Algebra és számelmélet 3 előadás

Waldhauser Tamás
2016 őszi félév

Ha ezt a fájlt kinyomtatod...

Tematika

Ekvivalenciák és osztályozások, leképezés magja, részbenrendezett halmazok. Ekvivalenciák alkalmazása a számfogalom kialakításában. Véges halmaz permutációi: idegen ciklusok szorzatára bontás, előállítás transzpozíciók szorzataként, páros és páratlan permutációk. Egész együtthatós polinomok racionális gyökei, irreducibilis polinomok a racionális együtthatós polinomok gyűrűjében, Schönemann–Eisenstein-tétel. A racionális törtfüggvények teste, parciális törtekre bontás. Test fölötti többhatározatlanú polinomok gyűrűje, szimmetrikus polinomok, algebrai és transzcendens számok. Lineáris diofantoszi egyenletek. A mod n kongruencia, maradékosztályok. Lineáris kongruenciák és kongruenciarendszerek, kínai maradéktétel. Lineáris kongruenciák és lineáris „diofantoszi" egyenletek test fölötti polinomgyűrűkben. Euler–Fermat-tétel, Wilson-tétel. Nevezetes számelméleti függvények (osztók száma, osztók összege, Euler-féle φ függvény), gyengén multiplikatív számelméleti függvények, számelméleti függvények konvolúciója, összegzési és megfordítási függvény, Möbius-féle inverziós formula. Tökéletes számok, Mersenne- és Fermat-prímek. Pitagoraszi számhármasok. A „nagy" Fermat-tétel, Waring-problémakör (ismertetés). Prímek száma, a 4k-1 alakú prímek. Dirichlet tétele a számtani sorozatokban előforduló prímekről (ismertetés). Tetszőlegesen nagy hézag a prímek között, felső becslés az n-edik prímszámra, a prímek reciprokainak összege. Csebisev-tétel, prímszámtétel (ismertetés). Valós számok approximációja racionális számokkal, Dirichlet approximációs tétele. Nevezetes számelméleti problémák, titkosírások (ismertetés).

Tematika

1. Permutációk
2. Relációk
3. Számelméleti kongruenciák
4. Számelméleti függvények
5. Polinomok
6. Többhatározatlanú polinomok
7. Nevezetes számelméleti problémák

Melyik a kakukktojás?

Érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, tudni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni,
érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni, érteni!

1. leképezések (injektív, szürjektív, bijektív), leképezések szorzása
2. oszthatóság, maradékos osztás, lnko az egész számok körében
3. prímszám, összetett szám, a számelmélet alaptétele
4. komplex számok, gyökvonás, egységgyökök
5. csoport, gyűrű és test fogalma, nevezetes példák
6. oszthatóság, maradékos osztás, lnko test feletti polinomokra
7. egyértelmű irreducibilis faktorizáció test feletti polinomokra
8. polinomok helyettesítési értékei és gyökei, Horner-elrendezés, Bézout tétele
9. irreducibilis polinomok a komplex és valós együtthatós polinomok gyűrűjében
10. gondolkozni, kérdezni, kételkedni

Követelmények

1. Házi feladatok
   háromfokozatú értékelés:

●		⋆

2. Elektronikus tesztek
   háromfokozatú értékelés:

●		⋆

3. Dolgozatok a gyakorlaton
   négyfokozatú értékelés:

●		⋆	⋆⋆

4. Dolgozat az előadáson
   háromfokozatú értékelés:

●		⋆

5. Szóbeli vizsga
   háromfokozatú értékelés:

●		⋆

Követelmények

1. Házi feladatok gyakorlatra
   - röpdolgozat vagy beadandó feladat
   - ellenőrizni, olvashatóan, szabatosan, igényesen leírni!
   - táblánál el kell mondani!
   - hetente 1 feladat lesz értékelve (legalább 10 alkalom lesz)
   - feladatonként 2 pont, összesen 20 pont
   - értékelés:

$$\begin{array}{rcl} 0 - 9 & \to & \bullet \\ 10 - 14 & \to & \\ 15 - 20 & \to & \star \end{array}$$

2. Elektronikus tesztek
   - rutinfeladatok
   - `http://www.math.u-szeged.hu/~hartm/practmath/mpract.html`
   - 12 feladat, (majdnem) korlátlan számú próbálkozási lehetőség
   - feladatonként 1 pont, mindegyiket 5-ször kell jól megoldani, összesen 60 pont
   - értékelés:

$$\begin{array}{rcl} 0 - 39 & \to & \bullet \\ 40 - 49 & \to & \\ 50 - 60 & \to & \star \end{array}$$

Követelmények

3. Dolgozatok a gyakorlaton
   - rutin- és nehezebb feladatok is
   - két dolgozat: október 20 és december 1
   - egyiket lehet pótolni/javítani
   - dolgozatonként 30 pont, összesen 60 pont
   - értékelés:

$$\begin{array}{rcl} 0-23 & \to & \bullet \\ 24-35 & \to & \\ 36-47 & \to & \star \\ 48-60 & \to & \star\star \end{array}$$

4. Dolgozat az előadáson
   - elméleti(bb) feladatok, egyszerűbb bizonyítások, ???
   - egy dolgozat: december 8
   - két javítási lehetőség a vizsgaidőszakban
   - összesen 60 pont
   - értékelés:

$$\begin{array}{rcl} 0-23 & \to & \bullet \\ 24-35 & \to & \\ 36-60 & \to & \star \end{array}$$

Követelmények

5. Szóbeli vizsga
   - bizonyítani kell!
   - érteni kell!
   - értékelés:

$$
\begin{array}{lcc}
:-(& \rightarrow & \bullet \\
:-| & \rightarrow & \\
:-) & \rightarrow & \star
\end{array}
$$

A végső osztályzatot a csillagok száma adja

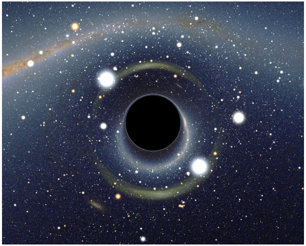
Követelmények

7. Szóbeli vizsga
   - bizonyítani kell!
   - érteni kell!
   - értékelés:

$$:-(\quad \rightarrow \quad \bullet$$

$$:-| \quad \rightarrow$$

$$:-) \quad \rightarrow \quad \star$$



A végső osztályzatot a csillagok száma adja, de a fekete lyuk mindent elnyel.

Tartalom

A permutáció fogalma

1.1. Definíció.

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

1.2. Definíció.

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

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

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

Vegyük észre, hogy π bijektivitása azt jelenti, hogy a mátrix alsó sorában az $1, 2, \ldots, n$ számok egy *permutációja* van.

Számolás permutációkkal

Példa.

Tekintsük S_6-ban az alábbi π és ρ permutációkat:

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

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

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

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

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

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 $a \in \{1, 2, \ldots, n\}$.

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

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* $\pi\rho = \rho\pi$.

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

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.

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

Házi feladat

1. feladat. Adja meg a $\pi\rho$, $\rho\pi^{-1}$ és π^{101} permutációkat kétsoros alakban és idegen ciklusok szorzataként is.

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

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

$$\pi\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix} = (14352), \rho\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix} = (14532)$$

$$\pi^{101} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (153)(24)$$

(c) $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 1 & 6 & 5 & 2 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 3 & 6 & 7 & 1 & 2 \end{pmatrix}$

(d) $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 6 & 5 & 3 & 7 & 1 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 7 & 2 & 5 & 3 \end{pmatrix}$

Házi feladat

2. feladat. Adja meg idegen ciklusok szorzataként az alábbi S_7-beli permutációkat.

(a) $(134)\,(3247)\,(14527)$ $\quad$ $(1234)^{-1}\,(1526)\,(1234)$

$(173)\,(25)$ $\quad$ (2536)

(b) $(375)(1357)(357)$ $\quad$ $(1356)\,(2463)^{-1}\,(342)$

(1573) $\quad$ $(16)(2435)$

(c) $(236)(15)(2754)$ $\quad$ $(4732)^{-1}\,(15423)\,(23)$

(d) $(1652)(35)(156)$ $\quad$ $(32647)\,(234)\,(5641)^{-1}$

Házi feladat

Kulin Júlia csoportjának:

Egy kártyakeverő gépbe betettünk 9 betűkártyát MATEKHÁZI sorrendben. A gép a keverés után a lapokat ZMKTIAEÁH sorrendben adta ki. Ezután a lapokat az első keverés utáni sorrendben újra beletettük a gépbe. A kártyakeverőgép a belehelyezett 9 kártyát egy keverés során mindig ugyanúgy rendezi át. (Például a 4. helyen lévő lapot mindig a 7. helyre teszi.) Milyen sorrendben jöttek ki a lapok a második keverés után?

Waldhauser Tamás csoportjának:

Egy kártyakeverő gép egy lépésben a behelyezett kártyák sorrendjéhez képest mindig ugyanúgy rendezi át a lapokat. Betettük a 13 darab treff lapot növekvő sorrendben 2-estől ászig. A gép egyszer megkeverte a lapokat, az így kapott csomagot újra visszatettük, ezt a gép ismét megkeverte, majd az alábbi sorrendben adta ki a 13 lapot:

Bubi, 10, Király, 9, Ász, 4, 5, 2, 6, Dáma, 7, 3, 8.

Mi volt a lapok sorrendje az első keverés után?

Tartalom

Transzpozíciók

1.9. Definíció.

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

1.10. Tétel.

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

Bizonyítás.

Elég ciklusokra igazolni:

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

Példa.

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

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

vagy

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

Egy játék

- Az alábbi kezdőállásból indul a játék:

$$5 \quad 3 \quad 8 \quad 7 \quad 4 \quad 6 \quad 2 \quad 1$$

- A játékosok felváltva megcserélhetnek két számot.
- Aki eléri az $1\ 2\ 3\ 4\ 5\ 6\ 7\ 8$ sorrendet, az a nyertes.

Kinek van nyerő stratégiája (és mi az)?

Permutáció paritása

1.11. Tétel.

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

Bizonyítás.

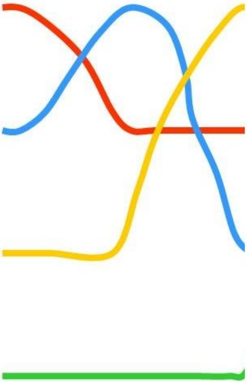
Tegyük fel, hogy

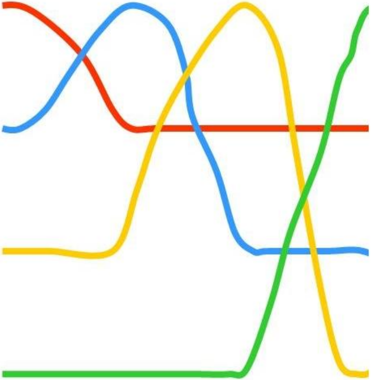
$$\tau_1\tau_2\cdots\tau_{2k+1} = \sigma_1\sigma_2\cdots\sigma_{2l},$$

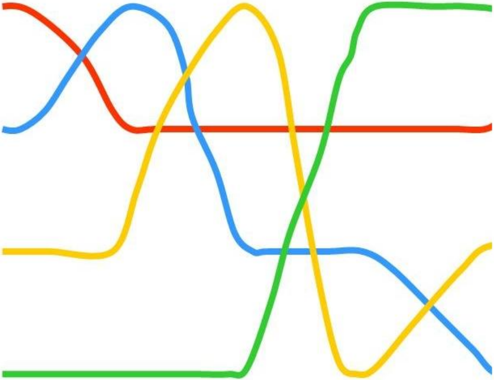
ahol mindegyik τ_i és σ_j transzpozíció. Ekkor az identikus permutáció előáll páratlan sok transzpozíció szorzataként:

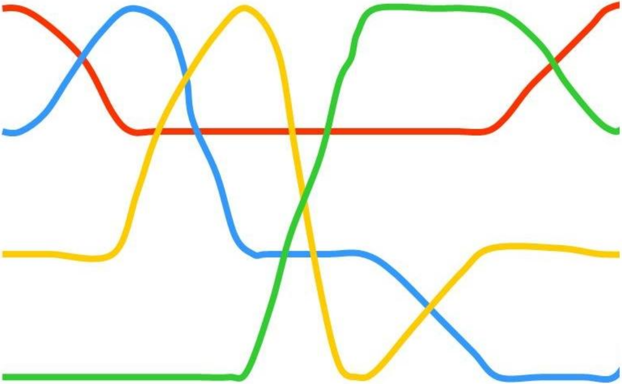
$$\mathrm{id} = \tau_1\tau_2\cdots\tau_{2k+1}\sigma_{2l}\cdots\sigma_2\sigma_1.$$

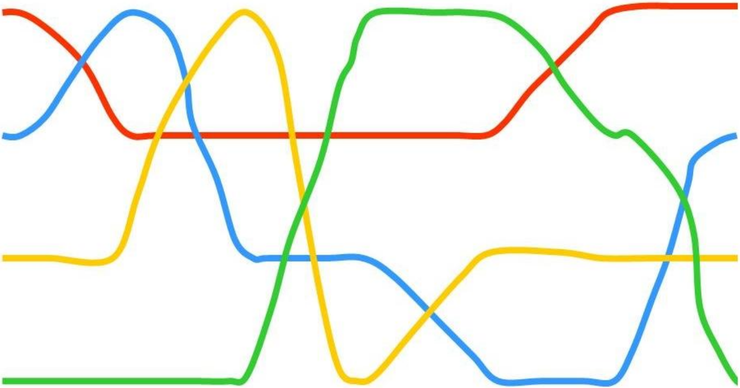
Megmutatjuk, hogy ez lehetetlen.

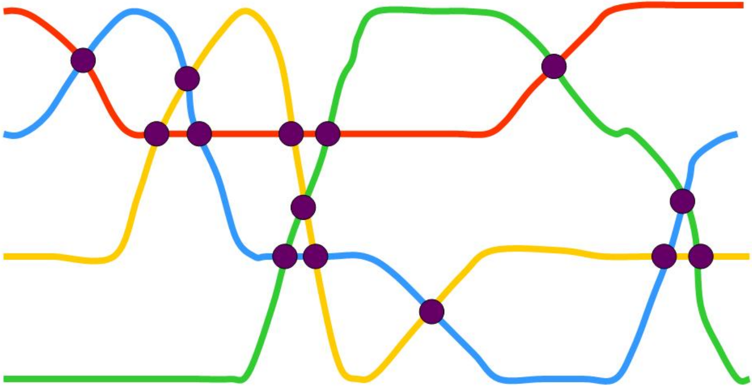


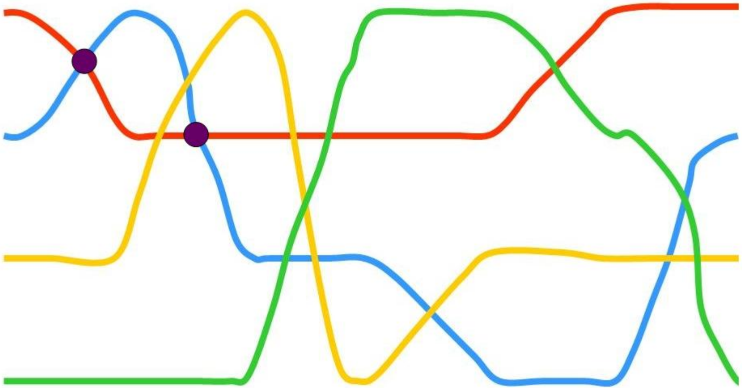




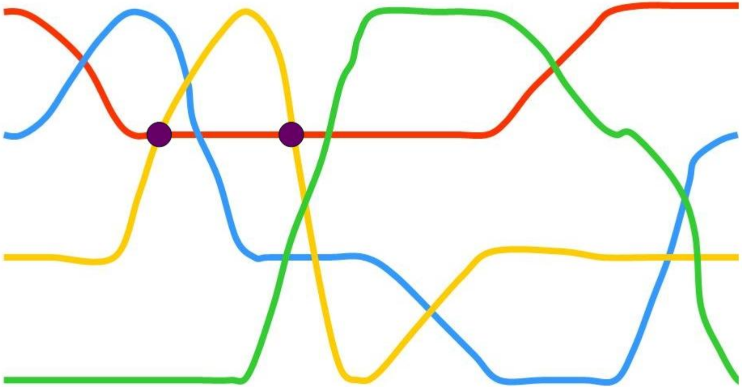




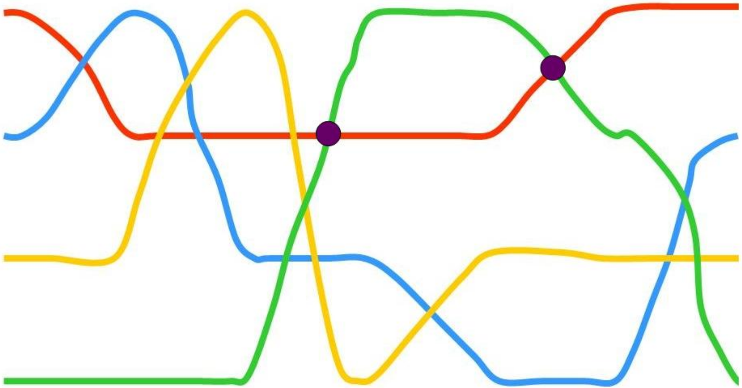




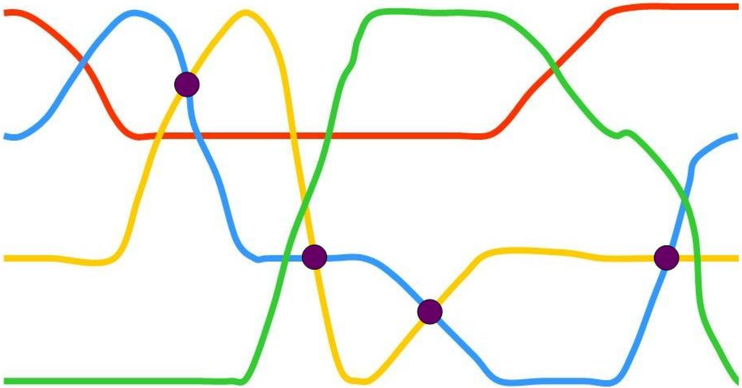
metszéspontok száma = 2



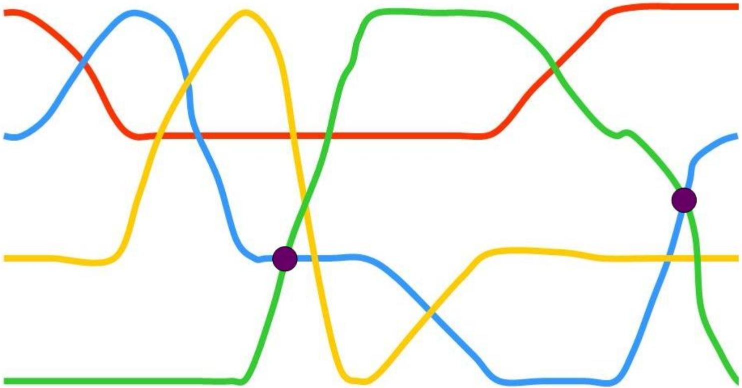
metszéspontok száma $= 2 + 2$



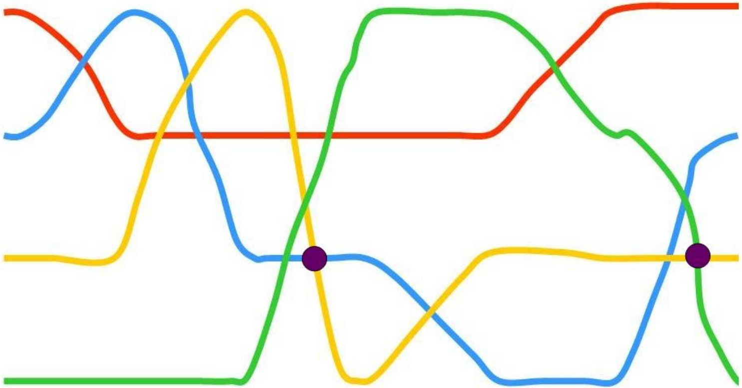
metszéspontok száma $= 2 + 2 + 2$



metszéspontok száma $= 2 + 2 + 2 + 4$

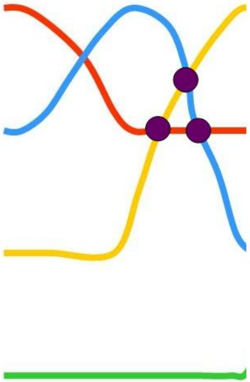


metszéspontok száma $= 2 + 2 + 2 + 4 + 2$

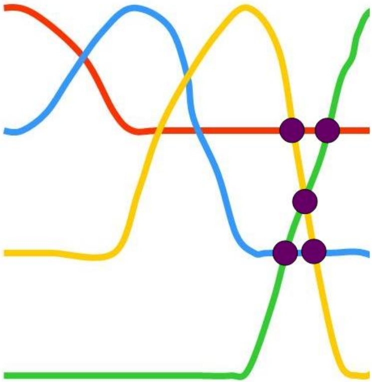


metszéspontok száma $= 2 + 2 + 2 + 4 + 2 + 2$ (páros szám)

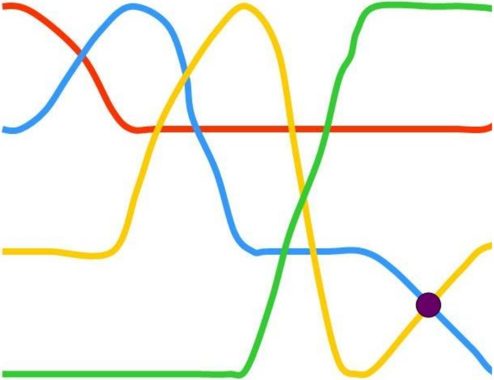
metszéspontok száma $= 1$



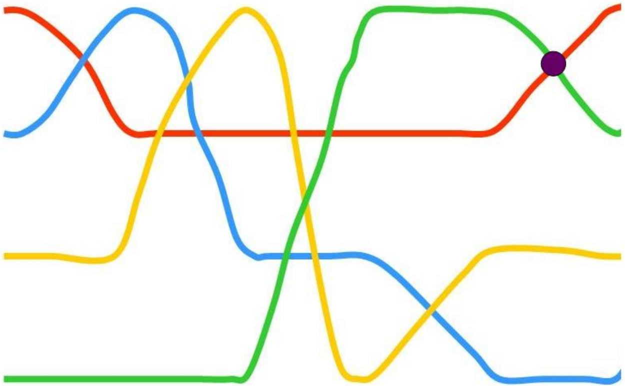
metszéspontok száma $= 1 + 3$



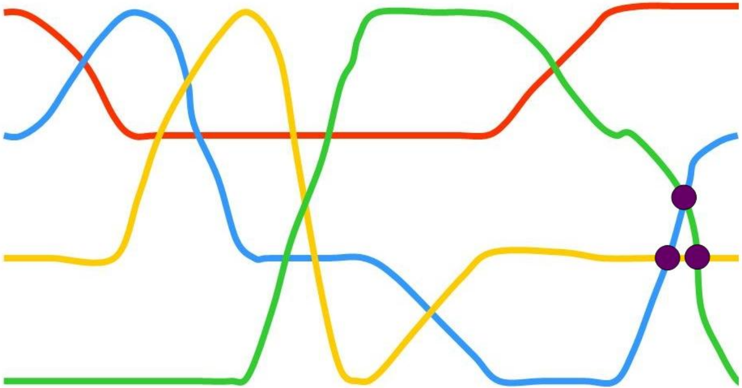
metszéspontok száma $= 1 + 3 + 5$



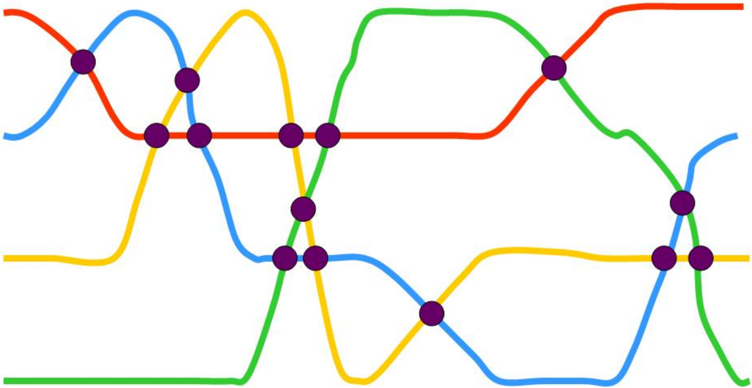
metszéspontok száma $= 1 + 3 + 5 + 1$



metszéspontok száma $= 1 + 3 + 5 + 1 + 1$



metszéspontok száma $= 1 + 3 + 5 + 1 + 1 + 3$ (annyi páratlan szám, ahány csere)



metszéspontok számának paritása $=$ cserék számának paritása $=$ páros QED

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.

$\square$

1.13. Állítás.

Permutációk szorzatának a paritása a következőképpen alakul:

$$\begin{array}{lclcl} \textit{páros} & \cdot & \textit{páros} & = & \textit{páros} \\ \textit{páratlan} & \cdot & \textit{páratlan} & = & \textit{páros} \end{array} \qquad \begin{array}{lclcl} \textit{páros} & \cdot & \textit{páratlan} & = & \textit{páratlan} \\ \textit{páratlan} & \cdot & \textit{páros} & = & \textit{páratlan} \end{array}$$

Bizonyítás.

Szorzáskor a permutációt előállító transzpozíciók száma összeadódik. $\square$

Házi feladat

3. feladat. Határozza meg a π, π^{2015} és π^{2016} permutációk paritását.

(a) $\pi = (123)\,(4567)$

π páratlan, π^{2015} páratlan, π^{2016} páros

(b) $\pi = (12)\,(345)\,(6789)$

π páros, π^{2015} páros, π^{2016} páros

(c) $\pi = (1346)\,(45761)\,(352)$

(d) $\pi = (365)\,(13624)$

Az alternáló csoport

1.14. Definíció.

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

Példa.

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

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

Példa.

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

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

$$\varphi\colon A_n \to S_n \setminus A_n,\ \pi \mapsto \pi\tau$$

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

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

□

1.16. Következmény.

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


1
6
9
11
5
15
7
14
12
10
3
13
4
8
2

Samuel Loyd (1841-1911)

SAM LOYD'S CYCLOPEDIA

OF

5000 PUZZLES TRICKS AND CONUNDRUMS

WITH ANSWERS

THE 14-15 PUZZLE IN PUZZLELAND

The older inhabitants of Puzzleland will remember how in the early seventies I drove the entire world crazy over a little box of movable blocks which became known as the "14-15 Puzzle." The fifteen blocks were arranged in the square box in regular order, only with the 14 and 15 reversed, as shown in the above illustration. The puzzle consisted in moving the blocks about, one at a time, so as to bring them back to the present position in every respect except that the error in the 14 and 15 must be corrected.

A prize of $1,000, which was offered for the first correct solution to the problem, has never been claimed, although there are thousands of persons who say they performed the required feat.

People became infatuated with the puzzle and ludicrous tales are told of shopkeepers who neglected to open their stores; of a distinguished clergyman who stood under a street lamp all through a wintry night trying to recall the way he had performed the feat. The mysterious feature of the puzzle is that no one seems to be able to recall the sequence of moves whereby they feel sure they succeeded in solving the puzzle. Pilots are said to have wrecked their ships, engineers rush their trains past stations and business generally became demoralized. A famous Baltimore editor tells how he went for his noon lunch and was discovered by his frantic staff long past midnight pushing little pieces of pie around on a plate! Farmers are known to have deserted their plows and I have taken one of such instances as an illustration for the sketch.

Several new problems developed from the original puzzle which are worth giving:

Second Problem—Start again with the blocks as in Fig. 1 and move them so as to get the numbers in regular order, but with the vacant square at upper left-hand corner instead of lower right-hand corner; see Fig. 2.

Third Problem—Start with Fig. 1, turn the box a quarter way round and so move the blocks that they will stand as in Fig. 3.

Fourth Problem—This is to move the pieces about until they form a "magic square," so that the numbers will add up thirty in ten different directions.

Fig 2.

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Fig 3.

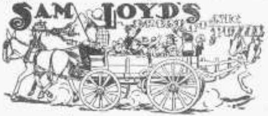
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

The Picnic Puzzle.

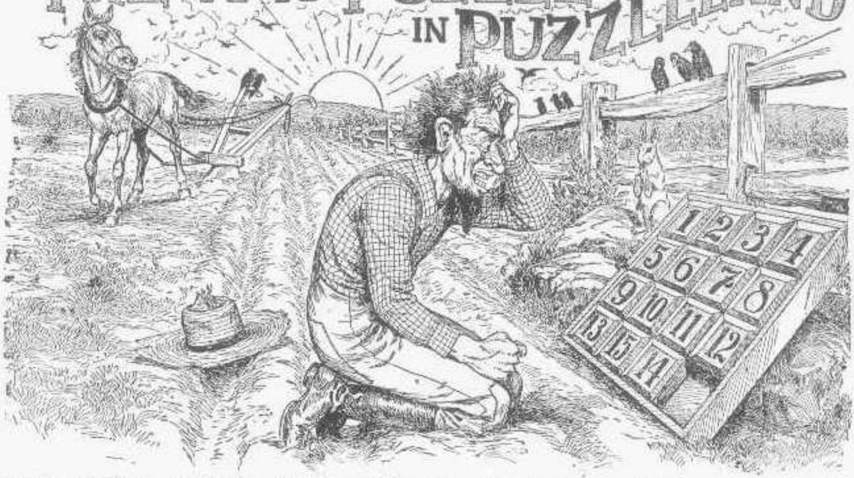
When they started off on the great annual picnic every wagon in town was pressed into service. Half way to the grounds ten wagons broke down, so it was necessary for each of the remaining wagons to carry one more person.

When they started for home it was discovered that fifteen more wagons were out of commission, so on the return trip there were three persons more in each wagon than when they started out in the morning.

Now who can tell how many people attended the great annual picnic?



THE 14-15 PUZZLE IN PUZZLELAND



The older inhabitants of Puzzleland will remember how in the early seventies I drove the entire world crazy over a little box of movable blocks which became known as the "14-15 Puzzle." The fifteen blocks were arranged in the square box in regular order, only with the 14 and 15 reversed, as shown in the above

he went for his noon lunch and was discovered by his frantic staff long past midnight pushing little pieces of pie around on a plate! Farmers are known to have deserted their plows and I have taken one of such instances as an illustration for the sketch.

Several new problems developed

Fig 2.

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Fig 3.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

The Picnic Puzzle

AMERICAN

Journal of Mathematics

PURE AND APPLIED.

EDITOR IN CHIEF: J. J. SYLVESTER.

ASSOCIATE EDITOR IN CHARGE: WILLIAM E. STORY.

WITH THE CO-OPERATION OF

SIMON NEWCOMB, H. A. NEWTON, AND H. A. ROWLAND.

PUBLISHED UNDER THE AUSPICES OF THE

JOHNS HOPKINS UNIVERSITY.

Πραγμάτων ἔλεγχος οὐ βλεπομένων.

Volume II. Number 4.

BALTIMORE:

PRINTED FOR THE EDITORS BY JOHN MURPHY & CO.

B. WESTERMANN & CO., D. VAN NOSTRAND, *New York*.
FERREE & CO., *Philadelphia*.

TRÜBNER & CO., *London*.
GAUTHIER-VILLARS, *Paris*.
A. ASHER & CO., *Berlin*.

DECEMBER, 1879.

Notes on the "15" Puzzle.

I.

By Wm. Woolsey Johnson, *Annapolis, Md.*

The puzzle described below has recently been exercising the ingenuity of many persons in Baltimore, Philadelphia and elsewhere. A ruled square of 16 compartments is numbered as in this diagram:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

the 16th square being left blank. Fifteen counters, numbered in like manner, are placed at random upon the squares so that one square is vacant. The counter occupying any adjacent square may now be moved into the vacant square—thus: If No. 7 is vacant, either of the counters occupying Nos. 3, 6, 8, 11 can be moved into it, but no diagonal move is allowed. The puzzle is to bring all the counters into their proper squares by successive moves.

It seems to be generally supposed, by those who have tried the puzzle, that this is always possible, whatever be the original random position of the counters, but this is an error, as the following demonstration will show:

When the blank or sixteenth square is the vacant one, the arrangement of the counters may be called a positive or negative one, according as the term of the 15-square determinant, which has for first and second subscripts the numbers on the squares and counters, is positive or negative. Let n

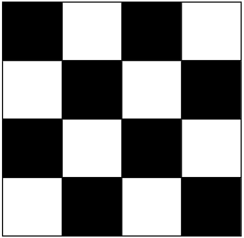
The "15" puzzle for the last few weeks has been prominently before the American public, and may safely be said to have engaged the attention of nine out of ten persons of both sexes and of all ages and conditions of the community. But this would not have weighed with the editors to induce them to insert articles upon such a subject in the American Journal of Mathematics, but for the fact that the principle of the game has its root in what all mathematicians of the present day are aware constitutes the most subtle and characteristic conception of modern algebra, viz: the law of dichotomy applicable to the separation of the terms of every complete system of permutations into two natural and indefeasible groups, a law of the inner world of thought, which may be said to prefigure the polar relation of left and right-handed screws, or of objects in space and their reflexions in a mirror. Accordingly the editors have thought that they would be doing no disservice to their science, but rather promoting its interests by exhibiting this *à priori* polar law under a concrete form, through the medium of a game which has taken so strong a hold upon the thought of the country that it may almost be said to have risen to the importance of a national institution. Whoever has made himself master of it may fairly be said to have taken his first lesson in the theory of determinants.

It may be mentioned as a parallel case that Sir William Rowan Hamilton invented, and Jacques & Co., the purveyors of toys and conjuring tricks, in London (from whom it may possibly still be procured), sold a game called the "Eikosion" game, for illustrating certain consequences of the method of quaternions.—Eds.

14	13	5	12
2	3	15	4
8		11	9
10	1	7	6

14	13	5	12
2		15	4
8	3	11	9
10	1	7	6

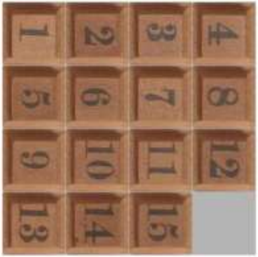
14	13	5	12	2	3	15	4	8	$\square$	11	9	10	1	7	6
14	13	5	12	2	$\square$	15	4	8	3	11	9	10	1	7	6



Ha az üres hely visszakerült a jobb alsó sarokba,
akkor páros számú csere történt.


1 2 3 4
5 6 7 8
9 10 11 12
13 15 14


4 8 12
3 7 11 15
2 6 10 14
1 5 9 13


1 2 3 4
5 6 7 8
9 10 11 12
13 14 15


13 14 15
9 10 11 12
5 6 7 8
1 2 3 4


1 2 3
4 5 6 7
8 9 10 11
12 13 14 15


4 3 2 1
8 7 6 5
12 11 10 9
15 14 13

Tizenötös játék

16 kis négyzet:

$$16! = 20\,922\,789\,888\,000 \text{ permutáció}$$

párosság miatt csak a fele lehetséges:

$$\frac{16!}{2} = \underline{10\,461\,394\,944\,000} \text{ lehetőség}$$

2×2×2-es bűvös kocka

8 kis kocka:

$$8! = 40\,320 \text{ permutáció}$$

egy kis kocka 3-féleképpen állhat:

$$3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^8 = 6561 \text{ orientáció}$$

az utolsó kis kocka állása kötött:

$$8! \cdot 3^7 = \underline{88\,179\,840} \text{ lehetőség}$$

3×3×3-as bűvös kocka

8 sarokkocka:

$$8! = 40\,320 \text{ permutáció}, \qquad 3^8 = 6561 \text{ orientáció}$$

12 élkocka:

$$12! = 479\,001\,600 \text{ permutáció}, \qquad 2^{12} = 4096 \text{ orientáció}$$

párosság, utolsó sarok-, ill. élkocka:

$$\frac{8! \cdot 12!}{2} \cdot 3^7 \cdot 2^{11} = \underline{43\,252\,003\,274\,489\,856\,000} \text{ lehetőség}$$

Megértést ellenőrző kérdések

Igazak-e az alábbi állítások?

1. $|S_3| = 8$.
2. S_5-ben tíz transzpozíció van.
3. S_3-ban minden permutáció ciklus vagy identitás.
4. Van olyan transzpozíció, aminek pontosan 3 fixpontja van.
5. Tetszőleges $\pi, \rho \in S_5$ permutációk esetén $(\pi\rho)^2 = \pi^2\rho^2$.
6. Minden $\pi \in S_4$ permutációra $\pi^6 = \mathrm{id}$ teljesül.
7. Minden három hosszúságú ciklus előáll négy transzpozíció szorzataként.
8. Páratlan permutáció inverze is páratlan.

Tartalom

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

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

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

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

Példa.

- $A =$ a sík egyeneseinek 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 $a \to b$ 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 $f\colon A \to B$ leképezés esetén a

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

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

Példa.

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

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

Példa.

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

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

Példa.

Az $f\colon A \to B$ 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

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

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

Jelölés.

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

A faktorhalmazt A/ρ jelöli, tehát

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

Ekvivalenciaosztályok

Példa.

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

Ekkor

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

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

Példa.

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

Ekkor

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

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

Figyeljük meg, hogy ha $a\rho b$, akkor $\overline{a} = \overline{b}$, egyébként pedig $\overline{a}$ és $\overline{b}$ 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) $\bigcup\limits_{B \in \mathcal{C}} B = A$.

2.6. Tétel.

Legyen A egy nemüres halmaz.

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

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

Házi feladat

4. feladat. Határozza meg az A/ρ osztályozást.

(a) $A = \{a, b, c, d\}$, $\rho = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a)\}$

$\{\{a, b\}, \{c\}, \{d\}\}$

(b) $A = \{a, b, c, d, e\}$, $\rho = \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$

$\{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\}$

(c) $A = \{a, b, c, d, e\}$, $\rho = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a), (c, d), (d, c), (c, e), (e, c), (d, e), (e, d)\}$

(d) $A = \{a, b, c, d\}$, $\rho = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (a, c), (c, a), (c, b), (b, c)\}$

Házi feladat

5. feladat. Határozza meg az $f: A \to B$ leképezés magjához tartozó $A/\ker f$ osztályozást.

(a) $f: \{-2, \ldots, 3\} \to \mathbb{Z}, \quad x \mapsto |x|$

$\{\{-2, 2\}, \{-1, 1\}, \{0\}, \{3\}\}$

(b) $f: \{0, \ldots, 7\} \to \mathbb{Z}, \quad x \mapsto \lfloor x/3 \rfloor$

$\{\{0, 1, 2\}, \{3, 4, 5\}, \{6, 7\}\}$

(c) $f: \{-2, \ldots, 3\} \to \mathbb{Z}, \quad x \mapsto \operatorname{sgn} x$

(d) $f: \{0, \ldots, 10\} \to \mathbb{Z}, \quad x \mapsto \lfloor \sqrt{x} \rfloor$

Az ekvivalenciareláció, mint fogalomalkotó eszköz

Példa.

- $A =$ a sík egyeneseinek 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 $a \to b$ 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 ρ ekvivalenciarelációt a következőképpen:

$$A \rho B \iff \text{létezik } A \to B \text{ bijekció.}$$

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

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

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

$2 + 3 =$ { ,  } $+ \overline{\{\spadesuit, \heartsuit, \clubsuit\}} =$ { ,  } $\dot\cup \{\spadesuit, \heartsuit, \clubsuit\} =$

$=$ { , , $\spadesuit, \heartsuit, \clubsuit$ } $= 5.$

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

$2 \cdot 3 =$ { ,  } $\cdot \overline{\{\spadesuit, \heartsuit, \clubsuit\}} =$ { ,  } $\times \{\spadesuit, \heartsuit, \clubsuit\} =$

$=$ { (, $\spadesuit$), (, $\heartsuit$), (, $\clubsuit$), (, $\spadesuit$), (, $\heartsuit$), (, $\clubsuit$) } $= 6.$

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 ρ 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

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

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 ρ 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

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

Az összeadás, kivonás, szorzás és osztás művelete értelmezhető ezen ekvivalencia-osztályok 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 ρ ekvivalenciarelációt a következőképpen:

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

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

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

Az összeadás, kivonás, szorzás és osztás művelete értelmezhető ezen ekvivalencia-osztályok 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.

Tartalom

Részbenrendezési reláció

2.7. Definíció.

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

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

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

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

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

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

Példa.

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

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:

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

Fedési reláció

2.9. Definíció.

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

Példa.

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

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:

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

2.11. Definíció.

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

Házi feladat

6. feladat. Rajzolja fel a megadott részbenrendezett halmazok Hasse-diagramját.

(a) $(\{1, 2, 3, 4\}; \leq)$ $(\{1, 2, 3, 4\}; |)$

(b) $(\mathcal{P}(\{a, b\}); \subseteq)$ $(D_{12}; |)$

(c) $(\mathcal{P}(\{a, b, c\}); \subseteq)$ $(D_{30}; |)$

(d) $(\mathbb{Z}; \leq)$ $(D_{36}; |)$

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 $(\mathbb{N}_0; |)$ 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.

Házi feladat

7. feladat. Adjon meg egy olyan $(A; \leq)$ részbenrendezett halmazt (például a Hasse-diagramjával), amely eleget tesz a megadott feltételeknek.

(a) $|A| = 7$, és A-ban 4 minimális és 2 maximális elem van.

(b) A végtelen, és A-nak van legkisebb és legnagyobb eleme is.

(c) $|A| = 4$, és A-ban 2 minimális és 3 maximális elem van.

(d) A-nak végtelen sok minimális eleme van, de csak egy maximális eleme van.

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

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

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 $A = \{a, b, c\}$ ábécé 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 $A = \{0, 1\}$ ábécé 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.
- antiszimmetria 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 $\mathbf{a} \sqsupset \mathbf{b}$ teljesül (és csak az egyik).
- tranzitivitás: ÁMNTFH. $\mathbf{a} \sqsubset \mathbf{b} \sqsubset \mathbf{c}$. Ekkor *valahogy így* fest a helyzet:

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

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

2.17. Tétel.

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

$$\mathbf{a} \sqsubseteq \mathbf{b},\;\; \widehat{\mathbf{a}} \sqsubseteq \widehat{\mathbf{b}} \quad\Longrightarrow\quad \mathbf{a} + \widehat{\mathbf{a}} \;\sqsubseteq\; \mathbf{b} + \widehat{\mathbf{b}},$$

és egyenlőség csak $\mathbf{a} = \mathbf{b},\; \widehat{\mathbf{a}} = \widehat{\mathbf{b}}$ *esetén teljesül.*

Megértést ellenőrző kérdések

Igazak-e az alábbi állítások?

1. Ha $\rho \subseteq A \times A$ ekvivalenciareláció, akkor minden $a, b, c \in A$ esetén $(a\rho b \text{ és } c\rho b) \implies a\rho c$.
2. Tetszőleges $\rho \subseteq A \times A$ ekvivalenciareláció és $a, b \in A$ esetén $a \neq b \implies \overline{a} \cap \overline{b} \neq \emptyset$.
3. Ha A végtelen halmaz, akkor minden A-n értelmezett ekvivalenciarelációnak végtelen sok osztálya van.
4. Ha a $\varphi\colon A \to B$ leképezés magjára $|A/\ker\varphi| = 2$ teljesül, akkor φ értékkészlete kételemű halmaz.
5. Az $(\mathbb{N}_0; |)$ részbenrendezett halmazban 6 fedi 2-t.
6. Ha egy részbenrendezett halmaznak két minimális eleme van, akkor nincs legkisebb eleme.
7. Az $(\mathbb{N}_0; |)$ részbenrendezett halmaz legkisebb eleme a nulla.
8. Minden véges részbenrendezett halmaznak van minimális eleme.

Tartalom

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 $\text{lnko}\,(a, b)$ vagy (a, b), legkisebb közös többszörösüket pedig $\text{lkkt}\,(a, b)$ vagy $[a, b]$ jelöli.

3.2. Megjegyzés.

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

3.3. Megjegyzés.

Az 3.1. Definíció szerint $\operatorname{lnko}(a, b)$ 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 $\operatorname{lnko}(a, b)$ nem csak nagyobb minden más közös osztónál, de *többszöröse* is minden más közös osztónak.

Tegyük fel, hogy $d = \operatorname{lnko}(a, b)$ 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 $(D_a \cap D_b; \leq)$ részben-rendezett halmaznak is. Tehát az „egyetemi definíció" és az „iskolás definíció" ekvivalens egymással — legalábbis pozitív egész számokra.

Mennyi $\operatorname{lnko}(0, 0)$?

- „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.

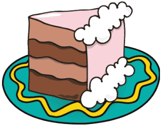
Euklideszi algoritmus

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:*

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

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



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

Euklideszi algoritmus

while $b \neq 0$ **do**
  $b_0 := b$
  $b := \text{maradék}(a, b)$
  $a := b_0$
end while
return a

while $a \neq b$ **do**
  if $a > b$ **then**
    $a := a - b$
  else
    $b := b - a$
  end if
end while
return a

Házi feladat

8. feladat. Az euklideszi algoritmus segítségével állítsa elő az a és b számok legnagyobb közös osztóját $ax + by$ alakban.

(a) $a = 66, \quad b = 51$

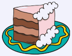
$$3 = 7 \cdot 66 + (-9) \cdot 51$$

(b) $a = 438, \quad b = 126$

$$6 = (-2) \cdot 438 + 7 \cdot 126$$

(c) $a = 754, \quad b = 221$

(d) $a = 564, \quad b = 450$

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. $j = 0, 1, \ldots, i$ 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:

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

Mivel $\operatorname{lnko}(a, b) \sim r_n$, azt kapjuk, hogy $ax_n + by_n \sim \operatorname{lnko}(a, b)$. $\square$

Relatív prímség

3.5. Definíció.

Azt mondjuk, hogy az a, b egész számok **relatív prímek**, ha $\operatorname{lnko}(a, b) = 1$.
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 $\operatorname{lnko}(a, b) \neq 0$, akkor

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

Házi feladat

9. feladat. Milyen számot kell a kérdőjel helyébe írni, hogy minden $k \in \mathbb{Z}$ esetén igaz legyen az ekvivalencia?

(a) $21 \mid 9k \iff ? \mid k$ $\quad$ $48 \mid 84k \iff ? \mid k$

$k = 7$ $\quad$ $k = 4$

(b) $125 \mid 150k \iff ? \mid k$ $\quad$ $150 \mid 125k \iff ? \mid k$

$k = 5$ $\quad$ $k = 6$

(c) $143 \mid 78k \iff ? \mid k$ $\quad$ $78 \mid 143k \iff ? \mid k$

(d) $116 \mid 203k \iff ? \mid k$ $\quad$ $203 \mid 116k \iff ? \mid k$

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 $\operatorname{lnko}(a, b) \mid c$. 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:*

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

Bizonyítás.

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

1. Van megoldás $\iff$ $d \mid c$.

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

$\Longleftarrow$: 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 $x_t = x_0 + \frac{b}{d} \cdot t,\ \ y_t = y_0 - \frac{a}{d} \cdot t$

   $\supseteq$: $\quad a\big(x_0 + \frac{b}{d}t\big) + b\big(y_0 - \frac{a}{d}t\big) = ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t = c$

   $\subseteq$: $\quad$ Legyen $(x, y) \in M$.

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

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

   ezután már egyszerű visszahelyettesítéssel kijön:

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

Házi feladat

10. feladat. Oldja meg az alábbi diofantoszi egyenletek. Adja meg az összes egész megoldást, majd határozza meg azokat a megoldásokat, amelyekre $0 \leq x, y \leq 20$ teljesül.

(a) $6x + 9y = 51$

$x = -17 + 3t,\ y = 17 - 2t, \quad \{(1,5)\,,\ (4,3)\,,\ (7,1)\}$

(b) $6x - 10y = 14$

$x = 14 + 5t,\ y = 7 + 3t, \quad \{(4,1)\,,\ (9,4)\,,\ (14,7)\,,\ (19,10)\}$

(c) $20x + 45y = 245$

(d) $117x - 63y = 36$

Tartalom

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

3.10. 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 $0 \leq r, s < m$.

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

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) $\left(a \equiv b \pmod{m}\right.$ *és* $\left.b \equiv c \pmod{m}\right) \implies a \equiv c \pmod{m}$ *(tranzitivitás);*

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

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

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

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

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

A kongruenciareláció tulajdonságai

Bizonyítás.

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

$$\begin{aligned} a_1 \cdot a_2 \overset{?}{\equiv} b_1 \cdot b_2 \pmod{m} \quad &\Longleftrightarrow \quad m \overset{?}{\mid} a_1 a_2 - b_1 b_2 \\ &\Longleftrightarrow \quad m \overset{?}{\mid} a_1 a_2 - b_1 a_2 + b_1 a_2 - b_1 b_2 \\ &\Longleftrightarrow \quad m \overset{?}{\mid} (a_1 - b_1) \cdot a_2 + b_1 \cdot (a_2 - b_2) \ \checkmark \end{aligned}$$

(5)
$$\begin{aligned} ca \equiv cb \pmod{m} \quad &\Longleftrightarrow \quad m \mid ca - cb = c\,(a-b) \\ &\Longleftrightarrow \quad \tfrac{m}{(m,c)} \mid a - b \\ &\Longleftrightarrow \quad a \equiv b \left(\bmod \tfrac{m}{(m,c)}\right) \end{aligned}$$

(7)
$$\begin{aligned} \left.\begin{array}{l} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{array}\right\} \quad &\Longleftrightarrow \quad m_1, m_2 \mid a - b \\ &\Longleftrightarrow \quad [m_1, m_2] \mid a - b \\ &\Longleftrightarrow \quad a \equiv b \pmod{[m_1, m_2]} \quad \square \end{aligned}$$

Házi feladat

11. feladat. Kongruenciák segítségével igazolja az alábbi oszthatóságokat.

(a) $24 \mid 5^{20} - 1$ $\qquad$ $19 \mid 3^{111} + 2^{444}$

(b) $7 \mid 3^{201} + 2^{102}$ $\qquad$ $7 \mid 3^{2n+1} + 2^{n+2}$

(c) $29 \mid 3^{333} + 2^{111}$ $\qquad$ $13 \mid 4^{2n+1} + 3^{n+2}$

(d) $40 \mid 29^{98} - 1$ $\qquad$ $27 \mid 2^{5n+1} + 5^{n+2}$

Maradékosztályok

3.12. Definíció.

Egy a egész szám modulo m **maradékosztályán** az

$$\overline{a} = \{b \in \mathbb{Z} \colon a \equiv b \pmod{m}\}$$

halmazt értjük.

Jelölés.

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

$$\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}.$$

3.13. Definíció.

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

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

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!

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

Példa.

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

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

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

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

Jelölés.

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

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

Példa.

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

Tartalom

3.17. Definíció.

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

Példa.

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

Egyik módszer:

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

Megoldjuk a diofantoszi egyenletet (y nem is kell):

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

Másik módszer:

$$\begin{aligned} 3x &\equiv 4 \pmod{5} & & \\ 3x &\equiv 9 \pmod{5} & & (\text{mert } 4 \equiv 9 \pmod{5}) \\ x &\equiv 3 \pmod{5} & & (\text{leosztottunk 3-mal (!)}) \end{aligned}$$

3.18. Tétel.

Az $ax \equiv b \pmod{m}$ *lineáris kongruencia akkor és csak akkor oldható meg, ha* $\operatorname{lnko}(a, m) \mid b$.
Ha ez teljesül, akkor a megoldások egyetlen modulo $\frac{m}{\operatorname{lnko}(a,m)}$ *maradékosztályt alkotnak, modulo* m *pedig* $\operatorname{lnko}(a, m)$ *a megoldások száma.*
Ha x_0 *egy megoldás, akkor az általános megoldás:*

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

Bizonyítás.

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

$$\begin{aligned} ax \equiv b \pmod{m} &\iff m \mid ax - b \\ &\iff \exists y \in \mathbb{Z} :\ ax - b = my \\ &\iff \exists y \in \mathbb{Z} :\ ax - my = b \end{aligned}$$

- 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?

$$\begin{aligned} x_{t_1} \equiv x_{t_2} \pmod{m} \quad &\iff x_0 + t_1 \cdot \tfrac{m}{d} \equiv x_0 + t_2 \cdot \tfrac{m}{d} \pmod{m} \\ &\iff t_1 \cdot \tfrac{m}{d} \equiv t_2 \cdot \tfrac{m}{d} \pmod{m} \\ &\iff t_1 \equiv t_2 \pmod{d} \end{aligned}$$

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

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

□

Házi feladat

12. feladat. Oldja meg az alábbi lineáris kongruenciákat.

(a) $3x \equiv 4 \pmod{5}$ $\qquad$ $6x \equiv 21 \pmod{9}$

$x \equiv 3 \pmod{5}$ $\qquad$ $x \equiv 2, 5, 8 \pmod{9}$

(b) $40x \equiv 28 \pmod{62}$ $\qquad$ $104x \equiv 74 \pmod{60}$

$x \equiv 10, 41 \pmod{62}$ $\qquad$ nincs megoldás

(c) $12x \equiv 44 \pmod{10}$ $\qquad$ $42x \equiv 3 \pmod{71}$

(d) $60x \equiv 14 \pmod{91}$ $\qquad$ $24x \equiv 84 \pmod{45}$

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

Jelölés.

Ha nem fenyeget a félreértés veszélye, akkor az a egész szám $\operatorname{mod} m$ multiplikatív inverzét a^{-1}-gyel jelöljük. Hasonlóan $\overline{a} \in \mathbb{Z}_m$ multiplikatív inverzét $\overline{a}^{-1}$ 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 $\operatorname{mod} m$ *egyértelműen meghatározott.*
Hasonlóan, $\overline{a} \in \mathbb{Z}_m$ akkor és csak akkor rendelkezik multiplikatív inverzzel, ha $\overline{a} \in \mathbb{Z}_m^*$. 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 $(p-1)! \equiv -1 \pmod{p}$.

Házi feladat

13. feladat. Határozza meg a $\mathbb{Z}_m$ maradékosztály-gyűrű minden elemének a multiplikatív inverzét (ha létezik).

(a) $m = 14$

$\overline{1}^{-1} = \overline{1},\ \overline{3}^{-1} = \overline{5},\ \overline{5}^{-1} = \overline{3},\ \overline{9}^{-1} = \overline{11},\ \overline{11}^{-1} = \overline{9},\ \overline{13}^{-1} = \overline{13}$

(b) $m = 15$

$\overline{1}^{-1} = \overline{1},\ \overline{2}^{-1} = \overline{8},\ \overline{8}^{-1} = \overline{2},\ \overline{4}^{-1} = \overline{4},$
$\overline{7}^{-1} = \overline{13},\ \overline{13}^{-1} = \overline{7},\ \overline{11}^{-1} = \overline{11},\ \overline{14}^{-1} = \overline{14}$

(c) $m = 18$

(d) $m = 20$

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 $a^{-k} \equiv \left(a^k\right)^{-1} \pmod{m}$.
Hasonlóképpen $\overline{a} \in \mathbb{Z}_m^*$ esetén legyen $\left(\overline{a}\right)^{-k} = \left(\overline{a}^k\right)^{-1}$.

3.24. Megjegyzés.

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

Házi feladat

14. feladat. Számítsa ki a hatványt a megadott maradékosztálytestben.

(a) $\overline{2}^{-3} \in \mathbb{Z}_{11}$

$\overline{7}$

(b) $\overline{3}^{-4} \in \mathbb{Z}_{17}$

$\overline{4}$

(c) $\overline{2}^{-4} \in \mathbb{Z}_{13}$

(d) $\overline{3}^{-3} \in \mathbb{Z}_{19}$

Tartalom

Lineáris kongruenciarendszerek

3.25. Definíció.

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

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

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:

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

Házi feladat

15. feladat. Oldja meg az alábbi kongruenciarendszereket.

(a) $$\left.\begin{aligned} 3x &\equiv 3 \pmod{12} \\ 5x &\equiv 3 \pmod{6} \\ 3x &\equiv 11 \pmod{8} \end{aligned}\right\}$$

$$x \equiv 9 \pmod{24}$$

(b) $$\left.\begin{aligned} 10x &\equiv 2 \pmod{6} \\ 4x &\equiv 3 \pmod{7} \\ 3x &\equiv 5 \pmod{8} \end{aligned}\right\}$$

$$x \equiv 167 \pmod{168}$$

(c) $$\left.\begin{aligned} 4x &\equiv 4 \pmod{6} \\ 11x &\equiv 5 \pmod{9} \\ 3x &\equiv 2 \pmod{5} \end{aligned}\right\}$$

(d) $$\left.\begin{aligned} 3x &\equiv 5 \pmod{10} \\ 3x &\equiv 1 \pmod{8} \\ 14x &\equiv 4 \pmod{6} \end{aligned}\right\}$$

Lineáris kongruenciarendszerek

3.27. Tétel.

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

3.28. Tétel.

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

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

Speciálisan, páronként relatív prím modulusok esetén mindig van megoldás.

3.29. Tétel.

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

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

3.30. Tétel (kínai maradéktétel).

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

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

Ekkor a $(*)$ *lineáris kongruenciarendszer megoldása:*

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

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

Házi feladat

16. feladat. A kínai maradéktétel segítségével oldja meg az alábbi paraméteres kongruenciarendszereket.

(a) $$\left.\begin{aligned} x &\equiv a \pmod 3 \\ x &\equiv b \pmod 4 \\ x &\equiv c \pmod 5 \end{aligned}\right\}$$

$$x \equiv -20a - 15b - 24c \pmod{60}$$

(b) $$\left.\begin{aligned} x &\equiv a \pmod 4 \\ x &\equiv b \pmod 5 \\ x &\equiv c \pmod 9 \end{aligned}\right\}$$

$$x \equiv 45a + 36b - 80c \pmod{180}$$

(c) $$\left.\begin{aligned} x &\equiv a \pmod 3 \\ x &\equiv b \pmod 5 \\ x &\equiv c \pmod 7 \end{aligned}\right\}$$

(d) $$\left.\begin{aligned} x &\equiv a \pmod 3 \\ x &\equiv b \pmod 4 \\ x &\equiv c \pmod 7 \end{aligned}\right\}$$

3.31. Következmény.

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

$$\beta\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ \overline{x} \mapsto (x \bmod m,\ x \bmod n)\,.$$

Bizonyítás.

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

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

A kínai maradéktétel szerint ennek a kongruenciarendszernak valóban létezik megoldása (szürjektivitás), azt pedig már korábban láttuk, hogy a megoldás modulo lkkt$\,(m, n) = mn$ egyértelműen meghatározott (injektivitás). $\square$

Megértést ellenőrző kérdések

Igazak-e az alábbi állítások?

- Az $ax \equiv b \pmod{m}$ lineáris kongruenciának akkor és csak akkor van megoldása, ha lnko $(a, b) \mid m$.
- A $30x \equiv 48 \pmod{58}$ kongruencia ekvivalens a $30x \equiv 48 \pmod{29}$ kongruenciával.
- Az $1, 133, 265, 397, \dots$ és az $1, 151, 301, 451, \dots$ számtani sorozatok második közös tagja 19801.
- Minden p prímszámra $(p-1)! \equiv p - 1 \pmod{p}$.
- Az egész számok halmazán a modulo m kongruencia antiszimmetrikus reláció.
- $|\mathbb{Z}_{15}^*| = |\mathbb{Z}_8|$
- Léteznek olyan a, b, c egész számok, amelyekre az $ax + by = c$ diofantoszi egyenletnek pontosan 2014 megoldása van (az egész számok körében).
- Tetszőleges a, b, c egész számokra $a \mid bc \implies a \mid b$ vagy $a \mid c$.

Tartalom

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

Gyenge multiplikativitás

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 $p_1, \ldots, p_n$ prímszámok és $\alpha_1, \ldots, \alpha_n$ pozitív kitevők esetén

$$f\left(p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}\right) = f\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot f\left(p_n^{\alpha_n}\right).$$

4.5. Tétel.

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

Képletek

4.6. Tétel.

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

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

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

Házi feladat

17. feladat. Határozza meg az n szám osztóinak számát és osztóinak összegét.

(a) $n = 1500$

$\tau\left(1500\right) = 24$, $\sigma\left(1500\right) = 4368$

(b) $n = 7!$

$\tau\left(7!\right) = 60$, $\sigma\left(7!\right) = 19344$

(c) $n = 2016$

(d) $n = 2015$

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: $M_{74\,207\,281}$, ami tízes számrendszerben 22 338 618 számjegyből áll.

Mersenne-prímek

p	$M_p = 2^p - 1$	$2^{p-1}\left(2^p - 1\right)$	
2	3	6	ókori görögök
3	7	28	ókori görögök
5	31	496	ókori görögök
7	127	8128	ókori görögök
13	8 191	3 3550 336	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	$\sim$ 2 trillió	$\sim$ 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
$\vdots$	$\vdots$	$\vdots$	$\vdots$
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*

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

4.12. Definíció.

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

Tartalom

Az Euler-féle φ-függvény

4.14. Definíció.

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

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

Az így kapott függvényt **Euler-féle φ függvénynek** nevezzük. Tömörebben:

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

Példa.

$$\begin{aligned}
\varphi(5) &= |\{1,2,3,4\}| = 4 \\
\varphi(6) &= |\{1,5\}| = 2 \\
\varphi(10) &= |\{1,3,7,9\}| = 4 \\
\varphi(81) &= |\{1,2,4,5,7,8,\ldots,76,77,79,80\}| = 81 - 27 = 54 \\
\varphi(1000) &= 1000 - 500 - 200 + 100 = 400
\end{aligned}$$

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 $c_1, c_2, \ldots, c_m$ egész számok teljes maradékrendszert alkotnak modulo m, és $a, b \in \mathbb{Z}$, $a \perp m$, akkor $ac_1 + b, ac_2 + b, \ldots, ac_m + b$ 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 $c_1, c_2, \ldots, c_{\varphi(m)}$ egész számok redukált maradékrendszert alkotnak modulo m, és $a \in \mathbb{Z}$, $a \perp m$, akkor $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ is redukált maradékrendszer modulo m.

Gyenge multiplikativitás

4.19. Tétel.

Az Euler-féle φ függvény gyengén multiplikatív.

Bizonyítás.

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

$$\beta\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n,\ \overline{x} \mapsto (x \bmod m,\ x \bmod n)\,.$$

Világos, hogy minden x-re

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

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

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

$\square$

Képlet

4.20. Tétel.

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

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

Bizonyítás.

A gyenge multiplikativitás miatt elegendő prímhatványokra igazolni az állítást:

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

□

Házi feladat

18. feladat. Számítsa ki $\varphi(n)$ értékét.

(a) $n = 1500$

$\varphi(1500) = 400$

(b) $n = 7!$

$\varphi(7!) = 1152$

(c) $n = 2015$

(d) $n = 2016$

4.21. Tétel (Euler–Fermat-tétel).

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

Bizonyítás.

Legyen $c_1, c_2, \ldots, c_{\varphi(m)}$ redukált maradékrendszer modulo m.
Mivel $a \perp m$, ezért $ac_1, ac_2, \ldots, ac_{\varphi(m)}$ is redukált maradékrendszer modulo m.

$$\begin{array}{rcll}
c_1 \cdot c_2 \cdot \ldots \cdot c_{\varphi(m)} & \equiv & ac_1 \cdot ac_2 \cdot \ldots \cdot ac_{\varphi(m)} & \pmod{m} \\
& \Downarrow & & \\
c_1 \cdot c_2 \cdot \ldots \cdot c_{\varphi(m)} & \equiv & a^{\varphi(m)} \cdot c_1 \cdot c_2 \cdot \ldots \cdot c_{\varphi(m)} & \pmod{m} \\
& \Downarrow & & \\
1 & \equiv & a^{\varphi(m)} & \pmod{m}
\end{array}$$

□

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 $a^p \equiv a \pmod{p}$.

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

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

$\square$

Házi feladat

19. feladat. Számítsa ki az alábbi hatványok maradékait a megadott modulusra nézve.

(a) $2014^{2014} \equiv ? \pmod 7$ $\qquad$ $2019^{2019} \equiv ? \pmod{11}$

$2014^{2014} \equiv 5^4 \equiv 2$ $\qquad$ $2019^{2019} \equiv 6^{-1} \equiv 2$

(b) $13^{170} \equiv ? \pmod{40}$ $\qquad$ $27^{159} \equiv ? \pmod{40}$

$13^{170} \equiv 13^{10} \equiv 9$ $\qquad$ $27^{159} \equiv 27^{-1} \equiv 3$

(c) $123^{123} \equiv ? \pmod{11}$ $\qquad$ $303^{4039} \equiv ? \pmod{100}$

(d) $4447^{2018} \equiv ? \pmod{44}$ $\qquad$ $10^{188} \equiv ? \pmod{27}$

Tartalom

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

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

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

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

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:
$D_a = \{u_1, \ldots, u_k\}\,,\ D_b = \{v_1, \ldots, v_\ell\}\,.$

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

Összegzési függvény

4.27. Definíció.

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

Jelölés.

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

4.28. Tétel.

Gyengén multiplikatív számelméleti függvény összegzési függvénye is gyengén multiplikatív.

Bizonyítás.

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

4.29. Tétel.

A tanult nevezetes számelméleti függvények között fennállnak az alábbi összefüggések:

$$\delta \to \mathbf{1} \to \tau, \quad \varphi \to \mathrm{id} \to \sigma.$$

Bizonyítás.

Jelölje Φ a φ függvény összegzési függvényét. Mivel φ gyengén multiplikatív, Φ is az (és persze id is), így elegendő a $\Phi(n) \stackrel{?}{=} \mathrm{id}(n)$ egyenlőséget prímhatványokra ellenőrizni. Tetszőleges p prím és $\alpha \in \mathbb{N}$ esetén

$$\begin{aligned}
\Phi(p^\alpha) &= \varphi(1) + \varphi(p) + \varphi\left(p^2\right) + \cdots + \varphi\left(p^{\alpha-1}\right) + \varphi(p^\alpha) \\
&= 1 + (p-1) + \left(p^2 - p\right) + \cdots + \left(p^{\alpha-1} - p^{\alpha-2}\right) + \left(p^\alpha - p^{\alpha-1}\right) \\
&= p^\alpha = \mathrm{id}(p^\alpha).
\end{aligned}$$

$\square$

A Möbius-féle μ-függvény

4.30. Definíció.

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

4.31. Megjegyzés.

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

4.32. Definíció.

Möbius-függvénynek nevezzük az alábbi képlettel definiált μ számelméleti függvényt:

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

4.33. Tétel.

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

Bizonyítás.

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

$$\begin{aligned} M(p^\alpha) &= \mu(1) + \mu(p) + \mu\left(p^2\right) + \cdots + \mu\left(p^{\alpha-1}\right) + \mu(p^\alpha) \\ &= 1 + (-1) + 0 + \cdots + 0 + 0 \\ &= 0 = \delta(p^\alpha). \end{aligned}$$

$\square$

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 $f \to F$ akkor és csak akkor áll fenn, ha $f = F * \mu$.

Részletesebben: tetszőleges f, F számelméleti függvények esetén

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

Bizonyítás.

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

$\Longrightarrow$: Tfh. $F = f * \mathbf{1}$. „Konvolváljuk be" az egyenlőség mindkét oldalát μ-vel:

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

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

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

4.35. Következmény.

Gyengén multiplikatív számelméleti függvény megfordítási függvénye is gyengén multiplikatív.

Bizonyítás.

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

□

Házi feladat

20. feladat. Legyen a f számelméleti függvény összegzési függvénye F. Számítsa ki a f függvény értékét a megadott helyen.

(a) $F(n) = n^2, \qquad f(12) = ?$

$$f(12) = 12^2 - 6^2 - 4^2 + 2^2 = 96$$

(b) $F(n) = \log n, \qquad f(81) = ?$

$$f(81) = \log 81 - \log 27 = \log 3$$

(c) $F(n) = \log n, \qquad f(36) = ?$

(d) $F(n) = n, \qquad f(100) = ?$

Megértést ellenőrző kérdések

Igazak-e az alábbi állítások?

- A 2015 tökéletes szám.
- Minden n természetes számra $\sum_{d|n} d\mu\left(\frac{n}{d}\right) = \varphi(n)$.
- Az n természetes szám akkor és csak akkor tökéletes, ha $\varphi(n) = 2n$.
- Az identikus függvény összegzési függvénye a σ (osztók összege) függvény.
- Tetszőleges a, m $(m \geq 2)$ egész számok esetén,
  $a \equiv 1 \pmod{m} \implies a^{m-1} \equiv 1 \pmod{m}$.
- Tetszőleges n pozitív egész szám esetén: n prím $\implies$ $2^n - 1$ prím.
- Bármely két modulo m redukált maradékrendszernek ugyanannyi eleme van.
- Ha n nem négyzetszám, akkor $\mu(n) \neq 0$.

Tartalom

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 $\operatorname{lnko}(f, g) \mid h$.

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:

$$u_t = u_0 + \frac{g}{\operatorname{lnko}(f, g)} \cdot t;$$

$$v_t = v_0 - \frac{f}{\operatorname{lnko}(f, g)} \cdot t.$$

Diofantoszi egyenlet polinomgyűrűben

Példa.

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

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

$$\begin{aligned} f &= (x+1) \cdot g && + \quad 2x^2 + 4x + 6 \\ g &= (x-1) \cdot \left(x^2 + 2x + 3\right) && + \quad 0 \end{aligned}$$

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

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: $u_0 = \dfrac{1}{2}, \quad v_0 = -\dfrac{1}{2}x - \dfrac{1}{2}.$

Házi feladat

21. feladat. Számítsa ki az f és g polinomok legnagyobb közös osztóját, és adja meg az $fu + gv = \text{lnko}\,(f, g)$ egyenlet egy megoldását az $\mathbb{R}\,[x]$ polinomgyűrűben.

(a) $f = x^4 + 2x^3 + 4x^2 + 2x + 3,$ $\quad g = x^3 + x^2 + x - 3$

$\text{lnko}\,(f, g) = x^2 + 2x + 3,$ $\quad u = \frac{1}{2},\ v = -\frac{1}{2}x - \frac{1}{2}$

(b) $f = x^4 + 2x^3 - x^2 - 4x - 2,$ $\quad g = x^4 + x^3 - x^2 - 2x - 2$

$\text{lnko}\,(f, g) = x^2 - 2,$ $\quad u = -x - 1,\ v = x + 2$

(c) $f = x^4 + x^3 + 2x^2 + 3x - 3,$ $\quad g = x^4 + x^3 + x^2 + 3x - 6$

(d) $f = x^5 + 3x^4 + x^3 + x^2 + 3x + 1,$ $\quad g = x^4 + 2x^3 + x + 2$

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

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

$$\begin{aligned}
x^3 + \overline{2}x^2 + \overline{4}x + \overline{2} &= (x + \overline{4}) \cdot (x^2 + \overline{3}x + \overline{1}) &&+ \quad x + \overline{3} \\
x^2 + \overline{3}x + \overline{1} &= x \cdot (x + \overline{3}) &&+ \quad \overline{1} \\
x + \overline{3} &= (x + \overline{3}) \cdot \overline{1} &&+ \quad \overline{0}
\end{aligned}$$

Fejezzük ki $\overline{1}$-et f és g segítségével:

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

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

Házi feladat

22. feladat. Határozza meg az $fu + gv = \overline{1}$ egyenlet egy megoldását a megadott polinomgyűrűben.

(a) $f = x^4 + \overline{6}x^3 + \overline{3}x^2 + \overline{2}x + \overline{4}$, $\quad g = x^2 + \overline{6}x + \overline{3} \in \mathbb{Z}_7[x]$

$u = \overline{5}x + \overline{6}$, $v = \overline{2}x^3 + x^2 + \overline{4}$

(b) $f = x^3 + x^2 + \overline{1}$, $\quad g = x^2 + \overline{1} \in \mathbb{Z}_2[x]$

$u = x$, $v = x^2 + x + \overline{1}$

(c) $f = x^3 + x + \overline{1}$, $\quad g = \overline{3}x^2 + \overline{2} \in \mathbb{Z}_5[x]$

(d) $f = x^3 + x^2 + \overline{2}$, $\quad g = \overline{2}x^2 + x + \overline{3} \in \mathbb{Z}_5[x]$

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 végiggondolni!). 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, melyenek elemei egyértelműen felírhatók az alábbi alakban:

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

5.3. Tétel.

Az $\overline{f} \in T[x] / (m)$ 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 $\mathbb{R}[x] \, / \, \left(x^2+1\right)$ 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 $\mathbb{R}[x] \, / \, \left(x^2+1\right)$ test minden eleme egyértelműen felírható a következő alakban:
$$\overline{a+bx} \qquad (a, b \in \mathbb{R}) \, .$$
- Összeadás: $$\overline{a+bx} + \overline{c+dx} = \overline{(a+c)+(b+d)x}.$$
- Szorzás: $$\begin{aligned} \overline{a+bx} \cdot \overline{c+dx} &= \overline{ac+(ad+bc)x+bdx^2} \\ &= \overline{ac+(ad+bc)x+bd\,(-1)} \\ &= \overline{(ac-bd)+(ad+bc)x}. \end{aligned}$$

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

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

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

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

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

A nyolcelemű test művelettáblázatai

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Számolás $\mathbb{Q}[x]$ faktortesteiben

Példa.

Határozzuk meg a $K = \mathbb{Q}[x] \,/\, \left(x^3 - 7\right)$ 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 $\overline{u} = \overline{2-x}^{\,-1}$ elemet is megkapni.

$$\begin{aligned}
\overline{2-x}^{\,-1} = \overline{u} &\iff \overline{2-x} \cdot \overline{u} = \overline{1} \\
&\iff (2-x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2-x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff \overline{u} = \overline{x^2 + 2x + 4}
\end{aligned}$$

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

Példa (folyt.).

Az előző számolás eredménye összefoglalva:

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

Írjunk x helyébe $\sqrt[3]{7}$-et:

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

Tehát azt kapjuk, hogy

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

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

Tartalom

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

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

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

A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

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 ...)

Házi feladat

23. feladat. Bontsa irreducibilis tényezők szorzatára az f polinomot a megadott polinomgyűrűben.

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

$(x-1)^2(x-3)(x-4)(x^2+4x+2)$

(b) $f = x^5 + x^4 + \overline{2}x^3 + x^2 + \overline{1} \in \mathbb{Z}_3[x]$

$(x-1)(x-2)\left(x^3+x^2+2\right)$

(c) $f = x^5 + x^4 + \overline{2}x^3 + \overline{2}x + \overline{1} \in \mathbb{Z}_3[x]$

(d) $f = x^5 + x^4 + \overline{2}x^3 + \overline{1} \in \mathbb{Z}_5[x]$

5.8. Tétel.

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

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 $\mathrm{GF}(q)$ jelöli (Galois Field).

Véges testek

Példa.

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

Emlékeztető

5.9. Definíció.
Az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinom $c \in T$ helyen vett **helyettesítési értékén** az $f(c) = a_n c^n + \cdots + a_1 c + a_0 \in T$ elemet értjük.
Az $f \in T[x]$ polinomhoz tartozó **polinomfüggvény** pedig nem más, mint az

$$f\colon T \to T,\ c \mapsto f(c)$$

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 határozatlannak).

Polinom vs. polinomfüggvény

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

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

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

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0},\ \overline{1} \mapsto \overline{1},\ \overline{2} \mapsto \overline{2}.$$

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 $T \to T$ 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!!!

Tartalom

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

$$f \text{ irreducibilis } K \text{ felett} \quad \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \quad f \text{ irreducibilis } T \text{ felett.}$$

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: $\sqrt{3},\ -\sqrt{3},\ \alpha,\ \overline{\alpha},\ \beta,\ \overline{\beta}$, ahol

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

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

$$f = (x - \sqrt{3})(x + \sqrt{3})\,(x - \alpha)\,(x - \overline{\alpha})\,(x - \beta)\,\left(x - \overline{\beta}\right).$$

Az $\mathbb{R}$ feletti felbontás:

$$\begin{aligned} f &= (x - \sqrt{3})(x + \sqrt{3})\left(x^2 - 2\,\mathrm{Re}\,\alpha \cdot x + |\alpha|^2\right)\left(x^2 - 2\,\mathrm{Re}\,\beta \cdot x + |\beta|^2\right) \\ &= (x - \sqrt{3})(x + \sqrt{3})\left(x^2 - \sqrt{3}x + 3\right)\left(x^2 + \sqrt{3}x + 3\right). \end{aligned}$$

A $\mathbb{Q}$ feletti felbontás:

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

Házi feladat

24. feladat. Határozza meg az f polinom irreducibilis felbontását $\mathbb{R}$ és $\mathbb{Q}$ felett.

(a) $f = x^6 - 27$

$\mathbb{R}[x]$-ben: $(x-\sqrt{3})(x+\sqrt{3})(x^2-\sqrt{3}x+3)(x^2+\sqrt{3}x+3)$

$\mathbb{Q}[x]$-ben: $(x^2-3)(x^4+3x^2+9)$

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

$\mathbb{R}[x]$-ben: $\left(x^2-\sqrt{3}x+1\right)\left(x^2+\sqrt{3}x+1\right)$

$\mathbb{Q}[x]$-ben: x^4-x^2+1

(c) $f = x^6 + 125$

(d) $f = x^8 - 81$

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

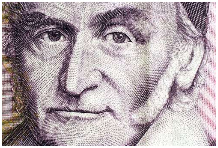
5.10. Tétel.

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

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

Bizonyítás.



$\square$

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 $0 < \deg g \overset{\text{ÁMN}}{\leq} \deg h < n$.

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) számhármasra 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.

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

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 $\|$ jelöli: $p \| a \iff p \mid a$ és $p^2 \nmid a$.

Példa.

$$3 \| 12 \quad \text{de} \quad 2 \not\| 12$$

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

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

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

akkor f *irreducibilis a racionális számok teste felett.*

Irreducibilis polinomok $\mathbb{Q}$ felett

5.14. Következmény.

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

Bizonyítás.

$x^n + 2$ $\square$

Érdemes 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 következzék inkább a tétel „tükörképe”.

5.16. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium).

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

5.17. Tétel (Rolle tétele).

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ *egy tetszőleges egész együtthatós polinom. Ha* $\frac{p}{q}$ *egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz* $p, q \in \mathbb{Z}$, $q \neq 0$ *és* $\mathrm{lnko}\,(p, q) = 1$), *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 $(\operatorname{lnko}(p,q)=1)$.

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

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1}}_{p\,\mid} + \underbrace{a_0 q^n}_{\Longrightarrow\quad p\,\mid} \quad\Longrightarrow\quad p \mid a_0$$

Hasonlóan:

$$q \mid a_n \quad\Longleftarrow\quad \underbrace{a_n p^n}_{q\,\mid} \quad\Longleftarrow\quad + \underbrace{a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n}_{q\,\mid} = 0$$

$\square$

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

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

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

Házi feladat

25. feladat. Határozza meg az f polinom irreducibilis felbontását $\mathbb{Q}$ felett.

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

$(2x+1)(x+1)^2(x^4+6x+12)$

(b) $f = 2x^5 + 3x^4 - 7x^3 - 3x^2 + 8x - 12$

$(2x-3)(x+2)^2(x^2-x+1)$

(c) $f = 5x^8 - 5x^7 + 4x^2 - 2x - 2$

(d) $f = 3x^6 + 2x^5 - 7x^4 + 2$

Tartalom

Elemi törtekre bontás a racionális számok körében

5.18. Definíció.

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

5.19. Tétel.

Minden racionális szám felírható egy egész szám és elemi törtek 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 prímhatvány nevezőjű törtek 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 törtekre bontás a racionális számok körében

Bizonyítás (folyt.)

2. Maradékos osztás segítségével leválasztva a törtek egészrészét, elérhetjük, hogy minden törtünk $\dfrac{c}{p^k}$ 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 $\dfrac{c}{p^k}$ 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** $\dfrac{f}{g}$ alakú formális kifejezést értünk, ahol $f, g \in T[x]$ és $g \neq 0$. Minden racionális törthöz tartozik egy **racionális törtfüggvény** (a két fogalom nem összekeverendő!). A T feletti racionális törtek halmazát $T(x)$ jelöli.

5.21. 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:

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

Elemi törtekre bontás test feletti racionális törtek körében

5.22. Tétel.

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

5.23. Következmény.

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

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

alakú racionális tört összegeként.

5.24. Következmény.

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

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

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

alakú racionális tört összegeként.

Elemi törtekre bontás test feletti racionális törtek körében

Példa.

Bontsuk parciális törtek összegére $\mathbb{R}$ felett az $\dfrac{1}{x^2+x}$ 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 törtekre bontás test feletti racionális törtek körében

Példa.

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

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

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

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

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

$$\Updownarrow$$

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

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

Példa (folyt.).

A kapott hétismeretlenes lineáris egyenletrendszert megoldjuk:

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

Tehát

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

Elemi törtekre bontás test feletti racionális törtek körében

Példa.

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

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

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

$$\Updownarrow$$

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

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

Példa (folyt.).

A kapott hétismeretlenes lineáris egyenletrendszert megoldjuk:

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

Tehát

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

Megértést ellenőrző kérdések

- Létezik-e harmadfokú irreducibilis polinom $\mathbb{Z}_2$ felett?
- Létezik-e 2014-edfokú irreducibilis polinom $\mathbb{R}$ felett?
- Igaz-e minden $f \in \mathbb{Q}[x]$ polinomra, hogy ha f irreducibilis $\mathbb{Q}$ felett, akkor f-nek nincs valós gyöke?
- Létezik-e olyan $f \in \mathbb{Q}[x]$ polinom, ami irreducibilis $\mathbb{R}$ felett, de nem irreducibilis $\mathbb{Q}$ felett?
- Igaz-e tetszőleges T testre és $f, g \in T[x]$ polinomokra, hogy ha minden $c \in T$ esetén $f(c) = g(c)$, akkor $f = g$?
- Létezik-e olyan $0 \neq f \in \mathbb{Z}[x]$ főpolinom, amelynek $\frac{1}{2}$ gyöke?
- Létezik-e olyan irreducibilis polinom $\mathbb{Q}$ felett, amelynek van racionális gyöke?
- Igaz-e tetszőleges $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomra, hogy ha nem létezik olyan p prímszám, amelyre $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_1$, $p \parallel a_0$, akkor f nem irreducibilis $\mathbb{Q}$ felett? Ha nem, akkor adjon meg egy ellenpéldát!

Tartalom

Gyökök és együtthatók közötti összefüggés

Ha az $f = x^2 + a_1 x + a_0 \in \mathbb{C}[x]$ polinom gyökei α_1 és α_2, akkor

$$x^2 + a_1 x + a_0 = (x - \alpha_1)(x - \alpha_2) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2,$$

következésképp

$$-a_1 = \alpha_1 + \alpha_2 \quad \text{és} \quad a_0 = \alpha_1\alpha_2.$$

Ha az $f = x^3 + a_2 x^2 + a_1 x + a_0 \in \mathbb{C}[x]$ polinom gyökei $\alpha_1, \alpha_2, \alpha_3$, akkor

$$\begin{aligned} x^3 + a_2 x^2 + a_1 x + a_0 &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = \\ &= x^3 - (\alpha_1+\alpha_2+\alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3, \end{aligned}$$

következésképp

$$\begin{aligned} -a_2 &= \alpha_1 + \alpha_2 + \alpha_3, \\ a_1 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3, \\ -a_0 &= \alpha_1\alpha_2\alpha_3. \end{aligned}$$

Gyökök és együtthatók közötti összefüggés

6.1. Tétel.

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

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

Bizonyítás.

Az $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha_1)\cdots(x - \alpha_n)$ egyenlőség bal oldalán x^{n-k} együtthatója a_{n-k}, míg a jobb oldalon

$$(-\alpha_1)\cdots(-\alpha_k) + \ldots$$

□

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 $\alpha_1, \ldots, \alpha_n$ betűkből képezett összes k-tényezős szorzat összege, tehát egy $\binom{n}{k}$-tagú összeg. Formálisan:

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

Még formálisabban:

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

Tartalom

Többhatározatlanú polinomok

6.3. Definíció.

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

Jelölés.

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

6.4. Tétel.

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

6.5. Megjegyzés.

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

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

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

Többhatározatlanú polinomok

Példa.

$$f = 7x_1^2x_3 - 2x_1x_2x_3^4 + 9x_1x_2 - 3x_1^2x_2x_3^2 + x_1x_2x_3^3 - 2x_1^2 + 5x_1x_2^2x_3 - x_1^2x_2x_3 - 6x_1x_3 + 2x_3^2 + x_1x_3^2 + 4x_2^2x_3^2 + 8 \qquad \in \mathbb{R}\left[x_1, x_2, x_3\right]$$

$$f = x_1^2 \cdot \left(-3x_2x_3^2 - x_2x_3 + 7x_3 - 2\right) + x_1 \cdot \left(5x_2^2x_3 - 2x_2x_3^4 + x_2x_3^3 + 9x_2 + x_3^2 - 6x_3\right) + \left(4x_2^2x_3^2 + 2x_3^2 + 8\right) \qquad \in \mathbb{R}\left[x_2, x_3\right]\left[x_1\right]$$

$$f = x_1^2 \cdot \Big(x_2 \cdot (-3x_3^2 - x_3) + (7x_3 - 2)\Big) + x_1 \cdot \Big(x_2^2 \cdot (5x_3) - x_2\left(2x_3^4 + x_3^3 + 9\right) + \left(x_3^2 - 6x_3\right)\Big) + \Big(x_2^2 \cdot \left(4x_3^2\right) + \left(2x_3^2 + 8\right)\Big) \qquad \in \mathbb{R}\left[x_3\right]\left[x_2\right]\left[x_1\right]$$

6.6. Definíció.

Azt mondjuk, hogy az $ax_1^{k_1} \cdots x_n^{k_n}$ monom **lexikografikusan megelőzi** a $bx_1^{l_1} \cdots x_n^{l_n}$ 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 $l_1, l_2, \dots, l_n$ kitevősorozatok között, és amelyikben 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, $M \sqsupseteq N$ pedig azt, hogy $M \sqsupset N$ vagy $M \sim N$. A $\sqsupseteq$ 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 $\underset{\sim}{\sqsupset}$ reflexív, tranzitív és dichotóm reláció, valamint $M \underset{\sim}{\sqsupset} N$ és $M \underset{\sim}{\sqsubset} N$ akkor és csak akkor áll fenn egyszerre, ha M és N asszociált.

6.8. Megjegyzés.

Az előző állítás szerint a $\underset{\sim}{\sqsupset}$ 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 $M \underset{\sim}{\sqsupset} N$ és $\hat{M} \underset{\sim}{\sqsupset} \hat{N}$, akkor $M\hat{M} \underset{\sim}{\sqsupset} N\hat{N}$, 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:

$$f = -3x_1^2x_2x_3^2 - x_1^2x_2x_3 + 7x_1^2x_3 - 2x_1^2 + 5x_1x_2^2x_3 - 2x_1x_2x_3^4 +$$
$$+ x_1x_2x_3^3 + 9x_1x_2 + x_1x_3^2 - 6x_1x_3 + 4x_2^2x_3^2 + 2x_3^2 + 8$$

6.10. Állítás.

Tetszőleges $f, g \in T[x_1, \ldots, x_n]$ 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:

$$f = M_1 + \cdots + M_s, \quad M_1 \sqsupset \cdots \sqsupset M_s, \quad \mathrm{LET}(f) = M_1;$$
$$g = N_1 + \cdots + N_t, \quad N_1 \sqsupset \cdots \sqsupset N_t, \quad \mathrm{LET}(g) = N_1.$$

$$fg = (M_1 + \cdots + M_s)(N_1 + \cdots + N_t) = M_1N_1 + \cdots + M_sN_t = \sum_{i=1}^{s}\sum_{j=1}^{t} M_iN_j.$$

Ha $(i, j) \neq (1, 1)$, akkor $M_1 \sqsupseteq M_i$, $N_1 \sqsupseteq N_j$, és e két egyenlőtlenség közül legalább az egyik szigorú. Tehát $M_1N_1 \sqsupset M_iN_j$, azaz $\mathrm{LET}(fg) = M_1N_1 = \mathrm{LET}(f)\,\mathrm{LET}(g)$. □

Tartalom

Szimmetrikus polinomok

6.11. Definíció.

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

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

6.12. Definíció.

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

Jelölés.

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

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

6.13. Megjegyzés.

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

Szimmetrikus polinomok

Példa.

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

$$\begin{aligned}
\alpha_1 + \alpha_2 + \alpha_3 &= \sigma_1(\alpha_1, \alpha_2, \alpha_3) = -2, \\
\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= \sigma_2(\alpha_1, \alpha_2, \alpha_3) = 8, \\
\alpha_1\alpha_2\alpha_3 &= \sigma_3(\alpha_1, \alpha_2, \alpha_3) = -6.
\end{aligned}$$

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* kifejezései a gyököknek.

A szimmetrikus polinomok alaptétele

6.14. Tétel.

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

6.15. Lemma.

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

$$k_1 \geq \cdots \geq k_n.$$

Bizonyítás.

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

6.16. Lemma.

Tetszőleges $k_1 \geq \cdots \geq k_n$ nemnegatív egészekhez léteznek olyan $l_1, \ldots, l_n$ nemnegatív egészek, hogy $\sigma_1^{l_1} \cdot \ldots \cdot \sigma_n^{l_n} \in T\left[x_1, \ldots, x_n\right]$ lexikografikusan első tagja éppen $x_1^{k_1} \cdots x_n^{k_n}$.

A szimmetrikus polinomok alaptétele

6.17. Tétel (a szimmetrikus polinomok alaptétele).

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

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

Példa.

Fejezzük ki az $f = x_1^3 + x_2^3 + x_3^3 \in \mathbb{R}\left[x_1, x_2, x_3\right]$ 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

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

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

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= \sigma_1(\alpha_1, \alpha_2, \alpha_3) = 3, \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= \sigma_2(\alpha_1, \alpha_2, \alpha_3) = 1, \\ \alpha_1\alpha_2\alpha_3 &= \sigma_3(\alpha_1, \alpha_2, \alpha_3) = 8. \end{aligned}$$

Az előző feladat alapján

$$\begin{aligned} \alpha_1^3 + \alpha_2^3 + \alpha_3^3 =& \sigma_1(\alpha_1, \alpha_2, \alpha_3)^3 - 3\sigma_1(\alpha_1, \alpha_2, \alpha_3)\sigma_2(\alpha_1, \alpha_2, \alpha_3) + 3\sigma_3(\alpha_1, \alpha_2, \alpha_3) = \\ =& 3^3 - 3 \cdot 3 \cdot 1 + 3 \cdot 8 = 42 \end{aligned}$$

Példa (folyt.).

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= \sigma_1(\alpha_1, \alpha_2, \alpha_3) = 3, \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= \sigma_2(\alpha_1, \alpha_2, \alpha_3) = 1, \\ \alpha_1\alpha_2\alpha_3 &= \sigma_3(\alpha_1, \alpha_2, \alpha_3) = 8. \end{aligned}$$

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:

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

Házi feladat

26. feladat. Legyenek az f polinom komplex gyökei $\alpha_1, \alpha_2, \alpha_3$. Határozza meg a megadott kifejezés értékét a gyökök kiszámítása nélkül.

(a) $f = x^3 - 3x^2 + x - 8,$ $\quad \alpha_1^3 + \alpha_2^3 + \alpha_3^3 = ?$

$\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \rightsquigarrow 42$

(b) $f = 2x^3 + 4x^2 - 6x + 2,$ $\quad \alpha_1^4 + \alpha_2^4 + \alpha_3^4 = ?$

$\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3 \rightsquigarrow 90$

(c) $f = 3x^3 + 6x^2 + 24x + 18,$ $\quad \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = ?$

(d) $f = x^3 + 6x^2 - 5x - 10,$ $\quad \alpha_1^2\alpha_2 + \alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 + \alpha_1\alpha_3^2 + \alpha_2^2\alpha_3 + \alpha_2\alpha_3^2 = ?$

Diszkrimináns

6.18. Definíció.

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

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

ahol $\alpha_1, \ldots, \alpha_n$ 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:

$$\begin{aligned} D &= (\alpha_1 - \alpha_2)^2 = \alpha_1^2 + \alpha_2^2 - 2\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 \\ &= (-b)^2 - 4c = b^2 - 4c \end{aligned}$$

A harmadfokú polinom diszkriminánsa

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

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

$$\sigma_2 = x_1 x_2 + x_1 x_3 + x_2 x_3$$

$$\sigma_3 = x_1 x_2 x_3$$

$$\begin{aligned} D = \quad & x_1^4 x_2^2 - 2x_1^4 x_2 x_3 + x_1^4 x_3^2 - 2x_1^3 x_2^3 + 2x_1^3 x_2^2 x_3 + 2x_1^3 x_2 x_3^2 - 2x_1^3 x_3^3 \\ & + x_1^2 x_2^4 + 2x_1^2 x_2^3 x_3 - 6x_1^2 x_2^2 x_3^2 + 2x_1^2 x_2 x_3^3 + x_1^2 x_3^4 - 2x_1 x_2^4 x_3 \\ & + 2x_1 x_2^3 x_3^2 + 2x_1 x_2^2 x_3^3 - 2x_1 x_2 x_3^4 + x_2^4 x_3^2 - 2x_2^3 x_3^3 + x_2^2 x_3^4 \end{aligned}$$

A harmadfokú polinom diszkriminánsa

$$D - \sigma_1^2\sigma_2^2 =$$

$$-4x_1^4x_2x_3 - 4x_1^3x_2^3 - 6x_1^3x_2^2x_3 - 6x_1^3x_2x_3^2 - 4x_1^3x_3^3$$
$$-6x_1^2x_2^3x_3 - 21x_1^2x_2^2x_3^2 - 6x_1^2x_2x_3^3 - 4x_1x_2^4x_3$$
$$-6x_1x_2^3x_3^2 - 6x_1x_2^2x_3^3 - 4x_1x_2x_3^4 - 4x_2^3x_3^3$$

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

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

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

$$18x_1^3x_2^2x_3 + 18x_1^3x_2x_3^2 + 18x_1^2x_2^3x_3 + 27x_1^2x_2^2x_3^2$$
$$+18x_1^2x_2x_3^3 + 18x_1x_2^3x_3^2 + 18x_1x_2^2x_3^3$$

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

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

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 Viéte-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

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

Tartalom

Pitagoraszi számhármasok

7.1. Definíció.

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

7.2. Megjegyzés.

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

Példa.

- $(3, 4, 5)$
- $(5, 12, 13)$
- $(8, 15, 17)$
- $(7, 24, 25)$
- $\ldots$

7.3. Lemma.

Primitív pitagoraszi számhármasban a tagok páronként is relatív prímek.

Bizonyítás.

Legyen (x, y, z) primitív pitagoraszi számhármas, $d := \operatorname{lnko}(x, y)$.

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

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

7.4. Lemma.

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

Bizonyítás.

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

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

$\square$

Pitagoraszi számhármasok

7.5. Tétel.

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

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

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

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.

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

7.9. Lemma.

A $4k + 1$ alakú prímszámok előállnak két négyzetszám összegeként, a $4k + 3$ alakú prímek 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 prímek páros kitevővel szerepelnek.

Példa.

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

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

$$13949 = 13 \cdot 29 \cdot 37 = \left(2^2 + 3^2\right) \cdot \left(2^2 + 5^2\right) \cdot \left(1^2 + 6^2\right) = \left(11^2 + 16^2\right) \cdot \left(1^2 + 6^2\right)$$

$$= 85^2 + 82^2$$

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 előállításaival kapcsolatos problémákat összefoglaló néven Waring-problémakörnek szokás nevezni. Edward Waring XVIII. századi angol matematikus Meditationes Algebraicae című művében azt állította (bizonyítás nélkül), hogy minden szám előállítható kilenc köbszám összegeként, illetve tizenkilenc negyedik hatvány összegeként. Ezek az állítások helyesnek bizonyultak, de csak a huszadik században találtak rájuk bizonyítást.

7.12. Megjegyzés (folyt.).

Általában $g\left(k\right)$ jelöli azt a legkisebb számot, amelyre igaz az, hogy minden természetes szám előállítható $g\left(k\right)$ darab k-adik hatvány összegeként.

Az előzőek alapján tehát $g\left(2\right)=4, g\left(3\right)\leq 9, g\left(4\right)\leq 19$, és példák mutatják, hogy 8 köb, illetve 18 negyedik hatvány nem mindig elég, tehát $g\left(3\right)=9$ és $g\left(4\right)=19$.

A $g\left(k\right)$ számok meghatározása igen nehéz probléma, még az sem világos, hogy egyáltalán léteznek[§] minden k-ra, bár ezt már Waring is sejtette. Hilbert igazolta Waring sejtését, és van egy feltételezett képlet is a $g\left(k\right)$ számokra:

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

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.

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

Tartalom

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

7.19. Definíció.

Ikerprímnek 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).

A prímharmonikus sor

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).

A prímszámtétel

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*

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

7.27. Következmény.

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

Tartalom

Algebrai és transzcendens számok

7.28. Definíció.

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

7.29. Definíció.

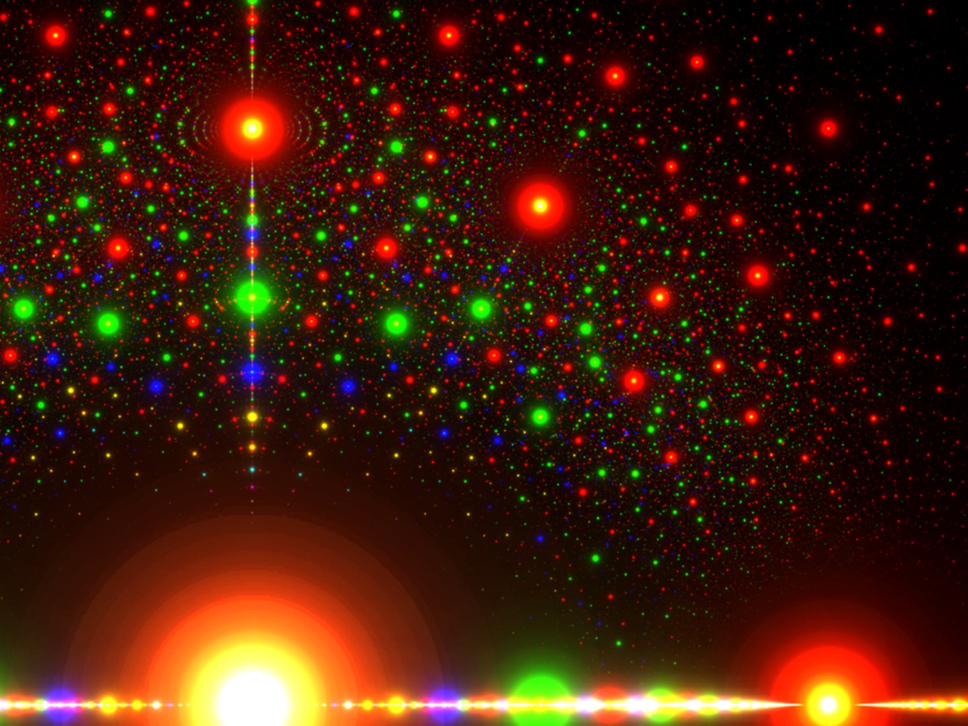
Ha $f \in \mathbb{Q}[x]$ minimális fokszámú mindazon nemzéró racionális együtthatós főpolinomok között, melyeknek α gyöke, akkor f-et az α algebrai szám **minimálpolinomjának** nevezzük.

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 α algebrai szám gyöke, akkor f megegyezik α minimálpolinomjával.

7.31. Tétel.

Létezik transzcendens szám.



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?).
- π 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 α^β transzcendens szám.

  Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $i^i = e^{-\pi/2}$ transzcendens számok.

Diofantoszi approximáció

Adott α valós számhoz szeretnénk olyan $\frac{p}{q}$ közelítő törtet találni ($p, q \in \mathbb{Z}$, $q > 0$, $p \perp q$), amelyre $\left|\alpha - \frac{p}{q}\right|$ kicsi, és q nem túl nagy.

7.32. Tétel (Dirichlet approximációs tétele).

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

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

7.33. Következmény.

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

7.34. Állítás.

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

7.35. Tétel (Hurwitz tétele).

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

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

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

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

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

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

Algebrai számok és gyökmennyiségek

7.37. Tétel.

Az algebrai számok résztestet alkotnak a komplex számok testében.

7.38. Tétel.

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

7.39. Definíció.

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

7.40. Következmény.

A gyökmennyiségek algebrai számok.

Példa.

Ez a szám algebrai:

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

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 megoldóképlete, 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* $f = a_n x^n + \cdots + a_1 x + a_0$ *polinomnak, ahol* $a_0, \ldots, a_n$ *algebrai számok, akkor* α *maga is algebrai szám.*