SZÁMELMÉLET

jegyzet az előadáshoz[†]

2023 őszi félév, OT

Waldhauser Tamás

1. Oszthatóság, legnagyobb közös osztó, prímfaktorizáció az egész számok körében

Az oszthatósági reláció alapvető tulajdonságai

1.1. Definíció. Azt mondjuk, hogy az a egész szám ***osztója*** a b egész számnak (b ***többszöröse*** a-nak), ha létezik olyan c egész szám, amelyre $b = ac$.

Jelölés. Az oszthatósági relációt $\mid$ jelöli: $a \mid b \iff \exists c \in \mathbb{Z}\colon\ b = ac$.

1.2. Tétel (az oszthatóság tulajdonságai). Tetszőleges a, b, c egész számokra érvényesek az alábbiak:

(1) $a \mid a$; (***reflexivitás***)

(2) $(a \mid b$ és $b \mid c) \implies a \mid c$; (***tranzitivitás***)

(3) $(a \mid b$ és $b \mid a) \iff a = \pm b$;

(4) $1 \mid a$;

(5) $a \mid 0$;

(6) $a \mid 1 \iff a = \pm 1$;

(7) $0 \mid a \iff a = 0$;

(8) $(a \mid b$ és $a \mid c) \implies a \mid b \pm c$;

(9) $a \mid b \implies a \mid bc$;

(10) $a \mid b \iff ac \mid bc$, ha $c \neq 0$;

(11) $a \mid b \implies |a| \leq |b|$, ha $b \neq 0$.

Bizonyítás.

(1) Az oszthatóság definíciója szerint olyan c egész számot kell találnunk, amelyre $a = ac$. Nyilván $c = 1$ megfelelő lesz.

(2) Tfh. $a \mid b$ és $b \mid c$, azaz $b = au$ és $c = bv$ alkalmas u, v egész számokkal. Az első egyenlőséget a másodikba helyettesítve rögtön megkapjuk, hogy c többszöröse a-nak: $c = bv = (au)v = a(uv)$.

(3) Tfh. $a \mid b$ és $b \mid a$, azaz $b = au$ és $a = bv$ alkalmas u, v egész számokkal. Az első egyenlőséget a másodikba helyettesítve azt kapjuk, hogy $a = bv = (au)v = a(uv)$. Ha $a \neq 0$, akkor egyszerűsíthetünk a-val: $1 = uv$. Ez csak $u = v = \pm 1$ esetén teljesül, és ekkor $a = bv = \pm b$. ✓ Hátra van még az $a = 0$ eset; ekkor $b = au = 0 \cdot u = 0$, és így persze $a = \pm b$. ✓

(4) Olyan c egész számot kell találnunk, amelyre $a = 1 \cdot c$. Nyilván $c = a$ megfelelő lesz.

(5) Olyan c egész számot kell találnunk, amelyre $0 = a \cdot c$. Nyilván $c = 0$ megfelelő lesz.

(6) Ez következik a (3)-as és (4)-es tulajdonságokból (de persze közvetlenül is könnyen belátható).

(7) Ez következik a (3)-as és (5)-ös tulajdonságokból (de persze közvetlenül is könnyen belátható).

(8) Tfh. $a \mid b$ és $a \mid c$, azaz $b = au$ és $c = av$ alkalmas u, v egész számokkal. Ekkor $b \pm c = au \pm av = a(u \pm v)$, tehát $b \pm c$ valóban többszöröse a-nak.

(9) Ez következik a tranzitivitásból, hiszen $b \mid bc$.

(10) Az állításnak az $a \mid b \implies ac \mid bc$ irányú része minden c esetén igaz (még akkor is, ha $c = 0$). Valóban, $a \mid b$ azt jelenti, hogy $b = au$ alkalmas u egész számmal, és ekkor $bc = (au)c = (ac)u$. ✓ A másik irányhoz tfh. $ac \mid bc$, vagyis $bc = (ac)u$, ahol u egész szám. Ha $c \neq 0$, akkor ezt az egyenlőséget c-vel egyszerűsíthetjük, és így azt kapjuk, hogy $b = au$. ✓

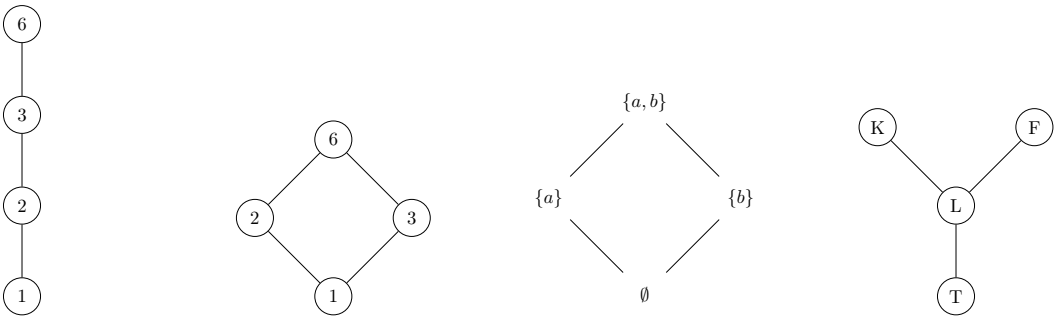
(11) Tfh. $a \mid b$, azaz $b = au$ alkalmas u egész számmal. Ha $b \neq 0$, akkor u sem lehet nulla (ugye?), és így $|u| \geq 1$. Ezért $|b| = |au| = |a| \cdot |u| \geq |a| \cdot 1 = |a|$. ✓

□

1.3. Megjegyzés. Ha csak nemnegatív számokat tekintünk, akkor (3) szerint ($a \mid b$ és $b \mid a$) $\iff a = b$. Ezt a tulajdonságot ***antiszimmetriának*** nevezzük. A reflexív, tranzitív és antiszimmetrikus relációk neve ***részbenrendezési reláció***. Tehát az oszthatóság részbenrendezés az $\mathbb{N}_0$ halmazon; másképp fogalmazva, $(\mathbb{N}_0; \mid)$ ***részbenrendezett halmaz***. A valós számok szokásos rendezése is részbenrendezési reláció, tehát $(\mathbb{R}; \leq)$ is részbenrendezett halmaz. Halmazok között pedig a tartalmazási reláció részbenrendezés, így például $(\mathcal{P}(U); \subseteq)$ részbenrendezett halmaz tetszőleges U halmaz esetén.

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

(Itt $\mathcal{P}(U)$ az U halmaz hatványhalmazát jelöli.) Véges részbenrendezett halmazokat (de néha még végteleneket is) lehet úgynevezett ***Hasse-diagrammal*** ábrázolni. Íme három négyelemű részbenrendezett halmaz Hasse-diagramja:



$(\{1,2,3,6\};\leq)$ $(\{1,2,3,6\};|)$ $(\mathcal{P}(\{a,b\});\subseteq)$ $(\{\mathrm{T},\mathrm{L},\mathrm{K},\mathrm{F}\};\sqsubseteq)$

1.4. Definíció. Azt mondjuk, hogy két egész szám ***asszociált***, ha kölcsönösen osztják egymást.

Jelölés. Az asszociáltsági relációt $\sim$ jelöli: $a \sim b \iff a \mid b$ és $b \mid a$.

1.5. Megjegyzés. Nem nehéz belátni, hogy az asszociáltság reflexív és tranzitív reláció, továbbá még ***szimmetrikus*** is: $a \sim b \implies b \sim a$. A reflexív, tranzitív és szimmetrikus relációkat ***ekvivalenciarelációnak*** nevezzük. Az ekvivalenciarelációk mindig meghatározzák az alaphalmaz egy ***osztályozását***. Az egész számok esetén $a \sim b \iff a = \pm b$, ezért az asszociáltsági osztályok itt $\{a, -a\}$ alakú halmazok ($a \neq 0$ esetén kételemű, $a = 0$ esetén egyelemű halmaz).

1.6. Definíció. Az $a \in \mathbb{Z}$ számot ***egységnek*** nevezzük, ha $a \sim 1$ (vagy, ami ezzel ekvivalens: $a \mid 1$).

1.7. Állítás. Az egész számok gyűrűjében csak két egység van: 1 és -1.

1.8. Megjegyzés. Az oszthatóság, asszociáltság, egység fogalma nemcsak az egész számok gyűrűjében, hanem bármilyen kommutatív, egységelemes, zérusosztómentes gyűrűben (azaz ***integritástartományban***) definiálható, és hasonló (de nem pont ugyanilyen!) tulajdonságokkal rendelkeznek.

Legnagyobb közös osztó, maradékos osztás, euklideszi algoritmus

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

(KO) $d \mid a$ és $d \mid b$;

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

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

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

1.10. Megjegyzés. A legnagyobb közös osztó nem egyértelmű: ha d legnagyobb közös osztója a-nak és b-nek, akkor $-d$ is az, hiszen $-d \sim d$, és így oszthatóság szempontjából megkülönböztethetetlenek (márpedig az lnko definíciójában csak oszthatóság szerepel, semmi más). E két számon kívül nincs más legnagyobb közös osztó, tehát az lnko asszociáltság erejéig egyértelműen meghatározott, ezért szoktuk így is írni: $d \sim \mathrm{lnko}(a,b)$. Szokásos megállapodás az is, hogy a két érték közül mindig a nemnegatívat tekintjük.

1.11. Megjegyzés. Jelölje egy a nemnegatív egész szám nemnegatív osztóinak halmazát D_a. Ekkor a és b nemnegatív 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 $\mathrm{lnko}(a,b)$ nem más, mint a $(D_a \cap D_b;\leq)$ rendezett halmaz legnagyobb eleme. Az általunk használt 1.9. Definíció szerint $\mathrm{lnko}(a,b)$ nem más, mint a $(D_a \cap D_b;|)$ részbenrendezett halmaz legnagyobb eleme. Például $a = 18$, $b = 30$ esetén $D_{18} \cap D_{30} = \{1,2,3,6\}$. A $(D_{18} \cap D_{30};\leq)$ és $(D_{18} \cap D_{30};|)$ részbenrendezett halmazok Hasse-diagramja az 1.3. Megjegyzésben látható (a bal oldali két diagram az ábrán). 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 1.9. 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).

1.12. Tétel (a maradékos osztás tétele). Ha $a, b \in \mathbb{Z}$, és $b \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és r egész számok, amelyekre $a = bq + r$ és $0 \leq r < |b|$.

Bizonyítás. Először az egzisztenciát bizonyítjuk. Tekintsük az $a - bq$ alakú *nemnegatív* számok halmazát:

$$R = \{a - bq : q \in \mathbb{Z}\} \cap \mathbb{N}_0.$$

Ez a halmaz nem üres (ugye?), így van legkisebb eleme. (A természetes számok egy fontos tulajdonsága, hogy $\mathbb{N}_0$ minden nemüres részhalmazának van legkisebb eleme.) Jelölje r a R halmaz legkisebb elemét. Az R halmaz definíciója szerint r előáll $r = a - bq$ alakban alkalmas q egész számmal, továbbá $r \geq 0$. Csak azt kell még igazolnunk, hogy $r < |b|$. Tfh. ezzel ellentétben $r \geq |b|$. Legyen $r' = r - |b|$; ekkor $r' \geq 0$, továbbá $r' = (a - bq) - |b| = a - b(q \pm 1)$. Ez azt jelenti, hogy $r' \in R$, ami ellentmondás, hiszen $r' < r$, és állítólag r volt az R halmaz legkisebb eleme.

Most igazoljuk az unicitást. Tfh. $a = bq_1 + r_1 = bq_2 + r_2$ és $0 \leq r_1, r_2 < |b|$. Átrendezéssel azt kapjuk, hogy $b(q_1 - q_2) = r_2 - r_1$, és így

$$|b| \cdot |q_1 - q_2| = |r_2 - r_1|\,.$$

Nézzük meg, hogy mekkora lehet itt a jobb, illetve a bal oldal. Mivel r_1 és r_2 is 0 és $|b| - 1$ között van, $|r_2 - r_1| < |b|$. Másrészt, $q_1 \neq q_2$ esetén a bal oldalra $|b| \cdot |q_1 - q_2| \geq |b|$ teljesülne. Ebből következik, hogy a két oldal csak $q_1 = q_2$ esetén lehet egyenlő, és ekkor persze $r_1 = r_2$ (ugye?). ✓ □

1.13. Definíció. Adott a és b egész számok esetén az előző tételbeli q és r kiszámítását ***maradékos osztásnak*** nevezzük. Az a szám az ***osztandó***, b az ***osztó*** q a ***hányados***, és r a ***maradék***.

1.14. Lemma. Tetszőleges $a, b, k \in \mathbb{Z}$ esetén a és b közös osztói ugyanazok, mint $a - kb$ és b közös osztói.

Bizonyítás. Ha $s \mid a$ és $s \mid b$, akkor $s \mid a - kb$, és így s közös osztója az $a - kb$ és b számoknak. Fordítva, ha $s \mid a - kb$ és $s \mid b$, akkor $s \mid (a - kb) + kb = a$ és, így s közös osztója a-nak és b-nek. □

1.15. Tétel (euklideszi algoritmus). Bármely két pozitív egész számnak van legnagyobb közös osztója, és az az euklideszi algoritmussal megkapható. Az $a = r_0$, $b = r_1$ pozitív egész számokon végrehajtott euklideszi algoritmus maradékos osztások ismételt elvégzését jelenti:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 && (0 \leq r_2 < r_1);\\
r_1 &= q_2 r_2 + r_3 && (0 \leq r_3 < r_2);\\
r_2 &= q_3 r_3 + r_4 && (0 \leq r_4 < r_3);\\
&\vdots\\
r_{i-1} &= q_i r_i + r_{i+1} && (0 \leq r_{i+1} < r_i);\\
&\vdots
\end{aligned}$$

Az eljárás véges számú lépés után véget ér: létezik olyan $n \in \mathbb{N}$, hogy $r_{n+1} = 0$. A legnagyobb közös osztó az utolsó nemnulla maradék, azaz $\mathrm{lnko}(a, b) = r_n$. A legnagyobb közös osztó kifejezhető a két szám „lineáris kombinációjaként": léteznek olyan x, y egész számok, melyekre $ax + by = \mathrm{lnko}(a, b)$.

Bizonyítás. A $b = r_1 > r_2 > r_3 > \cdots \geq 0$ egyenlőtlenségekből látható, hogy legfeljebb b lépés után nulla lesz a maradék. Tfh. $r_{n+1} = 0$, azaz r_n az utolsó nemnulla maradék.

Mivel $r_2 = r_0 - q_1 r_1$, az 1.14. Lemma szerint r_0 és r_1 közös osztói ugyanazok, mint r_1 és r_2 közös osztói: $D_{r_0} \cap D_{r_1} = D_{r_1} \cap D_{r_2}$. Ismét alkalmazva az 1.14. Lemmát, kapjuk, hogy $D_{r_1} \cap D_{r_2} = D_{r_2} \cap D_{r_3}$, és így tovább:

$$D_a \cap D_b = D_{r_0} \cap D_{r_1} = D_{r_1} \cap D_{r_2} = D_{r_2} \cap D_{r_3} = \cdots = D_{r_n} \cap D_{r_{n+1}} = D_{r_n} \cap D_0 = D_{r_n} \cap \mathbb{N}_0 = D_{r_n}.$$

Tehát a és b közös (pozitív) osztói pontosan ugyanazok, mint r_n (pozitív) osztói. Ezek között pedig r_n a legnagyobb (nemcsak az oszthatósági, hanem a nagyság szerinti rendezésben is).

A tétel utolsó állításnak bizonyításához i szerinti indukcióval igazoljuk, hogy mindegyik r_i előáll a és b „lineáris kombinációjaként":

$$\exists x_i, y_i \in \mathbb{Z}\colon\ \ r_i = ax_i + by_i. \tag{1.1}$$

(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 (1.1) 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 (1.1):

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

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

$$r_{i-1} = ax_{i-1} + by_{i-1} \text{ és } r_i = ax_i + by_i. \tag{IH}$$

Be kell látnunk, hogy (1.1) 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:

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

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. □

1.16. Következmény. Bármely két egész számnak létezik legnagyobb közös osztója.

Bizonyítás. Mivel minden szám asszociált az abszolút értékéhez, elegendő nemnegatív egészekre bizonyítani az állítást. Ha a és b is pozitív, akkor a fenti tétel szerint $\operatorname{lnko}(a,b)$ létezik. Ha $a = 0$, akkor a-nak minden szám osztója, ezért a és b közös osztói ugyanazok, mint b osztói, és így $\operatorname{lnko}(a,b) \sim \operatorname{lnko}(0,b) \sim b$. Hasonlóan, $b = 0$ esetén azt kapjuk, hogy $\operatorname{lnko}(a,0) \sim a$. □

1.17. 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:

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

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

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

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

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

Bizonyítás. Tfh. $d := \operatorname{lnko}(a,b) \neq 0$ (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?). Az 1.15. 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 $\operatorname{lnko}(a_0, b_0) \mid 1$, azaz a_0 és b_0 valóban relatív prímek. □

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

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

Bizonyítás. Tfh. $d := \operatorname{lnko}(a,b) \neq 0$, és írjuk fel az a és b számokat az 1.19. 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 ekvivalenciát kell igazolnunk:

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

A „$\Longleftarrow$” irány triviális (ugye?). A „$\Longrightarrow$” irányhoz tfh. $a_0 \mid b_0 c$. Az 1.15. 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. □

1.21. 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 $\{\ldots, -18, -9, 0, 9, 18, \ldots\}$.

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

1.23. Tétel. Tetszőleges a, b, c egész számokra teljesülnek az alábbiak:

(1) $\operatorname{lnko}(\operatorname{lnko}(a,b), c) \sim \operatorname{lnko}(a, \operatorname{lnko}(b,c))$;
(2) $\operatorname{lnko}(a,b) \sim \operatorname{lnko}(b,a)$;
(3) $\operatorname{lnko}(a,a) \sim a$;
(4) $\operatorname{lnko}(0,a) \sim a$;
(5) $\operatorname{lnko}(1,a) \sim 1$;
(6) $\operatorname{lnko}(a,b) \sim a \iff a \mid b$;
(7) $\operatorname{lnko}(a+bc, b) \sim \operatorname{lnko}(a,b)$;
(8) $\operatorname{lnko}(a,b)\cdot c \sim \operatorname{lnko}(ac, bc)$;
(9) $\operatorname{lnko}(a,b) \nsim 0 \implies \operatorname{lnko}\left(\frac{a}{\operatorname{lnko}(a,b)}, \frac{b}{\operatorname{lnko}(a,b)}\right) \sim 1$;
(10) $\operatorname{lnko}(a,b) \sim 1 \implies \operatorname{lnko}(a,bc) \sim \operatorname{lnko}(a,c)$.

Bizonyítás. Az állítások egy része következik a korábbi tételekből, más részük pedig könnyebben látható lesz majd abból, ahogyan a legnagyobb közös osztót kiszámítjuk a prímhatványtényezős felbontásból, ezért nem bizonyítjuk őket. □

1.24. Lemma. Ha a és b relatív prím egész számok, akkor tetszőleges $c \in \mathbb{Z}$ esetén

$$(a \mid c \text{ és } b \mid c) \iff ab \mid c.$$

Bizonyítás. A „$\Longleftarrow$” irány következik az oszthatóság tranzitivitásából (ugye?). Az „$\Longrightarrow$” irányhoz tfh. $a \mid c$ és $b \mid c$. Az utóbbiból az következik, hogy $c = bu$ alkalmas u egész számmal. Ekkor tehát $a \mid c = bu$, és így az 1.22. Következmény szerint $a \mid u$. Mindkét oldalt b-vel szorozva azt kapjuk, hogy $ab \mid ub = c$, és épp ezt kellett igazolnunk. □

1.25. Következmény. Bármely két egész számnak létezik legkisebb többszöröse, és minden $a, b \in \mathbb{Z}$ esetén

$$\text{lnko}\,(a,b) \cdot \text{lkkt}\,(a,b) \sim ab.$$

Bizonyítás. Ha $b = 0$, akkor $\text{lnko}(a,b) \sim \text{lnko}(a,0) \sim a$ és $\text{lkkt}(a,b) \sim \text{lkkt}(a,0) \sim 0$ (miért?), tehát ekkor teljesül az állítás. Az $a = 0$ eset hasonló, ezért most már tfh. se a se b nem nulla. Legyen $d \sim \text{lnko}(a,b)$, és legyen $t = \frac{ab}{d}$. Megmutatjuk, hogy t legkisebb közös többszöröse a-nak és b-nek. Az világos, hogy t egy közös többszörös, hiszen $t = a \cdot \frac{b}{d}$ és $t = b \cdot \frac{a}{d}$. Tfh. k egy tetszőleges közös többszörös, azaz $a \mid k$ és $b \mid k$. Ekkor $\frac{a}{d} \mid \frac{k}{d}$ és $\frac{b}{d} \mid \frac{k}{d}$ is teljesül (miért?), és így az 1.24. Lemma szerint $\frac{a}{d} \cdot \frac{b}{d} \mid \frac{k}{d}$, hiszen $\frac{a}{d} \perp \frac{b}{d}$ (lásd az 1.19. Következményt). Mindkét oldalt d-vel szorozva azt kapjuk, hogy $\frac{a}{d} \cdot \frac{b}{d} \cdot d \mid \frac{k}{d} \cdot d$, vagyis $t \mid k$, és épp ezt kellett bizonyítanunk (ugye?). □

Prímszám, felbonthatatlan szám, a számelmélet alaptétele

1.26. Definíció. A $p \in \mathbb{Z}$ egész szám ***felbonthatatlan*** (idegen szóval: ***irreducibilis***) elem az egész számok gyűrűjében, ha p nem nulla, nem egység, és csak úgy bontható két egész szám szorzatára, hogy az egyik tényező asszociált p-hez. (Ekkor a másik tényező szükségképpen egység; ilyenkor *triviális faktorizációról* beszélünk.) Formálisan:

$$p \nsim 0,1 \quad \text{és} \quad \forall a,b \in \mathbb{Z}\colon\ p = ab \implies (p \sim a \text{ vagy } p \sim b).$$

1.27. Megjegyzés. A $p \in \mathbb{Z}$ elem akkor és csak akkor felbonthatatlan, ha asszociáltság erejéig pontosan két osztója van: 1 és p (ugye?).

1.28. Definíció. A $p \in \mathbb{Z}$ egész szám ***prím(tulajdonságú)*** elem az egész számok gyűrűjében, ha p nem nulla, nem egység, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$p \nsim 0,1 \quad \text{és} \quad \forall a,b \in \mathbb{Z}\colon\ p \mid ab \implies (p \mid a \text{ vagy } p \mid b).$$

1.29. Megjegyzés. A fenti két definíció a felbonthatatlanság és a prímtulajdonság általános gyűrűelméleti definíciója (az egész számok gyűrűjére megfogalmazva). A „köznyelv” szóhasználata több ponton is eltér ettől. Egyrészt, a prímszámokat az 1.26. Definícióval (pontosabban annak az 1.27. Megjegyzésben leírt átfogalmazásával, a nemtriviális valódi osztók hiányával) szokták definiálni. Ez nem okoz nagy problémát, mert, amint a következő tételben látni fogjuk, az egész számok gyűrűjében a felbonthatatlanság és a prímtulajdonság ekvivalens. A másik eltérés, hogy általában csak pozitív számokat szokás prímszámnak (illetve összetett számnak) tekinteni. Ezt a konvenciót mi is megtartjuk: a továbbiakban prímszámon a $\mathbb{Z}$ gyűrű pozitív felbonthatatlan elemét értjük. Tehát $p \in \mathbb{Z}$ ***prímszám***, ha

$$p \geq 2 \quad \text{és} \quad \forall a,b \in \mathbb{N}\colon\ p = ab \implies (p = a \text{ vagy } p = b).$$

Hasonlóképpen, ***összetett számon*** olyan pozitív egész számot értünk, amelynek van nemtriviális faktorizációja. Ha negatív számokat is meg akarunk engedni, akkor nem prímszámokról, hanem prím elemekről beszélünk (noha persze ezek is számok).

1.30. Tétel. Az egész számok gyűrűjében a felbonthatatlanság és a prímtulajdonság ekvivalens.

Bizonyítás.

- $\boxed{\text{prím} \implies \text{felbonthatatlan}}$ Tfh. p prím elem a $\mathbb{Z}$ gyűrűben. Mivel $p \nsim 0,1$, csak azt kell igazolnunk, hogy p-nek minden felbontása triviális. Legyen $p = ab$ egy tetszőleges felbontás. Ekkor $a \mid p$ és $b \mid p$ (ugye?), továbbá $p \mid ab$ is teljesül(miért?). Utóbbiból a prímtulajdonság szerint következik, hogy $p \mid a$ vagy $p \mid b$. Az első esetben (figyelembe véve az $a \mid p$ oszthatóságot) azt kapjuk, hogy $p \sim a$, a második esetben pedig hasonlóan következik, hogy $p \sim b$. Ezzel beláttuk, hogy minden $p = ab$ felbontás triviális, tehát p felbonthatatlan.
- $\boxed{\text{felbonthatatlan} \implies \text{prím}}$ Tfh. p felbonthatatlan elem a $\mathbb{Z}$ gyűrűben. Ekkor $p \nsim 0,1$, ezért csak azt kell igazolnunk, hogy ha $p \mid ab$, akkor szükségképpen $p \mid a$ vagy $p \mid b$. A $p \mid ab$ oszthatóságból Euklidész lemmája szerint következik, hogy $\frac{p}{\text{lnko}(p,a)} \mid b$. Mivel p felbonthatatlan és $\text{lnko}(p,a)$ osztója p-nek, csak két lehetőség van a legnagyobb közös osztóra: $\text{lnko}(p,a) \sim 1$ vagy $\text{lnko}(p,a) \sim p$. Az első esetben a fenti $\frac{p}{\text{lnko}(p,a)} \mid b$ oszthatóság egyszerűen azt jelenti, hogy $p \mid b$ (ugye?). Ha pedig $\text{lnko}(p,a) \sim p$ teljesül, akkor $p \mid a$ (miért?). Ezzel beláttuk, hogy p osztója a és b közül legalább az egyiknek, tehát p prím.

□

1.31. Lemma. Legyen p prímszám, $n \in \mathbb{N}$ és $a_1, \ldots, a_n \in \mathbb{N}$. Ha $p \mid a_1 \cdot \ldots \cdot a_n$, akkor $p \mid a_i$ valamely $i \in \{1, \ldots, n\}$-re.

Bizonyítás. Az állítást n szerinti teljes indukcióval bizonyítjuk. Az $n = 1$ esetben semmitmondó az állítás, az $n = 2$ esetben pedig rögtön következik a prímtulajdonságból. Legyen most már $n \geq 3$, és tfh. valahányszor p osztója egy n-tényezős szorzatnak, mindannyiszor osztója a szorzat valamelyik tényezőjének (ez az indukciós feltevés). Tfh. p osztója egy n-tényezős szorzatnak: $p \mid a_1 \cdot \ldots \cdot a_n \cdot a_{n+1}$. A prímtulajdonságot az $a = a_1 \cdot \ldots \cdot a_n$, $b = a_{n+1}$ „szereposztással" alkalmazva kapjuk, hogy $p \mid a_1 \cdot \ldots \cdot a_n$ vagy $p \mid a_{n+1}$. A második esetben készen is vagyunk ($i = n + 1$ megfelelő lesz), az elsőben pedig az indukciós hipotézisből következik, hogy $p \mid a_i$ valamely $i \in \{1, \ldots, n\}$ indexre. □

1.32. Tétel (a számelmélet alaptétele). Bármely pozitív egész szám felbontható prímszámok szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

Bizonyítás.

- egzisztencia Legyen NIF mindazon pozitív egészek halmaza, amelyek nem bonthatóak prímek szorzatára, azaz Nincs Irreducibilis Faktorizációjuk. Tfh. NIF $\neq \emptyset$, és legyen n a NIF halmaz legkisebb eleme. Ekkor $n \neq 1$ (mert az üres szorzat prímfelbontása 1-nek), és nem lehet n prímszám (mert akkor az n egytényezős szorzat lenne a prímfelbontása). Tehát n összetett szám: $n = ab$, ahol $1 < a, b < n$. A NIF halmaz legkisebb eleme n, ezért, $a, b \notin$ NIF, és így felbonthatóak prímek szorzatára: $a = p_1 \cdot \ldots \cdot p_k$ és $b = q_1 \cdot \ldots \cdot q_\ell$. Ekkor n-nek is van prímfelbontása: $n = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_\ell$, ellentétben azzal a feltevésünkkel, hogy $n \in$ NIF.
- unicitás Legyen NEF mindazon pozitív egészek halmaza, amelyek többféleképpen is felbonthatóak prímek szorzatára, azaz Nem Egyértelmű a Faktorizációjuk. Tfh. NEF $\neq \emptyset$, és legyen n a NEF halmaz legkisebb eleme. Ekkor n-nek van két lényegesen (nemcsak a tényezők sorrendjében) különböző prímfelbontása: $n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_\ell$. Ebből következik, hogy $p_1 \mid q_1 \cdot \ldots \cdot q_\ell$ (ugye?), és így az 1.31. Lemma szerint p_1 osztója valamelyik q_i-nek. A jelölés egyszerűsége (és az általánosság megszorítása nélkül) tfh. $p_1 \mid q_1$. Mivel q_1 felbonthatatlan, ez nem lehet valódi oszthatóság, azaz szükségképpen $p_1 = q_1$. Így n mindkét felbontásából törölhetjük a $p_1 = q_1$ tényezőt: $p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_\ell$. Ez két lényegesen különböző irreducibilis faktorizációja az $\frac{n}{p_1}$ számnak (miért?), tehát $\frac{n}{p_1} \in$ NEF. Ez azonban ellentmondás, mert $\frac{n}{p_1} < n$, márpedig n volt a NEF halmaz legkisebb eleme. □

1.33. Megjegyzés. Figyeljük meg, hogy a bizonyítás során hol a felbonthatatlanságot, hol a prímtulajdonságot használtuk (mikor melyiket?), ezért (is) volt fontos előre belátni, hogy ez a két tulajdonság ekvivalens.

1.34. Megjegyzés. Ha az n szám felbontásában egy prím többször is szerepel, akkor azokat összevonhatjuk egy tényezővé, így kapjuk a ***prímhatványtényezős*** alakot: $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, ahol $p_1, \ldots, p_k$ páronként különböző prímszámok, az $\alpha_1, \ldots, \alpha_k$ kitevők pedig pozitív egész számok. Természetesen a prímhatványtényezős alak is a tényezők sorrendjétől eltekintve egyértelmű.

1.35. Megjegyzés. Negatív számokat is megengedve, a prímfelbontás csak a tényezők sorrendjétől és asszociáltságtól eltekintve lesz egyértelmű. Ezt fogalmazzuk meg a következő tételben.

1.36. Tétel. Az egész számok gyűrűjének minden nemnulla eleme felbontható irreducibilis elemek szorzatára, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű. Az egyértelműség pontosabban a következőt jelenti: ha $n = p_1 \cdot \ldots \cdot p_k$ és $n = q_1 \cdot \ldots \cdot q_\ell$, ahol a p_i és q_j elemek mind irreducibilisek, akkor $k = \ell$, és létezik olyan $\pi \in S_k$ permutáció, amelyre $p_i \sim q_{i\pi}$ minden $i \in \{1, \ldots, k\}$ esetén.

1.37. Következmény. Legyen az a és b pozitív egész számok prímhatványtényezős felbontása $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ és $b = p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}$ (azokat a prímeket, amelyek csak az egyik számban fordulnak elő, a másikban nulla kitevővel tüntetjük fel). Ekkor teljesülnek az alábbiak:

(1) $a \mid b \iff \alpha_i \leq \beta_i$ $(i = 1, \ldots, n)$;
(2) $\text{lnko}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$;
(3) $\text{lkkt}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

Bizonyítás.

(1)

- $\Longrightarrow$ Tfh. $a \mid b$, azaz $b = ac$ alkalmas c pozitív egész számmal. Legyen c prímhatványtényezős alakja a következő: $c = p_1^{\gamma_1} \cdot \ldots \cdot p_n^{\gamma_n}$, ahol a γ_i kitevők nemnegatív egész számok. (Ha c-ben esetleg fellépne olyan prímtényező, ami nem szerepel b-ben (persze ilyen nincs), akkor azt utólag tegyük be a és b felbontásába is, nulla kitevővel.) A $b = ac$ egyenlőségbe behelyettesítve b és c prímhatványtényezős felbontását, azt kapjuk, hogy $b = p_1^{\alpha_1 + \gamma_1} \cdot \ldots \cdot p_n^{\alpha_n + \gamma_n}$. Összehasonlítva ezt b „eredeti" prímfelbontásával, a számelmélet alaptételének unicitás része szerint $\alpha_i + \gamma_i = \beta_i$ minden i indexre. Mivel $\gamma_i \geq 0$, ebből következik, hogy $\alpha_i \leq \beta_i$ $(i = 1, \ldots, n)$.
- $\Longleftarrow$ Tfh. $\alpha_i \leq \beta_i$, és legyen $\gamma_i = \beta_i - \alpha_i$ minden i esetén. Ekkor a $c := p_1^{\gamma_1} \cdot \ldots \cdot p_n^{\gamma_n}$ pozitív egész számmal $a = bc$ teljesül (ugye?), és így $a \mid b$.

(2) Legyen $\delta_i = \min(\alpha_i, \beta_i)$ minden i esetén, és legyen $d = p_1^{\delta_1} \cdot \ldots \cdot p_n^{\delta_n}$. Megmutatjuk, hogy d legnagyobb közös osztója a-nak és b-nek.

(KO) Mivel $\delta_i \le \alpha_i$ minden i indexre (ugye?) a tétel (1)-es állításából következik, hogy $d \mid a$. Hasonlóan látható, hogy $d \mid b$, tehát d valóban közös osztója a-nak és b-nek.

(LN) Tfh. k egy pozitív közös osztója a-nak és b-nek, és legyen k prímhatványtényezős alakja $k = p_1^{\varkappa_1} \cdot \ldots \cdot p_n^{\varkappa_n}$. Mivel $k \mid a$ és $k \mid b$, az (1)-es állítás szerint $\varkappa_i \le \alpha_i$ és $\varkappa_i \le \beta_i$, következésképp $\varkappa_i \le \min(\alpha_i, \beta_i) = \delta_i$ minden i indexre. Ismét az (1)-es állítást használva adódik, hogy $k \mid d$, és épp ezt kellett bizonyítanunk.

(3) Ez a (2)-es állításhoz hasonlóan igazolható (HF). □

1.38. Következmény. Két egész szám akkor és csak akkor relatív prím, ha nincs közös prímosztójuk.

1.39. Megjegyzés. Az 1.8. Megjegyzésben említettük, hogy az oszthatóság tetszőleges integritástartomámyban definiálható. A legnagyobb közös osztó, legkisebb közös többszörös, felbonthatatlan és prím elem fogalma is bármely integritástartomámyban értelmezhető. Sajnos előfordulhat, hogy nem létezik bármely két elemnek legnagyobb közös osztója, az irreducibilis és prím elemek nem feltétlenül lesznek ugyanazok, és egyértelmű irreducibilis faktorizáció se mindig létezik.

Vannak olyan integritástartományok, amelyekben lehet valamiféle maradékos osztást végezni, és erre építve euklideszi algoritmust végrehajtani. Az ilyen gyűrűket ***euklideszi gyűrűknek*** nevezzük. Euklideszi gyűrűkben az eddig tanultak mind érvényesek, méghozzá szinte szó szerint ugyanazokkal a bizonyításokkal, mint az egész számoknál. A legfontosabb példa: test feletti polinomokkal lehet maradékos osztást végezni, ezért bármely T test esetén a T feletti polinomok egy $T[x]$ euklideszi gyűrűt alkotnak, és így a „polinomok számelmélete" az egész számok számelméletéhez hasonlóan felépíthető. Egy másik fontos példa: az „komplex egész számok", vagyis az $a+bi$ $(a, b \in \mathbb{Z})$ alakú komplex számok is euklideszi gyűrűt alkotnak. Az ilyen számokat ***Gauss-egészeknek*** nevezzük, és a Gauss–egészek gyűrűjét $\mathbb{Z}[i]$ jelöli.

2. Számelméleti kongruenciák

Lineáris diofantoszi egyenletek

2.1. 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. Az 1.15. 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: $M = \{(x, y) \in \mathbb{Z}^2 : ax + by = c\}$. Legyen $(x_0, y_0) \in M$ egy tetszőleges rögzített megoldás, azaz $ax_0 + by_0 = c$. Azt kell bizonyítanunk, hogy $M = \{(x_t, y_t) : t \in \mathbb{Z}\}$. 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 $x = x_t$. □

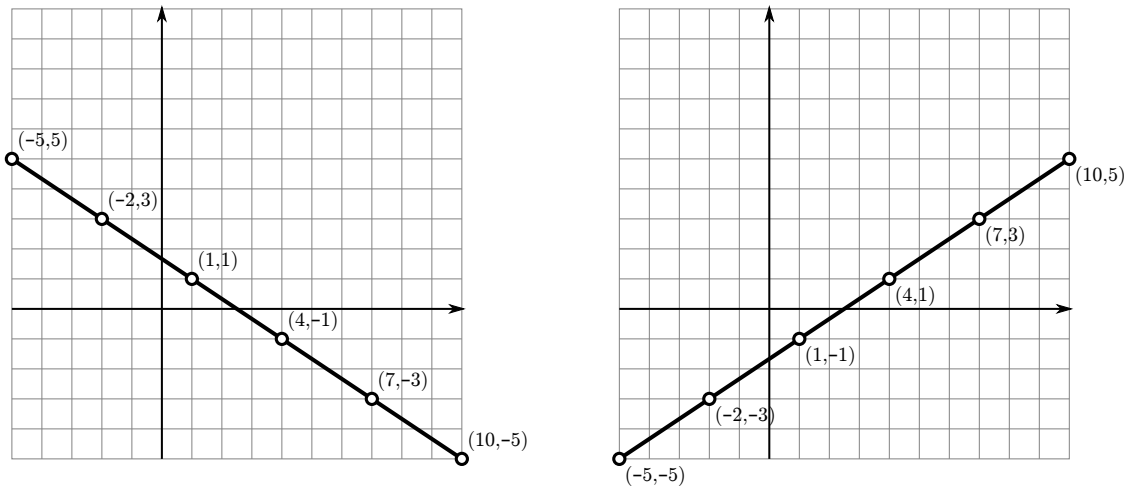
2.2. Példa. Oldjuk meg a $6x + 9y = 15$ diofantoszi egyenletet. Az euklideszi algoritmusból azt kapjuk, hogy $\operatorname{lnko}(6, 9) = 3 = 6 \cdot (-1) + 9 \cdot 1$. Szorozzuk be mindkét oldalt 5-tel: $15 = 6 \cdot (-5) + 9 \cdot 5$. Ebből látható, hogy $x_0 = -5, y_0 = 5$ egy partikuláris megoldása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

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

2.3. 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 2.2. 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.)



2.4. 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).

2.5. 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:

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

2.6. 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. (Lásd a fenti ábrán a jobb oldali grafikont.) 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 2.5. Példában másodikként felírt megoldástól, hogy t helyébe $-t$-t írunk, azaz a rácspontokat nem balra lefelé, hanem jobbra felfelé indexezzük.

Kongruenciareláció

2.7. 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.

2.8. 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 $a\equiv b \pmod m \iff m\mid a-b$.

2.9. 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 $0 \le r_1, r_2 \le m-1$. 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 $\{-(m-1), -(m-2), \dots, m-2, m-1\}$ 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. □

2.10. 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.
- $23 \equiv 4677863 \equiv -34267467 \not\equiv -497973413 \pmod{10}$.

2.11. Tétel. Tetszőleges $m, m_1, m_2 \ge 2, a, b, c, a_1, b_1, a_2, b_2 \in \mathbb{Z}$ 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) $\left.\begin{matrix} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{matrix}\right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2,\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$;

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

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

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

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

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

(3) $(a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}) \implies (m \mid a-b$ és $m \mid b-c) \implies m \mid (a-b)+(b-c) = a-c \implies a \equiv c \pmod{m}$.

(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" :

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

(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 2.9. Tétel szerint) az első lépésben

megint r lesz a maradék, hiszen $a \equiv b \pmod m$. Tehát a második lépéstől kezdve a két algoritmus megegyezik, így a végeredményük is ugyanaz lesz: $\operatorname{lnko}(a,m) \sim \operatorname{lnko}(b,m)$.
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 $\forall k \in \mathbb{Z}\colon k \mid b, m \implies k \mid a, m$, tehát a és m közös osztói ugyanazok, mint b és m közös osztói. Ebből pedig már következik, hogy $\operatorname{lnko}(a,m) \sim \operatorname{lnko}(b,m)$ (miért?). □

2.12. Megjegyzés. A fenti tételbeli (1)–(3) tulajdonságok szerint a modulo m kongruencia ***ekvivalenciareláció*** az egész számok halmazán; a megfelelő ekvivalenciaosztályokat ***maradékosztályoknak*** nevezzük.

2.13. Példa. A $10 \equiv -1 \pmod{11}$ kongruenciát önmagával k-szor megszorozva (a 2.11. 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

2.14. 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.

2.15. Példa. Oldjuk meg a $6x \equiv 15 \pmod 9$ lineáris kongruenciát. A kongruencia definíciója (2.7. 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 2.5. 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, vagyis a megoldáshalmaz egy mindkét irányba végtelen, 3-as differenciájú számtani sorozat:

$$M = \{3t - 5 : t \in \mathbb{Z}\} = \{\ldots, -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}.$$

Ez a halmaz pontosan azokból a számokból áll, amelyek 3-mal osztva 1-et adnak maradékul (egy úgynevezett modulo 3 maradékosztály). Tehát egyetlen megoldás van modulo 3, és a megoldást tömören „kongruenciásan” így is felírhatjuk: $x \equiv 1 \pmod 3$. Persze azt is írhatnánk, hogy $x \equiv -5 \pmod 3$, ha már -5 szerepelt a diofantoszi egyenlet megoldásában. Ez a két kongruencia ekivalens egymással, hiszen $-5 \equiv 1 \pmod 3$.

2.16. 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 2.1. 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. □

2.17. Példa. A 2.15. Példában szereplő kongruenciát megoldhatjuk tisztán „kongruenciás” számolással, diofantoszi egyenletre való átírás nélkül is (ellenőrizzük, hogy minden lépésben ekvivalens átalakítást végzünk!):

$$\begin{aligned} 6x &\equiv 15 \pmod{9} && \\ 6x &\equiv 6 \pmod{9} && \text{(mert } 15 \equiv 6 \pmod{9}\text{)} \\ x &\equiv 1 \pmod{3} && \text{(lásd a 2.11. Tételbeli (5) tulajdonságot)} \end{aligned}$$

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: $x \equiv 1, 4, 7 \pmod{9}$.

2.18. 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.

2.19. 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 a 2.16. Tételnek: amikor a modulo m multiplikatív inverzét keressük, akkor az $ax \equiv 1 \pmod{m}$ lineáris kongruenciát kell megoldanunk. A 2.16. 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. □

2.20. 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

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

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

2.22. Megjegyzés. A 2.16. Tétel segítségével a kongruenciarendszerbeli kongruenciákat külön-külön megoldhatjuk (ha van megoldásuk), és így a kongruenciarendszert a következő alakra hozhatjuk:

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

2.23. 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:

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

Az x-re kapott két kifejezést egyenlővé téve a $6y+7 = 9z+22$ diofantoszi egyenletet kaptuk, Ez lényegében ugyanaz, mint a 2.5. 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 $x \equiv 13 \pmod{18}$.

2.24. 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:

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

Tehát a kongruenciarendszerünknek akkor és csak akkor van megoldása, ha léteznek olyan y_1, y_2 egész számok, amelyekre $y_1 m_1 + c_1 = y_2 m_2 + c_2$ (ekkor $x = y_1 m_1 + c_1$ megoldása a kongruenciarendszernek). Átrendezve, azt kapjuk, hogy $y_1 m_1 - y_2 m_2 = c_2 - c_1$. Ennek a kétismeretlenes diofantoszi egyenletnek a 2.1. Tétel szerint akkor és csak akkor van megoldása, ha $\operatorname{lnko}(m_1, m_2) \mid c_2 - c_1$, tehát ez a kongruenciarendszer megoldhatóságának feltétele. A tétel második állítása megkapható a diofantoszi egyenlet általános megoldásának felírásával, de rögtön következik a 2.11. Tételben szereplő (7) tulajdonságból is. □

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

Bizonyítás. Tfh. s egy megoldása a kongruenciarendszernek. Ekkor minden $i \in \{1, \ldots, k\}$ 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 2.11. Tételben szereplő (7) tulajdonság alapján ez a kongruenciarendszer ekvivalens az $x \equiv s \pmod{[m_1, \ldots, m_k]}$ kongruenciával, amelynek megoldáshalmaza nyilván egyetlen $\bmod[m_1, \ldots, m_k]$ maradékosztály. □

2.26. Tétel. A $(*)$ lineáris kongruenciarendszernek akkor és csak akkor van megoldása, ha bármely két kongruenciából álló részrendszerének van megoldása, azaz $\forall i, j:\ \operatorname{lnko}(m_i, m_j) \mid c_i - c_j$. 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. □

2.27. Tétel (kínai maradéktétel). Ha a $(*)$ kongruenciarendszerben a modulusok páronként relatív prímek (azaz $i \neq j$ esetén $\operatorname{lnko}(m_i, m_j) = 1$), 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 ($i = 1, \ldots, k$). Ekkor az eredeti $(*)$ kongruenciarendszer általános megoldása:

$$x \equiv c_1 e_1 + \cdots + c_k e_k \pmod{m_1 \cdots m_k}.$$

Bizonyítás. Az m_i modulusok páronként relatív prímek, ezért a legkisebb közös többszörösük $[m_1, \ldots, m_k] = m_1 \cdot \ldots \cdot m_k$. 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 2.24. 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 $s := c_1e_1 + \cdots + c_ke_k$ szám megoldása a kongruenciarendszernek:

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

Tehát s kielégíti az i-edik kongruenciát minden i-re, azaz megoldása a kongruenciarendszernek. A 2.25 . Tétel szerint a kongruenciarendszer általános megoldása $x \equiv s \pmod{[m_1, \ldots, m_k]}$, és épp ezt kellett igazolnunk. □

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

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

Írjuk fel a három segéd-kongruenciarendszert:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 0 \pmod 4 \\ x &\equiv 0 \pmod 5 \end{aligned} \qquad \left| \qquad \begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 0 \pmod 5 \end{aligned} \right. \qquad \left| \qquad \begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 0 \pmod 4 \\ x &\equiv 1 \pmod 5 \end{aligned} \right.$$

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

$$\begin{aligned} x &\equiv 0 \pmod{20} \\ x &\equiv 1 \pmod 3 \end{aligned} \qquad \left| \qquad \begin{aligned} x &\equiv 0 \pmod{15} \\ x &\equiv 1 \pmod 4 \end{aligned} \right. \qquad \left| \qquad \begin{aligned} x &\equiv 0 \pmod{12} \\ x &\equiv 1 \pmod 5 \end{aligned} \right.$$

A segéd-kongruenciarendszerek megoldásai:

$$x \equiv 40 \pmod{60} \qquad \left| \qquad x \equiv 45 \pmod{60} \right. \qquad \left| \qquad x \equiv 36 \pmod{60} \right.$$

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

2.29. 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).

2.30. Megjegyzés. Az $\overline{a}$ jelölés nem utal a modulusra, de a szövegkörnyezetből mindig világosnak kell lennie, hogy mi a modulus. A definícióból 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 $\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$.

2.31. Példa. A modulo 3 maradékosztályok:

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

2.32. 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 $\{\overline{c_1}, \ldots, \overline{c_m}\} = \mathbb{Z}_m$.

2.33. 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?).

2.34. 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 2.11. 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. □

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

2.36. 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 2.35 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 2.11. 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 2.35 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 2.35 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. □

2.37. 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.

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

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

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

2.39. 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?).

2.40. 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.

2.41. 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 $\overline{4}^{-1} = \overline{16}$.

2.42. 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 2.19. Tételnek. □

2.43. Megjegyzés. A 2.11. 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.

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

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

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

2.46. Tétel. A $\mathbb{Z}_m^*$ halmaz csoportot alkot a szorzás műveletével.

Bizonyítás. Ha a és b relatív prímek m-hez, akkor ab is relatív prím m-hez (ugye?), tehát a $\mathbb{Z}_m^*$ halmaz zárt a szorzásra. A maradékosztályok szorzása asszociatív művelet, az egységelem $\overline{1}$, ami nyilván redukált maradékosztály, és $\mathbb{Z}_m^*$ minden elemének van inverze (és az inverz is $\mathbb{Z}_m^*$-ban van). □

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

2.48. Megjegyzés. Meg lehet mutatni, hogy a hatványozás szokásos azonosságai érvényben maradnak redukált maradékosztályok egész kitevős hatványozására. (Valójában nemcsak a $\mathbb{Z}_m^*$ csoportban, hanem bármely Abel-csoportban ez a helyzet.)

2.49. Tétel. 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 (2.36. 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 2.42. Tétel szerint $\overline{a}$-nak van multiplikatív inverze, és ezzel beláttuk, hogy $\mathbb{Z}_m$ test. □

2.50. 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 2.36. 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

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

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

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

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

2.52. 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) $\varphi(81) = |\mathbb{Z}_{81}^*| = \left|\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \ldots, \overline{79}, \overline{80}\}\right| = 81 - 81/3 = 54$.

2.53. 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 $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

2.54. Tétel. Legyen az n pozitív egész 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:

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

Ugyanezt felírhatjuk egyetlen szummában is:

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

(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.) □

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

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

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

2.56. Példa. Számítsuk ki a tanult képlet (2.54. 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) $\varphi(2023) = \varphi(7 \cdot 17^2) = \varphi(7) \cdot \varphi(17^2) = (7 - 1) \cdot (17^2 - 17) = 6 \cdot 272 = 1632$.

2.57. Definíció. A z komplex számot ***n-edik egységgyöknek*** nevezzük, ha $z^n = 1$. A z egységgyök ***rendjén*** azt a legkisebb n pozitív egész kitevőt értjük, amelyre $z^n{=}1$. A z egységgyök rendjét $o(z)$ jelöli (olvasd: *ordó*). Formálisan:

$$o(z) := \min\{\, n \in \mathbb{N} : z^n = 1 \,\}.$$

Ha $o(z) = n$, akkor azt mondjuk, hogy z ***primitív n-edik egységgyök***. Ebben az esetben z hatványaiként megkapható az összes n-edik egységgyök.

2.58. Állítás. A primitív n-edik egységgyökök száma $\varphi(n)$ minden n pozitív egész szám esetén.

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):

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

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 $o(\varepsilon_k) = \frac{n}{\operatorname{lnko}(n,k)}$. Így ε_k akkor és csak akkor primitív n-edik egységgyök, ha $\operatorname{lnko}(n,k) \sim 1$. Vagyis a primitív n-edik egységgyökök halmaza $\{\varepsilon_k : 0 \le k \le n-1 \text{ és } k \perp n\}$, ennek a halmaznak pedig éppen $\varphi(n)$ eleme van (ugye?). □

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

Bizonyítás. (törtekkel) Tekintsük a $T = \left\{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}\right\}$ 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 $1 \le k \le d$ (miért?). Fordítva, ha $d \mid n$, $k \perp d$ és $1 \le k \le d$, 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 $1 \le k \le d$) 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 $\sum_{d\mid n}\varphi(d)$ összeget kapjuk, és ezzel kész is a bizonyítás. □

Bizonyítás. (egységgyökökkel) Megmutatjuk, hogy a $\sum_{d\mid n}\varphi(d)$ összeg az n-edik egységgyököket számolja meg, ezekből pedig tudjuk, hogy n van. Legyen $E_n = \{\varepsilon_0, \dots, \varepsilon_{n-1}\}$ az n-edik egységgyökök halmaza, és tetszőleges $d \in \mathbb{N}$ esetén jelölje P_d a d-edik primitív egységgyökök halmazát. A 2.58. Állítás bizonyítása során láttuk, hogy az $\varepsilon_k = \operatorname{cis}\frac{2k\pi}{n}$ komplex szám rendje $d := \frac{n}{\operatorname{lnko}(n,k)}$, 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?):

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

Diszjunkt halmazok egyesítésénél az elemszámok összeadódnak, tehát

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

A 2.58 . Állításból tudjuk, hogy $|P_d| = \varphi(d)$, tehát a fenti egyenlőség igazolja, hogy $n = \sum_{d\mid n}\varphi(d)$. □

2.60. Állítás. 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. □

2.61. 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 $k = |\mathbb{Z}_m^*| = \varphi(m)$.)

2.62. Megjegyzés. A 2.60. Állítás 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. (Hasonlítsuk ezt össze a 2.34. Állítással!)

Hatványozás modulo m

2.63. Definíció. Ha $a \in \mathbb{Z}$ és $m \ge 2$ relatív prímek, akkor tetszőleges $k \in \mathbb{N}$ esetén értelmezzük az a^{-k} negatív kitevőjű hatványt modulo m: legyen $a^{-k} \equiv \left(a^k\right)^{-1} \pmod m$. Ez összhangban van a 2.47. Definícióval): $\overline{a} \in \mathbb{Z}_m^*$ esetén $(\overline{a})^{-k} = \left(\overline{a}^k\right)^{-1}$.

2.64. Megjegyzés. Meg lehet mutatni, hogy a hatványozás szokásos azonosságai érvényben maradnak az egész kitevős modulo m hatványozás fenti értelmezése mellett. Figyelni kell azonban arra, hogy a jelölés ugyanaz, mint a valós számok hatványozásánál, de a jelentése negatív kitevő esetén egészen más. Például $3^{-2} \equiv 9^{-1} \equiv 2^{-1} \equiv 4 \pmod 7$, de annak, hogy $3^{-2} \equiv 1/9 \pmod 7$ nincs értelme, mert a kongruencia csak egész számokra van értelmezve.

2.65. Definíció. Ha $a \in \mathbb{Z}$ és $m \geq 2$ relatív prímek, akkor a ***modulo*** m ***rendjén*** azt a legkisebb pozitív egész kitevőt értjük, amelyre a-t emelve olyan számot kapunk, ami m-mel osztva 1-et ad maradékul. Jelölés: $o_m(a)$. Hasonlóan, egy $\overline{a}$ redukált maradékosztály ***rendjén*** azt a legkisebb pozitív egész kitevőt értjük, amelyre $\overline{a}$-t emelve $\overline{1}$-t kapunk. Jelölés: $o(\overline{a})$. Formálisan:

$$o_m(a) := \min\left\{k \in \mathbb{N} : a^k \equiv 1 \pmod{m}\right\};$$
$$o(\overline{a}) := \min\left\{k \in \mathbb{N} : \overline{a}^k = \overline{1}\right\}.$$

Ha a nem relatív prím m-hez, akkor $o_m(a)$ és $o(\overline{a})$ nem értelmezett, $a \perp m$ esetén pedig mindkettő értelmezett (ez következik pl. a 2.69. Tételből, de anélkül sem nehéz belátni), és természetesen ekkor $o_m(a) = o(\overline{a})$.

2.66. Példa. Határozzuk meg $o_{18}(7)$ értékét. Ehhez kezdjük el hatványozni a $\overline{7} \in \mathbb{Z}_{18}^*$ elemet:

k	1	2	3	4	5	6	7	8	$\cdots$
$\overline{7}^k$	$\overline{7}$	$\overline{13}$	$\overline{1}$	$\overline{7}$	$\overline{13}$	$\overline{1}$	$\overline{7}$	$\overline{13}$	$\cdots$

A harmadik hatványra jött ki először $\overline{1}$, ezért $o(\overline{7}) = 3 = o_{18}(7)$.

2.67. Tétel. Tetszőleges $\overline{a} \in \mathbb{Z}_m^*$ redukált maradékosztály és $k, \ell \in \mathbb{Z}$ kitevők esetén érvényesek az alábbiak.

(1) $\overline{a}^k = \overline{1} \iff o(\overline{a}) \mid k$

(2) $\overline{a}^k = \overline{a}^\ell \iff k \equiv \ell \pmod{o(\overline{a})}$

(3) $o(\overline{a}^k) = \dfrac{o(\overline{a})}{\operatorname{lnko}(o(\overline{a}), k)}$

Bizonyítás.

(1) Osszuk el a k kitevőt maradékosan az $o(\overline{a})$ renddel: $k = q \cdot o(\overline{a}) + r$, ahol $0 \leq r < o(\overline{a})$. Ekkor

$$\overline{a}^k = \overline{a}^{q \cdot o(\overline{a}) + r} = (\overline{a}^{o(\overline{a})})^q \cdot \overline{a}^r = \overline{1}^q \cdot \overline{a}^r = \overline{a}^r.$$

- $\Longleftarrow$: Ha $o(\overline{a}) \mid k$, azaz $r = 0$, akkor $\overline{a}^k = \overline{a}^r = \overline{a}^0 = \overline{1}$.
- $\Longrightarrow$: Ha $o(\overline{a}) \nmid k$, azaz $0 < r < o(\overline{a})$, akkor $\overline{a}^k = \overline{a}^r \neq \overline{1}$, mert $o(\overline{a})$ a legkisebb olyan pozitív kitevő, melyre $\overline{a}$-t emelve a hatvány $\overline{1}$ lesz.

(2) Ezt könnyen visszavezethetjük az első állításra:

$$\overline{a}^k = \overline{a}^\ell \iff \overline{a}^{k-\ell} = \overline{1} \iff o(\overline{a}) \mid k - \ell \iff k \equiv \ell \pmod{o(\overline{a})}.$$

(3) Keressük meg mindazon j „jó” kitevőket, amelyekre $(\overline{a}^k)^j = \overline{1}$:

$$(\overline{a}^k)^j = \overline{1} \iff \overline{a}^{kj} = \overline{1} \iff o(\overline{a}) \mid kj \iff \frac{o(\overline{a})}{\operatorname{lnko}(o(\overline{a}), k)} \;\Big|\; j.$$

Tehát az $\overline{a}^k$-hoz tartozó jó kitevők éppen $\frac{o(\overline{a})}{\operatorname{lnko}(o(\overline{a}),k)}$ többszörösei, így a legkisebb jó kitevő $o(\overline{a}^k) = \frac{o(\overline{a})}{\operatorname{lnko}(o(\overline{a}),k)}$. □

2.68. Példa. Mit ad 18-cal osztva maradékul 7^{1001}? A 2.66. Példában megállapítottuk, hogy $o_{18}(7) = 3$. A 2.67. Tételből tudjuk, hogy ezt azt jelenti, hogy $\overline{7} \in \mathbb{Z}_{18}^*$ hatványozásakor a kitevő modulo 3 „számít”. Mivel $1001 \equiv 2 \pmod{3}$, azt kapjuk, hogy $\overline{7}^{1001} = \overline{7}^2 = \overline{13}$, vagyis $7^{1001} \equiv 13 \pmod{18}$.

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

Bizonyítás. Legyen $c_1, \ldots, c_{\varphi(m)}$ egy tetszőleges redukált maradékrendszer modulo m, azaz $\left\{\overline{c_1}, \ldots, \overline{c_{\varphi(m)}}\right\} = \mathbb{Z}_m^*$. Ha $a \perp m$, akkor a 2.60 . Állítás szerint $\left\{\overline{ac_1}, \ldots, \overline{ac_{\varphi(m)}}\right\} = \mathbb{Z}_m^*$. 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. □

2.70. 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?). □

2.71. 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?):

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

2.72. Következmény. Ha $a \in \mathbb{Z}$ relatív prím az $m \geq 2$ modulushoz, akkor tetszőleges $k, \ell \in \mathbb{Z}$ kitevők esetén

(1) $o_m(a) \mid \varphi(m)$;
(2) $k \equiv \ell \pmod{\varphi(m)} \implies a^k \equiv a^\ell \pmod{m}$.

Bizonyítás.

(1) Az Euler–Fermat-tétel szerint $\overline{a}^{\varphi(m)} = \overline{1}$, és így a 2.67. Tétel (1)-es állításából következik, hogy $o_m(a) \mid \varphi(m)$.
(2) Tfh. $k \equiv \ell \pmod{\varphi(m)}$. A most belátott $o_m(a) \mid \varphi(m)$ oszthatóság szerint ekkor $k \equiv \ell \pmod{o_m(a)}$ is teljesül (ugye?), és így a 2.67. Tétel (2)-es állításából következik, hogy $a^k \equiv a^\ell \pmod{m}$.

□

2.73. 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 $3 \perp 44$. Most számítsuk ki az Euler-féle φ függvény értékét a modulusnál: $\varphi(44) = \varphi(4) \cdot \varphi(11) = 2 \cdot 10 = 20$. A 2.72. 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 $x \equiv 5 \pmod{44}$.)

2.74. Tétel. Minden racionális szám tizedes tört alakja periodikus. Konkrétabban: ha a és b relatív prím természetes számok és $b > 1$, akkor

(i) ha b minden prímosztója 2 vagy 5, akkor $\frac{a}{b}$ véges tizedes tört;
(ii) ha b prímosztói között nem szerepel se 2 se 5, akkor $\frac{a}{b}$ tiszta szakaszos tizedes tört;
(iii) ha b prímosztói között szerepel 2 vagy 5, és szerepel más prímszám is, akkor $\frac{a}{b}$ vegyes szakaszos tizedes tört.

Bizonyítás.

(i) Tfh. $b = 2^k \cdot 5^\ell$ $(k, \ell \in \mathbb{N}_0)$, és legyen $m = \max(k, \ell)$. Ekkor a törtet tudjuk úgy bővíteni, hogy a nevező 10 hatványa legyen:

$$\frac{a}{b} = \frac{a}{2^k \cdot 5^\ell} = \frac{a \cdot 2^{m-k} \cdot 5^{m-\ell}}{2^m \cdot 5^m} = \frac{a \cdot 2^{m-k} \cdot 5^{m-\ell}}{10^m} = \frac{a'}{10^m}.$$

Ebből következik, hogy $\frac{a}{b}$ véges tizedes tört (ugye?).

(ii) Tfh. b prímosztói között nem szerepel se 2 se 5, és az általánosság megszorítása nélkül tfh. $a < b$. Ekkor $\frac{a}{b}$ tizedes tört alakja így fest:

$$\frac{a}{b} = 0, d_1 d_2 \ldots, \text{ ahol } d_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Mivel $b \perp 10$, értelmezett az $r = o_b(10)$ rend. Szorozzuk meg az $\frac{a}{b}$ törtet 10^r-rel:

$$\frac{10^r \cdot a}{b} = d_1 d_2 \ldots d_r, d_{r+1} d_{r+2} \ldots.$$

Vonjuk ki egymásból a fenti két törtet:

$$\frac{10^r \cdot a}{b} - \frac{a}{b} = \frac{10^r - 1}{b} \cdot a.$$

Ez egy egész szám (miért?), következésképp $\frac{a}{b}$ és $\frac{10^r \cdot a}{b}$ törtrésze megegyezik. A tizedes tört alakokat tekintve a törtrészek megegyezése azt jelenti, hogy $d_1 = d_{r+1}$, $d_2 = d_{r+2}$, és így tovább. Tehát $\frac{a}{b}$ valóban szakaszos tizedes tört, és a szakasz hossza r.

(iii) Tfh. $b = 2^k \cdot 5^\ell \cdot c$ $(k, \ell \in \mathbb{N}_0,\ c \perp 10)$, ahol k és ℓ közül legalább az egyik pozitív, és $c > 1$. Az első részhez hasonló módszerrel bővítjük a törtet (továbbra is az $m = \max(k, \ell)$ jelölést használva):

$$\frac{a}{b} = \frac{a}{2^k \cdot 5^\ell \cdot c} = \frac{a \cdot 2^{m-k} \cdot 5^{m-\ell}}{2^m \cdot 5^m \cdot c} = \frac{1}{10^m} \cdot \frac{a \cdot 2^{m-k} \cdot 5^{m-\ell}}{c} = \frac{1}{10^m} \cdot \frac{a'}{c}.$$

Itt (ii) alapján $\frac{a'}{c}$ tiszta szakaszos tizedes tört, és ebből következik, hogy $\frac{a}{b}$ vegyes szakaszos tizedes tört (ugye?).

□

2.75. Megjegyzés. A 2.74. Tétel természetesen általánosítható tetszőleges alapú számrendszerre (hogyan?).

2.76. Megjegyzés. A 2.74. Tétel megfordítása is érvényes: minden periodikus (azaz véges, tiszta szakaszos vagy vegyes szakaszos) tizedes tört racionális szám. Bizonyítás helyett egy példán mutatjuk meg, hogyan lehet az $x = 65,289\,\overline{3115}$ periodikus tizedes törtet felírni két egész szám hányadosaként:

$$\begin{aligned} x &= 65\,,289\,3115\,3115\,3115\,3115\ldots \\ 10^3x &= 65289\,,3115\,3115\,3115\,3115\ldots \\ 10^7x &= 652893115\,,3115\,3115\,3115\,3115\ldots \end{aligned}$$

A fenti számolásból következik, hogy 10^7x és 10^3x törtrésze megegyezik, ezért különbségük egész szám. Ebből meg is kapjuk x felírását két egész szám hányadosaként:

$$10^7x - 10^3x = 652\,827\,826 \implies x = \frac{652\,827\,826}{10^7 - 10^3} = \frac{652\,827\,826}{9\,999\,000} = \frac{326\,413\,913}{4\,999\,500}.$$

Primitív gyök, index

2.77. Definíció. Azt mondjuk, hogy a g egész szám ***primitív gyök*** modulo m, ha rendje éppen $\varphi(m)$.

2.78. Állítás. A g egész szám akkor és csak akkor primitív gyök modulo m, ha az összes $\bmod m$ redukált maradékosztály megkapható $\overline{g}$ hatványaként.

Bizonyítás. A 2.67. Tétel második állítása szerint éppen $o(\overline{g})$ darab redukált maradékosztály áll elő $\overline{g}$ hatványaként. Mivel összesen $\varphi(m)$ redukált maradékosztály van, pontosan akkor kapjuk meg mindet $\overline{g}$ hatványaként, ha $o(\overline{g}) = \varphi(m)$. □

2.79. Tétel. A következő modulusokhoz létezik primitív gyök (és csak ezekhez): $2, 4$, páratlan prímhatványok, páratlan prímhatványok kétszeresei. Ezekben az esetekben a $\bmod m$ primitív gyökök száma $\varphi(\varphi(m))$.

2.80. Megjegyzés. A fenti tétel bizonyítása nehéz, ezért nem ismertetjük. Csak annyit említünk meg, hogy prím modulus esetén a 2.59. Tétel fontos szerepet játszik a bizonyításban.

2.81. Definíció. Tegyük fel, hogy g primitív gyök az m modulushoz. Az a egész szám ***indexén*** (az m modulusra és a g primitív gyökre nézve) olyan i kitevőt értünk, amelyre $g^i \equiv a \pmod{m}$.

Jelölés. A modulust az egyszerűség kedvéért nem írjuk ki (ez többnyire amúgy is világos a szövegkörnyezetből), tehát a indexét röviden $\operatorname{ind}_g a$ jelöli.

2.82. Megjegyzés. Világos, hogy ha a és m nem relatív prím, akkor $\operatorname{ind}_g a$ nem értelmezett (ugyanis g^i mindig relatív prím m-hez). Ha viszont a és m relatív prím, akkor a 2.78. Állítás szerint a előáll g hatványaként modulo m, tehát ekkor $\operatorname{ind}_g a$ értelmezett.

2.83. Megjegyzés. Figyeljük meg, hogy az index nem más, mint a logaritmus mod m analogonja. Nem meglepő tehát, hogy hasonló tulajdonságokkal rendelkezik, amint ezt a következő tételben látjuk. A 2.67. Tétel második állítása szerint az index csak modulo $\varphi(m)$ van meghatározva, ezért az indexre vonatkozó alábbi azonosságokban nem egyenlőségeket, hanem $\pmod{\varphi(m)}$ kongruenciákat írunk.

2.84. Tétel. Legyen g primitív gyök modulo m, legyen k tetszőleges egész szám, a és b pedig relatív prímek m-hez. Ekkor érvényesek az alábbi azonosságok:

(i) $\operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$;

(ii) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$;

(iii) $\operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;

(iv) $\operatorname{ind}_g(ab^{-1}) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

Bizonyítás.

(i) $g^0 \equiv 1 \pmod{m} \implies \operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$.

(ii) $ab \equiv g^{\operatorname{ind}_g(a)} g^{\operatorname{ind}_g(b)} \equiv g^{\operatorname{ind}_g(a)+\operatorname{ind}_g(b)} \pmod{m} \implies \operatorname{ind}_g(ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$.

(iii) $a^k \equiv (g^{\operatorname{ind}_g(a)})^k \equiv g^{k \operatorname{ind}_g(a)} \pmod{m} \implies \operatorname{ind}_g a^k \equiv k \cdot \operatorname{ind}_g a \pmod{\varphi(m)}$;

(iv) $ab^{-1} \equiv g^{\operatorname{ind}_g(a)}(g^{\operatorname{ind}_g(b)})^{-1} \equiv g^{\operatorname{ind}_g(a)-\operatorname{ind}_g(b)} \pmod{m} \implies \operatorname{ind}_g(ab^{-1}) \equiv \operatorname{ind}_g a - \operatorname{ind}_g b \pmod{\varphi(m)}$.

□

2.85. Példa. Ellenőrizzük, hogy $g = 2$ primitív gyök a $p = 11$ modulushoz. Ehhez számítsuk ki 2 hatványaink modulo 11 maradékait:

i	0	1	2	3	4	5	6	7	8	9	10
2^i	1	2	4	8	5	10	9	7	3	6	1

(Az utolsó oszlopot nem is kellett volna kiszámolni, mert a kis Fermat-tételből tudjuk, hogy $2^{10} \equiv 1 \pmod{11}$. Nem is lesz szükségünk erre az oszlopra, ezért írtuk szürkével.) A táblázatból látható, hogy $o_{11}(2) = 10 = \varphi(11)$, tehát 2 valóban primitív gyök modulo 11. Az is látszik a táblázatból, hogy minden modulo 11 redukált maradékosztály megkapható $\overline{2}$ hatványaként. A táblázatban minden szám fölött az indexe található. Ha megcseréljük a két sort, és a fölső számok szerint rendezzük az oszlopokat, akkor kapjuk az alábbi ***indextáblázatot***:

a	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_g a$	0	1	8	2	4	9	7	3	6	5

2.86. Példa. Oldjuk meg a fenti példában konstruált indextáblázat segítségével az $x^6 \equiv 5 \pmod{11}$ kongruenciát. A megoldást kereshetjük $x \equiv 2^i \pmod{11}$ alakban (miért?), és a jobb oldali 5-öst is felírhatjuk 2 hatványaként. Így az $i = \operatorname{ind}_2 x$ ismeretlenre egy lineáris kongruenciát kapunk, amit könnyen meg tudunk oldani:

$$\begin{aligned} x^6 \equiv 5 \pmod{11} &\iff 2^{6i} \equiv 2^4 \pmod{11} \\ &\iff 6i \equiv 4 \pmod{10} \\ &\iff i \equiv 4 \pmod{5} \\ &\iff i \equiv 4, 9 \pmod{10} \\ &\iff 2^i \equiv 5, 6 \pmod{11} \\ &\iff x \equiv 5, 6 \pmod{11} \end{aligned}$$

Eredményünk így is megfogalmazható: a $\mathbb{Z}_{11}$ testben $\overline{5}$-nak két hatodik gyöke van, mégpedig $\overline{5}$ és $\overline{6}$.

2.87. Definíció. Azt mondjuk, hogy az a egész szám ***n-edik hatványmaradék*** modulo m, ha az $x^n \equiv a \pmod{m}$ kongruenciának van megoldása.

2.88. Tétel. Legyen g primitív gyök modulo m, és legyen a relatív prím m-hez. Ekkor a pontosan akkor n-edik hatványmaradék modulo m, ha $\operatorname{lnko}(n, \varphi(m)) \mid \operatorname{ind}_g a$.

Bizonyítás. Ha $a \perp m$, akkor az $x^n \equiv a \pmod{m}$ kongruencia megoldása(i) is relatív prím(ek) m-hez (ha van egyáltalán megoldás). Ezért kereshetjük a megoldást $x \equiv g^i \pmod{m}$ alakban. Írjul fel a-t is g hatványaként: $a \equiv g^{\operatorname{ind}_g a} \pmod{m}$. Helyettesítsük ezt be a kongruenciába, és „hozzuk le” a kitevőket:

$$x^n \equiv a \pmod{m} \iff g^{ni} \equiv g^{\operatorname{ind}_g a} \pmod{m} \iff ni \equiv \operatorname{ind}_g a \pmod{\varphi(m)}.$$

Egy lineáris kongruenciát kaptunk az i ismeretlenre, és ennek a kongruenciának akkor és csak akkor van megoldása, ha $\operatorname{lnko}(n, \varphi(m)) \mid \operatorname{ind}_g a$. □

Négyzetes maradékok, Legendre-szimbólum

2.89. Definíció. Az a egész számot ***négyzetes maradéknak*** nevezzük modulo m, ha az $x^2 \equiv a \pmod{m}$ kongruenciának van megoldása. Ellenkező esetben azt mondjuk, hogy a ***négyzetes nemmaradék*** modulo m.

2.90. Példa. Közismert (és könnyen ellenőrizhető), hogy négyzetszám nem adhat 2-t maradékul hárommal osztva (0-t és 1-et persze adhat). Tehát a akkor és csak akkor négyzetes nemmaradék modulo 3, ha $a \equiv 2 \pmod{3}$. Hasonlóan, modulo 4 a négyzetes maradékok 0 és 1, a négyzetes nemmaradékok pedig 2 és 3.

2.91. Tétel. Legyen p páratlan prímszám, g primitív gyök modulo p. Ekkor $a \in \mathbb{Z}$ pontosan akkor négyzetes maradék modulo p, ha $p \mid a$ vagy $\operatorname{ind}_g a$ páros.

Bizonyítás. Ha $p \mid a$, akkor $a \equiv 0 \pmod{p}$, és a 0 nyilván négyzetes maradék. Ha $p \nmid a$, akkor $a \perp p$, így alkalmazható a 2.88. Tétel: a akkor és csak akkor négyzetes maradék, ha $\operatorname{lnko}(2, \varphi(p)) \mid \operatorname{ind}_g a$. Mivel $\varphi(p) = p - 1$ páros szám, $\operatorname{lnko}(2, \varphi(p)) = 2$, és ezzel kész is a bizonyítás. □

2.92. Definíció. Tetszőleges p páratlan prímszám és p-vel nem osztható a egész szám esetén értelmezzük az $\left(\frac{a}{p}\right)$ ***Legendre-szimbólumot*** a következőképpen:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék } \bmod p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék } \bmod p. \end{cases}$$

2.93. Tétel (Euler-kritérium). Ha p páratlan prímszám és $p \nmid a$, akkor

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

2.94. Tétel. Tetszőleges p páratlan prímszám és p-vel nem osztható a, b egész számok esetén teljesülnek az alábbiak:

(1) $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

2.95. Tétel (négyzetes reciprocitási tétel). Tetszőleges p, q különböző páratlan prímszámok esetén

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

2.96. Tétel (a négyzetes reciprocitási tétel első kiegészítő tétele). Tetszőleges p páratlan prímszám esetén

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4}; \\ -1, & \text{ha } p \equiv 3 \pmod{4}. \end{cases}$$

2.97. Tétel (a négyzetes reciprocitási tétel második kiegészítő tétele). Tetszőleges p páratlan prímszámra

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{ha } p \equiv 1, 7 \pmod{8}; \\ -1, & \text{ha } p \equiv 3, 5 \pmod{8}. \end{cases}$$

3. Számelméleti függvények

Osztók száma, osztók összege

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

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

3.2. 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).

3.3. Példa. Mivel $D_{72} = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 73\}$, ezért $\tau(72) = 12$ és $\sigma(72) = 195$ (ellenőrizzük!).

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

$$\tau(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1).$$

Bizonyítás. Ha $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, akkor az 1.37. Következmény szerint n pozitív osztói pontosan az alábbi számok:

$$p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}, \text{ ahol } 0 \le \beta_i \le \alpha_i.$$

Itt minden i esetén a β_i kitevőre $\alpha_i + 1$ lehetőség van, ezért összesen $(\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1)$ lehetőség van a kitevőket megválasztani a fenti osztóban. □

3.5. Példa. Számítsuk ki 1500 osztóinak számát. A prímhatványtényezős felbontás: $1500 = 2^2 \cdot 3 \cdot 5^3$, ezért $\tau(1500) = (2+1) \cdot (1+1) \cdot (3+1) = 3 \cdot 2 \cdot 4 = 24$.

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

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

Bizonyítás. A 3.4. Tétel bizonyításában megadtuk n osztóit, tehát most már nincs más dolgunk, mint összegezni a $p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$ $(0 \le \beta_i \le \alpha_i)$ alakú számokat:

$$\sigma(n) = \sum_{0 \le \beta_i \le \alpha_i} p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}.$$

Ha a $\prod_{i=1}^{k} (1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i})$ szorzatban felbontjuk a zárójeleket, akkor valóban éppen a fenti összeget kapjuk:

$$\prod_{i=1}^{k} (1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}) = \left(\sum_{0 \le \beta_1 \le \alpha_1} p_1^{\beta_1} \right) \cdot \ldots \cdot \left(\sum_{0 \le \beta_k \le \alpha_k} p_k^{\beta_k} \right) = \sum_{0 \le \beta_i \le \alpha_i} p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}.$$

□

3.7. Példa. Ha n-nek csak két prímosztója van, azaz $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, akkor osztói a $p_1^{\beta_1} \cdot p_2^{\beta_2}$ $(0 \le \beta_i \le \alpha_i)$ alakú számok. Ebben az esetben így fest a fenti tétel bizonyítása:

$$(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) = \left(\sum_{0 \le \beta_1 \le \alpha_1} p_1^{\beta_1} \right) \cdot \left(\sum_{0 \le \beta_k \le \alpha_k} p_k^{\beta_k} \right) = \sum_{0 \le \beta_i \le \alpha_i} p_1^{\beta_1} \cdot p_2^{\beta_2} = \sigma(n).$$

A számolás áttekinthetőbb, ha táblázatba rendezzük n osztóit, először soronként összegzünk, majd a összeadjuk a sorösszegeket:

$$\begin{array}{lllllll}
1 & p_1 & p_1^2 & \cdots & p_1^{\alpha_1} & \longrightarrow & (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \\
p_2 & p_1p_2 & p_1^2p_2 & \cdots & p_1^{\alpha_1}p_2 & \longrightarrow & (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot p_2 \\
p_2^2 & p_1p_2^2 & p_1^2p_2^2 & \cdots & p_1^{\alpha_1}p_2^2 & \longrightarrow & (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot p_2^2 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
p_2^{\alpha_2} & p_1p_2^{\alpha_2} & p_1^2p_2^{\alpha_2} & \cdots & p_1^{\alpha_1}p_2^{\alpha_2} & \longrightarrow & (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot p_2^{\alpha_2} \\
 & & & & & & \downarrow \\
 & & & & & & (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2})
\end{array}$$

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

Gyengén multiplikatív számelméleti függvények

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

3.10. Tétel. Ha az f számelméleti függvény gyengén multiplikatív, akkor tetszőleges páronként különböző $p_1, \ldots, p_k$ prímszámok és tetszőleges $\alpha_1, \ldots, \alpha_k$ 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. 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. □

3.11. Megjegyzés. A fenti tétel következő megfordítása is igaz: ha $f(1) = 1$ és $f(n)$ értékeit a tételben leírt módon minden n esetén ki lehet számítani az $f(p_i^{\alpha_i})$ értékek szorzataként, akkor f gyengén multiplikatív.

3.12. Lemma. Ha a és b relatív prím pozitív egész számok, akkor ab pozitív osztói éppen a és b pozitív osztóinak szorzatai, továbbá ab minden pozitív osztója egyértelműen áll elő a egy pozitív osztójának és b egy pozitív osztójának szorzataként.

Bizonyítás. Legyenek a osztói $u_1, \ldots, u_k$ és b osztói $v_1, \ldots, v_\ell$ (itt persze $k = \tau(a)$ és $\ell = \tau(b)$). Három dolgot kell bizonyítanunk:

(i) minden i és j esetén $u_iv_j \mid ab$;
(ii) ha $d \mid ab$, akkor van olyan i és j, hogy $d = u_iv_j$;
(iii) ha $u_{i_1}v_{j_1} = u_{i_2}v_{j_2}$, akkor $i_1 = i_2$ és $j_1 = j_2$.

Lássunk hozzá:

(i) Tudjuk, hogy $a = u_is$ és $b = v_jt$ alkalmas s és t egész számokkal. Ebből következik, hogy $ab = u_jv_j \cdot st$, ez pedig igazolja, hogy $u_iv_j \mid ab$.
(ii) Tfh. $d \mid ab$, és legyen $u = \operatorname{lnko}(d, a)$, $v = \frac{d}{\operatorname{lnko}(d,a)}$. Ekkor $u \mid a$ (ugye?), tehát $u = u_i$ alkalmas i indexszel. Euklidész lemmája szerint teljesül $v \mid b$ is (miért?), tehát $v = v_j$ alkalmas j indexszel. Az $u = u_i$ és $v = v_j$ számokat eleve úgy konstruáltuk, hogy $d = uv = u_iv_j$ teljesüljön, ezzel tehát kész a bizonyítás.
(iii) Tfh. $u_{i_1}v_{j_1} = u_{i_2}v_{j_2}$. Abból, hogy a és b relatív prím, következik, hogy $u_{i_1} \perp v_{j_2}$ (miért?). Az $u_{i_1}v_{j_1} = u_{i_2}v_{j_2}$ egyenlőség miatt $u_{i_1} \mid u_{j_2}v_{j_2}$ (ugye?). Alkalmazva az 1.22. Következményt, nyerjük, hogy $u_{i_1} \mid u_{i_2}$. Hasonlóan belátható, hogy $u_{i_2} \mid u_{i_1}$, tehát $u_{i_1} = u_{i_2}$ (miért?), és így $i_1 = i_2$. Ezután már az $u_{i_1}v_{j_1} = u_{i_2}v_{j_2}$ egyenlőségből egyszerű egyszerűsítéssel kapjuk, hogy $v_{j_1} = v_{j_2}$, azaz $j_1 = j_2$. □

3.13. Megjegyzés. Az előző lemma állítása kicsit formálisabban így fogalmazható meg: ha $a \perp b$, akkor az alábbi leképezés bijekció:

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

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

Bizonyítás. Az világos, hogy $\tau(1) = \sigma(1) = 1$. Tfh. $a \perp b$, legyenek a osztói $u_1, \dots, u_k$ és b osztói $v_1, \dots, v_\ell$ (itt persze $k = \tau(a)$ és $\ell = \tau(b)$). A 3.12. Lemma szerint ab osztói pontosan az $u_i v_j$ $(i = 1, \dots, k,\ j = 1, \dots, \ell)$ alakú számok, és ab minden osztója egyértelműen áll elő ilyen alakban. Ebből rögtön következik, hogy ab osztóinak száma: $\tau(ab) = k \cdot \ell = \tau(a) \cdot \tau(b)$. Ezzel τ gyenge multiplikativitását be is láttuk.

A σ függvény gyenge multiplikativitásának igazolásához számítsuk ki a $\sigma(a) \cdot \sigma(b)$ szorzatot, bontsuk fel a zárójeleket, és győződjünk meg róla, hogy az eredmény éppen $\sigma(ab)$:

$$\sigma(a) \cdot \sigma(b) = (u_1 + \dots + u_k) \cdot (v_1 + \dots + v_\ell) = u_1 v_1 + u_1 v_2 + \dots + u_k v_\ell = \sum_{i,j} u_i v_j = \sigma(ab).$$

Az utolsó lépésben azt használtuk fel, hogy az $u_i v_j$ alakú számok éppen ab osztói (és ab minden osztója pontosan egyszer lép fel); ehhez volt szükségünk a 3.12. Lemmára. Ezzel beláttuk, hogy σ is gyengén multiplikatív. □

A gyenge multiplikativitást használva új, egyszerűbb bizonyítást kapunk $\tau(n)$ és $\sigma(n)$ képletére.

3.15. Tétel. Legyen az n pozitív egész 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, a 3.10. Tételt használva már kész is a bizonyítás. □

3.16. Tétel. Az Euler-féle φ függvény gyengén multiplikatív.

Bizonyítás. Tfh. $m \perp n$, és tekintsük az alábbi kongruenciarendszert:

$$\left.\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}\right\}$$

Ennek a kongruenciarendszernek minden a és b esetén van megoldása, és a megoldások egyetlen maradékosztályt alkotnak modulo $\operatorname{lkkt}(m, n) = mn$. Ezért pontosan egy megoldás esik a $\{0, 1, \dots, mn-1\}$ halmazba; jelölje ezt a megoldást $f(a, b)$. Ezzel definiáltunk egy f leképezést:

$$f\colon \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\} \to \{0, 1, \dots, mn-1\},\ (a, b) \mapsto f(a, b).$$

Tetszőleges $x \in \{0, 1, \dots, mn-1\}$ egész szám esetén egyértelműen meg lehet adni, hogy milyen a és b értékek esetén lesz x megoldása a fenti kongruenciarendszernek, így kapjuk az f leképezés inverzét:

$$f^{-1}\colon \{0, 1, \dots, mn-1\} \to \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\},\ x \mapsto \big(x \bmod m,\, x \bmod n\big).$$

(Itt „$x \bmod m$” azt jelöli, hogy mit ad x maradékul m-mel osztva. Bizonyos programozási nyelvekben használatos ez a jelölés; a matematikában sajnos nincs bevett jelölés a maradékra.) Látjuk tehát, hogy f bijektív leképezés.

Térjünk most már rá az Euler-féle φ függvény vizsgálatára: $\varphi(mn)$ azt adja meg, hogy a $\{0, 1, \dots, mn-1\}$ halmaznak hány olyan eleme van, ami relatív prím mn-hez (ugye)? Legyen $x \in \{0, 1, \dots, mn-1\}$, és legyen $f^{-1}(x) = (a, b)$. Az világos, hogy $x \perp mn \iff x \perp m$ és $x \perp n$ (miért?). Mivel $x \equiv a \pmod{m}$, a 2.11. Tételbeli (8)-as tulajdonság szerint $\operatorname{lnko}(x, m) = \operatorname{lnko}(a, m)$, tehát $x \perp m \iff a \perp m$. Hasonlóan kapjuk, hogy $x \perp n \iff b \perp n$. Összefoglalva:

$$x \perp mn \iff a \perp m \text{ és } b \perp n. \qquad (\spadesuit)$$

A bal oldalon x-re $\varphi(mn)$ lehetőség van, a jobb oldalon a-ra $\varphi(m)$ lehetőség van, b-re pedig $\varphi(n)$ lehetőség. Mivel az f leképezés bijekciót létesít a megfelelő x-ek és (a, b) párok között, kapjuk, hogy $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. □

3.17. Megjegyzés. A fenti tétel bizonyítását maradékosztályokkal is megfogalmazhatjuk. Ha $m \perp n$, akkor a bizonyításban definiált f és f^{-1} leképezések megadnak egy

$$\mathbb{Z}_{mn} \longleftrightarrow \mathbb{Z}_m \times \mathbb{Z}_n,$$

párbaállítást (oda-vissza bijekciót), ami ($\spadesuit$) következtében rendelkezik az alábbi tulajdonsággal:

$$\text{ha } \overline{x} \in \mathbb{Z}_{mn} \text{ és } (\overline{a}, \overline{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n \text{ egymásnak felel meg, akkor } x \in \mathbb{Z}_{mn}^* \iff a \in \mathbb{Z}_m^* \text{ és } b \in \mathbb{Z}_n^*.$$

Tehát a fenti párbaállítást megszorítva kapunk egy $\mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ bijekciót, következésképp a két halmaz elemszáma megegyezik, és ez igazolja φ gyenge multiplikativitását:

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

A gyenge multiplikativitást használva az Euler-féle φ függvény képletére is kaptunk egy új bizonyítást, ami egyszerűbb, mint a korábbi szita-formulás bizonyítás.

3.18. Tétel. Legyen az n pozitív egész 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. A 3.10. Tétel miatt elég prímhatványokra igazolni a képletet, ezt pedig már megtettük a 2.53. Állításban. □

Tökéletes számok, Mersenne- és Fermat-prímek

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

3.20. 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: $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1) \cdot (\ldots)$; 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. □

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

3.22. 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 $\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$.

3.23. 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 3.20. 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. □

3.24. 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.

3.25. 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 (2023. április 21.) ismert legnagyobb prímszám is Mersenne-prím: $M_{82\,589\,933}$, ami tízes számrendszerben 24 862 048 számjegyből áll.

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

3.27. Megjegyzés. A 3.20. 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).

4. Nevezetes számelméleti problémák

Prímszámok

4.1. 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. □

4.2. 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 $N \equiv -1 \pmod 4$. □

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

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

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

4.6. 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 $n \geq 2$, 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.) □

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

4.8. 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).

4.9. Tétel. A prímszámok reciprokaiból alkotott sor divergens, azaz $\sum_p \frac{1}{p} = \infty$.

4.10. 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).

4.11. 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).

4.12. 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 4.1. 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 $p_{n+1} \leq p \leq p_1 \cdot \ldots \cdot p_n + 1$ (miért?), azaz

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

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

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

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

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

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

4.13. 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:

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

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

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

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

Számok felbontása hatványok összegére

4.16. 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 $\text{lnko}(x, y, z) \sim 1$.

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

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

Bizonyítás. Legyen (x, y, z) primitív pitagoraszi számhármas, és legyen $d = \text{lnko}(x, y)$. 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 $d \mid \text{lnko}(x, y, z) \sim 1$ (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). □

4.19. 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. □

4.20. Lemma. Ha U és V relatív prím pozitív egész 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?). □

4.21. 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 4.19. 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 4.20 . 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 $y\perp z$. □

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

4.23. 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.

4.24. 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:

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

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

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

4.27. Tétel (Lagrange-féle négynégyzetszám-tétel). Minden pozitív egész szám előáll négy négyzetszám összegeként.

4.28. Megjegyzés. Lagrange tétele éles abban az értelemben, hogy három négyzetszám összegeként nem lehet minden pozitív egész számot előállítani (keressünk ellenpéldát!). A pozitív egész 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 pozitív egész 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?