ALGEBRA ÉS SZÁMELMÉLET 3

jegyzet az előadáshoz[†]

2022 őszi félév, OT

Waldhauser Tamás

1. Permutációk

Permutációk szorzása, ciklusfelbontás

1.1. Definíció. ***Permutációnak*** nevezzük egy nemüres (véges) halmaz önmagára való bijektív leképezését. Az A halmaz permutációinak halmazát S_A jelöli.

1.2. Definíció. Mivel a permutációk leképezések, értelmezhető rajtuk a leképezésszorzás művelete. A $\pi, \rho \in S_A$ permutációk ***szorzata*** az alábbi leképezés:

$$\pi \cdot \rho \colon A \to A,\ a \mapsto (a\pi)\rho.$$

Ez a leképezés szintén permutációja az A halmaznak (ugye?), tehát $\pi \cdot \rho \in S_A$.

1.3. Példa. Tekintsük az $A = \{1,2,3,4,5\}$ halmaz következő két permutációját:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}.$$

Ekkor

$$\pi \cdot \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}, \qquad \rho \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}.$$

1.4. Állítás. Egy A halmaz tetszőleges $\pi, \rho, \sigma \in S_A$ permutációi esetén

(1) $(\pi \cdot \rho) \cdot \sigma = \pi \cdot (\rho \cdot \sigma)$;
(2) $\pi \cdot \mathrm{id} = \mathrm{id} \cdot \pi = \pi$;
(3) $\pi \cdot \pi^{-1} = \pi^{-1} \cdot \pi = \mathrm{id}$;
(4) $(\pi \cdot \rho)^{-1} = \rho^{-1} \cdot \pi^{-1}$.

Bizonyítás. Csak a negyedik állítást bizonyítjuk, de közben felhasználjuk a korábbiakat (melyik lépésben melyiket?):

$$(\pi \cdot \rho) \cdot (\rho^{-1} \cdot \pi^{-1}) = \pi \cdot (\rho \cdot \rho^{-1}) \cdot \pi^{-1} = \pi \cdot \mathrm{id} \cdot \pi^{-1} = \pi \cdot \pi^{-1} = \mathrm{id};$$
$$(\rho^{-1} \cdot \pi^{-1}) \cdot (\pi \cdot \rho) = \rho^{-1} \cdot (\pi^{-1} \cdot \pi) \cdot \rho = \rho^{-1} \cdot \mathrm{id} \cdot \rho = \rho^{-1} \cdot \rho = \mathrm{id}\,. \qquad \square$$

1.5. Példa. Az 1.3. Példában szereplő permutációkra

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}, \qquad \rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = \rho;$$

$$(\pi \cdot \rho)^{-1} = \rho^{-1} \cdot \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}, \qquad (\rho \cdot \pi)^{-1} = \pi^{-1} \cdot \rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}.$$

1.6. Következmény. Tetszőleges A halmaz összes permutációi csoportot alkotnak a leképezésszorzás műveletével. Az $A = \{1,2,\dots,n\}$ esetben ezt a csoportot ***n-edfokú szimmetrikus csoportnak*** nevezzük, és S_n-nel jelöljük.

1.7. Definíció. Legyen $\pi \in S_n$ és $a \in \{1,2,\dots,n\}$. Ha $a\pi = a$, akkor azt mondjuk, hogy a ***fixpontja*** π-nek. Ha $a\pi \neq a$, akkor azt mondjuk, hogy a ***mozgatott eleme*** π-nek.

1.8. Példa. Az 1.3. Példában szereplő permutációkra $M_\pi = \{1,2,3,4,5\}$ és $M_\rho = \{1,2,4,5\}$.

1.9. Definíció. Két permutáció ***idegen***, ha mozgatott elemeik halmaza diszjunkt.

[†]A természetes számok halmazát $\mathbb{N}$, a nemnegatív egész számok halmazát $\mathbb{N}_0$ jelöli, azaz $\mathbb{N} = \{1,2,3,\dots\}$ és $\mathbb{N}_0 = \{0,1,2,\dots\}$.

1.10. Tétel. Ha $\pi, \rho \in S_n$ idegen permutációk, akkor fölcserélhetőek, azaz $\pi \cdot \rho = \rho \cdot \pi$.

Bizonyítás. Legyen M_π a π permutáció mozgatott elemeinek halmaza. Előkészületként belátjuk, hogy minden $a \in \{1, 2, \dots, n\}$ esetén

$$a \in M_\pi \implies a\pi \in M_\pi. \tag{1.1}$$

Valóban, ha az állítással ellentétben $a \in M_\pi$ és $b := a\pi \notin M_\pi$, akkor $a \neq b$ (miért?) és $a\pi = b = b\pi$ (miért?), ez pedig ellentmond π injektivitásának (ugye?).

Ezek után nekikezdhetünk a tétel bizonyításának: tfh. π és ρ idegen, azaz $M_\pi \cap M_\rho = \emptyset$. Azt kell belátnunk, hogy minden $a \in \{1, 2, \dots, n\}$ esetén $a(\pi \cdot \rho) = a(\rho \cdot \pi)$. Négy esetet különböztetünk meg:

1) $a \notin M_\pi$ és $a \notin M_\rho$: Ekkor $a\pi = a$ és $a\rho = a$, tehát a bal oldalon $a(\pi \cdot \rho) = (a\pi)\rho = a\rho = a$, a jobb oldalon pedig $a(\rho \cdot \pi) = (a\rho)\pi = a\pi = a$ áll (ugye?).
2) $a \in M_\pi$ és $a \notin M_\rho$: Ekkor (1.1) szerint $a\pi \in M_\pi$, következésképp $a\pi \notin M_\rho$ (miért?). Tehát ρ-nak fixpontja a és $a\pi$ is (ugye?). Ennek felhasználásával a bal oldal $a(\pi \cdot \rho) = (a\pi)\rho = a\pi$, a jobb oldal pedig $a(\rho \cdot \pi) = (a\rho)\pi = a\pi$.
3) $a \notin M_\pi$ és $a \in M_\rho$: Ez hasonló, mint az előző eset, csak π és ρ szerepet cserél.
4) $a \in M_\pi$ és $a \in M_\rho$: Ez lehetetlen (miért?).

Minden esetben (ami egyáltalán felléphet) ugyanazt kaptuk $a(\pi \cdot \rho)$ és $a(\rho \cdot \pi)$ kiszámításakor, ezzel tehát igazoltuk, hogy $\pi \cdot \rho = \rho \cdot \pi$. □

1.11. Definíció. Permutációk pozitív egész kitevős hatványát természetes módon értelmezhetjük: $\pi \in S_n$ és $k \in \mathbb{N}$ esetén legyen $\pi^k := \pi \cdot \ldots \cdot \pi$ (k darab π szorzata). A nulladik hatvány az identikus permutáció: $\pi^0 := \mathrm{id}$, a negatív kitevős hatványt pedig az inverz segítségével definiáljuk: $\pi^{-k} := (\pi^k)^{-1}$.

1.12. Állítás. A hatványozás szokásos azonosságainak *egy része* érvényben marad permutációkra is. Tetszőleges $\pi, \rho \in S_n$ permutációk és $k, \ell \in \mathbb{Z}$ kitevők esetén

(1) $\pi^k \cdot \pi^\ell = \pi^{k+\ell}$;
(2) $(\pi^k)^\ell = \pi^{k\ell}$;
(3) $(\pi \cdot \rho)^k = \pi^k \cdot \rho^k$, *ha π és ρ felcserélhetőek, azaz $\pi \cdot \rho = \rho \cdot \pi$.*

1.13. Példa. Az 1.3. Példában szereplő permutációkra

$$\pi^2 \cdot \rho^2 = \pi^2 \cdot \mathrm{id} = \pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}, \qquad (\pi \cdot \rho)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}.$$

A $\sigma := \pi \cdot \rho$ permutáció néhány hatványa:

$$\sigma^4 = \mathrm{id}, \qquad \sigma^{2020} = \sigma^{4 \cdot 505} = (\sigma^4)^{505} = \mathrm{id}^{505} = \mathrm{id}, \qquad \sigma^{2022} = \sigma^{4 \cdot 505 + 2} = (\sigma^4)^{505} \cdot \sigma^2 = \mathrm{id}^{505} \cdot \sigma^2 = \sigma^2.$$

1.14. Definíció. Legyenek $a_1, \dots, a_k \in \{1, 2, \dots, n\}$ különböző elemek ($k \geq 2$), és legyen $\pi \in S_n$ az alábbi permutáció:

$$a_1\pi = a_2,\ a_2\pi = a_3, \dots,\ a_{k-1}\pi = a_k,\ a_k\pi = a_1 \qquad \text{és} \qquad b\pi = b \text{ ha } b \notin \{a_1, \dots, a_k\}.$$

Ezt a π permutációt így jelöljük: $\pi = (a_1\, a_2\, \cdots\, a_{k-1}\, a_k)$ és ***ciklikus permutációnak*** vagy röviden ***ciklusnak*** nevezzük.

1.15. Tétel. Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelmű.

Bizonyítás. Csak az egzisztenciát igazoljuk, azt is csak vázlatosan. Legyen $A = \{1, 2, \dots, n\}$ és $\pi \in S_A = S_n$. Induljunk ki egy tetszőleges $a_1 \in A$ elemből, és alkalmazzuk rá a π permutációt többször egymás után. Így egy $a_1, a_2, a_3, \dots$ sorozatot kapunk, ahol $a_{i+1} = a_i\pi$ minden i-re. Mivel A véges, előbb-utóbb lesz ismétlődés ebben a sorozatban: $\exists i < j \colon a_i = a_j$. Tegyük fel, hogy ez a legelső ismétlődés; ekkor az $a_1, a_2, \dots, a_{j-1}$ elemek még páronként különbözőek. Azt állítjuk, hogy $i = 1$, vagyis a legelső elem, ami másodszorra is fellép a sorozatban, az csak a_1 lehet. Ha nem így lenne, azaz $i > 1$ lenne, akkor még az a_{i-1} elem is szerepelne a sorozatban, és felírhatnánk, hogy $a_{i-1}\pi = a_i = a_j = a_{j-1}\pi$, ami ellentmond π injektivitásának, hiszen $a_{i-1} \neq a_{j-1}$ (miért?). Tehát csak $i = 1$ lehet, és ezzel kialakult egy $(a_1\, a_2\, \cdots\, a_{j-1})$ ciklus (ugye?).

Ha $\{a_1, \dots, a_{j-1}\} \subsetneq A$, akkor vegyünk egy tetszőleges $b_1 \in A \setminus \{a_1, \dots, a_{j-1}\}$ elemet és arra is alkalmazzuk ismételten a π permutációt. Így egy $b_1, b_2, b_3, \dots$ sorozatot kapunk, ahol $b_{k+1} = b_k\pi$ minden k-ra. A fenti gondolatmenethez hasonlóan belátható, hogy ebben a sorozatban is b_1 lesz az első ismétlődő elem, pl. $b_1 = b_\ell$, és így kialakul egy $(b_1\, b_2\, \cdots\, b_{\ell-1})$ ciklus. Azt állítjuk, hogy ez a ciklus idegen az $(a_1\, a_2\, \cdots\, a_{j-1})$ ciklustól. Ellenkező esetben legyen b_k a $b_1, b_2, \dots$ sorozat első olyan tagja, ami szerepel az $(a_1\, a_2\, \cdots\, a_{j-1})$ ciklusban is; legyen mondjuk $b_k = a_i$. A b_1 elem megválasztása miatt szükségképpen $k > 1$ (ugye?), és megint ellentmondásba kerülünk π injektivitásával: $b_{k-1}\pi = b_k = a_i = a_{i-1}\pi$ (mi a helyzet akkor, ha $i = 1$?).

Ezt az eljárást folytatva újabb, a korábbiaktól idegen ciklusokat tudunk konstruálni (megengedve az 1 hosszúságú „ciklusokat", azaz fixpontokat is), amíg el nem fogynak A elemei. Mivel A véges, ez előbb-utóbb be fog következni, és ekkor megkapjuk π felbontását páronként idegen ciklusok szorzatára. (Tulajdonképpen azt láttuk be, hogy π gráfjának minden összefüggő komponense irányított kör. De a ciklusok, amelyek szorzatára π felbomlik, nem pont ezek a körök. Hanem mik?) □

1.16. Példa. Az 1.3. Példában szereplő permutációk ciklusfelbontása:

$$\pi = (13)(245) = \begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix},$$

$$\rho = (12)(3)(45) = (12)(45) = \begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix} = \begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix},$$

$$\pi\cdot\rho = (1325)(4) = (1325) = \begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix},$$

$$\rho\cdot\pi = (1423)(5) = (1423) = \begin{pmatrix}1&2&3&4&5\\4&3&1&2&5\end{pmatrix}.$$

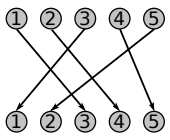
Páros és páratlan permutációk

1.17. Definíció. Legyen $\pi \in S_n$ és $1 \le a < b \le n$. Ha $a\pi > b\pi$, akkor azt mondjuk, hogy $a\pi$ és $b\pi$ ***inverziót*** alkot (vagy inverzióban áll) π-ben. A π-beli inverziók számát $\mathrm{inv}(\pi)$ jelöli.

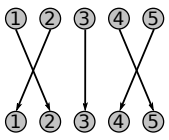
1.18. Példa. Az 1.3. Példában szereplő permutációkban az alábbi párok alkotnak inverziót:

π-beli inverziók:	$(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(2,5)$	$\Longrightarrow \mathrm{inv}(\pi) = 5;$
ρ-beli inverziók:	$(1,2)$, $(4,5)$	$\Longrightarrow \mathrm{inv}(\rho) = 2;$
$\pi\cdot\rho$-beli inverziók:	$(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(2,3)$, $(2,5)$, $(4,5)$	$\Longrightarrow \mathrm{inv}(\pi\cdot\rho) = 7;$
$\rho\cdot\pi$-beli inverziók:	$(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$, $(3,4)$	$\Longrightarrow \mathrm{inv}(\rho\cdot\pi) = 5.$

1.19. Megjegyzés. A π permutáció alábbi módon lerajzolt nyíldiagramjában az $a \longrightarrow a\pi$ és $b \longrightarrow b\pi$ nyilak akkor és csak akkor metszik egymást, ha $a\pi$ és $b\pi$ inverzióban áll (lásd az ábrát).



π



ρ

Tehát a metszéspontok száma éppen $\mathrm{inv}(\pi)$, feltéve, hogy soha nem metszi egymást három nyíl ugyanabban a pontban (ha igen, akkor ezt többszörös metszéspontnak kell számítani, aszerint, hogy hány nyílpár metszi egymást az adott pontban, vagy pedig igazítani kell egy kicsit a nyilakon, hogy megszűnjenek az ilyen többszörös metszéspontok).

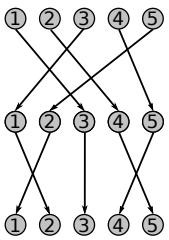
1.20. Definíció. Azt mondjuk, hogy a π permutáció ***páros permutáció***, ha $\mathrm{inv}(\pi)$ páros szám, és π ***páratlan permutáció***, ha $\mathrm{inv}(\pi)$ páratlan szám. A π permutáció ***előjele*** $\mathrm{sgn}(\pi) = (-1)^{\mathrm{inv}(\pi)}$. Tehát páros permutáció előjele $+1$, páratlan permutáció előjele -1.

1.21. Példa. Az 1.3. Példában szereplő permutációk paritása és előjele:

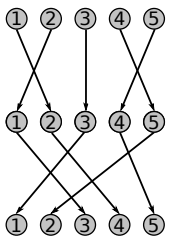
π páratlan, $\mathrm{sgn}(\pi) = -1$; ρ páros, $\mathrm{sgn}(\rho) = +1$; $\pi\cdot\rho$ páratlan, $\mathrm{sgn}(\pi\cdot\rho) = -1$; $\rho\cdot\pi$ páratlan, $\mathrm{sgn}(\rho\cdot\pi) = -1$.

1.22. Tétel. Tetszőleges $\pi, \rho \in S_n$ permutációk esetén $\mathrm{sgn}(\pi\cdot\rho) = \mathrm{sgn}(\pi)\cdot\mathrm{sgn}(\rho)$.

Bizonyítás. A $\pi\cdot\rho$ permutáció nyíldiagramját úgy kapjuk, hogy π diagramja alá helyezzük ρ diagramját, és „összefűzzük" a nyilakat (lásd az ábrát).



$\pi\cdot\rho$



$\rho\cdot\pi$

Tfh. nincsenek többszörös metszéspontok, azaz minden metszéspontban csak két nyíl metszi egymást (ha nem ez a helyzet, akkor kicsit igazítani kell a nyilakon). Az 1.19. Megjegyzés szerint a metszéspontok száma $\mathrm{inv}(\pi) + \mathrm{inv}(\rho)$. Másrészt, ha

$a\pi$ és $b\pi$ inverzióban van a $\pi\cdot\rho$ permutációban, akkor az $a \longrightarrow a\pi \longrightarrow (a\pi)\rho$ és $b \longrightarrow b\pi \longrightarrow (b\pi)\rho$ nyilak páratlan sokszor (egyszer) metszik egymást, ha pedig $a\pi$ és $b\pi$ nem alkot inverziót $\pi\cdot\rho$-ban, akkor ez a két nyíl páros sokszor (nullaszor vagy kétszer) metszi egymást (miért?). Tehát a metszéspontokat nyílpáronként megszámolva azt kapjuk, hogy a metszéspontok száma $\mathrm{inv}(\pi\cdot\rho)$-tól páros számban tér el (ugye?). Összevetve ezt a korábbi megfigyelésünkkel, az következik, hogy az $\mathrm{inv}(\pi)+\mathrm{inv}(\rho)$ és $\mathrm{inv}(\pi\cdot\rho)$ számok azonos paritásúak, és így

$$\mathrm{sgn}(\pi\cdot\rho) = (-1)^{\mathrm{inv}(\pi\cdot\rho)} = (-1)^{\mathrm{inv}(\pi)+\mathrm{inv}(\rho)} = (-1)^{\mathrm{inv}(\pi)}\cdot(-1)^{\mathrm{inv}(\rho)} = \mathrm{sgn}(\pi)\cdot\mathrm{sgn}(\rho). \qquad \square$$

1.23. Következmény. Az S_n-beli páros permutációk csoportot alkotnak. Ezt a csoportot ***n-edfokú alternáló csoportnak*** nevezzük, és A_n-nel jelöljük.

Bizonyítás. Az 1.22. Tételből azonnal következik, hogy páros permutációk szorzata is páros (miért?), az pedig világos, hogy az identikus permutáció páros, és páros permutáció inverze is páros (ugye?) $\square$

1.24. Definíció. A 2 hosszúságú ciklusokat, vagyis az $(i\,j)$ alakú permutációkat ***transzpozícióknak*** nevezzük.

1.25. Tétel. Az S_n csoportot *generálják* a transzpozíciók, azaz minden S_n-beli permutáció előáll transzpozíciók szorzataként.

Bizonyítás. Mivel minden permutáció felírható ciklusok szorzataként (1.15. Tétel), elég megmutatni, hogy minden ciklus előállítható transzpozíciók szorzataként. Az $(a_1\,a_2\,\cdots\,a_{k-1}\,a_k)$ ciklust például így írhatjuk fel (de sok más lehetőség is van): $(a_1\,a_2\,\cdots\,a_{k-1}\,a_k) = (a_1a_2)(a_1a_3)\cdots(a_1a_k)$ (ugye?). $\square$

1.26. Példa. Az 1.3. Példában szereplő permutációkat (például) így bonthatjuk fel transzpozíciók szorzatára:

$$\pi = (13)(24)(25);\quad \rho = (12)(45);\quad \pi\cdot\rho = (13)(12)(15);\quad \rho\cdot\pi = (14)(12)(13).$$

A $\pi\cdot\rho$ permutációra kaphatunk egy másik (hosszabb) felbontást úgy, hogy π és ρ fenti felbontását egymás mellé illesztjük: $\pi\cdot\rho = (13)(24)(25)(12)(45)$. Hasonlóan $\rho\cdot\pi = (12)(45)(13)(24)(25)$ (és persze van még sok más felbontása ezeknek a permutációknak).

1.27. Következmény. Ciklus paritása mindig ellentétes a hosszának paritásával: a páros hosszúságú ciklusok páratlan permutációk, a páratlan hosszúságú ciklusok páros permutációk.

1.28. Tétel. Bárhogyan is bontunk fel egy $\pi\in S_n$ permutációt transzpozíciók szorzatára, a felbontásban szereplő tényezők számának paritása megegyezik π paritásával. Tehát egy páros permutációt csak páros sok transzpozícióra lehet felbontani, egy páratlan permutációt pedig csak páratlan sokra.

Bizonyítás. Tekintsük egy $\pi\in S_n$ permutáció egy felbontását transzpozíciók szorzatára:

$$\pi = \tau_1\cdot\tau_2\cdot\ldots\cdot\tau_k.$$

ahol mindegyik τ_i transzpozíció. Minden transzpozíció páratlan permutáció (ugye?), ezért $\mathrm{sgn}(\tau_i) = -1$ minden i-re. Az 1.22. Tételt alkalmazva azt kapjuk, hogy

$$\mathrm{sgn}(\pi) = \mathrm{sgn}(\tau_1\cdot\tau_2\cdot\ldots\cdot\tau_k) = \mathrm{sgn}(\tau_1)\cdot\mathrm{sgn}(\tau_2)\cdot\ldots\cdot\mathrm{sgn}(\tau_k) = (-1)\cdot(-1)\cdot\ldots\cdot(-1) = (-1)^k.$$

Ebből már következik, hogy a k egész szám paritása ugyanaz, mint a π permutációé (miért?). $\square$

1.29. Tétel. Ha $n\geq 2$, akkor az S_n-beli permutációk fele páros és fele páratlan.

Bizonyítás. A tétel bizonyításához elegendő megadni egy bijekciót A_n és $S_n\setminus A_n$ között (ugye?). Legyen $\tau\in S_n\setminus A_n$ egy tetszőleges rögzített páratlan permutáció (pl. $\tau=(12)$), és definiáljunk egy β leképezést a következőképpen:

$$\beta\colon A_n\to S_n\setminus A_n,\ \pi\mapsto\pi\cdot\tau.$$

Három dolgot kell ellenőriznünk:

(i) β valóban az $S_n\setminus A_n$ halmazba képez, azaz ha $\pi\in A_n$, akkor $\pi\cdot\tau\in S_n\setminus A_n$. Ez világos (ugye?).

(ii) β szürjektív, azaz minden $\rho\in S_n\setminus A_n$ permutációhoz létezik olyan $\pi\in A_n$, amelyre $\pi\cdot\tau=\rho$. A $\pi=\rho\cdot\tau^{-1}$ permutáció megfelelő lesz (miért?), és ez valóban páros permutáció, mert ρ páratlan (ugye?).

(iii) β injektív, azaz minden $\pi_1,\pi_2\in S_n$ esetén $\pi_1\cdot\tau=\pi_2\cdot\tau \implies \pi_1=\pi_2$. Ezt könnyű igazolni, csak be kell szorozni jobbról a $\pi_1\cdot\tau=\pi_2\cdot\tau$ egyenlőség mindkét oldalát τ^{-1}-zel (ugye?).

$\square$

1.30. Következmény. Ha $n\geq 2$, akkor $|A_n| = |S_n\setminus A_n| = \frac{n!}{2}$.

2. Relációk

2.1. Definíció. Adott A halmazon értelmezett ***reláción*** A-beli elemekből alkotott elempárok halmazát értjük, azaz egy tetszőleges $\rho \subseteq A \times A$ halmazt.

Jelölés. Az egyszerűség kedvéért $(a,b) \in \rho$ helyett gyakran azt írjuk, hogy $a\rho b$.

2.2. Példa. Néhány példa relációkra:

- a „barátja” reláció az emberek halmazán,
- a „kisebb vagy egyenlő” reláció a valós számok halmazán (jelölés: $a \leq b$),
- az „egyenlő” reláció a komplex számok halmazán (jelölés: $a = b$),
- az „osztója” reláció a nemnegatív egész számok halmazán (jelölés: $a \mid b$),
- a „részhalmaza” reláció egy halmaz részhalmazainak halmazán (jelölés: $a \subseteq b$),
- a „párhuzamos” reláció a sík egyeneseinek halmazán (jelölés: $a \parallel b$),
- az „egybevágó” reláció a háromszögek (vagy bármilyen síkidomok) halmazán (jelölés: $a \cong b$).

Ekvivalenciák és osztályozások

2.3. Definíció. ***Ekvivalenciarelációnak*** nevezzük a $\rho \subseteq A \times A$ relációt, ha rendelkezik az alábbi három tulajdonsággal:

(1) $\forall a \in A : a\rho a$ (reflexivitás);
(2) $\forall a,b \in A : a\rho b \implies b\rho a$ (szimmetria);
(3) $\forall a,b,c \in A : (a\rho b \text{ és } b\rho c) \implies a\rho c$ (tranzitivitás).

2.4. Példa. A 2.2. Példában szereplő relációk közül az egyenlőség, a párhuzamosság és az egybevágóság ekvivalenciareláció.

2.5. Definíció. Az A halmazon értelmezett legszűkebb ekvivalenciareláció az $\omega_A := \{(a,a) : a \in A\}$ ***egyenlőség reláció***, a legbővebb ekvivalenciareláció pedig az $A \times A$ ***teljes reláció***.

2.6. Definíció. Legyen $f\colon A \to B$ egy tetszőleges leképezés, és értelmezzük az A halmazon a $\ker f$ relációt úgy, hogy két elem akkor van relációban egymással, ha f melletti képeik megegyeznek:

$$\ker f := \big\{(a_1,a_2)\colon a_1 f = a_2 f\big\} \subseteq A \times A.$$

Ezt a relációt az f leképezés ***magjának*** nevezzük.

2.7. Állítás. Tetszőleges $f\colon A \to B$ leképezés esetén f magja ekvivalenciareláció az A halmazon.

Bizonyítás. A mag tulajdonságai rendre visszavezethetőek az egyenlőség tulajdonságaira:

(1) $\ker f$ reflexív, mert $\forall a \in A : af = af$;
(2) $\ker f$ szimmetrikus, mert $\forall a_1,a_2 \in A : a_1 f = a_2 f \implies a_2 f = a_1 f$;
(3) $\ker f$ tranzitív, mert $\forall a_1,a_2,a_3 \in A : (a_1 f = a_2 f \text{ és } a_2 f = a_3 f) \implies a_1 f = a_3 f$. □

2.8. Példa. Tekintsük az egész számok halmazán a következő módon definiált ρ relációt: $a\rho b \iff 3 \mid a-b$. Ellenőrizzük, hogy ez ekvivalenciareláció. Tetszőleges $a,b \in \mathbb{Z}$ esetén

(1) $a\rho a \iff 3 \mid a-a$ (ugye?);
(2) $a\rho b \iff 3 \mid a-b \implies 3 \mid b-a \iff b\rho a$ (miért?);
(3) $(a\rho b \text{ és } b\rho c) \iff (3 \mid a-b \text{ és } 3 \mid b-c) \implies 3 \mid a-c \iff a\rho c$ (miért?).

A fenti számolást „megspórolhatnánk”, ha találnánk egy olyan f leképezést, amelyre $\ker f = \rho$; ekkor ugyanis a 2.7. Állításból „ingyen” megkapjuk, hogy ρ ekvivalenciareláció. Ilyen leképezés valóban létezik. Mi ez a leképezés?

2.9. Példa. Legyen $A = \{a,b,c,d,e,f\}$ és

$$\rho = \big\{(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),(a,b),(b,a),(d,e),(e,d),(d,f),(f,d),(e,f),(f,e)\big\}.$$

Ez egy ekvivalenciareláció, de ezt elég nehézkes volna ellenőrizni (főleg a tranzitivitást). Ha felrajzoljuk a reláció gráfját, akkor azt látjuk, hogy három összefüggő komponens van, és a komponensek mind irányított teljes gráfok (egy komponensen belül „mindenki mindenkivel, oda-vissza” össze van kötve). Így már a tranzitivitás is világos. Be fogjuk bizonyítani, hogy minden ekvivalenciareláció esetén így néznek ki az összefüggő komponensek (gondoljuk majd meg, hogy a 2.18. Tétel (i) állításának ez a szemléletes jelentése). A gráf alapján könnyen meg tudunk adni olyan leképezést, aminek éppen ez a reláció a magja. Vegyünk három tetszőleges elemet (pl. $\clubsuit, \heartsuit, \spadesuit$), és rendeljük az ugyanabba a komponensbe eső elemekhez ugyanazt az elemet:

$$f\colon A \to \{\clubsuit,\heartsuit,\spadesuit\}, \quad a \mapsto \clubsuit,\ b \mapsto \clubsuit,\ c \mapsto \heartsuit,\ d \mapsto \spadesuit,\ e \mapsto \spadesuit,\ f \mapsto \spadesuit.$$

2.10. Definíció. Legyen $\rho \subseteq A \times A$ egy ekvivalenciareláció és a tetszőleges eleme A-nak. Ekkor az

$$\overline{a} := \{b \in A : a \rho b\}$$

halmazt az a elem ρ szerinti ***ekvivalenciaosztályának***, az ekvivalenciaosztályok halmazát pedig az A halmaz ρ szerinti ***faktorhalmazának*** nevezzük. Az a elem ρ szerinti osztályát szokás a/ρ-val, $\overline{a}^{\rho}$-val vagy $[a]_{\rho}$-val jelölni, de mi inkább az egyszerűbb $\overline{a}$ jelölést használjuk. Ez ugyan nem utal ρ-ra, de általában kiderül a szövegkörnyezetből, hogy mi a szóban forgó ekvivalenciareláció. A faktorhalmazt A/ρ jelöli, tehát

$$A/\rho = \{\overline{a} : a \in A\}.$$

2.11. Példa. A 2.9. Példában szereplő ρ relációnál az ekvivalenciaosztályok éppen a gráf összefüggő komponensei (ez minden ekvivalenciarelációnál így van):

$$\overline{a} = \{a, b\},\ \ \overline{b} = \{a, b\},\ \ \overline{c} = \{c\},\ \ \overline{d} = \{d, e, f\},\ \ \overline{e} = \{d, e, f\},\ \ \overline{f} = \{d, e, f\}.$$

A faktorhalmaz tehát így fest:

$$A/\rho = \big\{\overline{a}, \overline{b}, \overline{c}, \overline{d}, \overline{e}, \overline{f}\big\} = \Big\{\{a, b\}, \{a, b\}, \{c\}, \{d, e, f\}, \{d, e, f\}, \{d, e, f\}\Big\} = \Big\{\{a, b\}, \{c\}, \{d, e, f\}\Big\}.$$

(Először a 2.10. Definíciót betű szerint alkalmazva írtuk fel a faktorhalmazt, azután úgy, hogy az ismétlődő elemekből csak egyet tartottunk meg. Célszerű mindig kihagyni az ismétlődéseket, mert így jobban áttekinthető a faktorhalmaz.)

2.12. Példa. A 2.8. Példában szereplő relációnál három ekvivalenciaosztály van:

$$\begin{aligned}\overline{0} &= \{\ldots, -3, 0, 3, 6, \ldots\} = \{3k : k \in \mathbb{Z}\},\\ \overline{1} &= \{\ldots, -2, 1, 4, 7, \ldots\} = \{3k + 1 : k \in \mathbb{Z}\},\\ \overline{2} &= \{\ldots, -1, 2, 5, 8, \ldots\} = \{3k + 2 : k \in \mathbb{Z}\}.\end{aligned}$$

A faktorhalmaznak tehát három eleme van: $\mathbb{Z}/\rho = \big\{\overline{0}, \overline{1}, \overline{2}\big\}$.

2.13. Állítás. Legyen ρ ekvivalenciareláció az A halmazon. Ekkor minden $a, b \in A$ esetén $\overline{a} = \overline{b} \iff a \rho b$.

Bizonyítás. Tegyük fel először, hogy $\overline{a} = \overline{b}$. A reflexivitásból következik, hogy $b \in \overline{b}$ (ugye?), tehát $b \in \overline{a}$ (miért?). Ez utóbbi pedig éppen azt jelenti, hogy $a \rho b$ (ugye?).

A másik irány igazolásához tfh. $a \rho b$, és legyen $x \in \overline{b}$ egy tetszőleges elem. Ekkor $b \rho x$ (ugye?), és ebből az $a \rho b$ feltevés és a tranzitivitás segítségével megkapjuk, hogy $a \rho x$ (miért?), ez pedig azt jelenti, hogy $x \in \overline{a}$. Ezzel beláttuk, hogy $\overline{b} \subseteq \overline{a}$ (ugye?). A másik irányú tartalmazás hasonlóan (de nem szó szerint ugyanígy!) látható be (HF). □

2.14. Következmény. Minden ekvivalenciareláció előáll egy leképezés magjaként: ha $\rho \subseteq A \times A$ ekvivalenciareláció, akkor létezik olyan B halmaz és $f\colon A \to B$ leképezés, amelyre $\ker f = \rho$.

Bizonyítás. Rendeljük minden elemhez az ekvivalenciaosztályát, azaz legyen f az alábbi leképezés:

$$f\colon A \to A/\rho, \quad a \mapsto \overline{a}.$$

A 2.13. Állítás pontosan azt mondja, hogy $\ker f = \rho$ (ugye?). □

2.15. Megjegyzés. A fenti bizonyításban megadott f leképezést *természetes leképezésnek* nevezzük, mert nincs annál természetesebb dolog, mint minden elemhez a saját osztályát rendelni.

2.16. Tétel. Az ekvivalenciaosztályok páronként diszjunktak: ha $\rho \subseteq A \times A$ ekvivalenciareláció, akkor minden $a, b \in A$ esetén $\overline{a} \neq \overline{b} \implies \overline{a} \cap \overline{b} = \emptyset$.

Bizonyítás. Kontrapozícióval bizonyítunk: azt mutatjuk meg, hogy $\overline{a} \cap \overline{b} \neq \emptyset \implies \overline{a} = \overline{b}$. Tegyük fel tehát, hogy $\overline{a} \cap \overline{b} \neq \emptyset$, és legyen $c \in \overline{a} \cap \overline{b}$. Ekkor $a \rho c$ és $b \rho c$ (miért?), ebből pedig a 2.13. Állítás alapján következik, hogy $\overline{a} = \overline{c}$ és $\overline{b} = \overline{c}$. Tehát valóban $\overline{a} = \overline{b}$ (ugye?). □

2.17. Definíció. Egy nemüres halmaz ***osztályozásán*** olyan páronként diszjunkt nemüres részhalmazainak halmazát értjük, amelyek együtt lefedik az alaphalmazt. Formálisan: $\mathcal{C} = \{O_i : i \in I\} \subseteq \mathcal{P}(A)$ osztályozás a nemüres A halmazon, ha

(a) $\forall O_i \in \mathcal{C} : O_i \neq \emptyset$;

(b) $\forall O_i, O_j \in \mathcal{C} : O_i \neq O_j \implies O_i \cap O_j = \emptyset$;

(c) $\bigcup_{i \in I} O_i = A$.

2.18. Tétel. Legyen A egy nemüres halmaz.

(i) Ha $\rho \subseteq A \times A$ ekvivalenciareláció, akkor A/ρ osztályozás az A halmazon.

(ii) Ha pedig $\mathcal{C} \subseteq \mathcal{P}(A)$ osztályozás, akkor az

$$a \rho b \iff \exists O_i \in \mathcal{C} : a, b \in O_i$$

formulával definiált ρ reláció ekvivalenciareláció az A halmazon.

Bizonyítás. Az első állítás bizonyításához tfh. ρ ekvivalenciareláció az A halmazon. Az osztályozás definíciójában szereplő (b) tulajdonság következik a 2.16. Tételből. Az (a) és (c) tulajdonságok kulcsa pedig az, hogy a reflexivitás miatt $a \in \overline{a}$ teljesül minden $a \in A$ esetén (ugye?). Ebből következik, hogy (a) az ekvivalenciaosztályok nem üresek (hiszen $\overline{a}$-nak a biztosan eleme), és az is, hogy (c) az ekvivalenciaosztályok együtt lefedik az A halmazt (hiszen az a elemet lefedi az $\overline{a}$ osztály).

A második állítás bizonyításához tfh. $\mathcal{C}$ osztályozás az A halmazon. Mivel az osztályok lefedik az alaphalmazt ((c) tulajdonság), minden elem benne van legalább egy osztályban. Mivel az osztályok páronként diszjunktak ((b) tulajdonság), minden elem lefeljebb egy osztályban lehet benne. Tehát az alaphalmaz minden eleme pontosan egy osztályban van benne. Legyen $f\colon A \to \mathcal{C}$ az a leképezés amelyik minden $a \in A$ elemhez hozzárendeli azt az egyetlen $O_i \in \mathcal{C}$ osztályt, amelyre $a \in O_i$. Az f leképezés magja éppen a tétel kimondásában szereplő ρ reláció (miért?), és így a 2.7. Állítás szerint ρ ekvivalenciareláció. □

2.19. Megjegyzés. Nem nehéz meggondolni, hogy a fenti tételben megadott „*ekvivalenciareláció* $\mapsto$ *osztályozás*” és „*osztályozás* $\mapsto$ *ekvivalenciareláció*” megfeleltetések egymás inverzei, vagyis egy tetszőleges alaphalmaz ekvivalenciarelációi és osztályozásai kölcsönösen egyértelműen megfelelnek egymásnak.

Részbenrendezések

2.20. Definíció. ***Részbenrendezési relációnak*** nevezzük a $\rho \subseteq A \times A$ relációt, ha rendelkezik az alábbi három tulajdonsággal:

(1) $\forall a \in A : a\rho a$ (reflexivitás);

(2) $\forall a, b \in A : (a\rho b \text{ és } b\rho a) \implies a = b$ (antiszimmetria);

(3) $\forall a, b, c \in A : (a\rho b \text{ és } b\rho c) \implies a\rho c$ (tranzitivitás).

Ha még a következő tulajdonság is teljesül, akkor ρ-t ***teljes rendezésnek*** (vagy lineáris rendezésnek, vagy röviden csak rendezésnek) nevezzük:

(4) $\forall a, b \in A : a\rho b$ vagy $b\rho a$ (dichotómia).

2.21. Példa. A 2.2. Példában szereplő relációk közül a „kisebb vagy egyenlő” reláció teljes rendezés, az egyenlőség, az oszthatóság és a tartalmazási reláció részbenrendezés.

Jelölés. A részbenrendezéseket szokás a $\leq$ szimbólummal jelölni, még akkor is, ha az alaphalmaz elemei esetleg nem is számok. Ha $a \leq b$ de $a \neq b$, akkor azt írjuk, hogy $a < b$.

2.22. Definíció. ***Részbenrendezett halmazon*** egy $(A; \leq)$ párt értünk, ahol A egy nemüres halmaz, és $\leq$ részbenrendezés A-n.

2.23. Definíció. Legyen $(A; \leq)$ egy részbenrendezett halmaz, és legyen $a, b \in A$. Azt mondjuk, hogy b ***fedi*** a-t, ha $a < b$, de nem létezik olyan $c \in A$, amelyre $a < c < b$. Ezt a tényt $a \prec b$ jelöli, és a $\prec$ relációt az adott részbenrendezéshez tartozó ***fedési relációnak*** hívjuk.

2.24. Példa. Íme néhány nevezetes (részben)rendezett halmaz és a hozzájuk tartozó fedési reláció:

(a) Az egész számok halmazán a szokásos „nagyság szerinti” rendezés teljes rendezés. A $(\mathbb{Z}; \leq)$ rendezett halmazban két szám akkor és csak akkor fedi egymást, ha a nagyobbik csak 1-gyel nagyobb a kisebbiknél: $a \prec b \iff b = a+1$.

(b) A valós számok halmazán is teljes rendezés a szokásos „nagyság szerinti” rendezés, de itt $a \prec b$ soha nem teljesül (miért?), vagyis a fedési reláció üres: $\prec = \emptyset$.

(c) A nemnegatív egész számok halmazán az oszthatóság részbenrendezés (de nem teljes rendezés). Az $(\mathbb{N}_0; |)$ részbenrendezett halmazban két szám akkor és csak akkor fedi egymást, ha a nagyobbik „prímszerese” a kisebbiknek: $a \prec b \iff \exists p$ prímszám$\colon b = p \cdot a$.

(d) Tetszőleges U halmaz esetén U hatványhalmazán (vagyis U összes részhalmazainak halmazán) a tartalmazási reláció részbenrendezés. A $(\mathcal{P}(U); \subseteq)$ részbenrendezett halmazban két elem akkor és csak akkor fedi egymást, ha a nagyobbik csak egyetlen elemmel bővebb a kisebbiknél: $A \prec B \iff \exists u \in U \setminus A\colon B = A \cup \{u\}$.

2.25. Definíció. Egy $(A; \leq)$ részbenrendezett halmaz ***Hasse-diagramján*** egy olyan ábrát értünk, amelynél A elemeit (síkbeli) pontokkal ábrázoljuk oly módon, hogy $a < b$ esetén a b-nek megfelelő pont „följebb” van, mint az a-nak megfelelő pont, és e két pontot akkor és csak akkor kötjük össze, ha b fedi a-t. A 2.29. Tétel szerint véges részbenrendezett halmazokat „érdemes” Hasse-diagrammal ábrázolni. Néha végtelen részbenrendezett halmazokról is jó képet ad a Hasse-diagram (például a $(\mathbb{Z}; \leq)$ és $(\mathbb{N}_0; |)$ részbenrendezett halmazok esetén), de például az $(\mathbb{R}; \leq)$ rendezett halmaz Hasse-diagramját bajos volna lerajzolni, mert itt a fedési reláció üres.

2.26. Példa. Tekintsük az $(\{1, 2, 3, 6\}; \leq)$ részbenrendezett halmazt. Ebben az esetben a részbenrendezési reláció és a fedési reláció így fest:

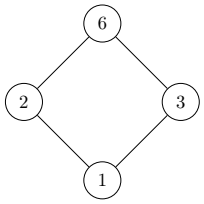
$$\leq = \big\{(1,1), (1,2), (1,3), (1,6), (2,2), (2,3), (2,6), (3,3), (3,6), (6,6)\big\}, \quad \prec = \big\{(1,2), (2,3), (3,6)\big\}.$$

Ennek megfelelően a Hasse-diagramon csak az $1-2$, $2-3$ és $3-6$ éleket kell berajzolni (nyílhegyeket nem rajzolunk, helyette a csúcsokat úgy rendezzük el, hogy a nagyobb szám mindig följebb legyen):

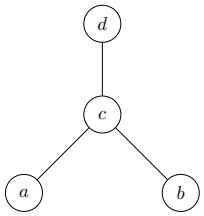
2.27. Példa. Tekintsük az $(\{1,2,3,6\};|)$ részbenrendezett halmazt. Ebben az esetben a részbenrendezési reláció és a fedési reláció így fest:

$$| = \big\{(1,1),(1,2),(1,3),(1,6),(2,2),(2,6),(3,3),(3,6),(6,6)\big\}, \quad \prec = \big\{(1,2),(1,3),(2,6),(3,6)\big\}.$$

Ennek megfelelően a Hasse-diagramon csak az $1-2$, $1-3$, $2-6$ és $3-6$ éleket kell berajzolni:



2.28. Példa. Tekintsük az alábbi Hasse-diagrammal megadott részbenrendezett halmazt:



Itt az alaphalmaz $A = \{a,b,c,d\}$, és a diagramról leolvashatjuk a megfelelő részbenrendezési relációt és fedési relációt:

$$\leq = \big\{(a,a),(a,c),(a,d),(b,b),(b,c),(b,d),(c,c),(c,d),(d,d)\big\}, \quad \prec = \big\{(a,c),(b,c),(c,d)\big\}.$$

2.29. Tétel. Véges részbenrendezett halmazt egyértelműen meghatározza a fedési relációja.

Bizonyítás. Legyen $(A;\leq)$ egy véges részbenrendezett halmaz, és legyen $\prec$ a megfelelő fedési reláció. Azt állítjuk, hogy minden $a,b \in A$ esetén

$$a \leq b \iff \exists n \in \mathbb{N}_0\ \exists c_0, c_1, \ldots, c_n \in A\colon\ a = c_0 \prec c_1 \prec \cdots \prec c_n = b.$$

(Ez szemléletesen azt jelenti, hogy $a \leq b$ akkor és csak akkor teljesül, ha a és b összeköthető egy véges hosszúságú, fedésekből álló lánccal.) A „ $\Longleftarrow$ ” irány igazolásához tfh. $a = c_0 \prec c_1 \prec \cdots \prec c_n = b$. Ekkor $a = c_0 < c_1 < \cdots < c_n = b$ (miért?), és így a tranzitivitás miatt $a \leq b$ (ugye?). A „ $\Longrightarrow$ ” irány igazolásához tfh. $a \leq b$. Ha $a = b$, akkor készen vagyunk ($n = 0$ és $c_0 = a = b$), feltehetjük tehát, hogy $a < b$. Legyen $a = c_0 < c_1 < \cdots < c_n = b$ a lehető leghosszabb szigorúan monoton növekedő sorozat, ami a-ból indul és b-be érkezik. (Ha több maximális hosszúságú sorozat van, akkor bármelyiket vehetjük közülük.) Ha itt valamelyik tag nem fedné az őt megelőző tagot (pl. $c_i \not\prec c_{i+1}$), akkor be lehetne illeszteni közéjük egy újabb elemet ($c_i \prec d \prec c_{i+1}$), és így kapnánk egy hosszabb szigorúan monoton növekedő sorozatot a-tól b-ig. Ez pedig ellentmond annak, hogy a sorozatunk a lehető leghosszabb volt. □

2.30. Definíció. Legyen $(A;\leq)$ egy részbenrendezett halmaz. Az $a \in A$ elemet ***minimális elemnek*** nevezzük, ha nincs nála kisebb elem, és ***legkisebb elemnek*** nevezzük, ha ő mindenki másnál kisebb. Hasonlóan $a \in A$ ***maximális***, ha nincs nála nagyobb elem, és $a \in A$ ***legnagyobb***, ha ő mindenki másnál nagyobb. Formálisan:

- a minimális $\iff \nexists c \in A : c < a$;
- a legkisebb $\iff \forall c \in A : a \leq c$;
- a maximális $\iff \nexists c \in A : c > a$;
- a legnagyobb $\iff \forall c \in A : a \geq c$.

2.31. Példa. A 2.26. Példában szereplő $(\{1,2,3,6\};\leq)$ részbenrendezett halmazban 1 minimális és legkisebb elem, 6 maximális és legnagyobb elem. Ugyanez érvényes a 2.27. Példában szereplő $(\{1,2,3,6\};|)$ részbenrendezett halmazra. A 2.28. Példában szereplő $(\{a,b,c,d\};\leq)$ részbenrendezett halmazban a és b minimális elemek, legkisebb elem nincs, d maximális és legnagyobb elem. A $(\mathbb{Z};\leq)$ részbenrendezett halmazban nincs se minimális, se legkisebb, se maximális, se legnagyobb elem. Az $(\mathbb{N}_0;\leq)$ részbenrendezett halmazban 0 minimális és legkisebb elem, és nincs se maximális, se legnagyobb elem. Az $(\mathbb{N}_0;|)$ részbenrendezett halmazban 1 minimális és legkisebb elem, 0 maximális és legnagyobb elem.

2.32. Tétel. Részbenrendezett halmazban legföljebb egy legkisebb elem létezhet. Ha van legkisebb elem, akkor az minimális elem is, sőt ilyenkor ő az egyetlen minimális elem. Formálisan: ha $(A;\leq)$ egy részbenrendezett halmaz és $a,b\in A$, akkor

(i) a és b is legkisebb elem $\implies a=b$;

(ii) a legkisebb $\implies a$ minimális;

(iii) a legkisebb és b minimális $\implies a=b$.

Hasonló érvényes a legnagyobb elemre is.

Bizonyítás.

(i) Ha a és b is legkisebb elem, akkor $a\leq b$ (miért?) és $b\leq a$ (miért?), és így az antiszimmetria miatt $a=b$.

(ii) Indirekten bizonyítunk: tfh. a legkisebb elem, de nem minimális. Mivel a nem minimális, létezik olyan $c\in A$, amelyre $c<a$. Mivel a a legkisebb, $a\leq c$. Triviálisnak tűnik, hogy $c<a$ és $a\leq c$ ellentmondanak egymásnak, de ne feledjük, hogy nem számokról és a szokásos „kisebb vagy egyenlő” relációról van szó, hanem egy tetszőleges részbenrendezett halmazról! Tehát a reflexivitáson, antiszimmetrián és tranzitivitáson kívül semmit nem tudunk; csak ezt a három tulajdonságot használhatjuk fel. A $c<a$ jelölés azt jelenti, hogy $c\leq a$, de $c\neq a$ (ugye?). Tehát tudjuk, hogy $c\leq a$ és $a\leq c$, és így az antiszimmetria miatt $c=a$. Node tudjuk azt is, hogy $c\neq a$, és ez már tényleg ellentmondás.

(iii) Tfh. a legkisebb elem és b minimális elem. Mivel a legkisebb, $a\leq b$. Ha itt egyenlőség teljesül, akkor készen vagyunk. Ha nem, akkor $a<b$, ami nem lehetséges, mert b minimális (ugye?). □

3. Számelméleti kongruenciák

Lineáris diofantoszi egyenletek

3.1. Definíció. A d egész számot az a és b egész számok ***legnagyobb közös osztójának*** nevezzük, ha kielégíti a következő két feltételt:

(1) $d\mid a$ és $d\mid b$;

(2) $\forall k\in\mathbb{Z}:(k\mid a \text{ és } k\mid b)\implies k\mid d$.

Hasonlóan definiálható egész számok ***legkisebb közös többszöröse*** is.

Jelölés. Az a és b számok legnagyobb közös osztóját $\text{lnko}(a,b)$ vagy (a,b), legkisebb közös többszörösüket pedig $\text{lkkt}(a,b)$ vagy $[a,b]$ jelöli.

3.2. Megjegyzés. A legnagyobb közös osztó nem egyértelmű: ha d legnagyobb közös osztója a-nak és b-nek, akkor $-d$ is az (de e két számon kívül nincs más legnagyobb közös osztó). Általában a két érték közül a nemnegatívat szoktuk tekinteni. Másképp fogalmazva, az lnko csak asszociáltság erejéig van meghatározva; ezért szoktuk így is írni: $d\sim\text{lnko}(a,b)$.

3.3. Megjegyzés. Jelölje egy a pozitív egész szám pozitív osztóinak halmazát D_a. Ekkor az a és b pozitív egészek, pozitív közös osztóinak halmaza $D_a\cap D_b$. Ezen a halmazon kétféle részbenrendezést is értelmezhetünk: a nagyság szerinti rendezést és az oszthatóság szerinti rendezést. A legnagyobb közös osztó általános és középiskolában használatos definíciója szerint $\text{lnko}(a,b)$ nem más, mint a $(D_a\cap D_b;\leq)$ rendezett halmaz legnagyobb eleme. Az általunk használt 3.1. Definíció szerint $\text{lnko}(a,b)$ nem más, mint a $(D_a\cap D_b;|)$ részbenrendezett halmaz legnagyobb eleme. (Például $a=18$, $b=30$ esetén $D_{18}\cap D_{30}=D_{\text{lnko}(18,30)}=D_6=\{1,2,3,6\}$. A $(D_a\cap D_b;\leq)$ rendezett halmaz Hasse-diagramját a 2.26. Példa, a $(D_a\cap D_b;|)$ részbenrendezett halmaz Hasse-diagramját pedig a 2.27. Példa mutatja ebben a konkrét esetben.) Ha a és b is pozitív (sőt, még akkor is, ha egyikük nulla), akkor a két definíció ekvivalens egymással: ha d a legnagyobb eleme a $(D_a\cap D_b;|)$ részbenrendezett halmaznak, akkor minden $k\in D_a\cap D_b$ esetén $k\mid d$, és így $k\leq d$ is teljesül, tehát d legnagyobb eleme a $(D_a\cap D_b;\leq)$ rendezett halmaznak is (ugye?). Ha azonban $a=b=0$, akkor a $(D_a\cap D_b;\leq)$ rendezett halmaznak nincs legnagyobb eleme (miért?), míg a $(D_a\cap D_b;|)$ részbenrendezett halmaz legnagyobb eleme 0 (ugye?). Tehát $a=b=0$ esetén az „iskolás” definíció nem használható, az „egyetemi” definíció viszont igen. Egy másik előnye az 3.1. Definíciónak, hogy általánosítható az egész számok gyűrűjéről más gyűrűkre, ahol nincs is „nagyság szerinti” rendezés (más kérdés, hogy legnagyobb közös osztók nem minden gyűrűben léteznek).

3.4. Tétel. Bármely két egész számnak van legnagyobb közös osztója, és az kifejezhető a két szám „lineáris kombinációjaként”: minden $a,b\in\mathbb{Z}$ esetén léteznek olyan x,y egész számok, melyekre $ax+by=\text{lnko}(a,b)$.

Bizonyítás. Az általánosság megszorítása nélkül feltehetjük, hogy a és b is pozitív (ha valamelyikük nulla, akkor az állítás triviális, a negatív szám(ok) esete pedig könnyen visszavezethető a pozitív esetre). Ekkor végrehajtható az a, b számokra az euklideszi algoritmus (technikai okokból a és b az r_0 és r_1 „fedőneveket" kapják):

$$\begin{aligned}
r_0 := a &= q_1 r_1 + r_2 && (0 \le r_2 < r_1);\\
r_1 := b &= q_2 r_2 + r_3 && (0 \le r_3 < r_2);\\
r_2 &= q_3 r_3 + r_4 && (0 \le r_4 < r_3);\\
&\vdots\\
r_{i-1} &= q_i r_i + r_{i+1} && (0 \le r_{i+1} < r_i);\\
&\vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && (0 \le r_n < r_{n-1});\\
r_{n-1} &= q_n r_n + 0.
\end{aligned}$$

Tudjuk (Algszám. 1), hogy az eljárás véges számú lépésben véget ér: előbb utóbb nulla lesz a maradék ($r_{n+1} = 0$), és a legnagyobb közös osztó az utolsó nemnulla maradék: $r_n \sim \mathrm{lnko}(a, b)$. Megmutatjuk i szerinti teljes indukcióval, hogy mindegyik r_i előáll a és b „lineáris kombinációjaként":

$$\exists x_i, y_i \in \mathbb{Z}\colon\ r_i = a x_i + b y_i. \tag{3.2}$$

(Két dologban eltérünk az indukció szokásos sémájától. Egyrészt nem minden i nemnegatív egészre bizonyítunk, hanem csak $i = 0, 1, \ldots, n$-re. Másrészt az indukciós lépésben két lépéssel nyúlunk vissza: amikor $i+1$-re bizonyítjuk az állítást, nemcsak i-re, hanem $i-1$-re is feltesszük, hogy (3.2) teljesül. Emiatt a kezdőlépésnél is az első két értékre ($i = 0$ és $i = 1$) kell ellenőriznünk az állítást.)

Kezdőlépés: $i = 0$ és $i = 1$ esetén triviálisan teljesül (3.2):

$$\begin{aligned}
r_0 = a = a \cdot 1 + b \cdot 0 &\qquad (\text{tehát } x_0 = 1 \text{ és } y_0 = 0 \text{ jó lesz});\\
r_1 = b = a \cdot 0 + b \cdot 1 &\qquad (\text{tehát } x_1 = 0 \text{ és } y_1 = 1 \text{ jó lesz}).
\end{aligned}$$

Indukciós lépés: Legyen $1 \le i < n$, és tfh. r_{i-1} és r_i előáll a kívánt módon; ez az indukciós feltevés:

$$r_{i-1} = a x_{i-1} + b y_{i-1} \text{ és } r_i = a x_i + b y_i. \tag{IH}$$

Be kell látnunk, hogy (3.2) teljesül $i+1$-re is. Ehhez fejezzük ki az r_{i+1} maradékot az euklideszi algoritmus megfelelő lépéséből: $r_{i+1} = r_{i-1} - q_i r_i$. Helyettesítsük r_{i-1} és r_i helyébe az indukciós hipotézisben szereplő felírásukat:

$$\begin{aligned}
r_{i+1} = r_{i-1} - q_i r_i &= (a x_{i-1} + b y_{i-1}) - q_i (a x_i + b y_i)\\
&= a(x_{i-1} - q_i x_i) + b(y_{i-1} - q_i y_i).
\end{aligned}$$

Azt kaptuk, hogy r_{i+1} is kifejezhető a és b segítségével az előírt módon, pl. $x_{i+1} = x_{i-1} - q_i x_i$ és $y_{i+1} = y_{i-1} - q_i y_i$ együtthatókkal. Ezzel kész az indukciós bizonyítás. □

3.5. Példa. Hajtsuk végre az euklideszi algoritmust az $a = 150$ és $b = 54$ számokra, és fejezzük ki minden osztásból (az utolsó kivételével) a maradékot a és b segítségével:

$$\begin{array}{rcl@{\quad}c@{\quad}rcl@{\quad}l}
150 &=& 2 \cdot 54 + 42 & \Longrightarrow & 42 &=& 150 - 2 \cdot 54 & = a - 2b\\
54 &=& 1 \cdot 42 + 12 & \Longrightarrow & 12 &=& 54 - 42 = b - (a - 2b) & = -a + 3b\\
42 &=& 3 \cdot 12 + \boxed{6} & \Longrightarrow & \boxed{6} &=& 42 - 3 \cdot 12 = (a - 2b) - 3(-a + 3b) & = \boxed{4a - 11b}\\
12 &=& 2 \cdot 6 + 0 & & & & &
\end{array}$$

Tehát $\mathrm{lnko}(a, b) = 6$, és ez így fejezhető ki a és b „lineáris kombinációjaként": $6 = 4a - 11b$.

3.6. Definíció. Azt mondjuk, hogy az a, b egész számok ***relatív prímek***, ha $\mathrm{lnko}(a, b) \sim 1$. Jelölés: $a \perp b$.

3.7. Következmény. Tetszőleges a, b egész számok esetén, ha $\mathrm{lnko}(a, b) \neq 0$, akkor

$$\frac{a}{\mathrm{lnko}(a, b)} \perp \frac{b}{\mathrm{lnko}(a, b)}.$$

Bizonyítás. Tfh. $d := \mathrm{lnko}(a, b) \neq 0$ (milyen a, b esetén teljesül ez?). Az a és b számokat $a = a_0 d$ és $b = b_0 d$ alakba írhatjuk alkalmas a_0, b_0 egész számokkal (miért?). A 3.4. Tétel szerint vannak olyan x, y egészek, amelyekre $ax + by = d$. Egyszerűsíthetünk d-vel (miért?), és így azt kapjuk, hogy $a_0 x + b_0 y = 1$. A bal oldal osztható a_0 és b_0 legnagyobb közös osztójával (miért?), tehát $\mathrm{lnko}(a_0, b_0) \mid 1$, azaz a_0 és b_0 valóban relatív prímek. □

3.8. Következmény (Euklidész lemmája). Tetszőleges a, b, c egész számok esetén, ha $\mathrm{lnko}(a, b) \neq 0$, akkor

$$a \mid bc \iff \frac{a}{\mathrm{lnko}(a, b)} \mid c.$$

Bizonyítás. Tfh. $d := \operatorname{lnko}(a,b) \neq 0$, és írjuk fel az a és b számokat a 3.7. Következmény bizonyításában látott módon $a = a_0 d$ és $b = b_0 d$ alakban. Ezzel a jelöléssel a bizonyítandó állítás így fest:

$$a_0 d \mid b_0 d \cdot c \overset{?}{\iff} a_0 \mid c.$$

Mivel $d \neq 0$, a bal oldali oszthatóságot d-vel egyszerűsíthetjük; így a következő ekivalenciát kell igazolnunk:

$$a_0 \mid b_0 c \overset{?}{\iff} a_0 \mid c.$$

A „ $\Longleftarrow$ ” irány triviális (ugye?). A „ $\Longrightarrow$ ” irányhoz tfh. $a_0 \mid b_0 c$. A 3.4. Tételt használva felírjuk a legnagyobb közös osztót $ax + by = d$ alakban. Mindkét oldalt d-vel egyszerűsítve, majd c-vel szorozva, azt kapjuk, hogy $a_0 cx + b_0 cy = c$. Itt a bal oldalon mindkét tag osztható a_0-lal (miért?), ezért c is osztható vele, és épp ezt kellett bizonyítanunk. □

3.9. Példa. Milyen x egész számokra lesz $150x$ osztható 54-gyel? Euklidész lemmája szerint

$$54 \mid 150x \iff \frac{54}{\operatorname{lnko}(54,150)} \;\Big|\; x \iff 9 \mid x.$$

Tehát az $54 \mid 150x$ „oszthatósági egyenlet” megoldáshalmaza $\{\ldots, -18, -9, 0, 9, 18, \ldots\}$.

3.10. Következmény. Tetszőleges $a, b, c \in \mathbb{Z}$ esetén, ha $a \perp b$, akkor $a \mid bc \iff a \mid c$.

3.11. Tétel. Tekintsük tetszőleges adott a, b, c $(a, b \neq 0)$ egész számok esetén az $ax + by = c$ ***kétismeretlenes lineáris diofantoszi egyenletet*** (a megoldásokat az egész számok gyűrűjében keressük).

(i) Az egyenletnek akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a,b) \mid c$.

(ii) Ha (x_0, y_0) egy megoldás, akkor bármely $t \in \mathbb{Z}$ esetén az alábbi (x_t, y_t) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t szám alkalmas megválasztásával:

$$x_t = x_0 + \frac{b}{\operatorname{lnko}(a,b)} \cdot t; \qquad y_t = y_0 - \frac{a}{\operatorname{lnko}(a,b)} \cdot t.$$

Bizonyítás.

(i) A feltétel szükségességét könnyű belátni: ha (x, y) egy megoldás, azaz $ax + by = c$, akkor a bal oldal osztható $\operatorname{lnko}(a,b)$-vel (miért?), és így $\operatorname{lnko}(a,b) \mid c$. Az elegendőség igazolásához tfh. $\operatorname{lnko}(a,b) \mid c$, azaz $c = \operatorname{lnko}(a,b) \cdot c_1$ alkalmas c_1 egész számmal. A 3.4. Tétel szerint létezik $u, v \in \mathbb{Z}$, hogy $au + bv = \operatorname{lnko}(a,b)$. Beszorozva mindkét oldalt c_1-gyel, azt kapjuk, hogy $a(uc_1) + b(vc_1) = c$, vagyis az (uc_1, vc_1) számpár megoldása az egyenletnek.

(ii) Jelölje M az egyenlet megoldáshalmazát: $M = \big\{(x,y) \in \mathbb{Z}^2 \colon ax + by = c\big\}$. Legyen $(x_0, y_0) \in M$ egy tetszőleges rögzített megoldás, azaz $ax_0 + by_0 = c$. Azt kell bizonyítanunk, hogy $M = \{(x_t, y_t) \colon t \in \mathbb{Z}\}$. A „$\supseteq$” tartalmazást (vagyis azt, hogy (x_t, y_t) minden t-re megoldás), egyszerű behelyettesítéssel lehet ellenőrizni:

$$ax_t + by_t = a\Big(x_0 + \frac{b}{\operatorname{lnko}(a,b)} \cdot t\Big) + b\Big(y_0 - \frac{a}{\operatorname{lnko}(a,b)} \cdot t\Big) = ax_0 + by_0 = c \qquad \text{(miért?)}.$$

A „$\subseteq$” tartalmazás azt jelenti, hogy tetszőleges $(x, y) \in M$ megoldás esetén van olyan $t \in \mathbb{Z}$, amelyre $(x, y) = (x_t, y_t)$. Ennek igazolásához tfh. $(x, y) \in M$, és ne feledjük, hogy korábban feltettük azt is, hogy $(x_0, y_0) \in M$. Tehát azt tudjuk, hogy $ax + by = c = ax_0 + by_0$. Átrendezve, azt kapjuk, hogy $a(x - x_0) = b(y_0 - y)$. Itt a bal oldal szemlátomást osztható a-val, és így $a \mid b(y_0 - y)$. Euklidész lemmája szerint ebből az következik, hogy $\frac{a}{\operatorname{lnko}(a,b)} \mid y_0 - y$, ez pedig az oszthatóság definíciója szerint azt jelenti, hogy $y_0 - y = \frac{a}{\operatorname{lnko}(a,b)} \cdot t$ alkalmas t egész számmal. Ezzel meg is kaptuk, hogy $y = y_0 - \frac{a}{\operatorname{lnko}(a,b)} \cdot t$, azaz $y = y_t$. Hogy megkapjuk x-et is, helyettesítsünk vissza az $a(x - x_0) = b(y_0 - y)$ egyenlőségbe: $a(x - x_0) = b(y_0 - y) = b \cdot \frac{a}{\operatorname{lnko}(a,b)} \cdot t$. Ebből már x-et könnyen kifejezhetjük: $x = x_0 + \frac{b}{\operatorname{lnko}(a,b)} \cdot t$, azaz $x = x_t$. □

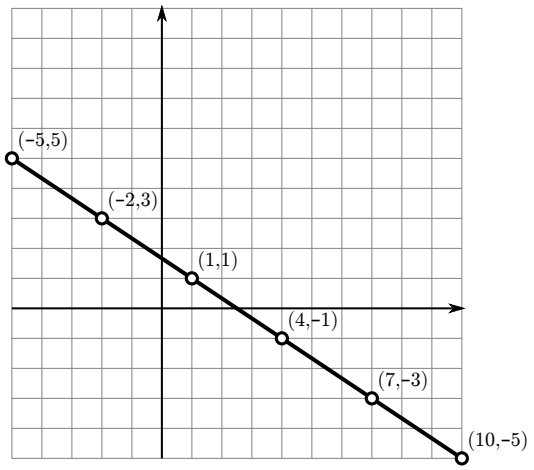
3.12. Példa. Oldjuk meg a $6x + 9y = 15$ diofantoszi egyenletet. Az euklideszi algoritmusból azt kapjuk, hogy $\operatorname{lnko}(6,9) = 3 = 6 \cdot (-1) + 9 \cdot 1$. Szorozzuk be mindkét oldalt 5-tel: $15 = 6 \cdot (-5) + 9 \cdot 5$. Ebből látható, hogy $x_0 = -5, y_0 = 5$ egy partikuláris megoldása az egyenletünknek. Az általános megoldás képlete (az $a = 6, b = 9$ „szereposztással”):

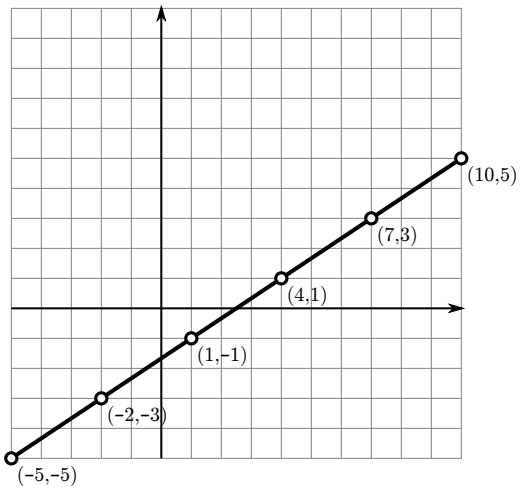
$$x_t = -5 + \frac{9}{3}t = -5 + 3t, \quad y_t = 5 - \frac{6}{3}t = 5 - 2t \qquad (t \in \mathbb{Z}).$$

3.13. Megjegyzés. A kapott megoldások nem mások, mint azon rácspontok koordinátái, amelyek illeszkednek a $6x + 9y = 15$ egyenletű egyenesre (lásd az ábrán a bal oldali grafikont). Az egyenes meredeksége $-\frac{2}{3}$, ezért egy rácspontból a következőbe úgy jutunk, hogy 3-at lépünk jobbra, és 2-t lépünk lefelé. Figyeljük meg, hogy az általános megoldás képletének éppen ez a szemléletes jelentése.
Az euklideszi algoritmus nélkül is könnyen kitalálhattuk volna, hogy $x = 1, y = 1$ megoldása az egyenletnek. Ha ebből a partikuláris megoldásból indultunk volna ki (azaz $x_0 = 1, y_0 = 1$), akkor így festene az általános megoldás képlete:

$$x_t = 1 + 3t, \quad y_t = 1 - 2t \qquad (t \in \mathbb{Z}).$$

Ez látszólag nem egyezik meg a 3.12. Példában kapott eredménnyel, de valójában a két képlet ugynazt a végtelen számpárhalmazt írja le, csak a t paraméterek el vannak csúsztatva egymáshoz képest. (Például a $(7, -3)$ megoldás ott $t = 4$-gyel jön ki, itt pedig $t = 2$-vel.)





3.14. Megjegyzés. Világos, hogy az egyenlet jobb oldalán 15 helyett bármilyen 3-mal osztható számot írva, az egyenletnek lesz megoldása (és egy megoldást megkaphatunk az euklideszi algoritmusból levezetett $\text{lnko}(6,9) = 3 = 6 \cdot (-1) + 9 \cdot 1$ összefüggésből). Ha viszont 15 helyébe 3-mal nem osztható számot írunk, akkor nem lesz megoldás, mert $6x + 9y$ mindig osztható 3-mal (ha x és y egész számok).

3.15. Példa. Oldjuk meg a $6x - 9y = 15$ diofantoszi egyenletet. Szorozzuk be ismét az euklideszi algoritmusból kapott $3 = 6 \cdot (-1) + 9 \cdot 1$ egyenlőség mindkét oldalát 5-tel, és alakítsuk az előjeleket úgy, hogy $6x - 9y$ alakú kifejezést kapjunk: $15 = 6 \cdot (-5) - 9 \cdot (-5)$. Ebből látható, hogy $x_0 = -5, y_0 = -5$ egy partikuláris megoldása az egyenletünknek. Az általános megoldás képlete (az $a = 6, b = -9$ „szereposztással”):

$$x_t = -5 + \frac{-9}{3}t = -5 - 3t, \quad y_t = -5 - \frac{6}{3}t = -5 - 2t \qquad (t \in \mathbb{Z}).$$

Az általános megoldás így is felírható, ha a legkisebb pozitív megoldást választjuk kiindulópontnak:

$$x_t = 4 - 3t, \quad y_t = 1 - 2t \qquad (t \in \mathbb{Z}).$$

3.16. Megjegyzés. Figyeljük meg, hogy a fenti képletben t előjele x_t-nél is és y_t-nél is negatív. Ez nem meglepő, hiszen a $6x - 9y = 15$ egyenletű egyenes meredeksége pozitív, tehát csökkenő x értékekhez csökkenő y értékek tartoznak. Helyes lenne az általános megoldás ebben a formában is:

$$x_t = 4 + 3t, \quad y_t = 1 + 2t \qquad (t \in \mathbb{Z}).$$

Ez csak abban különbözik a 3.15. Példában másodikként felírt megoldástól, hogy t helyébe $-t$-t írunk, azaz a rácspontokat nem balra lefelé, hanem jobbra felfelé indexezzük.

Kongruenciareláció

3.17. Definíció. Legyen $m \in \mathbb{N}_0$ és $a, b \in \mathbb{Z}$. Ha $a - b$ osztható m-mel, akkor azt mondjuk, hogy a ***kongruens*** b***-vel modulo*** m. Az m számot a kongruencia ***modulusának*** nevezzük.

3.18. Megjegyzés. A modulo 0 és a modulo 1 kongruencia nem túl érdekes: $a \equiv b \pmod{1}$ minden $a, b \in \mathbb{Z}$ esetén teljesül, $a \equiv b \pmod{0}$ pedig csak akkor, ha $a = b$ (ugye?). Ezért többnyire csak olyan kongruenciákkal foglalkozunk, ahol a modulus legalább 2.

Jelölés. A kongruenciát $\equiv$ jelöli, a modulust utána zárójelben tüntetjük fel a „mod” rövidítést használva (de ezt időnként elhagyjuk). Tehát $a \equiv b \pmod{m} \iff m \mid a - b$.

3.19. Tétel. Tetszőleges $m \geq 2, a, b \in \mathbb{Z}$ esetén $a \equiv b \pmod{m}$ akkor és csak akkor teljesül, ha a és b ugyanazt a maradékot adja m-mel osztva.

Bizonyítás. Osszuk el a-t és b-t maradékosan m-mel: $a = mq_1 + r_1$ és $b = mq_2 + r_2$, ahol $0 \leq r_1, r_2 \leq m - 1$. Ekkor

$$a \equiv b \pmod{m} \iff m \mid a - b \iff m \mid m(q_1 - q_2) + (r_1 - r_2) \iff m \mid r_1 - r_2 \quad \text{(miért?)}.$$

Az $r_1 - r_2$ szám a $\{-(m-1), -(m-2), \ldots, m-2, m-1\}$ halmazba esik (miért?), márpedig ebben a halmazban csak egyetlen m-mel osztható szám van, nevezetesen a nulla (ugye?). Azt kaptuk tehát, hogy $a \equiv b \pmod{m} \iff r_1 - r_2 = 0$, és éppen ezt kellett igazolnunk. □

3.20. Példa.

- $2021 \equiv 2035 \pmod 7$, mert $2035 - 2021 = 14$ osztható 7-tel.
- $12345 \not\equiv 6789 \pmod 9$, mert 9-cel osztva 12345 maradéka 6, míg 6789 maradéka 3.
- $23 \equiv 4677863 \equiv -34267467 \not\equiv -497973413 \pmod{10}$.

3.21. Tétel. Tetszőleges $m, m_1, m_2 \geq 2, a, b, c, a_1, b_1, a_2, b_2 \in \mathbb{Z}$ esetén érvényesek az alábbiak:

(1) $a \equiv a \pmod m$ (reflexivitás);

(2) $a \equiv b \pmod m \implies b \equiv a \pmod m$ (szimmetria);

(3) $(a \equiv b \pmod m$ és $b \equiv c \pmod m) \implies a \equiv c \pmod m$ (tranzitivitás);

(4) $\left.\begin{array}{l} a_1 \equiv b_1 \pmod m \\ a_2 \equiv b_2 \pmod m \end{array}\right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2,\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m$;

(5) ha $c \neq 0$, akkor $ca \equiv cb \pmod m \iff a \equiv b \left(\mathrm{mod}\ \frac{m}{\mathrm{lnko}(m,c)}\right)$;

(6) ha $m \perp c$, akkor $ca \equiv cb \pmod m \iff a \equiv b \pmod m$;

(7) $\left.\begin{array}{l} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{array}\right\} \iff a \equiv b \pmod{[m_1, m_2]}$;

(8) ha $a \equiv b \pmod m$, akkor $\mathrm{lnko}(a, m) \sim \mathrm{lnko}(b, m)$.

Bizonyítás. A bizonyítások során minden kongruenciát a definíció alapján átírunk oszthatóságra, majd használjuk az oszthatóság ismert tulajdonságait.

(1) $a \equiv a \pmod m \iff m \mid a - a \iff m \mid 0$, ez pedig minden m-re teljesül (ugye?).

(2) $a \equiv b \pmod m \implies m \mid a - b \implies m \mid -(a-b) = b - a \implies b \equiv a \,(\mathrm{mod}\, m)$.

(3) $(a \equiv b \,(\mathrm{mod}\ m)\,\text{és}\, b \equiv c \,(\mathrm{mod}\ m)) \implies (m \mid a-b \,\text{és}\, m \mid b-c) \implies m \mid (a-b)+(b-c) = a-c \implies a \equiv c \,(\mathrm{mod}\ m)$.

(4) Tfh. $a_1 \equiv b_1 \pmod m$ és $a_2 \equiv b_2 \pmod m$, azaz $m \mid a_1 - b_1$ és $m \mid a_2 - b_2$. Nézzük először az összegre vonatkozó állítást:

$$a_1 + a_2 \equiv b_1 + b_2 \pmod m \iff m \mid (a_1 + a_2) - (b_1 + b_2) \iff m \mid (a_1 - b_1) + (a_2 - b_2),$$

és ez utóbbi nyilván teljesül, mert feltevésünk szerint az összeg mindkét tagja osztható m-mel. A kivonásra vonatkozó állítás hasonlóan egyszerű.
A szorzásnál már be kell „csempészni" egy trükkösen $-a_1b_2 + a_1b_2$ alakban írt nullát:

$$\begin{aligned} a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m &\iff m \mid a_1a_2 - b_1b_2 \\ &\iff m \mid a_1a_2 - a_1b_2 + a_1b_2 - b_1b_2 = a_1(a_2 - b_2) + (a_1 - b_1)b_2. \end{aligned}$$

Az utolsó kifejezés osztható m-mel, mert mindkét tagban szerepel egy m-mel osztható tényező (ugye?).

(5) Ez gyakorlatilag Euklidész lemmája „álruhában" :

$$\begin{aligned} ca \equiv cb \pmod m &\iff m \mid ca - cb = c(a-b) \\ &\iff \frac{m}{\mathrm{lnko}(m,c)} \,\Big|\, a - b \\ &\iff a \equiv b \left(\mathrm{mod}\ \frac{m}{\mathrm{lnko}(m,c)}\right). \end{aligned}$$

(Hol használtuk ki azt, hogy $c \neq 0$? A fenti levezetés melyik lépésénél lenne baj, ha $c = 0$ lenne?)

(6) Ez speciális esete az előzőnek.

(7) Az $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2}$ kongruenciák azt jelentik, hogy $m_1, m_2 \mid a - b$, vagyis $a - b$ egy közös többszöröse m_1-nek és m_2-nek. A legkisebb közös többszörös definíciója szerint ez azzal ekvivalens, hogy $a - b$ többszöröse $[m_1, m_2]$-nek, azaz $[m_1, m_2] \mid a - b$. A kongruencia definíciója alapján ez azt jelenti, hogy $a \equiv b \pmod{[m_1, m_2]}$. (Hasonlóan lehet „összeolvasztani" kettőnél több kongruenciát is, ha azok csak a modulusaikban különböznek.)

(8) Hajtsuk végre gondolatban az euklideszi algoritmust az (a, m) számpárra. Az első lépésben a-t osztjuk m-mel maradékosan; legyen a maradék r. A második (és minden további) lépésben az a szám már nem szerepel, csak m és r. Ha a (b, m) számpárra hajtjuk végre az euklideszi algoritmust, akkor (a 3.19. Tétel szerint) az első lépésben megint r lesz a maradék, hiszen $a \equiv b \,(\mathrm{mod}\, m)$. Tehát a második lépéstől kezdve a két algoritmus megegyezik, így a végeredményük is ugyanaz lesz: $\mathrm{lnko}(a, m) \sim \mathrm{lnko}(b, m)$.
Egy másik bizonyítás, az euklideszi algoritmus felhasználása nélkül: Ha $a \equiv b \pmod m$, akkor $b = a + mt$ alkalmas t egész számmal (miért?). Ebből látszik, hogy ha k egy tetszőleges közös osztója a-nak és m-nek, akkor k osztója b-nek is (ugye?) és így közös osztója b-nek és m-nek. Hasonlóan belátható, hogy $\forall k \in \mathbb{Z}$: $k \mid b, m \implies k \mid a, m$, tehát a és m közös osztói ugyanazok, mint b és m közös osztói. Ebből pedig már következik, hogy $\mathrm{lnko}(a, m) \sim \mathrm{lnko}(b, m)$ (miért?). □

3.22. Megjegyzés. A fenti tételbeli (1)–(3) tulajdonságok szerint a modulo m kongruencia ekvivalenciareláció az egész számok halmazán. Itt az ekvivalenciaosztályokat ***maradékosztályoknak*** nevezzük. Ezt a három tulajdonságot levezethettük volna a 2.7. Állításból is, hiszen a 3.19. Tétel szerint a modulo m kongruenciareláció nem más, mint annak a leképezésnek a magja, ami minden egész számhoz az m-mel adott osztási maradékát rendeli.

3.23. Példa. A $10 \equiv -1 \pmod{11}$ kongruenciát önmagával k-szor megszorozva (a 3.21. Tételben szereplő (4) tulajdonság szorzásra vonatkozó részét alkalmazva) azt kapjuk, hogy $10^k \equiv (-1)^k \pmod{11}$ minden $k \in \mathbb{N}_0$ esetén. Ebből, ismét a (4)-es tulajdonságot használva (most már nemcsak a szorzásra, hanem az összeadásra vonatkozó részt is) levezethetjük a 11-gyel való oszthatóság szabályát:

$$\begin{aligned}\overline{a_n \cdots a_2 a_1 a_0} &= a_0 + 10 \cdot a_1 + 10^2 \cdot a_2 + \cdots + 10^n \cdot a_n \\ &\equiv a_0 + (-1) \cdot a_1 + (-1)^2 \cdot a_2 + \cdots + (-1)^n \cdot a_n \\ &= a_0 - a_1 + a_2 - \cdots \pm a_n \pmod{11}.\end{aligned}$$

Lineáris kongruenciák és multiplikatív inverzek

3.24. Definíció. ***Lineáris kongruenciának*** nevezzük az $ax \equiv b \pmod{m}$ alakú „egyenletet” , ahol a, b, m adott egész számok, és az x ismeretlent is az egész számok körében keressük.

3.25. Példa. Oldjuk meg a $6x \equiv 15 \pmod{9}$ lineáris kongruenciát. A kongruencia definíciója (3.17. Definíció) szerint $6x \equiv 15 \pmod{9} \iff 9 \mid 6x - 15$. Ez az oszthatóság pedig azt jelenti, hogy $6x - 15 = 9y$ alkalmas y egész számmal. A kongruenciát tehát sikerült átfogalmaznunk a $6x - 9y = 15$ diofantoszi egyenletté. Ezt már korábban megoldottuk (lásd a 3.15. Példát): azt kaptuk, hogy az általános megoldás $x_t = -5 - 3t$ $(t \in \mathbb{Z})$. (Most csak az x-re vonatkozó részt írtuk fel az általános megoldásból, mert y-ra nincs szükségünk.) Tehát x akkor és csak akkor megoldása a kongruenciánknak, ha előáll $-5 - 3t$ alakban alkalmas t egész számmal. Ez pedig pontosan akkor teljesül, ha $3 | x - (-5)$, azaz $x \equiv -5 \pmod{3}$ (ugye?). Mivel $-5 \equiv 1 \pmod{3}$, a megoldást így is felírhatjuk: $x \equiv 1 \pmod{3}$.

3.26. Tétel. Tekintsük tetszőleges adott a, b, m $(m \geq 2)$ egész számok esetén az $ax \equiv b \pmod{m}$ lineáris kongruenciát.

(i) A kongruenciának akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a, m) \mid b$.

(ii) Ha van megoldás, akkor egyetlen megoldás van modulo $\frac{m}{\operatorname{lnko}(a,m)}$.

(iii) Az eredeti m modulusra vonatkozóan $\operatorname{lnko}(a, m)$ különböző megoldás van. Ha x_0 egy megoldás, akkor az általános megoldás:

$$x \equiv x_0 + t \cdot \frac{m}{\operatorname{lnko}(a, m)} \pmod{m} \quad (t = 0, 1, \ldots, \operatorname{lnko}(a, m) - 1).$$

Bizonyítás. A kongruencia és az oszthatóság definícióját használva átírhatjuk a lineáris kongruenciát egy kétismeretlenes lineáris diofantoszi egyenletté:

$$ax \equiv b \pmod{m} \iff m \mid ax - b \iff \exists y \in \mathbb{Z}\colon ax - b = my \iff \exists y \in \mathbb{Z}\colon ax - my = b.$$

Tehát x akkor és csak akkor megoldása a lineáris kongruenciánknak, ha van olyan y egész szám, amelyre (x, y) megoldása az $ax - my = b$ diofantoszi egyenletnek. Így nincs más dolgunk, mint alkalmazni erre az egyenletre a 3.11. Tételt. A képleteket egyszerűbb lesz felírni, ha bevezetjük a $d = \operatorname{lnko}(a, m)$ jelölést.

(i) Az $ax - my = b$ diofantoszi egyenletnek akkor és csak akkor van megoldása, ha $d \mid b$.

(ii) Ha (x_0, y_0) egy megoldása az egyenletnek, akkor az általános megoldás (csak az x-re vonatkozó formulát írjuk fel, mert y-ra nincs szükségünk): $x_t = x_0 + \frac{m}{d} \cdot t$ $(t \in \mathbb{Z})$. A lineáris kongruenciánk megoldáshalmaza tehát $M := \left\{x_0 + \frac{m}{d} \cdot t : t \in \mathbb{Z}\right\}$, ez pedig szemlátomást egy modulo $\frac{m}{d}$ maradékosztály.

(iii) Láttuk, hogy a megoldások mind ugyanazt a maradékot adják modulo $\frac{m}{d}$; most nézzük meg, hogy a t paraméter különböző értékeire hányféle maradékot kaphatunk modulo m. Tekintsünk két tetszőleges $t_1, t_2 \in \mathbb{Z}$ értéket, és vizsgáljuk meg, hogy mikor lesz x_{t_1} és x_{t_2} kongruens egymással modulo m:

$$\begin{aligned}x_{t_1} \equiv x_{t_2} \pmod{m} &\iff x_0 + \frac{m}{d} \cdot t_1 \equiv x_0 + \frac{m}{d} \cdot t_2 \pmod{m} \\ &\iff \frac{m}{d} \cdot t_1 \equiv \frac{m}{d} \cdot t_2 \pmod{m} \\ &\iff t_1 \equiv t_2 \pmod{\frac{m}{\operatorname{lnko}(m, \frac{m}{d})}} \\ &\iff t_1 \equiv t_2 \pmod{\frac{m}{\frac{m}{d}}} \\ &\iff t_1 \equiv t_2 \pmod{d}.\end{aligned}$$

Tehát két megoldás akkor és csak akkor kongruens egymással modulo m, ha a felírásukban szereplő t paraméterek kongruensek modulo d. Ezért a megoldások annyiféle maradékot „tudnak” adni m-mel osztva, ahányféle maradékot egy tetszőleges t egész szám adhat d-vel osztva. Utóbbira nyilván d lehetőség van, és minden lehetséges maradékot megkapunk, ha a t paramétert 0-tól $(d-1)$-ig futtatjuk. Tehát az $ax \equiv b \pmod{m}$ lineáris kongruencia általános megoldása: $x \equiv x_t \pmod{m}$ $(t = 0, 1, \ldots, d-1)$, és éppen ezt kellett igazolnunk. □

3.27. Példa. A 3.25. Példában szereplő kongruenciát megoldhatjuk tisztán „kongruenciás” számolással, diofantoszi egyenletre való átírás nélkül is (ellenőrizzük, hogy minden lépésben ekvivalens átalakítást végzünk!):

$$\begin{aligned} 6x &\equiv 15 \pmod 9 \\ 6x &\equiv 6 \pmod 9 && \text{(mert } 15 \equiv 6 \pmod 9\text{)} \\ x &\equiv 1 \pmod 3 && \text{(lásd a 3.21. Tételbeli (5) tulajdonságot)} \end{aligned}$$

Tehát a kongruencia megoldásai a $3t+1$ ($t \in \mathbb{Z}$) alakú számok. Ezek 9-cel osztva háromféle maradékot adhatnak: 1-et, 4-et vagy 7-et, ezért az eredeti modulus szerint három megoldása van a kongruenciánknak: $x \equiv 1, 4, 7 \pmod 9$.

3.28. Definíció. Az a és b egész számok egymás ***multiplikatív inverzei modulo*** m, ha $ab \equiv 1 \pmod m$.

Jelölés. Ha nem fenyeget a félreértés veszélye, akkor az a egész szám $\bmod m$ multiplikatív inverzét a^{-1}-gyel jelöljük.

3.29. Tétel. Az a egész számnak akkor és csak akkor van multiplikatív inverze modulo m, ha $a \perp m$. Ilyenkor a multiplikatív inverz $\bmod m$ egyértelműen meghatározott.

Bizonyítás. Ez gyakorlatilag speciális esete az 3.26. Tételnek: amikor a modulo m multiplikatív inverzét keressük, akkor az $ax \equiv 1 \pmod m$ lineáris kongruenciát kell megoldanunk. Az 3.26. Tétel szerint ennek akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a,m) \mid 1$, vagyis, ha $a \perp m$. Ha ez teljesül, akkor a megoldások $\operatorname{lnko}(a,m)$-féle maradékot adnak m-mel osztva. Mivel $\operatorname{lnko}(a,m) = 1$, ez azt jelenti, hogy modulo m egyetlen megoldás van. □

3.30. Példa. A multiplikatív inverz egy lineáris kongruencia megoldásaként kapható meg. Másrészt, a multiplikatív inverz segíthet lineáris kongruenciák megoldásában is. Például a $3x \equiv 1 \pmod 7$ lineáris kongruenciát megoldva azt kapjuk, hogy 3 multiplikatív inverze 5 modulo 7 (ugye?). Ha ezt már tudjuk, akkor könnyen megoldhatjuk pl. a $3x \equiv 4 \pmod 7$ lineáris kongruenciát úgy, hogy mindkét oldalt beszorozzuk 5-tel (miért lesz ez ekvivalens átalakítás?): $15x \equiv 20 \pmod 7$. Ez a kongruencia már „meg van oldva”, hiszen $15 \equiv 1 \pmod 7$ miatt a bal oldalon csak $1 \cdot x$ áll: $x \equiv 6 \pmod 7$.

Lineáris kongruenciarendszerek

3.31. Definíció. Adott a_i, b_i, n_i ($i = 1, \dots, k$) egész számok esetén az alábbi „egyenletrendszert” ***lineáris kongruenciarendszernek*** nevezzük (az x ismeretlent is természetesen az egész számok körében keressük):

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ &\vdots \\ a_k x &\equiv b_k \pmod{n_k} \end{aligned}\right\}.$$

3.32. Megjegyzés. A 3.26. Tétel segítségével a kongruenciarendszerbeli kongruenciákat külön-külön megoldhatjuk (ha van megoldásuk), és így a kongruenciarendszert a következő alakra hozhatjuk:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}\right\}. \qquad (*)$$

3.33. Példa. Oldjuk meg az alábbi lineáris kongruenciarendszert:

$$\left.\begin{aligned} x &\equiv 7 \pmod 6 \\ x &\equiv 22 \pmod 9 \end{aligned}\right\}$$

Fogalmazzuk át mindkét kongruenciát oszthatóságra, majd „milyen alakú szám x” típusú állításra:

$$\begin{aligned} x \equiv 7 \pmod 6 &\iff 6 \mid x-7 \iff \exists y \in \mathbb{Z}\colon x = 6y+7; \\ x \equiv 22 \pmod 9 &\iff 9 \mid x-22 \iff \exists z \in \mathbb{Z}\colon x = 9z+22. \end{aligned}$$

Az x-re kapott két kifejezést egyenlővé téve a $6y+7 = 9z+22$ diofantoszi egyenletet kaptuk, Ez lényegében ugyanaz, mint a 3.15. Példában megoldott egyenlet, a megoldása tehát $y = 4+3t$, $z = 1+2t$ ($t \in \mathbb{Z}$). Ebből kifejezhetjük x-et: $x = 6y+7 = 6\cdot(4+3t)+7 = 18t+31$ (ugyanezt megkaphattuk volna z-ből is). Tehát a kongruenciarendszer megoldásai az $x = 18t+31$ ($t \in \mathbb{Z}$) alakú számok, vagyis x akkor és csak akkor megoldás, ha $x \equiv 31 \pmod{18}$ (ugye?). Mivel $31 \equiv 13 \pmod{18}$, a megoldást így is felírhatjuk $x \equiv 13 \pmod{18}$.

3.34. Tétel. A $(*)$ lineáris kongruenciarendszernek $k = 2$ esetén pontosan akkor van megoldása, ha $\operatorname{lnko}(m_1, m_2) \mid c_1 - c_2$. Ha van megoldás, akkor a megoldások egyetlen maradékosztályt alkotnak modulo $[m_1, m_2]$, vagyis az általános megoldás ilyen alakú: $x \equiv s \pmod{[m_1, m_2]}$.

Bizonyítás. Mindkét kongruenciát átfogalmazzuk a kongruenciareláció és az oszthatósági reláció definíciója alapján:

$$\begin{aligned} x \equiv c_1 \pmod{m_1} &\iff m_1 \mid x-c_1 \iff \exists y_1 \in \mathbb{Z}\colon x = y_1 m_1 + c_1; \\ x \equiv c_2 \pmod{m_2} &\iff m_2 \mid x-c_2 \iff \exists y_2 \in \mathbb{Z}\colon x = y_2 m_2 + c_2. \end{aligned}$$

Tehát a kongruenciarendszerünknek akkor és csak akkor van megoldása, ha léteznek olyan y_1, y_2 egész számok, amelyekre $y_1m_1 + c_1 = y_2m_2 + c_2$ (ekkor $x = y_1m_1 + c_1$ megoldása a kongruenciarendszernek). Átrendezve, azt kapjuk, hogy $y_1m_1 - y_2m_2 = c_2 - c_1$. Ennek a kétismeretlenes diofantoszi egyenletnek a 3.11. Tétel szerint akkor és csak akkor van megoldása, ha $\text{lnko}(m_1, m_2) \mid c_2 - c_1$, tehát ez a kongruenciarendszer megoldhatóságának feltétele. A tétel második állítása megkapható a diofantoszi egyenlet általános megoldásának felírásával, de rögtön következik a A 3.21. Tételben szereplő (7) tulajdonságból is. □

3.35. Tétel. Ha a $(*)$ lineáris kongruenciarendszernek van megoldása, akkor megoldásai egyetlen modulo $[m_1, \dots, m_k]$ maradékosztályt alkotnak.

Bizonyítás. Tfh. s egy megoldása a kongruenciarendszernek. Ekkor minden $i \in \{1, \dots, k\}$ esetén az $x \equiv c_i \pmod{m_i}$ kongruencia ekvivalens az $x \equiv s \pmod{m_i}$ kongruenciával, hiszen $s \equiv c_i \pmod{m_i}$ (ugye?). Tehát a $(*)$ kongruenciarendszer ekvivalens a következővel:

$$\left.\begin{array}{r} x \equiv s \pmod{m_1} \\ \vdots \\ x \equiv s \pmod{m_k} \end{array}\right\}.$$

A 3.21. Tételben szereplő (7) tulajdonság alapján ez a kongruenciarendszer ekvivalens az $x \equiv s \pmod{[m_1, \dots, m_k]}$ kongruenciával, amelynek megoldáshalmaza nyilván egyetlen $\text{mod}[m_1, \dots, m_k]$ maradékosztály. □

3.36. Tétel. A $(*)$ lineáris kongruenciarendszernek akkor és csak akkor van megoldása, ha bármely két kongruenciából álló részrendszerének van megoldása, azaz $\forall i, j: \ \text{lnko}(m_i, m_j) \mid c_i - c_j$. Speciálisan, páronként relatív prím modulusok esetén mindig van megoldás.

Bizonyítás. A feltétel szükségessége nyilvánvaló (ugye?), az elegendőség viszont egyáltalán nem az, de nem bizonyítjuk be. □

3.37. Tétel (kínai maradéktétel). Ha a $(*)$ kongruenciarendszerben a modulusok páronként relatív prímek (azaz $i \neq j$ esetén $\text{lnko}(m_i, m_j) = 1$), akkor mindig van megoldás, és a megoldás megkapható a következő módon. Tekintsük azt a kongruenciarendszert, amelyet úgy kapunk $(*)$-ból, hogy az i-edik sorban a jobb oldalra 1-et írunk, a többi sorban pedig 0-t:

$$\left.\begin{array}{r} x \equiv 0 \pmod{m_1} \\ \vdots \\ x \equiv 1 \pmod{m_i} \\ \vdots \\ x \equiv 0 \pmod{m_k} \end{array}\right\} \qquad (*_i)$$

Ennek a kongruenciarendszernek van megoldása; jelölje e_i egy tetszőleges megoldását $(i = 1, \dots, k)$. Ekkor az eredeti $(*)$ kongruenciarendszer általános megoldása:

$$x \equiv c_1e_1 + \dots + c_ke_k \pmod{m_1 \cdots m_k}.$$

Bizonyítás. Az m_i modulusok páronként relatív prímek, ezért a legkisebb közös többszörösük $[m_1, \dots, m_k] = m_1 \cdot \ldots \cdot m_k$. Legyen M_i az i-edik modulust kivéve a többiek legkisebb közös többszöröse: $M_i := m_1 \cdot \ldots m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_k$. A $(*_i)$ kongruenciarendszer ekvivalens az alábbival (miért?):

$$\left.\begin{array}{r} x \equiv 0 \pmod{M_i} \\ x \equiv 1 \pmod{m_i} \end{array}\right\}$$

Mivel $M_i \perp m_i$, a 3.34. Tétel szerint ennek a kongruenciarendszernek van megoldása (miért?). Ha e_i egy megoldás, akkor $(*_i)$ alapján $e_i \equiv 1 \pmod{m_i}$, és minden $j \neq i$ esetén $e_i \equiv 0 \pmod{m_j}$ (ugye?). Az e_i számoknak ezt a tulajdonságát felhasználva ellenőrizzük, hogy az $s := c_1e_1 + \dots + c_ke_k$ szám megoldása a kongruenciarendszernek:

$$\begin{aligned} s &= c_1e_1 + \dots + c_{i-1}e_{i-1} + c_ie_i + c_{i+1}e_{i+1} + \dots + c_ke_k \\ &\equiv c_1 \cdot 0 + \dots + c_{i-1} \cdot 0 + c_i \cdot 1 + c_{i+1} \cdot 0 + \dots + c_k \cdot 0 \equiv c_i \pmod{m_i}. \end{aligned}$$

Tehát s kielégíti az i-edik kongruenciát minden i-re, azaz megoldása a kongruenciarendszernek. A 3.35 . Tétel szerint a kongruenciarendszer általános megoldása $x \equiv s \pmod{[m_1, \dots, m_k]}$, és épp ezt kellett igazolnunk. □

3.38. Példa. Oldjuk meg a kínai maradéktétel segítségével az alábbi paraméteres kongruenciarendszert.

$$\left.\begin{array}{r} x \equiv c_1 \pmod{3} \\ x \equiv c_2 \pmod{4} \\ x \equiv c_3 \pmod{5} \end{array}\right\}$$

Írjuk fel a három segéd-kongruenciarendszert:

$$\begin{array}{l|l|l} x \equiv 1 \pmod 3 & x \equiv 0 \pmod 3 & x \equiv 0 \pmod 3 \\ x \equiv 0 \pmod 4 & x \equiv 1 \pmod 4 & x \equiv 0 \pmod 4 \\ x \equiv 0 \pmod 5 & x \equiv 0 \pmod 5 & x \equiv 1 \pmod 5 \end{array}$$

Mindegyikben a két 0 jobb oldalú kongruenciát „összeolvasztjuk” egyetlen kongruenciává:

$$\begin{array}{l|l|l} x \equiv 0 \pmod{20} & x \equiv 0 \pmod{15} & x \equiv 0 \pmod{12} \\ x \equiv 1 \pmod 3 & x \equiv 1 \pmod 4 & x \equiv 1 \pmod 5 \end{array}$$

A segéd-kongruenciarendszerek megoldásai:

$$\begin{array}{l|l|l} x \equiv 40 \pmod{60} & x \equiv 45 \pmod{60} & x \equiv 36 \pmod{60} \end{array}$$

Legyen tehát $e_1 = 40,\ e_2 = 45,\ e_3 = 36$, és így az eredeti kongruenciarendszer megoldása:

$$x \equiv 40 \cdot c_1 + 45 \cdot c_2 + 36 \cdot c_3 \pmod{60}.$$

Maradékosztályok

3.39. Definíció. Egy a egész szám modulo m ***maradékosztályán*** az $\overline{a} = \{b \in \mathbb{Z} : a \equiv b \pmod m\}$ halmazt értjük (vagyis az a elemnek a modulo m kongruenciareláció szerinti ekvivalenciaosztályát).

3.40. Megjegyzés. Az $\overline{a}$ jelölés nem utal a modulusra, de a szövegkörnyezetből mindig világosnak kell lennie, hogy mi a modulus. A definícióból (vagy a 2.13. Állításból) látható, hogy tetszőleges $a, b \in \mathbb{Z}$ esetén $\overline{a} = \overline{b} \iff a \equiv b \pmod m$.

Jelölés. A modulo m maradékosztályok halmazát $\mathbb{Z}_m$ jelöli. Tehát $\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

3.41. Példa. A modulo 3 maradékosztályok:

$$\overline{0} = \{\ldots, -3, 0, 3, 6, \ldots\} = \{3k : k \in \mathbb{Z}\},$$
$$\overline{1} = \{\ldots, -2, 1, 4, 7, \ldots\} = \{3k+1 : k \in \mathbb{Z}\},$$
$$\overline{2} = \{\ldots, -1, 2, 5, 8, \ldots\} = \{3k+2 : k \in \mathbb{Z}\}.$$

3.42. Definíció. Modulo m ***teljes maradékrendszernek*** nevezzük egész számok egy olyan rendszerét, amely minden mod m maradékosztályból pontosan egy elemet tartalmaz. Tehát $c_1, \ldots, c_m$ akkor és csak akkor teljes maradékrendszer modulo m, ha $\{\overline{c_1}, \ldots, \overline{c_m}\} = \mathbb{Z}_m$.

3.43. Példa. A „standard” modulo 3 teljes maradékrendszer $0, 1, 2$. Ezen kívül van még (végtelen) sok teljes maradékrendszer, például $2021, 2022, 2023$ és $239, -584, 729$ is teljes maradékrendszerek modulo 3 (ugye?).

3.44. Állítás. Ha a $c_1, \ldots, c_m$ egész számok teljes maradékrendszert alkotnak modulo m, és $a, b \in \mathbb{Z}, a \perp m$, akkor $ac_1 + b, \ldots, ac_m + b$ is teljes maradékrendszer modulo m.

Bizonyítás. Tfh. $c_1, \ldots, c_m$ teljes maradékrendszer modulo m, és nézzük meg, hogy az $ac_1 + b, \ldots, ac_m + b$ számok között vannak-e olyanok, amelyek kongruensek egymással modulo m (a számolás során a kongruenciareláció 3.21. Tételben felsorolt tulajdonságait használjuk):

$$ac_i + b \equiv ac_j + b \pmod m \iff ac_i \equiv ac_j \pmod m \iff c_i \equiv c_j \pmod m.$$

(Vegyük észre, hogy az utolsó lépésben kihasználtuk azt, hogy $a \perp m$.) Tudjuk, hogy $c_1, \ldots, c_m$ páronként inkongruensek modulo m, így $c_i \equiv c_j \pmod m$ csak $i = j$ esetén lehetséges. Ez pedig a fenti számolás alapján azt jelenti, hogy az $ac_1 + b, \ldots, ac_m + b$ számok is páronként inkongruensek modulo m, vagyis minden maradékosztályból legfeljebb egy elem szerepelhet közöttük. Mivel a maradékosztályok száma is éppen m, a skatulya-elvből adódik, hogy minden maradékosztályból fel is lép egy szám. Ezzel beláttuk, hogy $ac_1 + b, \ldots, ac_m + b$ teljes maradékrendszer modulo m. □

3.45. Definíció. A modulo m maradékosztályok halmazán értelmezzük az összeadást és a szorzást a következőképpen: tetszőleges $a, b \in \mathbb{Z}$ esetén legyen $\overline{a} \oplus \overline{b} = \overline{a+b},\ \overline{a} \odot \overline{b} = \overline{a \cdot b}$.

3.46. Tétel. A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik számot választjuk reprezentánsnak. Ezekkel a műveletekkel $\mathbb{Z}_m$ kommutatív egységelemes gyűrűt alkot (modulo m ***maradékosztály-gyűrű***).

Bizonyítás. Az $\overline{a}$ és $\overline{b}$ maradékosztályok összege a fenti definíció szerint $\overline{a} \oplus \overline{b} = \overline{a+b}$. Vegyünk az $\overline{a}$ maradékosztályból egy másik elemet, legyen ez a_1. Az, hogy a és a_1 ugyanabba a modulo m maradékosztályba tartoznak, azt jelenti, hogy $a \equiv a_1 \pmod m$. Hasonlóan, vegyünk egy $b_1 \in \overline{b}$ számot; ekkor $b \equiv b_1 \pmod m$. Ismét a 3.45 Definíciót használva, azt kapjuk, hogy $\overline{a_1} \oplus \overline{b_1} = \overline{a_1 + b_1}$. Node itt ugyanazt a két maradékosztályt adtuk össze mint az előbb (hiszen $\overline{a} = \overline{a_1}$ és $\overline{b} = \overline{b_1}$), tehát nagy baj lenne, ha az eredmény más lenne! (Ekkor azt mondanánk, hogy $\oplus$ nem jóldefiniált a $\mathbb{Z}_m$ halmazon.) Szerencsére nincs baj: a kongruencia 3.21. Tételbeli (4)-es tulajdonsága szerint $a \equiv a_1 \pmod m$ és $b \equiv b_1 \pmod m$

maga után vonja, hogy $a+b \equiv a_1+b_1 \pmod m$. Ez azt jelenti, hogy $\overline{a+b}=\overline{a_1+b_1}$, vagyis két maradékosztály összege nem függ attól, hogy mely elemeikkel reprezentáljuk őket a számolás során ($a \oplus$ művelet jóldefiniált a $\mathbb{Z}_m$ halmazon). Hasonlóan lehet belátni, hogy $\odot$ is jóldefiniált művelet a modulo m maradékosztályok halmazán, így tehát van értelme a $(\mathbb{Z}_m;\oplus,\odot)$ algebrai struktúráról beszélni.

Azt állítjuk, hogy ez a struktúra egy kommutatív egységelemes gyűrű. Ehhez sok mindent kell ellenőrizni, csak az egyik legösszetettebbet, a disztributivitást részletezzük (a többi HF!). A (bal oldali) disztributivitáshoz azt kell belátni, hogy minden $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}_m$ esetén $\overline{a}\odot(\overline{b}\oplus\overline{c})=(\overline{a}\odot\overline{b})\oplus(\overline{a}\odot\overline{c})$. Induljunk ki a bal oldalból, és alkalmazzuk a 3.45 Definíciót előbb az összeadásra, majd a szorzásra: $\overline{a}\odot(\overline{b}\oplus\overline{c})=\overline{a}\odot\overline{b+c}=\overline{a\cdot(b+c)}$. Itt a „vonás” alatt már egész számokon végezzük a műveleteket (nem pedig maradékosztályokon), azt pedig tudjuk, hogy az egész számok körében teljesül a disztributivitás: $\overline{a\cdot(b+c)}=\overline{(a\cdot b)+(a\cdot c)}$. Most „visszafelé” alkalmazzuk a 3.45 Definíciót előbb az összeadásra, majd a szorzásra: $\overline{(a\cdot b)+(a\cdot c)}=\overline{a\cdot b}\oplus\overline{a\cdot c}=(\overline{a}\odot\overline{b})\oplus(\overline{a}\odot\overline{c})$. Ezzel beláttuk, hogy a $\odot$ művelet (balról) disztributív a $\oplus$ műveletre, és, amint említettük, a kommutatív egységelemes gyűrű definíciójában szereplő többi tulajdonságot is hasonlóan vissza lehet vezetni a $(\mathbb{Z};+,\cdot)$ gyűrű megfelelő tulajdonságaira. □

3.47. Megjegyzés. A $\oplus$ és $\odot$ jelöléseket csak ideiglenesen, a fenti bizonyítás erejéig használtuk, hogy meg tudjuk különböztetni $\mathbb{Z}_m$ műveleteit $\mathbb{Z}$ műveleteitől. Ezentúl elhagyjuk a „karikákat”, de a szövegkörnyezetből mindig világosnak kell lennie, hogy $+$, illetve $\cdot$ éppen az egész számok, vagy pedig a modulo m maradékosztályok összeadását, illetve szorzását jelöli-e.

3.48. Példa. Íme $\mathbb{Z}_4$ összeadó- és szorzótáblája:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

3.49. Példa. A $\mathbb{Z}_{21}$ maradékosztály-gyűrűben $\overline{12}+\overline{17}=\overline{29}=\overline{8}$, $\overline{12}-\overline{17}=\overline{-5}=\overline{16}$ és $\overline{9}\cdot\overline{5}=\overline{45}=\overline{3}$ (ugye?).

3.50. Definíció. Azt mondjuk, hogy az $\overline{a},\overline{b}\in\mathbb{Z}_m$ maradékosztályok egymás ***multiplikatív inverzei***, ha $\overline{a}\cdot\overline{b}=\overline{1}$.

Jelölés. Az $\overline{a}\in\mathbb{Z}_m$ maradékosztály multiplikatív inverzét $\overline{a}^{-1}$ jelöli.

3.51. Példa. A $\mathbb{Z}_{21}$ maradékosztály-gyűrűben $\overline{4}$ inverzének meghatározásához meg kell oldanunk a $4x\equiv 1 \pmod{21}$ kongruenciát. A megoldás $x\equiv 16 \pmod{21}$, tehát $\mathbb{Z}_{21}$-ben $\overline{4}^{-1}=\overline{16}$.

3.52. Tétel. Az $\overline{a}\in\mathbb{Z}_m$ maradékosztálynak akkor és csak akkor van multiplikatív inverze, ha $a\perp m$. Ilyenkor a multiplikatív inverz egyértelműen meghatározott.

Bizonyítás. Ez csak átfogalmazása a 3.29. Tételnek. □

3.53. Megjegyzés. A 3.21. Tételbeli utolsó állítás szerint van értelme egy $\bmod m$ maradékosztály és az m modulus legnagyobb közös osztójáról beszélni (hiszen nem függ a reprezentáns választásától). Amint a fenti tételből is látható, fontos szerepet játszanak azok a maradékosztályok, amelyek relatív prímek a modulushoz, ezért erre külön elnevezést és jelölést vezetünk be.

3.54. Definíció. Az $\overline{a}\in\mathbb{Z}_m$ maradékosztályt ***redukált maradékosztálynak*** hívjuk, ha $\operatorname{lnko}(a,m)\sim 1$.

Jelölés. A $\bmod m$ redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli. Tehát $\mathbb{Z}_m^*=\{\overline{a}\in\mathbb{Z}_m : a\perp m\}$.

3.55. Példa. A modulo 15 redukált maradékosztályok halmaza: $\mathbb{Z}_{15}^*=\{\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}\}$.

3.56. Következmény. A $\mathbb{Z}_m$ maradékosztály-gyűrű akkor és csak akkor test, ha m prímszám.

Bizonyítás. A „csak akkor” rész igazolásához tfh. m összetett szám, vagyis van nemtriviális faktorizációja: $m=a\cdot b$, ahol $1<a,b<m$. Ekkor se a se b nem osztható m-mel, azaz $\overline{a},\overline{b}\neq\overline{0}$, viszont $\overline{a}\cdot\overline{b}=\overline{ab}=\overline{m}=\overline{0}$ (ugye?). Ez azt jelenti, hogy $\overline{a}$ és $\overline{b}$ zérusosztók $\mathbb{Z}_m$-ben, tehát $\mathbb{Z}_m$ nem test (sőt még csak nem is integritástartomány).

Az „akkor” rész bizonyításához tfh. m prímszám. Tudjuk, hogy $\mathbb{Z}_m$ kommutatív egységelemes gyűrű (3.46. Tétel), továbbá $|\mathbb{Z}_m|=m\geq 2$. Tehát a test definíciójából „majdnem minden” teljesül $\mathbb{Z}_m$-re, csak azt kell még belátnunk, hogy minden nemnulla elemének van multiplikatív inverze. Tekintsünk tehát egy tetszőleges $\overline{a}\in\mathbb{Z}_m\setminus\{\overline{0}\}$ elemet. Ekkor $m\nmid a$ (miért?), és ebből következik, hogy $a\perp m$ (miért?). A 3.52. Tétel szerint $\overline{a}$-nak van multiplikatív inverze, és ezzel beláttuk, hogy $\mathbb{Z}_m$ test. □

3.57. Tétel (Wilson tétele). Ha p prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.

Bizonyítás. Fogalmazzuk át az állítást maradékosztályokra: ha p prím, akkor az $\overline{1} \cdot \ldots \cdot \overline{p-1} = \overline{-1}$ egyenlőség teljesül $\mathbb{Z}_p$-ben. Mivel p prím, a $\mathbb{Z}_p \setminus \{0\} = \{\overline{1}, \ldots, \overline{p-1}\}$ halmaz minden elemének van multiplikatív inverze, és az inverz is megtalálható ebben a halmazban (miért?). Ez lehetővé teszi, hogy párokba rendezzük a tényezőket: $\overline{a}$ és $\overline{b}$ egy párt alkot, ha egymás inverzei, azaz $\overline{a} \cdot \overline{b} = \overline{1}$. Megtörténhet azonban, hogy egy maradékosztálynak saját maga lesz a párja; nézzük meg, hogy mikor fordul ez elő (minden lépéshez tessék odaképzelni egy „miért?” kérdést):

$$\begin{aligned}\overline{a} \text{ saját magának a párja} &\iff \overline{a} \cdot \overline{a} = \overline{1} \iff a^2 \equiv 1 \pmod{p} \\ &\iff p \mid a^2 - 1 = (a-1)(a+1) \iff p \mid a-1 \text{ vagy } p \mid a+1 \\ &\iff a \equiv 1 \pmod{p} \text{ vagy } a \equiv -1 \pmod{p} \iff \overline{a} = \overline{1} \text{ vagy } \overline{a} = \overline{p-1}.\end{aligned}$$

Tehát csak $\overline{1}$ és $\overline{p-1}$ lesz saját magának a párja. Rendezzük át úgy a szorzatot (felhasználva a maradékosztályok szorzásának asszociativitását és kommutativitását; lásd a 3.46. Tételt), hogy minden tényező a párja mellé kerüljön:

$$\overline{1} \cdot \ldots \cdot \overline{p-1} = \overline{1} \cdot (\_\_) \cdot \ldots \cdot (\_\_) \cdot \overline{p-1}.$$

Itt minden zárójelen belül a két tényező szorzata $\overline{1}$, tehát a végeredmény $\overline{p-1} = \overline{-1}$, és ezt kellett bizonyítanunk. □

Az Euler-féle φ függvény

3.58. Definíció. Jelöljük $\varphi(n)$-nel az n-nél nem nagyobb természetes számok közül azoknak a számát, amelyek n-hez relatív prímek:

$$\varphi(n) = |\{a : 1 \le a \le n \text{ és } a \perp n\}|.$$

Az így kapott függvényt ***Euler-féle φ függvénynek*** nevezzük. Ha megállapodunk abban, hogy $\mathbb{Z}_1^*$ egyelemű halmaz, akkor tömörebben is megfogalmazhatjuk a definíciót:

$$\varphi\colon \mathbb{N} \to \mathbb{N},\ n \mapsto |\mathbb{Z}_n^*|.$$

3.59. Példa. Számítsuk ki közvetlenül a definíció alapján φ néhány értékét:

(a) $\varphi(6) = |\mathbb{Z}_6^*| = \left|\{\overline{1}, \overline{5}\}\right| = 2$;
(b) $\varphi(7) = |\mathbb{Z}_7^*| = \left|\{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}\right| = 6$;
(c) $\varphi(8) = |\mathbb{Z}_8^*| = \left|\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}\right| = 4$;
(d) $\varphi(1024) = |\mathbb{Z}_{1024}^*| = \left|\{\overline{1}, \overline{3}, \overline{5}, \ldots, \overline{1023}\}\right| = 1024/2 = 512$;
(e) $\varphi(81) = |\mathbb{Z}_{81}^*| = \left|\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \ldots, \overline{79}, \overline{80}\}\right| = 81 - 81/3 = 54$.

3.60. Állítás. Tetszőleges p prím és α pozitív egész kitevő esetén

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha \cdot \left(1 - \frac{1}{p}\right).$$

Bizonyítás. Az $\{1, \ldots, p^\alpha\}$ halmaz minden p-edik eleme osztható p-vel (ezek száma $p^{\alpha-1}$), a többiek viszont relatív prímek p^α-hoz (ugye?). Így tehát $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

3.61. Tétel. Legyen az n természetes szám prímhatványtényezős felbontása $n = \prod_{i=1}^k p_i^{\alpha_i}$. Ekkor

$$\varphi(n) = n \cdot \prod_{i=1}^k (1 - \frac{1}{p_i}) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^k p_i^{\alpha_i - 1}(p_i - 1).$$

Bizonyítás. Legyen $U = \{1, \ldots, n\}$ és $A_i = \{a \in U : p_i \mid a\}$ minden $i = 1, \ldots, k$ esetén. Ekkor az U halmaz azon elemei, amelyek relatív prímek n-hez, éppen az $A_1 \cup \cdots \cup A_k$ halmaz komplementerét alkotják (ugye?), tehát $\varphi(n) = \left|\overline{A_1 \cup \cdots \cup A_k}\right|$. Ezt a szita-formula segítségével számíthatjuk ki:

$$\varphi(n) = \left|\overline{A_1 \cup \cdots \cup A_k}\right| = |U| - \sum_{1 \le i_1 \le k} |A_{i_1}| + \sum_{1 \le i_1 < i_2 \le k} |A_{i_1} \cap A_{i_2}| - \sum_{1 \le i_1 < i_2 < i_3 \le k} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| + \cdots + (-1)^k |A_1 \cap \cdots \cap A_k|.$$

Ugyanezt felírhatjuk egyetlen szummában is:

$$\varphi(n) = \left|\overline{A_1 \cup \cdots \cup A_k}\right| = \sum_{\substack{0 \le s \le k \\ 1 \le i_1 < \cdots < i_s \le k}} (-1)^s |A_{i_1} \cap \cdots \cap A_{i_s}|.$$

(Itt $s = 0$ esetén nulla db halmazt metszünk; ennek eredménye U. Ez hasonló megállapodás, mint az, hogy az üres összeg értéke 0, az üres szorzaté pedig 1. Gondoljuk meg, hogy miért értelmes az üres uniót $\emptyset$-nak, az üres metszetet pedig U-nak definiálni.) Ki kell tehát számítanunk tetszőleges $1 \le i_1 < \cdots < i_s \le k$ indexek esetén az $A_{i_1} \cap \cdots \cap A_{i_s}$ metszet elemszámát. Ez a halmaz azokból az $a \in U$ számokból áll, amelyek oszthatóak $p_{i_1}, \ldots, p_{i_s}$ mindegyikével, ami

azzal ekvivalens, hogy $p_{i_1} \cdot \ldots \cdot p_{i_s} \mid a$ (miért?). Ilyen a számból pedig $\frac{n}{p_{i_1} \cdot \ldots \cdot p_{i_s}}$ van az U halmazban (ugye?). Ezt behelyettesítve a szita-formulába, azt kapjuk, hogy

$$\varphi(n) = \left|\overline{A_1 \cup \cdots \cup A_k}\right| = \sum_{\substack{0 \le s \le k \\ 1 \le i_1 < \cdots < i_s \le k}} (-1)^s \frac{n}{p_{i_1} \cdot \ldots \cdot p_{i_s}}.$$

Egy kicsit részletesebben kiírva:

$$\varphi(n) = \left|\overline{A_1 \cup \cdots \cup A_k}\right| = n - \sum_{1 \le i_1 \le k} \frac{n}{p_{i_1}} + \sum_{1 \le i_1 < i_2 \le k} \frac{n}{p_{i_1} \cdot p_{i_2}} - \sum_{1 \le i_1 < i_2 < i_3 \le k} \frac{n}{p_{i_1} \cdot p_{i_2} \cdot p_{i_3}} + \cdots + (-1)^k \frac{n}{p_{i_1} \cdot \ldots \cdot p_{i_k}}.$$

Ezt ügyesen szorzattá alakítjuk:

$$\varphi(n) = n \cdot \Big(1 - \frac{1}{p_1}\Big) \cdot \ldots \cdot \Big(1 - \frac{1}{p_k}\Big),$$

és ezzel meg is kaptuk a tételbeli első alakot $\varphi(n)$-re. (Ez a szorzattá alakítás talán nem világos első látásra. Könnyebb „visszafelé" megérteni: bontsuk fel a zárójeleket az $(1 - \frac{1}{p_1}) \cdot \ldots \cdot (1 - \frac{1}{p_k})$ szorzatban, és győződjünk meg róla, hogy éppen a fenti összeget kapjuk. (Hány tagja van az összegnek?) Célszerű lehet először a $k = 2, 3$ esetekben felírni ezt a zárójelfelbontást.) □

3.62. Példa. Az előző tétel bizonyításának vázlata $k = 2$, azaz $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$ esetén:

$$\begin{aligned} U &= \{1, \ldots, n\} & |U| &= n \\ A_1 &= \{a \in U : p_1 \mid a\} & |A_1| &= \tfrac{n}{p_1} \\ A_2 &= \{a \in U : p_2 \mid a\} & |A_2| &= \tfrac{n}{p_2} \\ A_1 \cap A_2 &= \{a \in U : p_1 p_2 \mid a\} & |A_1 \cap A_2| &= \tfrac{n}{p_1 p_2} \end{aligned}$$

$$\varphi(n) = \left|\overline{A_1 \cup A_2}\right| = |U| - |A_1| - |A_2| + |A_1 \cap A_2| = n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} = n \cdot \Big(1 - \frac{1}{p_1}\Big) \cdot \Big(1 - \frac{1}{p_2}\Big)$$

3.63. Tétel. Ha $m \perp n$, akkor az alábbi ξ leképezés bijektív:

$$\xi \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ \overline{x} \mapsto (\widehat{x}, \widetilde{x}).$$

Bizonyítás. Egyszerre három különböző modulus szerint kell maradékosztályokat tekintenünk, ezért három különböző jelölést használunk: az x egész számot tartalmazó modulo mn maradékosztályt $\overline{x}$ jelöli, az x-et tartalmazó modulo m maradékosztályt $\widehat{x}$, az x-et tartalmazó modulo n maradékosztályt pedig $\widetilde{x}$ fogja jelölni. Először vizsgáljuk meg, hogy a ξ leképezés jóldefiniált-e egyáltalán. Ha $\overline{x_1} = \overline{x_2}$, akkor $x_1 \equiv x_2 \pmod{mn}$, ezért $x_1 \equiv x_2 \pmod{m}$ és $x_1 \equiv x_2 \pmod{n}$ is teljesül (miért?). Ez pedig azt jelenti, hogy $\widehat{x_1} = \widehat{x_2}$ és $\widetilde{x_1} = \widetilde{x_2}$, tehát $(\widehat{x_1}, \widetilde{x_1}) = (\widehat{x_2}, \widetilde{x_2})$, vagyis ξ jóldefiniált.

Tfh. $m \perp n$ és keressük meg egy tetszőleges $\big(\widehat{a}, \widetilde{b}\big) \in \mathbb{Z}_m \times \mathbb{Z}_n$ elempár összes ősét a ξ leképezés mellett. Tehát az összes olyan x egész számot (pontosabban ezek modulo mn maradékosztályait) keressük, amelyre $(\widehat{x}, \widetilde{x}) = \big(\widehat{a}, \widetilde{b}\big)$ teljesül. Ez azzal ekvivalens, hogy $\widehat{x} = \widehat{a}$ és $\widetilde{x} = \widetilde{b}$, amit pedig átírhatunk kongruenciarendszerré: $x \equiv a \pmod{m}$ és $x \equiv b \pmod{n}$ (miért?). A kínai maradéktétel szerint ennek a kongruenciarendszernek van megoldása, és a megoldások egyetlen modulo mn maradékosztályt alkotnak. Ez pedig azt mutatja, hogy az $\big(\widehat{a}, \widetilde{b}\big) \in \mathbb{Z}_m \times \mathbb{Z}_n$ elempárnak pontosan egy ősképe van a $\mathbb{Z}_{mn}$ halmazban. Ezzel beláttuk, hogy ξ valóban bijekció. □

3.64. Következmény. Tetszőleges m, n természetes számok esetén $m \perp n \implies \varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Bizonyítás. Tekintsük a 3.63. Tételben szereplő $\xi \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ \overline{x} \mapsto (\widehat{x}, \widetilde{x})$ bijekciót. Szorítsuk meg ezt a leképezést a redukált modulo mn maradékosztályokra. Egy a egész szám akkor és csak akkor relatív prím mn-hez, ha a relatív prím m-hez is és n-hez is (miért?) Tehát minden $\overline{a} \in \mathbb{Z}_{mn}$ esetén $\overline{a} \in \mathbb{Z}_{mn}^* \iff \xi(\overline{a}) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ (ugye?). Ezek szerint, ha a ξ leképezést megszorítjuk a $\mathbb{Z}_{mn}^*$ halmazra, akkor értékkészlete pont $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ lesz. Így tehát ξ megszorítása egy $\mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ bijekciót szolgáltat (miért?), és eszerint a két halmaz elemszáma egyenlő:

$$\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \cdot \varphi(n).$$ □

3.65. Tétel. Legyen az n természetes szám prímtényezős felbontása $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Ekkor

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Bizonyítás. Ezt a tételt már korábban bizonyítottuk (lásd a 3.61. Tételt), most egy másik, rövidebb bizonyítást adunk. Egyszerűen csak a 3.64. Következményt kell többször alkalmazni, felhasználva, hogy a $p_i^{\alpha_i}$ számok páronként relatív prímek.

$$\begin{aligned} \varphi(n) = \varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots \cdot p_k^{\alpha_k}) &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2} \cdot p_3^{\alpha_3} \ldots \cdot p_k^{\alpha_k}) \\ &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \varphi(p_3^{\alpha_3} \cdot p_4^{\alpha_4} \ldots \cdot p_k^{\alpha_k}) \\ &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \varphi(p_3^{\alpha_3}) \cdot \varphi(p_4^{\alpha_4} \ldots \cdot p_k^{\alpha_k}) \\ &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \varphi(p_3^{\alpha_3}) \cdot \varphi(p_4^{\alpha_4}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k}). \end{aligned}$$ □

3.66. Példa. Számítsuk ki a tanult képlet (3.61. vagy 3.65. Tétel) alapján φ néhány értékét:

(a) $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400$;

(b) $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) = (2^3 - 2^2) \cdot (3^2 - 3) \cdot (5 - 1) = 4 \cdot 6 \cdot 4 = 96$;

(c) $\varphi(2021) = \varphi(43 \cdot 47) = \varphi(43) \cdot \varphi(47) = (43 - 1) \cdot (47 - 1) = 42 \cdot 46 = 1932$.

3.67. Állítás. Minden n természetes szám esetén, a primitív n-edik egységgyökök száma $\varphi(n)$.

Bizonyítás. Az n-edik egységgyökök $\varepsilon_0, \dots, \varepsilon_{n-1}$, ahol $\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \operatorname{cis}\frac{2k\pi}{n}$. Nézzük meg, hogy mely ℓ pozitív egészekre teljesül, hogy $\varepsilon_k^\ell = 1$ (ε_k akkor és csak akkor primitív n-edik egységgyök, ha a legkisebb ilyen „jó” kitevő n):

$$\begin{aligned} \varepsilon_k^\ell = 1 \iff (\operatorname{cis}\tfrac{2k\pi}{n})^\ell = 1 &\iff \operatorname{cis}\tfrac{2k\ell\pi}{n} = 1 && \text{(miért?)} \\ &\iff n \mid k\ell && \text{(miért?)} \\ &\iff \tfrac{n}{\operatorname{lnko}(n,k)} \mid \ell && \text{(miért?).} \end{aligned}$$

Tehát $\frac{n}{\operatorname{lnko}(n,k)}$ többszörösei lesznek a jó kitevők ε_k-hoz, ezek közül a legkisebb (pozitív) nyilván maga $\frac{n}{\operatorname{lnko}(n,k)}$. Ez azt jelenti, hogy ε_k akkor és csak akkor primitív n-edik egységgyök, ha $\operatorname{lnko}(n,k) \sim 1$. Vagyis a primitív n-edik egységgyökök halmaza $\{\varepsilon_k \colon 0 \le k \le n-1 \text{ és } k \perp n\}$, ennek a halmaznak pedig éppen $\varphi(n)$ eleme van (ugye?). □

Hatványozás modulo m

3.68. Definíció. Ha a és m relatív prímek, akkor tetszőleges $k \in \mathbb{N}$ esetén értelmezzük az a^{-k} negatív kitevőjű hatványt modulo m: legyen $a^{-k} \equiv \left(a^k\right)^{-1} \pmod m$. Hasonlóképpen $\overline{a} \in \mathbb{Z}_m^*$ esetén legyen $(\overline{a})^{-k} = \left(\overline{a}^k\right)^{-1}$.

3.69. Megjegyzés. Meg lehet mutatni, hogy a hatványozás szokásos azonosságai érvényben maradnak az egész kitevős modulo m hatványozás fenti értelmezése mellett.

3.70. Definíció. Modulo m ***redukált maradékrendszernek*** nevezzük egész számok egy olyan rendszerét, amely minden mod m redukált maradékosztályból pontosan egy elemet tartalmaz. Tehát $c_1, \dots, c_k$ akkor és csak akkor redukált maradékrendszer modulo m, ha $\{\overline{c_1}, \dots, \overline{c_k}\} = \mathbb{Z}_m^*$. (Itt persze szükségképpen $k = |\mathbb{Z}_m^*| = \varphi(m)$.)

3.71. Lemma. Ha $a \perp m$, akkor az $\alpha \colon \mathbb{Z}_m^* \to \mathbb{Z}_m^*$, $\overline{x} \to \overline{a} \cdot \overline{x}$ leképezés bijekció.

Bizonyítás. Könnyen ellenőrizhető, hogy az α leképezés inverze $\alpha^{-1} \colon \mathbb{Z}_m^* \to \mathbb{Z}_m^*$, $\overline{x} \to \overline{a}^{-1} \cdot \overline{x}$ (ugye?), és ebből következik, hogy α bijektív. □

3.72. Megjegyzés. A 3.71. Lemma maradékrendszerekkel a következőképpen fogalmazható meg: ha a $c_1, \dots, c_{\varphi(m)}$ egész számok redukált maradékrendszert alkotnak modulo m, és $a \in \mathbb{Z}, a \perp m$, akkor $ac_1, \dots, ac_{\varphi(m)}$ is redukált maradékrendszer modulo m.

3.73. Tétel (Euler–Fermat-tétel). Ha az a egész szám relatív prím az m modulushoz, akkor $a^{\varphi(m)} \equiv 1 \pmod m$.

Bizonyítás. Legyen $c_1, \dots, c_{\varphi(m)}$ egy tetszőleges redukált maradékrendszer modulo m, azaz $\left\{\overline{c_1}, \dots, \overline{c_{\varphi(m)}}\right\} = \mathbb{Z}_m^*$. Ha $a \perp m$, akkor a 3.71 . Lemma szerint $\left\{\overline{ac_1}, \dots, \overline{ac_{\varphi(m)}}\right\} = \mathbb{Z}_m^*$. Ebből következik, hogy $\overline{c_1} \cdot \ldots \cdot \overline{c_{\varphi(m)}} = \overline{ac_1} \cdot \ldots \cdot \overline{ac_{\varphi(m)}}$, hiszen mindkét oldalon $\mathbb{Z}_m^*$ összes elemének szorzata áll. Ezt az egyenlőséget kongruenciával is megfogalmazhatjuk: $c_1 \cdot \ldots \cdot c_{\varphi(m)} \equiv ac_1 \cdot \ldots \cdot ac_{\varphi(m)} \pmod m$. Jelölje C a bal oldalon álló számot, és a jobb oldalon emeljük ki az a-kat: $C \equiv a^{\varphi(m)} \cdot C \pmod m$ (ugye?). Mivel $C \perp m$ (miért?), egyszerűsíthetünk C-vel (ugye?), és így megkapjuk a bizonyítani kívánt $1 \equiv a^{\varphi(m)} \pmod m$ kongruenciát. □

3.74. Következmény (kis Fermat-tétel). Ha p prímszám és a nem osztható p-vel, akkor $a^{p-1} \equiv 1 \pmod p$. Más (ekvivalens) megfogalmazásban: Ha p prímszám, akkor minden a egész számra $a^p \equiv a \pmod p$.

Bizonyítás. Alkalmazzuk az Euler–Fermat-tételt az $m = p$ esetben, ahol p prímszám. Ekkor az $a \perp m$ feltétel azt jelenti, hogy $p \nmid a$ (miért?) és $\varphi(m) = \varphi(p) = p - 1$ (ugye?). Tehát ebben az esetben így fest az Euler–Fermat-tétel: minden a egész számra $p \nmid a \implies a^{p-1} \equiv 1 \pmod p$. Ha beszorzunk a-val, akkor az $a^p \equiv a \pmod p$ kongruenciát kapjuk, ami még akkor is igaz, ha $p \mid a$ (miért?). □

3.75. Példa. Mit ad 11-gyel osztva maradékul 123^{765}? Mivel $123 \equiv 2 \pmod{11}$, a hatvány alapját kicserélhetjük 2-re: $123^{765} \equiv 2^{765} \pmod{11}$. Osszuk el a kitevőt maradékosan $\varphi(11)$-gyel (azaz 10-zel): $765 = 10 \cdot 76 + 5$. A hatványt átalakítva és az Euler-Fermat-tételt használva a következőképpen számolhatunk (melyik lépésben használjuk az Euler–Fermat-tételt, és miért használhatjuk egyáltalán?):

$$123^{765} \equiv 2^{765} \equiv 2^{10 \cdot 76 + 5} \equiv (2^{10})^{76} \cdot 2^5 \equiv 1^{76} \cdot 2^5 \equiv 2^5 \equiv 10 \pmod{11}.$$

3.76. Következmény. Ha $a \in \mathbb{Z}$ relatív prím az m modulushoz, akkor

$$k_1 \equiv k_2 \pmod{\varphi(m)} \implies a^{k_1} \equiv a^{k_2} \pmod m.$$

Bizonyítás. Tfh. $a \perp m$ és $k_1 \equiv k_2 \pmod{\varphi(m)}$. Ekkor $k_1 = \varphi(m) \cdot t + k_2$ alkalmas t egész számmal (ugye?), tehát

$$a^{k_1} \equiv a^{\varphi(m)\cdot t + k_2} \equiv \left(a^{\varphi(m)}\right)^t \cdot a^{k_2} \equiv 1^t \cdot a^{k_2} \equiv a^{k_2} \pmod{m} \text{ (miért?).}$$ □

3.77. Példa. Mit ad 44-gyel osztva maradékul 4447^{2018}? Hogy használhassuk az Euler–Fermat-tételt, meg kell győződnünk róla, hogy a hatvány alapja és a modulus relatív prím. Ha először az alapot redukáljuk modulo 44, akkor könnyebb dolgunk lesz: $4447^{2018} \equiv 3^{2018} \pmod{44}$, és az világos, hogy $3 \perp 20$. Most számítsuk ki az Euler-féle φ függvény értékét a modulusnál: $\varphi(44) = \varphi(4) \cdot \varphi(11) = 2 \cdot 10 = 20$. A 3.76. Következmény szerint a kitevő modulo 20 „számít”. Mivel $2018 \equiv 18 \pmod{20}$, a kitevőt kicserélhetnénk 18-ra, de talán jobban járunk, ha inkább -2-t írunk helyette:

$$4447^{2018} \equiv 3^{2018} \equiv 3^{-2} \equiv 9^{-1} \equiv 5 \pmod{44}.$$

(Az utolsó lépéshez meg kell oldanunk a $9x \equiv 1 \pmod{44}$ kongruenciát, ennek megoldása $x \equiv 5 \pmod{44}$.)

4. Számelméleti függvények

Osztók száma, osztók összege

Jelölés. Az n pozitív egész szám pozitív osztóinak halmazát D_n jelöli (1 és maga n is beletartozik).

4.1. Definíció. ***Számelméleti függvényen*** olyan leképezést értünk, amely a természetes számok halmazán van értelmezve, értékei pedig valós (vagy komplex) számok.

4.2. Definíció. Néhány nevezetes számelméleti függvény:

- $\tau(n) = |D_n|$ (n pozitív osztóinak száma);
- $\sigma(n) = \sum_{d|n} d$ (n pozitív osztóinak összege);
- $\varphi(n) = |\{a \in \mathbb{N} : 1 \le a \le n \text{ és } a \perp n\}|$ (redukált maradékosztályok száma, Euler-féle φ függvény).

4.3. Példa. Mivel $D_{12} = \{1, 2, 3, 4, 6, 12\}$, ezért $\tau(12) = 6$ és $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$.

4.4. Definíció. Azt mondjuk, hogy az f számelméleti függvény ***gyengén multiplikatív***, ha $f(1) = 1$ és minden $a, b \in \mathbb{N}$ esetén $a \perp b \implies f(ab) = f(a) \cdot f(b)$.

4.5. Példa. A 3.64. Következményben beláttuk, hogy az Euler-féle φ függvény gyengén multiplikatív (csak annyit kell még hozzátenni, hogy $\varphi(1) = 1$).

4.6. Tétel. Ha az f számelméleti függvény gyengén multiplikatív, akkor tetszőleges páronként különböző $p_1, \dots, p_k$ prímszámok és tetszőleges $\alpha_1, \dots, \alpha_k$ pozitív kitevők esetén

$$f(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \cdot \ldots \cdot f(p_k^{\alpha_k}).$$

Bizonyítás. A bizonyítás lényegében ugyanaz, mint a 3.65. Tétel bizonyítása (ott is csak azt használtuk ki a φ függvényről, hogy gyengén multiplikatív). Alkalmazzuk a gyenge multiplikativitás definícióját az $a = p_1^{\alpha_1}$, $b = p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ „szereposztással” (ezek relatív prímek, ugye?):

$$f(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = f(ab) = f(a) \cdot f(b) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}).$$

A második tényezőt hasonlóan „szétszedhetjük” , ismét alkalmazva a gyenge multiplikativitás definícióját: $f(p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = f(p_2^{\alpha_2}) \cdot f(p_3^{\alpha_3} \cdot \ldots \cdot p_k^{\alpha_k})$. Így folytatva, összesen $k-1$ alkalommal használva a gyenge multiplikativitást, megkapjuk a kívánt felbontást. □

4.7. Lemma. Ha a és b relatív prím pozitív egész számok, akkor ab minden pozitív osztója előáll, mégpedig egyértelműen, a egy pozitív osztójának és b egy pozitív osztójának szorzataként. Másképpen fogalmazva, az alábbi η leképezés bijekció:

$$\eta \colon D_a \times D_b \to D_{ab}, \quad (u, v) \mapsto uv.$$

Bizonyítás. Az injektivitás és szürjektivitás mellett (vagy inkább előtt) igazolni kell azt is, hogy η valóban a D_{ab} halmazba képez. Tehát összesen három dolgot kell bizonyítanunk (melyik az injektivitás és melyik a szürjektivitás?):

(i) $\forall u \in D_a \, \forall v \in D_b \colon \; uv \in D_{ab}$;
(ii) $\forall d \in D_{ab} \, \exists u \in D_a \, \exists v \in D_b \colon \; d = uv$;
(iii) $\forall u_1, u_2 \in D_a \, \forall v_1, v_2 \in D_b \colon \; u_1 v_1 = u_2 v_2 \implies u_1 = u_2$ és $v_1 = v_2$.

Lássunk hozzá:

(i) Ha $u \mid a$ és $v \mid b$, akkor $uv \mid ab$; ez triviális (ugye?).

(ii) Tfh. $d \mid ab$, és legyen $u = \text{lnko}(d, a)$, $v = \frac{d}{\text{lnko}(d,a)}$. Ekkor $u \mid a$ (miért?), $v \mid b$ (miért?) és nyilván $d = uv$ (ugye?).

(iii) Tfh. $u_1, u_2 \mid a$, $v_1, v_2 \mid b$ és $u_1 v_1 = u_2 v_2$. Abból, hogy a és b relatív prím, következik, hogy $u_1 \perp v_2$ (miért?). Az $u_1 v_1 = u_2 v_2$ egyenlőségből következik, hogy $u_1 \mid u_2 v_2$ (ugye?). Alkalmazva az 3.10. Következményt, nyerjük, hogy $u_1 \mid u_2$. Hasonlóan belátható, hogy $u_2 \mid u_1$, tehát $u_1 = u_2$ (miért?). Ezután már az $u_1 v_1 = u_2 v_2$ egyenlőségből egyszerű egyszerűsítéssel kapjuk, hogy $v_1 = v_2$.

□

4.8. Tétel. A τ és σ számelméleti függvények gyengén multiplikatívak.

Bizonyítás. Az világos, hogy $\tau(1) = \sigma(1) = 1$. Ha $a \perp b$, akkor a 4.7. Lemma szerint létezik bijekció a D_{ab} és $D_a \times D_b$ halmazok között, és így elemszámuk egyenlő:

$$\tau(ab) = |D_{ab}| = |D_a \times D_b| = |D_a| \cdot |D_b| = \tau(a) \cdot \tau(b).$$

Ezzel τ gyenge multiplikativitását be is láttuk. A σ függvény vizsgálatához célszerű lesz felsorolni a és b osztóit: legyen $D_a = \{u_1, \dots, u_k\}$, illetve $D_b = \{v_1, \dots, v_\ell\}$ (tehát $\tau(a) = k$ és $\tau(b) = \ell$). A 4.7. Lemma ezzel a jelöléssel azt adja, hogy $D_{ab} = \{u_i v_j \colon i = 1, \dots, k,\ j = 1, \dots, \ell\}$, és az itt felsorolt $k \cdot \ell$ elem páronként különböző (ez ismét azt mutatja, hogy $\tau(ab) = k \cdot \ell = \tau(a) \cdot \tau(b)$). Ezt felhasználva, ha felírjuk a $\sigma(a) \cdot \sigma(b)$ szorzatot és felbontjuk a zárójeleket, akkor éppen $\sigma(ab)$ fog kijönni:

$$\sigma(a) \cdot \sigma(b) = \left(\sum_{i=1,\dots,k} u_i \right) \cdot \left(\sum_{j=1,\dots,\ell} v_j \right) = \sum_{\substack{i=1,\dots,k \\ j=1,\dots,\ell}} u_i v_j = \sigma(ab).$$

Ugyanez „szumma” jelek nélkül:

$$\sigma(a) \cdot \sigma(b) = (u_1 + \dots + u_k) \cdot (v_1 + \dots + v_\ell) = u_1 v_1 + u_1 v_2 + \dots + u_k v_\ell = \sigma(ab).$$

(Akármelyik felírást is tekintjük, a lényeg az, hogy az utolsó összegben ab minden osztója pontosan egyszer lép fel, és ehhez volt szükségünk a 4.7 . Lemmára.) Ezzel beláttuk, hogy σ is gyengén multiplikatív. □

4.9. Tétel. Legyen az n természetes szám prímtényezős felbontása $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Ekkor

$$\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1); \qquad \sigma(n) = \prod_{i=1}^{k} (1 + p_i + p_i^2 + \dots + p_i^{\alpha_i}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}.$$

Bizonyítás. Ha $n = p^\alpha$ (prímhatvány), akkor $D_n = \{1, p, \dots, p^\alpha\}$, és így az osztók száma: $\tau(n) = |D_n| = \alpha + 1$, az osztók összege pedig: $\sigma(n) = 1 + p + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$ (miért?). Mivel a τ és σ függvények gyengén multiplikatívak (4.8. Tétel), a 4.6. Tételt használva már kész is a bizonyítás. □

4.10. Példa. Számítsuk ki 1500 osztóinak számát és osztóinak összegét. A prímhatványtényezős felbontás: $1500 = 2^2 \cdot 3 \cdot 5^3$, ezért $\tau(1500) = \tau(2^2) \cdot \tau(3) \cdot \tau(5^3) = 3 \cdot 2 \cdot 4 = 24$ és $\sigma(1500) = \sigma(2^2) \cdot \sigma(3) \cdot \sigma(5^3) = (1 + 2 + 4) \cdot (1 + 3) \cdot (1 + 5 + 25 + 125) = 7 \cdot 4 \cdot 156 = 4368$.

4.11. Definíció. Az $M_n = 2^n - 1$ alakú számokat ***Mersenne-számoknak***, az ilyen alakú prímeket ***Mersenne-prímeknek*** nevezzük.

4.12. Lemma. Ha M_n prímszám, akkor n is prímszám.

Bizonyítás. Kontrapozícióval bizonyítunk, vagyis azt mutatjuk meg, hogy ha n összetett szám, akkor M_n is összetett. (Az $n = 1$ eset HF.) Tehát tfh. n összetett, azaz $n = ab$ és $1 < a, b < n$. Ekkor az M_n számot szorzattá tudjuk alakítani: $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1) \cdot (\dots)$; itt a második tényező felírása HF. Mivel $1 < a < n$, ezért $1 < 2^a - 1 < M_n$ (ugye?), tehát a fenti szorzatfelbontás nem triviális, és így M_n valóban összetett szám. □

4.13. Definíció. Az n természetes számot ***tökéletes számnak*** nevezzük, ha megegyezik pozitív valódi osztóinak összegével, azaz $\sigma(n) = 2n$.

4.14. Példa. A legkisebb tökéletes szám a 6: pozitív valódi osztói $1, 2, 3$, és valóban $1 + 2 + 3 = 6$. Mivel $\sigma(6)$-ba maga a 6 is beleszámít, ezért $\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$.

4.15. Tétel (Euler tétele). Az n páros szám akkor és csak akkor tökéletes, ha előáll $n = 2^{p-1} \cdot (2^p - 1)$ alakban, ahol $2^p - 1$ prímszám (ekkor p is szükségképpen prím a 4.12. Lemma alapján).

Bizonyítás. Az „akkor” rész igazolásához tfh. $n = 2^{p-1} \cdot (2^p - 1)$, ahol $2^p - 1$ prímszám. Mivel $2^{p-1} \perp 2^p - 1$ (ugye?), alkalmazhatjuk a σ függvény gyenge multiplikativitását: $\sigma(n) = \sigma(2^{p-1}) \cdot \sigma(2^p - 1)$. Tudjuk, hogy $\sigma(2^{p-1}) = 2^p - 1$ (miért?) és $\sigma(2^p - 1) = 2^p$ (miért?). Tehát $\sigma(n) = (2^p - 1) \cdot 2^p$, ami valóban egyenlő $2n$-nel (ugye?), tehát n tökéletes szám.

A „csak akkor” irány bizonyításához tfh. n páros tökéletes szám. Mivel n páros, prímtényezős felbontásában szerepel a 2-es, mondjuk k-adik hatványon ($k \geq 1$), tehát n felírható $n = 2^k \cdot t$ alakban, ahol t páratlan szám. Akárcsak az előző

részben, $2^k \perp t$, és így $\sigma(n) = (2^{k+1}-1)\cdot\sigma(t)$. Feltettük, hogy n tökéletes, vagyis $\sigma(n) = 2n = 2^{k+1}\cdot t$. Összevetve az utóbbi két eredményt, azt kapjuk, hogy $(2^{k+1}-1)\cdot\sigma(t) = 2^{k+1}\cdot t$. Fejezzük ki innen $\sigma(t)$ értékét:

$$\sigma(t) = \frac{2^{k+1}\cdot t}{2^{k+1}-1} = \frac{(2^{k+1}-1+1)\cdot t}{2^{k+1}-1} = t + \frac{t}{2^{k+1}-1} = t + s.$$

A $\frac{t}{2^{k+1}-1}$ tört egész szám (hiszen nem más, mint $\sigma(t)-t$), ezt jelöltük s-sel. Ekkor $t = (2^{k+1}-1)\cdot s$, azaz s osztója t-nek. Sőt, $k \geq 1$ miatt $2^{k+1}-1 > 1$, tehát s valódi osztója t-nek ($s < t$). Nézzük meg most jól a $\sigma(t) = t + s$ egyenlőséget. A bal oldalon t összes osztójának összege áll, a jobb oldalon pedig két osztójának összege. Ez csak úgy lehetséges, hogy mindössze két osztója van t-nek, vagyis t prímszám (ugye?). Következésképp $s = 1$, és így $t = 2^{k+1}-1$. Már csak annyit kell tennünk, hogy „elnevezzük” $k+1$-et p-nek. Ezzel a jelöléssel $t = 2^p - 1$ (és már tudjuk, hogy ez prímszám) maga n pedig így fest: $n = 2^k\cdot t = 2^{p-1}\cdot(2^p-1)$. Ez pedig éppen az az előállítás, ami a célunk volt. □

4.16. Példa. A második legkisebb tökéletes szám a 28, ami a $p = 3$ értékkel adódik Euler tételéből: $28 = 2^2\cdot(2^3-1)$, és itt $M_3 = 2^3 - 1$ valóban prím.

4.17. Megjegyzés. Abból, hogy n prím, még nem következik, hogy M_n is az, például M_{11} összetett szám. Nem ismert, hogy létezik-e végtelen sok Mersenne-prím, tehát azt sem tudjuk, hogy létezik-e végtelen sok páros tökéletes szám. Páratlan tökéletes számot egyet sem ismerünk, de nincs bizonyítva az sem, hogy ilyen nem létezik. A jelenleg (2022. november 17.) ismert legnagyobb prímszám is Mersenne-prím: $M_{82\,589\,933}$, ami tízes számrendszerben 24 862 048 számjegyből áll.

4.18. Definíció. Az $F_n = 2^{2^n}+1$ alakú számokat ***Fermat-számoknak***, az ilyen alakú prímeket ***Fermat-prímeknek*** nevezzük.

4.19. Megjegyzés. A 4.12. Lemmához hasonlóan meggondolható, hogy ha 2^k+1 prímszám, akkor k szükségképpen kettőhatvány. Ezért a „kettőhatvány plusz egy” alakú prímeket csak az $F_n = 2^{2^n}+1$ Fermat-számok között érdemes keresni. Fermat azt sejtette, hogy F_n mindig prím. Az első öt Fermat-szám valóban prím:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537,$$

de Euler észrevette, hogy $F_5 = 641\cdot 6\,700\,417$. Minden további Fermat-szám, amit sikerült megvizsgálni (részben számítógéppel), összetettnek bizonyult. Az általánosan elfogadott sejtés az, hogy csak véges sok Fermat-prím van (valószínűleg csak a fenti öt).

Összegzési és megfordítási függvény

4.20. Tétel. Minden n pozitív egész számra $\sum_{d|n}\varphi(d) = n$.

Bizonyítás. (törtekkel) Tekintsük a $T = \left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\right\}$ halmazt; ennek szemlátomást n eleme van. Ha egy T-beli törtet egyszerűsítünk amennyire csak lehet, akkor egy olyan $\frac{k}{d}$ alakú törtet kapunk, ahol $d \mid n$ (miért?), $k \perp d$ (miért?) és $1 \leq k \leq d$ (miért?). Fordítva, ha $d \mid n$, $k \perp d$ és $1 \leq k \leq d$, akkor $\frac{k}{d} = \frac{kn/d}{n}$ szerepel a T halmazban (miért?). Azt látjuk tehát, hogy a T-beli törteket egyszerűsítve, éppen a $\frac{k}{d}$ ($d \mid n$, $k \perp d$ és $1 \leq k \leq d$) törteket kapjuk meg, tehát ezekből is n darab van. Rögzített d nevező esetén a k számlálóra $\varphi(d)$ lehetőség van (ugye?). Eszerint ha a T-beli törtek egyszerűsített alakjait a nevezőik szerint csoportosítva számoljuk össze, akkor éppen a $\sum_{d|n}\varphi(d)$ összeget kapjuk, és ezzel kész is a bizonyítás. □

Bizonyítás. (egységgyökökkel) Megmutatjuk, hogy a $\sum_{d|n}\varphi(d)$ összeg az n-edik egységgyököket számolja meg, ezekből pedig tudjuk, hogy n van. Legyen $E_n = \{\varepsilon_0, \ldots, \varepsilon_{n-1}\}$ az n-edik egységgyökök halmaza, és tetszőleges $d \in \mathbb{N}$ esetén jelölje P_d a d-edik primitív egységgyökök halmazát. A 3.67. Állítás bizonyítása során láttuk, hogy az $\varepsilon_k = \operatorname{cis}\frac{2k\pi}{n}$ komplex számhoz tartozó legkisebb pozitív jó kitevő $d := \frac{n}{\operatorname{lnko}(n,k)}$, vagyis ε_k primitív d-edik egységgyök (azaz $\varepsilon_k \in P_d$). Nyilván $d \mid n$ (miért?), tehát azt kaptuk, hogy minden n-edik egységgyök primitív d-edik egységgyök n valamely d osztójára. Fordítva, ha z primitív d-edik egységgyök n valamely d osztójára, akkor $z^n = (z^d)^{n/d} = 1^{n/d} = 1$ (ugye?), tehát $z \in E_n$. Látjuk tehát, hogy E_n felbontható a P_d ($d \mid n$) halmazok egyesítésére, és ezek a halmazok páronként diszjunktak (miért?):

$$E_n = \bigcup_{d|n} P_d.$$

Diszjunkt halmazok egyesítésénél az elemszámok összeadódnak, tehát

$$n = |E_n| = \left|\bigcup_{d|n} P_d\right| = \sum_{d|n}|P_d|.$$

A 3.67 . Állításból tudjuk, hogy $|P_d| = \varphi(d)$, tehát a fenti egyenlőség igazolja, hogy $n = \sum_{d|n}\varphi(d)$. □

4.21. Definíció. Az f számelméleti függvény ***összegzési függvényén*** az $F(n) = \sum_{d|n} f(d)$ számelméleti függvényt értjük. Az f függvényt az F függvény ***megfordítási függvényének*** nevezzük.

4.22. Példa. Legyen F az $f(n)=n^2$ képlettel megadott számelméleti függvény összegzési függvénye. Számítsuk ki $F(18)$ értékét.

$$F(18)=f(1)+f(2)+f(3)+f(6)+f(9)+f(18)=1^2+2^2+3^2+6^2+9^2+18^2=455$$

Jelölés. Azt a tényt, hogy F az f összegzési függvénye gyakran egyszerűen csak $f\to F$ jelöli.

4.23. Megjegyzés. A 4.20. Tétel szerint az Euler-féle φ függvény összegzési függvénye az identikus függvény: $\varphi\to\mathrm{id}$. Másképpen fogalmazva: az identikus függvény megfordítási függvénye az Euler-féle φ függvény. Ha nem ismernénk a 4.20. Tételt, akkor nem lenne könnyű feladat meghatározni az identikus függvény megfordítási függvényét. A következőkben bevezetünk egy kétváltozós műveletet a számelméleti függvények halmazán, aminek segítségével módszert (képletet) tudunk adni egy tetszőleges számelméleti függvény megfordítási függvényének kiszámítására.

4.24. Definíció. Szükségünk lesz az alábbi három nagyon egyszerű számelméleti függvényre:

- $\mathrm{id}(n)=n$ (identikus függvény);
- $\mathbf{1}(n)=1$ (konstans 1 függvény);
- $\delta(n)=\delta_{1n}=\begin{cases}1, & \text{ha } n=1;\\ 0, & \text{ha } n>1.\end{cases}$

4.25. Példa. A tanult számelméleti függvények között a következő „összegzési kapcsolatok” állnak fenn:

$$\delta\to\mathbf{1}\to\tau \qquad \text{és} \qquad \varphi\to\mathrm{id}\to\sigma.$$

4.26. Definíció. Az f és g számelméleti függvények ***konvolúcióján*** az alábbi képlettel definiált $f*g$ számelméleti függvényt értjük:

$$(f*g)(n)=\sum_{d\mid n} f(d)\cdot g\Big(\frac{n}{d}\Big)=\sum_{ab=n} f(a)g(b).$$

4.27. Megjegyzés. Az összegzési függvény képzése speciális esete a konvolúciónak: ha $f\to F$, akkor

$$F(n)=\sum_{d\mid n} f(d)\cdot 1=\sum_{d\mid n} f(d)\cdot\mathbf{1}\Big(\frac{n}{d}\Big)$$

minden n természetes számra, azaz $F=f*\mathbf{1}$.

4.28. Tétel. A konvolúció művelete kommutatív, asszociatív, és minden f számelméleti függvényre $f*\delta=\delta*f=f$.

Bizonyítás. Az asszociativitás igazolásához ki kell számolni az $(f*g)*h$ és $f*(g*h)$ konvolúciók n helyen felvett értékét; azt kapjuk, hogy

$$((f*g)*h)(n)=(f*(g*h))(n)=\sum_{abc=n} f(a)g(b)h(c).$$

A kommutativitás világos (ugye?) az utolsó állítás pedig egyszerűen adódik a δ függvény definíciójából:

$$(f*\delta)(n)=\sum_{d\mid n} f(d)\cdot\delta\Big(\frac{n}{d}\Big)=f(n)\cdot\delta(1)=f(n),$$

hiszen a $d=n$ eset kivételével az összeg minden tagja nulla (miért?). □

4.29. Definíció. Az n természetes számot ***négyzetmentesnek*** nevezzük, ha nem osztható egyetlen 1-nél nagyobb négyzetszámmal sem.

4.30. Megjegyzés. Könnyű meggondolni, hogy egy szám akkor és csak akkor négyzetmentes, ha prímfelbontásában minden prím csak egyszer (azaz első hatványon) fordul elő.

4.31. Definíció. ***Möbius-függvénynek*** nevezzük az alábbi képlettel definiált μ számelméleti függvényt:

$$\mu(n)=\begin{cases}0, & \text{ha } n \text{ nem négyzetmentes;}\\ (-1)^k, & \text{ha } n \text{ előáll } k \text{ különböző prím szorzataként.}\end{cases}$$

4.32. Tétel. A Möbius-függvény összegzési függvénye a δ függvény, azaz $\mu*\mathbf{1}=\delta$.

Bizonyítás. Az kell bizonyítanunk, hogy $\sum_{d\mid n}\mu(d)=\delta(n)$ minden n természetes számra. Az $n=1$ eset triviális (ugye?), ezért csak az $n>1$ esettel foglalkozunk (ekkor a bizonyítandó egyenlőség jobb oldalán $\delta(n)=0$ áll). A szokásos módon írjuk fel n-et prímhatványok szorzataként: $n=p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$. Elegendő az összegzésben n négyzetmentes osztóit tekinteni (mert a többi osztókon μ értéke nulla), ezek pedig nem mások, mint a $p_1,\ldots,p_k$ számokból alkotott szorzatok (beleértve az üres szorzatot is):

$$\sum_{d\mid n}\mu(d)=\mu(1)+\mu(p_1)+\cdots+\mu(p_k)+\mu(p_1p_2)+\cdots+\mu(p_{k-1}p_k)+\mu(p_1p_2p_3)+\cdots+\mu(p_{k-2}p_{k-1}p_k)+\cdots+\mu(p_1\cdots p_k)=$$

$$=(-1)^0+(-1)^1+\cdots+(-1)^1+(-1)^2+\cdots+(-1)^2+(-1)^3+\cdots+(-1)^3+\cdots+(-1)^k.$$

Az összeg tagjai megfelelnek a $\{p_1, \dots, p_k\}$ halmaz részhalmazainak, és -1 kitevőjében mindig az adott halmaz elemszáma van (ugye?). Mivel az i-elemű részhalmazok száma $\binom{k}{i}$, az összegben a $(-1)^i$ tag $\binom{k}{i}$ alkalommal lép fel, ezért tömörebben így is felírhatjuk az összeget:

$$\sum_{d|n} \mu(d) = \binom{k}{0} \cdot (-1)^0 + \binom{k}{1} \cdot (-1)^1 + \binom{k}{2} \cdot (-1)^2 + \binom{k}{3} \cdot (-1)^3 + \dots + \binom{k}{k} \cdot (-1)^k.$$

Azt kell igazolnunk, hogy ez az összeg 0 (hiszen $\delta(n) = 0$). Erre több lehetőség is van: tekinthetjük a $(-1+1)^k$ összeg kifejtését a binomiális tétel segítségével, vagy használhatjuk azt az ismert(?) kombinatorikai tényt, hogy egy tetszőleges véges (nem üres) halmaznak ugyanannyi páros elemszámú részhalmaza van, mint ahány páratlan elemszámú. □

4.33. Tétel (Möbius-féle megfordítási képlet). Tetszőleges F számelméleti függvény esetén F-nek egyetlen megfordítási függvénye van, mégpedig $F * \mu$. Másképpen fogalmazva $f \to F$ akkor és csak akkor áll fenn, ha $f = F * \mu$. Részletesebben: tetszőleges f, F számelméleti függvények esetén

$$\forall n \in \mathbb{N} : F(n) = \sum_{d|n} f(d) \quad \iff \quad \forall n \in \mathbb{N} : f(n) = \sum_{d|n} F(d) \cdot \mu\Big(\frac{n}{d}\Big).$$

Bizonyítás. Figyelembe véve a 4.27. Megjegyzést, a bizonyítandó állítást így is megfogalmazhatjuk: tetszőleges f és F számelméleti függvények esetén

$$F = f * \mathbf{1} \iff f = F * \mu.$$

Az „ $\Longrightarrow$ ” irányhoz tfh. $F = f * \mathbf{1}$, és „konvolváljuk be” mindkét oldalt μ-vel: $F * \mu = (f * \mathbf{1}) * \mu$. A jobb oldalt először zárójelezzük át, felhasználva a konvolúció asszociativitását (4.28. Tétel): $(f * \mathbf{1}) * \mu = f * (\mathbf{1} * \mu)$. Most használjuk a 4.32. Tételt, majd azt, hogy a konvolúciónak δ az egységeleme (4.28. Tétel): $f * (\mathbf{1} * \mu) = f * \delta = f$. Ezzel beláttuk, hogy $F = f * \mathbf{1} \implies f = F * \mu$.

Az „ $\Longleftarrow$ ” irányhoz tfh. $f = F * \mu$, és „konvolváljuk be” mindkét oldalt a konstans 1 függvénnyel. A számolás az előzőhöz hasonló (indokoljunk meg minden lépést!): $f * \mathbf{1} = (F * \mu) * \mathbf{1} = F * (\mu * \mathbf{1}) = F * \delta = F$. Ezzel beláttuk, hogy $f = F * \mu \implies F = f * \mathbf{1}$. □

4.34. Példa. Legyen f a $F(n) = \log n$ képlettel megadott számelméleti függvény megfordítási függvénye. Számítsuk ki $f(100)$ és $f(81)$ értékét:

$$\begin{aligned}
f(100) &= F(100)\mu(1) + F(50)\mu(2) + F(25)\mu(4) + F(20)\mu(5) + F(10)\mu(10) + \\
&\quad + F(5)\mu(20) + F(4)\mu(25) + F(2)\mu(50) + F(1)\mu(100) = \\
&= F(100) - F(50) - F(20) + F(10) = \\
&= \log 100 - \log 50 - \log 20 + \log 10 \\
&= 0 \\
f(81) &= F(81)\mu(1) + F(27)\mu(3) + F(9)\mu(9) + F(3)\mu(27) + F(1)\mu(81) = \\
&= F(81) - F(27) = \\
&= \log 81 - \log 27 \\
&= \log 3.
\end{aligned}$$

4.35. Tétel. Gyengén multiplikatív számelméleti függvények konvolúciója is gyengén multiplikatív.

Bizonyítás. Tfh. f és g is gyengén multiplikatív. Az világos, hogy $(f * g)(1) = f(1) \cdot g(1) = 1$ (ugye?). Tfh. $a \perp b$, és írjuk fel a definíció szerint $(f * g)(ab)$ értékét:

$$(f * g)(ab) = \sum_{d|ab} f(d) \cdot g\Big(\frac{ab}{d}\Big).$$

A 4.7. Lemma szerint ab minden d osztója egyértelműen felírható $d = uv$ alakban, ahol $u \mid a$ és $v \mid b$. Így a fenti összeget a következőképpen alakíthatjuk át, felhasználva f és g gyenge multiplikativitását:

$$\sum_{d|ab} f(d) \cdot g\Big(\frac{ab}{d}\Big) = \sum_{\substack{u|a \\ v|b}} f(uv) \cdot g\Big(\frac{ab}{uv}\Big) = \sum_{\substack{u|a \\ v|b}} f(u)f(v) \cdot g\Big(\frac{a}{u}\Big)g\Big(\frac{b}{v}\Big)$$

(honnan tudjuk, hogy $u \perp v$ és $\frac{a}{u} \perp \frac{b}{v}$?). Az utolsó lépés már csak egy szorzattá alakítás (jobbról balra olvasva könnyebb megérteni):

$$\sum_{\substack{u|a \\ v|b}} f(u)f(v) \cdot g\Big(\frac{a}{u}\Big)g\Big(\frac{b}{v}\Big) = \left(\sum_{u|a} f(u)g\Big(\frac{a}{u}\Big)\right) \cdot \left(\sum_{v|b} f(v)g\Big(\frac{b}{v}\Big)\right) = (f * g)(a) \cdot (f * g)(b).$$ □

4.36. Következmény. Gyengén multiplikatív számelméleti függvény összegzési függvénye is gyengén multiplikatív.

Bizonyítás. A f függvény összegzési függvénye $f * \mathbf{1}$ (lásd a 4.27. Megjegyzést). A konstans 1 függvény nyilván gyengén multiplikatív, ezért az előző tételből, következik, hogy ha f gyengén multiplikatív, akkor $f * \mathbf{1}$ is az. □

4.37. Következmény. Gyengén multiplikatív számelméleti függvény megfordítási függvénye is gyengén multiplikatív.

Bizonyítás. Először azt ellenőrizzük, hogy μ gyengén multiplikatív. A definícióból $\mu(1) = 1$, hiszen 1 nulla darab prím szorzata (üres szorzat). Tfh. $a \perp b$ és vizsgáljuk $\mu(ab)$ értékét. Ha a nem négyzetmentes, akkor ab sem az, (ugye?), tehát $\mu(a) = 0 \implies \mu(ab) = 0$, ekkor tehát teljesül, hogy $\mu(ab) = \mu(a) \cdot \mu(b)$. A $\mu(b) = 0$ eset hasonló, tehát feltehetjük, hogy a és b is négyzetmentes: $a = p_1 \cdot \ldots \cdot p_k$ (ahol $p_1, \ldots, p_k$ páronként különböző prímszámok) és $b = q_1 \cdot \ldots \cdot q_\ell$ (ahol $q_1, \ldots, q_\ell$ páronként különböző prímszámok). Az $a \perp b$ feltevésből következik, hogy a $\{p_1, \ldots, p_k\}$ és $\{q_1, \ldots, q_\ell\}$ halmazok diszjunktak (ugye?), így az $ab = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_\ell$ felbontásban $k + \ell$ különböző prímszám szerepel. Ebből már ki tudjuk számítani $\mu(ab)$ értékét: $\mu(ab) = (-1)^{k+\ell} = (-1)^k \cdot (-1)^\ell = \mu(a) \cdot \mu(b)$ (ugye?). Ezzel beláttuk, hogy μ gyengén multiplikatív.

A Möbius-féle megfordítási képlet szerint f megfordítási függvénye $f*\mu$. Ha f gyengén multiplikatív, akkor (felhasználva μ most igazolt gyenge multiplikativitását) a 4.35. Tételből következik, hogy $f * \mu$ is gyengén multiplikatív. □

5. Polinomok

Oszthatóság, asszociáltság, legnagyobb közös osztó test feletti polinomgyűrűben (ismétlés)

Legyen R egy tetszőleges integritástartomány (azaz kommutatív, egységelemes és zérusosztómentes gyűrű). Ekkor az R feletti polinomok is integritástartományt alkotnak (jelölés: $R[x]$). Speciálisan, ha T test (a továbbiakban T mindig egy tetszőleges testet jelöl), akkor $T[x]$ integritástartomány. A legfontosabb példák: $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$ (ahol p prímszám). Minden $f \in T[x]$ polinomhoz tartozik egy $f\colon T \to T$, $c \mapsto f(c)$ polinomfüggvény, amit szintén f-fel jelölünk, de ez nem egyezik meg az f polinommal! A következő példa mutatja, hogy véges testek fölött különböző polinomokhoz tartozhat ugyanaz a polinomfüggvény, ezért nagyon fontos, hogy ne keverjük össze a polinomot a polinomfüggvénnyel! (Végtelen test fölött ilyen nem fordulhat elő (miért?), de ott sem szabad összemosni a két fogalmat.)

5.1. Példa. Az $f = x$, $g = x^2 \in \mathbb{Z}_2[x]$ polinomok nyilván különbözőek (még a fokszámuk sem egyforma), de ugyanaz a polinomfüggvény tartozik hozzájuk:

$$f(\overline{0}) = \overline{0} = g(\overline{0}) \quad \text{és} \quad f(\overline{1}) = \overline{1} = g(\overline{1}).$$

Test feletti polinomok körében az oszthatóság hasonlóan értelmezhető, mint az egész számok körében, és hasonló tulajdonságokkal rendelkezik.

5.2. Definíció (ism.). Az $f \in T[x]$ polinom ***osztója*** a $g \in T[x]$ polinomnak (jelölés: $f \mid g$), ha létezik olyan $h \in T[x]$ polinom amelyre $g = fh$.

5.3. Definíció (ism.). Az f és g polinomok ***asszociáltak*** (jelölés: $f \sim g$), ha $f \mid g$ és $g \mid f$.

5.4. Tétel (ism.). A polinomok oszthatósága reflexív ($f \mid f$) és tranzitív ($f \mid g$ és $g \mid h \implies f \mid h$), de általában nem antiszimmetrikus ($f \mid g$ és $g \mid f \not\Rightarrow f = g$). Az antiszimmetria helyett a következőt mondhatjuk: tetszőleges $f, g \in T[x]$ polinomokra $f \sim g \iff \exists c \in T \setminus \{0\} : g = cf$. Ha $f \mid g$ és $g \neq 0$, akkor $\deg f \leq \deg g$.

5.5. Tétel (ism.). Az asszociáltság ekvivalenciareláció $T[x]$-en. A nulla osztályát kivéve minden asszociáltsági osztály tartalmaz pontosan egy főpolinomot.

5.6. Megjegyzés. Asszociált polinomokat nem érdemes (sőt nem is lehet) megkülönböztetni, ha csak az oszthatóságot vizsgáljuk. Ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor már nemcsak reflexív és tranzitív, hanem antiszimmetrikus is lesz, azaz részbenrendezés. A kapott $(T[x]/\sim; |)$ részbenrendezett halmaz legkisebb eleme $1/\sim = T \setminus \{0\}$, legnagyobb eleme $0/\sim = \{0\}$. Test feletti polinomgyűrűben minden asszociáltsági osztály (a nulláét kivéve) pontosan egy főpolinomot tartalmaz, itt tehát asszociáltság erejéig mindig dolgozhatunk főpolinomokkal. (Hasonlóképpen, az egész számok gyűrűjében minden asszociáltsági osztály $\{a, -a\}$ alakú, tehát minden osztályban van egy (és csak egy) nemnegatív szám. Ha minden asszociáltsági osztályt a nemnegatív elemével reprezentálunk, akkor az $(\mathbb{N}_0; |)$ részbenrendezett halmazt kapjuk, ami lényegében ugyanaz, mint a $(\mathbb{Z}/\sim; |)$ részbenrendezett halmaz.)

5.7. Tétel (ism.). Bármely $f \in T[x]$ és $\alpha \in T$ esetén

$$f(\alpha) = 0 \iff x - \alpha \mid f.$$

5.8. Tétel (ism.). Ha $f, g \in T[x]$, és $g \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és $r \in T[x]$ polinomok, amelyekre $f = qg + r$ és $\deg r < \deg g$.

5.9. Definíció (ism.). A $d \in T[x]$ polinom ***legnagyobb közös osztója*** az f és $g \in T[x]$ polinomoknak, ha teljesül a következő két feltétel:

(1) $d \mid f$ és $d \mid g$;
(2) $\forall k \in T[x] : (k \mid f \text{ és } k \mid g) \implies k \mid d$.

Hasonlóan definiálható polinomok ***legkisebb közös többszöröse*** is.

5.10. Megjegyzés. A legnagyobb közös osztó a 3.3 . Megjegyzés szellemében a következőképpen is értelmezhető. Tetszőleges $f \in T[x]$ polinomra jelölje D_f az f polinom összes osztóinak halmazát: $D_f = \{k \in T[x] : k \mid f\}$. Ekkor $D_f \cap D_g$ nem más, mint f és g közös osztóinak halmaza, $\operatorname{lnko}(f,g)$ pedig ennek az oszthatóság szerint részbenrendezett halmaznak a legnagyobb eleme. Pontosabban, mivel az oszthatóság csak asszociáltság erejéig antiszimmetrikus, a teljesen precíz megfogalmazás úgy szól, hogy $\operatorname{lnko}(f,g)$ asszociáltsági osztálya a $((D_f \cap D_g)/\sim; |)$ részbenrendezett halmaz legnagyobb eleme. Innen is látszik, hogy a legnagyobb közös osztó csak asszociáltság erejéig van meghatározva; megállapodás szerint általában főpolinomot választunk. Nemnulla polinomok esetén $\operatorname{lnko}(f,g)$ úgy is definiálható, mint f és g legnagyobb fokszámú közös osztója (asszociáltság erejéig). (Miért nem jó ez a definíció $\operatorname{lnko}(0,0)$ esetén?)

5.11. Tétel (ism.). Bármely két $f, g \in T[x]$ polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse, és ezek asszociáltság erejéig egyértelműen meghatározottak. A legnagyobb közös osztó kiszámítható az euklideszi algoritmussal.

Lineáris „diofantoszi" egyenlet test feletti polinomgyűrűben

5.12. Tétel. Az $f, g \in T[x]$ polinomok legnagyobb közös osztója mindig kifejezhető f és g „lineáris kombinációjaként" :

$$\exists u, v \in T[x] : \ fu + gv = \operatorname{lnko}(f,g). \tag{5.3}$$

Bizonyítás. A bizonyítás nagyon hasonló a 3.4. Tétel bizonyításához. Az általánosság megszorítása nélkül feltehetjük, hogy $f, g \neq 0$ (ha valamelyikük nulla, akkor az állítás triviális). Ekkor végrehajtható az f, g polinomokra az euklideszi algoritmus (technikai okokból f és g az r_0 és r_1 „fedőneveket" kapják):

$$\begin{aligned}
r_0 := f &= q_1 r_1 + r_2 && (\deg r_2 < \deg r_1);\\
r_1 := g &= q_2 r_2 + r_3 && (\deg r_3 < \deg r_2);\\
r_2 &= q_3 r_3 + r_4 && (\deg r_4 < \deg r_3);\\
&\vdots\\
r_{i-1} &= q_i r_i + r_{i+1} && (\deg r_{i+1} < \deg r_i);\\
&\vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && (\deg r_n < \deg r_{n-1});\\
r_{n-1} &= q_n r_n + 0.
\end{aligned}$$

Tudjuk (Algszám. 2), hogy az eljárás véges számú lépésben véget ér: előbb utóbb nulla lesz a maradék ($r_{n+1} = 0$), és a legnagyobb közös osztó az utolsó nemnulla maradék: $r_n \sim \operatorname{lnko}(f,g)$. Megmutatjuk i szerinti teljes indukcióval, hogy mindegyik r_i előáll f és g „lineáris kombinációjaként":

$$\exists u_i, v_i \in T[x]: \ r_i = fu_i + gv_i. \tag{5.4}$$

(Két dologban eltérünk az indukció szokásos sémájától. Egyrészt nem minden i nemnegatív egészre bizonyítunk, hanem csak $i = 0, 1, \ldots, n$-re. Másrészt az indukciós lépésben két lépéssel nyúlunk vissza: amikor $i+1$-re bizonyítjuk az állítást, nemcsak i-re, hanem $i-1$-re is feltesszük, hogy (5.4) teljesül. Emiatt a kezdőlépésnél is az első két értékre ($i = 0$ és $i = 1$) kell ellenőriznünk az állítást.)

Kezdőlépés: $i = 0$ és $i = 1$ esetén triviálisan teljesül (5.4):

$$\begin{aligned}
r_0 = f = f \cdot 1 + g \cdot 0 \qquad &\text{(tehát } u_0 = 1 \text{ és } v_0 = 0 \text{ jó lesz);}\\
r_1 = g = f \cdot 0 + g \cdot 1 \qquad &\text{(tehát } u_1 = 0 \text{ és } v_1 = 1 \text{ jó lesz).}
\end{aligned}$$

Indukciós lépés: Legyen $1 \leq i < n$, és tfh. r_{i-1} és r_i előáll a kívánt módon; ez az indukciós feltevés:

$$r_{i-1} = fu_{i-1} + gv_{i-1} \text{ és } r_i = fu_i + gv_i. \tag{IH}$$

Be kell látnunk, hogy (5.4) teljesül $i+1$-re is. Ehhez fejezzük ki az r_{i+1} maradékot az euklideszi algoritmus megfelelő lépéséből: $r_{i+1} = r_{i-1} - q_i r_i$. Helyettesítsük r_{i-1} és r_i helyébe az indukciós hipotézisben szereplő felírásukat:

$$\begin{aligned}
r_{i+1} = r_{i-1} - q_i r_i &= (fu_{i-1} + gv_{i-1}) - q_i(fu_i + gv_i)\\
&= f(u_{i-1} - q_i u_i) + g(v_{i-1} - q_i v_i).
\end{aligned}$$

Azt kaptuk, hogy r_{i+1} is kifejezhető f és g segítségével az előírt módon, pl. $u_{i+1} = u_{i-1} - q_i u_i$ és $v_{i+1} = v_{i-1} - q_i v_i$ együtthatókkal. Ezzel kész az indukciós bizonyítás. □

5.13. Definíció. Azt mondjuk, hogy az $f, g \in T[x]$ polinomok ***relatív prímek***, ha $\operatorname{lnko}(f,g) \sim 1$. Jelölés: $f \perp g$.

5.14. Tétel. Tetszőleges $f, g, h \in T[x]$ polinomok esetén, ha $f \perp g$, akkor $f \mid gh \iff f \mid h$.

Bizonyítás. Az nyilvánvaló, hogy $f \mid h \implies f \mid gh$ (ehhez nincs is szükség az $f \perp g$ feltevésre). A másik irány bizonyításához tegyük fel, hogy $f \mid gh$, és írjuk fel f és g legnagyobb közös osztóját (5.3) szerint $\operatorname{lnko}(f,g) \sim 1 = fu + gv$ alakban. Szorozzuk be az egyenlőséget h-val: $h = fhu + ghv$. Világos, hogy $f \mid fhu$, és az $f \mid gh$ feltevésünk miatt $f \mid ghv$ is teljesül. Tehát az összeg mindkét tagja osztható f-fel, és ez mutatja, hogy $f \mid h$. □

5.15. Tétel. Tetszőleges $f, g, h \in T[x]$ polinomok esetén, ha $\operatorname{lnko}(f,g) \neq 0$, akkor

$$f \mid gh \iff \frac{f}{\operatorname{lnko}(f,g)} \mid h. \tag{5.5}$$

Bizonyítás. Legyen $d \sim \operatorname{lnko}(f,g) \neq 0$, továbbá legyen $f = f_0 d$ és $g = g_0 d$ (miért tudjuk f-et és g-t így felírni alkalmas $f_0, g_0 \in T[x]$ polinomokkal?). Először megmutatjuk, hogy $f_0 \perp g_0$. Ismét (5.3)-et használva d felírható $d = fu + gv = d(f_0 u + g_0 v)$ alakban. Egyszerűsítve[1] d-vel azt kapjuk, hogy $f_0 u + g_0 v = 1$. Ebből már következik, hogy $f_0 \perp g_0$, hiszen f_0 és g_0 bármely k közös osztójára $k \mid f_0 u + g_0 v = 1$, tehát $k \sim 1$. A bizonyítandó (5.5) állítás így fest: $f_0 d \mid g_0 dh \iff f_0 \mid h$; a bal oldalt d-vel egyszerűsítve ezt átfogalmazhatjuk úgy, hogy $f_0 \mid g_0 h \iff f_0 \mid h$. Ez pedig már következik az előző tételből, hiszen $f_0 \perp g_0$. □

5.16. Tétel. Legyen T egy test és $f, g, h \in T[x]$ (nemnulla) polinomok. Ekkor az $fu + gv = h$ kétismeretlenes lineáris „diofantoszi" egyenlet akkor és csak akkor oldható meg az ismeretlen $u, v \in T[x]$ polinomokra nézve, ha $\operatorname{lnko}(f,g) \mid h$. Ha (u_0, v_0) egy megoldás, akkor bármely $t \in T[x]$ esetén az alábbi (u, v) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a $t \in T[x]$ polinom alkalmas megválasztásával:

$$u = u_0 + \frac{g}{\operatorname{lnko}(f,g)} \cdot t; \qquad v = v_0 - \frac{f}{\operatorname{lnko}(f,g)} \cdot t.$$

Bizonyítás. A bizonyítás nagyon hasonló a 3.11. Tétel bizonyításához. Tegyük fel, hogy $f, g \neq 0$; ekkor $d := \operatorname{lnko}(f,g) \neq 0$. Először azt igazoljuk, hogy az egyenlet megoldhatóságának szükséges és elegendő feltétele $d \mid h$. Az elegendőség bizonyításához tegyük fel, hogy $d \mid h$; ekkor $h = dh_0$ alkalmas $h_0 \in T[x]$ polinommal. Először (5.3) szerint keressünk olyan $\widetilde{u}, \widetilde{v} \in T[x]$ polinomokat, amelyekre $d = f\widetilde{u} + g\widetilde{v}$, majd szorozzuk be mindkét oldalt h_0-lal: $h = dh_0 = f(\widetilde{u}h_0) + g(\widetilde{v}h_0)$. Ez azt jelenti, hogy $u = \widetilde{u}h_0$ és $v = \widetilde{v}h_0$ megoldása az egyenletnek. A másik irány igazolásához tegyük fel, hogy van megoldás, azaz $fu + gv = h$ teljesül valamely $u, v \in T[x]$ polinomokra. Tudjuk, hogy $d \mid f, g$ (miért?), és ebből következik, hogy $d \mid fu + gv = h$. Tehát a $d \mid h$ feltétel nemcsak elegendő, hanem szükséges is az egyenlet megoldhatóságához.

A tétel másik állításának igazolásához tegyük fel, hogy van egy (u_0, v_0) megoldásunk; tudjuk, hogy ekkor $d \mid h$. Írjuk fel szokás szerint az f, g polinomokat $f = f_0 d$, $g = g_0 d$ alakban. Jelölje M az egyenlet összes megoldásainak halmazát: $M = \{(u,v) : fu + gv = h\} \subseteq T[x] \times T[x]$. Azt kell bizonyítanunk, hogy

$$(u,v) \in M \iff \exists t \in T[x] : u = u_0 + g_0 t,\ v = v_0 - f_0 t.$$

A „$\Longrightarrow$" irány igazolásához tegyük fel, hogy $(u,v) \in M$. Korábban feltettük azt is, hogy (u_0, v_0) is egy megoldás, tehát $fu + gv = h = fu_0 + gv_0$. Rendezés után azt kapjuk, hogy $f(u - u_0) = g(v_0 - v)$. Itt a jobb oldal szemlátomást osztható g-vel, ezért $g \mid f(u - u_0)$. Ebből (5.5) alapján következik, hogy $g_0 \mid u - u_0$. Az oszthatóság definíciója szerint ez azt jelenti, hogy van olyan $t \in T[x]$ polinom, amelyre $u - u_0 = g_0 t$. Ezzel megkaptuk, hogy $u = u_0 + g_0 t$, a v-re vonatkozó formulát pedig egyszerű visszahelyettesítéssel nyerjük: $g(v_0 - v) = f(u - u_0) = fg_0 t$, tehát $v_0 - v = f_0 t$ (miért?), amiből rögtön adódik, hogy $v = v_0 - f_0 t$.

A „$\Longleftarrow$" irány igazolásához tegyük fel, hogy $u = u_0 + g_0 t,\ v = v_0 - f_0 t$. Csak be kell helyettesíteni az egyenetbe, hogy lássuk, hogy (u,v) valóban megoldás: $fu + gv = f(u_0 + g_0 t) + g(v_0 - f_0 t) = fu_0 + gv_0 + (fg_0 - gf_0)t = fu_0 + gv_0$ (miért lesz $fg_0 - gf_0 = 0$?), ez pedig valóban egyenlő h-val, hiszen feltettük, hogy (u_0, v_0) egy megoldása az egyenletnek. □

5.17. Példa. Számítsuk ki az f és g polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \operatorname{lnko}(f,g)$ egyenlet egy megoldását az $\mathbb{R}[x]$ polinomgyűrűben. Az lnko segítségével határozzuk meg f és g komplex gyökeit.

$$f = x^4 + 2x^3 - x^2 - 4x - 2, \qquad g = x^4 + x^3 - x^2 - 2x - 2$$

Megoldás: Hajtsuk végre az euklideszi algoritmust az f és g polinomokra (amelyik polinomnak van „neve", arra mindig a nevével hivatkozunk a jobb átláthatóság kedvéért):

	osztandó	=	hányados · osztó	+	maradék
(1)	f	=	$1 \cdot g$	+	$x^3 - 2x$
(2)	g	=	$(x+1) \cdot (x^3 - 2x)$	+	$\boxed{x^2 - 2}$
(3)	$x^3 - 2x$	=	$x \cdot (x^2 - 2)$	+	0

A legnagyobb közös osztó az utolsó nemnulla maradék: $\operatorname{lnko}(f,g) \sim \boxed{x^2 - 2}$. Ezzel a polinommal f és g is osztható:

$$f = \left(\boxed{x^2 - 2}\right) \cdot (x^2 + 2x + 1) \quad \text{és} \quad g = \left(\boxed{x^2 - 2}\right) \cdot (x^2 + x + 1).$$

Ebből rögtön megkapjuk f és g gyökeit (multiplicitással):

$$f \text{ gyökei: } \sqrt{2}, -\sqrt{2}, -1, -1; \qquad g \text{ gyökei: } \sqrt{2}, -\sqrt{2}, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Megfigyelhetjük, hogy f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f,g)$ gyökei.

[1] Figyelem: nem leosztunk, hanem egyszerűsítünk! A $T[x]$ polinomgyűrűben nincs definiálva az osztás művelete (a racionális törtek $T(x)$ testében már igen, de erre nincs szükségünk). Minden integritástartományban, így $T[x]$-ben is érvényes ez az egyszerűsítési szabály: ha $ac = bc$ és $c \neq 0$, akkor $a = b$. Ezt a nullosztómentességre támaszkodva könnyű igazolni (HF). A tételben szereplő $\frac{f}{\operatorname{lnko}(f,g)}$ kifejezést sem kell osztásként értelmezni; ez csak egy jelölés az f_0 polinomra.

A „diofantoszi” egyenlet megoldásához fejezzük ki a maradékot az euklideszi algoritmus során elvégzett mindegyik osztásnál (az utolsót kivéve):

		maradék	=	osztandó	−	hányados · osztó
(1)		x^3-2x	=	f	−	g
(2)	$\operatorname{lnko}(f,g)\sim$	$\boxed{x^2-2}$	=	g	−	$(x+1)\cdot(x^3-2x)$

Az a célunk, hogy mindegyik maradékot f és g segítségével írjuk fel ($fu+gv$ alakban). Az első osztás maradéka máris ilyen alakban van: $x^3-2x=f-g$. Ezt behelyettesíthetjük a második osztás maradékának fenti felírásában x^3-2x helyére:

$$\operatorname{lnko}(f,g)\sim\boxed{x^2-2}=g-(x+1)\cdot(x^3-2x)=g-(x+1)\cdot(f-g)=(-x-1)\cdot f+(x+2)\cdot g.$$

Ebből leolvashatjuk az $fu+gv=\operatorname{lnko}(f,g)$ egyenlet egy megoldását: $u=-x-1$, $v=x+2$.

Kongruenciareláció, maradékosztályok

5.18. Definíció. Tetszőleges $f,g,m\in T[x]$ polinomok esetén azt mondjuk, hogy f ***kongruens*** g ***-vel modulo*** m (jelölés: $f\equiv g\pmod m$), ha $m\mid f-g$.

5.19. Megjegyzés. Egész számoknál fel szoktuk tenni, hogy $m\geq 2$. Itt semmilyen kikötést nem tettünk a modulusra, ezért előfordulnak „degenerált” esetek is. Ha $m=0$, akkor $f\equiv g\pmod m\iff f=g$ (miért?). Ha pedig $m\sim 1$ (azaz m nemzéró konstans polinom), akkor $f\equiv g\pmod m$ teljesül minden $f,g\in T[x]$ esetén (miért?).

5.20. Tétel. Ha $0\neq m\in T[x]$, akkor tetszőleges $f,g\in T[x]$ polinomok esetén $f\equiv g\pmod m$ akkor és csak akkor teljesül, ha f és g ugyanazt a maradékot adja m-mel osztva.

Bizonyítás. A bizonyítás hasonló a 3.19. Tétel bizonyításához. Osszuk el f-et és g-t maradékosan m-mel: $f=mq_1+r_1$ és $g=mq_2+r_2$, ahol $\deg r_1,\deg r_2<\deg m$. Ekkor

$$f\equiv g\pmod m\iff m\mid f-g\iff m\mid m(q_1-q_2)+(r_1-r_2)\iff m\mid r_1-r_2\quad\text{(miért?)}.$$

Az r_1-r_2 polinom foka kisebb, mint m foka (ugye?), ezért $m\mid r_1-r_2$ akkor és csak akkor teljesülhet, ha $r_1-r_2=0$ (miért?). Azt kaptuk tehát, hogy $f\equiv g\pmod m\iff r_1-r_2=0$, és éppen ezt kellett igazolnunk. □

5.21. Példa. Tetszőleges $f,g\in T[x]$ polinomok esetén $f\equiv g\pmod x$ akkor és csak akkor teljesül, ha $f(0)=g(0)$, azaz f és g konstans tagja megegyezik.

5.22. Tétel. A mod m kongruencia ekvivalenciareláció $T[x]$-en (azaz reflexív, szimmetrikus és tranzitív), továbbá tetszőleges $f_1,g_1,f_2,g_2\in T[x]$ esetén érvényesek az alábbiak:

$$\left.\begin{matrix}f_1\equiv g_1\pmod m\\ f_2\equiv g_2\pmod m\end{matrix}\right\}\implies f_1\pm f_2\equiv g_1\pm g_2,\quad f_1\cdot f_2\equiv g_1\cdot g_2\pmod m.$$

Bizonyítás. A bizonyítás nagyon hasonló a 3.21 . Tétel megfelelő részeinek bizonyításához; itt is ugyanúgy lehet visszavezetni a kongruencia tulajdonságait az oszthatóság tulajdonságaira, mint az egész számok körében (HF). □

5.23. Tétel. Tetszőleges $f,g,h\in T[x]$ esetén az $fu\equiv h\pmod m$ ***lineáris kongruencia*** akkor és csak akkor oldható meg (az ismeretlen $u\in T[x]$ polinomra nézve), ha $\operatorname{lnko}(f,m)\mid h$.

Bizonyítás. A bizonyítás nagyon hasonló a 3.26. Tétel (első állításának) bizonyításához; itt is ugyanúgy lehet visszavezetni a lineáris kongruenciát kétismeretlenes lineáris „diofantoszi” egyenletre, mint az egész számok körében (HF). □

5.24. Definíció. A mod m kongruenciához tartozó ekvivalenciaosztályokat modulo m ***maradékosztályoknak*** nevezzük. Az $f\in T[x]$ polinomot tartalmazó modulo m maradékosztályt $\overline{f}$ jelöli: $\overline{f}=\{g\in T[x]\colon f\equiv g\pmod m\}$. A maradékosztályok halmazát (vagyis a modulo m kongruenciához tartozó faktorhalmazt) $T[x]/(m)$ jelöli, azaz $T[x]/(m)=\{\overline{f}:f\in T[x]\}$.

5.25. Megjegyzés. A $T[x]/(m)$ halmaz a $\mathbb{Z}_m$ halmaz analogonja, csak itt kicsit csúnyább a jelölés. A jelölésnek megvan a pontos magyarázata: (m) jelöli az m polinom által generált *főideált* a $T[x]$ polinomgyűrűben, $T[x]/(m)$ pedig az ehhez az ideálhoz tartozó *faktorgyűrűje* $T[x]$-nek. Ezeket a fogalmakat majd absztrakt algebrából tanuljuk. (Lehetne $\mathbb{Z}_m$ helyett is $\mathbb{Z}/(m)$-et írni, de ott szokás az egyszerűbb $\mathbb{Z}_m$ jelölést használni.)

5.26. Példa. Az 5.21. Példa szerint $m=x$ esetén $\overline{f}=\{g\in T[x]:g(0)=f(0)\}$, ezért a modulo m maradékosztályok bijektíven megfelelnek T elemeinek. Így például $\mathbb{R}[x]/(x)$ végtelen halmaz (ellentétben $\mathbb{Z}_m$-mel, ami mindig véges).

5.27. Definíció. A modulo m maradékosztályok halmazán értelmezzük az összeadást és a szorzást a következőképpen: tetszőleges $f,g\in T[x]$ esetén legyen $\overline{f}\oplus\overline{g}=\overline{f+g}$, $\overline{f}\odot\overline{g}=\overline{f\cdot g}$.

5.28. Állítás. A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel $T[x]/(m)$ kommutatív egységelemes gyűrűt alkot (***maradékosztály-gyűrű***). Ha $\deg m = n \geq 1$, akkor a $T[x]/(m)$ maradékosztály-gyűrű minden eleme egyértelműen felírható az alábbi alakban:

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} \qquad (a_{n-1}, \ldots, a_1, a_0 \in T).$$

Bizonyítás. A bizonyítás nagyon hasonló a 3.46. Tétel bizonyításához; itt is a kongruencia tulajdonságai (5.22. Tétel) garantálják, hogy a maradékosztályok összege és szorzata jóldefiniált, és itt is ugyanúgy lehet visszavezetni a műveleti tulajdonságokat a $T[x]$ gyűrűbeli tulajdonságokra, mint ahogy a $\mathbb{Z}_m$ halmazon definiált műveletek tulajdonságait visszavezettük az egész számok megfelelő műveleti tulajdonságaira (HF). A tétel utolsó állítása annak a ténynek az analogonja, hogy $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, és azon múlik, hogy ha egy tetszőleges $f \in T[x]$ polinomot maradékosan osztunk az n-edfokú m polinommmal, akkor a maradék mindig egy legfeljebb $(n-1)$-edfokú polinom lesz, továbbá a maradék egyértelműen meghatározott. Tehát minden $f \in T[x]$ polinomhoz létezik egy és csak egy $f_1 \in T[x]$ polinom, amelyre $f \equiv f_1 \pmod{m}$ és $\deg f_1 \leq n-1$. □

5.29. Példa. A $\mathbb{Z}_2[x]/(x^2+x+1)$ maradékosztály-gyűrűnek 4 eleme van: $\mathbb{Z}_2[x]/(x^2+x+1) = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$. Írjuk fel ennek a gyűrűnek az összeadó- és szorzótábláját:

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

5.30. Példa. A $\mathbb{Z}_5[x]/(x^3+x^2+3)$ maradékosztály-gyűrű elemei egyértelműen felírhatóak $\overline{ax^2+bx+c}$ $(a,b,c \in \mathbb{Z}_5)$ alakban, tehát ennek a gyűrűnek 125 eleme van.

5.31. Példa. Az $\mathbb{R}[x]/(x^2+1)$ maradékosztály-gyűrű elemei egyértelműen felírhatóak $\overline{a+bx}$ $(a,b \in \mathbb{R})$ alakban. Az összeadás és a szorzás így végezhető ebben a gyűrűben:

$$\overline{a+bx} + \overline{c+dx} = \overline{(a+c)+(b+d)x},$$
$$\overline{a+bx} \cdot \overline{c+dx} = \overline{ac+(ad+bc)x+bdx^2} = \overline{ac+(ad+bc)x+bd(-1)} = \overline{(ac-bd)+(ad+bc)x}.$$

(A szorzat kiszámolásakor felhasználtuk azt, hogy $x^2 \equiv -1 \pmod{x^2+1}$, azaz $\overline{x}^2 = \overline{-1}$.) Látjuk tehát, hogy $\mathbb{R}[x]/(x^2+1)$ lényegében ugyanaz, mint a komplex számtest (szaknyelven: $\mathbb{R}[x]/(x^2+1)$ *izomorf* $\mathbb{C}$-vel).

5.32. Definíció. Azt mondjuk, hogy az $\overline{f}, \overline{g} \in T[x]/(m)$ maradékosztályok egymás ***multiplikatív inverzei***, ha $\overline{f} \cdot \overline{g} = \overline{1}$.

5.33. Tétel. Az $\overline{f} \in T[x]/(m)$ maradékosztálynak akkor és csak akkor létezik multiplikatív inverze, ha f és m relatív prímek.

Bizonyítás. A bizonyítás nagyon hasonló a 3.29 . Tétel bizonyításához; itt is a lineáris kongruencia megoldhatósági kritériumát (5.23 . Tétel) kell alkalmazni (HF). □

5.34. Példa. Az 5.29. Példában $\overline{x}$ és $\overline{x+1}$ egymás multiplikatív inverzei (és persze $\overline{1}$ inverze önmaga).

Irreducibilis polinomok, irreducibilis faktorizáció (jórészt ismétlés)

5.35. Definíció (ism.). A $p \in T[x]$ polinom ***irreducibilis***, ha legalább elsőfokú, és csak úgy bontható két polinom szorzatára, hogy az egyik tényező asszociált p-hez. (Ekkor a másik tényező szükségképpen asszociált 1-hez; ilyenkor ***triviális faktorizációról*** beszélünk.) Formálisan:

$$\forall f, g \in T[x] : p = fg \implies (p \sim f \text{ vagy } p \sim g).$$

5.36. Állítás (ism.). Legyen T egy test és $p \in T[x]$. A p polinom akkor és csak akkor irreducibilis T felett, ha legalább elsőfokú, és nem bontható $\deg p$-nél kisebb fokszámú polinomok szorzatára:

$$\nexists f, g \in T[x] : \; p = f \cdot g \quad \text{és} \quad 1 \leq \deg f, \deg g < \deg p.$$

5.37. Megjegyzés. Gyűrűk felett ez általában nem igaz! Például a $p = 2x \in \mathbb{Z}[x]$ polinom nem bontható kisebb fokszámú polinomok szorzatára (ugye?), de mégsem irreducibilis $\mathbb{Z}$ felett, mert a $p = 2 \cdot x$ felbontás itt nem triviális (miért?).

5.38. Definíció (ism.). A $p \in T[x]$ polinom ***prím***, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall f, g \in T[x] : p \mid fg \implies (p \mid f \text{ vagy } p \mid g).$$

5.39. Tétel (ism.). Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

5.40. Tétel (ism.). Test feletti polinomgyűrűben minden legalább elsőfokú polinom felbomlik irreducibilis polinomok szorzatára, és ez a felbontás lényegében (azaz a tényezők sorrendjétől és asszociáltságtól eltekintve) egyértelmű.

5.41. Megjegyzés. A felbontás tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű voltát a következőképpen lehet permutációk segítségével precízen megfogalmazni: Ha $p_1 \cdot \ldots \cdot p_n$ és $q_1 \cdot \ldots \cdot q_m$ ugyanazon polinom két irreducibilis faktorizációja, akkor $n = m$, és létezik olyan $\pi \in S_n$ permutáció, hogy $p_i \sim q_{\pi(i)}$ minden $i = 1, \ldots, n$ esetén.

5.42. Tétel. A $T[x]/(m)$ maradékosztály-gyűrű akkor és csak akkor test, ha m irreducibilis T felett.

Bizonyítás. A bizonyítás nagyon hasonló a 3.56. Következmény bizonyításához; csak a „degenerált” eseteket külön meg kell nézni.

(1) Ha $m \sim 1$, akkor m nem irreducibilis, és $T[x]/(m)$ valóban nem test, mert csak egyetlen eleme van (miért?).

(2) Ha $m = 0$, akkor m megint csak nem irreducibilis, és $T[x]/(m)$ valóban nem test. Ennek igazolásához idézzük fel, hogy a modulo 0 kongruencia nem más, mint az egyenlőség reláció (lásd az 5.19. Megjegyzést). Tehát például az $\overline{x} \neq \overline{0}$ maradékosztálynak nincs multiplikatív inverze, mert a multiplikatív inverz egy olyan $\overline{u}$ maradékosztály lenne, amelyre $\overline{x} \cdot \overline{u} = \overline{1}$, azaz $xu = 1$, de ilyen $u \in T[x]$ polinom nem létezik (miért?). (Megjegyzés: ha $m = 0$, akkor minden $f \in T[x]$ polinomra $\overline{f} = \{f\}$, tehát $T[x]/(m)$ lényegében ugyanaz, mint $T[x]$; szaknyelven: a $T[x]/(m)$ és $T[x]$ gyűrűk *izomorfak* egymással.)

(3) Ha $\deg m \geq 1$ és m nem irreducibilis, akkor van nemtriviális felbontása: $m = fg$, ahol $1 \leq \deg f, \deg g < \deg m$ (lásd az 5.36. Állítást). Ekkor $\overline{f}, \overline{g} \neq \overline{0}$, de $\overline{f} \cdot \overline{g} = \overline{0}$, tehát $T[x]/(m)$ nem test, sőt, még csak nem is integritástartomány (miért?).

(4) Ha m irreducibilis, akkor $T[x]/(m)$ kommutatív egységelemes gyűrű, amelynek legalább két eleme van (miért?), tehát ahhoz, hogy belássuk, hogy $T[x]/(m)$ test, elég ellenőrizni, hogy minden nemnulla elemének van multiplikatív inverze (ugye?). Legyen tehát $\overline{0} \neq \overline{f} \in T[x]/(m)$, és keressük $\overline{f}$ multiplikatív inverzét. Mivel m irreducibilis és $m \nmid f$, ezért $f \perp m$ (miért?). Az 5.33. Tétel szerint ekkor $\overline{f}$-nak valóban létezik multiplikatív inverze.

□

5.43. Példa. Az 5.29. Példában szereplő $\mathbb{Z}_2[x]/(x^2 + x + 1)$ gyűrű test, mert $x^2 + x + 1$ irreducibilis $\mathbb{Z}_2$ felett (ugye?). Persze a szorzótáblából is látszik, hogy minden nemnulla elemnek van multiplikatív inverze.

5.44. Példa. Az 5.30. Példában szereplő $\mathbb{Z}_5[x]/(x^3 + x^2 + 3)$ maradékosztály-gyűrű nem test, mert $x^3 + x^2 + 3$ nem irreducibilis $\mathbb{Z}_5$ felett: $x^3 + x^2 + 3 = (x - 1)(x^2 + 2x + 2)$. Ebből a felbontásból az is következik, hogy $\overline{x - 1}$ és $\overline{x^2 + 2x + 2}$ zérusosztók: $\overline{x - 1} \cdot \overline{x^2 + 2x + 2} = \overline{0}$.

5.45. Példa. Az 5.31. Példában szereplő $\mathbb{R}[x]/(x^2 + 1)$ maradékosztály-gyűrű test, mert $x^2 + 1$ irreducibilis $\mathbb{R}$ felett (ugye?). Persze ez abból is következik, hogy $\mathbb{R}[x]/(x^2 + 1)$ izomorf a komplex számtesttel.

5.46. Állítás (ism.). Tetszőleges T testre és $f \in T[x]$ polinomra . . .

- $\deg f = 1$ esetén f irreducibilis T felett, és van gyöke T-ben;
- $\deg f \in \{2, 3\}$ esetén f pontosan akkor irreducibilis T felett, ha nincs gyöke T-ben;
- $\deg f \geq 4$ esetén ha f irreducibilis T felett, akkor nincs gyöke T-ben.

5.47. Megjegyzés (ism.). Az utolsó pontbeli implikáció megfordítása nem igaz: ha $\deg f \geq 4$, akkor önmagában az a tény, hogy f-nek nincs gyöke T-ben még nem garantálja, hogy f irreducibilis T felett (keressünk példát!).

5.48. Tétel (ism.). Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

5.49. Következmény (ism.). A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

5.50. Következmény (ism.). Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n(x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom ***gyöktényezős felbontásának***.

5.51. Tétel (ism.). Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az $\mathbb{R}$ feletti irreducibilis polinomok a következők:

- $ax + b$ $(a, b \in \mathbb{R}, a \neq 0)$;
- $ax^2 + bx + c$ $(a, b, c \in \mathbb{R}, a \neq 0, b^2 - 4ac < 0)$.

Elemi törtekre bontás

5.52. Definíció. A T test feletti ***racionális törtön*** $\frac{f}{g}$ alakú formális kifejezést értünk, ahol $f, g \in T[x]$ és $g \neq 0$. Minden racionális törthöz tartozik egy ***racionális törtfüggvény*** (a két fogalom nem összekeverendő!). A T feletti racionális törtek halmazát $T(x)$ jelöli.

5.53. Definíció. A T test felett ***elemi törtnek*** (vagy parciális törtnek) olyan racionális törtet nevezünk, amelyben a nevező T felett irreducibilis (fő)polinom hatványa, és a számláló foka kisebb ezen irreducibilis polinom fokánál:

$$\frac{f}{p^k} \in T(x), \quad \text{ahol } f, p \in T[x],\ k \in \mathbb{N},\ p \text{ irreducibilis } T \text{ felett},\ \deg f < \deg p.$$

5.54. Tétel. Tetszőleges T test felett minden racionális tört felírható egy polinom és elemi törtek összegeként.

5.55. Következmény. A komplex számok teste felett minden racionális tört felírható egy polinom és véges sok

$$\frac{A}{(x+a)^k} \quad (A, a \in \mathbb{C},\ k \in \mathbb{N})$$

alakú racionális tört összegeként.

5.56. Következmény. A valós számok teste felett minden racionális tört felírható egy polinom és véges sok

$$\frac{A}{(x+a)^k} \quad (A, a \in \mathbb{R},\ k \in \mathbb{N}), \qquad \text{és} \qquad \frac{Bx+C}{(x^2+bx+c)^k} \quad (B, C, b, c \in \mathbb{R},\ b^2-4c<0,\ k \in \mathbb{N})$$

alakú racionális tört összegeként.

Irreducibilis polinomok a racionális számtest felett

5.57. Tétel (Rolle(?) tétele). Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és $p \perp q$), akkor

$$f\left(\tfrac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Bizonyítás. Tfh. $f\left(\frac{p}{q}\right) = 0$, ahol $p, q \in \mathbb{Z}$, $q \neq 0$ és $p \perp q$. Írjuk fel az $f\left(\frac{p}{q}\right)$ helyettesítési értéket:

$$f\left(\frac{p}{q}\right) = a_n \cdot \frac{p^n}{q^n} + a_{n-1} \cdot \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \cdot \frac{p}{q} + a_0 = 0.$$

Mindkét oldalt q^n–nel beszorozva azt kapjuk, hogy

$$\underbrace{a_n \cdot p^n + a_{n-1} \cdot p^{n-1} q + \cdots + a_1 \cdot p q^{n-1}}_{p|} + a_0 \cdot q^n = 0.$$

Itt az utolsó kivételével minden tag osztható p-vel, így $p \mid a_0 \cdot q^n$ (ugye?). Mivel p és q^n relatív prímek (miért?), az következik, hogy $p \mid a_0$ (miért?). Hasonlóan (a fenti összeg első tagját vizsgálva) belátható, hogy $q \mid a_n$ (HF). □

5.58. Példa. Keressük meg az $f = 2x^5 + 3x^4 - 7x^3 - 3x^2 + 8x - 12$ polinom racionális gyökeit. Az 5.57. Tétel szerint minden racionális gyök megkapható p/q alakban, ahol $q \mid 2$ és $p \mid 12$. Itt q-ra 4 lehetőség van, p-re pedig 12 lehetőség van (ugye?), tehát elvileg $4 \cdot 12 = 48$ törtet tudnánk felírni, de feltehetjük, hogy $q > 0$ és $p \perp q$ (miért?), így „csak" a következő 16 számot kell megvizsgálnunk: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm\frac{1}{2}, \pm\frac{3}{2}$. Egyenként behelyettesítve őket (pl. Horner-módszerrel), azt kapjuk, hogy -2 kétszeres gyök, $\frac{3}{2}$ pedig egyszeres gyök, és ezeken kívül más racionális gyök nincs. Ha Horner-módszerrel dolgoztunk, akkor rögtön ki is tudjuk emelni a megfelelő gyöktényezőket:

$$f = \big(x - (-2)\big)^2 \Big(x - \frac{3}{2}\Big)(2x^2 - 2x + 2) = (x+2)^2(2x-3)(x^2 - x + 1).$$

Mivel f minden racionális gyökét „leválasztottuk" (a megfelelő multiplicitásokkal), az $x^2 - x + 1$ polinomnak már nincs racionális gyöke (meg lehetne vizsgálni az 5.57. Tétellel, de felesleges). Másodfokú polinomok esetén a „gyöknélküliségből" következik az irreducibilitás (lásd az 5.46. Tételt), ezért az $x^2 - x + 1$ polinom irreducibilis $\mathbb{Q}$ felett, tehát a fenti felbontás valójában az f polinom irreducibilis faktorizációja $\mathbb{Q}[x]$-ben.

5.59. Tétel. Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\nexists g, h \in \mathbb{Z}[x] : f = gh$ és $0 < \deg g, \deg h < n$;
(2) $\nexists g, h \in \mathbb{Q}[x] : f = gh$ és $0 < \deg g, \deg h < n$.

Bizonyítás. Az egyik irány teljesen triviális (melyik az, és miért triviális?), a másik viszont nehéz (Gauss kell hozzá!), azt nem bizonyítjuk. □

5.60. Megjegyzés. A második feltétel azzal ekvivalens, hogy f irreducibilis $\mathbb{Q}$ felett. Az első viszont *nem* ekvivalens azzal, hogy f irreducibilis $\mathbb{Z}$ felett (miért?). Tehát a fenti tételt *nem* fogalmazhatjuk meg egyszerűen úgy, hogy egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett, ha irreducibilis $\mathbb{Q}$ felett.

5.61. Definíció. Azt mondjuk, hogy a p prímszám ***pontos osztója*** az a egész számnak, ha a osztható p-vel, de p^2-tel már nem.

Jelölés. A pontos oszthatóságot $\parallel$ jelöli: $p \parallel a \iff p \mid a$ és $p^2 \nmid a$.

5.62. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ p \mid a_{n-1}, \ldots,\ p \mid a_1,\ p \parallel a_0,$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás. Tfh. az f polinom együtthatóira teljesülnek a fenti oszthatósági feltételek, de ennek ellenére f nem irreducibilis $\mathbb{Q}$ felett. Ekkor léteznek olyan g_1, h_1 *racionális együtthatós* polinomok, amelyekre $f = g_1 h_1$ és $0 < \deg g_1, \deg h_1 < n$ (miért?). Az 5.59 . Tétel szerint vannak olyan g, h *egész együtthatós* polinomok, amelyekre $f = gh$ és $0 < \deg g, \deg h < n$. Legyen $g = b_k x^k + \cdots + b_1 x + b_0$ és $h = c_\ell x^\ell + \cdots + c_1 x + c_0$, és írjuk fel sorra az $f = gh$ egyenlőség mindkét oldalának együtthatóit. A konstans tag: $a_0 = b_0 c_0$ (ugye?), és tudjuk, hogy ez osztható p-vel, így $p \mid b_0$ vagy $p \mid c_0$ (miért?). Ha b_0 is és c_0 is osztható lenne p-vel, akkor $p^2 \mid a_0$, ami ellentmond a $p \parallel a_0$ feltevésnek (ugye?). Tehát b_0 és c_0 közül egyik osztható p-vel, a másik nem. Csak a $p \mid b_0,\ \ p \nmid c_0$ esetet vizsgáljuk; a másik eset hasonló (HF). Az $f = gh$ egyenlőségben az elsőfokú tagok együtthatói azt adják, hogy $a_1 = b_0 c_1 + b_1 c_0$. Mivel $p \mid a_1$ és $p \mid b_0$, ebből következik, hogy $p \mid b_1 c_0$ (ugye?). Feltettük, hogy $p \nmid c_0$, ezért $p \mid b_1$ (miért?). Tehát már tudjuk, hogy p osztja a g polinomban a b_0 és b_1 együtthatókat. Nézzük most a másodfokú tagokat az $f = gh$ egyenlőségben: $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$. Itt $b_2 c_0$ kivételével minden tagról tudjuk már, hogy osztható p-vel, ezért $p \mid b_2 c_0$ (ugye?). Ismét felhasználva, hogy $p \nmid c_0$, azt kapjuk, hogy $p \mid b_2$ (miért?). Most már tudjuk, hogy $p \mid b_0, b_1, b_2$, és ebből a harmadfokú tagokat vizsgálva levezethetjük, hogy $p \mid b_3$:

$$p \mid a_3 = b_0 c_3 + b_1 c_2 + b_2 c_1 + b_3 c_0 \overset{\text{miért?}}{\Longrightarrow} p \mid b_3 c_0 \overset{\text{miért?}}{\Longrightarrow} p \mid b_3.$$

Folytatva ezt a gondolatmenetet, sorra megkapjuk, hogy a $b_0, b_1, \ldots, b_k$ együtthatók mind oszthatók p-vel. Az utolsó lépés így fest:

$$p \mid a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_{k-1} c_1 + b_k c_0 \overset{\text{miért?}}{\Longrightarrow} p \mid b_k c_0 \overset{\text{miért?}}{\Longrightarrow} p \mid b_k.$$

Nézzük végül az n-edfokú tagot az $f = gh$ egyenlőségben: $a_n = b_k c_\ell$ (ugye?). Mivel $p \mid b_k$, ez ellentmond a $p \nmid a_n$ feltevésnek, tehát az f felbonthatóságára vonatkozó indirekt feltevésünk helytelen volt. (Keresztkérdés: Hol használtuk ki, hogy $0 < \deg g, \deg h < n$?) □

5.63. Példa. Az $f = 3x^{100} - 10x^{50} + 100x - 50$ polinomra alkalmazható a fenti tétel (a $p = 2$ prímszámmal), ezért f irreducibilis $\mathbb{Q}$ felett.

5.64. Következmény. Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás. Minden $n \in \mathbb{N}$ esetén az $x^n + 2$ polinom irreducibilis $\mathbb{Q}$ felett (miért?). □

5.65. Megjegyzés. A Schönemann–Eisenstein-tétel megfordítása nem igaz. Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, *nem következik*, hogy a polinom nem irreducibilis (keressünk ellenpéldát!). A megfordítás helyett következzék inkább a tétel „tükörképe" .

5.66. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \parallel a_n, p \mid a_{n-1}, \ldots, p \mid a_1, p \nmid a_0$, akkor f irreducibilis a racionális számok teste felett.

Szimmetrikus polinomok

5.67. Tétel (ism.). Legyenek az n-edfokú $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ főpolinom komplex gyökei $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:

$$\begin{aligned}
-a_{n-1} &= \alpha_1 + \alpha_2 + \cdots + \alpha_n;\\
a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n;\\
-a_{n-3} &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n;\\
&\vdots\\
(-1)^{n-1}a_1 &= \alpha_1\alpha_2\cdots\alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2\cdots\alpha_{n-2}\alpha_n + \cdots + \alpha_2\alpha_3\cdots\alpha_{n-1}\alpha_n;\\
(-1)^n a_0 &= \alpha_1\alpha_2\alpha_3\cdots\alpha_{n-1}\alpha_n.
\end{aligned}$$

5.68. Megjegyzés (ism.). A fenti képleteket ***Viète-formuláknak*** hívjuk. A k-adik sor bal oldalán $(-1)^k a_{n-k}$ áll, a jobb oldalon pedig az $\alpha_1, \dots, \alpha_n$ betűkből képezett összes k-tényezős szorzat összege, tehát egy $\binom{n}{k}$-tagú összeg. Formálisan:

$$(-1)^k a_{n-k} \;=\; \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} \alpha_{i_1} \cdot \alpha_{i_2} \cdot \ldots \cdot \alpha_{i_k}.$$

5.69. Definíció. Adott T test feletti ***n-határozatlanú monomnak*** nevezzük az $a x_1^{k_1} \cdots x_n^{k_n}$ alakú formális kifejezéseket, ahol $0 \neq a \in T$ és $k_1, \dots, k_n \in \mathbb{N}_0$. Az ilyen monomok véges összegeit pedig T feletti ***n-határozatlanú polinomoknak*** nevezzük.

Jelölés. A T feletti n-határozatlanú polinomok halmazát $T[x_1, \dots, x_n]$ jelöli.

5.70. Tétel. A természetes módon definiált szorzással és összeadással $T[x_1, \dots, x_n]$ integritástartomány.

5.71. Megjegyzés. Az n-határozatlanú polinomok gyűrűjét lehetne rekurzívan is definiálni: legyen

$$T[x_1, \dots, x_n] = (T[x_1, \dots, x_{n-1}])[x_n],$$

azaz a $T[x_1, \dots, x_{n-1}]$ integritástartomány feletti (egyhatározatlanú) polinomgyűrű.

5.72. Definíció. Az $f \in T[x_1, \dots, x_n]$ polinomot ***szimmetrikus polinomnak*** nevezzük, ha invariáns a határozatlanok minden permutációjára, azaz

$$\forall \pi \in S_n : f(x_{1\pi}, \dots, x_{n\pi}) = f(x_1, \dots, x_n).$$

5.73. Definíció. A k-adik n-határozatlanú ***elemi szimmetrikus polinom*** az $x_1, \dots, x_n$ határozatlanokból képezett összes k-tényezős szorzatok összege ($k = 1, \dots, n$).

Jelölés. A k-adik n-határozatlanú elemi szimmetrikus polinomot σ_k jelöli (az alaptest és n értéke általában világos a szövegkörnyezetből), tehát

$$\sigma_k \;=\; \sum_{1 \le i_1 < i_2 < \dots < i_k \le n} x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k} \;\in T[x_1, \dots, x_n].$$

5.74. Megjegyzés. Az elemi szimmetrikus polinomokkal már találkoztunk: segítségükkel fejezhetők ki egy komplex együtthatós főpolinom együtthatói a polinom gyökeiből. Tehát a Viète-formulák $\sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k a_{n-k}$ alakban is felírhatók.

5.75. Tétel. A szimmetrikus polinomok részgyűrűt alkotnak a $T[x_1, \dots, x_n]$ polinomgyűrűben.

5.76. Tétel (a szimmetrikus polinomok alaptétele). Bármely szimmetrikus polinom felírható, mégpedig egyetlen módon, az elemi szimmetrikus polinomok polinomjaként. Formálisan:

$$\forall f \in T[x_1, \dots, x_n] : f \text{ szimmetrikus} \implies \exists! h \in T[x_1, \dots, x_n] : f = h(\sigma_1, \dots, \sigma_n).$$

Algebrai és transzcendens számok

5.77. Definíció. Az α komplex számot ***algebrai számnak*** nevezzük, ha gyöke valamely nemzéró racionális együtthatós polinomnak. A nem algebrai számokat ***transzcendens számoknak*** nevezzük.

5.78. Definíció. Ha $f \in \mathbb{Q}[x]$ minimális fokszámú mindazon nemzéró racionális együtthatós főpolinomok között, melyeknek α gyöke, akkor f-et az α algebrai szám ***minimálpolinomjának*** nevezzük.

5.79. Tétel. Algebrai szám minimálpolinomja mindig egyértelműen meghatározott, és irreducibilis a racionális számtest felett. Továbbá, ha $f \in \mathbb{Q}[x]$ olyan irreducibilis főpolinom melynek az α algebrai szám gyöke, akkor f megegyezik α minimálpolinomjával.

5.80. Tétel. Létezik transzcendens szám.

5.81. Megjegyzés. A fenti tételt a megfelelő halmazelméleti ismeretek birtokában nem nehéz bebizonyítani: komplex számból „több” van, mint algebrai számból. (Az algebrai számok halmaza megszámlálhatóan végtelen, $\mathbb{C}$ viszont kontinuum számosságú.) Ez egy ún. *nemkonstruktív egzisztenciabizonyítás*: igazolja, hogy van transzcendens szám (sőt, a komplex (vagy valós) számok „túlnyomó többsége” transzcendens), de nem mutat egyetlen példát sem transzcendens számra. Nem könnyű feladat egy konkrét számról belátni, hogy transzcendens. Az ilyen bizonyítások általában azt használják fel, hogy algebrai számokat nem lehet nagyon jól közelíteni racionális számokkal (lásd az 5.86. Tételt). Ez a *diofantoszi approximáció* témaköre: adott α valós számhoz szeretnénk olyan $\frac{p}{q}$ közelítő törtet találni ($p, q \in \mathbb{Z}, q > 0, p \perp q$), amelyre $\left|\alpha - \frac{p}{q}\right|$ kicsi, és q nem túl nagy.

5.82. Tétel (Dirichlet approximációs tétele). Minden α valós szám és minden N természetes szám esetén van α-nak olyan $\frac{p}{q}$ közelítése, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq} \quad \text{és} \quad q \le N.$$

5.83. Következmény. Ha α irracionális szám, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

5.84. Állítás. Ha α racionális szám, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

5.85. Tétel (Hurwitz). Ha α irracionális szám, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Ha $\alpha = \frac{1+\sqrt{5}}{2}$, akkor az állítás nem javítható: nem írhatunk a nevezőbe semmilyen $\sqrt{5}$-nél nagyobb számot.

5.86. Tétel (Liouville, Thue, Siegel, Roth). Ha α irracionális algebrai szám és $\varepsilon > 0$, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}.$$

5.87. Tétel. Az algebrai számok résztestet alkotnak a komplex számok testében.

5.88. Tétel. Ha α algebrai szám és $n \geq 2$, akkor $\sqrt[n]{\alpha}$ is algebrai szám (a gyöknek mind az n értékére).

5.89. Definíció. Az α komplex számot ***gyökmennyiségnek*** nevezzük, ha megkapható racionális számokból kiindulva a négy alapművelet (összeadás, kivonás, szorzás, osztás) és egész kitevős gyökvonás véges számú alkalmazásával.

5.90. Következmény. A gyökmennyiségek algebrai számok.

5.91. Tétel. Van olyan algebrai szám, ami nem gyökmennyiség.

A fenti ártatlannak látszó tételből következik, hogy nem minden egyenlet oldható meg gyökjelek segítségével. Az ötödfokú egyenletnek már nincs általános megoldóképlete, sőt, például az $x^5 - 4x + 2 = 0$ egyenletnek még „ad hoc” megoldóképlete sincs, mert gyökei nem gyökmennyiségek.

5.92. Tétel. Az algebrai számok teste algebrailag zárt, azaz ha $\alpha \in \mathbb{C}$ gyöke a legalább elsőfokú $f = a_n x^n + \cdots + a_1 x + a_0$ polinomnak, ahol $a_0, \ldots, a_n$ algebrai számok, akkor α maga is algebrai szám.

6. Nevezetes számelméleti problémák

Számok felbontása hatványok összegére

6.1. Definíció. Az $(x, y, z) \in \mathbb{N}^3$ számhármast ***pitagoraszi számhármasnak*** nevezzük, ha $x^2 + y^2 = z^2$. Az (x, y, z) pitagoraszi számhármas ***primitív***, ha $\operatorname{lnko}(x, y, z) \sim 1$.

6.2. Megjegyzés. Tetszőleges (x, y, z) pitagoraszi számhármas esetén $(x/d, y/d, z/d)$ primitív pitagoraszi számhármas, ahol $d = \operatorname{lnko}(x, y, z)$. Tehát elegendő a primitív pitagoraszi számhármasokat meghatározni, mert ezekből minden pitagoraszi számhármas megkapható (egy konstanssal való szorzással).

6.3. Lemma. Primitív pitagoraszi számhármasban a tagok páronként is relatív prímek.

Bizonyítás. Legyen (x, y, z) primitív pitagoraszi számhármas, és legyen $d = \operatorname{lnko}(x, y)$. Ekkor $d \mid x, y$, és így $d^2 \mid x^2, y^2$ (ugye?), tehát $d^2 \mid x^2 + y^2 = z^2$. Ebből következik, hogy $d \mid z$ (miért?), azaz d osztja mindhárom számot, vagyis $d \mid \operatorname{lnko}(x, y, z) \sim 1$ (hiszen (x, y, z) *primitív* pitagoraszi számhármas). Tehát $d \sim 1$, és ezzel beláttuk, hogy x és y relatív prím. Hasonlóan igazolható, hogy $x \perp z$ és $y \perp z$ (HF). □

6.4. Lemma. Ha (x, y, z) primitív pitagoraszi számhármas, akkor x és y paritása különböző, z pedig páratlan.

Bizonyítás. Páros szám négyzete nullát, páratlan szám négyzete pedig egyet ad maradékul 4-gyel osztva (miért?). Ezt felhasználva négy esetet különböztethetünk meg:

$x \bmod 2$	$y \bmod 2$	$x^2 + y^2 = z^2 \bmod 4$
0	0	0
0	1	1
1	0	1
1	1	2

Az utolsó eset lehetetlen, mert, ahogy fent megfigyeltük, z^2 csak nullát vagy egyet adhat maradékul 4-gyel osztva. Az első esetben x, y, z mind párosak, és ez ellentmond annak, hogy (x, y, z) *primitív* pitagoraszi számhármas. Tehát csak a középső két eset fordulhat elő, és éppen ezt kellett igazolnunk. □

6.5. Lemma. Ha U és V relatív prím természetes számok, és UV négyzetszám, akkor U és V is négyzetszám.

Bizonyítás. Tekintsük U és V prímhatványtényezős felbontását: $U=\prod p_i^{\alpha_i}$, $V=\prod q_j^{\beta_j}$. Mivel U és V relatív prím, nincs közös prímosztójuk, vagyis az UV szorzat kiszámításakor nem lehet összevonni azonos alapú hatványokat; UV prímhatványtényezős felbontását egyszerűen U és V felbontását egymás mellé illesztve kapjuk: $UV=\prod p_i^{\alpha_i}\cdot\prod q_j^{\beta_i}$. Tudjuk, hogy UV négyzetszám, ezért prímhatványtényezős felbontásában minden kitevő páros (miért?), azaz minden α_i és minden β_j kitevő páros. Ez pedig azt jelenti, hogy U is és V is négyzetszám (ugye?). □

6.6. Tétel. Legyen (x,y,z) primitív pitagoraszi számhármas, és tegyük fel, hogy x páros. Ekkor léteznek olyan u,v természetes számok, melyekre

$$u>v,\ u\not\equiv v\pmod 2,\ u\perp v, \text{ és } x=2uv,\ y=u^2-v^2,\ z=u^2+v^2. \qquad (\triangle)$$

Fordítva, a fenti formulákkal definiált (x,y,z) számhármas mindig primitív pitagoraszi számhármas.

Bizonyítás. Először azt mutatjuk meg, hogy minden primitív pitagoraszi számhármas előáll a fenti módon. Tfh. (x,y,z) primitív pitagoraszi számhármas. A 6.4. Lemma alapján az általánosság megszorítása nélkül feltehetjük, hogy x páros, y és z pedig páratlan. Fejezzük ki x-et a „Pitagorasz-tételből" :

$$x^2+y^2=z^2 \implies x^2=z^2-y^2=(z+y)(z-y) \implies \left(\frac{x}{2}\right)^2=\underbrace{\frac{z+y}{2}}_{U}\cdot\underbrace{\frac{z-y}{2}}_{V}.$$

A paritásokra vonatkozó feltevésünk miatt itt minden tört értéke egész szám (ugye?). Megmutatjuk, hogy $U\perp V$. Ha $k\mid U,V$, akkor $k\mid U+V=z$ és $k\mid U-V=y$. Mivel $z\perp y$ (miért?), ez csak $k\sim 1$ esetén lehetséges, tehát U és V valóban relatív prímek. A 6.5 . Lemma szerint ekkor U és V is négyzetszám: $U=u^2$ és $V=v^2$. Tudjuk, hogy $u^2-v^2=y$ (ugye?), és ez egy pozitív páratlan szám, így $u>v$ és $u\not\equiv v \pmod 2$. Láttuk, hogy $U\perp V$, és ebből következik, hogy u és v is relatív prím (miért?). A $(\triangle)$-beli utolsó három egyenlőség u és v definíciójából könnyen levezethető:

$$\left(\frac{x}{2}\right)^2=UV=u^2v^2 \implies x=2uv, \qquad u^2-v^2=U-V=y, \qquad u^2+v^2=U+V=z.$$

A másik irány igazolásához tegyük fel, hogy $(\triangle)$ teljesül. Az $x^2+y^2=z^2$ egyenlőséget egyszerű számolás mutatja:

$$x^2+y^2=4u^2v^2+(u^2-v^2)^2=u^4+2u^2v^2+v^4=(u^2+v^2)^2=z^2.$$

Ezzel beláttuk, hogy (x,y,z) pitagoraszi számhármas. A számhármas primitívségéhez elegendő azt belátni, hogy $y\perp z$ (ugye?). Ha $k\mid y,z$, akkor $k\mid z+y=2u^2$ és $k\mid z-y=2v^2$. Mivel $u\perp v$, ez csak $k\sim 1,2$ esetén lehetséges (miért?). Node y (és z is) páratlan (miért?), tehát $k\sim 2$ lehetetlen, azaz $y\perp z$. □

6.7. Tétel (Fermat). Az $x^4+y^4=z^4$ egyenletnek nincs pozitív egészekből álló megoldása.

6.8. Tétel (nagy Fermat-tétel, Wiles és Taylor). Ha $n\geq 3$, akkor az $x^n+y^n=z^n$ egyenletnek nincs pozitív egészekből álló megoldása.

6.9. Lemma. Ha m és n előáll két négyzetszám összegeként, akkor mn is előáll.

Bizonyítás. Tfh. $m=a^2+b^2$ és $n=c^2+d^2$. Egyszerű számolás mutatja, hogy ekkor mn is felírható két négyzetszám összegeként:

$$mn=\left(a^2+b^2\right)\left(c^2+d^2\right)=(ac-bd)^2+(ad+bc)^2.$$ □

6.10. Lemma. A $4k+1$ alakú prímszámok előállnak két négyzetszám összegeként, a $4k+3$ alakú prímek viszont nem.

6.11. Tétel (Fermat-féle kétnégyzetszám-tétel). Pontosan azok a számok állnak elő két négyzetszám összegeként, amelyek prímfelbontásában a $4k+3$ alakú prímek páros kitevővel szerepelnek.

6.12. Tétel (Lagrange-féle négynégyzetszám-tétel). Minden természetes szám előáll négy négyzetszám összegeként.

6.13. Megjegyzés. Lagrange tétele éles abban az értelemben, hogy három négyzetszám összegeként nem lehet minden természetes számot előállítani (keressünk ellenpéldát!). A természetes számok hatványösszegekként való előállításaival kapcsolatos problémákat összefoglaló néven Waring-problémakörnek szokás nevezni. Edward Waring XVIII. századi angol matematikus Meditationes Algebraicae című művében azt állította (bizonyítás nélkül), hogy minden szám előállítható kilenc köbszám összegeként, illetve tizenkilenc negyedik hatvány összegeként. Ezek az állítások helyesnek bizonyultak, de csak a huszadik században találtak rájuk bizonyítást.

Általában $g(k)$ jelöli azt a legkisebb számot, amelyre igaz az, hogy minden természetes szám előállítható $g(k)$ darab k-adik hatvány összegeként. Az előzőek alapján tehát $g(2)=4, g(3)\leq 9, g(4)\leq 19$, és példák mutatják, hogy 8 köb, illetve 18 negyedik hatvány nem mindig elég, tehát $g(3)=9$ és $g(4)=19$. A $g(k)$ számok meghatározása igen nehéz probléma, még az sem világos, hogy egyáltalán léteznek minden k esetén;[§] ezt Hilbert igazolta 1909-ben. Van egy feltételezett képlet is a $g(k)$ számokra; bizonyított tény, hogy ez a képlet legfeljebb véges sok k-ra nem helyes, és általánosan elfogadott az a sejtés, hogy valójában minden k-ra érvényes:

$$g(k)=2^k+\left[\frac{3^k}{2^k}\right]-2.$$

[§]Mit jelentene az, hogy $g(k)$ nem létezik?

Prímszámok

6.14. Tétel (Euklidész). Végtelen sok prímszám van.

Bizonyítás. Tfh. véges sok prímszám van; legyenek ezek $p_1, \dots, p_n$, és legyen $N = p_1 \cdot \ldots \cdot p_n + 1$. Mivel $N > 1$, van prímosztója. Node N nem osztható a $p_1, \dots, p_n$ számok egyikével sem (ugye?). Tehát, feltevésünkkel ellentétben, van még további prím a $p_1, \dots, p_n$ számokon kívül. □

6.15. Tétel. Végtelen sok $4k-1$ alakú prímszám van.

Bizonyítás. Tfh. $p_1, \dots, p_n$ az összes $4k-1$ alakú prím, és legyen $N = 4 \cdot p_1 \cdot \ldots \cdot p_n - 1$. Mivel $N > 1$, van prímosztója. Node N nem osztható a $p_1, \dots, p_n$ számok egyikével sem (ugye?), tehát minden prímosztója $4k+1$ alakú. Eszerint N előáll $4k+1$ alakú számok szorzataként, és így maga is $4k+1$ alakú (miért?). Ez ellentmondás, hiszen szemlátomást $N \equiv -1 \pmod 4$. □

6.16. Tétel. Végtelen sok $4k+1$ alakú prímszám van.

6.17. Tétel (Dirichlet tétele). Ha egy nemkonstans számtani sorozat kezdőtagja és differenciája egymáshoz relatív prím, akkor a számtani sorozatban végtelen sok prímszám található.

6.18. Tétel (Csebisev tétele). Bármely szám és a kétszerese között van prímszám. Pontosabban: minden n természetes számhoz létezik olyan p prímszám, amelyre $n < p \le 2n$.

6.19. Tétel. A szomszédos prímek között tetszőlegesen nagy hézagok találhatók. (Azaz minden $N \in \mathbb{N}$ esetén lehet találni N egymást követő összetett számot.)

Bizonyítás. Ha $n \ge 2$, akkor az $n!+2,\ n!+3, \dots, n!+n$ számok mind összetettek, hiszen k valódi osztója az $n!+k$ számnak minden $k \in \{2, \dots, n\}$ esetén (miért?). Ez $n-1$ egymást követő összetett szám, és itt n tetszőlegesen nagy lehet. (Ha N egymást követő összetett számot akarunk találni, akkor az $n = N+1$ értékkel kell felírni a konstrukciót.) □

6.20. Definíció. ***Ikerprímnek*** nevezünk két prímszámot, ha különbségük 2.

6.21. Megjegyzés. Azt sejtik, hogy végtelen sok ikerprím van. Yitang Zhang 2013 áprilisában bebizonyította, hogy létezik olyan K korlát, amelyre végtelen sok olyan prímpár létezik, ahol a két tag különbsége legfeljebb K ($K = 70\,000\,000$ értékre, de ezt később levitték $K = 246$-ra).

6.22. Tétel. A prímszámok reciprokaiból alkotott sor divergens, azaz $\sum\limits_p \frac{1}{p} = \infty$.

6.23. Megjegyzés. Ez a tétel durván fogalmazva azt állítja, hogy „sok" prímszám van. Ismert tény, hogy „kevés" páratlan tökéletes szám, illetve „kevés" ikerprím van (ebből persze még nem derül ki, hogy végtelen sok van-e belőlük).

6.24. Megjegyzés. A $\sum \frac{1}{n}$ harmonikus sor lassan divergál, a $\sum \frac{1}{p}$ prímharmonikus sor még lassabban. Például $\sum_{p<10^{18}} \frac{1}{p} < 4$ (ez kb. a sor első huszonnégybilliárd tagja).

6.25. Tétel. Az n-edik prímszám nem nagyobb, mint $2^{2^{n-1}}$.

Bizonyítás. Legyen $p_1, p_2, \dots$ a prímek sorozata (növekvő sorrendben). Euklidész gondolatmenete szerint (lásd a 6.14. Tétel bizonyítását) az $N = p_1 \cdot \ldots \cdot p_n + 1$ számnak van olyan p prímosztója, amelyre $p \notin \{p_1, \dots, p_n\}$ teljesül. Ekkor tehát $p_{n+1} \le p \le p_1 \cdot \ldots \cdot p_n + 1$ (miért?), azaz

$$p_{n+1} \le p_1 \cdot \ldots \cdot p_n + 1. \tag{EU}$$

Ezt az egyenlőtlenséget használva teljes indukcióval bizonyítjuk, hogy $p_n \le 2^{2^{n-1}}$. A kezdőlépés: az $n = 1$ esetben $p_1 = 2 \le 2^{2^{1-1}} = 2^{2^0} = 2^1$. Az indukciós lépéshez tfh.

$$p_1 \le 2^{2^{1-1}},\ p_2 \le 2^{2^{2-1}},\ \dots,\ p_n \le 2^{2^{n-1}}. \tag{IH}$$

Azt kell megmutatnunk, hogy $p_{n+1} \le 2^{2^n}$ (ugye?). Ehhez becsüljük p_{n+1}-et az (EU) és (IH) egyenlőtlenségek segítségével:

$$p_{n+1} \overset{\text{(EU)}}{\le} p_1 \cdot \ldots \cdot p_n + 1 \overset{\text{(IH)}}{\le} 2^{2^{1-1}} \cdot 2^{2^{2-1}} \cdot \ldots \cdot 2^{2^{n-1}} + 1 = 2^{1+2+\dots+2^{n-1}} + 1 = 2^{2^n-1} + 1.$$

Azt kaptuk tehát, hogy $p_{n+1} \le 2^{2^n-1} + 1$, ez pedig (sokkal) kisebb, mint $2^{2^n} = 2^{2^n-1} + 2^{2^n-1}$ (ugye?). □

6.26. Definíció. A prímszámok eloszlásának pontosabb vizsgálatánál hasznos a $\pi(x)$ függvény, az úgynevezett ***prímszámláló függvény***, amely megadja az x pozitív valós számnál nem nagyobb prímek számát:

$$\pi(x) = \sum_{p \le x} 1.$$

6.27. Tétel (prímszámtétel). A $\pi(x)$ prímszámláló függvény aszimptotikusan ekvivalens az $\frac{x}{\log x}$ függvénnyel, azaz

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

6.28. Következmény. Az n-edik prímszám aszimptotikusan $n \log n$, azaz $\lim_{n\to\infty} \frac{p_n}{n \log n} = 1$.