Diszkrét matematika 1.

Nagy Gábor

nagy@compalg.inf.elte.hu
nagygabr@gmail.com
ELTE IK Komputeralgebra Tanszék

2014. ősz

Gyakorlat:

1. **ZH tervezett időpontja**: október 21.,
2. **ZH tervezett időpontja**: december 9.

Fontos információk az alábbi linken találhatók:
http://compalg.inf.elte.hu/~merai/Edu/DM1/index-dm1-gy.html
Ennek szerepét idővel átveszi:
http://compalg.inf.elte.hu/~burcsi
http://compalg.inf.elte.hu/~nagy

Előadás:
Fontos információk az alábbi linken találhatók:
http://compalg.inf.elte.hu/~ merai/Edu/DM1/index-dm1-ea.html

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:

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

Célunk olyan u, v találása, melyekre $-3uv = p$, $-(u^3 + v^3) = q$.
Ekkor $u + v$ megoldás lesz!
u, v megtalálása: $u^3v^3 = (-\frac{p}{3})^3$, $u^3 + v^3 = -q$, u^3, v^3 gyökei lesznek a $z^2 + qz + (\frac{-p}{3})^3 = 0$ másodfokú egyenletnek. A gyökökből u, v köbgyökvonással kijön:

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

Harmadfokú egyenlet

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

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

képletbe azt kapjuk, hogy

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

A négyzetgyök alatt negatív!
Meg lehet-e menteni a megoldóképletet?

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 $\sqrt{-3}$-mal 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 $x^2 = (-x)^2 > 0$.

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: $i \leftrightarrow (0, 1)$.
Az $a + bi$ formátum kényelmesebb számoláshoz.
Az (a, b) formátum kényelmesebb ábrázoláshoz
(grafikusan, számítógépen).
További formális számokra nincs szükség:

Tétel(Algebra alaptétele, NB)

Minden $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ kifejezés esetén, ahol $a_0, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, akkor létezik olyan $z \in \mathbb{C}$ komplex szám, hogy $a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n = 0$.

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 $r \in \mathbb{R}$ nemnulla szám reciproka: $\frac{1}{r}$.
Mi lesz $\frac{1}{1+i}$?
Ötlet: gyöktelenítés, kunjugálttal való bővítés:

$$\frac{1}{1+\sqrt{2}} = \frac{1}{1+\sqrt{2}} \cdot \frac{1-\sqrt{2}}{1-\sqrt{2}} = \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})} = \frac{1-\sqrt{2}}{1^2-(\sqrt{2})^2}$$

$$= \frac{1-\sqrt{2}}{1-2} = -1+\sqrt{2}.$$

Hasonlóan:

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

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

Számolás komplex számokkal

Definíció

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

Állítás(HF)

Egy z nemnulla komplex szám reciproka $\frac{1}{z} = \frac{\overline{z}}{z \cdot \overline{z}}$

A definíció értelmes, hiszen a nevezőben:

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

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

Két komplex szám hányadosa:

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

Számolás komplex számokkal

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. $z + \overline{z} = 2 \cdot Re(z)$;
5. $z - \overline{z} = 2i \cdot Im(z)$;
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 $|z| > 0$;
9. $|\overline{z}| = |z|$;
10. $|z \cdot w| = |z| \cdot |w|$;
11. $|z + w| \leq |z| + |w|$ (háromszög egyenlőtlenség).

Számolás komplex számokkal

Tétel(HF)

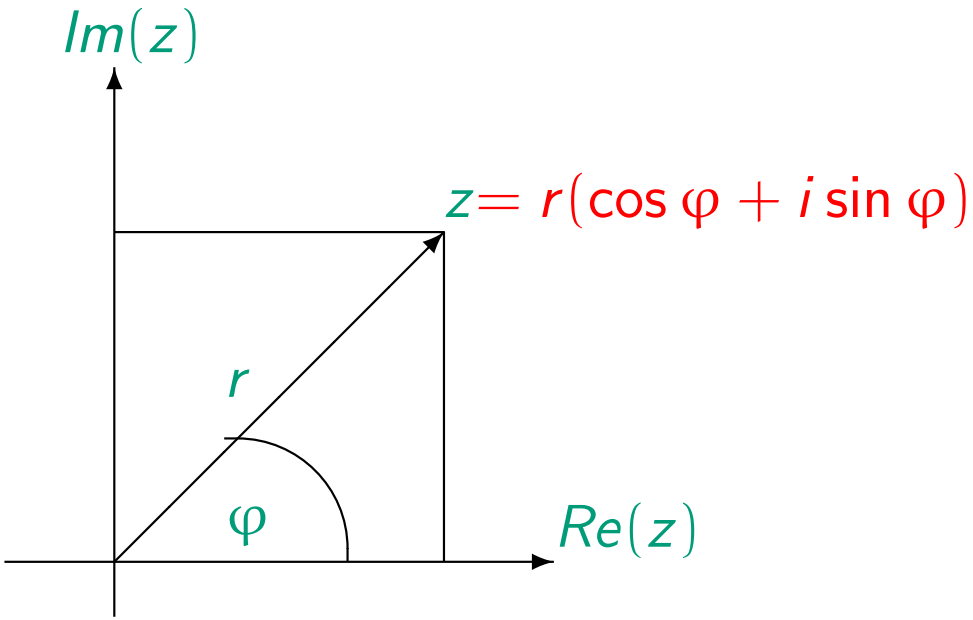
- $|z \cdot w| = |z| \cdot |w|$;

Bizonyítás

$$|z \cdot w|^2 = z \cdot w \cdot \overline{z \cdot w} = z \cdot w \cdot \overline{z} \cdot \overline{w} = z \cdot \overline{z} \cdot w \cdot \overline{w} = |z|^2 \cdot |w|^2 = (|z| \cdot |w|)^2.$$

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 nemnulla 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

$z \in \mathbb{C}$ nemnulla szám trigonometrikus alakja a
$z = r(\cos\varphi + i\sin\varphi)$,
ahol $r > 0$ a szám abszolút értéke.

Figyelem! A 0-nak nem használjuk a trigonometrikus alakját.
A trigonometrikus alak nem egyértelmű:
$r(\cos\varphi + i\sin\varphi) = r(\cos(\varphi + 2\pi) + i\sin(\varphi + 2\pi))$.

Definíció

Egy $z \in \mathbb{C}$ nemnulla 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 $z, w \in \mathbb{C}$ nemnulla komplex számok:

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

A szorzatuk:

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

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

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

Moivre-azonosságok

Tétel HF

Legyen $z, w \in \mathbb{C}$ nemnulla komplex számok:
$z = |z|(\cos\varphi + i\sin\varphi)$, $w = |w|(\cos\psi + i\sin\psi)$,
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 szögek 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. $|z|$-kel nyújt, $arg(z)$ szöggel forgat.

Példa

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

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

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

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

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

Tétel

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

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

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

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

Példa

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

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

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

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

$$\sqrt[6]{\frac{1-i}{\sqrt{3}+i}} = \sqrt[6]{\frac{1}{\sqrt{2}}\left(\cos\tfrac{19\pi}{12}+i\sin\tfrac{19\pi}{12}\right)} =$$

$$= \frac{1}{\sqrt[12]{2}}\left(\cos\tfrac{19\pi+2k\pi}{72}+i\sin\tfrac{19\pi+2k\pi}{72}\right) : k = 0,1,\ldots,5.$$

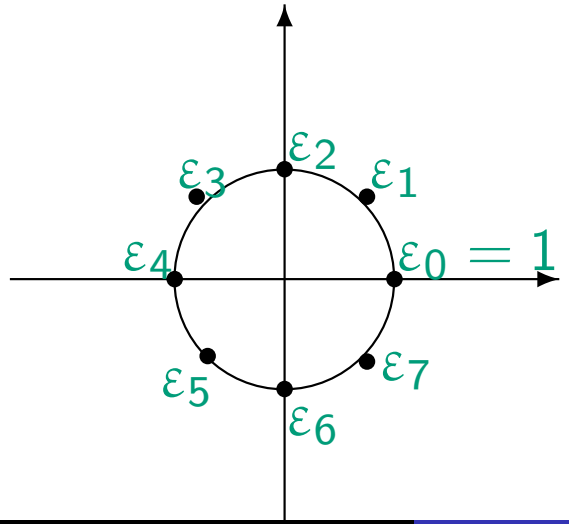
Komplex egységgyökök

Definíció

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

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

Nyolcadik komplex egységgyökök



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: $w\varepsilon_k : k = 0, 1, \ldots n-1$.

Bizonyítás

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

Rend

Bizonyos komplex számok hatványai periodikusan ismétlődnek:

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

Általában:
$\cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$-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 $\infty : 2, 4, 8, 16, \ldots$
- -1 rendje 2: $1, -1$
- i rendje 4: $1, i, -1, -i$

Rend

Tétel

Egy z komplex számnak vagy bármely két egész kitevős hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periodikusan 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 feltétlenül n:
4-edik 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. egységgyök: 1;
- Primitív 2. egységgyök: -1;
- Primitív 3. egységgyökök: $\frac{-1\pm i\sqrt{3}}{2}$;
- Primitív 4. egységgyökök: $\pm i$;
- Primitív 5. egységgyökök: $\ldots$ (HF)
- Primitív 6. egységgyökök: $\frac{1\pm i\sqrt{3}}{2}$;

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 $(n,k) = 1$.

Diszkrét matematika I. középszint

2. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Matematikai logika

A logika a helyes következtetés tudománya.
Alkalmazási területek:

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

Példa
Minden bogár rovar.
tagadás: Van olyan bogár, ami nem rovar.
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 feltevésekből (axiómákból) a logika szabályai szerint milyen következtetéseket vonunk le (milyen tételeket bizonyítunk).

Példa

Euklidészi geometria

Alapfogalmak

- pont,
- egyenes,
- sík.

Axiómák

- párhuzamossági axióma,
- ...

Az axiomatikus módszer előnye: elég ellenőrizni az axiómák teljesülését.

Predikátumok

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: I.
$Sz(x)$: x egy szám.	1-változós, értéke: Sz(1)=I, SZ(h)=H.
$E(x)$: x egy egyenes.	1-változós.
$P(x)$: x egy pont.	1-változós.
$I(x, y)$: x illeszkedik y-ra.	2-változós.
$F(x, y)$: x az y férje.	2-változós.
$Gy(x, y, z)$: x az y és z gyermeke.	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

A köznyelvben a **vagy** háromféle értelemmel bírhat:
Megengedő **vagy** ,,Átok reá ki gyávaságból **vagy** lomhaságból 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.”

$A \oplus B$	I	H
I	H	I
H	I	H

Összeférhetetlen **vagy**: ,,Iszik **vagy** vezet!”

$A \mid\mid B$	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

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

$2 \cdot 2 = 4 \quad \Rightarrow \quad$ kedd van

Hamis állításból minden következik:

Példa

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

Adott logikai jel, más módon is kifejezhető:

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

Kvantorok

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. $\exists x(M(x) \wedge V(x))$.

Minden veréb madár, de nem minden madár veréb.

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

Formulák

A formulák predikátumokból és logikai jelekből alkotott ,,mondatok".

Definíció(Formulák)

- A predikátumok a legegyszerűbb, ún. 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.

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

Ez egy formula.

Ha nem okoz félreértést, a zárójelek elhagyhatóak.

Zárt/ nyitott formulák

Definíció

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

Zárt/nyitott formulák

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 különbözőek.

$\mathcal{C}(x)$ 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.

Halmazok

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 ugyanazok az elemeik.
- Egy halmaznak egy elem csak egyszer lehet eleme.

Halmazok

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 egy további tulajdonságot is teljesít:
3'. $\forall A, B \quad A = B \Rightarrow B = A$ (szimmetria).

Halmazok

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

- $\{z \in \mathbb{C} : Im\ z = 0\}$: valós számok halmaza.
- $\{z \in \mathbb{C} : \exists n \in \mathbb{N} \quad z^n = 1\}$: komplex egységgyökök halmaza.

Halmazok

Speciális halmazok

Üres halmaz Annak a halmaznak, melynek nincs eleme a jele: $\emptyset$. A meghatározottsági axióma alapján ez egyértelmű.
$\forall A \quad A$ halmaz $\Rightarrow \emptyset \subset A$

Halmaz megadása elemei felsorolásával. Annak a halmaznak, melynek csak az a elem az eleme a jelölése: $\{a\}$. Annak a halmaznak, melynek az a és b az eleme a jelölése: $\{a, b\}$,...

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

Műveletek halmazokkal

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

Példa

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

Rövidebben, ha $\overline{a} = \{n : n \equiv a \mod m\}$, akkor

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

Általában

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

Műveletek halmazokkal

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 mindkét oldalnak, ha $x \in A$
- 2. Egy x pontosan akkor eleme mindkét oldalnak, ha $x \in A$ vagy $x \in B$
- 3-as, 4-es hasonló
- 5. $\Rightarrow$: $A \subset B \Rightarrow A \cup B \subset B$, de $A \cup B \supset B$ mindig teljesül, így $A \cup B = B$.
  $\Leftarrow$: Ha $A \cup B = B$, akkor A minden eleme eleme B-nek.

Műveletek halmazokkal

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

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

Műveletek halmazokkal

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.

Műveletek halmazokkal

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. $A \subset B \Leftrightarrow A \cap B = A$

Műveletek halmazokkal

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. $x \in A \cap (B \cup C) \Leftrightarrow x \in A \wedge x \in B \cup C$.
   Így x pontosan akkor eleme a bal oldalnak, 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 $\overline{A} = A' = X \setminus A$.

Komplementer tulajdonságai

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 ún. de Morgan szabályok.

Szimmetrikus differencia

Definíció

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

Állítás (Biz. HF)

$A \triangle B = (A \cup B) \setminus (A \cap B)$.

Hatványhalmaz

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)

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

Diszkrét matematika I. középszint

3. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Relációk

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

Definíció

Az X, Y halmazok Descartes-szorzatán az

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

rendezett párokból álló halmazt értjük.

Binér relációk

Adott X, Y halmazok esetén az $R \subset X \times Y$ halmazokat binér (kétváltozós) relációknak nevezzük.
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. $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \mid y\}$ 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 $f : \mathbb{R} \to \mathbb{R}$ 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, értékkészlete

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 $R \subset X \times Y$ reláció értelmezési tartománya a

$$\mathrm{dmn}(R) = \{x \in X | \exists y \in Y : (x, y) \in R\},$$

értékkészlete

$$\mathrm{rng}(R) = \{y \in Y | \exists x \in X : (x, y) \in R\}.$$

Példa

1. Ha $R = \{(x, 1/x^2) : x \in \mathbb{R}\}$, akkor $\mathrm{dmn}(R) = \{x \in \mathbb{R} : x \neq 0\}$, $\mathrm{rng}(R) = \{x \in \mathbb{R} : x > 0\}$.
2. Ha $R = \{(1/x^2, x) : x \in \mathbb{R}\}$, akkor $\mathrm{dmn}(R) = \{x \in \mathbb{R} : x > 0\}$, $\mathrm{rng}(R) = \{x \in \mathbb{R} : x \neq 0\}$.

Relációk kitejesztése, leszűkítése, inverze

Definíció

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

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

Példa

Legyen $R = \{(x, x^2) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$, $S = \{(\sqrt{x}, x) \in \mathbb{R} \times \mathbb{R} : x \in \mathbb{R}\}$.
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 inverze az $R^{-1} = \{(y, x) : (x, y) \in R\}$.

Példa

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

Halmaz képe, teljes inverz képe

Definíció

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

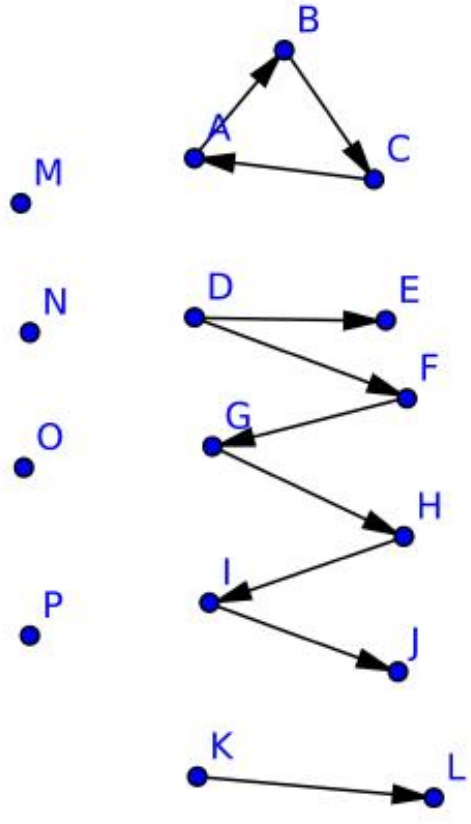
Példa

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

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

Példa

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



- $\mathrm{dmn}(R) = \{A, B, C, D, F, G, H, I, K\}$.
- $\mathrm{rng}(R) = \{A, B, C, E, F, G, H, I, J, L\}$.
- $R|_{\{A,B,C,D\}} = \{(A, B), (B, C), (C, A), (D, E), (D, F)\}$.

Kompozíció

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

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

Ekkor

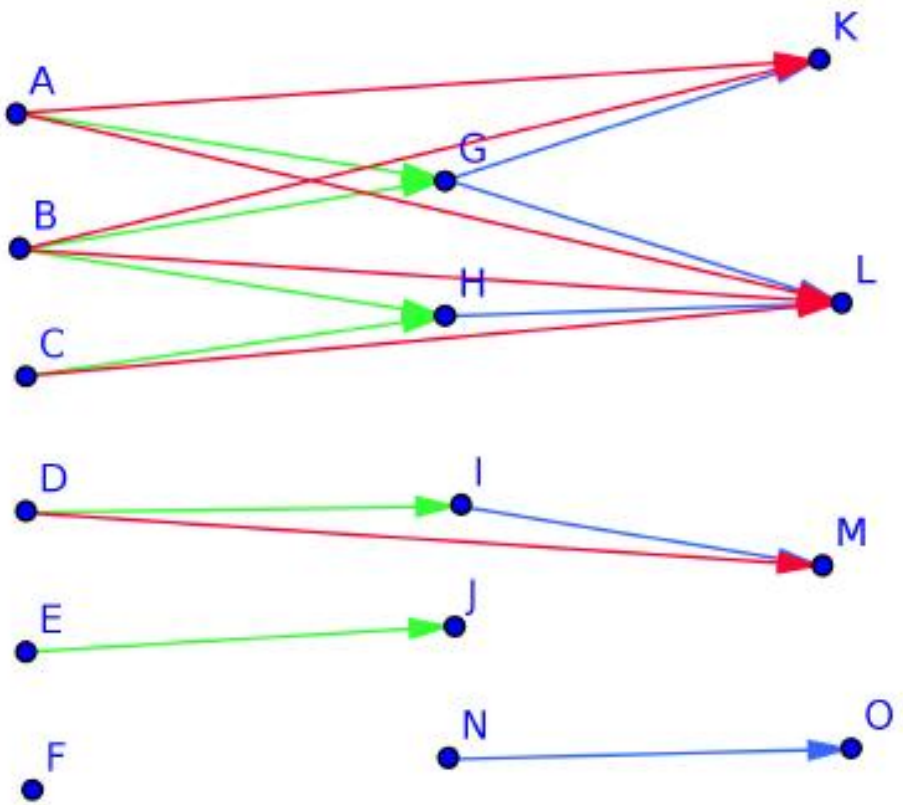
$$\begin{aligned} R_{\sin} \circ S_{\log} &= \{(x, y) | \exists z : \log x = z, \sin z = y\} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \sin \log x = y\}. \end{aligned}$$

Kompozíció

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

Példa

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



Példa

Adott cég esetén legyenek A ,B, . . . , 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	2014.12.31.
JÁTÉK	B, D, E, F, G, H	2015.01.31.

Legyen B a beosztás reláció: például A B menedzser.
P a projekt reláció: például A P BANK
H a határidő reláció: például BANK H 2014.12.31.

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

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 $\mathrm{rng}(S) \supset \mathrm{dmn}(R)$, akkor $\mathrm{rng}(R \circ S) = \mathrm{rng}(R)$.
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. $\mathrm{rng}(R) = \{y | \ \exists z : \ (z, y) \in R\}$. Mivel $\mathrm{rng}(S) \supset \mathrm{dmn}(R)$, 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. $(R \circ S)^{-1} = \{(y, x) | \exists z : (x, z) \in S, (z, y) \in R\} = \{(y, x) | \exists z : (z, x) \in S^{-1}, (y, z) \in R^{-1}\} = S^{-1} \circ R^{-1}$. □

Relációk tulajdonságai

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

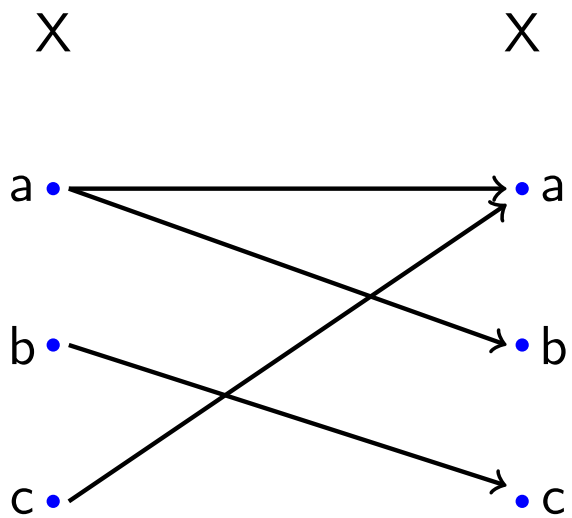
1. R tranzitív, ha $\forall x,y,z \in X : (xRy \wedge yRz) \Rightarrow xRz$;$(=,\ <,\ \leq,\ |,\ \subset)$
2. R szimmetrikus, ha $\forall x,y \in X : xRy \Rightarrow yRx$; $(=,\ T)$
3. R antiszimmetrikus, ha$\forall x,y \in X : (xRy \wedge yRx) \Rightarrow x = y$;$(=, \leq, \subset)$
4. R szigorúan antiszimmetrikus, 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 trichotóm, ha $\forall x,y \in X$ esetén $x = y$, xRy és yRx közül pontosan egy teljesül; $(<)$
8. R dichotóm, ha $\forall x,y \in X$ esetén xRy vagy yRx (esetleg mindkettő). $(\leq)$

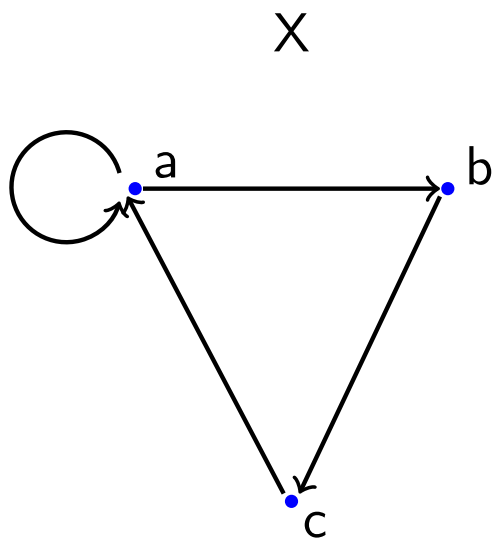
Relációk tulajdonságai

A reflexív, trichotóm, dichotóm 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 $\mathbb{C}$-n értelmezett reláció nem reflexív.

Példa



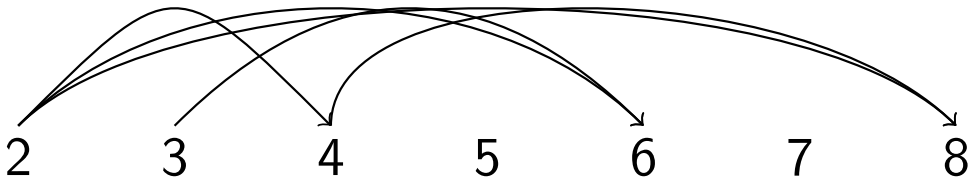


tranzitív	X	szigorúan antiszimmetrikus	X	trichotóm	X
szimmetrikus	X	reflexív	X	dichotóm	X
antiszimmetrikus	✓	irreflexív	X		

Relációk gráfja

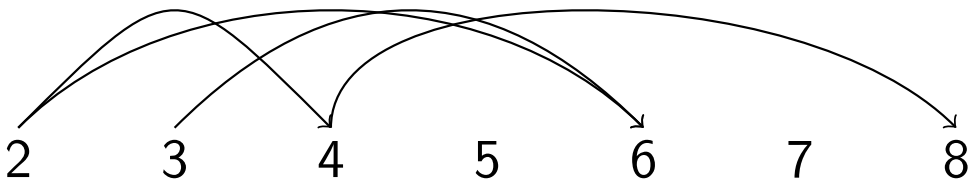
A relációk gráfját egyszerűsíthetjük:

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



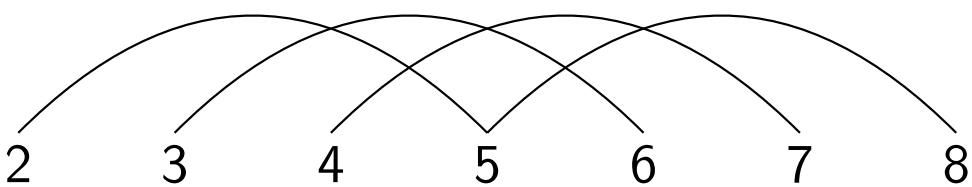
osztója reláció

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



osztója reláció

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



$\equiv \mod 3$

Ekvivalenciareláció, osztályozások

Definíció

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

Példa

1. $=$; 2. $z \sim w$, ha $\mathrm{Re}(z) = \mathrm{Re}(w)$.

Definíció

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

Példa

1. $\mathbb{R}$ egy osztályozása: $\{\{a\} : a \in \mathbb{R}\}$;
2. $\mathbb{C}$ egy osztályozása: $\{\{z \in \mathbb{C} : \mathrm{Re}(z) = r\} : r \in \mathbb{R}\}$.

Ekvivalenciareláció, osztályozások

Tétel

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

Bizonyítás

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

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

Ekvivalenciareláció, osztályozások

Tétel

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

Bizonyítás

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

Ekvivalenciareláció, osztályozások

Az ekvivalenciarelációk illetve osztályozások kölcsönösen egyértelműen meghatározzák egymást.

Példa

- $= \longleftrightarrow \{\{a\} : a \in \mathbb{R}\}$;
- $z \sim w$, ha $\mathrm{Re}(z) = \mathrm{Re}(w) \longleftrightarrow \{\{z \in \mathbb{C} : \mathrm{Re}(z) = r\} : r \in \mathbb{R}\}$.

Példa

- A síkon két egyenes legyen $\sim$ szerint relációban, ha párhuzamosak. Ekkor az osztályok az irány fogalomát adják.
- A síkon két szakasz legyen $\sim$ szerint relációban, ha egybevágóak. Ekkor az osztályok a hossz fogalomát adják.
- Két egész számpár esetén $(r, s) \sim (p, q)$ $(s, q \neq 0)$, ha $r \cdot q = p \cdot s$. Ekkor az osztályok a racionális számok halmaza.

Részbenrendezés, rendezés

Definíció

Az X halmazon értelmezett reflexív, tranzitív és antiszimmetrikus relációt részbenrendezésnek nevezzük. (Jele: $\leq$, $\preceq$ $\preccurlyeq$, ...)
Ha $x, y \in X$ esetén $x \preceq y$ vagy $y \preceq x$, akkor x és y összehasonlítható.
(Ha minden elempár összehasonlítható, akkor a reláció dichotóm.)
Az X halmazon értelmezett reflexív, tranzitív, antiszimmetrikus és dichotóm relációt rendezésnek nevezzük.

Ha egy részbenrendezés esetén bármely két elem összehasonlítható, akkor az rendezés.

Példa

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

Szigorú és gyenge reláció

Definíció

Az X-beli R relációhoz tartozó szigorú reláció, az az S reláció, melyre $xSy \iff xRy \wedge x \neq y$.
Az X-beli R relációhoz tartozó gyenge reláció, az a T reláció, melyre $xTy \iff xRy \vee x = y$.

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

Példa

- $\leq$ relációhoz tartozó szigorú reláció: $<$.
- $\subset$ relációhoz 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 nevezzük. (Jele: $<$, $\prec$, . . .)

Megjegyzések

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

Állítás

Ha a $\preceq$ reláció rendezés, akkor $\prec$ trichotóm, és fordítva.

Bizonyítás

Kell: $x = y$, $x \prec y$ és $y \prec x$ egyszerre nem teljesülhet. Ha $x = y$, akkor igaz az állítás. Továbbá $x \prec y$ és $y \prec x$ sem teljesülhet egyszerre.

Intervallumok

Definíció

Legyen X egy részbenrendezett halmaz. Ha $x \preceq z$ és $z \preceq y$, akkor azt mondjuk, hogy z az x és y közé esik, ha $x \prec z$ és $z \prec y$, akkor azt mondjuk, hogy z szigorúan az x és y közé esik. Az összes ilyen elem 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 $[\{a\}, \{a, b, c\}] = \big\{\{a\}, \{a, b\}, \{a, c\}, \{a, b, c\}\big\}$;
$(\{a\}, \{a, b, c\}) = \big\{\{a, b\}, \{a, c\}\big\}$.

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

Intervallumok

Definíció

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

Példa

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

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

Definíció

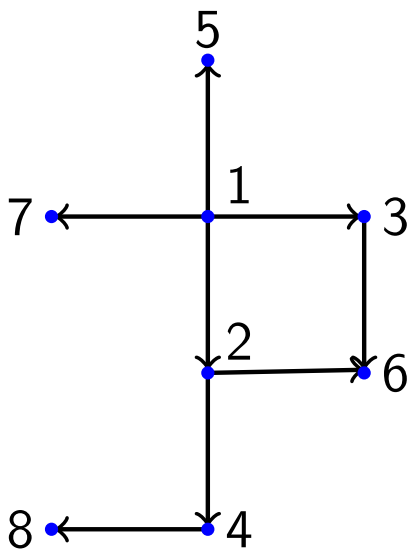
Az $\{y \in X : y < x\}$ részhalmazt az x elemhez tartozó kezdőszeletnek nevezzük.

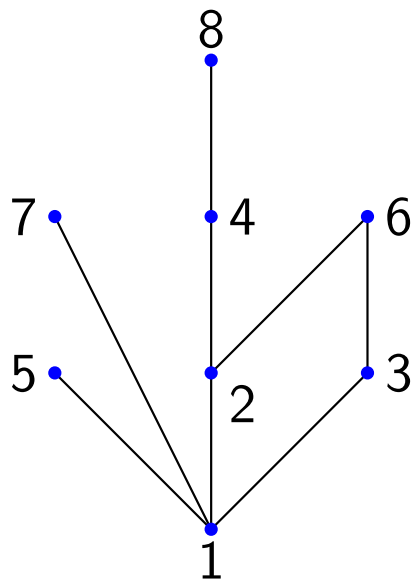
Példa

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

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 lejjebb.





Legkisebb, legnagyobb, minimális, maximális elem

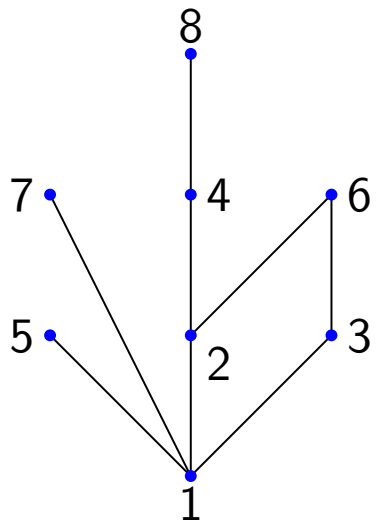
Definíció

Az X részbenrendezett halmaz
legkisebb eleme: olyan $x \in X : \forall y \in X,\ x \preceq y$;
legnagyobb eleme: olyan $x \in X : \forall y \in X,\ y \preceq x$;
minimális eleme: olyan $x \in X : \neg\exists y \in X, x \neq y,\ y \preceq x$;
maximális eleme: olyan $x \in X : \neg\exists y \in X, x \neq y,\ x \preceq y$.

Példa

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

legkisebb elem: 1,
legnagyobb elem: nincs,
minimális elem: 1,
maximális elemek: 5, 6, 7, 8.



Legkisebb, legnagyobb, minimális, maximális elem

Megjegyzések

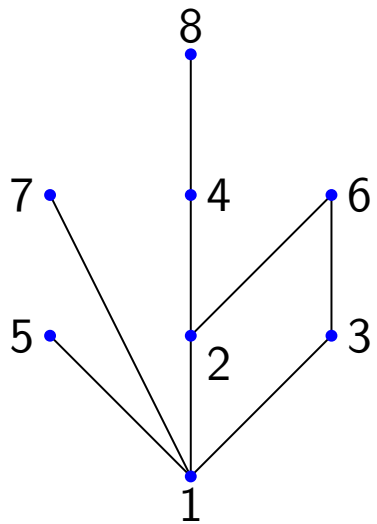
- Minimális és maximális elemből több is lehet.
- Ha a halmaz rendezett, akkor a minimális és legkisebb elem, továbbá a maximális és legnagyobb elem egybeesik.
- Ha X-nek létezik egyértelmű minimális, ill. maximális eleme, akkor azt $\min X$, ill. $\max X$ jelöli.

Példa

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

$\min X = 1$,

$\max X$ nincs.



Korlátok

Definíció

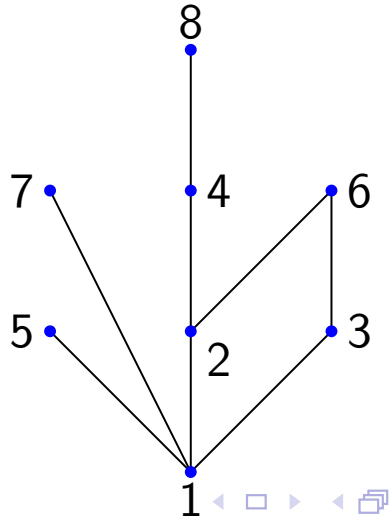
Egy X részbenrendezett halmaz x eleme az Y részhalmaz
alsó korlátja, ha $\forall y \in Y : x \preceq y$;
felső korlátja, ha $\forall y \in Y : y \preceq x$.
Ha az alsó korlátok halmazában van legnagyobb elem, akkor ez az Y infimuma: $\inf Y$, ha a felső korlátok halmazában van legkisebb elem, akkor ez az Y supremuma: $\sup Y$.

Példa

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

$\{1, 2, 3\}$ alsó korlátja: 1,
felső korlátja: 6,
infimuma: 1,
supremuma: 6.

$\{2, 3, 4\}$ alsó korlátja: 1,
felső korlátja: nincs,
infimuma: 1,
supremuma: nincs.



Korlátok

Definíció

Ha az X részbenrendezett 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

- A pozitív egész számok halmaza az oszthatóságra nézve alsó, és felső határ tulajdonságú:
  Ha $Y = \{a_1, a_2, \dots\}$, akkor $\inf Y = lnko(a_1, a_2, \dots)$, felső határa $lkkt(a_1, a_2, \dots)$.
- 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, ...), de nincs (racionális) supremuma (a supremum $\sqrt{2} \notin \mathbb{Q}$ lenne).

Diszkrét matematika I. középszint

4. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Függvények

Definíció

Egy f relációt függvénynek (leképezésnek, transzformációnak, hozzárendelésnek, operátornak) nevezünk, ha $(x, y) \in f \wedge (x, y') \in f \Rightarrow y = y'$. Az $(x, y) \in f$ jelölés helyett ilyenkor az $f(x) = y$ (vagy $f : x \mapsto y$, $f_x = y$) 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: $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$: $1, 1, 2, 3, 5, 8, \ldots$
  Ekkor az $F \subset \mathbb{N} \times \mathbb{N}$ reláció függvény, n helyen az értéke $F(n) = F_n$.

Függvények

Definíció

Az $f \subset X \times Y$ függvények halmazát $X \to Y$ jelöli. Ha $\mathrm{dmn}(f) = X$, akkor az $f : X \to Y$ jelölést használjuk.

Megjegyzés

Ha $f : X \to Y$, akkor $\mathrm{dmn}(f) = X$ és $\mathrm{rng}(f) \subset Y$.

Példa

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

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

Függvények

Definíció

Az $f : X \to Y$ függvény

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

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

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

Megjegyzés

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

Függvények

Definíció

Az $f : X \to X$ bijektív függvényt permutációnak nevezzük.

Példa

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

Függvények

Legyen $E_n \subset \mathbb{C}$ az n-edik egységgyökök halmaza: $E_n = \{z \in \mathbb{C} : z^n = 1\}$.
Rendnél szerepelt: $z^k = z^l \Leftrightarrow o(z) | k - l$.

Állítás

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

Bizonyítás

Ha $(n, k) = d > 1$, akkor f nem injektív: ha ε primitív n-edik egységgyök, akkor $f\left(\varepsilon^{n/d}\right) = f(1) = 1$, u.i. $\left(\varepsilon^{n/d}\right)^d = \varepsilon^n = 1$, de $\varepsilon^{n/d} \neq 1$.

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

Mivel $f : E_n \to E_n$ injektív, ezért E_n végessége miatt bijektív is. □

Függvények kompozíciója

Emlékeztető

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

Függvény 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 $f : X \to Y$, $g : Y \to Z$ szürjektívek, akkor $g \circ f : X \to Z$ is szürjektív.

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 függény $z = z'$, mivel g függvény $y = y'$.
2. Legyen $(g \circ f)(x) = (g \circ f)(x')$. Legyen $f(x) = y, f(x') = y'$, így $g(y) = g(y')$. Mivel g injektív: $y = y'$. Mivel f injektív: $x = x'$.
3. HF. □

Monoton függvények

Definíció

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

1. monoton növekedő, ha $x, y \in X$, $x \preceq y \Rightarrow f(x) \preceq f(y)$;
2. szigorúan monoton növekedő, ha $x, y \in X$, $x \prec y \Rightarrow f(x) \prec f(y)$;
3. monoton csökkenő, ha $x, y \in X$, $x \preceq y \Rightarrow f(x) \succeq f(y)$;
4. szigorúan monoton csökkenő, ha $x, y \in X$, $x \prec y \Rightarrow f(x) \succ f(y)$.

Példa

- Legyen $X = \mathbb{R}$ a szokásos rendezéssel. Ekkor az $f(x) = x$; $g(x) = x^3$ szigorúan monoton növekedő függvények.
- Legyen X az $\{a, b, c\}$ hatványhalmaza a részhalmaza részbenrendezéssel.
  Ekkor az $f(A) = A \setminus \{a\}$ monoton növekedő: $A \subset B \Rightarrow A \setminus \{a\} \subset B \setminus \{a\}$;
  A $g(A) = \overline{A}$ szigorúan monoton csökkenő: $A \subsetneq B \Rightarrow \overline{A} \supsetneq \overline{B}$.

Monoton függvények

Megjegyzés

- Ha X, Y rendezett halmazok, akkor egy szigorúan monoton növekedő (ill. csökkenő) függvény injektív is: Ha $x \neq y \Rightarrow x \prec y$ vagy $x \succ y \Rightarrow f(x) \prec f(y)$ vagy $f(x) \succ f(y) \Rightarrow f(x) \neq f(y)$.
- 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 $f(x) \prec f(y)$, akkor nem lehet $x \succeq y$.

Példa

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

Műveletek

Definíció

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

Példa

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

Műveletek

Egy véges halmazon bármely binér művelet megadható a műveleti táblájával.

$\wedge$	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 $*$ művelettel, $f, g : X \to Y$ függvények. Ekkor

$$(f * g)(x) = f(x) * g(x).$$

Példa

$(\sin + \cos)(x) = \sin x + \cos x$

Műveleti tulajdonságok

Definíció

A $* : X \times X \to X$ művelet
asszociatív, ha $\forall a, b, c \in X : (a * b) * c = a * (b * c)$;
kommutatív, ha $\forall a, b \in X : a * b = b * a$.

Példa

- $\mathbb{C}$-n az $+$ ill. a $\cdot$ műveletek asszociatívak, kommutatívak.
- A függvények halmazán a kompozíció művelete asszociatív:
  $(f \circ g) \circ h = f \circ (g \circ h)$.
- A függvények halmazán a kompozíció művelete 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: $\frac{a}{bc} = (a \div b) \div c \neq a \div (b \div c) = \frac{ac}{b}$.

Művelettartó leképezések

Definíció

Legyen X halmaz a $*$ művelettel, Y a $\circ$ művelettel. Az $f : X \to Y$ függvény művelettartó, ha $\forall x, y \in X$ esetén

$$f(x * y) = f(x) \circ f(y).$$

Példa

- Legyen $X = \mathbb{R}$ az $+$ művelettel, $Y = \mathbb{R}^+$ a $\cdot$ művelettel. Ekkor az $x \mapsto a^x$ művelettartó: $a^{x+y} = a^x \cdot a^y$.
- Legyen $X = Y = \mathbb{C}$ az $+$ művelettel. Ekkor a $z \mapsto \overline{z}$ művelettartó: $\overline{z + w} = \overline{z} + \overline{w}$.

Diszkrét matematika I. középszint

5. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Számfogalom bővítése

A természetes számokból kiindulva megkonstruálhatók a

- 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...

Természetes számok

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 $\mathbb{N}$-et.
- Mindegyik axióma szükséges.
- $\mathbb{N}$ halmaz megkonstruálható: $0 := \emptyset$, $0^+ := \{\emptyset\}$, $(0^+)^+ := \{\emptyset, \{\emptyset\}\}$,...
- $1 := 0^+$, $2 := 1^+$, ...

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

1. $(k+m)+n = k+(m+n)$ (asszociativitás);
2. $k+m = m+k$ (kommutativitás);
3. $0+n = n+0 = n$ (van nullelem/egységelem/semleges elem).

Félcsoportok

Definíció

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

Példa

- $\mathbb{N}$ az $+$ művelettel egységelemes félcsoport $n = 0$ egységelemmel.
- $\mathbb{Q}$ a $\cdot$ művelettel egységelemes félcsoport $n = 1$ egységelemmel.
- $\mathbb{C}^{k \times k}$ a mátrixszorzással egységelemes félcsoport az egységmátrixszal, mint egységelemmel.

Egész számok

Az $\mathbb{N}$ halmazon nem (mindig) 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 $*$ művelettel és n egységelemmel. A $g \in G$ elem inverze (ellentettje) a $g^{-1} \in G$ elem, melyre $g * g^{-1} = g^{-1} * g = n$.
Ha minden $g \in G$ elemnek létezik inverze, akkor G csoport. Ha $*$ 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: az $(r, s) \sim (p, q)$, ha $r + q = p + s$ ekvivalenciareláció osztályai az egész számok.

Csoportok

További példák csoportokra:

- $\mathbb{Q}$ az $+$ művelettel, a 0 egységelemmel.
- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ a $\cdot$ művelettel, az 1 egységelemmel.
- $\{M \in \mathbb{C}^{k \times k} : \det M \neq 0\}$ a mátrixszorzással, és az egységmátrixszal, mint egységelemmel.
- $X \to X$ bijektív függvények a $\circ$ művelettel, és az $id_X : x \mapsto x$ identikus leképzéssel, mint egységelemmel.

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 $n \cdot m = -\big((-n) \cdot m\big)$.

Állítás

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

A két művelet nem ,,független'':

Állítás

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

Gyűrűk

Definíció

Legyen R egy halmaz két binér művelettel: $*$, $\circ$. Ekkor az R gyűrű, ha

- R a $*$ művelettel Abel-csoport (0-val, mint egységelemmel);
- R a $\circ$ művelettel félcsoport;
- a $\circ$ a $*$-ra nézve disztributív:
  $r \circ (s * t) = (r \circ s) * (r \circ t)$; $\quad (s * t) \circ r = (s \circ r) * (t \circ r)$.

Az R egységelemes gyűrű, ha R-en a $\circ$ műveletre nézve van egységelem.
Az R kommutatív gyűrű, ha a $\circ$ művelet (is) kommutatív.

Példa

- $\mathbb{Z}$ az $(+, \cdot)$ 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 gyűrű, de nem kommutatív.

Nullosztómentes gyűrűk

A gyűrűkben általában nem lehet elvégezni az osztást:

- $\mathbb{Z}$-ben nem oldható meg a $2x = 1$ egyenlet.
- $\mathbb{R}^{2\times 2}$-ben nem oldható meg az alábbi egyenlet

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Definíció

Ha egy $(R, *, \circ)$ gyűrűben $\forall r, s \in R,\ r, s \neq 0$ esetén $r \circ s \neq 0$, akkor R nullosztómentes gyűrű.

Példa

Nem nullosztómentes gyűrű

- $\mathbb{R}^{2\times 2}$: $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Testek

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

Definíció

Legyen K egy halmaz, azon két művelet: $*$, $\circ$. A K ferdetest, ha

- K gyűrű;
- $K^* = K \setminus \{0\}$ a $\circ$ 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 $\mathbb{Z}$ segítségével: az $(r, s) \sim (p, q)$ $(s, q \neq 0)$, ha $r \cdot q = p \cdot s$ ekvivalenciareláció osztályai a racionális számok.

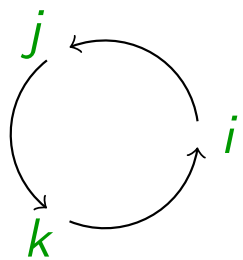
Testek

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 $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, ... Nemkommutatív ferdetest!



Számok és rendezés

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

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

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.

Rendezett testek

A $\mathbb{Z}$-n definiált rendezés kiterjeszthető $\mathbb{Q}$-ra: $\frac{p}{q} < \frac{r}{s}$, ha $ps < rq$.

A kiterjesztés azonban nem lesz ,,teljes", $\mathbb{Q}$ nem lesz felső határ tulajdonságú.

Emlékeztető

Egy X halmaz felső határ tulajdonságú, ha minden $\emptyset \neq Y \subset X$ felülről korlátos részhalmaznak van supremuma.

Állítás

$\sqrt{2} \notin \mathbb{Q}$.

Speciálisan $\mathbb{Q}$ nem felső határ tulajdonságú: $\{r \in \mathbb{Q} : r \leq \sqrt{2}\}$ felülről korlátos, de nincs supremuma ($\sup = \sqrt{2} \notin \mathbb{Q}$).

Bizonyítás

Indirekt tfh $\exists n, m \in \mathbb{N}^+$: $(m/n)^2 = 2$. Válasszuk azt az m, n párt, ahol $(m, n) = 1$. Most $m^2 = 2n^2 \Rightarrow 2 \mid m$. Legyen $m = 2k \Rightarrow$ $m^2 = 4k^2 = 2n^2 \Rightarrow 2 \mid n \Rightarrow (m, n) \geq 2$. □

Valós számok

Valós számok axiómája

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

Megjegyzés

- 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;
- $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$;
- $\mathbb{Q} = \{r/s \in \mathbb{R} : r, s \in \mathbb{Z}, s \neq 0\}$.

Összefoglaló

Műveletek halmazokon

Struktúra	Példa
Peano axiómák	$\mathbb{N}$
félcsoport: van asszociatív művelet	$(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$
csoport: van inverz	$(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Z}_m, +)$, $(\mathbb{Z}_p^*, \cdot)$
gyűrű: két művelet,	$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$,
$*$-ra kommutatív csoport,	$(\mathbb{R}^{k\times k}, +, \cdot)$
$\circ$-re félcsoport, disztributivitás	
ferdetest: két művelet,	$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{Z}_p$
$*$-ra kommutatív csoport,	
$\circ$-re a 0 kivételével csoport,	
disztributivitás	

Összefoglaló

Műveletek és rendezés

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

Diszkrét matematika I. középszint

6. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Felhívás 1.

Vasárnap lesz az ACM országos programozási verseny.
Bővebb információ:

http://people.inf.elte.hu/bzsr/acm/

Felhívás 2.

Csütörtökön Körtvélyessy Gábor (Vision-Software Kft) tart előadást.
A szakterületének érdekes kérdéseit, eredményeit mutatja be a hallgatóságnak.
Bővebb információ:

http://goo.gl/zJqyFL

A logikai műveletek tulajdonságai, ítéletlogikai tételek

Állítás

1. $(A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C)$, $(A \wedge (B \wedge C)) \Leftrightarrow ((A \wedge B) \wedge C)$ (asszociativitás);
2. $(A \vee B) \Leftrightarrow (B \vee A)$, $(A \wedge B) \Leftrightarrow (B \wedge A)$ (kommutativitás);
3. $(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$, $(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$ (disztributivitás);
4. $(\neg(A \vee B)) \Leftrightarrow (\neg A \wedge \neg B)$, $(\neg(A \wedge B)) \Leftrightarrow (\neg A \vee \neg B)$ (De Morgan);
5. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$ (a kontrapozíció tétele);
6. $((A \Rightarrow B) \wedge A) \Rightarrow B$;
7. $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ (szillogizmus);
8. $((A \Rightarrow B) \wedge (B \Rightarrow A)) \Leftrightarrow (A \Leftrightarrow B)$.

A logikai műveletek tulajdonságai, ítéletlogikai tételek

Bizonyítás (példa)

1. $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$ (a logikai vagy asszociativitása)

A	B	C	$B \vee C$	$A \vee (B \vee C)$	$A \vee B$	$(A \vee B) \vee C$	$(A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C)$
I	I	I	I	I	I	I	I
I	H	I	I	I	I	I	I
H	I	I	I	I	I	I	I
H	H	I	I	I	H	I	I
I	I	H	I	I	I	I	I
I	H	H	H	I	I	I	I
H	I	H	I	I	I	I	I
H	H	H	H	H	H	H	I

Áttérés algebrai alakról trigonometrikus alakra

$$a + bi = r(\cos\varphi + i\sin\varphi)$$

Áttérés algebrai alakról trigonometrikus alakra

$$a + bi = r(\cos\varphi + i\sin\varphi)$$

$$\left.\begin{aligned} a &= r\cos\varphi \\ b &= r\sin\varphi \end{aligned}\right\}$$

Áttérés algebrai alakról trigonometrikus alakra

$$a + bi = r(\cos\varphi + i\sin\varphi)$$

$$\left.\begin{aligned} a &= r\cos\varphi \\ b &= r\sin\varphi \end{aligned}\right\}$$

Ha $a \neq 0$, akkor $\operatorname{tg}\varphi = \frac{b}{a}$, és így

Áttérés algebrai alakról trigonometrikus alakra

$$a + bi = r(\cos\varphi + i\sin\varphi)$$

$$\left.\begin{array}{l} a = r\cos\varphi \\ b = r\sin\varphi \end{array}\right\}$$

Ha $a \neq 0$, akkor $\mathrm{tg}\varphi = \frac{b}{a}$, és így

$$\varphi = \begin{cases} \mathrm{arctg}\frac{b}{a}, \text{ ha } a > 0; \\ \\ \mathrm{arctg}\frac{b}{a} + \pi, \text{ ha } a < 0. \end{cases}$$

Diszkrét matematika I. középszint

7. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Kombinatorika

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:
$\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$, $\mathcal{B} = \{b_1, b_2, \ldots, b_m\}$.

Hányféleképpen tudunk választani egy elemet $\mathcal{A}$-ból vagy $\mathcal{B}$-ből?

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

Számuk: $n + m$.

Példa

Egy cukrászdában 3-féle édes sütemény (isler, zserbó, kókuszkocka) és 2-féle sós sütemény (pogácsa, perec) van. Hányféleképpen tudunk egy édes vagy egy sós sütemény enni? Megoldás: $3 + 2 = 5$.

Elemi leszámlálások

Adott két véges, diszjunkt halmaz:
$\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$, $\mathcal{B} = \{b_1, b_2, \ldots, b_m\}$.

Hányféleképpen tudunk választani elemet $\mathcal{A}$-ból és $\mathcal{B}$-ből?

Lehetséges választások:

	b_1	b_2	$\ldots$	b_m
a_1	(a_1, b_1)	(a_1, b_2)	$\ldots$	(a_1, b_m)
a_2	(a_2, b_1)	(a_2, b_2)	$\ldots$	(a_2, b_m)
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	(a_n, b_1)	(a_n, b_2)	$\ldots$	(a_n, b_m)

Számuk: $n \cdot m$.

Példa

Egy cukrászdában 3-féle édes sütemény (isler, zserbó, kókuszkocka) és 2-féle sós sütemény (pogácsa, perec) van. Hányféleképpen tudunk egy édes és egy sós sütemény enni? Megoldás: $3 \cdot 2 = 6$.

Permutáció

Tétel

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

Példa

Reggelire a
2 különböző szendvicset $2! = 2\cdot 1 = 2$ -féle sorrendben lehet megenni.
3 különböző szendvicset $3! = 3\cdot 2\cdot 1 = 6$-féle sorrendben lehet megenni.
4 különböző szendvicset $4! = 4\cdot 3\cdot 2\cdot 1 = 24$-féle sorrendben lehet megenni.

A 200 fős évfolyam $200! = 200\cdot 199\cdot 198\cdot\ldots\cdot 2\cdot 1 \approx 7,89\cdot 10^{374}$-féle sorrendben írhatja alá a jelenléti ívet.

Bizonyítás

Az n elemből az első helyre n-féleképpen választhatunk, a második helyre $n-1$-féleképpen választhatunk, ...
Így az össze lehetőségek száma $n(n-1)\cdot\ldots\cdot 2\cdot 1$. □

Ismétléses permutáció

Példa

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

Megoldás

Ha figyelembe vesszük a hallgatókat is: $(2+3)! = 5!$ lehetséges sorrend van.

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.

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

Ismétléses permutáció

Tétel

k_1 darab első típusú, k_2 második típusú, ..., k_m m-edik típusú elem lehetséges sorrendjét az elemek ismétléses permutációinak nevezzük, és számuk $n = k_1 + k_2 + \ldots + k_m$ esetén

$$^{i}P_n^{k_1,k_2,\ldots,k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_m!}.$$

Bizonyítás

Ha minden elem között különbséget teszünk: $(k_1 + k_2 + \ldots + k_m)!$ 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 $k_1! \cdot k_2! \cdot \ldots \cdot k_m!$ egyforma van. Így ekkor a lehetséges sorrendek száma: $\frac{(k_1 + k_2 + \ldots + k_m)!}{k_1! \cdot k_2! \cdot \ldots \cdot k_m!}$. □

Variáció

Példa

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

Megoldás

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

Tétel

Adott egy n elemű $\mathcal{A}$ halmaz. Ekkor k elemet $V_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = n!/(n-k)!$-féleképpen választhatunk ki.

Bizonyítás

Az $\mathcal{A}$ halmazból először n-féleképpen választhatunk, második esetben $(n-1)$, $\ldots$, k-adik esetben $n-k+1$-féleképpen választhatunk. □

Ismétléses variáció

Példa

A 0, 1, 2 számjegyekből hány legfeljebb kétjegyű szám képezhető?

Megoldás

Az első helyiértékre 3-féleképpen írhatunk számjegyet:

$$\begin{array}{l} \textvisiblespace 0 \\ \textvisiblespace 1 \\ \textvisiblespace 2 \end{array}$$

A második helyiértékre szintén 3-féleképpen írhatunk számjegyet:

$$\begin{array}{lll} 00 & 10 & 20 \\ 01 & 11 & 21 \\ 02 & 12 & 22 \end{array}$$

Összesen:

$$\begin{array}{l} \textvisiblespace\ \textvisiblespace \\ 3 \cdot 3 \quad = 9 \end{array}$$

Ismétléses variáció

Tétel

Egy n elemű $\mathcal{A}$ halmaz elemeiből ${}^{i}V_n^k = n^k$ darab k hosszú sorozat készíthető.

Bizonyítás

A sorozat első elemét n-féleképpen választhatjuk, a második elemét n-féleképpen választhatjuk, ... □

Példa

Egy totószelvényt ($13+1$ helyre 1, 2 vagy x kerülhet) $3^{14} = 4\,782\,969$-féleképpen lehet kitölteni.

Mennyi egy n elemű halmaz összes részhalmazainak száma?
Legyen $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$. Ekkor minden részhalmaz megfelel egy n hosszú $0-1$ sorozatnak: ha a sorozat i-edik eleme 1, akkor a_i benne van a részhalmazban.
$\varnothing \leftrightarrow (0,0,\ldots,0)$, $\{a_1, a_3\} \leftrightarrow (1,0,1,0,\ldots,0)$, ..., $\mathcal{A} \leftrightarrow (1,1,\ldots,1)$
Hány n hosszú $0-1$ sorozat van: 2^n.

Kombináció

Tétel

Egy n elemű $\mathcal{A}$ halmaznak a k elemű részhalmazainak száma

$$C_n^k = \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Bizonyítás

Először válasszunk $\mathcal{A}$ elemei közül k darabot a sorrendet figyelembevéve. Ezt $n(n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$-féleképpen tehetjük meg.
Ha a sorrendtől eltekintünk, akkor az előző leszámlálásnál minden k elemű részhalmaz pontosan $k!$-szor szerepel. Ezzel leosztva kapjuk a k elemű részhalmazok számát. □

Példa

Egy lottószelvény (90 számból 5) lehetséges kitöltéseinek száma:

$$\binom{90}{5} = \frac{90!}{5! \cdot 85!} = \frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 43\,949\,268.$$

Ismétléses kombináció

Tétel

Egy n elemű $\mathcal{A}$ halmaz elemeiből ha k-szor választhatunk úgy, hogy egy elemet többször is választhatunk, akkor a lehetséges választások száma

$$^{i}C_n^k = \binom{n+k-1}{k}.$$

Bizonyítás

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

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

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-t választunk. Ilyen sorozat $\binom{n+k-1}{k}$ darab van. □

Ismétléses kombináció

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:

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

Összefoglaló

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

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

Ismétlés nélküli variáció $n!/(n-k)!$, n elemből k-t 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-t 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

$$(x+y)^n = (x+y) \cdot (x+y) \cdot \ldots \cdot (x+y)$$

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

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

Binomiális együttható

Tétel

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

Bizonyítás

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

1. Az n hosszú $0-1$ sorozatok közül azok száma, melyek k darab 1-est tartalmaznak megegyezik azok számával, melyek $n-k$ darab 1-est tartalmaznak.
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

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

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?

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

Tétel

r, $n \in \mathbb{N}$ esetén

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

Bizonyítás

$(x_1+x_2+\ldots+x_r)^n =$
$(x_1+x_2+\ldots+x_r)(x_1+x_2+\ldots+x_r)\cdots(x_1+x_2+\ldots+x_r).$
Az $x_1^{i_1}x_2^{i_2}\ldots x_r^{i_r}$ együtthatója:

$$\binom{n}{i_1}\binom{n-i_1}{i_2}\binom{n-i_1-i_2}{i_3}\cdots\binom{n-i_1-i_2-\ldots-i_{r-1}}{i_r} =$$

$$\frac{n!}{i_1!(n-i_1)!}\frac{(n-i_1)!}{i_2!(n-i_1-i_2)!}\cdots\frac{(n-i_1-i_2-\ldots-i_{r-1})!}{i_r!(n-i_1-\ldots-i_{r-1}-i_r)!} = \frac{n!}{i_1!\cdot i_2!\cdots i_r!}$$

□

Polinomiális tétel

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

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

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

Skatulya-elv

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

Példa

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

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

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

Szita módszer

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

Az 1000-nél kisebb számok

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

Szita módszer

Tétel

Legyenek A_1, A_2, ..., A_n véges halmazok. Ekkor

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

Példa

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

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

$A_1 = \{1 \le n \le 999 : 2|n\} \to |A_1| = \left\lfloor \frac{999}{2} \right\rfloor$;

$A_2 = \{1 \le n \le 999 : 3|n\} \to |A_2| = \left\lfloor \frac{999}{3} \right\rfloor$;

$A_3 = \{1 \le n \le 999 : 5|n\} \to |A_3| = \left\lfloor \frac{999}{5} \right\rfloor$.

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:

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

Általános szita formula

Tétel

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

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

$$S_r = \sum_{0<i_1<i_2<\ldots<i_r \le n} \; \sum_{x \in A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}} f(x);$$

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

Ekkor $S_0 = S - S_1 + S_2 - S_3 \pm \ldots (-1)^n S_n$.

Példa

$A = \{1, 2, \ldots, 999\}$, $A_1 = \{n : \ 1 \le n < 1000, 2 \mid n\}$,
$A_2 = \{n : \ 1 \le n < 1000, 3 \mid n\}$, $A_3 = \{n : \ 1 \le n < 1000, 5 \mid n\}$,
$f(x) = 1$.
S_0: 2-vel, 3-mal, 5-tel nem osztható 1000-nél kisebb számok száma.

Általános szita formula bizonyítása

$S_0 = S - S_1 + S_2 - S_3 \pm \ldots (-1)^n S_n$:

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

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

Bizonyítás

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

$$\sum_{0<i_1<i_2<\cdots<i_r \leq n} \; \sum_{x \in A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_r}} f(x)$$

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

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

Diszkrét matematika I. középszint

8. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Oszthatóság

Ha a és b racionális számok ($b \neq 0$), akkor az a/b osztás mindig elvégezhető (és az eredmény szintén racionális).

Ha a és b egész számok, az a/b osztás nem mindig végezhető el (a hányados nem feltétlenül lesz egész).

Definíció

Az a egész osztja a b egészet (b osztható a-val): $a \mid b$, ha létezik olyan c egész, mellyel $a \cdot c = b$ (azaz $a \neq 0$ esetén b/a szintén egész).

Példák

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

A definíció kiterjeszthető például a Gauss-egészekre: $\{a + bi : \ a, b \in \mathbb{Z}\}$.

Példák

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

Oszthatóság tulajdonságai

Állítás (HF)

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

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

Példák

1. $6 \mid 6$;
2. $2 \mid 6$ és $6 \mid 12 \Rightarrow 2 \mid 12$;
3. $a \mid 3$ és $3 \mid a \Rightarrow a = \pm 3$;
4. $2 \mid 4$ és $3 \mid 9 \Rightarrow 2 \cdot 3 \mid 4 \cdot 9$;
5. $3 \mid 6 \Rightarrow 5 \cdot 3 \mid 5 \cdot 6$;
6. $3 \cdot 5 \mid 6 \cdot 5$ és $5 \neq 0 \Rightarrow 3 \mid 6$;
7. $3 \mid 6, 9 \Rightarrow 3 \mid 6c_1 + 9c_2$

Egységek

Definíció

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

Állítás

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

Bizonyítás

A ± 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: $a + bi = i(b - ai)$.

Megjegyzés

Pontosan 1 osztói az egységek.

Asszociáltak

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 $a \mid b$ és $b \mid a$.

Definíció

Egy számnak az asszociáltjai és az egységek a triviális osztói.

Prímek, felbonthatatlanok

Definíció

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

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

Definíció

Egy nem-nulla, nem egység p számot prímszámnak nevezünk, ha $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.

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

Prímek, felbonthatatlanok

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

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

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

Maradékos osztás

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:
$q = \lfloor a/b \rfloor$, ha $b > 0$, és $q = \lceil a/b \rceil$, ha $b < 0$.

Példa

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

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 116 óra múlva?
   Osszuk el maradékosan 116-ot 24-gyel: $116 = 24 \cdot 4 + 20$. Tehát $9 + 20 = 29$. Újabb redukció: $29 = 24 \cdot 1 + 5$: hajnali 5 óra lesz!
3. Milyen napra fog esni jövőre november 11-e?
   Milyen napra esett három éve november 15-e?

hétfő $\mapsto$ 0
kedd $\mapsto$ 1
szerda $\mapsto$ 2
csütörtök $\mapsto$ 3
péntek $\mapsto$ 4
szombat $\mapsto$ 5
vasárnap $\mapsto$ 6

Osszuk el maradékosan 365-öt 7-tel: $365 = 7 \cdot 52 + 1$.
kedd + 1 nap $\leftrightarrow$ 1+1=2$\leftrightarrow$ szerda

Osszuk el maradékosan -(365+365+366)-ot (2012. szökőév) 7-tel: $-1096 = 7 \cdot (-157) + 3$.

szombat + 3 nap $\leftrightarrow 5 + 3 = 8 \overset{\text{redukció}}{=} 1 \leftrightarrow$ kedd

Számrendszerek

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

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.
- $a_0, \ldots, a_k$ az n jegyei.
- $k = \lfloor \log_q n \rfloor$.

Számrendszerek

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

Bizonyítás

A tételt indukcióval bizonyítjuk.

1. $n = 0$ esetén a tétel igaz.
2. Tfh minden n-nél kisebb számot fel tudunk írni egyértelműen q alapú számrendszerben. A maradékos osztás tétele alapján létezik egyértelműen $0 \leq a_0 < q$ egész, hogy $q \mid n - a_0$. 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 $n = \sum_{i=0}^{k} a_i q^i$. □

Számrendszerek

Az előbbi bizonyítás módszert is ad a felírásra:

Példa

Írjuk 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	$\frac{3-1}{2}$	110011
6	1	1	$\frac{1-1}{2}$	1110011

Legnagyobb közös osztó

Definíció

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

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 $(a, b) = lnko(a, b)$ a nemnegatív kitüntetett közös osztó!

Definíció

Az a és b számoknak az m szám kitüntetett közös többszöröse (legkisebb közös többszöröse), ha : $a \mid m$, $b \mid m$, és $a \mid c$, $b \mid c \Rightarrow m \mid c$.
Legyen $[a, b] = lkkt(a, b)$ a nemnegatív kitüntetett közös többszörös!

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

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.
Tfh a, b nem-nulla számok. Végezzük el a következő osztásokat:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|,\\
b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

Ekkor az lnko az utolsó nem-nulla maradék: $(a, b) = r_n$.
Itt $a = r_{-1}$, $b = r_0$.

Euklideszi algoritmus helyessége

Bizonyítás (folyt.)

$$
\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|,\\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}
$$

Az algoritmus véges sok lépésben véget ér: $|b| > r_1 > r_2 > \dots$.
Az r_n maradék közös osztó: $r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2} \Rightarrow \dots \Rightarrow$
$\Rightarrow r_n \mid b \Rightarrow r_n \mid a$.
Az r_n maradék a legnagyobb közös osztó: legyen $c \mid a$, $c \mid b \Rightarrow$
$c \mid a - bq_1 = r_1 \Rightarrow c \mid b - r_1 q_2 = r_2 \Rightarrow \dots \Rightarrow c \mid r_{n-2} - r_{n-1}q_n = r_n$. $\square$

Legnagyobb közös osztó kiszámolása, euklideszi algoritmus

Példa

Számítsuk ki $(172, 62)$ értékét!

i	r_i	q_i	$r_{i-2} = r_{i-1}q_i + r_i$
-1	172	–	–
0	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 tétel nyilvánvaló. Mivel $(a, b) = (|a|, |b|)$, feltehető, hogy a, $b > 0$. 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)	$a \bmod \lvert b \rvert$
$(172, 62)$	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): $(a_1, a_2, \ldots, a_n)$.

Állítás (HF)

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

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

Bővitett euklideszi algoritmus

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

Példa

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

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

Diszkrét matematika I. középszint

9. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Felbonthatatlanok, prímek

Emlékeztető: f felbonthatatlan: csak triviális osztói vannak: ε, f, $\varepsilon \cdot f$ típusú osztók (ahol ε egy egység).
p prím: $p \mid ab \Rightarrow p \mid a$ vagy $p \mid b$.
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 $p \mid ab$. Tfh. $p \nmid b$. 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 bal oldalnak, így osztója a jobb oldalnak is: $p \mid a$. □

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 nemtriviális módon. A tényezők már felbonthatók indukció alapján.

Egyértelműség: Indukcióval: $n = 2$, $n = 3$ esetén igaz (prímek). Tfh. $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$, ahol $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_\ell$ prímek, és n a legkisebb olyan szám, aminek két lényegesen különböző előállítása van. p_1 osztja a bal oldalt $\Rightarrow$ osztja a jobb oldalt, feltehető $p_1 = q_1$. Egyszerűsítve: $n' = p_2 \cdots p_k = q_2 \cdots q_\ell$. Indukció alapján ez már egyértelmű. $\square$

Számelmélet alaptétele

Definíció

Egy n nem-nulla egész szám kanonikus alakja:

$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} = \pm \prod_{i=1}^{\ell} p_i^{\alpha_i}$, ahol p_1, p_2,..., p_ℓ pozitív prímek, α_1, α_2,..., α_ℓ pozitív egészek.

Következmény (HF)

Legyenek a, $b > 1$ pozitív egészek: $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}$, (ahol most α_i, $\beta_i \geq 0$ nemnegatív egészek!).
Ekkor

$(a, b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_\ell^{\min\{\alpha_\ell,\beta_\ell\}}$,

$[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_\ell^{\max\{\alpha_\ell,\beta_\ell\}}$,

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

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, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$ kanonikus alakkal. Ekkor $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_\ell + 1)$.

Bizonyítás

n lehetséges osztóit úgy kapjuk, hogy a $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}$ kifejezésben az összes β_i kitevő végigfut a $\{0, 1, \ldots, \alpha_i\}$ halmazon. Így ez a kitevő $\alpha_i + 1$-féleképpen választható. □

Példa

$\tau(2 \cdot 3) = (1 + 1) \cdot (1 + 1) = 4$; $\tau(2^5 \cdot 3) = (5 + 1) \cdot (1 + 1) = 12$.

Prímekről

Tétel (Euklidesz)

Végtelen sok prím van.

Bizonyítás

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

Tétel (Dirichlet, NB)

Ha a, d egész számok, $d > 0$, $(a, d) = 1$, akkor végtelen sok $ak + d$ alakú $(k \in \mathbb{Z})$ prím van.

Prímekről

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

Prímek száma:

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

Eratoszthenész 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 (ki nem húzott) szám 3 szintén prím. A 3 (valódi) többszörösei nem prímek, ezeket húzzuk ki...

Ismételjük az eljárást $\sqrt{n}$-ig. A ki nem húzott számok mind prímek.

Kongruenciák

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

- hét napjai;
- órák száma.

Példa

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

Definíció

Legyenek a, b, m egészek, ekkor $a \equiv b \pmod{m}$ (a és b kongruensek modulo m), ha $m \mid a - b$, 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 ugyanazt az osztási maradékot adják.

Példa

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

Kongruencia tulajdonságai

Tétel

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

1. $a \equiv a \pmod{m}$;
2. $a \equiv b \pmod{m}$, $m' \mid m \Rightarrow a \equiv b \pmod{m'}$;
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. $m \mid 0 = a - a$;
2. $m' \mid m \mid a - b \Rightarrow m' \mid a - b$;
3. $m \mid a - b \Rightarrow m \mid b - a = -(a - b)$;
4. $m \mid a - b$, $m \mid b - c \Rightarrow m \mid a - c = (a - b) + (b - c)$;
5. $m \mid a - b$, $m \mid c - d \Rightarrow m \mid (a + c) - (b + d) = (a - b) + (c - d)$;
6. $a = q_1 m + b$, $c = q_2 m + d$ $(q_1, q_2 \in \mathbb{Z}) \Rightarrow$
   $\Rightarrow ac = (q_1 m + b)(q_2 m + d) = m(q_1 q_2 m + q_1 d + q_2 b) + bd$. □

Kongruencia tulajdonságai

Példa

Mi lesz $345 \bmod 7 = ?$

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

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

$14 \equiv 6 \pmod 8 \Rightarrow 42 \equiv 18 \pmod 8$

A másik irány nem igaz!

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

Kongruencia tulajdonságai

Tétel

Legyenek a, b, c, m egész számok. Ekkor

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

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

Példa

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

Bizonyítás

Legyen $d = (c, m)$. Ekkor

$ac \equiv bc \pmod{m} \Leftrightarrow m \mid c(a-b) \Leftrightarrow \frac{m}{d} \left| \frac{c}{d}(a-b) \right.$. Mivel $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$,

ezért $\frac{m}{d} \left| \frac{c}{d}(a-b) \right. \Leftrightarrow \frac{m}{d} \left| (a-b) \right. \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$. □

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 a megoldást a $\{0, 1, \ldots, 6\}$ 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: $\{6 + 7\ell : \ \ell \in \mathbb{Z}\}$.

Van-e jobb módszer?
Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruencát! Kell-e 211 próbálkozás?

Lineáris kongruenciák

Tétel

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

Bizonyítás

$ax \equiv b \pmod{m} \Leftrightarrow ax + my = b$ valamely y egészre.
Mivel $(a, m) \mid a, m \Rightarrow (a, m) \mid ax + my = b$.
Ha $d = (a, m) \mid b$ legyen $a' = a/d$, $b' = b/d$, $m' = m/d$: $a'x + m'y = b'$
Mivel $(a', m') = 1$ bővített euklideszi algoritmussal kiszámolható x_0, y_0 együttható, hogy $a'x_0 + m'y_0 = 1 \Rightarrow a'(b'x_0) + m'(b'y_0) = b'$, 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:
$a'(x - x_1) = m'(y_1 - y) \Rightarrow m' \mid x - x_1 \Rightarrow x = x_1 + m'k$:
$k = 0, 1, \ldots, d - 1$. Ezek megoldások $y = y_1 - ka'$ választással. □

Lineáris kongruenciák

1. $ax \equiv b \pmod{m} \Leftrightarrow ax + my = b$.
2. Oldjuk meg az $ax + my = (a, m)$ egyenletet (bővített euklideszi algoritmus)!
2. Ha $(a, m) \mid b \Leftrightarrow$ van megoldás.
4. Megoldások: $x_i = \frac{b}{(a,m)}x + k\frac{m}{(a,m)}$: $k = 0, 1, \ldots, (a, m) - 1$.

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

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: $r_{i-2} = r_{i-1}q_i + r_i$,
$x_{-1} = 1$, $x_0 = 0$,
$x_i = x_{i-2} - q_i x_{i-1}$.

Lnko: $(23, 211) = 1 \mid 4 \Rightarrow$
Egy megoldás: $x_0 = 4(-55) \equiv 202 \pmod{211}$.

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

Ezek megoldások: $23 \cdot (202 + 211\ell) - 4 = 4642 + 211\ell = (22 + \ell) \cdot 211$

Lineáris kongruenciák

Példa

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

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

Algoritmus: $r_{i-2} = r_{i-1}q_i + r_i$,
$x_{-1} = 1$, $x_0 = 0$,
$x_i = x_{i-2} - q_i x_{i-1}$

Lnko: $(10, 22) = 2 \mid 8 \Rightarrow$
Két inkongruens megoldás:
$x_1 = 4(-2) \equiv 14 \pmod{22}$
$x_2 = 4(-2) + \frac{22}{2} \equiv 14 + 11 \equiv 3 \pmod{22}$.

Összes megoldás: $\{14 + 22\ell : \ \ell \in \mathbb{Z}\} \bigcup \{3 + 22\ell : \ \ell \in \mathbb{Z}\}$.

Ezek megoldások: $x_1 = 14$: $10 \cdot 14 - 8 = 132 = 6 \cdot 22$,
$x_2 = 3$: $10 \cdot 3 - 8 = 22 = 1 \cdot 22$.

Diszkrét matematika I. középszint

10. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Felhívás

Szakirányválasztó fórum december 4-én.
Jelentkezés november 26-ig:
http://goo.gl/forms/dYIHA8SQOZ

Bővebb információ:
http://compalg.inf.elte.hu/∼nagy

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 $(a, b) \mid c$, és ekkor a megoldások megkaphatók a bővített euklideszi algoritmussal.

További diofantikus egyenletek:
$x^2 + y^2 = -4$: nincs valós megoldás.

$x^2 - 4y^2 = 3$: nincs megoldás, u.i. 4-gyel való osztási maradékok:
$x^2 \equiv 3 \pmod{4}$. De ez nem lehet, a négyzetszám maradéka 0 vagy 1:

x	$x^2 \bmod 4$
$4k$	0
$4k+1$	1
$4k+2$	0
$4k+3$	1

Szimultán kongruenciák

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

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

A kongruenciákat külön megoldva:

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 5 \end{aligned}\right\}$$

Látszik, hogy $x = 2$ megoldás lesz!

Vannak-e más megoldások?

- $2, 17, 32, \ldots, 2 + 15\ell$;
- további megoldások?
- hogyan oldjuk meg az általános esetben:

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}\right\}$$

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruenciarendszert:

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}\right\}$$

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

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

Szimultán kongruenciák

Feladat: Oldjuk meg a következő kongruenciarendszert:

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

Feltehető, hogy az $m_1, m_2, \ldots, m_n$ modulusok relatív prímek:
ha pl. $m_1 = m_1' d$, $m_2 = m_2' d$, akkor az első két sor helyettesíthető (biz.: később)

$$\begin{aligned} x &\equiv c_1 \pmod{m_1'} \\ x &\equiv c_1 \pmod{d} \\ x &\equiv c_2 \pmod{m_2'} \\ x &\equiv c_2 \pmod{d} \end{aligned}$$

Ha itt $c_1 \not\equiv c_2 \pmod{d}$, akkor nincs megoldás, különben az egyik sor törölhető.

Kínai maradéktétel

Tétel

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

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

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

Kínai maradéktétel

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

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 kongruenciarendszer ekvivalens az

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

kongruenciarendszerrel. n szerinti indukcióval adódik az állítás. □

Szimultán kongruenciák

Példa

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

Oldjuk meg az $3x_1 + 5x_2 = 1$ egyenletet!
Megoldások: $x_1 = -3$, $x_2 = 2$. $\Rightarrow$
$\Rightarrow c_{1,2} = 3 \cdot (-3) \cdot 3 + 5 \cdot 2 \cdot 2 = -27 + 20 = -7$.
Összes megoldás: $\{-7 + 15\ell : \ \ell \in \mathbb{Z}\} = \{8 + 15\ell : \ \ell \in \mathbb{Z}\}$.

Példa

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

Oldjuk meg a $15x_{1,2} + 7x_3 = 1$ egyenletet!
Megoldások: $x_{1,2} = 1$, $x_3 = -2$. $\Rightarrow$
$\Rightarrow c_{1,2,3} = 15 \cdot 1 \cdot 4 + 7 \cdot (-2) \cdot 8 = 60 - 112 = -52$.
Összes megoldás: $\{-52 + 105\ell : \ \ell \in \mathbb{Z}\} = \{53 + 105\ell : \ \ell \in \mathbb{Z}\}$.

Maradékosztályok

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

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

Definíció

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

Példa

A $2x \equiv 5 \pmod 7$ megoldása: $\overline{6}$
A $10x \equiv 8 \pmod{22}$, megoldásai: $\overline{14}$, $\overline{3}$.
$m = 7$ modulussal $\overline{2} = \overline{23} = \{\ldots, -5, 2, 9, 16, 23, 30, \ldots\}$

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

Maradékosztályok

Definíció

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

Példa

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

Gyakori választás teljes maradékrendszerekre

- Legkisebb nemnegatív maradékok: $\{0, 1, \ldots, m-1\}$;
- Legkisebb abszolút értékű maradékok:
  $\left\{0, \pm 1, \ldots, \pm \frac{m-1}{2}\right\}$, ha $2 \nmid m$;
  $\left\{0, \pm 1, \ldots, \pm \frac{m-2}{2}, \frac{m}{2}\right\}$, ha $2 \mid m$.

Maradékosztályok

Megjegyzés: ha egy maradékosztály valamely eleme relatív prím a modulushoz, akkor az összes eleme az: $(a + \ell m, m) = (a, m) = 1$. Ezeket a maradékosztályokat redukált maradékosztályoknak nevezzük.

Definíció

Egy rögzített m modulus esetén, ha mindazon maradékosztályból, melyek elemei relatív prímek a modulushoz kiveszünk pontosan egy elemet, akkor az így kapott számok redukált maradékrendszert 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:

$$\overline{a} + \overline{b} \stackrel{\text{def}}{=} \overline{a+b}; \qquad \overline{a} \cdot \overline{b} \stackrel{\text{def}}{=} \overline{a \cdot b}.$$

Állítás

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

Bizonyítás

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

Maradékosztályok

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

Definíció

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

Példa

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

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

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

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

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

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

Maradékosztályok

Tétel

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

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

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

Példa

Legyen $m = 9$. $\overline{6} \cdot \overline{3} = \overline{18} = \overline{0}$.
$(2, 9) = 1$, így $\overline{2} \cdot \overline{5} = \overline{10} = \overline{1}$.

Bizonyítás

Legyen $d = (a, m)$. Ekkor $a \cdot \frac{m}{d} = \frac{a}{d} \cdot m \equiv 0 \pmod{m}$, ahonnan $b = m/d$ jelöléssel $\overline{a} \cdot \overline{b} = \overline{0}$.
Ha $(a, m) = 1$, akkor a bővített euklideszi algoritmussal megadhatóak x, y egészek, hogy $ax + my = 1$. Ekkor $ax \equiv 1 \pmod{m}$ azaz $\overline{a} \cdot \overline{x} = \overline{1}$. □

Euler-féle φ függvény

Definíció

Egy $m > 0$ egész szám esetén legyen $\varphi(m)$ az m-nél kisebb, hozzá relatív prím pozitív 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-hoz 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 kanonikus alakja $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$. Ekkor
$\varphi(m) = m \cdot \prod_{i=1}^{\ell} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{\ell} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$.

Példa

$\varphi(5) = 5\left(1 - \frac{1}{5}\right) = 5^1 - 5^0 = 4$;
$\varphi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = (2^1 - 2^0)(3^1 - 3^0) = 2$;
$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = (2^2 - 2^1)(3^1 - 3^0) = 4$;
$\varphi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = (3^1 - 3^0)(5^1 - 5^0) = 8$.

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

$\varphi(6) = 2 \Rightarrow 5^2 = 25 \equiv 1 \pmod{6}$;
$\varphi(12) = 4 \Rightarrow 5^4 = 625 \equiv 1 \pmod{12}$; $7^4 = 2401 \equiv 1 \pmod{12}$.

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

Euler-Fermat tétel bizonyítása

Lemma

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

Bizonyítás

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

$(a_i, m) = 1 \wedge (a, m) = 1 \Rightarrow (a \cdot a_i, m) = 1$. Továbbá $a \cdot a_1$, $a \cdot a_2$,..., $a \cdot a_{\varphi(m)}$ 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 $a_1, a_2, \ldots, a_{\varphi(m)}$ egy redukált maradékrendszer modulo m. Mivel $(a, m) = 1 \Rightarrow a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\varphi(m)}$ 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 tizes számrendszerben?
Mi lesz $3^{111} \bmod 10$?
$\varphi(10) = 4 \Rightarrow$
$3^{111} = 3^{4 \cdot 27+3} = \left(3^4\right)^{27} \cdot 3^3 \equiv 1^{27} \cdot 3^3 = 3^3 = 27 \equiv 7 \pmod{10}$

Oldjuk meg a $2x \equiv 5 \pmod{7}$ kongruenciát!
$\varphi(7) = 6$. Szorozzuk be mindkét oldalt 2^5-nel. Ekkor
$5 \cdot 2^5 \equiv 2^6 x \equiv x \pmod{7}$. És itt $5 \cdot 2^5 = 5 \cdot 32 \equiv 5 \cdot 4 = 20 \equiv 6 \pmod{7}$.

Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!
$\varphi(211) = 210$. Szorozzuk be mindkét oldalt 23^{209}-nel. Ekkor
$4 \cdot 23^{209} \equiv 23^{210} x \equiv x \pmod{211}$. És itt $4 \cdot 23^{209} \equiv \ldots \pmod{211}$.

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 $(0 \le j \le k)$ az első $j+1$ jegy által meghatározott szám:

$n_j = \lfloor n/2^{k-j} \rfloor = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_{k-j})_{(2)}$

Ekkor meghatározzuk minden j-re az $x_j \equiv a^{n_j} \pmod m$ maradékot:

$n_0 = \varepsilon_k = 1$, $x_0 = a$.

$n_j = 2 \cdot n_{j-1} + \varepsilon_{k-j} \Rightarrow$

$$x_j = a^{\varepsilon_{k-j}} x_{j-1}^2 \bmod m = \begin{cases} x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_{k-j} = 0 \\ a x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_{k-j} = 1 \end{cases} \Rightarrow$$

$x_k = a^n \bmod m$.

Az algoritmus helyessége az alábbi formulából következik (Biz.: HF):

$$a^n = a^{\sum_{i=0}^{k} \varepsilon_i 2^i} = \prod_{i=0}^{k} \left(a^{2^i}\right)^{\varepsilon_i}$$

Gyors hatványozás

Példa

Mi lesz $3^{111} \bmod 10$? (Euler-Fermat $\Rightarrow 7$)

$111_{(10)} = 1101111_{(2)}$ itt $k = 6$, $a = 3$, $m = 10$.

j	n_j	$x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$	$x_j \bmod 10$
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 $\Rightarrow x \equiv 4 \cdot 23^{209} \equiv \ldots \pmod{211}$.

Mi lesz $23^{209} \bmod 211$?
$209_{(10)} = 11010001_{(2)}$ itt $k = 7$, $a = 23$.

j	n_j	$x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$	$x_j \bmod 211$
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

$x \equiv 4 \cdot 23^{209} \equiv 4 \cdot 156 \equiv 202 \pmod{211}$.

Diszkrét matematika I. középszint

11. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

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 $(0 \le j \le k)$ az első $j+1$ jegy által meghatározott szám:

$n_j = \lfloor n/2^{k-j} \rfloor = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_{k-j})_{(2)}$

Ekkor meghatározzuk minden j-re az $x_j \equiv a^{n_j} \pmod m$ maradékot:

$n_0 = \varepsilon_k = 1$, $x_0 = a$.

$n_j = 2 \cdot n_{j-1} + \varepsilon_{k-j} \Rightarrow$

$$x_j = a^{\varepsilon_{k-j}} x_{j-1}^2 \bmod m = \begin{cases} x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_{k-j} = 0 \\ a x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_{k-j} = 1 \end{cases} \Rightarrow$$

$x_k = a^n \bmod m$.

Az algoritmus helyessége az alábbi formulából következik (Biz.: HF):

$$a^n = a^{\sum_{i=0}^{k} \varepsilon_i 2^i} = \prod_{i=0}^{k} \left(a^{2^i}\right)^{\varepsilon_i}$$

Gyors hatványozás

Példa

Mi lesz $3^{111} \bmod 10$? (Euler-Fermat $\Rightarrow 7$)

$111_{(10)} = 1101111_{(2)}$ itt $k = 6$, $a = 3$, $m = 10$.

j	n_j	$x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$	$x_j \bmod 10$
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 $\Rightarrow x \equiv 4 \cdot 23^{209} \equiv \ldots \pmod{211}$.

Mi lesz $23^{209} \bmod 211$?
$209_{(10)} = 11010001_{(2)}$ itt $k = 7$, $a = 23$.

j	n_j	$x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$	$x_j \bmod 211$
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

$x \equiv 4 \cdot 23^{209} \equiv 4 \cdot 156 \equiv 202 \pmod{211}$.

Generátor

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: $\{\overline{g^0} = \overline{1}, \overline{g}, \overline{g^2}, \ldots, \overline{g^{p-2}}\} = \mathbb{Z}_p^*$, azaz
$\{1 = g^0, g \bmod p, g^2 \bmod p, \ldots, g^{p-2} \bmod p\} = \{1, 2, \ldots, p-1\}$.

Példa

3 generátor modulo 7:

$$
\begin{aligned}
3^0 &= 1 = 1 \equiv 1 = 1 \equiv 1 \pmod 7\\
3^1 &= 3 = 3^0 \cdot 3 \equiv 1 \cdot 3 = 3 \equiv 3 \pmod 7\\
3^2 &= 9 = 3^1 \cdot 3 \equiv 3 \cdot 3 = 9 \equiv 2 \pmod 7\\
3^3 &= 27 = 3^2 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 6 \pmod 7\\
3^4 &= 81 = 3^3 \cdot 3 \equiv 6 \cdot 3 = 18 \equiv 4 \pmod 7\\
3^5 &= 243 = 3^4 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 5 \pmod 7
\end{aligned}
$$

Generátor

Példa

2 generátor modulo 11:

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6

2 nem generátor modulo 7:

n	0	1	2	3	4	5
$2^n \bmod 7$	1	2	4	1	2	4

Diszkrét logaritmus

Definíció

Legyen p prímszám, g generátor modulo p. Ekkor az $a \in \mathbb{Z}$ $(p \nmid a)$ g alapú diszkrét logaritmusa (indexe):

$$\log_g a = n: \quad a \equiv g^n \pmod{p}, \quad 0 \leq n < p.$$

Példa

3 generátor modulo 7:

n	0	1	2	3	4	5
3^n	1	3	2	6	4	5

$\longrightarrow$

3^n	1	3	2	6	4	5
n	0	1	2	3	4	5

azaz

a	1	3	2	6	4	5
$\log_3 a$	0	1	2	3	4	5

$\longrightarrow$

a	1	2	3	4	5	6
$\log_3 a$	0	2	1	4	5	3

Diszkrét logaritmus

Példa

2 generátor modulo 11:

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6

Logaritmus-táblázat:

a	1	2	3	4	5	6	7	8	9	10
$\log_2 a$	0	1	8	2	4	9	7	3	6	5

Tétel (HF)

Legyen p prímszám, g generátor modulo p, $1 \leq a, b < p$, $n \in \mathbb{Z}$. Ekkor

$$\log_g(a \cdot b) \equiv \log_g a + \log_g b \pmod{p-1}$$
$$\log_g(a^n) \equiv n \cdot \log_g a \pmod{p-1}$$

Alkalmazások

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 $\{0, 1, \ldots, 25\}$ halmaznak:

$$\begin{aligned} \mathrm{a} &\mapsto 0 \\ \mathrm{b} &\mapsto 1 \\ \mathrm{c} &\mapsto 2 \\ &\vdots \\ \mathrm{z} &\mapsto 25 \end{aligned}$$

Titkos kulcs: $s \in \{0, 1, \ldots, 25\}$.

Titkosítás: adott $a \in \{0, 1, \ldots, 25\}$ esetén a titkosítása $a \mapsto a + s \bmod 26$. Üzenet titkosítása betűnként.

Kititkosítás: adott $b \in \{0, 1, \ldots, 25\}$ esetén b kititkosítása $b \mapsto b - s \bmod 26$. Üzenet kititkosítása betűnként.

Példa

`hello` titkosítása az $s = 13$ kulccsal:

$\texttt{hello} \longrightarrow 7\ 4\ 11\ 11\ 14 \overset{\text{titkosítás}}{\longrightarrow} 20\ 17\ 24\ 24\ 1 \longrightarrow \texttt{uryyb}$

`uryyb` kititkosítása az $s = 13$ kulccsal:

$\texttt{uryyb} \longrightarrow 20\ 17\ 24\ 24\ 1 \overset{\text{kititkosítás}}{\longrightarrow} 7\ 4\ 11\ 11\ 14 \longrightarrow \texttt{hello}$

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 i.sz. 9 sz.)

Ha a különböző pozíciókban különböző kulcsokat választhatunk
(véletlenszerűen) $\Rightarrow$ bizonyítottan biztonságos

Gyakorlatban: One Time Pad – OTP

Üzenetek: bináris formában: $\mathtt{m}=100100101$
Kulcs: bináris sorozat: $\mathtt{s}=010110110$
Titkosítás: bitenkénti XOR (mod2 összeadás):

$$\begin{array}{rr} & \mathtt{m}=100100101 \\ \text{XOR} & \mathtt{s}=010110110 \\ \hline & \mathtt{c}=110010011 \end{array}$$

Kritikus pont: az s titkos kulcs átadása.

RSA

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 $e \in \{1, \ldots, \varphi(n)\}$ olyan, 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:
$c = m^e \bmod n$.

Kititkosítás Adott $0 \leq c < n$ titkosított üzenet kititkosítása:
$m = c^d \bmod n$.

Algoritmus helyessége:
$c^d = (m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n)+1} \overset{\text{E-F}}{\equiv} m \pmod{n}$

RSA

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 =
522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

RSA-2048=
251959084756578934940271832400483985714292821262040320277771378360436620207075955562640185258807844069182906412495150821892985591491761845028084891200728449926873928072877767359714183472702618963750149718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242811981638150106748104516603773060562016196762561338441436038339044149526344321901146575444541784240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643912120103971228221207203 57

RSA

RSA-2048 faktorizálása:

Próbaosztás (Eratoszthenész szitája): n szám esetén $\sim \sqrt{n}$ osztást kell végezni:

RSA-2048 $n \sim 2^{2048}$, $\sqrt{n} \sim 2^{1024}$ 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 $\approx 2^{969}$ év.

Ugyanezt 2 db géppel: 2^{968} év.

Ugyanezt a legjobb (ismert) algoritmussal:
$2500000000000000000000000000000$ év $(= 2,5 \cdot 10^{30})$

Univerzum életkora: $1,38 \cdot 10^{10}$ év.

RSA

Példa

Kulcsgenerálás:

Legyen $p = 61$, $q = 53$ és $n = 61 \cdot 53 = 3233$, $\varphi(3233) = 3120$.

Legyen $e = 17$. Bővített euklidészi 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 $s = m^d \bmod n$, 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 $a \in_R \{0, 1, \ldots, p-2\}$		választ $b \in_R \{0, 1, \ldots, p-2\}$
	$\xrightarrow{g^a}$	
	$\xleftarrow{g^b}$	
kiszámolja $\left(g^b\right)^a$	közös titkos kulcs: g^{ab}	kiszámolja $\left(g^a\right)^b$

Diffie-Hellman kulcscsere protokoll

Nyilvános paraméterek: p (nagy) prím, g generátor $\bmod p$.
Kulcsok: Alice titkos kulcsa a: $1 \leq a < p-1$, nyilvános kulcsa $g^a \bmod p$,
Bob titkos kulcsa b: $1 \leq a < p-1$, nyilvános kulcsa $g^b \bmod p$.
Közös kulcs: $g^{ab} \bmod p$.

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 $2^4 \bmod p = 5$.
Bob titkos kulcsa $b = 8$, nyilvános kulcsa $2^8 \bmod p = 3$.

Közös kulcs: $\left(g^b\right)^a = 3^4 \bmod p = 4$, $\left(g^a\right)^b = 5^8 \bmod = 4$.