

## A permutáció fogalma

### 1.1. Definíció.

**Permutációknak** nevezük egy nemüres (véges) halmaz önmagára való bijektív leképezését.

### 1.2. Definíció.

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

Egy  $\pi \in S_n$  permutációt megadhatunk egy  $2 \times n$ -es mátrixszal úgy, hogy  $\{1, 2, \dots, n\}$  minden eleme alá odaírjuk a  $\pi$  melletti képét:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1\pi & 2\pi & 3\pi & \cdots & n\pi \end{pmatrix}.$$

Vegyünk észre, hogy  $\pi$  bijektivitása azt jelenti, hogy a mátrix alsó sorában az  $1, 2, \dots, n$  számok egy **permutációja** van.

## Számolás permutációkkal

### Példa.

Tekintsük  $S_6$ -ban az alábbi  $\pi$  és  $\rho$  permutációkat:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}.$$

$$\pi\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 5 & 4 \end{pmatrix} \quad \rho\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 4 & 6 \end{pmatrix}$$

$$\pi^{-1} = \begin{pmatrix} 3 & 5 & 1 & 2 & 6 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix}$$

$$\rho\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 6 & 5 & 2 \end{pmatrix}$$

$$\pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 5 & 4 & 2 \end{pmatrix} \implies \pi^4 = \text{id} \implies \pi^{101} = (\pi^4)^{25} \cdot \pi = \pi$$

## Ciklusfelbontás

### 1.7. Definíció.

Legyenek  $a_1, \dots, a_k \in \{1, 2, \dots, n\}$  különböző elemek, és legyen  $\pi \in S_n$  az alábbi permutáció:

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

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

### 1.8. Tétel.

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

### Példa.

Bontsuk idegen ciklusok szorzatára a korábban kiszámolt permutációkat.

$$\pi = (13)(2564), \rho = (123)(56), \pi\rho = (2643), \rho\pi = (1542), \rho\pi^{-1} = (1462)$$

## Transzpozíciók

### 1.9. Definíció.

A 2 hosszúságú ciklusokat, vagyis az  $(ij)$  alakú permutációkat **transzpozícióknak** nevezük.

### 1.10. Tétel.

Az  $S_n$  csoportot generálják a transzpozíciók, azaz minden  $S_n$ -beli permutáció előáll transzpozíciók szorzataként.

### Bizonyítás.

Elég ciklusokra igazolni:

$$(a_1 a_2 \cdots a_{k-1} a_k) = (a_1 a_2)(a_1 a_3)(a_1 a_4) \cdots (a_1 a_{k-1})(a_1 a_k). \quad \square$$

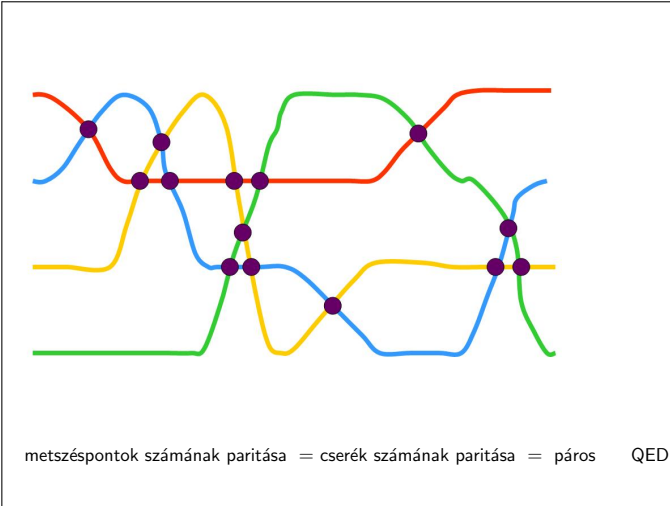
### Példa.

Bontsuk transzpozíciók szorzatára a  $\pi = (137)(2564)$  permutációt.

$$\pi = (137) \cdot (2564) = (13)(17) \cdot (25)(26)(24)$$

vagy

$$\pi \cdot (13)(25)(47)(34)(45)(56)(67) = \text{id} \implies \pi = (67)(56)(45)(34)(47)(25)(13)$$



## A paritás kiszámítása

### 1.12. Állítás.

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

### Bizonyítás.

Egy  $k$  hosszúságú ciklus előáll  $k - 1$  transzpozíció szorzataként. □

### 1.13. Állítás.

Permutációk szorzatának a paritása a következőképpen alakul:

$$\begin{array}{ll} \text{páros} \cdot \text{páros} = \text{páros} & \text{páros} \cdot \text{páratlan} = \text{páratlan} \\ \text{páratlan} \cdot \text{páratlan} = \text{páros} & \text{páratlan} \cdot \text{páros} = \text{páratlan} \end{array}$$

### Bizonyítás.

Szorzáskor a permutációt előállító transzpozíciók száma összeadódik. □

## Felcserélhetőség

### 1.3. Állítás.

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

### 1.4. Definíció.

Legyen  $\pi \in S_n$  és  $a \in \{1, 2, \dots, n\}$ .

- ▶ Ha  $a\pi = a$ , akkor azt mondjuk, hogy  $a$  **fixpontja**  $\pi$ -nek.
- ▶ Ha  $a\pi \neq a$ , akkor azt mondjuk, hogy  $a$  **mozgatott eleme**  $\pi$ -nek.

### 1.5. Definíció.

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

### 1.6. Tétel.

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

## Permutáció paritása

### 1.11. Tétel.

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

### Bizonyítás.

Tegyünk fel, hogy

$$\tau_1 \tau_2 \cdots \tau_{2k+1} = \sigma_1 \sigma_2 \cdots \sigma_{2l},$$

ahol mindegyik  $\tau_i$  és  $\sigma_j$  transzpozíció. Ekkor az identikus permutáció előáll páratlan sok transzpozíció szorzataként:

$$\text{id} = \tau_1 \tau_2 \cdots \tau_{2k+1} \sigma_{2l} \cdots \sigma_2 \sigma_1.$$

Megmutatjuk, hogy ez lehetetlen.

## Az alternáló csoport

### 1.14. Definíció.

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

### Példa.

$$S_3 = \{\text{id}, (12), (13), (23), (123), (132)\}$$

$$A_3 = \{\text{id}, (123), (132)\}$$

### Példa.

$$A_4 = \{\text{id}, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$$

## Az alternáló csoport

### 1.15. Tétel.

Az  $S_n$ -beli permutációk fele páros és fele páratlan.

### Bizonyítás.

Legyen  $\tau \in S_n$  egy tetszőleges transzpozíció, pl.  $\tau = (12)$ . Ekkor a

$$\varphi: A_n \rightarrow S_n \setminus A_n, \pi \mapsto \pi\tau$$

leképezés bijekciót létesít a páros permutációk halmaza és a páratlan permutációk halmaza között. Valóban,

$$\bullet \forall \pi \in A_n: \pi\tau \in S_n \setminus A_n;$$

$$\bullet \forall \rho \in S_n \setminus A_n \exists! \pi \in A_n: \pi\tau = \rho \quad (\text{nevezetesen } \pi = \rho\tau^{-1} = \rho\tau \in A_n).$$

□

### 1.16. Következmény.

$$|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$$

## Relációk

„reláció” *lat.* **1.** kapcsolat, viszony; összefüggés vmivel **2.** viszonylat, vonatkozás **3.** *mat* halmazok elemei közötti kapcsolat [...]”  
Bakos Ferenc: Idegen szavak és kifejezések szótára

### 2.1. Definíció.

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

### Jelölés.

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

### Példa.

- ▶  $A = \mathbb{N}$ ,  $a\rho b \iff a \mid b$
- ▶  $A = \mathbb{R}$ ,  $a\rho b \iff a \leq b$
- ▶  $A = a$  sík egyenesének halmaza,  $a\rho b \iff a \perp b$
- ▶  $A =$  háromszögek halmaza,  $a\rho b \iff a$  és  $b$  egybevágó
- ▶  $A =$  emberek halmaza,  $a\rho b \iff a$  gyermeke  $b$ -nek
- ▶  $A = \{1, 2, 3\}$ ,  $\rho = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$
- ▶ ...

## Ekvivalenciarelációk

### 2.2. Definíció.

**Ekvivalenciarelációnak** nevezük 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)  $\forall a, b, c \in A: (a\rho b \text{ és } b\rho c) \implies a\rho c$  (transzitivitás).

### Példa.

- ▶  $A = a$  sík egyenesének halmaza,  $a\rho b \iff a \parallel b$
- ▶  $A =$  háromszögek halmaza,  $a\rho b \iff a$  és  $b$  hasonló
- ▶  $A = \mathcal{P}(U)$ ,  $a\rho b \iff$  létezik  $a \rightarrow b$  bijekció
- ▶  $A =$  emberek halmaza,  $a\rho b \iff a$  testvére  $b$ -nek
- ▶  $A = \{1, 2, 3\}$ ,  $\rho = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$
- ▶ ...

## Leképezés magja

### 2.3. Állítás.

Tetszőleges  $f: A \rightarrow B$  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**.

### Példa.

Legyen  $f: \{-1, 0, 1, 2, 3\} \rightarrow \mathbb{Z}$ ,  $x \mapsto x^2$ . Határozzuk meg  $f$  magját.

$$\ker f = \{(-1, -1), (-1, 1), (1, -1), (1, 1), (0, 0), (2, 2), (3, 3)\}$$

### Példa.

Az  $f: A \rightarrow B$  leképezés akkor és csak akkor injektív, ha magja az **egyenlőség reláció**:

$$\ker f = \{(a, a) : a \in A\}.$$

### Példa.

Az  $f: A \rightarrow B$  leképezés akkor és csak akkor konstans, ha magja a **teljes reláció**:

$$\ker f = A \times A.$$

## Ekvivalenciaosztályok

### 2.4. Definíció.

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

Ekkor az

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

halmazt az  $a$  elem  $\rho$  szerinti **(ekvivalencia)osztályának** (vagy blokkjának), az ekvivalenciaosztályok halmazát pedig az  $A$  halmaz  $\rho$  szerinti **faktorhalmazának** nevezzük.

### Jelölés.

Az  $a$  elem  $\rho$  szerinti osztályát szokás  $a/\rho$ -val,  $\bar{a}$ -val vagy  $[a]_\rho$ -val jelölni, de mi inkább az egyszerűbb  $\bar{a}$  jelölést használjuk. Ez ugyan nem utal  $\rho$ -ra, de általában kiderül a szövegkörnyezetből, hogy mi a szóban forgó ekvivalenciareláció.

A faktorhalmazt  $A/\rho$  jelöli, tehát

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

## Ekvivalenciaosztályok

### Példa.

Legyen  $A = \{1, 2, 3\}$ ,  $\rho = \{(1, 1), (2, 2), (3, 3), (2, 3), (3, 2)\}$ .

Ekkor

$$\bar{1} = \{1\}, \quad \bar{2} = \{2, 3\}, \quad \bar{3} = \{2, 3\};$$

$$A/\rho = \{\{1\}, \{2, 3\}\}.$$

### Példa.

Legyen  $A = \{-1, 0, 1, 2, 3\}$ ,  $f: A \rightarrow \mathbb{Z}$ ,  $x \mapsto x^2$  és  $\rho = \ker f$ .

Ekkor

$$\bar{-1} = \{-1, 1\}, \quad \bar{1} = \{-1, 1\}, \quad \bar{0} = \{0\}, \quad \bar{2} = \{2\}, \quad \bar{3} = \{3\};$$

$$A/\rho = \{\{-1, 1\}, \{0\}, \{2\}, \{3\}\}.$$

Figyeljük meg, hogy ha  $a\rho b$ , akkor  $\bar{a} = \bar{b}$ , egyébként pedig  $\bar{a}$  és  $\bar{b}$  diszjunkt halmazok.

## Ekvivalenciák és osztályozások

### 2.5. 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

- (1)  $\forall B \in \mathcal{C} : B \neq \emptyset$ ;
- (2)  $\forall B_1 \neq B_2 \in \mathcal{C} : B_1 \cap B_2 = \emptyset$ ;
- (3)  $\bigcup_{B \in \mathcal{C}} B = A$ .

### 2.6. Tétel.

Legyen  $A$  egy nemüres halmaz.

- ▶ Ha  $\rho \subseteq A \times A$  ekvivalenciareláció, akkor  $A/\rho$  osztályozás az  $A$  halmazon.
- ▶ 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  $\rho$  reláció ekvivalenciareláció az  $A$  halmazon.

A most megadott „ekvivalenciareláció  $\mapsto$  osztályozás” és „osztályozás  $\mapsto$  ekvivalenciareláció” megfeleltetések egymás inverzei.

## Az ekvivalenciareláció, mint fogalomalkotó eszköz

### Példa.

- ▶  $A = a$  sík egyenesének halmaza,  $a\rho b \iff a \parallel b$   $\rightsquigarrow$  az irány fogalma
- ▶  $A =$  háromszögek halmaza,  $a\rho b \iff a$  és  $b$  hasonló  $\rightsquigarrow$  az „alak” fogalma
- ▶  $A = \mathcal{P}(U)$ ,  $a\rho b \iff$  létezik  $a \rightarrow b$  bijekció  $\rightsquigarrow$  a számosság fogalma
- ▶  $A = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ ,  $(a_1, a_2)\rho(b_1, b_2) \iff a_1 b_2 = a_2 b_1$   $\rightsquigarrow$  a tört fogalma

## A számfogalom (egy) felépítése

### Természetes számok

A véges halmazok „halmazán” értelmezzük a  $\rho$  ekvivalenciarelációt a következőképpen:

$$a\rho b \iff \text{létezik } A \rightarrow B \text{ bijekció.}$$

A természetes számok nem mások, mint a megfelelő ekvivalenciaosztályok. Például

$$3 = \overline{\{1, 2, 3\}} = \overline{\{a, b, c\}} = \overline{\{\spadesuit, \heartsuit, \clubsuit\}} = \dots$$

Az összeadás a diszjunkt unió segítségével definiálható:  $\bar{A} + \bar{B} = \overline{A \cup B}$ . Például

$$2 + 3 = \overline{\{\spadesuit, \heartsuit\}} + \overline{\{\clubsuit, \diamondsuit\}} = \overline{\{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}} = \overline{\{\spadesuit, \heartsuit, \clubsuit\} \cup \{\spadesuit, \heartsuit, \diamondsuit\}} = \overline{\{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}} = 5.$$

A szorzás a Descartes-szorzat segítségével definiálható:  $\bar{A} \cdot \bar{B} = \overline{A \times B}$ . Például

$$2 \cdot 3 = \overline{\{\spadesuit, \heartsuit\}} \cdot \overline{\{\clubsuit, \diamondsuit\}} = \overline{\{\spadesuit, \heartsuit\} \times \{\clubsuit, \diamondsuit\}} = \overline{\{(\spadesuit, \clubsuit), (\spadesuit, \diamondsuit), (\heartsuit, \clubsuit), (\heartsuit, \diamondsuit)\}} = 6.$$

Ezek a műveletek *jóldefiniáltak* (mit jelent ez?) és rendelkeznek a szokásos műveleti tulajdonságokkal. (Lásd még: **Peano-axiómarendszer**.)

## A számfogalom (egy) felépítése

### Egész számok

Az  $\mathbb{N}_0 \times \mathbb{N}_0$  halmazon értelmezzük a  $\rho$  ekvivalenciarelációt a következőképpen:

$$(a_1, a_2) \rho (b_1, b_2) \iff a_1 + b_2 = a_2 + b_1.$$

Az egész számok nem mások, mint a megfelelő ekvivalenciaosztályok. Például

$$-3 = \overline{(0, 3)} = \overline{(1, 4)} = \overline{(2, 5)} = \dots$$

Az összeadás, kivonás és szorzás művelete értelmezhető ezen ekvivalenciaosztályok halmazán (hogyan?), és rendelkeznek a szokásos műveleti tulajdonságokkal. Így kapjuk az egész számok  $\mathbb{Z}$  gyűrűjét.

### Racionális számok

A  $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$  halmazon értelmezzük a  $\rho$  ekvivalenciarelációt a következőképpen:

$$(a_1, a_2) \rho (b_1, b_2) \iff a_1 b_2 = a_2 b_1.$$

A racionális számok nem mások, mint a megfelelő ekvivalenciaosztályok. Például

$$\frac{2}{5} = \overline{(2, 5)} = \overline{(4, 10)} = \overline{(6, 15)} = \dots$$

Az összeadás, kivonás, szorzás és osztás művelete értelmezhető ezen ekvivalenciaosztályok halmazán (hogyan?), és rendelkeznek a szokásos műveleti tulajdonságokkal. Így kapjuk a racionális számok  $\mathbb{Q}$  testét.

## A számfogalom (egy) felépítése

### Valós számok

A racionális számokból álló **Cauchy-sorozatok** halmazán értelmezzük a  $\rho$  ekvivalenciarelációt a következőképpen:

$$\{a_n\} \rho \{b_n\} \iff \lim_{n \rightarrow \infty} (a_n - b_n) = 0.$$

A valós számok nem mások, mint a megfelelő ekvivalenciaosztályok. Például

$$\pi = \overline{(3, 3,1, 3,14, 3,141, \dots)} = \overline{(4, 3,2, 3,15, 3,142, \dots)} = \dots$$

Az összeadás, kivonás, szorzás és osztás művelete értelmezhető ezen ekvivalenciaosztályok halmazán (hogyan?), és rendelkeznek a szokásos műveleti tulajdonságokkal. Így kapjuk a valós számok  $\mathbb{R}$  testét. (Lásd még: **Dedekind-szeletek**.)

### Komplex számok

A komplex számok szokásos definíciója nem használ ekvivalenciarelációkat, de később majd látunk egy alternatív definíciót valós polinomok ekvivalenciaosztályai segítségével.

## Részbenrendezési reláció

### 2.7. Definíció.

**Részbenrendezési relációknak** nevezzük a  $\rho \subseteq A \times A$  relációt, ha rendelkezik az alábbi három tulajdonsággal:

- (1)  $\forall a \in A : a \rho a$  (reflexivitás);
- (2)  $\forall a, b \in A : (a \rho b \text{ és } b \rho a) \implies a = b$  (antiszimetria);
- (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  $\rho$ -t **teljes rendezésnek** (vagy lineáris rendezésnek) nevezzük:

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

### Példa.

- ▶  $A = \mathbb{R}$ ,  $a \rho b \iff a \leq b$
- ▶  $A = \mathbb{N}_0$ ,  $a \rho b \iff a \mid b$
- ▶  $A = \mathcal{P}(U)$ ,  $a \rho b \iff a \subseteq b$

## Részbenrendezett halmaz

### Jelölés.

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

### 2.8. Definíció.

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

### Példa.

Íme három négyelemű részbenrendezett halmaz:

- ▶  $(\{1, 2, 3, 4\}; \leq)$ ,
- ▶  $(\{1, 2, 3, 4\}; \mid)$ ,
- ▶  $(\mathcal{P}(\{a, b\}); \subseteq)$ .

## Fedési reláció

### 2.9. Definíció.

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

### Példa.

- ▶ Az  $(\mathbb{N}; \leq)$  részbenrendezett halmazban  $a < b \iff b = a + 1$
- ▶ Az  $(\mathbb{R}; \leq)$  részbenrendezett halmazban  $a < b \iff$  SOHA!
- ▶ Az  $(\mathbb{N}; \mid)$  részbenrendezett halmazban  $a < b \iff b = ap$  ( $p$  prím)
- ▶ A  $(\mathcal{P}(U); \subseteq)$  részbenrendezett halmazban  $A < B \iff |B \setminus A| = 1$

## Hasse-diagram

### 2.10. Tétel.

Véges részbenrendezett halmazt egyértelműen meghatározza a fedési relációja.

### Bizonyítás.

A végességnek köszönhetően  $a < b$  akkor és csak akkor teljesül, ha  $a$  és  $b$  összeköthető fedések láncolatával:

$$a < b \iff \exists n \in \mathbb{N} \exists c_0, \dots, c_n \in A : a = c_0 < c_1 < \dots < c_{n-1} < c_n = b. \quad \square$$

### 2.11. Definíció.

Egy  $(A; \leq)$  részbenrendezett halmaz **Hasse-diagramján** egy ábrát értünk, amelyen  $A$  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  $b$  fedí  $a$ -t.

## Minimális, maximális, legkisebb, legnagyobb elem

### 2.12. 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  $\iff \nexists b \in A : b < a$ ;
- ▶  $a$  legkisebb  $\iff \forall b \in A : a \leq b$ ;
- ▶  $a$  maximális  $\iff \nexists b \in A : b > a$ ;
- ▶  $a$  legnagyobb  $\iff \forall b \in A : a \geq b$ .

### Példa.

Az  $(\mathbb{N}_0; \mid)$  részbenrendezett halmaz legkisebb eleme 1, a legnagyobb eleme pedig 0.

### 2.13. Tétel.

Részbenrendezett halmazban legföljebb egy legkisebb elem létezhet. Ha van legkisebb elem, akkor az minimális elem is, sőt ő az egyetlen minimális elem. Hasonló érvényes a legnagyobb elemre is.

## Lexikografikus rendezés

### 2.14. Definíció.

Legyen  $(A; \leq)$  egy lineárisan rendezett halmaz (ábécé) és legyen  $A^n$  az  $A$  elemeiből képezett elem  $n$ -esek halmaza (szavak).

Azt mondjuk, hogy az  $\mathbf{a} = (a_1, \dots, a_n) \in A^n$  szó **lexikografikusan kisebb** a  $\mathbf{b} = (b_1, \dots, b_n) \in A^n$  szónál (jelölés:  $\mathbf{a} \sqsubset \mathbf{b}$ ), ha

$$\exists i \in \{1, \dots, n\} : a_i < b_i \text{ és minden } j < i \text{ esetén } a_j = b_j.$$

Az  $\mathbf{a} \sqsubseteq \mathbf{b} \iff \mathbf{a} \sqsubset \mathbf{b}$  vagy  $\mathbf{a} = \mathbf{b}$  képlettel definiált  $\sqsubseteq$  relációt **lexikografikus rendezésnek** nevezzük.

### Példa.

Soroljuk fel lexikografikusan növekvő sorrendben az  $A = \{a, b, c\}$  abécé feletti kétbetűs szavakat.

$$aa \sqsubset ab \sqsubset ac \sqsubset ba \sqsubset bb \sqsubset bc \sqsubset ca \sqsubset cb \sqsubset cc$$

### Példa.

Soroljuk fel lexikografikusan növekvő sorrendben az  $A = \{0, 1\}$  abécé feletti hárombetűs szavakat.

$$000 \sqsubset 001 \sqsubset 010 \sqsubset 011 \sqsubset 100 \sqsubset 101 \sqsubset 110 \sqsubset 111$$

## Lexikografikus rendezés

### 2.15. Tétel.

Tetszőleges  $(A; \leq)$  lineárisan rendezett halmaz és  $n$  pozitív egész szám esetén a  $\sqsubseteq$  reláció lineáris rendezés az  $A^n$  halmazon.

### Bizonyítás.

- ▶ reflexivitás: Világos.
- ▶ antiszimetria és dichotómia: Ha  $\mathbf{a} \neq \mathbf{b}$  akkor az  $\mathbf{a}$  és  $\mathbf{b}$  közötti első eltérés szerint vagy  $\mathbf{a} \sqsubset \mathbf{b}$  vagy  $\mathbf{a} \supset \mathbf{b}$  teljesül (és csak az egyik).
- ▶ tranzitivitás: ÁMNTFH.  $\mathbf{a} \sqsubset \mathbf{b} \sqsubset \mathbf{c}$ . Ekkor *valahogy így* fest a helyzet:

$$\begin{array}{cccccccccccc} a_1 & a_2 & \dots & a_{i-1} & a_i & \dots & a_j & a_{j+1} & \dots & a_{n-1} & a_n \\ \parallel & \parallel & & & \parallel & \wedge & & & & & \\ b_1 & b_2 & \dots & b_{i-1} & b_i & \dots & b_j & b_{j+1} & \dots & b_{n-1} & b_n \\ \parallel & \parallel & & & \parallel & \parallel & \wedge & & & & \\ c_1 & c_2 & \dots & c_{i-1} & c_i & \dots & c_j & c_{j+1} & \dots & c_{n-1} & c_n \end{array}$$

Tehát  $\mathbf{a}$  és  $\mathbf{c}$  között az első eltérés az  $i$ -edik helyen van:  $a_i < c_i$ . Ezért  $\mathbf{a} \sqsubset \mathbf{c}$ .

## Lexikografikus rendezés

### 2.16. Tétel.

Az  $(\mathbb{N}_0^2; \sqsubseteq)$  rendezett halmazban nincs végtelen hosszú csökkenő sorozat.

### 2.17. Tétel.

A szám  $n$ -esek komponensenkénti összeadása **szigorúan monoton** a lexikografikus rendezésre nézve: bármely  $a, b, \hat{a}, \hat{b} \in \mathbb{N}_0^n$  esetén

$$a \sqsubseteq b, \hat{a} \sqsubseteq \hat{b} \implies a + \hat{a} \sqsubseteq b + \hat{b},$$

és egyenlőség csak  $a = b, \hat{a} = \hat{b}$  esetén teljesül.

## Emlékeztető

### 3.1. Definíció.

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

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

A  $t$  egész szám **legkisebb közös többszöröse**  $a$ -nak és  $b$ -nek, ha kielégíti a következő két feltételt:

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

### Jelölés.

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

### 3.2. Megjegyzés.

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

## Az Inko rendezéseméleti megközelítése

### 3.3. Megjegyzés.

Az 3.1. Definíció szerint  $\text{Inko}(a, b)$  nem más, mint  $(D_a \cap D_b; |)$  legnagyobb eleme. Nem triviális, hogy létezik legnagyobb eleme ennek a részbenrendezett halmaznak (miért?), de az euklideszi algoritmus garantálja, hogy létezik.

Az „iskolás definíció” szerint az  $a, b \in \mathbb{N}$  számok legnagyobb közös osztója nem más, mint  $(D_a \cap D_b; \leq)$  legnagyobb eleme. Erről világos, hogy létezik, de az nem világos, hogy  $\text{Inko}(a, b)$  nem csak nagyobb minden más közös osztónál, de **többszöröse** is minden más közös osztónak.

Tegyük fel, hogy  $d = \text{Inko}(a, b)$  az 3.1. Definíció értelmében. Ha  $k \in D_a \cap D_b$ , akkor  $k \mid d$  és így  $k \leq d$ , azaz  $d$  legnagyobb eleme a  $(D_a \cap D_b; \leq)$  részbenrendezett halmaznak is. Tehát az „egyetemi definíció” és az „iskolás definíció” ekvivalens egymással — legalábbis pozitív egész számokra.

Mennyi  $\text{Inko}(0, 0)$ ?

- ▶ „iskolás definíció”:  $(D_0 \cap D_0; \leq) = (\mathbb{N}_0 \cap \mathbb{N}_0; \leq) = (\mathbb{N}_0; \leq)$  legnagyobb eleme, ami nem létezik!
- ▶ „egyetemi definíció”:  $(D_0 \cap D_0; |) = (\mathbb{N}_0 \cap \mathbb{N}_0; |) = (\mathbb{N}_0; |)$  legnagyobb eleme, azaz 0.

## Euklideszi algoritmus

### 3.4. Tétel (euklideszi algoritmus).

Bármely két természetes számnak van legnagyobb közös osztója, és az az euklideszi algoritmussal megkapható. Az  $a = r_0, b = r_1$  természetes számokon végrehajtott **euklideszi algoritmus** maradékos osztások ismételt elvégzését jelenti:

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

Az eljárás véges számú lépés után véget ér: létezik olyan  $n \in \mathbb{N}$ , hogy  $r_{n+1} = 0$ . A legnagyobb közös osztó az utolsó nemnulla maradék, azaz  $\text{Inko}(a, b) = r_n$ .



A legnagyobb közös osztó kifejezhető a két szám „lineáris kombinációjaként”: léteznek olyan  $x, y$  egész számok, melyekre  $ax + by = \text{Inko}(a, b)$ .

## Euklideszi algoritmus

### Bizonyítás.

„Teljes indukcióval” megmutatjuk, hogy minden  $i$ -re  $\exists x_i, y_i \in \mathbb{Z} : ax_i + by_i = r_i$ .

Kezdőlépések:  $r_0 = a \cdot 1 + b \cdot 0$  és  $r_1 = a \cdot 0 + b \cdot 1$ .

Tfh.  $j = 0, 1, \dots, i$  esetén  $\exists x_j, y_j \in \mathbb{Z} : ax_j + by_j = r_j$ . (IH)

Fejezzük ki  $r_{i+1}$ -et  $a$  és  $b$  segítségével:

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

Mivel  $\text{Inko}(a, b) \sim r_n$ , azt kapjuk, hogy  $ax_n + by_n \sim \text{Inko}(a, b)$ . □

## Relatív prímesség

### 3.5. Definíció.

Azt mondjuk, hogy az  $a, b$  egész számok **relatív prímek**, ha  $\text{Inko}(a, b) = 1$ . Jelölés:  $a \perp b$ .

### 3.6. Tétel.

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

### 3.7. Tétel (Euklidesz lemmája).

Tetszőleges  $a, b, c$  egész számok esetén ha  $\text{Inko}(a, b) \neq 0$ , akkor

$$a \mid bc \iff \frac{a}{\text{Inko}(a, b)} \mid c.$$

## Diofantoszi egyenlet

### 3.8. Tétel.

Tetszőleges adott  $a, b, c$  (nemnulla) egész számok esetén az  $ax + by = c$  **kétismeretlenes lineáris diofantoszi egyenlet** akkor és csak akkor oldható meg, ha  $\text{Inko}(a, b) \mid c$ . 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:

$$x_t = x_0 + \frac{b}{\text{Inko}(a, b)} \cdot t; \quad y_t = y_0 - \frac{a}{\text{Inko}(a, b)} \cdot t.$$

### Bizonyítás.

Legyen  $d \sim \text{Inko}(a, b) \neq 0$ . Tudjuk, hogy  $\exists u, v \in \mathbb{Z} : au + bv = d$ .

1. Van megoldás  $\iff d \mid c$ .

$\implies$ : Ha  $(x, y)$  egy megoldás, akkor  $d \mid ax + by = c$ .

$\impliedby$ : Ha  $d \mid c$ , akkor  $c = d \frac{c}{d} = (au + bv) \frac{c}{d} = a \cdot u \frac{c}{d} + b \cdot v \frac{c}{d}$ , tehát

$x = u \frac{c}{d}, y = v \frac{c}{d}$  egy megoldás.

## Diofantoszi egyenlet

### Biz. (folyt.)

Legyen  $M$  a megoldáshalmaz:  $M = \{(x, y) : ax + by = c\} \subseteq \mathbb{Z} \times \mathbb{Z}$ . Tfh.  $(x_0, y_0) \in M$ , azaz  $ax_0 + by_0 = c$ .

2.  $M = \{(x_t, y_t) : t \in \mathbb{Z}\}$ , ahol  $x_t = x_0 + \frac{b}{d} \cdot t, y_t = y_0 - \frac{a}{d} \cdot t$   
 $\supseteq$ :  $a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t = c$   
 $\subseteq$ : Legyen  $(x, y) \in M$ .

$$\begin{aligned} ax + by = c = ax_0 + by_0 &\implies ax - ax_0 = by_0 - by \\ &\implies b \mid a(x - x_0) \\ &\implies \frac{b}{d} \mid x - x_0 \\ &\implies \exists t \in \mathbb{Z} : x - x_0 = \frac{b}{d}t \end{aligned}$$

Tehát  $x = x_0 + \frac{b}{d} \cdot t = x_t$ . Az  $y$ -ra vonatkozó képlet

ezután már egyszerű visszahelyettesítéssel kijön:

$$by_0 - by = a(x - x_0) = \frac{ab}{d}t \implies y = y_0 - \frac{a}{d}t = y_t. \quad \square$$

## A kongruenciareláció definíciója

### 3.9. 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 modulus utána zárójelben tüntetjük fel a mod rövidítést használva (de ezt időnként elhagyjuk). Tehát  $a \equiv b \pmod{m} \iff m \mid a - b$ .

### 3.10. 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.

### Bizonyítás.

Legyen  $a = mq + r$  és  $b = mt + s$ , ahol  $0 \leq r, s < m$ .

$$m \mid a - b = m(q - t) + r - s \iff m \mid r - s \iff r - s = 0 \iff r = s \quad \square$$

## A kongruenciareláció tulajdonságai

### 3.11. 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)  $(a \equiv b \pmod{m} \text{ és } b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$  (transzitivitás);
- (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  $ca \equiv cb \pmod{m} \iff a \equiv b \pmod{\frac{m}{\text{Inko}(m,c)}}$ ;
- (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  $\text{Inko}(a, m) = \text{Inko}(b, m)$ .

## A kongruenciareláció tulajdonságai

### Bizonyítás.

- (4) Tfh.  $a_1 \equiv b_1 \pmod{m}$  és  $a_2 \equiv b_2 \pmod{m}$ . Ekkor  $m \mid a_1 - b_1$  és  $m \mid a_2 - b_2$ .  

$$a_1 \cdot a_2 \stackrel{?}{\equiv} b_1 \cdot b_2 \pmod{m} \iff m \stackrel{?}{\mid} a_1 a_2 - b_1 b_2$$

$$\iff m \stackrel{?}{\mid} a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2$$

$$\iff m \stackrel{?}{\mid} (a_1 - b_1) \cdot a_2 + b_1 \cdot (a_2 - b_2) \quad \checkmark$$
- (5)  $ca \equiv cb \pmod{m} \iff m \mid ca - cb = c(a - b)$   

$$\iff \frac{m}{\text{Inko}(m,c)} \mid a - b$$

$$\iff a \equiv b \pmod{\frac{m}{\text{Inko}(m,c)}}$$
- (7)  $\left. \begin{matrix} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{matrix} \right\} \iff m_1, m_2 \mid a - b$   

$$\iff [m_1, m_2] \mid a - b$$

$$\iff a \equiv b \pmod{[m_1, m_2]} \quad \square$$

## Maradékosztályok

### 3.12. Definíció.

Egy  $a$  egész szám modulo  $m$  **maradékosztálya**n az

$$\bar{a} = \{b \in \mathbb{Z} : a \equiv b \pmod{m}\}$$

halmazt értjük.

### Jelölés.

A modulo  $m$  maradékosztályok halmazát  $\mathbb{Z}_m$  jelöli. Tehát

$$\mathbb{Z}_m = \{\bar{a} : a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}.$$

### 3.13. Definíció.

A modulo  $m$  maradékosztályok halmazán értelmezzük az első három alapműveletet a következőképpen: tetszőleges  $a, b \in \mathbb{Z}$  esetén legyen

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} - \bar{b} = \overline{a-b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

### 3.14. Tétel.

A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (különbsége, 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**).

## Számolás maradékosztályokkal

### Példa.

Számoljunk  $\mathbb{Z}_{12}$ -ben!

- ▶  $\bar{6} + \bar{8} = \bar{2}$
- ▶  $\bar{6} - \bar{8} = \bar{10}$
- ▶  $\bar{6} \cdot \bar{8} = \bar{0}$
- ▶  $\bar{5}^3 = \bar{5}$

### Példa.

$\mathbb{Z}_4$  összeadó- és szorozótáblája:

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

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

## Redukált maradékosztályok

### 3.15. Megjegyzés.

A 3.11. Tételbeli utolsó állítás szerint van értelme egy mod  $m$  maradékosztály és az  $m$  modulus legnagyobb közös osztójáról beszélni (hiszen nem függ a reprezentáns választásától). Később fontos szerepet játszanak majd azok a maradékosztályok, amelyek relatív prímek a modulushoz, ezért erre külön elnevezést és jelölést vezetünk be.

### 3.16. Definíció.

Az  $\bar{a} \in \mathbb{Z}_m$  maradékosztályt **redukált maradékosztálynak** hívjuk, ha  $\text{Inko}(a, m) = 1$ .

### Jelölés.

A mod  $m$  redukált maradékosztályok halmazát  $\mathbb{Z}_m^*$  jelöli. Tehát

$$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m : a \perp m\}.$$

### Példa.

$$\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}, \quad \mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}, \quad \mathbb{Z}_{10}^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$$

## Lineáris kongruenciák

### 3.17. Definíció.

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

### Példa.

Oldjuk meg a  $3x \equiv 4 \pmod{5}$  kongruenciát.

Egyik módszer:

$$3x \equiv 4 \pmod{5} \iff 5 \mid 3x - 4 \iff \exists y \in \mathbb{Z} : 3x - 4 = 5y$$

Megoldjuk a diofantoszi egyenletet ( $y$  nem is kell):

$$x = 3 + 5t \iff x \equiv 3 \pmod{5}.$$

Másik módszer:

$$3x \equiv 4 \pmod{5}$$

$$3x \equiv 9 \pmod{5} \quad (\text{mert } 4 \equiv 9 \pmod{5})$$

$$x \equiv 3 \pmod{5} \quad (\text{leosztottunk 3-mal (!)})$$

## Lineáris kongruenciák

### 3.18. Tétel.

Az  $ax \equiv b \pmod{m}$  lineáris kongruencia akkor és csak akkor oldható meg, ha  $\text{Inko}(a, m) \mid b$ .

Ha ez teljesül, akkor a megoldások egyetlen modulo  $\frac{m}{\text{Inko}(a,m)}$  maradékosztályt alkotnak, modulo  $m$  pedig  $\text{Inko}(a, m)$  megoldások száma.

Ha  $x_0$  egy megoldás, akkor az általános megoldás:

$$x \equiv x_0 + t \cdot \frac{m}{\text{Inko}(a, m)} \pmod{m} \quad (t = 0, 1, \dots, \text{Inko}(a, m) - 1).$$

### Bizonyítás.

Legyen  $d = \text{Inko}(a, m)$ . Fogalmazzuk át a kongruenciát diofantoszi egyenletté:

$$ax \equiv b \pmod{m} \iff m \mid ax - b$$

$$\iff \exists y \in \mathbb{Z} : ax - b = my$$

$$\iff \exists y \in \mathbb{Z} : ax - my = b$$

▶ Akkor és csak akkor van megoldás, ha  $d \mid b$ .

▶ Ha  $x_0$  egy partikuláris megoldás, akkor az általános megoldás:  $x_t = x_0 + t \cdot \frac{m}{d}$ . Ezek az  $x_t$  számok egyetlen modulo  $\frac{m}{d}$  maradékosztályt alkotnak.

## Lineáris kongruenciák

### Bizonyítás. (folyt.)

▶ Hány megoldás van modulo  $m$ ?

$$x_{t_1} \equiv x_{t_2} \pmod{m} \iff x_0 + t_1 \cdot \frac{m}{d} \equiv x_0 + t_2 \cdot \frac{m}{d} \pmod{m}$$

$$\iff t_1 \cdot \frac{m}{d} \equiv t_2 \cdot \frac{m}{d} \pmod{m}$$

$$\iff t_1 \equiv t_2 \pmod{d}$$

Tehát  $d$  megoldás van modulo  $m$ , mert ennyiféleképp lehet a  $t$  paramétert megválasztani modulo  $d$ . Elég a  $t = 0, 1, \dots, d - 1$  értékeket tekinteni; ezek megadják az összes megoldást modulo  $m$ :

$$x \equiv x_0 + t \cdot \frac{m}{d} \pmod{m} \quad (t = 0, 1, \dots, d - 1)$$

□

## Multiplikatív inverz

### 3.19. Definíció.

Azt mondjuk, hogy az  $a, b$  egész számok egymás **multiplikatív inverzei** modulo  $m$ , ha  $ab \equiv 1 \pmod{m}$ .

Hasonlóan  $\bar{a}, \bar{b} \in \mathbb{Z}_m$  egymás multiplikatív inverzei, ha  $\bar{a} \cdot \bar{b} = \bar{1}$ .

### Jelölés.

Ha nem fenyeget a félreértés veszélye, akkor az  $a$  egész szám mod  $m$  multiplikatív inverzét  $a^{-1}$ -gyel jelöljük. Hasonlóan  $\bar{a} \in \mathbb{Z}_m$  multiplikatív inverzét  $\bar{a}^{-1}$  jelöli.

### 3.20. Tétel.

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

Hasonlóan,  $\bar{a} \in \mathbb{Z}_m$  akkor és csak akkor rendelkezik multiplikatív inverzzel, ha  $\bar{a} \in \mathbb{Z}_m^*$ . Ilyenkor a multiplikatív inverz egyértelműen meghatározott.

### 3.21. Következmény.

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

### 3.22. Tétel (Wilson tétele).

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

## Negatív kitevős hatványozás

### 3.23. Definíció.

Ha  $a$  és  $m$  relatív prímek, akkor tetszőleges  $k \in \mathbb{N}$  esetén értelmezzük az  $a^{-k}$  negatív kitevőjű hatványt modulo  $m$ : legyen  $a^{-k} \equiv (a^k)^{-1} \pmod{m}$ .

Hasonlóképpen  $\bar{a} \in \mathbb{Z}_m^*$  esetén legyen  $(\bar{a})^{-k} = (\bar{a}^k)^{-1}$ .

### 3.24. Megjegyzés.

Meg lehet mutatni, hogy a hatványozás szokásos azonosságai érvényben maradnak az egész kitevős mod  $m$  hatványok fenti értelmezése mellett.

## Lineáris kongruenciarendszerek

### 3.25. Definíció.

Adott  $a_i, b_i, n_i$  ( $i = 1, 2, \dots, k$ ) egész számok esetén az alábbi „egyenletrendszert” **lineáris kongruenciarendszerek** nevezzük (az  $x$  ismeretlent is természetesen az egész számok körében keressük):

$$\left. \begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{n_k} \end{aligned} \right\}$$

### 3.26. Megjegyzés.

A 3.18. Tétel segítségével a kongruenciarendszerbeli kongruenciákat külön-külön megoldhatjuk (ha van megoldásuk), és így a kongruenciarendszert a következő alakra hozhatjuk:

$$\left. \begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \right\} (*)$$

## Lineáris kongruenciarendszerek

### 3.27. Tétel.

A (\*) lineáris kongruenciarendszer  $k = 2$  esetén pontosan akkor oldható meg, ha  $\text{Inko}(m_1, m_2) \mid c_1 - c_2$ .

### 3.28. Tétel.

A (\*) lineáris kongruenciarendszer akkor és csak akkor oldható meg, ha bármely két kongruenciából álló részszeresere megoldható, azaz

$$\forall i, j: \text{Inko}(m_i, m_j) \mid c_i - c_j.$$

Speciálisan, páronként relatív prím modulusok esetén mindig van megoldás.

### 3.29. Tétel.

Ha a (\*) lineáris kongruenciarendszernek van megoldása, akkor megoldásai egyetlen mod  $[m_1, m_2, \dots, m_k]$  maradékosztályt alkotnak.

$$\left. \begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \right\} (*)$$

## Kínai maradéktétel

### 3.30. Tétel (kínai maradéktétel).

Tegyük fel, hogy az  $m_1, m_2, \dots, m_k$  modulusok páronként relatív prímek, jelölje a szorzatukat  $M$ , továbbá legyen  $M_i = \frac{M}{m_i}$  ( $i = 1, 2, \dots, k$ ).

Jelölje  $z_i$  az  $M_i z_i \equiv 1 \pmod{m_i}$  segédkongruencia egy megoldását ( $i = 1, \dots, k$ ).

Ekkor a (\*) lineáris kongruenciarendszer megoldása:

$$x \equiv \sum_{i=1}^k c_i M_i z_i \pmod{M}.$$

$$\left. \begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \right\} (*)$$



### 3.31. Következmény.

Ha  $m \perp n$ , akkor az alábbi  $\beta$  leképezés bijektív:

$$\beta: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, \bar{x} \mapsto (x \pmod{m}, x \pmod{n}).$$

### Bizonyítás.

A  $\beta$  leképezés bijektivitása azt jelenti, hogy tetszőleges  $a, b \in \mathbb{Z}$  esetén pontosan egy olyan  $\bar{x} \in \mathbb{Z}_{mn}$  létezik, amelyre

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

A kínai maradéktétel szerint ennek a kongruenciarendszernek valóban létezik megoldása (szürjektív), azt pedig már korábban láttuk, hogy a megoldás modulo  $\text{lkk}(m, n) = mn$  egyértelműen meghatározott (injektivitás).  $\square$

## Nevezetes számelméleti függvények

### 4.1. Definíció.

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

### 4.2. Definíció.

Néhány nevezetes számelméleti függvény:

▶  $\tau(n) = \sum_{d|n} 1$  —  $n$  pozitív osztóinak száma;

▶  $\sigma(n) = \sum_{d|n} d$  —  $n$  pozitív osztóinak összege;

▶  $\text{id}(n) = n$ ;

▶  $\mathbf{1}(n) = 1$ ;

▶  $\delta(n) = \begin{cases} 1, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1. \end{cases}$

## Gyenge multiplikatívitas

### 4.3. Definíció.

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

$$a \perp b \implies f(ab) = f(a) \cdot f(b).$$

### 4.4. Tétel.

Egy  $f$  számelméleti függvény akkor és csak akkor gyengén multiplikatív, ha  $f(1) = 1$  és tetszőleges páronként különböző  $p_1, \dots, p_n$  prímszámok és  $\alpha_1, \dots, \alpha_n$  pozitív kitevők esetén

$$f(p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n}) = f(p_1^{\alpha_1}) \cdot \dots \cdot f(p_n^{\alpha_n}).$$

### 4.5. Tétel.

A  $\tau, \sigma, \text{id}, \mathbf{1}, \delta$  számelméleti függvények gyengén multiplikatívak.

## Képletek

### 4.6. Tétel.

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

$$\tau(n) = \prod_{i=1}^k (\alpha_i + 1);$$

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

## Tökéletes számok

### 4.7. Definíció.

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

### 4.8. 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.

### 4.9. Definíció.

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

### 4.10. Megjegyzés.

Abból, hogy  $n$  prím, még nem következik, hogy  $M_n$  is az, például  $M_{11}$  nem prím. 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 (2016. szeptember 7.) ismert legnagyobb prímszám is Mersenne-prím:  $M_{74207281}$ , ami tízes számrendszerben 22 338 618 számjegyből áll.

## Mersenne-prímek

$p$	$M_p = 2^p - 1$	$2^{p-1} (2^p - 1)$	
2	3	6	ókori görögök
3	7	28	ókori görögök
5	31	496	ókori görögök
7	127	8128	ókori görögök
13	8 191	3 355 036	1456
17	131 071	8 589 869 056	1588, Cataldi
19	524 287	137 438 691 328	1588, Cataldi
31	2 147 483 647	2 305 843 008 139 952 128	1772, Euler
61	~ 2 trillió	~ 2 szextillió	1883, Pervushin
89	27-jegyű szám	54-jegyű szám	1911, Powers
107	33-jegyű szám	65-jegyű szám	1914, Powers
127	39-jegyű szám	77-jegyű szám	1876, Lucas
⋮	⋮	⋮	⋮
74 207 281	22 338 618-jegyű szám	44 677 235-jegyű szám	2016, GIMPS

## Fermat-prímek

### 4.11. Állítás.

Minden  $n \in \mathbb{N}$  esetén

$$2^n + 1 \text{ prím szám} \implies n \text{ kettőhatvány.}$$

### 4.12. Definíció.

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

### 4.13. Megjegyzés.

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 az első öt).

## Az Euler-féle $\varphi$ -függvény

### 4.14. Definíció.

Jelöljük  $\varphi(m)$ -mel az  $m$ -nél nem nagyobb természetes számok közül azoknak a számát, amelyek  $m$ -hez relatív prímekek:

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

Az így kapott függvényt **Euler-féle  $\varphi$  függvénynek** nevezzük. Tömörebben:

$$\varphi: \mathbb{N} \rightarrow \mathbb{N}, m \mapsto |\mathbb{Z}_m^*|.$$

### Példa.

$$\varphi(5) = |\{1, 2, 3, 4\}| = 4$$

$$\varphi(6) = |\{1, 5\}| = 2$$

$$\varphi(10) = |\{1, 3, 7, 9\}| = 4$$

$$\varphi(81) = |\{1, 2, 4, 5, 7, 8, \dots, 76, 77, 79, 80\}| = 81 - 27 = 54$$

$$\varphi(1000) = 1000 - 500 - 200 + 100 = 400$$

## Maradékrendszerek

### 4.15. Definíció.

Modulo  $m$  **teljes maradékrendszernek** nevezzük egész számok egy olyan rendszerét, amely minden mod  $m$  maradékosztályból pontosan egy elemet tartalmaz.

### 4.16. Állítás.

Ha  $a, c_1, c_2, \dots, c_m$  egész számok teljes maradékrendszert alkotnak modulo  $m$ , és  $a, b \in \mathbb{Z}, a \perp m$ , akkor  $ac_1 + b, ac_2 + b, \dots, ac_m + b$  is teljes maradékrendszer modulo  $m$ .

### 4.17. Definíció.

Modulo  $m$  **redukált maradékrendszernek** nevezzük egész számok egy olyan rendszerét, amely minden mod  $m$  redukált maradékosztályból pontosan egy elemet tartalmaz.

### 4.18. Állítás.

Ha  $a, c_1, c_2, \dots, c_{\varphi(m)}$  egész számok redukált maradékrendszert alkotnak modulo  $m$ , és  $a \in \mathbb{Z}, a \perp m$ , akkor  $ac_1, ac_2, \dots, ac_{\varphi(m)}$  is redukált maradékrendszer modulo  $m$ .

## Gyenge multiplikatívitas

### 4.19. Tétel.

Az Euler-féle  $\varphi$  függvény gyengén multiplikatív.

### Bizonyítás.

Tfh.  $m$  és  $n$  relatív prímekek, és tekintsük a „birkás” bijekciót:

$$\beta: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, \bar{x} \mapsto (x \bmod m, x \bmod n).$$

Világos, hogy minden  $x$ -re

$$x \perp mn \iff x \perp m \text{ és } x \perp n.$$

Ez azt jelenti, hogy  $\beta$  bijekciót létesít a  $\mathbb{Z}_{mn}^*$  és  $\mathbb{Z}_m^* \times \mathbb{Z}_n^*$  halmazok között, tehát ezek azonos elemszámúak:

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

## Képlet

### 4.20. Tétel.

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

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

### Bizonyítás.

A gyenge multiplikatívitas miatt elegendő prímtényezőkre igazolni az állítást:

$$\begin{aligned} \varphi(p^\alpha) &= |\{a : 1 \leq a \leq p^\alpha \text{ és } a \perp p^\alpha\}| \\ &= |\{a : 1 \leq a \leq p^\alpha \text{ és } p \nmid a\}| = p^\alpha - p^{\alpha-1}. \end{aligned}$$

## Az Euler–Fermat-tétel

### 4.21. Tétel (Euler–Fermat-tétel).

Ha  $a$  az  $a$  egész szám relatív prím az  $m$  modulushoz, akkor  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

### Bizonyítás.

Legyen  $c_1, c_2, \dots, c_{\varphi(m)}$  redukált maradékrendszer modulo  $m$ .

Mivel  $a \perp m$ , ezért  $ac_1, ac_2, \dots, ac_{\varphi(m)}$  is redukált maradékrendszer modulo  $m$ .

$$\begin{aligned} c_1 \cdot c_2 \cdot \dots \cdot c_{\varphi(m)} &\equiv ac_1 \cdot ac_2 \cdot \dots \cdot ac_{\varphi(m)} \pmod{m} \\ &\downarrow \\ c_1 \cdot c_2 \cdot \dots \cdot c_{\varphi(m)} &\equiv a^{\varphi(m)} \cdot c_1 \cdot c_2 \cdot \dots \cdot c_{\varphi(m)} \pmod{m} \\ &\downarrow \\ 1 &\equiv a^{\varphi(m)} \pmod{m} \end{aligned}$$

### 4.22. Következmény (kis Fermat-tétel).

Ha  $p$  prímszám és  $a$  nem osztható  $p$ -vel, akkor  $a^{p-1} \equiv 1 \pmod{p}$ .

Ha  $p$  prímszám, akkor minden  $a$  egész számra  $a^p \equiv a \pmod{p}$ .

## Az Euler–Fermat-tétel

### 4.23. Következmény.

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

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

### Bizonyítás.

Ha  $k_1 \equiv k_2 \pmod{\varphi(m)}$ , akkor  $k_2 = k_1 + \varphi(m) \cdot t$  alkalmas  $t$  egész számmal. Ezért

$$a^{k_2} \equiv a^{k_1 + \varphi(m) \cdot t} \equiv a^{k_1} \cdot (a^{\varphi(m)})^t \equiv a^{k_1} \cdot (1)^t \equiv a^{k_1} \pmod{m}.$$

## Konvolúció

### 4.24. Definíció.

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

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

### 4.25. Tétel.

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

### Bizonyítás.

A kommutativitás világos, az asszociativitáshoz pedig azt kell ellenőrizni, hogy

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

Mivel  $b > 1$  esetén  $\delta(b) = 0$ , ezért

$$(f * \delta)(n) = \sum_{ab=n} f(a) \delta(b) = \sum_{a=n, b=1} f(a) \delta(b) = f(n) \delta(1) = f(n). \quad \square$$

## Konvolúció

### 4.26. Tétel.

Gyengén multiplikatív számelméleti függvények konvolúciója is gyengén multiplikatív.

### Bizonyítás.

Tfh.  $f$  és  $g$  gyengén multiplikatív és  $a \perp b$ . Soroljuk fel  $a$  és  $b$  osztóit:

$$D_a = \{u_1, \dots, u_k\}, \quad D_b = \{v_1, \dots, v_\ell\}.$$

$$\begin{aligned} (f * g)(ab) &= \sum_{d|ab} f(d) \cdot g\left(\frac{ab}{d}\right) \\ &= \sum_{\substack{i=1, \dots, k \\ j=1, \dots, \ell}} f(u_i v_j) \cdot g\left(\frac{a}{u_i} \frac{b}{v_j}\right) \\ &= \sum_{\substack{i=1, \dots, k \\ j=1, \dots, \ell}} f(u_i) f(v_j) \cdot g\left(\frac{a}{u_i}\right) g\left(\frac{b}{v_j}\right) \\ &= \sum_{i=1, \dots, k} f(u_i) g\left(\frac{a}{u_i}\right) \cdot \sum_{j=1, \dots, \ell} f(v_j) g\left(\frac{b}{v_j}\right) \\ &= (f * g)(a) \cdot (f * g)(b) \quad \square \end{aligned}$$

## Összegési függvény

### 4.27. Definíció.

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

### Jelölés.

Azt a tény, hogy  $F$  az  $f$  összegési függvénye gyakran egyszerűen csak  $f \rightarrow F$  jelöli.

### 4.28. Tétel.

Gyengén multiplikatív számelméleti függvény összegési függvénye is gyengén multiplikatív.

### Bizonyítás.

$$\left. \begin{array}{l} f \text{ gyengén multiplikatív} \\ \mathbf{1} \text{ gyengén multiplikatív} \end{array} \right\} \implies F = f * \mathbf{1} \text{ is gyengén multiplikatív} \quad \square$$

## Összegési függvény

### 4.29. Tétel.

A tanult nevezetes számelméleti függvények között fennállnak az alábbi összefüggések:

$$\delta \rightarrow \mathbf{1} \rightarrow \tau, \quad \varphi \rightarrow \text{id} \rightarrow \sigma.$$

### Bizonyítás.

Jelölje  $\Phi$  a  $\varphi$  függvény összegési függvényét. Mivel  $\varphi$  gyengén multiplikatív,  $\Phi$  is az (és persze id is), így elegendő a  $\Phi(n) \stackrel{?}{=} \text{id}(n)$  egyenlőséget prímszámokra ellenőrizni. Tetszőleges  $p$  prim és  $\alpha \in \mathbb{N}$  esetén

$$\begin{aligned} \Phi(p^\alpha) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^{\alpha-1}) + \varphi(p^\alpha) \\ &= 1 + (p-1) + (p^2-p) + \dots + (p^{\alpha-1} - p^{\alpha-2}) + (p^\alpha - p^{\alpha-1}) \\ &= p^\alpha = \text{id}(p^\alpha). \quad \square \end{aligned}$$

## A Möbius-féle $\mu$ -függvény

### 4.30. Definíció.

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

### 4.31. Megjegyzés.

Könnyű megmondolni, hogy egy szám akkor és csak akkor négyzetmentes, ha prímfelbontásában minden prim csak egyszer (azaz első hatványon) fordul elő.

### 4.32. Definíció.

**Möbius-függvények** nevezzük az alábbi képlettel definiált  $\mu$  számelméleti függvényt:

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

## A Möbius-féle $\mu$ -függvény

### 4.33. Tétel.

A Möbius-függvény összegési függvénye a  $\delta$  függvény, azaz  $\mu * \mathbf{1} = \delta$ .

### Bizonyítás.

Jelölje  $M$  a  $\mu$  függvény összegési függvényét. Mivel  $\mu$  gyengén multiplikatív,  $M$  is az (és persze  $\delta$  is), így elegendő az  $M(n) \stackrel{?}{=} \delta(n)$  egyenlőséget prímszámokra ellenőrizni. Tetszőleges  $p$  prim és  $\alpha \in \mathbb{N}$  esetén

$$\begin{aligned} M(p^\alpha) &= \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^{\alpha-1}) + \mu(p^\alpha) \\ &= 1 + (-1) + 0 + \dots + 0 + 0 \\ &= 0 = \delta(p^\alpha). \quad \square \end{aligned}$$

## Möbius-féle inverziós formula

### 4.34. Tétel (Möbius-féle megfordítási képlet).

Tetszőleges  $F$  számelméleti függvény esetén  $F$ -nek egyetlen megfordítási függvénye van, mégpedig  $F * \mu$ .

Másképpen fogalmazva  $f \rightarrow F$  akkor és csak akkor áll fenn, ha  $f = F * \mu$ .

Részletesebben: tetszőleges  $f, F$  számelméleti függvények esetén

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

### Bizonyítás.

Tetszőleges  $f, F$  számelméleti függvény esetén  $F = f * \mathbf{1} \stackrel{?}{\iff} f = F * \mu$ .

$\implies$ : Tfh.  $F = f * \mathbf{1}$ . „Konvolváljuk be” az egyenlőség mindkét oldalát  $\mu$ -vel:

$$F = f * \mathbf{1} \implies F * \mu = (f * \mathbf{1}) * \mu = f * (\mathbf{1} * \mu) = f * \delta = f.$$

$\impliedby$ : Tfh.  $f = F * \mu$ . „Konvolváljuk be” az egyenlőség mindkét oldalát  $\mathbf{1}$ -gyel:

$$f = F * \mu \implies f * \mathbf{1} = (F * \mu) * \mathbf{1} = F * (\mu * \mathbf{1}) = F * \delta = F.$$

## Möbius-féle inverziós formula

### 4.35. Következmény.

Gyengén multiplikatív számelméleti függvény megfordítási függvénye is gyengén multiplikatív.

### Bizonyítás.

$$\left. \begin{array}{l} F \text{ gyengén multiplikatív} \\ \mu \text{ gyengén multiplikatív} \end{array} \right\} \implies f = F * \mu \text{ is gyengén multiplikatív} \quad \square$$

## Diofantoszi egyenlet polinomgyűrűben

Test fölötti polinomokra ugyanúgy elvégezhető a maradékos osztás és az arra épülő euklideszi algoritmus, akárcsak az egész számokra. Az előbbi tételek (és azok bizonyítása) szinte szó szerint lemásolhatók (HF végiggondolni!). Íme a diofantoszi egyenletekről szóló tétel polinomos megfelelője:

### 5.1. 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  $\text{Inko}(f, g) \mid h$ .

Ha  $(u_0, v_0)$  egy megoldás, akkor bármely  $t \in T[x]$  esetén az alábbi  $(u_t, v_t)$  pár is megoldás, továbbá minden megoldás előáll ilyen alakban a  $t$  polinom alkalmas megválasztásával:

$$\begin{aligned} u_t &= u_0 + \frac{g}{\text{Inko}(f, g)} \cdot t; \\ v_t &= v_0 - \frac{f}{\text{Inko}(f, g)} \cdot t. \end{aligned}$$

## Diofantoszi egyenlet polinomgyűrűben

### Példa.

Oldjuk meg az  $fu + gv = \text{Inko}(f, g)$  egyenletet az  $\mathbb{R}[x]$  polinomgyűrűben, ahol

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

$$f = (x+1) \cdot g + 2x^2 + 4x + 6$$

$$g = (x-1) \cdot (x^2 + 2x + 3) + 0$$

Tehát  $\text{Inko}(f, g) \sim x^2 + 2x + 3$ .

Fejezzük ki a legnagyobb közös osztót  $f$  és  $g$  segítségével:

$$x^2 + 2x + 3 = \frac{1}{2}(f - (x+1) \cdot g) = \frac{1}{2} \cdot f + \left(-\frac{1}{2}x - \frac{1}{2}\right) \cdot g$$

Az egyenlet egy megoldása:  $u_0 = \frac{1}{2}, \quad v_0 = -\frac{1}{2}x - \frac{1}{2}$ .



## Diofantoszi egyenlet polinomgyűrűben

Ha  $p$  prím, akkor  $\mathbb{Z}_p$  test, és így beszélhetünk  $\mathbb{Z}_p$  feletti polinomokról. Ezekkel ugyanúgy (vagy könnyebben!) lehet számolni, mint számtest feletti polinomokkal.

**Példa.**

Oldja meg az  $fu + gv = \bar{1}$  egyenletet az  $\mathbb{Z}_5[x]$  polinomgyűrűben, ahol

$$f = x^2 + \bar{3}x + \bar{1}, \quad g = x^3 + \bar{2}x^2 + \bar{4}x + \bar{2}.$$

$$x^3 + \bar{2}x^2 + \bar{4}x + \bar{2} = (x + \bar{4}) \cdot (x^2 + \bar{3}x + \bar{1}) + x + \bar{3}$$

$$x^2 + \bar{3}x + \bar{1} = x \cdot (x + \bar{3}) + \bar{1}$$

$$x + \bar{3} = (x + \bar{3}) \cdot \bar{1} + \bar{0}$$

Fejtsük ki  $\bar{1}$ -et  $f$  és  $g$  segítségével:

$$\bar{1} = f - x \cdot (x + \bar{3}) = f - x \cdot (g - (x + \bar{4}) \cdot f) = (x^2 + \bar{4}x + \bar{1}) \cdot f - x \cdot g$$

Az egyenlet egy megoldása:  $u_0 = x^2 + \bar{4}x + \bar{1}, \quad v_0 = -x.$

## Polinomgyűrű faktortestei

Ha  $T$  egy test (például  $T = \mathbb{Q}, \mathbb{R}, \mathbb{C}$  vagy  $\mathbb{Z}_p$ ) és  $m \in T[x]$ , akkor a modulo  $m$  kongruencia és a modulo  $m$  maradékosztályok ugyanúgy definiálhatóak, mint az egész számok körében, és hasonló tulajdonságokkal rendelkeznek (HF végig-gondolni!). A maradékosztály-gyűrűt itt  $T[x] / (m)$  jelöli.

**5.2. Tétel.**

Ha  $m$  egy  $n$ -edfokú polinom a  $T$  test felett, akkor a  $T[x] / (m)$  maradékosztály-gyűrű kommutatív egységelemes gyűrű, melynek elemei egyértelműen felírhatók az alábbi alakban:

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

**5.3. Tétel.**

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

**5.4. Következmény.**

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

## Egy fontos maradékosztálytest

Az  $\mathbb{R}[x] / (x^2 + 1)$  maradékosztály-gyűrű test, mert  $x^2 + 1$  irreducibilis a valós számok teste felett. Mik az elemei ennek a testnek, és hogyan kell számolni velük?

► Elemek: Az  $\mathbb{R}[x] / (x^2 + 1)$  test minden eleme egyértelműen felírható a következő alakban:

$$\overline{a + bx} \quad (a, b \in \mathbb{R}).$$

► Összeadás:  $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}.$

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

Ez szinte szó szerint ugyanaz, mint a komplex számok teste:  $\mathbb{R}[x] / (x^2 + 1) \cong \mathbb{C}.$

**5.5. Megjegyzés.**

A fenti példához hasonlóan minden  $m \in T[x]$  irreducibilis polinomnak lehet „gyököt csinálni”: a  $T[x] / (m)$  maradékosztálytest egy olyan kibővítése a  $T$  testnek, amelyben  $m$ -nek van gyöke.

## Egy véges test

**Példa.**

Számoljunk a  $\mathbb{Z}_2[x] / (x^3 + x + \bar{1})$  testben! Ennek 8 eleme van:

$$\bar{0}, \bar{1}, \bar{x}, \overline{x + \bar{1}}, \overline{x^2}, \overline{x^2 + \bar{1}}, \overline{x^2 + x}, \overline{x^2 + x + \bar{1}}.$$

$$\overline{x + \bar{1} + x^2 + x} = \overline{x^2 + \bar{2}x + \bar{1}} = \overline{x^2 + \bar{1}} \quad (\text{semmi vész})$$

$$\overline{x + \bar{1} \cdot x^2 + x} = \overline{x^3 + \bar{2}x^2 + x} = \overline{x^3 + x} = \bar{1} \quad (\text{redukció mod } x^3 + x + \bar{1})$$

## A nyolcelemű test művelet táblázatai

+	0	1	a	a+1	a <sup>2</sup>	a <sup>2</sup> +1	a <sup>2</sup> +a	a <sup>2</sup> +a+1
0	0	1	a	a+1	a <sup>2</sup>	a <sup>2</sup> +1	a <sup>2</sup> +a	a <sup>2</sup> +a+1
1	a	0	a+1	a	a <sup>2</sup> +1	a <sup>2</sup>	a <sup>2</sup> +a+1	a <sup>2</sup> +a
a	a+1	a	0	1	a <sup>2</sup> +a	a <sup>2</sup> +a+1	a <sup>2</sup>	a <sup>2</sup> +1
a+1	a <sup>2</sup>	a <sup>2</sup> +1	a <sup>2</sup> +a	a <sup>2</sup> +a+1	0	1	a	a+1
a <sup>2</sup>	a <sup>2</sup> +1	a <sup>2</sup>	a <sup>2</sup> +a+1	a <sup>2</sup> +a	1	0	a+1	a
a <sup>2</sup> +1	a <sup>2</sup> +a	a <sup>2</sup> +a+1	a <sup>2</sup>	a <sup>2</sup> +1	a	a+1	0	1
a <sup>2</sup> +a	a <sup>2</sup> +a+1	a <sup>2</sup> +a	a <sup>2</sup> +1	a <sup>2</sup>	a+1	a	1	0

·	0	1	a	a+1	a <sup>2</sup>	a <sup>2</sup> +1	a <sup>2</sup> +a	a <sup>2</sup> +a+1
0	0	0	0	0	0	0	0	0
1	0	1	a	a+1	a <sup>2</sup>	a <sup>2</sup> +1	a <sup>2</sup> +a	a <sup>2</sup> +a+1
a	0	a	a <sup>2</sup>	a <sup>2</sup> +a	a+1	1	a <sup>2</sup> +a+1	a <sup>2</sup> +1
a+1	0	a+1	a <sup>2</sup> +a	a <sup>2</sup> +1	a <sup>2</sup> +a+1	a <sup>2</sup>	1	a
a <sup>2</sup>	0	a <sup>2</sup>	a+1	a <sup>2</sup> +a+1	a <sup>2</sup> +a	a	a <sup>2</sup> +1	1
a <sup>2</sup> +1	0	a <sup>2</sup> +1	1	a <sup>2</sup>	a	a <sup>2</sup> +a+1	a+1	a <sup>2</sup> +a
a <sup>2</sup> +a	0	a <sup>2</sup> +a	a <sup>2</sup> +a+1	1	a <sup>2</sup> +1	a+1	a	a <sup>2</sup>
a <sup>2</sup> +a+1	0	a <sup>2</sup> +a+1	a <sup>2</sup> +1	a	1	a <sup>2</sup> +a	a <sup>2</sup>	a+1

## Számolás Q[x] faktortesteiben

**Példa.**

Határozzuk meg a  $K = \mathbb{Q}[x] / (x^3 - 7)$  testben a  $\overline{2 - x}$  elem multiplikatív inverzét.

$K$  elemei  $\overline{ax^2 + bx + c}$  ( $a, b, c \in \mathbb{Q}$ ) alakúak, ilyen alakban szeretnénk az  $\bar{u} = \overline{2 - x}^{-1}$  elemet is megkapni.

$$\overline{2 - x}^{-1} = \bar{u} \iff \overline{2 - x} \cdot \bar{u} = \bar{1}$$

$$\iff (2 - x)u \equiv 1 \pmod{x^3 - 7}$$

$$\iff \exists v \in \mathbb{Q}[x] : (2 - x)u = 1 + (x^3 - 7)v$$

$$\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7}$$

$$\iff \bar{u} = \overline{x^2 + 2x + 4}$$

Tehát  $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}.$



**Példa (folyt.).**

Az előző számolás eredménye összefoglalva:

$$(2 - x)(x^2 + 2x + 4) = 1 + (x^3 - 7) \cdot (\dots \text{valami polinom} \dots).$$

Írjunk  $x$  helyébe  $\sqrt[3]{7}$ -et:

$$(2 - \sqrt[3]{7})(\sqrt[3]{49} + 2\sqrt[3]{7} + 4) = 1 + (7 - 7) \cdot (\dots \text{valami szám} \dots).$$

Tehát azt kapjuk, hogy

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Ezzel a módszerrel (lényegében az euklideszi algoritmus) lehet bonyolult nevezőket gyökteleníteni.

## Emlékeztető

**Definíció vagy tétel?**

Legyen  $T$  egy test és  $p \in T[x]$ . A  $p$  polinom **irreducibilis**  $T$  felett, ha legalább elsőfokú, és nem bontható deg  $p$ -nél kisebb fokszámú polinomok szorzatára:

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

**Vigyázat!**

Gyűrűk felett ez általában nem igaz! Például a  $p = 2x \in \mathbb{Z}[x]$  polinom nem irreducibilis  $\mathbb{Z}$  felett, mert a  $p = 2 \cdot x$  felbontás itt nem triviális (miért?).

**5.6. Tétel.**

- Az elsőfokú polinomok bármely test felett irreducibilisek.
- Ha  $f \in T[x]$  irreducibilis és  $\deg f \geq 2$ , akkor  $f$ -nek nincs gyöke  $T$ -ben.
- Ha  $f \in T[x]$  és  $2 \leq \deg f \leq 3$ , akkor  $f$  pontosan akkor irreducibilis, ha nincs gyöke  $T$ -ben.

**5.7. Tétel.**

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

## Irreducibilitás vs. gyökök

Összefoglalva:

Az

irreducibilis  $\implies$  nincs gyöke

implikáció igaz a legalább másodfokú polinomokra. **Elsőfokúakra nem igaz:** azok mindig irreducibilisek és mindig van gyökük!

A

nincs gyöke  $\implies$  irreducibilis

implikáció igaz a másod- és harmadfokú polinomokra, **de magasabbfokúakra nem!**

**Példa.**

Az  $f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$  polinomnak nincs valós gyöke, mégsem irreducibilis  $\mathbb{R}$  felett:

$$f = (x^2 + 1)(x^2 + 1).$$

## Irreducibilitás vs. gyökök

Legalább negyedfokú polinomok esetén

### A GYÖKNÉLKÜLISÉGBŐL

**NEM NEM NEM NEM NEM NEM NEM**  
**KÖVETKEZIK**  
**AZ IRREDUCIBILITÁS!!!**

## Egy irreducibilis faktorizáció

Példa.

Bontsuk irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = x^6 + 3x^4 - x^3 + 2x^2 + x - 1 \in \mathbb{Z}_5[x].$$

Mivel az alaptestnek csak öt eleme van, egyenként kipróbálhatjuk, hogy gyöke-e valamelyik az  $f$  polinomnak.

Amelyik igen, annál a Horner-módszerrel megállapítjuk a multiplicitást, és leválasztjuk a gyöktényezőket:

$$f = (x - 1)^2 (x - 3) (x - 4) (x^2 + 4x + 2).$$

Az  $x^2 + 4x + 2$  polinomnak nincs gyöke (ha lenne, megtaláltuk volna), és **csak másodfokú**, ezért irreducibilis.

(Ha negyed- vagy magasabb fokú polinom marad a gyöktényezők kiemelése után, akkor valami trükkre van szükség ...)

## Véges testek

5.8. Tétel.

Akkor és csak akkor létezik  $q$ -elemű test, ha  $q$  prímszám.

Bizonyítás helyett.

Bármely  $p$  prímszám és  $n$  pozitív egész szám esetén létezik  $n$ -edfokú irreducibilis polinom  $\mathbb{Z}_p$  felett (messze nem triviális!).

Ha  $f \in \mathbb{Z}_p[x]$  egy ilyen polinom, akkor  $T[x] / (f)$  egy  $p^n$ -elemű test.

Ha  $K$  egy véges test, akkor tartalmaz prím elemszámú résztestet (közel sem triviális!).

Ha  $T$  egy  $p$ -elemű részteste  $K$ -nak, akkor  $K$  vektorteret alkot  $T$  felett.

Ha ez a vektortér  $n$ -dimenziós, akkor  $K \cong T^n$ , ezért  $|K| = p^n$ .  $\square$

A  $q$ -elemű testet (mely izomorfia erejéig egyértelműen meghatározott), Galois tiszteletére  $\text{GF}(q)$  jelöli (Galois Field).

## Véges testek

Példa.

- ▶ kételemű test:  $\text{GF}(2) \cong \mathbb{Z}_2$
- ▶ háromelemű test:  $\text{GF}(3) \cong \mathbb{Z}_3$
- ▶ négyelemű test:  $\text{GF}(4) \cong \mathbb{Z}_2[x] / (x^2 + x + 1)$
- ▶ ötelemű test:  $\text{GF}(5) \cong \mathbb{Z}_5$
- ▶ hatelemű test: nincs!
- ▶ hételemű test:  $\text{GF}(7) \cong \mathbb{Z}_7$
- ▶ nyolcelemű test:  $\text{GF}(8) \cong \mathbb{Z}_2[x] / (x^3 + x + 1)$
- ▶ kilencelemű test:  $\text{GF}(9) \cong \mathbb{Z}_3[x] / (x^2 + 1) = \{a + bi : a, b \in \mathbb{Z}_3\}$
- ▶ tízelemű test: nincs!
- ▶ ...

## Emlékeztető

5.9. Definíció.

Az  $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$  polinom  $c \in T$  helyen vett **helyettesítési értékén** az  $f(c) = a_n c^n + \dots + a_1 c + a_0 \in T$  elemet értjük.

Az  $f \in T[x]$  polinomhoz tartozó **polinomfüggvény** pedig nem más, mint az

$$f: T \rightarrow T, c \mapsto f(c)$$

leképezés.

A polinomot és a hozzá tartozó polinomfüggvényt ugyanúgy jelöljük; a szövegkörnyezetből kiderül, hogy mikor melyikről van szó. Ha polinomfüggvényekről van szó, akkor  $x$ -et **változónak** nevezzük (nem pedig határozatlanak).

## Polinom vs. polinomfüggvény

Példa.

Az  $f = x^3 \in \mathbb{Z}_3[x]$  polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \rightarrow \mathbb{Z}_3, \bar{0} \mapsto \bar{0}^3 = \bar{0}, \bar{1} \mapsto \bar{1}^3 = \bar{1}, \bar{2} \mapsto \bar{2}^3 = \bar{2}.$$

A  $g = x \in \mathbb{Z}_3[x]$  polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \rightarrow \mathbb{Z}_3, \bar{0} \mapsto \bar{0}, \bar{1} \mapsto \bar{1}, \bar{2} \mapsto \bar{2}.$$

Látjuk, hogy  $f$ -hez és  $g$ -hez ugyanaz a polinomfüggvény tartozik (nevezetesen az identikus függvény), noha  $f$  és  $g$  két különböző polinom. Ezért nagyon fontos, hogy

**NE KEVERJÜK A POLINOMOT  
A POLINOMFÜGGVÉNNYEL!!!**

## Polinom vs. polinomfüggvény

Általánosabban, ha  $T$  egy  $q$ -elemű test, akkor

- ▶ a  $T \rightarrow T$  leképezések száma  $q^q$ , míg
- ▶  $T$  feletti polinomból végtelen sok van,

így végtelen sok különböző polinomhoz tartozik ugyanaz a polinomfüggvény. Ezért nagyon fontos, hogy

**NE KEVERJÜK A POLINOMOT  
A POLINOMFÜGGVÉNNYEL!!!**

## Irreducibilitás különböző testek felett

Példa.

Az  $f = x^2 + 1 \in \mathbb{R}[x]$  polinom irreducibilis, de ugyanez a polinom  $\mathbb{C}[x]$ -ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$ .

Példa.

Az  $f = x^2 - 2 \in \mathbb{Q}[x]$  polinom irreducibilis, de ugyanez a polinom  $\mathbb{R}[x]$ -ben már felbomlik:  $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ .

(És persze  $\mathbb{C}[x]$ -ben is felbomlik.)

Általában, minél nagyobb az alaptest, annál „több esélye” van egy polinomnak felbomlani.

Ha  $T$  részteste  $K$ -nak és  $f \in T[x]$ , akkor

$$f \text{ irreducibilis } K \text{ felett} \not\Rightarrow f \text{ irreducibilis } T \text{ felett.}$$

Emlékeztető

A komplex számtest felett csak az elsőfokú polinomok irreducibilisek, a valós számtest felett pedig csak az elsőfokúak és a negatív diszkriminánsú másodfokúak.

## Irreducibilis faktorizáció a racionális számtest felett

Példa.

Határozza meg az  $f = x^6 - 27$  polinom irreducibilis felbontását  $\mathbb{Q}$  felett.

A polinom komplex gyökei:  $\sqrt{3}, -\sqrt{3}, \alpha, \bar{\alpha}, \beta, \bar{\beta}$ , ahol

$$\alpha = \sqrt{3} \cdot \left( \frac{1}{2} + \frac{\sqrt{3}}{2}i \right) = \frac{\sqrt{3}}{2} + \frac{3}{2}i, \quad \beta = \sqrt{3} \cdot \left( -\frac{1}{2} + \frac{\sqrt{3}}{2}i \right) = -\frac{\sqrt{3}}{2} + \frac{3}{2}i$$

A  $\mathbb{C}$  feletti felbontás (azaz a gyöktényezőző alak):

$$f = (x - \sqrt{3})(x + \sqrt{3})(x - \alpha)(x - \bar{\alpha})(x - \beta)(x - \bar{\beta}).$$

Az  $\mathbb{R}$  feletti felbontás:

$$f = (x - \sqrt{3})(x + \sqrt{3})(x^2 - 2\text{Re}\alpha \cdot x + |\alpha|^2)(x^2 - 2\text{Re}\beta \cdot x + |\beta|^2) \\ = (x - \sqrt{3})(x + \sqrt{3})(x^2 - \sqrt{3}x + 3)(x^2 + \sqrt{3}x + 3).$$

A  $\mathbb{Q}$  feletti felbontás:

$$f = (x^2 - 3)(x^4 + 3x^2 + 9).$$

## Felbontás $\mathbb{Q}$ , illetve $\mathbb{Z}$ felett

### 5.10. 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:

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

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

Bizonyítás.



### 5.11. 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 irreducibilis  $\mathbb{Z}$  felett, ha irreducibilis  $\mathbb{Q}$  felett.

□

## Kronecker módszere

### Példa.

Irreducibilis-e az  $f = x^4 - 4x^3 + 7x^2 - 6x + 3 \in \mathbb{Q}[x]$  polinom?

Tfh.  $f = g \cdot h$ , ahol  $g, h \in \mathbb{Z}[x]$  és  $0 < \deg g \stackrel{\text{AMN}}{\leq} \deg h < n$ .

Ekkor  $\deg g \leq 2$ , és minden  $k \in \mathbb{Z}$  esetén  $g(k) \mid f(k)$ . Például

$$a := g(0) \mid f(0) = 3, \quad b := g(1) \mid f(1) = 1, \quad c := g(2) \mid f(2) = 3.$$

Tehát az  $(a, b, c)$  számhármásra 32 lehetőség van:

$$(a, b, c) \in \{-3, -1, 1, 3\} \times \{-1, 1\} \times \{-3, -1, 1, 3\}.$$

Mind a 32 esetben egyértelműen meg tudjuk határozni a  $g$  polinomot Lagrange-interpolációval.

Ha valamelyik osztja  $f$ -et, akkor kapunk egy nemtriviális felbontást; ha egyik se osztja  $f$ -et, akkor  $f$  irreducibilis.

$$(a, b, c) = (1, 1, 3) \rightsquigarrow g = x^2 - x + 1 \rightsquigarrow f = (x^2 - x + 1)(x^2 - 3x + 3)$$

## Irreducibilis polinomok $\mathbb{Q}$ felett

### 5.14. Következmény.

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

Bizonyítás.

$$x^n + 2$$

□

Érdekes ezt összehasonlítani a komplex és a valós számtest esetével:

- ▶  $\mathbb{C}$  felett csak az elsőfokúak,
- ▶  $\mathbb{R}$  felett csak az elsőfokúak és bizonyos másodfokúak

irreducibilisek.

Még szerencse, hogy a racionális számok testének már nincs valódi részteste! (miért?)

## VIZSGÁN KÉRDEZNI FOGOM!

### 5.15. 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 következzezz inkább a tétel „tükrképe”.

### 5.16. Tétel (müihétik izétildidubertni elét-nietzenziE-nnsmenöbZ).

Legyen  $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ . Ha létezik olyan  $p$  prímszám amelyre  $p \mid a_n, p \mid a_{n-1}, \dots, p \mid a_1, p \nmid a_0$ , akkor  $f$  irreducibilis a racionális számok teste felett.

## Schönemann–Eisenstein

### 5.12. Definíció.

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

Jelölés.

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

Példa.

$$3 \parallel 12 \text{ de } 2 \nparallel 12$$

### 5.13. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium).

Legyen  $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ . Ha létezik olyan  $p$  prímszám amelyre

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

akkor  $f$  irreducibilis a racionális számok teste felett.

## Racionális gyökök

### 5.17. Tétel (Rolle tétele).

Legyen  $f = a_n x^n + \dots + a_1 x + a_0$  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  $\text{Inko}(p, q) = 1$ ), akkor

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

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Természetesen a fenti nyíl nem fordítható meg:  $q \mid a_n$  és  $p \mid a_0$  nem garantálja, hogy  $\frac{p}{q}$  gyöke  $f$ -nek.

A Rolle-tételben „az a jó”, hogy egy véges halmazt ad meg, amelyben az összes racionális gyököt megtalálhatjuk (ha van egyáltalán racionális gyök).

## Racionális gyökök

Bizonyítás.

Tegyük fel, hogy  $\frac{p}{q}$  gyöke  $f$ -nek ( $\text{Inko}(p, q) = 1$ ).

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

Szorozzunk be  $q^n$ -nel:

$$0 = \underbrace{a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1}}_{p \mid} + \underbrace{a_0 q^n}_{p \mid} \implies p \mid a_0$$

Hasonlóan:

$$q \mid a_n \iff q \mid \underbrace{a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n}_{q \mid} = 0 \quad \square$$

## Irreducibilis felbontás $\mathbb{Q}$ felett

Példa.

Bontsuk  $\mathbb{Q}$  felett irreducibilis polinomok szorzatára az alábbi polinomot:

$$f = 2x^7 + 5x^6 + 4x^5 + 13x^4 + 54x^3 + 84x^2 + 54x + 12$$

Racionális gyök csak  $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}$  lehet.

Ezek közül  $-1$  és  $-\frac{1}{2}$  valóban gyök. Horner-módszerrel leválasztva a gyökényezőket azt kapjuk, hogy

$$f = \left(x + \frac{1}{2}\right)(x+1)^2(2x^4 + 12x + 24) = (2x+1)(x+1)^2(x^4 + 6x + 12).$$

A **kék** polinom irreducibilis  $\mathbb{Q}$  felett (Schönemann–Eisenstein,  $p = 3$ ).

## Elemi törtkre bontás a racionális számok körében

### 5.18. Definíció.

**Elemi törteknek** nevezzük a  $\frac{c}{p^k}$  alakú törteteket, ahol  $p$  prímszám,  $k$  és  $c$  pozitív egészek, és  $c < p$ .

### 5.19. Tétel.

Minden racionális szám felírható egy egész szám és elemi törtök összegeként.

Bizonyítás (vázlat).

Három „trükkre” lesz szükségünk:

1. Tetszőleges  $a, b, c \in \mathbb{Z}$  ( $a, b \neq 0$ ) esetén

$$a \perp b \implies \exists x, y \in \mathbb{Z} : \frac{c}{ab} = \frac{x}{a} + \frac{y}{b}.$$

Ezt ismételten alkalmazva minden racionális számot fel tudunk bontani prímhatalvány nevezőjű törtök összegére. Például:

$$\frac{157}{72} = \frac{157}{2^3 \cdot 3^2} = \frac{x}{2^3} + \frac{y}{3^2} = \frac{21}{2^3} + \frac{-4}{3^2}.$$

## Elemi törtre bontás a racionális számok körében

### Bizonyítás (folyt.)

2. Maradékos osztás segítségével leválasztva a törték egészrészét, elérhetjük, hogy minden törtünk  $\frac{c}{p^k}$  alakú legyen, ahol  $0 < c < p^k$ :

$$\frac{157}{72} = \frac{21}{2^3} + \frac{-4}{3^2} = 2 + \frac{5}{2^3} + (-1) + \frac{5}{3^2} = 1 + \frac{5}{2^3} + \frac{5}{3^2}.$$

3. Minden  $\frac{c}{p^k}$  alakú törtben a nevezőt felírjuk  $p$ -alapú számrendszerben, és „számjegyenként szétszedjük”:

$$\frac{5}{2^3} = \frac{101_2}{2^3} = \frac{2^2 + 1}{2^3} = \frac{2^2}{2^3} + \frac{1}{2^3} = \frac{1}{2} + \frac{1}{2^3};$$

$$\frac{5}{3^2} = \frac{12_3}{3^2} = \frac{3+2}{3^2} = \frac{3}{3^2} + \frac{2}{3^2} = \frac{1}{3} + \frac{2}{3^2}.$$

Tehát a végeredmény:

$$\frac{157}{72} = 1 + \frac{1}{2} + \frac{1}{2^3} + \frac{1}{3} + \frac{2}{3^2}.$$

## Polinomokra minden ugyanúgy megy

Tetszőleges  $T$  test esetén a  $T[x]$  polinomgyűrű elemeivel „ugyanúgy” lehet számolni, mint egész számokkal (maradékos osztás, euklideszi algoritmus), ezért az előbbi eljárás  $T$  feletti polinomokra is működik.

### 5.20. 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 törték halmazát  $T(x)$  jelöli.

### 5.21. 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:

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

## Elemi törtre bontás test feletti racionális törték körében

### 5.22. Tétel.

Tetszőleges  $T$  test felett minden racionális tört felírható egy polinom és elemi racionális törték összegeként.

### 5.23. Következmény.

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

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

alakú racionális tört összegeként.

### 5.24. Következmény.

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

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

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

alakú racionális tört összegeként.

## Elemi törtre bontás test feletti racionális törték körében

### Példa.

Bontsuk parciális törték összegére  $\mathbb{R}$  felett az  $\frac{1}{x^2+x}$  racionális törtet.

$$\frac{1}{x^2+x} = \frac{1}{x(x+1)} = \frac{A}{x} + \frac{B}{x+1} = \frac{A(x+1)+Bx}{x(x+1)} = \frac{(A+B)x+A}{x(x+1)}$$

$\Updownarrow$

$$A+B=0 \text{ és } A=1$$

$\Updownarrow$

$$A=1 \text{ és } B=-1$$

Tehát

$$\frac{1}{x^2+x} = \frac{1}{x} - \frac{1}{x+1}.$$

## Elemi törtre bontás test feletti racionális törték körében

### Példa.

Bontsuk parciális törték összegére  $\mathbb{R}$  felett a  $\frac{3x^2+2x+1}{x^7+2x^5+x^3}$  racionális törtet.

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{3x^2+2x+1}{x^3(x^4+2x^2+1)} = \frac{3x^2+2x+1}{x^3(x^2+1)^2} =$$

$$= \frac{A}{x} + \frac{B}{x^2} + \frac{C}{x^3} + \frac{Dx+E}{x^2+1} + \frac{Fx+G}{(x^2+1)^2} =$$

$$= \frac{Ax^2(x^2+1)^2 + Bx(x^2+1)^2 + C(x^2+1)^2 + (Dx+E)x^3(x^2+1) + (Fx+G)x^3}{x^3(x^2+1)^2} =$$

$$= \frac{(A+D)x^6 + (B+E)x^5 + (2A+C+D+F)x^4 + (2B+E+G)x^3 + (A+2C)x^2 + Bx + C}{x^3(x^2+1)^2}$$

$\Updownarrow$

$$A+D=0, \quad B+E=0, \quad 2A+C+D+F=0,$$

$$2B+E+G=0, \quad A+2C=3, \quad B=2, \quad C=1$$

## Elemi törtre bontás test feletti racionális törték körében

### Példa (folyt.).

A kapott hétismeretlenes lineáris egyenletrendszert megoldjuk:

$$A=1, \quad B=2, \quad C=1, \quad D=-1, \quad E=-2, \quad F=-2, \quad G=2.$$

Tehát

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{1}{x} + \frac{2}{x^2} + \frac{1}{x^3} + \frac{-x-2}{x^2+1} + \frac{-2x-2}{(x^2+1)^2}.$$

## Elemi törtre bontás test feletti racionális törték körében

### Példa.

Bontsuk parciális törték összegére  $\mathbb{C}$  felett a  $\frac{3x^2+2x+1}{x^7+2x^5+x^3}$  racionális törtet.

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{3x^2+2x+1}{x^3(x^2+1)^2} = \frac{3x^2+2x+1}{x^3(x+i)^2(x-i)^2} =$$

$$= \frac{A}{x} + \frac{B}{x^2} + \frac{C}{x^3} + \frac{D}{x+i} + \frac{E}{(x+i)^2} + \frac{F}{x-i} + \frac{G}{(x-i)^2}$$

$\Updownarrow$

$$A+D+F=0, \quad B-iD+E+iF+G=0, \quad 2A+C+D-2iE+F+2iG=0,$$

$$2B-iD-E+iF-G=0, \quad A+2C=3, \quad B=2, \quad C=1$$

## Elemi törtre bontás test feletti racionális törték körében

### Példa (folyt.).

A kapott hétismeretlenes lineáris egyenletrendszert megoldjuk:

$$A=1, \quad B=2, \quad C=1, \quad D=-\frac{1}{2}-\frac{3}{2}i, \quad E=\frac{1}{2}-\frac{1}{2}i, \quad F=-\frac{1}{2}+\frac{3}{2}i, \quad G=\frac{1}{2}+\frac{1}{2}i.$$

Tehát

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{1}{x} + \frac{2}{x^2} + \frac{1}{x^3} + \frac{-\frac{1}{2}-\frac{3}{2}i}{x+i} + \frac{\frac{1}{2}-\frac{1}{2}i}{(x+i)^2} + \frac{-\frac{1}{2}+\frac{3}{2}i}{x-i} + \frac{\frac{1}{2}+\frac{1}{2}i}{(x-i)^2}.$$

## Gyökök és együtthatók közötti összefüggés

Ha az  $f = x^2 + a_1x + a_0 \in \mathbb{C}[x]$  polinom gyökei  $\alpha_1$  és  $\alpha_2$ , akkor

$$x^2 + a_1x + a_0 = (x - \alpha_1)(x - \alpha_2) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2,$$

következésképp

$$-\alpha_1 = \alpha_1 + \alpha_2 \quad \text{és} \quad a_0 = \alpha_1\alpha_2.$$

Ha az  $f = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{C}[x]$  polinom gyökei  $\alpha_1, \alpha_2, \alpha_3$ , akkor

$$x^3 + a_2x^2 + a_1x + a_0 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) =$$

$$= x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3,$$

következésképp

$$-\alpha_2 = \alpha_1 + \alpha_2 + \alpha_3,$$

$$a_1 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3,$$

$$-\alpha_0 = \alpha_1\alpha_2\alpha_3.$$

## Gyökök és együtthatók közötti összefüggés

### 6.1. Tétel.

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

$$-a_{n-1} = \alpha_1 + \alpha_2 + \dots + \alpha_n;$$

$$a_{n-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n;$$

$$-a_{n-3} = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \dots + \alpha_{n-2}\alpha_{n-1}\alpha_n;$$

⋮

$$(-1)^{n-1} a_1 = \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_n + \dots + \alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n;$$

$$(-1)^n a_0 = \alpha_1\alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n.$$

### Bizonyítás.

Az  $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - \alpha_1) \dots (x - \alpha_n)$  egyenlőség bal oldalán  $x^{n-k}$  együtthatója  $a_{n-k}$ , míg a jobb oldalon

$$(-\alpha_1) \dots (-\alpha_k) + \dots \quad \square$$

## Viète-formulák

### 6.2. Megjegyzés.

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:

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

Még formálisabban:

$$(-1)^k a_{n-k} = \sum_{\substack{I \subseteq \{1, \dots, n\} \\ |I|=k}} \prod_{i \in I} \alpha_i.$$

## Többhatározatlanú polinomok

### 6.3. Definíció.

Adott  $T$  test feletti  $n$ -határozatlanú monomnak nevezzük az  $a x_1^{k_1} \dots x_n^{k_n}$  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 oknak nevezzük.

### Jelölés.

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

### 6.4. Tétel.

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

### 6.5. 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.

## Többhatározatlanú polinomok

### Példa.

$$f = 7x_1^2x_3 - 2x_1x_2x_3^4 + 9x_1x_2 - 3x_1^2x_2x_3^2 + x_1x_2x_3^3 - 2x_1^2 +$$

$$5x_1x_2^2x_3 - x_1^2x_2x_3 - 6x_1x_3 + 2x_3^2 + x_1x_3^2 + 4x_2^2x_3^2 + 8 \in \mathbb{R}[x_1, x_2, x_3]$$

$$f = x_1^2 \cdot (-3x_2x_3^2 - x_2x_3 + 7x_3 - 2) +$$

$$x_1 \cdot (5x_2^2x_3 - 2x_2x_3^4 + x_2x_3^3 + 9x_2 + x_3^2 - 6x_3) +$$

$$(4x_2^2x_3^2 + 2x_3^2 + 8) \in \mathbb{R}[x_2, x_3][x_1]$$

$$f = x_1^2 \cdot (x_2 \cdot (-3x_3^2 - x_3) + (7x_3 - 2)) +$$

$$x_1 \cdot (x_2^2 \cdot (5x_3) - x_2(2x_3^4 + x_3^3 + 9) + (x_3^2 - 6x_3)) +$$

$$(x_2^2 \cdot (4x_3^2) + (2x_3^2 + 8)) \in \mathbb{R}[x_3][x_2][x_1]$$

## Lexikografikus rendezés

### 6.6. Definíció.

Azt mondjuk, hogy az  $a x_1^{k_1} \dots x_n^{k_n}$  monom **lexikografikusan megelőzi** a  $b x_1^{l_1} \dots x_n^{l_n}$  monomot, ha

$$\exists i \in \{1, \dots, n\} : k_1 = l_1, \dots, k_{i-1} = l_{i-1} \text{ és } k_i > l_i.$$

(Vagyis megkeressük az első eltérést a  $k_1, k_2, \dots, k_n$  és az  $l_1, l_2, \dots, l_n$  kitevősorozat között, és amelyekben nagyobb szám áll ezen a helyen, az kerül előrébb a lexikografikus sorrendben.)

### Jelölés.

Tetszőleges  $M, N \in T[x_1, \dots, x_n]$  monomok esetén  $M \sqsupset N$  jelöli azt, hogy  $M$  lexikografikusan megelőzi  $N$ -et,  $M \supseteq N$  pedig azt, hogy  $M \sqsupset N$  vagy  $M \sim N$ . A  $\supseteq$  relációt **lexikografikus rendezésnek** nevezzük.

## Lexikografikus rendezés

### Példa.

$$x_1^2 x_2^{99} x_3^{23} x_4^{71} \quad ? \sqsubset \quad x_1^3 x_2 x_3^2 x_4^5$$

$$-2x_1^3 x_2 x_3^4 x_4^2 \quad ? \sqsupset \quad 14x_1^3 x_2 x_3^2 x_4^3$$

$$x_1 x_2 x_3^2 x_4 \quad ? \sqsupset \quad 3x_2^4 x_3^6 x_4^2$$

$$12x_1^2 x_2^3 x_3 x_4^5 \quad ? \sim \quad -9x_1^2 x_2^3 x_3 x_4^5$$

## Lexikografikus rendezés

### 6.7. Állítás.

A monomok halmazán  $\supseteq$  reflexív, tranzitív és dichotóm reláció, valamint  $M \supseteq N$  és  $M \sqsubseteq N$  akkor és csak akkor áll fenn egyszerre, ha  $M$  és  $N$  asszociáltak.

### 6.8. Megjegyzés.

Az előző állítás szerint a  $\supseteq$  reláció teljes rendezés (dichotóm részbenrendezés) a monomok halmazán „modulo asszociáltság”. Általában egyszerre csak egy adott polinomban előforduló monomokat vizsgálunk, ezek között pedig nincsenek asszociáltak (azokat össze lehetne vonni egy taggá), tehát ilyenkor valójában teljesen rendezett halmazzal dolgozhatunk.

### 6.9. Állítás.

A monomok szorzása monoton a lexikografikus rendezésre nézve, azaz tetszőleges  $M, \hat{M}, N, \hat{N}$  monomokra ha  $M \supseteq N$  és  $\hat{M} \supseteq \hat{N}$ , akkor  $M\hat{M} \supseteq N\hat{N}$ , és itt asszociáltság csak akkor teljesül, ha  $M \sim N$  és  $\hat{M} \sim \hat{N}$ .

## Lexikografikus rendezés

### Példa.

A korábbi példában szereplő polinom tagjai lexikografikusan csökkenő sorrendben:

$$f = -3x_1^2 x_2 x_3^2 - x_1^2 x_2 x_3 + 7x_1^2 x_3 - 2x_1^2 + 5x_1 x_2^2 x_3 - 2x_1 x_2 x_3^4 + \\ + x_1 x_2 x_3^3 + 9x_1 x_2 + x_1 x_3^2 - 6x_1 x_3 + 4x_2^2 x_3^2 + 2x_3^2 + 8$$

### 6.10. Állítás.

Tetszőleges  $f, g \in T[x_1, \dots, x_n]$  nemzéró polinomokra  $fg$  lexikografikusan első tagja nem más, mint  $f$  és  $g$  lexikografikusan első tagjának szorzata.

### Bizonyítás.

Írjuk fel  $f$  és  $g$  tagjait lexikografikusan csökkenő sorrendben:

$$f = M_1 + \dots + M_s, \quad M_1 \supset \dots \supset M_s, \quad \text{LET}(f) = M_1;$$

$$g = N_1 + \dots + N_t, \quad N_1 \supset \dots \supset N_t, \quad \text{LET}(g) = N_1.$$

$$fg = (M_1 + \dots + M_s)(N_1 + \dots + N_t) = M_1 N_1 + \dots + M_s N_t = \sum_{i=1}^s \sum_{j=1}^t M_i N_j.$$

Ha  $(i, j) \neq (1, 1)$ , akkor  $M_i \supset M_j$ ,  $N_1 \supset N_j$ , és e két egyenlőtlenség közül legalább az egyik szigorú. Tehát  $M_i N_1 \supset M_i N_j$ , azaz  $\text{LET}(fg) = M_1 N_1 = \text{LET}(f) \text{LET}(g)$ .  $\square$

## Szimmetrikus polinomok

### 6.11. Definíció.

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

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

### 6.12. 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  $\sigma_k$  jelöli (az alaptest és  $n$  értéke általában világos a szövegkörnyezetből), tehát

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_k} = \sum_{\substack{I \subseteq \{1, \dots, n\} \\ |I|=k}} \prod_{i \in I} x_i \in T[x_1, \dots, x_n].$$

### 6.13. Megjegyzés.

Az elemi szimmetrikus polinomokkal már találkoztunk: segítségével 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.

## Szimmetrikus polinomok

### Példa.

Írjuk fel a Viète-formulákat az  $x^3 + 2x^2 + 8x + 6$  polinomra.

$$\alpha_1 + \alpha_2 + \alpha_3 = \sigma_1(\alpha_1, \alpha_2, \alpha_3) = -2,$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \sigma_2(\alpha_1, \alpha_2, \alpha_3) = 8,$$

$$\alpha_1\alpha_2\alpha_3 = \sigma_3(\alpha_1, \alpha_2, \alpha_3) = -6.$$

A fentiek segítségével a gyökök sok más kifejezését is kiszámolhatjuk, pl.:

$$\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3} = \frac{\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3}{\alpha_1\alpha_2\alpha_3} = \frac{8}{-6} = -\frac{4}{3}$$

$$\alpha_1^2\alpha_2\alpha_3 + \alpha_1\alpha_2^2\alpha_3 + \alpha_1\alpha_2\alpha_3^2 = \alpha_1\alpha_2\alpha_3 \cdot (\alpha_1 + \alpha_2 + \alpha_3) = (-6) \cdot (-2) = 12$$

Figyeljük meg, hogy ezek mind *szimmetrikus* kifejezések a gyököknek.

## A szimmetrikus polinomok alaptétele

### 6.14. Tétel.

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

### 6.15. Lemma.

Ha  $ax_1^{k_1} \dots x_n^{k_n}$  egy szimmetrikus polinom lexicografikusan első tagja, akkor

$$k_1 \geq \dots \geq k_n.$$

### Bizonyítás.

Tf.  $f$  szimmetrikus polinom,  $\text{LET}(f) = ax_1^{k_1} \dots x_n^{k_n}$ , és  $k_i < k_{i+1}$ . A szimmetria miatt  $f$  tagjai között szerepel az  $M := ax_1^{k_1} \dots x_i^{k_i+1} x_{i+1}^{k_i} \dots x_n^{k_n}$  monom is. Node  $M \sqsupset \text{LET}(f)$ .  $\square$

### 6.16. Lemma.

Tetszőleges  $k_1 \geq \dots \geq k_n$  nemnegatív egészekhez léteznek olyan  $l_1, \dots, l_n$  nemnegatív egészek, hogy  $\sigma_1^{l_1} \dots \sigma_n^{l_n} \in T[x_1, \dots, x_n]$  lexicografikusan első tagja éppen  $x_1^{k_1} \dots x_n^{k_n}$ .

## A szimmetrikus polinomok alaptétele

### 6.17. Tétel (a szimmetrikus polinomok alaptétele).

Bármely szimmetrikus polinom felírható, mégpedig egyetlen módon, az elemi szimmetrikus polinomok polinomjaként. Formálisan:

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

### Példa.

Fejezzük ki az  $f = x_1^3 + x_2^3 + x_3^3 \in \mathbb{R}[x_1, x_2, x_3]$  polinomot az elemi szimmetrikus polinomok polinomjaként.

$$f = x_1^3 + x_2^3 + x_3^3$$

$$f - \sigma_1^3 = -3x_1^2x_2 - 3x_1^2x_3 - 3x_1x_2^2 - 6x_1x_2x_3 - 3x_1x_3^2 - 3x_2^2x_3 - 3x_2x_3^2$$

$$f - \sigma_1^3 + 3\sigma_1\sigma_2 = 3x_1x_2x_3$$

$$f - \sigma_1^3 + 3\sigma_1\sigma_2 - 3\sigma_3 = 0$$

Tehát

$$f = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = h(\sigma_1, \sigma_2, \sigma_3), \text{ ahol } h(x_1, x_2, x_3) = x_1^3 - 3x_1x_2 + 3x_3.$$

## SZPAT+Viète

### Példa.

Anélkül, hogy megkeresnénk a gyököket, határozzuk meg az  $f = x^3 - 3x^2 + x - 8$  polinom gyökeinek köbösszegét, valamint számtani, mértani és harmonikus közepét.

A Viète-formulák szerint

$$\alpha_1 + \alpha_2 + \alpha_3 = \sigma_1(\alpha_1, \alpha_2, \alpha_3) = 3,$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \sigma_2(\alpha_1, \alpha_2, \alpha_3) = 1,$$

$$\alpha_1\alpha_2\alpha_3 = \sigma_3(\alpha_1, \alpha_2, \alpha_3) = 8.$$

Az előző feladat alapján

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = \sigma_1(\alpha_1, \alpha_2, \alpha_3)^3 - 3\sigma_1(\alpha_1, \alpha_2, \alpha_3)\sigma_2(\alpha_1, \alpha_2, \alpha_3) + 3\sigma_3(\alpha_1, \alpha_2, \alpha_3) = 3^3 - 3 \cdot 3 \cdot 1 + 3 \cdot 8 = 42$$

## SZPAT+Viète

### Példa (folyt.).

$$\alpha_1 + \alpha_2 + \alpha_3 = \sigma_1(\alpha_1, \alpha_2, \alpha_3) = 3,$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \sigma_2(\alpha_1, \alpha_2, \alpha_3) = 1,$$

$$\alpha_1\alpha_2\alpha_3 = \sigma_3(\alpha_1, \alpha_2, \alpha_3) = 8.$$

számtani közép:

$$\frac{\alpha_1 + \alpha_2 + \alpha_3}{3} = \frac{3}{3} = 1$$

mértani közép:

$$\sqrt[3]{\alpha_1\alpha_2\alpha_3} = \sqrt[3]{8} = 2$$

harmonikus közép:

$$\frac{3}{\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3}} = \frac{3}{\frac{\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3}{\alpha_1\alpha_2\alpha_3}} = \frac{3\alpha_1\alpha_2\alpha_3}{\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3} = \frac{3 \cdot 8}{1} = 24$$

## Diszkrimináns

### 6.18. Definíció.

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

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

ahol  $\alpha_1, \dots, \alpha_n$  az  $f$  polinom komplex gyökei (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása).

A diszkrimináns a gyökök szimmetrikus polinomja, ezért kifejezhető a polinom együtthatói segítségével.

### Példa.

Az  $f = x^2 + bx + c = (x - \alpha_1)(x - \alpha_2)$  polinom diszkriminánsa:

$$D = (\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-b)^2 - 4c = b^2 - 4c$$

## A harmadfokú polinom diszkriminánsa

$$D = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$$

$$\sigma_1 = x_1 + x_2 + x_3$$

$$\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$$

$$\sigma_3 = x_1x_2x_3$$

$$D = x_1^4x_2^2 - 2x_1^4x_2x_3 + x_1^4x_3^2 - 2x_1^3x_2^3 + 2x_1^3x_2^2x_3 + 2x_1^3x_2x_3^2 - 2x_1^3x_3^3 + x_1^2x_2^4 + 2x_1^2x_2^3x_3 - 6x_1^2x_2^2x_3^2 + 2x_1^2x_2x_3^3 + x_1^2x_3^4 - 2x_1x_2^4x_3 + 2x_1x_2^3x_3^2 + 2x_1x_2^2x_3^3 - 2x_1x_2x_3^4 + x_2^4x_3^2 - 2x_2^3x_3^3 + x_2^2x_3^4$$

## A harmadfokú polinom diszkriminánsa

$$D - \sigma_1^2\sigma_2^2 = -4x_1^4x_2x_3 - 4x_1^3x_2^3 - 6x_1^3x_2^2x_3 - 6x_1^3x_2x_3^2 - 4x_1^3x_3^3 - 6x_1^2x_2^3x_3 - 21x_1^2x_2^2x_3^2 - 6x_1^2x_2x_3^3 - 4x_1x_2^4x_3 - 6x_1x_2^3x_3^2 - 6x_1x_2^2x_3^3 - 4x_1x_2x_3^4 - 4x_2^3x_3^3$$

$$D - \sigma_1^2\sigma_2^2 + 4\sigma_1^3\sigma_3 = -4x_1^4x_2^3 + 6x_1^3x_2^2x_3 + 6x_1^3x_2x_3^2 - 4x_1^3x_3^3 + 6x_1^2x_2^3x_3 + 3x_1^2x_2^2x_3^2 + 6x_1^2x_2x_3^3 + 6x_1x_2^2x_3^2 + 6x_1x_2x_3^3 - 4x_2^2x_3^3$$

$$D - \sigma_1^2\sigma_2^2 + 4\sigma_1^3\sigma_3 + 4\sigma_2^3 = 18x_1^3x_2^2x_3 + 18x_1^3x_2x_3^2 + 18x_1^2x_2^3x_3 + 27x_1^2x_2^2x_3^2 + 18x_1^2x_2x_3^3 + 18x_1x_2^3x_3^2 + 18x_1x_2^2x_3^3$$

$$D - \sigma_1^2\sigma_2^2 + 4\sigma_1^3\sigma_3 + 4\sigma_2^3 - 18\sigma_1\sigma_2\sigma_3 = -27x_1^2x_2^2x_3^2$$

$$D - \sigma_1^2\sigma_2^2 + 4\sigma_1^3\sigma_3 + 4\sigma_2^3 - 18\sigma_1\sigma_2\sigma_3 + 27\sigma_3^2 = 0$$

## A harmadfokú polinom diszkriminánsa

$$D = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2$$

Ha  $(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 + px + q$ , akkor a Viète-formulák szerint

$$\sigma_1(\alpha_1, \alpha_2, \alpha_3) = 0,$$

$$\sigma_2(\alpha_1, \alpha_2, \alpha_3) = p,$$

$$\sigma_3(\alpha_1, \alpha_2, \alpha_3) = -q,$$

tehát

$$D(\alpha_1, \alpha_2, \alpha_3) = -4\sigma_2(\alpha_1, \alpha_2, \alpha_3)^3 - 27\sigma_3(\alpha_1, \alpha_2, \alpha_3)^2 = -4p^3 - 27q^2 = -108 \left( \left( \frac{q}{2} \right)^2 + \left( \frac{p}{3} \right)^3 \right).$$

## Pitagorasi számhármások

### 7.1. Definíció.

Az  $(x, y, z) \in \mathbb{N}^3$  számhármast **pitagorasi számhármásnak** nevezzük, ha  $x^2 + y^2 = z^2$ . Az  $(x, y, z)$  pitagorasi számhármás **primitív**, ha  $\text{Inko}(x, y, z) = 1$ .

### 7.2. Megjegyzés.

Tetszőleges  $(x, y, z)$  pitagorasi számhármás esetén  $(x/d, y/d, z/d)$  primitív pitagorasi számhármás, ahol  $d = \text{Inko}(x, y, z)$ . Tehát elegendő a primitív pitagorasi számhármásokat meghatározni, mert ezekből minden pitagorasi számhármás megkapható (egy konstanssal való szorzással).

### Példa.

- ▶ (3, 4, 5)
- ▶ (5, 12, 13)
- ▶ (8, 15, 17)
- ▶ (7, 24, 25)
- ▶ ...

## Pitagorasi számhármások

### 7.3. Lemma.

*Primitív pitagorasi számhármásban a tagok páronként is relatív prímek.*

### Bizonyítás.

Legyen  $(x, y, z)$  primitív pitagorasi számhármás,  $d := \text{Inko}(x, y)$ .

$$\begin{aligned}d \mid x, y &\implies d^2 \mid x^2, y^2 \\ &\implies d^2 \mid x^2 + y^2 = z^2 \\ &\implies d \mid z \\ &\implies d \mid \text{Inko}(x, y, z) \\ &\implies d = 1 \\ &\implies x \perp y\end{aligned}$$

Hasonlóan igazolható, hogy  $x \perp z$  és  $y \perp z$ . □

## Pitagorasi számhármások

### 7.4. Lemma.

*Ha  $(x, y, z)$  primitív pitagorasi számhármás, akkor  $x$  és  $y$  paritása különböző,  $z$  pedig páratlan.*

### Bizonyítás.

Páros szám négyzete nullát, páratlan szám négyzete pedig egyet ad maradékkal 4-gyel osztva. Ezt felhasználva ...

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

□

## Pitagorasi számhármások

### 7.5. Tétel.

*Legyen  $(x, y, z)$  primitív pitagorasi számhármás, és tegyük fel, hogy  $x$  páros. Ekkor léteznek olyan  $u, v$  természetes számok, melyekre*

$$u > v, \quad u \not\equiv v \pmod{2}, \quad \text{Inko}(u, v) = 1, \quad \text{és } x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2.$$

*Fordítva, a fenti formulákkal definiált  $(x, y, z)$  számhármás mindig primitív pitagorasi számhármás.*

### 7.6. Tétel (Fermat).

*Az  $x^4 + y^4 = z^4$  egyenletnek nincs pozitív egészekből álló megoldása.*

### 7.7. Tétel (nagy Fermat-tétel, Wiles és Taylor, 1993-95).

*Ha  $n \geq 3$ , akkor az  $x^n + y^n = z^n$  egyenletnek nincs pozitív egészekből álló megoldása.*

## Két négyzetszám összege

### 7.8. Lemma.

*Ha  $m$  és  $n$  előáll két négyzetszám összegeként, akkor  $mn$  is előáll.*

### Bizonyítás.

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \quad \square$$

### 7.9. Lemma.

*A  $4k + 1$  alakú prímszámok előállnak két négyzetszám összegeként, a  $4k + 3$  alakú prímeke viszont nem.*

### 7.10. Tétel (Fermat-féle két négyzetszám tétel).

*Pontosan azok a számok állnak elő két négyzetszám összegeként, amelyek prímfelbontásában a  $4k + 3$  alakú prímeke páros kitevővel szerepelnek.*

### Példa.

$$153 = 3^2 \cdot 17 = 3^2 \cdot (4^2 + 1^2) = (3 \cdot 4)^2 + (3 \cdot 1)^2 = 12^2 + 3^2$$

$$2173 = 41 \cdot 53 = (4^2 + 5^2) \cdot (2^2 + 7^2) = 27^2 + 38^2$$

$$\begin{aligned}13949 &= 13 \cdot 29 \cdot 37 = (2^2 + 3^2) \cdot (2^2 + 5^2) \cdot (1^2 + 6^2) = (11^2 + 16^2) \cdot (1^2 + 6^2) \\ &= 85^2 + 82^2\end{aligned}$$

## Waring-problémakör

### 7.11. Tétel (Lagrange-féle négy négyzetszám tétel).

*Minden természetes szám előáll négy négyzetszám összegeként.*

### 7.12. Megjegyzés.

Lagrange tétele éles abban az értelemben, hogy három négyzetszám összegeként nem lehet minden természetes számot előállítani (keressünk ellenpéldát!).

A természetes számok hatványösszegekként való előállításával 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.

## Waring-problémakör

### 7.12. Megjegyzés (folyt.).

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<sup>§</sup> minden  $k$ -ra, bár ezt már Waring is sejtette. Hilbert igazolta Waring sejtését, és van egy feltételezett képlet is a  $g(k)$  számokra:

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

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.

<sup>§</sup>Mit jelentene az, hogy  $g(k)$  nem létezik?

## Végtelen sok prím

### 7.13. Tétel.

*Végtelen sok prímszám van.*

### 7.14. Tétel.

*Végtelen sok  $4k - 1$  alakú prímszám van.*

### 7.15. Tétel.

*Végtelen sok  $4k + 1$  alakú prímszám van.*

### 7.16. Tétel (Dirichlet tétele).

*Ha egy nemkonstans számtani sorozat kezdőtagja és differenciája egymáshoz relatív prím, akkor a számtani sorozatban végtelen sok prímszám található.*

## Hézagok a prímekek között

### 7.17. Tétel (Csebisev tétele).

*Bármely szám és a kétszerese között van prímszám. Pontosabban: minden  $n$  természetes számhoz létezik olyan  $p$  prímszám, amelyre  $n < p \leq 2n$ .*

### 7.18. Tétel.

*A szomszédos prímekek között tetszőlegesen nagy hézagok találhatóak. (Azaz minden  $N \in \mathbb{N}$  esetén lehet találni  $N$  egymást követő összetett számot.)*

### 7.19. Definíció.

**Ikerprímek** nevezünk két prímszámot, ha különbségük 2.

### Ikerprímsejtés.

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 azóta jóval lejjebb vitték).

## Al prímszámok

### 7.20. Lemma.

A  $\sum_{n=1}^{\infty} \frac{1}{n}$  harmonikus sor divergens, míg a  $\sum_{n=1}^{\infty} \frac{1}{n^2}$  sor konvergens.

### 7.21. Tétel.

A prímszámok reciprokaiból alkotott sor divergens, azaz

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

### 7.22. Megjegyzés.

Ez a tétel durván fogalmazva azt állítja, hogy „sok” prímszám van (négyzetszámból viszont a 7.20. Lemma szerint „kevés” van). Ismert tény, hogy „kevés” páratlan tökéletes szám, illetve „kevés” ikerprím van (ebből persze még nem derül ki, hogy végtelen sok van-e belőlük).

### 7.23. Megjegyzés.

A harmonikus sor lassan divergál, a prímszámok reciprokaiból alkotott sor még lassabban. Például  $\sum_{p < 10^{18}} \frac{1}{p} < 4$  (ez kb. a sor első huszonnégybilliárd tagja).

## Al prímszámok

### 7.24. Tétel.

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

### 7.25. 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:

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

### 7.26. Tétel (prímszámtétel).

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

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

### 7.27. Következmény.

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

## Algebrai és transzcendens számok

### Példa.

- $\sqrt{2}$  algebrai szám, minimálpolinomja:  $x^2 - 2$  (miért irreducibilis?).
- $\sqrt[n]{2}$  algebrai szám, minimálpolinomja:  $x^n - 2$  (miért irreducibilis?).
- $i$  algebrai szám, minimálpolinomja:  $x^2 + 1$  (miért irreducibilis?).
- $\pi$  és  $e$  transzcendens számok.
- A Liouville-féle  $\sum \frac{1}{10^n}$  konstans transzcendens szám.
- Gelfond–Schneider-tétel: Ha  $\alpha \neq 0, 1$  és  $\beta \notin \mathbb{Q}$  algebrai számok, akkor  $\alpha^\beta$  transzcendens szám.  
Például  $2^{\sqrt{2}}$ ,  $\sqrt{2}^{\sqrt{2}}$  és  $i^i = e^{-\pi/2}$  transzcendens számok.

## Diofantoszi approximáció

Adott  $\alpha$  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.

### 7.32. Tétel (Dirichlet approximációs tétele).

Minden  $\alpha$  valós szám és minden  $N$  természetes szám esetén van  $\alpha$ -nak olyan  $\frac{p}{q}$  közelítése, amelyre

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

### 7.33. Következmény.

Ha  $\alpha$  irracionális szám, akkor végtelen sok olyan  $\frac{p}{q}$  közelítése van, amelyre

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

### 7.34. Állítás.

Ha  $\alpha$  racionális szám, akkor csak véges sok olyan  $\frac{p}{q}$  közelítése van, amelyre

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

## Algebrai és transzcendens számok

### 7.28. Definíció.

Az  $\alpha$  komplex számot **algebrai számnak** nevezzük, ha gyöke valamely nemzéró racionális együtthatós polinomnak. A nem algebrai számokat **transzcendens számoknak** nevezzük.

### 7.29. Definíció.

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

### 7.30. 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  $\alpha$  algebrai szám gyöke, akkor  $f$  megegyezik  $\alpha$  minimálpolinomjával.

### 7.31. Tétel.

Létezik transzcendens szám.

## Diofantoszi approximáció

### 7.35. Tétel (Hurwitz tétele).

Ha  $\alpha$  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.

### 7.36. Tétel (Liouville, Thue, Siegel, Roth).

Ha  $\alpha$  irracionális algebrai szám és  $\varepsilon > 0$ , akkor csak véges sok olyan  $\frac{p}{q}$  közelítése van, amelyre

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

## Algebrai számok és gyökmennyiségek

### 7.37. Tétel.

Az algebrai számok résztestet alkotnak a komplex számok testében.

### 7.38. Tétel.

Ha  $\alpha$  algebrai szám és  $n \geq 2$ , akkor  $\sqrt[n]{\alpha}$  is algebrai szám (a gyököknek mind az  $n$  értéke).

### 7.39. Definíció.

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

### 7.40. Következmény.

A gyökmennyiségek algebrai számok.

### Példa.

Ez a szám algebrai:

$$\frac{\sqrt[3]{3 - \sqrt{4\sqrt{2} + \sqrt{\frac{3}{17}}}} + \sqrt[17]{323 - \sqrt{2014}}}{\sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}}$$

## Algebrai számok és gyökmennyiségek

### 7.41. 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 megoldóképlet, sőt, például az  $x^5 - 4x + 2 = 0$  egyenletnek még „ad hoc” megoldóképlete sincs, mert gyökei nem gyökmennyiségek.

### 7.42. Tétel.

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