ALGEBRA ÉS SZÁMELMÉLET 3

jegyzet az előadáshoz[†]

2020 őszi félév, OT

Waldhauser Tamás

szeptember 10.

1. Számelméleti kongruenciák

Lineáris diofantoszi egyenletek

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

(1) $d \mid a$ és $d \mid b$;

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

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

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

1.2. Megjegyzés. A legnagyobb közös osztó nem egyértelmű: ha d legnagyobb közös osztója a-nak és b-nek, akkor $-d$ is az (de e két számon kívül nincs más legnagyobb közös osztó). Általában a két érték közül a nemnegatívat szoktuk tekinteni.

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

Biz. (nyuszibogyókkal) Ha $a = 0$, akkor az állítás triviális: $\operatorname{lnko}(0,b) = b = 0 \cdot 239 + b \cdot 1$ (tehát pl. $x = 239, y = 1$ jó lesz). A $b = 0$ eset hasonló, ezért a továbbiakban feltesszük, hogy se a se b nem nulla. Legyen B az $ax + by$ alakban előálló pozitív egész számok halmaza: $B = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}$. Ez a halmaz nem üres (miért?), tehát van legkisebb eleme; jelöljük ezt d-vel: $d := \min B$. Mivel $d \in B$, alkalmas x_0, y_0 egész számokkal $d = ax_0 + by_0$. Bebizonyítjuk, hogy $d \sim \operatorname{lnko}(a,b)$. Az lnko definíciójának második része könnyen igazolható: ha $k \mid a$ és $k \mid b$, akkor $k \mid ax_0 + by_0 = d$ (ugye?).

Az első tulajdonság bizonyításához tfh. $d \nmid a$; ebből ellentmondásra fogunk jutni. Ha a-t maradékosan osztjuk d-vel, a maradék nem lesz nulla: $a = dq + r$, ahol $q, r \in \mathbb{Z}$ és $0 < r < d$ (miért?). Fejezzük ki innen a maradékot, és írjuk d helyébe az $ax_0 + by_0$ kifejezést: $r = a - dq = a - (ax_0 + by_0)\, q = a\,(1 - x_0 q) + b\,(-y_0 q)$. Azt kaptuk, hogy r előáll $ax + by\,(x, y \in \mathbb{Z})$ alakban, tehát $r \in B$ (miért?). Ez ellentmondás, hiszen $r < d$, pedig állítólag d volt a B halmaz legkisebb eleme. Tehát, feltevésünkkel ellentétben, d mégis osztója a-nak, és hasonlóan belátható, hogy $d \mid b$.

Ezzel igazoltuk, hogy d eleget tesz az lnko definíciójának, vagyis $d \sim \operatorname{lnko}(a,b)$. Beláttuk tehát, hogy létezik legnagyobb közös osztója a-nak és b-nek, és mivel d-t eleve $d = ax_0 + by_0$ alakban írtuk fel, a tétel „lineáris kombinációs" állítása is bizonyítást nyert. □

Biz. (euklideszi algoritmussal) Megint feltesszük, hogy $a \neq 0$ és $b \neq 0$. Ekkor végrehajtható az a, b számokra az euklideszi algoritmus (technikai okokból a és b az r_0 és r_1 „fedőneveket" kapják):

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

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

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

(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,

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

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):

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

Indukciós lépés: Legyen $2\le i<n$, 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: $r_{i+1}=r_{i-1}-q_ir_i$. Helyettesítsük r_{i-1} és r_i helyébe az indukciós hipotézisben szereplő felírásukat:

$$\begin{aligned} r_{i+1} = r_{i-1}-q_ir_i &= (ax_{i-1}+by_{i-1}) - q_i\,(ax_i+by_i)\\ &= a\,(x_{i-1}-q_ix_i) + b\,(y_{i-1}-q_iy_i)\,. \end{aligned}$$

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

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

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

Biz. A „$\Longleftarrow$” irány triviális (miért?). A „$\Longrightarrow$” irány bizonyításához tfh. $a\mid bc$ és persze azt is, hogy $a\perp b$. Használjuk az 1.3. Tételt: léteznek olyan x,y egész számok, amelyekre $ax+by=1\sim\operatorname{lnko}(a,b)$. Beszorozva c-vel azt kapjuk, hogy $acx+bcy=c$. Itt a bal oldalon mindkét tag osztható a-val (miért?), tehát az összegük is osztható a-val, vagyis $a\mid c$. □

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

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

Biz. Tfh. $d:=\operatorname{lnko}(a,b)\neq 0$ (milyen a,b esetén teljesül ez?). Az a és b számokat $a=a_0d$ és $b=b_0d$ alakba írhatjuk alkalmas a_0,b_0 egész számokkal (miért?). Az 1.3. Tétel szerint vannak olyan x,y egészek, amelyekre $ax+by=d$. Egyszerűsíthetünk d-vel (miért?), és így azt kapjuk, hogy $a_0x+b_0y=1$. 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. □

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

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

Biz. Tfh. $d:=\operatorname{lnko}(a,b)\neq 0$, és írjuk fel az a és b számokat az 1.6. Következmény bizonyításában látott módon $a=a_0d$ és $b=b_0d$ alakban; ekkor tehát $a_0\perp b_0$. A két irányt egyszerre igazoljuk:

$$\begin{aligned} a\mid bc &\iff a_0d\mid b_0dc && \text{(miért?)}\\ &\iff a_0\mid b_0c && \text{(miért?)}\\ &\iff a_0\mid c && \text{(miért?).} \end{aligned}$$

Ezzel kész is a bizonyítás, hiszen a tételben szereplő $\frac{a}{\operatorname{lnko}(a,b)}$ hányados nem más, mint a_0. □

1.8. Tétel. Tekintsük tetszőleges adott a,b,c egész számok esetén az $ax+by=c$ ***kétismeretlenes lineáris diofantoszi egyenletet***.

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

(ii) Tfh. $\operatorname{lnko}(a,b)\neq 0$. 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:

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

Biz.

(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 1.3. 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: $M=\{(x,y)\in\mathbb{Z}^2\colon ax+by=c\}$. Tfh. a és b egyike sem nulla (HF megvizsgálni azt az esetet, amikor az egyikük nulla). Legyen $(x_0,y_0)\in M$ egy tetszőleges rögzített megoldás, azaz $ax_0+by_0=c$. Azt kell bizonyítanunk, hogy $M=\{(x_t,y_t)\colon t\in\mathbb{Z}\}$. A „$\supseteq$” tartalmazást (vagyis azt, hogy (x_t,y_t) minden t-re megoldás), egyszerű behelyettesítéssel lehet ellenőrizni:

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

A „⊆” 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 $x = x_t$. □

szeptember 17.

Kongruenciareláció

1.9. Definíció. Legyen $m \geq 2, a, b \in \mathbb{Z}$. Ha $a - b$ osztható m-mel, akkor azt mondjuk, hogy *a **kongruens** b-**vel** **modulo** m*. Az m számot a kongruencia ***modulusának*** nevezzük.

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

1.10. 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.

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

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

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

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

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

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

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

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

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

(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 $\operatorname{lnko}(a,m) = \operatorname{lnko}(b,m)$.

Biz. Az első három tulajdonság az 1.10. Tétel alapján triviális (visszavezet az egyenlőség reláció reflexivitására, szimmetriájára és tranzitivitására), de be lehet látni őket (és a többi tulajdonságot is) úgy is, hogy 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.

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

(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:

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

Az utolsó kifejezés megint csak osztható m-mel, mert mindkét tagban szerepel egy m-mel osztható tényező.

(5) Ez gyakorlatilag Euklidész lemmája „álruhában”:

$$ca \equiv cb \pmod{m} \iff m \mid ca - cb \iff m \mid c(a-b) \iff \frac{m}{\operatorname{lnko}(m,c)} \,\Big|\, a - b \iff a \equiv b \pmod{\frac{m}{\operatorname{lnko}(m,c)}}.$$

(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 lkkt(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 (az 1.10. 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: $\operatorname{lnko}(a, m) = \operatorname{lnko}(b, m)$.

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 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?). □

Lineáris kongruenciák és multiplikatív inverzek

1.12. 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.

1.13. 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:

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

Biz. 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 az 1.8. 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:

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

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 egy modulo d teljes maradékrendszeren futtatjuk végig, pl. $t = 0, 1, \ldots, d-1$. 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.

□

szeptember 24.

1.14. Definíció. Azt mondjuk, hogy az a, 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.

1.15. 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.

Biz. Ez gyakorlatilag speciális esete az 1.13. Tételnek: amikor a modulo m multiplikatív inverzét keressük, akkor az $ax \equiv 1 \pmod m$ lineáris kongruenciát kell megoldanunk. Az 1.13. Tétel szerint ennek akkor és csak akkor van megoldása, ha $\mathrm{lnko}\,(a, m) \mid 1$, vagyis, ha $a \perp m$. Ha ez teljesül, akkor a megoldások $\mathrm{lnko}\,(a, m)$-féle maradékot adnak m-mel osztva. Mivel $\mathrm{lnko}\,(a, m) = 1$, ez azt jelenti, hogy modulo m egyetlen megoldás van. □

Maradékosztályok

1.16. Definíció. Egy a egész szám modulo m ***maradékosztályán*** az $\overline{a} = \{b \in \mathbb{Z} \colon a \equiv b \pmod m\}$ halmazt értjük.

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

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

1.18. 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.

Biz. 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 1.11. 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. □

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

1.20. 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***).

Biz. 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 az 1.19 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 (4)-es tulajdonsága (1.11. Tétel) 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 $\overline{a} \odot \left(\overline{b} \oplus \overline{c}\right) = \left(\overline{a} \odot \overline{b}\right) \oplus \left(\overline{a} \odot \overline{c}\right)$. Induljunk ki a bal oldalból, és alkalmazzuk az 1.19 Definíciót előbb az összeadásra, majd a szorzásra: $\overline{a} \odot \left(\overline{b} \oplus \overline{c}\right) = \overline{a} \odot \overline{b+c} = \overline{a \cdot (b+c)}$. 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 az 1.19 Definíciót előbb az összeadásra, majd a szorzásra: $\overline{(a \cdot b) + (a \cdot c)} = \overline{a \cdot b} \oplus \overline{a \cdot c} = \left(\overline{a} \odot \overline{b}\right) \oplus \left(\overline{a} \odot \overline{c}\right)$. 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. □

1.21. 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.

1.22. 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.

1.23. 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.

Biz. Ez csak átfogalmazása az 1.15. Tételnek. □

1.24. Megjegyzés. Az 1.11. 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.

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

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

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

Biz. 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 $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$. 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 (1.20. 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 $\overline{a} \in \mathbb{Z}_m \setminus \left\{\overline{0}\right\}$ elemet. Ekkor $m \nmid a$ (miért?), és ebből következik, hogy $a \perp m$ (miért?). Az 1.23. Tétel szerint $\overline{a}$-nak van multiplikatív inverze, és ezzel beláttuk, hogy $\mathbb{Z}_m$ test. □

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

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

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

Biz. 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 $\mathbb{Z}_p \setminus \{0\} = \left\{\overline{1}, \ldots, \overline{p-1}\right\}$ 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 az 1.20. 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. □

október 1.

Az Euler-féle φ függvény

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

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

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

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

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

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

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

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

Ugyanezt felírhatjuk egyetlen szummában is:

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

(Itt $s=0$ esetén nulla db halmazt metszünk; ennek eredménye U. Ez hasonló megállapodás, mint az, hogy az üres összeg értéke 0, az üres szorzaté pedig 1. Gondoljuk meg, hogy miért értelmes az üres uniót $\emptyset$-nak, az üres metszetet pedig U-nak definiálni.) Ki kell tehát számítanunk tetszőleges $1\le i_1<\cdots<i_s\le k$ indexek esetén az $A_{i_1}\cap\cdots\cap A_{i_s}$ metszet elemszámát. Ez a halmaz azokból az $a\in U$ számokból áll, amelyek oszthatóak $p_{i_1},\ldots,p_{i_s}$ mindegyikével, ami azzal ekvivalens, hogy $p_{i_1}\cdot\ldots\cdot p_{i_s}\mid a$ (miért?). Ilyen a számból pedig $\frac{n}{p_{i_1}\cdot\ldots\cdot p_{i_s}}$ van az U halmazban (ugye?). Ezt behelyettesítve a szita-formulába, azt kapjuk, hogy

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

Egy kicsit részletesebben kiírva:

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

Ezt ügyesen szorzattá alakítjuk:

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

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 $\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$ 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.) □

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

1.33. Állítás. 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.

Biz. Tfh. $c_1, \dots, c_{\varphi(m)}$ redukált maradékrendszer modulo m. Az 1.18. Állítás bizonyításához hasonlóan belátható, hogy az $ac_1, \dots, ac_{\varphi(m)}$ számok is páronként inkongruensek modulo m, vagyis $\{\overline{ac_1}, \dots, \overline{ac_{\varphi(m)}}\} \subseteq \mathbb{Z}_m$ egy $\varphi(m)$-elemű halmaz. (Itt most még nem elég a skatulya-elvre hivatkozni, mert a $\mathbb{Z}_m$ halmaznak több $\varphi(m)$-elemű részhalmaza is van.) A redukált maradékrendszer definíciójából következik, hogy $c_i \perp m$ minden $i = 1, \dots, \varphi(m)$ esetén. Mivel $a \perp m$, azt kapjuk, hogy $ac_i \perp m$ minden $i = 1, \dots, \varphi(m)$ esetén (ugye?). Ez azt jelenti, hogy $\{\overline{ac_1}, \dots, \overline{ac_{\varphi(m)}}\} \subseteq \mathbb{Z}_m^*$, és most már jöhet a skatulya-elv: mindkét halmaznak $\varphi(m)$ eleme van, ezért $\{\overline{ac_1}, \dots, \overline{ac_{\varphi(m)}}\} = \mathbb{Z}_m^*$, vagyis $ac_1, \dots, ac_{\varphi(m)}$ valóban redukált maradékrendszer modulo m. □

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

Biz. Legyen $c_1, \dots, c_{\varphi(m)}$ egy tetszőleges redukált maradékrendszer modulo m, azaz $\{\overline{c_1}, \dots, \overline{c_{\varphi(m)}}\} = \mathbb{Z}_m^*$. Ha $a \perp m$, akkor az 1.33. Állítás szerint $ac_1, \dots, ac_{\varphi(m)}$ is redukált maradékrendszer modulo m, azaz $\{\overline{ac_1}, \dots, \overline{ac_{\varphi(m)}}\} = \mathbb{Z}_m^*$. 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. □

1.35. 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 $a^p \equiv a \pmod p$.

Biz. 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?). □

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

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

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

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

□

október 8.

Lineáris kongruenciarendszerek

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

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

1.38. Megjegyzés. Az 1.13. Tétel segítségével a kongruenciarendszerbeli kongruenciákat külön-külön megoldhatjuk (ha van megoldásuk), és így a kongruenciarendszert a következő alakra hozhatjuk:

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

1.39. Tétel. A $(*)$ lineáris kongruenciarendszernek $k = 2$ esetén pontosan akkor van megoldása, ha $\operatorname{lnko}(m_1, m_2) \mid c_1 - c_2$.

Biz. 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 az 1.8. Tétel szerint akkor és csak akkor van megoldása, ha $\operatorname{lnko}(m_1, m_2) \mid c_2 - c_1$, tehát ez a kongruenciarenszer megoldhatóságának feltétele. □

1.40. 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.

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

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

$$\left.\begin{aligned} x&\equiv b\pmod{m_1}\\ &\vdots\\ x&\equiv b\pmod{m_k}\end{aligned}\right\}.$$

Az 1.11. Tételben szereplő (7) tulajdonság alapján ez a kongruenciarendszer ekvivalens az $x\equiv b\pmod{[m_1,\dots,m_k]}$ kongruenciával, amelynek megoldáshalmaza nyilván egyetlen $\bmod[m_1,\dots,m_k]$ maradékosztály. □

1.42. Tétel (kínai maradéktétel). Tegyük fel, hogy az $m_1,\dots,m_k$ modulusok páronként relatív prímek, jelölje a szorzatukat M, továbbá legyen $M_i=\frac{M}{m_i}$ $(i=1,\dots,k)$. Jelölje y_i az $M_iy_i\equiv 1\pmod{m_i}$ segédkongruencia egy megoldását $(i=1,\dots,k)$, és legyen $x_i=M_iy_i$. Ekkor a $(*)$ lineáris kongruenciarendszer megoldása:

$$x\equiv\sum_{i=1}^{k}c_ix_i\pmod{M}.$$

Biz. Mivel az m_i modulusok páronként relatív prímek, $M_i\perp m_i$ teljesül minden $i=1,\dots,k$ esetén (miért?). Így az 1.15. Tétel (vagy ízlés szerint az 1.13. Tétel) alapján minden i-re létezik olyan $y_i\in\mathbb{Z}$, amelyre $M_iy_i\equiv 1\pmod{m_i}$. Legyen $x_i=M_iy_i$, ekkor y_i megválasztása miatt $x_i\equiv 1\pmod{m_i}$; ha pedig $j\neq i$, akkor $x_i\equiv 0\pmod{m_j}$, hiszen $m_j\mid M_i$ (ugye?). Tehát minden $i,j\in\{1,\dots,k\}$ esetén $x_i\equiv\delta_{ij}\pmod{m_j}$; pontosan ez az a tulajdonság, amit az x_i számok konstrukciójával el akartunk érni.* Ellenőrizzük, hogy a $b:=c_1x_1+\dots+c_kx_k$ szám megoldása a kongruenciarendszernek:

$$\begin{aligned} b&=c_1x_1+\dots+c_{j-1}x_{j-1}+c_jx_j+c_{j+1}x_{j+1}+\dots+c_kx_k\\ &\equiv c_1\cdot 0+\dots+c_{j-1}\cdot 0+c_j\cdot 1+c_{j+1}\cdot 0+\dots+c_k\cdot 0\equiv c_j\pmod{m_j}.\end{aligned}$$

Tehát b kielégíti a j-edik kongruenciát minden j-re, azaz megoldása a kongruenciarendszernek. Az 1.41. Tétel szerint a kongruenciarendszer általános megoldása $x\equiv b\pmod{[m_1,\dots,m_k]}$, és épp ezt kellett igazolnunk. □

1.43. Következmény. Ha $m\perp n$, akkor az alábbi ξ leképezés bijektív:

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

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

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

október 15.

2. Számelméleti függvények

Osztók száma, osztók összege

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

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

*Itt δ_{ij} a *Kronecker-szimbólum*, melynek értéke $i=j$ esetén 1, $i\neq j$ esetén pedig 0.

2.2. 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).

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

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

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

Biz. 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. □

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

Biz. Tekintsük az 1.43. Következményben szereplő $\xi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$, $\overline{x} \mapsto (\widehat{x}, \widetilde{x})$ bijekciót. Szorítsuk meg ezt a leképezést a redukált modulo mn maradékosztályokra. Egy a egész szám akkor és csak akkor relatív prím mn-hez, ha a relatív prím m-hez is és n-hez is (miért?) Tehát minden $\overline{a} \in \mathbb{Z}_{mn}$ esetén $\overline{a} \in \mathbb{Z}_{mn}^* \iff \xi(\overline{a}) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ (ugye?). Ezek szerint, ha a ξ leképezést megszorítjuk a $\mathbb{Z}_{mn}^*$ halmazra, akkor értékkészlete pont $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$ lesz. Így tehát ξ megszorítása egy $\mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ bijekciót szolgáltat (miért?), és eszerint a két halmaz elemszáma egyenlő: $\varphi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \cdot \varphi(n)$ (ugye?). □

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

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

Biz. Ezt a tételt már korábban bizonyítottuk (lásd az 1.31. Tételt), most a gyenge multiplikativitás segítségével egy rövidebb bizonyítást adunk. Először tekintsük azt a speciális esetet, amikor n prímhatvány: $n = p^\alpha$. Az $\{1, \dots, p^\alpha\}$ halmaz minden p-edik eleme osztható p-vel (ezek száma $p^{\alpha-1}$), a többiek viszont relatív prímek p^α-hoz (ugye?). Így tehát $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Az általános esetben, ha n prímtényezős felbontása $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, akkor a 2.4. Tételt (és φ imént bizonyított gyenge multiplikativitását) felhasználva kapjuk, hogy $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$. Ha itt minden prímhatványra alkalmazzuk a fenti megfigyelésünket ($\varphi(p_i^{\alpha_i}) = p^{\alpha_i} - p^{\alpha_i - 1}$), akkor megkapjuk bizonyítandó formulát. □

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

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

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

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

Lássunk hozzá:

(i) Ha $u \mid a$ és $v \mid b$, akkor $uv \mid ab$; ez triviális (ugye?).
(ii) Tfh. $d \mid ab$, és legyen $u = \text{lnko}(d, a)$, $v = \frac{d}{\text{lnko}(d,a)}$. Ekkor $u \mid a$ (miért?), $v \mid b$ (miért?) és nyilván $d = uv$ (ugye?).
(iii) Tfh. $u_1, u_2 \mid a$, $v_1, v_2 \mid b$ és $u_1 v_1 = u_2 v_2$. Abból, hogy a és b relatív prím, következik, hogy $u_1 \perp v_2$ (miért?). Az $u_1 v_1 = u_2 v_2$ egyenlőségből következik, hogy $u_1 \mid u_2 v_2$ (ugye?). Alkalmazva az 1.5. Következményt, nyerjük, hogy $u_1 \mid u_2$. Hasonlóan belátható, hogy $u_2 \mid u_1$, tehát $u_1 = u_2$ (miért?). Ezután már az $u_1 v_1 = u_2 v_2$ egyenlőségből egyszerű egyszerűsítéssel kapjuk, hogy $v_1 = v_2$.

□

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

Biz. Az világos, hogy $\tau(1) = \sigma(1) = 1$. Ha $a \perp b$, akkor a 2.7. Lemma szerint létezik bijekció a D_{ab} és $D_a \times D_b$ halmazok között, és így elemszámuk egyenlő: $\tau(ab) = |D_{ab}| = |D_a \times D_b| = |D_a| \cdot |D_b| = \tau(a) \cdot \tau(b)$ (miért?). Ezzel τ gyenge multiplikativitását be is láttuk. A σ függvény vizsgálatához célszerű lesz felsorolni a és b osztóit: legyen $D_a = \{u_1, \dots, u_k\}$, illetve $D_b = \{v_1, \dots, v_\ell\}$ (tehát $\tau(a) = k$ és $\tau(b) = \ell$). A 2.7. Lemma ezzel a jelöléssel azt adja, hogy

$D_{ab} = \{u_i v_j \colon i = 1, \dots, k,\ j = 1, \dots, \ell\}$, és az itt felsorolt $k \cdot \ell$ elem páronként különböző (ez ismét azt mutatja, hogy $\tau(ab) = k \cdot \ell = \tau(a) \cdot \tau(b)$). Ezt felhasználva, ha felírjuk a $\sigma(a) \cdot \sigma(b)$ szorzatot és felbontjuk a zárójeleket, akkor éppen $\sigma(ab)$ fog kijönni:

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

Ugyanez „szumma" jelek nélkül:

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

(Akármelyik felírást is tekintjük, a lényeg az, hogy az utolsó összegben ab minden osztója pontosan egyszer lép fel, és ehhez volt szükségünk a 2.7. Lemmára.) Ezzel beláttuk, hogy σ is gyengén multiplikatív. □

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

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

Biz. Ha $n = p^\alpha$ (prímhatvány), akkor $D_n = \{1, p, \dots, p^\alpha\}$, és így $\tau(n) = |D_n| = \alpha + 1$, illetve $\sigma(n) = 1 + p + \dots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$ (miért?). Mivel a τ és σ függvények gyengén multiplikatívak (2.8. Tétel), a 2.4. Tételt használva már kész is a bizonyítás. □

október 29.

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

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

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

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

2.13. Tétel (Euler tétele). Az n páros szám akkor és csak akkor tökéletes, ha előáll $n = 2^{p-1}(2^p - 1)$ alakban, ahol $2^p - 1$ prímszám (ekkor p is szükségképpen prím a 2.11. Lemma alapján).

Biz. Az „akkor" rész igazolásához tfh. $n = 2^{p-1}(2^p - 1)$, ahol $2^p - 1$ prímszám. Mivel $2^{p-1} \perp 2^p - 1$ (ugye?), alkalmazhatjuk a σ függvény gyenge multiplikativitását: $\sigma(n) = \sigma\left(2^{p-1}\right) \cdot \sigma(2^p - 1)$. Tudjuk, hogy $\sigma\left(2^{p-1}\right) = 2^p - 1$ (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 $\sigma(n) = \left(2^{k+1} - 1\right) \cdot \sigma(t)$. Feltettük, hogy n tökéletes, vagyis $\sigma(n) = 2n = 2^{k+1} \cdot t$. Összevetve az utóbbi két eredményt, azt kapjuk, hogy $\left(2^{k+1} - 1\right) \cdot \sigma(t) = 2^{k+1} \cdot t$. Fejezzük ki innen $\sigma(t)$ értékét:

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

A $\frac{t}{2^{k+1}-1}$ tört egész szám (hiszen nem más, mint $\sigma(t) - t$), jelöljük ezt s-sel. Ekkor $t = \left(2^{k+1} - 1\right) \cdot s$, 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. □

2.14. 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 (2020. október 22.) ismert legnagyobb prímszám is Mersenne-prím: $M_{82\,589\,933}$, ami tízes számrendszerben 24 862 048 számjegyből áll.

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

2.16. Megjegyzés. A 2.11. Lemmához hasonlóan meggondolható, hogy ha 2^k+1 prímszám, akkor k szükségképpen kettőhatvány. Ezért a „kettőhatvány plusz egy" alakú prímeket csak az $F_n = 2^{2^n}+1$ Fermat-számok között érdemes keresni. Fermat azt sejtette, hogy F_n mindig prím. Az első öt Fermat-szám valóban prím:

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

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

Összegzési és megfordítási függvény

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

Biz. 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):

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

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

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

Biz. (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 2.17. Állítás bizonyítása során láttuk, hogy az $\varepsilon_k = \operatorname{cis}\frac{2k\pi}{n}$ komplex számhoz tartozó legkisebb pozitív jó kitevő $d := \frac{n}{\operatorname{lnko}(n,k)}$, vagyis ε_k primitív d-edik egységgyök (azaz $\varepsilon_k \in P_d$). Nyilván $d \mid n$ (miért?), tehát azt kaptuk, hogy minden n-edik egységgyök primitív d-edik egységgyök n valamely d osztójára. Fordítva, ha z primitív d-edik egységgyök n valamely d osztójára, akkor $z^n = \left(z^d\right)^{n/d} = 1^{n/d} = 1$ (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 2.17. Állításból tudjuk, hogy $|P_d| = \varphi(d)$, tehát a fenti egyenlőség igazolja, hogy $n = \sum_{d\mid n}\varphi(d)$. □

Biz. (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. □

november 5.

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

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

2.20. Megjegyzés. A 2.18. Tétel szerint az Euler-féle φ függvény összegzési függvénye az identikus függvény: $\varphi \to \mathrm{id}$. Másképpen fogalmazva: az identikus függvény megfordítási függvénye az Euler-féle φ függvény. Ha nem ismernénk a 2.18. Tételt, akkor nem lenne könnyű feladat meghatározni az identikus függvény megfordítási függvényét. A következőkben bevezetünk egy kétváltozós műveletet a számelméleti függvények halmazán, aminek segítségével módszert (képletet) tudunk adni egy tetszőleges számelméleti függvény megfordítási függvényének kiszámítására.

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

$$(f*g)(n)=\sum_{d|n} f(d)\cdot g\left(\frac{n}{d}\right)=\sum_{ab=n} f(a)\,g(b)\,.$$

2.22. Definíció. A konvolúció tulajdonságainak vizsgálatához szükségünk lesz az alábbi három – a korábban tárgyaltakhoz képest nagyon egyszerű – számelméleti függvényre:

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

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

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

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

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

$$(f*\delta)(n)=\sum_{d|n} f(d)\cdot\delta\left(\frac{n}{d}\right)=f(n)\cdot\delta(1)=f(n)\,,$$

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

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

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

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

A 2.7. Lemma szerint ab minden d osztója egyértelműen felírható $d=uv$ alakban, ahol $u\mid a$ és $v\mid b$. Így a fenti összeget a következőképpen alakíthatjuk át, felhasználva f és g gyenge multiplikativitását:

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

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

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

□

2.25. Tétel. Gyengén multiplikatív számelméleti függvény összegzési függvénye is gyengén multiplikatív.

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

$$F(n)=\sum_{d|n} f(d)\cdot 1=\sum_{d|n} f(d)\cdot\mathbf{1}\left(\frac{n}{d}\right)$$

minden n természetes számra, azaz $F=f*\mathbf{1}$. Ha f gyengén multiplikatív, akkor a 2.24. Tétel szerint $f*\mathbf{1}$ is gyengén multiplikatív (miért?). □

2.26. Tétel. A tanult nevezetes számelméleti függvények között fennállnak a következő összefüggések: $\delta\to\mathbf{1}\to\tau$ és $\varphi\to\mathrm{id}\to\sigma$.

Biz. Írjuk fel a bizonyítandó összegzéseket:

$$\sum_{d|n}\delta(d)=\mathbf{1}(n)\,,\qquad\sum_{d|n}\mathbf{1}(d)=\tau(n)\,,\qquad\sum_{d|n}\varphi(d)=\mathrm{id}(n)\,,\qquad\sum_{d|n}\mathrm{id}(d)=\sigma(n)\,.$$

A harmadik állítás kivételével mindegyik triviális (ugye?). A harmadik állítás pedig nem más, mint a 2.18. Tétel. Ezt már kétféleképpen is bizonyítottuk, de most egy harmadik, egyszerűbb bizonyítást is adunk, φ gyenge multiplikativitásának felhasználásával. Legyen $\Phi(n)=\sum_{d|n}\varphi(d)$; ezzel a jelöléssel a bizonyítandó állítás az, hogy $\Phi(n)=n$ minden $n\in\mathbb{N}$ esetén, azaz Φ az identikus függvény (az $\mathbb{N}$ halmazon). A 2.25. Tétel szerint φ gyenge multiplikativitásából következik Φ gyenge multiplikativitása. Így a 2.4. Tétel szerint a Φ függvényt egyértelműen meghatározzák a prímhatvány helyeken

felvett értékei, ezért elég prímhatványokra ellenőrizni, hogy $\Phi(n) = n$. Legyen tehát $n = p^\alpha$ (p prím, $\alpha \in \mathbb{N}$), és számítsuk ki a $\sum_{d|n} \varphi(d)$ összeget:

$$\Phi(p^\alpha) = \sum_{d|p^\alpha} \varphi(d) = \sum_{i=0}^{\alpha} \varphi\left(p^i\right) = \varphi(1) + \varphi(p) + \varphi\left(p^2\right) + \cdots + \varphi\left(p^{\alpha-1}\right) + \varphi(p^\alpha)$$
$$= 1 + (p-1) + \left(p^2 - p\right) + \cdots + \left(p^{\alpha-2} - p^{\alpha-1}\right) + \left(p^\alpha - p^{\alpha-1}\right) = p^\alpha.$$

(Minden lépéshez tessék odaképzelni, hogy „miért?”.) □

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

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

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

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

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

Biz. A 2.25. Tételt szeretnénk használni, ezért először azt ellenőrizzük, hogy μ gyengén multiplikatív. A definícióból $\mu(1) = 1$, hiszen 1 nulla darab prím szorzata (üres szorzat). Tfh. $a \perp b$ és vizsgáljuk $\mu(ab)$ értékét. Ha a nem négyzetmentes, akkor ab sem az, (ugye?), tehát $\mu(a) = 0 \implies \mu(ab) = 0$, ekkor tehát teljesül, hogy $\mu(ab) = \mu(a) \cdot \mu(b)$. A $\mu(b) = 0$ eset hasonló, tehát feltehetjük, hogy a és b is négyzetmentes: $a = p_1 \cdot \ldots \cdot p_k$ (ahol $p_1, \ldots, p_k$ páronként különböző prímszámok) és $b = q_1 \cdot \ldots \cdot q_\ell$ (ahol $q_1, \ldots, q_\ell$ páronként különböző prímszámok). Az $a \perp b$ feltevésből következik, hogy a $\{p_1, \ldots, p_k\}$ és $\{q_1, \ldots, q_\ell\}$ halmazok diszjunktak, így az $ab = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_\ell$ felbontásban $k + \ell$ különböző prímszám szerepel. Ebből már ki tudjuk számítani $\mu(ab)$ értékét: $\mu(ab) = (-1)^{k+\ell} = (-1)^k \cdot (-1)^\ell = \mu(a) \cdot \mu(b)$ (ugye?). Ezzel beláttuk, hogy μ gyengén multiplikatív.

Jelöje μ összegzési függvényét M (nagy „mű” betű). A 2.25. Tétel szerint M gyengén multiplikatív. Tudjuk, hogy δ is gyengén multiplikatív, ezért az $M(n) = \delta(n)$ egyenlőséget elegendő prímhatványokra ellenőrizni (lásd a 2.4. Tételt). Legyen tehát $n = p^\alpha$; ekkor

$$M(n) = \sum_{d|n} \mu(d) = \sum_{i=0}^{\alpha} \mu\left(p^i\right) = \mu(1) + \mu(p) + \mu\left(p^2\right) + \cdots + \mu(p^\alpha) = 1 + (-1) + 0 + \cdots + 0 = 0 = \delta(n).$$

□

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

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

Biz. Azt kell igazolnunk, hogy tetszőleges f és F számelméleti függvények esetén

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

Az „$\implies$” irányhoz tfh. $F = f * \mathbf{1}$, és „konvolváljuk be” mindkét oldalt μ-vel: $F * \mu = (f * \mathbf{1}) * \mu$. A jobb oldalt először zárójelezzük át, felhasználva a konvolúció asszociativitását (2.23. Tétel): $(f * \mathbf{1}) * \mu = f * (\mathbf{1} * \mu)$. Most használjuk a 2.30. Tételt, majd azt, hogy a konvolúciónak δ az egységeleme (2.23. Tétel): $f * (\mathbf{1} * \mu) = f * \delta = f$. Ezzel beláttuk, hogy $F = f * \mathbf{1} \implies f = F * \mu$.

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

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

Biz. A Möbius-féle megfordítási képlet szerint F megfordítási függvénye $F * \mu$. A 2.30. Tétel bizonyítása során láttuk, hogy μ gyengén multiplikatív. Ha még F is gyengén multiplikatív, akkor a 2.24. Tétel alapján $F * \mu$ is gyengén multiplikatív. □

3. Polinomok

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lineáris „diofantoszi" egyenlet test feletti polinomgyűrűben

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

$$\exists u, v \in T[x]: \quad fu + gv = \operatorname{lnko}(f, g). \tag{3.2}$$

Biz. A bizonyítás nagyon hasonló az 1.3. Tétel bizonyításához. Ha $f = 0$ vagy $g = 0$, akkor az állítás triviális (ugye?). Tegyük fel tehát, hogy $f, g \neq 0$, és tekintsük az összes $fu + gv$ alakú polinomok I halmazát:

$$I = \{fu + gv : u, v \in T[x]\}.$$

Nyilván $0 \in I$, de vannak I-ben nemzéró polinomok is (például f és g). Legyen d az $I \setminus \{0\}$ halmaz (egyik) legkisebb fokszámú eleme. Mivel $d \in I$, vannak olyan $u_0, v_0 \in T[x]$ polinomok, amelyekre $fu_0 + gv_0 = d$. Megmutatjuk, hogy $d \sim \operatorname{lnko}(f, g)$. A legnagyobb közös osztó definíciójának második pontja nyilván teljesül d-re: ha $k \mid f$ és $k \mid g$, akkor $k \mid fu_0 + gv_0 = d$ (ugye?). A definíció első pontjához igazolnunk kell, hogy $d \mid f$. Tegyük fel, hogy $d \nmid f$; ekkor ha f-et maradékosan osztjuk d-vel, a keletkező r maradék nem lesz nulla: $f = qd + r$, ahol $\deg r < \deg d$ és $r \neq 0$. Az r polinom is eleme az I halmaznak, hiszen $r = f - qd = f - q(fu_0 + gv_0) = f(1 - qu_0) + g(-qv_0)$. Mivel r nem nulla, és foka szigorúan kisebb d fokánál, ellentmondást kaptunk, hiszen d minimális fokszámú eleme volt az $I \setminus \{0\}$ halmaznak. Ez az ellentmondás azt mutatja, hogy $d \mid f$, és hasonlóan bizonyítható a $d \mid g$ oszthatóság is. Ezzel beláttuk, hogy d eleget tesz a legnagyobb közös osztó definíciójának, azaz $d \sim \operatorname{lnko}(f, g)$; másrészt $d = fu_0 + gv_0$, és ez igazolja a tétel állítását. □

3.12. Megjegyzés. A fenti bizonyítás az 1.3. Tétel „nyuszibogyós" bizonyításának gondolatmenetét követte. Itt is lehet egy másik bizonyítást adni az euklideszi algoritmus segítségével. Ezt nem részletezzük, de a számolásokban használni fogjuk.

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

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

Biz. A bizonyítás nagyon hasonló az 1.5. Tétel bizonyításához (HF). □

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

$$f \mid gh \iff \frac{f}{\operatorname{lnko}(f, g)} \mid h. \tag{3.3}$$

Biz. A bizonyítás nagyon hasonló az 1.7. Következmény bizonyításához (HF). □

3.16. Tétel. Legyen T egy test és $f, g, h \in T[x]$ (nemnulla) polinomok. Ekkor az $fu + gv = h$ kétismeretlenes lineáris „diofantoszi" egyenlet akkor és csak akkor oldható meg az ismeretlen $u, v \in T[x]$ polinomokra nézve, ha $\operatorname{lnko}(f, g) \mid h$.

Biz. A bizonyítás nagyon hasonló az 1.8. Tétel (első állításának) bizonyításához (HF). □

Kongruenciareláció, maradékosztályok

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

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

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

Biz. A bizonyítás nagyon hasonló az 1.10. Tétel bizonyításához (HF), a test feletti polinomok maradékos osztásáról szóló tételt (3.8. Tétel) használva. □

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

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

Biz. A bizonyítás nagyon hasonló az 1.11. Tétel megfelelő részeinek bizonyításához; itt is ugyanúgy lehet visszavezetni a kongruencia tulajdonságait az oszthatóság tulajdonságaira, mint az egész számok körében (HF). □

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

Biz. A bizonyítás nagyon hasonló az 1.13. Tétel (első állításának) bizonyításához; itt is ugyanúgy lehet visszavezetni a lineáris kongruenciát kétismeretlenes lineáris „diofantoszi" egyenletre, mint az egész számok körében (HF). □

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

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

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

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

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

Biz. A bizonyítás nagyon hasonló az 1.20. Tétel bizonyításához; itt is a kongruencia tulajdonságai (3.20. Tétel) garantálják, hogy a maradékosztályok összege és szorzata jóldefiniált, és itt is ugyanúgy lehet visszavezetni a műveleti tulajdonságokat a $T[x]$ gyűrűbeli tulajdonságokra, mint ahogy a $\mathbb{Z}_m$ halmazon definiált műveletek tulajdonságait visszavezettük az egész számok megfelelő műveleti tulajdonságaira (HF). A tétel utolsó állítása annak a ténynek az analogonja, hogy $\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}$, és azon múlik, hogy ha egy tetszőleges $f \in T[x]$ polinomot maradékosan osztunk az n-edfokú m polinommmal, akkor a maradék mindig egy legfeljebb $(n-1)$-edfokú polinom lesz, továbbá a maradék egyértelműen meghatározott. Tehát minden $f \in T[x]$ polinomhoz létezik egy és csak egy $f_1 \in T[x]$ polinom, amelyre $f \equiv f_1 \pmod m$ és $\deg f_1 \leq n-1$. □

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

Biz. A bizonyítás nagyon hasonló az 1.15. Tétel bizonyításához; itt is a lineáris kongruencia megoldhatósági kritériumát (3.21. Tétel) kell alkalmazni (HF). □

Irreducibilis polinomok, irreducibilis faktorizáció (jórészt ismétlés)

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

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

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

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

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

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

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

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

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

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

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

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

november 19.

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

Biz. A bizonyítás nagyon hasonló az 1.26. Következmény bizonyításához; csak a „degenerált" eseteket külön meg kell nézni.

- Ha $m = 0$, akkor m nem irreducibilis, és $T[x]/(m)$ valóban nem test, mert minden $f \in T[x]$ polinomra $\overline{f} = \{f\}$ (lásd a 3.18. Megjegyzést), tehát $T[x]/(m)$ lényegében ugyanaz, mint $T[x]$ (szaknyelven: a $T[x]/(m)$ és $T[x]$ gyűrűk *izomorfak* egymással), márpedig $T[x]$ nem test (miért?).
- Ha $m \sim 1$, akkor m megint csak nem irreducibilis, és $T[x]/(m)$ valóban nem test (miért?).
- Ha $\deg m \geq 1$ és m nem irreducibilis, akkor van nemtriviális felbontása: $m = fg$, ahol $1 \leq \deg f, \deg g < \deg m$ (lásd a 3.28. Állítást). Ekkor $\overline{f}, \overline{g} \neq \overline{0}$, de $\overline{f} \cdot \overline{g} = \overline{0}$, tehát $T[x]/(m)$ nem test, sőt, még csak nem is integritástartomány (miért?).
- Ha m irreducibilis, akkor $T[x]/(m)$ kommutatív egységelemes gyűrű, amelynek legalább két eleme van (miért?), tehát ahhoz, hogy belássuk, hogy $T[x]/(m)$ test, elég ellenőrizni, hogy minden nemnulla elemének van multiplikatív inverze. Legyen tehát $\overline{0} \neq \overline{f} \in T[x]/(m)$, és keressük $\overline{f}$ multiplikatív inverzét. Mivel m irreducibilis és $m \nmid f$, ezért $f \perp m$ (miért?). A 3.26. Tétel szerint ekkor $\overline{f}$-nak valóban létezik multiplikatív inverze.

□

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

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

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

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

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

Irreducibilis polinomok a racionális számtest felett

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

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

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

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

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

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

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

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

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

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

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

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

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

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

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

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

akkor f irreducibilis a racionális számok teste felett.

Biz. Tfh. az f polinom együtthatóira teljesülnek a fenti oszthatósági feltételek, de ennek ellenére f nem irreducibilis $\mathbb{Q}$ felett. Ekkor léteznek olyan g_1, h_1 *racionális együtthatós* polinomok, amelyekre $f = g_1 h_1$ és $0 < \deg g_1, \deg h_1 < n$ (miért?). A 3.41. Tétel szerint vannak olyan g, h *egész együtthatós* polinomok, amelyekre $f = gh$ és $0 < \deg g, \deg h < n$. Legyen $g = b_k x^k + \cdots + b_1 x + b_0$ és $h = c_\ell x^\ell + \cdots + c_1 x + c_0$, és írjuk fel sorra az $f = gh$ egyenlőség mindkét oldalának együtthatóit. A konstans tag: $a_0 = b_0 c_0$ (ugye?), és tudjuk, hogy ez osztható p-vel, így $p \mid b_0$ vagy $p \mid c_0$ (miért?). Ha b_0 is és c_0 is osztható lenne p-vel, akkor $p^2 \mid a_0$, ami ellentmond a $p \| a_0$ feltevésnek (ugye?). Tehát b_0 és c_0 közül egyik osztható p-vel, a másik nem. Csak a $p \mid b_0, \;\; p \nmid c_0$ esetet vizsgáljuk; a másik eset hasonló (HF). Az $f = gh$ egyenlőségben az elsőfokú tagok együtthatói azt adják, hogy $a_1 = b_0 c_1 + b_1 c_0$. Mivel $p \mid a_1$ és $p \mid b_0$, ebből következik, hogy $p \mid b_1 c_0$ (ugye?). Feltettük, hogy $p \nmid c_0$, ezért $p \mid b_1$ (miért?). Tehát már tudjuk, hogy p osztja a g polinomban a b_0 és b_1 együtthatókat. Nézzük most a másodfokú tagokat az $f = gh$ egyenlőségben: $a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$. Itt $b_2 c_0$ kivételével minden tagról tudjuk már, hogy osztható p-vel, ezért $p \mid b_2 c_0$ (ugye?). Ismét felhasználva, hogy $p \nmid c_0$, azt kapjuk, hogy $p \mid b_2$ (miért?). Most már tudjuk, hogy $p \mid b_0, b_1, b_2$, és ebből a harmadfokú tagokat vizsgálva levezethetjük, hogy $p \mid b_3$:

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

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

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

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

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

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

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

3.47. Tétel (muirétirk isátilidicuderri eléf-nietsnesiE–nnamenöhcS). Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \| a_n, p \mid a_{n-1}, \ldots, p \mid a_1, p \nmid a_0$, akkor f irreducibilis a racionális számok teste felett.

Elemi törtekre bontás

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

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

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

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

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

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

alakú racionális tört összegeként.

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

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

alakú racionális tört összegeként.

Szimmetrikus polinomok

3.53. Tétel (ism.). Legyenek az n-edfokú $f=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{C}[x]$ főpolinom komplex gyökei $\alpha_1,\dots,\alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:

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

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

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

3.55. Definíció. Az $f\in\mathbb{C}[x]$ főpolinom ***diszkriminánsa***:

$$\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2,$$

3.56. Definíció. Adott T test feletti ***n-határozatlanú monomnak*** nevezzük az $ax_1^{k_1}\cdots x_n^{k_n}$ alakú formális kifejezéseket, ahol $0\neq a\in T$ és $k_1,\dots,k_n\in\mathbb{N}_0$. Az ilyen monomok véges összegeit pedig T feletti ***n-határozatlanú polinomoknak*** nevezzük.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Algebrai és transzcendens számok

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

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

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

3.67. Tétel. Létezik transzcendens szám.

3.68. Megjegyzés. A fenti tételt a megfelelő halmazelméleti ismeretek birtokában nem nehéz bebizonyítani: komplex számból „több" van, mint algebrai számból. (Az algebrai számok halmaza megszámlálhatóan végtelen, $\mathbb{C}$ viszont kontinuum számosságú.) Ez egy ún. *nemkonstruktív egzisztenciabizonyítás*: igazolja, hogy van transzcendens szám (sőt, a komplex (vagy valós) számok „túlnyomó többsége" transzcendens), de nem mutat egyetlen példát sem transzcendens számra. Nem könnyű feladat egy konkrét számról belátni, hogy transzcendens. Az ilyen bizonyítások általában azt használják fel, hogy algebrai számokat nem lehet nagyon jól közelíteni racionális számokkal (lásd a 3.73. Tételt). Ez a *diofantoszi approximáció* témaköre: adott α valós számhoz szeretnénk olyan $\frac{p}{q}$ közelítő törtet találni ($p, q \in \mathbb{Z}, q > 0, p \perp q$), amelyre $\left|\alpha - \frac{p}{q}\right|$ kicsi, és q nem túl nagy.

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

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

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

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

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

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

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

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

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

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

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

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

3.77. Következmény. A gyökmennyiségek algebrai számok.

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

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

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

november 12.

4. Relációk

Ekvivalenciák és osztályozások

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

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

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

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

(2) $\forall a,b \in A : a\rho b \implies b\rho a$ (szimmetria);

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

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

4.4. Példa. Az egész számok halmazán a modulo m kongruencia ekvivalenciareláció (lásd az 1.11. Tétel első három pontját). Ahogy az egész számokat a modulo m kongruencia alapján maradékosztályokba tudjuk sorolni, úgy tetszőleges $\rho \subseteq A \times A$ ekvivalenciareláció is meghatároz egy osztályozást az A halmazon. A következőkben definiáljuk a maradékosztályok mintájára az ekvivalenciaosztályokat, és megmutatjuk, hogy ezek valóban „osztályozzák" az A halmaz elemeit.

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

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

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

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

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

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

Ez egy ekvivalenciareláció, de ezt elég nehézkes volna ellenőrizni (főleg a tranzitivitást). Ha felrajzoljuk a reláció gráfját (a gráf csúcsai az A halmaz elemei, és minden $(v,w) \in \rho$ csúcspárnál berajzolunk egy $v \to w$ nyilat), akkor azt látjuk, hogy három összefüggő komponens van, és a komponensek mind irányított teljes gráfok (egy komponensen belül „mindenki mindenkivel, oda-vissza"). Így már a tranzitivitás is világos. Be fogjuk bizonyítani, hogy minden ekvivalenciareláció esetén így néznek ki az összefüggő komponensek (gondoljuk majd meg, hogy a 4.11. Tétel (i) állításának ez a szemléletes jelentése). Az összefüggő komponensek éppen az ekvivalenciaosztályok:

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

A faktorhalmaz tehát így fest:

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

(Először a 4.5. Definíciót betű szerint alkalmazva írtuk fel a faktorhalmazt, azután úgy, hogy az ismétlődő elemekből csak egyet tartottunk meg. Célszerű mindig kihagyni az ismétlődéseket, mert így jobban áttekinthető a faktorhalmaz.)

4.7. Példa. Ha ρ a modulo m kongruencia az egész számok halmazán (azaz $a\rho b \iff a \equiv b \pmod m$), akkor az ekvivalenciaosztályok éppen a maradékosztályok (lásd az 1.16. Definíciót), a faktorhalmaz pedig $\mathbb{Z}_m$ lesz: $\mathbb{Z}/\rho = \big\{\overline{0},\overline{1},\dots,\overline{m-1}\big\} = \mathbb{Z}_m$. A maradékosztályok esetén világos, hogy két egész szám akkor és csak akkor esik ugyanabba a maradékosztályba, ha relációban vannak egymással (azaz kongruensek modulo m). Megmutatjuk, hogy ez minden ekvivalenciarelációra érvényes (lásd a 4.8. Állítást), majd ennek segítségével igazoljuk, hogy az ekvivalenciaosztályok páronként diszjunktak (lásd a 4.9. Tételt). A maradékosztályoknál ez triviális, mert egy szám nem adhat kétféle maradékot m-mel osztva. Ugyan a kongruenciás-maradékosztályos példa segít elképzelni ezeket az elvont fogalmakat, az alábbi bizonyításoknál nagyon kell figyelni arra, hogy ne használjunk semmit pusztán a szemléletünk alapján: csak arra támaszkodhatunk, amit feltettünk, vagyis arra, hogy ρ reflexív, szimmetrikus és tranzitív.

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

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

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

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

Biz. Kontrapozícióval bizonyítunk: azt mutatjuk meg, hogy $\overline{a} \cap \overline{b} \neq \emptyset \implies \overline{a} = \overline{b}$. Tegyük fel tehát, hogy $\overline{a} \cap \overline{b} \neq \emptyset$, és legyen $c \in \overline{a} \cap \overline{b}$. Ekkor $a\rho c$ és $b\rho c$ (miért?), és a szimmetriát használva $c\rho b$ is teljesül. A tranzitivitásnak köszönhetően $a\rho c$ és $c\rho b$ maga után vonja, hogy $a\rho b$ (ugye?). Ebből pedig a 4.8. Állítás alapján következik, hogy $\overline{a} = \overline{b}$. □

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

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

(b) $\forall B_1, B_2 \in \mathcal{C} : B_1 \neq B_2 \implies B_1 \cap B_2 = \emptyset$;

(c) $\bigcup_{B \in \mathcal{C}} B = A$.

4.11. Tétel. Legyen A egy nemüres halmaz.

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

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

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

formulával definiált ρ reláció ekvivalenciareláció az A halmazon.

Biz. Az első állítás bizonyításához tfh. ρ ekvivalenciareláció az A halmazon. Az osztályozás definíciójában szereplő (b) tulajdonság következik a 4.9. Tételből. Az (a) és (c) tulajdonságok kulcsa pedig az, hogy a reflexivitás miatt $a \in \overline{a}$ teljesül minden $a \in A$ esetén (ugye?). Ebből következik, hogy $\overline{a}$ nem üres (hiszen a biztosan eleme), és az is, hogy az ekvivalenciaosztályok együtt lefedik az a halmazt (hiszen az a elemet lefedi az $\overline{a}$ osztály).

A második állítás bizonyításához tfh. $\mathcal{C}$ osztályozás az A halmazon. Mivel az osztályok lefedik az alaphalmazt ((c) tulajdonság), minden elem benne van legalább egy osztályban. Mivel az osztályok páronként diszjunktak ((b) tulajdonság), minden elem lefeljebb egy osztályban lehet benne. Tehát az alaphalmaz minden eleme pontosan egy osztályban van benne. Legyen $f\colon A \to \mathcal{C}$ az a leképezés amelyik minden $a \in A$ elemhez hozzárendeli azt az egyetlen $B \in \mathcal{C}$ osztályt, amelyre $a \in B$. Az f leképezés magja éppen a tétel kimondásában szereplő ρ reláció (miért?), és így a 4.14. Állítás szerint ρ ekvivalenciareláció. □

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

4.13. Megjegyzés. Ha egy „szép szabályos” ekvivalenciarelációról van szó, akkor meg lehet mondani, hogy milyen szabály szerint soroljuk ekvivalenciaosztályokba az elemeket (a 4.7. Példában például az m-mel adott osztási maradékaik szerint). A következő fogalom ezt a jelenséget ragadja meg absztrakt formában: minden elemhez hozzárendelünk „valamit” (pl. a modulo m maradékát), és két elemet akkor teszünk egy osztályba (vagyis akkor állnak relációban egymással), ha ez a „valamijük” megegyezik.

4.14. Állítás. Tetszőleges $f\colon A \to B$ leképezés esetén a

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

reláció ekvivalenciareláció az A halmazon, amelynek neve az f leképezés ***magja***.

Biz. A mag tulajdonságai rendre visszavezethetőek az egyenlőség tulajdonságaira:

(1) $\ker f$ reflexív, mert $\forall a \in A : af = af$;

(2) $\ker f$ szimmetrikus, mert $\forall a_1, a_2 \in A : a_1 f = a_2 f \implies a_2 f = a_1 f$;

(3) $\ker f$ tranzitív, mert $\forall a_1, a_2, a_3 \in A : (a_1 f = a_2 f \text{ és } a_2 f = a_3 f) \implies a_1 f = a_3 f$.

□

4.15. Példa. A 4.6. Példában szereplő ρ reláció elég szabálytalannak tűnik; elsőre talán nem látszik, hogy van-e olyan leképezés, aminek éppen ez a reláció a magja. Ha belegondolunk a mag (és az ekvivalenciaosztály) definíciójába, akkor észrevehetjük, hogy nagyon sok ilyen leképezés van: minden olyan $f\colon A \to B$ leképezés jó (bármilyen legalább háromelemű B halmazzal), amire $xf = yf$ akkor és csak akkor áll fenn, ha x és y ugyanabba az osztályba esnek. Íme egy ilyen lelépezés:

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

Ha a „szarvánál ragadjuk meg a bikát”, akkor nem is kell gondolkoznunk rajta, hogy miket rendeljünk az A halmaz elemeihez: legyen $B = A/\rho$, és rendeljük minden elemhez a saját ekvivalenciaosztályát. Ezt nevezzük *természetes leképezésnek*:

$$\nu\colon A \to A/\rho, \quad x \mapsto \overline{x}.$$

Gondoljuk meg, hogy a 4.8. Állítás épp azt jelenti, hogy tetszőleges A halmaz és $\rho \subseteq A \times A$ ekvivalenciareláció esetén az így definiált ν leképezés magja éppen ρ. Tehát a 4.14. Állításban szereplő példa „univerzális”: minden ekvivalenciareláció egy alkalmas leképezés magja.

Részbenrendezések

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

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

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

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

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

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

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

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

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

4.19. Példa. Íme néhány nevezetes (részben)rendezett halmaz:

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

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

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

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

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

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

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

(Ez szemléletesen azt jelenti, hogy $a \leq b$ akkor és csak akkor teljesül, ha a és b összeköthető egy véges hosszúságú, fedésekből álló lánccal.) A „$\Longleftarrow$” irány igazolásához tfh. $a = c_0 \prec c_1 \prec \cdots \prec c_n = b$. Ekkor $a = c_0 < c_1 < \cdots < c_n = b$ (miért?), és így a tranzitivitás miatt $a \leq b$ (ugye?). A „$\Longrightarrow$” irány igazolásához tfh. $a \leq b$. Ha $a = b$, akkor készen vagyunk ($n = 0$ és $c_0 = a = b$); ha $a \prec b$, akkor is készen vagyunk ($n = 1$ és $c_0 = a, c_1 = b$). Ellenkező esetben létezik a és b „között” legalább egy d elem: $a < d < b$. Ha $a \prec d \prec b$, akkor készen vagyunk ($n = 2$ és $c_0 = a, c_1 = d, c_2 = b$). Ellenkező esetben a és d közé, vagy d és b közé (esetleg mindkét helyre) tudunk újabb elemeket illeszteni, és így tovább. Mivel A véges, ez nem mehet végtelen sokáig: előbb-utóbb olyan láncot kapunk, amelynek szomszédos „láncszemei” közé már nem lehet újabb elemeket illeszteni, vagyis a szomszédos elemek fedik egymást. (Ezt a gondolatmenetet az $[a, b] = \{x \in A\colon a \leq x \leq b\}$ intervallum elemszáma szerinti teljes indukcióval lehet precízzé tenni.) □

4.21. Definíció. Egy $(A; \leq)$ részbenrendezett halmaz ***Hasse-diagramján*** egy olyan ábrát értünk, amelynél A elemeit (síkbeli) pontokkal ábrázoljuk oly módon, hogy $a < b$ esetén a b-nek megfelelő pont „följebb” van, mint az a-nak megfelelő pont, és e két pontot akkor és csak akkor kötjük össze, ha b fedi a-t. Az előző tétel szerint véges részbenrendezett

halmazokat „érdemes” Hasse-diagrammal ábrázolni. Néha végtelen részbenrendezett halmazokról is jó képet ad a Hasse-diagram (például a $(\mathbb{Z};\leq)$ és $(\mathbb{N}_0;|)$ részbenrendezett halmazok esetén), de például az $(\mathbb{R};\leq)$ rendezett halmaz Hasse-diagramját bajos volna lerajzolni, mert itt a fedési reláció üres.

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

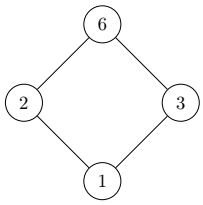
$$\leq = \big\{(1,1),(1,2),(1,3),(1,6),(2,2),(2,3),(2,6),(3,3),(3,6),(6,6)\big\}, \quad \prec = \big\{(1,2),(2,3),(3,6)\big\}.$$

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

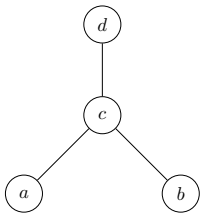
4.23. Példa. Tekintsük az $(\{1,2,3,6\};|)$ részbenrendezett halmazt. Ebben az esetben a részbenrendezési reláció és a fedési reláció így fest:

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

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



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



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

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

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

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

4.26. Példa. A 4.22. Példában szereplő $(\{1,2,3,6\};\leq)$ részbenrendezett halmazban 1 minimális és legkisebb elem, 6 maximális és legnagyobb elem. Ugyanez érvényes a 4.23. Példában szereplő $(\{1,2,3,6\};|)$ részbenrendezett halmazra. A 4.24. Példában szereplő $(\{a,b,c,d\};\leq)$ részbenrendezett halmazban a és b minimális elemek, legkisebb elem nincs, d maximális és legnagyobb elem. A $(\mathbb{Z};\leq)$ részbenrendezett halmazban nincs se minimális, se legkisebb, se maximális, se legnagyobb elem. Az $(\mathbb{N}_0;\leq)$ részbenrendezett halmazban 0 minimális és legkisebb elem, és nincs se maximális, se legnagyobb elem. Az $(\mathbb{N}_0;|)$ részbenrendezett halmazban 1 minimális és legkisebb elem, 0 maximális és legnagyobb elem.

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

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

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

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

Hasonló érvényes a legnagyobb elemre is.

Biz.

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

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

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

□

4.28. Megjegyzés. Ha a és b pozitív egészek, akkor a és b pozitív közös osztóinak halmaza $D_a\cap D_b$. Ezen a halmazon kétféle részbenrendezést is értelmezhetünk: a nagyság szerinti rendezést és az oszthatóság szerinti rendezést. A legnagyobb közös osztó általános és középiskolában használatos definíciója szerint $\operatorname{lnko}(a,b)$ nem más, mint a $(D_a\cap D_b;\leq)$ rendezett halmaz legnagyobb eleme. Az általunk használt 1.1. Definíció szerint $\operatorname{lnko}(a,b)$ nem más, mint a $(D_a\cap D_b;|)$ részbenrendezett halmaz legnagyobb eleme. (Például $a=18$, $b=30$ esetén $D_{18}\cap D_{30}=D_{\operatorname{lnko}(18,30)}=D_6=\{1,2,3,6\}$. A $(D_a\cap D_b;\leq)$ rendezett halmaz Hasse-diagramját a 4.22. Példa, a $(D_a\cap D_b;|)$ részbenrendezett halmaz Hasse-diagramját pedig a 4.23. Példa mutatja ebben a konkrét esetben.) Ha a és b is pozitív (sőt, még akkor is, ha egyikük nulla), akkor a két definíció ekvivalens egymással: ha d a legnagyobb eleme a $(D_a\cap D_b;|)$ részbenrendezett halmaznak, akkor minden $k\in D_a\cap D_b$ esetén $k\mid d$, és így $k\leq d$ is teljesül, tehát d legnagyobb eleme a $(D_a\cap D_b;\leq)$ rendezett halmaznak is (ugye?). Ha azonban $a=b=0$, akkor a $(D_a\cap D_b;\leq)$ rendezett halmaznak nincs legnagyobb eleme (miért?), míg a $(D_a\cap D_b;|)$ részbenrendezett halmaz legnagyobb eleme 0 (ugye?). Tehát $a=b=0$ esetén az „iskolás” definíció nem használható, az „egyetemi” definíció viszont igen. Egy másik előnye az 1.1. Definíciónak, hogy általánosítható az egész számok gyűrűjéről más gyűrűkre, ahol nincs is „nagyság szerinti” rendezés (más kérdés, hogy legnagyobb közös osztók nem minden gyűrűben léteznek).

november 26.

5. Permutációk

Permutációk szorzása, ciklusfelbontás

5.1. Definíció. ***Permutációnak*** nevezzük egy nemüres (véges) halmaz önmagára való bijektív leképezését.

5.2. Definíció. Az $\{1,2,\ldots,n\}$ halmaz összes permutációi csoportot alkotnak a leképezésszorzás műveletével. Ezt a csoportot ***n-edfokú szimmetrikus csoportnak*** nevezzük, és S_n-nel jelöljük.

5.3. Állítás. Tetszőleges $\pi,\rho\in S_n$ permutációk esetén $(\pi\rho)^{-1}=\rho^{-1}\pi^{-1}$.

Biz. A permutációk szorzásának asszociativitását használva: $(\pi\rho)\left(\rho^{-1}\pi^{-1}\right)=\pi\left(\rho\rho^{-1}\right)\pi^{-1}=\pi\,\mathrm{id}\,\pi^{-1}=\pi\pi^{-1}=\mathrm{id}$ és $\left(\rho^{-1}\pi^{-1}\right)(\pi\rho)=\rho^{-1}\left(\pi^{-1}\pi\right)\rho=\rho^{-1}\,\mathrm{id}\,\rho=\rho^{-1}\rho=\mathrm{id}$. □

5.4. Definíció. Permutációk pozitív egész kitevős hatványát természetes módon értelmezhetjük: $\pi\in S_n$ és $k\in\mathbb{N}$ esetén legyen $\pi^k:=\pi\cdot\ldots\cdot\pi$ (k darab π szorzata). A nulladik hatvány az identikus permutáció: $\pi^0:=\mathrm{id}$, a negatív kitevős hatványt pedig az inverz segítségével definiáljuk: $\pi^{-k}:=(\pi^k)^{-1}$. A hatványozás szokásos azonosságainak egy része érvényben marad permutációkra is: $\pi^k\cdot\pi^\ell=\pi^{k+\ell}$, $(\pi^k)^\ell=\pi^{k\ell}$, ellenben a $(\pi\sigma)^k=\pi^k\cdot\sigma^k$ egyenlőség már nem mindig érvényes. Egy fontos speciális esetben azonban az utóbbi is teljesül: ha π és σ *felcserélhetőek*, azaz $\pi\cdot\sigma=\sigma\cdot\pi$, akkor $(\pi\sigma)^k=\pi^k\cdot\sigma^k$.

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

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

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

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

$$a \in M_\pi \implies a\pi \in M_\pi. \tag{5.4}$$

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

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

1) $a \notin M_\pi$ és $a \notin M_\rho$: Ekkor $a\pi = a$ és $a\rho = a$, tehát a bal oldalon $a(\pi\rho) = (a\pi)\rho = a\rho = a$, a jobb oldalon pedig $a(\rho\pi) = (a\rho)\pi = a\pi = a$ áll (ugye?).
2) $a \in M_\pi$ és $a \notin M_\rho$: Ekkor (5.4) szerint $a\pi \in M_\pi$, következésképp $a\pi \notin M_\rho$ (miért?). Tehát ρ-nak fixpontja a és $a\pi$ is (ugye?). Ennek felhasználásával a bal oldal $a(\pi\rho) = (a\pi)\rho = a\pi$, a jobb oldal pedig $a(\rho\pi) = (a\rho)\pi = a\pi$.
3) $a \notin M_\pi$ és $a \in M_\rho$: Ez ugyanaz, mint az előző eset, csak π és ρ szerepet cserél.
4) $a \in M_\pi$ és $a \in M_\rho$: Ez lehetetlen (miért?).

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

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

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

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

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

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

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

Ezt az eljárást folytatva újabb, a korábbiaktól idegen ciklusokat tudunk konstruálni (megengedve az 1 hosszúságú ciklusokat, azaz fixpontokat is), amíg el nem fogynak A elemei. Mivel A véges, ez előbb-utóbb be fog következni, és ekkor megkapjuk π felbontását páronként idegen ciklusok szorzatára. □

Páros és páratlan permutációk

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

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

Biz. Mivel minden permutáció felírható ciklusok szorzataként (5.9. Tétel), elég megmutatni, hogy minden ciklus előállítható transzpozíciók szorzataként. Az $(a_1\, a_2\, \cdots\, a_{k-1}\, a_k)$ ciklust például így írhatjuk fel (de sok más lehetőség is van): $(a_1\, a_2\, \cdots\, a_{k-1}\, a_k) = (a_1a_2)\,(a_1a_3)\cdots(a_1a_k)$ (ugye?). □

5.12. Tétel. Egy S_n-beli permutáció transzpozíciók szorzataként való felírásában a tényezők számának paritása egyértelműen meghatározott. Eszerint beszélhetünk ***páros permutációkról*** és ***páratlan permutációkról***.

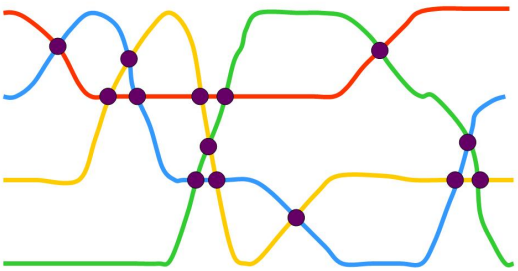
Biz. Tekintsük egy $\pi \in S_n$ permutáció két különböző felbontását transzpozíciók szorzatára:

$$\pi = \tau_1\tau_2\cdots\tau_k = \sigma_1\sigma_2\cdots\sigma_\ell,$$

ahol mindegyik τ_i és σ_j transzpozíció. Azt kell igazolnunk, hogy $k \equiv \ell \pmod 2$, vagy, ami ezzel ekvivalens, hogy $k+\ell$ páros. Átrendezve az egyenlőséget, azt kapjuk, hogy az identikus permutáció előáll $k+\ell$ transzpozíció szorzataként:

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_k\sigma_\ell\cdots\sigma_2\sigma_1.$$

Az ábra mutat egy ilyen előállítást S_4-ben: a négy elemet különböző színek jelzik, és az elemek „húzzák a csíkot”, ahogy cserélgetjük őket. Jelölje m a keletkező metszéspontok számát; két különböző módon is meg fogjuk határozni m-et (pontosabban csak m paritását), és a két eredményt összehasonlítva kapjuk majd, hogy $k+\ell$ páros. (A csíkokat úgy kanyarítjuk, hogy ne menjen át három csík egy ponton, tehát minden metszéspontban két szín találkozik.)



(i) Az első transzpozíció (piros–kék csere) 1 metszéspontot hozott létre, a második transzpozíció (kék–sárga csere) 3 metszéspontot, a további transzpozíciók rendre 5, 1, 1, 3 metszéspontot hoztak létre. Nem véletlen, hogy ezek a számok mind páratlanok: ha két olyan csíkot cserélünk meg, amelyek között t darab csík fut, akkor $2t+1$ metszéspont keletkezik (miért?). Azt látjuk tehát, hogy modulo 2 számolva minden csere 1 metszéspontot ad, azaz $m \equiv k+\ell \pmod 2$ (ugye?).

(ii) Most számoljuk meg a metszéspontokat színpáronként: a piros és a kék csík 2 helyen metszi egymást, a kék és a sárga csík 4 pontban metszi egymást, és így tovább. Itt azt figyelhetjük meg, hogy bármely két csík páros számú pontban metszi egymást. Ez sem véletlen: mivel a sok csere után az identikus permutációt kaptuk, az ábra bal és jobb szélén ugyanaz a színek sorrendje. Minden metszéspontnál az adott két szín helyet cserél (amelyik eddig felül volt, az alulra kerül), ezért bármely két csíknak páros sokszor kell metszenie egymást, hogy a végére visszaálljon a két szín eredeti sorrendje. Tehát a metszéspontok színpáronkénti összeszámolásakor csupa páros számot adunk össze, vagyis $m \equiv 0 \pmod 2$

Először azt kaptuk, hogy $m \equiv k+\ell \pmod 2$, másodszor pedig azt, hogy $m \equiv 0 \pmod 2$, ebből pedig az következik, hogy $k+\ell$ páros, és épp ezt kellett bizonyítanunk. □

Biz. (inverziókkal, csak vázlatosan) Legyen $\pi \in S_n$ és $i, j \in \{1, 2, \ldots, n\}$, $i < j$. Azt mondjuk, hogy i és j ***inverziót*** alkot, ha $i\pi > j\pi$. Meg lehet mutatni, hogy minden $\pi \in S_n$ permutáció és $\tau \in S_n$ transzpozíció esetén $\mathrm{inv}(\pi\tau)$ és $\mathrm{inv}(\pi)$ paritása különböző (itt $\mathrm{inv}(\pi)$ jelöli a π permutáció inverzióinak számát). Ebből következik, hogy π bármely transzpozíciók szorzatára való felírásában a tényezők számának paritása megegyezik $\mathrm{inv}(\pi)$ paritásával. □

5.13. Állítás. A páros hosszúságú ciklusok páratlan permutációk, míg a páratlan hosszúságú ciklusok páros permutációk.

Biz. A 5.11. Tétel bizonyítása során láttuk, hogy bármely k hosszúságú ciklus előáll $k-1$ transzpozíció szorzataként. □

5.14. Definíció. Az S_n-beli páros permutációk csoportot alkotnak (miért?). Ezt a csoportot ***n-edfokú alternáló csoportnak*** nevezzük, és A_n-nel jelöljük.

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

Biz. A tétel bizonyításához elegendő megadni egy bijekciót A_n és $S_n \setminus A_n$ között (ugye?). Legyen $\tau \in S_n$ egy tetszőleges rögzített transzpozíció (pl. $\tau = (12)$), és definiáljuk a φ leképezést a következőképpen: $\varphi\colon A_n \to S_n \setminus A_n$, $\pi \mapsto \pi\tau$. Három dolgot kell ellenőriznünk:

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

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

(iii) φ injektív, azaz minden $\pi_1, \pi_2 \in S_n$ esetén $\pi_1\tau = \pi_2\tau \implies \pi_1 = \pi_2$. Ezt könnyű igazolni, csak be kell szorozni jobbról a $\pi_1\tau = \pi_2\tau$ egyenlőség mindkét oldalát τ-val (ugye?).

□

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

december 3.

6. Nevezetes számelméleti problémák

Számok felbontása hatványok összegére

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Prímszámok

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

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

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

Biz. Tfh. $p_1, \ldots, p_n$ 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 $p_1, \ldots, p_n$ számok egyikével sem (ugye?), tehát minden prímosztója $4k + 1$ alakú. Eszerint N előáll $4k + 1$ alakú számok szorzataként, és így maga is $4k + 1$ alakú (miért?). Ez ellentmondás, hiszen szemlátomást $N \equiv -1 \pmod 4$. □

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

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

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

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

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

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

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

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

6.22. Tétel. A prímszámok reciprokaiból alkotott sor divergens, azaz

$$\sum_p \frac{1}{p} = \infty.$$

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

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

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

Biz. Legyen $p_1, p_2, \ldots$ a prímek sorozata (növekvő sorrendben). Euklidész gondolatmenete szerint (lásd a 6.14. Tétel bizonyítását) az $N = p_1 \cdot \ldots \cdot p_n + 1$ számnak van olyan p prímosztója, amelyre $p \notin \{p_1, \ldots, p_n\}$ 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.

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

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

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

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?). □

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

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

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

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

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