

Diszkrét matematika 1.

Fülöp Ágnes

ELTE IK Komputeralgebra Tanszék

2015. május 2.

Gyakorlat:

- ZH időpontja:** március 30-án 14-től Mogyoródi teremben
 - ZH időpontja:** május 11-én 14-től Mogyoródi teremben
- PotZH időpontja:**

Vizsga időpontok: szerda, péntek (NEPTUN)

Vizsa tételek: 204-222

Előadás:

- előadás: 1-30 (február 9.)
- előadás: 31-72 (február 16.)
- előadás: 73-90 (február 23.)
- előadás: 91-122 (március 2.)
- előadás: 123-138 (március 9.)
- előadás: 139-159 (március 16.)
- előadás: 160-186 (március 23.)
- előadás: 1. ZH (március 30.)

9. előadás: 186-202 (április 13.)

10. előadás: (április 20.)

11. előadás (április 27.)

12. előadás (május 4.)

előadás: 2. ZH (május 11.)

PotZH

Harmadfokú egyenlet

Harmadfokú egyenlet megoldása

Keressük meg az

$$ax^3 + bx^2 + cx + d = 0$$

egyenlet megoldásait ($a \neq 0$)!

Végigosztva a -val kapjuk az $x^3 + b'x^2 + c'x + d' = 0$ egyszerűbb egyenletet.

Emlékeztető: másodfokú egyenlet megoldása: $x^2 + px + q = 0$.

Az $x = y - \frac{p}{2}$ helyettesítéssel eltűnik az x -es tag: $y^2 + q' = 0$.

Innen átrendezéssel és gyökvonással megkapjuk a lehetséges megoldásokat y -ra, ahonnan kiszámolhatóak az x_1, x_2 megoldások.

Hasonló helyettesítéssel a harmadfokú egyenlet $y^3 + py + q = 0$ alakra hozható.

Harmadfokú egyenlet

Keressük meg az $y^3 + py + q = 0$ egyenlet megoldásait!

Ötlet: keressük a megoldásokat $y = u + v$ alakban!

Most $(u + v)^3 = u^3 + 3u^2v + 3uv^2 + v^3$.

A harmadfokú egyenlet:

$$\begin{array}{cccc} (u + v)^3 & -3uv(u + v) & -(u^3 + v^3) & = 0 \\ y^3 & +py & +q & = 0 \end{array}$$

Célunk olyan u, v találása, melyekre $-3uv = p$, $-(u^3 + v^3) = q$.

Ekkor $u + v$ megoldás lesz!

u, v megtalálása: $u^3 v^3 = (-\frac{p}{3})^3$, $u^3 + v^3 = -q$, u^3, v^3 gyökei lesznek a $z^2 + qz + (\frac{-p}{3})^3 = 0$ másodfokú egyenletnek. A gyökökből u, v köbgyökvonással kijön:

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{-q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{-q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Harmadfokú egyenlet

Keressük meg az $x^3 - 21x + 20 = 0$ egyenlet megoldásait!
(Most $x = y$, és rögtön látszik, hogy az $x = 1$ gyök lesz.)
 $q = 20, p = -21$ helyettesítéssel a

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{-q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{-q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

képletbe azt kapjuk, hogy

$$x = \sqrt[3]{-10 + \sqrt{-243}} + \sqrt[3]{-10 - \sqrt{-243}}$$

A négyzetgyök alatt negatív!

Meg lehet-e menteni a megoldható képletet?

Harmadfokú egyenlet

$$x = \sqrt[3]{-10 + \sqrt{-243}} + \sqrt[3]{-10 - \sqrt{-243}}$$

Formálisan számolva, a $(\sqrt{-3})^2 = -3$ feltétellel:

$$-10 + \sqrt{-243} = -10 + 9\sqrt{-3} =$$

$$2^3 + 3 \cdot 2^2 \cdot \sqrt{-3} + 3 \cdot 2(\sqrt{-3})^2 + (\sqrt{-3})^3 = (2 + \sqrt{-3})^3.$$

Hasonlóan $-10 - \sqrt{-243} = (2 - \sqrt{-3})^3$.

Ezzel a megoldás: $x = (2 + \sqrt{-3}) + (2 - \sqrt{-3}) = 4$.

Felmerülő kérdések

- Számolhatunk-e $\sqrt{-3}$ -al formálisan?
- Miért épp így kell számolni a $-10 + \sqrt{-243}$ értékét?
- Hova tűnt az $x = 1$ megoldás?
- Mi a harmadik gyöke az egyenletnek?

Számfogalom bővítése

Természetes számok: $\mathbb{N} = \{0, 1, 2, \dots\}$

Nincs olyan $x \in \mathbb{N}$ természetes szám, melyre $x + 2 = 1$!
 \mathbb{N} halmazon a kivonás nem értelmezett!

Egész számok: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

A kivonás elvégezhető: $x = -1$.

Nincs olyan $x \in \mathbb{Z}$ egész szám, melyre $x \cdot 2 = 1$!

\mathbb{Z} halmazon az osztás nem értelmezett!

Racionális számok: $\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}$

Az osztás elvégezhető: $x = \frac{1}{2}$.

Nincs olyan $x \in \mathbb{Q}$ racionális szám, melyre $x^2 = 2$!

\mathbb{Q} halmazon a négyzetgyökvonás nem (mindig) elvégezhető!

Valós számok: \mathbb{R} .

Nincs olyan $x \in \mathbb{R}$ valós szám, melyre $x^2 = -1$!

U.i.: Ha $x \geq 0$, akkor $x^2 \geq 0$.

Ha $x < 0$, akkor $x^2 = (-x)^2 \geq 0$.

Számfogalom bővítése

Komplex számok körében az $x^2 = -1$ egyenlet megoldható!

Komplex számok alkalmazása:

- egyenletek megoldása;
- geometria;
- fizika (áramlástan, kvantummechanika, relativitáselmélet);
- grafika, kvantumszámítógépek.

Komplex számok bevezetése

Legyen i az $x^2 = -1$ egyenlet megoldása.

A szokásos számolási szabályok szerint számoljunk az i szimbólummal formálisan, $i^2 = -1$ helyettesítéssel:

$$(1 + i)^2 = 1 + 2i + i^2 = 1 + 2i + (-1) = 2i$$

Általában

$$(a + bi)(c + di) = ac - bd + i(ad + bc)$$

A komplex számok definíciója

Definíció

Az $a + bi$ alakú kifejezéseket, ahol $a, b \in \mathbb{R}$, komplex számoknak (\mathbb{C}) hívjuk.

Összeadás: $(a + bi) + (c + di) = a + c + i(b + d)$.

Szorzás: $(a + bi)(c + di) = ac - bd + i(ad + bc)$.

A $z = a + bi \in \mathbb{C}$ komplex szám, valós része: $Re(z) = a$.

A $z = a + bi \in \mathbb{C}$ komplex szám képzetes része: $Im(z) = b$.

Figyelem! $Im(z) \neq bi$

Az $a + i0$ alakú komplex számok a valós számok.

A $0 + ib$ alakú komplex számok a tisztán képzetes számok.

Az $a + bi$ és a $c + di$ komplex számok egyenlőek: $a + bi = c + di$, ha

$$a = c, \quad \text{és} \quad b = d$$

A komplex számok definíciója

Megjegyzés

A komplex számok alternatív definíciója:

$(a, b) \in \mathbb{R} \times \mathbb{R}$ párok halmaza, ahol az

összeadás koordinátánként: $(a, b) + (c, d) = (a + c, d + b)$;

szorzás $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

A két definíció **ekvivalens**: $i \rightarrow (0, 1)$.

Az $a + bi$ formátum kényelmesebb számoláshoz.

Az (a, b) formátum kényelmesebb ábrázoláshoz
(grafikusan, számítógépen).

További formális számokra nincs szükség:

Tétel(Algebra alaptétele, NB)

Minden $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ kifejezés esetén, ahol
 $a_0, \dots, a_n \in \mathbb{C}$, $a_n \neq 0$, akkor létezik olyan $z \in \mathbb{C}$ komplex szám,
hogy $a_0 + a_1z + a_2z^2 + \cdots + a_nz^n = 0$.

Számolás komplex számokkal

Definíció

Egy x szám **ellentettje** az az \hat{x} szám, melyre $x + \hat{x} = 0$.

Egy $r \in \mathbb{R}$ szám ellentettje: $-r$

Állítás (HF)

Egy $z = a + bi \in \mathbb{C}$ szám ellentettje a $-z = -a - bi$ komplex szám.

Definíció

Egy $z = a + bi \in \mathbb{C}$ komplex szám **abszolút értéke**:

$$|z| = |a + bi| = \sqrt{a^2 + b^2}.$$

Valós számok esetében ez a hagyományos abszolút érték:

$$|a| = \sqrt{a^2}.$$

Állítás(HF)

$$|z| = |a + bi| \geq 0, \quad |z| = |a + bi| = 0 \Leftrightarrow z = a + bi = 0.$$



Definíció

Egy x szám reciproka az az \hat{x} szám, melyre $x \cdot \hat{x} = 1$.

Egy $r \in \mathbb{R}$ szám reciproka: $\frac{1}{r}$.

Mi lesz $\frac{1}{1+i}$?

Ötlet: gyöktelenítés, konjugálattal való bővítés:

$$\begin{aligned}\frac{1}{1+\sqrt{2}} &= \frac{1}{1+\sqrt{2}} \cdot \frac{1-\sqrt{2}}{1-\sqrt{2}} = \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})} = \frac{1-\sqrt{2}}{1^2 - (\sqrt{2})^2} \\ &= \frac{1-\sqrt{2}}{1-2} = -1 + \sqrt{2}.\end{aligned}$$

Hasonlóan:

$$\frac{1}{1+i} = \frac{1}{1+i} \frac{1-i}{1-i} = \frac{1-i}{(1+i)(1-i)} = \frac{1-i}{1^2 - i^2} = \frac{1-i}{1 - (-1)} = \frac{1-i}{2}.$$

Számolás komplex számokkal

Definíció

Egy $z = a + bi$ komplex szám **konjugáltja** a $\bar{z} = \overline{a+bi} = a - bi$ szám.

Állítás(HF)

Egy z komplex szám **reciproka** $\frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}}$

A definíció értelmes, hiszen a nevezőben:

$$z \cdot \bar{z} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2 = |z|^2.$$

Nulosztómentesség: $z \cdot w = 0 \rightarrow z = 0$ vagy $w = 0$.

Két komplex szám **hányadosa**:

$$\frac{z}{w} = z \cdot \frac{1}{w}.$$

Tétel (HF)

- 1 $\overline{\overline{z}} = z;$
- 2 $\overline{z + w} = \overline{z} + \overline{w};$
- 3 $\overline{z \cdot w} = \overline{z} \cdot \overline{w};$
- 4 $z + \overline{z} = 2 \cdot \operatorname{Re}(z);$
- 5 $z - \overline{z} = 2i \cdot \operatorname{Im}(z);$
- 6 $z \cdot \overline{z} = |z|^2;$
- 7 $z \neq 0$ esetén $z^{-1} = \frac{\overline{z}}{|z|^2};$
- 8 $|0| = 0$ és $z \neq 0$ esetén $|z| \geq 0;$
- 9 $|\overline{z}| = |z|;$
- 10 $|z \cdot w| = |z| \cdot |w|;$
- 11 $|z + w| \leq |z| + |w|$ (háromszög egyenlőtlenség).

Tétel(HF)

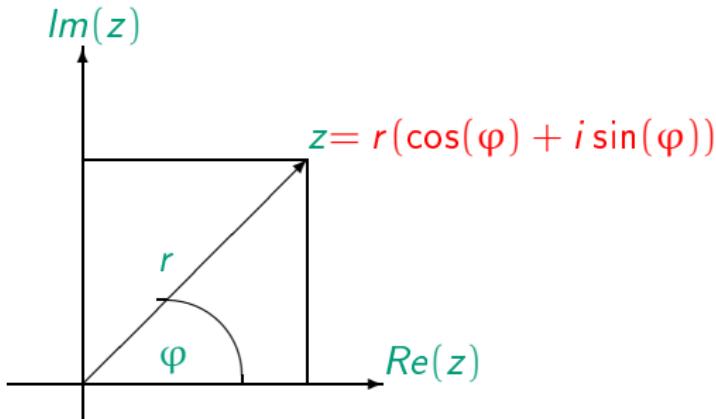
- $|z \cdot w| = |z| \cdot |w|$;

Bizonyítás

$$|z \cdot w| = z \cdot w \cdot \overline{z \cdot w} = z \cdot w \cdot \overline{z} \cdot \overline{w} = z \cdot \overline{z} \cdot w \cdot \overline{w} = |z| \cdot |w|.$$

Komplex számok ábrázolása

A komplex számok a **komplex számsíkon**:



Ha $z = a + bi \in \mathbb{C}$, akkor $Re(z) = a$, $Im(z) = b$.

A $(Re(z), Im(z))$ vektor hossza: $r = \sqrt{a^2 + b^2} = \sqrt{|z|^2}$.

A z nem-nulla szám **argumentuma** $\varphi = \arg(z) \in [0, 2\pi)$

A koordináták trigonometrikus függvényekkel kifejezve:

$$Re(z) = a = r \cdot \cos(\varphi), Im(z) = b = r \cdot \sin(\varphi)$$

Komplex számok trigonometrikus alakja

Definíció

$z \in \mathbb{C}$ nem-nulla szám **trigonometrikus alakja** a

$$z = r(\cos(\varphi) + i \sin(\varphi)),$$

ahol $r > 0$ a szám **abszolút értéke**.

Figyelem! A 0-nak nincs trigonometrikus alakja.

A trigonometrikus alak nem egyértelmű:

$$r(\cos(\varphi) + i \sin(\varphi)) = r(\cos(\varphi + 2\pi) + i \sin(\varphi + 2\pi)).$$

Definíció

Egy $z \in \mathbb{C}$ nem-nulla **argumentuma**: az a $\varphi = \arg(z) \in [0, 2\pi)$, melyre $z = |z|(\cos(\varphi) + i \sin(\varphi))$.

- $z = a + bi$ algebrai alak;
- $z = r(\cos(\varphi) + i \sin(\varphi))$ trigonometrikus alak.

Itt $a = r \cos(\varphi)$, $b = r \sin(\varphi)$.

Számolás trigonometrikus alakkal

Legyen $z, w \in \mathbb{C}$ nem-nulla komplex számok:

$$z = |z|(\cos(\varphi) + i \sin(\varphi)), \quad w = |w|(\cos(\psi) + i \sin(\psi))$$

A szorzatuk:

$$\begin{aligned} zw &= |z|(\cos(\varphi) + i \sin(\varphi)) \cdot |w|(\cos(\psi) + i \sin(\psi)) \\ &= |z||w|(\cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi) + \\ &\quad i(\cos(\varphi)\sin(\psi) + \sin(\varphi)\cos(\psi))) \end{aligned}$$

addíciós képletek: $\cos(\varphi + \psi) = \cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi)$
 $\sin(\varphi + \psi) = \cos(\varphi)\sin(\psi) + \sin(\varphi)\cos(\psi)$
 $= |z||w|(\cos(\varphi + \psi) + i \sin(\varphi + \psi))$

A szorzat **abszolút értéke**: $|zw| = |z||w|$.

A szorzat **argumentuma**:

- ha $0 \leq \arg(z) + \arg(w) \leq 2\pi$, akkor
 $\arg(zw) = \arg(z) + \arg(w)$;
- ha $2\pi \leq \arg(z) + \arg(w) \leq 4\pi$, akkor
 $\arg(zw) = \arg(z) + \arg(w) - 2\pi$.

A sin, cos függvények 2π szerint periódikusak, az argumentum meghatározásánál **redukálni** kell az argumentumok összegét.

Tétel HF

Legyen $z, w \in \mathbb{C}$ nem-nulla komplex számok:

$$z = |z|(\cos(\varphi) + i \sin(\varphi)), \quad w = |w|(\cos(\psi) + i \sin(\psi)),$$

és legyen $n \in \mathbb{N}$. Ekkor

$$zw = |z||w|(\cos(\varphi + \psi) + i \sin(\varphi + \psi));$$

$$\frac{z}{w} = \frac{|z|}{|w|}(\cos(\varphi - \psi) + i \sin(\varphi - \psi))$$

$$z^n = |z|^n(\cos(n\varphi) + i \sin(n\varphi)).$$

A szögekre összeadódnak, kivonódnak, szorzódnak. Az argumentumot ezek után **redukcióval** kapjuk!

Geometriai jelentés

Egy $z \in \mathbb{C}$ komplex szám a komplex számsíkon mint nyújtva-forgatás hat. $|z|$ -vel nyújt, $\arg(z)$ szöggel forgat.

Komplex számok gyökei

Példa

Számoljuk ki a $\left(\frac{1+i}{\sqrt{2}}\right)^8$ hatványát:

$$\begin{aligned}\left(\frac{1+i}{\sqrt{2}}\right)^8 &= \left(\frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}}\right)^8 = \left(\cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right)\right)^8 \\ &= \cos\left(8 \cdot \frac{\pi}{4}\right) + i \sin\left(8 \cdot \frac{\pi}{4}\right) = \cos(2\pi) + i \sin(2\pi) = 1\end{aligned}$$

További komplex számok, melyeknek a 8-adik hatványa 1:

- 1;
- -1;
- i : $i^8 = (i^2)^4 = (-1)^4 = 1$;
- $-i$;
- $\frac{1+i}{\sqrt{2}}$; $-\frac{1+i}{\sqrt{2}}$;
- sőt: $\pm i \cdot \frac{1+i}{\sqrt{2}}$: $\left(i \cdot \frac{1+i}{\sqrt{2}}\right)^8 = i^8 \cdot \left(\frac{1+i}{\sqrt{2}}\right)^8 = 1 \cdot 1 = 1$.

Gyökvonás

A $z = |z|(\cos(\varphi) + i \sin(\varphi))$ és $w = |w|(\cos(\psi) + i \sin(\psi))$ számok **egyenlőek**,

$$|z|(\cos(\varphi) + i \sin(\varphi)) = |w|(\cos(\psi) + i \sin(\psi))$$

ha

- $|z| = |w|$
- $\varphi = \psi + k \cdot 2\pi$ valamely $k \in \mathbb{Z}$ szám esetén.

n-edik gyökvonás: Legyen $z^n = w$:

$$z^n = |z|^n(\cos(n\varphi) + i \sin(n\varphi)) = |w|(\cos(\psi) + i \sin(\psi)).$$

Ekkor

- $|z|^n = |w| \rightarrow |z| = \sqrt[n]{|w|}$
- $n\varphi = \psi + k \cdot 2\pi$ valamely $k \in \mathbb{Z}$ esetén

$$\rightarrow \varphi = \frac{\psi}{n} + k \cdot \frac{2\pi}{n} \text{ valamely } k \in \mathbb{Z} \text{ esetén}$$

ha $k \in \{0, 1, \dots, n-1\}$, akkor ezek minden különböző komplex számot adnak.

Tétel

Legyen $z = |z|(\cos(\varphi) + i \sin(\varphi))$, $n \in \mathbb{N}$. Ekkor a z n -edik gyökei $w^n = z$:

$$w = \sqrt[n]{|z|} \left(\cos \left(\frac{\varphi}{n} + \frac{2k\pi}{n} \right) + i \sin \left(\frac{\varphi}{n} + \frac{2k\pi}{n} \right) \right)$$

$$k = 0, 1, \dots, n - 1.$$

Gyökvonás

$$w = \sqrt[n]{|z|} \left(\cos \left(\frac{\varphi}{n} + \frac{2k\pi}{n} \right) + i \sin \left(\frac{\varphi}{n} + \frac{2k\pi}{n} \right) \right) : k = 0, 1, \dots, n-1.$$

Példa

Számítsuk ki a $\sqrt[6]{\frac{1-i}{\sqrt{3}+i}}$ értékét!

$$1-i = \sqrt{2} \left(\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2} \right) = \sqrt{2} \left(\cos \left(\frac{7\pi}{4} \right) - i \sin \left(\frac{7\pi}{4} \right) \right)$$

$$\sqrt{3}+i = 2 \left(\frac{\sqrt{3}}{2} - i \frac{1}{2} \right) = 2 \left(\cos \left(\frac{\pi}{6} \right) - i \sin \left(\frac{\pi}{6} \right) \right)$$

$$\text{Mivel } \frac{7\pi}{4} - \frac{\pi}{6} = \frac{19\pi}{12}$$

$$\begin{aligned} \sqrt[6]{\frac{1-i}{\sqrt{3}+i}} &= \sqrt[6]{\frac{1}{\sqrt{2}}} \left(\cos \left(\frac{19\pi}{12} \right) + i \sin \left(\frac{19\pi}{12} \right) \right) = \\ &= \frac{1}{\sqrt[12]{2}} \left(\cos \left(\frac{19\pi+2k\pi}{72} \right) + i \sin \left(\frac{19\pi+2k\pi}{72} \right) \right) : k = 0, 1, \dots, 5 \end{aligned}$$

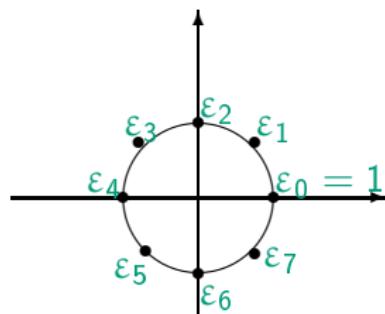
Komplex egységgökök

Definíció

Az $\varepsilon^n = 1$ feltételnek eleget tevő komplex számok az **n-edik egységgökök**:

$$\varepsilon_k = \varepsilon_k^{(n)} = \left(\cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right) \right) : k = 0, 1, \dots, n - 1.$$

Nyolcadik komplex egységgökök



Gyökvonás

Pozitív valós számok négyzetgyöke: legyen $r > 0$ valós.

Ekkor az $x^2 = r$ megoldása: $\pm\sqrt{r}$.

Tétel

Legyen $z \in \mathbb{C}$ nem-nulla komplex szám. $n \in \mathbb{N}$ és $w \in \mathbb{C}$ olyan, hogy $w^n = z$. Ekkor az n -edik gyökök: $w\varepsilon_k : k = 0, 1, \dots, n - 1$.

Bizonyítás

A $w\varepsilon_k$ számok minden n -edik gyöökök: $(w\varepsilon_k)^n = w^n\varepsilon_k^n = w^n = z$. Ez n különböző szám, így az összes gyököt megkaptuk.

Bizonyos komplex számok hatványai periódikusak ismétlődnek:

- $1, 1, 1 \dots$
- $-1, 1, -1, 1 \dots$
- $i, -1, -i, 1, i, -1, \dots$
- $\frac{1+i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, -1, \frac{-1-i}{\sqrt{2}}, -i, \frac{1-i}{\sqrt{2}}, 1, \frac{1+i}{\sqrt{2}}, i \dots$

Általában:

$\cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ -nek n darab különböző hatványa van.

Definíció

Egy z komplex szám különböző (egész kitevős) hatványainak számát a z rendjének nevezzük és $o(z)$ -vel jelöljük.

Példa

- 1 rendje 1
- 2 rendje ∞ : $2, 4, 8, 16$
- -1 rendje 2: $1, -1$
- i rendje 4: $1, i, -1, -i$

Tétel

Egy z komplex számnak vagy bármely két egész kitevős hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periódikusan ismétlődnek. A rend a legkisebb olyan pozitív d szám, melyre $z^d = 1$.

Továbbá $z^k = z^l \Leftrightarrow o(z)|k - l$. Speciálisan $z^k = 1 \Leftrightarrow o(z)|k$

Bizonyítás

Tegyük fel, hogy z rendje véges. Ekkor léteznek olyan k, l különböző egészek, melyekre $z^k = z^l$. Legyen $k > l$. Ekkor $z^{k-l} = 1$.

Legyen d legkisebb olyan pozitív szám, melyre $z^d = 1$. Ha $z^n = 1$, akkor osszuk el maradékosan n -et d -vel: $n = q \cdot d + r$, ahol $0 \leq r < d$. Tehát $1 = z^n = z^{q \cdot d + r} = (z^d)^q z^r = 1^q z^r = z^r$. A d minimalitása miatt $r = 0$ azaz $d|n$. Visszafelé is igaz: $d|n \Rightarrow z^n = 1$. Beláttuk: $d|n \Leftrightarrow z^n = 1$.



Primitív gyökök

Az n -edik egységgyökök rendje nem n :

4-rdik egységgyökök: $1, i, -1, -i$.

- 1 rendje 1 ;
- -1 rendje 2 ;
- i rendje 4 .

Definíció

Az n -ed rendű n -edik egységgyökök a **primitív n -edik egységgyökök**.

A téTEL következményei:

Következmény(HF)

- Egy primitív n -edik egységgyök hatványai pontosan az n -edik egységgyökök.
- Egy primitív n -edik egységgyök pontosan akkor k -adik egységgyök, ha $n|k$.

Primitív egységgyökök

Példa

- Primitív 1. egységgyöök: 1 ;
- Primitív 2. egységgyöök: -1 ;
- Primitív 3. egységgyöök: $\frac{-1 \pm i\sqrt{3}}{2}$;
- Primitív 4. egységgyöök: $\pm i$;
- Primitív 5. egységgyöök: \dots (HF)
- Primitív 6. egységgyöök: $\frac{1 \pm i\sqrt{3}}{2}$;

Állítás(HF)

Egy $\cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right)$ n -edik egységgyök pontosan akkor primitív n -edik egységgyök, ha $(n, k) = 1$.

Matematikai logika

A logika a helyes következtetés tudománya.

Alkalmazási területek:

- matematika;
- informatika;
- mesterséges intelligencia;
- ...

Példa

Minden bogár rovar.

tagadás: Van olyan rovar, ami nem bogár.

Esik az eső, de meleg van, bár a nap is elbújt, és az idő is későre jár.

tagadás: ?

Axiomatikus módszer

A tudományok a valóság egy részének modellezésével foglalkoznak.

Axiomatikus módszer: közismert, nem definiált fogalmakból (**alapfogalmakból**) és bizonyos feltevések ből (**axiómákból**) a logika szabályai szerint milyen következtetéseket vonunk le (milyen tételeket bizonyítunk.)

Példa

Euklidész geometria

Alapfogalmak

- pont
- egyenes
- sík

Az axiomatikus módszer előnye: elég ellenőrizni az axiómák teljesülését.

Axiómák

- párhuzamossági axióma
- ...

Definíció

Predikátum: olyan változóktól függő definiálatlan alapfogalom, amelyhez a változóik értékétől függően valamilyen **igazságérték** tartozik:

igaz(I, \uparrow), hamis (H, \downarrow) és a kettő egyidejűleg nem teljesül.

Példa

$M()$: minden jogász hazudik.	0-változós, értéke: l.
$Sz(x)$: x egy szám.	1-változós, értéke: $Sz(i) = l$, $Sz(h) = H$.
$E(x)$: x egy egyenes	1-változós.
$P(x)$: x egy pont.	1-változós.
$I(x, y)$: x illeszkedik y -re.	2-változós.
$F(x, y)$: x az y férje.	2-változós.
$Gy(x, y, z)$: x az y és z gyermeké.	3-változós.

Logikai jelek

A predikátumokat logikai jelekkel tudjuk összekötni:

Tagadás, jele $\neg A$

És, jele $A \wedge B$

Vagy, (megengedő), jele $A \vee B$

Ha..., akkor... (implikáció), jele $A \Rightarrow B$

Ekvivalencia, jele $A \Leftrightarrow B$

Igazságtáblázat

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
I	I	H	I	I	I	I
I	H	H	H	I	H	H
H	I	I	H	I	I	H
H	H	I	H	H	I	I

Logikai jelek

Köznyelvbe a **vagy** háromféle értelemmel bírhat:

Megengedő vagy "Átok reá ki gyávaságból **vagy** lustaságból elmarad"

$A \vee B$	I	H
I	I	I
H	I	H

Kizáró vagy: "Vagy bolondok vagyunk és elveszünk egy szálig, **vagy** ez a mi hitünk valóságra válik"

	I	H
I	H	I
H	I	H

Összeférhetetlen vagy: "Iszik **vagy** vezet!"

	I	H
I	H	I
H	I	I

Logikai jelek

Az implikáció ($A \Rightarrow B$) csak **logikai** összefüggést jelent és nem okozatit!

$A \Rightarrow B$	I	H
I	I	H
H	I	I

Példa

$$2 \cdot 2 = 4 \Rightarrow i^2 = -1$$

$$2 \cdot 2 = 4 \Rightarrow \text{hétfő van}$$

Hamis állításból minden következik:

Példa

$$2 \cdot 2 = 5 \Rightarrow i^2 = -2$$

Adott logikai jel, más módon is kifejezhető:

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$$

Kvantorok

\exists egzisztenciális kvantor: "létezik", "van olyan"

\forall univerzális kvantor: "minden"

Példa

$V(x)$: x veréb

$M(x)$: x madár

Minden veréb madár: $\forall x(V(x) \Rightarrow M(x))$.

Van olyan madár, ami veréb: $\exists x(M(x) \Rightarrow V(x))$.

Minden veréb madár, de nem minden madár veréb:

$(\forall x(V(x) \Rightarrow M(x))) \wedge (\exists x(M(x) \wedge \neg V(x)))$.

A formulák predikátumokból és logikai jelekből alkotott "mondatok".

Definíció(Definíció) Formulák)

- A predikátumok a legegyszerűbb, un. elemi formulák.
- Ha \mathcal{A}, \mathcal{B} két formula, akkor $\neg\mathcal{A}, (\mathcal{A} \wedge \mathcal{B}), (\mathcal{A} \vee \mathcal{B}), (\mathcal{A} \Rightarrow \mathcal{B}), (\mathcal{A} \Leftrightarrow \mathcal{B})$ is formulák.
- Ha \mathcal{A} egy formula és x egy változó, akkor $(\exists x \mathcal{A})$ és $(\forall x \mathcal{A})$ is formulák.

Példa

Minden veréb madár, de nem minden madár veréb.:

$$(\forall x(V(x) \Rightarrow M(x))) \wedge (\exists x(M(x) \wedge \neg V(x))).$$

egy formula.

Ha nem okoz félreértést, a zárójelek elhagyhatóak.

Definíció

Ha \mathcal{A} egy formula és x egy változó, akkor $(\exists x \mathcal{A})$ és $(\forall x \mathcal{A})$ formulákban az x változó az \mathcal{A} formulában minden előfordulása a **kvantor hatáskörében** van.

Ha egy formulában a változó adott előfordulása egy kvantor hatáskörében van, akkor az előfordulás **kötött**, egyébként **szabad**.

Ha egy formulában a változónak van szabad előfordulása, akkor a változó **szabad változó**, egyébként **kötött változó**.

Ha egy formulának van szabad változója, akkor **nyitott formula**, egyébként **zárt formula**.

Példa

$Gy(x, y)$: x gyereke y -nak

$\exists y \ Gy(x, y)$: x -nek létezik szülője.

Példa

$E(x)$: x egy egyenes.

$P(x)$: x egy pont.

$I(x, y)$: x illeszkedik y -ra.

$E(x), P(x), I(x, y)$ (elemi) nyitott formulák.

$\mathcal{A}(x, y)$ legyen $E(x) \wedge P(y) \wedge I(x, y)$

Az x egyenes illeszkedik az y pontra.

$\mathcal{B}(x, y)$ legyen $P(x) \wedge P(y) \wedge \neg(x = y)$ Az x és y pontok különbözők.

$\mathcal{C}(x)$ legyen $\exists y E(x) \wedge P(y) \wedge I(x, y)$

Van olyan y pont, ami illeszkedik az x egyenesre.

Itt x szabad y kötött változó.

$\mathcal{D}()$ legyen $\forall x E(x) \Rightarrow \exists y E(x) \wedge P(y) \wedge I(x, y)$

Minden x egyenes esetén, van olyan y pont, ami illeszkedik az x egyenesre.

Itt x, y kötött változó.

Halmazelméletben az alapvető fogalmak **predikátumok**, nem definiáljuk őket:

- A **halmaz** (rendszer, osztály, összesség,...) elemeinek gondolati burka.
- $x \in \mathcal{A}$, ha az x eleme az \mathcal{A} halmaznak.

A halmazok alapvető tulajdonságai **axiómák**, nem bizonyítjuk őket.

Példa:

Meghatározottsági axióma

Egy halmazt az elemei egyértelműen meghatároznak.

- Két halmaz pontosan akkor egyenlő, ha ugyan azok az elemeik.
- Egy halmaznak egy elem csak egyszerre lehet eleme.

Részhalmazok

Definíció

Az A halmaz részhalmaza a B halmaznak: $A \subset B$, ha
 $\forall x(x \in A \Rightarrow x \in B)$.

Ha $A \subset B$ -nek, de $A \neq B$, akkor A valódi részhalmaza B -nek:
 $A \subsetneq B$.

A részhalmazok tulajdonságai:

Állítás (Biz. HF)

- ① $\forall A \quad A \subset A$ (reflexivitás).
- ② $\forall A, B, C \quad A \subset B \wedge B \subset C \Rightarrow A \subset C$. (tranzitivitás)
- ③ $\forall A, B \quad A \subset B \wedge B \subset A \Rightarrow A = B$ (antiszimmetria)

Halmazok egyenlősége az 1. és 2. tulajdonságot teljesíti, de a 3. nem:

3'. $\forall A, B \quad A = B \Rightarrow B = A$ (szimmetria).

Definíció

A halmaz és $\mathcal{F}(x)$ formula esetén $\{x \in A : \mathcal{F}(x)\} = \{x \in A | \mathcal{F}(x)\}$ halmaz elemei pontosan azon elemei A -nak, melyre $\mathcal{F}(x)$ igaz.

Példa

- $\{n \in \mathbb{Z} : n \equiv 0 \pmod{2}\}$ páros számok halmaza.
- $\{g \in \mathbb{Z}_p : \forall a \in \mathbb{Z}_p^* \quad \exists n \in \mathbb{N} \quad g^n \equiv a \pmod{p}\}$: generátorok, primitív gyökök.
- $\{z \in \mathbb{C} : \operatorname{Im} z = 0\}$: valós számok halmaza.
- $\{z \in \mathbb{C} : \exists n \in \mathbb{N} \quad z^n = 1\}$: komplex egységggyökök.

Speciális halmazok

Üres halmaz Azt a halmazt, melynek nincs eleme \emptyset -el jelöljük. A **meghatározottsági axióma** alapján ez egyértelmű.

$$\forall A \quad A \text{ halmaz} \Rightarrow \emptyset \subset A$$

Halmaz megadása elemei felsorolásával. Azt a halmazt, melynek csak az a elem az eleme $\{a\}$ -el jelöljük. Azt a halmazt, melynek az a és b az eleme, $\{a, b\}$ -vel jelöljük,....

Speciálisan $\emptyset = \{\}$, illetve, ha $a = b$, akkor $\{a\} = \{a, b\} = \{b\}$.

Definíció

Az A és B halmazok **uniója**: $A \cup B$ az a halmaz, mely pontosan az A és a B elemeit tartalmazza.

Általában: Legyen \mathcal{A} egy olyan halmaz, melynek az elemei is halmazok (halmazrendszer). Ekkor $\cup \mathcal{A} = \cup \{A : A \in \mathcal{A}\} = \cup_{A \in \mathcal{A}} A$ az a halmaz, mely az \mathcal{A} összes elemének elemét tartalmazza.

Speciálisa: $A \cup B = \cup \{A, B\}$.

Példa

- $\{a, b, c\} \cup \{b, c, d\} = \{a, b, c, d\}$
- $\{n : n \equiv 0 \pmod{2}\} \cup \{n : n \equiv 1 \pmod{2}\} = \mathbb{Z}$
- $\{n : n \equiv 0 \pmod{3}\} \cup \{n : n \equiv 1 \pmod{3}\} \cup \{n : n \equiv 2 \pmod{3}\} = \mathbb{Z}$

Rövidebben, ha $\bar{a} = \{n : n \equiv a \pmod{m}\}$, akkor

- $m = 2$ esetén $\bar{0} \cup \bar{1} = \mathbb{Z}$
- $m = 3$ esetén $\bar{0} \cup \bar{1} \cup \bar{2} = \mathbb{Z}$

Műveletek halmazokkal

Általában

- $\cup\{\bar{a} : a \in \{0, 1, \dots, m-1\}\} = \cup_{a=0}^{m-1} \bar{a} = \mathbb{Z}$

Az unió tulajdonságai

Állítás

- ① $A \cup \emptyset = A$
- ② $A \cup B = B \cup A$ (kommutativitás)
- ③ $A \cup (B \cup C) = (A \cup B) \cup C$ (asszociativitás)
- ④ $A \cup A = A$ (idempotencia)
- ⑤ $A \subset B \Leftrightarrow A \cup B = B$

Bizonyítás

- 1. Egy x pontosan akkor eleme minden két oldalnak, ha $x \in A$
- 2. Egy x pontosan akkor eleme minden két oldalnak, ha $x \in A$ vagy $x \in B$
- 3-as, 4-es hasonló



Bizonyítás folyt.

- 5. $\Rightarrow: A \subset B \Rightarrow A \cup B \subset B$, de $A \cup B \supset B$ mindenkorban teljesül, így $A \cup B = B$.
 $\Leftarrow:$ Ha $A \cup B = B$, akkor A minden eleme eleme B -nek.

Definíció

Az A és B halmazok metszete: $A \cap B$ az a halmaz, mely pontosan az A és a B közös elemeit tartalmazza: $A \cap B = \{x \in A : x \in B\}$

Általában: Legyen \mathcal{A} egy olyan halmaz, melynek az elemei is halmazok (halmazrendszer). Ekkor $\cap \mathcal{A} = \cap \{A : A \in \mathcal{A}\} = \cap_{A \in \mathcal{A}} A$ a következő halmaz

$$\cap \mathcal{A} = \{x : \forall A \in \mathcal{A} \quad x \in A\}$$

Speciálisan: $A \cap B = \cap \{A, B\}$.

Példa

- $\{a, b, c\} \cap \{b, c, d\} = \{b\}$.
- Ha $E_n = \{z \in \mathbb{C} : z^n = 1\}$ az n-edik egységggyökök halmaza, akkor
 - $E_2 \cap E_4 = E_2$
 - $E_6 \cap E_8 = E_2$
 - $E_n \cap E_m = E_{(n,m)}$
 - $\bigcap_{n=1}^{\infty} E_n = E_1 = \{1\}$

Definíció

Ha $A \cap B = \emptyset$, akkor A és B diszjunktak.

Ha \mathcal{A} egy halmazrendszer és $\cap \mathcal{A} = \emptyset$, akkor \mathcal{A} diszjunkt, illetve \mathcal{A} elemei diszjunktak.

Ha \mathcal{A} egy halmazrendszer és \mathcal{A} bármely két eleme diszjunkt, akkor \mathcal{A} elemei páronként diszjunktak.

Példa

- Az $\{1, 2\}$ és $\{3, 4\}$ halmazok diszjunktak.
- Az $\{1, 2\}$, $\{2, 3\}$ és $\{1, 3\}$ halmazok diszjunktak, de nem páronként diszjunktak.
- Az $\{1, 2\}$, $\{3, 4\}$ és $\{5, 6\}$ halmazok páronként diszjunktak.

A metszet tulajdonságai

Állítás (Biz. HF)

- 1 $A \cap \emptyset = \emptyset$
- 2 $A \cap B = B \cap A$ (kommutativitás)
- 3 $A \cap (B \cap C) = (A \cap B) \cap C$ (asszociativitás)
- 4 $A \cap A = A$ (idempotencia)
- 5 $A \subset B \Leftrightarrow A \cap B = A$

Az unió és metszet disztributivitási tulajdonságai

Állítás

- ① $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- ② $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Bizonyítás

- ① $x \in A \cap (B \cup C) \Leftrightarrow x \in A \wedge x \in B \cup C.$

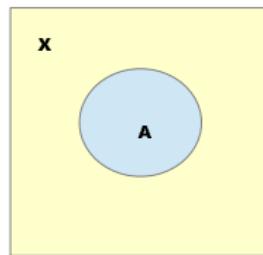
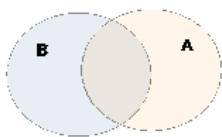
Igy x pontosan akkor eleme a baloldalnak, ha $x \in A \wedge x \in B$ vagy $x \in A \wedge x \in C$ azaz $x \in (A \cap B) \cup (A \cap C).$

- ② HF. hasonló

Különbség, komplementer

Definíció

Az A és B halmazok különbsége az $A \setminus B = \{x \in A : x \notin B\}$

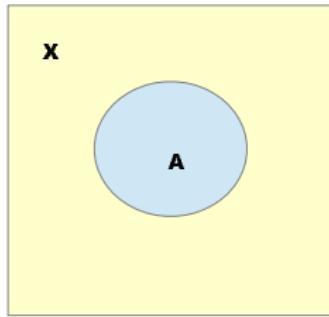


Definíció

Egy rögzített X alaphalmaz és $A \subset X$ részhalmaz esetén az A halmaz **komplementere** az $\bar{A} = A' = X \setminus A$.

Állítás (Biz. HF)

- ① $\overline{\overline{A}} = A;$
- ② $\overline{\emptyset} = X;$
- ③ $\overline{X} = \emptyset;$
- ④ $A \cap \overline{A} = \emptyset;$
- ⑤ $A \cup \overline{A} = X;$
- ⑥ $A \subset B \Leftrightarrow \overline{B} \subset \overline{A};$
- ⑦ $\overline{A \cap B} = \overline{A} \cup \overline{B};$
- ⑧ $\overline{A \cup B} = \overline{A} \cap \overline{B};$

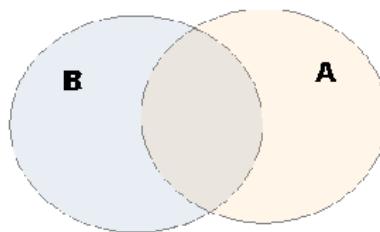


A 7. és 8. összefüggések az un. de Morgan szabályok.

Definíció

Az A és B halmazok **szimmetrikus differenciája** az
 $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Jelölés: $x \in (A \cup B) \wedge x \notin (A \cap B)$



Definíció

Ha A egy halmaz, akkor azt a halmazrendszert, melynek elemei az A halmaz összes részhalmaza az A **hatványhalmazának** mondjuk és 2^A -val jelöljük.

- $A = \emptyset, 2^\emptyset = \{\emptyset\}$
- $A = \{a\}, 2^{\{a\}} = \{\emptyset, \{a\}\}$
- $A = \{a, b\}, 2^{\{a, b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Állítás (Biz. HF)

$$|2^A| = 2^{|A|}$$

A relációk

- a függvényfogalom általánosításai:
 - "hagyományos" függvények pontos definiálása
 - "többértékű függvények"
- kapcsolatot ír le
 - $=, <, \leq$, oszthatóság, ...

Rendezett pár

Adott $x \neq y$ és (x, y) rendezett pár esetén számít a sorrend:

- $\{x, y\} = \{y, x\}$
- $(x, y) \neq (y, x)$

Definíció

Az (x, y) rendezett pár az $\{\{x\}, \{x, y\}\}$ halmazzal definiáljuk. Az (x, y) rendezett pár esetén az x az első az y a második koordináta.

Definíció

Az X, Y halmazok Descart-szorzatán az

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

rendezett párokból álló halmazt értjük.

Adott X , Y halmazok esetén az $R \subset X \times Y$ halmazokat **binér (kétváltozós) relációknak** nevezük.

Ha R binér reláció, akkor gyakran $(x, y) \in R$ helyett xRy -t írunk.

Példa

1. $\mathbb{I}_X = \{(x, x) \in X \times X : x \in X\}$ az **egyenlőség** reláció.
2. $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x|y\}$ az **osztója** reláció.
3. \mathcal{F} halmazrendszer esetén az $\{(X, Y) \in \mathcal{F} \times \mathcal{F} : X \subset Y\}$ a **tartalmazás** reláció.
4. Adott $f : \mathbb{R} \rightarrow \mathbb{R}$ függvény esetén a függvény grafikonja
 $\{(x, f(x)) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$

Definíció

Ha valamely, X , Y halmazokra $R \subset X \times Y$, akkor azt mondjuk, hogy R reláció X és Y között.

Ha $X = Y$, akkor azt mondjuk, hogy R **X-beli reláció** (homogén binér reláció).

Relációk értelmezési tartománya, érték készlete

Ha R reláció X és Y között ($R \subset X \times Y$) és $X \subset X'$ $Y \subset Y'$, akkor R reláció X' és Y' között is!

Definíció

Az R reláció értelmezési tartománya a

$$dmn(R) = \{x : \exists y : (x, y) \in R\}$$

érték készlete

$$rng(R) = \{y : \exists x : (x, y) \in R\}$$

Példa

- Ha $R = \left\{ \left(x, \frac{1}{x^2} \right) : x \in \mathbb{R} \right\}$, akkor $dmc(R) = \{x \in \mathbb{R} : x \neq 0\}$, $rng(R) = \{x \in \mathbb{R} : x > 0\}$.
- Ha $R = \left\{ \left(\frac{1}{x^2}, x \right) : x \in \mathbb{R} \right\}$, akkor $dmc(R) = \{x \in \mathbb{R} : x > 0\}$, $rng(R) = \{x \in \mathbb{R} : x \neq 0\}$.

Relációk kiterjesztése, leszűkítése, inverze

Definíció

Egy R binér relációt az S binér reláció **kiterjesztésének**, illetve S -et az R **leszűkítésének** (megszorításának) nevezük, ha $S \subset R$. Ha A egy halmaz, akkor az R reláció A -ra való **leszűkítésén** (az A -ra való megszorításán) az

$$R|_A = \{(x, y) \in R : x \in A\}.$$

Példa

Legyen $R = \{(x^2, x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$,
 $S = \{(x, \sqrt{x}) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$. Ekkor R az S kiterjesztése, S az R leszűkítése, $S = R|_{\mathbb{R}_0^+}$
(ahol \mathbb{R}_0^+ a nemnegatív valós számok halmaza.)

Definíció

Egy R binér reláció **inverzén** az $R^{-1} = \{(y, x) : (x, y) \in R\}$.

Halmaz képe, teljes inverz képe

Példa

$$R^{-1} = \{(x, x^2) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\} \quad S^{-1} = \{(\sqrt{x}, x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$$

Definíció

Legyen R egy binér reláció, A egy halmaz. Az A halmaz képe az $R(A) = \{y : \exists x \in A : (x, y) \in R\}$. Adott B halmaz inverz képe, vagy teljes ősképe az $R^{-1}(B)$, a B halmaz képe az R^{-1} reláció esetén.

Példa

$$\text{Legyen } R = \{(x^2, x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\},$$

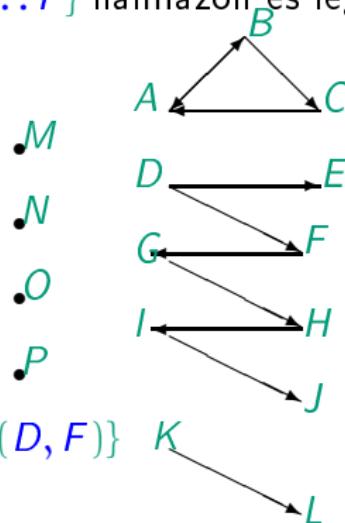
$$S = \{(x, \sqrt{x}) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$$

- $R(\{9\}) = \{-3, 3\}$ (vagy röviden $R(9) = \{-3, 3\}$)
- $S(9) = \{+3\}$.

Példa

Legyen R reláció az $X = \{A, B, C, \dots, P\}$ halmazon és legyen $T \rightarrow T'$, ha $(T, T') \in R$.

- $dmn(R) = \{A, B, C, D, F, \dots, H\}$
- $rng(R) = \{A, B, C, E, \dots, J, L\}$
- $R_{\{A, B, C, D\}} = \{(A, B), (B, C), (C, A), (D, E), (D, F)\}$



Definíció

Legyenek R és S binér relációk. Ekkor az $R \circ S$ kompozíció (összetétel, szorzat) reláció:

$$R \circ S = \{(x, y) : \exists z : (x, z) \in S, (z, y) \in R\}$$

Kompozíció esetén a relációkat "jobbról-balra írjuk".

Példa

$$\text{Legyen } R_{\sin} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \sin x = y\}$$

$$S_{\log} = \{(x, y) \in \mathbb{R} \times \mathbb{R} : \log x = y\}$$

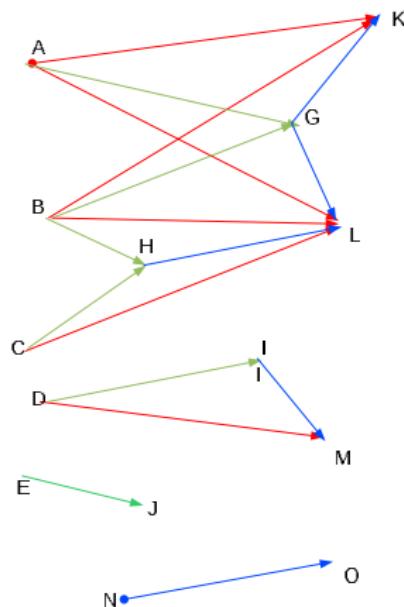
$$\begin{aligned}\text{Ekkor } R_{\sin} \circ S_{\log} &= \{(x, y) : \exists z : \log x = z, \sin z = y\} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \sin \log x = y\}\end{aligned}$$

Kompozíció

$$R \circ S = \{(x, y) : \exists z : (x, z) \in S, (z, y) \in R\}$$

Példa

Legyen S, R két reláció és tekintsük az $T = R \circ S$ kompozíciót:



Példa

Adott cég esetén legyenek $A, B \dots J$ az alkalmazottak. A cég két projekten dolgozik: BANK, JÁTÉK

beosztás	alkalmazott
menedzser	A,B
programozó	C,D,E
tesztelő	F,G,H
HR	I
tech. dolgozó	J

projekt	alkalmazott	határidő
BANK	A,C,D,F	2013.12.31
JÁTÉK	B,D,E,F,G,H	2014.01.31

Legyen B a beosztás reláció: például $A \ B$ menedzser.

P a projekt reláció: például $A \ P$ BANK

H a határidő reláció: például $BANK \ H$ 2013.12.31.

- Kik dolgoznak a BANK projekten? $B(\text{BANK})$
- Kik a tesztelők? B^{-1} (tesztelő)
- Mi a BANK projekt határideje? $H(\text{BANK})$
- Milyen határidejei vannak az alkalmazottaknak? $H \circ P$
- Milyen határidejei vannak a tesztelőknek? $H \circ P \circ B^{-1}$

Kompozíció

$$R \circ S = \{(x, y) : \exists z : (x, z) \in S, (z, y) \in R\}$$

Állítás

Legyen R, S, T binér reláció. Ekkor

- 1 Ha $\text{rng}(S) \supset \text{dmn}(R)$, akkor $\text{rng}(R \circ S) = \text{rng}(R)$
- 2 $R \circ (S \circ T) = (R \circ S) \circ T$ (a kompozíció asszociatív)
- 3 $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$.

Bizonyítás

- 1 $\text{rng}(R) = \{y : \exists z : (z, y) \in R\}$. Mivel $\text{rng}(S) \supset \text{dmn}(R)$, ezért minden $(z, y) \in R$ esetén $\exists x : (x, z) \in S$, így $(x, y) \in R \circ S$
- 2 $R \circ (S \circ T) = \{(w, z) : \exists y : (w, y) \in S \circ T, (y, z) \in R\} = \{(w, z) : \exists y \exists x : (w, x) \in T, (x, y) \in S, (y, z) \in R\} = (R \circ S) \circ T$
- 3 $(R \circ S)^{-1} = \{(y, x) : \exists z : (x, z) \in S, (z, y) \in R\} = \{(y, x) : \exists z : (z, x) \in S^{-1}, (y, z) \in R^{-1}\} = S^{-1} \circ R^{-1}$

Példa

Relációk: $=, <, \leq, |, \subset, T = \{(x, y) : x, y \in \mathbb{R}, |x - y| < 1\}$

Definíció

Legyen R reláció X -en. Ekkor azt mondjuk, hogy

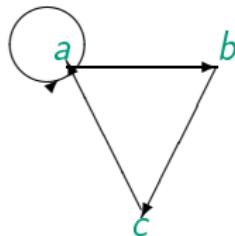
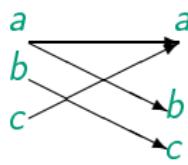
- ① R tranzitív, ha $xRy \wedge yRz \Rightarrow xRz$ ($=, <, \leq, |, \subset$)
- ② R szimmetrikus, ha $xRy \Rightarrow yRx$ ($=, T$)
- ③ R antiszimmetrikus, ha $xRy \wedge yRx \Rightarrow x = y$ ($=, \leq, \subset$)
- ④ R szigorúan antiszimmetrikus, ha xRy és yRx egyszerre nem teljesülhet ($<$)
- ⑤ R reflexív, ha $\forall x \in X : xRx$ ($=, \leq | \subset, T$)
- ⑥ R irreflexív, ha $\forall x \in X : \neg xRx$ ($<$)
- ⑦ R trichotom, ha $\forall x, y \in X$ esetén $x = y, xRy$ és yRx közül pontosan egy teljesül ($<$)
- ⑧ R dichotom, ha $\forall x, y \in X$ esetén xRy vagy yRx (esetleg mindkettő) ($=, \leq$)

Relációk tulajdonságai

A reflexív, irreflexív, trichotom, dichotom tulajdonságok nem csak a relációtól függnek, hanem az alaphalmaztól is:

Az $\{(x, x) \in \mathbb{R} \times \mathbb{R}, x \in \mathbb{R}\} \subset \mathbb{R} \times \mathbb{R} \subset \mathbb{C} \times \mathbb{C}$, mint \mathbb{R} -en értelmezett reláció reflexív, de mint \mathbb{C} -én értelmezett reláció nem reflexív.

Példa

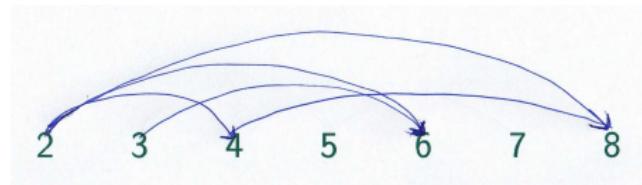


tranzitív X	sziigorúan antiszimmetrikus X	trichotom X
szimmetrikus X	reflexív X	dichotom X
antiszimmetrikus ✓	irreflexív X	

Relációk gráfja

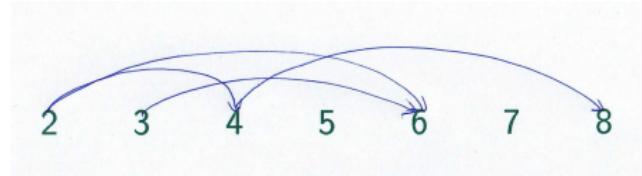
A relációk gráfját egyszerűsíthetjük:

- Ha egy reláció **reflexív**, akkor a hurokéleket nem rajzoljuk.



osztója reláció

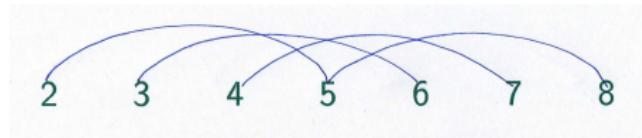
- Ha egy reláció **tranzitív**, akkor elhagyjuk az olyan éleket, amelyek létezése a tranzitivitás miatt a már berajzolt élekből következik.



osztója reláció

Reláció gráfja, Ekvivalenciareláció, osztályozások

- Ha egy reláció **szimmetrikus**, akkor irányított élek helyett csak éleket (vonalakat) rajzolunk.



$\equiv \text{ mod } 3$

Definíció

Legyen X egy halmaz, R reláció X -en. Az R relációt **ekvivalenciareláció** mondjuk, ha **reflexív**, **szimmetrikus**, **tranzitív**.

Példa

1. $=$; 2. $\equiv (\text{ mod } m)$; 3. $z \sim w$, ha $Re(z) = Re(w)$.

Definíció

Az X részhalmazainak egy \mathcal{O} rendszerét az X **osztályozásának** nevezik, ha \mathcal{O} páronként diszjunkt nem-üres halmazokból álló halmazrendszer és $\cup \mathcal{O} = X$.

Ekvivalenciareláció, osztályozások

Példa

1. \mathbb{R} egy osztályozása: $\{\{a\} : a \in \mathbb{R}\}$;
2. \mathbb{Z} egy osztályozása: $\{\overline{0}; \overline{1}, \dots, \overline{m-1}\}$ (maradékosztályok $\text{mod } m$);
3. \mathbb{C} egy osztályozása: $\{\{z \in \mathbb{C} : \operatorname{Re}(z) = r\} : r \in \mathbb{R}\}$.

Tétel

Valamely X halmazon értelmezett \sim ekvivalenciareláció esetén az $\bar{x} = \{y \in X : y \sim x\}$ ($x \in X$), ekvivalenciaosztályok X -nek egy osztályozását adják, ezt az osztályozást X/\sim -el jelöljük.

Bizonyítás

Legyen \sim egy X -beli ekvivalenciareláció. Azt kell megmutatni, hogy $X/\sim = \{\bar{x} : x \in X\}$ az X egy osztályozását adja.

- Mivel \sim reflexív, így $x \in \bar{x} \Rightarrow \cup_x \bar{x} = X$.

Biz. folyt.

- Különböző ekvivalenciaosztályok páronként diszjunktak. Tfh.
 $\bar{x} \cap \bar{y} \neq \emptyset$, legyen $z \in \bar{x} \cap \bar{y}$. Mivel $z \in \bar{x} \Rightarrow z \sim x$, ahonnan a szimmetria miatt $x \sim z$. Hasonlóan $z \in \bar{y} \Rightarrow z \sim y$. A tranzitivitás miatt $x \sim z \sim y \Rightarrow x \sim y \Rightarrow x \in \bar{y}$. Hasonlóan $y \in \bar{x} \Rightarrow \bar{x} = \bar{y}$.

Tétel

Valamely X halmazon bármely \mathcal{O} osztályozás esetén az $R = \{Y \times Y : Y \in \mathcal{O}\}$ reláció ekvivalenciareláció, amelyekhez tartozó ekvivalenciaosztályok halmaza \mathcal{O} .

Bizonyítás

- R reflexív: legyen az x osztálya $Y : x \in Y \in \mathcal{O}$. Ekkor $(x, x) \in Y \times Y$.

Biz. folyt.

- **R szimmetrikus:** legyen az $(x, y) \in R$. Ekkor $x, y \in Y$ valamely Y osztályra, speciálisan $(y, x) \in Y \times Y$.
- **R tranzitív:** hasonlóan legyen $(x, y), (y, z) \in R$, ezért $x, y \in Y, y, z \in Y'$. Mivel az osztályok páronként diszjunktak, így $Y = Y'$, speciálisan $z \in Y$, azaz $(x, z) \in Y \times Y$.

Az ekvivalenciarelációk illetve osztályozások kölcsönösen egyértelműen meghatározzák egymást.

Példa

- $\longleftrightarrow \{\{a\} : a \in \mathbb{R}\}$;
- $\equiv (\text{ mod } m) \longleftrightarrow \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$;

Példa

- A síkon két **egyenes** legyen \sim , ha párhuzamosak. Ekkor az osztályok az **irány** fogalmát adják.

Definíció

Az X halmazon értelmezett reflexív, tranzitív és antiszimmetrikus relációt részbenrendezésnek nevezzük. (jele: \leq, \preceq, \dots)

Ha $x, y \in X$ esetén $x \leq y$ vagy $y \leq x$, akkor x és y összehasonlítható.

(Ha minden elempár összehasonlítható, akkor a reláció dichotom.)

Az X halmazon értelmezett reflexív, tranzitív, antiszimmetrikus és dichotom relációt rendezésnek nevezzük.

Ha egy részbenrendezés esetén minden elem összehasonlítható, akkor az rendezés.

Példa

- \mathbb{R} -en a \leq reláció rendezés: $\forall x, y \in \mathbb{R} : x \leq y$ vagy $y \leq x$.
- \mathbb{Z} -n az $|$ (osztója) reláció részbenrendezés: $4 | 5, 5 | 4$
- Az X halmaz összes részhalmazán a \subset reláció részbenrendezés $X = \{a, b, c\}, \{a\} \not\subset \{b, c\}, \{b, c\} \not\subset \{a\}$

Definíció

Az X -beli R relációhoz tartozó **szigorú** reláció, az az S reláció, melyre $xSy \Leftrightarrow xRy \wedge x \neq y$.

Az X -beli R relációhoz tartozó **gyenge** reláció, az az T reláció, melyre $xTy \Leftrightarrow xRy \vee x = y$.

Másképpen megfogalmazva:

$S = R \setminus \mathbb{I}_X$, $T = R \cup \mathbb{I}_X$, ahol $\mathbb{I}_X = \{(x, x) : x \in X\}$.

Példa

- \leq -hez tartozó szigorú reláció: $<$.
- \subset -hez tartozó szigorú reláció: \subsetneq .
- osztója relációhoz tartozó szigorú reláció: valódi osztója.

Szigorú és gyenge rendezés

Definíció

Az X halmazon értelmezett tranzitív és irreflexív relációt **szigorú részbenrendezésnek** nevezük. (jele: $<$, \prec , ...)

Megjegyzések

- A tranzitivitásból és az irreflexivitásból következik a szigorú antiszimmetria: ha $x < y$ és $y < x$ tranzitivitás miatt $x < x$, ami ellentmondás.
- Egy részbenrendezés relációjának szigorú változata a szigorú részbenrendezés és fordítva:
 $"<" = " \leq \setminus \mathbb{I}_X"$, $"\leq" = " < \cup \mathbb{I}_X"$.

Állítás

Ha a \leq reláció rendezés, akkor $<$ trichotom, és fordítva.

Bizonyítás

Kell: $x = y$, $x < y$ és $y < x$ egyszerre nem teljesülhet. Ha $x = y$,



Bizonyítás folyt.

Továbbá $x < y$ és $y < x$ sem teljesülhet egyszerre.

Definíció (Intervallum)

Legyen X egy részbenrendezett halmaz. Ha $x \leq z$ és $z \leq y$, akkor azt mondjuk, hogy z az x és y közé esik, ha $x < z$ és $z < y$, akkor azt mondjuk, hogy z az x és y szigorúan közé esik. Az összes ilyen elemek halmazát $[x, y]$ ill. (x, y) jelöli. A $[x, y]$, ill. (x, y) jelölések definíciója analóg.

Példa

Legyen X az $\{a, b, c\}$ halmaz hatványhalmaza a részhalmaz relációval. Ekkor $\{\{a\}, \{a, b, c\}\} = \{\{a\}, \{a, b\}, \{a, b, c\}\}$
 $(\{a\}, \{a, b, c\}) = \{\{a, b\}\}$

Legyen X az pozitív egész számok halmaza az osztója relációval.
Ekkor $[2, 12] = \{2, 4, 6, 12\}$
 $[2, 12] = \{4, 6\}$

Definíció

Ha $x < y$, de nem létezik szigorúan x és y közé eső elem, akkor x megelőzi y -t.

Példa

Legyen X az $\{a, b, c\}$ halmaz hatványhalmaza a részhalmaz relációval. Ekkor az $\{a\}$ megelőzi $\{a, b\}$ -t, illetve $\{a, c\}$ -t.

Legyen X a pozitív egész számok halmaza az osztója relációval. Ekkor 2 megelőzi a 4, 6, 10, 14 elemeket.

Definíció

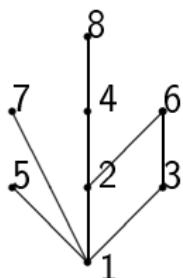
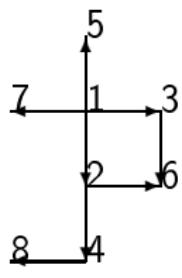
A $\{y \in X : y < x\}$ részhalmazt az x elemhez tartozó kezdőszeletnek nevezzük.

Példa

Legyen X az $\{a, b, c\}$ halmaz hatványhalmaza a részhalmaz relációval. Ekkor az $\{a, b\}$ elemhez tartozó kezdőszelet:
 $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Részbenrendezések Hasse-diagramja

Ha egy részbenrendezett halmaz elemeit pontokkal ábrázoljuk és csak azon x, y párok esetén rajzolunk irányított élt, amelyre x közvetlenül megelőzi y -t, akkor a részbenrendezett halmaz **Hasse-diagramját** kapjuk. Néha irányított élek helyett irányítatlan élt rajzolunk és a kisebb elem kerül lejebb.



Legkisebb, legnagyobb, minimális, maximális elem

Definíció

Az X részbenrendezett halmaz:

legkisebb eleme: olyan $x \in X : \forall y \in X, x \leq y$;

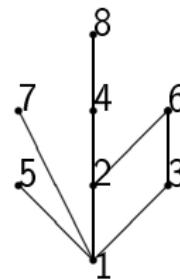
legnagyobb eleme: olyan $x \in X : \forall y \in X, y \leq x$

minimális eleme: olyan $x \in X : \neg \exists y \in X, y \leq x$

maximális eleme: olyan $x \in X : \neg \exists y \in X, x \leq y$;

Példa

Legyen $X = \{1, 2, \dots, 8\}$ az oszthatóságra:



legkisebb elem: 1

legnagyobb elem: nincs

minimális elem: 1

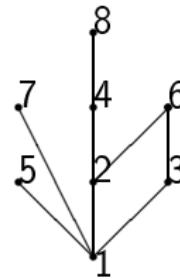
maximális elemek: 5, 6, 7, 8

Megjegyzések

- Minimális és maximális elemből több is lehet.
- Ha a halmaz **rendezett**, akkor a minimális, és legkisebb elem, továbbá a maximális és legnagyobb elem egybeesik.
- Ha X -nek létezik egyértelmű minimális, ill. maximális eleme, akkor azt $\min X$, ill. $\max X$ jelöli.

Példa

Legyen $X = \{1, 2, \dots, 8\}$ az oszthatóságra:



$$\min X \quad 1$$

$\max X$ elem: nincs

Definíció

Egy X részben rendezett halmaz x elemét az Y részhalmaz alsó korlátja, ha $\forall y \in Y : x \leq y$;

felső korlátja, ha $\forall y \in Y : y \leq x$

Ha az alsó korlátok halmazában van legnagyobb elem, akkor ez az Y infimuma: $\inf Y$, ha a felső korlátok halmazában van legkisebb elem, akkor ez az Y supremuma: $\sup Y$

Példa Legyen $X = \{1, 2, \dots, 8\}$ az oszthatóságra:

$\{1, 2, 3\}$ alsó korlátja: 1

felső korlátja: 6

inf: 1

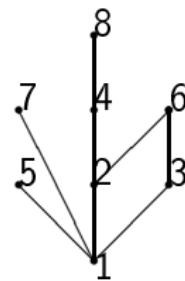
sup: 6.

$\{2, 3, 4\}$ alsó korlátja: 1

felső korlátja: nincs

inf: 1

sup: nincs



Definíció

Ha az X részben rendezett halmaz bármely nem üres, felülről korlátos részhalmazának van supremuma, akkor **felső határ tulajdonságúnak** nevezzük, ha bármely nem üres alulról korlátos részhalmazának van infimuma, akkor X -et **alsó határ tulajdonságúnak** nevezzük.

Példa

- Az egész számok halmaza az oszthatóságra nézve alsó és felső határ tulajdonságú: Ha $Y = \{a_1, a_2, \dots\}$, akkor $\inf Y = \text{Inko}(a_1, a_2, \dots)$ felső határa $\text{Ikkt}(a_1, a_2, \dots)$
- A racionális számok halmaza a szokásos rendezésre nézve sem alsó sem felső határ tulajdonságú:
 $Y = \{r \in \mathbb{Q} : r \leq \sqrt{2}\}$ halmaznak van felső korlátja (pl.: $1000, 999, 2, 1, 42, \dots$), de nincs (racionális) supremuma (a supremum $\sqrt{2} \notin \mathbb{Q}$ lenne).

Definíció

Egy f relációt **függvénynek** (leképezésnek, transzformációnak, hozzárendelésnek, operátornak) nevezzük, ha

$(x, y) \in f \wedge (x, y') \in f \Rightarrow y = y'$. A $(x, y) \in f$ jelölés helyett ilyenkor a $f(x) = y$ (vagy $f : x \rightarrow y, f_x = y$) jelölést használjuk. Az y az f függvény x helyen (**argumentumban**) felvett értéke.

Példa

- $f = \{(x, x^2) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$ reláció függvény: $f(x) = x^2$.
- Az $f^{-1} = \{(x^2, x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$ inverz reláció **nem** függvény: $(4, 2), (4, -2) \in f^{-1}$.
- Legyen F_n a Fibonacci sorozat:
 $F_1 = F_2 = 1, F_n = F_{n-1} + F_{n-2} : 1, 1, 2, 3, 5, 8 \dots$ Ekkor az $F \subset \mathbb{N} \times \mathbb{N}$ reláció, n helyen az értéke $F_n = F(n)$.

Definíció

Az $f \subset X \times Y$ függvények halmazát $X \rightarrow Y$ jelöli. Ha $d\text{mn}(f) = X$, akkor az $f : X \rightarrow Y$ jelölést használjuk.

Megjegyzés

Ha $f : X \rightarrow Y$, akkor $d\text{mn}(f) = X$ és $\text{rng}(f) \subset Y$.

Példa

egyen $f(x) = \sqrt{x}$. Ekkor

- $f \in \mathbb{R} \rightarrow \mathbb{R}$, de nem $f : \mathbb{R} \rightarrow \mathbb{R}$.
- $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}$.
- $f : \mathbb{R}_0^+ \rightarrow \mathbb{C}$.

Definíció

Az $f : X \rightarrow Y$ függvény

- **injektív**, ha $f(x) = y \wedge f(x') = y \Rightarrow x = x'$;
- **szürjektív** ha $\text{rng}(f) = Y$;
- **bijektív**, ha **injektív** és **szürjektív**.

Megjegyzés: Egy f függvény pontosan akkor **injektív**, ha f^{-1} reláció függvény.

- Az $f : \mathbb{R} \rightarrow \mathbb{R}$, $f : x \rightarrow x^2$ függvény **nem injektív** és **nem szürjektív**: $f(-1) = f(1)$, $\text{rng}(f) = \mathbb{R}_0^+$
- Az $f : \mathbb{R} \rightarrow \mathbb{R}_0^+$, $f : x \rightarrow x^2$ függvény **nem injektív**, de **szürjektív**
- Az $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$, $f : x \rightarrow x^2$ függvény **injektív** és **szürjektív**, tehát **bijektív**.

Megjegyzés: Az, hogy egy $f : X \rightarrow Y$ függvény szürjektív-e, függ Y -tól. Ha $Y \subsetneq Y'$ akkor $f \subset X \times Y \subset X \times Y'$ így az $f : X \rightarrow Y$ függvény biztos **nem** szürjektív.

Definíció

Az $f : X \rightarrow X$ bijektív függvényt **permutációnak** nevezzük.

Példa

- Ha $X = \{1, 2, \dots, n\}$, akkor az $X \times X$ permutációk száma $n!$: az $f(1), f(2), \dots, f(n)$ az $1, 2, \dots, n$ elemek egy **ismétlés nélküli permutációja**.
- Az $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = x^3$ a valós számok egy permutációja.
- Az $f(x) = x^3$ függvény **nem** permutációja \mathbb{C} -nek: legyen ε primitív 3-ik egységggyök, ekkor $f(\varepsilon) = f(1)$, de $\varepsilon \neq 1$.

Legyen $E_n \subset \mathbb{C}$ az n -edik egységgökök halmaza:
 $E_n = \{z \in \mathbb{C} : z^n = 1\}.$

Állítás

Ekkor az $f : x \rightarrow x^k$ függvény pontosan akkor bijekció, ha $(n, k) = 1$.

Bizonyítás

Ha $(n, k) = d > 1$, akkor f nem injektív, ha ε primitív n -edik egységgöök, akkor $f(\varepsilon^{n/d}) = f(1) = 1$, ui. $(\varepsilon^{n/d})^d = \varepsilon^n = 1$, de $\varepsilon^{n/d} \neq 1$.

Ha $(n, k) = 1$, f injektív: ha ε primitív n -edik egységgöök és $f(\varepsilon^i) = f(\varepsilon^j) \Leftrightarrow \varepsilon^{ik} = \varepsilon^{jk} \Leftrightarrow \varepsilon^{k(i-j)} = 1 \Leftrightarrow n|k(i-j) \Leftrightarrow n|i-j \Leftrightarrow \varepsilon^i = \varepsilon^j$.

Mivel $f : E_n \rightarrow R_n$ injektív, ezért a skatulya-elv miatt bijektív is.

Függvények kompozíciója

Emlékeztető

Relációk kompozíciója $R \circ S = \{(x, y) : \exists z : (x, z) \in S, (z, y) \in R\}$

Függvények Az f reláció függvény, ha

$$(x, y) \in f \wedge (x, y') \in f \Rightarrow y = y'$$

Tétel

- ① Ha f és g függvény, akkor $g \circ f$ is függvény.
- ② Ha f és g injektív, akkor $g \circ f$ is injektív.
- ③ Ha $f : X \rightarrow Y$, $g : Y \rightarrow Z$, akkor $g \circ f : X \rightarrow Z$.

Bizonyítás

- ① Legyen $(x, y) \in g \circ f$, $(x, y') \in g \circ f$:
 $\exists z : (x, z) \in f, (z, y) \in g, \exists z' : (x, z') \in f, (z', y') \in g$. Mivel f függvény $z = z'$, mivel g függvény $y = y'$.
- ② Legyen $(g \circ f)(x) = (g \circ f)(x')$. Legyen $f(x) = y, f(x') = y'$.
Igy $g(y) = g(y')$. Mivel g injektív: $y = y'$. Mivel f injektív:
 $x = x'$.

3. Állítás bizonyítása: HF

Monoton függvények

Definíció

Legyenek X, Y részbenrendezett halmazok. Az $f : X \rightarrow Y$ függvény

- ❶ monoton növekedő, ha $x, y \in X, x \leq y \Rightarrow f(x) \leq f(y)$
- ❷ szigorúan monoton növekedő, ha
 $x, y \in X, x < y \Rightarrow f(x) < f(y)$
- ❸ monoton csökken, ha $x, y \in X, x \leq y \Rightarrow f(x) \geq f(y)$
- ❹ szigorúan monoton csökkenő, ha
 $x, y \in X, x < y \Rightarrow f(x) > f(y)$

Példa

- Legyen $X = \mathbb{R}$ a szokásos rendezéssel. Ekkor az $f(x) = x; x^3$ szigorúan monoton növekedő függvények.
- Legyen $X = \mathbb{Z}$ az oszthatóság részbenrendezéssel. Ekkor az $f(x) = 5x$ szigorúan monoton növekedő függvény:
 $x|y \Rightarrow 5x|5y$.

Megjegyzés

- Ha X, Y rendezett halmazok, akkor egy szigorúan monoton növekedő (ill csökkenő) függvény injektív is: Ha $x \neq y \Rightarrow x < y$ vagy $x > y \Rightarrow f(x) < f(y)$ vagy $f(x) > f(y) \Rightarrow f(x) \neq f(y)$.
- Ha X, Y rendezett halmazok és f szigorúan monoton növekedő (ill csökkenő) függvény, akkor f^{-1} szigorúan monoton növekedő (ill csökkenő) függvény:
Mivel f injektív, f^{-1} is függvény.
Ha $f(x) < f(y)$, akkor nem lehet $x \geq y$.

Példa

Legyen $X = \mathbb{R}$ a szokásos rendezéssel. Ekkor az $f(x) = \sqrt[3]{x}$ szigorúan monoton növekvő függvény.

Definíció

Egy X halmazon értelemezett **binér** (kétváltozós) **művelet** egy $\otimes : X \times X \rightarrow X$ függvény. Gyakran $\otimes(x, y)$ helyett $x \otimes y$ -t írunk.
Egy X halmazon értelmezett **unér** (egyváltozós) **művelet** egy $\otimes : X \rightarrow X$ függvény.

Példa

- \mathbb{C} halmazon a $+, \cdot$ binér, $z \rightarrow -z$ (ellentett) unér művelet.
- \mathbb{C} halmazon a $/$ (osztás) nem művelet, mert $dmn(/) \neq \mathbb{C} \times \mathbb{C}$.
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ halmazon a $/$ binér, a $x \rightarrow 1/x$ (reciprok) unér művelet.
- \mathbb{C} halmazon a 0 ill 1 konstans kijelölése nullér művelet.

Egy véges halmazon bármely binér művelet megadható a műveleti táblával.

\wedge	I	H
I	I	H
H	H	H

\vee	I	H
I	I	I
H	I	H

XOR	I	H
I	H	I
H	I	H

\neg	I	H
	H	I

Definíció (Műveletek függvényekkel)

Legyen X tetszőleges halmaz, Y halmaz a \otimes művelettel,
 $f, g : X \rightarrow Y$ függvények. Ekkor
 $(f \otimes g)(x) = f(x) \otimes g(x)$

Definíció

A \otimes művelet asszociatív, ha $(a \otimes b) \otimes c = a \otimes (b \otimes c)$;
kommutatív, ha $a \otimes b = b \otimes a$.

Példa

- \mathbb{C} -n a + ill. műveletek asszociatívak, kommutatívak.
- A függvények a kompozíció művelete, asszociatív:
 $(f \circ g) \circ h = f \circ (g \circ h)$
- A függvények a kompozíció műveltem nem kommutatív:
 $f(x) = x + 1, g(x) = x^2$:
 $x^2 + 1 = (f \circ g)(x) \neq (g \circ f)(x) = (x + 1)^2$.
- Az osztás nem asszociatív: $\frac{a}{bc} = (a/b)/c \neq a/(b/c) = \frac{ac}{b}$

Művelettartó leképezések

Definíció

Legyen X halmaz az \otimes művelettel. Az $g : X \rightarrow Y$ függvény művelettartó, ha $f(x \otimes y) = f(x) \otimes f(y)$

Példa

- Legyen $X = \mathbb{R}$ a + művelettel, $Y = \mathbb{R}^+$ a · művelettel. Ekkor a $x \rightarrow a^x$ művelettartó: $a^{x+y} = a^x \cdot a^y$.
- Legyen $X = Y = \mathbb{C}$ a + művelettel. Ekkor a $z \rightarrow \bar{z}$ művelettartó: $\overline{z+w} = \bar{z} + \bar{w}$
- Legyen $X = \mathbb{Z}$ a + művelettel, $Y = \mathbb{Z}_m$ a $+_m$ (összeadás modulo m) művelettel. Ekkor a $n \rightarrow n \text{ mod } m$ művelettartó: $k+n \text{ mod } m = (k \text{ mod } m) +_m (n \text{ mod } m)$.
- Legyen $X = \{I, H\}$ a XOR , \wedge művelettel, \mathbb{Z}_2 a $+, \cdot$ művelettel. Ekkor a $H \rightarrow 0$, $I \rightarrow 1$ művelettartó.

A természetes számokból kiindulva megkonstruálhatók az

- természetes számok: $\mathbb{N} = \{0, 1, \dots\}$
- egész számok: $\mathbb{Z} = \{\dots - 1, 0, 1 \dots\}$
- racionális számok: $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$:
- valós számok: $\mathbb{R} = ?$
- komplex számok: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$

Kérdések

- Milyen fontos tulajdonságokkal rendelkeznek az adott számhalmazok?
- Mik a valós számok?
- Mi a pontos kapcsolat a műveletek és a számhalmazok között?
 \mathbb{N} -ben nincs kivonás, de \mathbb{Z} -ben van.
 \mathbb{Z} -ben nincs osztás, de \mathbb{Q} -ban van...

Peano-axiómák

Legyen \mathbb{N} egy halmaz, ' $+$ ' egy unér művelet (rákövetkező). Ekkor

- ① $0 \in \mathbb{N}$
- ② $n \in \mathbb{N} \Rightarrow n^+ \in \mathbb{N}$
- ③ $n \in \mathbb{N} \Rightarrow n^+ \neq 0$
- ④ $n, m \in \mathbb{N}$ esetén $n^+ = m^+ \Rightarrow n = m$
- ⑤ $S \subset \mathbb{N}, 0 \in S, (n \in S \Rightarrow n^+ \in S) \Rightarrow S = \mathbb{N}$.

Megjegyzések

- Az axiómák egyértelműen definiálják \mathbb{N} -t.
- Mindegyik axióma szükséges
- \mathbb{N} halmaz megkonstruálható:
 $0 := \emptyset, 0^+ := \{\emptyset\}, (0^+)^+ := \{\emptyset, \{\emptyset\}\}, \dots$
- $1 := 0^+, 2 := 1^+ \dots$

Műveletek természetes számokkal

\mathbb{N} -en természetes módon definiálhatjuk az összeadást (HF), például $n + 1 := n^+$, $n + 2 := (n^+)^+$...

Állítás

Ha $k, m, n \in \mathbb{N}$, akkor

- ❶ $(k + m) + n = k + (m + n)$ (asszociativitás)
- ❷ $0 + n = n + 0 = n$ (van nullelem/egységelem)

Definíció

A G halmaz a \otimes művelettel **félcsoport**, ha \otimes asszociatív. Ha létezik $n \in G : \forall g \in G : n \otimes g = g \otimes n = g$, akkor az n **egységelem** (nullelem, neutrális elem), G pedig **egységelemes félcsoport**.

Példa

- ❶ \mathbb{N} a + művelettel egységelemes félcsoport, $n = 0$ egységelemmel.

- \mathbb{Q} a \cdot művelettel egységelemes félcsoport, $n = 1$ egységelemmel.
- $\mathbb{C}^{k \times k}$ mátrixszorzással egységelemes félcsoport, az egységmátrixszal.

\mathbb{N} halmazon nem (mindíg) tudjuk a kivonást elvégezni.

A kivonás elvégzéséhez elég (lenne), hogy a 0-ból ki tudjuk vonni az adott n számot (ellentett).

Definíció

Legyen G egy egységelemes félcsoport a \otimes művelettel és n egységelemmel. A $g \in G$ elem **inverze** (elltentetteje) az $g^{-1} \in G$ elem, melyre $g \otimes g^{-1} = g^{-1} \otimes g = n$. Ha minden $g \in G$ elemnek létezik inverze, akkor G **csoport**.

Ha \otimes kommutatív, akkor G **Abel csoport**.

Állítás

\mathbb{Z} a legszűkebb olyan (Abel) csoport, mely tartalmazza \mathbb{N} -et.

Megjegyzés

\mathbb{Z} megkonstruálható \mathbb{N} -ből.

További példák csoportokra.

- \mathbb{Q} a + művelettel a 0 egységelemmel
- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ a · művelettel az 1 egységelemmel
- \mathbb{Z}_m a + művelettel $\bar{0}$ egységelemmel
- \mathbb{Z}_p^* a · művelettel az $\bar{1}$ egységelemmel
- $\{M \in \mathbb{C}^{k \times k} : \det M \neq 0\}$ a mátrixszorzással és az egységmátrixszal, mint egységelemmel.
- $X \rightarrow X$ bijektív függvények \circ művelettel és az $\text{id}_X : x \rightarrow x$ identikus leképezéssel

Egész számok szorzása

Az egész számok körében definiálhatjuk a \cdot műveletet:

Ha $n \in \mathbb{N}, m \in \mathbb{Z}$, akkor legyen $n \cdot m = \underbrace{m + m + \cdots + m}_{n \text{ darab}}$.

Ha $n \notin \mathbb{N}$ akkor legyen $n \cdot m = -((-n) \cdot m)$

Állítás

Az \mathbb{Z} a \cdot műveletekre kommutatív egységelemes félcsoport (A \cdot kommutatív, asszociatív, van egységelem.)

A két művelet nem független:

Állítás

\mathbb{Z} -n a \cdot a $+$ -ra nézve disztributív: $k \cdot (l + m) = k \cdot l + k \cdot m$.

Definíció

Legyen R egy halmaz két művelettel: \oplus, \otimes . Ekkor az R gyűrű, ha

- R az \oplus Abel csoport (0 -val, mint egységelemmel)
- R az \otimes művelettel félcsoport
- a \otimes az \oplus -ra nézve disztributív:
 $r \otimes (s \oplus t) = (r \otimes s) \oplus (r \otimes t)$
 $(s \oplus t) \otimes r = (s \otimes r) \oplus (t \otimes r).$

Az R egységelemes gyűrű, ha $\mathbb{R} \setminus \{0\}$ az \otimes művelet esetén van egységelem. Az R kommutatív gyűrű, ha a \otimes művelet (is) kommutatív.

Példa

- \mathbb{Z} a $(+, \cdot)$ műveletekre egységelemes kommutatív gyűrű.
- A páros számok halmaza gyűrű, de nem egységelemes
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ egységelemes kommutatív gyűrűk
- $\mathbb{C}^{k \times k}$ egységelemes gyűrűm de nem kommutatív.

Nullosztómentes gyűrűk

A gyűrűkben általában nem lehet elvégezni az osztást:

- \mathbb{Z} -ben nem oldható meg a $2x = 1$ egyenlet.
- $\mathbb{R}^{2 \times 2}$ -ban nem oldható meg az alábbi egyenlet
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
- \mathbb{Z}_4 -ben nem oldható meg a $2x \equiv 1 \pmod{4}$

Definíció

Ha egy R gyűrűben $r, s \in R$ $r, s \neq 0$ esetén $r \otimes s \neq 0$, ekkor R nullosztómentes gyűrű.

Példa

Nem nullosztómentes gyűrűk

- $\mathbb{R}^{k \times k}$:
$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
- \mathbb{Z}_4 : $2 \cdot 2 \equiv 0 \pmod{4}$.

Szeretnénk \mathbb{Z} -ben az osztást elvégezni. Mivel az osztás nem "szép" művelet (nem asszociatív), ezért azt a reciprokkal (inverrel) való szorzással helyettesítenénk.

Definíció

Legyen K egy halmaz, azon két művelet: \oplus, \otimes . A K test, ha

- K gyűrű;
- $K^* = K \setminus \{0\}$ a \otimes művelettel csoport.

Megjegyzés Ha K^* csoport, akkor minden elemnek létezik inverze (reciproka), így minden elemmel tudunk osztani.

Állítás

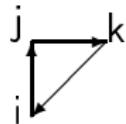
\mathbb{Q} az \mathbb{N} -et tartalmazó legszűkebb test.

Megjegyzés

\mathbb{Q} megkonstruálható: A $(r, s) \sim (p, q)$ ($s, q \neq 0$), ha $r \cdot q = p \cdot s$ ekvivalenciareláció osztályai a racionális számok.

Példa

- \mathbb{R}, \mathbb{C}
- $\{r + s\sqrt{2} : r, s \in \mathbb{Q}\}$: $\frac{1}{r+s\sqrt{2}} = \frac{1}{r+s\sqrt{2}} \cdot \frac{r-s\sqrt{2}}{r-s\sqrt{2}}$
 $= \frac{r-s\sqrt{2}}{r^2-2s^2} = \frac{r}{r^2-2s^2} + \frac{-s}{r^2-2s^2}\sqrt{2}$
- Kvaterniók $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ továbbá
 $i^2 = j^2 = k^2 = -1, ij = k, ji = -k, \dots$ Nem kommutatív test!



\mathbb{Z} -n a természetes módon definiálhatjuk a rendezést:

- Adott $n \in \mathbb{N}, n \neq 0$ esetén legyen $0 < n$.
- Legyen továbbá $n < m$, ha $0 < n - m$

Ekkor a rendezés kompatibilis a műveletekkel:

Állítás

Ha $k, m, n \in \mathbb{Z}$, akkor

- $k < m \Rightarrow k + n < m + n$
- $m, n > 0 \Rightarrow m \cdot n > 0$.

Definíció

Egy R gyűrű rendezett gyűrű, ha van az R -en definiálva egy rendezés, mely kielégíti a fenti tulajdonságokat.

A \mathbb{Z} -n definiált rendezés kiterjeszthető \mathbb{Q} -ra: $\frac{p}{q} < \frac{r}{s}$, ha $ps < rq$. Kiterjesztés azonban nem lesz "teljes", \mathbb{Q} nem lesz felsőhatár tulajdonságú.

Emlékeztető: Egy X halmaz felsőhatár tulajdonságú, ha minden $Y \subset X$ felülről korlátos részhalmaznak van supremuma.

Allítás

Nincs olyan racionális szám, melynek a négyzete 2.

Bizonyítás

Ha lenne, akkor $(-\frac{m}{n})^2 = (\frac{m}{n})^2$ miatt lenne olyan is, amely felírható $\frac{m}{n}$ alakban, ahol $m, n \in \mathbb{N}^+$. Válasszuk azt a felírást, melyre a számláló minimális. Mivel $m^2 = 2n^2$, m páros kell legyen. Legyen $m = 2k$, $k \in \mathbb{N}^+$. Ekkor $4k^2 = 2n^2$, ahonnan $2k^2 = n^2$. Innen n is páros. Ez ellentmond annak, hogy a számláló minimális.

Valós számok definíciója

Legyen \mathbb{R} az \mathbb{N} -et tartalmazó legszűkebb felsőhatár tulajdonsággal rendelkező rendezett test.

Mejegyzés

- A valós számok halmaza lényegében egyértelmű.
- \mathbb{R} megkonstruálható: legyen \mathbb{R} a \mathbb{Q} kezdőszeletei:
Egy $A \subset \mathbb{Q}$ kezdőszelet, ha $A \neq \mathbb{Q}$ és $r \in A, s < r \Rightarrow s \in A$.
például $\sqrt{2} \leftrightarrow \{r \in \mathbb{Q} : r \leq \sqrt{2}\}$

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ definiálható \mathbb{R} segítségével is:

- \mathbb{N} : a $0, 1 \in \mathbb{R}$ elemeket tartalmazó legszűkebb félcsoport
- $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$
- $\mathbb{Q} = \{r/s \in \mathbb{R} : r, s \in \mathbb{Z}, s \neq 0\}$.

Műveletek halmazokon

Struktúra

Peano axiómák

félcsoporthoz: van asszociatív művelet

csoport: van inverz

gyűrű: két művelet,

\oplus -ra kommutatív csoport

\otimes -ra félcsoport, disztributivitás

test: két művelet,

\oplus -ra kommutatív csoport,

\otimes -ra a 0 kivételével csoport,

disztributivitás

Példa

\mathbb{N}

$(\mathbb{N}, +), (\mathbb{Z}, \cdot)$

$(\mathbb{Z}, +), (\mathbb{Q}^*, \cdot), (\mathbb{Z}_m, +), (\mathbb{Z}_p^*, \cdot)$

$(\mathbb{Z}, +, \cdot), (\mathbb{Z}_m, +, \cdot)$

$(\mathbb{R}^{k \times k}, +, \cdot)$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{Z}_p$

Műveletek és rendezés

Struktúra	Példa
rendezett gyűrű	\mathbb{Z}
rendezett test	\mathbb{Q}, \mathbb{R}
felsőhatár tulajdonságú test	\mathbb{R}

Kombinatorika fő célja:

- véges halmazok elemeinek elrendezése;
- elrendezések különböző lehetőségeinek megszámlálása.

Példák:

- Nyolc ember közül van legalább kettő, aki a hét ugyanazon napján született.
- Minimálisan hány ember esetén lesz legalább két embernek ugyanazon a napon a születésnapja?
- Minimálisan hány ember esetén lesz legalább egy ember, aki januárban született?
- Mennyi a lehetséges rendszámok /telefonszámok /IP címek száma?
- Legalább hány szelvényt kell kitölteni, hogy biztosan nyerjünk a lottón /totón?

Elemi leszámlálások

Adott két véges, diszjunkt halmaz

$$A = \{a_1, a_2, \dots, a_n\}, \quad B = \{b_1, b_2, \dots, b_m\}.$$

Hányféleképpen tudunk választani egy elemet A -ból vagy B -ből?

Lehetséges választások: $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m$

Számuk: $n + m$

Példa

Egy cukrászdában 3-féle édes sütemény van (isler, zserbó, kókuszkocka) és 2-féle sós sütemény (pogácsa, perec).

Hányféleképpen tudunk egy édes vagy egy sós süteményt enni?

Megoldás: $3 + 2 = 5$

Elemi leszámlálások

Adott két véges, diszjunkt halmaz:

$$A = \{a_1, a_2, \dots, a_n\}, \quad B = \{b_1, b_2, \dots, b_m\}.$$

Hányféleképpen tudunk választani elemet A-ból és B-ből?

Lehetséges választások:

	b_1	b_2	\dots	b_m
a_1	(a_1, b_1)	(a_1, b_2)	\dots	(a_1, b_m)
a_2	(a_2, b_1)	(a_2, b_2)	\dots	(a_2, b_m)
\vdots				\vdots
a_n	(a_n, b_1)	(a_n, b_2)	\dots	(a_n, b_m)

Számuk: $n \cdot m$

Példa

Egy cukrászdában 3-féle édes sütemény van (isler, zserbő, kókuszkocka) és 2-féle sós sütemény (pogácsa, perec).

Hányféleképpen tudunk egy édes és egy sós sütemény enni?

Megoldás: $3 \cdot 2 = 6$.

Tétel

Legyen A egy n elemű halmaz. Ekkor az A elemeinek lehetséges sorrendje: $n! = n(n - 1)(n - 2) \dots 2 \cdot 1$ (n faktoriális). Itt $0! = 1$.

Bizonyítás

Az n elemből az első helyre n -féleképpen választhatunk, a második helyre $n - 1$ -féleképpen választhatunk, ...

Igy az összes lehetőségek száma $n(n - 1) \dots 2 \cdot 1$.

Példa: Reggelire a

2 különböző szendvicset $2! = 2 \cdot 1 = 2$ - féleképpen lehet megenni.

3 különböző szendvicset $3! = 3 \cdot 2 \cdot 1 = 6$ - féleképpen lehet megenni.

4 különböző szendvicset $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ - féleképpen lehet megenni.

A 200 fős évfolyam

$200! = 200 \cdot 199 \cdot 198 \dots 2 \cdot 1 \approx 7.89 \cdot 10^{374}$ -féleképpen írhatja alá a jelenléti ívet.

Ismétléses permutáció

Példa

Egy vizsgán 5 hallgató vett részt, 2 darab 4-est, 3 darab 5-ös született. Hány sorrendben írhatjuk le az eredményeket.

Megoldás

Ha figyelembe vesszük a hallgatókat is $(2 + 3)! = 5!$ lehetséges sorrend. Ha a hallgatókat nem tüntetjük fel, egy lehetséges sorrendet többször is figyelembe vettünk:

5	5	5	5	5	5	5	5	5	5	5	5
5	5	5	5	5	5	4	4	4	4	4	4
5	5	5	5	5	5	5	5	5	5	5	5
4	4	4	4	4	4	5	5	5	5	5	5
4	4	4	4	4	4	4	4	4	4	4	4

Az 5-ösöket $3! = 6$ féleképpen cserélhetjük, ennyiszer vettünk figyelembe minden sorrendet.

Hasonlóan a 4-eseket $2! = 2$ -féleképpen cserélhetjük, ennyiszer vettünk figyelembe minden sorrendet.

$$\text{Összes lehetőség: } \frac{5!}{2 \cdot 3!} = \frac{120}{2 \cdot 6} = 10$$

Tétel

k_1 darab első típusú, k_2 második típusú, … k_m m -edik típusú elem lehetséges sorrendjét az elemek **ismétléses permutációjának** nevezzük és számuk:

$$\frac{(k_1+k_2+\cdots+k_m)!}{k_1!k_2!\cdots k_m!}$$

Bizonyítás

Ha minden elem között különbséget teszünk: $(k_1 + k_2 + \cdots + k_m)!$ lehetséges sorrend létezik.

Ha az i -edik típusú elemek között nem teszünk különbséget, akkor az előbb megkapott lehetséges sorrendek között $k_i!$ egyforma van.

Ha az azonos típusú elemek között nem teszünk különbséget, akkor az előbb megkapott lehetséges sorrendek között $k_1!k_2!\cdots k_m!$ egyforma van. Igy ekkor a lehetséges sorrendek száma:

$$\frac{(k_1+k_2+\cdots+k_m)!}{k_1!k_2!\cdots k_m!}$$

Példa

Az egyetemen 10 tárgyunk van, ezek közül 3-at szeretnénk hétfőre tenni. Hányféleképpen tehetjük ezt?

Megoldás

Hétfőn az első óránk 10-féle lehet. A második 9-féle, a harmadik 8-féle lehet. Igy összesen $10 \cdot 9 \cdot 8$ féleképpen tehetjük meg.

Tétel

Adott egy n elemű A halmaz. Ekkor k elemet

$$n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$
-féleképpen választhatjuk ki.

Bizonyítás

Az A halmazból először n -féleképpen választhatunk, második esetben $(n-1), \dots, k$ -adik esetben $n-k+1$ -féleképpen választhatunk.

Példa

A 0, 1, 2 számjegyből hány legfeljebb 2 jegyű szám képezhető?

Megoldás

Az első helyi értékre 3-féleképpen írhatunk számjegyet:

- 0
- 1
- 2

A második helyi értékre szintén 3-féleképpen írhatunk számjegyet:

- | | | |
|----|----|----|
| 00 | 10 | 20 |
| 01 | 11 | 21 |
| 02 | 12 | 22 |

Összesen

$$\begin{array}{ccc} - & - \\ 3 & \cdot 3 & = 9 \end{array}$$

Tétel

Egy n elemű A halmaz elemeiből n^k darab k hosszú sorozat készíthető.

Bizonyítás

A sorozat első elemét n -féleképpen választhatjuk, a második elemét n -féleképpen választhatjuk, ... k -adik elemét is n -féleképpen választhatjuk ki.

Példa

Egy totószelvényt ($13 + 1$ helyre, 1, 2, vagy x kerülhet)

$3^{14} = 4782969$ -féleképpen lehet kitölteni.

Mennyi egy n elemű halmaz összes részhalmazának száma?

Legyen $A = \{a_1, a_2 \dots a_n\}$. Ekkor minden részhalmaz megfelel egy $0 - 1$ n hosszú sorozatnak: ha a sorozat i -edik eleme 1, akkor a_i benne van a részhalmazban.

$\emptyset \leftrightarrow (0, 0, \dots 0), \{a_1, a_3\} \leftrightarrow (1, 0, 1, 0 \dots 0), \dots, A \leftrightarrow (1, 1, \dots 1)$

Tétel

Egy n elemű A halmaznak a k elemű részhalmazainak száma

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Bizonyítás

Először válasszunk A elemei közül k darabot a sorrendet figyelembe véve. Ezt $n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}$ -féleképpen lehetjük meg. Ha a sorrendtől eltekintünk, akkor az előző számolásnál minden k elemű részhalmaz pontosan $k!$ -szor szerepel. Ezzel leosztva kapjuk a k elemű részhalmazok számát.

Példa

Egy lottószelvényt (90 számból 5) lehetséges kitöltéseinek száma:

$$\binom{90}{5} = \frac{90!}{5!85!} = \frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 43949268$$

Tétel

Egy n elemű A halmaz eleméből, ha k -szor választunk úgy, hogy egy elemet többször is választhatunk, akkor a lehetséges választások száma

$$\binom{n+k-1}{k}$$

Bizonyítás

Legyen $A = \{a_1, a_2 \dots a_n\}$. Ekkor minden egyes lehetőségnak megfeleltetünk egy $0 - 1$ sorozatot:

$$\underbrace{1, 1 \dots 1}_{a_1\text{-ek száma}}, 0, \underbrace{1, 1, \dots 1}_{a_2\text{-ek száma}}, 0, \dots, 0, \underbrace{1, 1 \dots 1}_{a_n\text{-ek száma}}$$

Ekkor a sorozatban k darab 1 -es van (választott elemek száma), $n-1$ darab 0 van (szeparátorok száma). Összesen $n-1+k$ pozíció, ezekből k -at választunk. Ilyen sorozat $\binom{n+k-1}{k}$ darab van.

Példa

5-féle sütemény van a cukrászdában, 8 darabot szeretnénk vásárolni. Hányféleképpen tehetjük ezt meg?

Itt $n = 5, k = 8$:

$$\binom{5+8-1}{8} = \binom{12}{8} = \frac{12!}{8! \cdot 4!} = 495$$

Hányféleképpen dobhatunk 5 dobókockával?

Az $\{1, 2, 3, 4, 5, 6\}$ halmazból 5-ször választunk (sorrend nem számít, egy elemet többször is választhatunk).

Ismétléses kombináció $n = 6, k = 5$ választással:

$$\binom{6+5-1}{5} = \binom{10}{5} = \frac{10!}{5! \cdot 5!} = 252$$

Ismétlés nélküli permutáció $n!$, n elem lehetséges sorrendje (sorrend számít, egy elem (pontosan) egyszer).

Ismétléses permutáció $\frac{(k_1+k_2+\dots+k_m)!}{k_1!k_2!\dots k_m!}$, $n = k_1 + k_2 + \dots + k_m$ elem lehetséges sorrendje, ahol az i típusú elemet k_i -szer választjuk (sorrend számít, egy elem többször).

Ismétlés nélküli variáció $\frac{n!}{(n-k)!}$, n elemből k -at választunk (sorrend számít, egy elem legfeljebb egyszer)

Ismétléses variáció n^k , n elemből k -szor választunk (sorrend számít, egy elem többször is)

Ismétlés nélküli kombináció $\binom{n}{k}$, n elemből k -at választunk (sorrend nem számít egy elem legfeljebb egyszer)

Ismétléses kombináció $\binom{n+k-1}{k}$, n elemből k -szor választunk (sorrend nem számít, egy elem többször is)

Binomiális téTEL

TéTEL

Adott x, y és $n \in \mathbb{N}$ esetén $(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$.

Bizonyítás

$$(x + y)^n = (x + y)(x + y) \cdots (x + y)$$

Ha elvégezzük a beszorzást, akkor $x^k y^{n-k}$ alakú tagokat kapunk és ezen tagot annyiszor kapjuk meg, ahányszor az n tényezőből k darab x -et választunk.

Definíció

A $\binom{n}{k}$ alakú számokat ($n, k \in \mathbb{N}$) **binomiális együtthatónak** nevezzük.

Binomiális együttható

Tétel

$$\textcircled{1} \quad \binom{n}{k} = \binom{n}{n-k}$$

$$\textcircled{2} \quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Bizonyítás

$\binom{n}{k}$ azon n hosszú $0 - 1$ sorozatok száma, melyekben k darab 1 -es van,

$\textcircled{1}$ Az n hosszú $0 - 1$ sorozatok közül azok száma, mely k darab 1 -est tartalmaz megegyezik azok számával, melyek $n - k$ darab 1 -est tartalmaz.

$\textcircled{2}$ Azon n hosszú $0 - 1$ sorozatok száma, melynek első tagja $1: \binom{n-1}{k-1}$.

Azon n hosszú $0 - 1$ sorozatok száma, melynek első tagja $0: \binom{n-1}{k}$.

Binomiális együttható

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}; \quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Pascal-háromszög:

n	$\binom{n}{k}$	$(x + y)^n$
0	1	1
1	1 1	$x + y$
2	1 2 1	$x^2 + 2xy + y^2$
3	1 3 3 1	$x^3 + 3x^2y + 3xy^2 + y^3$
4	1 4 6 4 1	$x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$
5	1 5 10 10 5 1	$x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$

Polinomiális téTEL

Példa

Mennyi lesz

$$(x + y + z)^2 = x^2 + y^2 + z^2 + 2xy + 2xz + 2yz. \quad (x + y + z)^3 = \dots$$

TéTEL

$r, n \in \mathbb{N}$ esetén

$$(x_1 + x_2 + \dots + x_r)^n = \sum_{i_1+i_2+\dots+i_r=n} \frac{n!}{i_1!i_2!\dots i_r!} x_1^{i_1} x_2^{i_2} \dots x_r^{i_r}$$

Bizonyítás

$$\begin{aligned} & (x_1 + x_2 + \dots + x_r)^n = \\ & = (x_1 + x_2 + \dots + x_r)(x_1 + x_2 + \dots + x_r) \cdots (x_1 + x_2 + \dots + x_r) \end{aligned}$$

Az $x_1^{i_1} x_2^{i_2} \dots x_r^{i_r}$ együtthatója:

$$\begin{aligned} & \binom{n}{i_1} \binom{n-i_1}{i_2} \binom{n-i_1-i_2}{i_3} \cdots \binom{n-i_1-i_2-\dots-i_{r-1}}{i_r} = \\ & \frac{n!}{i_1!(n-i_1)!} \frac{(n-i_1)!}{i_2!(n-i_2)!} \cdots \frac{(n-i_1-i_2-\dots-i_{r-1})!}{i_r!(n-i_1-i_2-\dots-i_{r-1}-i_r)!} = \frac{n!}{i_1!i_2!\dots i_r!} \end{aligned}$$

Polinomiális téTEL

$$(x_1 + x_2 + \cdots + x_r)^n = \sum_{i_1+i_2+\cdots+i_r=n} \frac{n!}{i_1!i_2!\cdots i_r!} x_1^{i_1} x_2^{i_2} \cdots x_r^{i_r}$$

$$(x + y + z)^3 = \dots$$

i_1	i_2	i_3	$\frac{3!}{i_1!i_2!i_3!}$	$(x + y + z)^3 =$
3	0	0	$\frac{3!}{3!0!0!} = 1$	x^3
2	1	0	$\frac{3!}{2!1!0!} = 3$	$+3x^2y$
2	0	1	$\frac{3!}{2!0!1!} = 3$	$+3x^2z$
1	2	0	$\frac{3!}{1!2!0!} = 3$	$+3xy^2$
1	1	1	$\frac{3!}{1!1!1!} = 6$	$+6xyz$
1	0	2	$\frac{3!}{1!0!2!} = 3$	$+3xz^2$
0	3	0	$\frac{3!}{0!3!0!} = 1$	$+y^3$
0	2	1	$\frac{3!}{0!2!1!} = 3$	$+3y^2z$
0	1	2	$\frac{3!}{0!1!2!} = 3$	$+3yz^2$
0	0	3	$\frac{3!}{0!0!3!} = 1$	$+z^3$

Skatulya-elv

Ha n darab gyufásdobozunk és $n + 1$ gyufaszálunk van, akkor akárhogyan rakjuk bele az összes gyufát a skatulyába, valamelyikben legalább kettő gyufa lesz.

Példa

Nyolc ember közül van legalább kettő, aki a hét ugyanazon napján született.

Az $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ halmazból bárhogyan választunk ki ötöt, akkor lesz közülük kettő, amelyek összege 9.

Tekintsük az $\{1, 8\}, \{2, 7\}, \{3, 6\}, \{4, 5\}$ halmazokat. Ekkor a kiválasztott öt elem közül lesz kettő, amelynek azonos halmazban lesznek, így összegük 9.

Hány olyan 1000-nél kisebb szám van, amely nem osztható 2-vel, 3-mal és 5-tel?

Az 1000-nél kisebb számok

	összes	999	999
2-vel osztható	$\lfloor \frac{999}{2} \rfloor = 499$	-499	
3-mal osztható	$\lfloor \frac{999}{3} \rfloor = 333$	-333	
5-tel osztható	$\lfloor \frac{999}{5} \rfloor = 199$	-199	
$2 \cdot 3$ -mal osztható	$\lfloor \frac{999}{2 \cdot 3} \rfloor = 166$	166	
$2 \cdot 5$ -nal osztható	$\lfloor \frac{999}{2 \cdot 5} \rfloor = 99$	99	
$3 \cdot 5$ -tel osztható	$\lfloor \frac{999}{3 \cdot 5} \rfloor = 66$	66	
$2 \cdot 3 \cdot 5$ -tel osztható	$\lfloor \frac{999}{2 \cdot 3 \cdot 5} \rfloor = 33$	-33	
			=266

Tétel

Legyenek $A_1, A_2 \dots A_n$ véges halmazok. Ekkor

$$|\cup_{i=1}^n A_i| = \sum_{i=1}^n |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| \mp \dots$$

Példa

Hány olyan 1000-nél kisebb szám van, amely nem osztható 2-vel, 3-mal és 5-tel?

Először: Hány olyan 1000-nél kisebb szám van, amely osztható 2-vel vagy 3-mal vagy 5-tel?

$$A_1 = \{1 \leq n < 999 : n = 0 \pmod 2\} \rightarrow |A_1| = \left\lfloor \frac{999}{2} \right\rfloor$$

$$A_2 = \{1 \leq n < 999 : n = 0 \pmod 3\} \rightarrow |A_2| = \left\lfloor \frac{999}{3} \right\rfloor$$

$$A_3 = \{1 \leq n < 999 : n = 0 \pmod 5\} \rightarrow |A_3| = \left\lfloor \frac{999}{5} \right\rfloor$$

$$\text{Hasonlóan } |A_1 \cap A_2| = \left\lfloor \frac{999}{2 \cdot 3} \right\rfloor, |A_1 \cap A_3| = \left\lfloor \frac{999}{2 \cdot 5} \right\rfloor, |A_2 \cap A_3| = \left\lfloor \frac{999}{3 \cdot 5} \right\rfloor,$$

$$|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{999}{2 \cdot 3 \cdot 5} \right\rfloor$$

2-vel vagy 3-mal vagy 5-tel osztható számok száma:

$$\left\lfloor \frac{999}{2} \right\rfloor + \left\lfloor \frac{999}{3} \right\rfloor + \left\lfloor \frac{999}{5} \right\rfloor - \left\lfloor \frac{999}{2 \cdot 3} \right\rfloor - \left\lfloor \frac{999}{2 \cdot 5} \right\rfloor - \left\lfloor \frac{999}{3 \cdot 5} \right\rfloor + \left\lfloor \frac{999}{2 \cdot 3 \cdot 5} \right\rfloor$$

Tétel

Legyenek A_1, \dots, A_n az A véges halmaz részhalmazai, $f : A \rightarrow \mathbb{R}$ tetszőleges függvény. Legyenek

$$S = \sum_{x \in A} f(x)$$

$$S_r = \sum_{0 \leq i_1 < i_2 < \dots < i_r \leq k} \sum_{x \in A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_r}} f(x)$$

$$S_0 = \sum_{x \in A \setminus \bigcup_{i=1}^n A_i} f(x)$$

$$\text{Ekkor } S_0 = S - S_1 + S_2 - S_3 \pm \dots (-1)^k S_k$$

Példa

$$A = \{1, 2, \dots, 999\}, A_1 = \{n : 1 \leq n < 1000, 2|n\},$$

$$A_2 = \{n : 1 \leq n < 1000, 3|n\} \quad A_3 = \{n : 1 \leq n < 1000, 5|n\}$$

$$f(x) = 1.$$

S_0 : 2-vel, 3-mal, 5-tel nem osztható 1000-nél kisebb számok száma.

Általános szita formula bizonyítása

$$S_0 = S - S_1 + S_2 - S_3 \pm \dots (-1)^k S_k :$$

$$S_0 = \sum_{x \in A \setminus \bigcup_{i=1}^n A_i} f(x), \quad S = \sum_{x \in A} f(x)$$

$$S_r = \sum_{0 \leq i_1 < i_2 < \dots < i_r \leq k} \sum_{x \in A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_r}} f(x)$$

Bizonyítás

Ha $x \in A \setminus \bigcup_{i=1}^n A_i$, akkor $f(x)$ minden oldalon egyszer szerepel.

Ha $\bigcup_{i=1}^n A_i$, legyenek $A_{j_1} \dots A_{j_t}$ azon részhalmazok, melyeknek x eleme. Ekkor $f(x)$ a bal oldalon nem szerepel. Jobb oldalon a

$$\sum_{0 \leq i_1 < i_2 < \dots < i_r \leq k} \sum_{x \in A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_r}} f(x)$$

összegben szerepel, ha $\{i_1, \dots, i_r\} \subset \{j_1 \dots j_t\}$. Ilyen r elemű indexhalmaz $\binom{t}{r}$ darab van. Igy $f(x)$ együtthatója

$$\sum_{r=0}^t \binom{t}{r} (-1)^r = 0$$
 (Biz. gyakorlaton)

Oszthatóság

Ha a és b racionális számok, akkor az $\frac{a}{b}$ osztás mindenkor végezhető (és az eredmény szintén racionális).

Ha a és b egész számok, az $\frac{a}{b}$ osztás nem mindenkor végezhető el (a hányados nem feltétlenül lesz egész.)

Definíció

Az a egész osztja a b egészet: $a|b$, ha létezik olyan c egész, amellyel $a \cdot c = b$ (azaz $a \neq 0$ esetén $\frac{b}{a}$ szintén egész.)

Példák

- $1|13$, mert $1 \cdot 13 = 13$;
- $1|n$, mert $1 \cdot n = n$;
- $6|12$, mert $6 \cdot 2 = 12$;
- $-6|12$, mert $(-6)(-2) = 12$;

Gauss-egészek: $\{a + bi : a, b \in \mathbb{Z}\}$

Példák

- $i|13$, mert $i \cdot (-13i) = 13$;
- $1+i|2$, mert $(1+i)(1-i) = 2$.

Oszthatóság tulajdonságai

Állítás(HF)

Minden $a, b, c, \dots, \in \mathbb{Z}$ esetén

- ① $a|a$
- ② $a|b$ és $b|c \Rightarrow a|c$;
- ③ $a|b$ és $b|a \Rightarrow a = \pm b$;
- ④ $a|b$ és $a'|b' \Rightarrow aa'|bb'$;
- ⑤ $a|b \Rightarrow ac|bc$
- ⑥ $ac|bc$ és $c \neq 0 \Rightarrow a|b$;
- ⑦ $a|b_1 \dots b_k \Rightarrow a|c_1 b_1 + \dots + c_k b_k$;
- ⑧ $a|0$ ui. $a \cdot 0 = 0$;
- ⑨ $0|a \Leftrightarrow a = 0$;
- ⑩ $1|a$ és $-1|a$;

Példák

- ① $6|6$;
- ② $2|6$ és $6|12 \Rightarrow 2|12$
- ③ $2|4$ és $3|9 \Rightarrow 2 \cdot 3|4 \cdot 9$;
- ④ $3|6 \Rightarrow 5 \cdot 3|5 \cdot 6$;
- ⑤ $3 \cdot 5|6 \cdot 5$ és $5 \neq 0 \Rightarrow 3|6$;
- ⑥ $3|6, 9 \Rightarrow 3|6c_1 + 9c_2$

Egyések

A ± 1 oszthatóság szempontjából nem különbözteti meg az egész számokat

Definíció

Ha egy ε szám bármely másiknak osztója, akkor ε -t **egységnak** nevezzük.

Állítás

Az egész számok körében két egység van $1, -1$.

Bizonyítás

Az ± 1 nyilván egység. Megfordítva, ha ε egység, akkor $1 = \varepsilon \cdot q$ valamely q egész számra. Mivel $|\varepsilon| \geq 1, |q| \geq 1 \Rightarrow |\varepsilon| = 1$ azaz $\varepsilon = \pm 1$.

Példa A Gauss-egészek körében az i is egység: $a + bi = i(b - ai)$.

Oszthatóság szempontjából nincs különbség a 12 ill. -12 között.

Definíció

Két szám asszociált, ha egymás egységszeresei.

Megjegyzés(HF)

a és b pontosan akkor asszociált, ha $a|b$ és $b|a$.

Definíció

Egy számnak az asszociáltjai és az egységek a triviális osztói.

Definíció

Ha egy nem-nulla számnak a triviális osztóin kívül nincs más osztója, akkor **felbonthatatlannak (irreducibilisnek)** nevezzük.

Példa: 2,-2,3,-3,5,-5 felbonthatatlanok. 6 nem felbonthatatlan, mert $6 = 2 \cdot 3$.

Definíció

Egy nem nulla, nem egység p számot **prímszámnak** nevezzük, ha $p|ab \Rightarrow p|a$ vagy $p|b$.

Példa: 2,-2,3,-3,5,-5 6 nem prímszám, mert $6|2 \cdot 3$ de $6 \nmid 2$ és $6 \nmid 3$.

Állítás

Minden prímszám felbonthatatlan.

Bizonyítás

Legyen p prímszám és legyen $p = ab$ egy felbontás. Igazolnunk kell, hogy a vagy b egység.

Mivel $p = ab$, így $p \mid ab$, ahonnan például $p \mid a$. Ekkor $a = pk = a(bk)$, azaz $bk = 1$, ahonnan következik, hogy b és k is egység.

A fordított irány nem feltétlenül igaz:

- \mathbb{Z} -ben igaz, (lásd később);
- $\{a + bi\sqrt{5} : a, b \in \mathbb{Z}\}$ -ben nem igaz.

Maradékos osztás

A számelméletben a fő eszközünk a maradékos osztás lesz:

Tétel

Tetszőleges $a, b \neq 0$ egész számokhoz egyértelműen léteznek q, r egészek, hogy

$$a = bq + r \text{ és } 0 \leq r < |b|.$$

Bizonyítás

A tételt csak nemnegatív számok esetében bizonyítjuk.

① Létezés: a szerinti indukcióval.

- Ha $a < b$, akkor $a = b \cdot 0 + a$ ($q = 0, r = a$).
- Ha $a \geq b$, akkor tegyük fel, hogy a -nál kisebb számok már felírhatók ilyen alakban. Legyen $a - b = bq^* + r^*$. Ekkor $a = b(q^* + 1) + r^*$ és legyen $q = q^* + 1, r = r^*$.

② Egyérteműség: legyen $a = bq + r = bq^* + r^*$. Ekkor $b(q - q^*) = r^* - r$. Ez csak akkor lehet, ha $q = q^*$ és $r = r^*$.



Definíció

Legyenek a, b egész számok ($b \neq 0$). Legyen $a = b \cdot q + r$ ($0 \leq r < |b|$). Ekkor $a \bmod b = r$.

Megjegyzés:

$q = \lfloor \frac{a}{b} \rfloor$, ha $b > 0$, és $q = \lceil \frac{a}{b} \rceil$, ha $b < 0$.

Példa

- $123 \bmod 10 = 3$, $123 \bmod 100 = 23$,
 $123 \bmod 1000 = 123$;
- $123 \bmod -10 = 3, \dots$
- $-123 \bmod 10 = 7$, $-123 \bmod 100 = 77$,
 $-123 \bmod 1000 = 877$;
- $-123 \bmod -10 = 7, \dots$

Maradékos osztás

Példa

- ① Ha most 9 óra van, hány óra lesz 123 óra múlva?

Osszuk el maradékosan 123-at 24-gyel: $123 = 24 \cdot 5 + 3$.

Tehát $9 + 3 = 12$: déli 12 óra lesz!

- ② Ha most 9 óra van, hány óra lesz 104 óra múlva? Osszuk el maradékosan 104-et 24-gyel: $104 = 24 \cdot 4 + 20$

Tehát $9 + 20 = 29$. Újabb redukció: $29 = 24 \cdot 1 + 5$. hajnali 5 óra lesz!

- ③ Milyen napra fog esni jövőre szeptember 16-a? Milyen napra esett két éve jövőre szeptember 20-a?

hétfő → 0 Osszuk el maradékosan 365-öt 7-tel:

kedd → 1 $365 = 7 \cdot 22 + 1$.

szerda → 2 hétfő+1 nap = 0+1=1=kedd

csütörtök → 3 Osszuk el maradékosan $-(365 + 366)$ -öt (2012 szökőév)

péntek → 4

szombat → 5 7-tel: $-731 = 7 \cdot (104) + 4$

vasárnap → 6 péntek +3nap = 4 + 3 = 7 $\stackrel{\text{redukció}}{=} 0 =$ hétfő

Számrendszerök

10-es számrendszerben a 123 :

$$123 = 100 + 20 + 3 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0.$$

2-es számrendszerben a 123 :

$$\begin{aligned}1111011_{(2)} &= 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0_{(10)} \\&= 1 \cdot 64 + 1 \cdot 32 + 1 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1_{(10)}\end{aligned}$$

Tétel

Legyen $q > 1$ rögzített egész. Ekkor bármely n pozitív egész egyértelműen felírható $n = \sum_{i=0}^k a_i q^i$ alakban, ahol $0 \leq a_i < q$ egészek, $a_k \neq 0$

- Ez a felírás n q számrendszerben történő felírása
- q a számrendszer alapja
- a_0, \dots, a_k az n jegyei
- $k = \lceil \log_q n \rceil$

n felírása a q alapú számrendszerben: $n = \sum_{i=0}^k a_i q^i$.

Bizonyítás

A témát indukcióval bizonyítjuk.

- ① $n = 0$ esetén a téTEL igaz.
- ② Tegyük fel, hogy minden n -nél kisebb számot fel tudjuk írni egyértelműen q alapú számrendszerben. A maradékos osztás tétele alapján létezik egyértelműen $0 \leq a_0 < q$ egész, hogy $q|n - a_0$. Indukció alapján írjuk fel q alapú számrendszerben $\frac{n-a_0}{q} = \sum_{i=1}^k a_i q^{i-1}$, indukció alapján a felírás egyértelmű.
Ekkor $n = \sum_{i=0}^k a_i q^i$.

Számrendszerlek

Az előbbi bizonyítás módszert is ad a felírásra:

Példa

Irjuk fel az $n = 123$ 10-es számrendszerben felírt számot 2-es számrendszerben.

i	n	$n \bmod 2$	$\frac{n-a_i}{2}$	jegyek
0	123	1	$\frac{123-1}{2}$	1
1	61	1	$\frac{61-1}{2}$	11
2	30	0	$\frac{30-0}{2}$	011
3	15	1	$\frac{15-1}{2}$	1011
4	7	1	$\frac{7-1}{2}$	11011
5	3	1	$\frac{3-1}{2}$	111011
6	1	1	$\frac{1-1}{2}$	1111011

Legnagyobb közös osztó

Definíció

Az a és b számoknak a d szám **kitüntetett közös osztója** (legnagyobb közös osztója), ha: $d|a, d|b$ és $c|a, c|b \Rightarrow c|d$.

Figyelem! Itt a "legnagyobb" nem a szokásos rendezésre utal:
12-nek és 9-nek legnagyobb közös osztója lesz a -3 is.

A legnagyobb közös osztó csak asszociáltság erejéig egyértelmű.

Definíció

Legyen $(a, b) = \text{lnko}(a, b)$ a **nem-negatív** kitüntetett közös osztó!

Definíció

Az a és b számoknak az m szám **kitüntetett közös többszöröse** (legkisebb közös többszöröse), ha: $a|m, b|m$ és $a|c, b|c \Rightarrow m|c$.

Legyen $[a, b] = \text{lkkt}(a, b)$ a **nem-negatív** kitüntetett közös többszörös!

Tétel

Bármely két egész számnak létezik legnagyobb közös osztója, és ez meghatározható az euklideszi algoritmussal.

Bizonyítás

Ha valamelyik szám 0, akkor a legnagyobb közös osztó a másik szám. Tegyük fel, hogy a, b nem-nulla számok. Végezzük el a következő osztásokat:

$$a = bq_1 + r_1, \quad 0 < r_1 < |b|,$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2,$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_nq_{n+1}$$

Ekkor a lnko utolsó nem-nulla maradék: $(a, b) = r_n$.

Euklideszi algoritmus helyessége

Bizonyítás folyt.

$$a = bq_1 + r_1, \quad 0 < r_1 < |b|,$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2,$$

⋮

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_nq_{n+1}$$

Az algoritmus véges sok lépésben véget ér: $|b| > r_1 > r_2 > \dots$

Az r_n maradék közös osztó:

$$r_n|r_{n-1} \Rightarrow r_n|r_{n-1}q_n + r_n = r_{n-2} \Rightarrow \dots \Rightarrow r_n|b \Rightarrow r_n|a.$$

Az r_n maradék a legnagyobb közös osztó: legyen $c|a, c|b \Rightarrow c|a - bq_1 = r_1 \Rightarrow c|b - r_1q_2 = r_2 \Rightarrow \dots \Rightarrow c|r_{n-2} - r_{n-1}q_n = r_n.$

A legnagyobb közös osztó kiszámolása euklideszi algoritmussal

Példa

Számítsuk ki $(172, 62)$ értékét!

i	r_i	q_i	$r_{i-2} = r_{i-1}q_i + r_i$
-	172	-	-
-	62	-	-
1	48	2	$172 = 62 \cdot 2 + 48$
2	14	1	$62 = 48 \cdot 1 + 14$
3	6	3	$48 = 14 \cdot 3 + 6$
4	2	2	$14 = 6 \cdot 2 + 2$
5	0	3	$6 = 2 \cdot 3 + 0$

A legnagyobb közös osztó: $(172, 62) = 2$

Legnagyobb közös osztó kiszámolása rekurzióval

Tétel

Legyen $a \neq 0$. Ha $b = 0$, akkor $(a, b) = a$. Ha $b \neq 0$, akkor $(a, b) = (|b|, a \bmod |b|)$.

Bizonyítás

Ha $b = 0$, akkor a tételek nyilvánvaló.

Ha $b \neq 0$ osszuk el maradékosan a -t $|b|$ -vel:

$$a = |b| \cdot q + (a \bmod |b|).$$

Ez az euklideszi algoritmus első sora.

Példa Számítsuk ki $(172, 62)$ értékét!

(a, b)	$a \bmod b $
$(172, 62)$	48
$(62, 48)$	14
$(48, 14)$	6
$(14, 6)$	2
$(6, 2)$	0

A legnagyobb közös osztó: $(172, 62) = 2$.

Legnagyobb közös osztó, további észrevételek

Hasonló módon definiálható több szám legnagyobb közös osztója is (HF): (a_1, a_2, \dots, a_n)

Állítás(HF)

Bármely a_1, a_2, \dots, a_n egész számokra létezik (a_1, a_2, \dots, a_n) és $(a_1, a_2, \dots, a_n) = ((\dots(a_1, a_2), \dots, a_{n-1}), a_n)$.

Állítás(HF)

Bármely a, b, c egész számokra $(ca, cb) = c(a, b)$.

Bővített euklideszi algoritmus

Tétel

Minden a, b egész számok esetén léteznek x, y egészek, hogy $(a, b) = x \cdot a + y \cdot b$.

Bizonyítás

Legyenek q_i, r_i az euklideszi algoritmussal megkapott hányadosok, maradékok.

Legyen $x_{-1} = 1, x_0 = 0$ és $i \geq 1$ esetén legyen $x_i = x_{i-2} - q_i x_{i-1}$.

Hasonlóan legyen $y_{-1} = 0, y_0 = 1$ és $i \geq 1$ esetén legyen

$y_i = y_{i-2} - q_i y_{i-1}$.

Ekkor $i \geq 1$ esetén $x_i a + y_i b = r_i$ (Biz.:HF, indukcióval)

Speciálisan $x_n a + y_n b = r_n = (a, b)$.

Bővített euklideszi algoritmus

$$r_{i-2} = r_{i-1}q_i + r_i,$$

Algoritmus: $x_{-1} = 1, x_0 = 0, x_i = x_{i-2} - q_i x_{i-1}$
 $y_{-1} = 0, y_0 = -1, y_i = y_{i-2} - q_i y_{i-1}$

Példa

Számítsuk ki $(172, 62)$ értékét és oldjuk meg az
 $172x + 62y = (172, 62)$ egyenlet!

i	r_n	q_n	x_i	y_i	$r_i = 172x_i + 62y_i$
-1	172	-	1	0	$172 = 172 \cdot 1 + 62 \cdot 0$
0	62	-	0	1	$62 = 172 \cdot 0 + 62 \cdot 1$
1	48	2	1	-2	$48 = 172 \cdot 1 + 62 \cdot (-2)$
2	14	1	-1	3	$14 = 172 \cdot (-1) + 62 \cdot 3$
3	6	3	4	-11	$6 = 172 \cdot 4 + 62 \cdot (-11)$
4	2	2	-9	25	$2 = 172 \cdot (-9) + 62 \cdot 25$
5	0	3	-	-	-

A felírás: $2 = 172 \cdot (-9) + 62 \cdot 25, x = -9, y = 25.$

Felbonthatatlanok és prímek

Emlékeztető: t felbonthatatlan: csak triviális osztói vannak:

$\varepsilon, t, \varepsilon \cdot t$ típusú osztók (ahol ε egy egység)

p prím: $p|ab \Rightarrow p|a$ vagy $p|b$.

p prím $\Rightarrow p$ felbonthatatlan.

Az egész számok körében a fordított irány is igaz:

Tétel

Minden felbonthatatlan szám prímszám.

Bizonyítás

Legyen p felbonthatatlan és legyen $p|ab$. Tegyük fel, hogy $p \nmid b$.

Ekkor p és b relatív prímek. A bővített euklideszi algoritmussal kaphatunk x, y egészeket, hogy $px + by = 1$. Innen $pax + aby = a$. Mivel p osztója a baloldalnak, így osztója a jobb oldalnak is: $p|a$.

Számelmélet alaptétele

Tétel

Minden nem-nulla, nem egység egész szám sorrendtől és asszociáltaktól eltekintve egyértelműen felírható prímszámok szorzataként.

Bizonyítás

Csak nemnegatív számokra.

Létezés: indukcióval: $n = 2, n = 3$ esetén igaz (prímek). Általában, ha n prím, akkor készen vagyunk, ha nem akkor szorzatra bomlik nem triviális módon. A tényezők már felbonthatók indukció alapján.

Egyértelműség: Indukcióval: $n = 2, n = 3$ esetén igaz (prímek).

Tegyük fel, hogy $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, ahol $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ prímek. p_1 osztja a bal oldalt \Rightarrow osztja a jobb oldalt is, feltehető $p_1 = q_1$.

Egyszerűsítve: $n' = p_2 \cdots p_k = q_2 \cdots q_l$. Indukció alapján ez már egyértelmű.



Definíció

Egy n nem nulla egész szám kanonikus alakja:

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_I^{\alpha_I} = \pm \prod_{i=1}^I p_i^{\alpha_i},$$

ahol p_1, p_2, \dots, p_I pozitív prímek, $\alpha_1, \alpha_2, \dots, \alpha_I$ pozitív egészek.

Következmény(HF)

Legyenek $n, m > 1$ pozitív egészek: $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_I^{\alpha_I}$,

$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_I^{\beta_I}$, (ahol most $\alpha_i, \beta_i \geq 0$ nemnegatív egészek!).

Ekkor $(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_I^{\min\{\alpha_I, \beta_I\}}$

$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_I^{\max\{\alpha_I, \beta_I\}}$

$(a, b) \cdot [a, b] = a \cdot b$.

Osztók száma

Definíció

Egy $n > 1$ egész esetén legyen $\tau(n)$ az n pozitív osztóinak száma:

Példa

$\tau(6) = 4$: osztók: 1, 2, 3, 6, $\tau(96) = 12$: osztók:
1, 2, 3, 4, 6, 8 ...

Tétel

Legyen $n > 1$ egész, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_I^{\alpha_I}$ kanonikus alakkal. Ekkor $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_I + 1)$.

Bizonyítás

n lehetséges osztóit úgy kapjuk, hogy a $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_I^{\beta_I}$ kifejezésben az összes β_i kitevő végigfut a $\{0, 1, \dots, \alpha_i\}$ halmazon. Igy ez a kitevő $\alpha_i + 1$ féleképpen választható.

Példa: $\tau(2 \cdot 3) = (1 + 1) \cdot (1 + 1)$; $\tau(2^5 \cdot 3) = (5 + 1)(1 + 1)$

Tétel Euklidész

Végtelen sok prím van.

Bizonyítás

Indirekt tegyük fel, hogy csak véges sok prím van. Legyenek ezek p_1, \dots, p_k . Tekintsük az $n = p_1 \cdots p_k + 1$ számot. Ez nem osztható egyetlen p_1, \dots, p_k prímmel sem, így n prímtényezős felbontásában kell szerepelnie egy újabb prímszámnak.

Tétel (Dirichlet)

Ha a, d egész számok, $d > 0$, $(a, b) = 1$, akkor végtelen sok $ak + d$ alakú prím van.

Prímszámítételel: x -ig a prímek száma $\sim \frac{x}{\ln x}$. (Sok prím van!)

Prímek száma:

x	$\frac{x}{\ln x}$	prímek száma
10	4	4, 33
100	25	21, 71
1000	168	144, 76
10000	1229	1085, 73

Erathosztenész szitája: keressük meg egy adott n -ig az összes prímet. Soroljuk fel 2-től n -ig az egész számokat. Ekkor 2 prím. A 2 (valódi) többszörösei nem prímek, ezeket húzzuk ki. A következő szám 3 szintén prím. A 3 (valódi) többszörösei nem prímek, ezeket húzzuk ki... Ismételjük az eljárást \sqrt{n} -ig. A ki nem húzott számok minden prímek.

Kongruenciák

Oszthatósági kérdésekben sokszor csak a maradékos osztás esetén csak a maradék fontos:

- hét napjai;
- órák száma,....

Példa 16 $16 \bmod 3 = 1$; $4 \bmod 3 = 1$: 3-mal való oszthatóság esetén $16'' = "4"$.

Definíció

Legyenek a, b, m egészek, akkor $a \equiv b \pmod{m}$ (a és b kongruensek), ha $m|a - b$, és $a \not\equiv b \pmod{m}$ (a és b inkongruensek), ha $m \nmid a - b$.

Ekvivalens megfogalmazás: $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$ azaz m-mel osztva ugyan azt az osztási maradékot adják.

Példa $16 \equiv 4 \pmod{3}$ ui. $3|16 - 4 \Leftrightarrow 16 \bmod 3 = 1 = 4 \bmod 3$;
 $16 \equiv 4 \pmod{2}$ ui $2|16 - 4 \Leftrightarrow 16 \bmod 2 = 0 = 4 \bmod 2$
 $16 \not\equiv 4 \pmod{5}$ ui $5 \nmid 16 - 4 \Leftrightarrow 16 \bmod 5 = 1 \neq 4 \bmod 5$.



Kongruencia tulajdonságai

Tétel

Minden a, b, c, d és m egész számra igaz

1. $a \equiv a \pmod{m}$;
2. $a \equiv b \pmod{m}; m' | m \Rightarrow a \equiv b \pmod{m'}$;
3. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$;
4. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$;
5. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$;
6. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$.

Bizonyítás

1. $m|0 = a - a$;
2. $m'|m|a - b \Rightarrow m'|a - b$;
3. $m|a - b \Rightarrow m|b - a = -(a - b)$;
4. $m|a - b, m|b - c \Rightarrow m|a - c = (a - b) + (b - c)$;
5. $m|a - b, m|c - d \Rightarrow m|(a + c) - (b + d) = (a - b) + (c - d)$;
6. $a = q_1m + b, c = q_2m + d \Rightarrow$
 $ac = (q_1m + b)(q_2m + d) = m(q_1q_2m + q_1d + q_2b) + bd$

Kongruencia tulajdonságai

6.

$$a = q_1 m + b, c = q_2 m + d \Rightarrow$$

$$ac = (q_1 m + b)(q_2 m + d) = m(q_1 q_2 m + q_1 d + q_2 b) + bd.$$

Példa

Mi lesz $345 \pmod{7} = ?$

$$345 = 34 \cdot 10 + 5 \equiv 6 \cdot 3 + 5 = 18 + 5 \equiv 4 + 5 = 9 \equiv 2 \pmod{7}.$$

Emlékeztető: $a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}$

Következmény: $a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}.$

Példa

$$14 \equiv 6 \pmod{8} \Rightarrow 42 \equiv 18 \pmod{24}$$

A másik irány nem igaz!

$$2 \cdot 7 \equiv 2 \cdot 3 \pmod{8} \not\Rightarrow 7 \equiv 3 \pmod{8}.$$

Kongruencia tulajdonságai

Tétel (NB)

Legyenek a, b, c, m egész számok.

Ekkor $ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{(c,m)}}$

Következmény: $ac \equiv bc \pmod{m}, (c, m) = 1 \Leftrightarrow a \equiv b \pmod{m}$.

Példa

$$2 \cdot 7 \equiv 2 \cdot 3 \pmod{8} \Rightarrow 7 \equiv 3 \pmod{\frac{8}{2}}.$$

Bizonyítás

Legyen $d = (c, m)$. Ekkor $m|c(a - b) \Leftrightarrow \frac{m}{d}|\frac{c}{d}(a - b)$. Mivel $(\frac{m}{d}, \frac{c}{d}) = 1$, ezért $\frac{m}{d}|(a - b) \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$.

Lineáris kongruenciák

Oldjuk meg a $2x \equiv 5 \pmod{7}$ kongruenciát.

Ha x egy megoldás és $x \equiv y \pmod{7}$, akkor y szintén megoldás.
Keressük megoldást a $\{0, 1 \dots 6\}$ halmazból!

$$x = 0 \Rightarrow 2x = 0 \not\equiv 5 \pmod{7};$$

$$x = 1 \Rightarrow 2x = 2 \not\equiv 5 \pmod{7};$$

$$x = 2 \Rightarrow 2x = 4 \not\equiv 5 \pmod{7};$$

$$x = 3 \Rightarrow 2x = 6 \not\equiv 5 \pmod{7};$$

$$x = 4 \Rightarrow 2x = 8 \equiv 1 \not\equiv 5 \pmod{7};$$

$$x = 5 \Rightarrow 2x = 10 \equiv 3 \not\equiv 5 \pmod{7};$$

$$x = 6 \Rightarrow 2x = 12 \equiv 5 \pmod{7};$$

A kongruencia megoldása: $\{6 + 7l : l \in \mathbb{Z}\}$

Van-e jobb módszer?

Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!

Kell-e 211 próbálkozás?

Lineáris kongruenciák

Tétel

Legyenek a, b, m egész számok, $m > 1$. Ekkor az $ax \equiv b \pmod{m}$ megoldható $\Leftrightarrow (a, m)|b$. Ez esetben pontosan (a, m) darab inkongruens megoldás van \pmod{m} .

Bizonyítás

$ax \equiv b \pmod{m} \Leftrightarrow ax + my = b$ valamely y egészre.

Mivel $(a, m)|a, m \Leftrightarrow (a, m)|ax + my = b$.

Ha $d = (a, m)|b$ legyen $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$: $a'x + m'y = b'$.

Mivel $(a', m') = 1$ bővített euklideszi algoritmussal kiszámolható x_0, y_0 együttható, hogy

$a'x_0 + b'y_0 = 1 \Rightarrow a'(b'x_0) + m'(b'y_0) = b'$, azaz

$x_1 = b'x_0, y_1 = b'y_0$ megoldás lesz.

Megoldások száma: legyenek x ill. y megoldások. Az $a'x + m'y = b'$ és $a'x_1 + m'y_1 = b'$ egyenleteket kivonva egymásból kapjuk:

$$a'(x - x_1) = m'(y_1 - y) \Rightarrow m'|x - x_1 \Rightarrow x = x_1 + m'k :$$

Lineáris kongruenciák

- $ax \equiv b \pmod{m} \Leftrightarrow ax + my = b.$
- Oldjuk meg $ax + my = (a, m)$ egyenletet (**Bővített euklideszi algoritmus**).
- Ha $(a, m) | b \Leftrightarrow$ van megoldás.
- Megoldások: $x_1 = \frac{b}{(a, m)}x + k\frac{m}{(a, m)}$: $k = 0, 1, \dots, (a, m) - 1$.

Példa Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!

i	r_n	q_n	x_i
-1	23	-	1
0	211	-	0
1	23	0	1
2	4	9	-9
3	3	5	46
4	1	1	-55
5	0	3	-

Algoritmus:

$$r_{i-2} = r_{i-1}q_i + r_i$$

$$x_{-1} = 1, x_0 = 0,$$

$$x_i = x_{i-2} - q_i x_{i-1}$$

$$\text{Ínko: } (23, 211) = 1 | 4 \Rightarrow$$

$$\begin{aligned} \text{Egy megoldás } x &= 4(-55) \equiv \\ &\equiv 202 \pmod{211}. \end{aligned}$$

Összes megoldás: $\{202 + 211l : l \in \mathbb{Z}\}$.

Ezek a megoldások:

$$23 \cdot (202 + 211l) - 4 = 4642 + 211l = (22 + l) \cdot 211.$$

Lineáris kongruenciák

Példa

Oldjuk meg a $10x \equiv 8 \pmod{22}$ kongruenciát!

Algoritmus:

i	r_n	q_n	x_i
-1	10	-	1
0	22	-	0
1	10	0	1
2	2	2	-2
3	0	5	-

$$r_{i-2} = r_{i-1}q_i + r_i$$

$$x_{-1} = 1, x_0 = 0,$$

$$x_i = x_{i-2} - q_i x_{i-1}$$

$$\text{Ínko: } (10, 22) = 2 | 8 \Rightarrow$$

Egy megoldás pá�:

$$x_1 = 4(-2) \equiv 14 \pmod{22}$$

$$x_2 = 4(-2) + \frac{22}{2} \equiv 14 + 11 \equiv \\ \equiv 3 \pmod{22}.$$

Összes megoldás: $\{14 + 22l : l \in \mathbb{Z}\} \cup \{3 + 22l : l \in \mathbb{Z}\}$.

Ezek megoldások: $x_1 = 14 : 10 \cdot 14 - 8 = 132 = 6 \cdot 22$

$x_2 = 3 : 10 \cdot 3 - 8 = 22 = 1 \cdot 22$.

Lineáris diofantikus egyenletek

Diofantikus egyenletek: egyenletek **egész** megoldásait keressük.

Lineáris diofantikus egyenletek: $ax + by = c$, ahol a, b, c egészek.

Ez ekvivalens az $ax \equiv c \pmod{b}$, $by \equiv c \pmod{a}$ kongruenciákkal.

Az $ax + by = c$ pontosan akkor oldható meg, ha $(a, b)|c$ és ekkor a megoldások megkaphatók a **bővített euklideszi algoritmussal**.

További diofantikus egyenletek:

$x^2 + y^2 = -4$: nincs megoldás.

$x^2 - 4y^2 = 3$: nincs megoldás, ui. 4-gyel való osztási maradékok:

$x^2 \equiv 3 \pmod{4}$. De ez nem lehet, a négyzetszám maradéka 0 vagy 1:

x	$x^2 \pmod{4}$
$4k$	0
$4k+1$	1
$4k+2$	0
$4k+3$	1

Szimultán kongruenciák

Szeretnénk olyan x egészet, mely **egyszerre** elégíti ki a következő kongruenciákat:

$$\left. \begin{array}{l} 2x \equiv 1 \pmod{3} \\ 4x \equiv 3 \pmod{5} \end{array} \right\}$$

A kongruenciákat külön megoldva:

$$\left. \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \end{array} \right\}$$

Látszik, hogy $x = 2$ megoldás lesz!

Vannak-e más megoldások?

- $2, 17, 32, \dots, 2+15i$
- további megoldások?
- hogyan oldjuk meg az általános esetben:

$$\left. \begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{array} \right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruencia rendszert:

$$\left. \begin{array}{rcl} a_1x & \equiv & b_1 \pmod{m_1} \\ a_2x & \equiv & b_2 \pmod{m_2} \\ \vdots & & \\ a_nx & \equiv & b_n \pmod{m_n} \end{array} \right\}$$

Az egyes lineáris kongruenciák $a_i x \equiv b_i \pmod{m_i}$ külön megoldhatóak:

$$\left. \begin{array}{rcl} x & \equiv & c_1 \pmod{m_1} \\ x & \equiv & c_2 \pmod{m_2} \\ \vdots & & \\ x & \equiv & c_n \pmod{m_n} \end{array} \right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruencia rendszert:

$$\left. \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \vdots \\ x \equiv c_n \pmod{m_n} \end{array} \right\}$$

Feltehető, hogy az m_1, m_2, \dots, m_n modulusok relatív prímek. Ha pl. $m_1 = m'_1 d, m_2 = m'_2 d$, akkor az első két sor helyettesíthető (Biz később)

$$\left. \begin{array}{l} x \equiv c_1 \pmod{m'_1} \\ x \equiv c_1 \pmod{d} \\ x \equiv c_2 \pmod{m'_2} \\ x \equiv c_2 \pmod{d} \end{array} \right\}$$

Ha itt $c_1 \neq c_2 \pmod{d}$, akkor nincs megoldás, különben az egyik sor törölhető.

TéTEL

Legyenek $1 < m_1, m_2 \dots m_n$ relatív prím számok, $c_1, c_2, \dots c_n$ egészek. Ekkor a

$$\left. \begin{array}{l} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \vdots \\ x \equiv c_n \pmod{m_n} \end{array} \right\}$$

kongruencia rendszer megoldható és bármely két megoldás kongruens egymással modulo $m_1 \cdot m_2 \cdots m_n$.

$$x \equiv c_1 \pmod{m_1}, x \equiv c_2 \pmod{m_2}, \dots x \equiv c_n \pmod{m_n}. \quad x = ?$$

Bizonyítás

A bizonyítás konstruktív!

Legyen $m = m_1 m_2$. A **bővített euklideszi algoritmussal** oldjuk meg az $m_1 x_1 + m_2 x_2 = 1$ egyenletet. Legyen $c_{1,2} = m_1 x_1 c_2 + m_2 x_2 c_1$. Ekkor $c_{1,2} \equiv c_j \pmod{m_j} (j = 1, 2)$. Ha $x \equiv c_{1,2} \pmod{m}$, akkor x megoldása az első két kongruenciának. Megfordítva: ha x megoldása az első két kongruenciának, akkor $x - c_{1,2}$ osztható m_1 -gyel, m_2 -vel, így a szorzatukkal is: $x \equiv c_{1,2} \pmod{m}$. Az eredeti kongruencia rendszer ekvivalens a

$$\left. \begin{array}{l} x \equiv c_{1,2} \pmod{m_1 m_2} \\ x \equiv c_3 \pmod{m_3} \\ \vdots \\ x \equiv c_n \pmod{m_n} \end{array} \right\}$$

Az n szerinti indukcióval adódik az állítás.

Szimultán kongruenciák

Példa

$$\begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{array} \quad \left. \right\}$$

Oldjuk meg az $3x_1 + 5x_2 = 1$ egyenletet.

Megoldások: $x_1 = -3, x_2 = 2 \Rightarrow$

$$c_{1,2} = 3 \cdot (-3) \cdot 3 + 5 \cdot 2 \cdot 2 = -27 + 20 = -7.$$

Összes megoldás: $\{-7 + 15l : l \in \mathbb{Z}\} = \{8 + 15l : l \in \mathbb{Z}\}.$

Példa

$$\begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{array} \quad \left. \right\} \quad c_{1,2}=8 \Rightarrow \begin{array}{l} x \equiv 8 \pmod{15} \\ x \equiv 4 \pmod{7} \end{array} \quad \left. \right\}$$

Oldjuk meg a $15x_{1,2} + 7x_3 = 1$ egyenletet. Megoldások:

$$x_{1,2} = 1, x_3 = -2 \Rightarrow$$

$$c_{1,2,3} = 15 \cdot 1 \cdot 4 + 7 \cdot (-2) \cdot 8 = 60 - 112 = -52.$$

Összes megoldás: $\{-52 + 105l : l \in \mathbb{Z}\} = \{53 + 105l : l \in \mathbb{Z}\}.$

Sokszor egy adott probléma megoldása nem egy konkrét szám (számok családja), hanem egy egész halmaz (halmazok családja):

- $2x \equiv 5 \pmod{7}$, megoldások: $\{6 + 7l : l \in \mathbb{Z}\}$
- $10x \equiv 8 \pmod{22}$,
megoldások: $\{14 + 22l : l \in \mathbb{Z}\} \cup \{3 + 22l : l \in \mathbb{Z}\}$.

Definíció

Egy rögzített m modulus és a egész esetén, az a -val kongruens elemek halmazát az a által reprezentált **maradékosztálynak** nevezzük: $\bar{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\} = \{a + lm : l \in \mathbb{Z}\}$.

Példa

Az $2x \equiv 5 \pmod{7}$ megoldása: $\bar{6}$.

A $10x \equiv 8 \pmod{22}$ megoldásai: $\bar{14}, \bar{3}$.

$m = 7$ modulussal $\bar{2} = \bar{23} = \{\dots, -5, 2, 9, 16, 23, 30, \dots\}$

Általában: $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}$.

Definíció

Egy rögzített m modulus esetén, ha minden maradékosztályból pontosan egy elemet kiveszünk, akkor az így kapott számok **teljes maradékrendszerét** alkotnak modulo m .

Példa

$\{33, -5, 11, -11, -8\}$ teljes maradékrendszer modulo 5.

Gyakori választás teljes maradékrendszerekre

- Legkisebb nemnegatív maradékok: $\{0, 1, \dots, m-1\}$
- Legkisebb abszolút értékű maradékok:

$\{0, \pm 1, \dots, \pm \frac{m-1}{2}\}$, ha $2 \nmid m$;

$\{0, \pm 1, \dots, \pm \frac{m-2}{2}, \frac{m}{2}\}$, ha $2|m$.

Megjegyzés: ha egy maradékosztály valamely eleme relatív prím a modulushoz, akkor az összes eleme az: $(a + lm, m) = (a, m) = 1$.

Definíció

Egy rögzített m modulus esetén, ha minden maradékosztályból, melyek elemei relatív prímek a modulushoz kiveszünk pontosan egy elemet, akkor az így kapott számok **redukált maradékrendszerét** alkotnak modulo m .

Példa

$\{1, 2, 3, 4\}$ redukált maradékrendszer modulo 5.

$\{-1, 1\}$ redukált maradékrendszer modulo 3.

$\{1, 19, 29, 7\}$ redukált maradékrendszer modulo 8.

$\{0, 1, 2, 3, 4\}$ **nem** redukált maradékrendszer modulo 5.

Maradékosztályok

A maradékosztályok között természetes módon műveleteket definiálhatunk:

Definíció

Rögzített m modulus és a, b egészek esetén legyen:

$$\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a+b}; \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b}$$

Állítás

Ez értelme definíció, azaz, ha $\bar{a} = \overline{a^*}$, $\bar{b} = \overline{b^*}$, akkor
 $\bar{a} + \bar{b} = \overline{a^*} + \overline{b^*}$, illetve $\bar{a} \cdot \bar{b} = \overline{a^*} \cdot \overline{b^*}$

Bizonyítás

Mivel $\bar{a} = \overline{a^*}$, $\bar{b} = \overline{b^*}$, $\Rightarrow a \equiv a^* \pmod{m}$,
 $b \equiv b^* \pmod{m} \Rightarrow a + b = a^* + b^* \pmod{m} \Rightarrow \overline{a+b} = \overline{a^*+b^*}$
 $\Rightarrow \bar{a} + \bar{b} = \overline{a^*} + \overline{b^*}$. Szorzás hasonlóan.

Maradékosztályok

A maradékosztályok között természetes módon műveleteket definiálhatunk: $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

Definíció

Rögzített m modulus, legyen \mathbb{Z}_m a maradékosztályok halmaza.
Ekkor a halmaz elemei között definiálhatunk összeadást, ill. szorzást.

Példa

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

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

$$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

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

.	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

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

Maradékosztályok

Tétel

legyen $m > 1$ egész. Ha $1 \leq (a, m) < m$, akkor \bar{a} nullosztó \mathbb{Z}_m -ben \bar{a} -hoz van olyan \bar{b} , hogy $\bar{a} \cdot \bar{b} = \bar{0}$.

Ha $(a, m) = 1$, akkor \bar{a} -nak van reciproka (multiplikatív inverze) \mathbb{Z}_m -ben: \bar{a} -hoz van olyan \bar{x} , hogy $\bar{a} \cdot \bar{x} = \bar{1}$.

Speciálisan, ha m prím, minden nem-nulla maradékosztállyal lehet osztani.

Példa: Legyen $m = 9$, $\bar{6} \cdot \bar{3} = \bar{18} = \bar{0}$.

$(2, 9) = 1$, így $\bar{2} \cdot \bar{5} = \bar{10} = \bar{1}$.

Bizonyítás

Legyen $d = (a, m)$. Ekkor $a \cdot \frac{m}{d} = \frac{a}{d} \cdot 0 \equiv 0 \pmod{m}$, ahonnan $b = \frac{m}{d}$ jelöléssel $\bar{a} \cdot \bar{b} = \bar{0}$.

Ha $(a, m) = 1$, akkor a bővített euklideszi algoritmussal megadhatóak x, y egészek, hogy $ax + my = 1$.

Ekkor $ax \equiv 1 \pmod{m}$ azaz $\bar{a} \cdot \bar{x} = \bar{1}$.



Euler-féle φ függvény

Definíció

Egy $m > 0$ egész szám esetén legyen $\varphi(m)$ az m -nél kisebb, hozzá relatív prím egészek száma $\varphi(m) = |\{i : 0 < i < m, (m, i) = 1\}|$.

Példa:

$\varphi(5) = 4 : 5$ – höz relatív prím pozitív egészek : 1, 2, 3, 4;

$\varphi(6) = 2 : 6$ – höz relatív prím pozitív egészek : 1, 5;

$\varphi(12) = 4 : 12$ – höz relatív prím pozitív egészek : 1, 5, 7, 11;

$\varphi(15) = 8 : 15$ – höz relatív prím pozitív egészek :
1, 2, 4, 7, 8, 11, 13, 14

Megjegyzés: $\varphi(m)$ a redukált maradékosztályok száma modulo m .

Euler-féle φ függvény

$$\varphi(m) = |\{i : 0 < i < m, (m, i) = 1\}|$$

Tétel(NB)

Legyen m prímtényezős felbontása $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$. Ekkor

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

Példa

$$\varphi(5) = 5 \left(1 - \frac{1}{5}\right) = 4;$$

$$\varphi(6) = 6 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 2;$$

$$\varphi(12) = 12 \left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{3}\right) = 4;$$

$$\varphi(15) = 15 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 8.$$

Euler-Fermat téTEL

TéTEL

Legyen $m > 1$ egész szám, a olyan egész, melyre $(a, m) = 1$. Ekkor

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Következmény(Fermat téTEL)

Legyen p prímszám, $p \nmid a$. Ekkor $a^{p-1} \equiv 1 \pmod{p}$, illetve tetszőleges a esetén $a^p \equiv a \pmod{p}$.

Példa

$$\varphi(6) = 2 \Rightarrow 5^2 = 36 \equiv 1 \pmod{6};$$

$$\varphi(12) = 4 \Rightarrow 5^4 = 625 \equiv 1 \pmod{12}; 7^4 = 2401 \equiv 1 \pmod{12}.$$

Figyelem! $2^4 = 16 \equiv 2 \not\equiv 1 \pmod{12}$, mert $(2, 12) = 2 \neq 1$.

Euler-Fermat téTEL bIzonyításA

Lemma

Legyen $m > 1$ egész, a_1, a_2, \dots, a_m teljes maradékrendszer modulo m . Ekkor minden a, b egészre, melyre $(a, m) = 1$ $a \cdot a_1 + b, a \cdot a_2 + b, \dots, a \cdot a_m + b$ szintén teljes maradékrendszer. Továbbá, ha $a_1, a_2, \dots, a_{\varphi(m)}$ redukált maradékrendszer modulo m , akkor $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\varphi(m)}$ szintén redukált maradékrendszer.

Bizonyítás

Ha $i \neq j$ esetén $aa_i + b \equiv aa_j + b \pmod{m} \Leftrightarrow aa_i \equiv aa_j \pmod{m}$.

Mivel $(a, m) = 1$, egyszerűsíthetünk a -val: $a_i \equiv a_j \pmod{m}$. Tehát $a \cdot a_1 + b, a \cdot a_2 + b, \dots, a \cdot a_m + b$ páronként inkongruensek. Mivel számuk m , így teljes maradékrendszert alkotnak.

Ha $(a_i, m) = 1, (a, m) = 1 \Rightarrow (a \cdot a_i, m) = 1$. Továbbá

$a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\varphi(m)}$ páronként inkongruensek, számuk $\varphi(m) \Leftrightarrow$ redukált maradékrendszert alkotnak.

Euler-Fermat téTEL bIzonyításA

TéTEL (Euler-Fermat) $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bizonyítás

Legyen $a_1, a_2, \dots, a_{\varphi(m)}$ egy redukált maradékrendszer modulo m .

Mivel $(a, m) = 1 \Rightarrow a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\varphi(m)}$ szintén redukált maradékrendszer. Innen

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} a_j = \prod_{j=1}^{\varphi(m)} a \cdot a_j \equiv \prod_{j=1}^{\varphi(m)} a_j \pmod{m}$$

Mivel $\prod_{j=1}^{\varphi(m)} a_j$ relatív prím m -hez, így egyszerűsíthetünk vele:

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Euler-Fermat téTEL

TéTEL(Euler-Fermat) $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

Példa

Mi lesz a 3^{111} utolsó számjegye tízes szárendszerben?

Mi lesz $3^{111} \pmod{10}$?

$$\varphi(10) = 4 \Rightarrow$$

$$3^{111} = 3^{4 \cdot 27 + 3} = (3^4)^{27} \cdot 3^3 \equiv 1^{27} \cdot 3^3 = 3^3 = 27 \equiv 7 \pmod{10}$$

Oldjuk meg a $2x \equiv 5 \pmod{7}$ kongruenciát!

$\varphi(7) = 6$. Szorozzuk be minden oldalt 2^5 -el. Ekkor

$$5 \cdot 2^5 \equiv 2^6 x \equiv x \pmod{7}. \text{ És itt } 5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 4 = 20 \equiv \\ \equiv 6 \pmod{7}.$$

Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!

$\varphi(211) = 210$. Szorozzuk be minden oldalt 2^{209} -el. Ekkor

$$4 \cdot 23^{209} \equiv 23^{210} x \equiv x \pmod{211}. \text{ És itt } 4 \cdot 23^{209} \equiv \dots \pmod{211}.$$

Gyors hatványozás

Legyenek m, a, n pozitív egészek, $m > 1$. Szeretnénk kiszámolni $a^n \bmod m$ maradékot hatékonyan.

Ábrázoljuk n -et 2-es számrendszerben:

$$n = \sum_{i=0}^k \varepsilon_i 2^i = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_1 \varepsilon_0)_{(2)}, \text{ ahol } \varepsilon_0, \varepsilon_1, \dots, \varepsilon_k \in \{0, 1\}.$$

Legyen n_j ($0 \leq j \leq k$) az első $j+1$ jegy által meghatározott szám:

$$n_j = \lfloor \frac{n}{2^{k-j}} \rfloor = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_{k-j+1})_{(2)}$$

Ekkor meghatározzuk minden j -re az $x_j \equiv a^{n_j} \bmod m$ maradékot:

$$n_0 = \varepsilon_0 = 1, x_0 = a.$$

$$n_j = 2 \cdot n_{j-1} + \varepsilon_j \Rightarrow$$

$$x_j = a^{\varepsilon_j} x_{j-1}^2 \bmod m = \begin{cases} x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_j = 0 \\ a^{\varepsilon_j} x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_j = 1 \end{cases}$$

$$\Rightarrow x_k = a^n \bmod m.$$

Az algoritmus helyessége az alábbi formulából következik (Biz.: HF):

$$a^n = a^{\sum_{i=0}^k \varepsilon_i 2^i} = \prod_{i=0}^k (a^{2^i})^{\varepsilon_i}.$$

Gyors hatványozás

Példa

Mi lesz $3^{111} \pmod{10}$? (Euler-Fermat $\Rightarrow 7$)

$111_{(10)} = 1101111_{(2)}$ itt $k = 6, a = 3$.

j	n_j	$x_j = a^{\varepsilon_j} \cdot x_{j-2}^2$	$x_j \pmod{10}$
0	1	-	3
1	11	$x_1 = 3 \cdot 3^2$	7
2	110	$x_2 = 7^2$	9
3	1101	$x_3 = 3 \cdot 9^2$	3
4	11011	$x_4 = 3 \cdot 3^2$	7
5	110111	$x_5 = 3 \cdot 7^2$	7
6	1101111	$x_6 = 3 \cdot 7^2$	7

Gyors hatványozás

Példa

Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!

Euler-Fermat $\Rightarrow x \equiv 3 \cdot 23^{209} \equiv \dots \pmod{211}$.

Mi lesz $23^{209} \pmod{211}$?

$209_{(10)} = 11010001_{(2)}$ itt $k = 7, a = 23$.

j	n_j	$x_j = a^{\varepsilon_j} \cdot x_{j-1}^2$	$x_j \pmod{211}$
0	1	-	23
1	11	$x_1 = 23 \cdot 23^2$	140
2	110	$x_2 = 140^2$	188
3	1101	$x_3 = 23 \cdot 188^2$	140
4	11010	$x_4 = 140^2$	188
5	110100	$x_5 = 188^2$	107
6	1101000	$x_6 = 107^2$	55
7	11010001	$x_6 = 23 \cdot 55^2$	156

$x \equiv 4 \cdot 23^{209} \equiv 4 \cdot 156 \equiv 202 \pmod{211}$.

Tétel (NB)

Legyen p prímszám. Ekkor \mathbb{Z}_p^* -ban van generátor (primitív gyök): van olyan $1 < g < p$ egész, mely hatványaiként előáll minden redukált maradékosztály: $\{\overline{g^0} = \overline{1}, \overline{g}, \overline{g^2}, \dots, \overline{g^{p-1}}\} = \mathbb{Z}_p^*$, azaz $\{1 = g^0, g \text{ mod } p, g^2 \text{ mod } p, \dots, g^{p-1} \text{ mod } p\} = \{1, 2, \dots, p-1\}$.

Példa

3 generátor modulo 7

$$3^1 = 3 = 3^0 \cdot 3 \equiv 1 \cdot 3 = 3 \equiv 3 \text{ mod } 7$$

$$3^2 = 9 = 3^1 \cdot 3 \equiv 3 \cdot 3 = 9 \equiv 2 \text{ mod } 7$$

$$3^3 = 27 = 3^2 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 6 \text{ mod } 7$$

$$3^4 = 81 = 3^3 \cdot 3 \equiv 6 \cdot 3 = 18 \equiv 4 \text{ mod } 7$$

$$3^5 = 243 = 3^4 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 5 \text{ mod } 7$$

$$3^6 = 729 = 3^5 \cdot 3 \equiv 5 \cdot 3 = 15 \equiv 1 \text{ mod } 7$$

Példa

2 generátor modulo 11

n	1	2	3	4	5	6	7	8	9	10
$2^n \text{ mod } 11$	2	4	8	5	10	9	7	3	6	1

2 nem generátor modulo 7

n	1	2	3	4	5	6
$2^n \text{ mod } 7$	2	4	1	2	4	1

Diszkrét logaritmus

Definíció

Legyen p prímszám, g generátor modulo p . Ekkor az $a \in \mathbb{Z} : (p \nmid a)$ g alapú diszkrét logaritmusa (indexe):

$$\log_g a = n : a \equiv g^n \pmod{p}, \quad 0 \leq n < p - 1.$$

Példa

3 generátor modulo 7:

n	1	2	3	4	5	6
3^n	3	2	6	4	5	1



3^n	3	2	6	4	5	1
n	1	2	3	4	5	6

azaz

a	3	2	6	4	5	1
$\log_3 a$	1	2	3	4	5	6



a	1	2	3	4	5	6
$\log_3 a$	6	2	1	4	5	3



Diszkrét logaritmus

Példa

2 generátor modulo 11

n	1	2	3	4	5	6	7	8	9	10
$2^n \bmod 11$	2	4	8	5	10	9	7	3	6	1

Logaritmus-táblázat:

a	1	2	3	4	5	6	7	8	9	10
$\log_2 a$	10	1	8	2	4	9	7	3	6	2

Tétel (HF)

Legyen p prímszám, g generátor modulo p , $1 \leq a, b < p$, $n \in \mathbb{Z}$.

Ekkor

$$\log_g(a \cdot b) \equiv \log_g a + \log_g b \pmod{p-1}$$

$$\log_g(a^n) \equiv n \cdot \log_g a \pmod{p-1}$$

Számelmélet alkalmazási területei:

- Kriptográfia
 - üzenetek titkosítása;
 - digitális aláírás;
 - azonosítás, ...
- Kódelmélet
- ...

Caesar kód

Julius Caesar katonáival a következő módon kommunikált:
Feleltessük meg az (angol) ábécé betűit a $\{0, 1, \dots, 25\}$ halmaznak:

a	\rightarrow	0
b	\rightarrow	1
c	\rightarrow	2
\vdots		
z	\rightarrow	25

Titkos kulcs $s \in \{0, 1 \dots 25\}$

Titkosítás adott $a \in \{0, 1 \dots 25\}$ esetén a titkosítása $a \rightarrow a + s \pmod{26}$. Üzenet titkosítás betűnként.

Kititkosítás adott $b \in \{0, 1 \dots 25\}$ esetén b kititkosítása $b \rightarrow b - s \pmod{26}$. Üzenet kititkosítás betűnként.

Példa

hello titkosítása az $s = 13$ kulccsal:

hello $\rightarrow 7 \ 4 \ 11 \ 11 \ 14$ **titkosítás** $\Rightarrow 20 \ 17 \ 24 \ 24 \ 1 \rightarrow$ uryyyb

urzzc kititkosítása az $s = 13$ kulccsal:

uryyyb $20 \ 17 \ 24 \ 24 \ 1$ **kititkosítás** $\Rightarrow 7 \ 4 \ 11 \ 11 \ 14 \rightarrow$ hello

Caesar kód

Ha $s = 13$ kulcsot választjuk: Rot13

Titkosítás és kititkosítás ugyanazzal a kulccsal:

$$-13 \equiv 13 \pmod{26}.$$

A titkosítás nem biztonságos: betűgyakoriság vizsgálattal törhető
(al-Kindi isz. 9 sz.)

Ha a különböző pozíciókban különböző kulcsokat választhatunk
(véletlenszerűen) \Rightarrow bizonyítottan biztonságos

Gyakorlatban: One Time Pad = OTP

Üzenetek: bináris formában: $m=100100101$

Kulcs: bináris sorozat: $s=010110110$

Titkosítás: bitenkénti XOR ($\pmod{2}$ összeadás)

$$m=100100101 \text{ XOR } s=010110110 \rightarrow c=110010011$$

Kritikus pont az s titkos kulcs átadása.

Ron Rivest, Adi Shamir és Leonard Adleman 1977-ben a következő eljárást javasolták:

Kulcsgenerálás Legyen p, q két (nagy, 1024 bites) prím, $n = p \cdot q$.

Legyen $e \in \{1 \dots \varphi(n)\}$, hogy $(e, \varphi(n)) = 1$.

Legyen d az $ex \equiv 1 \pmod{\varphi(n)}$ kongruencia megoldása.

Kulcsok: nyilvános kulcs (n, e) .

titkos kulcs d .

Titkosítás Adott $0 \leq m < n$ üzenet titkosítása:

$$c = m^e \pmod{n}.$$

Kititkosítás Adott $0 \leq c < n$ titkosított üzenet kititkosítása:

$$m = c^d \pmod{n}.$$

Algoritmus helyessége

$$c^d \equiv (m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n) + 1} \stackrel{E-F}{\equiv} m \pmod{n}$$

Valóságban az m üzenet egy titkos kulcs további titkosításhoz.
Az eljárás biztonsága azon múlik, hogy nem tudjuk hatékonyan faktorizálni az $n = p \cdot q$ szorzatot.

Feladat

Találjuk meg a következő szám osztóit.

RSA-100=

5226050279225333605356183781326374297180681149613806886

57908494580122963258952897654000350692006139

RSA-2048=

25195908475657893494027183240048398571429282126204032027777137

26401852588078440691829064124951508218929855914917618450280848

72877767359714183472702618963750149718246911650776133798590957

01797429100642458691817195118746121515172654632282216869987549

86546204357679842338718477444792073993423658482382428119816381

60562016196762561338441436038339044149526344321901146575444541

50778707749817125772467962926386356373289912154831438167899885

378636564391212010397122822120720357

RSA-2048 faktorizálása:

Próbaosztás (Eratoszthenész szitája): n számot esetén $\sim \sqrt{n}$ osztást kell végezni:

RSA-2048 $\sim 2^{2048}$, $\sim 2^{1024}$ próbaosztás.

Ha 1 másodperc alatt $\sim 10^9 \approx 2^{30}$ osztás $\Rightarrow 2^{1024}/2^{30} = 2^{994}$ másodperc kell a faktorizáláshoz.

2^{994} másodperc = 2^{969} év.

Ugyan ezt 2 db géppel: 2^{968} év.

Ugyan ezt a legjobb (ismert) algoritmussal:

Univerzum életkora: $1.38 \cdot 10^{10}$ év.

Példa**Kulcsgenerálás**

Legyen $p = 61$, $q = 53$ és $n = 61 \cdot 53 = 3233$, $\varphi(3233) = 3120$.

Legyen $e = 17$. Bővített euklideszi algoritmussal: $d = 2753$.

Nyilvános kulcs: $(n = 3233, e = 17)$;

Titkos kulcs: $d = 2753$,

Titkosítás Legyen $m = 65$.

$$c = 2790 \equiv 65^{17} \pmod{3233}$$

Kititkosítás Ha $c = 2790$:

$$2790^{2753} \equiv 65 \pmod{3233}$$

Digitális aláírást is lehet generálni: e és d felcserélésével:
 (Ekkor külön n' , e' , d' kell a titkosításhoz!)

Aláírás Legyen $s = m^d \pmod{n}$, ekkor az aláírt üzenet: (m, s) .

Ellenőrzés $m \stackrel{?}{\equiv} s^e \pmod{n}$,

Diffie-Hellman kulcscsere protokoll

Az első nyilvános kulcsú kriptográfiai rendszert Whitfield **Diffie** és Martin **Hellman** 1976-ban publikálta.

Alice

Bob

nem megbízható csatorna

választ

választ

$$a \in_R \{0, 1, \dots, p-2\}$$

$$b \in_R \{0, 1, \dots, p-2\}$$

$$\xrightarrow{g^a}$$

$$\xleftarrow{g^b}$$

kiszámolja $(g^b)^a$

kiszámolja $(g^a)^b$

közös titkos kulcs

$$g^{ab}$$

Diffie-Hellman kulcscsere protokoll

Nyilvános paraméterek p (nagy) prím, g generátor $\mod p$.

Kulcsok Alice titkos kulcsa $a : 1 \leq a < p - 1$, nyilvános kulcsa $g^a \mod p$

Bob titkos kulcsa $b : 1 \leq b < p - 1$, nyilvános kulcs $g^b \mod p$

Közös kulcs $g^{ab} \mod p$

A protokoll biztonsága azon múlik, hogy a diszkrét logaritmus kiszámítás nehéz.

Ha $p \sim 2^{2048}$ (2048 bites), diszkrét logaritmus számolása $\sim 10^{30}$ év.

Példa

Nyilvános paraméterek Legyen $p = 11, g = 2$.

Kulcsok

Alice titkos kulcsa $a = 4$, nyilvános kulcsa $2^4 \mod p = 5$

Bob titkos kulcsa $b = 8$, nyilvános kulcsa $2^8 \mod p = 3$

Közös kulcs $(g^b)^a = 3^4 \mod p = 4$, $(g^a)^b = 5^8 \mod p = 4$.

Irodalom

- Mérai László: Diszkrét matematika előadás (2013 1.félév)
- Járai Antal: Bevezetés a matematikába (jegyzet)

Definíciók és téTEL kimondások

- Mondjon legalább három példát predikátumra.
- Sorolja fel a logikai jeleket.
- Milyen kvantorokat ismer? Mi a jelük?
- Hogyan kapjuk a logikai formulákat?
- Mikor van egy változó egy kvantor hatáskörében?
- Mik a nyitott és mik a zárt formulák?
- Mondjon két példát nyitott formulára.
- Mondjon egy példát zárt formulára.
- Definiálja a részhalmaz és a valódi részhalmaz fogalmát és adja meg jelöléseiket.
- Milyen tulajdonságokkal rendelkezik a "részHalmaz" fogalom?



- Milyen tulajdonságokkal rendelkezik a halmazok egyenlősége?
- Irja le az üres halmaz fogalmát.
- Igaz-e, hogy csak egy üres halmaz van?
- Irja le két halmaz unióját és a megfelelő jelöléseket.
- Irja le halmazrendszer unióját és a megfelelő jelöléseket.
- Fogalmazza meg a halmazok uniójának alaptulajdonságait.
- Definiálja halmazrendszer és két halmaz metszetét, és adja meg a jelöléseket.
- Definiálja a diszjunktság és páronként diszjunktság fogalmát.
- Fogalmazza meg a halmazok metszetének alaptulajdonságait.
- Fogalmazza meg az unió és a metszet disztributivitását.
- Definiálja halmazok különbségét, szimmetrikus differenciáját és komplementerét.
- Fogalmazza meg a halmazok komplementerének alaptulajdonságait.
- Irja le a hatványhalmaz fogalmát. Milyen jelölések kapcsolódnak hozzá?

- Definiálja a rendezett pár fogalmát és koordinátáit.
- Definiálja két halmaz Descartes-szorzatát.
- Definiálja a binér reláció fogalmát és adja meg a kapcsolódó jelöléseket.
- Adjon három példát binér relációra.
- Mit jelent az, hogy R reláció és X és Y között? Mit jelent az, hogy R egy X -beli reláció?
- Definiálja binér reláció értelmezési tartományát és érték készletét, és adja meg a kapcsolódó jelöléseket.
- Definiálja binér reláció kiterjesztését, leszűkítését egy halmazra és adja meg a kapcsolódó jelöléseket.
- Definiálja egy binér reláció inverzét.
- Definiálja halmaz képét és inverz képét binér relációnál és adja meg a kapcsolódó jelöléseket.
- Definiálja binér relációk kompozícióját. Lehet-e a kompozíció üres?
- Fogalmazzon meg három, binér relációk kompozíciójára vonatkozó állítást.

- Mit jelent az, hogy egy reláció tranzitív, szimmetrikus, illetve dichotóm? Ezek közül mi az, ami csak a reláción múlik?
- Definiálja az ekvivalenciareláció, illetve az osztályozás fogalmát.
- Mi a kapcsolat az ekvivalenciarelációk és az osztályozások között?
- Definiálja a részbenrendezést és a rendezést az X halmazon.
- Definiálja egy relációt megfelelő szigorú illetve gyenge reláció fogalmát.
- Definiálja a szigorú részbenrendezést az X halmazon.
- Mi az hogy kisebb, nagyobb, megelőzi, követi? Adja meg a kapcsolódó jelöléseket.
- Definiálja az intervallumokat és adja meg a kapcsolódó jelöléseket.
- Definiálja a kezdőszelet fogalmát és adja meg a kapcsolódó jelöléseket.
- Definiálja a legkisebb és a legnagyobb elem fogalmát.

- Definiálja a minimális és a maximális elem fogalmát és adja meg a kapcsolódó jelöléseket.
- Definiálja az alsó és a felső korlát fogalmát.
- Definiálja az alsó és a felső határ tulajdonságot.
- Definiálja az innfimum és a szuprénum fogalmát.
- Definiálja a függvény fogalmát. Ismertesse a kapcsolódó jelöléseket.
- Deiniálja függvény injektív, szürjektív, bijektív tulajdonságait.
- Igaz-e, hogy az identikus leképezés mindig szürjektív?
- Definiálja a permutáció fogalmát függvényekre.
- Igaz-e, hogy két függvény összetétele függvény?
- Mikor állíthatjuk, hogy két függvény összetétele injektív, szürjektív illetve bijektív?
- Mikor nevezünk egy függvényt monoton növekedőnek illetve monoton csökkenőnek?
- Mikor nevezünk egy függvényt szigorúan monoton növekedőnek illetve szigorúan monoton csökkenőnek?

- Mi a kapcsolat a szigorúan monoton növekedő függvények és a kölcsönösen egyértelmű függvények között?
- Mit állíthatunk a monoton növekedő függvények inverz függvényéről?
- Definiálja a binér, unér művelet fogalmát és ismertesse a kapcsolódó jelöléseket.
- Adjon meg egy binér és egy unér műveletet táblázattal.
- Hogyan definiálunk műveleteket függvények között?
- Definiálja az asszociatív és kommutatív műveleteket.
- Definiálja a művelettartó leképezés fogalmát.
- Adjon példát művelettartó leképezésekre.
- Fogalmazza meg a Peano-axiómákat.
- Definiálja a baloldali semleges elem, jobboldali semlegeselem és a semleges elem fogalmát.
- Definiálja a félcsoport, a balinverz, a jobbinverz és az inverz fogalmát és ismertesse a kapcsolódó jelöléseket.
- Igaz-e, hogy ha X tetszőleges halmaz, akkor $(p(X), \cap)$ egy egységelemes félcsoport?

- Igaz-e, hogy ha X tetszőleges halmaz, akkor $(\wp(X), \cup)$ egy csoport?
- Igaz-e, hogy ha X tetszőleges halmaz, akkor az X -beli binér relációk a kompozícióval egységelemes félcsoportot alkotnak?
- Milyen algebrai struktúrát alkot a természetes számok az összeadásra nézve. Indokolja meg az állítást.
- Igaz-e, hogy az egész számok a szorzás műveletre kommutatív egységelemes félcsoportot alkotnak?
- Definiálja a csoport, Abel csoport fogalmát.
- Igaz-e, hogy ha X tetszőleges halmaz, akkor az X -et X -re képező bijektív leképezések a kompozícióval, mint műveettel csoportot alkotnak?
- Definiálja a bal és a jobb oldali nullosztó és a nullosztópár fogalmát.
- Definiálja a gyűrű fogalmát, mondjon példát gyűrűre.
- Igaz-e, hogy az egész számok az összeadásra és a szorzásra nézve disztributív.

- Fogalmazza meg a természetes számok egész számokba történő beágyazásáról szóló állítást.
- Definiálja a nullosztómentes gyűrű fogalmát.
- Fogalmazza meg a természetes számoknak a racionális számokba történő beágyazására vonatkozó állítást.
- Definiálja a test fogalmát és adjon három példát testre.
- Definiálja a rendezett gyűrű fogalmát.
- Fogalmazza meg az egész számokon értelmezett rendezésre vonatkozó tételeit.
- Definiálja a rendezett test fogalmát és adjon példát olyan testre, amely nem tehető rendezett testé.
- Fogalmazza meg a valós számok definícióját.
- Fogalmazza meg a valós számok körében a gyökvonásra vonatkozó tételeit.
- Definiálja a komplex számok halmazát a műveletekkel.
- Adja meg \mathbb{R} beágyazását \mathbb{C} -be.
- Definiálja i -t, komplex szám valós és képzetes részét, konjugáltját és a képzetes számok fogalmát.

- Fogalmazza meg a komplex konjugálás tulajdonságait.
- Definiálja komplex szám abszolút értékét.
- Fogalmazza meg a komplex számok abszolút értékének tulajdonságait.
- Definiálja komplex számok trigonometrikus alakját és argumentumát.
- Irja fel két komplex szám szorzatát és hányadosát trigonometrikus alakjuk segítségével.
- Ha $n \in \mathbb{N}^+$ és $w \in \mathbb{C}$, írja fel a $w^n = z$ egyenlet összes megoldását.
- Fogalmazza meg komplex szám rendjét.
- Irja fel az n-edik komplex egységgököket. Mit értünk primitív n-edik egységgöök alatt?
- Ha $n \in \mathbb{N}^+$ és $w \in \mathbb{C}$, írha fel a $w^n = z$ egyenlet összes megoldását az n-edik egységgöök segítségével.
- Fogalmazza meg az algebra alaptételét.
- Fogalmazza meg a skatulyaelvet.

- Mit mondhatunk egy véges halmaz összes permutációinak számáról?
- Mit értünk egy véges halmaz variációin és mit mondhatunk az összes variációk számáról?
- Definiálja az ismétléses variációk fogalmát. Mit mondhatunk egy véges halmaz összes ismétléses variációinak számáról?
- Mit értünk egy véges halmaz kombinációin és mit mondhatunk az összes kombinációk számáról?
- Mit értünk egy véges halmaz ismétléses kombinációin és mit mondhatunk az összes ismétléses kombinációk számáról?
- Mit értünk egy véges halmaz ismétléses permutációin és mit mondhatunk az összes ismétléses permutációk számáról?
- Definiálja a binomiális együttható fogalmát.
- Fogalmazza meg a binomiális tételet.
- Irja fel a Pascal-háromszög első 8 sorát.
- Fogalmazza meg a polinomiális tételet.
- Fogalmazza meg a skatulya-elvet.

- Fogalmazza meg a szita módszerre vonatkozó tételeit.
- Definiálja az egész számok körében az oszthatóságot és adja meg a jelölését.
- Sorolja fel a egész számok körében az oszthatóság alaptulajdonságait.
- Definiálja az asszociáltak fogalmát.
- Definiálja az egységek fogalmát.
- Definiálja az egész számok körében a prímszám és a felbonthatatlan fogalmát. Mi a kapcsolat a két fogalom között?
- Mondja ki a maradékos osztás tételeit az egész számok körében.
- Definiálja egy a egész szám b egész számmal vett osztási maradékát.
- Fogalmazza meg a számrendszerekre vonatkozó tételeit.
- Definiálja két egész szám legnagyobb közös osztóját.
- Definiálja két egész szám legkisebb közös többszörösét.
- Egyértelmű-e az egész számok körében a legnagyobb közös osztó? Ismertesse a kapcsolódó jelölést.

- Egyértelmű-e az egész számok körében a legkisebb közös többszörös? Ismertesse a kapcsolódó jelölést.
- Ismertesse a bővített euklideszi algoritmust.
- Mely téTEL alapján számolhatjuk ki véges sok egész szám legnagyobb közös osztóját prímfelbontás nélkül?
- Fogalmazza meg legnagyobb közös osztó rekurzióval történő meghatározását.
- Fogalmazza meg egész szám kanonikus alakját.
- Definiálja $\tau(n)$ számelméleti függvényt. Mondja ki a $\tau(n)$ meghatározására vonatkozó állítást.
- Fogalmazza meg a számelmélet alaptételét?
- Ismertesse Eratoszthenész szitáját.
- Fogalmazza meg Euklidész téTELét.
- Definiálja egész számok kongruenciáját és adja meg a kapcsolódó jelölésekET.
- Fogalmazza meg az egész számok kongruenciájának egyszerű tulajdonságait.

- Fogalmazza meg a $ac \equiv bc \pmod{m}$ kongruenciával ekvivalens kongruenciára vonatkozó állítást.
- Fogalmazza meg az egész számok kongruenciájának megoldására vonatkozó állítást.
- Definiálja a maradékosztály, redukált maradékosztály, teljes és redukált maradékrendszer fogalmát.
- Definiálja \mathbb{Z}_m -t. Milyen algebrai struktúra \mathbb{Z}_m az összeadással és szorzással?
- Fogalmazza meg a maradék osztályok közt értelmezett műveletekre vonatkozó állítást.
- Fogalmazza meg a maradékosztály reciprokára vonatkozó téltet.
- Definiálja az Euler-féle φ függvényt. Fogalmazza meg $\varphi(m)$ függvény értékét meghatározó állítást.
- Mit mondhatunk az $a a_i + b$ számokról, ha a_i egy maradékrendszer, illetve egy redukált maradékrendszer elemeit futja be?
- Fogalmazza meg az Euler-Fermat téltet.

- Fogalmazza meg a Fermat-tételt.
- Mit értünk diofantikus problémán?
- Mondjon két példát diofantikus problémára.
- Fogalmazza meg a szimultán kongruencia megoldásának módszerét.
- Fogalmazza meg a kínai maradéktételt.
- Fogalmazza meg az \mathbb{Z}_m^* -ban a generátorra vonatkozó tételt.
- Definiálja a diszkrét logitmus fogalmát.

Bizonyítások

- Fogalmazza meg a halmazok uniójának kommutativitását, asszociativitását és idempotenciáját és bizonyítsa be.
- Fogalmazza meg a halmazok metszetének kommutativitását, asszociativitását és idempotenciáját és bizonyítsa be.

- Fogalmazza meg és bizonyítsa be az unió és a metszet disztributivitását.
- Fogalmazza meg és bizonyítsa be a De Morgan azonosságokat két halmazra.
- Bizonyítsa be, hogy binér relációk kompozíciója asszociatív.
- Fogalmazza meg az ekvivalenciareláció az X halmaz osztályozását adja meg. Bizonyítsa be az állítást.
- Fogalmazza meg, hogy az osztályozás ekvivalenciarelációt határonak meg az X halmazon. Bizonyítsa be az állítást.
- Fogalmazza meg a rendezés és a trichotómia kapcsolatát, bizonyítsa be az állítást.
- Mi a kapcsolat a szigorúan monoton növekedő függvények és a kölcsönösen egyértelmű függvények között? A megfogalmazott állítást bizonyítsa be.
- Fogalmazza meg, hogy az $f : x \rightarrow x^k$ függvény milyen feltétel teljesülése esetén bijektív, bizonyítsa be az állítást.
- Fogalmazza meg függvény kompozíójára vonatkozó állításokat. Bizonyítsa be.

- Van-e olyan racionális szám, amelynek a négyzete 2? Bizonyítsa be az állítást.
- Definiálja a komplex számok halmazát a műveletekkel és bizonyítsa be, hogy test.
- Fogalmazza meg komplex számok abszolút értékének tulajdonságait és bizonyítsa be.
- Fogalmazza meg az állítást az n-edik komplex egységgökökre, primitív n-edik egységgöök felhasználásával. Bizonyítsa be az állítást.
- Fogalmazza meg a komplex szám rendjére vonatkozó állítást és bizonyítsa be.
- Mit mondhatunk egy véges halmaz összes permutációinak számáról? Bizonyítsa be az állítást.
- Mit értünk egy véges halmaz variációin és mit mondhatunk az összes variációk számáról? Bizonyítsa be állítását.
- Mit értünk egy véges halmaz kombinációin és mit mondhatunk az összes kombinációk számáról? Bizonyítsa be az állítást.



- Mit értünk egy véges halmaz ismétléses kombinációin és mit mondhatunk az összes ismétléses kombinációk számáról? Bizonyítsa be az állítást.
- Mit mondhatunk egy véges halmaz összes ismétléses permutációinak számáról? Bizonyítsa be az állítást.
- Mit értünk egy véges halmaz ismétléses variációin és mit mondhatunk az összes ismétléses variációk számáról? Bizonyítsa be állítását.
- Fogalmazza meg a binomiális együtthatókra vonatkozó téltel és bizonyítsa be az állítást.
- Fogalmazza meg a binomiális téltel és bizonyítsa be.
- Fogalmazza meg a polinomiális téltel és bizonyítsa be.
- Fogalmazza meg az általános szita formulát és bizonyítsa be.
- Bizonyítsa be, hogy az egész számok körében két egység van.
- Mi a kapcsolat \mathbb{Z} -ben a prímelemek és az irreducibilis elemek között? Bizonyítsa állítását.
- Mondja ki a maradékos osztás tételét az egész számok körében. Bizonyítsa be az állítást.

- Fogalmazza meg a számrendszerekre vonatkozó tételeket. Bizonyítsa be az állítát.
- Ismertesse a bővített euklideszi algoritmust. Bizonyítsa be hogy működik.
- Fogalmazza meg a prímszámok és a felbonthatatlan kapcsolatát. Bizonyítsa be az állítást bővített euklideszi algoritmussal.
- Fogalmazza meg és bizonyítsa be a számelmélet alaptételét.
- Fogalmazza meg a legnagyobb közös osztó meghatározását Euklidész algoritmussal és bizonyítsa be.
- Fogalmazza meg legnagyobb közös osztó rekurzióval történő meghatározását. Bizonyítsa be az állítást.
- Definiálja $\tau(n)$ számelméleti függvényt. Mondja ki a $\tau(n)$ meghatározására vonatkozó állítást. Bizonyítsa be az állítást.
- Fogalmazza meg Euklidész tételeit és bizonyítsa be az állítást.
- Fogalmazza meg a kongruenciák tulajdonságait leíró tételeit és bizonyítsa be az állítást.

- Fogalmazza meg a $ac \equiv bc \pmod{m}$ kongruenciával ekvivalens kongruenciára vonatkozó állítást és bizonyítsa be.
- Fogalmazza meg a lineáris kongruencia megoldására vonatkozó tételet. Bizonyítsa be az állítást.
- Fogalmazza meg a maradék osztályok közt értelmezett műveletekre vonatkozó állítást és bizonyítsa be.
- Fogalmazza meg a maradékosztály reciprokára vonatkozó tételet és bizonyítsa be.
- Mit mondhatunk az $aa_i + b$ számokról, ha a_i egy teljes maradékrendszer, illetve az $aa_i + b$ számokról, ha a_i egy redukált maradékrendszer elemeit futja be? Bizonyítsa be az állítást.
- Fogalmazza meg és bizonyítsa be az Euler-Fermat tételet.
- Fogalmazza meg és bizonyítsa be a kínai maradéktételt.