve $\mathbf{i}$ (igaz) logikai értékeket, akkor $\wedge$ éppen a szorzás, $\not\leftrightarrow$ pedig éppen az (úgynevezett modulo 2) összeadás (ami csak annyiban különbözik a szokásostól, hogy $1 + 1 = 0$. Erről pedig már említettük, hogy ez test. Tehát a válasz a feladatra: **test**, és akkor persze gyűrű is. Q.e.d.

Részalgebra

Kérdés: hogyan lehet újabb algebrákat (algebrai struktúrákat) kapni?

Részalgebra

Kérdés: hogyan lehet újabb algebrákat (algebrai struktúrákat) kapni? Egyik lehetőség: adott algebrának csak egy „részét” vesszük.

Definíció: Legyen $\mathbf{A} = (A; F)$ egy algebra. Ha H nemüres részhalmaza A-nak és **zárt** az algebra műveleteire,

Definíció: Legyen $\mathbf{A} = (A; F)$ egy algebra. Ha H nemüres részhalmaza A-nak és **zárt** az algebra műveleteire, azaz bármely $f \in F$ — mondjuk $n = n_f$-változós — művelet és bármely $a_1, \ldots, a_n \in H$ esetén $f(a_1, \ldots, a_n) \in H$, akkor $\mathbf{H} = (H; \{f_H : f \in F\})$-t az $\mathbf{A} = (A; F)$ egy algebra **részalgebrájának** nevezzük.

Definíció: Legyen $\mathbf{A} = (A; F)$ egy algebra. Ha H nemüres részhalmaza A-nak és **zárt** az algebra műveleteire, azaz bármely $f \in F$ — mondjuk $n = n_f$-változós — művelet és bármely $a_1, \ldots, a_n \in H$ esetén $f(a_1, \ldots, a_n) \in H$, akkor $\mathbf{H} = (H; \{f_H : f \in F\})$-t az $\mathbf{A} = (A; F)$ egy algebra **részalgebrájának** nevezzük. Itt $f \in F$-re f_H az f művelet H-ra való **megszorítását** jelöli, azaz

$$f_H : H^n \to H, \qquad (h_1, \ldots, h_n) \mapsto f(h_1, \ldots, h_n).$$

(Ennek azért van értelme, mert a zártság miatt csakugyan $f(h_1, \ldots, h_n) \in H$.)

Megjegyzés A műveleteket többnyire műveleti jelekkel (pl. $+$, f, ...) jelöljük, és

Megjegyzés A műveleteket többnyire műveleti jelekkel (pl. $+$, f, $\dots$) jelöljük, és rendszerint ugyanazon jel (tehát $+$, f, $\dots$) jelöli a megszorításukat is.

Megjegyzés A műveleteket többnyire műveleti jelekkel (pl. $+$, f, ...) jelöljük, és rendszerint ugyanazon jel (tehát $+$, f, ...) jelöli a megszorításukat is. Azaz $+_H$, f_H, ... helyett marad a $+$, f, ...) jelölés, és csak félreértés veszélye esetén alkalmazzuk a $+_H$, f_H, ... valamint a $+_A$, f_A, ... jelöléseket.

Megjegyzés A műveleteket többnyire műveleti jelekkel (pl. $+$, f, ...) jelöljük, és rendszerint ugyanazon jel (tehát $+$, f, ...) jelöli a megszorításukat is. Azaz $+_H$, f_H, ... helyett marad a $+$, f, ...) jelölés, és csak félreértés veszélye esetén alkalmazzuk a $+_H$, f_H, ... valamint a $+_A$, f_A, ... jelöléseket.

Gyakran, amikor a műveletek mibenléte nem kérdéses, az algebrák helyett csak a tartóhalmazukat adjuk meg.

Megjegyzés A műveleteket többnyire műveleti jelekkel (pl. $+$, f, ...) jelöljük, és rendszerint ugyanazon jel (tehát $+$, f, ...) jelöli a megszorításukat is. Azaz $+_H$, f_H, ... helyett marad a $+$, f, ...) jelölés, és csak félreértés veszélye esetén alkalmazzuk a $+_H$, f_H, ... valamint a $+_A$, f_A, ... jelöléseket.

Gyakran, amikor a műveletek mibenléte nem kérdéses, az algebrák helyett csak a tartóhalmazukat adjuk meg. Ennek megfelelően mondhatjuk, hogy az $\mathbf{A} = (A; F)$ algebra egy

Megjegyzés A műveleteket többnyire műveleti jelekkel (pl. $+$, f, ...) jelöljük, és rendszerint ugyanazon jel (tehát $+$, f, ...) jelöli a megszorításukat is. Azaz $+_H$, f_H, ... helyett marad a $+$, f, ...) jelölés, és csak félreértés veszélye esetén alkalmazzuk a $+_H$, f_H, ... valamint a $+_A$, f_A, ... jelöléseket.

Gyakran, amikor a műveletek mibenléte nem kérdéses, az algebrák helyett csak a tartóhalmazukat adjuk meg. Ennek megfelelően mondhatjuk, hogy az $\mathbf{A} = (A; F)$ algebra egy H részhalmaza

Megjegyzés A műveleteket többnyire műveleti jelekkel (pl. $+$, f, ...) jelöljük, és rendszerint ugyanazon jel (tehát $+$, f, ...) jelöli a megszorításukat is. Azaz $+_H$, f_H, ... helyett marad a $+$, f, ...) jelölés, és csak félreértés veszélye esetén alkalmazzuk a $+_H$, f_H, ... valamint a $+_A$, f_A, ... jelöléseket.

Gyakran, amikor a műveletek mibenléte nem kérdéses, az algebrák helyett csak a tartóhalmazukat adjuk meg. Ennek megfelelően mondhatjuk, hogy az $\mathbf{A} = (A; F)$ algebra egy H részhalmaza **részalgebra**: ez azt jelenti, hogy H nemüres és zárt a műveletekre.

Gyakran speciális algebrákat (grupoidokat, félcsoportokat, csoportokat, gyűrűket, stb.) tekintünk, és csak az olyan részalgebrákra vagyunk kíváncsiak, amelyek maguk is ugyanolyan értelemben speciálisak

Gyakran speciális algebrákat (grupoidokat, félcsoportokat, csoportokat, gyűrűket, stb.) tekintünk, és csak az olyan részalgebrákra vagyunk kíváncsiak, amelyek maguk is ugyanolyan értelemben speciálisak (tehát grupoidok, félcsoportok, csoportok, gyűrűk, stb.)

Gyakran speciális algebrákat (grupoidokat, félcsoportokat, csoportokat, gyűrűket, stb.) tekintünk, és csak az olyan részalgebrákra vagyunk kíváncsiak, amelyek maguk is ugyanolyan értelemben speciálisak (tehát grupoidok, félcsoportok, csoportok, gyűrűk, stb.) Van amikor ez a kívánalom tetszőleges részalgebra esetén teljesül, és van amikor értelemszerűen módosítanunk kell a definíciót, hogy teljesüljön.

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak**, *illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén:

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak**, *illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens.

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak***, illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli,

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak***, illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli, hanem tetszőleges A-beli elemekre is teljesül és H-ban a szorzás ugyanazt jelenti, mint A-ban.

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak***, illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli, hanem tetszőleges A-beli elemekre is teljesül és H-ban a szorzás ugyanazt jelenti, mint A-ban. Még részletesebben:

$$(x \cdot_H y) \cdot_H z =$$

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak**, *illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli, hanem tetszőleges A-beli elemekre is teljesül és H-ban a szorzás ugyanazt jelenti, mint A-ban. Még részletesebben:

$$(x \cdot_H y) \cdot_H z = (x \cdot_A y) \cdot_A z =$$

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak**, *illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli, hanem tetszőleges A-beli elemekre is teljesül és H-ban a szorzás ugyanazt jelenti, mint A-ban. Még részletesebben:

$$(x \cdot_H y) \cdot_H z = (x \cdot_A y) \cdot_A z = x \cdot_A (y \cdot_A z) =$$

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak**, *illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli, hanem tetszőleges A-beli elemekre is teljesül és H-ban a szorzás ugyanazt jelenti, mint A-ban. Még részletesebben:

$$(x \cdot_H y) \cdot_H z = (x \cdot_A y) \cdot_A z = x \cdot_A (y \cdot_A z) = x \cdot_H (y \cdot_H z).$$

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak**, *illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli, hanem tetszőleges A-beli elemekre is teljesül és H-ban a szorzás ugyanazt jelenti, mint A-ban. Még részletesebben:

$$(x \cdot_H y) \cdot_H z = (x \cdot_A y) \cdot_A z = x \cdot_A (y \cdot_A z) = x \cdot_H (y \cdot_H z).$$

Tehát az asszociativitás **öröklődik** $\mathbf{A}$-ról $\mathbf{H}$-ra, és így $\mathbf{H} = (H; \cdot)$ is félcsoport.

6. Állítás. *Grupoid részalgebrája grupoid. Félcsoport részalgebrája félcsoport. (Ezért ezen esetekben a részalgebrát* **részgrupoidnak**, *illetve* **részfélcsoportnak** *nevezzük.)*

Bizonyítás: Grupoid esetén: evidens. Félcsoport esetén: legyen $\mathbf{H} = (H; \cdot)$ részalgebrája az $\mathbf{A} = (A; \cdot)$ félcsoportnak. Ha $x, y, z \in H$, akkor $(xy)z = x(yz)$ azért teljesül, mert ez nemcsak H-beli, hanem tetszőleges A-beli elemekre is teljesül és H-ban a szorzás ugyanazt jelenti, mint A-ban. Még részletesebben:

$$(x \cdot_H y) \cdot_H z = (x \cdot_A y) \cdot_A z = x \cdot_A (y \cdot_A z) = x \cdot_H (y \cdot_H z).$$

Tehát az asszociativitás **öröklődik** $\mathbf{A}$-ról $\mathbf{H}$-ra, és így $\mathbf{H} = (H; \cdot)$ is félcsoport. Q.e.d.

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra),

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t)

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t) az $\mathbf{S} = (S, \cdot)$ félcsoport **részfélcsoportjának** nevezzük.

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t) az $\mathbf{S} = (S, \cdot)$ félcsoport **részfélcsoportjának** nevezzük.

Példák: $(\mathbf{N}; +)$ részfélcsoportja $(\mathbf{R}; +)$-nak.

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t) az $\mathbf{S} = (S, \cdot)$ félcsoport **részfélcsoportjának** nevezzük.

Példák: $(\mathbf{N}; +)$ részfélcsoportja $(\mathbf{R}; +)$-nak. ($\{$páros egészek$\}; +)$ részfélcsoportja $(\mathbf{Z}; +)$-nak.

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t) az $\mathbf{S} = (S, \cdot)$ félcsoport **részfélcsoportjának** nevezzük.

Példák: $(\mathbf{N}; +)$ részfélcsoportja $(\mathbf{R}; +)$-nak. $(\{$páros egészek$\}; +)$ részfélcsoportja $(\mathbf{Z}; +)$-nak. Ellenben a

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t) az $\mathbf{S} = (S, \cdot)$ félcsoport **részfélcsoportjának** nevezzük.

Példák: $(\mathbf{N}; +)$ részfélcsoportja $(\mathbf{R}; +)$-nak. ($\{$páros egészek$\}; +)$ részfélcsoportja $(\mathbf{Z}; +)$-nak. Ellenben a $\{$páratlan egészek$\}$ **nem** részfélcsoportja $(\mathbf{Z}; +)$-nak,

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t) az $\mathbf{S} = (S, \cdot)$ félcsoport **részfélcsoportjának** nevezzük.

Példák: $(\mathbf{N}; +)$ részfélcsoportja $(\mathbf{R}; +)$-nak. ($\{$páros egészek$\}; +)$ részfélcsoportja $(\mathbf{Z}; +)$-nak. Ellenben a $\{$páratlan egészek$\}$ **nem** részfélcsoportja $(\mathbf{Z}; +)$-nak, hiszen nem zárt az összeadásra.

Fontossága miatt külön félcsoportokra is leírjuk a részfélcsoport fogalmát (amely itt azonos a részalgebra fogalmával):

Definíció: Legyen $\mathbf{S} = (S, \cdot)$ egy félcsoport. Ha H nemüres részhalmaza S-nek és **zárt** a félcsoport-műveletre (a szorzásra), azaz ha bármely $a, b \in H$ esetén $ab \in H$, akkor $\mathbf{H} = (H; \cdot)$-t (vagy röviden csak H-t) az $\mathbf{S} = (S, \cdot)$ félcsoport **részfélcsoportjának** nevezzük.

Példák: $(\mathbf{N}; +)$ részfélcsoportja $(\mathbf{R}; +)$-nak. ({páros egészek}$; +$) részfélcsoportja $(\mathbf{Z}; +)$-nak. Ellenben a {páratlan egészek} **nem** részfélcsoportja $(\mathbf{Z}; +)$-nak, hiszen nem zárt az összeadásra.

Láttuk, hogy a asszociativitás öröklődik a részalgebrára. Ezért volt a félcsoport részalgebrája automatikusan félcsoport.

Láttuk, hogy a asszociativitás öröklődik a részalgebrára. Ezért volt a félcsoport részalgebrája automatikusan félcsoport. Hasonlóan látható, hogy bármely **univerzálisan kvantifikált** feltétel, azaz bármely olyan, a függvénykalkulusban felírt zárt formula, amelyben minden változó a $\forall$ univerzális kvantor hatálya alatt áll, szintén öröklődik a részalgebrákra. Ilyen például a kommutativitás, a disztributivitás és a kancellativitás.

Viszont az egzisztenciális kvantort tartalmazó feltételek —

Viszont az egzisztenciális kvantort tartalmazó feltételek — ilyen pl. az egységelem létezésére, az inverz elem létezésére vonatkozó feltétel —

Viszont az egzisztenciális kvantort tartalmazó feltételek — ilyen pl. az egységelem létezésére, az inverz elem létezésére vonatkozó feltétel — általában nem öröklődnek a részalgebrákra. Ezért az ilyen feltételek segítségével definiált speciális algebrák, pl. monoidok, csoportok, gyűrűk, testek esetében nem érjük be a részalgebra általános fogalmával.

Viszont az egzisztenciális kvantort tartalmazó feltételek — ilyen pl. az egységelem létezésére, az inverz elem létezésére vonatkozó feltétel — általában nem öröklődnek a részalgebrákra. Ezért az ilyen feltételek segítségével definiált speciális algebrák, pl. monoidok, csoportok, gyűrűk, testek esetében nem érjük be a részalgebra általános fogalmával. Hanem az egyébként nem öröklődő feltételek kiszabásával csak olyan részalgebrákat tekintünk, amelyek maguk is monoidok, csoportok, gyűrűk, testek.

Definíció: Legyen $\mathbf{G} = (G, \cdot)$ egy csoport. Ha H nemüres részhalmaza G-nek és

Definíció: Legyen $\mathbf{G} = (G, \cdot)$ egy csoport. Ha H nemüres részhalmaza G-nek és

(1) H **zárt** a félcsoport-műveletre (azaz a szorzásra)

Definíció: Legyen $\mathbf{G} = (G, \cdot)$ egy csoport. Ha H nemüres részhalmaza G-nek és

(1) H **zárt** a félcsoport-műveletre (azaz a szorzásra) (azaz H részalgebra),

(2) H tartalmazza G **egységelemét**, és

Definíció: Legyen $\mathbf{G} = (G, \cdot)$ egy csoport. Ha H nemüres részhalmaza G-nek és

(1) H **zárt** a félcsoport-műveletre (azaz a szorzásra) (azaz H részalgebra),

(2) H tartalmazza G **egységelemét**, és

(3) H **zárt az inverzképzésre is**, azaz ha $a \in H$,

Definíció: Legyen $\mathbf{G} = (G, \cdot)$ egy csoport. Ha H nemüres részhalmaza G-nek és

(1) H **zárt** a félcsoport-műveletre (azaz a szorzásra) (azaz H részalgebra),

(2) H tartalmazza G **egységelemét**, és

(3) H **zárt az inverzképzésre is**, azaz ha $a \in H$, akkor a-nak a $\mathbf{G}$-ben tekintett a^{-1} inverze is H-beli,

Definíció: Legyen $\mathbf{G} = (G, \cdot)$ egy csoport. Ha H nemüres részhalmaza G-nek és

(1) H **zárt** a félcsoport-műveletre (azaz a szorzásra) (azaz H részalgebra),

(2) H tartalmazza G **egységelemét**, és

(3) H **zárt az inverzképzésre is**, azaz ha $a \in H$, akkor a-nak a $\mathbf{G}$-ben tekintett a^{-1} inverze is H-beli,

akkor $\mathbf{H} = (H; \cdot)$-t $\mathbf{G}$ (egyik) **részcsoportjának** nevezzük.

Például $(\mathbf{R} \setminus \{0\}; \cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q} \setminus \{0\}; \cdot)$,

Például $(\mathbf{R} \setminus \{0\}; \cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q} \setminus \{0\}; \cdot)$,

$(\{-1, 1\}; \cdot)$,

Például $(\mathbf{R} \setminus \{0\}; \cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q} \setminus \{0\}; \cdot)$,

$(\{-1, 1\}; \cdot)$, viszont nem részcsoportjai az alábbiak:

Például $(\mathbf{R} \setminus \{0\}; \cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q} \setminus \{0\}; \cdot)$,

$(\{-1, 1\}; \cdot)$, viszont nem részcsoportjai az alábbiak:

$(\{\text{irracionális számok}\}; \cdot)$,

Például $(\mathbf{R} \setminus \{0\}; \cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q} \setminus \{0\}; \cdot)$,

$(\{-1, 1\}; \cdot)$, viszont nem részcsoportjai az alábbiak:

$(\{\text{irracionális számok}\}; \cdot)$, (ez mégcsak nem is részalgebra, hiszen nem zárt a szorzásra: $\sqrt{2} \cdot \sqrt{2}$ nem irracionális),

Például $(\mathbf{R} \setminus \{0\}; \cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q} \setminus \{0\}; \cdot)$,

$(\{-1, 1\}; \cdot)$, viszont nem részcsoportjai az alábbiak:

$(\{\text{irracionális számok}\}; \cdot)$, (ez mégcsak nem is részalgebra, hiszen nem zárt a szorzásra: $\sqrt{2} \cdot \sqrt{2}$ nem irracionális),

$(\mathbf{N}; \cdot)$,

Például $(\mathbf{R}\setminus\{0\};\cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q}\setminus\{0\};\cdot)$,

$(\{-1,1\};\cdot)$, viszont nem részcsoportjai az alábbiak:

$(\{\text{irracionális számok}\};\cdot)$, (ez mégcsak nem is részalgebra, hiszen nem zárt a szorzásra: $\sqrt{2}\cdot\sqrt{2}$ nem irracionális),

$(\mathbf{N};\cdot)$, (nem zárt az inverzképzésre).

Például $(\mathbf{R}\setminus\{0\};\cdot)$ csoportnak részcsoportjai az alábbiak:

$(\mathbf{Q}\setminus\{0\};\cdot)$,

$(\{-1,1\};\cdot)$,   viszont nem részcsoportjai az alábbiak:

$(\{\text{irracionális számok}\};\cdot)$, (ez mégcsak nem is részalgebra, hiszen nem zárt a szorzásra: $\sqrt{2}\cdot\sqrt{2}$ nem irracionális),

$(\mathbf{N};\cdot)$, (nem zárt az inverzképzésre).

Látható, hogy $(\mathbf{N};\cdot)$ részalgebrája és ezért részfélcsoportja a $(\mathbf{R}\setminus\{0\};\cdot)$ csoportnak, de nem részcsoportja!

Definíció: Legyen $(R;+,\cdot)$ gyűrű, és legyen S nemüres részhalmaza R-nek. Akkor mondjuk, hogy $\mathbf{S} = (S;+,\cdot)$ **részgyűrűje** az $(R;+,\cdot)$ gyűrűnek, ha egyrészt részalgebrája (azaz zárt a szorzásra és az összeadásra), másrészt tartalmazza a nullát (azaz R additív egységelemét) és minden elemével együtt az elem ellentettjét.

Definíció: Legyen $(R;+,\cdot)$ gyűrű, és legyen S nemüres részhalmaza R-nek. Akkor mondjuk, hogy $\mathbf{S} = (S;+,\cdot)$ **részgyűrűje** az $(R;+,\cdot)$ gyűrűnek, ha egyrészt részalgebrája (azaz zárt a szorzásra és az összeadásra), másrészt tartalmazza a nullát (azaz R additív egységelemét) és minden elemével együtt az elem ellentettjét. Azaz ha $a, b \in S$, akkor ab, $a+b$, $-a \in S$ és $0 \in S$.

Definíció: Legyen $(R;+,\cdot)$ gyűrű, és legyen S nemüres részhalmaza R-nek. Akkor mondjuk, hogy $\mathbf{S} = (S;+,\cdot)$ **részgyűrűje** az $(R;+,\cdot)$ gyűrűnek, ha egyrészt részalgebrája (azaz zárt a szorzásra és az összeadásra), másrészt tartalmazza a nullát (azaz R additív egységelemét) és minden elemével együtt az elem ellentettjét. Azaz ha $a, b \in S$, akkor ab, $a+b$, $-a \in S$ és $0 \in S$.

Legyen $\mathbf{T} = (T;+,\cdot)$ test. Azokat a részgyűrűit, amelyek maguk is testek, a $\mathbf{T}$ test **résztesteinek** nevezzük.

Definíció: Legyen $(R;+,\cdot)$ gyűrű, és legyen S nemüres részhalmaza R-nek. Akkor mondjuk, hogy $\mathbf{S} = (S;+,\cdot)$ **részgyűrűje** az $(R;+,\cdot)$ gyűrűnek, ha egyrészt részalgebrája (azaz zárt a szorzásra és az összeadásra), másrészt tartalmazza a nullát (azaz R additív egységelemét) és minden elemével együtt az elem ellentettjét. Azaz ha $a,b \in S$, akkor ab, $a+b$, $-a \in S$ és $0 \in S$.

Legyen $\mathbf{T} = (T;+,\cdot)$ test. Azokat a részgyűrűit, amelyek maguk is testek, a $\mathbf{T}$ test **résztesteinek** nevezzük. Tehát $\emptyset \neq S \subseteq T$ résztest, ha $0, 1 \in S$, továbbá bármely $a,b \in S$ esetén ab, $a+b, -a \in S$ és $a \neq 0 \Longrightarrow a^{-1} \in S$.

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$,

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga (ezek az ún. triviális részgyűrűk),

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga (ezek az ún. triviális részgyűrűk), és pl. $\{$páros egészek$\}$.

N

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga (ezek az ún. triviális részgyűrűk), és pl. $\{$páros egészek$\}$.

Nem részgyűrűje a $\{$páratlan egészek$\}$

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga (ezek az ún. triviális részgyűrűk), és pl. $\{$páros egészek$\}$.

Nem részgyűrűje a $\{$páratlan egészek$\}$ (hiszen nem zárt az összadásra, tehát még csak nem is részalgebra),

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga (ezek az ún. triviális részgyűrűk), és pl. $\{$páros egészek$\}$.

Nem részgyűrűje a $\{$páratlan egészek$\}$ (hiszen nem zárt az összeadásra, tehát még csak nem is részalgebra),és nem részgyűrűje $(\mathbf{N}_0; +, \cdot)$

Példák: Az egész számok $(\mathbf{Z};+,\cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga (ezek az ún. triviális részgyűrűk), és pl. $\{$páros egészek$\}$.

Nem részgyűrűje a $\{$páratlan egészek$\}$ (hiszen nem zárt az összadásra, tehát még csak nem is részalgebra),és nem részgyűrűje $(\mathbf{N}_0;+,\cdot)$ (ez ugyan részalgebra, de nem zárt az ellentettképzésre).

Példák: Az egész számok $(\mathbf{Z}; +, \cdot)$ gyűrűjének részgyűrűje a $\{0\}$, önmaga (ezek az ún. triviális részgyűrűk), és pl. {páros egészek}.

Nem részgyűrűje a {páratlan egészek} (hiszen nem zárt az összeadásra, tehát még csak nem is részalgebra),és nem részgyűrűje $(\mathbf{N}_0; +, \cdot)$ (ez ugyan részalgebra, de nem zárt az ellentettképzésre).

Az $(\mathbf{R}; +, \cdot)$ testnek részteste $(\mathbf{Q}; +, \cdot)$, de nem részteste hanem csupán részgyűrűje $(\mathbf{Z}; +, \cdot)$.

Az eddigiek után már nem nehéz kitalálni, hogy

Definíció: Monoid **részmonoidján** olyan részfélcsoportot értünk, amelyik

Az eddigiek után már nem nehéz kitalálni, hogy

Definíció: Monoid **részmonoidján** olyan részfélcsoportot értünk, amelyik tartalmazza az eredeti monoid egységelemét.

Példa: Az $(\mathbf{Z}; \cdot)$ monoidnak részmonoidja $(\mathbf{N}; \cdot)$, részmonoidja a páratlan egészek halmaza is.

Az eddigiek után már nem nehéz kitalálni, hogy

Definíció: Monoid **részmonoidján** olyan részfélcsoportot értünk, amelyik tartalmazza az eredeti monoid egységelemét.

Példa: Az $(\mathbf{Z}; \cdot)$ monoidnak részmonoidja $(\mathbf{N}; \cdot)$, részmonoidja a páratlan egészek halmaza is. Csak részfélcsoportja de nem részmonoidja a páros egészek halmaza.

Az eddigiek után már nem nehéz kitalálni, hogy

Definíció: Monoid **részmonoidján** olyan részfélcsoportot értünk, amelyik tartalmazza az eredeti monoid egységelemét.

Példa: Az $(\mathbf{Z};\cdot)$ monoidnak részmonoidja $(\mathbf{N};\cdot)$, részmonoidja a páratlan egészek halmaza is. Csak részfélcsoportja de nem részmonoidja a páros egészek halmaza.

Érdekes észrevétel, hogy a $(\{0\},\cdot)$ monoid.

Az eddigiek után már nem nehéz kitalálni, hogy

Definíció: Monoid **részmonoidján** olyan részfélcsoportot értünk, amelyik tartalmazza az eredeti monoid egységelemét.

Példa: Az $(\mathbf{Z};\cdot)$ monoidnak részmonoidja $(\mathbf{N};\cdot)$, részmonoidja a páratlan egészek halmaza is. Csak részfélcsoportja de nem részmonoidja a páros egészek halmaza.

Érdekes észrevétel, hogy a $(\{0\},\cdot)$ monoid. (Csakugyan, az egyetlen eleme egyúttal egységeleme is). Ez a monoid

Az eddigiek után már nem nehéz kitalálni, hogy

Definíció: Monoid **részmonoidján** olyan részfélcsoportot értünk, amelyik tartalmazza az eredeti monoid egységelemét.

Példa: Az $(\mathbf{Z}; \cdot)$ monoidnak részmonoidja $(\mathbf{N}; \cdot)$, részmonoidja a páratlan egészek halmaza is. Csak részfélcsoportja de nem részmonoidja a páros egészek halmaza.

Érdekes észrevétel, hogy a $(\{0\}, \cdot)$ monoid. (Csakugyan, az egyetlen eleme egyúttal egységeleme is). Ez a monoid részfélcsoportja a $(\mathbf{Z}; \cdot)$ monoidnak,

Az eddigiek után már nem nehéz kitalálni, hogy

Definíció: Monoid **részmonoidján** olyan részfélcsoportot értünk, amelyik tartalmazza az eredeti monoid egységelemét.

Példa: Az $(\mathbb{Z}; \cdot)$ monoidnak részmonoidja $(\mathbb{N}; \cdot)$, részmonoidja a páratlan egészek halmaza is. Csak részfélcsoportja de nem részmonoidja a páros egészek halmaza.

Érdekes észrevétel, hogy a $(\{0\}, \cdot)$ monoid. (Csakugyan, az egyetlen eleme egyúttal egységeleme is). Ez a monoid részfélcsoportja a $(\mathbb{Z}; \cdot)$ monoidnak, de nem részmonoidja (hiszen nem tartalmazza az eredeti egységelemet, az 1-et).

Generátorrendszer

Definíció: Legyen $(A; F)$ egy algebra és X nemüres részhalmaza A-nak. Ekkor az X-nél bővebb részalgebrák metszetét az X **által generált részalgebrának** nevezzük.

Definíció: Legyen $(A; F)$ egy algebra és X nemüres részhalmaza A-nak. Ekkor az X-nél bővebb részalgebrák metszetét az X **által generált részalgebrának** nevezzük. Képletben (és a jelölést is megadva):

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részalgebrája } A\text{-nak}}} H \ .$$

Definíció: Legyen $(A; F)$ egy algebra és X nemüres részhalmaza A-nak. Ekkor az X-nél bővebb részalgebrák metszetét az X **által generált részalgebrának** nevezzük. Képletben (és a jelölést is megadva):

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részalgebrája } A\text{-nak}}} H \ .$$

Az $X \neq \emptyset$ kikötés csak azért kellett, nehogy a metszet üres legyen. Amennyiben valamilyen ok miatt a metszet nem lehet üres, az $X \neq \emptyset$ kikötést elhagyhatjuk.

Ezen általános definíció mintájára teljesen hasonlóan beszélhetünk félcsoport, csoport, gyűrű, test, stb. esetén az X részhalmaz által generált részfélcsoportról, részcsoportról, részgyűrűről, résztestről, stb.

Ezen általános definíció mintájára teljesen hasonlóan beszélhetünk félcsoport, csoport, gyűrű, test, stb. esetén az X részhalmaz által generált részfélcsoportról, részcsoportról, részgyűrűről, résztestről, stb. Egy-két példa:

Definíció: Legyen $(A; \cdot)$ egy félcsoport és X nemüres részhalmaza A-nak. Ekkor az X-nél bővebb részfélcsoportok metszetét az X **által generált részfélcsoportnak** nevezzük.

Definíció: Legyen $(A;\cdot)$ egy félcsoport és X nemüres részhalmaza A-nak. Ekkor az X-nél bővebb részfélcsoportok metszetét az X **által generált részfélcsoportnak** nevezzük. Képletben (és a jelölést is megadva):

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részfélcsoportja } A\text{-nak}}} H \,.$$

Definíció: Legyen $(R;+,\cdot)$ egy gyűrű és X részhalmaza R-nek. Ekkor az X-nél bővebb részgyűrűk metszetét az X **által generált részgyűrűnek** nevezzük.

Definíció: Legyen $(R; +, \cdot)$ egy gyűrű és X részhalmaza R-nek. Ekkor az X-nél bővebb részgyűrűk metszetét az X **által generált részgyűrűnek** nevezzük. Képletben (és a jelölést is megadva):

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részgyűrűje } R\text{-nek}}} H \ .$$

Definíció: Legyen $(R;+,\cdot)$ egy gyűrű és X részhalmaza R-nek. Ekkor az X-nél bővebb részgyűrűk metszetét az X **által generált részgyűrűnek** nevezzük. Képletben (és a jelölést is megadva):

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részgyűrűje } R\text{-nek}}} H\ .$$

Itt nem volt szükség az $X \neq \emptyset$ kikötésre, hiszen a fenti metszet biztos nem üres, mert mindegyik H tartalmazza a 0 elemet.

Szóhasználat: Néha szokás $[X]$-et az X **generátumának** nevezni. Amennyiben $[X]$ az egész kiindulási $(A;F)$ algebra, illetve csoport, gyűrű, stb., akkor X-et a kiindulási algebra (illetve csoport, gyűrű, stb.) **generátorrendszerének** nevezzük.

7. Állítás. *A generált részalgebra (*

7. Állítás. *A generált részalgebra (illetve generált részfélcsoport, generált részcsoport, generált részgyűrű)*

7. Állítás. *A generált részalgebra (illetve generált részfélcsoport, generált részcsoport, generált részgyűrű) valóban részalgebra (*

7. Állítás. *A generált részalgebra (illetve generált részfélcsoport, generált részcsoport, generált részgyűrű) valóban részalgebra (illetve részfélcsoport, részcsoport, részgyűrű).*

7. Állítás. *A generált részalgebra (illetve generált részfélcsoport, generált részcsoport, generált részgyűrű) valóban részalgebra (illetve részfélcsoport, részcsoport, részgyűrű).*

Bizonyítás (példaként csak csoportokra). Legyen $X \subseteq G$, ahol $(G; \cdot)$ csoport. Ekkor

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \, .$$

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H\ .$$

Ha $a, b \in [X]$, akkor

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H .$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$.

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \ .$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \ .$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz $[X]$ zárt a szorzásra.

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \ .$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz $[X]$ zárt a szorzásra.

Ha $a \in [X]$, akkor

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \,.$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz $[X]$ zárt a szorzásra.

Ha $a \in [X]$, akkor a metszet összes H tényezőjére $a \in H$.

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H\ .$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz $[X]$ zárt a szorzásra.

Ha $a \in [X]$, akkor a metszet összes H tényezőjére $a \in H$. De H részcsoport, ezért $a^{-1} \in H$. Tehát a^{-1} benne van a metszet összes tényezőjében, ezért $a^{-1} \in [X]$. Azaz

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \ .$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz $[X]$ zárt a szorzásra.

Ha $a \in [X]$, akkor a metszet összes H tényezőjére $a \in H$. De H részcsoport, ezért $a^{-1} \in H$. Tehát a^{-1} benne van a metszet összes tényezőjében, ezért $a^{-1} \in [X]$. Azaz $[X]$ zárt az inverzképzésre.

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \,.$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz $[X]$ zárt a szorzásra.

Ha $a \in [X]$, akkor a metszet összes H tényezőjére $a \in H$. De H részcsoport, ezért $a^{-1} \in H$. Tehát a^{-1} benne van a metszet összes tényezőjében, ezért $a^{-1} \in [X]$. Azaz $[X]$ zárt az inverzképzésre. Végül az összes H-ban benne van $1 = 1_G$, ezért a metszetben, azaz $[X]$-ben is.

$$[X] := \bigcap_{\substack{X \subseteq H \\ H \text{ részcsoportja } G\text{-nek}}} H \, .$$

Ha $a, b \in [X]$, akkor a metszet összes H tényezőjére $a, b \in H$. De H részcsoport, ezért $ab \in H$. Tehát ab benne van a metszet összes tényezőjében, ezért $ab \in [X]$. Azaz $[X]$ zárt a szorzásra.

Ha $a \in [X]$, akkor a metszet összes H tényezőjére $a \in H$. De H részcsoport, ezért $a^{-1} \in H$. Tehát a^{-1} benne van a metszet összes tényezőjében, ezért $a^{-1} \in [X]$. Azaz $[X]$ zárt az inverzképzésre. Végül az összes H-ban benne van $1 = 1_G$, ezért a metszetben, azaz $[X]$-ben is. Az eddigiek szerint $[X]$ részcsoport. Q.e.d.

Feladat Legyen $X_1 = \{2, 6\}$, $X_2 = \{2, 7\}$ és $X_3 = \{5, 12\}$.
Közülük melyik generátorrendszere az egész számok gyűrűjének?

Feladat Legyen $X_1 = \{2, 6\}$, $X_2 = \{2, 7\}$ és $X_3 = \{5, 12\}$. Közülük melyik generátorrendszere az egész számok gyűrűjének?

Megoldás: Tudjuk, hogy az $[X]$ az X-nél bővebb részgyűrűk metszete. Ez pontosan akkor lesz $\mathbf{Z}$, ha $\mathbf{Z}$ az egyetlen olyan részgyűrűje $(\mathbf{Z}; +, \cdot)$-nak, amelyiknek X részhalmaza.

Feladat Legyen $X_1 = \{2, 6\}$, $X_2 = \{2, 7\}$ és $X_3 = \{5, 12\}$. Közülük melyik generátorrendszere az egész számok gyűrűjének?

Megoldás: Tudjuk, hogy az $[X]$ az X-nél bővebb részgyűrűk metszete. Ez pontosan akkor lesz $\mathbf{Z}$, ha $\mathbf{Z}$ az egyetlen olyan részgyűrűje $(\mathbf{Z}; +, \cdot)$-nak, amelyiknek X részhalmaza. És pontosan ez esetben lesz X generátorrendszer.

Feladat Legyen $X_1 = \{2, 6\}$, $X_2 = \{2, 7\}$ és $X_3 = \{5, 12\}$. Közülük melyik generátorrendszere az egész számok gyűrűjének?

Megoldás: Tudjuk, hogy az $[X]$ az X-nél bővebb részgyűrűk metszete. Ez pontosan akkor lesz $\mathbf{Z}$, ha $\mathbf{Z}$ az egyetlen olyan részgyűrűje $(\mathbf{Z}; +, \cdot)$-nak, amelyiknek X részhalmaza. És pontosan ez esetben lesz X generátorrendszer.

X_1 esetén:

Feladat Legyen $X_1 = \{2, 6\}$, $X_2 = \{2, 7\}$ és $X_3 = \{5, 12\}$. Közülük melyik generátorrendszere az egész számok gyűrűjének?

Megoldás: Tudjuk, hogy az $[X]$ az X-nél bővebb részgyűrűk metszete. Ez pontosan akkor lesz $\mathbf{Z}$, ha $\mathbf{Z}$ az egyetlen olyan részgyűrűje $(\mathbf{Z}; +, \cdot)$-nak, amelyiknek X részhalmaza. És pontosan ez esetben lesz X generátorrendszer.

X_1 esetén: a $H = \{\text{páros egészek}\}$ részgyűrű és $X_1 \subseteq H$. Ezért X_1 nem generátorrendszer.

Feladat Legyen $X_1 = \{2, 6\}$, $X_2 = \{2, 7\}$ és $X_3 = \{5, 12\}$. Közülük melyik generátorrendszere az egész számok gyűrűjének?

Megoldás: Tudjuk, hogy az $[X]$ az X-nél bővebb részgyűrűk metszete. Ez pontosan akkor lesz $\mathbf{Z}$, ha $\mathbf{Z}$ az egyetlen olyan részgyűrűje $(\mathbf{Z}; +, \cdot)$-nak, amelyiknek X részhalmaza. És pontosan ez esetben lesz X generátorrendszer.

X_1 esetén: a $H = \{\text{páros egészek}\}$ részgyűrű és $X_1 \subseteq H$. Ezért X_1 nem generátorrendszer. Az előző bekezdés utólagos megvilágítására: a $H = \{\text{páros egészek}\}$ részgyűrű is részt vesz az $[X]$-et definiáló metszetképzésben. Ezért $[X]$, azaz a metszet, részhalmaza H-nak, és

Feladat Legyen $X_1 = \{2, 6\}$, $X_2 = \{2, 7\}$ és $X_3 = \{5, 12\}$. Közülük melyik generátorrendszere az egész számok gyűrűjének?

Megoldás: Tudjuk, hogy az $[X]$ az X-nél bővebb részgyűrűk metszete. Ez pontosan akkor lesz $\mathbf{Z}$, ha $\mathbf{Z}$ az egyetlen olyan részgyűrűje $(\mathbf{Z}; +, \cdot)$-nak, amelyiknek X részhalmaza. És pontosan ez esetben lesz X generátorrendszer.

X_1 esetén: a $H = \{$páros egészek$\}$ részgyűrű és $X_1 \subseteq H$. Ezért X_1 nem generátorrendszer. Az előző bekezdés utólagos megvilágítására: a $H = \{$páros egészek$\}$ részgyűrű is részt vesz az $[X]$-et definiáló metszetképzésben. Ezért $[X]$, azaz a metszet, részhalmaza H-nak, és ezért $[X] \neq \mathbf{Z}$.

$X_2 = \{2, 7\}$:

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7 + (-2) + (-2) + (-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1 + 1 + \cdots + 1 \in H$

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1+1+\cdots+1 \in H$ és $-n \in H$, azaz $H = \mathbf{Z}$.

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1+1+\cdots+1 \in H$ és $-n \in H$, azaz $H = \mathbf{Z}$. Tehát $\mathbf{Z}$ az egyetlen olyan részgyűrű, amelyik X_2-nél bővebb.

$X_2 = \{2,7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1+1+\cdots+1 \in H$ és $-n \in H$, azaz $H = \mathbf{Z}$. Tehát $\mathbf{Z}$ az egyetlen olyan részgyűrű, amelyik X_2-nél bővebb. Ezért (mint egytényezős metszet)

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1+1+\cdots+1 \in H$ és $-n \in H$, azaz $H = \mathbf{Z}$. Tehát $\mathbf{Z}$ az egyetlen olyan részgyűrű, amelyik X_2-nél bővebb. Ezért (mint egytényezős metszet) $[X_2] = \mathbf{Z}$.

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1+1+\cdots+1 \in H$ és $-n \in H$, azaz $H = \mathbf{Z}$. Tehát $\mathbf{Z}$ az egyetlen olyan részgyűrű, amelyik X_2-nél bővebb. Ezért (mint egytényezős metszet) $[X_2] = \mathbf{Z}$. Tehát X_2 generátorrendszer.

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1+1+\cdots+1 \in H$ és $-n \in H$, azaz $H = \mathbf{Z}$. Tehát $\mathbf{Z}$ az egyetlen olyan részgyűrű, amelyik X_2-nél bővebb. Ezért (mint egytényezős metszet) $[X_2] = \mathbf{Z}$. Tehát X_2 generátorrendszer.

$X_3 = \{5, 12\}$ esetén: mivel

$X_2 = \{2, 7\}$: ha egy H részgyűrűre $X_2 \subseteq H$, akkor $1 = 7+(-2)+(-2)+(-2) \in H$, és így $n \in \mathbf{N}$-re $n = 1+1+\cdots+1 \in H$ és $-n \in H$, azaz $H = \mathbf{Z}$. Tehát $\mathbf{Z}$ az egyetlen olyan részgyűrű, amelyik X_2-nél bővebb. Ezért (mint egytényezős metszet) $[X_2] = \mathbf{Z}$. Tehát X_2 generátorrendszer.

$X_3 = \{5, 12\}$ esetén: mivel $1 = 5{\cdot}5+(-12)+(-12)$, az előzőhöz hasonlóan adódik, hogy X_3 is generátorrendszer.

Azt sem nehéz belátni, hogy ha m és n relatív prímek, akkor $\{m, n\}$ generátorrendszere az egész számok gyűrűjének.

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete —

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg.

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, ehhez hozzávesszük az X-beli elemekből a műveletekkel

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, ehhez hozzávesszük az X-beli elemekből a műveletekkel **előállítható** elemeket, A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, ehhez hozzávesszük az X-beli elemekből a műveletekkel **előállítható** elemeket, az így kapott immár bővebb halmazhoz hozzávesszük a műveletek révén

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, ehhez hozzávesszük az X-beli elemekből a műveletekkel **előállítható** elemeket, az így kapott immár bővebb halmazhoz hozzávesszük a műveletek révén **előállítható** további elemeket, és így tovább.

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, ehhez hozzávesszük az X-beli elemekből a műveletekkel **előállítható** elemeket, az így kapott immár bővebb halmazhoz hozzávesszük a műveletek révén **előállítható** további elemeket, és így tovább. Így egyre bővülő halmazokat kapunk, és ezek uniója lesz a generátum.

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, ehhez hozzávesszük az X-beli elemekből a műveletekkel **előállítható** elemeket, az így kapott immár bővebb halmazhoz hozzávesszük a műveletek révén **előállítható** további elemeket, és így tovább. Így egyre bővülő halmazokat kapunk, és ezek uniója lesz a generátum. A szótár szerint: „to generate” = előállít, kivált, okoz.

A fenti példa mutatja, hogy a definíció — az X-nél bővebb részalgebrák, részgyűrűk, stb. metszete — alapján nem könnyű meghatározni az X generátumát. A definíció tulajdonképpen a szemléletünknek sem felel meg. Szemléletesen a generátumot úgy képzeljük el, hogy kiindulunk X elemeiből, ehhez hozzávesszük az X-beli elemekből a műveletekkel **előállítható** elemeket, az így kapott immár bővebb halmazhoz hozzávesszük a műveletek révén **előállítható** további elemeket, és így tovább. Így egyre bővülő halmazokat kapunk, és ezek uniója lesz a generátum. A szótár szerint: „to generate" = előállít, kivált, okoz.

Mivel a műveletek egymás utáni alkalmazása az elsőrendű nyelvben tanult kifejezéseknek felel meg, a fenti gondolat az alábbi tételben is megfogalmazható.

54. Tétel. *Legyen* $(A; F)$ *egy algebra és* $X \subseteq A$. *Ekkor az* X *által generált részalgebra*

$$[X] = \{t(b_1, \ldots, b_n) : b_1, \ldots, b_n \in X \text{ és } t \text{ kifejezés}\}.$$

Itt kifejezésen az egyenlőségjelből (mint egyetlen predikátumjelből) és az F *elemeiből mint függvényjelekből és az felépülő elsőrendű nyelv kifejezéseit értjük.*

54. Tétel. *Legyen* $(A; F)$ *egy algebra és* $X \subseteq A$. *Ekkor az* X *által generált részalgebra*

$$[X] = \{t(b_1, \ldots, b_n) : b_1, \ldots, b_n \in X \text{ és } t \text{ kifejezés}\}.$$

Itt kifejezésen az egyenlőségjelből (mint egyetlen predikátumjelből) és az F *elemeiből mint függvényjelekből és az felépülő elsőrendű nyelv kifejezéseit értjük.*

A változók maguk is kifejezések; ez biztosítja, hogy $X \subseteq [X]$.)

Részletesen csak a tétel speciális eseteit tárgyaljuk.

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A; \cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

Pl. ha $X = \{a, b, c\}$, akkor $[\{a, b, c\}]$ (szokásosabb jelöléssel $[a, b, c]$) tartalmazza az alábbi elemeket:

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

Pl. ha $X = \{a, b, c\}$, akkor $[\{a, b, c\}]$ (szokásosabb jelöléssel $[a, b, c]$) tartalmazza az alábbi elemeket: b,

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

Pl. ha $X = \{a, b, c\}$, akkor $[\{a, b, c\}]$ (szokásosabb jelöléssel $[a, b, c]$) tartalmazza az alábbi elemeket: b, $bcbcabc$,

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N}, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

Pl. ha $X = \{a, b, c\}$, akkor $[\{a, b, c\}]$ (szokásosabb jelöléssel $[a, b, c]$) tartalmazza az alábbi elemeket: b, $bcbcabc$, $aaaa = a^4$.

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

Pl. ha $X = \{a, b, c\}$, akkor $[\{a, b, c\}]$ (szokásosabb jelöléssel $[a, b, c]$) tartalmazza az alábbi elemeket: b, $bcbcabc$, $aaaa = a^4$.

(A bizonyítás meglehetősen egyszerű és hasznos gyakorló feladat.

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

Pl. ha $X = \{a, b, c\}$, akkor $[\{a, b, c\}]$ (szokásosabb jelöléssel $[a, b, c]$) tartalmazza az alábbi elemeket: b, $bcbcabc$, $aaaa = a^4$.

(A bizonyítás meglehetősen egyszerű és hasznos gyakorló feladat. A „véges” jelző a szorzat előtt fölösleges, hiszen félcsoportban végtelen szorzatot nem is definiáltunk.)

55. Tétel. *(A generált részfélcsoport leírása) Ha* $(A;\cdot)$ *félcsoport és* $X \subseteq A$*, akkor*

$$[X] = \{a_1 \cdots a_n : n \in \mathbf{N},\, a_1, \ldots, a_n \in X\},$$

azaz az X *által generált részfélcsoport az* X*-beli elemekből képezhető véges szorzatokból áll.*

Pl. ha $X = \{a, b, c\}$, akkor $[\{a, b, c\}]$ (szokásosabb jelöléssel $[a, b, c]$) tartalmazza az alábbi elemeket: b, $bcbcabc$, $aaaa = a^4$.

(A bizonyítás meglehetősen egyszerű és hasznos gyakorló feladat. A „véges” jelző a szorzat előtt fölösleges, hiszen félcsoportban végtelen szorzatot nem is definiáltunk.) Csoportok esetén a megfelelő fogalom és tétel hasonló.

56. Tétel. *(A generált részcsoport leírása) Ha* $(G; \cdot)$ *csoport és* $X \subseteq G$, *akkor*

56. Tétel. *(A generált részcsoport leírása) Ha* $(G;\cdot)$ *csoport és* $X \subseteq G$*, akkor*

$$[X] = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} : n \in \mathbf{N}_0,\, a_1, \ldots, a_n \in X,\, \epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}\},$$

azaz X *által generált részcsoport az* X*-beli elemekből és inverzeikből képezhető véges szorzatokból áll; beleértve az üresszorzatot, amelynek értéke 1 (*G *egységeleme).*

56. Tétel. *(A generált részcsoport leírása) Ha* $(G;\cdot)$ *csoport és* $X \subseteq G$, *akkor*

$$[X] = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} : n \in \mathbf{N}_0,\, a_1, \ldots, a_n \in X,\, \epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}\},$$

azaz X *által generált részcsoport az* X*-beli elemekből és inverzeikből képezhető véges szorzatokból áll; beleértve az üresszorzatot, amelynek értéke 1 (*G *egységeleme).*

Például $[a, b, c]$ tartalmazza az alábbi elemeket:

56. Tétel. *(A generált részcsoport leírása) Ha* $(G;\cdot)$ *csoport és* $X \subseteq G$*, akkor*

$$[X] = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} : n \in \mathbf{N}_0,\, a_1, \ldots, a_n \in X,\, \epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}\},$$

azaz X *által generált részcsoport az* X*-beli elemekből és inverzeikből képezhető véges szorzatokból áll; beleértve az üresszorzatot, amelynek értéke 1 (*G *egységeleme).*

Például $[a, b, c]$ tartalmazza az alábbi elemeket: b, b^{-1}, $c^{-1}c^{-1}c^{-1} = c^{-3}$,

56. Tétel. *(A generált részcsoport leírása) Ha* $(G;\cdot)$ *csoport és* $X \subseteq G$, *akkor*

$$[X] = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} : n \in \mathbf{N}_0,\, a_1, \ldots, a_n \in X,\, \epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}\},$$

azaz X *által generált részcsoport az* X*-beli elemekből és inverzeikből képezhető véges szorzatokból áll; beleértve az üres-szorzatot, amelynek értéke 1 (*G *egységeleme).*

Például $[a, b, c]$ tartalmazza az alábbi elemeket: b, b^{-1}, $c^{-1}c^{-1}c^{-1} = c^{-3}$, $b^{-1}cb^{-1}c^{-1}abc^{-1}$,

56. Tétel. *(A generált részcsoport leírása) Ha* $(G;\cdot)$ *csoport és* $X \subseteq G$*, akkor*

$$[X] = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} : n \in \mathbf{N}_0,\, a_1, \ldots, a_n \in X,\, \epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}\},$$

azaz X *által generált részcsoport az* X*-beli elemekből és inverzeikből képezhető véges szorzatokból áll; beleértve az üresszorzatot, amelynek értéke 1 (*G *egységeleme).*

Például $[a, b, c]$ tartalmazza az alábbi elemeket: b, b^{-1}, $c^{-1}c^{-1}c^{-1} = c^{-3}$, $b^{-1}cb^{-1}c^{-1}abc^{-1}$, $aaaa = a^4$.

56. Tétel. *(A generált részcsoport leírása) Ha* $(G; \cdot)$ *csoport és* $X \subseteq G$*, akkor*

$$[X] = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} : n \in \mathbf{N}_0,\ a_1, \ldots, a_n \in X,\ \epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}\},$$

azaz X *által generált részcsoport az* X*-beli elemekből és inverzeikből képezhető véges szorzatokból áll; beleértve az üres-szorzatot, amelynek értéke 1 (*G *egységeleme).*

Például $[a, b, c]$ tartalmazza az alábbi elemeket: b, b^{-1}, $c^{-1}c^{-1}c^{-1} = c^{-3}$, $b^{-1}cb^{-1}c^{-1}abc^{-1}$, $aaaa = a^4$.

Megjegyzés: $[X]$ jelölhetne generált részalgebrát, azaz esetünkben generált részfélcsoportot is, de ha csoportokról van szó, akkor egyéb kitétel híján $[X]$ természetesen a generált részcsoportot jelöli.

Definíció: Az egy elem által generált (azaz egyelemű generátorrendszerrel rendelkező) csoportot, illetve félcsoportot **ciklikus csoportnak**, illetve **ciklikus félcsoportnak** nevezzük.

Definíció: Az egy elem által generált (azaz egyelemű generátorrendszerrel rendelkező) csoportot, illetve félcsoportot **ciklikus csoportnak**, illetve **ciklikus félcsoportnak** nevezzük.

A generált részfélcsoportot, illetve részcsoportot leíró tétel speciális esete az alábbi állítás. (Később majd tökéletesítjük.) $[\{a\}]$ helyett a (rövidebb) $[a]$ jelölést alkalmazzuk.

Definíció: Az egy elem által generált (azaz egyelemű generátorrendszerrel rendelkező) csoportot, illetve félcsoportot **ciklikus csoportnak**, illetve **ciklikus félcsoportnak** nevezzük.

A generált részfélcsoportot, illetve részcsoportot leíró tétel speciális esete az alábbi állítás. (Később majd tökéletesítjük.) $[\{a\}]$ helyett a (rövidebb) $[a]$ jelölést alkalmazzuk.

8. Állítás. *Az a elem által generált $[a]$ ciklikus félcsoport elemei éppen az a^n $(n \in \mathrm{N})$ elemek.*

Definíció: Az egy elem által generált (azaz egyelemű generátorrendszerrel rendelkező) csoportot, illetve félcsoportot **ciklikus csoportnak**, illetve **ciklikus félcsoportnak** nevezzük.

A generált részfélcsoportot, illetve részcsoportot leíró tétel speciális esete az alábbi állítás. (Később majd tökéletesítjük.) $[\{a\}]$ helyett a (rövidebb) $[a]$ jelölést alkalmazzuk.

8. Állítás. *Az a elem által generált $[a]$ ciklikus félcsoport elemei éppen az a^n $(n \in \mathbf{N})$ elemek. Az a elem által generált $[a]$ ciklikus csoport elemei éppen az a^n $(n \in \mathbf{Z})$ elemek. (*

Definíció: Az egy elem által generált (azaz egyelemű generátorrendszerrel rendelkező) csoportot, illetve félcsoportot **ciklikus csoportnak**, illetve **ciklikus félcsoportnak** nevezzük.

A generált részfélcsoportot, illetve részcsoportot leíró tétel speciális esete az alábbi állítás. (Később majd tökéletesítjük.) $[\{a\}]$ helyett a (rövidebb) $[a]$ jelölést alkalmazzuk.

8. Állítás. *Az a elem által generált $[a]$ ciklikus félcsoport elemei éppen az a^n $(n \in \mathbf{N})$ elemek. Az a elem által generált $[a]$ ciklikus csoport elemei éppen az a^n $(n \in \mathbf{Z})$ elemek. (Egyik esetben sem állítjuk, hogy végtelen sok elemű, hiszen $n \neq m$ esetén $a^n = a^m$ is előfordulhat.)*

Példák: Az $(\mathbb{N};\cdot)$ félcsoportnak generátorrendszere $\mathbb{N}$ (ez evidens),

Példák: Az $(\mathbf{N};\cdot)$ félcsoportnak generátorrendszere $\mathbf{N}$ (ez evidens), továbbá az $X := \{1\} \cup \{\text{prímszámok}\}$ halmaz is,

Példák: Az $(\mathbf{N}; \cdot)$ félcsoportnak generátorrendszere $\mathbf{N}$ (ez evidens), továbbá az $X := \{1\} \cup \{\text{prímszámok}\}$ halmaz is, hiszen $\mathbf{N}$ minden eleme előáll X-beli elemek szorzataként.

Példák: Az $(\mathbf{N};\cdot)$ félcsoportnak generátorrendszere $\mathbf{N}$ (ez evidens), továbbá az $X := \{1\} \cup \{\text{prímszámok}\}$ halmaz is, hiszen $\mathbf{N}$ minden eleme előáll X-beli elemek szorzataként.

Ugyanezen félcsoportban [2] a 2-hatványok halmaza;

Példák: Az $(\mathbf{N}; \cdot)$ félcsoportnak generátorrendszere $\mathbf{N}$ (ez evidens), továbbá az $X := \{1\} \cup \{\text{prímszámok}\}$ halmaz is, hiszen $\mathbf{N}$ minden eleme előáll X-beli elemek szorzataként.

Ugyanezen félcsoportban $[2]$ a 2-hatványok halmaza; $[\{1\} \cup \{\text{páratlan prímszámok}\}]$ pedig a páratlan természetes számok halmaza.

Példák: Az $(\mathbf{N}; \cdot)$ félcsoportnak generátorrendszere $\mathbf{N}$ (ez evidens), továbbá az $X := \{1\} \cup \{\text{prímszámok}\}$ halmaz is, hiszen $\mathbf{N}$ minden eleme előáll X-beli elemek szorzataként.

Ugyanezen félcsoportban $[2]$ a 2-hatványok halmaza; $[\{1\} \cup \{\text{páratlan prímszámok}\}]$ pedig a páratlan természetes számok halmaza.

Példák: Az $(\mathbb{N};\cdot)$ félcsoportnak generátorrendszere $\mathbb{N}$ (ez evidens), továbbá az $X := \{1\} \cup \{\text{prímszámok}\}$ halmaz is, hiszen $\mathbb{N}$ minden eleme előáll X-beli elemek szorzataként.

Ugyanezen félcsoportban $[2]$ a 2-hatványok halmaza; $[\{1\} \cup \{\text{páratlan prímszámok}\}]$ pedig a páratlan természetes számok halmaza.

Az $(\mathbb{N};+)$ félcsoportnak az $\{1\}$ generátorrendszere, tehát ez a félcsoport ciklikus.

Példák: Az $(\mathbf{N};\cdot)$ félcsoportnak generátorrendszere $\mathbf{N}$ (ez evidens), továbbá az $X := \{1\} \cup \{\text{prímszámok}\}$ halmaz is, hiszen $\mathbf{N}$ minden eleme előáll X-beli elemek szorzataként.

Ugyanezen félcsoportban $[2]$ a 2-hatványok halmaza; $[\{1\} \cup \{\text{páratlan prímszámok}\}]$ pedig a páratlan természetes számok halmaza.

Az $(\mathbf{N};+)$ félcsoportnak az $\{1\}$ generátorrendszere, tehát ez a félcsoport ciklikus. Valóban, az additív írásmód miatt most nem az a^n-ekből hanem az $na = a + a + \cdots + a$ -kból $(n \in \mathbf{N})$ áll az $[a]$. Esetünkben $a = 1$ és az 1 többszöröseinek halmaza éppen $\mathbf{N}$.

A $(\mathbf{Z};+)$ csoport esetén az $\{1\}$ által generált rész**fél**csoport

A $(\mathbf{Z};+)$ csoport esetén az $\{1\}$ által generált rész**félcsoport** az $\mathbf{N}$, viszont az $\{1\}$ által generált részcsoport

A $(\mathbf{Z}; +)$ csoport esetén az $\{1\}$ által generált rész**fél**csoport az $\mathbf{N}$, viszont az $\{1\}$ által generált részcsoport $\mathbf{Z}$, tehát az $\{1\}$ generátorrendszer, és a tekintett csoport ciklikus.

A $(\mathbf{Z};+)$ csoport esetén az $\{1\}$ által generált rész**fél**csoport az $\mathbf{N}$, viszont az $\{1\}$ által generált részcsoport $\mathbf{Z}$, tehát az $\{1\}$ generátorrendszer, és a tekintett csoport ciklikus.

(Az $[X]$ jelölés csak akkor problémamentes, ha tudjuk, csoportot vagy félcsoportot akarunk-e generálni.)

Izomorfizmusok

A

Izomorfizmusok

A geometriában az egybevágó síkidomokat sok esetben nem szokás megkülönböztetni. Ilyen eset pl. az, amikor területet vagy kerületet számolunk.

Izomorfizmusok

A geometriában az egybevágó síkidomokat sok esetben nem szokás megkülönböztetni. Ilyen eset pl. az, amikor területet vagy kerületet számolunk. Az algebrák körében is van egy, az egybevágóságnak megfelelő fontos fogalom, amelyet izomorfiának nevezünk. Itt is érvényes lesz az, hogy az egymással izomorf algebrákat — sok esetben — nem fogjuk megkülönböztetni.

Izomorfizmusok

A geometriában az egybevágó síkidomokat sok esetben nem szokás megkülönböztetni. Ilyen eset pl. az, amikor területet vagy kerületet számolunk. Az algebrák körében is van egy, az egybevágóságnak megfelelő fontos fogalom, amelyet izomorfiának nevezünk. Itt is érvényes lesz az, hogy az egymással izomorf algebrákat — sok esetben — nem fogjuk megkülönböztetni.

Most egyidejűleg két olyan algebrát fogunk tekinteni, amelyek esetén azonos a műveletek jelölési módja.

(Az is elegendő lenne, hogy bijekció legyen az egyik algebra műveleti jeleinek halmaza és a másik algebra műveleti jeleinek halmaza között.

(Az is elegendő lenne, hogy bijekció legyen az egyik algebra műveleti jeleinek halmaza és a másik algebra műveleti jeleinek halmaza között. Ezért pl. grupoidok esetében — ellentétben a fenti megállapodással — a művelet eltérő jelölését is megengedjük.

(Az is elegendő lenne, hogy bijekció legyen az egyik algebra műveleti jeleinek halmaza és a másik algebra műveleti jeleinek halmaza között. Ezért pl. grupoidok esetében — ellentétben a fenti megállapodással — a művelet eltérő jelölését is megengedjük. Azt viszont csak kellő elővigyázatossággal mondhatjuk, hogy tekintsük az $(R_1; \spadesuit, \clubsuit)$ és az $(R_2; \oplus, \diamond)$ gyűrűket:

(Az is elegendő lenne, hogy bijekció legyen az egyik algebra műveleti jeleinek halmaza és a másik algebra műveleti jeleinek halmaza között. Ezért pl. grupoidok esetében — ellentétben a fenti megállapodással — a művelet eltérő jelölését is megengedjük. Azt viszont csak kellő elővigyázatossággal mondhatjuk, hogy tekintsük az $(R_1; \spadesuit, \clubsuit)$ és az $(R_2; \oplus, \diamond)$ gyűrűket: ilyenkor ugyanis mindkettőnél előre meg kell mondani, hogy melyik műveleti jel jelöli az összadást és melyik a szorzást, azaz hogy melyik disztributív a másokra.

(Az is elegendő lenne, hogy bijekció legyen az egyik algebra műveleti jeleinek halmaza és a másik algebra műveleti jeleinek halmaza között. Ezért pl. grupoidok esetében — ellentétben a fenti megállapodással — a művelet eltérő jelölését is megengedjük. Azt viszont csak kellő elővigyázatossággal mondhatjuk, hogy tekintsük az $(R_1; \spadesuit, \clubsuit)$ és az $(R_2; \oplus, \diamond)$ gyűrűket: ilyenkor ugyanis mindkettőnél előre meg kell mondani, hogy melyik műveleti jel jelöli az összadást és melyik a szorzást, azaz hogy melyik disztributív a másokra. Azaz tudnunk kell, hogy az $\oplus$, $\diamond$ műveleti jelek közül melyik felel meg a $\spadesuit$-nek és melyik felel meg a $\clubsuit$-nek.)

(Az is elegendő lenne, hogy bijekció legyen az egyik algebra műveleti jeleinek halmaza és a másik algebra műveleti jeleinek halmaza között. Ezért pl. grupoidok esetében — ellentétben a fenti megállapodással — a művelet eltérő jelölését is megengedjük. Azt viszont csak kellő elővigyázatossággal mondhatjuk, hogy tekintsük az $(R_1; \spadesuit, \clubsuit)$ és az $(R_2; \oplus, \diamond)$ gyűrűket: ilyenkor ugyanis mindkettőnél előre meg kell mondani, hogy melyik műveleti jel jelöli az összadást és melyik a szorzást, azaz hogy melyik disztributív a másokra. Azaz tudnunk kell, hogy az $\oplus$, $\diamond$ műveleti jelek közül melyik felel meg a $\spadesuit$-nek és melyik felel meg a $\clubsuit$-nek.) Ezen gondolatokat az alábbiakban pontosítjuk.

Legyen adva műveletjeleknek (k

Legyen adva műveletjeleknek (korábbi terminológiával: függvényjeleknek)

Legyen adva műveletjeleknek (korábbi terminológiával: függvényjeleknek) egy $\mathbf{F}$ halmaza, és ezzel együtt minden egyes $f \in \mathbf{F}$-re adott az f műveleti jel m_f változószáma.
Á

Legyen adva műveletjeleknek (korábbi terminológiával: függvényjeleknek) egy $\mathbf{F}$ halmaza, és ezzel együtt minden egyes $f \in \mathbf{F}$-re adott az f műveleti jel m_f változószáma. Álljon $\mathbf{P}$ az $=$ jelből, amely kétváltozós. Csak olyan algebrákat tekintsünk egyidejűleg, amelyek (**ugyanazon**) $(\{=\}; \mathbf{F})$ típusú L nyelv azon modelljei (

Legyen adva műveletjeleknek (korábbi terminológiával: függvényjeleknek) egy $\mathbf{F}$ halmaza, és ezzel együtt minden egyes $f \in \mathbf{F}$-re adott az f műveleti jel m_f változószáma. Álljon $\mathbf{P}$ az $=$ jelből, amely kétváltozós. Csak olyan algebrákat tekintsünk egyidejűleg, amelyek (**ugyanazon**) $(\{=\}; \mathbf{F})$ típusú L nyelv azon modelljei (természetesen azon a szokásos módon, hogy az $=$ jelnek az $\{(x, x) : x \in \text{alaphalmaz}\}$ relácónak megfelelő predikátum felel meg.

Legyen adva műveletjeleknek (korábbi terminológiával: függvényjeleknek) egy $\mathbf{F}$ halmaza, és ezzel együtt minden egyes $f \in \mathbf{F}$-re adott az f műveleti jel m_f változószáma. Álljon $\mathbf{P}$ az $=$ jelből, amely kétváltozós. Csak olyan algebrákat tekintsünk egyidejűleg, amelyek (**ugyanazon**) $(\{=\}; \mathbf{F})$ típusú L nyelv azon modelljei (természetesen azon a szokásos módon, hogy az $=$ jelnek az $\{(x,x) : x \in$ alaphalmaz$\}$ relácónak megfelelő predikátum felel meg.

Azaz ha egyebet nem mondunk, akkor (más szóhasználattal) **azonos típusú**, azaz **azonos műveleti jelkészletű** algebrákat tekintünk egyszerre.

Legyen adva műveletjeleknek (korábbi terminológiával: függvényjeleknek) egy $\mathbf{F}$ halmaza, és ezzel együtt minden egyes $f \in \mathbf{F}$-re adott az f műveleti jel m_f változószáma. Álljon $\mathbf{P}$ az $=$ jelből, amely kétváltozós. Csak olyan algebrákat tekintsünk egyidejűleg, amelyek (**ugyanazon**) $(\{=\}; \mathbf{F})$ típusú L nyelv azon modelljei (természetesen azon a szokásos módon, hogy az $=$ jelnek az $\{(x, x) : x \in$ alaphalmaz$\}$ relácónak megfelelő predikátum felel meg.

Azaz ha egyebet nem mondunk, akkor (más szóhasználattal) **azonos típusú**, azaz **azonos műveleti jelkészletű** algebrákat tekintünk egyszerre.

Többnyire nem teszünk jelölésbeli különbséget a műveleti jel és az általa jelölt művelet között.

Definíció: Legyen $\mathbf{A} = (A; F)$ és $\mathbf{B} = (B; F)$ két azonos típusú algebra, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**,

Definíció: Legyen $\mathbf{A} = (A; F)$ és $\mathbf{B} = (B; F)$ két azonos típusú algebra, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletekkel**, azaz bármely $f \in F$-re és bármely $a_1, \ldots, a_{m_f} \in A$ elemekre

$$f(a_1, \ldots, a_{m_f})\varphi = f(a_1\varphi, \ldots, a_{m_f}\varphi).$$

Definíció: Legyen $\mathbf{A} = (A; F)$ és $\mathbf{B} = (B; F)$ két azonos típusú algebra, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletekkel**, azaz bármely $f \in F$-re és bármely $a_1, \ldots, a_{m_f} \in A$ elemekre

$$f(a_1, \ldots, a_{m_f})\varphi = f(a_1\varphi, \ldots, a_{m_f}\varphi).$$

Még precízebben:

$$f_A(a_1, \ldots, a_{m_f})\varphi = f_B(a_1\varphi, \ldots, a_{m_f}\varphi).$$

Definíció: Legyen $\mathbf{A} = (A; F)$ és $\mathbf{B} = (B; F)$ két azonos típusú algebra, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletekkel**, azaz bármely $f \in F$-re és bármely $a_1, \ldots, a_{m_f} \in A$ elemekre

$$f(a_1, \ldots, a_{m_f})\varphi = f(a_1\varphi, \ldots, a_{m_f}\varphi).$$

Még precízebben:

$$f_A(a_1, \ldots, a_{m_f})\varphi = f_B(a_1\varphi, \ldots, a_{m_f}\varphi).$$

Szavakban: mindegy, hogy előbb a műveletet majd a leképezést alkalmazzuk vagy fordítva, előbb a leképezést majd a műveletet, ugyanazt a végeredményt kell kapnunk.

Definíció: Legyen $\mathbf{A} = (A; F)$ és $\mathbf{B} = (B; F)$ két azonos típusú algebra, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletekkel**, azaz bármely $f \in F$-re és bármely $a_1, \ldots, a_{m_f} \in A$ elemekre

$$f(a_1, \ldots, a_{m_f})\varphi = f(a_1\varphi, \ldots, a_{m_f}\varphi).$$

Még precízebben:

$$f_A(a_1, \ldots, a_{m_f})\varphi = f_B(a_1\varphi, \ldots, a_{m_f}\varphi).$$

Szavakban: mindegy, hogy előbb a műveletet majd a leképezést alkalmazzuk vagy fordítva, előbb a leképezést majd a műveletet, ugyanazt a végeredményt kell kapnunk.

Definíció: Legyen $\mathbf{A} = (A; F)$ és $\mathbf{B} = (B; F)$ két azonos típusú algebra, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletekkel**, azaz bármely $f \in F$-re és bármely $a_1, \ldots, a_{m_f} \in A$ elemekre

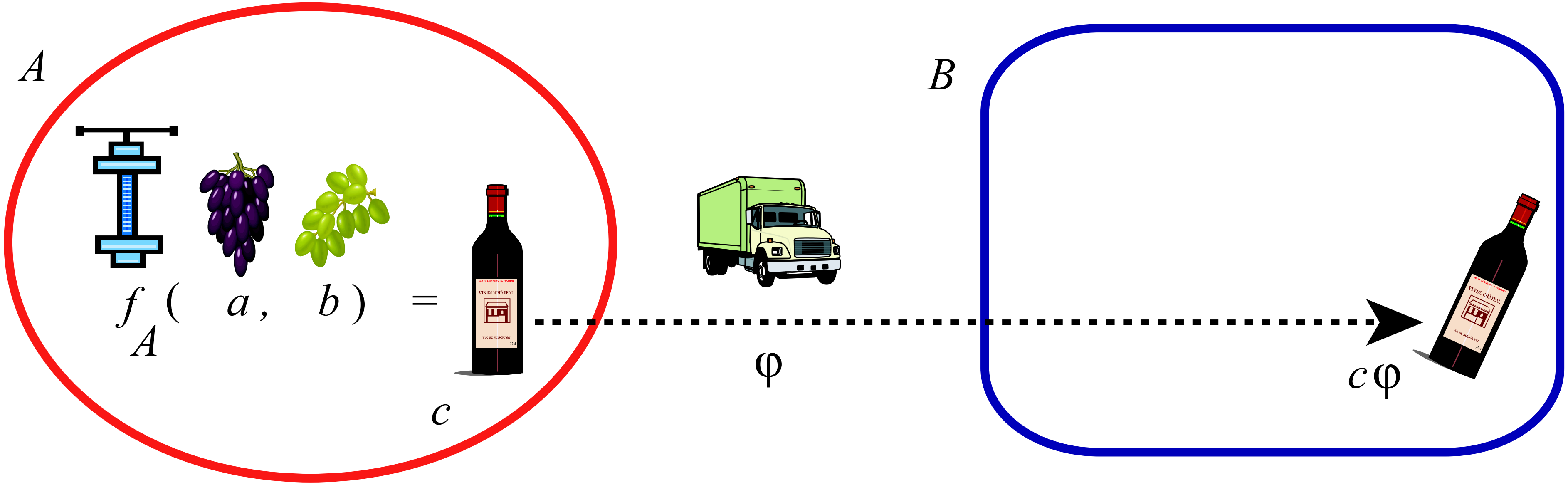
$$f(a_1, \ldots, a_{m_f})\varphi = f(a_1\varphi, \ldots, a_{m_f}\varphi).$$

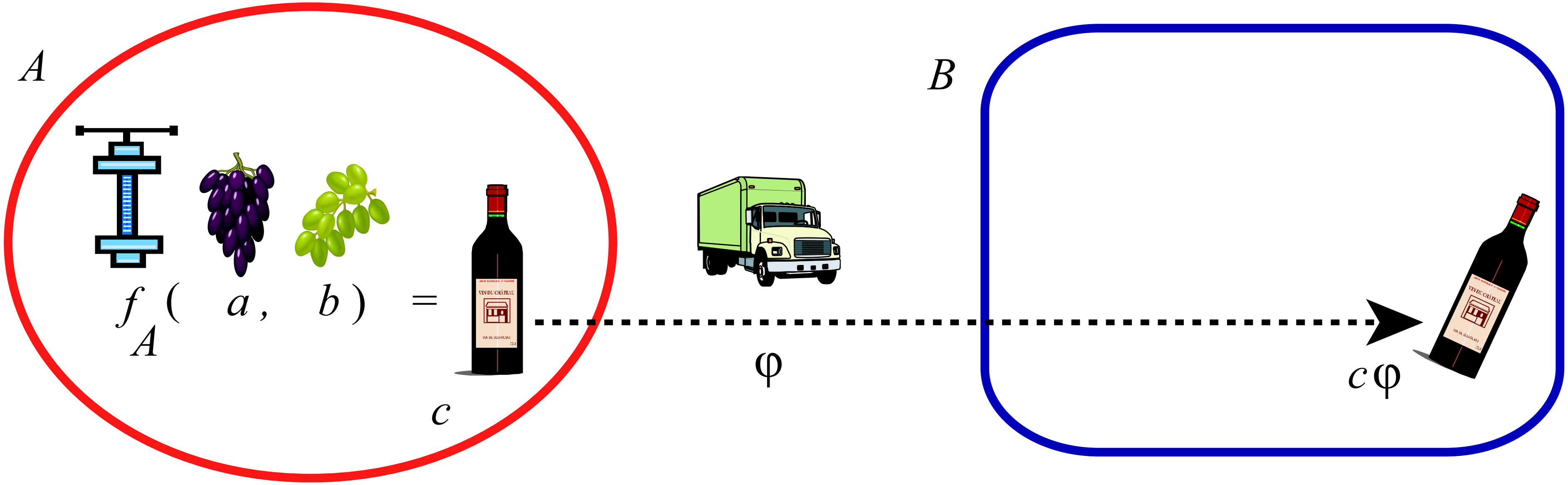
Még precízebben:

$$f_A(a_1, \ldots, a_{m_f})\varphi = f_B(a_1\varphi, \ldots, a_{m_f}\varphi).$$

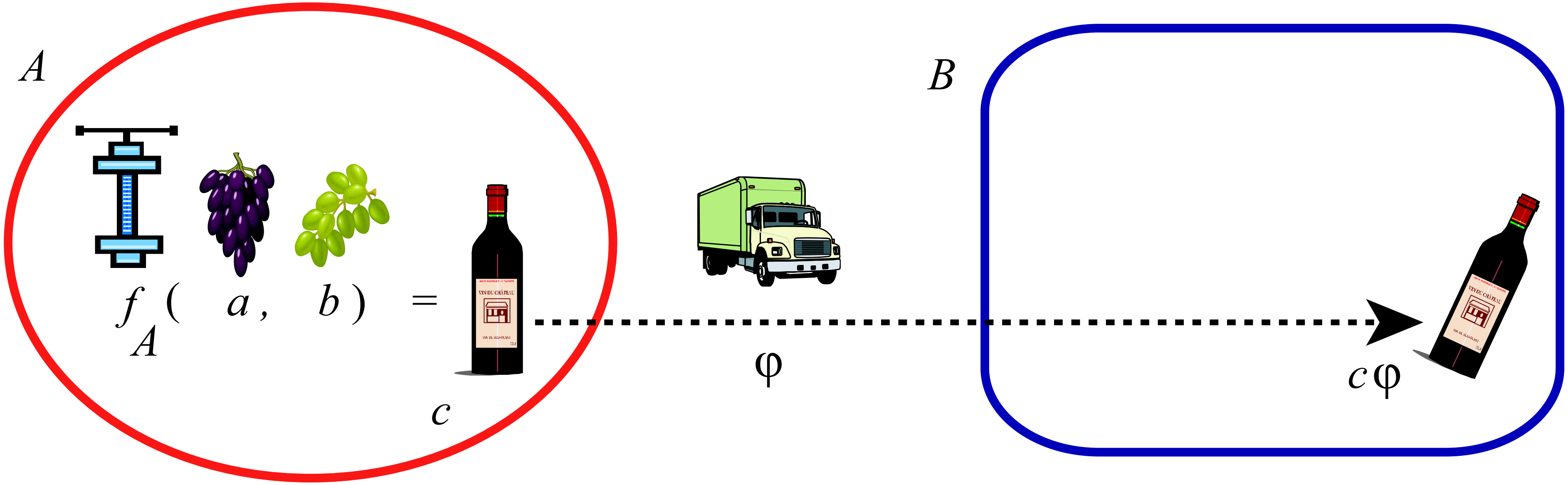
Szavakban: mindegy, hogy előbb a műveletet majd a leképezést alkalmazzuk vagy fordítva, előbb a leképezést majd a műveletet, ugyanazt a végeredményt kell kapnunk.

Az izomorfizmus fogalma oly fontos a matematikában, hogy érdemes egy ábrával is szemléltetni:

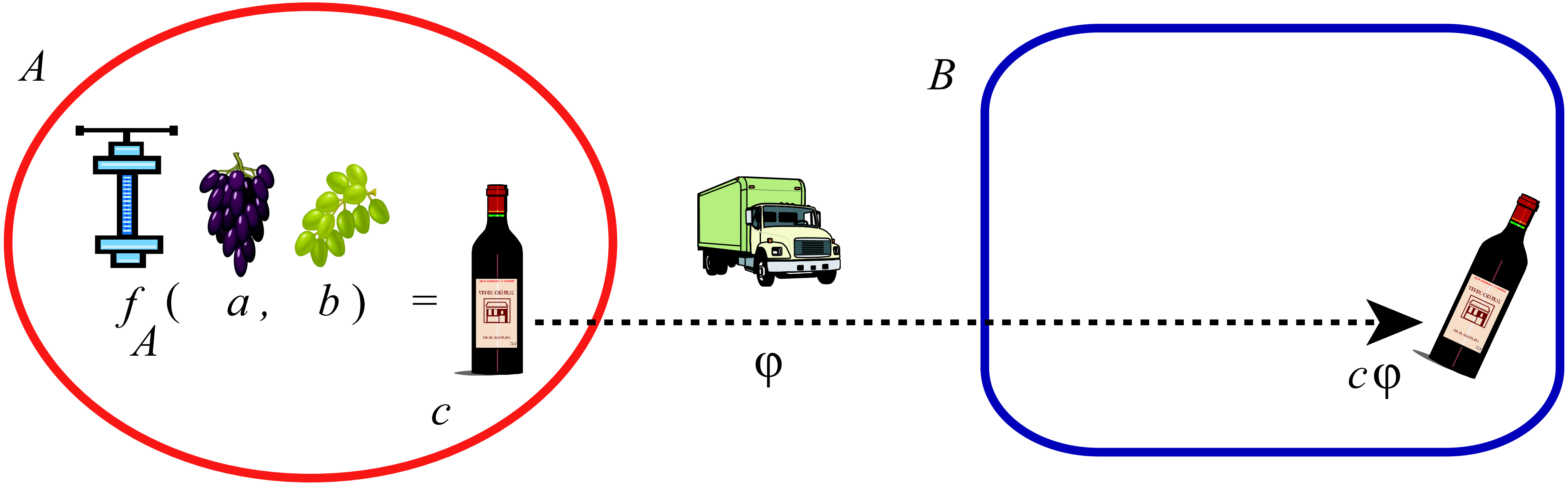

A
f
A
(a , b) =
c
φ
B
cφ



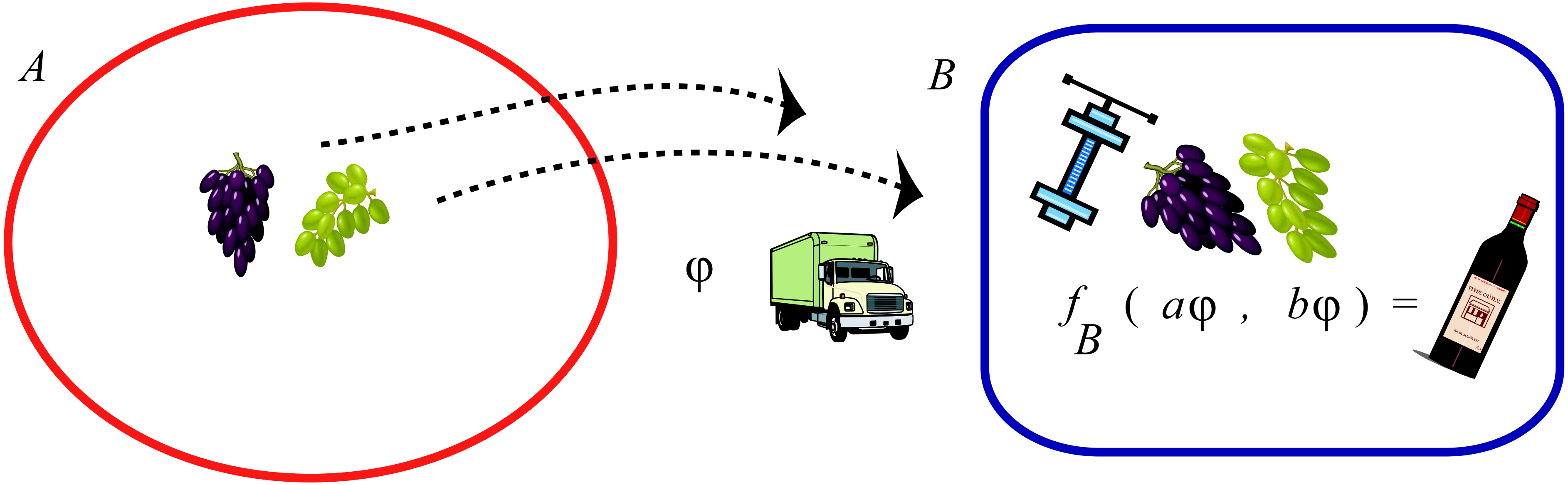
Tekintsünk (algebrák helyett) két borkombinátot, és



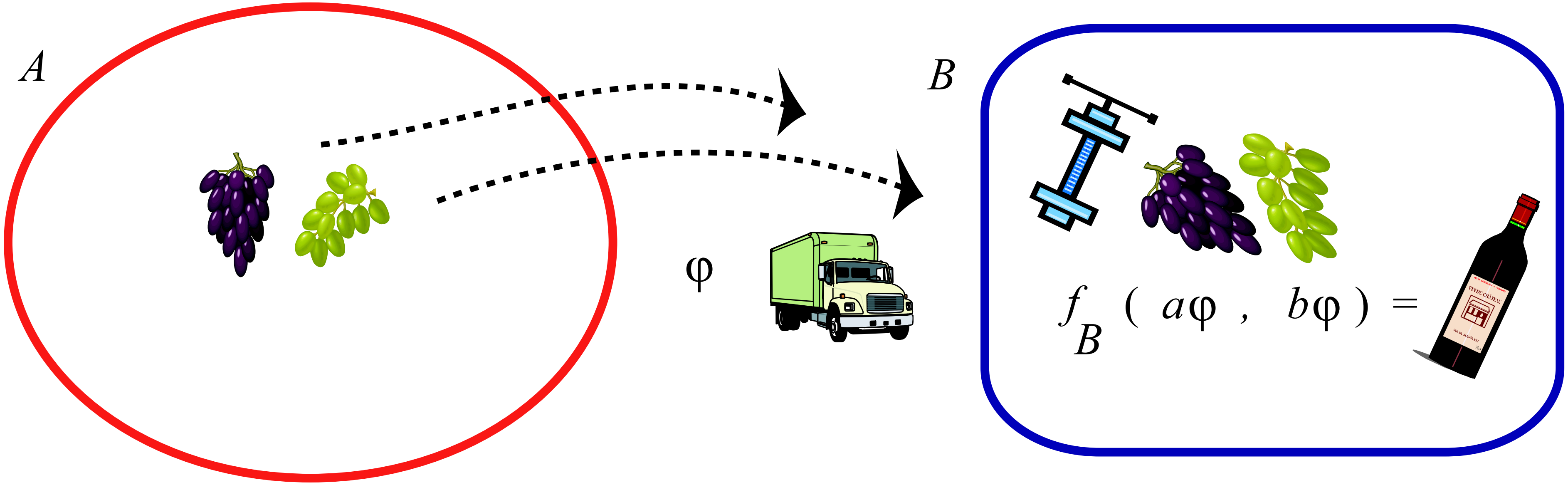
Tekintsünk (algebrák helyett) két borkombinátot, és tekintsük a borkészítés „műveletét” !



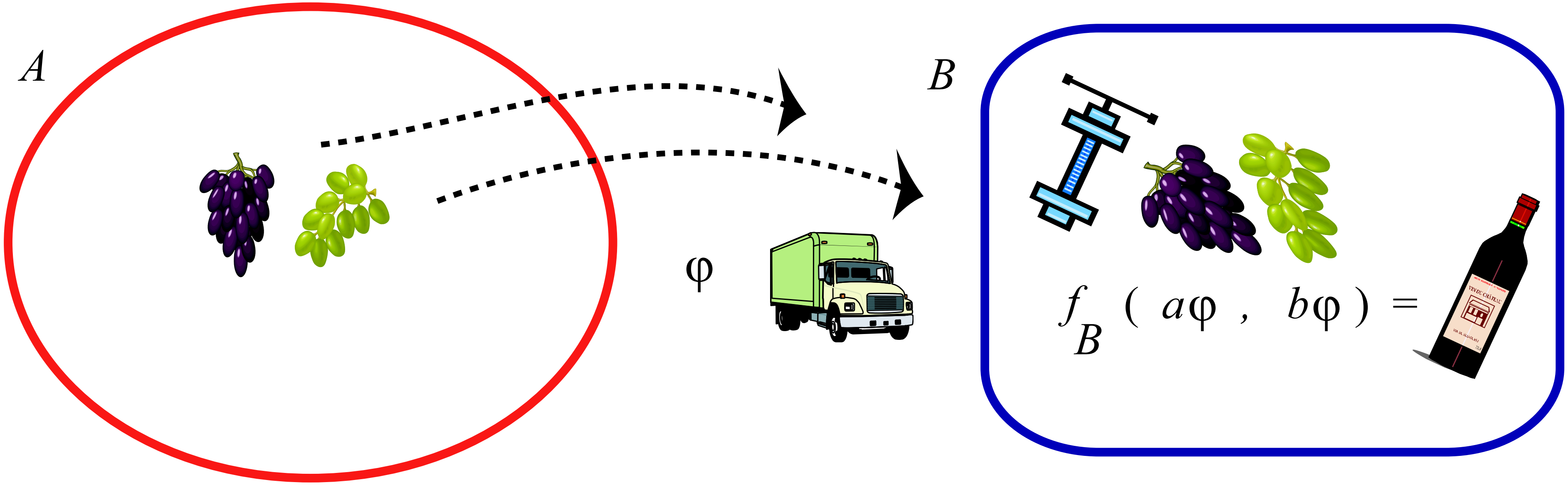
Tekintsünk (algebrák helyett) két borkombinátot, és tekintsük a borkészítés „műveletét”! A leképezést a „szállítás” szimbolizálja.



A
φ
B
$f_B(a\varphi, b\varphi) =$



Tehát **izomorfizmus** = bijektív + műveletekkel felcserélhető.



Tehát **izomorfizmus** = bijektív + műveletekkel felcserélhető.

Fontossága miatt a definíciót egy egyszerűbb esetben, a grupoidok esetén is megismételjük:

A vizsga feltétele: 20 pont a gyakorlaton!

Definíció: Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ egy-egy grupoid, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**,

Definíció: Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ egy-egy grupoid, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletettel**, azaz bármely bármely $a, b \in A$ elemekre

$$(ab)\varphi = (a\varphi)(b\varphi).$$

Definíció: Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ egy-egy grupoid, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletettel**, azaz bármely bármely $a, b \in A$ elemekre

$$(ab)\varphi = (a\varphi)(b\varphi).$$

Szavakban: mindegy, hogy előbb szorzunk majd leképezezünk, vagy fordítva, előbb leképezünk majd szorzunk, ugyanazt a végeredményt kell kapnunk.

Definíció: Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ egy-egy grupoid, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **izomorfizmus**, ha φ **bijektív** és **felcserélhető a műveletettel**, azaz bármely bármely $a, b \in A$ elemekre

$$(ab)\varphi = (a\varphi)(b\varphi).$$

Szavakban: mindegy, hogy előbb szorzunk majd leképezezünk, vagy fordítva, előbb leképezünk majd szorzunk, ugyanazt a végeredményt kell kapnunk. Azaz a szorzás és a leképezés sorrendje felcserélhető.

Definíció: Ha két algebra között létezik izomorfizmus, akkor a két algebrát **izomorfnak** mondjuk.

Definíció: Ha két algebra között létezik izomorfizmus, akkor a két algebrát **izomorfnak** mondjuk. Az ún. **Steinitz-elv** szerint izomorf algebrák között (többnyire) nem teszünk különbséget.

Definíció: Ha két algebra között létezik izomorfizmus, akkor a két algebrát **izomorfnak** mondjuk. Az ún. **Steinitz-elv** szerint izomorf algebrák között (többnyire) nem teszünk különbséget.

A Steinitz-elvet az alábbi tétel (is) indokolja.

57. Tétel. *(„***ha izomorf, akkor ekvivalens***" tétel)* *Legyen* $\mathbf{A} = (A; F)$ *és* $\mathbf{B} = (B; F)$ *két izomorf algebra, és legyen* T *egy zárt formula a közös elsőrendű nyelvükön. Ekkor* $\models_{\mathbf{A}} T$ *akkor és csak akkor, ha* $\models_{\mathbf{B}} T$

57. Tétel. *(„***ha izomorf, akkor ekvivalens***" tétel)* *Legyen* $\mathbf{A} = (A; F)$ *és* $\mathbf{B} = (B; F)$ *két izomorf algebra, és legyen* T *egy zárt formula a közös elsőrendű nyelvükön. Ekkor* $\models_{\mathbf{A}} T$ *akkor és csak akkor, ha* $\models_{\mathbf{B}} T$ *(azaz pontosan ugyanazok a zárt formulák teljesülnek a két algebrában).*

57. Tétel. *(„***ha izomorf, akkor ekvivalens***" tétel)* *Legyen* $\mathbf{A} = (A; F)$ *és* $\mathbf{B} = (B; F)$ *két izomorf algebra, és legyen* T *egy zárt formula a közös elsőrendű nyelvükön. Ekkor* $\models_{\mathbf{A}} T$ *akkor és csak akkor, ha* $\models_{\mathbf{B}} T$ *(azaz pontosan ugyanazok a zárt formulák teljesülnek a két algebrában).*

A

57. Tétel. *(„***ha izomorf, akkor ekvivalens***" tétel)* *Legyen* $\mathbf{A} = (A; F)$ *és* $\mathbf{B} = (B; F)$ *két izomorf algebra, és legyen* T *egy zárt formula a közös elsőrendű nyelvükön. Ekkor* $\models_{\mathbf{A}} T$ *akkor és csak akkor, ha* $\models_{\mathbf{B}} T$ *(azaz pontosan ugyanazok a zárt formulák teljesülnek a két algebrában).*

A bizonyítást — amely a formula hossza szerinti teljes indukcióval történik — nem részletezzük, mindössze egy speciális formula esetén illusztráljuk.

Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ két izomorf grupoid, és tekintsük az alábbi formulát:

$$T := (\forall x)(\forall y)(\forall z)(x(yz) = (xy)z).$$

T

Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ két izomorf grupoid, és tekintsük az alábbi formulát:

$$T := (\forall x)(\forall y)(\forall z)(x(yz) = (xy)z).$$

T nem más, mint az asszociativitást kifejező formula. A tétel ebben a speciális esetben tehát azt állítja, hogy $\mathbf{A}$ pontosan akkor asszociatív grupoid (azaz félcsoport), ha $\mathbf{B}$ félcsoport.

Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ két izomorf grupoid, és tekintsük az alábbi formulát:

$$T := (\forall x)(\forall y)(\forall z)(x(yz) = (xy)z).$$

T nem más, mint az asszociativitást kifejező formula. A tétel ebben a speciális esetben tehát azt állítja, hogy $\mathbf{A}$ pontosan akkor asszociatív grupoid (azaz félcsoport), ha $\mathbf{B}$ félcsoport. Ezt mutatjuk meg az alábbiakban.

Legyen $\varphi : A \longrightarrow B$ egy izomorfizmus.

Legyen $\varphi : A \longrightarrow B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport.

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges.

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$.

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z =$$

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) =$$

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi =$$

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi = ((ab)c)\varphi =$$

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi = ((ab)c)\varphi =$$
$$(a(bc))\varphi =$$

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi = ((ab)c)\varphi =$$
$$(a(bc))\varphi = a\varphi \cdot (bc)\varphi =$$

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi = ((ab)c)\varphi =$$
$$(a(bc))\varphi = a\varphi \cdot (bc)\varphi = (a\varphi)((b\varphi)(c\varphi)) =$$

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi = ((ab)c)\varphi =$$
$$(a(bc))\varphi = a\varphi \cdot (bc)\varphi = (a\varphi)((b\varphi)(c\varphi)) = x(yz).$$

Tehát ha $\mathbf{A}$ félcsoport, akkor a vele izomorf $\mathbf{B}$ grupoid is félcsoport.

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi = ((ab)c)\varphi =$$
$$(a(bc))\varphi = a\varphi \cdot (bc)\varphi = (a\varphi)((b\varphi)(c\varphi)) = x(yz).$$

Tehát ha $\mathbf{A}$ félcsoport, akkor a vele izomorf $\mathbf{B}$ grupoid is félcsoport.

A fordított irány igazolása nem igényel újabb számolást, csak azt kell átgondolni, hogy tetszőleges izomorfizmus inverze (amely létezik, hiszen az izomorfizmus bijektív leképezés) szintén izomorfizmus

Legyen $\varphi : A \to B$ egy izomorfizmus. Tegyük fel, hogy $\mathbf{A}$ félcsoport. Legyen $x, y, z \in B$ tetszőleges. Mivel φ bijektív, ezen elemeknek van őse, azaz van olyan $a, b, c \in A$, hogy $a\varphi = x$, $b\varphi = y$ és $c\varphi = z$. Ekkor

$$(xy)z = ((a\varphi)(b\varphi))(c\varphi) = (ab)\varphi \cdot c\varphi = ((ab)c)\varphi =$$
$$(a(bc))\varphi = a\varphi \cdot (bc)\varphi = (a\varphi)((b\varphi)(c\varphi)) = x(yz).$$

Tehát ha $\mathbf{A}$ félcsoport, akkor a vele izomorf $\mathbf{B}$ grupoid is félcsoport.

A fordított irány igazolása nem igényel újabb számolást, csak azt kell átgondolni, hogy tetszőleges izomorfizmus inverze (amely létezik, hiszen az izomorfizmus bijektív leképezés) szintén izomorfizmus — hiszen ekkor $\mathbf{A}$ és $\mathbf{B}$ szerepe a fenti megfontolásban szimmetrikus.

Jelölje $\psi : B \longrightarrow A$ a $\varphi : A \longrightarrow B$ izomorfizmus inverzét.

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív.

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \stackrel{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni,

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi =^{?} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi =^{?} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi =$$

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \stackrel{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi = (xy)(\psi\varphi) =$$

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \overset{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi = (xy)(\psi\varphi) = (xy)\mathrm{id}_B =$$

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \stackrel{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi = (xy)(\psi\varphi) = (xy)\mathrm{id}_B = xy,$$

$$((x\psi)(y\psi))\varphi$$

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \stackrel{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi = (xy)(\psi\varphi) = (xy)\mathrm{id}_B = xy,$$
$$((x\psi)(y\psi))\varphi = ((x\psi)\varphi)((y\psi)\varphi) =$$

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \stackrel{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi = (xy)(\psi\varphi) = (xy)\mathrm{id}_B = xy,$$
$$((x\psi)(y\psi))\varphi = ((x\psi)\varphi)((y\psi)\varphi) = (x(\psi\varphi))(y(\psi\varphi)) =$$

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \stackrel{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi = (xy)(\psi\varphi) = (xy)\mathrm{id}_B = xy,$$
$$((x\psi)(y\psi))\varphi = ((x\psi)\varphi)((y\psi)\varphi) = (x(\psi\varphi))(y(\psi\varphi)) =$$
$$(x\,\mathrm{id}_B)(y\,\mathrm{id}_B) =$$

Jelölje $\psi : B \to A$ a $\varphi : A \to B$ izomorfizmus inverzét. Ekkor — mint bijektív leképezés inverze — ψ is bijektív. Legyen $x, y \in B$ tetszőleges. Mivel φ többek között injektív, a kérdéses

$$(xy)\psi \stackrel{?}{=} (x\psi)(y\psi)$$

egyenlőség igazolásául elég belátni, hogy a két oldal φ melletti képe azonos. Valóban:

$$((xy)\psi)\varphi = (xy)(\psi\varphi) = (xy)\mathrm{id}_B = xy,$$
$$((x\psi)(y\psi))\varphi = ((x\psi)\varphi)((y\psi)\varphi) = (x(\psi\varphi))(y(\psi\varphi)) =$$
$$(x\,\mathrm{id}_B)(y\,\mathrm{id}_B) = xy.$$

Q.e.d.

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni,

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni, hogy megadunk egy izomorfizmust.

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni, hogy megadunk egy izomorfizmust. Azt viszont, hogy **nem izomorfak**, így aligha lehet belátni, túl sok bijekcióról kellene kimutatni, hogy nem izomorfizmusok

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni, hogy megadunk egy izomorfizmust. Azt viszont, hogy **nem izomorfak**, így aligha lehet belátni, túl sok bijekcióról kellene kimutatni, hogy nem izomorfizmusok — két n-elemű halmaz között $n!$ darab bijekció van.

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni, hogy megadunk egy izomorfizmust. Azt viszont, hogy **nem izomorfak**, így aligha lehet belátni, túl sok bijekcióról kellene kimutatni, hogy nem izomorfizmusok — két n-elemű halmaz között $n!$ darab bijekció van. Többnyire az előbbi tétel alapján tudjuk megmutatni, hogy két algebra **nem** izomorf.

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni, hogy megadunk egy izomorfizmust. Azt viszont, hogy **nem izomorfak**, így aligha lehet belátni, túl sok bijekcióról kellene kimutatni, hogy nem izomorfizmusok — két n-elemű halmaz között $n!$ darab bijekció van. Többnyire az előbbi tétel alapján tudjuk megmutatni, hogy két algebra **nem** izomorf.

Példa: Izomorf-e az alábbi két grupoid (valójában két csoportról van szó): $(\mathbf{R};+)$ és $(\mathbf{R}^+;\cdot)$?

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni, hogy megadunk egy izomorfizmust. Azt viszont, hogy **nem izomorfak**, így aligha lehet belátni, túl sok bijekcióról kellene kimutatni, hogy nem izomorfizmusok — két n-elemű halmaz között $n!$ darab bijekció van. Többnyire az előbbi tétel alapján tudjuk megmutatni, hogy két algebra **nem** izomorf.

Példa: Izomorf-e az alábbi két grupoid (valójában két csoportról van szó): $(\mathbf{R}; +)$ és $(\mathbf{R}^+; \cdot)$? (Itt $\mathbf{R}^+$ a pozitív valós számok halmaza.)

Megoldás: Az $\mathbf{R} \to \mathbf{R}^+$, $x \to e^x$ leképezés izomorfizmus, hiszen

Megjegyzés: azt, hogy két algebra izomorf, többnyire úgy lehet belátni, hogy megadunk egy izomorfizmust. Azt viszont, hogy **nem izomorfak**, így aligha lehet belátni, túl sok bijekcióról kellene kimutatni, hogy nem izomorfizmusok — két n-elemű halmaz között $n!$ darab bijekció van. Többnyire az előbbi tétel alapján tudjuk megmutatni, hogy két algebra **nem** izomorf.

Példa: Izomorf-e az alábbi két grupoid (valójában két csoportról van szó): $(\mathbf{R}; +)$ és $(\mathbf{R}^+; \cdot)$? (Itt $\mathbf{R}^+$ a pozitív valós számok halmaza.)

Megoldás: Az $\mathbf{R} \to \mathbf{R}^+$, $x \to e^x$ leképezés izomorfizmus, hiszen bijektív és $e^{x+y} = e^x \cdot e^y$.

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

Példa: Izomorf-e az alábbi két grupoid : $(\mathbf{Q}; +)$ és $(\mathbf{Q}^+; \cdot)$?

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

Példa: Izomorf-e az alábbi két grupoid : $(\mathbf{Q}; +)$ és $(\mathbf{Q}^+; \cdot)$?

(Amikor $\mathbf{Q}$ helyett $\mathbf{R}$ volt, akkor a válasz igenlő volt!)

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

Példa: Izomorf-e az alábbi két grupoid : $(\mathbf{Q}; +)$ és $(\mathbf{Q}^+; \cdot)$?

(Amikor $\mathbf{Q}$ helyett $\mathbf{R}$ volt, akkor a válasz igenlő volt!) ?

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

Példa: Izomorf-e az alábbi két grupoid : $(\mathbf{Q}; +)$ és $(\mathbf{Q}^+; \cdot)$?

(Amikor $\mathbf{Q}$ helyett $\mathbf{R}$ volt, akkor a válasz igenlő volt!) ?

Megoldás: jelölje $*$ a műveletet! Ekkor az

$$F := (\forall x)(\exists y)(x = y * y)$$

formula

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

Példa: Izomorf-e az alábbi két grupoid : $(\mathbf{Q};+)$ és $(\mathbf{Q}^+;\cdot)$?

(Amikor $\mathbf{Q}$ helyett $\mathbf{R}$ volt, akkor a válasz igenlő volt!) ?

Megoldás: jelölje $*$ a műveletet! Ekkor az

$$F := (\forall x)(\exists y)(x = y * y)$$

formula teljesül $(\mathbf{Q};+)$-ban

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

Példa: Izomorf-e az alábbi két grupoid : $(\mathbf{Q};+)$ és $(\mathbf{Q}^{+};\cdot)$?

(Amikor $\mathbf{Q}$ helyett $\mathbf{R}$ volt, akkor a válasz igenlő volt!) ?

Megoldás: jelölje $*$ a műveletet! Ekkor az

$$F := (\forall x)(\exists y)(x = y * y)$$

formula teljesül $(\mathbf{Q};+)$-ban (hiszen x fele szintén racionális),

(Az előbbi példában a két algebrában a műveletet máshogy jelöltük, de ez nem okozhat zavart, hiszen csak egy-egy művelet volt.)

Példa: Izomorf-e az alábbi két grupoid : $(\mathbf{Q};+)$ és $(\mathbf{Q}^+;\cdot)$?

(Amikor $\mathbf{Q}$ helyett $\mathbf{R}$ volt, akkor a válasz igenlő volt!) ?

Megoldás: jelölje $*$ a műveletet! Ekkor az

$$F := (\forall x)(\exists y)(x = y * y)$$

formula teljesül $(\mathbf{Q};+)$-ban (hiszen x fele szintén racionális), de nem teljesül $(\mathbf{Q}^+;\cdot)$-ban, hiszen pl. $x = 2$ esetén $\pm\sqrt{2}$ nem racionális. Tehát *nem izomorfak*.

Ha az izomorfizmus definíciójában φ-ről nem tesszük fel, hogy bijektív, akkor a homomorfizmus fogalmát kapjuk. Ennél bővebben (az egyszerűség kedvéért) csak grupoidokra fogalmazzuk meg részletesen:

Ha az izomorfizmus definíciójában φ-ről nem tesszük fel, hogy bijektív, akkor a homomorfizmus fogalmát kapjuk. Ennél bővebben (az egyszerűség kedvéért) csak grupoidokra fogalmazzuk meg részletesen:

Definíció: Legyen $\mathbf{A} = (A; \cdot)$ és $\mathbf{B} = (B; \cdot)$ egy-egy grupoid, $\varphi : A \to B$ pedig egy leképezés. Akkor mondjuk, hogy φ egy $\mathbf{A} \to \mathbf{B}$ **homomorfizmus**, ha **felcserélhető a művelettel**, azaz bármely bármely $a, b \in A$ elemekre

$$(ab)\varphi = (a\varphi)(b\varphi).$$

Az injektív homomorfizmus neve **beágyazás**.

Példák

Példák Minden izomorfizmus homomorfizmus (sőt beágyazás).

Az alábbi leképezés is homomorfizmus:

Példák Minden izomorfizmus homomorfizmus (sőt beágyazás).

Az alábbi leképezés is homomorfizmus:

$$\varphi : (\mathbf{Z}; \cdot) \to (\{-1, 0, 1\}; \cdot), \quad x \mapsto \begin{cases} -1 & \text{ha } x < 0, \\ 0 & \text{ha } x{=}0, \\ 1 & \text{ha } x > 0. \end{cases}$$

Példák Minden izomorfizmus homomorfizmus (sőt beágyazás).

Az alábbi leképezés is homomorfizmus:

$$\varphi : (\mathbf{Z}; \cdot) \to (\{-1, 0, 1\}; \cdot), \quad x \mapsto \begin{cases} -1 & \text{ha x} < 0, \\ 0 & \text{ha x=0}, \\ 1 & \text{ha x} > 0. \end{cases}$$

Az identikus $\varphi : \mathbf{Z} \rightarrow \mathbf{R}$, $x \mapsto x$ leképezés az egész számok gyűrűjének beágyazása a valós számok testébe. Az alábbi leképezés (a négyzetre emelés) is homomorfizmus:

Az identikus $\varphi : \mathbf{Z} \to \mathbf{R}$, $x \mapsto x$ leképezés az egész számok gyűrűjének beágyazása a valós számok testébe. Az alábbi leképezés (a négyzetre emelés) is homomorfizmus:

$$\psi : (\mathbf{R} \setminus \{0\}; \cdot) \to (\mathbf{R} \setminus \{0\}; \cdot), \quad x \mapsto x^2;$$

Az identikus $\varphi : \mathbf{Z} \to \mathbf{R}$, $x \mapsto x$ leképezés az egész számok gyűrűjének beágyazása a valós számok testébe. Az alábbi leképezés (a négyzetre emelés) is homomorfizmus:

$$\psi : (\mathbf{R} \setminus \{0\}; \cdot) \to (\mathbf{R} \setminus \{0\}; \cdot), \quad x \mapsto x^2;$$

Jelölje $(\mathbf{R}_{n\times n},\cdot)$ az $n \times n$ -es valós mátrixok multiplikatív félcsoportját. (Művelet a mátrixszorzás.) Ekkor a

$$\mathrm{det} : \mathbf{R}_{n\times n} \to \mathbf{R}, \qquad A \mapsto \mathrm{det}(A)$$

leképezés a tekintett félcsoport homomorfizmusa a valós számok multiplikatív félcsoportjába. Ezen kijelentésünk ekvivalens a determinánsok szorzástételével —

Jelölje $(\mathbf{R}_{n\times n},\cdot)$ az $n \times n$ -es valós mátrixok multiplikatív félcsoportját. (Művelet a mátrixszorzás.) Ekkor a

$$\det : \mathbf{R}_{n\times n} \to \mathbf{R}, \qquad A \mapsto \det(A)$$

leképezés a tekintett félcsoport homomorfizmusa a valós számok multiplikatív félcsoportjába. Ezen kijelentésünk ekvivalens a determinánsok szorzástételével — ez is arra utal, hogy a homomorfizmus fontos és gyakori fogalom.

Jelölje $(\mathbf{R}_{n\times n},\cdot)$ az $n \times n$ -es valós mátrixok multiplikatív félcsoportját. (Művelet a mátrixszorzás.) Ekkor a

$$\det : \mathbf{R}_{n\times n} \to \mathbf{R}, \qquad A \mapsto \det(A)$$

leképezés a tekintett félcsoport homomorfizmusa a valós számok multiplikatív félcsoportjába. Ezen kijelentésünk ekvivalens a determinánsok szorzástételével — ez is arra utal, hogy a homomorfizmus fontos és gyakori fogalom.

A Kalkulus tantárgy sok-sok tétele tulajdonképpen semmi mást nem állít csak annyit, hogy bizonyos leképezések Abel-csoportok közötti hommorfizmusok!

Jelölje $(\mathbf{R}_{n\times n},\cdot)$ az $n \times n$ -es valós mátrixok multiplikatív félcsoportját. (Művelet a mátrixszorzás.) Ekkor a

$$\det : \mathbf{R}_{n\times n} \to \mathbf{R}, \qquad A \mapsto \det(A)$$

leképezés a tekintett félcsoport homomorfizmusa a valós számok multiplikatív félcsoportjába. Ezen kijelentésünk ekvivalens a determinánsok szorzástételével — ez is arra utal, hogy a homomorfizmus fontos és gyakori fogalom.

A Kalkulus tantárgy sok-sok tétele tulajdonképpen semmi mást nem állít csak annyit, hogy bizonyos leképezések Abel-csoportok közötti hommorfizmusok! Néhány példa azok számára, akik már tanultak Kalkulust:

Legyen (a, b) egy rögzített (véges vagy végtelen) intervallum. Jelölje $F(a, b)$ az (a, b)-n értelmezett valós függvények halmazát, $D(a, b)$ az (a, b) intervallumon értelmezett diffferenciálható függvények halmazát, $I(a, b)$ pedig az (a, b)-n értelmezett integrálható függvények halmazát. Az összeadás jelentése a szokásos. Az alábbi leképezések Abel-csoportok közötti homomorfizmusok:

$$\lim : (\{\text{konvergens sorozatok}\}; +) \to (\mathbf{R}; +), \quad (a_n)_{n\in\mathbf{N}} \mapsto \lim a_n,$$

Legyen (a, b) egy rögzített (véges vagy végtelen) intervallum. Jelölje $F(a, b)$ az (a, b)-n értelmezett valós függvények halmazát, $D(a, b)$ az (a, b) intervallumon értelmezett diffferenciálható függvények halmazát, $I(a, b)$ pedig az (a, b)-n értelmezett integrálható függvények halmazát. Az összeadás jelentése a szokásos. Az alábbi leképezések Abel-csoportok közötti homomorfizmusok:

$$\lim : (\{\text{konvergens sorozatok}\}; +) \to (\mathbf{R}; +), \quad (a_n)_{n \in \mathbf{N}} \mapsto \lim a_n,$$
$$' : (D(a, b); +) \to (F(a, b); +), \quad f \mapsto f',$$

Legyen (a, b) egy rögzített (véges vagy végtelen) intervallum. Jelölje $F(a, b)$ az (a, b)-n értelmezett valós függvények halmazát, $D(a, b)$ az (a, b) intervallumon értelmezett diffferenciálható függvények halmazát, $I(a, b)$ pedig az (a, b)-n értelmezett integrálható függvények halmazát. Az összeadás jelentése a szokásos. Az alábbi leképezések Abel-csoportok közötti homomorfizmusok:

$$\lim : (\{\text{konvergens sorozatok}\}; +) \to (\mathbf{R}; +), \quad (a_n)_{n\in\mathbf{N}} \mapsto \lim a_n,$$

$$' : (D(a, b); +) \to (F(a, b); +), \quad f \mapsto f',$$

$$\int_a^b : (I(a, b); +) \to (\mathbf{R}; +), \quad f \mapsto \int_a^b f(x)dx$$

Legyen (a, b) egy rögzített (véges vagy végtelen) intervallum. Jelölje $F(a, b)$ az (a, b)-n értelmezett valós függvények halmazát, $D(a, b)$ az (a, b) intervallumon értelmezett diffferenciálható függvények halmazát, $I(a, b)$ pedig az (a, b)-n értelmezett integrálható függvények halmazát. Az összeadás jelentése a szokásos. Az alábbi leképezések Abel-csoportok közötti homomorfizmusok:

$$\lim : (\{\text{konvergens sorozatok}\}; +) \to (\mathbf{R}; +), \quad (a_n)_{n\in\mathbf{N}} \mapsto \lim a_n,$$
$$' : (D(a, b); +) \to (F(a, b); +), \quad f \mapsto f',$$
$$\int_a^b : (I(a, b); +) \to (\mathbf{R}; +), \quad f \mapsto \int_a^b f(x)dx$$

Az izomorfizmusokkal szemben a homomorfizmusok jóval kevesebb tulajdonságot őriznek meg (és többnyire azt is csak akkor, ha feltesszük a szürjektivitást). Íme egy példa:

9. Állítás. *Legyen* φ *egy* **szürjektív homomorfizmus** *egy* $\mathbf{A} = (A, \cdot)$ *grupoidból egy* $\mathbf{B} = (B, \cdot)$ *grupoidba. Ha* $\mathbf{A}$ *félcsoport, akkor* $\mathbf{B}$ *is az.*

9. Állítás. *Legyen* φ *egy* **szürjektív homomorfizmus** *egy* $\mathbf{A} = (A, \cdot)$ *grupoidból egy* $\mathbf{B} = (B, \cdot)$ *grupoidba. Ha* $\mathbf{A}$ *félcsoport, akkor* $\mathbf{B}$ *is az.*

Bizonyítás: amikor azt igazoltuk, hogy az izomorfizmusok megőrzik az asszociativitást, akkor az injektivitást ki sem használtuk (csak a szürjektivitást) — az ottani gondolatmenet tehát most is érvényes.

Most a célunk a ciklikus csoportok megadása. Legyen

$$\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

(ahol $n \in \mathbf{N}$) és tekintsük az

$$(\mathbf{Z}_n; +)$$

csoportot, ahol az összeadás **modulo n** történik.

Most a célunk a ciklikus csoportok megadása. Legyen

$$\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

(ahol $n \in \mathbf{N}$) és tekintsük az

$$(\mathbf{Z}_n; +)$$

csoportot, ahol az összeadás **modulo n** történik. Ezen csoport neve a **modulo n maradékosztályok additív csoportja**.

Most a célunk a ciklikus csoportok megadása. Legyen

$$\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

(ahol $n \in \mathbf{N}$) és tekintsük az

$$(\mathbf{Z}_n; +)$$

csoportot, ahol az összeadás **modulo n** történik. Ezen csoport neve a **modulo n maradékosztályok additív csoportja**.

A modulo n összadás azt jelenti, hogy

Most a célunk a ciklikus csoportok megadása. Legyen

$$\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

(ahol $n \in \mathbf{N}$) és tekintsük az

$$(\mathbf{Z}_n; +)$$

csoportot, ahol az összeadás **modulo n** történik. Ezen csoport neve a **modulo n maradékosztályok additív csoportja**.

A modulo n összadás azt jelenti, hogy amennyiben az összeg eléri vagy meghaladja az n-et, akkor levonunk belőle n-et, hogy $\mathbf{Z}_n$-be essen.

Most a célunk a ciklikus csoportok megadása. Legyen

$$\mathbf{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

(ahol $n \in \mathbf{N}$) és tekintsük az

$$(\mathbf{Z}_n; +)$$

csoportot, ahol az összeadás **modulo n** történik. Ezen csoport neve a **modulo n maradékosztályok additív csoportja**.

A modulo n összadás azt jelenti, hogy amennyiben az összeg eléri vagy meghaladja az n-et, akkor levonunk belőle n-et, hogy $\mathbf{Z}_n$-be essen.

Példák: A modulo 10 összeadás esetén az összeg az utolsó számjegy.

Példák: A modulo 10 összeadás esetén az összeg az utolsó számjegy.

Az órákat modulo 12 szoktuk összadni, azaz $(\mathbf{Z}_{12};+)$-ban számolunk:

Példák: A modulo 10 összeadás esetén az összeg az utolsó számjegy.

Az órákat modulo 12 szoktuk összadni, azaz $(\mathbf{Z}_{12};+)$-ban számolunk: ha most 9-et mutat az óra, akkor mit mutat majd 7 óra múlva? A válasz: $9+7=4\in\mathbf{Z}_{12}$.

Példák: A modulo 10 összeadás esetén az összeg az utolsó számjegy.

Az órákat modulo 12 szoktuk összadni, azaz $(\mathbf{Z}_{12};+)$-ban számolunk: ha most 9-et mutat az óra, akkor mit mutat majd 7 óra múlva? A válasz: $9+7=4 \in \mathbf{Z}_{12}$.

A fokokat gyakran a $(\mathbf{Z}_{360};+)$ csoportban adjuk össze. Ha pl. az Adobe Illustrator-ban egy ábrát előbb elforgatok 200 fokkal, majd 300 fokkal, akkor végeredményben mennyivel lesz elforgatva?

Példák: A modulo 10 összeadás esetén az összeg az utolsó számjegy.

Az órákat modulo 12 szoktuk összadni, azaz $(\mathbf{Z}_{12};+)$-ban számolunk: ha most 9-et mutat az óra, akkor mit mutat majd 7 óra múlva? A válasz: $9+7=4\in\mathbf{Z}_{12}$.

A fokokat gyakran a $(\mathbf{Z}_{360};+)$ csoportban adjuk össze. Ha pl. az Adobe Illustrator-ban egy ábrát előbb elforgatok 200 fokkal, majd 300 fokkal, akkor végeredményben mennyivel lesz elforgatva? Válasz: $200+300=140\in\mathbf{Z}_{360}$.

0 fok

200 fok

200+300=140 fok

0 fok   200 fok   200+300=140 fok

Célszerű a $(\mathbf{Z}_n;+)$ csoportot úgy elképzelni, mint egy olyan (hagyományos) óra számlapját, amelyen 12 helyett n beosztás van.

Világos, hogy $(\mathbf{Z}_n; +)$ ciklikus csoport,

Világos, hogy $(\mathbf{Z}_n; +)$ ciklikus csoport, hiszen az $\{1\}$ generálja:

$$1 \in [1],$$

Világos, hogy $(\mathbf{Z}_n; +)$ ciklikus csoport, hiszen az $\{1\}$ generálja:

$$1 \in [1], \quad 2 = 1 + 1 \in [1],$$

Világos, hogy $(\mathbf{Z}_n;+)$ ciklikus csoport, hiszen az $\{1\}$ generálja:

$$1 \in [1], \quad 2 = 1+1 \in [1], \quad 3 = 1+1+1 \in [1],$$

Világos, hogy $(\mathbf{Z}_n;+)$ ciklikus csoport, hiszen az $\{1\}$ generálja:

$$1 \in [1], \quad 2 = 1+1 \in [1], \quad 3 = 1+1+1 \in [1], \ldots$$

miatt $[1] = \mathbf{Z}_n$.

Világos, hogy $(\mathbf{Z}_n; +)$ ciklikus csoport, hiszen az $\{1\}$ generálja:

$$1 \in [1], \quad 2 = 1 + 1 \in [1], \quad 3 = 1 + 1 + 1 \in [1], \ldots$$

miatt $[1] = \mathbf{Z}_n$.

Azt is láttuk, hogy a $(\mathbf{Z}; +)$ csoport is ciklikus (az $\{1\}$ annak is generátorrendszere.)

Világos, hogy $(\mathbf{Z}_n; +)$ ciklikus csoport, hiszen az $\{1\}$ generálja:

$$1 \in [1], \quad 2 = 1 + 1 \in [1], \quad 3 = 1 + 1 + 1 \in [1], \ldots$$

miatt $[1] = \mathbf{Z}_n$.

Azt is láttuk, hogy a $(\mathbf{Z}; +)$ csoport is ciklikus (az $\{1\}$ annak is generátorrendszere.)

Meglepő módon több ciklikus csoport nincs is (

Világos, hogy $(\mathbf{Z}_n; +)$ ciklikus csoport, hiszen az $\{1\}$ generálja:

$$1 \in [1], \quad 2 = 1 + 1 \in [1], \quad 3 = 1 + 1 + 1 \in [1], \ldots$$

miatt $[1] = \mathbf{Z}_n$.

Azt is láttuk, hogy a $(\mathbf{Z}; +)$ csoport is ciklikus (az $\{1\}$ annak is generátorrendszere.)

Meglepő módon több ciklikus csoport nincs is (feltéve, hogy követjük a Steinitz-elvet, és izomorf csoportok között nem teszünk különbséget)! Pontosabban fogalmazva:

58. Tétel. *(***A ciklikus csoportok leírása***) Az* $(\mathbf{Z}_n;+)$ $(n \in \mathbf{N})$ *és a* $(\mathbf{Z};+)$ *csoportok mindegyike ciklikus. Továbbá bármely ciklikus csoport a felsoroltak közül pontosan eggyel izomorf.*

58. Tétel. *(**A ciklikus csoportok leírása**) Az* $(\mathbf{Z}_n; +)$ $(n \in \mathbb{N})$ *és a* $(\mathbf{Z}; +)$ *csoportok mindegyike ciklikus. Továbbá bármely ciklikus csoport a felsoroltak közül pontosan eggyel izomorf.*

Bizonyítás vázlata: Legyen $G = [a]$ egy ciklikus csoport.

58. Tétel. *(***A ciklikus csoportok leírása***) Az* $(\mathbf{Z}_n; +)$ $(n \in \mathrm{N})$ *és a* $(\mathbf{Z}; +)$ *csoportok mindegyike ciklikus. Továbbá bármely ciklikus csoport a felsoroltak közül pontosan eggyel izomorf.*

Bizonyítás vázlata: Legyen $G = [a]$ egy ciklikus csoport. A hatványozás azonosságai szerint $a^n a^m = a^{m+n} = a^{n+m} = a^m a^n$.

58. Tétel. *(**A ciklikus csoportok leírása**) Az* $(\mathbf{Z}_n; +)$ $(n \in \mathrm{N})$ *és a* $(\mathbf{Z}; +)$ *csoportok mindegyike ciklikus. Továbbá bármely ciklikus csoport a felsoroltak közül pontosan eggyel izomorf.*

Bizonyítás vázlata: Legyen $G = [a]$ egy ciklikus csoport. A hatványozás azonosságai szerint $a^n a^m = a^{m+n} = a^{n+m} = a^m a^n$. Mivel $[a]$ éppen az ilyen a^n $(n \in \mathbf{Z})$ hatványokból áll, ezért $G = [a]$ kommutatív, azaz

58. Tétel. *(**A ciklikus csoportok leírása**) Az* $(\mathbf{Z}_n;+)$ *(*$n \in \mathrm{N}$*) és a* $(\mathbf{Z};+)$ *csoportok mindegyike ciklikus. Továbbá bármely ciklikus csoport a felsoroltak közül pontosan eggyel izomorf.*

Bizonyítás vázlata: Legyen $G=[a]$ egy ciklikus csoport. A hatványozás azonosságai szerint $a^n a^m = a^{m+n} = a^{n+m} = a^m a^n$. Mivel $[a]$ éppen az ilyen a^n $(n \in \mathbf{Z})$ hatványokból áll, ezért $G=[a]$ kommutatív, azaz Abel-csoport. A továbbiakban additív írásmódot alkalmazunk. Ekkor

58. Tétel. *(**A ciklikus csoportok leírása**) Az* $(\mathbf{Z}_n;+)$ $(n \in \mathbf{N})$ *és a* $(\mathbf{Z};+)$ *csoportok mindegyike ciklikus. Továbbá bármely ciklikus csoport a felsoroltak közül pontosan eggyel izomorf.*

Bizonyítás vázlata: Legyen $G = [a]$ egy ciklikus csoport. A hatványozás azonosságai szerint $a^n a^m = a^{m+n} = a^{n+m} = a^m a^n$. Mivel $[a]$ éppen az ilyen a^n $(n \in \mathbf{Z})$ hatványokból áll, ezért $G = [a]$ kommutatív, azaz Abel-csoport. A továbbiakban additív írásmódot alkalmazunk. Ekkor

$$G = [a] = \{\ldots - 3a, -2a, -a, 0, a, 2a, 3a, 4a, \ldots\}.$$

Ha az itt felsorolt elemek mind különbözők, akkor könnyen látható, hogy a $\varphi : (\mathbf{Z},+) \to G$, $n \mapsto na$ leképezés izomorfizmus:

Nyilván bijektív,

Nyilván bijektív, továbbá

$$(i + j)\varphi =$$

Nyilván bijektív, továbbá

$$(i + j)\varphi = (i + j)a =$$

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja =$$

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha a

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha a $\ldots, -3a, -2, -a, 0, a, 2a, 3a, 4a, \ldots$ elemek nem mind különbözők, akkor van olyan $k < \ell \in \mathbf{Z}$ hogy $ka = \ell a$.

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha a $\ldots, -3a, -2, -a, 0, a, 2a, 3a, 4a, \ldots$ elemek nem mind különbözők, akkor van olyan $k < \ell \in \mathbf{Z}$ hogy $ka = \ell a$. Ekkor $(\ell - k)a =$

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha a $\ldots, -3a, -2, -a, 0, a, 2a, 3a, 4a, \ldots$ elemek nem mind különbözők, akkor van olyan $k < \ell \in \mathbf{Z}$ hogy $ka = \ell a$. Ekkor $(\ell - k)a = \ell a - ka =$

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha a $\ldots, -3a, -2, -a, 0, a, 2a, 3a, 4a, \ldots$ elemek nem mind különbözők, akkor van olyan $k < \ell \in \mathbf{Z}$ hogy $ka = \ell a$. Ekkor $(\ell - k)a = \ell a - ka = 0$ és $\ell - k > 0$. Ezért van olyan n-nel jelölt

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha a $\ldots, -3a, -2, -a, 0, a, 2a, 3a, 4a, \ldots$ elemek nem mind különbözők, akkor van olyan $k < \ell \in \mathbf{Z}$ hogy $ka = \ell a$. Ekkor $(\ell - k)a = \ell a - ka = 0$ és $\ell - k > 0$. Ezért van olyan n-nel jelölt **legkisebb** pozitív egész szám, hogy $na = 0$.

Nyilván bijektív, továbbá

$$(i+j)\varphi = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha a $\ldots, -3a, -2, -a, 0, a, 2a, 3a, 4a, \ldots$ elemek nem mind különbözők, akkor van olyan $k < \ell \in \mathbf{Z}$ hogy $ka = \ell a$. Ekkor $(\ell - k)a = \ell a - ka = 0$ és $\ell - k > 0$. Ezért van olyan n-nel jelölt **legkisebb** pozitív egész szám, hogy $na = 0$.

Most azt lehet megmutatni, hogy a $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés izomorfizmus.

Ha a $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés nem lenne injektív, akkor lenne olyan $0 \leq i < j \leq n-1$, hogy $i\varphi = j\varphi$, Ha a $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés nem lenne injektív, akkor lenne olyan $0 \leq i < j \leq n-1$, hogy $i\varphi = j\varphi$, azaz $ia = ja$, azaz

Ha a $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés nem lenne injektív, akkor lenne olyan $0 \leq i < j \leq n-1$, hogy $i\varphi = j\varphi$, azaz $ia = ja$, azaz $(j-i)a = 0$, ami

Ha a $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés nem lenne injektív, akkor lenne olyan $0 \leq i < j \leq n-1$, hogy $i\varphi = j\varphi$, azaz $ia = ja$, azaz $(j-i)a = 0$, ami $0 < j-i \leq j < n$ miatt ellentmondana annak, hogy n a legkisebb olyan pozitív egész szám, hogy $na = 0$.

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$.

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú (

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \le r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$).

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel:

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot.

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$ka =$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = (a + \cdots + a)$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Ármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{(a + \cdots + a)}_{n} +$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Ármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{(a + \cdots + a)}_{n} + \cdots$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{\underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}_{n}}_{}$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{\underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}_{n}}_{q} +$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{\underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}_{n}}_{q} + \underbrace{(a + \cdots + a)}$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{\underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}_{n}}_{q} + \underbrace{(a + \cdots + a)}_{r}$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{\underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}_{n}}_{q} + \underbrace{(a + \cdots + a)}_{r}$$

$$= na + \cdots + na + ra =$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{\underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}_{n}}_{q} + \underbrace{(a + \cdots + a)}_{r}$$

$$= na + \cdots + na + ra = 0 + \cdots + 0 + ra =$$

A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés szürjektivitásához azt kell belátni, hogy $G = [a]$ minden eleme felírható $r\varphi = ra$ alakban, ahol $0 \leq r < n$. Mármost $[a]$ tetszőleges eleme ka alakú ($k \in \mathbf{Z}$). Osszuk el k-t maradékosan n-nel: jelölje q a hányadost és r a maradékot. Azaz $k = qn + r$ és $0 \leq r < n$. Ekkor

$$ka = (qn+r)a = \underbrace{\underbrace{(a + \cdots + a)}_{n} + \cdots + \underbrace{(a + \cdots + a)}_{n}}_{q} + \underbrace{(a + \cdots + a)}_{r}$$

$$= na + \cdots + na + ra = 0 + \cdots + 0 + ra = ra,$$

valóban. Tehát φ szürjektív.

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus,

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja = i\varphi + j\varphi.$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$,

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$(i + j)\varphi =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$(i + j)\varphi = (k - n)\varphi =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i+j)\varphi = k\varphi = ka = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$(i+j)\varphi = (k-n)\varphi = (k-n)a =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$(i + j)\varphi = (k - n)\varphi = (k - n)a = ka - na =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i + j)\varphi = k\varphi = ka = (i + j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$\begin{aligned}&(i + j)\varphi = (k - n)\varphi = (k - n)a = ka - na = \\ &ka - 0 = ka =\end{aligned}$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i+j)\varphi = k\varphi = ka = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$\begin{aligned}&(i+j)\varphi = (k-n)\varphi = (k-n)a = ka - na = \\ &ka - 0 = ka = (i+j)a =\end{aligned}$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i+j)\varphi = k\varphi = ka = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$(i+j)\varphi = (k-n)\varphi = (k-n)a = ka - na =$$
$$ka - 0 = ka = (i+j)a = ia + ja =$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i+j)\varphi = k\varphi = ka = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$(i+j)\varphi = (k-n)\varphi = (k-n)a = ka - na =$$
$$ka - 0 = ka = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Végül a A $\varphi : \mathbf{Z}_n \to G$, $i \mapsto ia$ leképezés azért homomorfizmus, mert ha az i, j egész számok $\mathbf{Z}$-ben tekintett k összege kisebb mint n, akkor $\mathbf{Z}_n$-ben is $i + j = k$, és így

$$(i+j)\varphi = k\varphi = ka = (i+j)a = ia + ja = i\varphi + j\varphi.$$

Ha pedig $\mathbf{Z}$-ben $k > n$, akkor $\mathbf{Z}_n$-ben $i + j = k - n$, és ezért

$$\begin{gathered}(i+j)\varphi = (k-n)\varphi = (k-n)a = ka - na = \\ ka - 0 = ka = (i+j)a = ia + ja = i\varphi + j\varphi.\end{gathered}$$

Q.e.d.

Lagrange-tétel

Definíció: Legyen $G = (G, \cdot)$ csoport, és legyen H részcsoportja G-nek.

Lagrange-tétel

Definíció: Legyen $G = (G, \cdot)$ csoport, és legyen H részcsoportja G-nek. (Nyomdatechnikai okokból most ugyanúgy jelöljük a csoportot és a tartóhalmazát.)

Lagrange-tétel

Definíció: Legyen $G = (G, \cdot)$ csoport, és legyen H részcsoportja G-nek. (Nyomdatechnikai okokból most ugyanúgy jelöljük a csoportot és a tartóhalmazát.) Ha $g \in G$, akkor jelölje

$$gH := \{gh : h \in H\}$$

a g elem

Lagrange-tétel

Definíció: Legyen $G = (G, \cdot)$ csoport, és legyen H részcsoportja G-nek. (Nyomdatechnikai okokból most ugyanúgy jelöljük a csoportot és a tartóhalmazát.) Ha $g \in G$, akkor jelölje

$$gH := \{gh : h \in H\}$$

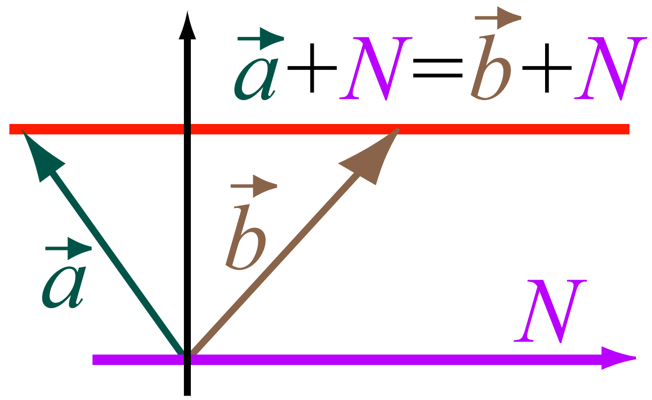
a g elem úgynevezett H szerinti **baloldali mellékosztályát**. Hasonlóképpen, a

$$Hg := \{hg : h \in H\}$$

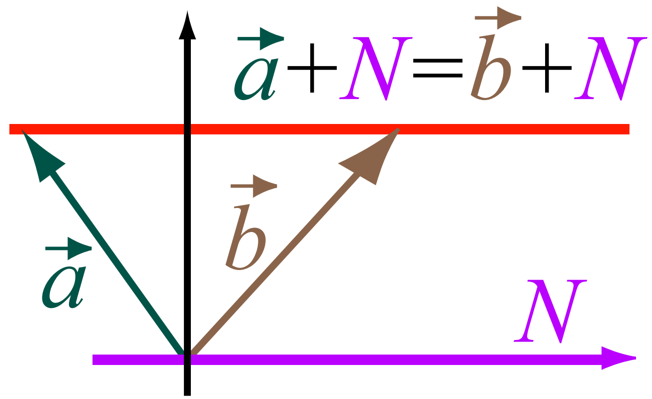
halmaz neve a g elem H **szerinti jobboldali mellékosztálya**. (A gH, illetve Hg jelölés elég találó.)

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza).

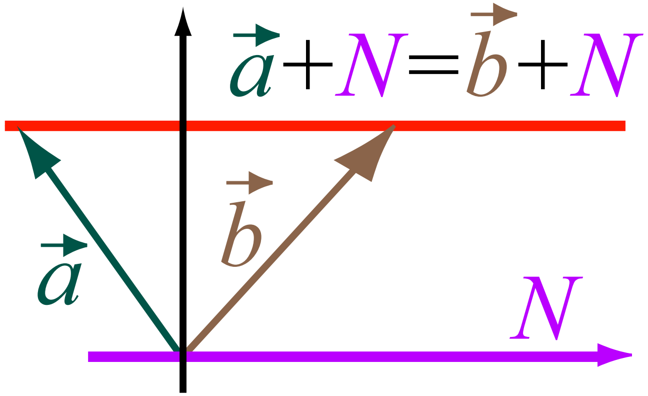


Példa: Legyen $(\mathbf{R}^2;+)$ a síkvektorok additív csoportja. Legyen $N=\{(r,0) : r\in\mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza).



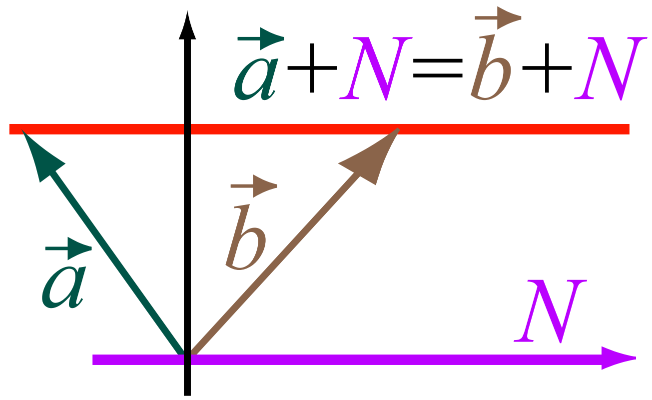
Ekkor N részcsoport.

Példa: Legyen $(\mathbf{R}^2;+)$ a síkvektorok additív csoportja. Legyen $N = \{(r,0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza).



Ekkor N részcsoport. Az N szerinti baloldali mellékosztályok éppen az

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza).

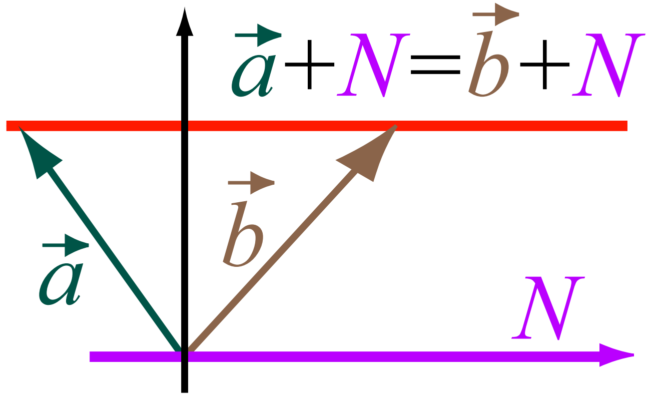


Ekkor N részcsoport. Az N szerinti baloldali mellékosztályok éppen az

$$(0, s) + N = \{(r, s) : s \in \mathbf{R}\} \qquad (s \in \mathbf{R})$$

halmazok

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza).



Ekkor N részcsoport. Az N szerinti baloldali mellékosztályok éppen az

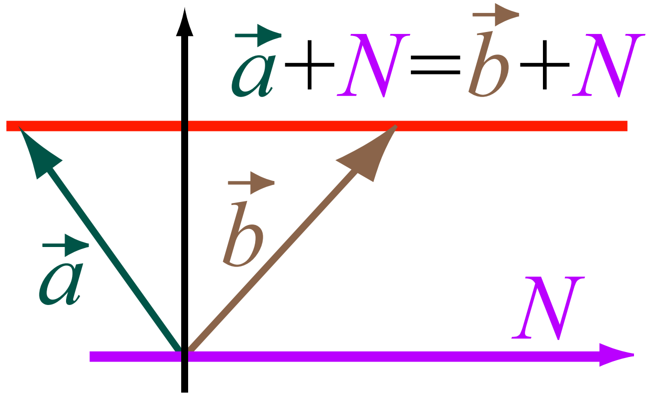
$$(0, s) + N = \{(r, s) : s \in \mathbf{R}\} \qquad (s \in \mathbf{R})$$

halmazok (figyelem, az írásmód most additív!).

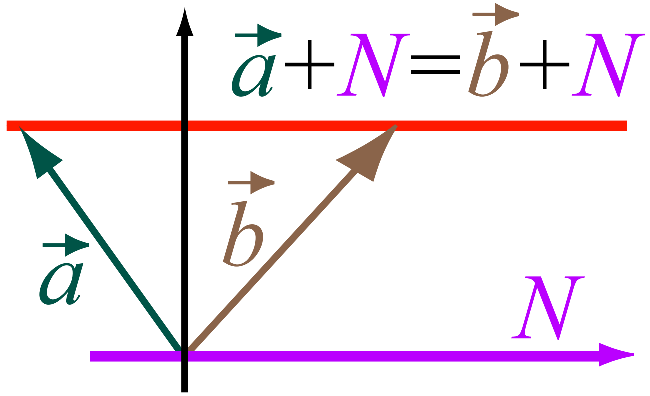
Ez a példa (legalábbis Abel-csoportok esetén) jól mutatja a mellékosztály jelentését: a mellékosztályok a részcsoport

Ez a példa (legalábbis Abel-csoportok esetén) jól mutatja a mellékosztály jelentését: a mellékosztályok a részcsoport **eltoltjai**.

Ez a példa (legalábbis Abel-csoportok esetén) jól mutatja a mellékosztály jelentését: a mellékosztályok a részcsoport **eltoltjai**. Megjegyzendő, hogy ezen mellékosztályok persze (amint az ábra mutatja) nemcsak a $(0, s)$ alakú **reprezentánsokkal** adhatók meg:



Ez a példa (legalábbis Abel-csoportok esetén) jól mutatja a mellékosztály jelentését: a mellékosztályok a részcsoport **eltoltjai**. Megjegyzendő, hogy ezen mellékosztályok persze (amint az ábra mutatja) nemcsak a $(0, s)$ alakú **reprezentánsokkal** adhatók meg:



Jelen esetben (mivel a csoport kommutatív), ugyanezek a jobb-oldali mellékosztályok is.

Példa: Legyen S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja.

Példa: Legyen S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. (Elemei az $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$ bijekciók, művelet a leképezésszorzás.) Legyen $H = \{\mathrm{id}, (12)\}$. (Emlékeztető: $(i_1\, i_2\, \ldots\, i_k)$ azt ciklust — azaz speciális bijekciót — jelöli, amelynél $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$ és $i_k \mapsto i_1$. E

Példa: Legyen S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. (Elemei az $\{1, 2, 3\} \to \{1, 2, 3\}$ bijekciók, művelet a leképezésszorzás.) Legyen $H = \{\mathrm{id}, (12)\}$. (Emlékeztető: $(i_1\, i_2\, \dots\, i_k)$ azt ciklust — azaz speciális bijekciót — jelöli, amelynél $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\dots$, $i_{k-1} \mapsto i_k$ és $i_k \mapsto i_1$. Ezen jelölés esetén $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$.)

Példa: Legyen S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. (Elemei az $\{1,2,3\} \to \{1,2,3\}$ bijekciók, művelet a leképezésszorzás.) Legyen $H = \{\text{id}, (12)\}$. (Emlékeztető: $(i_1\, i_2\, \ldots\, i_k)$ azt ciklust — azaz speciális bijekciót — jelöli, amelynél $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$ és $i_k \mapsto i_1$. Ezen jelölés esetén $S_3 = \{\text{id}, (12), (13), (23), (123), (132)\}$.) Mármost a H szerinti baloldali mellékosztályok:

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(1\,2)\}$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} =$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\, H =$$

$$\mathsf{id}\, H = \{\mathsf{id}\,\mathsf{id}, \mathsf{id}\,(12)\} = \{\mathsf{id}, (12)\} = H,$$

$$(12)\, H = \{(12)\mathsf{id}, (12)\,(12)\} =$$

$$\operatorname{id} H = \{\operatorname{id}\operatorname{id}, \operatorname{id}(12)\} = \{\operatorname{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\operatorname{id}, (12)\,(12)\} = \{(12), \operatorname{id})$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)}$$

$$\mathrm{id}\,H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\,H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$

$$(13)\,H =$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} =$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$

$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13),$$

$$\begin{aligned}\mathrm{id}\,H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\ (12)\,H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\ (13)\,H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (1\end{aligned}$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (13$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$

$$
\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &=
\end{aligned}
$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H, \\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)}, \\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\}, \\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} =
\end{aligned}$$

$$\mathrm{id}\,H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\,H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\,H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$
$$(132)\,H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132),$$

$$\mathrm{id}\,H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\,H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$

$$(13)\,H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$

$$(132)\,H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (1$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13
\end{aligned}$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},
\end{aligned}$$

$$\begin{aligned}
\text{id}\, H &= \{\text{id}\,\text{id}, \text{id}\,(12)\} = \{\text{id}, (12)\} = H,\\
(12)\, H &= \{(12)\text{id}, (12)\,(12)\} = \{(12), \text{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\text{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\text{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\, H &=
\end{aligned}$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} =
\end{aligned}$$

$$
\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23),
\end{aligned}
$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H, \\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)}, \\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\}, \\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)}, \\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23), (1
\end{aligned}$$

$$
\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23), (12
\end{aligned}
$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$

$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$

$$(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$

$$(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \ \text{(az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \ \text{(az előbbi)},\\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},
\end{aligned}$$

$$
\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},\\
(123)\, H &=
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{id}\, H &= \{\mathsf{id}\,\mathsf{id}, \mathsf{id}\,(12)\} = \{\mathsf{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathsf{id}, (12)\,(12)\} = \{(12), \mathsf{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathsf{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathsf{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\, H &= \{(23)\mathsf{id}, (23)(12)\} = \{(23), (123)\},\\
(123)\, H &= \ = \{(123)\mathsf{id}\,(13), (123)\,(12)\} =
\end{aligned}
$$

$$
\begin{gathered}
\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H, \\
(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \ \text{(az előbbi)}, \\
(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\}, \\
(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \ \text{(az előbbi)}, \\
(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\}, \\
(123)\, H = \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123),
\end{gathered}
$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$

$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$

$$(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$

$$(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},$$

$$(123)\, H = \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (2$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H, \\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)}, \\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\}, \\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)}, \\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\}, \\
(123)\, H &= \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23
\end{aligned}$$

$$\begin{gathered}
\mathrm{id}\,H=\{\mathrm{id}\,\mathrm{id},\mathrm{id}\,(12)\}=\{\mathrm{id},(12)\}=H,\\
(12)\,H=\{(12)\mathrm{id},(12)\,(12)\}=\{(12),\mathrm{id})=H\ \text{(az előbbi)},\\
(13)\,H=\{(13)\mathrm{id},(13)(12)\}=\{(13),(132)\},\\
(132)\,H=\{(132)\mathrm{id},(132)\,(12)\}=\{(132),(13)\}\ \text{(az előbbi)},\\
(23)\,H=\{(23)\mathrm{id},(23)(12)\}=\{(23),(123)\},\\
(123)\,H==\{(123)\mathrm{id}\,(13),(123)\,(12)\}=\{(123),(23)\}\ \text{(az előbbi)}.
\end{gathered}$$

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\, H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\, H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\, H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\, H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},\\
(123)\, H &= \; = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.
\end{aligned}$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. M

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$

$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$

$$(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$

$$(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},$$

$$(123)\, H = \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. Mivel pl.

$$H\,(13) =$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$
$$(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$
$$(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},$$
$$(123)\, H = \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. Mivel pl.

$$H\,(13) = \{\mathrm{id}\,(13), (12)(13)\} =$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$
$$(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$
$$(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},$$
$$(123)\, H = \; = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. Mivel pl.

$$H\,(13) = \{\mathrm{id}\,(13), (12)(13)\} = \{(13),$$

$$\mathrm{id}\,H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\,H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\,H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$
$$(132)\,H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$
$$(23)\,H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},$$
$$(123)\,H = \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. Mivel pl.

$$H\,(13) = \{\mathrm{id}\,(13), (12)(13)\} = \{(13), (1$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$

$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$

$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$

$$(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$

$$(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},$$

$$(123)\, H = \; = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. Mivel pl.

$$H\,(13) = \{\mathrm{id}\,(13), (12)(13)\} = \{(13), (12$$

$$
\begin{aligned}
\mathrm{id}\,H &= \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,\\
(12)\,H &= \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},\\
(13)\,H &= \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},\\
(132)\,H &= \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},\\
(23)\,H &= \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},\\
(123)\,H &= \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.
\end{aligned}
$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. Mivel pl.

$$
H\,(13) = \{\mathrm{id}\,(13), (12)(13)\} = \{(13), (123)\}
$$

$$\mathrm{id}\, H = \{\mathrm{id}\,\mathrm{id}, \mathrm{id}\,(12)\} = \{\mathrm{id}, (12)\} = H,$$
$$(12)\, H = \{(12)\mathrm{id}, (12)\,(12)\} = \{(12), \mathrm{id}) = H \text{ (az előbbi)},$$
$$(13)\, H = \{(13)\mathrm{id}, (13)(12)\} = \{(13), (132)\},$$
$$(132)\, H = \{(132)\mathrm{id}, (132)\,(12)\} = \{(132), (13)\} \text{ (az előbbi)},$$
$$(23)\, H = \{(23)\mathrm{id}, (23)(12)\} = \{(23), (123)\},$$
$$(123)\, H = \ = \{(123)\mathrm{id}\,(13), (123)\,(12)\} = \{(123), (23)\} \text{ (az előbbi)}.$$

Tehát három darab baloldali mellékosztály van, és mindegyik kételemű. Mivel pl.

$$H\,(13) = \{\mathrm{id}\,(13), (12)(13)\} = \{(13), (123)\}$$

nem szerepel az előző listán, látható, hogy a jobboldali mellékosztályok általában különböznek a baloldaliaktól.

Az S_3-mal kapcsolatos példa jól illusztrálja az alábbi tételt, amely magyarázatot ad a „mellékosztály” elnevezésre.

Az S_3-mal kapcsolatos példa jól illusztrálja az alábbi tételt, amely magyarázatot ad a „mellékosztály” elnevezésre.

59. Tétel. *Ha G csoport és H részcsoportja G-nek, akkor*

$$\{gH : g \in G\},$$

Az S_3-mal kapcsolatos példa jól illusztrálja az alábbi tételt, amely magyarázatot ad a „mellékosztály” elnevezésre.

59. Tétel. *Ha G csoport és H részcsoportja G-nek, akkor*

$$\{gH : g \in G\},$$

azaz a H szerinti baloldali mellékosztályok halmaza

Az S_3-mal kapcsolatos példa jól illusztrálja az alábbi tételt, amely magyarázatot ad a „mellékosztály” elnevezésre.

59. Tétel. *Ha G csoport és H részcsoportja G-nek, akkor*

$$\{gH : g \in G\},$$

azaz a H szerinti baloldali mellékosztályok halmaza **osztályozás** *a G tartóhalmazán.*

Az S_3-mal kapcsolatos példa jól illusztrálja az alábbi tételt, amely magyarázatot ad a „mellékosztály” elnevezésre.

59. Tétel. *Ha G csoport és H részcsoportja G-nek, akkor*

$$\{gH : g \in G\},$$

azaz a H szerinti baloldali mellékosztályok halmaza **osztályozás** *a G tartóhalmazán. Analóg állítás érvényes a jobboldali mellékosztályok halmazára is.*

Bizonyítás: (1)

Bizonyítás: (1) Tetszőleges $g \in G$-re $g = g{\cdot}1 \in gH$ miatt $gH \neq \emptyset$.
Tehát a mellékosztályok nem üresek.

Bizonyítás: (1) Tetszőleges $g \in G$-re $g = g \cdot 1 \in gH$ miatt $gH \neq \emptyset$. Tehát a mellékosztályok nem üresek.

(2) Ha $g \in G$, akkor $g =$

Bizonyítás: (1) Tetszőleges $g \in G$-re $g = g{\cdot}1 \in gH$ miatt $gH \neq \emptyset$.
Tehát a mellékosztályok nem üresek.

(2) Ha $g \in G$, akkor $g = g \cdot 1 \in$

Bizonyítás: (1) Tetszőleges $g \in G$-re $g = g{\cdot}1 \in gH$ miatt $gH \neq \emptyset$.
Tehát a mellékosztályok nem üresek.

(2) Ha $g \in G$, akkor $g = g \cdot 1 \in gH$ miatt

Bizonyítás: (1) Tetszőleges $g \in G$-re $g = g{\cdot}1 \in gH$ miatt $gH \neq \emptyset$. Tehát a mellékosztályok nem üresek.

(2) Ha $g \in G$, akkor $g = g \cdot 1 \in gH$ miatt a G minden eleme benne van valamelyik mellékosztályban, tehát a mellékosztályok uniója $= G$.

(3) Tegyük fel, hogy $g_1 H \cap g_2 H \neq \emptyset$,

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$.

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$.

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról)

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$.

(3) Tegyük fel, hogy $g_1 H \cap g_2 H \neq \emptyset$, mondjuk $a \in g_1 H \cap g_2 H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1 h_1$ és $a = g_2 h_2$. Innen persze $g_1 h_1 = g_2 h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2 h_2 h_1^{-1}$. Ármost tetszőleges $x \in g_1 H$-ra $x = g_1 h_3$ $(h_3 \in H)$ alakú,

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ $(h_3 \in H)$ alakú, és ezért

$$x =$$

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3$$

(3) Tegyük fel, hogy $g_1 H \cap g_2 H \neq \emptyset$, mondjuk $a \in g_1 H \cap g_2 H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1 h_1$ és $a = g_2 h_2$. Innen persze $g_1 h_1 = g_2 h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2 h_2 h_1^{-1}$. Mármost tetszőleges $x \in g_1 H$-ra $x = g_1 h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1 h_3 = (g_2 h_2 h_1^{-1}) h_3 =$$

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — ré

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ $(h_3 \in H)$ alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet.

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$.

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$. Mivel g_1 és g_2 szerepe a megfontolásban szimmetrikus, $g_2H \subseteq g_1H$ is teljesül.

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ $(h_3 \in H)$ alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$. Mivel g_1 és g_2 szerepe a megfontolásban szimmetrikus, $g_2H \subseteq g_1H$ is teljesül. Ezzel beláttuk, hogy $g_1H \cap g_2H \neq \emptyset \Longrightarrow g_1H = g_2H$. A

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$. Mivel g_1 és g_2 szerepe a megfontolásban szimmetrikus, $g_2H \subseteq g_1H$ is teljesül. Ezzel beláttuk, hogy $g_1H \cap g_2H \neq \emptyset \implies g_1H = g_2H$. Azaz (

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$. Mivel g_1 és g_2 szerepe a megfontolásban szimmetrikus, $g_2H \subseteq g_1H$ is teljesül. Ezzel beláttuk, hogy $g_1H \cap g_2H \neq \emptyset \implies g_1H = g_2H$. Azaz (kontrapozícióval):

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$. Mivel g_1 és g_2 szerepe a megfontolásban szimmetrikus, $g_2H \subseteq g_1H$ is teljesül. Ezzel beláttuk, hogy $g_1H \cap g_2H \neq \emptyset \Longrightarrow g_1H = g_2H$. Azaz (kontrapozícióval): a diszjunkt mellékosztályok különbözők.

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Ármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$. Mivel g_1 és g_2 szerepe a megfontolásban szimmetrikus, $g_2H \subseteq g_1H$ is teljesül. Ezzel beláttuk, hogy $g_1H \cap g_2H \neq \emptyset \Longrightarrow g_1H = g_2H$. Azaz (kontrapozícióval): a diszjunkt mellékosztályok különbözők.

(1), (2) és (3) azt jelenti, hogy $\{gH : g \in G\}$ osztályozás.

(3) Tegyük fel, hogy $g_1H \cap g_2H \neq \emptyset$, mondjuk $a \in g_1H \cap g_2H$. Ekkor alkalmas $h_1, h_2 \in H$ elemekre $a = g_1h_1$ és $a = g_2h_2$. Innen persze $g_1h_1 = g_2h_2$, ahonnan (h_1 inverzével beszorozva jobbról) $g_1 = g_2h_2h_1^{-1}$. Mármost tetszőleges $x \in g_1H$-ra $x = g_1h_3$ ($h_3 \in H$) alakú, és ezért

$$x = g_1h_3 = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H,$$

ugyanis — részcsoport lévén — H tartalmazza a $h_2h_1^{-1}h_3$ elemet. Ez azt mutatja, hogy $g_1H \subseteq g_2H$. Mivel g_1 és g_2 szerepe a megfontolásban szimmetrikus, $g_2H \subseteq g_1H$ is teljesül. Ezzel beláttuk, hogy $g_1H \cap g_2H \neq \emptyset \Longrightarrow g_1H = g_2H$. Azaz (kontrapozícióval): a diszjunkt mellékosztályok különbözők.

(1), (2) és (3) azt jelenti, hogy $\{gH : g \in G\}$ osztályozás. A jobboldali mellékosztályokra a megfontolás hasonló. Q.e.d.

10. Állítás. *Ha* G *csoport és* H *részcsoportja* G*-nek, akkor bármely* H*-szerinti baloldali és bármely* H*-szerinti jobboldali mellékosztálynak ugyanannyi eleme van.*

10. Állítás. *Ha G csoport és H részcsoportja G-nek, akkor bármely H-szerinti baloldali és bármely H-szerinti jobboldali mellékosztálynak ugyanannyi eleme van.*

Bizonyítás: Legyen $g_1, g_2 \in G$ tetszőleges. Állítjuk (és ezt elegendő is belátni), hogy a

$$\varphi : g_1H \to Hg_2, \qquad g_1h \mapsto hg_2 \qquad (h \in H)$$

leképezés bijekció.

10. Állítás. *Ha G csoport és H részcsoportja G-nek, akkor bármely H-szerinti baloldali és bármely H-szerinti jobboldali mellékosztálynak ugyanannyi eleme van.*

Bizonyítás: Legyen $g_1, g_2 \in G$ tetszőleges. Állítjuk (és ezt elegendő is belátni), hogy a

$$\varphi : g_1 H \to H g_2, \qquad g_1 h \mapsto h g_2 \qquad (h \in H)$$

leképezés bijekció. Mindenekelőtt ha $g_1 h = g_1 h'$, akkor $h = g_1^{-1} g_1 h = g_1^{-1} g_1 h' = h'$ miatt $h g_2 = h' g_2$, azaz a leképezés jóldefiniált.

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h =$

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) =$

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} =$

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} =$

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) =$

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így $g_1h = g_1h'$. Tehát φ injektív.

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így $g_1h = g_1h'$. Tehát φ injektív.

A Hg_2 tetszőleges eleme hg_2 $(h \in H)$ alakú, és ezen elemnek nyilván őse a g_1H-beli g_1h elem.

Ha $(g_1 h)\varphi = (g_1 h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2 g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2 g_2^{-1}) = h'$, és így $g_1 h = g_1 h'$. Tehát φ injektív.

A Hg_2 tetszőleges eleme hg_2 $(h \in H)$ alakú, és ezen elemnek nyilván őse a $g_1 H$-beli $g_1 h$ elem. Ezért φ szürjektív.

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így $g_1h = g_1h'$. Tehát φ injektív.

A Hg_2 tetszőleges eleme hg_2 $(h \in H)$ alakú, és ezen elemnek nyilván őse a g_1H-beli g_1h elem. Ezért φ szürjektív. Az eddigiek szerint bijektív.

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így $g_1h = g_1h'$. Tehát φ injektív.

A Hg_2 tetszőleges eleme hg_2 $(h \in H)$ alakú, és ezen elemnek nyilván őse a g_1H-beli g_1h elem. Ezért φ szürjektív. Az eddigiek szerint bijektív. Q.e.d.

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így $g_1h = g_1h'$. Tehát φ injektív.

A Hg_2 tetszőleges eleme hg_2 $(h \in H)$ alakú, és ezen elemnek nyilván őse a g_1H-beli g_1h elem. Ezért φ szürjektív. Az eddigiek szerint bijektív. Q.e.d.

Definíció: A tradicionális szóhasználat szerint egy (véges) csoport elemszámát a

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így $g_1h = g_1h'$. Tehát φ injektív.

A Hg_2 tetszőleges eleme hg_2 $(h \in H)$ alakú, és ezen elemnek nyilván őse a g_1H-beli g_1h elem. Ezért φ szürjektív. Az eddigiek szerint bijektív. Q.e.d.

Definíció: A tradicionális szóhasználat szerint egy (véges) csoport elemszámát a **a csoport rendjének** nevezzük.

Ha $(g_1h)\varphi = (g_1h')\varphi$, azaz $hg_2 = h'g_2$, akkor $h = h(g_2g_2^{-1}) = (hg_2)g_2^{-1} = (h'g_2)g_2^{-1} = h'(g_2g_2^{-1}) = h'$, és így $g_1h = g_1h'$. Tehát φ injektív.

A Hg_2 tetszőleges eleme hg_2 $(h \in H)$ alakú, és ezen elemnek nyilván őse a g_1H-beli g_1h elem. Ezért φ szürjektív. Az eddigiek szerint bijektív. Q.e.d.

Definíció: A tradicionális szóhasználat szerint egy (véges) csoport elemszámát a **a csoport rendjének** nevezzük. Egy részcsoport baloldali mellékosztályainak számát pedig a **részcsoport indexének** nevezzük. Ha H részcsoportja G-nek, akkor H indexét $[G : H]$ jelöli.

60. Tétel. *Legyen* G *véges csoport,* H *pedig részcsoportja* G*-nek.*

60. Tétel. *Legyen G véges csoport, H pedig részcsoportja G-nek.*

(1) H jobboldali mellékosztályainak száma megegyezik a baloldali mellékosztályainak számával, azaz $[G : H]$-val.

60. Tétel. *Legyen G véges csoport, H pedig részcsoportja G-nek.*

(1) H jobboldali mellékosztályainak száma megegyezik a baloldali mellékosztályainak számával, azaz $[G : H]$-val.

*(2) (**Lagrange-tétel**) $|G| = [G : H] \cdot |H|$,*

60. Tétel. *Legyen G véges csoport, H pedig részcsoportja G-nek.*

(1) H jobboldali mellékosztályainak száma megegyezik a baloldali mellékosztályainak számával, azaz $[G:H]$-val.

*(2) (**Lagrange-tétel**) $|G| = [G:H] \cdot |H|$, azaz véges csoport tetszőleges* **részcsoportjának rendje is és indexe is osztja a kiindulási csoport rendjét**,

60. Tétel. *Legyen G véges csoport, H pedig részcsoportja G-nek.*

(1) H jobboldali mellékosztályainak száma megegyezik a baloldali mellékosztályainak számával, azaz $[G : H]$-val.

*(2) (**Lagrange-tétel**) $|G| = [G : H] \cdot |H|$, azaz véges csoport tetszőleges* **részcsoportjának rendje is és indexe is osztja a kiindulási csoport rendjét**, *sőt a* **részcsoport rendjének és indexének szorzata az eredeti csoport rendje** *(azaz elemszáma).*

Bizonyítás: Legyen $g_2 \in G$. L

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával.

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos.

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) $=$

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) $=$ az osztályok száma (

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) $=$ az osztályok száma (esetünkben $[G : H]$, azaz H indexe)

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) = az osztályok száma (esetünkben $[G : H]$, azaz H indexe) szorozva

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) = az osztályok száma (esetünkben $[G : H]$, azaz H indexe) szorozva egy tetszőleges osztály elemszámával

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) = az osztályok száma (esetünkben $[G : H]$, azaz H indexe) szorozva egy tetszőleges osztály elemszámával (esetünkben $|1H| = |H|$-val, azaz H rendjével).

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) $=$ az osztályok száma (esetünkben $[G : H]$, azaz H indexe) szorozva egy tetszőleges osztály elemszámával (esetünkben $|1H| = |H|$-val, azaz H rendjével). Ezzel beláttuk, hogy

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) = az osztályok száma (esetünkben $[G : H]$, azaz H indexe) szorozva egy tetszőleges osztály elemszámával (esetünkben $|1H| = |H|$-val, azaz H rendjével). Ezzel beláttuk, hogy

$$|G| = [G : H] \cdot |H|.$$

Bizonyítás: Legyen $g_2 \in G$. Láttuk, hogy tetszőleges baloldali mellékosztály elemszáma azonos a Hg_2 jobboldali mellékosztály elemszámával. Ezért H baloldali mellékosztályainak elemszáma azonos. Mármost ha egy osztályozás osztályai azonos elemszámúak, akkor az alaphalmaz elemszáma (esetünkben $|G|$, azaz G rendje) = az osztályok száma (esetünkben $[G : H]$, azaz H indexe) szorozva egy tetszőleges osztály elemszámával (esetünkben $|1H| = |H|$-val, azaz H rendjével). Ezzel beláttuk, hogy

$$|G| = [G : H] \cdot |H|.$$

Innen persze az is következik, hogy H **bal**oldali mellékosztályainak száma

$$[G : H] = \frac{|G|}{|H|}.$$

Az í

$$[G : H] = \frac{|G|}{|H|}.$$

Az ízlés dolga, hogy a bal- vagy a jobboldali mellékosztályokkal számolunk —

$$[G : H] = \frac{|G|}{|H|}.$$

Az ízlés dolga, hogy a bal- vagy a jobboldali mellékosztályokkal számolunk — a bal- és jobboldalak szisztematikus felcserélésével az jött volna ki,

$$[G : H] = \frac{|G|}{|H|}.$$

Az ízlés dolga, hogy a bal- vagy a jobboldali mellékosztályokkal számolunk — a bal- és jobboldalak szisztematikus felcserélésével az jött volna ki, hogy a jobboldali mellékosztályok száma is

$$\frac{|G|}{|H|},$$

$$[G:H]=\frac{|G|}{|H|}.$$

Az ízlés dolga, hogy a bal- vagy a jobboldali mellékosztályokkal számolunk — a bal- és jobboldalak szisztematikus felcserélésével az jött volna ki, hogy a jobboldali mellékosztályok száma is

$$\frac{|G|}{|H|},$$

tehát azonos a baloldali mellékosztályok számával. Q.e.d.

Példa: Legyen S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja, és legyen $H = \{\mathrm{id}, (12)\}$. A korábbi példa során felsoroltuk H baloldali mellékosztályait:

Példa: Legyen S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja, és legyen $H = \{\mathrm{id}, (12)\}$. A korábbi példa során felsoroltuk H baloldali mellékosztályait: három darab vol. H rendje $|H| =$

Példa: Legyen S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja, és legyen $H = \{\mathrm{id}, (12)\}$. A korábbi példa során felsoroltuk H baloldali mellékosztályait: három darab vol. H rendje $|H| = 2$. S_3 rendje $|S_3| =$

Példa: Legyen S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja, és legyen $H = \{\mathrm{id}, (12)\}$. A korábbi példa során felsoroltuk H baloldali mellékosztályait: három darab vol. H rendje $|H| = 2$. S_3 rendje $|S_3| = 3! = 6$. Ez a példa jól szemlélteti a Lagrange-tételt:

Példa: Legyen S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja, és legyen $H = \{\mathrm{id}, (12)\}$. A korábbi példa során felsoroltuk H baloldali mellékosztályait: három darab vol. H rendje $|H| = 2$. S_3 rendje $|S_3| = 3! = 6$. Ez a példa jól szemlélteti a Lagrange-tételt: $6 = |S_3| = [S_3 : H] \cdot |H| = 3 \cdot 2$.

Példa: Legyen S_{20} az $\{1, 2, 3, \ldots, 20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Példa: Legyen S_{20} az $\{1, 2, 3, \ldots, 20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Mert ha H részcsoport és $|H| = 29$, akkor a

Példa: Legyen S_{20} az $\{1,2,3,\dots,20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Mert ha H részcsoport és $|H| = 29$, akkor a Lagrange-tétel miatt

$$29 \mid |S_{20}| =$$

Példa: Legyen S_{20} az $\{1,2,3,\ldots,20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Mert ha H részcsoport és $|H| = 29$, akkor a Lagrange-tétel miatt

$$29 \mid |S_{20}| = 20! = 1 \cdot 2 \cdot \cdots \cdot 20,$$

Példa: Legyen S_{20} az $\{1, 2, 3, \ldots, 20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Mert ha H részcsoport és $|H| = 29$, akkor a Lagrange-tétel miatt

$$29 \mid |S_{20}| = 20! = 1 \cdot 2 \cdot \dots \cdot 20,$$

ami lehetetlen (h

Példa: Legyen S_{20} az $\{1, 2, 3, \ldots, 20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Mert ha H részcsoport és $|H| = 29$, akkor a Lagrange-tétel miatt

$$29 \mid |S_{20}| = 20! = 1 \cdot 2 \cdot \dots \cdot 20,$$

ami lehetetlen (hiszen a 29 prímszám, és a húsz közül egyik tényezőt sem osztja).

Példa: Legyen S_{20} az $\{1, 2, 3, \ldots, 20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Mert ha H részcsoport és $|H| = 29$, akkor a Lagrange-tétel miatt

$$29 \mid |S_{20}| = 20! = 1 \cdot 2 \cdot \cdots \cdot 20,$$

ami lehetetlen (hiszen a 29 prímszám, és a húsz közül egyik tényezőt sem osztja). (A Lagrange-tétel nélkül — pusztán a részcsoport definíciójára támaszkodva ezt aligha lehetett volna kihozni, hiszen S_{20} 29-elemű részhalmazainak száma

$$\binom{20!}{29} \approx 1,7826868841832 \times 10^{502} \ ,$$

Példa: Legyen S_{20} az $\{1, 2, 3, \ldots, 20\}$ halmazon ható permutációk csoportja. (Művelet a leképezésszorzás). Ekkor S_{20}-nak nincs 29-elemű részcsoportja.

Mert ha H részcsoport és $|H| = 29$, akkor a Lagrange-tétel miatt

$$29 \mid |S_{20}| = 20! = 1 \cdot 2 \cdot \cdots \cdot 20,$$

ami lehetetlen (hiszen a 29 prímszám, és a húsz közül egyik tényezőt sem osztja). (A Lagrange-tétel nélkül — pusztán a részcsoport definíciójára támaszkodva ezt aligha lehetett volna kihozni, hiszen S_{20} 29-elemű részhalmazainak száma

$$\binom{20!}{29} \approx 1,7826868841832 \times 10^{502} ,$$

és ezek műveleti zártságát nincs idő ellenőrizni.)

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$.

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük.

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) =$

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\mathrm{id}) =$

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\mathrm{id}) = 1$, $o((1\,2\,3)) = 3$.

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\mathrm{id}) = 1$, $o((1\,2\,3)) = 3$. Az $(\mathbf{R}\setminus\{0\};\cdot)$ csoportban $o(1) =$

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\mathrm{id}) = 1$, $o((1\,2\,3)) = 3$. Az $(\mathbf{R} \setminus \{0\};\cdot)$ csoportban $o(1) = 1$, $o(-1) =$

Definíció: Legyen $(G;\cdot)$ csoport és $b\in G$. A b **elem rendjén** a legkisebb olyan $k\in\mathbf{N}$ kitevőt értjük, amelyre $b^k=1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k\in\mathbf{N}$ hogy $b^k=1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k\in\mathbf{N}$ hogy $b^k=1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2))=2$, $o(\mathrm{id})=1$, $o((1\,2\,3))=3$. Az $(\mathbf{R}\setminus\{0\};\cdot)$ csoportban $o(1)=1$, $o(-1)=2$, és az összes többi b elem végtelen rendű.

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\mathrm{id}) = 1$, $o((1\,2\,3)) = 3$. Az $(\mathbf{R}\setminus\{0\};\cdot)$ csoportban $o(1) = 1$, $o(-1) = 2$, és az összes többi b elem végtelen rendű. A $(\mathbf{Z}_4;+)$ csoportban $o(0) =$

Definíció: Legyen $(G;\cdot)$ csoport és $b\in G$. A b **elem rendjén** a legkisebb olyan $k\in\mathbf{N}$ kitevőt értjük, amelyre $b^k=1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k\in\mathbf{N}$ hogy $b^k=1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k\in\mathbf{N}$ hogy $b^k=1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2))=2$, $o(\mathrm{id})=1$, $o((1\,2\,3))=3$. Az $(\mathbf{R}\setminus\{0\};\cdot)$ csoportban $o(1)=1$, $o(-1)=2$, és az összes többi b elem végtelen rendű. A $(\mathbf{Z}_4;+)$ csoportban $o(0)=1$, $o(1)=$

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\mathrm{id}) = 1$, $o((1\,2\,3)) = 3$. Az $(\mathbf{R} \setminus \{0\};\cdot)$ csoportban $o(1) = 1$, $o(-1) = 2$, és az összes többi b elem végtelen rendű. A $(\mathbf{Z}_4;+)$ csoportban $o(0) = 1$, $o(1) = 4$, $o(2) =$

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\text{id}) = 1$, $o((1\,2\,3)) = 3$. Az $(\mathbf{R} \setminus \{0\};\cdot)$ csoportban $o(1) = 1$, $o(-1) = 2$, és az összes többi b elem végtelen rendű. A $(\mathbf{Z}_4;+)$ csoportban $o(0) = 1$, $o(1) = 4$, $o(2) = 2$ és $o(3) =$

Definíció: Legyen $(G;\cdot)$ csoport és $b \in G$. A b **elem rendjén** a legkisebb olyan $k \in \mathbf{N}$ kitevőt értjük, amelyre $b^k = 1$. A b elem rendjét $o(b)$ („ordó bé") jelöli. Ha létezik $o(b)$ (azaz ha van olyan $k \in \mathbf{N}$ hogy $b^k = 1$), akkor b-t végesrendű elemnek nevezzük. Ha nincs olyan $k \in \mathbf{N}$ hogy $b^k = 1$, akkor b-t végtelen rendű elemnek nevezzük.

Példák: Az $(S_3;\circ)$ csoportban $o((1\,2)) = 2$, $o(\mathrm{id}) = 1$, $o((1\,2\,3)) = 3$. Az $(\mathbf{R}\setminus\{0\};\cdot)$ csoportban $o(1) = 1$, $o(-1) = 2$, és az összes többi b elem végtelen rendű. A $(\mathbf{Z}_4;+)$ csoportban $o(0) = 1$, $o(1) = 4$, $o(2) = 2$ és $o(3) = 4$.

Könnyen látható, hogy $o(b) = 1 \iff b = 1$ (a csoport egységeleme). (E

Könnyen látható, hogy $o(b) = 1 \iff b = 1$ (a csoport egységeleme). (Ez nincs ellentmondásban az előző példával: ott az additív írásmód miatt az 1 nem a csoport egységeleme volt!)

Könnyen látható, hogy $o(b) = 1 \iff b = 1$ (a csoport egységeleme). (Ez nincs ellentmondásban az előző példával: ott az additív írásmód miatt az 1 nem a csoport egységeleme volt!)

A ciklikus csoportok leírásából könnyen látható, hogy

11. Állítás.

11. Állítás.

Ha G *csoport és* $b \in G$, *akkor* $|[b]| = o(b)$. *Azaz*

11. Állítás.

Ha G csoport és $b \in G$, akkor $|[b]| = o(b)$. Azaz elem rendje egyenlő az általa generált (ciklikus) részcsoport rendjével.

11. Állítás.

Ha G *csoport és* $b \in G$*, akkor* $|[b]| = o(b)$*. Azaz elem rendje egyenlő az általa generált (ciklikus) részcsoport rendjével.*

Fenti állításunkat a Lagrange-tétellel kombinálva kapjuk az alábbit:

11. Állítás.

Ha G csoport és $b \in G$, akkor $|[b]| = o(b)$. Azaz elem rendje egyenlő az általa generált (ciklikus) részcsoport rendjével.

Fenti állításunkat a Lagrange-tétellel kombinálva kapjuk az alábbit:

61. Tétel. *(**Cauchy tétele**) Véges csoportban bármely elem rendje osztja a csoport rendjét.*

Innen persze az egyébként is könnyen látható tény is következik, hogy véges csoportban minden elem végesrendű.

Innen persze az egyébként is könnyen látható tény is következik, hogy véges csoportban minden elem végesrendű.

12. Állítás. *Legyen b egy végesrendű elem egy tetszőleges csoportban, és legyen $k \in \mathbf{Z}$. Ekkor*

$$b^k = 1 \iff o(b) \mid k.$$

Bizonyítás: Legyen $n = o(b)$.

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k =$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq}$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q =$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan:

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan: $k = nq + r$, ahol $q \in \mathbf{Z}$ a hányados és $r \in \{0, 1, \ldots, n-1\}$ a maradék. Ekkor

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan: $k = nq + r$, ahol $q \in \mathbf{Z}$ a hányados és $r \in \{0, 1, \ldots, n-1\}$ a maradék. Ekkor

$$b^r =$$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan: $k = nq + r$, ahol $q \in \mathbf{Z}$ a hányados és $r \in \{0, 1, \ldots, n-1\}$ a maradék. Ekkor

$$b^r = b^{k-nq} =$$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan: $k = nq + r$, ahol $q \in \mathbf{Z}$ a hányados és $r \in \{0, 1, \ldots, n-1\}$ a maradék. Ekkor

$$b^r = b^{k-nq} = b^k (b^n)^{-q} =$$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan: $k = nq + r$, ahol $q \in \mathbf{Z}$ a hányados és $r \in \{0, 1, \ldots, n-1\}$ a maradék. Ekkor

$$b^r = b^{k-nq} = b^k (b^n)^{-q} = 1^k \cdot 1^{-q} = 1.$$

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan: $k = nq + r$, ahol $q \in \mathbf{Z}$ a hányados és $r \in \{0, 1, \ldots, n-1\}$ a maradék. Ekkor

$$b^r = b^{k-nq} = b^k (b^n)^{-q} = 1^k \cdot 1^{-q} = 1.$$

Mivel $n = o(b)$ volt a minimális olyan pozitív egész kitevő, amelyre $b^n = 1$ és $r < n$, ezért a kivetett képletből $r = 0$, azaz $o(b) = n \mid k$ következik.

Bizonyítás: Legyen $n = o(b)$. Ha $n \mid k$, mondjuk $k = nq$, akkor $b^k = b^{nq} = (b^n)^q = 1^q = 1$.

Fordítva, ha $b^k = 1$, akkor osszuk el k-t n-nel maradékosan: $k = nq + r$, ahol $q \in \mathbf{Z}$ a hányados és $r \in \{0, 1, \ldots, n-1\}$ a maradék. Ekkor

$$b^r = b^{k-nq} = b^k (b^n)^{-q} = 1^k \cdot 1^{-q} = 1.$$

Mivel $n = o(b)$ volt a minimális olyan pozitív egész kitevő, amelyre $b^n = 1$ és $r < n$, ezért a kivetett képletből $r = 0$, azaz $o(b) = n \mid k$ következik. Q.e.d.

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G; \cdot)$ csoport, $|G| = p$ prímszám és

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G;\cdot)$ csoport, $|G| = p$ prímszám és $b \in G\setminus\{1\}$. (

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G; \cdot)$ csoport, $|G| = p$ prímszám és $b \in G \setminus \{1\}$. ($|G| = p > 1$ miatt létezik ilyen b elem.

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G; \cdot)$ csoport, $|G| = p$ prímszám és $b \in G \setminus \{1\}$. ($|G| = p > 1$ miatt létezik ilyen b elem.) Ekkor $1 < o(b)$

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G;\cdot)$ csoport, $|G| = p$ prímszám és $b \in G \setminus \{1\}$. ($|G| = p > 1$ miatt létezik ilyen b elem.) Ekkor $1 < o(b) \mid |G| = p$ miatt $|[b]| =$

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G; \cdot)$ csoport, $|G| = p$ prímszám és $b \in G \setminus \{1\}$. ($|G| = p > 1$ miatt létezik ilyen b elem.) Ekkor $1 < o(b) \mid |G| = p$ miatt $|[b]| = o(b) = p = |G|$, így $[b] = G$,

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G;\cdot)$ csoport, $|G| = p$ prímszám és $b \in G \setminus \{1\}$. ($|G| = p > 1$ miatt létezik ilyen b elem.) Ekkor $1 < o(b) \mid |G| = p$ miatt $|[b]| = o(b) = p = |G|$, így $[b] = G$, tehát G ciklikus.

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G;\cdot)$ csoport, $|G| = p$ prímszám és $b \in G \setminus \{1\}$. ($|G| = p > 1$ miatt létezik ilyen b elem.) Ekkor $1 < o(b) \mid |G| = p$ miatt $|[b]| = o(b) = p = |G|$, így $[b] = G$, tehát G ciklikus. Q.e.d.

62. Tétel. *Ha egy csoport rendje (azaz elemszáma) prímszám, akkor a csoport ciklikus.*

Bizonyítás: Legyen $(G;\cdot)$ csoport, $|G| = p$ prímszám és $b \in G \setminus \{1\}$. ($|G| = p > 1$ miatt létezik ilyen b elem.) Ekkor $1 < o(b) \mid |G| = p$ miatt $|[b]| = o(b) = p = |G|$, így $[b] = G$, tehát G ciklikus. Q.e.d.

A kis Fermat-tételt (és az azt általánosító Euler-tételt) a Lagrange-tétel következményének is felfogható. Ez a kis-Fermat-tétel kapcsán demonstráljuk.

Legyen p prímszám és jelölje $R_p = \mathbf{Z}_p^*$ az $\{1, 2, \ldots, p-1\}$ halmazt. Ezen a halmazon egy új szorzás műveletet definiálunk: ha $a, b \in \mathbf{Z}_p^*$, akkor legyen $c = a \cdot b$ az az eleme R_p-nek, amelyre $c \equiv ab \pmod p$.

Legyen p prímszám és jelölje $R_p = \mathbf{Z}_p^*$ az $\{1, 2, \ldots, p-1\}$ halmazt. Ezen a halmazon egy új szorzás műveletet definiálunk: ha $a, b \in \mathbf{Z}_p^*$, akkor legyen $c = a \cdot b$ az az eleme R_p-nek, amelyre $c \equiv ab \pmod{p}$. Például $(R_5; \cdot)$ művelettáblázata itt látható:

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

A lineáris kongruenciákról tanultak szerint nem nehéz látni, hogy ily módon egy csoportot definiáltunk.

A lineáris kongruenciákról tanultak szerint nem nehéz látni, hogy ily módon egy csoportot definiáltunk. Ha $a, b \in \mathbf{Z}_p^*$, akkor $p \not| \; ab$ miatt létezik

A lineáris kongruenciákról tanultak szerint nem nehéz látni, hogy ily módon egy csoportot definiáltunk. Ha $a, b \in \mathbf{Z}_p^*$, akkor $p \not| ab$ miatt létezik és nyilván pontosan egy $c \in \mathbf{Z}_p^*$ hogy $ab \equiv c \pmod p$. Az $1 \in \mathbf{Z}_p^*$ egységelem. Ha $a \in \mathbf{Z}_p^*$, akkor az $ax \equiv 1 \pmod p$ lineáris kongruencia megoldhatósága miatt a-nak van inverze $\mathbf{Z}_p^*$-ben (hiszen választhatunk egy x_0 megoldással kongruens $\mathbf{Z}_p^*$-beli elemet.

A lineáris kongruenciákról tanultak szerint nem nehéz látni, hogy ily módon egy csoportot definiáltunk. Ha $a, b \in \mathbf{Z}_p^*$, akkor $p \not| ab$ miatt létezik és nyilván pontosan egy $c \in \mathbf{Z}_p^*$ hogy $ab \equiv c \pmod p$. Az $1 \in \mathbf{Z}_p^*$ egységelem. Ha $a \in \mathbf{Z}_p^*$, akkor az $ax \equiv 1 \pmod p$ lineáris kongruencia megoldhatósága miatt a-nak van inverze $\mathbf{Z}_p^*$-ben (hiszen választhatunk egy x_0 megoldással kongruens $\mathbf{Z}_p^*$-beli elemet. Az asszociativitás is könnyen adódik a kongruencia tulajdonságaiból (de itt nem részletezzük).

A lineáris kongruenciákról tanultak szerint nem nehéz látni, hogy ily módon egy csoportot definiáltunk. Ha $a, b \in \mathbf{Z}_p^*$, akkor $p \not| \, ab$ miatt létezik és nyilván pontosan egy $c \in \mathbf{Z}_p^*$ hogy $ab \equiv c \pmod p$. Az $1 \in \mathbf{Z}_p^*$ egységelem. Ha $a \in \mathbf{Z}_p^*$, akkor az $ax \equiv 1 \pmod p$ lineáris kongruencia megoldhatósága miatt a-nak van inverze $\mathbf{Z}_p^*$-ben (hiszen választhatunk egy x_0 megoldással kongruens $\mathbf{Z}_p^*$-beli elemet. Az asszociativitás is könnyen adódik a kongruencia tulajdonságaiból (de itt nem részletezzük).

Szokás a $(\mathbf{Z}_p^*; \cdot)$ csoportot a **modulo p redukált maradékosztályok multiplikatív csoportjának** nevezni.

Mármost az $(R_p; \cdot)$ csoportban minden elem rendje osztja $|R_p| = p - 1$ -et.

Mármost az $(R_p;\cdot)$ csoportban minden elem rendje osztja $|R_p| = p-1$ -et. Ezért bármely $b \in R_p$-re $b^{p-1} = 1$ teljesül R_b-ben.

Mármost az $(R_p;\cdot)$ csoportban minden elem rendje osztja $|R_p| = p-1$ -et. Ezért bármely $b \in R_p$-re $b^{p-1} = 1$ teljesül R_b-ben. Ha $a \in \mathbf{Z}$ olyan szám, amelyre $p \not| \ a$, akkor van olyan $b \in R_p$, hogy $a \equiv b \pmod p$.

Mármost az $(R_p;\cdot)$ csoportban minden elem rendje osztja $|R_p| = p-1$ -et. Ezért bármely $b \in R_p$-re $b^{p-1} = 1$ teljesül R_b-ben. Ha $a \in \mathbf{Z}$ olyan szám, amelyre $p \not| \; a$, akkor van olyan $b \in R_p$, hogy $a \equiv b \pmod p$. Erre a b-re is a $b^{p-1} = 1$, és —

Mármost az $(R_p;\cdot)$ csoportban minden elem rendje osztja $|R_p| = p-1$ -et. Ezért bármely $b \in R_p$-re $b^{p-1} = 1$ teljesül R_b-ben. Ha $a \in \mathbf{Z}$ olyan szám, amelyre $p \nmid a$, akkor van olyan $b \in R_p$, hogy $a \equiv b \pmod p$. Erre a b-re is a $b^{p-1} = 1$, és — figyelembe véve az R_p definícióját és a modulo (p) kongruencia tulajdonságait — innen $a^{p-1} \equiv 1 \pmod p$ következik.

Mármost az $(R_p;\cdot)$ csoportban minden elem rendje osztja $|R_p| = p-1$ -et. Ezért bármely $b \in R_p$-re $b^{p-1} = 1$ teljesül R_b-ben. Ha $a \in \mathbf{Z}$ olyan szám, amelyre $p \not| \, a$, akkor van olyan $b \in R_p$, hogy $a \equiv b \pmod p$. Erre a b-re is a $b^{p-1} = 1$, és — figyelembe véve az R_p definícióját és a modulo (p) kongruencia tulajdonságait — innen $a^{p-1} \equiv 1 \pmod p$ következik. Q.e.d.

Mármost az $(R_p;\cdot)$ csoportban minden elem rendje osztja $|R_p| = p-1$ -et. Ezért bármely $b \in R_p$-re $b^{p-1} = 1$ teljesül R_b-ben. Ha $a \in \mathbf{Z}$ olyan szám, amelyre $p \not| \, a$, akkor van olyan $b \in R_p$, hogy $a \equiv b \pmod{p}$. Erre a b-re is a $b^{p-1} = 1$, és — figyelembe véve az R_p definícióját és a modulo (p) kongruencia tulajdonságait — innen $a^{p-1} \equiv 1 \pmod{p}$ következik. Q.e.d.

A ciklikus csoportoknak és a kis-Fermat-tételnek fontos szerep jut a titkosírások elméletében.

Definíció: A $G = (G, \cdot)$ csoport egy N részcsoportját **normális részcsoportnak** vagy más néven **normálosztónak** nevezzük, ha bármely $a \in G$ elemre $aN = Na$.

Definíció: A $G = (G, \cdot)$ csoport egy N részcsoportját **normális részcsoportnak** vagy más néven **normálosztónak** nevezzük, ha bármely $a \in G$ elemre $aN = Na$. (Azaz, ha az N által indukált baloldali osztályozás megegyezik az általa indukált jobboldali osztályozással.) **Jelölje** $N \lhd G$ azt, hogy N normálosztója a G csoportnak.)

Definíció: A $G = (G, \cdot)$ csoport egy N részcsoportját **normális részcsoportnak** vagy más néven **normálosztónak** nevezzük, ha bármely $a \in G$ elemre $aN = Na$. (Azaz, ha az N által indukált baloldali osztályozás megegyezik az általa indukált jobboldali osztályozással.) **Jelölje** $N \triangleleft G$ azt, hogy N normálosztója a G csoportnak.)

13. Állítás. *Legyen N részcsoportja a $G = (G, \cdot)$ csoportnak. N akkor és csak akkor normálosztó, ha bármely $g \in G$-re*

$$g^{-1}Ng \subseteq N.$$

(

Definíció: A $G = (G, \cdot)$ csoport egy N részcsoportját **normális részcsoportnak** vagy más néven **normálosztónak** nevezzük, ha bármely $a \in G$ elemre $aN = Na$. (Azaz, ha az N által indukált baloldali osztályozás megegyezik az általala indukált jobboldali osztályozással.) **Jelölje** $N \lhd G$ azt, hogy N normálosztója a G csoportnak.)

13. Állítás. *Legyen N részcsoportja a $G = (G, \cdot)$ csoportnak. N akkor és csak akkor normálosztó, ha bármely $g \in G$-re*

$$g^{-1}Ng \subseteq N.$$

(Itt természetesen $g^{-1}Ng$ a

Definíció: A $G = (G, \cdot)$ csoport egy N részcsoportját **normális részcsoportnak** vagy más néven **normálosztónak** nevezzük, ha bármely $a \in G$ elemre $aN = Na$. (Azaz, ha az N által indukált baloldali osztályozás megegyezik az általa indukált jobboldali osztályozással.) **Jelölje** $N \lhd G$ azt, hogy N normálosztója a G csoportnak.)

13. Állítás. *Legyen N részcsoportja a $G = (G, \cdot)$ csoportnak. N akkor és csak akkor normálosztó, ha bármely $g \in G$-re*

$$g^{-1}Ng \subseteq N.$$

(Itt természetesen $g^{-1}Ng$ a $\{g^{-1}xg : x \in N\}$ halmazt jelöli.)

Bizonyítás: Formálisan egyszerűnek tűnik:

Bizonyítás: Formálisan egyszerűnek tűnik: ha

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng =$

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$.

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor $Ng \subseteq gN$.

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor $Ng \subseteq gN$. Ha pedig jobbról g^{-1}-gyel szorunk át, akkor $g^{-1}N \subseteq Ng^{-1}$. De ez minden g-re fennáll, tehát akkor is, ha g helyére g^{-1}-et írunk: $gN \subseteq Ng$.

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor $Ng \subseteq gN$. Ha pedig jobbról g^{-1}-gyel szorunk át, akkor $g^{-1}N \subseteq Ng^{-1}$. De ez minden g-re fennáll, tehát akkor is, ha g helyére g^{-1}-et írunk: $gN \subseteq Ng$. Az eddigiek szerint bármely g-re $gN = Ng$, azaz N normálosztó.

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor $Ng \subseteq gN$. Ha pedig jobbról g^{-1}-gyel szorunk át, akkor $g^{-1}N \subseteq Ng^{-1}$. De ez minden g-re fennáll, tehát akkor is, ha g helyére g^{-1}-et írunk: $gN \subseteq Ng$. Az eddigiek szerint bármely g-re $gN = Ng$, azaz N normálosztó. Q.e.d.

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor $Ng \subseteq gN$. Ha pedig jobbról g^{-1}-gyel szorunk át, akkor $g^{-1}N \subseteq Ng^{-1}$. De ez minden g-re fennáll, tehát akkor is, ha g helyére g^{-1}-et írunk: $gN \subseteq Ng$. Az eddigiek szerint bármely g-re $gN = Ng$, azaz N normálosztó. Q.e.d.

A precíz bizonyítás azért ennél többet kíván: meg kellene (és meg is lehetne) mutatni, hogy amikor egy szorzatban elemek és halmazok is vannak, akkor is érvényes az asszociativitás. (

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor $Ng \subseteq gN$. Ha pedig jobbról g^{-1}-gyel szorunk át, akkor $g^{-1}N \subseteq Ng^{-1}$. De ez minden g-re fennáll, tehát akkor is, ha g helyére g^{-1}-et írunk: $gN \subseteq Ng$. Az eddigiek szerint bármely g-re $gN = Ng$, azaz N normálosztó. Q.e.d.

A precíz bizonyítás azért ennél többet kíván: meg kellene (és meg is lehetne) mutatni, hogy amikor egy szorzatban elemek és halmazok is vannak, akkor is érvényes az asszociativitás. (Ezt a fontos tényt nemcsak lila színnel mindjárt ki is hangsúlyozzuk.)

Bizonyítás: Formálisan egyszerűnek tűnik: ha N normálosztó, akkor $Ng = gN$, és így $g^{-1}Ng = g^{-1}gN = 1N = N \subseteq N$. Ha pedig bármely g-re $g^{-1}Ng \subseteq N$, akkor ha balról g-vel átszorzunk, akkor $Ng \subseteq gN$. Ha pedig jobbról g^{-1}-gyel szorunk át, akkor $g^{-1}N \subseteq Ng^{-1}$. De ez minden g-re fennáll, tehát akkor is, ha g helyére g^{-1}-et írunk: $gN \subseteq Ng$. Az eddigiek szerint bármely g-re $gN = Ng$, azaz N normálosztó. Q.e.d.

A precíz bizonyítás azért ennél többet kíván: meg kellene (és meg is lehetne) mutatni, hogy amikor egy szorzatban elemek és halmazok is vannak, akkor is érvényes az asszociativitás. (Ezt a fontos tényt nemcsak lila színnel mindjárt ki is hangsúlyozzuk.) Q.e.d.

Egy G csoport (vagy félcsoport) részhalmazait — amennyiben számolni akarunk velük, pl. így:

$$XY =$$

Egy G csoport (vagy félcsoport) részhalmazait — amennyiben számolni akarunk velük, pl. így:

$$XY = \{xy : x \in X,\ y \in Y\},$$

Egy G csoport (vagy félcsoport) részhalmazait — amennyiben számolni akarunk velük, pl. így:

$$XY = \{xy : x \in X,\ y \in Y\}, \qquad X^{-1} = \{x^{-1} : x \in X\},$$

Egy G csoport (vagy félcsoport) részhalmazait — amennyiben számolni akarunk velük, pl. így:

$$XY = \{xy : x \in X,\ y \in Y\}, \qquad X^{-1} = \{x^{-1} : x \in X\},$$

akkor **komplexusoknak** is szoktuk nevezni.

Egy G csoport (vagy félcsoport) részhalmazait — amennyiben számolni akarunk velük, pl. így:

$$XY = \{xy : x \in X,\ y \in Y\}, \qquad X^{-1} = \{x^{-1} : x \in X\},$$

akkor **komplexusoknak** is szoktuk nevezni. Tehát a komplexusok számolás céljára (is) használt részhalmazok, és a fenti képletben szereplő szorzást **komplexusszorzásnak** nevezzük.

Egy G csoport (vagy félcsoport) részhalmazait — amennyiben számolni akarunk velük, pl. így:

$$XY = \{xy : x \in X,\ y \in Y\}, \qquad X^{-1} = \{x^{-1} : x \in X\},$$

akkor **komplexusoknak** is szoktuk nevezni. Tehát a komplexusok számolás céljára (is) használt részhalmazok, és a fenti képletben szereplő szorzást **komplexusszorzásnak** nevezzük. Egyszerű gyakorló feladat lenne annak igazolása, hogy

14. Állítás. *Félcsoportok esetén a komplexusszorzás asszociatív művelet.*

Tehát ha $(S; \cdot)$ félcsoport, akkor $(P(S); \cdot)$

Tehát ha $(S;\cdot)$ félcsoport, akkor $(P(S);\cdot)$ — ahol a szorzás a komplexusszorzást jelenti — szintén félcsoport.

Tehát ha $(S; \cdot)$ félcsoport, akkor $(P(S); \cdot)$ — ahol a szorzás a komplexusszorzást jelenti — szintén félcsoport. Csoport komplexusaira az is érvényes, hogy

Tehát ha $(S;\cdot)$ félcsoport, akkor $(P(S);\cdot)$ — ahol a szorzás a komplexusszorzást jelenti — szintén félcsoport. Csoport komplexusaira az is érvényes, hogy

$$(XY)^{-1} = Y^{-1}X^{-1},$$

de a komplexusműveleteknek az egységelemhez csak annyi köze van, hogy nemüres X esetén $1 \in XX^{-1}$ és $1 \in X^{-1}X$.

Tehát ha $(S;\cdot)$ félcsoport, akkor $(P(S);\cdot)$ — ahol a szorzás a komplexusszorzást jelenti — szintén félcsoport. Csoport komplexusaira az is érvényes, hogy

$$(XY)^{-1} = Y^{-1}X^{-1},$$

de a komplexusműveleteknek az egységelemhez csak annyi köze van, hogy nemüres X esetén $1 \in XX^{-1}$ és $1 \in X^{-1}X$. Azt viszont **nem állíthatjuk**, hogy $XX^{-1} = 1$ —

Tehát ha $(S;\cdot)$ félcsoport, akkor $(P(S);\cdot)$ — ahol a szorzás a komplexusszorzást jelenti — szintén félcsoport. Csoport komplexusaira az is érvényes, hogy

$$(XY)^{-1} = Y^{-1}X^{-1},$$

de a komplexusműveleteknek az egységelemhez csak annyi köze van, hogy nemüres X esetén $1 \in XX^{-1}$ és $1 \in X^{-1}X$. Azt viszont **nem állíthatjuk**, hogy $XX^{-1} = 1$ — ennek nem is lenne értelme, hiszen egy halmaz (komplexus) hogyan is lehetne egyenlő egy elemével —,

Tehát ha $(S;\cdot)$ félcsoport, akkor $(P(S);\cdot)$ — ahol a szorzás a komplexusszorzást jelenti — szintén félcsoport. Csoport komplexusaira az is érvényes, hogy

$$(XY)^{-1} = Y^{-1}X^{-1},$$

de a komplexusműveleteknek az egységelemhez csak annyi köze van, hogy nemüres X esetén $1 \in XX^{-1}$ és $1 \in X^{-1}X$. Azt viszont **nem állíthatjuk**, hogy $XX^{-1} = 1$ — ennek nem is lenne értelme, hiszen egy halmaz (komplexus) hogyan is lehetne egyenlő egy elemével —, de még azt sem állíthatjuk általában, hogy $XX^{-1} = \{1\}$.)

Adott $a \in G$ esetén a $g^{-1}ag$ $(g \in G)$ alakú elemeket az a elem **konjugáltjainak** nevezzük.

Adott $a \in G$ esetén a $g^{-1}ag$ $(g \in G)$ alakú elemeket az a elem **konjugáltjainak** nevezzük. Ha G kommutatív, akkor természetesen $g^{-1}ag = ag^{-1}g = a \cdot 1 = a$, tehát

Adott $a \in G$ esetén a $g^{-1}ag$ $(g \in G)$ alakú elemeket az a elem **konjugáltjainak** nevezzük. Ha G kommutatív, akkor természetesen $g^{-1}ag = ag^{-1}g = a \cdot 1 = a$, tehát ebben az esetben a-nak csak egyetlen konjugáltja van: önmaga.

Adott $a \in G$ esetén a $g^{-1}ag$ $(g \in G)$ alakú elemeket az a elem **konjugáltjainak** nevezzük. Ha G kommutatív, akkor természetesen $g^{-1}ag = ag^{-1}g = a \cdot 1 = a$, tehát ebben az esetben a-nak csak egyetlen konjugáltja van: önmaga. Mellesleg g-vel való átszorzás útján kapjuk, hogy $g^{-1}ag = a$ pontosan akkor, ha $ag = ga$.

Adott $a \in G$ esetén a $g^{-1}ag$ $(g \in G)$ alakú elemeket az a elem **konjugáltjainak** nevezzük. Ha G kommutatív, akkor természetesen $g^{-1}ag = ag^{-1}g = a \cdot 1 = a$, tehát ebben az esetben a-nak csak egyetlen konjugáltja van: önmaga. Mellesleg g-vel való átszorzás útján kapjuk, hogy $g^{-1}ag = a$ pontosan akkor, ha $ag = ga$.

Az előző állítás úgy is fogalmazható, hogy **egy részcsoport akkor és csak akkor normálosztó, ha zárt a konjugálásra**, azaz ha a eleme, akkor a-nak minden $g^{-1}ag$ konjugáltja is eleme.

Adott $a \in G$ esetén a $g^{-1}ag$ $(g \in G)$ alakú elemeket az a elem **konjugáltjainak** nevezzük. Ha G kommutatív, akkor természetesen $g^{-1}ag = ag^{-1}g = a \cdot 1 = a$, tehát ebben az esetben a-nak csak egyetlen konjugáltja van: önmaga. Mellesleg g-vel való átszorzás útján kapjuk, hogy $g^{-1}ag = a$ pontosan akkor, ha $ag = ga$.

Az előző állítás úgy is fogalmazható, hogy **egy részcsoport akkor és csak akkor normálosztó, ha zárt a konjugálásra**, azaz ha a eleme, akkor a-nak minden $g^{-1}ag$ konjugáltja is eleme. Abel-csoport esetén minden részcsoport normálosztó.

Példa: Legyen (

Példa: Legyen (ismét

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható:

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) =$$

Példa: Legyen (ismét) S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1$$

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3$$

Példa: Legyen (ismét) S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\text{id}, (12)\}$ és $N = \{\text{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) =$$

Példa: Legyen (ismét) S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id},(12)\}$ és $N = \{\mathrm{id},(123),(132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = ($$

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = (2$$

Példa: Legyen (ismét) S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = (2\,3) \notin H.$$

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = (2\,3) \notin H.$$

Most vizsgáljuk meg, hogy N normálosztó-e.

Példa: Legyen (ismét) S_3 az $\{1, 2, 3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = (2\,3) \notin H.$$

Most vizsgáljuk meg, hogy N normálosztó-e. Látható, hogy részcsoport. Legyen

Példa: Legyen (ismét) S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = (2\,3) \notin H.$$

Most vizsgáljuk meg, hogy N normálosztó-e. Látható, hogy részcsoport. Legyen $a \in N$. Ha $g \in N$, akkor

Példa: Legyen (ismét) S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id}, (12)\}$ és $N = \{\mathrm{id}, (123), (132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = (2\,3) \notin H.$$

Most vizsgáljuk meg, hogy N normálosztó-e. Látható, hogy részcsoport. Legyen $a \in N$. Ha $g \in N$, akkor természetesen $g^{-1}ag \in N$, hiszen N zárt az inverzképzésre és a szorzásra.

Példa: Legyen (ismét) S_3 az $\{1,2,3\}$ halmazon ható permutációk csoportja. Legyen $H = \{\mathrm{id},(12)\}$ és $N = \{\mathrm{id},(123),(132)\}$. Ekkor — amint azt korábban láttuk — H nem normálosztó, hiszen a baloldali mellékosztályai nem ugyanazok, mint a jobboldaliak. De ez egyszerűbben is látható: $(1\,2) \in H$, de

$$(1\,2\,3)^{-1}(1\,2)(1\,2\,3) = (1\,3\,2)(1\,2)(1\,2\,3) = (2\,3) \notin H.$$

Most vizsgáljuk meg, hogy N normálosztó-e. Látható, hogy részcsoport. Legyen $a \in N$. Ha $g \in N$, akkor természetesen $g^{-1}ag \in N$, hiszen N zárt az inverzképzésre és a szorzásra. Ha $a = 1 = \mathrm{id}$, akkor $g^{-1}ag = g^{-1}g = \mathrm{id} \in N$ úgyszintén.

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} =$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is.

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) =$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$\begin{aligned}
&(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,\\
&(1\,3)(1\,2\,3)(1\,3) =
\end{aligned}$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,$$
$$(1\,3)(1\,2\,3)(1\,3) = (1$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,$$
$$(1\,3)(1\,2\,3)(1\,3) = (1\,3$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,$$
$$(1\,3)(1\,2\,3)(1\,3) = (1\,3\,2) \in N,$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$\begin{aligned}
&(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,\\
&(1\,3)(1\,2\,3)(1\,3) = (1\,3\,2) \in N,\\
&(2\,3)(1\,2\,3)(2\,3)
\end{aligned}$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$
\begin{aligned}
(1\,2)(1\,2\,3)(1\,2) &= (1\,3\,2) \in N,\\
(1\,3)(1\,2\,3)(1\,3) &= (1\,3\,2) \in N,\\
(2\,3)(1\,2\,3)(2\,3) &= (1
\end{aligned}
$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,$$
$$(1\,3)(1\,2\,3)(1\,3) = (1\,3\,2) \in N,$$
$$(2\,3)(1\,2\,3)(2\,3) = (1\,3$$

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$\begin{aligned}
(1\,2)(1\,2\,3)(1\,2) &= (1\,3\,2) \in N,\\
(1\,3)(1\,2\,3)(1\,3) &= (1\,3\,2) \in N,\\
(2\,3)(1\,2\,3)(2\,3) &= (1\,3\,2) \in N.
\end{aligned}$$

Tehát N normálosztó.

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$(1\,2)(1\,2\,3)(1\,2) = (1\,3\,2) \in N,$$
$$(1\,3)(1\,2\,3)(1\,3) = (1\,3\,2) \in N,$$
$$(2\,3)(1\,2\,3)(2\,3) = (1\,3\,2) \in N.$$

Tehát N normálosztó.

A példa kapcsán oly nagy munkával ritkítottuk a vizsgálandó esetek számát,

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$\begin{aligned}
(1\,2)(1\,2\,3)(1\,2) &= (1\,3\,2) \in N,\\
(1\,3)(1\,2\,3)(1\,3) &= (1\,3\,2) \in N,\\
(2\,3)(1\,2\,3)(2\,3) &= (1\,3\,2) \in N.
\end{aligned}$$

Tehát N normálosztó.

A példa kapcsán oly nagy munkával ritkítottuk a vizsgálandó esetek számát, hogy annyi idő alatt meg is lehetett volna vizsgálni azokat.

Észrevehetjük még azt is, hogy $(g^{-1}ag)^{-1} = g^{-1}a^{-1}g$, tehát ha a összes konjugáltja N-beli, akkor ugyanez érvényes az inverzére is. Mivel $(1\,2\,3)^{-1} = (1\,3\,2)$, az eddigiek szerint elegendő azon eseteket vizsgálnunk, amikor $a = (1\,2\,3)$ és $g \notin N$ (ilyenkor — legalábbis most — $g^{-1} = g$):

$$\begin{aligned}
(1\,2)(1\,2\,3)(1\,2) &= (1\,3\,2) \in N,\\
(1\,3)(1\,2\,3)(1\,3) &= (1\,3\,2) \in N,\\
(2\,3)(1\,2\,3)(2\,3) &= (1\,3\,2) \in N.
\end{aligned}$$

Tehát N normálosztó.

A példa kapcsán oly nagy munkával ritkítottuk a vizsgálandó esetek számát, hogy annyi idő alatt meg is lehetett volna vizsgálni azokat. Érdekes, hogy van olyan megoldás, amelynek során semmit sem kell számolni:

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály,

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő,

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik.

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak.

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak. Q.e.d.

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak. Q.e.d.

Az előző példára visszatérve (és a Lagrange-tételt is használva)

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak. Q.e.d.

Az előző példára visszatérve (és a Lagrange-tételt is használva):

$[S_3 : N] =$

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak. Q.e.d.

Az előző példára visszatérve (és a Lagrange-tételt is használva):

$$[S_3 : N] = \frac{|S_3|}{|N|} =$$

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak. Q.e.d.

Az előző példára visszatérve (és a Lagrange-tételt is használva):
$[S_3 : N] = \frac{|S_3|}{|N|} = \frac{6}{3} = 2$,

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak. Q.e.d.

Az előző példára visszatérve (és a Lagrange-tételt is használva): $[S_3 : N] = \frac{|S_3|}{|N|} = \frac{6}{3} = 2$, tehát (

15. Állítás. *Bármely 2-indexű részcsoport normálosztó.*

Bizonyítás: Legyen H részcsoportja a G csoportnak és $[G : H] = 2$. Ekkor (az index jelentése miatt) kettő darab H szerinti mellékosztály van: H (amely mindig baloldali mellékosztály, t.i. az 1 osztálya: $H = 1H$) és $G \setminus H$.

De ugyanez mondható el a jobboldali mellékosztályokról: azok száma is kettő, $H = H1$ az egyik, és — mivel más lehetőség nem marad — $G \setminus H$ a másik. Tehát ugyanazok a baloldali mellékosztályok, mint a jobboldaliak. Q.e.d.

Az előző példára visszatérve (és a Lagrange-tételt is használva): $[S_3 : N] = \frac{|S_3|}{|N|} = \frac{6}{3} = 2$, tehát (minden további számolás nélkül) N normálosztó.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \lhd G$.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \triangleleft G$.

Valóban, a síkon $N = \{a \in G : a \text{ forgásiránytartó}\}$.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \lhd G$.

Valóban, a síkon $N = \{a \in G : a \text{ forgásiránytartó}\}$. Azt is vegyük észre, hogy g pontosan akkor forgásiránytartó (azaz N-beli), ha inverze is az.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \triangleleft G$.

Valóban, a síkon $N = \{a \in G : a \text{ forgásiránytartó}\}$. Azt is vegyük észre, hogy g pontosan akkor forgásiránytartó (azaz N-beli), ha inverze is az. Mivel $\mathrm{id} \in N$, az eddigiek szerint N részcsoport.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \triangleleft G$.

Valóban, a síkon $N = \{a \in G : a \text{ forgásiránytartó}\}$. Azt is vegyük észre, hogy g pontosan akkor forgásiránytartó (azaz N-beli), ha inverze is az. Mivel id $\in N$, az eddigiek szerint N részcsoport. Legyen most $a \in N$ tetszőleges.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \triangleleft G$.

Valóban, a síkon $N = \{a \in G : a \text{ forgásiránytartó}\}$. Azt is vegyük észre, hogy g pontosan akkor forgásiránytartó (azaz N-beli), ha inverze is az. Mivel id $\in N$, az eddigiek szerint N részcsoport. Legyen most $a \in N$ tetszőleges. Ha g is N-beli, akkor $g^{-1}ag$ —

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \triangleleft G$.

Valóban, a síkon $N = \{a \in G : a$ forgásiránytartó$\}$. Azt is vegyük észre, hogy g pontosan akkor forgásiránytartó (azaz N-beli), ha inverze is az. Mivel id $\in N$, az eddigiek szerint N részcsoport. Legyen most $a \in N$ tetszőleges. Ha g is N-beli, akkor $g^{-1}ag$ — mint három forgásiránytartó transzformáció szorzata — szintén forgásiránytartó, tehát N-beli.

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \triangleleft G$.

Valóban, a síkon $N = \{a \in G : a$ forgásiránytartó$\}$. Azt is vegyük észre, hogy g pontosan akkor forgásiránytartó (azaz N-beli), ha inverze is az. Mivel id $\in N$, az eddigiek szerint N részcsoport. Legyen most $a \in N$ tetszőleges. Ármost ha g is N-beli, akkor $g^{-1}ag$ — mint három forgásiránytartó transzformáció szorzata — szintén forgásiránytartó, tehát N-beli. Ha pedig $g \in G \setminus N$, akkor $g^{-1}ag$ azért lesz forgásiránytartó (azaz N-beli),

Példa: Legyen K egy síkidom vagy térbeli test. Jelölje G a K szimmetriacsoportját (tehát a K-t önmagára képező egybevágósági transzformációk csoportját a síkon, illetve a térben.) Legyen N a K mozgáscsoportja. Ekkor $N \triangleleft G$.

Valóban, a síkon $N = \{a \in G : a \text{ forgásiránytartó}\}$. Azt is vegyük észre, hogy g pontosan akkor forgásiránytartó (azaz N-beli), ha inverze is az. Mivel id $\in N$, az eddigiek szerint N részcsoport. Legyen most $a \in N$ tetszőleges. Mármost ha g is N-beli, akkor $g^{-1}ag$ — mint három forgásiránytartó transzformáció szorzata — szintén forgásiránytartó, tehát N-beli. Ha pedig $g \in G \setminus N$, akkor $g^{-1}ag$ azért lesz forgásiránytartó (azaz N-beli), mert a három egymás után végrehajtandó transzformáció közül pontosan kettő változtatja ellenkezőjére a forgásirányt.

Térben a megfontolás hasonló, csak ott forgásirány helyett

Térben a megfontolás hasonló, csak ott forgásirány helyett jobb-, illetve balsodrású rendszert kell mondanunk. (Vagy azt, hogy a balkezünket átviszi-e a jobbkezünkbe a tekintett transzformáció.)

Faktorcsoport

Definíció: Legyen G csoport és $N \lhd G$. Ekkor a

$$G/N = (\{aN : a \in G\}; \cdot)$$

grupoidot, ahol

Faktorcsoport

Definíció: Legyen G csoport és $N \triangleleft G$. Ekkor a

$$G/N = (\{aN : a \in G\}; \cdot)$$

grupoidot, ahol

$$(aN)(bN) :=$$

Faktorcsoport

Definíció: Legyen G csoport és $N \lhd G$. Ekkor a

$$G/N = (\{aN : a \in G\}; \cdot)$$

grupoidot, ahol

$$(aN)(bN) := (ab)N\,,$$

a G csoportnak az N normálosztó szerinti **faktorcsoportjának** nevezzük.

Faktorcsoport

Definíció: Legyen G csoport és $N \lhd G$. Ekkor a

$$G/N = (\{aN : a \in G\}; \cdot)$$

grupoidot, ahol

$$(aN)(bN) := (ab)N\,,$$

a G csoportnak az N normálosztó szerinti **faktorcsoportjának** nevezzük. Tehát a faktorcsoport az N szerinti mellékosztályokból áll (

Faktorcsoport

Definíció: Legyen G csoport és $N \lhd G$. Ekkor a

$$G/N = (\{aN : a \in G\}; \cdot)$$

grupoidot, ahol

$$(aN)(bN) := (ab)N\,,$$

a G csoportnak az N normálosztó szerinti **faktorcsoportjának** nevezzük. Tehát a faktorcsoport az N szerinti mellékosztályokból áll (mivel az N normálosztó, mindegy, hogy jobb- vagy baloldali mellékosztályokat tekintünk) és a műveletet a **reprezentánsokon** végezzük.

63. Tétel. *(1) A faktorcsoport tényleg csoport.*

63. Tétel. *(1) A faktorcsoport tényleg csoport.*

(2) A faktorcsoportbeli szorzás művelete éppen a komplexus-szorzás.

63. Tétel. *(1) A faktorcsoport tényleg csoport.*

(2) A faktorcsoportbeli szorzás művelete éppen a komplexus-szorzás.

Bizonyítás: A legfőbb teendő annak a kimutatása, hogy G/N grupoid, azaz hogy a művelet jóldefiniált!

63. Tétel. *(1) A faktorcsoport tényleg csoport.*

(2) A faktorcsoportbeli szorzás művelete éppen a komplexus-szorzás.

Bizonyítás: A legfőbb teendő annak a kimutatása, hogy G/N grupoid, azaz hogy a művelet jóldefiniált!

Ugyanis mi a mellékosztályok halmazán definiáltunk egy szorzást oly módonk, hogy tetszés szerinti a, b

63. Tétel. *(1) A faktorcsoport tényleg csoport.*

(2) A faktorcsoportbeli szorzás művelete éppen a komplexus-szorzás.

Bizonyítás: A legfőbb teendő annak a kimutatása, hogy G/N grupoid, azaz hogy a művelet jóldefiniált!

Ugyanis mi a mellékosztályok halmazán definiáltunk egy szorzást oly módonk, hogy tetszés szerinti a, b ún. reprezentánsokon végezzük a műveletet, majd az így kapott elem mellékosztályát tekintjük.

63. Tétel. *(1) A faktorcsoport tényleg csoport.*

(2) A faktorcsoportbeli szorzás művelete éppen a komplexus-szorzás.

Bizonyítás: A legfőbb teendő annak a kimutatása, hogy G/N grupoid, azaz hogy a művelet jóldefiniált!

Ugyanis mi a mellékosztályok halmazán definiáltunk egy szorzást oly módonk, hogy tetszés szerinti a, b ún. reprezentánsokon végezzük a műveletet, majd az így kapott elem mellékosztályát tekintjük. Igen ám, de megeshetne, hogy

$$a_1N = b_1N, \quad a_2N = b_2N, \quad \text{de} \quad (a_1b_1)N \neq (a_2b_2)N,$$

és akkor a műveletre adott definíciónk értelmetlen lenne, azaz nem definiálna műveletet!

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N,$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N,$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$

$$(\mathrm{id} \cdot (1\,3))N =$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$
$$(\mathrm{id} \cdot (1\,3))N = (1\,3)N =$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$
$$(\mathrm{id} \cdot (1\,3))N = (1\,3)N = \{(1\,3), (1\,3\,2)\}$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$

$$(\mathrm{id} \cdot (1\,3))N = (1\,3)N = \{(1\,3), (1\,3\,2)\}$$

$$\neq$$

$$\{(2\,3), (1\,2\,3)\}$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$

$$(\mathrm{id} \cdot (1\,3))N = (1\,3)N = \{(1\,3), (1\,3\,2)\}$$

$$\neq$$

$$\{(2\,3), (1\,2\,3)\} = (2\,3)N =$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$

$$(\mathrm{id} \cdot (1\,3))N = (1\,3)N = \{(1\,3), (1\,3\,2)\}$$

$$\neq$$

$$\{(2\,3), (1\,2\,3)\} = (2\,3)N = ((1\,2) \cdot (1\,3\,2))N.$$

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\text{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\text{id}\,N = (1\,2)\,N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$

$$(\text{id} \cdot (1\,3))N = (1\,3)N = \{(1\,3), (1\,3\,2)\}$$

$$\neq$$

$$\{(2\,3), (1\,2\,3)\} = (2\,3)N = ((1\,2) \cdot (1\,3\,2))N.$$

Itt viszont N nem normálosztó!

Hogy ez a veszély valóban fennáll, arra példa az alábbi: $G = S_3$, $N = \{\mathrm{id}, (12)\}$. Ekkor (egy korábbi példához visszalapozva vagy újból kiszámolva) a piros, illetve a kék színű reprezentánsokat választva

$$\mathrm{id}\, N = (1\,2)\, N, \qquad (1\,3)N = (1\,3\,2)N, \quad \text{de ennek ellenére}$$

$$(\mathrm{id} \cdot (1\,3))N = (1\,3)N = \{(1\,3), (1\,3\,2)\}$$
$$\neq$$
$$\{(2\,3), (1\,2\,3)\} = (2\,3)N = ((1\,2) \cdot (1\,3\,2))N.$$

Itt viszont N nem normálosztó! Ezért kellett a tételben kikötni, hogy N normálosztó legyen!

Ahhoz, hogy kimutassuk, hogy a művelet $(aN)(bN) := (ab)N$ definíciója (azaz a mellékosztály reprezentánsaival megadott definíció) korrekt, nyilván elég belátni a tétel (2) pontját, hiszen a komplexusművelet korrektségéhez nem férhet kétség.

Legyen $C = (aN) \cdot (bN) =$

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$.

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$.

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$.

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért van olyan $n_3 \in N$, hogy

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért van olyan $n_3 \in N$, hogy $n_1b =$

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért van olyan $n_3 \in N$, hogy $n_1b = bn_3$ alakú.

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért van olyan $n_3 \in N$, hogy $n_1b = bn_3$ alakú. Az eddigiek szerint $u = an_1bn_2 =$

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért van olyan $n_3 \in N$, hogy $n_1b = bn_3$ alakú. Az eddigiek szerint $u = an_1bn_2 = abn_3n_2 = (ab)(n_3n_2)$

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért van olyan $n_3 \in N$, hogy $n_1b = bn_3$ alakú. Az eddigiek szerint $u = an_1bn_2 = abn_3n_2 = (ab)(n_3n_2) \in (ab)N$, hiszen (mivel N zárt szorzásra)

Legyen $C = (aN) \cdot (bN) = \{xy : x \in aN,\ y \in bN\}$ a komplexus-szorzás eredménye; azt kell belátni, hogy

$$C \stackrel{?}{=} (ab)N$$

Ha $u \in C$, akkor $u = xy$ alakú, ahol $x \in aN$ és $y \in bN$. Tehát $x = an_1$ és $y = bn_2$ alakú, ahol $n_1, n_2 \in N$. Ekkor $u = xy = an_1bn_2$. Mármost $n_1b \in Nb = bN$ (itt használjuk ki, hogy N nemcsak részcsoport, hanem normálosztó), ezért van olyan $n_3 \in N$, hogy $n_1b = bn_3$ alakú. Az eddigiek szerint $u = an_1bn_2 = abn_3n_2 = (ab)(n_3n_2) \in (ab)N$, hiszen (mivel N zárt szorzásra) $n_3n_2 \in N$. Ezért $C \subseteq (ab)N$ teljesül.

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x =$

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn$

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn)$

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$ és persze $bn \in bN$.

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$ és persze $bn \in bN$. Tehát $C \supseteq (ab)N$.

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$ és persze $bn \in bN$. Tehát $C \supseteq (ab)N$.

A bizonyítás további része már könnyű, csak

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$ és persze $bn \in bN$. Tehát $C \supseteq (ab)N$.

A bizonyítás további része már könnyű, csak azt kell hozzá észrevenni, hogy $NN = N$, hiszen $N = N\{1\} \subseteq NN$

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$ és persze $bn \in bN$. Tehát $C \supseteq (ab)N$.

A bizonyítás további része már könnyű, csak azt kell hozzá észrevenni, hogy $NN = N$, hiszen $N = N\{1\} \subseteq NN \subseteq N$.

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$ és persze $bn \in bN$. Tehát $C \supseteq (ab)N$.

A bizonyítás további része már könnyű, csak azt kell hozzá észrevenni, hogy $NN = N$, hiszen $N = N\{1\} \subseteq NN \subseteq N$. Így tetszőleges $a \in G$ elemre (

Fordítva, ha $x \in (ab)N$, akkor alkalmas $n \in N$ esetén $x = abn = (a \cdot 1)(bn) \in C$, hiszen $1 \in N$ miatt $a \cdot 1 \in aN$ és persze $bn \in bN$. Tehát $C \supseteq (ab)N$.

A bizonyítás további része már könnyű, csak azt kell hozzá észrevenni, hogy $NN = N$, hiszen $N = N\{1\} \subseteq NN \subseteq N$. Így tetszőleges $a \in G$ elemre (más szóval, a faktorcsoport tetszőleges aN elemére)

$$N(aN) =$$

$$N(aN) = (Na)N =$$

$$N(aN) = (Na)N = (aN)N =$$

$$N(aN) = (Na)N = (aN)N = a(NN) =$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$

$$(aN)N =$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$
$$(aN)N = a(NN) =$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$

$$(aN)N = a(NN) = aN,$$

$$(a^{-1}N)(aN) =$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$

$$(aN)N = a(NN) = aN,$$

$$(a^{-1}N)(aN) = (a^{-1}a)N =$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$

$$(aN)N = a(NN) = aN,$$

$$(a^{-1}N)(aN) = (a^{-1}a)N = 1N = N,$$

$$(aN)(a^{-1}N) =$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$

$$(aN)N = a(NN) = aN,$$

$$(a^{-1}N)(aN) = (a^{-1}a)N = 1N = N,$$

$$(aN)(a^{-1}N) = (aa^{-1})N =$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$
$$(aN)N = a(NN) = aN,$$
$$(a^{-1}N)(aN) = (a^{-1}a)N = 1N = N,$$
$$(aN)(a^{-1}N) = (aa^{-1})N = 1N = N.$$

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$
$$(aN)N = a(NN) = aN,$$
$$(a^{-1}N)(aN) = (a^{-1}a)N = 1N = N,$$
$$(aN)(a^{-1}N) = (aa^{-1})N = 1N = N.$$

Tehát (és jól jegyezzük meg) G/N **egységeleme az** $N = 1N$ **(azaz az egységelem mellékosztálya), és**

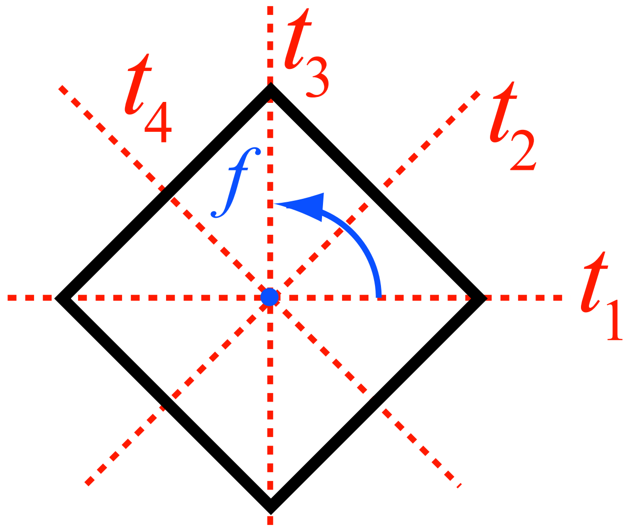
$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$
$$(aN)N = a(NN) = aN,$$
$$(a^{-1}N)(aN) = (a^{-1}a)N = 1N = N,$$
$$(aN)(a^{-1}N) = (aa^{-1})N = 1N = N.$$

Tehát (és jól jegyezzük meg) G/N **egységeleme az** $N = 1N$ **(azaz az egységelem mellékosztálya), és az** aN **mellékosztály inverze az** $a^{-1}N$ **mellékosztály.**

$$N(aN) = (Na)N = (aN)N = a(NN) = aN,$$
$$(aN)N = a(NN) = aN,$$
$$(a^{-1}N)(aN) = (a^{-1}a)N = 1N = N,$$
$$(aN)(a^{-1}N) = (aa^{-1})N = 1N = N.$$

Tehát (és jól jegyezzük meg) G/N **egységeleme az** $N = 1N$ **(azaz az egységelem mellékosztálya), és az** aN **mellékosztály inverze az** $a^{-1}N$ **mellékosztály.**
Q.e.d.

Példa: Legyen D_4 a négyzet szimmetriacsoportja, M_4 pedig a mozgáscsoportja. Ekkor $D_4 = \{t_1, t_2, t_3, t_4, f, f^2, f^3, f^4 = \text{id}\}$, ahol t_i az ábrán jelölt egyenesre való tükrözés, $f, f^2, f^3, f^4 = \text{id}$ pedig rendre a 90, 180, 270 és 360 fokos (pozitív irányba történő) elforgatás. (Elemi geometria $\Longrightarrow$ nincs több eleme.)



Ekkor $M_4 = \{f, f^2, f^3, f^4 = \text{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \dfrac{|D_4|}{|M_4|} = \dfrac{8}{4} = 2$, ezért $M_4 \triangleleft D_4$.

A

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \text{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \frac{|D_4|}{|M_4|} = \frac{8}{4} = 2$, ezért $M_4 \triangleleft D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll,

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \dfrac{|D_4|}{|M_4|} = \dfrac{8}{4} = 2$, ezért $M_4 \lhd D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4,

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \dfrac{|D_4|}{|M_4|} = \dfrac{8}{4} = 2$, ezért $M_4 \lhd D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján)

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \dfrac{|D_4|}{|M_4|} = \dfrac{8}{4} = 2$, ezért $M_4 \lhd D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján) $t_1 M_4 = D_4 \setminus M_4 = \{t_1, t_2, t_3, t_4\}$. A faktorcsoportban M_4 az egységelem.

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \frac{|D_4|}{|M_4|} = \frac{8}{4} = 2$, ezért $M_4 \triangleleft D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján) $t_1M_4 = D_4 \setminus M_4 = \{t_1, t_2, t_3, t_4\}$. A faktorcsoportban M_4 az egységelem. Mivel $t_1M_4 \cdot t_1M_4 =$

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \frac{|D_4|}{|M_4|} = \frac{8}{4} = 2$, ezért $M_4 \lhd D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján) $t_1 M_4 = D_4 \setminus M_4 = \{t_1, t_2, t_3, t_4\}$. A faktorcsoportban M_4 az egységelem. Mivel $t_1 M_4 \cdot t_1 M_4 = t_1^2 M_4 =$

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \dfrac{|D_4|}{|M_4|} = \dfrac{8}{4} = 2$, ezért $M_4 \lhd D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján) $t_1M_4 = D_4 \setminus M_4 = \{t_1, t_2, t_3, t_4\}$. A faktorcsoportban M_4 az egységelem. Mivel $t_1M_4 \cdot t_1M_4 = t_1^2M_4 = \mathrm{id}\, M_4 =$

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \dfrac{|D_4|}{|M_4|} = \dfrac{8}{4} = 2$, ezért $M_4 \lhd D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján) $t_1M_4 = D_4 \setminus M_4 = \{t_1, t_2, t_3, t_4\}$. A faktorcsoportban M_4 az egységelem. Mivel $t_1M_4 \cdot t_1M_4 = t_1^2M_4 = \mathrm{id}\, M_4 = M_4$, ezért t_1M_4 négyzete az egységelem.

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \frac{|D_4|}{|M_4|} = \frac{8}{4} = 2$, ezért $M_4 \triangleleft D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján) $t_1 M_4 = D_4 \setminus M_4 = \{t_1, t_2, t_3, t_4\}$. A faktorcsoportban M_4 az egységelem. Mivel $t_1 M_4 \cdot t_1 M_4 = t_1^2 M_4 = \mathrm{id}\, M_4 = M_4$, ezért $t_1 M_4$ négyzete az egységelem. Innen látszik, hogy

$$D_4/M_4 =$$

Ekkor $M_4 = \{f, f^2, f^3, f^4 = \mathrm{id}\}$, azaz a mozgáscsoport a négy forgatásból áll. Mivel — a Lagrange-tétel szerint — indexe $[D_4 : M_4] = \dfrac{|D_4|}{|M_4|} = \dfrac{8}{4} = 2$, ezért $M_4 \triangleleft D_4$.

A D_4/M_4 faktorcsoport az M_4 szerinti mellékosztályokból áll, ezek egyike M_4, a másik pedig (más lehetőség híján) $t_1M_4 = D_4 \setminus M_4 = \{t_1, t_2, t_3, t_4\}$. A faktorcsoportban M_4 az egységelem. Mivel $t_1M_4 \cdot t_1M_4 = t_1^2M_4 = \mathrm{id}\, M_4 = M_4$, ezért t_1M_4 négyzete az egységelem. Innen látszik, hogy

$$D_4/M_4 = [t_1M_4]$$

a kételemű ciklikus csoport.

Példa: Legyen $m \in \mathbf{N}$. Az egész számok additív csoportja, $(\mathbf{Z}; +)$ esetén a $H = \{mx : x \in \mathbf{Z}\}$ normálosztó.

Példa: Legyen $m \in \mathbf{N}$. Az egész számok additív csoportja, $(\mathbf{Z}; +)$ esetén a $H = \{mx : x \in \mathbf{Z}\}$ normálosztó. (Hiszen Abel-csoport esetén minden részcsoport normálosztó.)

Példa: Legyen $m \in \mathbf{N}$. Az egész számok additív csoportja, $(\mathbf{Z}; +)$ esetén a $H = \{mx : x \in \mathbf{Z}\}$ normálosztó. (Hiszen Abel-csoport esetén minden részcsoport normálosztó.) A faktorcsoport a mellékosztályokból áll (vigyázat, most additív írásmódot alkalmazunk):

$$0 + H = H = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$$

$$0+H=H=\{\ldots,-3m,-2m,-m,0,m,2m,3m,\ldots\}$$
$$1+H=\{\ldots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\ldots\}$$

$$0+H=H=\{\ldots,-3m,-2m,-m,0,m,2m,3m,\ldots\}$$
$$1+H=\{\ldots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\ldots\}$$
$$2+H=\{\ldots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\ldots\}$$

$$0 + H = H = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$$
$$1+H = \{\ldots, -3m+1, -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, \ldots\}$$
$$2+H = \{\ldots, -3m+2, -2m+2, -m+2, 2, m+2, 2m+2, 3m+2, \ldots\}$$
$$3+H = \{\ldots, -3m+3, -2m+3, -m+3, 3, m+3, 2m+3, 3m+3, \ldots\}$$

$$0+H=H=\{\ldots,-3m,-2m,-m,0,m,2m,3m,\ldots\}$$
$$1+H=\{\ldots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\ldots\}$$
$$2+H=\{\ldots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\ldots\}$$
$$3+H=\{\ldots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\ldots\}$$
$$\ldots$$

$$
\begin{gathered}
0+H=H=\{\ldots,-3m,-2m,-m,0,m,2m,3m,\ldots\}\\
1{+}H=\{\ldots,-3m{+}1,-2m{+}1,-m{+}1,1,m{+}1,2m{+}1,3m{+}1,\ldots\}\\
2{+}H=\{\ldots,-3m{+}2,-2m{+}2,-m{+}2,2,m{+}2,2m{+}2,3m{+}2,\ldots\}\\
3{+}H=\{\ldots,-3m{+}3,-2m{+}3,-m{+}3,3,m{+}3,2m{+}3,3m{+}3,\ldots\}\\
\cdots\\
m{-}1{+}H=\{\ldots,-2m{-}1,-m{-}1,-1,m{-}1,2m{-}1,3m{-}1,4m{-}1,\ldots\}
\end{gathered}
$$

$$
\begin{gathered}
0+H=H=\{\ldots,-3m,-2m,-m,0,m,2m,3m,\ldots\} \\
1+H=\{\ldots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\ldots\} \\
2+H=\{\ldots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\ldots\} \\
3+H=\{\ldots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\ldots\} \\
\cdots \\
m-1+H=\{\ldots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\ldots\}.
\end{gathered}
$$

$$0+H=H=\{\dots,-3m,-2m,-m,0,m,2m,3m,\dots\}$$
$$1+H=\{\dots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\dots\}$$
$$2+H=\{\dots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\dots\}$$
$$3+H=\{\dots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\dots\}$$
$$\dots$$
$$m-1+H=\{\dots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\dots\}.$$

(Több mellékosztály nincs, pl.

$$0 + H = H = \{\dots, -3m, -2m, -m, 0, m, 2m, 3m, \dots\}$$

$$1{+}H = \{\dots, -3m{+}1, -2m{+}1, -m{+}1, 1, m{+}1, 2m{+}1, 3m{+}1, \dots\}$$

$$2{+}H = \{\dots, -3m{+}2, -2m{+}2, -m{+}2, 2, m{+}2, 2m{+}2, 3m{+}2, \dots\}$$

$$3{+}H = \{\dots, -3m{+}3, -2m{+}3, -m{+}3, 3, m{+}3, 2m{+}3, 3m{+}3, \dots\}$$

$$\dots$$

$$m{-}1{+}H = \{\dots, -2m{-}1, -m{-}1, -1, m{-}1, 2m{-}1, 3m{-}1, 4m{-}1, \dots\}.$$

(Több mellékosztály nincs, pl. $m + H = H$,

$$0+H=H=\{\dots,-3m,-2m,-m,0,m,2m,3m,\dots\}$$

$$1+H=\{\dots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\dots\}$$

$$2+H=\{\dots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\dots\}$$

$$3+H=\{\dots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\dots\}$$

$$\dots$$

$$m-1+H=\{\dots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\dots\}.$$

(Több mellékosztály nincs, pl. $m+H=H$, $m+1+H=1+H$, stb.)

$$0+H=H=\{\ldots,-3m,-2m,-m,0,m,2m,3m,\ldots\}$$
$$1+H=\{\ldots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\ldots\}$$
$$2+H=\{\ldots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\ldots\}$$
$$3+H=\{\ldots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\ldots\}$$
$$\ldots$$
$$m-1+H=\{\ldots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\ldots\}.$$

(Több mellékosztály nincs, pl. $m+H=H$, $m+1+H=1+H$, stb.)

$$
\begin{aligned}
0+H=H&=\{\dots,-3m,-2m,-m,0,m,2m,3m,\dots\}\\
1{+}H&=\{\dots,-3m{+}1,-2m{+}1,-m{+}1,1,m{+}1,2m{+}1,3m{+}1,\dots\}\\
2{+}H&=\{\dots,-3m{+}2,-2m{+}2,-m{+}2,2,m{+}2,2m{+}2,3m{+}2,\dots\}\\
3{+}H&=\{\dots,-3m{+}3,-2m{+}3,-m{+}3,3,m{+}3,2m{+}3,3m{+}3,\dots\}\\
&\dots\\
m{-}1{+}H&=\{\dots,-2m{-}1,-m{-}1,-1,m{-}1,2m{-}1,3m{-}1,4m{-}1,\dots\}.
\end{aligned}
$$

(Több mellékosztály nincs, pl. $m+H=H$, $m+1+H=1+H$, stb.) A faktorcsoport tehát ezen mellékosztályokból áll. A számolás (példák):

$$\begin{aligned}
0+H = H &= \{\dots,-3m,-2m,-m,0,m,2m,3m,\dots\}\\
1{+}H &= \{\dots,-3m{+}1,-2m{+}1,-m{+}1,1,m{+}1,2m{+}1,3m{+}1,\dots\}\\
2{+}H &= \{\dots,-3m{+}2,-2m{+}2,-m{+}2,2,m{+}2,2m{+}2,3m{+}2,\dots\}\\
3{+}H &= \{\dots,-3m{+}3,-2m{+}3,-m{+}3,3,m{+}3,2m{+}3,3m{+}3,\dots\}\\
&\dots\\
m{-}1{+}H &= \{\dots,-2m{-}1,-m{-}1,-1,m{-}1,2m{-}1,3m{-}1,4m{-}1,\dots\}.
\end{aligned}$$

(Több mellékosztály nincs, pl. $m+H=H$, $m+1+H=1+H$, stb.) A faktorcsoport tehát ezen mellékosztályokból áll. A számolás (példák): $(2+H)+(1+H)=$

$$
\begin{aligned}
0+H=H&=\{\ldots,-3m,-2m,-m,0,m,2m,3m,\ldots\}\\
1+H&=\{\ldots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\ldots\}\\
2+H&=\{\ldots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\ldots\}\\
3+H&=\{\ldots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\ldots\}\\
&\ldots\\
m-1+H&=\{\ldots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\ldots\}.
\end{aligned}
$$

(Több mellékosztály nincs, pl. $m+H=H$, $m+1+H=1+H$, stb.) A faktorcsoport tehát ezen mellékosztályokból áll. A számolás (példák): $(2+H)+(1+H)=3+H$,

$$0+H=H=\{\dots,-3m,-2m,-m,0,m,2m,3m,\dots\}$$
$$1+H=\{\dots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\dots\}$$
$$2+H=\{\dots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\dots\}$$
$$3+H=\{\dots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\dots\}$$
$$\dots$$
$$m-1+H=\{\dots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\dots\}.$$

(Több mellékosztály nincs, pl. $m+H=H$, $m+1+H=1+H$, stb.) A faktorcsoport tehát ezen mellékosztályokból áll. A számolás (példák): $(2+H)+(1+H)=3+H$, $(m-2+H)+(m-1+H)=$

$$0 + H = H = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$$
$$1{+}H = \{\ldots, -3m{+}1, -2m{+}1, -m{+}1, 1, m{+}1, 2m{+}1, 3m{+}1, \ldots\}$$
$$2{+}H = \{\ldots, -3m{+}2, -2m{+}2, -m{+}2, 2, m{+}2, 2m{+}2, 3m{+}2, \ldots\}$$
$$3{+}H = \{\ldots, -3m{+}3, -2m{+}3, -m{+}3, 3, m{+}3, 2m{+}3, 3m{+}3, \ldots\}$$
$$\ldots$$
$$m{-}1{+}H = \{\ldots, -2m{-}1, -m{-}1, -1, m{-}1, 2m{-}1, 3m{-}1, 4m{-}1, \ldots\}.$$

(Több mellékosztály nincs, pl. $m + H = H$, $m + 1 + H = 1 + H$, stb.) A faktorcsoport tehát ezen mellékosztályokból áll. A számolás (példák): $(2 + H) + (1 + H) = 3 + H$, $(m - 2 + H) + (m - 1 + H) = 2m - 3 + H = m - 3 + H$, stb.

$$0+H=H=\{\dots,-3m,-2m,-m,0,m,2m,3m,\dots\}$$
$$1+H=\{\dots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\dots\}$$
$$2+H=\{\dots,-3m+2,-2m+2,-m+2,2,m+2,2m+2,3m+2,\dots\}$$
$$3+H=\{\dots,-3m+3,-2m+3,-m+3,3,m+3,2m+3,3m+3,\dots\}$$
$$\dots$$
$$m-1+H=\{\dots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\dots\}.$$

(Több mellékosztály nincs, pl. $m+H=H$, $m+1+H=1+H$, stb.) A faktorcsoport tehát ezen mellékosztályokból áll. A számolás (példák): $(2+H)+(1+H)=3+H$, $(m-2+H)+(m-1+H)=2m-3+H=m-3+H$, stb. A faktorcsoport — izomorfia erejéig — nem más, mint a $(\mathbf{Z}_m;+)$ ciklikus csoport, azaz a modulo m maradékosztályok csoportja.

(Az elnevezéssel kapcsolatban: éppen az itt látott mellékosztályokat nevezik

(Az elnevezéssel kapcsolatban: éppen az itt látott mellékosztályokat nevezik „maradékosztályoknak”, hiszen pl. a $2+H$ mellékosztály pontosan azon egész számokból áll,

(Az elnevezéssel kapcsolatban: éppen az itt látott mellékosztályokat nevezik „maradékosztályoknak”, hiszen pl. a $2+H$ mellékosztály pontosan azon egész számokból áll, amelyek m-mel osztva a 2 maradékot adják.)

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza).

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza). Ekkor N normálosztó és,

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza). Ekkor N normálosztó és, amint korábban láttuk,

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza). Ekkor N normálosztó és, amint korábban láttuk, az N szerinti mellékosztályok éppen az

Példa: Legyen $(\mathbf{R}^2; +)$ a síkvektorok additív csoportja. Legyen $N = \{(r, 0) : r \in \mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza). Ekkor N normálosztó és, amint korábban láttuk, az N szerinti mellékosztályok éppen az

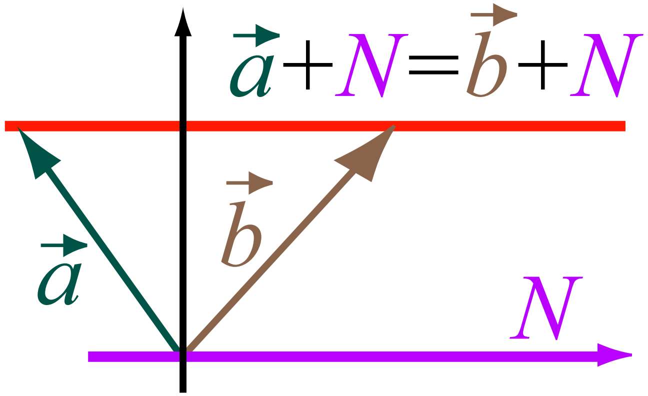
$$(0, s) + N = \{(r, s) : s \in \mathbf{R}\} \qquad (s \in \mathbf{R})$$

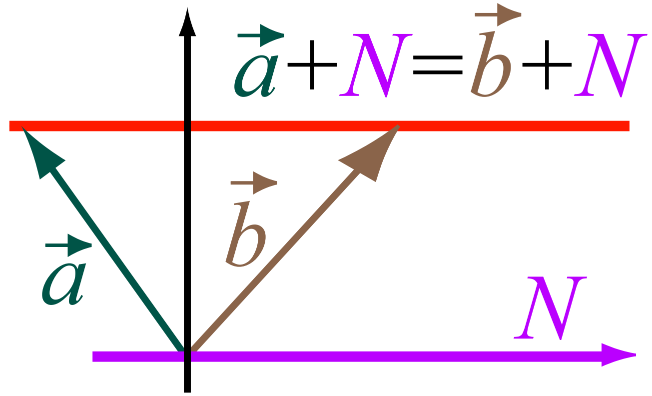
halmazok,

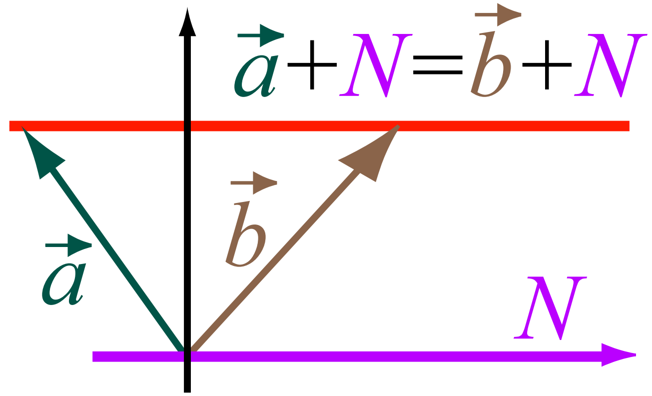
Példa: Legyen $(\mathbf{R}^2;+)$ a síkvektorok additív csoportja. Legyen $N=\{(r,0) : r\in\mathbf{R}\}$ (az x tengelyen fekvő síkvektorok halmaza). Ekkor N normálosztó és, amint korábban láttuk, az N szerinti mellékosztályok éppen az

$$(0,s)+N=\{(r,s) : s\in\mathbf{R}\} \qquad (s\in\mathbf{R})$$

halmazok, és ezekből áll a faktorcsoport.

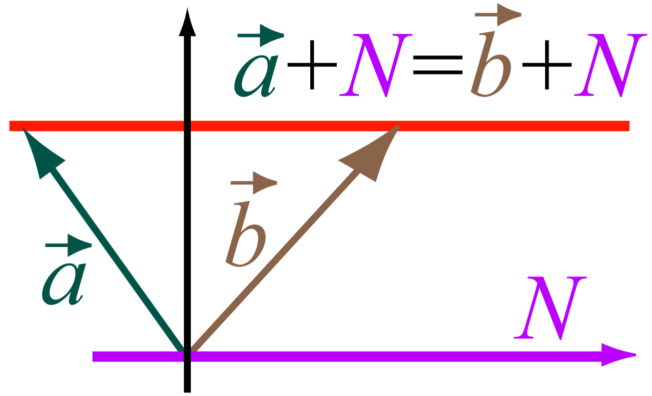



$\vec{a} + N = \vec{b} + N$
$\vec{b}$
$\vec{a}$
N



Mivel $((0,s_1)+N)+((0,s_2)+N)=(0,s_1+s_2)+N$, ezért a

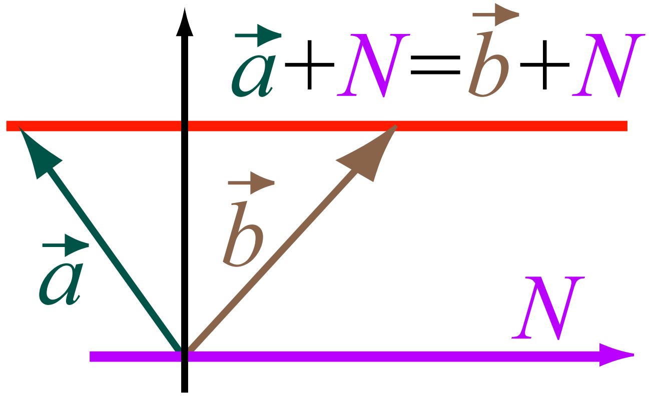
$$\varphi:(\mathbf{R};+)\to(\mathbf{R}^2;+)/N,\qquad s\mapsto(s,0)+N$$



Mivel $((0, s_1) + N) + ((0, s_2) + N) = (0, s_1 + s_2) + N$, ezért a

$$\varphi : (\mathbf{R}; +) \to (\mathbf{R}^2; +)/N, \qquad s \mapsto (s, 0) + N$$

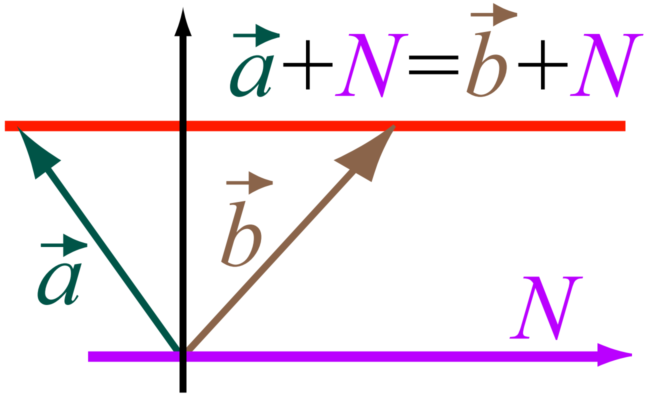
leképezés (



Mivel $((0,s_1)+N)+((0,s_2)+N)=(0,s_1+s_2)+N$, ezért a

$$\varphi:(\mathbf{R};+)\to(\mathbf{R}^2;+)/N, \qquad s\mapsto(s,0)+N$$

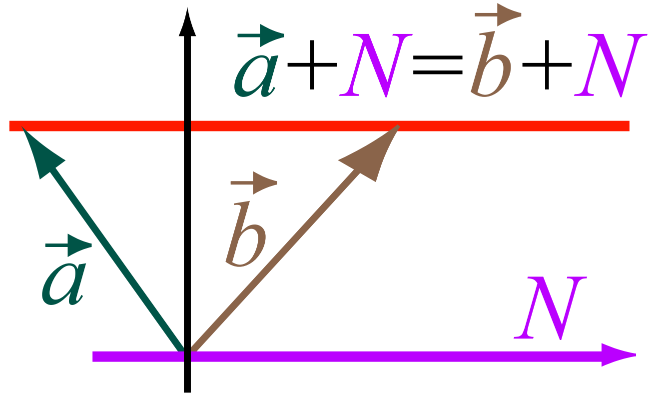
leképezés (amely nyilván bijektív) izomorfizmus. Tehát



Mivel $((0, s_1) + N) + ((0, s_2) + N) = (0, s_1 + s_2) + N$, ezért a

$$\varphi : (\mathbf{R}; +) \to (\mathbf{R}^2; +)/N, \qquad s \mapsto (s, 0) + N$$

leképezés (amely nyilván bijektív) izomorfizmus. Tehát a faktorcsoport izomorf a valós számok additív csoportjával.



Mivel $((0,s_1)+N)+((0,s_2)+N)=(0,s_1+s_2)+N$, ezért a

$$\varphi : (\mathbf{R};+) \to (\mathbf{R}^2;+)/N, \qquad s \mapsto (s,0)+N$$

leképezés (amely nyilván bijektív) izomorfizmus. Tehát a faktorcsoport izomorf a valós számok additív csoportjával. (Szemléletesen: a mellékosztályokat úgy adjuk össze, hogy az

y-tengellyel való metszeteiket —

y-tengellyel való metszeteiket — amelyek valós számok — adjuk össze, és ezen összegnél „húzunk egy vízszintes vonalat.)

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$.

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$. Ekkor H részcsoport és —

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$. Ekkor H részcsoport és — a kommutativitás miatt — normálosztó is. A (

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$. Ekkor H részcsoport és — a kommutativitás miatt — normálosztó is. A (baloldali) mellékosztályok a kételemű $gH =$

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$. Ekkor H részcsoport és — a kommutativitás miatt — normálosztó is. A (baloldali) mellékosztályok a kételemű $gH = \{g, -g\}$ halmazok ($g \in \mathbf{R} \setminus \{0\}$), ezekből áll a G/H faktorcsoport.

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$. Ekkor H részcsoport és — a kommutativitás miatt — normálosztó is. A (baloldali) mellékosztályok a kételemű $gH = \{g, -g\}$ halmazok ($g \in \mathbf{R} \setminus \{0\}$), ezekből áll a G/H faktorcsoport. Jelölje $(\mathbf{R}^+; \cdot)$ a pozitív valós számok multiplikatív csoportját. Könnyen látható, hogy a

$$G/H \to \mathbf{R}^+, \qquad gH \to |g|$$

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$. Ekkor H részcsoport és — a kommutativitás miatt — normálosztó is. A (baloldali) mellékosztályok a kételemű $gH = \{g, -g\}$ halmazok ($g \in \mathbf{R} \setminus \{0\}$), ezekből áll a G/H faktorcsoport. Jelölje $(\mathbf{R}^+; \cdot)$ a pozitív valós számok multiplikatív csoportját. Könnyen látható, hogy a

$$G/H \to \mathbf{R}^+, \qquad gH \to |g|$$

leképezés izomorfizmus.

Példa: Legyen $G = (\mathbf{R} \setminus \{0\}; \cdot)$, a nemnulla valós számok multiplikatív csoportja, és legyen $H = \{-1, 1\}$. Ekkor H részcsoport és — a kommutativitás miatt — normálosztó is. A (baloldali) mellékosztályok a kételemű $gH = \{g, -g\}$ halmazok ($g \in \mathbf{R} \setminus \{0\}$), ezekből áll a G/H faktorcsoport. Jelölje $(\mathbf{R}^+; \cdot)$ a pozitív valós számok multiplikatív csoportját. Könnyen látható, hogy a

$$G/H \to \mathbf{R}^+, \qquad gH \to |g|$$

leképezés izomorfizmus. Tehát a faktorcsoport izomorf a pozitív valós számok multiplikatív csoportjával.

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \det(A) = 1\}.$$

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \mathsf{det}(A) = 1\}.$$

Ekkor H részcsoport

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \mathrm{det}(A) = 1\}.$$

Ekkor H részcsoport (ez a determinánsok szorzástételéből adódik). Továbbá H normálosztó is, hiszen ha $A \in H$ és $B \in G$ akkor

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \det(A) = 1\}.$$

Ekkor H részcsoport (ez a determinánsok szorzástételéből adódik). Továbbá H normálosztó is, hiszen ha $A \in H$ és $B \in G$ akkor (bár a mátrixszorzás nem kommutatív, a determinánsok szorzástétele mégis segít):

$\det(B^{-1}AB) =$

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \mathrm{det}(A) = 1\}.$$

Ekkor H részcsoport (ez a determinánsok szorzástételéből adódik). Továbbá H normálosztó is, hiszen ha $A \in H$ és $B \in G$ akkor (bár a mátrixszorzás nem kommutatív, a determinánsok szorzástétele mégis segít):

$\mathrm{det}(B^{-1}AB) = \mathrm{det}(B^{-1})\,\mathrm{det}(A)\,\mathrm{det}(B) =$

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \det(A) = 1\}.$$

Ekkor H részcsoport (ez a determinánsok szorzástételéből adódik). Továbbá H normálosztó is, hiszen ha $A \in H$ és $B \in G$ akkor (bár a mátrixszorzás nem kommutatív, a determinánsok szorzástétele mégis segít):

$$\det(B^{-1}AB) = \det(B^{-1})\det(A)\det(B) = \det(A)(\det(B^{-1})\det(B))$$
$$=$$

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \det(A) = 1\}.$$

Ekkor H részcsoport (ez a determinánsok szorzástételéből adódik). Továbbá H normálosztó is, hiszen ha $A \in H$ és $B \in G$ akkor (bár a mátrixszorzás nem kommutatív, a determinánsok szorzástétele mégis segít):

$$\begin{aligned}\det(B^{-1}AB) &= \det(B^{-1})\det(A)\det(B) = \det(A)(\det(B^{-1})\det(B)) \\ &= \det(A)\det(B^{-1}B) =\end{aligned}$$

Példa: Legyen $n \in \mathbf{N}$ és legyen G a nemelfajuló $n \times n$ méretű valós mátrixok multiplikatív csoportja. (Tanultuk, hogy a nemelfajuló — más néven invertálható — mátrixok szorzata és inverze sem elfajuló, tehát tényleg csoportról van szó.) Legyen

$$H = \{A \in G : \det(A) = 1\}.$$

Ekkor H részcsoport (ez a determinánsok szorzástételéből adódik). Továbbá H normálosztó is, hiszen ha $A \in H$ és $B \in G$ akkor (bár a mátrixszorzás nem kommutatív, a determinánsok szorzástétele mégis segít):

$$\begin{aligned}\det(B^{-1}AB) &= \det(B^{-1})\det(A)\det(B) = \det(A)(\det(B^{-1})\det(B)) \\ &= \det(A)\det(B^{-1}B) = \det(A)\det(E) = 1 \cdot 1 = 1\end{aligned}$$

miatt $B^{-1}AB \in H$.

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza.

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) =$

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A) \det(B) = r \cdot 1 = r$.

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$,

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\det(A^{-1}C) = \det(A^{-1})\det(C) =$$

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r =$$

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r = \det(A^{-1}) \cdot \det(A)$$

$$=$$

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\begin{aligned}\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r = \det(A^{-1}) \cdot \det(A) \\ = \det(A^{-1}A) =\end{aligned}$$

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r = \det(A^{-1}) \cdot \det(A)$$
$$= \det(A^{-1}A) = \det(E) =$$

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r = \det(A^{-1}) \cdot \det(A)$$
$$= \det(A^{-1}A) = \det(E) = 1$$

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\begin{aligned}\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r = \det(A^{-1}) \cdot \det(A) \\ = \det(A^{-1}A) = \det(E) = 1\end{aligned}$$

miatt $A^{-1}C \in H$.

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r = \det(A^{-1}) \cdot \det(A) \\ = \det(A^{-1}A) = \det(E) = 1$$

miatt $A^{-1}C \in H$. Ezek után jól látható, hogy a

$$\varphi : G/H \to (\mathbf{R} \setminus \{0\}; \cdot), \qquad M_r \mapsto r$$

leképezés izomorfizmus.

Legyen $A \in G$ egy olyan mátrix, amelynek a determinánsa $r \in \mathbf{R} \setminus \{0\}$. Ekkor az AH mellékosztály éppen az r determinánsú $n \times n$-es mátrixoknak a továbbiakban M_r-rel jelölt halmaza. Ugyanis ha $B \in H$, akkor $\det(AH) = \det(A)\det(B) = r \cdot 1 = r$. Ha pedig $C \in M_r$, akkor $C = A(A^{-1}C) \in AH$, hiszen

$$\det(A^{-1}C) = \det(A^{-1})\det(C) = \det(A^{-1}) \cdot r = \det(A^{-1}) \cdot \det(A) = \det(A^{-1}A) = \det(E) = 1$$

miatt $A^{-1}C \in H$. Ezek után jól látható, hogy a

$$\varphi : G/H \to (\mathbf{R} \setminus \{0\}; \cdot), \qquad M_r \mapsto r$$

leképezés izomorfizmus. Tehát a faktorcsoport izomorf a nemnulla valós számok multiplikatív csoportjával.

További algebrai konstrukciók

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $\mathcal{A} = (A; F)$ és $\mathcal{B} = (B; F)$ két azonos típusú algebra.

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $\mathcal{A} = (A; F)$ és $\mathcal{B} = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.)

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $A = (A; F)$ és $B = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $\mathcal{A} = (A; F)$ és $\mathcal{B} = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$ Descartes-szorzaton, mint alaphalmazon definiált $(A \times B; F)$ algebra, ahol $f \in F$-re — amely mondjuk $m = m_f$-változós —

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $\mathcal{A} = (A; F)$ és $\mathcal{B} = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$ Descartes-szorzaton, mint alaphalmazon definiált $(A \times B; F)$ algebra, ahol $f \in F$-re — amely mondjuk $m = m_f$-változós — és (a_1, b_1),

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $A = (A; F)$ és $B = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$ Descartes-szorzaton, mint alaphalmazon definiált $(A \times B; F)$ algebra, ahol $f \in F$-re — amely mondjuk $m = m_f$-változós — és (a_1, b_1), $\ldots$,

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $A = (A; F)$ és $B = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$ Descartes-szorzaton, mint alaphalmazon definiált $(A \times B; F)$ algebra, ahol $f \in F$-re — amely mondjuk $m = m_f$-változós — és (a_1, b_1), …, $(a_m, b_m) \in A \times B$-re

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $A = (A; F)$ és $B = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$ Descartes-szorzaton, mint alaphalmazon definiált $(A \times B; F)$ algebra, ahol $f \in F$-re — amely mondjuk $m = m_f$-változós — és (a_1, b_1), …, $(a_m, b_m) \in A \times B$-re

$$f((a_1, b_1), \ldots, (a_m, b_m)) := (f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)).$$

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $A = (A; F)$ és $B = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$ Descartes-szorzaton, mint alaphalmazon definiált $(A \times B; F)$ algebra, ahol $f \in F$-re — amely mondjuk $m = m_f$-változózós — és (a_1, b_1), …, $(a_m, b_m) \in A \times B$-re

$$f((a_1, b_1), \ldots, (a_m, b_m)) := (f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)).$$

(Azaz a műveleteket

További algebrai konstrukciók

Egy már volt: a részalgebraképzés.

Direkt szorzat

Def. Legyen $\mathcal{A} = (A; F)$ és $\mathcal{B} = (B; F)$ két azonos típusú algebra. (Tehát azonos módon jelölt műveleteik vannak, azaz a műveleti jelek F halmaza közös.) Ekkor **direkt szorzatuk** nem más, mint az $A \times B$ Descartes-szorzaton, mint alaphalmazon definiált $(A \times B; F)$ algebra, ahol $f \in F$-re — amely mondjuk $m = m_f$-változós — és (a_1, b_1), ..., $(a_m, b_m) \in A \times B$-re

$$f((a_1, b_1), \ldots, (a_m, b_m)) := (f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)).$$

(Azaz a műveleteket **komponensenként** végezzük.)

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük.

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az $(A \times B \times C; \cdot)$ grupoid, és

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az $(A \times B \times C; \cdot)$ grupoid, és (a, b, c), $(a', b', c') \in A \times B \times C$ esetén $(a, b, c) \cdot (a', b', c') =$

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az $(A \times B \times C; \cdot)$ grupoid, és $(a, b, c), (a', b', c') \in A \times B \times C$ esetén $(a, b, c) \cdot (a', b', c') = (aa', bb', cc')$.

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az $(A \times B \times C; \cdot)$ grupoid, és (a, b, c), $(a', b', c') \in A \times B \times C$ esetén $(a, b, c) \cdot (a', b', c') = (aa', bb', cc')$.

Az azonos tényezők direkt szorzatát

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az $(A \times B \times C; \cdot)$ grupoid, és $(a, b, c), (a', b', c') \in A \times B \times C$ esetén $(a, b, c) \cdot (a', b', c') = (aa', bb', cc')$.

Az azonos tényezők direkt szorzatát **direkt hatványnak** nevezzük.

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az $(A \times B \times C; \cdot)$ grupoid, és $(a, b, c), (a', b', c') \in A \times B \times C$ esetén $(a, b, c) \cdot (a', b', c') = (aa', bb', cc')$.

Az azonos tényezők direkt szorzatát **direkt hatványnak** nevezzük. Definiálható végtelen sok azonos típusú algebra direkt szorzata is, de ezzel nem foglalkozunk.

Teljesen hasonlóan definiálhatjuk n darab azonos típusú algebra direkt szorzatát: a direkt szorzat tartóhalmaza most is az egyes algebrák Descartes-szorzata, a műveleteket pedig komponensenként végezzük. Tehát pl. grupoidok esetére ha $A = (A; \cdot)$, $B = (B; \cdot)$ és $C = (C; \cdot)$ grupoidok, akkor direkt szorzatuk az $(A \times B \times C; \cdot)$ grupoid, és $(a, b, c), (a', b', c') \in A \times B \times C$ esetén $(a, b, c) \cdot (a', b', c') = (aa', bb', cc')$.

Az azonos tényezők direkt szorzatát **direkt hatványnak** nevezzük. Definiálható végtelen sok azonos típusú algebra direkt szorzata is, de ezzel nem foglalkozunk. Az egytényezős direkt szorzat izomorf az egyetlen direkt tényezővel, tehát nem ad újat, ezért nem túl érdekes.

64. Tétel. *A direkt szorzás megőrzi az alább műveleti tulajdonságokat:*

64. Tétel. *A direkt szorzás megőrzi az alábbi műveleti tulajdonságokat: asszociativitás,*

64. Tétel. *A direkt szorzás megőrzi az alábbi műveleti tulajdonságokat: asszociativitás, kommutativitás,*

64. Tétel. *A direkt szorzás megőrzi az alább műveleti tulajdonságokat: asszociativitás, kommutativitás, disztributivitás,*

64. Tétel. *A direkt szorzás megőrzi az alábbb műveleti tulajdonságokat: asszociativitás, kommutativitás, disztributivitás, kancellativitás,*

64. Tétel. *A direkt szorzás megőrzi az alább műveleti tulajdonságokat: asszociativitás, kommutativitás, disztributivitás, kancellativitás, tehát általában tetszőleges ún. azonosság, továbbá*

64. Tétel. *A direkt szorzás megőrzi az alábbi műveleti tulajdonságokat: asszociativitás, kommutativitás, disztributivitás, kancellativitás, tehát általában tetszőleges ún. azonosság, továbbá egységelemesség,*

64. Tétel. *A direkt szorzás megőrzi az alább műveleti tulajdonságokat: asszociativitás, kommutativitás, disztributivitás, kancellativitás, tehát általában tetszőleges ún. azonosság, továbbá egységelemesség, „minden elemnek van inverze".*

64. Tétel. *A direkt szorzás megőrzi az alább műveleti tulajdonságokat: asszociativitás, kommutativitás, disztributivitás, kancellativitás, tehát általában tetszőleges ún. azonosság, továbbá egységelemesség, „minden elemnek van inverze". Ha tehát pl. a tényezők mindegyikében a kétváltozós f művelet asszociatív, akkor f a direkt szorzatban is asszociatív.*

64. Tétel. *A direkt szorzás megőrzi az alább műveleti tulajdonságokat: asszociativitás, kommutativitás, disztributivitás, kancellativitás, tehát általában tetszőleges ún. azonosság, továbbá egységelemesség, „minden elemnek van inverze". Ha tehát pl. a tényezők mindegyikében a kétváltozós f művelet asszociatív, akkor f a direkt szorzatban is asszociatív. Innen az is következik, hogy félcsoportok, monoidok, csoportok, Abel-csoportok, kommutatív félcsoportok, gyűrűk, kommutatív gyűrűk direkt szorzata szintén félcsoport, illetve monoid, illetve csoport, stb.*

Viszont nem őrződik meg *általában gyűrűk esetén a zérusosztómentesség. Egynél több test direkt szorzata sohasem lehet test.*

Bizonyítás — részletek: Ha az $\mathcal{A} = (A;\cdot)$ és a $\mathcal{B} = (B;\cdot)$ grupoidok mindketten kommutatívak, akkor

Bizonyítás — részletek: Ha az $A = (A; \cdot)$ és a $B = (B; \cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges $(a_1, b_1), (a_2, b_2)$ elemre

Bizonyítás — részletek: Ha az $A = (A;\cdot)$ és a $B = (B;\cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges $(a_1, b_1), (a_2, b_2)$ elemre $(a_1, b_1) \cdot (a_2, b_2) =$

Bizonyítás — részletek: Ha az $A = (A;\cdot)$ és a $B = (B;\cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges $(a_1, b_1), (a_2, b_2)$ elemre $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2) =$

Bizonyítás — részletek: Ha az $A = (A; \cdot)$ és a $B = (B; \cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges $(a_1, b_1), (a_2, b_2)$ elemre $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) =$

Bizonyítás — részletek: Ha az $\mathcal{A} = (A;\cdot)$ és a $\mathcal{B} = (B;\cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges $(a_1, b_1), (a_2, b_2)$ elemre $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2) = (a_2 a_1, b_2 b_1) = (a_2, b_2) \cdot (a_1, b_1)$, tehát a direkt szorzat megőrzi a kommutativitást.

Bizonyítás — részletek: Ha az $A = (A;\cdot)$ és a $B = (B;\cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges $(a_1,b_1), (a_2,b_2)$ elemre $(a_1,b_1)\cdot(a_2,b_2) = (a_1a_2,b_1b_2) = (a_2a_1,b_2b_1) = (a_2,b_2)\cdot(a_1,b_1)$, tehát a direkt szorzat megőrzi a kommutativitást. Az egyszerű megfontolás azon múlt, hogy a műveleteket komponensenként végezzük.

Bizonyítás — részletek: Ha az $A = (A; \cdot)$ és a $B = (B; \cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges (a_1, b_1), (a_2, b_2) elemre $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2, b_2) \cdot (a_1, b_1)$, tehát a direkt szorzat megőrzi a kommutativitást. Az egyszerű megfontolás azon múlt, hogy a műveleteket komponensenkét végezzük.

Teljesen hasonlóan igazolható a többi tulajdonság megőrződése is. Pl. ha

Bizonyítás — részletek: Ha az $\mathcal{A} = (A; \cdot)$ és a $\mathcal{B} = (B; \cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges (a_1, b_1), (a_2, b_2) elemre $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2) = (a_2 a_1, b_2 b_1) = (a_2, b_2) \cdot (a_1, b_1)$, tehát a direkt szorzat megőrzi a kommutativitást. Az egyszerű megfontolás azon múlt, hogy a műveleteket komponensenkét végezzük.

Teljesen hasonlóan igazolható a többi tulajdonság megőrződése is. Pl. ha $\mathcal{A}$ és $\mathcal{B}$ egységelemes, akkor $(1, 1)$ egységeleme lesz $\mathcal{A} \times \mathcal{B}$-nek. Ha az $\mathcal{A}$ és $\mathcal{B}$ egységelemes grupoid esetén minden elemnek van inverze, akkor a direkt szorzatban

Bizonyítás — részletek: Ha az $\mathcal{A} = (A;\cdot)$ és a $\mathcal{B} = (B;\cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges (a_1, b_1), (a_2, b_2) elemre $(a_1, b_1)\cdot(a_2, b_2) = (a_1a_2, b_1b_2) = (a_2a_1, b_2b_1) = (a_2, b_2)\cdot(a_1, b_1)$, tehát a direkt szorzat megőrzi a kommutativitást. Az egyszerű megfontolás azon múlt, hogy a műveleteket komponensenkét végezzük.

Teljesen hasonlóan igazolható a többi tulajdonság megőrződése is. Pl. ha $\mathcal{A}$ és $\mathcal{B}$ egységelemes, akkor $(1, 1)$ egységeleme lesz $\mathcal{A}\times\mathcal{B}$-nek. Ha az $\mathcal{A}$ és $\mathcal{B}$ egységelemes grupoid esetén minden elemnek van inverze, akkor a direkt szorzatban (a, b)-nek is van: (a', b'), ahol

Bizonyítás — részletek: Ha az $A = (A; \cdot)$ és a $B = (B; \cdot)$ grupoidok mindketten kommutatívak, akkor direkt szorzatukban tetszőleges (a_1, b_1), (a_2, b_2) elemre $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2) = (a_2 a_1, b_2 b_1) = (a_2, b_2) \cdot (a_1, b_1)$, tehát a direkt szorzat megőrzi a kommutativitást. Az egyszerű megfontolás azon múlt, hogy a műveleteket komponensenkét végezzük.

Teljesen hasonlóan igazolható a többi tulajdonság megőrződése is. Pl. ha A és B egységelemes, akkor $(1, 1)$ egységeleme lesz $A \times B$-nek. Ha az A és B egységelemes grupoid esetén minden elemnek van inverze, akkor a direkt szorzatban (a, b)-nek is van: (a', b'), ahol a' inverze a-nak A-ban, b' pedig inverze b-nek B-ben.

Ha $K = (K; +, \cdot)$ és $L = (L; +, \cdot)$ test, akkor direkt szorzatuk-ban

Ha $K = (K; +, \cdot)$ és $L = (L; +, \cdot)$ test, akkor direkt szorzatukban $(1, 0) \cdot (0, 1) = (0, 0)$. Tehát $K \times L$ nem zérusosztómentes, és ezért nem is test.

Ha $K = (K;+,\cdot)$ és $L = (L;+,\cdot)$ test, akkor direkt szorzatukban $(1,0)\cdot(0,1) = (0,0)$. Tehát $K \times L$ nem zérusosztómentes, és ezért nem is test. Tehát a „test" és a „zérussztómentes" tulajdonságok nem őrződnek meg. Q.e.d.

Ha $K = (K; +, \cdot)$ és $L = (L; +, \cdot)$ test, akkor direkt szorzatukban $(1, 0) \cdot (0, 1) = (0, 0)$. Tehát $K \times L$ nem zérusosztómentes, és ezért nem is test. Tehát a „test” és a „zérussztómentes” tulajdonságok nem őrződnek meg. Q.e.d.

Megjegyzés: meglepő

Ha $K = (K; +, \cdot)$ és $L = (L; +, \cdot)$ test, akkor direkt szorzatukban $(1,0) \cdot (0,1) = (0,0)$. Tehát $K \times L$ nem zérusosztómentes, és ezért nem is test. Tehát a „test'' és a „zérussztómentes'' tulajdonságok nem őrződnek meg. Q.e.d.

Megjegyzés: meglepő lehet, hogy bár a gyűrű és az invertálhatóság direkt szorzat képzésekor megőrződik, a test (ami csak annyival több a gyűrűnél, hogy minden nemzérus elemnek van inverze) nem.

Ha $K = (K; +, \cdot)$ és $L = (L; +, \cdot)$ test, akkor direkt szorzatukban $(1, 0) \cdot (0, 1) = (0, 0)$. Tehát $K \times L$ nem zérusosztómentes, és ezért nem is test. Tehát a „test" és a „zérussztómentes" tulajdonságok nem őrződnek meg. Q.e.d.

Megjegyzés: meglepő lehet, hogy bár a gyűrű és az invertálhatóság direkt szorzat képzésekor megőrződik, a test (ami csak annyival több a gyűrűnél, hogy minden nemzérus elemnek van inverze) nem. Ez azzal van összefüggésben, hogy — szemben a „minden"-nel — az „egy kivételével minden" nem őrződik meg;

Ha $K = (K; +, \cdot)$ és $L = (L; +, \cdot)$ test, akkor direkt szorzatukban $(1, 0) \cdot (0, 1) = (0, 0)$. Tehát $K \times L$ nem zérusosztómentes, és ezért nem is test. Tehát a „test” és a „zérussztómentes” tulajdonságok nem őrződnek meg. Q.e.d.

Megjegyzés: meglepő lehet, hogy bár a gyűrű és az invertálhatóság direkt szorzat képzésekor megőrződik, a test (ami csak annyival több a gyűrűnél, hogy minden nemzérus elemnek van inverze) nem. Ez azzal van összefüggésben, hogy — szemben a „minden”-nel — az „egy kivételével minden” nem őrződik meg; éppúgy nem, mint pl. a „kételemű” sem.

Adott egy tetszőleges $A_1 \times \cdots \times A_n$ direkt szorzat. Legyen $i \in \{1, \ldots, n\}$.

Adott egy tetszőleges $A_1 \times \cdots \times A_n$ direkt szorzat. Legyen $i \in \{1, \ldots, n\}$. A

$$\pi_i : A_1 \times \cdots \times A_n \to A_i, \quad (a_1, \ldots, a_n) \mapsto a_i$$

leképezést az ***i*-edik direkt tényezőre való vetítésnek** nevezzük.

65. Tétel. *Algebrák direkt szorzatának bármelyik direkt tényezőre való vetítése szürjektív homomorfizmus.*

A

Adott egy tetszőleges $A_1 \times \cdots \times A_n$ direkt szorzat. Legyen $i \in \{1, \ldots, n\}$. A

$$\pi_i : A_1 \times \cdots \times A_n \to A_i, \quad (a_1, \ldots, a_n) \mapsto a_i$$

leképezést az **i-edik direkt tényezőre való vetítésnek** nevezzük.

65. Tétel. *Algebrák direkt szorzatának bármelyik direkt tényezőre való vetítése szürjektív homomorfizmus.*

A tétel nyilvánvaló következménye a definícióknak, azaz

Adott egy tetszőleges $A_1 \times \cdots \times A_n$ direkt szorzat. Legyen $i \in \{1, \ldots, n\}$. A

$$\pi_i : A_1 \times \cdots \times A_n \to A_i, \quad (a_1, \ldots, a_n) \mapsto a_i$$

leképezést az ***i*-edik direkt tényezőre való vetítésnek** nevezzük.

65. Tétel. *Algebrák direkt szorzatának bármelyik direkt tényezőre való vetítése szürjektív homomorfizmus.*

A tétel nyilvánvaló következménye a definícióknak, azaz annak, hogy a direkt szorzatban a műveleteket komponensenként végezzük.

Példa: Az $\mathbf{R} = (\mathbf{R}; +)$ csoport direkt négyzete, azaz $(\mathbf{R}^2; +)$ szolgál a sík koordinátázására.

Példa: Az $\mathbf{R} = (\mathbf{R}; +)$ csoport direkt négyzete, azaz $(\mathbf{R}^2; +)$ szolgál a sík koordinátázására. Ez esetben az $\mathbf{R}^2 \to \mathbf{R}$, $(x_1, x_2) \mapsto x_i \quad (i \in \{1, 2\}$ rögzített) leképezést (

Példa: Az $\mathbf{R} = (\mathbf{R}; +)$ csoport direkt négyzete, azaz $(\mathbf{R}^2; +)$ szolgál a sík koordinátázására. Ez esetben az $\mathbf{R}^2 \to \mathbf{R}$, $(x_1, x_2) \mapsto x_i \quad (i \in \{1, 2\}$ rögzített) leképezést (merőleges) vetítésnek nevezzük. Innen ered az elnevezés.

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1, 1)$. Ekkor

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1, 1)$. Ekkor $a + a = (0, 2) \neq (0, 0)$ miatt

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1, 1)$. Ekkor $a + a = (0, 2) \neq (0, 0)$ miatt $o(a) \neq 2$.

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1,1)$. Ekkor $a + a = (0,2) \neq (0,0)$ miatt $o(a) \neq 2$. $a + a + a = (1,0) \neq (0,0)$

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1, 1)$. Ekkor $a + a = (0, 2) \neq (0, 0)$ miatt $o(a) \neq 2$. $a + a + a = (1, 0) \neq (0, 0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0, 0)$,

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1, 1)$. Ekkor $a + a = (0, 2) \neq (0, 0)$ miatt $o(a) \neq 2$. $a + a + a = (1, 0) \neq (0, 0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0, 0)$, $o(a) \neq 1$.

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1, 1)$. Ekkor $a + a = (0, 2) \neq (0, 0)$ miatt $o(a) \neq 2$. $a + a + a = (1, 0) \neq (0, 0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0, 0)$, $o(a) \neq 1$. Viszont a Lagrange-tétel (Cauchy-tétel nevű következménye) miatt

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1,1)$. Ekkor $a + a = (0,2) \neq (0,0)$ miatt $o(a) \neq 2$. $a + a + a = (1,0) \neq (0,0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0,0)$, $o(a) \neq 1$. Viszont a Lagrange-tétel (Cauchy-tétel nevű következménye) miatt $o(a) \mid 6$. Ezért

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1,1)$. Ekkor $a + a = (0,2) \neq (0,0)$ miatt $o(a) \neq 2$. $a + a + a = (1,0) \neq (0,0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0,0)$, $o(a) \neq 1$. Viszont a Lagrange-tétel (Cauchy-tétel nevű következménye) miatt $o(a) \mid 6$. Ezért $o(a) = 6$, tehát $|[a]| = o(a) = 6 = |\mathbf{Z}_2 \times Z_3|$, és

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2;+)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3;+)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3;+)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6;+)$ ciklikus csoporttal.

Valóban, legyen $a = (1,1)$. Ekkor $a + a = (0,2) \neq (0,0)$ miatt $o(a) \neq 2$. $a + a + a = (1,0) \neq (0,0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0,0)$, $o(a) \neq 1$. Viszont a Lagrange-tétel (Cauchy-tétel nevű következménye) miatt $o(a) \mid 6$. Ezért $o(a) = 6$, tehát $|[a]| = o(a) = 6 = |\mathbf{Z}_2 \times Z_3|$, és így $[a] = \mathbf{Z}_2 \times \mathbf{Z}_3$.

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1, 1)$. Ekkor $a + a = (0, 2) \neq (0, 0)$ miatt $o(a) \neq 2$. $a + a + a = (1, 0) \neq (0, 0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0, 0)$, $o(a) \neq 1$. Viszont a Lagrange-tétel (Cauchy-tétel nevű következménye) miatt $o(a) \mid 6$. Ezért $o(a) = 6$, tehát $|[a]| = o(a) = 6 = |\mathbf{Z}_2 \times Z_3|$, és így $[a] = \mathbf{Z}_2 \times \mathbf{Z}_3$. Q.e.d. (A 6

Példa direkt szorzatra: Tekintsük a $\mathbf{Z}_2 = (\mathbf{Z}_2; +)$ és $\mathbf{Z}_3 = (\mathbf{Z}_3; +)$ (ciklikus) csoportok direkt szorzatát: azaz a $(\mathbf{Z}_2 \times \mathbf{Z}_3; +)$ csoportot.

Állítjuk, hogy ez a direkt szorzat izomorf a hatelemű $(\mathbf{Z}_6; +)$ ciklikus csoporttal.

Valóban, legyen $a = (1,1)$. Ekkor $a + a = (0,2) \neq (0,0)$ miatt $o(a) \neq 2$. $a + a + a = (1,0) \neq (0,0)$ miatt $o(a) \neq 3$. Mivel $a \neq 0 = (0,0)$, $o(a) \neq 1$. Viszont a Lagrange-tétel (Cauchy-tétel nevű következménye) miatt $o(a) \mid 6$. Ezért $o(a) = 6$, tehát $|[a]| = o(a) = 6 = |\mathbf{Z}_2 \times Z_3|$, és így $[a] = \mathbf{Z}_2 \times \mathbf{Z}_3$. Q.e.d. (A 6 nem olyan nagy szám, a Lagrange-tétel nélkül is boldogultunk volna, de így sokkal tanulságosabb volt.)

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata.

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni).

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni). Hasonló ez ahhoz, mint amikor a pozitív egész számokat prímszámok szorzatára bontjuk

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni). Hasonló ez ahhoz, mint amikor a pozitív egész számokat prímszámok szorzatára bontjuk — mindjárt könnyebb pl. a legnagyobb közös osztó meghatározása.

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni). Hasonló ez ahhoz, mint amikor a pozitív egész számokat prímszámok szorzatára bontjuk — mindjárt könnyebb pl. a legnagyobb közös osztó meghatározása. Az előző példa felfogható úgy is, hogy a $(\mathbf{Z}_6; +)$ Abel-csoportot két kisebb Abel-csoport direkt szorzatára bontottuk.

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni). Hasonló ez ahhoz, mint amikor a pozitív egész számokat prímszámok szorzatára bontjuk — mindjárt könnyebb pl. a legnagyobb közös osztó meghatározása. Az előző példa felfogható úgy is, hogy a $(\mathbf{Z}_6; +)$ Abel-csoportot két kisebb Abel-csoport direkt szorzatára bontottuk. Ez általában is lehetséges
;

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni). Hasonló ez ahhoz, mint amikor a pozitív egész számokat prímszámok szorzatára bontjuk — mindjárt könnyebb pl. a legnagyobb közös osztó meghatározása. Az előző példa felfogható úgy is, hogy a $(\mathbf{Z}_6;+)$ Abel-csoportot két kisebb Abel-csoport direkt szorzatára bontottuk. Ez általában is lehetséges ; az alábbi mély tételt

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni). Hasonló ez ahhoz, mint amikor a pozitív egész számokat prímszámok szorzatára bontjuk — mindjárt könnyebb pl. a legnagyobb közös osztó meghatározása. Az előző példa felfogható úgy is, hogy a $(\mathbf{Z}_6; +)$ Abel-csoportot két kisebb Abel-csoport direkt szorzatára bontottuk. Ez általában is lehetséges ; az alábbi mély tételt — amely a számok prímhatványtényezős felbontására és ezáltal a számelmélet alaptételére emlékeztet

Gyakran nem az a feladat, hogy adott algebrákat direkt összeszorozzunk, hanem az, hogy felismerjük, hogy egy adott algebra más — kisebb, egyszerűbb, jobban ismert — algebrák direkt szorzata. Ezen ún. **direkt tényezők** ismeretében az eredeti algebrával is könnyebben tudunk dolgozni (és ráadásul kevesebb adattal meg tudjuk adni). Hasonló ez ahhoz, mint amikor a pozitív egész számokat prímszámok szorzatára bontjuk — mindjárt könnyebb pl. a legnagyobb közös osztó meghatározása. Az előző példa felfogható úgy is, hogy a $(\mathbf{Z}_6; +)$ Abel-csoportot két kisebb Abel-csoport direkt szorzatára bontottuk. Ez általában is lehetséges ; az alábbi mély tételt — amely a számok prímhatványtényezős felbontására és ezáltal a számelmélet alaptételére emlékeztet — bizonyítás nélkül közöljük.

66. Tétel. **(Véges Abel-csoportok alaptétele)** *Minden véges Abel-csoport felbontható prímhatványrendű ciklikus csoportok direkt szorzatára. Tetszőleges ilyen felbontás esetén a fellépő rendek rendszere egyértelműen meghatározott.*

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (Steinitz-elv), a „felbontható” itt azt jelenti, hogy „izomorf” egy ilyen direkt szorzattal.

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (Steinitz-elv), a „felbontható” itt azt jelenti, hogy „izomorf” egy ilyen direkt szorzattal.

Az egyértelmű meghatározottság azt jelenti, hogy a direkt szorzatban a tényezők sorrendjétől eltekintve a fellépő rendek,

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (Steinitz-elv), a „felbontható” itt azt jelenti, hogy „izomorf” egy ilyen direkt szorzattal.

Az egyértelmű meghatározottság azt jelenti, hogy a direkt szorzatban a tényezők sorrendjétől eltekintve a fellépő rendek, az is hogy melyik hányszor lép fel,

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (Steinitz-elv), a „felbontható” itt azt jelenti, hogy „izomorf” egy ilyen direkt szorzattal.

Az egyértelmű meghatározottság azt jelenti, hogy a direkt szorzatban a tényezők sorrendjétől eltekintve a fellépő rendek, az is hogy melyik hányszor lép fel, egyértelműen meg vannak határozva.

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (Steinitz-elv), a „felbontható” itt azt jelenti, hogy „izomorf” egy ilyen direkt szorzattal.

Az egyértelmű meghatározottság azt jelenti, hogy a direkt szorzatban a tényezők sorrendjétől eltekintve a fellépő rendek, az is hogy melyik hányszor lép fel, egyértelműen meg vannak határozva. Pl. ha az A Abel-csoport három darab négyelmű és egy darab nyolcelemű ciklikus csoport direkt szorzata, akkor egyrészt $|A| = 4^3 \cdot 8 = 2^9 = 512$,

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (Steinitz-elv), a „felbontható” itt azt jelenti, hogy „izomorf” egy ilyen direkt szorzattal.

Az egyértelmű meghatározottság azt jelenti, hogy a direkt szorzatban a tényezők sorrendjétől eltekintve a fellépő rendek, az is hogy melyik hányszor lép fel, egyértelműen meg vannak határozva. Pl. ha az A Abel-csoport három darab négyelmű és egy darab nyolcelemű ciklikus csoport direkt szorzata, akkor egyrészt $|A| = 4^3 \cdot 8 = 2^9 = 512$, másrészt semmilyen más felbontás nem képzelhető el, pl. nem lehet egy 32-elemű és egy 16-elemű ciklikus csoport direkt szorzatára bontani (

Értelmező megjegyések: Annak megfelelően, hogy izomorf algebrákat általában nem óhajtunk megkülönböztetni (Steinitz-elv), a „felbontható” itt azt jelenti, hogy „izomorf” egy ilyen direkt szorzattal.

Az egyértelmű meghatározottság azt jelenti, hogy a direkt szorzatban a tényezők sorrendjétől eltekintve a fellépő rendek, az is hogy melyik hányszor lép fel, egyértelműen meg vannak határozva. Pl. ha az A Abel-csoport három darab négyelmű és egy darab nyolcelemű ciklikus csoport direkt szorzata, akkor egyrészt $|A| = 4^3 \cdot 8 = 2^9 = 512$, másrészt semmilyen más felbontás nem képzelhető el, pl. nem lehet egy 32-elemű és egy 16-elemű ciklikus csoport direkt szorzatára bontani (jóllehet $32 \cdot 16 = 512 = |A|$).

A véges Abel-csoportok alaptételét először egy olyan példán illusztráljuk, amelyet ugyan enélkül is meg tudnánk oldani (csak nehezebben).

Feladat: Legyen A egy n-elemű halmaz, $n \in \mathbf{N}$. Bontsuk ciklikus csoportok direkt szorzatára a $P(A) = (P(A); \triangle)$ Abel-csoportot.

A véges Abel-csoportok alaptételét először egy olyan példán illusztráljuk, amelyet ugyan enélkül is meg tudnánk oldani (csak nehezebben).

Feladat: Legyen A egy n-elemű halmaz, $n \in \mathbf{N}$. Bontsuk ciklikus csoportok direkt szorzatára a $P(A) = (P(A); \triangle)$ Abel-csoportot. (Az első félév elejére — a halmazműveletek témakörébe — való gyakorló feladat annak igazolása, hogy valóban Abel-csoportról van szó.

A véges Abel-csoportok alaptételét először egy olyan példán illusztráljuk, amelyet ugyan enélkül is meg tudnánk oldani (csak nehezebben).

Feladat: Legyen A egy n-elemű halmaz, $n \in \mathbf{N}$. Bontsuk ciklikus csoportok direkt szorzatára a $P(A) = (P(A); \triangle)$ Abel-csoportot. (Az első félév elejére — a halmazműveletek témakörébe — való gyakorló feladat annak igazolása, hogy valóban Abel-csoportról van szó.

Megoldás (A véges Abel-csoportok alaptételére és a Lagrange-tételre építve):

A véges Abel-csoportok alaptételét először egy olyan példán illusztráljuk, amelyet ugyan enélkül is meg tudnánk oldani (csak nehezebben).

Feladat: Legyen A egy n-elemű halmaz, $n \in \mathbf{N}$. Bontsuk ciklikus csoportok direkt szorzatára a $P(A) = (P(A); \triangle)$ Abel-csoportot. (Az első félév elejére — a halmazműveletek témakörébe — való gyakorló feladat annak igazolása, hogy valóban Abel-csoportról van szó.

Megoldás (A véges Abel-csoportok alaptételére és a Lagrange-tételre építve): Világos, hogy ha $(P(A); \triangle)$ izomorf a

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i :=$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| =$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i|$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i| \ \ |$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i| \mid |B_1 \times \cdots \times B_k| =$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i| \mid |B_1 \times \cdots \times B_k| = |P(A)| =$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i| \mid |B_1 \times \cdots \times B_k| = |P(A)| = 2^{|A|} =$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i| \mid |B_1 \times \cdots \times B_k| = |P(A)| = 2^{|A|} = 2^n.$$

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i| \mid |B_1 \times \cdots \times B_k| = |P(A)| = 2^{|A|} = 2^n.$$

Az a Lagrange-tétel nélkül is kijött volna a Descartes-szorzat elemszámára gondolva, sőt nemcsak csoportokra hanem tetszőleges véges algebrákra is, hogy

$$B_1 \times \cdots \times B_k$$

direkt szorzattal, akkor $i = 1, \ldots, k$-ra B_i izomorf a direkt szorzat alábbi részcsoportjával:

$$S_i := \{(0, \ldots, 0, \overbrace{x}^{i\text{-edik}}, 0, \ldots, 0) : x \in B_i\}.$$

Ezért a Lagrange-tételből

$$|B_i| = |S_i| \mid |B_1 \times \cdots \times B_k| = |P(A)| = 2^{|A|} = 2^n.$$

Az a Lagrange-tétel nélkül is kijött volna a Descartes-szorzat elemszámára gondolva, sőt nemcsak csoportokra hanem tetszőleges véges algebrákra is, hogy a direkt tényező elemszáma (azaz rendje) osztja a direkt szorzat rendjét. Azonban nekünk a részcsoportra is szükségünk lesz.)

Tehát (

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$.

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban nem léphet fel 2-nél nagyobb rendű direkt tényező, mert akkor

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban nem léphet fel 2-nél nagyobb rendű direkt tényező, mert akkor valamelyik S_i

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban nem léphet fel 2-nél nagyobb rendű direkt tényező, mert akkor valamelyik S_i c

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban nem léphet fel 2-nél nagyobb rendű direkt tényező, mert akkor valamelyik S_i ci

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Ármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban nem léphet fel 2-nél nagyobb rendű direkt tényező, mert akkor valamelyik S_i cik

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban nem léphet fel 2-nél nagyobb rendű direkt tényező, mert akkor valamelyik S_i ciklikus részcsoport rendje is nagyobb lenne 2-nél,

Tehát (és ez általában is igaz véges csoportokra, nemcsak ebben a feladatban):

16. Állítás. *Véges csoportok esetén mindegyik direkt tényező egyrészt izomorf a direkt szorzat valamely részcsoportjával, másrészt a rendje osztja a direkt szorzat rendjét.*

Mármost ha $X \in P(A)$, akkor $X \triangle X = \emptyset =$ egységelem miatt $o(X) \leq 2$. Ezért a keresett direkt felbontásban nem léphet fel 2-nél nagyobb rendű direkt tényező, mert akkor valamelyik S_i ciklikus részcsoport rendje is nagyobb lenne 2-nél, és így $P(A)$-ban lenne 2-nél nagyobb rendű elem.

Tehát mindegyik direkt tényező a kételemű ciklikus csoport.

Tehát mindegyik direkt tényező a kételemű ciklikus csoport. Mivel direkt szorzáskor az elemszámok (

Tehát mindegyik direkt tényező a kételemű ciklikus csoport. Mivel direkt szorzáskor az elemszámok (azaz a rendek) szorzódnak, kapjuk, hogy $(P(A);\triangle)$ izomorf a kételemű $(\mathbf{Z}_2;+)$ ciklikus csoport

Tehát mindegyik direkt tényező a kételemű ciklikus csoport. Mivel direkt szorzáskor az elemszámok (azaz a rendek) szorzódnak, kapjuk, hogy $(P(A); \triangle)$ izomorf a kételemű $(\mathbf{Z}_2; +)$ ciklikus csoport n-edik direkt hatványával.

Tehát mindegyik direkt tényező a kételemű ciklikus csoport. Mivel direkt szorzáskor az elemszámok (azaz a rendek) szorzódnak, kapjuk, hogy $(P(A); \triangle)$ izomorf a kételemű $(\mathbf{Z}_2; +)$ ciklikus csoport n-edik direkt hatványával. Q.e.d.

Feladat Legyen p és q két különböző prímszám. Ciklikus-e a $(\mathbf{Z}_p \times \mathbf{Z}_q; +)$ csoport?

Megoldás:

Megoldás:

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot.

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata,

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok)

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t.

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t. Ezért a direkt tényezők rendje p, illetve q. A véges ciklikus csoportok leírása szerint a direkt tényezők —

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t. Ezért a direkt tényezők rendje p, illetve q. A véges ciklikus csoportok leírása szerint a direkt tényezők — izomorfia erejéig —

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t. Ezért a direkt tényezők rendje p, illetve q. A véges ciklikus csoportok leírása szerint a direkt tényezők — izomorfia erejéig — $(\mathbf{Z}_p;+)$ és a $(\mathbf{Z}_q;+)$.

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t. Ezért a direkt tényezők rendje p, illetve q. A véges ciklikus csoportok leírása szerint a direkt tényezők — izomorfia erejéig — $(\mathbf{Z}_p;+)$ és a $(\mathbf{Z}_q;+)$. Tehát $(\mathbf{Z}_{pq};+)$ —

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t. Ezért a direkt tényezők rendje p, illetve q. A véges ciklikus csoportok leírása szerint a direkt tényezők — izomorfia erejéig — $(\mathbf{Z}_p;+)$ és a $(\mathbf{Z}_q;+)$. Tehát $(\mathbf{Z}_{pq};+)$ — ami ciklikus — izomorf $(\mathbf{Z}_p \times \mathbf{Z}_q;+)$-szal. Ezért $(\mathbf{Z}_p \times \mathbf{Z}_q;+)$ is ciklikus.

Megoldás: Tekintsük a $(\mathbf{Z}_{pq}; +)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t. Ezért a direkt tényezők rendje p, illetve q. A véges ciklikus csoportok leírása szerint a direkt tényezők — izomorfia erejéig — $(\mathbf{Z}_p; +)$ és a $(\mathbf{Z}_q; +)$. Tehát $(\mathbf{Z}_{pq}; +)$ — ami ciklikus — izomorf $(\mathbf{Z}_p \times \mathbf{Z}_q; +)$-szal. Ezért $(\mathbf{Z}_p \times \mathbf{Z}_q; +)$ is ciklikus.

(A feladat a véges Abel-csoportok alaptétele nélkül is könnyen megoldható.

Megoldás: Tekintsük a $(\mathbf{Z}_{pq};+)$ ciklikus csoportot. A véges Abel-csoportok alaptétele szerint ez prímhatványrendű ciklikus csoportok direkt szorzata, és azt is tudjuk, hogy a direkt tényezők rendjei (tehát a szóbanforgó prímhatványok) osztják $|\mathbf{Z}_{pq}| = pq$-t. Ezért a direkt tényezők rendje p, illetve q. A véges ciklikus csoportok leírása szerint a direkt tényezők — izomorfia erejéig — $(\mathbf{Z}_p;+)$ és a $(\mathbf{Z}_q;+)$. Tehát $(\mathbf{Z}_{pq};+)$ — ami ciklikus — izomorf $(\mathbf{Z}_p \times \mathbf{Z}_q;+)$-szal. Ezért $(\mathbf{Z}_p \times \mathbf{Z}_q;+)$ is ciklikus.

(A feladat a véges Abel-csoportok alaptétele nélkül is könnyen megoldható. Nemsokára többet is igazolunk.)

Kongruencia

Kongruencia(reláció)

Kongruencia(reláció)

Legyen $\Theta \subseteq A^2$ egy ekvivalenciareláció az $\mathbf{A} = (A; F)$ algebra tartóhalmazán.

Kongruencia(reláció)

Legyen $\Theta \subseteq A^2$ egy ekvivalenciareláció az $\mathbf{A} = (A; F)$ algebra tartóhalmazán. Ha az algebra műveletei **megőrzik** Θ-t, azaz

Kongruencia(reláció)

Legyen $\Theta \subseteq A^2$ egy ekvivalenciareláció az $\mathbf{A} = (A; F)$ algebra tartóhalmazán. Ha az algebra műveletei **megőrzik** Θ-t, azaz bármely $f \in F$-re, mondjuk $m = m_f$-változósra,

Kongruencia(reláció)

Legyen $\Theta \subseteq A^2$ egy ekvivalenciareláció az $\mathbf{A} = (A; F)$ algebra tartóhalmazán. Ha az algebra műveletei **megőrzik** Θ-t, azaz bármely $f \in F$-re, mondjuk $m = m_f$-változósra, és bármely $a_1, \ldots, a_m, b_1, \ldots, b_m \in A$ elemekre

Kongruencia(reláció)

Legyen $\Theta \subseteq A^2$ egy ekvivalenciareláció az $\mathbf{A} = (A; F)$ algebra tartóhalmazán. Ha az algebra műveletei **megőrzik** Θ-t, azaz bármely $f \in F$-re, mondjuk $m = m_f$-változósra, és bármely $a_1, \ldots, a_m,\ b_1, \ldots, b_m \in A$ elemekre

$$(a_1, b_1), \ldots, (a_m, b_m) \in \Theta \Longrightarrow$$
$$(f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)) \in \Theta.$$

Kongruencia(reláció)

Legyen $\Theta \subseteq A^2$ egy ekvivalenciareláció az $\mathcal{A} = (A; F)$ algebra tartóhalmazán. Ha az algebra műveletei **megőrzik** Θ-t, azaz bármely $f \in F$-re, mondjuk $m = m_f$-változósra, és bármely $a_1, \ldots, a_m, b_1, \ldots, b_m \in A$ elemekre

$$(a_1, b_1), \ldots, (a_m, b_m) \in \Theta \Longrightarrow$$
$$(f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)) \in \Theta.$$

akkor azt mondjuk, hogy Θ **kongruencia** vagy **kongruenciareláció** az $\mathcal{A}$ algebrán.

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$,

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 :\ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia.

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \; m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m)$)

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \implies a_1 + a_2 \equiv b_1 + b_2 \pmod m,$$

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m$,
$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m))$

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m,$$
$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 a_2 \equiv b_1 b_2 \pmod m,$$

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m,$$
$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 a_2 \equiv b_1 b_2 \pmod m,$$

azaz a mostani jelöléssel

$$(a_1, b_1), (a_2, b_2) \in \Theta$$

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m,$$
$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 a_2 \equiv b_1 b_2 \pmod m,$$

azaz a mostani jelöléssel

$$(a_1, b_1), (a_2, b_2) \in \Theta \Longrightarrow (a_1 + a_2, b_1 + b_2) \in \Theta,$$

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x,y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$$(a_1 \equiv b_1 \pmod m \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m,$$
$$(a_1 \equiv b_1 \pmod m \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 a_2 \equiv b_1 b_2 \pmod m,$$

azaz a mostani jelöléssel

$$(a_1, b_1), (a_2, b_2) \in \Theta \Longrightarrow (a_1 + a_2, b_1 + b_2) \in \Theta,$$
$$(a_1, b_1), (a_2, b_2) \in \Theta$$

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \ m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$$(a_1 \equiv b_1 \pmod m \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m,$$
$$(a_1 \equiv b_1 \pmod m \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 a_2 \equiv b_1 b_2 \pmod m,$$

azaz a mostani jelöléssel

$$(a_1, b_1), (a_2, b_2) \in \Theta \Longrightarrow (a_1 + a_2, b_1 + b_2) \in \Theta,$$
$$(a_1, b_1), (a_2, b_2) \in \Theta \Longrightarrow (a_1 a_2, b_1 b_2) \in \Theta.$$

Motiváló példa: A $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrű és $m \in \mathbf{N}_0$ esetén legyen $\Theta = \{(x, y) \in \mathbf{Z}^2 : \; m \mid x - y\}$, azaz a modulo m *számelméleti* kongruencia. Ekkor Θ az imént definiált absztrakt algebrai értelemben is kongruencia, hiszen tanultuk a múlt félévben, hogy ekvivalencia, továbbá

$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m,$$
$$(a_1 \equiv b_1 \pmod m) \wedge a_2 \equiv b_2 \pmod m) \Longrightarrow a_1 a_2 \equiv b_1 b_2 \pmod m,$$

azaz a mostani jelöléssel

$$(a_1, b_1), (a_2, b_2) \in \Theta \Longrightarrow (a_1 + a_2, b_1 + b_2) \in \Theta,$$
$$(a_1, b_1), (a_2, b_2) \in \Theta \Longrightarrow (a_1 a_2, b_1 b_2) \in \Theta.$$

T

Természetesen a modulo m kongruencia egyúttal a $(\mathbf{Z}; +)$ csoportnak is és a $(\mathbf{Z}; \cdot)$ félcsoportnak is kongruenciája.

Másik példa: az $\{(a, a) : a \in A\}$ **egyenlőségreláció**

Természetesen a modulo m kongruencia egyúttal a $(\mathbf{Z}; +)$ csoportnak is és a $(\mathbf{Z}; \cdot)$ félcsoportnak is kongruenciája.

Másik példa: az $\{(a, a) : a \in A\}$ **egyenlőségreláció** és az A^2 **teljes reláció**

Természetesen a modulo m kongruencia egyúttal a $(\mathbf{Z}; +)$ csoportnak is és a $(\mathbf{Z}; \cdot)$ félcsoportnak is kongruenciája.

Másik példa: az $\{(a, a) : a \in A\}$ **egyenlőségreláció** és az A^2 **teljes reláció** mindig kongruencia.

Természetesen a modulo m kongruencia egyúttal a $(\mathbf{Z};+)$ csoportnak is és a $(\mathbf{Z};\cdot)$ félcsoportnak is kongruenciája.

Másik példa: az $\{(a,a) : a \in A\}$ **egyenlőségreláció** és az A^2 **teljes reláció** mindig kongruencia. Ezen két kongruenciát az A algebra **triviális kongruenciáinak** nevezzük.

Emlékeztető: Ha $\Theta \subseteq A^2$ ekvivalenciareláció, akkor $a \in A$-ra $\overline{a}$
(

Emlékeztető: Ha $\Theta \subseteq A^2$ ekvivalenciareláció, akkor $a \in A$-ra $\overline{a}$ (vagy esetleg $[a]\Theta$)

Emlékeztető: Ha $\Theta \subseteq A^2$ ekvivalenciareláció, akkor $a \in A$-ra $\overline{a}$ (vagy esetleg $[a]\Theta$) jelöli az

$$\{x \in A : (a, x) \in \Theta\}$$

halmazt, azaz a a elem Θ-osztályát.

Emlékeztető: Ha $\Theta \subseteq A^2$ ekivalenciareláció, akkor $a \in A$-ra $\overline{a}$ (vagy esetleg $[a]\Theta$) jelöli az

$$\{x \in A : (a, x) \in \Theta\}$$

halmazt, azaz a a elem Θ-osztályát. Ezen Θ-osztályok halmaza, azaz

$$\{\overline{a} : a \in A\}$$

egy osztályozást alkot az A halmazon.

Emlékeztető: Ha $\Theta \subseteq A^2$ ekivalenciareláció, akkor $a \in A$-ra $\overline{a}$ (vagy esetleg $[a]\Theta$) jelöli az

$$\{x \in A : (a,x) \in \Theta\}$$

halmazt, azaz a a elem Θ-osztályát. Ezen Θ-osztályok halmaza, azaz

$$\{\overline{a} : a \in A\}$$

egy osztályozást alkot az A halmazon. Ezt az osztályozást a Θ-hoz tartozó osztályozásnak nevezzük és

Emlékeztető: Ha $\Theta \subseteq A^2$ ekivalenciareláció, akkor $a \in A$-ra $\overline{a}$ (vagy esetleg $[a]\Theta$) jelöli az

$$\{x \in A : (a, x) \in \Theta\}$$

halmazt, azaz a a elem Θ-osztályát. Ezen Θ-osztályok halmaza, azaz

$$\{\overline{a} : a \in A\}$$

egy osztályozást alkot az A halmazon. Ezt az osztályozást a Θ-hoz tartozó osztályozásnak nevezzük és $\mathcal{C}_\Theta$-val jelöljük.

Azt is tanultuk, hogy rögzített A halmaz esetén az ekvivalenciák és az osztályozások halmaza között bijekció van, a $\Theta \mapsto \mathcal{C}_\Theta$ leképezés bijektív, Azt is tanultuk, hogy rögzített A halmaz esetén az ekvivalenciák és az osztályozások halmaza között bijekció van, a $\Theta \mapsto \mathcal{C}_\Theta$ leképezés bijektív, tehát az ekvivalenciák és az osztályozások egymást kölcsönösen meghatározzák, „lényegében ugyanazok”.

Azt is tanultuk, hogy rögzített A halmaz esetén az ekvivalenciák és az osztályozások halmaza között bijekció van, a $\Theta \mapsto \mathcal{C}_\Theta$ leképezés bijektív, tehát az ekvivalenciák és az osztályozások egymást kölcsönösen meghatározzák, „lényegében ugyanazok".

Ha A algebra, akkor a kongruenciák — mint speciális ekvivalenciák — által meghatározott osztályozásokat **kompatibilis osztályozásoknak** szokás nevezni.

Faktoralgebra

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció)

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $A = (A; F)$ algebrán. Jelölje

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathcal{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát,

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathbf{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_{\Theta}$.

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathcal{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_\Theta$. Az A/Θ halmazt egy $\mathcal{A}/\Theta = (A/\Theta; F)$ algebrává tesszük azáltal, hogy

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathcal{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_\Theta$. Az A/Θ halmazt egy $\mathcal{A}/\Theta = (A/\Theta; F)$ algebrává tesszük azáltal, hogy minden egyes, mondjuk m-változós, $f \in F$-re definiáljuk az $f = f_{\mathcal{A}/\Theta}$ műveletet:

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathbf{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_\Theta$. Az A/Θ halmazt egy $\mathbf{A}/\Theta = (A/\Theta; F)$ algebrává tesszük azáltal, hogy minden egyes, mondjuk m-változós, $f \in F$-re definiáljuk az $f = f_{\mathbf{A}/\Theta}$ műveletet: ha $X_1, \ldots, X_m \in A/\Theta$,

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathbf{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_\Theta$. Az A/Θ halmazt egy $\mathbf{A}/\Theta = (A/\Theta; F)$ algebrává tesszük azáltal, hogy minden egyes, mondjuk m-változós, $f \in F$-re definiáljuk az $f = f_{A/\Theta}$ műveletet: ha $X_1, \ldots, X_m \in A/\Theta$, akkor tetszőlegesen választott $a_1 \in X_1$, ..., $a_m \in X_m$ **reprezentánsokat** véve legyen

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathcal{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_\Theta$. Az A/Θ halmazt egy $\mathcal{A}/\Theta = (A/\Theta; F)$ algebrává tesszük azáltal, hogy minden egyes, mondjuk m-változós, $f \in F$-re definiáljuk az $f = f_{\mathcal{A}/\Theta}$ műveletet: ha $X_1, \ldots, X_m \in A/\Theta$, akkor tetszőlegesen választott $a_1 \in X_1$, ..., $a_m \in X_m$ **reprezentánsokat** véve legyen $f(X_1, \ldots, X_m)$ az

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathbf{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_\Theta$. Az A/Θ halmazt egy $\mathbf{A}/\Theta = (A/\Theta; F)$ algebrává tesszük azáltal, hogy minden egyes, mondjuk m-változós, $f \in F$-re definiáljuk az $f = f_{A/\Theta}$ műveletet: ha $X_1, \ldots, X_m \in A/\Theta$, akkor tetszőlegesen választott $a_1 \in X_1$, ..., $a_m \in X_m$ **reprezentánsokat** véve legyen $f(X_1, \ldots, X_m)$ az $f(a_1, \ldots, a_m)$ elem Θ-osztálya.

Faktoralgebra

Definíció: Legyen Θ egy kongruencia(reláció) az $\mathcal{A} = (A; F)$ algebrán. Jelölje A/Θ a Θ-osztályok halmazát, azaz $A/\Theta = \mathcal{C}_\Theta$. Az A/Θ halmazt egy $\mathcal{A}/\Theta = (A/\Theta; F)$ algebrává tesszük azáltal, hogy minden egyes, mondjuk m-változós, $f \in F$-re definiáljuk az $f = f_{\mathcal{A}/\Theta}$ műveletet: ha $X_1, \ldots, X_m \in A/\Theta$, akkor tetszőlegesen választott $a_1 \in X_1$, …, $a_m \in X_m$ **reprezentánsokat** véve legyen $f(X_1, \ldots, X_m)$ az $f(a_1, \ldots, a_m)$ elem Θ-osztálya. Formulákkal:

$$f(\overline{a_1}, \ldots, \overline{a_m}) = \overline{f(a_1, \ldots, a_m)}.$$

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától.

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától. Ha $a_1 \in X_1$, $\ldots$, $a_m \in X_m$ és

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától. Ha $a_1 \in X_1$, …, $a_m \in X_m$ és $b_1 \in X_1$, …, $b_m \in X_m$, azaz ha kétféleképpen választunk reprezentánsokat, akkor a reláció–osztályozás kapcsolat szerint

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától. Ha $a_1 \in X_1$, ..., $a_m \in X_m$ és $b_1 \in X_1$, ..., $b_m \in X_m$, azaz ha kétféleképpen választunk reprezentánsokat, akkor a reláció–osztályozás kapcsolat szerint $(a_1, b_1), \ldots, (a_m, b_m) \in \Theta$.

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától. Ha $a_1 \in X_1$, ..., $a_m \in X_m$ és $b_1 \in X_1$, ..., $b_m \in X_m$, azaz ha kétféleképpen választunk reprezentánsokat, akkor a reláció–osztályozás kapcsolat szerint $(a_1, b_1), \ldots, (a_m, b_m) \in \Theta$. Mivel a műveletek definíció szerint megőrzik a kongruenciát, kapjuk hogy $(f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)) \in \Theta$.

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától. Ha $a_1 \in X_1$, ..., $a_m \in X_m$ és $b_1 \in X_1$, ..., $b_m \in X_m$, azaz ha kétféleképpen választunk reprezentánsokat, akkor a reláció–osztályozás kapcsolat szerint $(a_1, b_1), \ldots, (a_m, b_m) \in \Theta$. Mivel a műveletek definíció szerint megőrzik a kongruenciát, kapjuk hogy $(f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)) \in \Theta$. Innen adódik, hogy

$$\overline{f(a_1, \ldots, a_m)} = \overline{f(b_1, \ldots, b_m)},$$

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától. Ha $a_1 \in X_1$, ..., $a_m \in X_m$ és $b_1 \in X_1$, ..., $b_m \in X_m$, azaz ha kétféleképpen választunk reprezentánsokat, akkor a reláció–osztályozás kapcsolat szerint $(a_1, b_1), \ldots, (a_m, b_m) \in \Theta$. Mivel a műveletek definíció szerint megőrzik a kongruenciát, kapjuk hogy $(f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)) \in \Theta$. Innen adódik, hogy

$$\overline{f(a_1, \ldots, a_m)} = \overline{f(b_1, \ldots, b_m)},$$

ami azt mutatja, hogy az eredmény valóban nem függ a reprezentánsok választásától.

17. Állítás. *A faktoralgebra definíciója értelmes.*

Bizonyítás: Csak azt kell bizonyítani, hogy a művelet eredménye nem függ a reprezentánsok választásától. Ha $a_1 \in X_1$, ..., $a_m \in X_m$ és $b_1 \in X_1$, ..., $b_m \in X_m$, azaz ha kétféleképpen választunk reprezentánsokat, akkor a reláció–osztályozás kapcsolat szerint $(a_1, b_1), \ldots, (a_m, b_m) \in \Theta$. Mivel a műveletek definíció szerint megőrzik a kongruenciát, kapjuk hogy $(f(a_1, \ldots, a_m), f(b_1, \ldots, b_m)) \in \Theta$. Innen adódik, hogy

$$\overline{f(a_1, \ldots, a_m)} = \overline{f(b_1, \ldots, b_m)},$$

ami azt mutatja, hogy az eredmény valóban nem függ a reprezentánsok választásától. Q.e.d.

Példa: A $(\mathbf{Z};\cdot)$ monoidon tekintsük az „azonos előjelűek” relációt. Tehát $\Theta := \{(x,y)\in \mathbf{Z}^2$: x és y azonos előjelűek.$\}$.

Példa: A $(\mathbf{Z};\cdot)$ monoidon tekintsük az „azonos előjelűek" relációt. Tehát $\Theta := \{(x, y) \in \mathbf{Z}^2 \ : \ x$ és y azonos előjelűek.$\}$. Ekkor Θ kongruencia, hiszen

Példa: A $(\mathbf{Z};\cdot)$ monoidon tekintsük az „azonos előjelűek” relációt. Tehát $\Theta := \{(x,y) \in \mathbf{Z}^2 \,:\, x$ és y azonos előjelűek.$\}$. Ekkor Θ kongruencia, hiszen a szorzat előjele csak a tényezők előjelétől függ, tehát ha a szorzat tényezőit azonos előjelű tényezőkre cseréljük le,

Példa: A $(\mathbf{Z};\cdot)$ monoidon tekintsük az „azonos előjelűek” relációt. Tehát $\Theta := \{(x,y) \in \mathbf{Z}^2 :\ x$ és y azonos előjelűek.$\}$. Ekkor Θ kongruencia, hiszen a szorzat előjele csak a tényezők előjelétől függ, tehát ha a szorzat tényezőit azonos előjelű tényezőkre cseréljük le, az eredetivel azonos előjelű szorzathoz jutunk.

Példa: A $(\mathbf{Z}; \cdot)$ monoidon tekintsük az „azonos előjelűek” relációt. Tehát $\Theta := \{(x, y) \in \mathbf{Z}^2 :\ x$ és y azonos előjelűek.$\}$. Ekkor Θ kongruencia, hiszen a szorzat előjele csak a tényezők előjelétől függ, tehát ha a szorzat tényezőit azonos előjelű tényezőkre cseréljük le, az eredetivel azonos előjelű szorzathoz jutunk.

Ekkor a faktoralgebra a Θ-nak megfelelő osztályozásból áll, azaz

Példa: A $(\mathbf{Z};\cdot)$ monoidon tekintsük az „azonos előjelűek" relációt. Tehát $\Theta := \{(x, y) \in \mathbf{Z}^2 : x$ és y azonos előjelűek.$\}$. Ekkor Θ kongruencia, hiszen a szorzat előjele csak a tényezők előjelétől függ, tehát ha a szorzat tényezőit azonos előjelű tényezőkre cseréljük le, az eredetivel azonos előjelű szorzathoz jutunk.

Ekkor a faktoralgebra a Θ-nak megfelelő osztályozásból áll, azaz a tartóhalmaza

Példa: A $(\mathbf{Z};\cdot)$ monoidon tekintsük az „azonos előjelűek" relációt. Tehát $\Theta := \{(x,y) \in \mathbf{Z}^2 :\ x$ és y azonos előjelűek.$\}$. Ekkor Θ kongruencia, hiszen a szorzat előjele csak a tényezők előjelétől függ, tehát ha a szorzat tényezőit azonos előjelű tényezőkre cseréljük le, az eredetivel azonos előjelű szorzathoz jutunk.

Ekkor a faktoralgebra a Θ-nak megfelelő osztályozásból áll, azaz a tartóhalmaza $\{\{$pozitív egészek$\}$, $\{$negatív egészek$\}, \{0\}\}$.

Példa: A $(\mathbf{Z}; \cdot)$ monoidon tekintsük az „azonos előjelűek" relációt. Tehát $\Theta := \{(x, y) \in \mathbf{Z}^2 :\ x$ és y azonos előjelűek.$\}$. Ekkor Θ kongruencia, hiszen a szorzat előjele csak a tényezők előjelétől függ, tehát ha a szorzat tényezőit azonos előjelű tényezőkre cseréljük le, az eredetivel azonos előjelű szorzathoz jutunk.

Ekkor a faktoralgebra a Θ-nak megfelelő osztályozásból áll, azaz a tartóhalmaza $\{\{$pozitív egészek$\}$, $\{$negatív egészek$\}, \{0\}\}$.

A $-\mathbf{N} = \{$negatív egészek$\}$ jelölést bevezetve a $(\mathbf{Z}; \cdot)/\Theta$ faktoralgebra

Példa: A $(\mathbf{Z};\cdot)$ monoidon tekintsük az „azonos előjelűek” relációt. Tehát $\ominus := \{(x,y)\in \mathbf{Z}^2 :\ x$ és y azonos előjelűek.$\}$. Ekkor $\ominus$ kongruencia, hiszen a szorzat előjele csak a tényezők előjelétől függ, tehát ha a szorzat tényezőit azonos előjelű tényezőkre cseréljük le, az eredetivel azonos előjelű szorzathoz jutunk.

Ekkor a faktoralgebra a $\ominus$-nak megfelelő osztályozásból áll, azaz a tartóhalmaza $\{\{$pozitív egészek$\}$, $\{$negatív egészek$\}, \{0\}\}$.

A $-\mathbf{N} = \{$negatív egészek$\}$ jelölést bevezetve a $(\mathbf{Z};\cdot)/\ominus$ faktoralgebra (azaz faktorgrupoid) művelettáblázata az alábbi.

$\cdot$	$\mathbf{N}$	$-\mathbf{N}$	$\{0\}$
$\mathbf{N}$	$\mathbf{N}$	$-\mathbf{N}$	$\{0\}$
$-\mathbf{N}$	$-\mathbf{N}$	$\mathbf{N}$	$\{0\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$

A $(-\mathbf{N}) \cdot \mathbf{N} = -\mathbf{N}$ például azért igaz, mert (a szorzás általános iskolai előjelszabálya miatt) a $(-2) \cdot 3$, a $(-7) \cdot 4$, a $(-1) \cdot 1$, stb. szorzatok mindegyikének $-\mathbf{N}$ az osztálya.

$\cdot$	$\mathbf{N}$	$-\mathbf{N}$	$\{0\}$
$\mathbf{N}$	$\mathbf{N}$	$-\mathbf{N}$	$\{0\}$
$-\mathbf{N}$	$-\mathbf{N}$	$\mathbf{N}$	$\{0\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$

A $(-\mathbf{N}) \cdot \mathbf{N} = -\mathbf{N}$ például azért igaz, mert (a szorzás általános iskolai előjelszabálya miatt) a $(-2) \cdot 3$, a $(-7) \cdot 4$, a $(-1) \cdot 1$, stb. szorzatok mindegyikének $-\mathbf{N}$ az osztálya.

Látható, hogy a faktoralgebra izomorf a $\{\{0, 1, -1\}; \cdot\}$ monoiddal.

Példa: Már korábban is szó volt a $(\mathbf{Z}_m; +)$ ciklikus csoportról.

Példa: Már korábban is szó volt a $(\mathbf{Z}_m;+)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Példa: Már korábban is szó volt a $(\mathbf{Z}_m;+)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z} = (\mathbf{Z};+,\cdot)$ gyűrűn a modulo m (számelméleti) kongruencia

Példa: Már korábban is szó volt a $(\mathbf{Z}_m; +)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrűn a modulo m (számelméleti) kongruencia algebrai értelemben is kongruencia (

Példa: Már korábban is szó volt a $(\mathbf{Z}_m;+)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z} = (\mathbf{Z};+,\cdot)$ gyűrűn a modulo m (számelméleti) kongruencia algebrai értelemben is kongruencia ($m \in \mathbf{N}$). A megfelelő kompatibilis osztályozás osztályai az $\bar{i} := \{i + mx : x \in \mathbf{Z}\}$ maradékosztályok,

Példa: Már korábban is szó volt a $(\mathbf{Z}_m;+)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z} = (\mathbf{Z};+,\cdot)$ gyűrűn a modulo m (számelméleti) kongruencia algebrai értelemben is kongruencia ($m \in \mathbf{N}$). A megfelelő kompatibilis osztályozás osztályai az $\bar{i} := \{i + mx : x \in \mathbf{Z}\}$ maradékosztályok, $i \in \mathbf{Z}$.

Példa: Már korábban is szó volt a $(\mathbf{Z}_m;+)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z}=(\mathbf{Z};+,\cdot)$ gyűrűn a modulo m (számelméleti) kongruencia algebrai értelemben is kongruencia ($m \in \mathbf{N}$). A megfelelő kompatibilis osztályozás osztályai az $\bar{i} := \{i+mx : x \in \mathbf{Z}\}$ maradékosztályok, $i \in \mathbf{Z}$. Ezek nem mind különbözők;

Példa: Már korábban is szó volt a $(\mathbf{Z}_m; +)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrűn a modulo m (számelméleti) kongruencia algebrai értelemben is kongruencia ($m \in \mathbf{N}$). A megfelelő kompatibilis osztályozás osztályai az $\bar{i} := \{i + mx : x \in \mathbf{Z}\}$ maradékosztályok, $i \in \mathbf{Z}$. Ezek nem mind különbözők; a páronként különbözők éppen a $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$. A $\mathbf{Z}/(\mathrm{mod}\ m)$ faktoralgebra

Példa: Már korábban is szó volt a $(\mathbf{Z}_m; +)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z} = (\mathbf{Z}; +, \cdot)$ gyűrűn a modulo m (számelméleti) kongruencia algebrai értelemben is kongruencia ($m \in \mathbf{N}$). A megfelelő kompatibilis osztályozás osztályai az $\bar{i} := \{i + mx : x \in \mathbf{Z}\}$ maradékosztályok, $i \in \mathbf{Z}$. Ezek nem mind különbözők; a páronként különbözők éppen a $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$. A $\mathbf{Z}/(\mathrm{mod}\ m)$ faktoralgebra — amely gyűrű — a $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$ maradékosztályokból áll, és (

Példa: Már korábban is szó volt a $(\mathbf{Z}_m;+)$ ciklikus csoportról. Most sokkal természetesebb módon jutunk el ugyanezen fogalomhoz, sőt egyúttal a szorzást is definiáljuk, és ily módon gyűrűt definiálunk.

Láttuk, hogy a $\mathbf{Z} = (\mathbf{Z};+,\cdot)$ gyűrűn a modulo m (számelméleti) kongruencia algebrai értelemben is kongruencia ($m \in \mathbf{N}$). A megfelelő kompatibilis osztályozás osztályai az $\bar{i} := \{i + mx : x \in \mathbf{Z}\}$ maradékosztályok, $i \in \mathbf{Z}$. Ezek nem mind különbözők; a páronként különbözők éppen a $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$. A $\mathbf{Z}/(\mathrm{mod}\ m)$ faktoralgebra — amely gyűrű — a $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$ maradékosztályokból áll, és (ahogy azt korábban tanultuk), a műveleteket a reprezentánsokon végezzük.

Tehát a továbbiakban a $(\mathbf{Z}_m;+,\cdot)$ gyűrűt, azaz a **modulo m maradékosztályok gyűrűjét** úgy definiáljuk, mint az egész számok gyűrűjének a modulo m kongruencia szerinti faktoralgebráját!

Tehát a továbbiakban a $(\mathbf{Z}_m;+,\cdot)$ gyűrűt, azaz a **modulo m maradékosztályok gyűrűjét** úgy definiáljuk, mint az egész számok gyűrűjének a modulo m kongruencia szerinti faktoralgebráját! Tetszőleges elemét jelölheti

Tehát a továbbiakban a $(\mathbf{Z}_m;+,\cdot)$ gyűrűt, azaz a **modulo m maradékosztályok gyűrűjét** úgy definiáljuk, mint az egész számok gyűrűjének a modulo m kongruencia szerinti faktoralgebráját! Tetszőleges elemét jelölheti

$$\bar{i} = \{x \in \mathbf{Z} : x \equiv i \pmod{m}\} \qquad (i \in \mathbf{Z})$$

Tehát a továbbiakban a $(\mathbf{Z}_m; +, \cdot)$ gyűrűt, azaz a **modulo m maradékosztályok gyűrűjét** úgy definiáljuk, mint az egész számok gyűrűjének a modulo m kongruencia szerinti faktoralgebráját! Tetszőleges elemét jelölheti

$$\overline{i} = \{x \in \mathbf{Z} : x \equiv i \pmod m\} \qquad (i \in \mathbf{Z}), \text{ vagy}$$
$$\overline{i} \qquad (0 \le i < m)$$

Tehát a továbbiakban a $(\mathbf{Z}_m;+,\cdot)$ gyűrűt, azaz a **modulo m maradékosztályok gyűrűjét** úgy definiáljuk, mint az egész számok gyűrűjének a modulo m kongruencia szerinti faktoralgebráját! Tetszőleges elemét jelölheti

$$\overline{i}=\{x\in\mathbf{Z}: x\equiv i \pmod m\} \qquad (i\in\mathbf{Z}),\ \text{vagy}$$

$$\overline{i} \qquad (0\le i<m),\ \text{vagy ha nem okoz}$$

$$\text{félreértést: } i \qquad (0\le i<m).$$

Tehát a továbbiakban a $(\mathbf{Z}_m;+,\cdot)$ gyűrűt, azaz a **modulo m maradékosztályok gyűrűjét** úgy definiáljuk, mint az egész számok gyűrűjének a modulo m kongruencia szerinti faktoralgebráját! Tetszőleges elemét jelölheti

$$\overline{i} = \{x \in \mathbf{Z} : x \equiv i \pmod m\} \qquad (i \in \mathbf{Z}), \text{ vagy}$$

$$\overline{i} \qquad (0 \le i < m), \text{ vagy ha nem okoz}$$

$$\text{félreértést: } i \qquad (0 \le i < m).$$

Ha

Tehát a továbbiakban a $(\mathbf{Z}_m;+,\cdot)$ gyűrűt, azaz a **modulo m maradékosztályok gyűrűjét** úgy definiáljuk, mint az egész számok gyűrűjének a modulo m kongruencia szerinti faktoralgebráját! Tetszőleges elemét jelölheti

$$\overline{i} = \{x \in \mathbf{Z} : x \equiv i \pmod m\} \qquad (i \in \mathbf{Z}),\ \text{vagy}$$

$$\overline{i} \qquad (0 \le i < m),\ \text{vagy ha nem okoz}$$

$$\text{félreértést: } i \qquad (0 \le i < m).$$

Ha $m = 5$, akkor mindezt az alábbi két ábra szemlélteti:

$\mathbf{Z}$					
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	20	21	22	23	24
	15	16	17	18	19
	10	11	12	13	14
	5	6	7	8	9
	0	1	2	3	4
	-5	-4	-3	-2	-1
	-10	-9	-8	-7	-6
	-15	-14	-13	-12	-11
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{Z}_5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

A $\bar{2}$ és a $\bar{3}$ szorzata $\mathbf{Z}_5$-ben

⋮	⋮	⋮	⋮	⋮
20	21	22	23	24
15	16	17	18	19
10	11	12	13	14
5	6	7	8	9
0	1	2	3	4
-5	-4	-3	-2	-1
-10	-9	-8	-7	-6
-15	-14	-13	-12	-11
⋮	⋮	⋮	⋮	⋮
$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

67. Tétel. *Legyen* Θ *az* $A = (A; F)$ *algebra kongruenciája.*

67. Tétel. *Legyen* Θ *az* $A = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (

67. Tétel. *Legyen* Θ *az* $\mathcal{A} = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ *az* x Θ*-osztálya)*

67. Tétel. *Legyen* Θ *az* $\mathbf{A} = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ *az* x Θ*-osztálya) szürjektív homomorfizmus.*

67. Tétel. *Legyen* Θ *az* $\mathcal{A} = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ *az* x Θ*-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.*

67. Tétel. *Legyen* Θ *az* $\mathbf{A} = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ *az* x Θ*-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.*

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás:

67. Tétel. *Legyen* Θ *az* $\mathbf{A} = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ *az* x Θ*-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.*

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás: mivel a faktoralgebra éppen az $\overline{x}$-okból áll, φ szürjektív.

67. Tétel. *Legyen Θ az $\mathbf{A} = (A; F)$ algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ az x Θ-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás: mivel a faktoralgebra éppen az $\overline{x}$-okból áll, φ szürjektív. Mivel a műveleteket a reprezentánsokon végezzük, kapjuk, hogy ha $f \in F$ mondjuk m-változós, akkor

67. Tétel. *Legyen* Θ *az* $\mathbf{A} = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ *az* x Θ*-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.*

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás: mivel a faktoralgebra éppen az $\overline{x}$-okból áll, φ szürjektív. Mivel a műveleteket a reprezentánsokon végezzük, kapjuk, hogy ha $f \in F$ mondjuk m-változós, akkor $f(a_1\varphi, \ldots, a_m\varphi) =$

67. Tétel. *Legyen Θ az $\mathbf{A} = (A; F)$ algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ az x Θ-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás: mivel a faktoralgebra éppen az $\overline{x}$-okból áll, φ szürjektív. Mivel a műveleteket a reprezentánsokon végezzük, kapjuk, hogy ha $f \in F$ mondjuk m-változós, akkor $f(a_1\varphi, \ldots, a_m\varphi) = f(\overline{a_1}, \ldots, \overline{a_m}) =$

67. Tétel. *Legyen* Θ *az* $A = (A; F)$ *algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ *az* x Θ*-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.*

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás: mivel a faktoralgebra éppen az $\overline{x}$-okból áll, φ szürjektív. Mivel a műveleteket a reprezentánsokon végezzük, kapjuk, hogy ha $f \in F$ mondjuk m-változós, akkor $f(a_1\varphi, \ldots, a_m\varphi) = f(\overline{a_1}, \ldots, \overline{a_m}) = \overline{f(a_1, \ldots, a_m)} =$

67. Tétel. *Legyen Θ az $\mathbf{A} = (A; F)$ algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ az x Θ-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás: mivel a faktoralgebra éppen az $\overline{x}$-okból áll, φ szürjektív. Mivel a műveleteket a reprezentánsokon végezzük, kapjuk, hogy ha $f \in F$ mondjuk m-változós, akkor $f(a_1\varphi, \ldots, a_m\varphi) = f(\overline{a_1}, \ldots, \overline{a_m}) = \overline{f(a_1, \ldots, a_m)} = f(a_1, \ldots, a_m)\varphi$,

67. Tétel. *Legyen Θ az $\mathcal{A} = (A; F)$ algebra kongruenciája. Ekkor a*

$$\varphi : A \to A/\Theta, \quad x \mapsto \overline{x}$$

leképezés (ahol $\overline{x}$ az x Θ-osztálya) szürjektív homomorfizmus. Tehát a faktoralgebra a kiindulási algebra homomorf képe.

A tételben szereplő φ homomorfizmust a faktoralgebrára való **természetes homomorfizmusnak** szokás nevezni.

Bizonyítás: mivel a faktoralgebra éppen az $\overline{x}$-okból áll, φ szürjektív. Mivel a műveleteket a reprezentánsokon végezzük, kapjuk, hogy ha $f \in F$ mondjuk m-változós, akkor $f(a_1\varphi, \ldots, a_m\varphi) = f(\overline{a_1}, \ldots, \overline{a_m}) = \overline{f(a_1, \ldots, a_m)} = f(a_1, \ldots, a_m)\varphi$, tehát φ homomorfizmus.

Például a $\mathbf{Z}_m = (\mathbf{Z}_m; +, \cdot)$ maradékosztálygyűrű ($m \in \mathbf{N}_0$) homomorf képe az egész számok gyűrűjének.

Például a $\mathbf{Z}_m = (\mathbf{Z}_m; +, \cdot)$ maradékosztálygyűrű $(m \in \mathbf{N}_0)$ homomorf képe az egész számok gyűrűjének.

Abból a tényből, hogy a faktoralgebra egyúttal homomorf kép, könnyen következik, hogy faktoralgebra képzésekor az azonosságok megőrződnek.

Például a $\mathbf{Z}_m = (\mathbf{Z}_m; +, \cdot)$ maradékosztálygyűrű ($m \in \mathbf{N}_0$) homomorf képe az egész számok gyűrűjének.

Abból a tényből, hogy a faktoralgebra egyúttal homomorf kép, könnyen következik, hogy faktoralgebra képzésekor az azonosságok megőrződnek. Ennek speciális eseteként kapjuk az alábbi tételt:

68. Tétel. *Félcsoport, monoid, csoport, Abel-csoport, gyűrű faktoralgebrája*

68. Tétel. *Félcsoport, monoid, csoport, Abel-csoport, gyűrű faktoralgebrája rendre*

68. Tétel. *Félcsoport, monoid, csoport, Abel-csoport, gyűrű faktoralgebrája rendre félcsoport, monoid, csoport, Abel-csoport, gyűrű.*

68. Tétel. *Félcsoport, monoid, csoport, Abel-csoport, gyűrű faktoralgebrája rendre félcsoport, monoid, csoport, Abel-csoport, gyűrű. (Ennek megfelelően faktorfélcsoportról, faktormonoidról, stb. beszélünk.)*

Megjegyzés:

68. Tétel. *Félcsoport, monoid, csoport, Abel-csoport, gyűrű faktoralgebrája rendre félcsoport, monoid, csoport, Abel-csoport, gyűrű. (Ennek megfelelően faktorfélcsoportról, faktormonoidról, stb. beszélünk.)*

Megjegyzés: testre a tétel nem érvényes, hiszen

68. Tétel. *Félcsoport, monoid, csoport, Abel-csoport, gyűrű faktoralgebrája rendre félcsoport, monoid, csoport, Abel-csoport, gyűrű. (Ennek megfelelően faktorfélcsoportról, faktormonoidról, stb. beszélünk.)*

Megjegyzés: testre a tétel nem érvényes, hiszen — a teljes A^2 relációt választva Θ-nak — a faktoralgebra egyelemű is lehet, ami nem lehet test, hiszen a testek def. szerint legalább kételeműek.

69. Tétel. *Legyen* $\mathcal{A} = (A; F)$ *és* $\mathcal{B} = (B; F)$ *azonos típusú algebra.*

69. Tétel. *Legyen* $A = (A; F)$ *és* $B = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : A \to B$ *homomorfizmus, akkor a*

69. Tétel. *Legyen* $\mathcal{A} = (A; F)$ *és* $\mathcal{B} = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : A \to B$ *homomorfizmus, akkor a*

$$\textit{ker}\varphi := \{(u, v) \in A^2 : u\varphi = v\varphi\}$$

reláció (

69. Tétel. *Legyen* $\mathcal{A} = (A; F)$ *és* $\mathcal{B} = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : \mathcal{A} \to \mathcal{B}$ *homomorfizmus, akkor a*

$$\textit{ker}\varphi := \{(u, v) \in A^2 : u\varphi = v\varphi\}$$

reláció (amelyet a φ *homomorfizmus* **magjának** *nevezünk)*

69. Tétel. *Legyen* $A = (A; F)$ *és* $B = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : A \to B$ *homomorfizmus, akkor a*

$$\text{ker}\varphi := \{(u, v) \in A^2 : u\varphi = v\varphi\}$$

reláció (amelyet a φ *homomorfizmus* **magjának** *nevezünk) kongruencia az* A *algebrán.*

69. Tétel. *Legyen* $\mathcal{A} = (A; F)$ *és* $\mathcal{B} = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : \mathcal{A} \to \mathcal{B}$ *homomorfizmus, akkor a*

$$\text{ker}\varphi := \{(u, v) \in A^2 : u\varphi = v\varphi\}$$

reláció (amelyet a φ *homomorfizmus* **magjának** *nevezünk) kongruencia az* $\mathcal{A}$ *algebrán.*

*(B) (***Homomorfiatétel***) algebra bármely homomorf képe izomorf az algebra egy alkalmas faktoralgebrájával.*

69. Tétel. *Legyen* $\mathcal{A} = (A; F)$ *és* $\mathcal{B} = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : \mathcal{A} \to \mathcal{B}$ *homomorfizmus, akkor a*

$$\text{ker}\varphi := \{(u, v) \in A^2 : u\varphi = v\varphi\}$$

reláció (amelyet a φ *homomorfizmus* **magjának** *nevezünk) kongruencia az* $\mathcal{A}$ *algebrán.*

*(B) (***Homomorfiatétel***) algebra bármely homomorf képe izomorf az algebra egy alkalmas faktoralgebrájával. Pontosabban: ha a fenti* φ *homomorfizmus szürjektív, akkor a*

69. Tétel. *Legyen* $\mathcal{A} = (A; F)$ *és* $\mathcal{B} = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : A \to B$ *homomorfizmus, akkor a*

$$\text{ker}\varphi := \{(u, v) \in A^2 : u\varphi = v\varphi\}$$

reláció (amelyet a φ *homomorfizmus* **magjának** *nevezünk) kongruencia az* $\mathcal{A}$ *algebrán.*

*(B) (***Homomorfiatétel***) algebra bármely homomorf képe izomorf az algebra egy alkalmas faktoralgebrájával. Pontosabban: ha a fenti* φ *homomorfizmus szürjektív, akkor a* $\mathcal{B}$ *algebra izomorf az* $\mathcal{A}/\text{ker}\varphi$ *faktoralgebrával, és*

69. Tétel. *Legyen* $A = (A; F)$ *és* $B = (B; F)$ *azonos típusú algebra. (A) Ha* $\varphi : A \to B$ *homomorfizmus, akkor a*

$$\text{ker}\varphi := \{(u, v) \in A^2 : u\varphi = v\varphi\}$$

reláció (amelyet a φ *homomorfizmus* **magjának** *nevezünk) kongruencia az* A *algebrán.*

*(B) (***Homomorfiatétel***) algebra bármely homomorf képe izomorf az algebra egy alkalmas faktoralgebrájával. Pontosabban: ha a fenti* φ *homomorfizmus szürjektív, akkor a* B *algebra izomorf az* $A/\text{ker}\varphi$ *faktoralgebrával, és a* $\tau : A/\text{ker}\varphi \to B$*,* $\overline{a} \mapsto a\varphi$ *leképezés izomorfizmus.*

A bizonyítás

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy $\ker\varphi$ kongruencia.

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy kerφ kongruencia.

Ha

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy kerφ kongruencia.

Ha $a, b \in A$-ra

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy kerφ kongruencia.

Ha $a, b \in A$-ra $\overline{a} = \overline{b}$, akkor

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy kerφ kongruencia.

Ha $a, b \in A$-ra $\overline{a} = \overline{b}$, akkor $(a, b) \in$ kerφ,

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy kerφ kongruencia.

Ha $a, b \in A$-ra $\overline{a} = \overline{b}$, akkor $(a, b) \in$ kerφ, innen $a\varphi = b\varphi$,

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy kerφ kongruencia.

Ha $a, b \in A$-ra $\overline{a} = \overline{b}$, akkor $(a, b) \in$ kerφ, innen $a\varphi = b\varphi$, tehát $\tau : \overline{a} \mapsto a\varphi$ jóldefiniált.

A bizonyítás egyszerű de hasznos gyakorló feladat annak megmutatása, hogy kerφ kongruencia.

Ha $a, b \in A$-ra $\overline{a} = \overline{b}$, akkor $(a, b) \in$ kerφ, innen $a\varphi = b\varphi$, tehát $\tau : \overline{a} \mapsto a\varphi$ jóldefiniált.

Mivel — φ szürjektivitása miatt — B minden eleme előáll $a\varphi$ alakban, τ szürjektív.

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$.
Ekkor

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$.
Ekkor $a\varphi = b\varphi$,

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$.
Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$,

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in$ kerφ, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor $f(\overline{a_1}\tau, \ldots, \overline{a_m}\tau) =$

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in$ kerφ, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor $f(\overline{a_1}\tau, \ldots, \overline{a_m}\tau) = f(a_1\varphi, \ldots, a_m\varphi) =$

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor $f(\overline{a_1}\tau, \ldots, \overline{a_m}\tau) = f(a_1\varphi, \ldots, a_m\varphi) = f(a_1, \ldots, a_m)\varphi =$

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor $f(\overline{a_1}\tau, \ldots, \overline{a_m}\tau) = f(a_1\varphi, \ldots, a_m\varphi) = f(a_1, \ldots, a_m)\varphi = \overline{f(a_1, \ldots, a_m)}\tau =$

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor $f(\overline{a_1}\tau, \dots, \overline{a_m}\tau) = f(a_1\varphi, \dots, a_m\varphi) = f(a_1, \dots, a_m)\varphi = \overline{f(a_1, \dots, a_m)}\tau = f(\overline{a_1}, \dots, \overline{a_m})\tau$,

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor $f(\overline{a_1}\tau, \ldots, \overline{a_m}\tau) = f(a_1\varphi, \ldots, a_m\varphi) = f(a_1, \ldots, a_m)\varphi = \overline{f(a_1, \ldots, a_m)}\tau = f(\overline{a_1}, \ldots, \overline{a_m})\tau$, tehát τ homomorfizmus.

Az injektivitás igazolásához tegyük fel, hogy $a, b \in A$-ra $\overline{a}\tau = \overline{b}\tau$. Ekkor $a\varphi = b\varphi$, így $(a, b) \in \ker\varphi$, tehát $\overline{a} = \overline{b}$. Azaz τ injektív.

Legyen most $f \in F$, mondjuk m-változós. Ekkor $f(\overline{a_1}\tau, \ldots, \overline{a_m}\tau) = f(a_1\varphi, \ldots, a_m\varphi) = f(a_1, \ldots, a_m)\varphi = \overline{f(a_1, \ldots, a_m)}\tau = f(\overline{a_1}, \ldots, \overline{a_m})\tau$, tehát τ homomorfizmus. Az eddigiek szerint τ izomorfizmus. Q.e.d.

A homomorfiatétel szép alkalmazása az alábbi, A homomorfiatétel szép alkalmazása az alábbi, egyébként is fontos tétel bizonyítása.

70. Tétel. *Ha* $m, n \in \mathbf{N}$*-re* m *és* n *relatív prím, akkor a* $\mathbf{Z}_{mn} = (\mathbf{Z}_{mn}; +, \cdot)$ *maradékosztálygyűrű izomorf a* $\mathbf{Z}_m \times \mathbf{Z}_n$ *direkt szorzattal.*

70. Tétel. *Ha* $m, n \in \mathbf{N}$*-re* m *és* n *relatív prím, akkor a* $\mathbf{Z}_{mn} = (\mathbf{Z}_{mn}; +, \cdot)$ *maradékosztálygyűrű izomorf a* $\mathbf{Z}_m \times \mathbf{Z}_n$ *direkt szorzattal.*

Bizonyítás: Most $\mathbf{Z}_k$ tetszőleges elemét

$$\bar{i} = \{x \in \mathbf{Z} : x \equiv i \pmod{k}\}$$

fogja jelölni.

70. Tétel. *Ha* $m, n \in \mathbf{N}$*-re* m *és* n *relatív prím, akkor a* $\mathbf{Z}_{mn} = (\mathbf{Z}_{mn}; +, \cdot)$ *maradékosztálygyűrű izomorf a* $\mathbf{Z}_m \times \mathbf{Z}_n$ *direkt szorzattal.*

Bizonyítás: Most $\mathbf{Z}_k$ tetszőleges elemét

$$\bar{i} = \{x \in \mathbf{Z} : x \equiv i \pmod{k}\}$$

fogja jelölni. k értelemszerű lesz: az első komponensek esetén $k = m$, a második komponensek esetén $k = n$.

Tekintsük a

$$\varphi : \mathbf{Z} \longrightarrow \mathbf{Z}_m \times \mathbf{Z}_n,$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést.

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x + y)\varphi =$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x + y)\varphi = (\overline{x + y}, \overline{x + y}) =$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x} + \bar{y},$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x + y)\varphi = (\overline{x + y}, \overline{x + y}) = (\bar{x} + \bar{y}, \bar{x} + \bar{y}) =$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Ugyanez érvényes a szorzásra is:

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Ugyanez érvényes a szorzásra is:

$$(xy)\varphi =$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Ugyanez érvényes a szorzásra is:

$$(xy)\varphi = (\overline{xy}, \overline{xy}) =$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Ugyanez érvényes a szorzásra is:

$$(xy)\varphi = (\overline{xy}, \overline{xy}) = (\bar{x}\bar{y},$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Ugyanez érvényes a szorzásra is:

$$(xy)\varphi = (\overline{xy}, \overline{xy}) = (\bar{x}\bar{y}, \bar{x}\bar{y}) =$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Ugyanez érvényes a szorzásra is:

$$(xy)\varphi = (\overline{xy}, \overline{xy}) = (\bar{x}\bar{y}, \bar{x}\bar{y}) =$$
$$(\bar{x}, \bar{x})\,(\bar{y}, \bar{y}) = x\varphi\, y\varphi.$$

Tekintsük a

$$\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n, \qquad x \mapsto (\bar{x}, \bar{x})$$

leképezést. Ha $x, y \in \mathbf{Z}$, akkor számoljunk

$$(x+y)\varphi = (\overline{x+y}, \overline{x+y}) = (\bar{x}+\bar{y}, \bar{x}+\bar{y}) =$$
$$(\bar{x}, \bar{x}) + (\bar{y}, \bar{y}) = x\varphi + y\varphi.$$

Ugyanez érvényes a szorzásra is:

$$(xy)\varphi = (\overline{xy}, \overline{xy}) = (\bar{x}\bar{y}, \bar{x}\bar{y}) =$$
$$(\bar{x}, \bar{x})\,(\bar{y}, \bar{y}) = x\varphi\, y\varphi.$$

tehát φ homomorfizmus.

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges.

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges. Mivel m és n relatív prím, a

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges. Mivel m és n relatív prím, a kínai maradéktétel szerint az alábbi kongruenciarendszernek:

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges. Mivel m és n relatív prím, a kínai maradéktétel szerint az alábbi kongruenciarendszernek:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

van megoldása.

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges. Mivel m és n relatív prím, a kínai maradéktétel szerint az alábbi kongruenciarendszernek:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

van megoldása. Ha x megoldása a fenti kongruenciarendszernek, akkor

$$x\varphi =$$

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges. Mivel m és n relatív prím, a kínai maradéktétel szerint az alábbi kongruenciarendszernek:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

van megoldása. Ha x megoldása a fenti kongruenciarendszernek, akkor

$$x\varphi = (\bar{x}, \bar{x}) =$$

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges. Mivel m és n relatív prím, a kínai maradéktétel szerint az alábbi kongruenciarendszernek:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

van megoldása. Ha x megoldása a fenti kongruenciarendszernek, akkor

$$x\varphi = (\bar{x}, \bar{x}) = (\bar{a}, \bar{b}).$$

A szürjektivitás igazolása érdekében legyen $(\bar{a}, \bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$ tetszőleges. Mivel m és n relatív prím, a kínai maradéktétel szerint az alábbi kongruenciarendszernek:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

van megoldása. Ha x megoldása a fenti kongruenciarendszernek, akkor

$$x\varphi = (\bar{x}, \bar{x}) = (\bar{a}, \bar{b}).$$

Ez igazolja φ szürjektivitását.

Most határozzuk meg a $\varphi : \mathbf{Z} \longrightarrow \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t!

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \mathrm{ker}\varphi$$

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \mathrm{ker}\varphi \iff x\varphi = y\varphi$$

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \text{ker}\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y})$$

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \ker\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod m \ \wedge \ x \equiv y \pmod n)$$

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \ker\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod{m} \wedge x \equiv y \pmod{n} \iff$$
$$m \mid x - y \quad \wedge \quad n \mid x - y$$

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x,y) \in \ker\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$

$$x \equiv y \pmod{m} \ \wedge\ x \equiv y \pmod{n} \iff$$

$$m \mid x - y \quad \wedge \quad n \mid x - y \iff$$

mivel relatív prímek $mn \mid x - y$

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \mathrm{ker}\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod{m} \ \wedge \ x \equiv y \pmod{n} \iff$$
$$m \mid x - y \quad \wedge \quad n \mid x - y \iff$$
$$\text{mivel relatív prímek } mn \mid x - y \iff x \equiv y \pmod{mn}.$$

Mivel

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \text{ker}\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod{m} \ \wedge \ x \equiv y \pmod{n} \iff$$
$$m \mid x - y \quad \wedge \quad n \mid x - y \iff$$
$$\text{mivel relatív prímek } mn \mid x - y \iff x \equiv y \pmod{mn}.$$

Mivel kerφ a modulo (mn) kongruencia,

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \ker\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod m \ \wedge \ x \equiv y \pmod n \iff$$
$$m \mid x - y \quad \wedge \quad n \mid x - y \iff$$
$$\text{mivel relatív prímek } mn \mid x - y \iff x \equiv y \pmod{mn}.$$

Mivel kerφ a modulo (mn) kongruencia, ezért —

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz $\ker\varphi$-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \ker\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod{m} \wedge x \equiv y \pmod{n} \iff$$
$$m \mid x - y \quad \wedge \quad n \mid x - y \iff$$
$$\text{mivel relatív prímek } mn \mid x - y \iff x \equiv y \pmod{mn}.$$

Mivel $\ker\varphi$ a modulo (mn) kongruencia, ezért — a homomorfiatétel értelmében —

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \ker\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod{m} \ \wedge \ x \equiv y \pmod{n} \iff$$
$$m \mid x - y \quad \wedge \quad n \mid x - y \iff$$
$$\text{mivel relatív prímek } mn \mid x - y \iff x \equiv y \pmod{mn}.$$

Mivel kerφ a modulo (mn) kongruencia, ezért — a homomorfiatétel értelmében — $\mathbf{Z}_m \times \mathbf{Z}_n$ izomorf $\mathbf{Z}$-nek a modulo (mn) kongruencia szerinti faktoralgebrájával, azaz $\mathbf{Z}_{mn}$-nel.

Most határozzuk meg a $\varphi : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$, $x \mapsto (\bar{x}, \bar{x})$ szürjektív homomorfizmus magját, azaz kerφ-t! Ha $x, y \in \mathbf{Z}$, akkor

$$(x, y) \in \text{ker}\varphi \iff x\varphi = y\varphi \iff (\bar{x}, \bar{x}) = (\bar{y}, \bar{y}) \iff$$
$$x \equiv y \pmod{m} \ \wedge \ x \equiv y \pmod{n} \iff$$
$$m \mid x - y \quad \wedge \quad n \mid x - y \iff$$
$$\text{mivel relatív prímek } mn \mid x - y \iff x \equiv y \pmod{mn}.$$

Mivel kerφ a modulo (mn) kongruencia, ezért — a homomorfiatétel értelmében — $\mathbf{Z}_m \times \mathbf{Z}_n$ izomorf $\mathbf{Z}$-nek a modulo (mn) kongruencia szerinti faktoralgebrájával, azaz $\mathbf{Z}_{mn}$-nel. Q.e.d.

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében?

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg
(

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig)

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig) a faktoralgebrát!

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig) a faktoralgebrát!

Megoldás: Legyen $\Theta = \{(a, b)\colon$ a és b azonos előjelű$\}$.

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig) a faktoralgebrát!

Megoldás: Legyen $\Theta = \{(a, b)\colon\ a$ és b azonos előjelű$\}$. Ez nyilván ekvivalenciareláció.

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig) a faktoralgebrát!

Megoldás: Legyen $\Theta = \{(a, b)$: a és b azonos előjelű$\}$. Ez nyilván ekvivalenciareláció.

(a) $(\mathbf{Q}; +)$:

Feladat: kongruencia-e az „azonos előjelűek'' reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig) a faktoralgebrát!

Megoldás: Legyen $\Theta = \{(a,b)\colon\ a$ és b azonos előjelű$\}$. Ez nyilván ekvivalenciareláció.

(a) $(\mathbf{Q};+)$: $(5,10) \in \Theta$, $(-7,-7) \in \Theta$,

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig) a faktoralgebrát!

Megoldás: Legyen $\Theta = \{(a,b)\colon\ a$ és b azonos előjelű$\}$. Ez nyilván ekvivalenciareláció.

(a) $(\mathbf{Q};+)$: $(5,10) \in \Theta$, $(-7,-7) \in \Theta$, de

$$(5+(-7), 10+(-7)) = (-2,3) \notin \Theta.$$

Feladat: kongruencia-e az „azonos előjelűek” reláció a racionális számok (a) additív csoportjában, (b) multiplikatív félcsoportjában, (c) testében? Ha igen, határozzuk meg (izomorfia erejéig) a faktoralgebrát!

Megoldás: Legyen $\Theta = \{(a, b)\colon\ a$ és b azonos előjelű$\}$. Ez nyilván ekvivalenciareláció.

(a) $(\mathbf{Q}; +)$: $(5, 10) \in \Theta$, $(-7, -7) \in \Theta$, de

$$(5 + (-7), 10 + (-7)) = (-2, 3) \notin \Theta.$$

Tehát a válasz nemleges.

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korábbi megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

$$\varphi : (\mathbf{Q};\cdot) \to$$

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

$$\varphi : (\mathbf{Q};\cdot) \to (\{-1,0,1\};\cdot),$$

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

$$\varphi : (\mathbf{Q};\cdot) \to (\{-1,0,1\};\cdot), \quad x \mapsto \begin{cases} -1 & \text{ha } x < 0 \\ 0 & \text{ha } x = 0 \\ 1 & \text{ha } x > 0 \end{cases}$$

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

$$\varphi : (\mathbf{Q};\cdot) \to (\{-1,0,1\};\cdot), \quad x \mapsto \begin{cases} -1 & \text{ha } x < 0 \\ 0 & \text{ha } x = 0 \\ 1 & \text{ha } x > 0 \end{cases}$$

leképezés nyilván szürjektív homomorfizmus és

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

$$\varphi : (\mathbf{Q};\cdot) \to (\{-1,0,1\};\cdot), \quad x \mapsto \begin{cases} -1 & \text{ha } x < 0 \\ 0 & \text{ha } x = 0 \\ 1 & \text{ha } x > 0 \end{cases}$$

leképezés nyilván szürjektív homomorfizmus és $\Theta = \ker\varphi$, ezért

—

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

$$\varphi : (\mathbf{Q};\cdot) \to (\{-1,0,1\};\cdot), \quad x \mapsto \begin{cases} -1 & \text{ha } x < 0 \\ 0 & \text{ha } x = 0 \\ 1 & \text{ha } x > 0 \end{cases}$$

leképezés nyilván szürjektív homomorfizmus és $\Theta = \ker\varphi$, ezért — a homomorfiatétel miatt —

(b) $(\mathbf{Q};\cdot)$: (A szorzás előjelszabályára hivatkozva szó szerint működik az $(\mathbf{Z};\cdot)$-ra adott korább megoldás. Ezért most egy másik — ötletesebb — megoldást mutatunk.)

Mivel — a szorzás előjelszabálya szerint — a

$$\varphi : (\mathbf{Q};\cdot) \to (\{-1,0,1\};\cdot), \quad x \mapsto \begin{cases} -1 & \text{ha } x < 0 \\ 0 & \text{ha } x = 0 \\ 1 & \text{ha } x > 0 \end{cases}$$

leképezés nyilván szürjektív homomorfizmus és $\Theta = \ker\varphi$, ezért — a homomorfiatétel miatt — Θ homomorfizmus és a Θ szerinti faktoralgebra izomorf a $(\{-1,0,1\};\cdot)$ monoiddal.

(c) A $(\mathbf{Q}; +, \cdot)$ test esetén: ha

(c) A $(\mathbf{Q}; +, \cdot)$ test esetén: ha Θ kongruencia lenne,

(c) A $(\mathbf{Q};+,\cdot)$ test esetén: ha Θ kongruencia lenne, akkor a $(\mathbf{Q};+)$-nak is kongruenciája lenne, holott az (a) részben láttuk, hogy nem az. Tehát a válasz nemleges.

Feladat: Tekintsük az $(\mathbb{N};+)$ félcsoport direkt négyzetén (

Feladat: Tekintsük az $(\mathbf{N};+)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\Theta := \{((a_1,b_1),(a_2,b_2)) : a_1+b_2=b_1+a_2\}$$

relációt. Kongruencia-e Θ,

Feladat: Tekintsük az $(\mathbf{N}; +)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\Theta := \{((a_1, b_1), (a_2, b_2)) : a_1 + b_2 = b_1 + a_2\}$$

relációt. Kongruencia-e Θ, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a Θ szerinti faktoralgebra?

Feladat: Tekintsük az $(\mathbf{N};+)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\Theta := \{((a_1,b_1),(a_2,b_2)) : a_1+b_2=b_1+a_2\}$$

relációt. Kongruencia-e Θ, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a Θ szerinti faktoralgebra? (A második, $(*)$-gal kezdődő kérdés távolról sem könnyű!)

Feladat: Tekintsük az $(\mathbb{N};+)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\ominus := \{((a_1,b_1),(a_2,b_2)) : a_1+b_2 = b_1+a_2\}$$

relációt. Kongruencia-e $\ominus$, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a $\ominus$ szerinti faktoralgebra? (A második, $(*)$-gal kezdődő kérdés távolról sem könnyű!)

Megoldás: Az első kérdés az, hogy ekvivalencia-e $\ominus$. Az itt nem részletezett triviális megfontolás miatt:

Feladat: Tekintsük az $(\mathbb{N};+)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\ominus := \{((a_1,b_1),(a_2,b_2)) : a_1+b_2=b_1+a_2\}$$

relációt. Kongruencia-e $\ominus$, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a $\ominus$ szerinti faktoralgebra? (A második, $(*)$-gal kezdődő kérdés távolról sem könnyű!)

Megoldás: Az első kérdés az, hogy ekvivalencia-e $\ominus$. Az itt nem részletezett triviális megfontolás miatt:

Feladat: Tekintsük az $(\mathbb{N}; +)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\Theta := \{((a_1, b_1), (a_2, b_2)) : a_1 + b_2 = b_1 + a_2\}$$

relációt. Kongruencia-e Θ, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a Θ szerinti faktoralgebra? (A második, $(*)$-gal kezdődő kérdés távolról sem könnyű!)

Megoldás: Az első kérdés az, hogy ekvivalencia-e Θ. Az itt nem részletezett triviális megfontolás miatt: igen. (Vegyük észre, hogy Θ szemléletes jelentése az, hogy a

Feladat: Tekintsük az $(\mathbb{N};+)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\Theta := \{((a_1, b_1), (a_2, b_2)) : a_1 + b_2 = b_1 + a_2\}$$

relációt. Kongruencia-e Θ, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a Θ szerinti faktoralgebra? (A második, $(*)$-gal kezdődő kérdés távolról sem könnyű!)

Megoldás: Az első kérdés az, hogy ekvivalencia-e Θ. Az itt nem részletezett triviális megfontolás miatt: igen. (Vegyük észre, hogy Θ szemléletes jelentése az, hogy a „kültagok” összege egyenlő a „beltagok” összegével.)

Feladat: Tekintsük az $(\mathbb{N};+)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\Theta := \{((a_1, b_1), (a_2, b_2)) : a_1 + b_2 = b_1 + a_2\}$$

relációt. Kongruencia-e Θ, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a Θ szerinti faktoralgebra? (A második, $(*)$-gal kezdődő kérdés távolról sem könnyű!)

Megoldás: Az első kérdés az, hogy ekvivalencia-e Θ. Az itt nem részletezett triviális megfontolás miatt: igen. (Vegyük észre, hogy Θ szemléletes jelentése az, hogy a „kültagok” összege egyenlő a „beltagok” összegével.)

A második kérdés az, hogy megőrzi-e az összeadás Θ-t?

Feladat: Tekintsük az $(\mathbb{N}; +)$ félcsoport direkt négyzetén (azaz az önmagával vett direkt szorzatán) a

$$\Theta := \{((a_1, b_1), (a_2, b_2)) : a_1 + b_2 = b_1 + a_2\}$$

relációt. Kongruencia-e Θ, és ha igen, akkor $(*)$ milyen ismert algebrával izomorf a Θ szerinti faktoralgebra? (A második, $(*)$-gal kezdődő kérdés távolról sem könnyű!)

Megoldás: Az első kérdés az, hogy ekvivalencia-e Θ. Az itt nem részletezett triviális megfontolás miatt: igen. (Vegyük észre, hogy Θ szemléletes jelentése az, hogy a „kültagok” összege egyenlő a „beltagok” összegével.)

A második kérdés az, hogy megőrzi-e az összeadás Θ-t? Tetszőleges elemeket tekintve számoljunk:

$$((a_1, b_1), (a_2, b_2)) \in \Theta \text{ és } ((c_1, d_1), (c_2, d_2)) \in \Theta \Longrightarrow$$

$$((a_1, b_1), (a_2, b_2)) \in \Theta \text{ és } ((c_1, d_1), (c_2, d_2)) \in \Theta \Longrightarrow$$

$$a_1 + b_2 = b_1 + a_2 \text{ és } c_1 + d_2 = d_1 + c_2 \Longrightarrow$$

$$((a_1, b_1), (a_2, b_2)) \in \ominus \text{ és } ((c_1, d_1), (c_2, d_2)) \in \ominus \Longrightarrow$$
$$a_1 + b_2 = b_1 + a_2 \text{ és } c_1 + d_2 = d_1 + c_2 \Longrightarrow$$
$$a_1 + b_2 + c_1 + d_2 = b_1 + a_2 + d_1 + c_2 \Longrightarrow$$

$$((a_1, b_1), (a_2, b_2)) \in \ominus \text{ és } ((c_1, d_1), (c_2, d_2)) \in \ominus \Longrightarrow$$

$$a_1 + b_2 = b_1 + a_2 \text{ és } c_1 + d_2 = d_1 + c_2 \Longrightarrow$$

$$a_1 + b_2 + c_1 + d_2 = b_1 + a_2 + d_1 + c_2 \Longrightarrow$$

$$((a_1 + c_1, b_1 + d_1), (a_2 + c_2, b_2 + d_2)) \in \ominus \Longrightarrow$$

$$((a_1, b_1), (a_2, b_2)) \in \Theta \text{ és } ((c_1, d_1), (c_2, d_2)) \in \Theta \Longrightarrow$$
$$a_1 + b_2 = b_1 + a_2 \text{ és } c_1 + d_2 = d_1 + c_2 \Longrightarrow$$
$$a_1 + b_2 + c_1 + d_2 = b_1 + a_2 + d_1 + c_2 \Longrightarrow$$
$$((a_1 + c_1, b_1 + d_1), (a_2 + c_2, b_2 + d_2)) \in \Theta \Longrightarrow$$
$$((a_1, b_1) + (c_1, d_1), (a_2, b_2) + (c_2, d_2)) \in \Theta.$$

$$((a_1, b_1), (a_2, b_2)) \in \Theta \text{ és } ((c_1, d_1), (c_2, d_2)) \in \Theta \Longrightarrow$$

$$a_1 + b_2 = b_1 + a_2 \text{ és } c_1 + d_2 = d_1 + c_2 \Longrightarrow$$

$$a_1 + b_2 + c_1 + d_2 = b_1 + a_2 + d_1 + c_2 \Longrightarrow$$

$$((a_1 + c_1, b_1 + d_1), (a_2 + c_2, b_2 + d_2)) \in \Theta \Longrightarrow$$

$$((a_1, b_1) + (c_1, d_1), (a_2, b_2) + (c_2, d_2)) \in \Theta.$$

Ezek szerint Θ kongruencia.

Tekintsük a

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez h

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi =$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) =$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Szürjektív, hiszen bármely egész szám előáll két pozitív egész szám különbségeként.

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Szürjektív, hiszen bármely egész szám előáll két pozitív egész szám különbségeként. Továbbá

$$((a_1, b_1), (a_2, b_2)) \in \mathrm{ker}\varphi \iff$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Szürjektív, hiszen bármely egész szám előáll két pozitív egész szám különbségeként. Továbbá

$$((a_1, b_1), (a_2, b_2)) \in \text{ker}\varphi \iff (a_1, b_1)\varphi = (a_2, b_2)\varphi \iff$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Szürjektív, hiszen bármely egész szám előáll két pozitív egész szám különbségeként. Továbbá

$$((a_1, b_1), (a_2, b_2)) \in \mathsf{ker}\varphi \iff (a_1, b_1)\varphi = (a_2, b_2)\varphi \iff$$
$$a_1 - b_1 = a_2 - b_2 \iff$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Szürjektív, hiszen bármely egész szám előáll két pozitív egész szám különbségeként. Továbbá

$$((a_1, b_1), (a_2, b_2)) \in \text{ker}\varphi \iff (a_1, b_1)\varphi = (a_2, b_2)\varphi \iff$$
$$a_1 - b_1 = a_2 - b_2 \iff a_1 + b_2 = b_1 + a_2 \iff$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Szürjektív, hiszen bármely egész szám előáll két pozitív egész szám különbségeként. Továbbá

$$((a_1, b_1), (a_2, b_2)) \in \text{ker}\varphi \iff (a_1, b_1)\varphi = (a_2, b_2)\varphi \iff$$
$$a_1 - b_1 = a_2 - b_2 \iff a_1 + b_2 = b_1 + a_2 \iff$$
$$((a_1, b_1), (a_2, b_2)) \in \Theta.$$

Tekintsük a

$$\varphi : (\mathbf{N} \times \mathbf{N}; +) \to (\mathbf{Z}; +), \qquad (a, b) \mapsto a - b$$

leképezést. Ez homomorfizmus, hiszen

$$((a_1, b_1) + (a_2, b_2))\varphi = (a_1 + a_2, b_1 + b_2)\varphi =$$
$$a_1 + a_2 - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) =$$
$$(a_1, b_1)\varphi + (a_2, b_2)\varphi.$$

Szürjektív, hiszen bármely egész szám előáll két pozitív egész szám különbségeként. Továbbá

$$((a_1, b_1), (a_2, b_2)) \in \mathrm{ker}\varphi \iff (a_1, b_1)\varphi = (a_2, b_2)\varphi \iff$$
$$a_1 - b_1 = a_2 - b_2 \iff a_1 + b_2 = b_1 + a_2 \iff$$
$$((a_1, b_1), (a_2, b_2)) \in \Theta.$$

Tehát $\ker\varphi =$

Tehát $\ker\varphi = \Theta$, és a homomorfiatétel szerint a kérdéses faktoralgebra az egész számok additív csoportjával izomorf.

Tehát $\ker\varphi = \Theta$, és a homomorfiatétel szerint a kérdéses faktoralgebra az egész számok additív csoportjával izomorf. Q.e.d.

Tehát ker$\varphi = \Theta$, és a homomorfiatétel szerint a kérdéses faktoralgebra az egész számok additív csoportjával izomorf. Q.e.d.

Megjegyzés: Az $(\mathbb{N}; +, \cdot)$ algebrát az emberiség sokezer éve ismeri, ezzel szemben az egész számok (és azokra a $+$, $\cdot$ műveletek) fogalma csak a középkorban alakult ki.

Tehát $\ker\varphi = \Theta$, és a homomorfiatétel szerint a kérdéses faktoralgebra az egész számok additív csoportjával izomorf. Q.e.d.

Megjegyzés: Az $(\mathbb{N}; +, \cdot)$ algebrát az emberiség sokezer éve ismeri, ezzel szemben az egész számok (és azokra a $+$, $\cdot$ műveletek) fogalma csak a középkorban alakult ki. Az egész számok bevezetését célzó mindenféle motiváló magyarázat —

Tehát $\ker\varphi = \Theta$, és a homomorfiatétel szerint a kérdéses faktoralgebra az egész számok additív csoportjával izomorf. Q.e.d.

Megjegyzés: Az $(\mathbb{N}; +, \cdot)$ algebrát az emberiség sokezer éve ismeri, ezzel szemben az egész számok (és azokra a $+$, $\cdot$ műveletek) fogalma csak a középkorban alakult ki. Az egész számok bevezetését célzó mindenféle motiváló magyarázat — pl. ha a pénztárcánk megsemmisül (azaz kivonjuk), akkor szegényebbek leszünk, de ha az adósságunkról szóló kötelezvény semmisül meg, akkor pedig gazdagabbak, Tehát ker$\varphi = \Theta$, és a homomorfiatétel szerint a kérdéses faktoralgebra az egész számok additív csoportjával izomorf. Q.e.d.

Megjegyzés: Az $(\mathbb{N}; +, \cdot)$ algebrát az emberiség sokezer éve ismeri, ezzel szemben az egész számok (és azokra a $+$, $\cdot$ műveletek) fogalma csak a középkorban alakult ki. Az egész számok bevezetését célzó mindenféle motiváló magyarázat — pl. ha a pénztárcánk megsemmisül (azaz kivonjuk), akkor szegényebbek leszünk, de ha az adósságunkról szóló kötelezvény semmisül meg, akkor pedig gazdagabbak, az előjeles szorzás még sokkal bonyolultabb motiválásáról nem is beszélve — után lássuk az

Tehát $\ker\varphi = \Theta$, és a homomorfiatétel szerint a kérdéses faktoralgebra az egész számok additív csoportjával izomorf. Q.e.d.

Megjegyzés: Az $(\mathbb{N}; +, \cdot)$ algebrát az emberiség sokezer éve ismeri, ezzel szemben az egész számok (és azokra a $+$, $\cdot$ műveletek) fogalma csak a középkorban alakult ki. Az egész számok bevezetését célzó mindenféle motiváló magyarázat — pl. ha a pénztárcánk megsemmisül (azaz kivonjuk), akkor szegényebbek leszünk, de ha az adósságunkról szóló kötelezvény semmisül meg, akkor pedig gazdagabbak, az előjeles szorzás még sokkal bonyolultabb motiválásáról nem is beszélve — után lássuk az **igazi tényállást**:

Tekintsük az $(\mathbf{N} \times \mathbf{N}; +, \cdot)$ algebrát, ahol az összadás az előbbi, a szorzást pedig így definiáljuk:

$$(a_1, b_1) \cdot (a_2, b_2) :=$$

Tekintsük az $(\mathbf{N} \times \mathbf{N}; +, \cdot)$ algebrát, ahol az összadás az előbbi, a szorzást pedig így definiáljuk:

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1).$$

Ekkor megmutatható, hogy az előbb definiált Θ kongruencia.

Tekintsük az $(\mathbf{N} \times \mathbf{N}; +, \cdot)$ algebrát, ahol az összadás az előbbi, a szorzást pedig így definiáljuk:

$$(a_1, b_1) \cdot (a_2, b_2) := (a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1).$$

Ekkor megmutatható, hogy az előbb definiált Θ kongruencia. **Definiáljuk úgy az egész számok gyűrűjét**, mint az

$$(\mathbf{N} \times \mathbf{N}; +, \cdot)/\Theta$$

faktoralgebrát!!!

Az $(\mathbf{N}\times\mathbf{N};+,\cdot)$ algebra az itáliai városállamokban kialakult kettős könyvelésre emlékeztet: $(a,b)\in\mathbf{N}\times\mathbf{N}$ esetén jelentheti pl. a a bevételt, b a kiadást. Ez esetben

$$((a_1,b_1),(a_2,b_2))\in\Theta \iff a_1+b_2=a_2+b_1$$

úgy interpretálható, hogy az (a_1,b_1) mérlegű és az (a_2,b_2) mérlegű cég profitja egyenlő.

Az $(\mathbf{N}\times\mathbf{N};+,\cdot)$ algebra az itáliai városállamokban kialakult kettős könyvelésre emlékeztet: $(a,b)\in\mathbf{N}\times\mathbf{N}$ esetén jelentheti pl. a a bevételt, b a kiadást. Ez esetben

$$((a_1,b_1),(a_2,b_2))\in\Theta \iff a_1+b_2=a_2+b_1$$

úgy interpretálható, hogy az (a_1,b_1) mérlegű és az (a_2,b_2) mérlegű cég profitja egyenlő. Az $(\mathbf{N}\times\mathbf{N};+,\cdot)/\Theta \cong (\mathbf{Z};+,\cdot)$ izomorfia ebből a szempontból is érdekes lehet.

Feladat: Legyen A és B tetszőleges félcsoport. Igaz-e, hogy A izomorf az $A \times B$ direkt szorzat egy faktoralgebrájával?

Megoldás: $\top$

Megoldás: Tanultuk, hogy a

$$\pi_1 : A \times B \to A, \qquad (a, b) \mapsto a,$$

Megoldás: Tanultuk, hogy a

$$\pi_1 : A \times B \to A, \qquad (a, b) \mapsto a,$$

azaz az első tényezőre való vetítés

Megoldás: Tanultuk, hogy a

$$\pi_1 : A \times B \to A, \qquad (a, b) \mapsto a,$$

azaz az első tényezőre való vetítés szürjektív homomorfizmus.

Megoldás: Tanultuk, hogy a

$$\pi_1 : A \times B \to A, \qquad (a, b) \mapsto a,$$

azaz az első tényezőre való vetítés szürjektív homomorfizmus. A homomorfiatétel szerint ezért

Megoldás: Tanultuk, hogy a

$$\pi_1 : A \times B \to A, \qquad (a,b) \mapsto a,$$

azaz az első tényezőre való vetítés szürjektív homomorfizmus. A homomorfiatétel szerint ezért A izomorf az $(A \times B)/\mathrm{ker}\varphi$ faktoralgebrával. Tehát a válasz igenlő.

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás:

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor —

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} =$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$.

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 =$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 =$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 =$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 =$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$
$$\bar{5}^3 =$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$
$$\bar{5}^3 = (-\bar{2})^3$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$

$$\bar{5}^3 = (-\bar{2})^3 = -\bar{2}^3$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$
$$\bar{5}^3 = (-\bar{2})^3 = -\bar{2}^3 = -\bar{1},$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$
$$\bar{5}^3 = (-\bar{2})^3 = -\bar{2}^3 = -\bar{1},\ \bar{6}^3 =$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$
$$\bar{5}^3 = (-\bar{2})^3 = -\bar{2}^3 = -\bar{1},\ \bar{6}^3 = (-\bar{1})^3$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$
$$\bar{5}^3 = (-\bar{2})^3 = -\bar{2}^3 = -\bar{1},\ \bar{6}^3 = (-\bar{1})^3 = -\bar{1},$$

Feladat: Hány megoldása van a $\mathbf{Z}_{35}$ maradékosztálygyűrűben az $x^3 = -\bar{1}$ egyenletnek?

Megoldás: Nyilván ugyanannyi, mint a $\mathbf{Z}_{35}$-tel izomorf $\mathbf{Z}_7 \times \mathbf{Z}_5$ direkt szorzatban!

Keressük a megoldást $x = (y, z) \in \mathbf{Z}_7 \times \mathbf{Z}_5$ alakban! Ekkor — mivel a direkt szorzatban komponensenként számolunk — $\mathbf{Z}_7$-ben $y^3 = -\bar{1} = \bar{6}$. $\mathbf{Z}_7$ mind a hét elemét kipróbálva:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{1},\ \bar{3}^3 = -\bar{1},\ \bar{4}^3 = \bar{1},$$
$$\bar{5}^3 = (-\bar{2})^3 = -\bar{2}^3 = -\bar{1},\ \bar{6}^3 = (-\bar{1})^3 = -\bar{1},$$

tehát y háromféle lehet.

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 =$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 =$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 =$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3 = \bar{2},$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3 = \bar{2},\ \bar{4}^3$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3 = \bar{2},\ \bar{4}^3 = (-\bar{1})^3$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3 = \bar{2},\ \bar{4}^3 = (-\bar{1})^3 = -\bar{1},$$

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3 = \bar{2},\ \bar{4}^3 = (-\bar{1})^3 = -\bar{1},$$

tehát z egyféle lehet.

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3 = \bar{2},\ \bar{4}^3 = (-\bar{1})^3 = -\bar{1},$$

tehát z egyféle lehet. Ezért a feladatra a válasz:

Hasonlóan járunk el $\mathbf{Z}_5$-ben:

$$\bar{0}^3 = \bar{0},\ \bar{1}^3 = \bar{1},\ \bar{2}^3 = \bar{3},\ \bar{3}^3 = \bar{2},\ \bar{4}^3 = (-\bar{1})^3 = -\bar{1},$$

tehát z egyféle lehet. Ezért a feladatra a válasz: $3 \cdot 1 = 3$ megoldás van.

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 =$$

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} =$$

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff$$

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff y^3 \equiv -1 \pmod{35} \iff$$

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff y^3 \equiv -1 \pmod{35} \iff$$
$$35 \mid y^3 + 1 \iff$$

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff y^3 \equiv -1 \pmod{35} \iff$$
$$35 \mid y^3 + 1 \iff y^3 \equiv -1 \pmod{5} \text{ és } y^3 \equiv -1 \pmod{7}.$$

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff y^3 \equiv -1 \pmod{35} \iff$$
$$35 \mid y^3 + 1 \iff y^3 \equiv -1 \pmod 5 \text{ és } y^3 \equiv -1 \pmod 7.$$

Éppúgy ahogy az előbb, az első kongruenciának egy, a másodiknak három megoldása van.

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff y^3 \equiv -1 \pmod{35} \iff$$
$$35 \mid y^3 + 1 \iff y^3 \equiv -1 \pmod 5 \text{ és } y^3 \equiv -1 \pmod 7.$$

Éppúgy ahogy az előbb, az első kongruenciának egy, a másodiknak három megoldása van. Rögzítve egy (x_5, x_7) megoldáspárt (megtehető $1 \cdot 3 = 3$-féleképpen), az $y \equiv x_5 \pmod 5$ és $y \equiv x_7 \pmod 7$ kongruenciákból álló rendszernek —

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff y^3 \equiv -1 \pmod{35} \iff$$
$$35 \mid y^3 + 1 \iff y^3 \equiv -1 \pmod 5 \text{ és } y^3 \equiv -1 \pmod 7.$$

Éppúgy ahogy az előbb, az első kongruenciának egy, a másodiknak három megoldása van. Rögzítve egy (x_5, x_7) megoldáspárt (megtehető $1 \cdot 3 = 3$-féleképpen), az $y \equiv x_5 \pmod 5$ és $y \equiv x_7 \pmod 7$ kongruenciákból álló rendszernek — a kínai maradéktétel szerint — pontosan egy megoldása van modulo 35.

Megjegyzés: A feladat anélkül is megoldható, hogy a $\mathbf{Z}_{35} \cong \mathbf{Z}_7 \times \mathbf{Z}_5$ izomorfiát felhasználnánk: keressük a megoldást $\bar{y}$ alakban, ahol $y \in \mathbf{Z}$. Ekkor

$$\bar{y}^3 = \overline{y^3} = -\bar{1} = \overline{-1} \iff y^3 \equiv -1 \pmod{35} \iff$$
$$35 \mid y^3 + 1 \iff y^3 \equiv -1 \pmod{5} \text{ és } y^3 \equiv -1 \pmod{7}.$$

Éppúgy ahogy az előbb, az első kongruenciának egy, a másodiknak három megoldása van. Rögzítve egy (x_5, x_7) megoldáspárt (megtehető $1 \cdot 3 = 3$-féleképpen), az $y \equiv x_5 \pmod{5}$ és $y \equiv x_7 \pmod{7}$ kongruenciákból álló rendszernek — a kínai maradéktétel szerint — pontosan egy megoldása van modulo 35. Tehát az $y^3 \equiv -1 \pmod{35}$ kongruenciának pontosan három megoldása van modulo 35, és nyilván ugyanennyi megoldása van az $x^3 = -\bar{1}$ egyenletnek $\mathbf{Z}_{35}$-ben.

Ma csak feladatokat veszünk — és persze megoldási fogásokat is.

Feladat: Legyen $\mathbf{R}^2$ a sík pontjainak halmaza. Ezen a halmazon legyen $*$ a számtani közép képzésének művelete, pontosabban szólva a helyvektorok számtani képzésének művelete.

Feladat: Legyen $\mathbf{R}^2$ a sík pontjainak halmaza. Ezen a halmazon legyen $*$ a számtani közép képzésének művelete, pontosabban szólva a helyvektorok számtani képzésének művelete. Azaz a sík A és B pontjaira jelölje $A * B$ az AB szakasz felezőpontját.

Feladat: Legyen $\mathbf{R}^2$ a sík pontjainak halmaza. Ezen a halmazon legyen $*$ a számtani közép képzésének művelete, pontosabban szólva a helyvektorok számtani képzésének művelete. Azaz a sík A és B pontjaira jelölje $A * B$ az AB szakasz felezőpontját. Legyen K az origó középpontú zárt kör, azaz

$$K = \{(x, y) : x^2 + y^2 \leq 1\},$$

és legyen

$$N = \{(x, y) \in \mathbf{R}^2 : 0 \leq x \leq 1,\ 0 \leq y \leq 1\}$$

a zárt egységnégyzet.

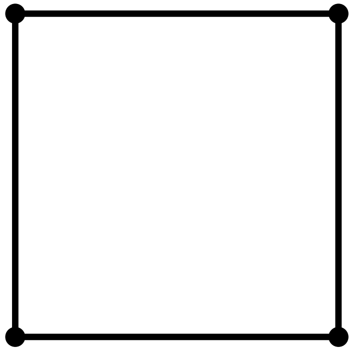
Feladat: Legyen $\mathbf{R}^2$ a sík pontjainak halmaza. Ezen a halmazon legyen $*$ a számtani közép képzésének művelete, pontosabban szólva a helyvektorok számtani képzésének művelete. Azaz a sík A és B pontjaira jelölje $A * B$ az AB szakasz felezőpontját. Legyen K az origó középpontú zárt kör, azaz

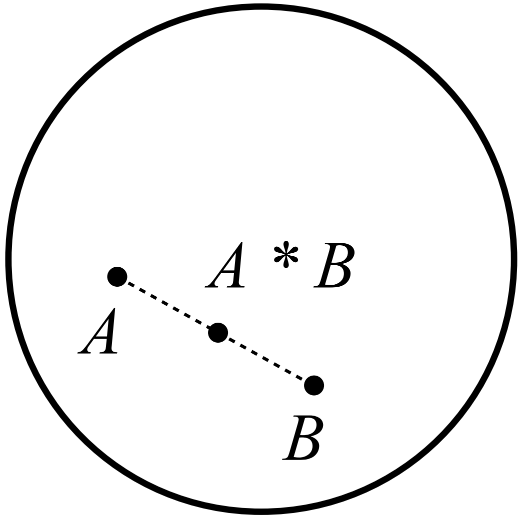
$$K = \{(x, y) : x^2 + y^2 \leq 1\},$$

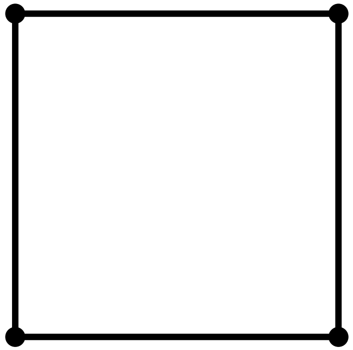
és legyen

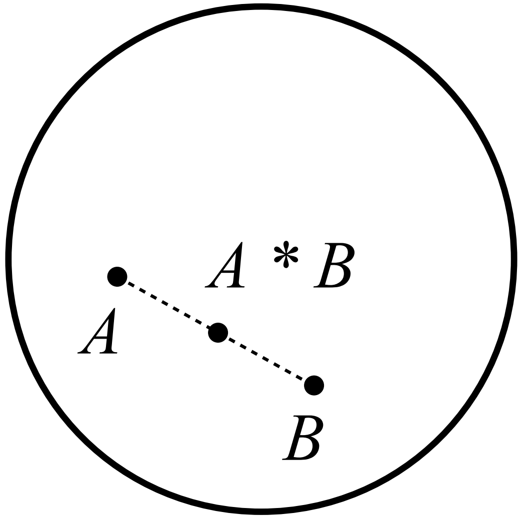
$$N = \{(x, y) \in \mathbf{R}^2 : 0 \leq x \leq 1,\ 0 \leq y \leq 1\}$$

a zárt egységnégyzet. Ekkor $(K; *)$ és $(N; *)$ egy-egy grupoid. Izomorfak-e?

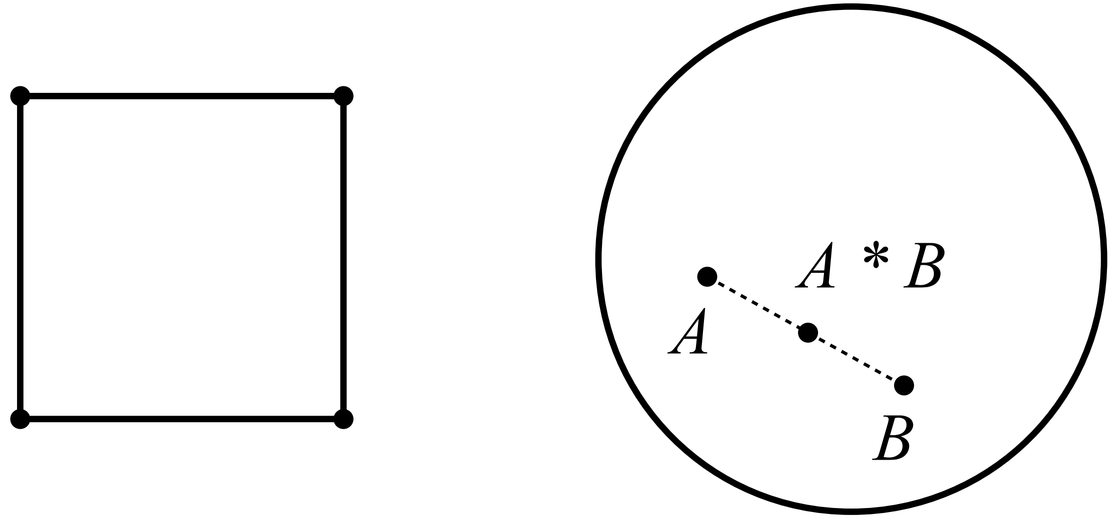



A * B
A
B





Megjegyzés: ily módon minden konvex síkidom grupoidnak tekinthető.



Megjegyzés: ily módon minden konvex síkidom grupoidnak tekinthető. A művelet idempotens, azaz bármely x-re $x * x = x$.

Megoldás: $\top$

Megoldás: Tekintsük azt az $F(x)$ formulát a tekintett grupoidok nyelvében, amelyik azt fejezi ki, hogy x csak triviálisan (azaz csakis $x * x$ módon) áll elő művelet eredményeként. (Nevezhetnénk ezt a tulajdonságot ideiglenesen pl. „izoláltnak”.)

Megoldás: Tekintsük azt az $F(x)$ formulát a tekintett grupoidok nyelvében, amelyik azt fejezi ki, hogy x csak triviálisan (azaz csakis $x * x$ módon) áll elő művelet eredményeként. (Nevezhetnénk ezt a tulajdonságot ideiglenesen pl. „izoláltnak”.) Ilyen formula nyilván van,

Megoldás: Tekintsük azt az $F(x)$ formulát a tekintett grupoidok nyelvében, amelyik azt fejezi ki, hogy x csak triviálisan (azaz csakis $x * x$ módon) áll elő művelet eredményeként. (Nevezhetnénk ezt a tulajdonságot ideiglenesen pl. „izoláltnak”.) Ilyen formula nyilván van, például $F(x)$ jelölheti a

Megoldás: Tekintsük azt az $F(x)$ formulát a tekintett grupoidok nyelvében, amelyik azt fejezi ki, hogy x csak triviálisan (azaz csakis $x * x$ módon) áll elő művelet eredményeként. (Nevezhetnénk ezt a tulajdonságot ideiglenesen pl. „izoláltnak”.) Ilyen formula nyilván van, például $F(x)$ jelölheti a

$$(\forall y)(\forall z)(x = y * z \to (y = x \land z = x)))$$

formulát.

Megoldás: Tekintsük azt az $F(x)$ formulát a tekintett grupoidok nyelvében, amelyik azt fejezi ki, hogy x csak triviálisan (azaz csakis $x * x$ módon) áll elő művelet eredményeként. (Nevezhetnénk ezt a tulajdonságot ideiglenesen pl. „izoláltnak”.) Ilyen formula nyilván van, például $F(x)$ jelölheti a

$$(\forall y)(\forall z)(x = y * z \to (y = x \wedge z = x)))$$

formulát. Ennek segítségével legyen

$$G = (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)(F(x_1) \wedge \cdots \wedge F(x_4) \wedge$$
$$\neg(x_1 = x_2) \wedge \cdots \wedge \neg(x_3 = x_4) \wedge$$
$$(\forall y)(F(y) \to (y = x_1 \vee \cdots \vee y = x_4))).$$

(Ez természetesen csak akkor lesz formula, ha F definícióját behelyettesítjük, és a $\cdots$ helyett részletesen kiírjuk.) G azt fejezi ki, hogy pontosan négy izolált pont van. Nyilván G teljesül N-ben (ahol éppen a csúcsok az izolált pontok), de

$$G = (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)(F(x_1) \wedge \cdots \wedge F(x_4) \wedge$$
$$\neg(x_1 = x_2) \wedge \cdots \wedge \neg(x_3 = x_4) \wedge$$
$$(\forall y)(F(y) \to (y = x_1 \vee \cdots \vee y = x_4))).$$

(Ez természetesen csak akkor lesz formula, ha F definícióját behelyettesítjük, és a $\cdots$ helyett részletesen kiírjuk.) G azt fejezi ki, hogy pontosan négy izolált pont van. Nyilván G teljesül N-ben (ahol éppen a csúcsok az izolált pontok), de nem teljesül K-ban (ahol minden kerületi pont izolált).

$$G = (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)(F(x_1) \wedge \cdots \wedge F(x_4) \wedge$$
$$\neg(x_1 = x_2) \wedge \cdots \wedge \neg(x_3 = x_4) \wedge$$
$$(\forall y)(F(y) \to (y = x_1 \vee \cdots \vee y = x_4))).$$

(Ez természetesen csak akkor lesz formula, ha F definícióját behelyettesítjük, és a $\cdots$ helyett részletesen kiírjuk.) G azt fejezi ki, hogy pontosan négy izolált pont van. Nyilván G teljesül N-ben (ahol éppen a csúcsok az izolált pontok), de nem teljesül K-ban (ahol minden kerületi pont izolált). Egy korábbi tételünket alkalmazva (

$$G = (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)(F(x_1) \wedge \cdots \wedge F(x_4) \wedge$$
$$\neg(x_1 = x_2) \wedge \cdots \wedge \neg(x_3 = x_4) \wedge$$
$$(\forall y)(F(y) \to (y = x_1 \vee \cdots \vee y = x_4))).$$

(Ez természetesen csak akkor lesz formula, ha F definícióját behelyettesítjük, és a $\cdots$ helyett részletesen kiírjuk.) G azt fejezi ki, hogy pontosan négy izolált pont van. Nyilván G teljesül N-ben (ahol éppen a csúcsok az izolált pontok), de nem teljesül K-ban (ahol minden kerületi pont izolált). Egy korábbi tételünket alkalmazva („izomorf algebrákban pontosan ugyanazok a zárt formulák teljesülnek")

$$G = (\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)(F(x_1) \wedge \cdots \wedge F(x_4) \wedge$$
$$\neg(x_1 = x_2) \wedge \cdots \wedge \neg(x_3 = x_4) \wedge$$
$$(\forall y)(F(y) \to (y = x_1 \vee \cdots \vee y = x_4))).$$

(Ez természetesen csak akkor lesz formula, ha F definícióját behelyettesítjük, és a $\cdots$ helyett részletesen kiírjuk.) G azt fejezi ki, hogy pontosan négy izolált pont van. Nyilván G teljesül N-ben (ahol éppen a csúcsok az izolált pontok), de nem teljesül K-ban (ahol minden kerületi pont izolált). Egy korábbi tételünket alkalmazva („izomorf algebrákban pontosan ugyanazok a zárt formulák teljesülnek") kapjuk, hogy N és K nem izomorf.

Nehezebb feladat:

Nehezebb feladat: a **nyílt** kör és a **nyílt** négyzet

$$K^- = (\{(x,y) : x^2 + y^2 < 1\}; *)$$

és

$$N^- = (\{(x,y) \in \mathbf{R}^2 : 0 < x < 1,\ 0 < y < 1\}; *),$$

mint az előbbi értelemben vett grupoidok, izomorfak-e?

Nehezebb feladat: a **nyílt** kör és a **nyílt** négyzet

$$K^- = (\{(x,y) : x^2 + y^2 < 1\}; *)$$

és

$$N^- = (\{(x,y) \in \mathbf{R}^2 : 0 < x < 1,\ 0 < y < 1\}; *),$$

mint az előbbi értelemben vett grupoidok, izomorfak-e?

Aki ezt a feladatot elsőnek megoldja (matematikailag szabatos indoklás is kell!),

Nehezebb feladat: a **nyílt** kör és a **nyílt** négyzet

$$K^{-} = (\{(x, y) : x^2 + y^2 < 1\}; *)$$

és

$$N^{-} = (\{(x, y) \in \mathbf{R}^2 : 0 < x < 1,\ 0 < y < 1\}; *),$$

mint az előbbi értelemben vett grupoidok, izomorfak-e?

Aki ezt a feladatot elsőnek megoldja (matematikailag szabatos indoklás is kell!), 30, azaz **harminc**

Nehezebb feladat: a **nyílt** kör és a **nyílt** négyzet

$$K^{-} = (\{(x,y) : x^2 + y^2 < 1\}; *)$$

és

$$N^{-} = (\{(x,y) \in \mathbf{R}^2 : 0 < x < 1,\ 0 < y < 1\}; *),$$

mint az előbbi értelemben vett grupoidok, izomorfak-e?

Aki ezt a feladatot elsőnek megoldja (matematikailag szabatos indoklás is kell!), 30, azaz **harminc** vizsgapont kap; legfeljebb öt próbálkozást bírálok el! (EHA kódot is kérek, a próbálkozások számáról és eredményéről a honlapomon tudósítok. Vizsgapontról van szó, a gyakorlaton szerzett 20 pont továbbra is a vizsga előfeltétele marad.)

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Feladat: A fenti műveletTáblázatával megadott $(A;*)$ grupoid esetén határozzunk meg mindent, amit tanultunk!

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Feladat: A fenti művelettáblázatával megadott $(A; *)$ grupoid esetén határozzunk meg mindent, amit tanultunk!

A művelet kommutatív?

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Feladat: A fenti művelettáblázatával megadott $(A; *)$ grupoid esetén határozzunk meg mindent, amit tanultunk!

A művelet kommutatív? Nem, mert a táblázat nem szimmetrikus az ÉNy — DK egyenesre (átlóra), pl. $a = a * c \neq c * a = c$.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Feladat: A fenti művelettáblázatával megadott $(A;*)$ grupoid esetén határozzunk meg mindent, amit tanultunk!

A művelet kommutatív? Nem, mert a táblázat nem szimmetrikus az ÉNy — DK egyenesre (átlóra), pl. $a = a*c \neq c*a = c$. A továbbiakban a műveletet egymás mellé írással is jelöljük.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív?

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő. Nem, pl.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő. Nem, pl.

$$(aa)c =$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő. Nem, pl.

$$(aa)c = ec =$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő. Nem, pl.

$$(aa)c = ec = d,$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő. Nem, pl.

$$(aa)c = ec = d, \qquad a(ac) =$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő. Nem, pl.

$$(aa)c = ec = d, \qquad a(ac) = aa =$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

A művelet asszociatív? Ez általában nehéz kérdés, igen sok eset vizsgálatát igényli, de most szerencsénk van — egy-két próbálkozás elegendő. Nem, pl.

$$(aa)c = ec = d, \qquad a(ac) = aa = e \neq d.$$

Ezért $(A;*)$ nem félcsoport, és nem csoport.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem?

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (Hiszen nincs olyan elem, amelynek sorában a fejléc sor, oszlopában a fejléc oszlop lenne.)

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (Hiszen nincs olyan elem, amelynek sorában a fejléc sor, oszlopában a fejléc oszlop lenne.) Van-e zéruselem?

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (Hiszen nincs olyan elem, amelynek sorában a fejléc sor, oszlopában a fejléc oszlop lenne.) Van-e zéruselem? Nincs,

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (Hiszen nincs olyan elem, amelynek sorában a fejléc sor, oszlopában a fejléc oszlop lenne.) Van-e zéruselem? Nincs, mert nincs olyan elem, hogy csak ő szerepelne a sorában is és oszlopában is.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (Hiszen nincs olyan elem, amelynek sorában a fejléc sor, oszlopában a fejléc oszlop lenne.) Van-e zéruselem? Nincs, mert nincs olyan elem, hogy csak ő szerepelne a sorában is és oszlopában is. A művelet kancellatív-e (más szóval: egyszerűsítéses-e)?

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (Hiszen nincs olyan elem, amelynek sorában a fejléc sor, oszlopában a fejléc oszlop lenne.) Van-e zéruselem? Nincs, mert nincs olyan elem, hogy csak ő szerepelne a sorában is és oszlopában is. A művelet kancellatív-e (más szóval: egyszerűsítéses-e)? Nem, hiszen

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Van egységelem? Nincs! (Hiszen nincs olyan elem, amelynek sorában a fejléc sor, oszlopában a fejléc oszlop lenne.) Van-e zéruselem? Nincs, mert nincs olyan elem, hogy csak ő szerepelne a sorában is és oszlopában is. A művelet kancellatív-e (más szóval: egyszerűsítéses-e)? Nem, hiszen ha az lenne, akkor minden sorban az elemek különbözőek lennének, és ugyanez lenne az oszlopokra is érvényes.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Mik a részalgebrák?

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Mik a részalgebrák? (**Ez tanulságos lesz!**) Kezdjük a **ciklikus részalgebrák**

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Mik a részalgebrák? (**Ez tanulságos lesz!**) Kezdjük a **ciklikus részalgebrák** meghatározásával! (Emlékeztető: $[X]$ pontosan azon elemekből áll, amelyek megkaphatók X elemeiből a műveletek egyszeri vagy többszöri alkalmazásával. $[x]$ pedig azokból, amelyek x-ből nyerhetők —

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Mik a részalgebrák? (**Ez tanulságos lesz!**) Kezdjük a **ciklikus részalgebrák** meghatározásával! (Emlékeztető: $[X]$ pontosan azon elemekből áll, amelyek megkaphatók X elemeiből a műveletek egyszeri vagy többszöri alkalmazásával. $[x]$ pedig azokból, amelyek x-ből nyerhetők — de most nem mondhatunk hatványt, x^n-t, mert

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Mik a részalgebrák? (**Ez tanulságos lesz!**) Kezdjük a **ciklikus részalgebrák** meghatározásával! (Emlékeztető: $[X]$ pontosan azon elemekből áll, amelyek megkaphatók X elemeiből a műveletek egyszeri vagy többszöri alkalmazásával. $[x]$ pedig azokból, amelyek x-ből nyerhetők — de most nem mondhatunk hatványt, x^n-t, mert annak csak félcsoportban van értelme, most viszont pl. $(bb)b = eb = b$ de

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Mik a részalgebrák? (**Ez tanulságos lesz!**) Kezdjük a **ciklikus részalgebrák** meghatározásával! (Emlékeztető: $[X]$ pontosan azon elemekből áll, amelyek megkaphatók X elemeiből a műveletek egyszeri vagy többszöri alkalmazásával. $[x]$ pedig azokból, amelyek x-ből nyerhetők — de most nem mondhatunk hatványt, x^n-t, mert annak csak félcsoportban van értelme, most viszont pl. $(bb)b = eb = b$ de $b(bb) = be = d$.)

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az alábbiakhoz: mondjuk $[a]$ meghatározásához:

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az alábbiakhoz: mondjuk $[a]$ meghatározásához: biztos benne van a, tehát elindulunk $\{a\}$-ból.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az alábbiakhoz: mondjuk $[a]$ meghatározásához: biztos benne van a, tehát elindulunk $\{a\}$-ból. Ha ez részgrupoid, akkor kész.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az alábbiakhoz: mondjuk $[a]$ meghatározásához: biztos benne van a, tehát elindulunk $\{a\}$-ból. Ha ez részgrupoid, akkor kész. De most nem az, mert $aa = e$ nincs benne.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az alábbiakhoz: mondjuk $[a]$ meghatározásához: biztos benne van a, tehát elindulunk $\{a\}$-ból. Ha ez részgrupoid, akkor kész. De most nem az, mert $aa = e$ nincs benne. Ezért e-t is hozzávesszük: $\{a, e\}$. Megint vizsgáljuk, hogy ez zárt-e a szorzásra.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az alábbiakhoz: mondjuk $[a]$ meghatározásához: biztos benne van a, tehát elindulunk $\{a\}$-ból. Ha ez részgrupoid, akkor kész. De most nem az, mert $aa = e$ nincs benne. Ezért e-t is hozzávesszük: $\{a, e\}$. Megint vizsgáljuk, hogy ez zárt-e a szorzásra. Nem, mert $ae = c$ (és mellesleg $ee = c$). Hozzávesszük c-t is. Megint vizsgáljuk, hogy zárt-e a műveletre.

És így tovább.

És így tovább. Tehát mindig csak művelet eredményét vesszük hozzá.

És így tovább. Tehát mindig csak művelet eredményét vesszük hozzá. Ha nem tudunk hozzávenni, akkor vagyunk készen.

És így tovább. Tehát mindig csak művelet eredményét vesszük hozzá. Ha nem tudunk hozzávenni, akkor vagyunk készen. Ugyanígy határozzuk meg a részhalmaz által generált részalgebrát is.

És így tovább. Tehát mindig csak művelet eredményét vesszük hozzá. Ha nem tudunk hozzávenni, akkor vagyunk készen. Ugyanígy határozzuk meg a részhalmaz által generált részalgebrát is.

Azért célszerű előbb a ciklikus (azaz egy elem által generált) részgrupoidokat meghatározni, mert amikor a későbbiekben $[X]$-et számoljuk

És így tovább. Tehát mindig csak művelet eredményét vesszük hozzá. Ha nem tudunk hozzávenni, akkor vagyunk készen. Ugyanígy határozzuk meg a részhalmaz által generált részalgebrát is.

Azért célszerű előbb a ciklikus (azaz egy elem által generált) részgrupoidokat meghatározni, mert amikor a későbbiekben $[X]$-et számoljuk — X egyelemű is lehet —

És így tovább. Tehát mindig csak művelet eredményét vesszük hozzá. Ha nem tudunk hozzávenni, akkor vagyunk készen. Ugyanígy határozzuk meg a részhalmaz által generált részalgebrát is.

Azért célszerű előbb a ciklikus (azaz egy elem által generált) részgrupoidokat meghatározni, mert amikor a későbbiekben $[X]$-et számoljuk — X egyelemű is lehet — és egy y elemet bevettünk a halmazba (vagy eleve benne volt), akkor nyilván $[y]$ összes elemét is bevehetjük. (

És így tovább. Tehát mindig csak művelet eredményét vesszük hozzá. Ha nem tudunk hozzávenni, akkor vagyunk készen. Ugyanígy határozzuk meg a részhalmaz által generált részalgebrát is.

Azért célszerű előbb a ciklikus (azaz egy elem által generált) részgrupoidokat meghatározni, mert amikor a későbbiekben $[X]$-et számoljuk — X egyelemű is lehet — és egy y elemet bevettünk a halmazba (vagy eleve benne volt), akkor nyilván $[y]$ összes elemét is bevehetjük. (És ezáltal gyorsabban haladunk.)

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c,$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e,$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$
$$[b] = \{b, e, d, c\},$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c,$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b,$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b, \ \ldots\} \subseteq [b] \ni c \Longrightarrow [c] = [b],$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b, \ \ldots\} \subseteq [b] \ni c \Longrightarrow [c] = [b],$$

$$[d] \ni b$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b, \ \ldots\} \subseteq [b] \ni c \Longrightarrow [c] = [b],$$

$$[d] \ni b \wedge d \in [b]$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b, \ \ldots\} \subseteq [b] \ni c \Longrightarrow [c] = [b],$$

$$[d] \ni b \wedge d \in [b] \Longrightarrow [d] = [b],$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b, \ \ldots\} \subseteq [b] \ni c \implies [c] = [b],$$

$$[d] \ni b \wedge d \in [b] \implies [d] = [b],$$

$$[e] \ni c$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b, \ \ldots\} \subseteq [b] \ni c \implies [c] = [b],$$

$$[d] \ni b \wedge d \in [b] \implies [d] = [b],$$

$$[e] \ni c \wedge$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$[a] = \{a, e, c, b, d\} = A,$$

$$[b] = \{b, e, d, c\},$$

$$[c] = \{c, b, \ldots\} \subseteq [b] \ni c \Longrightarrow [c] = [b],$$

$$[d] \ni b \wedge d \in [b] \Longrightarrow [d] = [b],$$

$$[e] \ni c \wedge e \in [c] \Longrightarrow [e] = [c] = [b].$$

Megvannak a ciklikus részalgebrák:

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$.

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is.

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többbit is. Ha S egy részalgebra és $a \in S$, akkor

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$.

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} =$

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq$

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq S \subseteq$

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq S \subseteq A \setminus \{a\}$ miatt

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq S \subseteq A \setminus \{a\}$ miatt $S = [b]$.

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq S \subseteq A \setminus \{a\}$ miatt $S = [b]$.

Tehát csak két részalgebra van: A és $\{b, c, d, e\}$. Mindkettő ciklikus. Az eredeti algebra is ciklikus.

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq S \subseteq A \setminus \{a\}$ miatt $S = [b]$.

Tehát csak két részalgebra van: A és $\{b, c, d, e\}$. Mindkettő ciklikus. Az eredeti algebra is ciklikus.

A **kongruenciák** meghatározása is hasonlóképpen történik. A ciklikus részalgebra szerepét az egyetlen elempár „által generált” (

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq S \subseteq A \setminus \{a\}$ miatt $S = [b]$.

Tehát csak két részalgebra van: A és $\{b, c, d, e\}$. Mindkettő ciklikus. Az eredeti algebra is ciklikus.

A **kongruenciák** meghatározása is hasonlóképpen történik. A ciklikus részalgebra szerepét az egyetlen elempár „által generált" (azaz az adott elempárt tartalmazó legszűkebb) kongruencia veszi át.

Megvannak a ciklikus részalgebrák: A és $\{b, c, d, e\}$. Innen már roppant könnyen kapjuk a többit is. Ha S egy részalgebra és $a \in S$, akkor $[a] \subseteq S$ miatt $S = A$. Ha pedig $a \notin S$, akkor a b, c, d, e elemek valamelyike, mondjuk pl. b benne van S-ben, és így $A \setminus \{a\} = [b] \subseteq S \subseteq A \setminus \{a\}$ miatt $S = [b]$.

Tehát csak két részalgebra van: A és $\{b, c, d, e\}$. Mindkettő ciklikus. Az eredeti algebra is ciklikus.

A **kongruenciák** meghatározása is hasonlóképpen történik. A ciklikus részalgebra szerepét az egyetlen elempár „által generált" (azaz az adott elempárt tartalmazó legszűkebb) kongruencia veszi át. Ezeket érdemes legelőször meghatároznunk. A számolást csökkenti az alábbi észrevétel is:

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A; \cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely*

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A; \cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

ha $(a, b) \in \Theta$ *akkor*

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A; \cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\text{ha } (a, b) \in \Theta \text{ akkor } (ac, bc) \in \Theta \text{ és } (ca, cb) \in \Theta.$$

Bizonyítás:

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a,b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c, c) \in \Theta$, a feltétel

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a,b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c,c) \in \Theta$, a feltétel szükséges.

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A; \cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a, b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c, c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1, b_1), (a_2, b_2) \in \Theta$ tetszőleges. Ekkor

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a,b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c,c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1, b_1), (a_2, b_2) \in \Theta$ tetszőleges. Ekkor $(a_1 a_2, b_1 a_2) \in \Theta$ (

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a,b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c,c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1, b_1), (a_2, b_2) \in \Theta$ tetszőleges. Ekkor $(a_1a_2, b_1a_2) \in \Theta$ (itt a_2 játszotta c szerepét) és $(b_1a_2, b_1b_2) \in \Theta$ (

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A; \cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a, b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c, c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1, b_1), (a_2, b_2) \in \Theta$ tetszőleges. Ekkor $(a_1 a_2, b_1 a_2) \in \Theta$ (itt a_2 játszotta c szerepét) és $(b_1 a_2, b_1 b_2) \in \Theta$ (itt pedig b_1 játszotta c szerepét).

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A; \cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a, b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c, c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1, b_1), (a_2, b_2) \in \Theta$ tetszőleges. Ekkor $(a_1 a_2, b_1 a_2) \in \Theta$ (itt a_2 játszotta c szerepét) és $(b_1 a_2, b_1 b_2) \in \Theta$ (itt pedig b_1 játszotta c szerepét). A tranzitivitás miatt így $(a_1 a_2, b_1 b_2) \in \Theta$.

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a,b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c,c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1, b_1), (a_2, b_2) \in \Theta$ tetszőleges. Ekkor $(a_1a_2, b_1a_2) \in \Theta$ (itt a_2 játszotta c szerepét) és $(b_1a_2, b_1b_2) \in \Theta$ (itt pedig b_1 játszotta c szerepét). A tranzitivitás miatt így $(a_1a_2, b_1b_2) \in \Theta$. Q.e.d.

18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a,b) \in \Theta \textit{ akkor } (ac, bc) \in \Theta \textit{ és } (ca, cb) \in \Theta.$$

Bizonyítás: Mivel $(c, c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1, b_1), (a_2, b_2) \in \Theta$ tetszőleges. Ekkor $(a_1a_2, b_1a_2) \in \Theta$ (itt a_2 játszotta c szerepét) és $(b_1a_2, b_1b_2) \in \Theta$ (itt pedig b_1 játszotta c szerepét). A tranzitivitás miatt így $(a_1a_2, b_1b_2) \in \Theta$. Q.e.d.

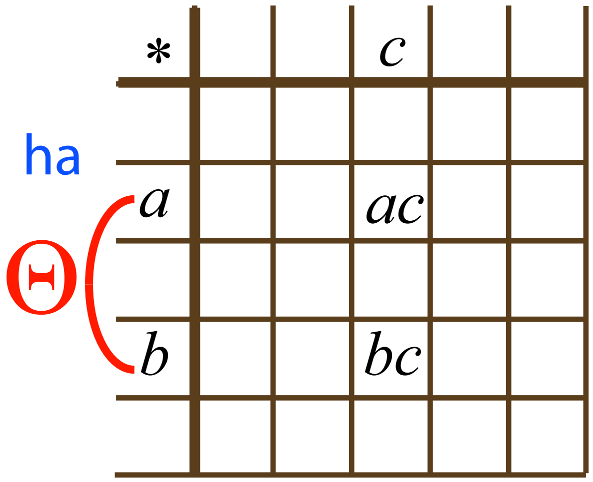
A fenti állítás a művelettáblázatok nyelvén?

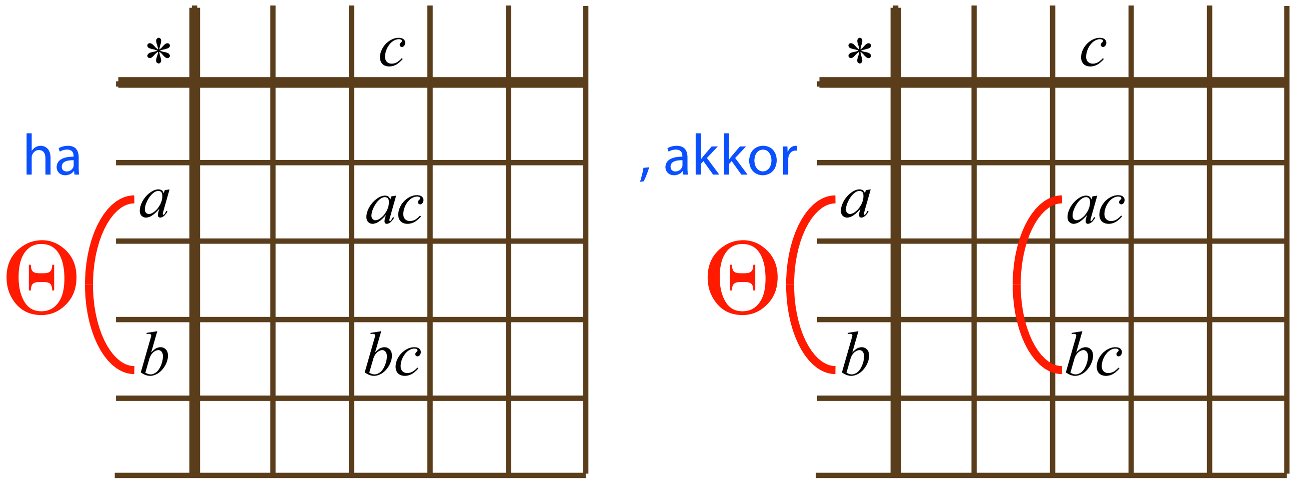
18. Állítás. *Ha* $\Theta \subseteq A^2$ *ekvivalenciareláció egy* $(A;\cdot)$ *grupoidon, akkor* Θ *akkor és csak akkor kongruencia, ha bármely* $a, b, c \in A$ *esetén*

$$\textit{ha } (a,b) \in \Theta \textit{ akkor } (ac,bc) \in \Theta \textit{ és } (ca,cb) \in \Theta.$$

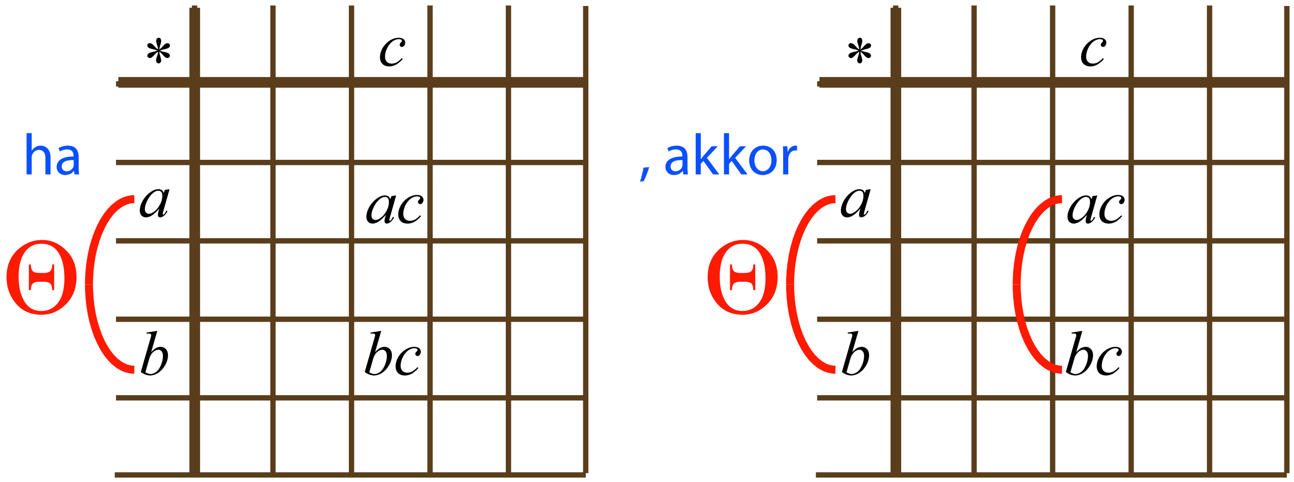
Bizonyítás: Mivel $(c,c) \in \Theta$, a feltétel szükséges. Most tegyük fel, hogy a feltétel teljesül. Legyen $(a_1,b_1),(a_2,b_2) \in \Theta$ tetszőleges. Ekkor $(a_1a_2,b_1a_2) \in \Theta$ (itt a_2 játszotta c szerepét) és $(b_1a_2,b_1b_2) \in \Theta$ (itt pedig b_1 játszotta c szerepét). A tranzitivitás miatt így $(a_1a_2,b_1b_2) \in \Theta$. Q.e.d.

A fenti állítás a műveletttáblázatok nyelvén?: $(\forall a)(\forall b)(\forall c)$

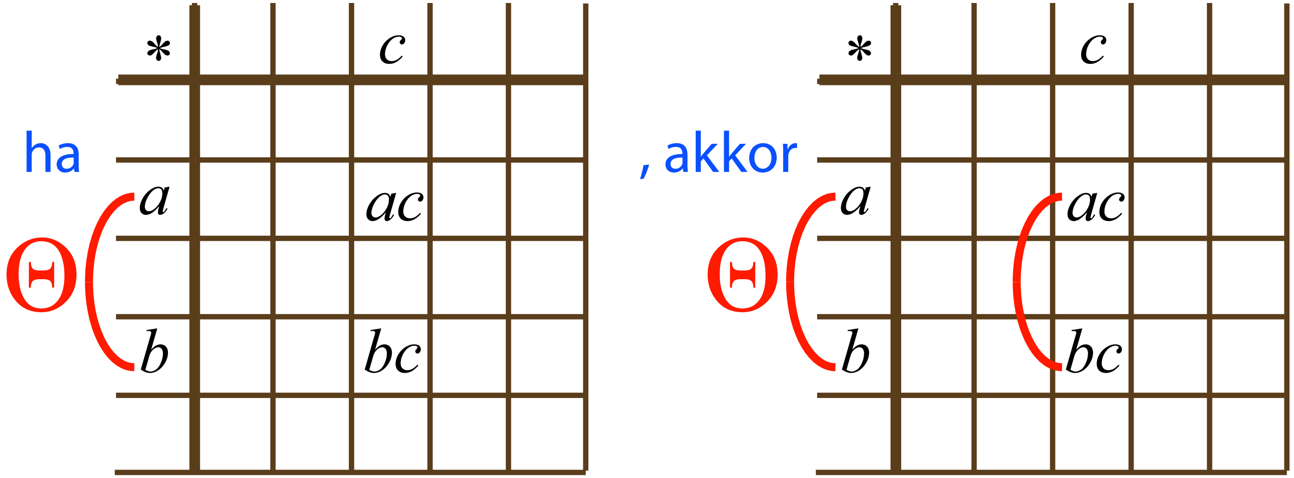

*
c
ha
a
ac
Θ
b
bc



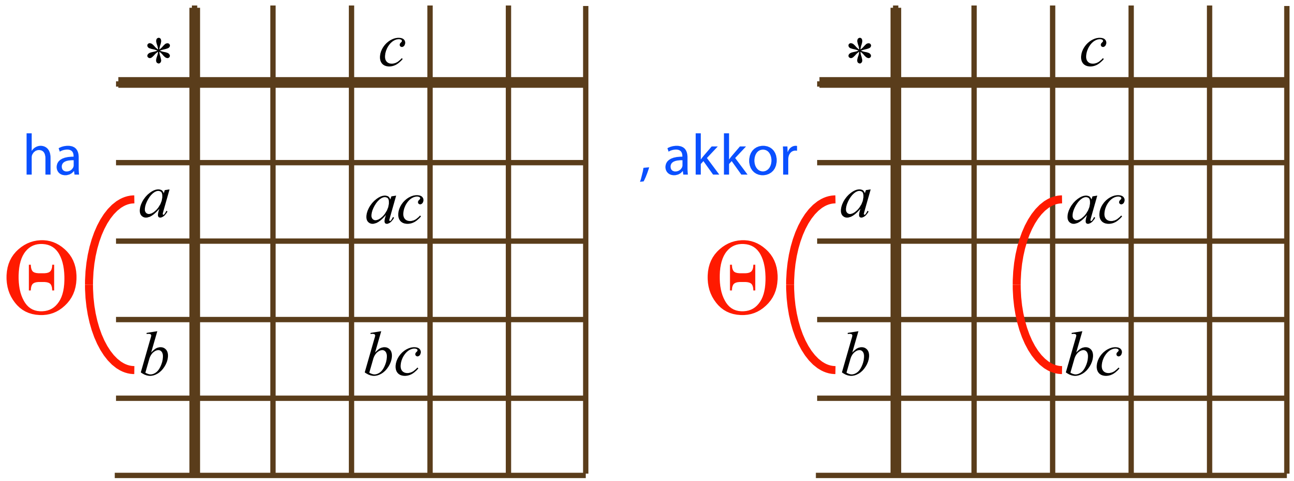
ha
*
c
a
ac
Θ
b
bc
, akkor
*
c
a
ac
Θ
b
bc



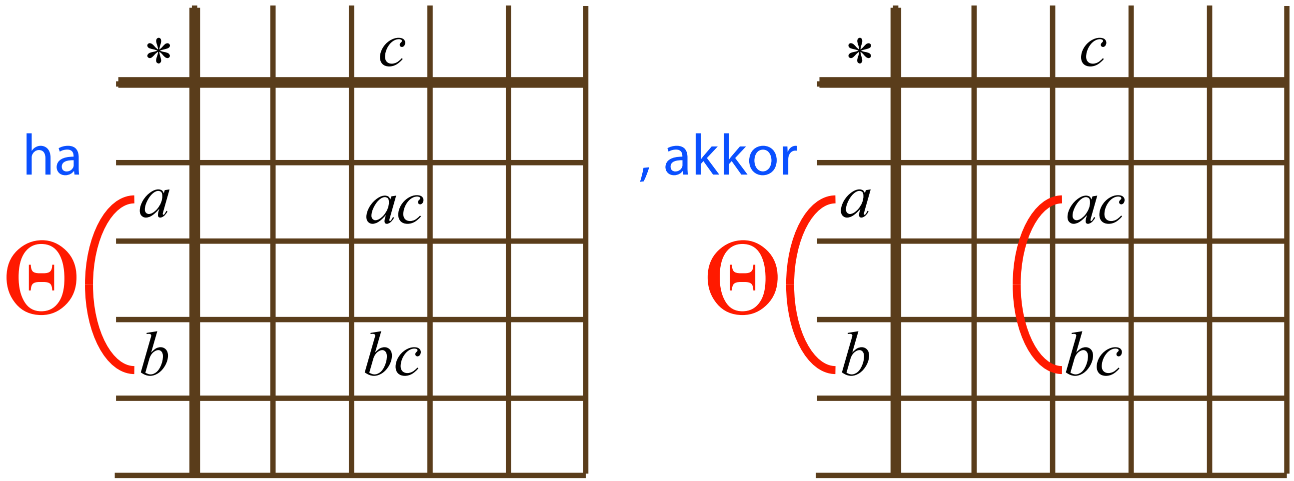
Azaz a kongruencia a sorfejlécekről „végigterjed az egész sorra” ,



Azaz a kongruencia a sorfejlécekről „végigterjed az egész sorra”, és persze ugyanez az oszlopokra is:



Azaz a kongruencia a sorfejlécekről „végigterjed az egész sorra”, és persze ugyanez az oszlopokra is: a kongruencia az „oszlopfejlécekről végigterjed az egész oszlopra” is.



Azaz a kongruencia a sorfejlécekről „végigterjed az egész sorra”, és persze ugyanez az oszlopokra is: a kongruencia az „oszlopfejlécekről végigterjed az egész oszlopra” is. Ez tehát a szükséges és elegendő feltétele annak, hogy egy Θ ekvivalencia kongruencia legyen.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ha $x \neq y \in A$, akkor jelölje Θ_{xy} a legszűkebb olyan kongruenciát, amelynek (x, y) eleme.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ha $x \neq y \in A$, akkor jelölje Θ_{xy} a legszűkebb olyan kongruenciát, amelynek (x, y) eleme. Jelölje $\mathcal{C}_{xy}$ a Θ_{xy}-nak megfelelő osztályozást.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ha $x \neq y \in A$, akkor jelölje Θ_{xy} a legszűkebb olyan kongruenciát, amelynek (x, y) eleme. Jelölje $\mathcal{C}_{xy}$ a Θ_{xy}-nak megfelelő osztályozást. Ekkor — a sorokon és oszlopokon való terjedést figyelembe véve egyre bővítve és bővítve —

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ha $x \neq y \in A$, akkor jelölje Θ_{xy} a legszűkebb olyan kongruenciát, amelynek (x, y) eleme. Jelölje $\mathcal{C}_{xy}$ a Θ_{xy}-nak megfelelő osztályozást. Ekkor — a sorokon és oszlopokon való terjedést figyelembe véve egyre bővítve és bővítve —

$$\Theta_{ab} \ni$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ha $x \neq y \in A$, akkor jelölje Θ_{xy} a legszűkebb olyan kongruenciát, amelynek (x, y) eleme. Jelölje $\mathcal{C}_{xy}$ a Θ_{xy}-nak megfelelő osztályozást. Ekkor — a sorokon és oszlopokon való terjedést figyelembe véve egyre bővítve és bővítve —

$$\Theta_{ab} \ni (a, b),$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ha $x \neq y \in A$, akkor jelölje Θ_{xy} a legszűkebb olyan kongruenciát, amelynek (x, y) eleme. Jelölje $\mathcal{C}_{xy}$ a Θ_{xy}-nak megfelelő osztályozást. Ekkor — a sorokon és oszlopokon való terjedést figyelembe véve egyre bővítve és bővítve —

$$\Theta_{ab} \ni (a, b), (c, d) \Longrightarrow \mathcal{C}_{a,b} = \{\{a, b\}, \{c, d\}, \{e\}\},$$

hiszen ez már nem „terjed tovább" a sorokon és oszlopokon.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ugyanígy:

$$\Theta_{cd} \ni$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ugyanígy:

$$\Theta_{cd} \ni (c, d),$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ugyanígy:

$$\Theta_{cd} \ni (c, d), (a, b)$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ugyanígy:

$$\Theta_{cd} \ni (c,d),(a,b), \qquad \mathcal{C}_{cd} = \{\{a,b\},\{c,d\},\{e\}\}$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ugyanígy:

$$\Theta_{cd} \ni (c,d),(a,b), \qquad \mathcal{C}_{cd} = \{\{a,b\},\{c,d\},\{e\}\} = \mathcal{C}_{ab}.$$

A továbbiakban az eddigieket is felhasználjuk, tehát ha pl. $(c,d) \in$ Θ (

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ugyanígy:

$$\Theta_{cd} \ni (c,d),(a,b), \qquad \mathcal{C}_{cd} = \{\{a,b\},\{c,d\},\{e\}\} = \mathcal{C}_{ab}.$$

A továbbiakban az eddigieket is felhasználjuk, tehát ha pl. $(c,d) \in \Theta$ ($\iff$ $(d,c) \in \Theta$),

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Ugyanígy:

$$\Theta_{cd} \ni (c,d), (a,b), \qquad \mathcal{C}_{cd} = \{\{a,b\},\{c,d\},\{e\}\} = \mathcal{C}_{ab}.$$

A továbbiakban az eddigieket is felhasználjuk, tehát ha pl. $(c,d) \in \Theta$ ($\iff$ $(d,c) \in \Theta$), akkor $\Theta_{cd} \subseteq \Theta$.

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e, c),$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e,c),(a,b)$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e, c), (a, b) \Longrightarrow$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e,c),(a,b) \Longrightarrow \Theta_{ac} = A^2,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e,c),(a,b) \Longrightarrow \Theta_{ac} = A^2,$$

$$\Theta_{ad} \ni (e,d),$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e, c), (a, b) \Longrightarrow \Theta_{ac} = A^2,$$

$$\Theta_{ad} \ni (e, d), (a, b)$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e,c),(a,b) \Longrightarrow \Theta_{ac} = A^2,$$

$$\Theta_{ad} \ni (e,d),(a,b) \Longrightarrow$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e,c),(a,b) \Longrightarrow \Theta_{ac} = A^2,$$
$$\Theta_{ad} \ni (e,d),(a,b) \Longrightarrow \Theta_{ad} = A^2,$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e, c), (a, b) \Longrightarrow \Theta_{ac} = A^2,$$
$$\Theta_{ad} \ni (e, d), (a, b) \Longrightarrow \Theta_{ad} = A^2,$$
$$\Theta_{ae} \ni (a, d)$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e, c), (a, b) \Longrightarrow \Theta_{ac} = A^2,$$
$$\Theta_{ad} \ni (e, d), (a, b) \Longrightarrow \Theta_{ad} = A^2,$$
$$\Theta_{ae} \ni (a, d) \Longrightarrow \Theta_{ae} = A^2,$$

tehát

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e,c),(a,b) \Longrightarrow \Theta_{ac} = A^2,$$
$$\Theta_{ad} \ni (e,d),(a,b) \Longrightarrow \Theta_{ad} = A^2,$$
$$\Theta_{ae} \ni (a,d) \Longrightarrow \Theta_{ae} = A^2,$$

tehát ha $x \notin \{a,b\}$ akkor

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ac} \ni (e,c),(a,b) \Longrightarrow \Theta_{ac} = A^2,$$
$$\Theta_{ad} \ni (e,d),(a,b) \Longrightarrow \Theta_{ad} = A^2,$$
$$\Theta_{ae} \ni (a,d) \Longrightarrow \Theta_{ae} = A^2,$$

tehát ha $x \notin \{a,b\}$ akkor $\Theta_{ax} = A^2$.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Θ_{bc}

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a)$$

*	*a*	*b*	*c*	*d*	*e*
a	*e*	*e*	*a*	*b*	*c*
b	*e*	*e*	*b*	*b*	*d*
c	*c*	*d*	*b*	*b*	*e*
d	*d*	*c*	*b*	*b*	*e*
e	*a*	*b*	*d*	*c*	*c*

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$

$$\Theta_{bd}$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$

$$\Theta_{bd} \ni (c, b)$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$
$$\Theta_{bd} \ni (c, b) \Longrightarrow \Theta_{bd} = A^2,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$
$$\Theta_{bd} \ni (c, b) \Longrightarrow \Theta_{bd} = A^2,$$
$$\Theta_{be}$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$
$$\Theta_{bd} \ni (c, b) \Longrightarrow \Theta_{bd} = A^2,$$
$$\Theta_{be} \ni (e, a)$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$
$$\Theta_{bd} \ni (c, b) \Longrightarrow \Theta_{bd} = A^2,$$
$$\Theta_{be} \ni (e, a) \Longrightarrow \Theta_{be} = A^2,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e,a) \Longrightarrow \Theta_{bc} = A^2,$$
$$\Theta_{bd} \ni (c,b) \Longrightarrow \Theta_{bd} = A^2,$$
$$\Theta_{be} \ni (e,a) \Longrightarrow \Theta_{be} = A^2,$$

tehát

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e, a) \Longrightarrow \Theta_{bc} = A^2,$$
$$\Theta_{bd} \ni (c, b) \Longrightarrow \Theta_{bd} = A^2,$$
$$\Theta_{be} \ni (e, a) \Longrightarrow \Theta_{be} = A^2,$$

tehát ha $x \notin \{a, b\}$ akkor

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{bc} \ni (e,a) \Longrightarrow \Theta_{bc} = A^2,$$
$$\Theta_{bd} \ni (c,b) \Longrightarrow \Theta_{bd} = A^2,$$
$$\Theta_{be} \ni (e,a) \Longrightarrow \Theta_{be} = A^2,$$

tehát ha $x \notin \{a,b\}$ akkor $\Theta_{bx} = A^2$.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$\ominus_{ce}$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ce} \ni (c, a)$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ce} \ni (c, a) \Longrightarrow \Theta_{ce} = A^2,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ce} \ni (c, a) \Longrightarrow \Theta_{ce} = A^2,$$

$$\Theta_{de}$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ce} \ni (c, a) \Longrightarrow \Theta_{ce} = A^2,$$

$$\Theta_{de} \ni (d, a)$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ce} \ni (c, a) \Longrightarrow \Theta_{ce} = A^2,$$
$$\Theta_{de} \ni (d, a) \Longrightarrow \Theta_{de} = A^2$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

$$\Theta_{ce} \ni (c,a) \Longrightarrow \Theta_{ce} = A^2,$$
$$\Theta_{de} \ni (d,a) \Longrightarrow \Theta_{de} = A^2$$

Tehát

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$,

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor $\Theta = A^2$. Ha nem tartalmaz ilyen elemet (

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor $\Theta = A^2$. Ha nem tartalmaz ilyen elemet (azaz $\Theta \subseteq \Theta_{ab}$)

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor $\Theta = A^2$. Ha nem tartalmaz ilyen elemet (azaz $\Theta \subseteq \Theta_{ab}$) és nem az egyenlőségreláció, akkor

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor $\Theta = A^2$. Ha nem tartalmaz ilyen elemet (azaz $\Theta \subseteq \Theta_{ab}$) és nem az egyenlőségreláció, akkor — más választás nem lévén — (a, b) vagy (c, d) benne van Θ-ban, és ezért $\Theta_{cd} =$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor $\Theta = A^2$. Ha nem tartalmaz ilyen elemet (azaz $\Theta \subseteq \Theta_{ab}$) és nem az egyenlőségreláció, akkor — más választás nem lévén — (a, b) vagy (c, d) benne van Θ-ban, és ezért $\Theta_{cd} = \Theta_{ab}$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor $\Theta = A^2$. Ha nem tartalmaz ilyen elemet (azaz $\Theta \subseteq \Theta_{ab}$) és nem az egyenlőségreláció, akkor — más választás nem lévén — (a, b) vagy (c, d) benne van Θ-ban, és ezért $\Theta_{cd} = \Theta_{ab} \subseteq \Theta$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

ha $(x, y) \notin \Theta_{ab}$, ami a $\mathcal{C}_{ab} = \{\{a, b\}, \{c, d\}, \{e\}\}$ osztályozásnak felel meg, akkor $\Theta_{x,y} = A^2$. Ezért ha egy Θ kongruencia tartalmaz olyan (x, y) elempárt, amely $\notin \Theta_{ab}$, akkor $\Theta = A^2$. Ha nem tartalmaz ilyen elemet (azaz $\Theta \subseteq \Theta_{ab}$) és nem az egyenlőségreláció, akkor — más választás nem lévén — (a, b) vagy (c, d) benne van Θ-ban, és ezért $\Theta_{cd} = \Theta_{ab} \subseteq \Theta$ miatt $\Theta = \Theta_{ab}$.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az eddigiek szerint **pontosan három kongrueciareláció van**:

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az eddigiek szerint **pontosan három kongrueciareláció van**:

$$A^2,$$

*	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az eddigiek szerint **pontosan három kongrueciareláció van**:

$$A^2,$$

$$\omega_A = \{(x,x) : x \in A\},\ \text{továbbá a}$$

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az eddigiek szerint **pontosan három kongrueciareláció van**:

$$A^2,$$

$\omega_A = \{(x,x) : x \in A\}$, továbbá a

$\mathcal{C}_{ab} = \{\{a,b\},\{c,d\},\{e\}\}$ osztályozáshoz tartozó.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az A^2 szerinti faktoralgebra

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az A^2 szerinti faktoralgebra az egyelemű grupoid.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az A^2 szerinti faktoralgebra az egyelemű grupoid. Az ω_A (azaz az egyenlőségreláció) szerinti

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az A^2 szerinti faktoralgebra az egyelemű grupoid. Az ω_A (azaz az egyenlőségreláció) szerinti izomorf A-val.

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az A^2 szerinti faktoralgebra az egyelemű grupoid. Az ω_A (azaz az egyenlőségreláció) szerinti izomorf A-val. $C_{ab} = \{\{a,b\},\{c,d\},\{e\}\}$ esetén legyen $p = \{a,b\}$,

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az A^2 szerinti faktoralgebra az egyelemű grupoid. Az ω_A (azaz az egyenlőségreláció) szerinti izomorf A-val. $C_{ab} = \{\{a,b\},\{c,d\},\{e\}\}$ esetén legyen $p = \{a,b\}$, $q = \{c,d\}$ és $r = \{e\}$ —

$*$	a	b	c	d	e
a	e	e	a	b	c
b	e	e	b	b	d
c	c	d	b	b	e
d	d	c	b	b	e
e	a	b	d	c	c

Az A^2 szerinti faktoralgebra az egyelemű grupoid. Az ω_A (azaz az egyenlőségreláció) szerinti izomorf A-val. $C_{ab} = \{\{a,b\},\{c,d\},\{e\}\}$ esetén legyen $p = \{a,b\}$, $q = \{c,d\}$ és $r = \{e\}$ — ezekből áll a faktorgrupoid:

		p		q		r
	*	a	b	c	d	e
p	a	e	e	a	b	c
	b	e	e	b	b	d
q	c	c	d	b	b	e
	d	d	c	b	b	e
r	e	a	b	d	c	c

*	p	q	r
p	r	p	q
q	q	p	r
r	p	q	q

*	p	q	r
p	r	p	q
q	q	p	r
r	p	q	q

A jobb szélén van az A/Θ_{ab} faktorgrupoid.

		p		q		r
	$*$	a	b	c	d	e
p	a	e	e	a	b	c
p	b	e	e	b	b	d
q	c	c	d	b	b	e
q	d	d	c	b	b	e
r	e	a	b	d	c	c

$\longrightarrow$

$*$	p	q	r
p	r	p	q
q	q	p	r
r	p	q	q

$\longrightarrow$

$*$	p	q	r
p	r	p	q
q	q	p	r
r	p	q	q

A jobb szélén van az A/Θ_{ab} faktorgrupoid. Megjegyzés (és korábbi ismeretek illusztrálása):

		p		q		r
	$*$	a	b	c	d	e
p	a	e	e	a	b	c
	b	e	e	b	b	d
q	c	c	d	b	b	e
	d	d	c	b	b	e
r	e	a	b	d	c	c

$\longrightarrow$

$*$	p	q	r
p	r	p	q
q	q	p	r
r	p	q	q

$\longrightarrow$

$*$	p	q	r
p	r	p	q
q	q	p	r
r	p	q	q

A jobb szélén van az A/Θ_{ab} faktorgrupoid. Megjegyzés (és korábbi ismeretek illusztrálása): A „színtartó” $\varphi : A \to A/\Theta_{ab}$ leképezés a természetes homomorfizmus, amelynek magja éppen Θ_{ab}.

$$\begin{array}{cc|cc|cc|c}
 & & p & & q & & r \\
 & * & a & b & c & d & e \\ \hline
p & a & e & e & a & b & c \\
 & b & e & e & b & b & d \\ \hline
q & c & c & d & b & b & e \\
 & d & d & c & b & b & e \\ \hline
r & e & a & b & d & c & c
\end{array}
\longrightarrow
\begin{array}{c|c|c|c}
* & p & q & r \\ \hline
p & r & p & q \\ \hline
q & q & p & r \\ \hline
r & p & q & q
\end{array}
\longrightarrow
\begin{array}{c|c|c|c}
* & p & q & r \\ \hline
p & r & p & q \\ \hline
q & q & p & r \\ \hline
r & p & q & q
\end{array}$$

A jobb szélén van az A/Θ_{ab} faktorgrupoid. Megjegyzés (és korábbi ismeretek illusztrálása): A „színtartó” $\varphi : A \to A/\Theta_{ab}$ leképezés a természetes homomorfizmus, amelynek magja éppen Θ_{ab}. A feladatot megoldottuk.

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás:

Feladat Legyen G csoport és $N \lhd G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a,b) \in G^2 : aN = bN\}$.

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a,b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor

Feladat Legyen G csoport és $N \lhd G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a, b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$.

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a, b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért —

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a, b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért — a G/N faktorcsoportbeli művelet jelentését felhasználva —

Feladat Legyen G csoport és $N \lhd G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a, b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért — a G/N faktorcsoportbeli művelet jelentését felhasználva —

$$(a_1a_2)N =$$

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a, b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért — a G/N faktorcsoportbeli művelet jelentését felhasználva —

$$(a_1a_2)N = (a_1N)(a_2N) =$$

Feladat Legyen G csoport és $N \lhd G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a,b) \in G^2 : aN = bN\}$. Mármost ha $(a_1,b_1) \in \Theta$ és $(a_2,b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért — a G/N faktorcsoportbeli művelet jelentését felhasználva —

$$(a_1a_2)N = (a_1N)(a_2N) = (b_1N)(b_2N) =$$

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a,b) \in G^2 : aN = bN\}$. Mármost ha $(a_1,b_1) \in \Theta$ és $(a_2,b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért — a G/N faktorcsoportbeli művelet jelentését felhasználva —

$$(a_1a_2)N = (a_1N)(a_2N) = (b_1N)(b_2N) = (b_1b_2)N,$$

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a,b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért — a G/N faktorcsoportbeli művelet jelentését felhasználva —

$$(a_1a_2)N = (a_1N)(a_2N) = (b_1N)(b_2N) = (b_1b_2)N,$$

tehát $(a_1a_2, b_1b_2) \in \Theta$.

Feladat Legyen G csoport és $N \triangleleft G$. Mutassuk meg, hogy az N szerinti osztályozáshoz tartozó ekvivalencia kongruenciája a G csoportnak.

Megoldás: Most $\Theta = \{(a,b) \in G^2 : aN = bN\}$. Mármost ha $(a_1, b_1) \in \Theta$ és $(a_2, b_2) \in \Theta$, akkor $a_1N = b_1N$ és $a_2N = b_2N$. Ezért — a G/N faktorcsoportbeli művelet jelentését felhasználva —

$$(a_1a_2)N = (a_1N)(a_2N) = (b_1N)(b_2N) = (b_1b_2)N,$$

tehát $(a_1a_2, b_1b_2) \in \Theta$. Q.e.d.

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Megoldás: Additív írásmódban az

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Megoldás: Additív írásmódban az $A = (\mathbf{Z}_2^2; +)$ csoportról van szó. Elemeit jelöljük így:

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Megoldás: Additív írásmódban az $A = (\mathbf{Z}_2^2; +)$ csoportról van szó. Elemeit jelöljük így: $0 = (0, 0)$ (egységelem), $a = (1, 0)$, $b = (0, 1)$ és $c = (1, 1)$. Ekkor

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Megoldás: Additív írásmódban az $A = (\mathbf{Z}_2^2; +)$ csoportról van szó. Elemeit jelöljük így: $0 = (0, 0)$ (egységelem), $a = (1, 0)$, $b = (0, 1)$ és $c = (1, 1)$. Ekkor minden elem sajátmaga ellentettje (azaz inverze), azaz $a+a = b+b = c+c = 0$. Továbbá a, b, c közül

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Megoldás: Additív írásmódban az $A = (\mathbf{Z}_2^2; +)$ csoportról van szó. Elemeit jelöljük így: $0 = (0,0)$ (egységelem), $a = (1,0)$, $b = (0,1)$ és $c = (1,1)$. Ekkor minden elem sajátmaga ellentettje (azaz inverze), azaz $a+a = b+b = c+c = 0$. Továbbá a, b, c közül bármelyik kettő összege a harmadik.

Feladat: Határozzuk meg a kételemű ciklikus csoport direkt négyzetének részcsoportjait, automorfizmusait, kongruenciáit és izomorfia erejéig a faktorcsoportjait.

Megoldás: Additív írásmódban az $A = (\mathbf{Z}_2^2; +)$ csoportról van szó. Elemeit jelöljük így: $0 = (0, 0)$ (egységelem), $a = (1, 0)$, $b = (0, 1)$ és $c = (1, 1)$. Ekkor minden elem sajátmaga ellentettje (azaz inverze), azaz $a+a = b+b = c+c = 0$. Továbbá a, b, c közül bármelyik kettő összege a harmadik. Ezek szerint a megfontolás során a, b és c szerepe szimmetrikus.

A Lagrange-tétel szerint egy részcsoport elemszáma $\in$

A Lagrange-tétel szerint egy részcsoport elemszáma $\in \{1, 2, 4\}$ lehet. Mivel egy részcsoport mindig tartalmazza a 0-t, ezért csak az alábbiak jönnek szóba részcsoportként:

$$\{0\},\ \{0, a\},\ \{0, b\},\ \{0, c\},\ A.$$

Ezek valóban részcsoportok.

A Lagrange-tétel szerint egy részcsoport elemszáma $\in \{1, 2, 4\}$ lehet. Mivel egy részcsoport mindig tartalmazza a 0-t, ezért csak az alábbiak jönnek szóba részcsoportként:

$$\{0\},\ \{0, a\},\ \{0, b\},\ \{0, c\},\ A.$$

Ezek valóban részcsoportok. Ugyanezek a normálosztók is, hiszen a csoport kommutatív.

A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok —

A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok — a Lagrange-tétel szerint —

A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok — a Lagrange-tétel szerint — kételeműek, ezért —

A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok — a Lagrange-tétel szerint — kételeműek, ezért — mivel minden prímelemű csoport ciklikus — ciklikusak, A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok — a Lagrange-tétel szerint — kételeműek, ezért — mivel minden prímelemű csoport ciklikus — ciklikusak, de izomorfia erejéig csak egyetlen kételemű csoport van: $(\mathbf{Z}_2; +)$. Az A/A faktorcsoport az egyelemű (ciklikus) csoport.

A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok — a Lagrange-tétel szerint — kételeműek, ezért — mivel minden prímelemű csoport ciklikus — ciklikusak, de izomorfia erejéig csak egyetlen kételemű csoport van: $(\mathbf{Z}_2; +)$. Az A/A faktorcsoport az egyelemű (ciklikus) csoport. Tehát izomorfia

A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok — a Lagrange-tétel szerint — kételeműek, ezért — mivel minden prímelemű csoport ciklikus — ciklikusak, de izomorfia erejéig csak egyetlen kételemű csoport van: $(\mathbf{Z}_2; +)$. Az A/A faktorcsoport az egyelemű (ciklikus) csoport. Tehát izomorfia erejéig a faktorcsoportok:

A $\{0\}$ normálosztó szerinti mellékosztályok egyeleműek, és az ezen normálosztó szerinti faktorcsoport izomorf az eredeti A csoporttal. A kételemű normálosztók szerinti faktorcsoportok — a Lagrange-tétel szerint — kételeműek, ezért — mivel minden prímelemű csoport ciklikus — ciklikusak, de izomorfia erejéig csak egyetlen kételemű csoport van: $(\mathbf{Z}_2;+)$. Az A/A faktorcsoport az egyelemű (ciklikus) csoport. Tehát izomorfia erejéig a faktorcsoportok: $A=(\mathbf{Z}_2^2;+)$, $(\mathbf{Z}_2;+)$, egyelemű csoport.

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$.

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) =$

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$.

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$ (a $z = b$, illetve $z = c$) eset hasonló).

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$ (a $z = b$, illetve $z = c$) eset hasonló). Mivel tehát $(0, a) \in \Theta$

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$ (a $z = b$, illetve $z = c$) eset hasonló). Mivel tehát $(0, a) \in \Theta$ és persze a reflexivitás miatt $(b, b) \in \Theta$, ezért $(b, c) =$

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$ (a $z = b$, illetve $z = c$) eset hasonló). Mivel tehát $(0, a) \in \Theta$ és persze a reflexivitás miatt $(b, b) \in \Theta$, ezért $(b, c) = (0 + b, a + b) \in \Theta$. Minthogy feltettük, hogy $\Theta \neq A^2$, az eddigiek szerint Θ

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$ (a $z = b$, illetve $z = c$) eset hasonló). Mivel tehát $(0, a) \in \Theta$ és persze a reflexivitás miatt $(b, b) \in \Theta$, ezért $(b, c) = (0 + b, a + b) \in \Theta$. Minthogy feltettük, hogy $\Theta \neq A^2$, az eddigiek szerint Θ éppen az $\{\{0, a\}, \{b, c\}\}$ osztályozáshoz —

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$ (a $z = b$, illetve $z = c$) eset hasonló). Mivel tehát $(0, a) \in \Theta$ és persze a reflexivitás miatt $(b, b) \in \Theta$, ezért $(b, c) = (0 + b, a + b) \in \Theta$. Minthogy feltettük, hogy $\Theta \neq A^2$, az eddigiek szerint Θ éppen az $\{\{0, a\}, \{b, c\}\}$ osztályozáshoz — azaz a $\{0, a\}$ normálosztó szerinti osztályozáshoz — tartozó ekvivalencia. Láttuk, hogy ekkor kongruencia.

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x,y) \in \Theta$. Na de $(-y,-y) \in \Theta$, ezért $(x+(-y), y+(-y)) = (x-y, 0) \in \Theta$, és itt $x-y \neq 0$ mert $x-y=0$-ból $x=y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0,z) \in \Theta$. Legyen $z=a$ (a $z=b$, illetve $z=c$) eset hasonló). Mivel tehát $(0,a) \in \Theta$ és persze a reflexivitás miatt $(b,b) \in \Theta$, ezért $(b,c) = (0+b, a+b) \in \Theta$. Minthogy feltettük, hogy $\Theta \neq A^2$, az eddigiek szerint Θ éppen az $\{\{0,a\}, \{b,c\}\}$ osztályozáshoz — azaz a $\{0,a\}$ normálosztó szerinti osztályozáshoz — tartozó ekvivalencia. Láttuk, hogy ekkor kongruencia. Az abc szimmetria miatt

Az egyenlőségreláció és a teljes reláció (azaz A^2) mindig kongruencia. Legyen $\Theta \subseteq A^2$ egy ezektől különböző. Mivel nem az egyenlőségreláció, van olyan $x \neq y \in A$, hogy $(x, y) \in \Theta$. Na de $(-y, -y) \in \Theta$, ezért $(x + (-y), y + (-y)) = (x - y, 0) \in \Theta$, és itt $x - y \neq 0$ mert $x - y = 0$-ból $x = y$ adódna. Tehát van olyan $z \in A \setminus \{0\}$, hogy $(0, z) \in \Theta$. Legyen $z = a$ (a $z = b$, illetve $z = c$) eset hasonló). Mivel tehát $(0, a) \in \Theta$ és persze a reflexivitás miatt $(b, b) \in \Theta$, ezért $(b, c) = (0 + b, a + b) \in \Theta$. Minthogy feltettük, hogy $\Theta \neq A^2$, az eddigiek szerint Θ éppen az $\{\{0, a\}, \{b, c\}\}$ osztályozáshoz — azaz a $\{0, a\}$ normálosztó szerinti osztályozáshoz — tartozó ekvivalencia. Láttuk, hogy ekkor kongruencia. Az abc szimmetria miatt a keresett kongruenciák:

az egyenlőségreláció, a teljes reláció, továbbá az $\{\{0,a\},\{b,c\}\}$, $\{\{0,b\},\{a,c\}\}$, $\{\{0,c\},\{a,b\}\}$ osztályozásokhoz tartozó ekvivalenciák.

az egyenlőségreláció, a teljes reláció, továbbá az $\{\{0, a\}, \{b, c\}\}$, $\{\{0, b\}, \{a, c\}\}$, $\{\{0, c\}, \{a, b\}\}$ osztályozásokhoz tartozó ekvivalenciák.

Megfigyelhető, hogy a kongruenciák éppen normálosztókhoz tartozó osztályozásokhoz tartozó ekvivalenciák —

az egyenlőségreláció, a teljes reláció, továbbá az $\{\{0, a\}, \{b, c\}\}$, $\{\{0, b\}, \{a, c\}\}$, $\{\{0, c\}, \{a, b\}\}$ osztályozásokhoz tartozó ekvivalenciák.

Megfigyelhető, hogy a kongruenciák éppen normálosztókhoz tartozó osztályozásokhoz tartozó ekvivalenciák — ez nemcsak itt érvényes, hanem tetszőleges csoport esetében is, és nem is lenne olyan nehéz igazolni.

Legyen $\varphi : A \longrightarrow A$ autormorfizmus. Ekkor —

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez —

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció.

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva:

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva: elemet önmagához adva a nullát kapjuk, másik elemhez adva

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a,b,c\} \to \{a,b,c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva: elemet önmagához adva a nullát kapjuk, másik elemhez adva a kimaradó harmadikat —

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva: elemet önmagához adva a nullát kapjuk, másik elemhez adva a kimaradó harmadikat — ez nyilván felcserélhető a φ bijekcióval. (Hiszen a bijekció az „önmaga", „kimaradó" fogalmakat megőrzi.) Az eddigiek szerint

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva: elemet önmagához adva a nullát kapjuk, másik elemhez adva a kimaradó harmadikat — ez nyilván felcserélhető a φ bijekcióval. (Hiszen a bijekció az „önmaga”, „kimaradó” fogalmakat megőrzi.) Az eddigiek szerint az automorfizmusok

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva: elemet önmagához adva a nullát kapjuk, másik elemhez adva a kimaradó harmadikat — ez nyilván felcserélhető a φ bijekcióval. (Hiszen a bijekció az „önmaga”, „kimaradó” fogalmakat megőrzi.) Az eddigiek szerint az automorfizmusok pontosan azok az $A \to A$ bijekciók, amelyeknek a 0 fixpontja.

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva: elemet önmagához adva a nullát kapjuk, másik elemhez adva a kimaradó harmadikat — ez nyilván felcserélhető a φ bijekcióval. (Hiszen a bijekció az „önmaga", „kimaradó" fogalmakat megőrzi.) Az eddigiek szerint az automorfizmusok pontosan azok az $A \to A$ bijekciók, amelyeknek a 0 fixpontja. Tehát összesen hat autormorfizmus van.

Legyen $\varphi : A \to A$ autormorfizmus. Ekkor — mivel egységelemet egységelembe képez — $0\varphi = 0$, és $\varphi|_{\{a,b,c\}} : \{a, b, c\} \to \{a, b, c\}$ is bijekció. Ez az utóbbi bijekció tetszőleges lehet, hiszen erre a háromelemű részhalmazra a művelet így van definiálva: elemet önmagához adva a nullát kapjuk, másik elemhez adva a kimaradó harmadikat — ez nyilván felcserélhető a φ bijekcióval. (Hiszen a bijekció az „önmaga”, „kimaradó” fogalmakat megőrzi.) Az eddigiek szerint az automorfizmusok pontosan azok az $A \to A$ bijekciók, amelyeknek a 0 fixpontja. Tehát összesen hat autormorfizmus van. Q.e.d.

Feladat: A „jaj csak kört ne" játékot a következő módon játszák. A táblán (vagy papíron) előre adott n szögpont. Élek kezdetben nincsenek. A két játékos felváltva rajzol be egy új élet a gráfba. (

Feladat: A „jaj csak kört ne” játékot a következő módon játszák. A táblán (vagy papíron) előre adott n szögpont. Élek kezdetben nincsenek. A két játékos felváltva rajzol be egy új élet a gráfba. (Csak az adott szögpontok köthetők össze, többszörös élek nem megengedettek.) Minden játékosnak az a célja, hogy az él berajzolása után ne legyen kör a gráfban. Akinek ez nem sikerül (

Feladat: A „jaj csak kört ne'' játékot a következő módon játszák. A táblán (vagy papíron) előre adott n szögpont. Élek kezdetben nincsenek. A két játékos felváltva rajzol be egy új élet a gráfba. (Csak az adott szögpontok köthetők össze, többszörös élek nem megengedettek.) Minden játékosnak az a célja, hogy az él berajzolása után ne legyen kör a gráfban. Akinek ez nem sikerül (pontosabban: akinek az ellenfele a következő lépésben kört talál), vesztett.

Feladat: A „jaj csak kört ne” játékot a következő módon játszák. A táblán (vagy papíron) előre adott n szögpont. Élek kezdetben nincsenek. A két játékos felváltva rajzol be egy új élet a gráfba. (Csak az adott szögpontok köthetők össze, többszörös élek nem megengedettek.) Minden játékosnak az a célja, hogy az él berajzolása után ne legyen kör a gráfban. Akinek ez nem sikerül (pontosabban: akinek az ellenfele a következő lépésben kört talál), vesztett.

A játékteremben két ilyen tábla is van. Az egyiken 19, a másikon 20 szögpont van. Kezdő játékosként melyiket válasszuk? És mekkora tétben fogadjunk a sikerünkre?

Megoldás: E

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens:

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf.

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van.

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő).

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf.

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Ezek szerint

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Ezek szerint (bárhogy is kezdtük el az éleket rajzolni)

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Ezek szerint (bárhogy is kezdtük el az éleket rajzolni) $n-1$ alkalommal biztos lehetséges élet berajzolni, viszont az n-edik alkalommal óhatatlanul keletkezik kör.

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Ezek szerint (bárhogy is kezdtük el az éleket rajzolni) $n-1$ alkalommal biztos lehetséges élet berajzolni, viszont az n-edik alkalommal óhatatlanul keletkezik kör. Hogy ez az ellenfelet sújtsa, ahhoz n-nek párosnak lennie.

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Ezek szerint (bárhogy is kezdtük el az éleket rajzolni) $n-1$ alkalommal biztos lehetséges élet berajzolni, viszont az n-edik alkalommal óhatatlanul keletkezik kör. Hogy ez az ellenfelet sújtsa, ahhoz n-nek párosnak lennie. Tehát kezdőjátékosként a 20 szögpontú táblát választva biztos nyerünk. (Feltéve, hogy nem nézzük el.)

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Ezek szerint (bárhogy is kezdtük el az éleket rajzolni) $n-1$ alkalommal biztos lehetséges élet berajzolni, viszont az n-edik alkalommal óhatatlanul keletkezik kör. Hogy ez az ellenfelet sújtsa, ahhoz n-nek párosnak lennie. Tehát kezdőjátékosként a 20 szögpontú táblát választva biztos nyerünk. (Feltéve, hogy nem nézzük el.) A másik táblánál pedig biztos veszítünk (feltéve, hogy ellenfelünk nem nézi el.)

Megoldás: Emlékezzünk vissza arra a tételre, amely szerint egy G egy véges n-szögpontú egyszerű gráf esetén az alábbi két feltétel ekvivalens: (3) G maximális körmentes gráf. (5) G körmentes és $n-1$ éle van. (A további három ekvivalens feltétel: (1) G fa (azaz körmentes és összefüggő). (2) G minimális összefüggő gráf. (4) G összefüggő és $n-1$ éle van.

Ezek szerint (bárhogy is kezdtük el az éleket rajzolni) $n-1$ alkalommal biztos lehetséges élet berajzolni, viszont az n-edik alkalommal óhatatlanul keletkezik kör. Hogy ez az ellenfelet sújtsa, ahhoz n-nek párosnak lennie. Tehát kezdőjátékosként a 20 szögpontú táblát választva biztos nyerünk. (Feltéve, hogy nem nézzük el.) A másik táblánál pedig biztos veszítünk (feltéve, hogy ellenfelünk nem nézi el.) Q.e.d.

Feladat: Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(P(U); \setminus)$ grupoidot, ahol ahol U nemüres halmaz.

Feladat: Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $(P(U); \setminus)$ grupoidot, ahol ahol U nemüres halmaz.

Mik a részalgebrák, kongruenciák és (izomorfia erejéig) a faktoralgebrák, ha $U = \{1, 2\}$?

Megoldás: Mivel csak annyit tudunk biztosan, hogy $U, \emptyset \in P(U)$ - és esetleg más eleme nincs is, ezért legcélszerűbb először ezt a két elemet (részhalmazt vizsgálni), amikor a tulajdonságokat teszteljük.

Megoldás: Mivel csak annyit tudunk biztosan, hogy $U, \emptyset \in P(U)$ - és esetleg más eleme nincs is, ezért legcélszerűbb először ezt a két elemet (részhalmazt vizsgálni), amikor a tulajdonságokat teszteljük. Grupoid.

Megoldás: Mivel csak annyit tudunk biztosan, hogy $U, \emptyset \in P(U)$ - és esetleg más eleme nincs is, ezért legcélszerűbb először ezt a két elemet (részhalmazt vizsgálni), amikor a tulajdonságokat teszteljük. Grupoid. Nem kommutatív, hiszen

$$U \setminus \emptyset = U \neq \emptyset = \emptyset \setminus U.$$

Nem asszociatív, hiszen

$$(U \setminus U) \setminus U = \emptyset \setminus U = \emptyset \neq U = U \setminus \emptyset = U \setminus (U \setminus U).$$

Ha $E \in P(U)$ egységelem lenne, akkor

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$,

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \setminus Z$, ami ellentmondás, hiszen ezen egyenlőségből

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \setminus Z$, ami ellentmondás, hiszen ezen egyenlőségből

$$\emptyset =$$

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \setminus Z$, ami ellentmondás, hiszen ezen egyenlőségből

$$\emptyset = Z \cap (U \setminus Z) =$$

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \backslash E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \backslash Z$, ami ellentmondás, hiszen ezen egyenlőségből

$$\emptyset = Z \cap (U \setminus Z) = Z \cup (U \setminus Z) =$$

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \setminus Z$, ami ellentmondás, hiszen ezen egyenlőségből

$$\emptyset = Z \cap (U \setminus Z) = Z \cup (U \setminus Z) = U,$$

azaz ellentmondás adódna. Tehát **nincs zéruselem**.

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \setminus Z$, ami ellentmondás, hiszen ezen egyenlőségből

$$\emptyset = Z \cap (U \setminus Z) = Z \cup (U \setminus Z) = U,$$

azaz ellentmondás adódna. Tehát **nincs zéruselem**.

Mivel $\emptyset \setminus U = \emptyset \setminus \emptyset$, ezért nem kancellatív.

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \backslash E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \backslash Z$, ami ellentmondás, hiszen ezen egyenlőségből

$$\emptyset = Z \cap (U \setminus Z) = Z \cup (U \setminus Z) = U,$$

azaz ellentmondás adódna. Tehát **nincs zéruselem**.

Mivel $\emptyset \setminus U = \emptyset \setminus \emptyset$, ezért nem kancellatív.

Az eddigiek alapján **nem félcsoport, nem monoid, nem csoport, nem kancellatív**.

Ha $E \in P(U)$ egységelem lenne, akkor $E = E \setminus E = \emptyset$, de az $\emptyset$ nem egységelem, hiszen $\emptyset \setminus U = \emptyset \neq U$. Tehát **nincs egységelem**.

Ha $Z \in P(U)$ zéruselem lenne, akkor $Z = U \setminus Z$, ami ellentmondás, hiszen ezen egyenlőségből

$$\emptyset = Z \cap (U \setminus Z) = Z \cup (U \setminus Z) = U,$$

azaz ellentmondás adódna. Tehát **nincs zéruselem**.

Mivel $\emptyset \setminus U = \emptyset \setminus \emptyset$, ezért nem kancellatív.

Az eddigiek alapján **nem félcsoport, nem monoid, nem csoport, nem kancellatív**.

A továbbiakban $U = \{1, 2\}$.

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X,$

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$,
ezekből van

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] =$

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha egy S részalgebrában benne van U, továbbá $\{1\}$ és $\{2\}$ közül az egyik, akkor a másik is, hiszen $U\setminus$ egyik $=$ másik. Az eddigiek alapján már fel tudjuk sorolni a részalgebrákat:

$$S_1 = \{\emptyset\},$$

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha egy S részalgebrában benne van U, továbbá $\{1\}$ és $\{2\}$ közül az egyik, akkor a másik is, hiszen $U\setminus$ egyik $=$ másik. Az eddigiek alapján már fel tudjuk sorolni a részalgebrákat:

$$S_1 = \{\emptyset\}, \quad S_2 = \{\emptyset, \{1\}\},$$

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha egy S részalgebrában benne van U, továbbá $\{1\}$ és $\{2\}$ közül az egyik, akkor a másik is, hiszen $U\setminus$ egyik $=$ másik. Az eddigiek alapján már fel tudjuk sorolni a részalgebrákat:

$$S_1 = \{\emptyset\}, \quad S_2 = \{\emptyset, \{1\}\}, \quad S_3 = \{\emptyset, \{2\}\},$$

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha egy S részalgebrában benne van U, továbbá $\{1\}$ és $\{2\}$ közül az egyik, akkor a másik is, hiszen $U\setminus$ egyik $=$ másik. Az eddigiek alapján már fel tudjuk sorolni a részalgebrákat:

$$S_1 = \{\emptyset\}, \quad S_2 = \{\emptyset, \{1\}\}, \quad S_3 = \{\emptyset, \{2\}\}, \quad S_4 = \{\emptyset, U\},$$

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha egy S részalgebrában benne van U, továbbá $\{1\}$ és $\{2\}$ közül az egyik, akkor a másik is, hiszen $U\setminus$ egyik $=$ másik. Az eddigiek alapján már fel tudjuk sorolni a részalgebrákat:

$$S_1 = \{\emptyset\}, \quad S_2 = \{\emptyset, \{1\}\}, \quad S_3 = \{\emptyset, \{2\}\}, \quad S_4 = \{\emptyset, U\},$$
$$S_5 = \{\emptyset, \{1\}, \{2\}\},$$

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha egy S részalgebrában benne van U, továbbá $\{1\}$ és $\{2\}$ közül az egyik, akkor a másik is, hiszen $U \setminus$ egyik $=$ másik. Az eddigiek alapján már fel tudjuk sorolni a részalgebrákat:

$$S_1 = \{\emptyset\}, \quad S_2 = \{\emptyset, \{1\}\}, \quad S_3 = \{\emptyset, \{2\}\}, \quad S_4 = \{\emptyset, U\},$$
$$S_5 = \{\emptyset, \{1\}, \{2\}\}, \quad S_6 = P(A).$$

Tehát pontosan hat részalgebra van.

A ciklikus részalgebrák: $X \in P(U) \setminus \{\emptyset\}$ esetén $[X] = \{X, \emptyset\}$, ezekből van három darab. Természetesen ciklikus az $[\emptyset] = \{\emptyset\}$ részalgebra is. Ha egy S részalgebrában benne van U, továbbá $\{1\}$ és $\{2\}$ közül az egyik, akkor a másik is, hiszen $U\setminus$ egyik $=$ másik. Az eddigiek alapján már fel tudjuk sorolni a részalgebrákat:

$$S_1 = \{\emptyset\}, \quad S_2 = \{\emptyset, \{1\}\}, \quad S_3 = \{\emptyset, \{2\}\}, \quad S_4 = \{\emptyset, U\},$$
$$S_5 = \{\emptyset, \{1\}, \{2\}\}, \quad S_6 = P(A).$$

Tehát pontosan hat részalgebra van.

A kongruenciákat a korábban már látott módon határozzuk meg (jelölje ∇ a teljes relációt, ω pedig az egyenlőségrelációt):

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$\ominus_{\emptyset,\{1\}} \ni$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\})$$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}),$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}),$ $\quad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\}, \{\{2\}, U\}\},$

$\Theta_{\emptyset,\{2\}} \ni$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}),$ $\qquad$ $\mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\}, \ \{\{2\}, U\}\},$

$\Theta_{\emptyset,\{2\}} \ni (U, \{1\})$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}),$ $\mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$

$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}),$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$

$$\Theta_{\emptyset,U} \ni$$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$
$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$
$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\})$$

/	Ø	{1}	{2}	U
Ø	Ø	Ø	Ø	Ø
{1}	{1}	Ø	{1}	Ø
{2}	{2}	{2}	Ø	Ø
U	U	{2}	{1}	Ø

$$\ominus_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$

$$\ominus_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$

$$\ominus_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow$$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\emptyset,U} =$$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni$$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\})$$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow$$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$
$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$
$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} =$$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$
$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$
$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$

$$\Theta_{\{1\},U} \ni$$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$

$$\Theta_{\{1\},U} \ni (\emptyset, \{2\})$$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$

$$\Theta_{\{1\},U} \ni (\emptyset,\{2\}), \Longrightarrow$$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U, \{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U, \{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$

$$\Theta_{\{1\},U} \ni (\emptyset, \{2\}), \Longrightarrow \mathcal{C}_{\{1\},U} = C_{\emptyset,\{2\}},$$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$

$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$

$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$

$$\Theta_{\{1\},U} \ni (\emptyset,\{2\}), \Longrightarrow \mathcal{C}_{\{1\},U} = C_{\emptyset,\{2\}},$$

$$\Theta_{\{2\},U} \ni$$

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$\Theta_{\emptyset,\{1\}} \ni (U, \{2\})$, $\quad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\}$,

$\Theta_{\emptyset,\{2\}} \ni (U, \{1\})$, $\quad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\}$,

$$\Theta_{\emptyset,U} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$

$$\Theta_{\{1\},\{2\}} \ni (\emptyset, \{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$

$$\Theta_{\{1\},U} \ni (\emptyset, \{2\}), \Longrightarrow \mathcal{C}_{\{1\},U} = C_{\emptyset,\{2\}},$$

$$\Theta_{\{2\},U} \ni (\emptyset, \{1\})$$

$/$	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$
$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$
$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$
$$\Theta_{\{1\},U} \ni (\emptyset,\{2\}), \Longrightarrow \mathcal{C}_{\{1\},U} = C_{\emptyset,\{2\}},$$
$$\Theta_{\{2\},U} \ni (\emptyset,\{1\}), \Longrightarrow$$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$
$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$
$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$
$$\Theta_{\{1\},U} \ni (\emptyset,\{2\}), \Longrightarrow \mathcal{C}_{\{1\},U} = C_{\emptyset,\{2\}},$$
$$\Theta_{\{2\},U} \ni (\emptyset,\{1\}), \Longrightarrow \mathcal{C}_{\{2\},U} = C_{\emptyset,\{1\}}.$$

/	∅	{1}	{2}	U
∅	∅	∅	∅	∅
{1}	{1}	∅	{1}	∅
{2}	{2}	{2}	∅	∅
U	U	{2}	{1}	∅

$$\Theta_{\emptyset,\{1\}} \ni (U,\{2\}), \qquad \mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\Theta_{\emptyset,\{2\}} \ni (U,\{1\}), \qquad \mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\},$$
$$\Theta_{\emptyset,U} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\emptyset,U} = \nabla,$$
$$\Theta_{\{1\},\{2\}} \ni (\emptyset,\{1\}) \Longrightarrow \Theta_{\{1\},\{2\}} = \nabla,$$
$$\Theta_{\{1\},U} \ni (\emptyset,\{2\}), \Longrightarrow \mathcal{C}_{\{1\},U} = C_{\emptyset,\{2\}},$$
$$\Theta_{\{2\},U} \ni (\emptyset,\{1\}), \Longrightarrow \mathcal{C}_{\{2\},U} = C_{\emptyset,\{1\}}.$$

Az eddigiek alapján könnyen meggondolható, hogy több kongru-
encia nincs. C

Az eddigiek alapján könnyen meggondolható, hogy több kongruencia nincs. Csakugyan, a két osztállyal rendelkezőket bármelyik osztályuk két elemének egybeejtése generálja. Ha pedig két elem nem tartozik a két említett kétosztályú kongruencia valamelyik osztályába, akkor ∇-t generálja.

Az eddigiek alapján könnyen meggondolható, hogy több kongruencia nincs. Csakugyan, a két osztállyal rendelkezőket bármelyik osztályuk két elemének egybeejtése generálja. Ha pedig két elem nem tartozik a két említett kétosztályú kongruencia valamelyik osztályába, akkor ∇-t generálja.

Tehát a kongruenciák: ω, ∇, valamint az alábbi osztályozásokhoz tartozó ekvivalenciák:

$$\mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$
$$\mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\}.$$

Az eddigiek alapján könnyen meggondolható, hogy több kongruencia nincs. Csakugyan, a két osztállyal rendelkezőket bármelyik osztályuk két elemének egybeejtése generálja. Ha pedig két elem nem tartozik a két említett kétosztályú kongruencia valamelyik osztályába, akkor ∇-t generálja.

Tehát a kongruenciák: ω, ∇, valamint az alábbi osztályozásokhoz tartozó ekvivalenciák:

$$\mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\}.$$

Mármost az ω szerinti faktoralgebra izomorf a kiindulásival, a ∇ szerinti az egyelemű grupoid.

Az eddigiek alapján könnyen meggondolható, hogy több kongruencia nincs. Csakugyan, a két osztállyal rendelkezőket bármelyik osztályuk két elemének egybeejtése generálja. Ha pedig két elem nem tartozik a két említett kétosztályú kongruencia valamelyik osztályába, akkor ∇-t generálja.

Tehát a kongruenciák: ω, ∇, valamint az alábbi osztályozásokhoz tartozó ekvivalenciák:

$$\mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset, \{1\}\},\ \{\{2\}, U\}\},$$
$$\mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset, \{2\}\},\ \{\{1\}, U\}\}.$$

Mármost az ω szerinti faktoralgebra izomorf a kiindulásival, a ∇ szerinti az egyelemű grupoid. A $\mathcal{C}_{\emptyset,\{1\}}$ szerinti pedig:

Az eddigiek alapján könnyen meggondolható, hogy több kongruencia nincs. Csakugyan, a két osztállyal rendelkezőket bármelyik osztályuk két elemének egybeejtése generálja. Ha pedig két elem nem tartozik a két említett kétosztályú kongruencia valamelyik osztályába, akkor ∇-t generálja.

Tehát a kongruenciák: ω, ∇, valamint az alábbi osztályozásokhoz tartozó ekvivalenciák:

$$\mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\}.$$

Mármost az ω szerinti faktoralgebra izomorf a kiindulásival, a ∇ szerinti az egyelemű grupoid. A $\mathcal{C}_{\emptyset,\{1\}}$ szerinti pedig:

Az eddigiek alapján könnyen meggondolható, hogy több kongruencia nincs. Csakugyan, a két osztállyal rendelkezőket bármelyik osztályuk két elemének egybeejtése generálja. Ha pedig két elem nem tartozik a két említett kétosztályú kongruencia valamelyik osztályába, akkor ∇-t generálja.

Tehát a kongruenciák: ω, ∇, valamint az alábbi osztályozásokhoz tartozó ekvivalenciák:

$$\mathcal{C}_{\emptyset,\{1\}} = \{\{\emptyset,\{1\}\},\ \{\{2\},U\}\},$$
$$\mathcal{C}_{\emptyset,\{2\}} = \{\{\emptyset,\{2\}\},\ \{\{1\},U\}\}.$$

Mármost az ω szerinti faktoralgebra izomorf a kiindulásival, a ∇ szerinti az egyelemű grupoid. A $\mathcal{C}_{\emptyset,\{1\}}$ szerinti pedig:

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

/	i	h
i	i	i
h	h	i

Ez éppen

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

/	i	h
i	i	i
h	h	i

Ez éppen az $(\{\mathbf{i}, \mathbf{h}\}, \leftarrow)$ grupoid, ahol $\mathbf{i}$ és

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

/	i	h
i	i	i
h	h	i

Ez éppen az $(\{\mathbf{i}, \mathbf{h}\}, \leftarrow)$ grupoid, ahol $\mathbf{i}$ és $\mathbf{h}$ a logikai értékek és $\leftarrow$ a „fordított sorrendben vett implikáció”, azaz $x \leftarrow y := y \rightarrow x$.

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

/	i	h
i	i	i
h	h	i

Ez éppen az $(\{\mathbf{i}, \mathbf{h}\}, \leftarrow)$ grupoid, ahol $\mathbf{i}$ és $\mathbf{h}$ a logikai értékek és $\leftarrow$ a „fordított sorrendben vett implikáció”, azaz $x \leftarrow y := y \to x$.

Mivel a megfontolásban az $1 \in U$ és $2 \in U$ szerepe szimmetrikus, ugyanez(

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

/	i	h
i	i	i
h	h	i

Ez éppen az $(\{\mathbf{i},\mathbf{h}\},\leftarrow)$ grupoid, ahol $\mathbf{i}$ és $\mathbf{h}$ a logikai értékek és $\leftarrow$ a „fordított sorrendben vett implikáció", azaz $x \leftarrow y := y \rightarrow x$.

Mivel a megfontolásban az $1 \in U$ és $2 \in U$ szerepe szimmetrikus, ugyanez(zel izomorf) a másik nemtriviális faktorgrupoid is.

/	$\emptyset$	$\{1\}$	$\{2\}$	U
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$
$\{2\}$	$\{2\}$	$\{2\}$	$\emptyset$	$\emptyset$
U	U	$\{2\}$	$\{1\}$	$\emptyset$

/	i	h
i	i	i
h	h	i

Ez éppen az $(\{\mathbf{i}, \mathbf{h}\}, \leftarrow)$ grupoid, ahol $\mathbf{i}$ és $\mathbf{h}$ a logikai értékek és $\leftarrow$ a „fordított sorrendben vett implikáció", azaz $x \leftarrow y := y \rightarrow x$.

Mivel a megfontolásban az $1 \in U$ és $2 \in U$ szerepe szimmetrikus, ugyanez(zel izomorf) a másik nemtriviális faktorgrupoid is. Q.e.d.

A vizsga feltétele: 20 pont a gyakorlaton!

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás:

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) =$$

Feladat. Legyen $B = \{1,2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A;\sharp)$ grupoidot, ahol $(a,b)\,\sharp\,(c,d) := (a,d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a,b)\sharp(c,d))\sharp(e,f) = (a,d)\sharp(e,f) =$$

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) =$$

Feladat. Legyen $B = \{1,2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a,b) \sharp (c,d) := (a,d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a,b)\sharp(c,d))\sharp(e,f) = (a,d)\sharp(e,f) = (a,f),$$
$$(a,b)\sharp((c,d)\sharp(e,f)) = (a,b)\sharp(c,f) =$$

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) = (a, b)\sharp(c, f) = (a, f),$$

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $A = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) = (a, b)\sharp(c, f) = (a, f),$$

tehát **félcsoport**.

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) = (a, b)\sharp(c, f) = (a, f),$$

tehát **félcsoport**. **Nem kommutatív**, hiszen pl. $(1, 2)\sharp(1, 1) = (1, 1)$, de $(1, 1)\sharp(1, 2) = (1, 2)$.

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) = (a, b)\sharp(c, f) = (a, f),$$

tehát **félcsoport**. **Nem kommutatív**, hiszen pl. $(1, 2)\sharp(1, 1) = (1, 1)$, de $(1, 1)\sharp(1, 2) = (1, 2)$. Tegyük fel, hogy (e, f) egységelem.

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) = (a, b)\sharp(c, f) = (a, f),$$

tehát **félcsoport**. **Nem kommutatív**, hiszen pl. $(1, 2)\sharp(1, 1) = (1, 1)$, de $(1, 1)\sharp(1, 2) = (1, 2)$. Tegyük fel, hogy (e, f) egységelem. Ekkor tetszőleges (a, b)-re $(a, b) = (a, b)\sharp(e, f) =$

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) = (a, b)\sharp(c, f) = (a, f),$$

tehát **félcsoport**. **Nem kommutatív**, hiszen pl. $(1, 2)\sharp(1, 1) = (1, 1)$, de $(1, 1)\sharp(1, 2) = (1, 2)$. Tegyük fel, hogy (e, f) egységelem. Ekkor tetszőleges (a, b)-re $(a, b) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen:

Feladat. Legyen $B = \{1, 2\}$ és $A = B \times B$. Vizsgáljuk a tanult tulajdonságok (pl. kancellatív-e, monoid-e, kommutatív-e, csoport-e, stb.) szempontjából az $\mathcal{A} = (A; \sharp)$ grupoidot, ahol $(a, b) \sharp (c, d) := (a, d)$. Határozzuk meg a részalgebráit, kongruenciáit és (izomorfia erejéig) a faktoralgebráit is.

Megoldás: Valóban grupoid.

$$((a, b)\sharp(c, d))\sharp(e, f) = (a, d)\sharp(e, f) = (a, f),$$
$$(a, b)\sharp((c, d)\sharp(e, f)) = (a, b)\sharp(c, f) = (a, f),$$

tehát **félcsoport**. **Nem kommutatív**, hiszen pl. $(1, 2)\sharp(1, 1) = (1, 1)$, de $(1, 1)\sharp(1, 2) = (1, 2)$. Tegyük fel, hogy (e, f) egységelem. Ekkor tetszőleges (a, b)-re $(a, b) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített f nem lehet minden $b \in B$-vel egyenlő.

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem.

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) =$

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen:

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített e nem lehet minden a-val egyenlő. Tehát

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített e nem lehet minden a-val egyenlő. Tehát **nincs zéruselem**.

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített e nem lehet minden a-val egyenlő. Tehát **nincs zéruselem**.

Mivel pl. $(1, 2)\sharp(1, 1) = (1, 2)\sharp(2, 1)$, ezért

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített e nem lehet minden a-val egyenlő. Tehát **nincs zéruselem**.

Mivel pl. $(1, 2)\sharp(1, 1) = (1, 2)\sharp(2, 1)$, ezért **nem kancellatív**.

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített e nem lehet minden a-val egyenlő. Tehát **nincs zéruselem**.

Mivel pl. $(1, 2)\sharp(1, 1) = (1, 2)\sharp(2, 1)$, ezért **nem kancellatív**.

A továbbiakban — a jelölés egyszerűsítése miatt — állapodjunk meg abban, hogy (i, j) helyett ij-t írunk;

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített e nem lehet minden a-val egyenlő. Tehát **nincs zéruselem**.

Mivel pl. $(1, 2)\sharp(1, 1) = (1, 2)\sharp(2, 1)$, ezért **nem kancellatív**.

A továbbiakban — a jelölés egyszerűsítése miatt — állapodjunk meg abban, hogy (i, j) helyett ij-t írunk; tehát $A = \{11, 12, 21, 22\}$.

Tehát nincs egységelem, azaz a tekintett grupoid **nem monoid**, és ezért **nem csoport**.

Tegyük fel, hogy (e, f) zéruselem. Ekkor tetszőleges (a, b)-re $(e, f) = (a, b)\sharp(e, f) = (a, f)$, ami lehetetlen: egy rögzített e nem lehet minden a-val egyenlő. Tehát **nincs zéruselem**.

Mivel pl. $(1, 2)\sharp(1, 1) = (1, 2)\sharp(2, 1)$, ezért **nem kancellatív**.

A továbbiakban — a jelölés egyszerűsítése miatt — állapodjunk meg abban, hogy (i, j) helyett ij-t írunk; tehát $A = \{11, 12, 21, 22\}$.

Mivel $ij\sharp ij = ij$, ezért <u>minden egyelemű részhalmaz</u> részalgebra.

$$[11, 12] =$$

$[11,12] = \{11,12$

$$[11, 12] = \underline{\{11, 12\}},$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] =$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] =$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$

$$[11,22] = \{11,22,12$$

$$[11, 12] = \underline{\{11, 12\}}, \qquad [11, 21] = \underline{\{11, 21\}},$$

$$[11, 22] = \{11, 22, 12, 21\}$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$

$$[11,22] = \{11,22,12,21\} = \underline{A},$$

$$[12,21] =$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\}$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\} = A,$$

$$[11, 12] = \underline{\{11, 12\}}, \qquad [11, 21] = \underline{\{11, 21\}},$$
$$[11, 22] = \{11, 22, 12, 21\} = \underline{A},$$
$$[12, 21] = \{12, 21, 11, 22\} = A,$$
$$[12, 22] =$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$

$$[11,22] = \{11,22,12,21\} = \underline{A},$$

$$[12,21] = \{12,21,11,22\} = A,$$

$$[12,22] = \{12,22$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\} = A,$$
$$[12,22] = \underline{\{12,22\}},$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$

$$[11,22] = \{11,22,12,21\} = \underline{A},$$

$$[12,21] = \{12,21,11,22\} = A,$$

$$[12,22] = \underline{\{12,22\}}, \qquad [21,22] =$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\} = A,$$
$$[12,22] = \underline{\{12,22\}}, \qquad [21,22] = \underline{\{21,22\}},$$

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\} = A,$$
$$[12,22] = \underline{\{12,22\}}, \qquad [21,22] = \underline{\{21,22\}},$$

Mivel

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\} = A,$$
$$[12,22] = \underline{\{12,22\}}, \qquad [21,22] = \underline{\{21,22\}},$$

Mivel ha $X \subseteq A$-ra $|X| > 2$, akkor $\{12,21\} \subseteq X$ vagy $\{11,22\} \subseteq X$, ezért ez esetben $[X] = A$.

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\} = A,$$
$$[12,22] = \underline{\{12,22\}}, \qquad [21,22] = \underline{\{21,22\}},$$

Mivel ha $X \subseteq A$-ra $|X| > 2$, akkor $\{12,21\} \subseteq X$ vagy $\{11,22\} \subseteq X$, ezért ez esetben $[X] = A$. Tehát az aláhúzott részhalmazok, szám szerint kilenc, a részalgebrák.

$$[11,12] = \underline{\{11,12\}}, \qquad [11,21] = \underline{\{11,21\}},$$
$$[11,22] = \{11,22,12,21\} = \underline{A},$$
$$[12,21] = \{12,21,11,22\} = A,$$
$$[12,22] = \underline{\{12,22\}}, \qquad [21,22] = \underline{\{21,22\}},$$

Mivel ha $X \subseteq A$-ra $|X| > 2$, akkor $\{12,21\} \subseteq X$ vagy $\{11,22\} \subseteq X$, ezért ez esetben $[X] = A$. Tehát az aláhúzott részhalmazok, szám szerint kilenc, a részalgebrák.

Az $(ij, k\ell)$ elempárt tartalmazó (vagy más szóval az ij és $k\ell$ elemeket **egybeejtő**) legszűkebb kongruenciát $\Theta_{ij,k\ell}$, a neki megfelelő osztályozást $\mathcal{C}_{ij,k\ell}$ fogja jelölni. Ezek meghatározásával kezdjük. (

$$[11,12]=\underline{\{11,12\}}, \qquad [11,21]=\underline{\{11,21\}},$$
$$[11,22]=\{11,22,12,21\}=\underline{A},$$
$$[12,21]=\{12,21,11,22\}=A,$$
$$[12,22]=\underline{\{12,22\}}, \qquad [21,22]=\underline{\{21,22\}},$$

Mivel ha $X \subseteq A$-ra $|X|>2$, akkor $\{12,21\}\subseteq X$ vagy $\{11,22\}\subseteq X$, ezért ez esetben $[X]=A$. Tehát az aláhúzott részhalmazok, szám szerint kilenc, a részalgebrák.

Az $(ij,k\ell)$ elempárt tartalmazó (vagy más szóval az ij és $k\ell$ elemeket **egybeejtő**) legszűkebb kongruenciát $\Theta_{ij,k\ell}$, a neki megfelelő osztályozást $\mathcal{C}_{ij,k\ell}$ fogja jelölni. Ezek meghatározásával kezdjük. (Az $=^{\text{uú}}$ jelentése: ugyanúgy kapjuk.)

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21, 22).$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$\Theta_{11,12} \ni (21, 22)$. $\quad \mathcal{C}_{11,12} =$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$\Theta_{11,12} \ni (21, 22)$. $\quad \mathcal{C}_{11,12} = \{\{11, 12\},\ \{21, 22\}\}$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21,22). \quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\mathsf{u\acute{u}}} \mathcal{C}_{21,22},$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$\Theta_{11,12} \ni (21,22)$. $\quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22}$,

$\Theta_{11,21} \ni (12,22)$.

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$\Theta_{11,12} \ni (21, 22)$. $\quad \mathcal{C}_{11,12} = \{\{11, 12\},\ \{21, 22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$

$\Theta_{11,21} \ni (12, 22)$. $\quad \mathcal{C}_{11,21} =$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21,22). \quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12,22). \quad \mathcal{C}_{11,21} = \{\{11,21\},\ \{12,22\}\}$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21, 22). \quad \mathcal{C}_{11,12} = \{\{11, 12\},\ \{21, 22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12, 22). \quad \mathcal{C}_{11,21} = \{\{11, 21\},\ \{12, 22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$\Theta_{11,12} \ni (21,22)$. $\quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22}$,

$\Theta_{11,21} \ni (12,22)$. $\quad \mathcal{C}_{11,21} = \{\{11,21\},\ \{12,22\}\} =^{\text{uú}} \mathcal{C}_{12,22}$,

$\Theta_{11,22} \ni (11,12)$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21,22). \quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12,22). \quad \mathcal{C}_{11,21} = \{\{11,21\},\ \{12,22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

$$\Theta_{11,22} \ni (11,12),(11,21)$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21,22). \quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12,22). \quad \mathcal{C}_{11,21} = \{\{11,21\},\ \{12,22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

$$\Theta_{11,22} \ni (11,12),(11,21) \Longrightarrow \Theta_{11,22} =$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21,22). \quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12,22). \quad \mathcal{C}_{11,21} = \{\{11,21\},\ \{12,22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

$$\Theta_{11,22} \ni (11,12),(11,21) \Longrightarrow \Theta_{11,22} = A^2,$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21,22). \quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12,22). \quad \mathcal{C}_{11,21} = \{\{11,21\},\ \{12,22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

$$\Theta_{11,22} \ni (11,12),(11,21) \Longrightarrow \Theta_{11,22} = A^2,$$

$$\Theta_{12,21} \ni (11,12)$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21, 22). \quad \mathcal{C}_{11,12} = \{\{11, 12\},\ \{21, 22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12, 22). \quad \mathcal{C}_{11,21} = \{\{11, 21\},\ \{12, 22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

$$\Theta_{11,22} \ni (11, 12), (11, 21) \Longrightarrow \Theta_{11,22} = A^2,$$

$$\Theta_{12,21} \ni (11, 12), (11, 21)$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21, 22). \quad \mathcal{C}_{11,12} = \{\{11, 12\},\ \{21, 22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12, 22). \quad \mathcal{C}_{11,21} = \{\{11, 21\},\ \{12, 22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

$$\Theta_{11,22} \ni (11, 12), (11, 21) \Longrightarrow \Theta_{11,22} = A^2,$$

$$\Theta_{12,21} \ni (11, 12), (11, 21) \Longrightarrow \Theta_{12,21} =$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21, 22). \quad \mathcal{C}_{11,12} = \{\{11, 12\},\ \{21, 22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$
$$\Theta_{11,21} \ni (12, 22). \quad \mathcal{C}_{11,21} = \{\{11, 21\},\ \{12, 22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$
$$\Theta_{11,22} \ni (11, 12), (11, 21) \Longrightarrow \Theta_{11,22} = A^2,$$
$$\Theta_{12,21} \ni (11, 12), (11, 21) \Longrightarrow \Theta_{12,21} = A^2.$$

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

$$\Theta_{11,12} \ni (21,22). \quad \mathcal{C}_{11,12} = \{\{11,12\},\ \{21,22\}\} =^{\text{uú}} \mathcal{C}_{21,22},$$

$$\Theta_{11,21} \ni (12,22). \quad \mathcal{C}_{11,21} = \{\{11,21\},\ \{12,22\}\} =^{\text{uú}} \mathcal{C}_{12,22},$$

$$\Theta_{11,22} \ni (11,12),(11,21) \Longrightarrow \Theta_{11,22} = A^2,$$

$$\Theta_{12,21} \ni (11,12),(11,21) \Longrightarrow \Theta_{12,21} = A^2.$$

Az eddigiekből könnyen adódik, hogy a kongruenciák: az egyenlőségreláció, a teljes reláció, továbbá az

$$\{\{11, 12\}, \{21, 22\}\}$$

osztályozáshoz tartozó, valamint az

$$\{\{11, 21\}, \{12, 22\}\}$$

osztályozáshoz tartozó. Az első kettő esetén a faktoralgebra triviális. Az

$$\{\{11, 12\}, \{21, 22\}\}$$

szerinti faktoralgebra:

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

#	a	b
a	a	a
b	b	b

(

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

#	a	b
a	a	a
b	b	b

(A faktoralgebrában a szorzást az $xy = x$ képlet definiálja, az eredmény mindig az első tényező.)

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

#	a	b
a	a	a
b	b	b

(A faktoralgebrában a szorzást az $xy = x$ képlet definiálja, az eredmény mindig az első tényező.)

Az

$$\{\{11, 21\},\ \{12, 22\}\}$$

szerinti faktoralgebra az alábbi:

#	11	12	21	22
11	11	12	11	12
12	11	12	11	12
21	21	22	21	22
22	21	22	21	22

#	a	b
a	a	b
b	a	b

(Itt az ábra kevésbé szemléletes, mint az előbb, csupán a színek jelzik a kongruenciát.) A faktoralgebrában a szorzást az $xy = y$ képlet definiálja, az eredmény mindig a második tényező.

A vizsga feltétele: 20 pont a gyakorlaton!