DIMAT

összeadás $(a+c)+(b+d)i$

$$(\overset{a}{3}+\overset{b}{4}i)+(\overset{c}{7}\overset{d}{-5}i)=10-1i$$

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

---

szorzás $(ac-bd)+(ad+bc)i$

$\underline{\underline{i^2=-1}}$ $\Rightarrow (a+bi)(c+di)=ac+adi+bci+bdi^2=$ $\quad i^2=-1$

$$=(ac-bd)+(ad+bc)i$$

$$(3+4i)(7-5i)=(21+20)\ (-15+28)i=41+13i$$

---

kivonás $(a-c)+(b-d)i$

$$(3+4i)-(7-5i)=-4+9i$$

ellentett (-1-szeres)

$$-(a+bi)=(-a)+(-b)i$$

$$-(3+4i)=-3-4i$$

---

osztás (reciprokkal szorzás)

$$\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{(c+di)(c-di)}=\frac{(ac+bd)+(bc-ad)i}{c^2+dci-dci-di^2}=$$

$$=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i$$

$$\frac{3+4i}{7-5i}=\frac{(3+4i)(7+5i)}{(7-5i)(7+5i)}=\frac{(21+20)+(28-15)i}{49+25}=\frac{41}{74}+\frac{13}{74}i$$

---

konjugált $\overline{(a+bi)}=a-bi$

$$\overline{(3+4i)}=3-4i$$

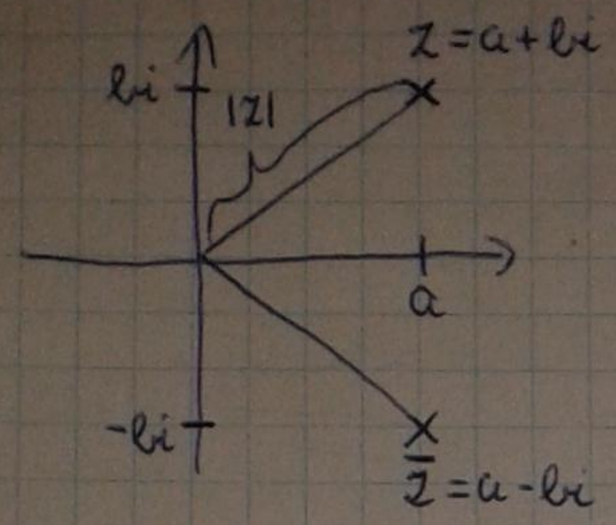
abszolút érték $|(a+bi)|=\sqrt{a^2+b^2}$

$$|(3+4i)|=\sqrt{3^2+4^2}=\sqrt{25}=5$$

① algebrai alak

$z = a + bi$

(Gauss-számsík)



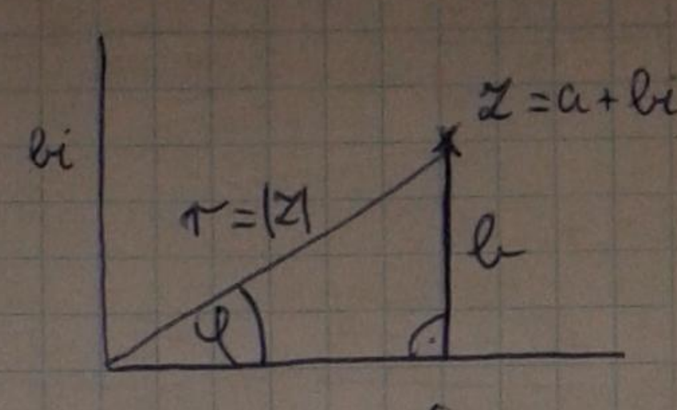
$(a \pm b)^3 = a^3 \pm 3a^2b + 3ab^2 \pm b^3$

$a^2 - b^2 = (a-b)(a+b)$

$a^3 - b^3 = (a-b)(a^2+ab+b^2)$

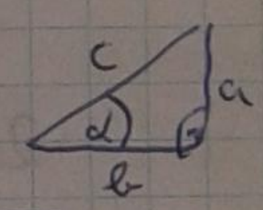
② trigonometrikus alak

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



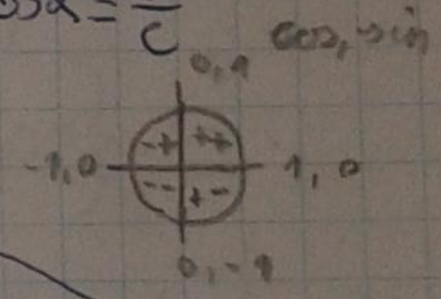
	0°	30°	45°	60°	90°	180°	270°	360°
sin	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	0	-1	0
cos	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	-1	0	1
tg	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	–	0	–	0
ctg	–	$\sqrt{3}$	1	$\frac{\sqrt{3}}{3}$	0	–	0	–

$\frac{\sqrt{2}}{2} = \frac{1}{\sqrt{2}}$



$\sin\alpha = \frac{a}{c}$

$\cos\alpha = \frac{b}{c}$



Feladatok

① Fejezd ki algebrai alakban

a, $(3+i)(2+3i) = (6-3)+(2+9)i = 3+11i$

b, $(2-5i)^2 = 4+(5i)^2-2\cdot 2\cdot 5i = 4-25-20i = -21-20i$

c, $(1-i)^3 = 1-3i+3i^2-i^3 = -2-2i$

d, $(4-2i)^4 = \left((4-2i)^2\right)^2 = (16+16i-4)^2 = (12+16i)^2 = 144-256+192i =$
$= -112+192i$

② Egyszerűsítsd

a, $i^3 = -i \Rightarrow i^3 = \overbrace{i^2}^{-1}\cdot i = -i$

b, $i^5 = \underbrace{i^4}_{(-1)^2}\cdot i = i$

c, $i^8 = (i^4)^2 = 1$

d, $\frac{1}{i^2} = -1 \quad \left(\frac{i^4}{i^2} = \frac{1}{-1}\right)$

e, $\frac{1}{i} = \frac{i^4}{i} = i^3 = -i$ $\quad i^2\cdot i = -1\cdot i$

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

g, $\frac{1}{i^3} = \frac{i^4}{i^3} = i$

h, $(1+i)^{2015} = \left[\overbrace{(1+i)^2}^{2i}\right]^{1007}\cdot(1+i) =$

$= 2^{1007}\cdot \underbrace{i^{1007}}_{i^{1004}\cdot i^3}\cdot(1+i) = -2^{1007}\cdot \underbrace{i(1+i)}_{-i} =$

$i^{1004} \to 1$, $i^3 \to -i$

$=$

③ Másodfokú egyenlet a $\mathbb{C}$-ben

a, $x^2+x+1=0$

$$x_{1,2}=\frac{-1\pm\sqrt{1-4}}{2}=\frac{-1\pm\overset{\sqrt{-1}\cdot\sqrt{3}}{\sqrt{-3}}}{2}=\underline{\underline{\frac{-1\pm\sqrt{3}\,i}{2}}}$$

b, $x^2+2x+2=0$

$$x_{1,2}=\frac{-2\pm\sqrt{4-8}}{2}=\frac{-2\pm\sqrt{-4}}{2}=\frac{-2\pm\overset{2}{\sqrt{4}}\,i}{2}=\underline{\underline{-1\pm i}}$$

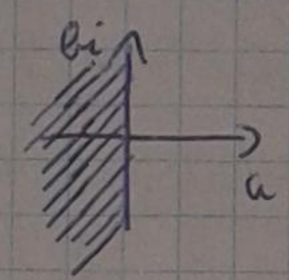
c, $x^2+2ix-1=0$

$$x_{1,2}=\frac{-2i\pm\sqrt{-4+4}}{2}=\frac{-2i}{2}=\underline{\underline{-i}}$$

④ Rajzoljuk le a $\underbrace{\text{komplex számsíkra}}_{\text{Gauss-számsík}}$ a köv. halmazokat

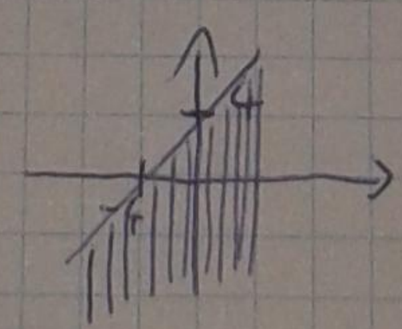
a, $\{z \mid \mathrm{Re}(z+2i)\le 0\} \equiv \{a+bi \mid \mathrm{Re}(a+bi+2i)\le 0\} \equiv$

$\equiv \{a+bi \mid a\le 0\}$



b, $\{z \mid \mathrm{Re}(z+1)\ge \mathrm{Im}(z-3i)\} \equiv \{a+bi \mid \mathrm{Re}(a+bi+1)\ge \overset{a+(b-3)i}{\mathrm{Im}(a+bi-3i)}\}$

$\equiv \{a+bi \mid a+1\ge b-3\} \Rightarrow b\le a+4$



4

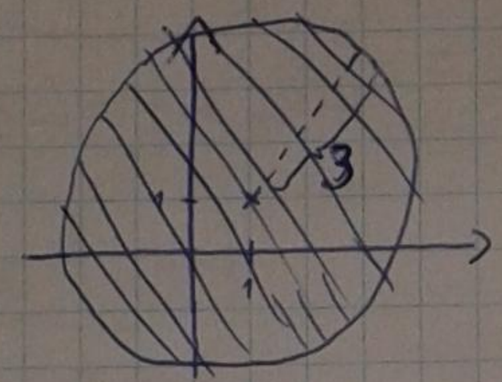
$$\{z \mid |z-i-1| \le 3\} \equiv \{a+bi \mid |a+bi-i-1| \le 3\} \equiv$$

$$\equiv \{a+bi \mid |\underbrace{a-1}_{Re}+\underbrace{(b-1)}_{Im}i| \le 3\} \equiv \{a+bi \mid \sqrt{(a-1)^2+(b-1)^2} \le 3\} \equiv$$

$$\equiv \{a+bi \mid (a-1)^2+(b-1)^2 \le 9\}$$

// $(x-x_0)^2+(y-y_0)^2=r^2$

↳ kör egyenlet



5. Fejezd ki algebrai alakban

a, $\frac{3+4i}{1-2i} = \frac{(3+4i)(1+2i)}{(1-2i)(1+2i)} = \frac{(3-8)+(6+4)i}{1+4} = \frac{-5+10i}{5} = -1+2i$

b, $\frac{\sqrt{3}-i}{\sqrt{3}+i} = \frac{(\sqrt{3}-i)(\sqrt{3}-i)}{(\sqrt{3}+i)(\sqrt{3}-i)} = \frac{3-2\sqrt{3}i-1}{3+1} = \frac{2-2\sqrt{3}i}{4} = \frac{1-\sqrt{3}i}{2} =$

$= \frac{1}{2} - \frac{1}{2}\sqrt{3}i$

c, $\frac{1}{1+7i} = \frac{1(1-7i)}{(1+7i)(1-7i)} = \frac{1-7i}{50} = \frac{1}{50} - \frac{7}{50}i$

6. Add meg $a, b \in \mathbb{R}$ értékeit

a, $(a+bi)(2-i) = a+3i$

$$(a+bi)(2-i) = a+3i \equiv \underbrace{(2a+b)}_{Re} + \underbrace{(-a+2b)}_{Im}i = \underbrace{a}_{Re} + \underbrace{3}_{Im}i$$

$$\left.\begin{array}{l} ① \ \overbrace{2a+b}^{Re} = \overbrace{a}^{Re} \\ ② \ \underbrace{2b-a}_{Im} = \underbrace{3}_{Im} \end{array}\right\}$$

↳ $b=-a$; $-3a=3 \Rightarrow \boxed{a=-1}$ $\boxed{b=1}$

b) $(a+i)(1+bi) = 3b + a\cdot i$ $\qquad (a-b)+(ab+1)i$

$$(a+i)(1+bi) = 3b + a\cdot i \equiv \overset{a \quad ab \quad bi \quad bi^2}{a + abi + i + bi^2} = 3b + a\cdot i$$

$$\equiv a + abi + i - b = 3b + a\cdot i \equiv \overbrace{\underbrace{a-b}_{Re} + \underbrace{(ab+1)}_{Im} i}^{z_1} = \overbrace{\underbrace{3b}_{Re} + \underbrace{a}_{Im} i}^{z_2}$$

$$\left.\begin{array}{l} ① \quad a - b = 3b \\ ② \quad ab + 1 = a \end{array}\right\}$$

másodfokú!

$$\hookrightarrow a = 4b; \quad \overbrace{4b^2 + 1 = 4b} \rightarrow 4b^2 - 4b + 1$$

$$b_{1,2} = \frac{4 \pm \sqrt{16-16}}{8} = \frac{1}{2}$$

$$\boxed{b = \frac{1}{2}} \quad \boxed{a = 2}$$

⑦ Legyen $\frac{5}{x+yi} + \frac{2}{1+3i} = 1$, $x, y \in \mathbb{R}$, $x, y = ?$

$$\frac{5(1+3i) + 2(x+yi)}{(x+yi)(1+3i)} = 1 \qquad / \cdot (x+yi)(1+3i)$$

$$5 + 15i + 2x + 2yi = (x+yi)(1+3i)$$

$$\underbrace{(5+2x)}_{Re} + \underbrace{(15+2y)}_{Im} i = \underbrace{(x-3y)}_{Re} + \underbrace{(3x+y)}_{Im} i$$

$$\left.\begin{array}{l} ① \quad 5 + 2x = x - 3y \\ ② \quad 15 + 2y = 3x + y \end{array}\right\}$$

$$\hookrightarrow x = -3y - 5$$

$$15 + 2y = 3(-3y - 5) + y$$

$$15 + 2y = -9y - 15 + y$$

$$30 = -10y$$

$$\boxed{y = -3} \quad \boxed{x = 4}$$

⑧ Add meg trigonometrikus alakban

a) $\sqrt{3}+i$

$\rightarrow \sqrt{3}+1i$ ($\rightarrow$ Re, $\rightarrow$ Im)

$$\sqrt{3}+i = |\sqrt{3}+i|\,(\cos\alpha + i\sin\alpha) \equiv \sqrt{(\sqrt{3})^2+1^2}\,(\cos\alpha + i\sin\alpha) \equiv$$

$$\equiv 2(\cos\alpha + i\sin\alpha)$$

$$\left.\begin{array}{ll} 2\cos\alpha = \sqrt{3} \rightarrow \mathrm{Re} & \cos\alpha = \frac{\sqrt{3}}{2} \\ 2\sin\alpha = 1 \rightarrow \mathrm{Im} & \sin\alpha = \frac{1}{2} \end{array}\right\} \alpha = 30^\circ = \frac{\pi}{6}$$

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

Moivre azonosságok

- szorzás

$$z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$$
$$z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$$
$$z_1 z_2 = r_1 r_2\left(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)\right)$$

- osztás (ha $z_2 \neq 0$)

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}\left(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)\right)$$

- hatványozás

$$z_1^n = r_1^n\left(\cos(n\cdot\varphi_1) + i\sin(n\cdot\varphi_1)\right)$$

- n. gyök $(z \in \mathbb{C}, z \neq 0)$
$n \in \mathbb{Z}, n \geq 1$

$w^n = z$ megoldásai $w = \sqrt[n]{r} \cdot \left(\cos\left(\frac{\varphi + 2\pi k}{n}\right) + i \sin\left(\frac{\varphi + 2\pi k}{n}\right)\right)$
ahol $k = 0, 1, 2, \dots n-1$ (n. megoldás ua. mint a 0.)

z-nek pontosan n db n-edik gyöke van, és azok egy origó központú szabályos n-szög csúcsai.

Pl.: $z = 1 \ (+0i)$
$z = 1 \cdot (\cos 0 + i \sin 0)$

$w^4 = 1$

$w_k = \sqrt[4]{1} \cdot \left(\cos \frac{0 + 2\pi k}{4} + i \sin \frac{0 + 2\pi k}{4}\right)$

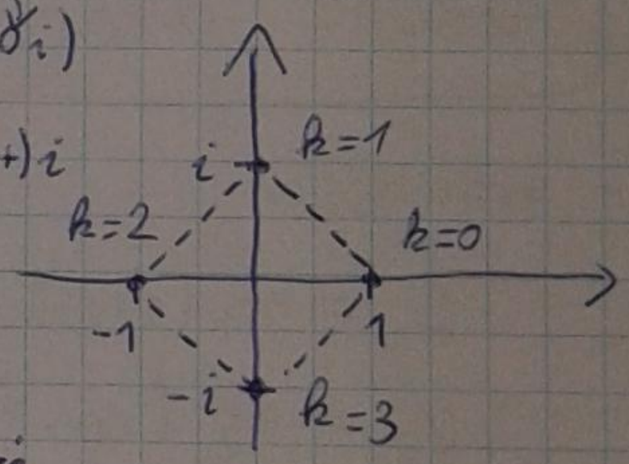
$\boxed{k = 0, 1, 2, 3}$

$w_0 = \sqrt[4]{1} \left(\overbrace{\cos 0}^{Re} + i \overbrace{\sin 0}^{Im}\right) = 1 \ (+0i)$

$w_1 = \sqrt[4]{1} \left(\cos \frac{2\pi}{4} + i \sin \frac{2\pi}{4}\right) = (0+)i$

$w_2 = \sqrt[4]{1} \left(\cos \pi + i \sin \pi\right) = -1$

$w_3 = \sqrt[4]{1} \left(\cos \frac{6\pi}{4} + i \sin \frac{6\pi}{4}\right) = (0-)i$



A $w^n = 1$ komplex megoldásait n-edik egységgyököknek nevezzük.

$i^4 = (i^2)^2 = (-1)^2 = 1$ (i negyedik egységgyök)
$i^8 = (i^4)^2 = 1$ (i nyolcadik egységgyök is)

↳ i 4-gyel osztható hatványai

→ Az 1-nek az n-edik gyökeit n-edik egységgyököknek nevezzük.

Pl.: $1, i, -1, -i$

~~tan~~ w n-edik egységgyök primitív n-edik egységgyök,
ha $w^n = 1$, de $w^1, w^2, \dots, w^{n-1}$ nem 1.
Pl.: primitív n-edik egységgyök: $i, -i$

Egy egységgyök rendje az a legkisebb pozitív egész szám (n), melyre $w^n = 1$

A primitív n-edik egységgyökök rendje n, vagyis n különböző hatványuk van.

<u>Az algebra alaptétele</u>

Legyen $a_0, a_1, a_2, \dots, a_n \in \mathbb{C}$, $(n \geq 1 \in \mathbb{Z})$, $a_n \neq 0$, ekkor
$\exists z \in \mathbb{C}: a_n z^n + a_{n-1} z^{n-1} + \dots a_2 z^2 + a_1 z^1 + a_0 = 0$

<u>Komplex számok trigonometrikus alakban (feladatok)</u>

1. $1 - i = |1-i|(\cos\varphi + i \sin\varphi)$

$\downarrow$

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

$$\left.\begin{aligned} \sqrt{2}\cos\varphi &= 1 \\ \sqrt{2}\sin\varphi &= -1 \end{aligned}\right\} \begin{aligned} \cos\varphi &= \frac{1}{\sqrt{2}} \\ \sin\varphi &= -\frac{1}{\sqrt{2}} \end{aligned}$$

$\varphi = 45° = 2\pi - \frac{\pi}{4} = \frac{7}{4}\pi$

$$\boxed{\sqrt{2}\left(\cos\frac{7}{4}\pi + i \sin\frac{7}{4}\pi\right)}$$

2. $-2 + i = |-2+i|(\cos\beta + i \sin\beta)$

$\downarrow$

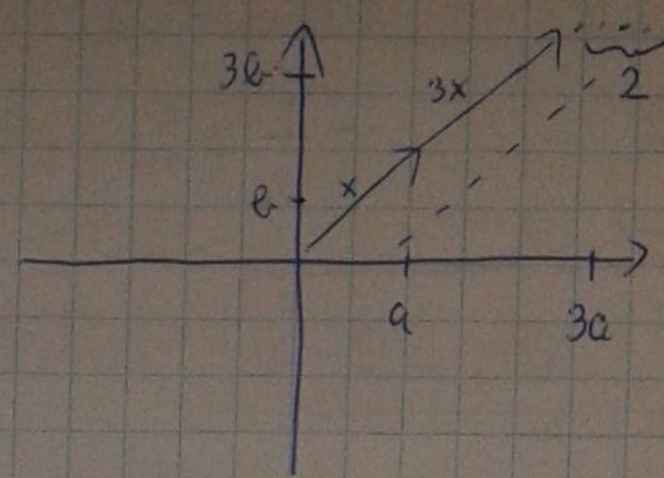
$\sqrt{5}$

$$\left.\begin{aligned} \sqrt{5}\cos\beta &= -2 \\ \sqrt{5}\sin\beta &= 1 \end{aligned}\right\} \begin{aligned} \cos\beta &= -\frac{2}{\sqrt{5}} \\ \sin\beta &= \frac{1}{\sqrt{5}} \end{aligned}$$

⑤ A sík mely geo. transzformációjának felel meg?

[a] $z \mapsto 3z+2 \equiv 3(a+bi)+2 \equiv 3a+3bi+2 \equiv (3a+2)+3bi$

$z=a+bi,\ a,b \in \mathbb{R}$



eltolás

nyújtás

[b] $z \mapsto (1+i)z$

$z=a+bi,\ a,b \in \mathbb{R}$

$(ac-bd)+(ad+bc)i$

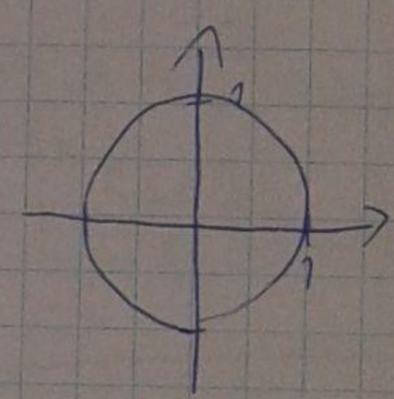
$a+bi \mapsto (1+i)(a+bi) \equiv a-b+i(a+b)$

$$\left.\begin{aligned} 1+i &= \sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right) \\ a+bi &= \underbrace{\sqrt{a^2+b^2}}_{|z|}\left(\cos\varphi+i\sin\varphi\right) \end{aligned}\right\} \cdot \quad \sqrt{2}\cdot|z|\left(\cos\left(\varphi+\frac{\pi}{4}\right)+i\sin\left(\varphi+\frac{\pi}{4}\right)\right)$$

nyújtás forgatás

[c] $z \mapsto \frac{1}{z} = \frac{1}{a-bi} = \frac{a+bi}{a^2+b^2} = \frac{z}{|z|^2}$

A körön kívül eső pontok közelebb kerülnek az originhoz és fordítva



⑥ Vonjunk négyzetgyököt

[a] $\sqrt{3-4i}$ (algebrai megoldás)

$\sqrt{3-4i} = w \qquad w=c+di,\ c,d \in \mathbb{R},\ c,d \neq 0$

$w^2 = 3-4i \equiv (c+di)^2 = 3-4i \equiv c^2+2cdi-d^2 = 3-4i$

$\underbrace{c^2-d^2}_{Re}+\underbrace{2cd}_{Im}i = \underbrace{3}_{Re}-\underbrace{4}_{Im}i \qquad \left.\begin{aligned} c^2-d^2 &= 3 \\ 2cd &= -4 \end{aligned}\right\} \quad c = -\frac{4}{2d}$

$\left(-\frac{4}{2d}\right)^2 - d^2 = 3 \equiv \left(-\frac{2}{d}\right)^2 - d^2 = 3 \equiv \frac{4}{d^2} - d^2 = 3 \quad /\cdot d^2$

$4-d^4 = 3d^2 \equiv -d^4-3d^2+4$ visszavezethető másodfokú egyenletre az ismeretlen bevezetésével

$y=d^2$

$y^2+3y-4=0$ $\quad y_{1,2}=\frac{-3\pm\sqrt{9+16}}{2}$

$y_1=1 \Rightarrow \boxed{\begin{matrix} d_1=1 \\ d_2=-1 \end{matrix}}$

$y_2=-4$

nem megoldás mivel $y=d^2$ és $c,d\in\mathbb{R}$

$\boxed{c_1=-\frac{4}{2}=-2}$ $\quad \boxed{c_2=-\frac{4}{-2}=2}$

$w_1=\overset{c_1}{-2}+\overset{d_1}{i}$; $w_2=\overset{c_2}{2}-\overset{d_2}{i}$

b) trigonometrikus megoldás, n. gyök

$\sqrt{2i}=w \qquad w^2=2i$

$2i=2\left(\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}\right)$

$w_k=\sqrt{2}\left(\cos\frac{\frac{\pi}{2}+2k\pi}{2}+i\sin\frac{\frac{\pi}{2}+2k\pi}{2}\right) \quad k\in[0,1]$

$$\boxed{\begin{aligned} w_0&=\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right)=1+i \\ w_1&=\sqrt{2}\left(\cos\frac{\frac{\pi}{2}+2\pi}{2}+i\sin\frac{5}{4}\pi\right)=-1-i \end{aligned}}$$

7. $x\in\mathbb{C}$

$(2+i)x^2-(5-i)x+(2-2i)=0$

$x_{1,2}=\frac{5-i\pm\sqrt{(5-i)^2-4\cdot(2+i)(2-2i)}}{2\cdot(2+i)}$ *

$*\ \sqrt{25-1-10i-4(4+2+i(2-4))}=\sqrt{24-10i-4(6-2i)}=$

$=\sqrt{24-10i-24+8i}=\sqrt{-2i}$

$\sqrt{-2i}=w \qquad w^2=-2i$

⑨ $x^3 = 1 \quad x \in \mathbb{C}$

$1(\cos 0 + i \sin 0)$

$x_k = 1 \cdot \left(\cos \frac{0+2k\pi}{3} + i \sin \frac{0+2k\pi}{3}\right) \quad k \in [0,1,2]$

$x_0 = (\cos 0 + i \sin 0) = 1$

$x_1 = \left(\cos \frac{2}{3}\pi + i \sin \frac{2}{3}\pi\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

$x_2 = \left(\cos \frac{4}{3}\pi + i \sin \frac{4}{3}\pi\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$

logika

Predikátum kalkulus

az állítások egyszerű alapkijelentésekből logikai jelekkel alkotott bonyolultabb kijelentések.

predikátum: alapkijelentés, melyet mi határozunk meg

pl.: $P(x)$ – x páros

értéke: hamis vagy igaz

logikai jelek

$\wedge$ - és, $\vee$ - vagy, $\oplus$ - kizáró vagy, $\Rightarrow$ - implikáció, $\Leftrightarrow$ - ekvivalencia, $\neg$ - tagadás

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

A	$\neg A$
I	H
H	I

kvantorok

$\forall$: univerzális (minden)

$\exists$: egzisztenciális (létezik)

– $\forall x(A)$: igaz, ha bármilyen konkrét értéket x helyébe írva A igaz

– $\exists x(A)$: igaz, ha van olyan konkrét érték, melyet x helyébe írva A igaz

kvantoros állítások tagadása

$\neg \forall x(A) \Leftrightarrow \exists x(\neg A)$

$\neg \exists x(A) \Leftrightarrow \forall x(\neg A)$

Def.: Egy x változó egy előfordulása egy kvantor hatáskörében van, ha a $\forall x(\dots)$, $\exists x(\dots)$ kifejezésekben a zárójelpár között szerepel. Más szavakkal a változó előfordulása kötött.
(Szabad, ha nincs kvantorhatáskörben.)

Def.: Egy formula (kijelentés) zárt, ha minden változó előfordulása kötött. (egyéb esetben nyílt)

$\forall x(P(x)) \wedge O(x) \wedge G(y)$

kvantor hatásköre — nem a kvantor hatásköre

$\forall x(O(x) \vee P(x))$ - zárt formula $\qquad$ $P(x)$ - nyílt formula

de Morgan azonosságok (logika és halmazelmélet)

$\neg(A \wedge B) = (\neg A) \vee (\neg B) \equiv \overline{A \cap B} = \bar{A} \cup \bar{B}$

$\neg(A \vee B) = (\neg A) \wedge (\neg B) \equiv \overline{A \cup B} = \bar{A} \cap \bar{B}$

Halmazok

1. nincs multiplicitása (egy elem csak egyszer szerepel)
2. az elemek sorrendje nem definiált

- a halmazokat általában nagy betűvel, elemeiket kis betűvel jelöljük ($x \in A$ - x eleme A-nak)

3. $A = B \iff \forall x(x \in A \iff x \in B)$ - Két halmaz akkor egyenlő, ha az elemeik benne vannak mindkét halmazban.

Halmazok létrehozása

1. elemek felsorolása

$\{1, 4, 9, 16\}$; $\{1, 2, 3, 4 \dots\}$ → egyértelmű legyen hogy mivel folytatódik

② névvel

$\mathbb{N} = \{0, 1, 2 \dots\}$ - természetes számok

$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ - egész számok

$\mathbb{Q} = \{$racionális számok$\}$

$\mathbb{R} = \{$valós számok$\}$

$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ - komplex számok

③ leírással

$\{p+1 \mid p$ poz. prím$\} = \{3, 4, 6, 8, 12, \dots\}$

$A = \{1, 7, 12\}$

$\{x^2+3 \mid x \in A\} = \{4, 52, 147\}$ - végigmegyünk A elemein és elvégezzük rájuk az x^2+3-at

$\{x \in A \mid x$ prím$\} = \{7\}$

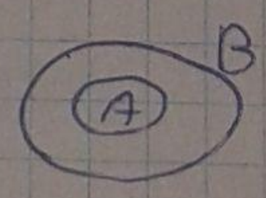
<u>Üres halmaz</u>

az a halmaz, melynek nincsenek elemei. Jele: $\emptyset = \{\}$

<u>Halmazokkal kapcsolatos műveletek</u>

① A részhalmaza B-nek

$A \subseteq B$, ha $\forall x (x \in A \Rightarrow x \in B)$



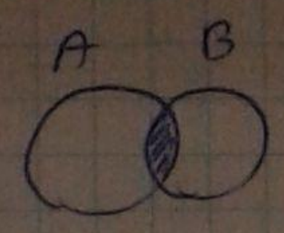
② A valódi részhalmaza B-nek

$A \subsetneq B$, $A \neq B$

Állítás: $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

Biz: $(x \in A \Leftrightarrow x \in B) \Leftrightarrow (x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)$

③ A és B metszete



$A \cap B = \{x \mid x \in A \wedge x \in B\}$

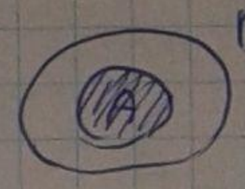
a) $A \cap B = B \cap A$ (tz $\wedge$ művelet szimmetrikus miatt)

b) $A \cap (B \cap C) = (A \cap B) \cap C$ (tz $\wedge$ művelet asszociatív)

c) $A \cap A = A$ (idempotens)

d) $A \cap \emptyset = \emptyset$

e) $A \subseteq B \Leftrightarrow A \cap B = A$



Def.: Ha $\mathcal{A}$ egy olyan halmaz melynek elemei is halmazok, akkor

$\bigcap \mathcal{A} := \{x \mid \forall A \in \mathcal{A} : x \in A\}$

↳ a benne lévő halmazokra

Pl.: $\mathcal{A} = \{\{1,2,3\}, \{3,4,5\}, \{1,5,7\}\}$

$\bigcap \mathcal{A} = \emptyset$

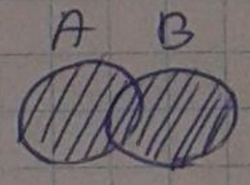
[diszjunkt]

sok halmaz metszete: $\bigcap_{j=1}^{\infty} A_j$

↳ nagy gamma

Def.: legyen Γ egy halmaz és A_γ minden $\gamma \in \Gamma$-ra egy-egy halmaz. Ekkor: $\bigcap_{\gamma \in \Gamma} A_\gamma := \{x \mid \forall \gamma \in \Gamma : x \in A_\gamma\}$

④ A és B uniója



$A \cup B = \{x \mid x \in A \vee x \in B\}$

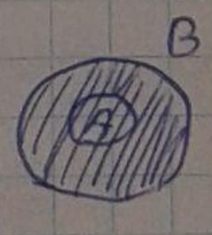
a) $A \cup B = B \cup A$

b) $A \cup (B \cup C) = (A \cup B) \cup C$

c) $A \cup A = A$

d) $A \cup \emptyset = A$

e) $A \subseteq B \Leftrightarrow A \cup B = B$



Def.: Ha $\mathcal{A}$ egy olyan halmaz melynek elemei is halmazok, akkor

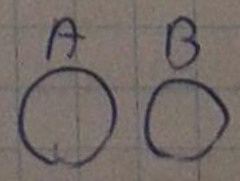
$\bigcup \mathcal{A} := \{x \mid \exists A \in \mathcal{A} : x \in A\}$

Pl.: $\mathcal{A} = \{\{1,2,3\}, \{3,4,5\}, \{1,5,7\}\}$

$\bigcup \mathcal{A} = \{1,2,3,4,5,7\}$

Def.: legyen Γ egy halmaz és A_γ minden $\gamma \in \Gamma$-ra egy-egy halmaz. Ekkor: $\bigcup_{\gamma \in \Gamma} A_\gamma := \{x \mid \exists \gamma : x \in A_\gamma\}$

Def.: A és B diszjunkt, ha $A \cap B = \emptyset$

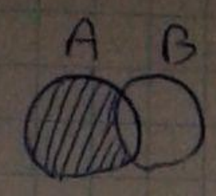


Egy halmazrendszer diszjunkt, ha $\bigcap \mathcal{A} = \emptyset$

– páronként diszjunkt, ha $\forall A_1, A_2 \in \mathcal{A}, A_1 \neq A_2 : A_1 \cap A_2 = \emptyset$

⑤ A és B különbsége

$A \setminus B := \{x \mid x \in A \wedge x \notin B\}$

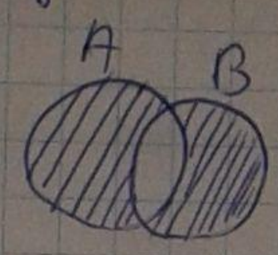


⑥ A és B szimmetrikus differenciája

$A \triangle B = \{x \mid x \in A \oplus x \in B\}$

$= (A \setminus B) \cup (B \setminus A)$

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



a) $A \triangle B = B \triangle A$

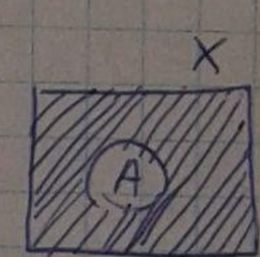
b) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$

c) $A \triangle A = \emptyset$

d) $A \triangle \emptyset = A$

⑦ komplementer

<u>Def.:</u> legyen X, A halmaz, $A \subseteq X$. Ekkor A-nak az X-re vonatkozó komplementere $\overline{A}_X = \overline{A} := X \setminus A$



Általában X-et rögzítjük. (pl. egész számok)

Állítás: X rögzített, $\forall A, B \subseteq X$

a) $\overline{\overline{A}} = A$

b) $\overline{\emptyset} = X$

c) $\overline{X} = \emptyset$

d) $A \cap \overline{A} = \emptyset$

e) $A \cup \overline{A} = X$

f) $(A \subseteq B) \Longleftrightarrow \overline{A} \supseteq \overline{B}$

g) $\overline{A \cup B} = \overline{A} \cap \overline{B}$

h) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

de Morgan

⑧ hatványhalmaz

A hatványhalmaza $= \mathcal{P}(A)$. Mindazon halmazokat tartalmazza elemekként, melyek A részei.

$X \in \mathcal{P}(A) \Longleftrightarrow X \subseteq A$

Ha A n elemű, akkor $\mathcal{P}(A)$ 2^n elemű.

Pl.: $A = \{1, 2, 3\}$

$\mathcal{P}(A) = \{\{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}, \emptyset\}$

$\mathcal{P}(\emptyset) = \{\emptyset\}$

9. A és B direkt szorzata (Descartes)

rendezett pár: (x,y)

$(x,y) := \{\{x\},\{x,y\}\}$

$(x,x) := \{\{x\},\{x,x\}\} = \{\{x\}\}$

$(x,y) = (a,b)$ ha $x=a$ és $y=b$

/sorend számít!/

$x \to$ első komponens

$y \to$ második komponens

$$A \times B = \{(a,b) \mid a \in A, b \in B\}$$

↳ összes lehetséges pár

pl.: ilk $\mathbb{R} \times \mathbb{R} = \{(x,y) \mid x,y \in \mathbb{R}\}$

$A = \{1,2,3\}$
$B = \{x,y\}$ $\Rightarrow A \times B = \{\{1,x\},(1,y),(2,x),(2,y),(3,x),(3,y)\}$

logikai és halmaz jelek

logika	halmaz
$\wedge$	$\cap$
$\vee$	$\cup$
$\oplus$	Δ
$\Rightarrow$	$\subseteq$
$\neg A$	$\overline{A}$
ANDNOT	$\setminus$

Relációk

Def.: (bináris) reláción rendezett párok halmazát értjük

$R \subseteq A \times B$ – R az A és B közti reláció. R elemei olyan rendezett párok, melyek első komponensei A-beliek, másodikak pedig B-beliek.

Pl.:

anna	matek
anna	töri
Béla	testi
zsolt	tánc

anna → matek
→ töri

Béla → testi

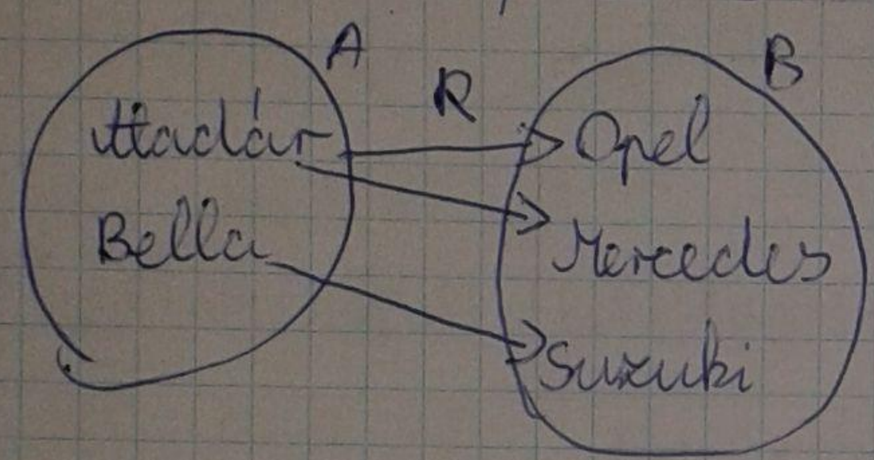
zsolt → tánc

$R = \{(\text{anna}, \text{matek}), (\text{anna}, \text{töri}), (\text{Béla}, \text{testi}), (\text{zsolt}, \text{tánc})\}$

Relációk

Legyen A, B halmaz. Azt mondjuk hogy R reláció
- ha rendezett párok halmaza
- A és B közötti reláció, ha $R \subseteq A \times B$
- A - beli homogén reláció, ha $R \subseteq A \times A$

Pl.: $A = \{\text{emberek}\}$; $B = \{\text{autók}\}$

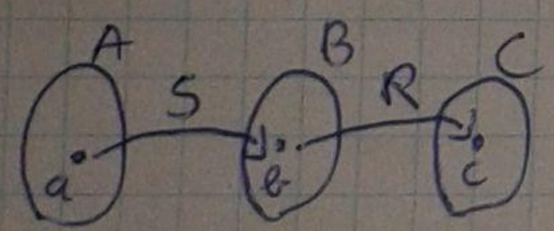


Inverz: Ha R reláció ($\{(a,b) \mid (a,b) \in R\}$), akkor az inverze
$R^{-1} = \{(b,a) \mid (a,b) \in R\}$

Relációk kompozíciója/szorzata: R, S relációk, akkor

$R \circ S = \{(a,c) \mid \exists b : (a,b) \in S, (b,c) \in R\}$ (köt)

Pl.: $S \subseteq A \times B$, $R \subseteq B \times C \rightarrow R \circ S \subseteq A \times C$



Legyen R reláció, A halmaz
A-nak az R szerinti
képe: $R(A) = \{y \mid \exists x \in A : (x,y) \in R\}$
- inverz képe: $R^{-1}(A) = \{x \mid \exists y \in A : (x,y) \in R\}$

R-nek az A-ra vonatkozó megszorítása: $R|_A = \{x,y \mid x \in A \wedge (x,y) \in R\}$

R reláció értelmezési tartománya: $\mathrm{dmn}(R) = \{a \mid \exists b : (a,b) \in R\}$
(olyan „a", melyhez létezik kapcsolat „b"-vel az R relációban)

R reláció értékkészlete: $\mathrm{rng}(R) = \{b \mid \exists a : (a,b) \in R\}$

Állítás: $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$

Bizonyítás: $(a,c) \in (R \circ S)^{-1} \Leftrightarrow (c,a) \in (R \circ S)$

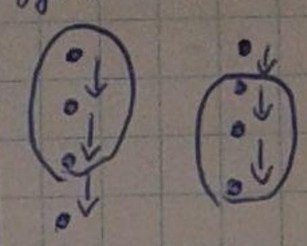
$\exists b : (c,b) \in S \wedge (b,a) \in R \Leftrightarrow \exists b : (b,c) \in S^{-1} \wedge (a,b) \in R^{-1}$

$(a,c) \in (S^{-1} \circ R^{-1})$ ✓

A relációkompozíció asszociativitása

$\forall R, S, T$ relációra $(R \circ S) \circ T = R \circ (S \circ T)$

Mindegy hogy:
gyerekem unokája - unokám gyereke



Bizonyítás: átírjuk logikai jelekkel, o-ból $\exists$ lesz, majd visszaalakítjuk

$(a,d) \in (R \circ S) \circ T \Leftrightarrow \exists b : (a,b) \in T \wedge (b,d) \in (R \circ S)$

$\exists b \, \exists c : \underbrace{(a,b) \in T \wedge (b,c) \in S}_{\text{relációkompozíció } \exists b\text{-vel}} \wedge (c,d) \in R$

$\exists c : (a,c) \in (S \circ T) \wedge (c,d) \in R$

$(a,d) \in (R \circ (S \circ T))$ ✓

R reláció:

- szimmetrikus: $\forall a, b : (a,b) \in R \Rightarrow (b,a) \in R$ // $R = R^{-1}$
- antiszimmetrikus: $\forall a, b : (a \neq b \wedge (a,b) \in R) \Rightarrow (b,a) \notin R$ // pl.: $\leq$
- szigorúan antiszimmetrikus: $\forall a, b : (a,b) \in R \Rightarrow (b,a) \notin R$ // pl.: $<$ párhuz.
- tranzitív: $\forall a, b, c : ((a,b) \in R \wedge (b,c) \in R) \Rightarrow (a,c) \in R$ // pl. $<, \leq, \parallel, =$

↳ a reláció több lépésen át is megmarad

R relációt az X alaphalmazon ($R \subseteq X \times X$):

- reflexív: $\forall a \in X : (a,a) \in R$ // pl. $\leq, =, \parallel$
  ↳ mindegyik relációban van önmagával

- irreflexív: $\forall a \in X : (a,a) \notin R$ // pl.: $<$
  ↳ önmagával nincs relációban

- dichotom: $\forall a, b \in X : (a,b) \in R \vee (b,a) \in R$

- trichotom: $\forall a, b : \underbrace{(a,b) \in R,\ (b,a) \in R,\ a = b}_{\text{pontosan 1 igaz}}$

— — — — — — — —

- <u>részben rendezés</u>: ha tranzitív, reflexív, antiszimmetrikus // pl.: $\leq$

  tranzitív: $a \leq b \leq c \Rightarrow a \leq c$ reflexív: $a \leq a$ antiszimmetrikus: $a \leq b,\ b \leq a \Rightarrow a = b$

  ↳ $\forall a, b \in X$-re 4 lehetőség van:
  1. $(a,b) \in R,\ a \neq b$ // $a < b$
  2. $(b,a) \in R,\ a \neq b$ // $b < a$
  3. $a = b$
  4. nem összehasonlíthatóak ($(a,b) \notin R$ és $(b,a) \notin R$)

- <u>teljes rendezés</u>: ha részben rendezés <u>és dichotom</u>
  ↳ bármely két elem összehasonlítható

- R-hez tartozó szigorú reláció: $\{(a,b) \mid (a,b) \in R \wedge a \neq b\}$

- R-hez tartozó gyenge reláció: $\{(a,b) \mid (a,b) \in R \vee a = b\}$

- szigorú részben rendezés: tranzitív és irreflexív (ilyenkor kötelezően szigorúan antiszimmetrikus)

- szigorú teljes rendezés: ha szigorúan részben rendezés és trichotom

gyenge	szigorú
tranzitív	tranzitív
r.r. reflexív	irreflexív
antiszimmetrikus	szigorúan antiszimmetrikus
dichotom (teljes rendezés)	trichotom

<u>Def.</u>: R az X-en részben rendezés (jelöljük $\leq$)

- x minimális, ha $\nexists y : y < x$
- x maximális, ha $\nexists y : y > x$
- x legnagyobb, ha $\forall y : y \leq x$
- x legkisebb, ha $\forall y : x \leq y$

① legnagyobb elemből legfeljebb egy létezik

② Ha a rendezés teljes, akkor legfeljebb egy maximális elem van, és az a legnagyobb

③ legnagyobb $\Rightarrow$ maximális

<u>a és b közti zárt intervallum</u>

$[a, b] := \{c \mid a \leq c, c \leq b\}$

pl.: osztója: $[2, 12] = \{2, 4, 6, 12\}$

nyílt intervallum: $]a, b]$, $[a, b[$, $]a, b[$

<u>szakaszok</u>

$]\leftarrow, a] = \{c \mid c \leq a\}$ zárt

$]\leftarrow, a[= \{c \mid c < a\}$ nyílt

Def.: Egy $Y \subseteq X$ halmaznak x felső korlátja, ha $\forall y \in Y \; y \leq x$

- ha van köztük legkisebb felső korlát, neve szuprémum
- ha van köztük legkisebb alsó korlát, neve infimum

Def.: X halmaz egy $\mathcal{O}$ osztályozása (particionálása) olyan halmaz, melynek Y elemei páronként diszjunkt nemüres halmazok, melyek uniója X. → alaphalmaz

Pl.: $\mathcal{O} = \{\{1,2\}, \{3\}, \{4,5\}\}$ $\quad X = \{1,2,3,4,5\}$ // 1 2 | 3 | 4 5

Áll.: Minden az X halmazbeli R ekvivalenciarelációt meghatároz egy $\mathcal{O}_R$ osztályozást X-en.

– és –

Minden $\mathcal{O}$ osztályozása X-nek meghatároz egy $R_{\mathcal{O}}$ ekvivalenciarelációt.

továbbá: $R_{\mathcal{O}_R} = R$ és $\mathcal{O}_{R_{\mathcal{O}}} = \mathcal{O}$ (*)

- ~~ekvivalencia reláció~~: reflexív, tranzitív, szimmetrikus

osztályozásra példa: $\mathbb{Z}$ alaphalmaz

$R = \{(x,y) \mid x, y \in \mathbb{Z}, x-y: \text{páros}\}$

$\mathcal{O} = \{\{\text{páros sz.}\}, \{\text{páratlan sz.}\}\}$

(*) biz.: R ekvivalenciarelációt. legyen $x \in X$, az $\bar{x}$ halmaz a köv.:

$\bar{x} = \{y \in X \mid (y,x) \in R\}$ „x osztálya"

áll.: $\{\bar{x} \mid x \in X\}$ egy osztályozás

$\bar{x}$ nem üres: $x \in \bar{x}$, mert az R reflexív

$\bigcup \{\bar{x} \mid x \in R\} = X$

$\bar{x} \neq \bar{y}$ esetén: $\bar{x} \cap \bar{y} = \emptyset$

TFH. $\exists z \in \bar{x} \cap \bar{y} : (z,x) \in R, (z,y) \in R$

$\Updownarrow$ szimm. miatt

$\underbrace{(x,z) \in R, (z,y) \in R}$

$\Downarrow$ tranzitív

$(x,y) \in R \Leftrightarrow x \in \bar{y}$

$\Updownarrow$ szimm.

$(y,x) \in R \Leftrightarrow y \in \bar{x}$

$\bar{x} = \bar{y}$ esetén

$z \in \bar{x} \Rightarrow (z,x) \in R \quad (x,y) \in R \overset{\text{tranz.}}{\Rightarrow} (z,y) \in R \Rightarrow z \in \bar{y}$

$\Rightarrow z \in \bar{x}$

Függvények

<u>Def.</u>: Egy f relációt függvény, ha $\forall x, y, y' : (x,y) \in f$, $(x,y') \in f$ esetén $y = y'$

megjegyzés: Minden pontból legfeljebb egy nyíl megy ki

<u>Def.</u>: Legyen X, Y halmaz. Ekkor $f : X \to Y$ jelölés azt jelenti, hogy f függvény, $\mathrm{dmn}(f) = X$, $\mathrm{rng}(f) \subseteq Y$ (f az X-ből Y-ba képez)

Pl.: $f : \mathbb{N} \to \mathbb{N}$

Jelölés: ha $x \in dmn(f)$, akkor pontosan egy olyan y létezik, melyre $(x, y) \in f$. Ezt az y-t $f(x)$-el jelöljük

Függvények megadása:

$f: \mathbb{N} \to \mathbb{N}$, $f(n) = n^2$, $n \mapsto n^2$

<u>Def.</u>: f fv. X-ből Y-ba képező parciális fv., ha $dmn(f), rng(f) \subseteq Y$ $(f \in X \to Y)$

<u>Def.</u>: f fv. injektív ha x_1, x_2 a $dmn(f)$ elemei,
$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ $[f(x_1) = f(x_2) \Rightarrow x_1 = x_2]$ // $A \Rightarrow B \Leftrightarrow \neg B \Rightarrow \neg A$

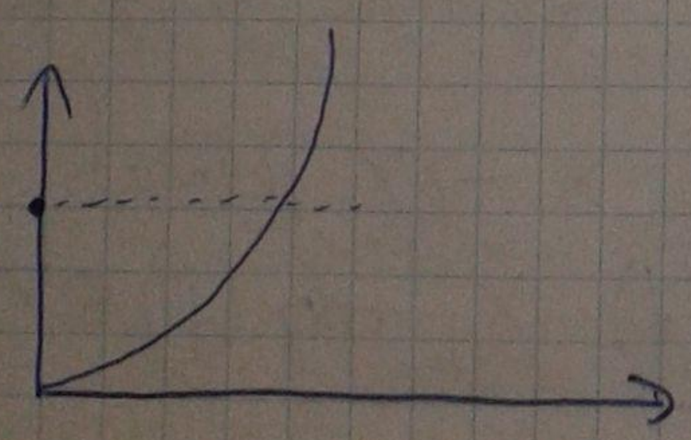
megj.: f injektív $\Leftrightarrow f^{-1}$ is fv.
↳ f inverze

<u>Def.</u>: $f: X \to Y$ szürjektív ha $rng(f) = Y$
az egész Y halmazt lefedi, nem csak részhalmaza
$[\forall y \in Y\ \exists x: f(x) = y]$ [f az X-ből az Y-<u>ra</u> képez]

<u>Def.</u>: $f: X \to Y$ bijektív, ha injektív és szürjektív

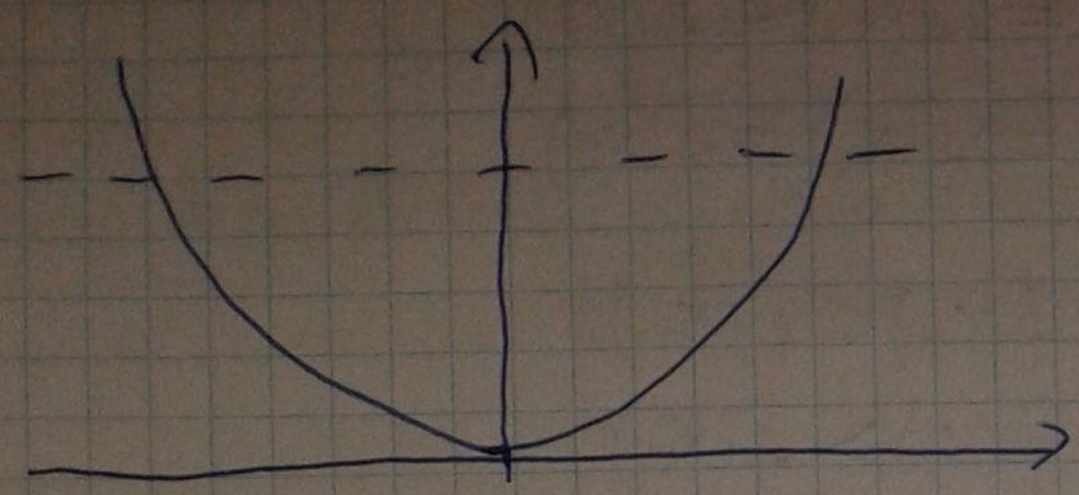
Pl.: $x \to x^2$ (nincs specifikálva hogy miből mibe képez)

① $f: \mathbb{R}^{+0} \to \mathbb{R}^{+0}$ $x \to x^2$



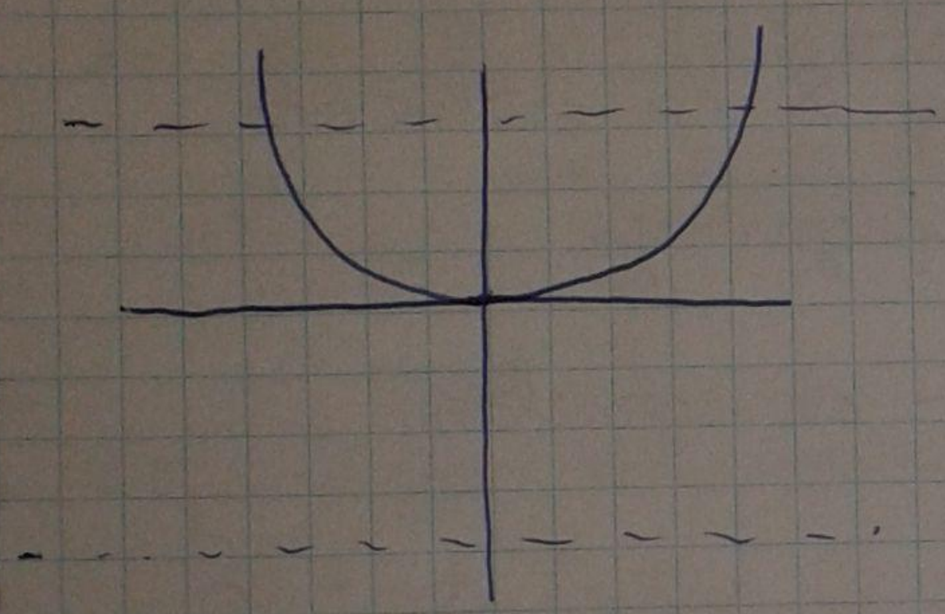
bijektív

② $f: \mathbb{R} \to \mathbb{R}^{+0}$



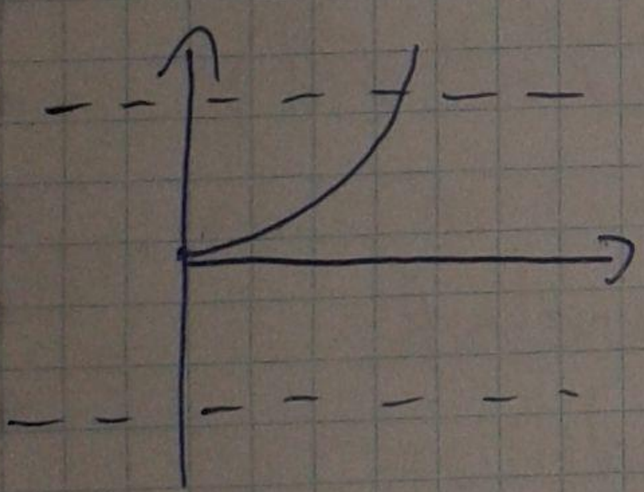
nem injektív
szürjektív

③ $f: \mathbb{R} \to \mathbb{R}$



nem injektív
nem szürjektív

④ $f: \mathbb{R}^{+0} \to \mathbb{R}$



nem injektív (?)
nem szürjektív

<u>Áll.:</u> Ha f és g is fv., akkor $(f \circ g)$ is fv.
és $\forall x \in dmn(g)$-re $(f \circ g)(x) = f(g(x))$

<u>Áll.:</u> Ha f és g fv.

① f és g injektív $\Rightarrow f \circ g$ is ilyen
② f és g szürjektív $\Rightarrow f \circ g$ is ilyen
③ f és g bijektív $\Rightarrow f \circ g$ is ilyen

Def.: X, Y halmaz, $f: X \to Y$

- f monoton nő, ha: $x_1 \leq x_2 \Rightarrow f(x_1) \leq f(x_2)$
- f monoton csökken, ha: $x_1 \leq x_2 \Rightarrow f(x_1) \geq f(x_2)$

- f szig. mon. nő, ha $x_1 < x_2 \Rightarrow f(x_1) < f(x_2)$
- f szig. mon. csök, ha $x_1 < x_2 \Rightarrow f(x_1) > f(x_2)$

<u>Műveletek</u>: legyen X egy halmaz. Egy X-en értelmezett bináris művelet egy $f: X \times X \to X$ függvény.

pl.: összeadás $(2,3) = 5$, $+, \cdot, -$ az egészeken

bináris művelet: szám $\to$ szám

bináris reláció: szám $\to$ logikai

ellenpl.: nem művelet a kivonás $\mathbb{N}$-en $(5-7=-2 \notin \mathbb{N})$

<u>jelölés</u>: általában a műveleti jelet infix jelöléssel leírjuk a bemenő pár két komponense közé

$f((2,3)) = 5$ postfix (fordított lengyel): $2\ 3\ +$

$\hookrightarrow 2+3=5$

$(a+b)\cdot(c+d) \Leftrightarrow a, b, +, c, d, +, \cdot$

unáris művelet X-en: $X \to X$ fv. (pl reciprok)

Nullás művelet X-en: $\{\emptyset\} \to X$ (nincs bemenete)

Legyen $\otimes$ általános műveleti jel.

<u>Def.</u>: Egy X-en értelmezett $\otimes$ műveletet kommutatív, ha $\forall a, b \in X : a \otimes b = b \otimes a$

pl.: $+$ az $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}_{X \times X}$ -en

$\cap, \cup, \triangle$

<u>Def.</u>: Egy X-en értelmezett $\otimes$ műveletet asszociatív, ha $\forall a, b, c \in X : (a \otimes b) \otimes c = a \otimes (b \otimes c)$

pl.: $+$ az $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ -en

$\cap, \cup, \triangle, \circ$

Def.: Legyen X halmaz. $\otimes, \square$ bináris műveletek X-en.
– $\otimes$ disztributív $\square$-re, ha $\forall a, b, c \in X$:

$a \otimes (b \square c) = (a \otimes b) \square (a \otimes c)$ // balról disztributív

$(b \square c) \otimes a = (b \otimes a) \square (c \otimes a)$ // jobbról disztributív

pl.: $a \cdot (b + c) = ab + ac$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

<u>Műveletek függvényeken</u>

Legyen $\otimes$ művelet X-en, $f : H \to X$, $g : H \to X$ fv.

$f \otimes g : H \to X$

$h \to f(h) \otimes g(h)$

pl.: $\sin + \cos \quad \mathbb{R} \to \mathbb{R}$

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

Def.: Legyen $\otimes$ művelet az X-en, és $\square$ művelet az Y-on. $f: X \to Y$ fv.

a fv. átképezi Y-ba

f műveletartó, ha $\forall x_1, x_2 \in X: f(\underbrace{x_1 \otimes x_2}_{\text{ez X-ben van}}) = f(x_1) \square f(x_2)$

pl.: $\mathbb{N}, \mathbb{N}, f: x \mapsto x^2$

$$f(x_1 \cdot x_2) = f(x_1) \cdot f(x_2)$$

$$(x_1 \cdot x_2)^2 = x_1^2 \cdot x_2^2 \checkmark$$

<u>struktúra</u>: halmaz, és a rajta értelmezett műveletek

Def.: Legyen G halmaz a $\circ$ bináris művelettel.

$(G, \circ)$ félcsoport, ha $\circ$ asszociatív.

$(G, \circ)$ csoport, ha félcsoport és

- $\exists e \in G: \forall g: g \circ e = e \circ g = g$ (e egységelem létezik)
- $\forall g \in G: \exists g^{-1} \in G: g \circ g^{-1} = g^{-1} \circ g = e$ (g^{-1} inverz létezik)

$(G, \circ)$ Abel-csoport, ha csoport és $\circ$ kommutatív.

Def.: Egy $(R, +, \cdot)$ struktúra gyűrű, ha (ring)

1. $(R, +)$ Abel-csoport
2. $(R, \cdot)$ félcsoport
3. $\cdot$ disztributív az $+$-ra

pl.: $(\mathbb{Z}, +, \cdot)$

Def.: Egy R gyűrű nulloszétosztóes, ha nincsen nulloszétosztópár benne. ($a \neq 0$, $b \neq 0$ ahol $ab = 0$)

Def.: R gyűrű integritási tartomány, ha

1. kommutatív a szorzás
2. nulloszétosztóes
3. legalább kételemű (megj.: a nullgyűrűt $(\{0\}, +, \cdot)$ kizárva (egy elemű))

Pl.: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, +, \cdot$

Zérógyűrű: $(R, +, \cdot)$ $\forall a, b: a \cdot b = 0$

Def.: Egy $(R, +, \cdot)$ gyűrű test, ha $(R \setminus \{0\}, \cdot)$ Abel csoport.

Def.: Egy R integritási tartományt rendezett integritási tartománynak hívunk, ha R-en létezik egy $\leq$ jelű rendezés, valamint

1. az összeadás monoton: $\forall x, y, z: x \geq y \Rightarrow x + z \geq y + z$
2. a szorzás monoton: $\forall x, y: x, y \geq 0 \Rightarrow x \cdot y \geq 0$

megj.: lehet $>$ a $\geq$ helyett

Pl.: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

Tétel: A számolás szabályai rendezett integritási tartományban

1. $x \geq y,\ z \geq 0 \Rightarrow xz \geq yz$

   az összeadás monoton

   biz.: $x \geq y \Rightarrow (x - y) \geq 0 \Rightarrow (x - y)z \geq 0 \Rightarrow xz - yz \geq 0 \Rightarrow xz \geq yz$

2. $x \geq y,\ z \leq 0 \Rightarrow xz \leq yz$

   biz.: $z \leq 0 \Leftrightarrow -z \geq 0$ mert $z \leq 0$ $\quad / + (-z)$

   $z - z \leq -z$

   $0 \leq -z$

3. $x^2 \geq 0$

   ha $x \geq 0 \Rightarrow x \cdot x \geq 0$

   $x \leq 0 \Rightarrow x \cdot x \geq 0$

④ ha van egységelem 1, akkor $1 \geq 0$

⑤ ha $0 \leq x \leq y$ és $\exists \frac{1}{x}, \frac{1}{y}$ akkor $0 \leq \frac{1}{y} \leq \frac{1}{x}$

<u>biz.:</u>

$0 \leq x$ ha $\frac{1}{x} < 0$ lenne: $0 \leq x \quad / \cdot \frac{1}{x}$ → negatív szám, reláció megfordul

$0 \geq 1$ ↯

$y - x \geq 0 \quad / \cdot \frac{1}{xy} \rightarrow \geq 0$

$\frac{1}{x} - \frac{1}{y} \geq 0$

A tételből adódik: $\mathbb{K}$ nem lehet rendezett integritási tartomány

biz: ha az lenne ...

$$\left.\begin{array}{l} 1 > 0 \Rightarrow -1 < 0 \\ -1 = i^2 \geq 0 \end{array}\right\} ↯$$

<u>Def.:</u> Egy testet, ami rendezett integritási tartomány, rendezett testnek nevezünk

Pl.: $\mathbb{Q}, \mathbb{R}$

$\mathbb{R} \Leftrightarrow \mathbb{C}$

rendezett — nem rendezett

$\mathbb{R} \Leftrightarrow \mathbb{Q}$

rendezettek, de $\mathbb{Q}$-ban vannak ugrások! ($\sqrt{2}$)

<u>Áll.:</u> $\sqrt{2}$ nem racionális

<u>biz.:</u> TFH. $\sqrt{2}$ racionális. Ekkor felírható $\sqrt{2} = \frac{a}{b}$ alakban, és feltehetjük, hogy „a" a lehető legkisebb poz. egész, amivel felírható így.

$a, b \in \mathbb{Z}$

$\sqrt{2} = a/b \quad /()^2$

$2 = a^2/b^2$

$2b^2 = a^2$ → ebből adódóan „a" páros (2c alakú)

$2b^2 = 4c^2$

$b^2 = 2c^2$

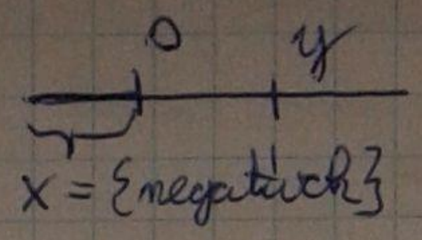
$\sqrt{2} = \frac{b}{c} \quad b < a$

↯ van kisebb „a"-nál???

Def.: A legkisebb felső korlátot szuprémumnak hívjuk.

X részhalmaz $\mathbb{R}$-ben, X felső korlátja

$\forall y \in \mathbb{R} : \forall x \in X \; x \leq y$ pl.:



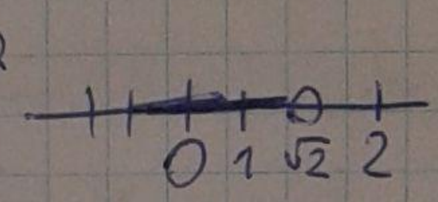
$\mathbb{R}$-ben ha van felső korlát, akkor van szuprémum.

$y=0$ legkisebb felső korlát

$\mathbb{Q}$-ban $X = \{x \mid x^2 < 2\}$

felső korlát $y=10$ pl.

nincs legkisebb felső korlát $\rightarrow$



Def.: Egy rendezett test felsőhatár tulajdonságú, ha minden nem üres felülről korlátos halmaznak van szuprémuma

Áll.: Létezik felsőhatár tulajdonságú rendezett test.

Ha $(K_1, +, \cdot)$ és $(K_2, +, \cdot)$ is ilyen, akkor $\exists f : K_1 \to K_2$ bijekció, mely műveletartó, és rendezéstartó.

(vagyis K_1 és K_2 lényegében ua. a struktúra)

↳ pl. lényegében ua. az összeadásra

$\{0, 1, 2, \dots\}, +$

$\{0, 10, 20, \dots\}, +$

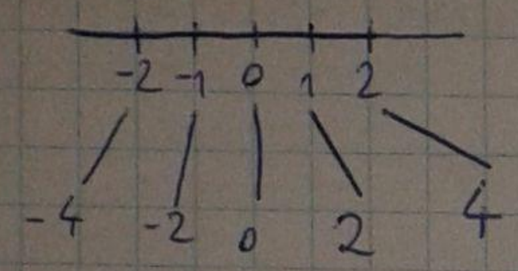
Peano-axiómák

1. $0 \in \mathbb{N}$
2. $n \in \mathbb{N} \Rightarrow n^+ \in \mathbb{N}$ [az „n" rákövetkezője]
3. $n^+ = m^+ \Rightarrow n = m$
4. $n \in \mathbb{N} \Rightarrow n^+ \neq 0$
5. $\forall S \subseteq \mathbb{N} : (0 \in S \wedge \forall n (n \in S \Rightarrow n^+ \in S)) \Rightarrow S = \mathbb{N}$ (indukció sémája)

véges halmazok, kombinatorika

Def.: két halmaz ekvivalens ($A \sim B$), ha $\exists f: A \to B$ bijektív („ugyanakkora")

pl.: $\mathbb{Z} \sim 2\mathbb{Z}$ → páros egészek



Tétel: Ha egy halmaz nem ekvivalens egy valódi részhalmazával sem, akkor véges

Def.: Egy X halmaz véges, ha
$\exists n \in \mathbb{N}: X \sim \{k \in \mathbb{N}^+ \mid k \leq n\} = \{1, 2 \dots n\}$

Áll.: Ha X véges, akkor a def-ben szereplő n egyértelmű.
A neve az, hogy X elemszáma: $|X|$ vagy $\#X$

Áll.: A, B véges diszjunkt halmazok: $|A \cup B| = |A| + |B|$

biz.:

$|A| = n$ $\quad A = \underset{1}{\cdot}\ \underset{2}{\cdot}\ \underset{3}{\cdot} \dots \underset{n}{\cdot}$

$|B| = m$ $\quad B = \underset{n+1}{\cdot}\ \underset{n+2}{\cdot} \dots \cdot$ $\quad A \cup B \to n+m$

pl.: olyan lehetőségek összeszámolása, ahol ezek egymást kizárta, „diszjunkt" események.

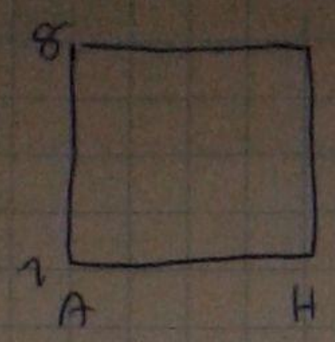
Hány olyan 5 jegyű szám van, melynek első jegye prímszám?

2 .... 10^4
3 .... 10^4
5 .... 10^4
7 .... 10^4

Tétel: A és B tetszőleges véges halmazok $\Rightarrow |A \cup B| = |A| + |B| - |A \cap B|$

Tétel: Ha A és B véges halmazok, akkor $|A \times B| = |A| \cdot |B|$

Pl.: sakktábla



$64 = 8 \cdot 8$

bizi.: indukció B elemszáma szerint

$|B| = 0 \Rightarrow B = \emptyset \Rightarrow A \times B = \emptyset \Rightarrow |A \times B| = 0$

$|B| = 1$

$f: A \to A \times B$ bijektív

$a \mapsto (a, b)$ $B = \{b\}$

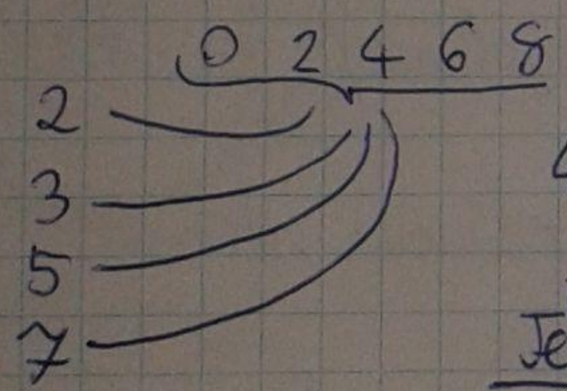
$|B| \leq m$-re már OK, most $|B| = m+1$

$B = \{b_1, b_2, b_3, \dots, b_m, \underbrace{b^*}_{\text{egy elem}}\}$

$$A \times B = \underbrace{A \times \{b_1, b_2, \dots b_m\}}_{|A| \cdot m} \cup \underbrace{A \times \{b^*\}}_{|A|}$$

$|A| \cdot m + |A| = |A| \cdot (m+1)$ ✓

Pl.: hány olyan kétjegyű szám van, aminek első jegye prím, a második pedig páros?



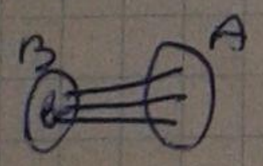
$4 \cdot 5 = 20$ eset

Tétel: ha A, B véges halmazok, akkor a $f: B \to A$ függvények száma $|A|^{|B|}$ → a kitevő a fv. elmn-je
↳ az alap az rng

bizi.: $|B|$ szerinti indukció

$|B| = 0$ ✓

$|B| = 1$ $B = \{b\}$



$f: b \mapsto a_k$

az A elemszámával megegyező db fv.

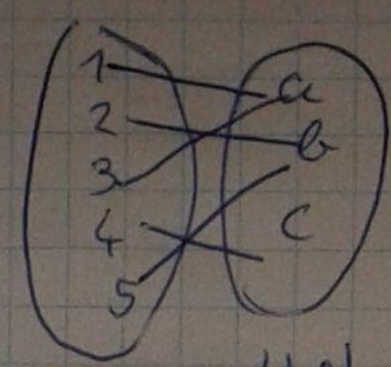
$|B| \leq m$ ✓ $|B| = m+1$ $B = \{b_1, b_2, \dots b_m, b^*\}$

Minden $f: B \to A$ felépíthető egy $\{b_1, b_2 \dots b_m\} \to A$ és $\{b^*\} \to A$ fv-ek megoldásával. Az első fv. $|A|^m$ lehetőség, másodikra $|A|$ lehet

Összesen $|A|^m \cdot |A| = |A|^{m+1}$

Def.: Egy A halmazbeli k hosszúságú sorozat:
$\{1,2,3\dots k\} \to A$ függvény

Pl.: $A=\{a,b,c\}$ $\quad a,b,a,c,b \leftrightarrow$



Def.: Egy A halmaz k-ad osztályú ismétléses variációja k hosszú sorozat A elemeiből
Ezek száma: $|A|^k = n^k$ ha $|A|=n$

Def.: A halmaz permutációin az $A \to A$ bijektív függvényeket értjük. pl.:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 5 & 1 & 4 \end{array}$$

Áll.: Egy véges halmaz permutációinak száma csak a halmaz elemszámától függ.

Def.: n faktoriálisa $n! = \prod_{k=1}^{n} k = 1\cdot 2\cdot 3\dots n$

ha $n \in \mathbb{N}$ megj.: $0! = 1$ (szorzás egységeleme)

Áll.: Egy n elemű halmaz permutációinak száma: $n!$
pl.: Egy futóversenyen hányféle eredmény lehet?

biz.: indukció $n=0,1$ ✓

n-re OK, n+1?
↳ $|A| = (n+1)$-re $A=\{1,2,\dots n\}$

Szorzunk egy osztályba azon $f,g: A\to A$ bijekciókat melyekre $f(1)=g(1)$ ← ekviv. rel, tehát osztályok
az osztályok száma $n+1$, osztályok mérete $n!$ → ind. miatt
össz méret: $(n+1)n! = (n+1)!$

Def.: Egy A halmaz k-ad osztályú ismétlés nélküli variációin az A elemeiből képezhető olyan k hosszú sorozatokat értjük, melyekben minden elem különböző.

Megj.: $\{1,2\dots,k\} \to A$ injektív fv.

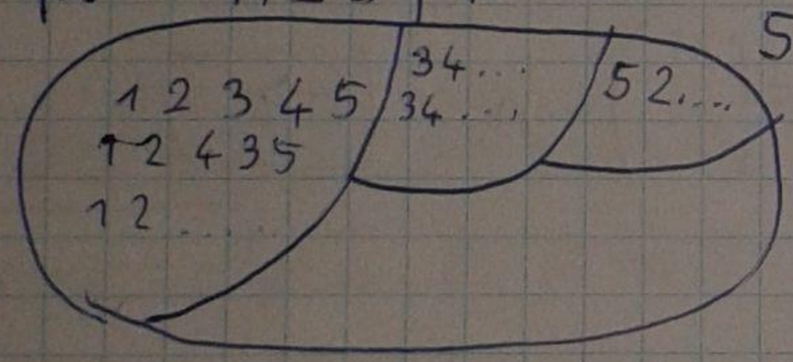
Megj.: $|A| = n$ és $k = n$, akkor az A k-ad osztályú variációinak száma $n!$

Áll.: Egy n elemű halmaz k-ad osztályú variációinak száma: $V_n^k = \frac{n!}{(n-k)!}$, ha $k = 0, 1, 2 \dots n$

Pl.: 10-en futnak, a dobogó $\frac{10!}{(10-3)!}$ féle lehet.

Biz.: Vegyjük az összes permutációt (n-ed osztályú variációt) $\cdot n!$
Legyen két ilyen ekvivalens, ha az első k pozícióban megegyeznek

pl.: $n = 5$, $k = 2$



5! összesen jönnek létre. Osztályok mérete: ahányféleképpen a maradék (n-k) elem permutálható: $(n-k)!$

Tehát: $\underbrace{V_n^k}_{\frac{n!}{(n-k)!}} \cdot (n-k)! = n!$

Megj.: $\frac{n!}{(n-k)!} = \frac{1 \cdot 2 \cdot 3 \cdot \dots n}{1 \cdot 2 \cdot 3 \cdot \dots (n-k)} =$
$= n \cdot (n-1) \cdot (n-2) \dots (n-k+1)$

Def.: Egy A halmaz k-ad osztályú kombinációján az A egy k elemű részhalmazát értjük

Áll.: Egy n elemű halmaznak $k = 0, 1, \dots, n$ esetén $C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$ k-ad osztályú kombinációja van.

Pl.: lottó: 90 szám közül hányféleképp választhatunk 5-t?

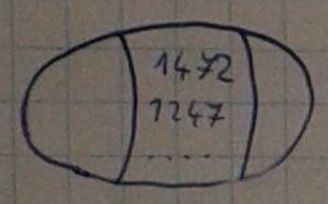
$\binom{90}{5} = \frac{90!}{5!\,85!} = \frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{120}$

Def.: Ha $n \in \mathbb{N}$, $k \in \{0,1 \dots n\}$ akkor $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (binomiális együttható)

↳ visszavezethető a variációkra

Biz.: Egy n elemű halmaznak $\frac{n!}{(n-k)!}$ darab k-ad osztályú variációja van.

Legyen két variáció ekvivalens, ha ugyanazokat az elemeket tartalmazzák (pl.: $1,4,7,2 \sim 2,1,4,7 \sim 1,2,4,7$)



V_n^k osztályok száma: C_n^k

osztályok mérete: $k!$

$$\underbrace{C_n^k}_{\frac{n!}{k!(n-k)!}} \cdot k! = \frac{n!}{(n-k)!}$$

Fermi féle becslés: mindent 10 hatványára kerekítünk (durva becslés)

Pl.: $\frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{120} \approx \frac{100 \cdot 100 \cdot 100 \cdot 100 \cdot 100}{100}$

Stirling formula: $n! \approx \sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n$

- $\pi = 3.14\dots$
- $e = 2.7182\dots$

Áll.: $\binom{n}{k} = \binom{n}{n-k}$ **Megj.:** $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = \binom{n}{n-1} = n$ $\boxed{n \geq 1}$

Áll.: $0 \leq k \leq n-1$, $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

Biz.: ① számolás ② $(n+1)$-ből $(k+1)$ elem választható úgy, hogy a legkisebb

szerepel $\binom{n}{k}$ | nem szerepel $\binom{n}{k+1}$

Áll.: $\boxed{\sum_{k=0}^{n} \binom{n}{k} = 2^n}$ **Biz.:** Egy n elemű halmaznak $\binom{n}{0}$ db 0 elemű, $\binom{n}{1}$ db 1 elemű, … $\binom{n}{n}$ db n elemű részhalmaza van. Egy n elemű halmaznak összesen 2^n részhalmaza van. Pl.: $A = \{1,2,3,4,5\}$

$A \supseteq B = \{1,3,4\}$

↳ $\mathbb{N} \parallel \mathbb{N}$

$\{1,N\}$-ből 2^5 db 5 hosszú sorozat van

Def.: Egy multihalmazon egy olyan függvényt értünk, mely egy alaphalmaz elemeihez renkel $\mathbb{N}$-beli multiplicitásokat.

Pl.: $\{1,3,5\} \to \mathbb{N}$ $\quad 1 \mapsto 2,\ 3 \mapsto 4,\ 5 \mapsto 1$ $\quad \sim$ 1 1 / 3 3 3 3 / 5

(2db 1-es, 4db 3-as, 1db 5-ös)

Ábrázolás: $\square\square XX\square\square\square\square XX\square$ $\quad 7 = k$ db négyzet

$4 = n-1$ db X

↳ a halmaz legnagyobb eleme (itt 5)

Biz.: Képezzünk egy olyan $(n+k-1)$ hosszú sorozatot $\square, X$ jelekből, melyben k db $\square$, $n-1$ db X szerepel. Az ilyen sorozatok pontosan megfeleltethetők az $f: \{1,2,\dots,n\} \to \mathbb{N}$ k-ad osztályú ismétléses kombinációknak.

$f(j)$ megegyezik a $(j-1)$-edik és j-edik X közti $\square$ jelek számával. [Ha $j=1$ az első X előtti, $j=n$ az utolsó X után]

Az $\square, X$ sorozatok száma: ahányféleképp kijelölhető az a k db pozíció, ahová $\square$-et teszünk $\binom{n+k-1}{k}$

Def.: Egy A halmaz k-ad osztályú ismétléses kombinációján egy olyan $f: A \to \mathbb{N}$ fv-t értünk, melyre $\sum_{a \in A} f(a) = k$

Megj.: lottó, visszatevéssel (13, 42, 42, 42, 57)

Áll.: Egy n elemű halmaznak $\binom{n+k-1}{k}$ db k-ad osztályú ismétléses kombinációja van.

Def.: Legyen A egy r elemű halmaz, $i_1, i_2, \dots i_r \in \mathbb{N}$, $i_1 + i_2 + \dots + i_r = n$

Az A-nak egy $i_1, i_2, \dots, i_r$ osztályú ismétléses permutációján egy olyan n hosszú sorozatot értünk, melyben az A egyes elemei pontosan i_1-szer, i_2-szer, i_r-szer fordulnak elő.

Pl.: MAMA → AMAM, AAMM, AMMA

$\frac{4!}{2!\,2!}$

Áll.: Az ismétléses permutációk száma [$i_1, i_2, \dots, i_r$ osztályú, $n = i_1 + i_2 + \dots + i_r$]

$$P_n^{i_1, i_2 \dots i_r} = \frac{n!}{i_1!\, i_2! \dots i_r!}$$

Biz.: r szerinti indukció

$r=0,1$ ✓ $\quad r=2$ Azt kell megmondani, hogy az n hosszú sorozat melyik i_1 db pozícióra írjuk az első elemet: $\binom{n}{i_1} = \frac{n!}{i_1!(n-i_1)!}$

de $(n-i_1)=i_2$ ✓

Ha $(r-1)$ már ok, meg kell mondani

① Hova kerül az r-edik $\binom{n}{i_r}$

② A maradék $(n-i_r)$ pozíciót hogy töltjük ki $i_1, i_2, \dots, i_{r-1}$ ismétlődéssel

Lehetőségek: $\binom{n}{i_r} \cdot \frac{(n-i_r)!}{i_1!\, i_2! \dots i_r!} = \frac{n!}{i_r!\,\cancel{(n-i_r)!}} \cdot \frac{\cancel{(n-i_r)!}}{i_1!\, i_2! \dots i_{r-1}!}$

	Ism. nélkül	Ism.-sel
P	$n!$	$\frac{n!}{i_1!\, i_2! \dots i_r!}$
V	$\frac{n!}{(n-k)!}$	n^k
K	$\binom{n}{k}$	$\binom{n+k-1}{k}$

Binomiális tétel

Ha x, y egy kommutatív gyűrű elemei (van egységelem is), akkor $n \geq 1$-re $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k$

Pl.: $(x+y)^4 = \binom{4}{0} \cdot x^4 + \binom{4}{1} \cdot x^3 \cdot y + \binom{4}{2} \cdot x^2 \cdot y^2 + \binom{4}{3} \cdot x y^3 + \binom{4}{4} \cdot y^4 =$

$= x^4 + 4x^3 y + 6x^2 y^2 + 4x y^3 + y^4$

<u>biz.:</u> $n=0,1$ ✓

n-re ok, $n+1$?

$$(x+y)^{n+1}=(x+y)(x+y)^n=(x+y)\cdot\sum_{k=0}^{n}\binom{n}{k}\cdot x^{n-k}\cdot y^k=$$

$$=\sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}\cdot y^k+\sum_{k=0}^{n}\binom{n}{k}\cdot x^{n-k}\cdot y^{k+1}$$

[Mennyi $x^{(n+1)-k}\cdot y^k$ együtthatója? tx első Σ-ban: $\binom{n}{k}$,
a másodikban: $\binom{n}{k+1}$
Tudjuk: $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$ ✓ [$k=(n+1)$-re ✓]
0 ✓]

<u>Összevonásokkal</u>

$x^{n+1-j}\cdot y^j$ együtthatója

$j=0$ bal oldali Σ, $\binom{n}{0}=1=\binom{n+1}{0}$ együtthatóval

$j=n+1$ csak a jobb Σ $\binom{n}{n}=1=\binom{n+1}{n+1}$ együtthatóval

$1\le j\le n$ közötti j-re bal oldali Σ: $k=j$ $\binom{n}{j}$
jobb oldali Σ: $k=j-1$ $\binom{n}{j-1}$

<u>összesen</u>: $x^{n+1-j}\cdot y^j$ együtthatója: $\binom{n}{j}+\binom{n}{j-1}=\binom{n+1}{j}$

<u>összevonások után</u>

$$(x+y)^{n+1}=\sum_{j=0}^{n+1}\binom{n+1}{j}\cdot x^{n-j+1}\cdot y^j$$

<u>Polinomiális tétel</u>

Egységelemes kommutatív gyűrűben, $n\ge 1$

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

$i_1, i_2 \dots i_r\in\mathbb{N}$

$i_1+i_2+\dots+i_r=n$

Pl.:

$$(x+y+z)^3 = \sum_{i+j+k=3} \frac{3!}{i!j!k!} \cdot x^i y^j z^k$$

$i,j,k \in \mathbb{N}$

$i+j+k=3$

111 $\rightarrow \frac{3!}{1!1!1!} \cdot x^1 y^1 z^1 = 6xyz$

210 $\rightarrow \frac{3!}{2!1!0!} \cdot x^2 y^1 z^0 = 3x^2 y$

300

201

102

120

012

021

003 $\rightarrow \frac{3!}{0!0!3!} \cdot x^0 y^0 z^3 = z^3$

030

Áll.: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

biz.:

$$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = \sum_{k=0}^{n} \binom{n}{k}$$

lényege: a Pascal Δ - soraiban az elemek összege 2 hatványa

Áll.: $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} \ldots = 0$ Ha a sorok elemeit váltakozó előjellel adjuk össze, akkor 0 lesz.

$$\sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} = 0$$

biz.: $0^n = (1-1)^n = (1+(-1))^n = \sum_{k=0}^{n} \binom{n}{k} \cdot 1^{n-k} \cdot (-1)^k$

biz.: indukció r-re

$r = 0, 1$ ✓

$r = 2$ binom. tétel

$(r-1)$-re ok, r-re?

$$(x_1+x_2+\ldots x_r)^n = ((x_1+x_2\ldots+x_{r-1})+x_r)^n \overset{\text{binom. tétel miatt}}{=}$$

$$= \sum_{i_r=0}^{n} \binom{n}{i_r} (x_1+x_2\ldots+x_{r-1})^{n-i_r} x_r^{i_r} \overset{\text{ind. miatt}}{=}$$

$$= \sum_{i_r=0}^{n} \sum \binom{n}{i_r} \frac{(n-i_r)!}{i_1! i_2! \ldots i_r!} \cdot x_1^{i_1} x_2^{i_2} \ldots x_r^{i_r}$$

$i_1 \ldots i_{r-1} \in \mathbb{N}$

$i_1 + \ldots + i = n - i_r$

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

logikai szita

$A_1, A_2, \ldots A_n$ véges halmazok

$$|A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n| = |A_1| + |A_2| + |A_3| \ldots + |A_n| - |A_1 \cap A_2| - |A_1 \cap A_3| -$$

$$- \ldots - |A_1 \cap A_n| - |A_2 \cap A_3| \ldots - |A_{n-1} \cap A_n| + |A_1 \cap A_2 \cap A_3| + \ldots$$

páronkénti metszetek

3-as metszetek

$$\mp (-1)^n \cdot |A_1 \cap A_2 \cap \ldots \cap A_n|$$

Skatulyaelv

Ha X, Y véges halmazok, és $|X| > |Y|$, akkor nem létezik $f: X \to Y$ injektív fv. [nincs elég hely Y-ban]

Megj.: $|X| > |Y| \Rightarrow \nexists f: Y \to X$ szürjektív [fordított megfogalmazás]

pl.: 99 skatulyában elhelyezünk 100 kavicsot, akkor lesz olyan skatulya, ahová legalább 2 kavics kerül.

Fibonacci-számok

$1, 1, 2, 3, 5, 8 \dots$

$F_1 = 1$

$F_2 = 1$

$F_n = F_{n-1} + F_{n-2}$

$n \geq 3$

Homogén sorozat, ami könnyen számolható: $1, \alpha, \alpha^2, \alpha^3, \dots \alpha^k$

szabály: $\alpha^n = \alpha^{n-1} + \alpha^{n-2} \quad / : \alpha^{n-2}$

$$\alpha^2 = \alpha + 1$$

$$\alpha^2 - \alpha - 1 = 0 \to \alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}$$

$1, \alpha, \alpha^2, \dots \quad \alpha = 1{,}618$ (aranymetszés száma)

$1, \beta, \beta^2, \dots \quad \beta = -0{,}618$

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$ → Fib. számok zárt alakja

Fibonacci vektorsorozat

$$\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}3\\2\end{pmatrix}, \begin{pmatrix}5\\3\end{pmatrix}, \begin{pmatrix}8\\5\end{pmatrix}, \dots \begin{pmatrix}F_{n+1}\\F_n\end{pmatrix}$$

Számelmélet

Def.: $n, m \in \mathbb{N}$

n osztható m-mel (n az m többszöröse / m az n osztója)

ha $\exists k \in \mathbb{N}: k \cdot m = n$

jele: $m | n$ [m osztója n-nek] pl.: $2|6$, $23|69$

Megj.: ha $m \neq 0$: $m | n \Leftrightarrow \frac{n}{m} \in \mathbb{N}$

Tétel: $\mathbb{N}$-en az osztathatóság tulajdonságai

① Ha $m|n$ és $m'|n'$, akkor $mm'|nn'$

biz.: ha $n=mk$, $n'=m'k'$ $\Rightarrow nn'=(mm')(kk')$

② $\forall m: \ m|0$

biz.: $k=0$ [k lehet 0]

③ $\forall n: \ 0|n \Rightarrow n=0$

④ $\forall n: \ 1|n$

⑤ Ha $m|n \Rightarrow mt|nt$ [①-es speciális esete]

pl.: $2|4 \Rightarrow 20|40$

⑥ $t\neq 0: \ mt|nt \Rightarrow m|n$ pl.: $20|40 \Rightarrow 2|4$

biz.: $mtk=nt \Rightarrow mk=n$

⑦ Ill. lineáris kombinációs tulajdonság

Ha $m|n_1, m|n_2, \dots, m|n_r$ és $t_1, t_2, \dots, t_r$ tetszőleges

$$m \Big| \sum_{i=1}^{r} t_i n_i = t_1 n_1 + t_2 n_2 \dots + t_r n_r$$

⑧ Ha $n\neq 0$ és $m|n$, akkor $m\leq n$

biz.: $mk \geq m\cdot 1 = m$

ha $k\geq 1$

⑨ Részben rendezés

itt osztója relációt reflexív [$n|n$ $n\cdot 1=n$]

antiszimm. [lásd: ⑧]

tranzitív [$m|n, n|r \Rightarrow m|r$
$mk=n$ $nl=r$ $m(kl)=r$]

Def.: Legyen R egy egységelemes integritási tartomány ($\mathbb{Z}$) → jellemzően

$n, m \in R$ $\quad$ m osztója n-nek

$m | n$, ha $\exists k : mk = n$ $\quad$ $\boxed{k \in R}$ → pl. $\mathbb{Z}$

Áll.: Az $\mathbb{N}$-en megismert tulajdonságok közül 1-7 teljesül (8 nem jó, 9 nem cancellativum)

Áll.: Ha $n, m \in \mathbb{Z}$: $m | n \Leftrightarrow |m| \,\big|\, |n|$

Def.: Egy R integritási tartományban m és n asszociáltak, ha $m | n$ és $n | m$ pl.: $-5, 5 \in \mathbb{Z}$

Áll.: az asszociáltság ekvivalenciareláció

Biz.: def. alapján

Áll.: Ha m és m' ill. n és n' asszociáltak

$m | n \Leftrightarrow m' | n \Leftrightarrow m' | n' \Leftrightarrow m | n'$

Def.: Az 1 asszociáltjait egységeknek hívjuk (pl.: -1 a $\mathbb{Z}$-ben)

Áll.: $x \in R$ egység

$\Updownarrow$ $\quad$ $\Leftrightarrow x$ $\forall n \in R$-nek osztója

$x | 1$ [hiszen $1 | x$] $\quad$ [$x | 1$, $1 | n \Rightarrow x | n$]

$\Leftrightarrow$ x-nek van inverze a szorzásra: $\exists k : xk = 1$

Áll.: n és m asszociáltak, ha egymás egységszeresei

$\exists x$ egység: $n = mx$

$n = mk$
$m = nl$
$n = nkl$
$1 = kl$ → x egység
$n = mx$
$xl = 1$
$m = mxl = ml$

Def.: Egy $f \in R$ felbonthatatlan (irreducibilis/törzsszám), ha minden olyan felírásban, melyre $f = a \cdot b$, $a, b \in R$ teljesül, hogy vagy a, vagy b egység; továbbá $f \neq 0$ és f nem egység

pl.: $\mathbb{Z}$-ben $\quad -7 = 7 \cdot (-1)$

$(-1) \cdot 7$

$1 \cdot (-7)$

$(-7) \cdot 1$

Def.: $n \in R$ összetett, ha nem 0, nem egység, és nem felbonthatatlan $(a + b\sqrt{5}i)$ alakú számoknál

$$6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$$

Def.: $p \in R$ prím, ha nem 0, nem egység, és $\forall a, b \in R$:
$p \mid ab \Rightarrow p \mid a \vee p \mid b$

$p = 2$ $\mathbb{Z}$-ben $\quad ab$ páros $\Rightarrow a \vee b$ páros

6 nem prím: $6 \mid 9 \cdot 20$, de $6 \nmid 9$, $6 \nmid 20$

Tétel: $\mathbb{N}$-ben végtelen sok prímszám van

biz.: tegyük fel, hogy véges sok prím van

$p_1, p_2, p_3 \dots p_n$ ekkor tekintsük az $x = p_1 \cdot p_2 \cdot p_3 \dots p_n + 1$ számot. Ha felbonthatatlan, akkor találtunk újat. Ha nem az, akkor valamelyik osztója biztosan az.

De: $p_1 \nmid x$, $p_2 \nmid x$, $\dots$ $p_n \nmid x$ mert $p_j \mid x - 1$ és két szomszédos szám nem lehet osztható ugyanazzal a $p_j \geq 2$ számmal. (eredeti feltevés így $\lightning$)

megj.: $\mathbb{Z}$-ben prím $\Leftrightarrow$ felbonthatatlan

Def.: legyen a és $b \in R$ → integritási tartomány

d az a és b LNKO-ja, ha

- $d \mid a$ és $d \mid b$ (közös osztó)
- $d' \mid a$ és $d' \mid b$, akkor $d' \mid d$ $(d' \leq d)$

megj.: Előre nem feltétlenül látszik, hogy ilyennek muszáj léteznie ($\mathbb{Z}$-ben van, de máshol nem minelig)

Def.: k az a és b LKKT-je, ha

- $a \mid k$ és $b \mid k$
- $a \mid k'$ és $b \mid k'$, akkor $k \mid k'$ $(k' \geq k)$

Áll.: $\mathbb{Z}$-ben $\forall a, b$-re $\exists d$ LNKO

biz.: megadunk egy algoritmust (Euklideszi algoritmus)

pl.: 172, 62 LNKO-ja

$172 = 62 \cdot 2 + 48$

$62 = 48 \cdot 1 + 14$

$48 = 14 \cdot 3 + 6$

$14 = 6 \cdot 2 + 2$ ← ez a visszatérési érték (az utolsó nem 0 maradék az LNKO)

$6 = 2 \cdot 3 + 0$

Az algoritmus véget ér, ha 0 a maradék.

Legyen a, b a bemenet, és $a = b \cdot q + r$ az első maradékos osztás. (itt: $172 = 62 \cdot 2 + 48$)

Áll.: ha $d' \mid a$ és $d' \mid b$, akkor $d' \mid r$

biz.: $r = a - b \cdot q$ (lineáris kombinációs tulajdonság miatt)

Áll.: Az algoritmus véget ér: a maradékok szigorúan monoton csökkennek, és a maradékok szorzata nemnegatív egészekből áll

Tétel: Legyen $a, b \in \mathbb{N}^+$, ekkor $\exists d \in \mathbb{N}^+$, melyre d egy LNKO-ja a-nak és b-nek és $\exists u, v \in \mathbb{Z}$ melyre $d = a \cdot u + b \cdot v$

pl.: $\underset{u}{3} \cdot 23 \underset{v}{-4} \cdot 17 = 1$

biz: bővített Euklideszi algoritmus (be: a, b)

① inicializálás

$r_0 \leftarrow a,\ r_1 \leftarrow b,\ x_0 \leftarrow 1,\ x_1 \leftarrow 0,\ y_0 \leftarrow 0,\ y_1 \leftarrow 1,\ n \leftarrow 0$

② ciklus

ha $r_{n+1} = 0$, akkor ki: r_n, x_n, y_n $[d, u, v]$

// maradj

$r_n = r_{n+1} \cdot q_{n+1} + r_{n+2}$

$x_{n+2} \leftarrow x_n - x_{n+1} \cdot q_{n+1}$

$y_{n+2} \leftarrow y_n - y_{n+1} \cdot q_{n+1}$

$n \leftarrow n + 1$

vissza a ciklus elejére

Pl.:

n	$r_{n-2} - r_{n-1} \cdot q_{n-1}$	r_n	x_n	y_n
0		172	1	0
1		62	0	1
2	$172 - 62 \cdot 2$	48	$1 - 0 \cdot 2 = 1$	$0 - 1 \cdot 2 = -2$
3	$62 - 48 \cdot 1$	14	$0 - 1 \cdot 1 = -1$	$1 - (-2) \cdot 1 = 3$
4	$48 - 14 \cdot 3$	6	$1 - (-1) \cdot 3 = 4$	$-2 - 3 \cdot 3 = -11$
5	$14 - 6 \cdot 2$	2	$-1 - 4 \cdot 2 = -9$	$3 - (-11) \cdot 2 = 25$
6	$6 - 3 \cdot 2$	0		

← kimenet $(2, -9, 25)$
↓
LNKO

$2 = 172 \cdot (-9) + 62 \cdot 25$

Tétel: Minden integritási tartományban p prím $\Rightarrow p$ felbonthatatlan

biz: $p = a \cdot b \Rightarrow p \mid ab \overset{p \text{ prím}}{\Rightarrow} p \mid a$ vagy $p \mid b$

Mondjuk $p \cdot k = a \Rightarrow p \cdot k \cdot b = a \cdot b = p$

$$\Downarrow$$

$$k \cdot b = 1$$

$$\Downarrow$$

b egység ✓

Tétel: $\mathbb{Z}$-ben f felbonthatatlan $\Rightarrow f$ prím

biz: $f \mid ab$ esetén ha $f \nmid a$:

LNKO f-re és a-ra: f osztói: $\pm 1, \pm f$

a osztói: ?, de $f, -f$ nem

LNKO: $1 = d = au + fv$ (eukl. alg.)

$1 = a \cdot u + f \cdot v \quad / \cdot b$

$b = \underbrace{a \cdot b}_{\text{osztható } f\text{-fel}} \cdot u + \underbrace{f \cdot v \cdot b}_{\text{osztható } f\text{-fel}} \Rightarrow f \mid b$ ✓

Tétel: a számelmélet alaptétele

Minden egész szám: $n \geq 2$ felírható prímek (felbonthatatlanok) szorzatakent és ez a felbontás lényegében egyértelmű (legfeljebb sorrendben és előjelekben térhet el)

Pl.: $21 = 3 \cdot 7, 7 \cdot 3, (-3) \cdot (-7), (-7) \cdot (-3)$

biz:

① létezik felbontás

Ha n prím: kész ✓

ha nem: $\exists n_1, n_2 < n$

$n_1, n_2 > 1$

$n = n_1 \cdot n_2$

$n_1 = p_1 p_2 \dots p_r \qquad n_2 = q_1 q_2 \dots q_s$

$n = p_1 p_2 \dots p_r q_1 \dots q_s$

② egyértelműség (indirekt biz.)

Ha $\exists n$, melynek két lényegesen különböző felbontása van, akkor $\exists$ legkisebb ilyen: n

két felbontás

$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$

p_1 prím és $p_1 \mid q_1 q_2 \dots q_s \Rightarrow \exists k: p_1 \mid q_k$

de q_k is prím $\Rightarrow p_1 = \pm q_k$

$\frac{n}{p_1} = \pm \frac{n}{q_k}$ egy még kisebb szám két felbontással $\lightning$

Tétel: Ha $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$ alakú, ahol $p_1, p_2 \dots p_r$ páronként különböző poz. prímek és $\alpha_1, \alpha_2 \dots \geq 1$ [kanonikus alak], akkor n pozitív osztói pontosan a $k = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ alakú számok, ahol $\forall i: 0 \leq \beta_i \leq \alpha_i$

tz osztók száma: $(\alpha_1+1)(\alpha_2+1) \cdot (\alpha_r+1)$

pl.: $60 = 2^2 \cdot 3^1 \cdot 5^1$ (kanonikus alak)

osztók: $\underset{0,1,2}{2^{\square}}, \underset{0,1}{3^{\square}}, \underset{0,1}{5^{\square}}$ $12 = 3 \cdot 2 \cdot 2$ db

bíz: $k|n$, mert $k(p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \dots p_r^{\alpha_r-\beta_r}) = n$

másrészt ha q prímre $k|n$ $q|k \Rightarrow q|n \Rightarrow$ ilyen alakú

$\pm q \in \{p_1, p_2, \dots, p_r\}$

$p_1^{\beta_1} | n \Rightarrow \beta_1 \leq \alpha_1$, mert ha $\beta_1 > \alpha_1$: $p_1^{\beta_1-\alpha_1} \Big| n / p_1^{\alpha_1-\beta_1} = p_r$

áll: Ha $n_1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $n_2 = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$

ahol $0 \leq \alpha_i, \beta_i$ (módosított kanonikus alak)

p_1, p_2 páronként különözek

akkor a pozitív LNKO, LKKT:

$$LNKO = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_1,\beta_1)} \dots p_r^{\min(\alpha_1,\beta_1)}$$

$$LKKT = p_1^{\max(\alpha_1,\beta_1)} \dots p_r^{\max(\alpha_1,\beta_1)}$$

megj.: általánosítható több számra is

bíz: az előző tétel következménye

áll: $\mathbb{Z}$-ben ha $a, b \geq 1$, $a \cdot b = \text{lnko}(a,b) \cdot \text{lkkt}(a,b)$

megj.: LNKO ill. LKKT nem egyértelmű, de $\pm$ előjel erejéig az

tétel: $\alpha + \beta = \min(\alpha, \beta) + \max(\alpha, \beta)$

Def: a és b- relatív prímek, ha LNKO-juk 1 (és -1)

megjj: Pontosan akkor lesznek a, b- ≥ 2 relatív prímek, ha nincs közös prímosztójuk

Def: $a_1, a_2, \dots a_n$: relatív prímek (LNKO=1)

páronként relatív prímek: $\forall i, j \quad i < j \quad LNKO(a_i, a_j) = 1$

tétel: Ha a és b- relatív prímek, és $a \mid b \cdot c$ akkor $a \mid c$

biz: b·c-ben szerepel „a" minden prímosztója $\Rightarrow$ c-ben is, mert b- nem tartalmazza őket

pl.: $17 \mid 52700 = 527 \cdot 100 \Rightarrow 17 \mid 527$

$6 \mid 17 \cdot n = 6 \mid n$

tétel: $a \mid b \cdot c \Leftrightarrow \frac{a}{\text{lnko}(a,b)}$

biz: Ha a és b- nem relatív prímek, akkor $d = \text{lnko}(a, b)$

$\frac{a}{d}$ és $\frac{b}{d} \in \mathbb{Z}$ relatív prím

$\frac{a}{\cancel{d}} \cdot \cancel{d} \mid \frac{b}{\cancel{d}} \cdot \cancel{d}\, c \Leftrightarrow \underbrace{\frac{a}{d} \mid \frac{b}{d}}_{\text{rel. prím}} \cdot c \Leftrightarrow \frac{a}{d} \mid c$

Jelölés: Ha két számnak ugyanaz a maradéka m-mel osztva, akkor kongruensek modulo m $[a \equiv b \pmod{m}]$

pl.: $27 \equiv 32 \pmod 5$

Def: legyenek a, b-, m egészek. $a \equiv b \pmod{m}$, ha $m \mid a - b$

tétel: maradékos osztás

$\forall a, b \in \mathbb{Z}, \quad b \neq 0$

$\exists! \quad q, r : a = b \cdot q + r \qquad 0 \leq r \leq |b| - 1$

egyértelműen létezik

tétel: $a \equiv b \pmod{m} \Leftrightarrow$ a és b ugyanazt a maradékot adja m-mel osztva

biz: $a \equiv m \cdot q_1 + r_1$

$b \equiv m \cdot q_2 + r_2 \qquad a - b = m \cdot (q_1 - q_2) + (r_1 - r_2)$

Tehát $a \equiv b \pmod{m} \Leftrightarrow m \mid a - b \Leftrightarrow m \mid r_1 - r_2 \Leftrightarrow$

$\Leftrightarrow r_1, r_2 \in \{0, 1, \dots |m| - 1\} \Leftrightarrow r_1 = r_2$

pl.: $62 \equiv 13 \ (7)$

a mod-ot elhagyhatjuk

$62 = 7 \cdot 8 + \boxed{6}$

$13 = 7 \cdot 1 + \boxed{6}$

tétel: $\equiv \pmod{m}$ kongruencia ekvivalencia-reláció

biz: (reflexivitás)

$m \mid a - a = 0 \quad \forall a$-ra ✓

(szimmetria) $m \mid a - b \Rightarrow m \mid b - a \quad \forall a, b$ ✓

(tranzitivitás) $m \mid a - b, \ m \mid b - c \Rightarrow m \mid a - c$

igaz, mert $(a - b) \setminus (b - c) = a - c \quad \forall a, b, c$

Def: A kongruencia szerinti osztályokat „modulo m maradékosztályok"-nak hívjuk

mod 10

0			
10 - 10	1 - 9	2 - 3	⋮
20 - 20	11 - 19	12 - 13	
30 - 30	21 - 29	22 - 23	
⋮	⋮	⋮	

Áll.: Ha $a \equiv b\ (m)$ és $c \equiv d\ (m)$ akkor ① $a+c \equiv b+d\ (m)$
② $a-c \equiv b-d\ (m)$ ③ $a \cdot c \equiv b \cdot d\ (m)$

pl.: $7 \cdot 3 \equiv 1\ (10)$

biz.: ① és ②

$m \mid a-b$ és $m \mid c-d \rightarrow m \mid (a-b) \pm (c-d)$

vagyis $m \mid (a+c)-(b+d) \Leftrightarrow a+c \equiv b+d\ (m)$

$m \mid (a-c)-(b-d) \Leftrightarrow a-c \equiv b-d\ (m)$

③ $ac - bd = \underbrace{ac - bc}_{(a-b)c} + bc - bd$

$(a-b)c + b(c-d) \Rightarrow m \mid ac - bd$

osztható m-mel

Következmény: ≡ olyan, mint egy egyenlet

$x \equiv y\ (m) \quad | \cdot 3$ $\qquad$ $x+4 \equiv z\ (m) \quad | -4$

$3x \equiv 3y\ (m)$ $\qquad$ $x \equiv 3\ (m)$

Mi a helyzet az osztással?

$cx \equiv cy\ (m)$
$\Downarrow ?$
$x \equiv y\ (m)$

Nem, pl.: $6 \cdot x \equiv 6 \cdot y\ (10)$

$6 \cdot 3 \equiv 6 \cdot 8 \equiv 8\ (10)$

$\not\Downarrow$

$3 \equiv 8\ (10)$ nem ok!

Áll: legyen $c, m \in \mathbb{Z}$, $d = LNKO(c, m)$ ekkor

$$cx \equiv cy \ (m)$$
$$\Downarrow$$
$$x \equiv y \ (\text{mod } \tfrac{m}{d})$$

bíz: $m \mid c(x-y)$

$$\Updownarrow$$

$$\frac{m}{d} \mid \frac{c}{d}(x-y)$$

$\frac{m}{d}$ és $\frac{c}{d}$ prímosztói diszjunktak

(ha nem az lenne, akkor az LNKO meg növelhető lenne

$$\Downarrow$$

$$\frac{m}{d} \mid x-y \Rightarrow x \equiv y \ (\text{mod } \tfrac{m}{d})$$

Maradékosztálygyűrűk

$\mathbb{Z}_m$, a modulo m maradékosztályokból áll, a köv. műveletekkel: $+, \cdot$

→ gyűrűt kapunk

$\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$0 \cdot x = x \cdot 0 = 0$

·	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

„a·b osztva 6-tal" maradék

$$6x \equiv 6y \ (10)$$

$$10 \mid 6(x-y)$$

$$5 \mid 3(x-y)$$

$$5 \mid x-y$$

Tehát

$$3x \equiv 3y \ (10)$$
$$\Updownarrow$$
$$x \equiv y \ (10)$$

[mert rel. prímek, le lehet osztani 3-mal]

Áll: Ha p prím, akkor $\mathbb{Z}_p$ test:

$\forall a \neq 0,\ a \in \mathbb{Z}_p$ esetén $\exists a^{-1}$ $a \cdot a^{-1} = 1$

pl.: $a = 4$ $\quad p = 17$

$\exists x : ax \equiv 1 \ (17)$

$x = 13 \qquad 4 \cdot 13 = 52 \equiv 1 \ (17)$

biz: bőv. eukl. alg. p, a -val

$LNKO \cdot 1 = p \cdot u + a \cdot v$

mod p

$1 \equiv p \cdot u + a \cdot v \ (p)$

$1 \equiv a \cdot v$

lineáris kongruenciák megoldása

legyen $a, m, b \in \mathbb{Z}$

$ax \equiv b \ (m)$ // keressük meg az x-eket!

pl.: Mi az x utolsó 2 jegye, ha a $34x$ utolsó két jegye 92?

$\underline{\quad |?|?|} \qquad 34 \cdot \underline{\quad |9|2|}$

$34x \equiv 92 \ (\text{mod } 100)$

megoldás: bőv. eukl. alg., a és m bemenettel