Bevezetés az algebrába – az egész számok

Wettl Ferenc

V. 15-09-11

- Egész számok: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ (*Zahlen*, $\mathbf{Z}$)
- Pozitív egész számok: $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ (*Natural*, $\mathbf{N}^+$)
- Nemnegatív egész számok: $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ ($\mathbf{N}_0$)
- Természetes számoknak az előző két halmaz valamelyikét szokás nevezni, nincs egységes terminológia. Jelölése: $\mathbb{N}$ ($\mathbf{N}$).
- A természetes számok halmazára igaz, hogy **bármely nem üres részhalmazának van legkisebb eleme** (az e tulajdonsággal rendelekző halmazokat jólrendezett halmazoknak nevezzük).
- Az egészek halmaza nem jólrendezett halmaz.
- Valós számok halmaza: $\mathbb{R}$ ($\mathbf{R}$).

Definíció

- Racionális számok: $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$, a nem racionális valósokat irracionális számoknak nevezzük. (*Quotient*, $\mathbf{Q}$)
- Algebrai számok: gyökei valamely egész együtthatós polinomnak (pl. $\sqrt{2}$ gyöke a $x^2 - 2$ polinomnak). A racionális számok is algebrai számok. A nem algebrai számokat transzcendens számoknak nevezzük (pl. π, e).

Tétel

A $\sqrt{2}$ irracionális.

Bizonyítás.

Indirekt bizonyítás: tegyük fel, hogy $\sqrt{2}$ racionális, azaz van olyan p és q természetes szám, hogy $\sqrt{2} = \frac{p}{q}$. Ekkor $p = \sqrt{2}q$, tehát az

$$K = \{\sqrt{2}k \mid k, \sqrt{2}k \in \mathbb{N}^+\}$$

halmaz nem üres. Legyen K legkisebb eleme $a = \sqrt{2}b$ (ilyen van!).
$\sqrt{2}a = 2b$ egész $\rightsquigarrow$ $\sqrt{2}a - a = \sqrt{2}a - \sqrt{2}b = \sqrt{2}(a-b)$ is egész.
Ugyanakkor pozitív, mert $a = \sqrt{2}b > b$,
és kisebb a-nál, azaz $\sqrt{2}(a-b) < a = \sqrt{2}b$, mert $a = \sqrt{2}b < 2b$.
Ellentmondás! (Lásd még: cut-the-knot)

□

Definíció

Egy x valós szám (alsó) egész részén azt a legnagyobb egészt értjük (jelölése $\lfloor x \rfloor$ vagy $[x]$), mely kisebb vagy egyenlő x-szel, azaz melyre $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$. x tört része $\{x\} = x - \lfloor x \rfloor$.

- $\lfloor 0 \rfloor = 0$, $\lfloor -\frac{1}{1000} \rfloor = -1$, $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$, $\{\frac{9}{4}\} = \frac{1}{4}$, $\{-\frac{9}{4}\} = \frac{3}{4}$.
- hasonlóan definiálható a felső egész rész: $\lceil x \rceil - 1 < x \leqslant \lceil x \rceil$.
- $\lceil \pi \rceil = 4$, $\lceil -\pi \rceil = -3$.
- $0 \leqslant \{x\} < 1$.

Tétel (Dirichlet approximációs tétele)

Tetszőleges $x \in \mathbb{R}$ valós számhoz és tetszőleges $n \in \mathbb{N}^+$ számhoz létezik olyan $a, b \in \mathbb{Z}$, ahol $1 \leqslant a \leqslant n$, hogy

$$|ax - b| < \frac{1}{n}.$$

Bizonyítás.

A skatulyaelv szerint a 0, $\{x\}$, $\{2x\}$,..., $\{nx\}$ számok között van kettő, amelyik azonos intervallumba esik a következők közül: $[0, \frac{1}{n})$, $[\frac{1}{n}, \frac{2}{n})$, $[\frac{2}{n}, \frac{3}{n})$,... $[\frac{n-1}{n}, 1)$.

Legyen $|\{ix\} - \{jx\}| < \frac{1}{n}$, ahol $i < j$ és $a = j - i$, $b = \lfloor jx \rfloor - \lfloor ix \rfloor$.

$$\begin{aligned} |ax - b| &= |(j-i)x - (\lfloor jx \rfloor - \lfloor ix \rfloor)| \\ &= |jx - \lfloor jx \rfloor - (ix - \lfloor ix \rfloor)| \\ &= |\{jx\} - \{ix\}| < \frac{1}{n}. \end{aligned}$$

□

- Indukció: következtetés az egyes esetekből az általánosra (általában bizonyos valószínűséggel).
- Teljes indukció (mathematical induction): ha egy n paramétertől függő állítás igaz valamely $n_0 \in \mathbb{N}_0$ kezdőértékre, és az állítás öröklődik egy egészről az 1-gyel nagyobb egészre, akkor igaz minden n-re, melyre $n \geqslant n_0$.

Tétel (Teljes indukció)

Ha $H \subseteq \mathbb{N}^+$, $1 \in H$, és $n \in H$ esetén $n+1 \in H$, akkor $H = \mathbb{N}^+$.

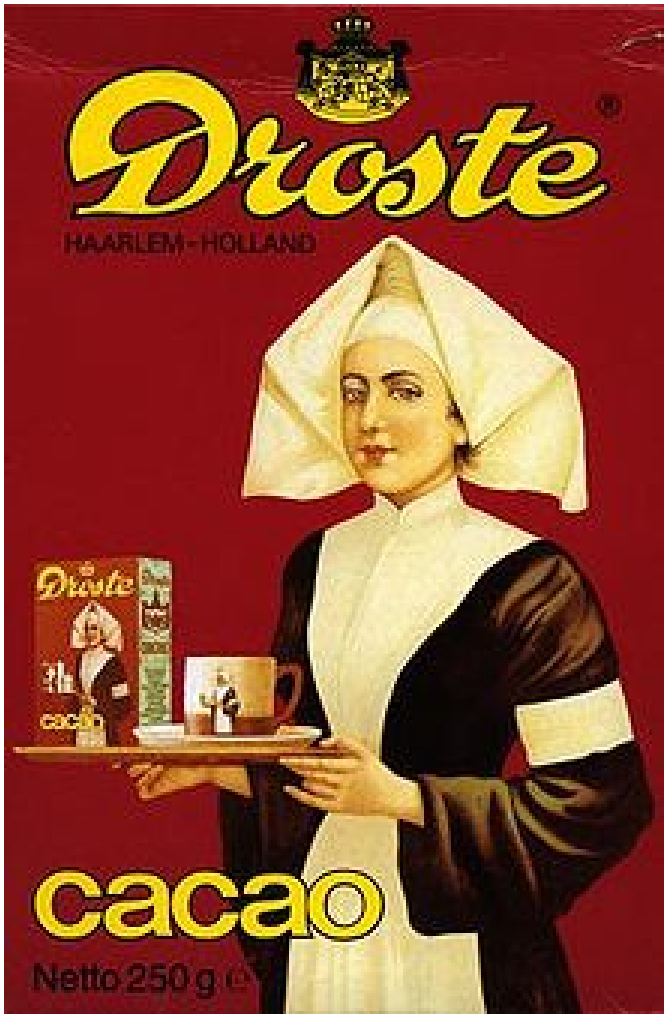
- Gondoljuk meg: a teljes indukció következik a természetes számok jólrendezettségéből!

P Igazoljuk, hogy $\sum_{k=1}^{n} k = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

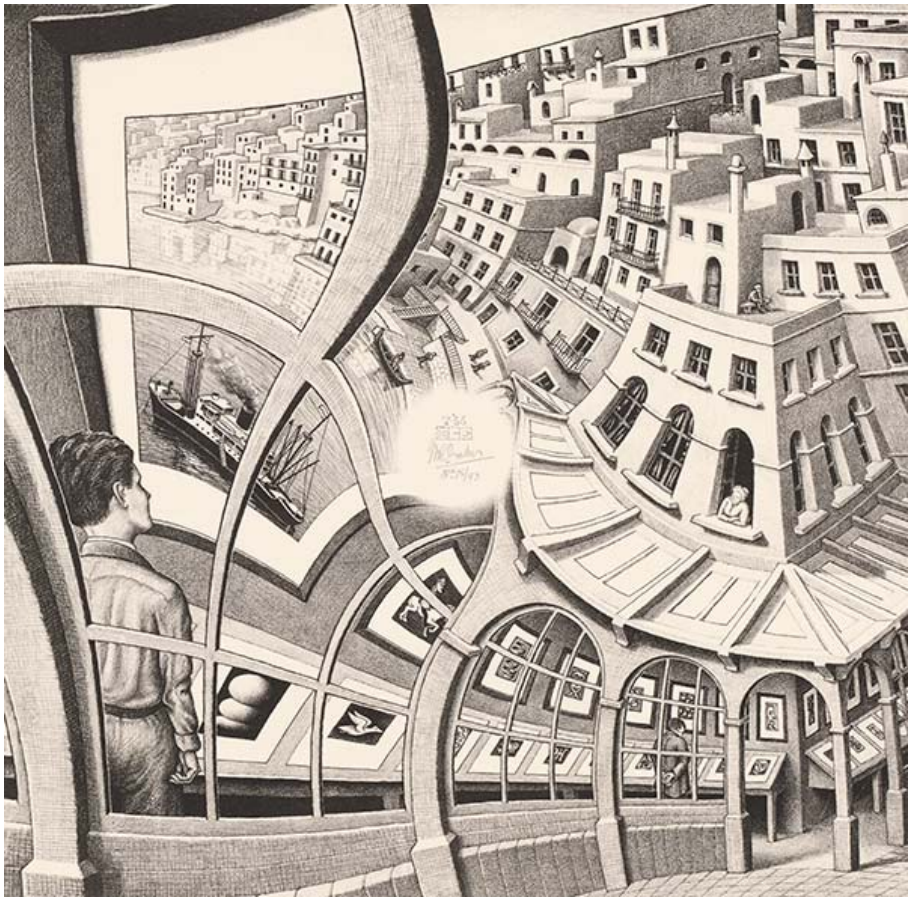
M n-re vonatkozó teljes indukcióval:

- $n = 1$ esetén: $1 = 1$.
- $(1 + 2 + \ldots + n) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$.


VERSENY
CIPŐPASZTA


Droste
HAARLEM - HOLLAND
cacao
Netto 250 g

Escher: Print Gallery



http://escherdroste.math.leidenuniv.nl/

https://www.youtube.com/watch?v=wzfTzj2tiew

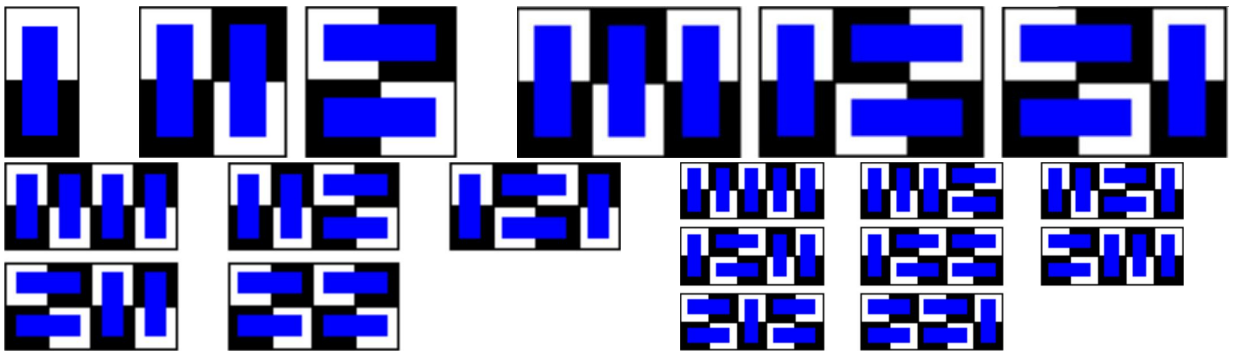
Rekurzió: valamely objektum önhasonló módon való konstrukciója, definíciója, értelmezése.

Rekurzív sorozat: a sorozat n-edik tagjának definíciójában a kisebb indexű tagok is szerepelnek.

Definíció (Fibonacci-sorozat)

$f_0 = 0$, $f_1 = 1$, $f_n = f_{n-1} + f_{n-2}$ (első néhány tagja: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, . . . , (OEIS A000045)

- Hányféleképp fedhető le egy $2 \times (n-1)$-es sakktábla $n-1$ dominóval?

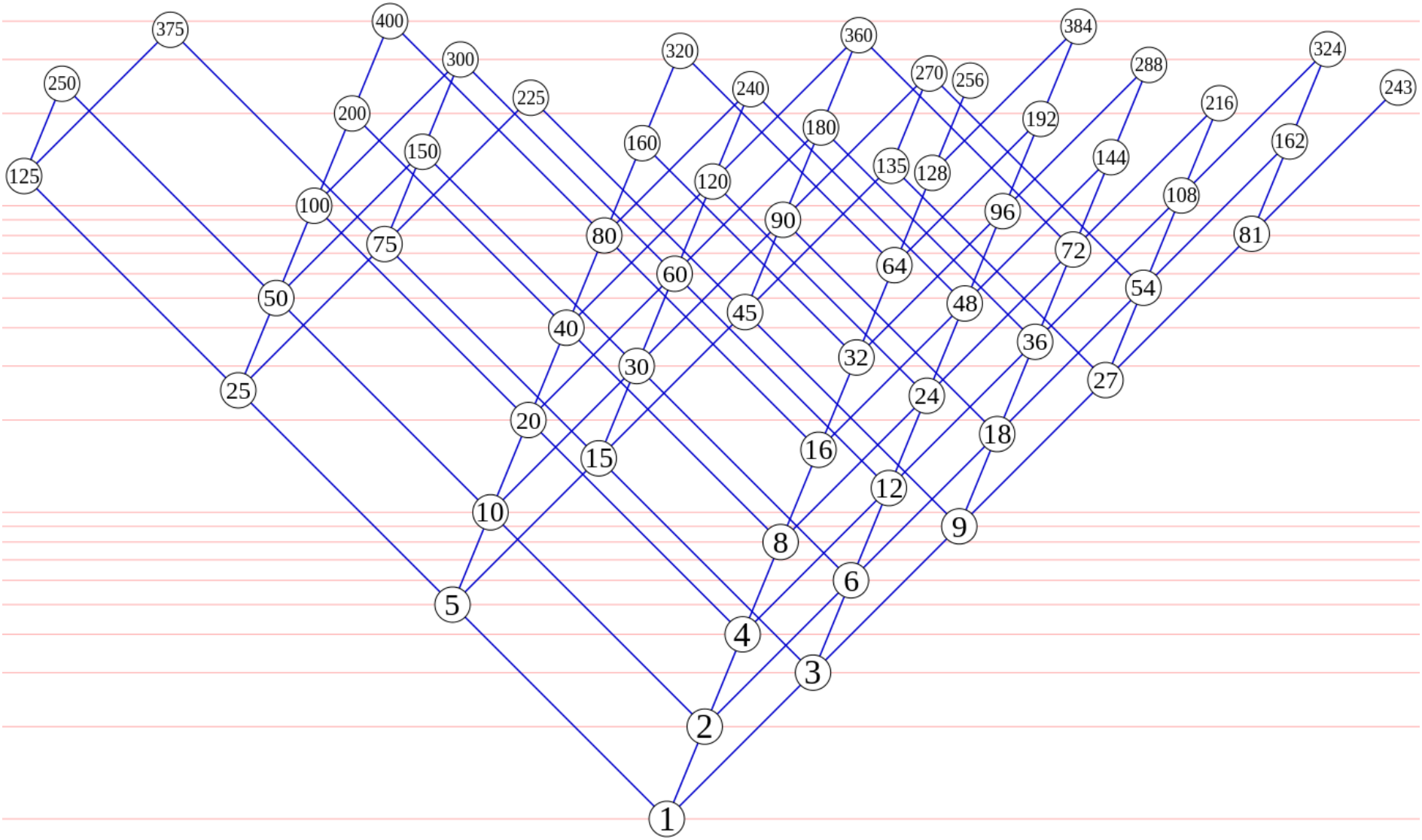


Definíció

A b egész számot az a egész szám osztójának nevezzük (a osztható b-vel, a többszöröse b-nek, jelölése $b \mid a$), ha van olyan q egész, hogy $a = bq$.

- b valódi osztó, ha nem azonos $\pm a$-val vagy ± 1-gyel.
- 0 minden egésszel osztható, a 0-val is: $0 = b \cdot 0$.
- a 0 csak a 0-nak osztója.
- $-5 \mid 15$, $5 \mid -15$, $-5 \mid -15$, $2 \mid 0$, $0 \mid 0$, $7 \nmid 8$,
- Az oszthatóság hasonlóképp definiálható pl. az egész vagy a valós együtthatós polinomok körében: $x - 1 \mid x^3 - 1$, mert $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

K A páros számok körében mit mondhatunk? Pl. van minden (páros) számnak (páros) osztója?



ábra : A prímek közül csak 2-vel, 3-mal és 5-tel osztható 400 alatti számok oszthatósági diagramja (Hasse-diagram) ("Regular divisibility lattice" by David Eppstein az angol Wikipédiáról)

Tétel (Az oszthatóság alaptulajdonságai)

Minden a, b, c, m, n egészekre igazak a következők

- $a \mid a$
- *ha* $a \mid b$ *és* $b \mid c$, *akkor* $a \mid c$
- *ha* $a \mid b$ *és* $a \mid c$, *akkor* $a \mid (mb + nc)$
- *ha* $a \mid b$ *és* $m \mid n$, *akkor* $am \mid bn$

P Bizonyítsuk be, hogy egy egész szám négyzete vagy osztható 4-gyel, vagy 8-cal osztva 1-et ad maradékul!

M $(2k)^2 = 4k^2$, $(2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k+1)$, de k és $k+1$ egyike osztható 2-vel.

P $7 \mid 3^{2n+1} + 2^{n+2}$ $(n \in \mathbb{N})$

M $3^{2n+1} + 2^{n+2} = 3 \cdot 9^n + 4 \cdot 2^n = 3 \cdot (9^n - 2^n) + 3 \cdot 2^n + 4 \cdot 2^n$ és $7 \mid 9^n - 2^n$, $7 \mid 3 \cdot 2^n + 4 \cdot 2^n$.

Definíció

Egységnek nevezzük azokat a számokat, melyek minden számnak osztói.

- Az egészek közt két egység van: 1, -1. (Miért?)
- Az egység nem tévesztendő össze az egységelemmel, mely egy algebrai struktúra azon e eleme, melyre $ea = a$ minden a-ra.

K A páros számok körében van-e egység?

P Az $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ számhalmazban a szokásos műveletek mellett a $\pm(1+\sqrt{2})^n$ alakú számok egységek, ahol n tetszőleges egész (például $(1+\sqrt{2})^3 \mid 13 - 77\sqrt{2}$). (Igazolható, hogy más egység nincs).

M $(1+\sqrt{2})(-1+\sqrt{2}) = 1$, így $(1+\sqrt{2})$ és annak minden nemnegatív egész hatványa is oszt minden $a + b\sqrt{2}$ alakú számot. Hasonlóképp a negatív egész kitevős hatványai is, mivel $1/(1+\sqrt{2}) = -1+\sqrt{2}$.

Tétel (Maradékos osztás nemnegatív maradékkal)

Tetszőleges $a, b \in \mathbb{Z}$, $b \neq 0$ egészekhez egyértelműen léteznek olyan $q, r \in \mathbb{Z}$ egészek, hogy

$$a = bq + r, \text{ és } 0 \leqslant r < |b|$$

P Osszuk el maradékosan a-t b-vel, ha $|a| = 20$ és $|b| = 7$.

M Négy eset lehetséges: $20 = 7 \cdot 2 + 6$, $-20 = 7 \cdot (-3) + 1$, $20 = (-7) \cdot (-2) + 6$, $-20 = (-7) \cdot 3 + 1$.

- A tételbeli $0 \leqslant r < |b|$ feltételt kicserélhető erre: $-\left\lfloor \frac{|b|}{2} \right\rfloor < r \leqslant \left\lfloor \frac{|b|}{2} \right\rfloor$. Ekkor a **nemnegatív maradék** helyett a **legkisebb abszolút értékű maradékot** kapjuk.

M Az előző példabeli számokkal: $20 = 7 \cdot 3 - 1$, $-20 = 7 \cdot (-3) + 1$, $20 = (-7) \cdot (-3) - 1$, $-20 = (-7) \cdot 3 + 1$.

Bizonyítás.

Olyan q egészt keresünk, melyre bq a legnagyobb egész, mely nem nagyobb a-nál.

$$\begin{array}{ll} \text{ha } b>0: & bq \leqslant a < bq+b \\ \text{ha } b<0: & bq \leqslant a < bq-b \end{array} \quad \rightsquigarrow \quad \begin{array}{l} q \leqslant \frac{a}{b} < q+1 \\ q \geqslant \frac{a}{b} > q-1 \end{array} \quad \rightsquigarrow \quad \begin{array}{l} q = \left\lfloor \frac{a}{b} \right\rfloor \\ q = \left\lceil \frac{a}{b} \right\rceil \end{array}$$

és így az $r = a - bq$ számra $0 \leqslant r < |b|$. Mivel q a fentiek alapján egyértelmű, ezért r is. □

Tétel (b-alapú számrendszer)

Legyen $b > 1$ egész szám. Ekkor bármely $m \in \mathbb{N}^+$ szám egyértelműen előáll

$$m = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0, \quad 0 \leqslant a_i < b, \quad a_n \neq 0$$

alakban.

- Az m szám b-alapú számrendszerbeli alakját $(a_n a_{n-1} \ldots a_1 a_0)_b$ jelöli (a zárójel vagy a b index a elhagyható, ha nem okoz félreértést).
- Ha $b > 10$, a számjegyeket az ábécé betűivel pótoljuk, pl. a 16-os számrendszer számjegyei: 0, 1,. . . ,9, A, B, C, D, E, F.
- $26 = 26_{10} = 1A_{16} = 32_8 = 122_4 = 11010_2 = 101_5 = 10_{26}$.

Bizonyítás.

Ha van ilyen alakú előállítása m-nek, akkor a_0 csak a b-vel való maradékos osztás maradéka lehet. Ezt ismételve a számjegyek egyértelműen adódnak:

$$
\begin{aligned}
m &= bq_0 + a_0, & 0 \leqslant a_0 < b, \quad & q_0 = a_n b^{n-1} + \ldots + a_2 b + a_1 \\
q_0 &= bq_1 + a_1, & 0 \leqslant a_1 < b, \quad & q_1 = a_n b^{n-2} + \ldots + a_3 b + a_2 \\
q_1 &= bq_2 + a_2, & 0 \leqslant a_2 < b, \quad & q_2 = a_n b^{n-3} + \ldots + a_4 b + a_3 \\
&\vdots & & \\
q_{n-2} &= bq_{n-1} + a_{n-1}, & 0 \leqslant a_{n-1} < b, \quad & q_{n-1} = a_n \\
q_{n-1} &= b \cdot 0 + a_n, & 0 < a_n < b &
\end{aligned}
$$

A maradékos osztások láncolata addig tart, míg valamely osztás hányadosa 0 nem lesz. Ez véges sok lépésben megtörténik, mert $m > q_0 > q_1 > \cdots > q_{n-1} > 0$. Az a_i számok pedig valóban m kívánt előállítását adják, mert $((\ldots(a_n b + a_{n-1})b + \ldots)b + a_1)b + a_0 = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0 = m$. □

Állítás (Horner-módszer polinom kiértékelésére)

Bármely n-edfokú polinom kiértékelhető legföljebb n szorzás és n összeadás használatával, ugyanis

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = (\ldots((a_n x + a_{n-1})x + a_{n-2})x + \ldots + a_1)x + a_0.$$

- A polinom kiértékelése egy egyszerű táblázatban követhető:

	a_n	a_{n-1}	$\ldots$	a_0
x	a_n	$a_n x + a_{n-1}$	$\ldots$	$(\ldots(a_n x + a_{n-1})x + \ldots + a_1)x + a_0$

P Legyen $p(x) = x^5 - 3x^4 - 6x^3 - 90x + 3$. Határozzuk meg $p(5)$ értékét!

M $5^5 = 3125$, így a természetes mód hosszadalmas. Horner módszerrel:

	1	−3	−6	0	−90	3
5	1	2	4	20	10	53

Tehát $p(5) = 53$.

- A Horner módszer további alkalmazásaira később visszatérünk.

P Írjuk át az alábbi számokat 10-es számrendszerbe: 110100101_2, 1201201_3, AAF_{16}. Használjuk a Horner-módszert!

M

	1	1	0	1	0	0	1	0	1
2	1	3	6	13	26	52	105	210	421

	1	2	0	1	2	0	1
3	1	5	15	46	140	420	1261

	A	A	F
16	10	$16 \cdot 10 + 10$	$16 \cdot 170 + 15$
16	10	170	2735

P Használjuk az ismételt maradékos osztás technikáját az alábbi számok megadott számrendszerbe való átírására!
$1001 = X_2$, $27648 = Y_3$, $6252 = Z_5$

M $X = 1111101001$

1001		
500	1	$1001 = 2 \cdot 500 + 1$
250	0	$500 = 2 \cdot 250 + 0$
125	0	$250 = 2 \cdot 125 + 0$
62	1	$125 = 2 \cdot 62 + 1$
31	0	$62 = 2 \cdot 31 + 0$
15	1	$31 = 2 \cdot 15 + 1$
7	1	$15 = 2 \cdot 7 + 1$
3	1	$7 = 2 \cdot 3 + 1$
1	1	$3 = 2 \cdot 1 + 1$
0	1	$1 = 2 \cdot 0 + 1$

$Y = 1101221000$

27648	
9216	0
3072	0
1024	0
341	1
113	2
37	2
12	1
4	0
1	1
0	1

$Z = 200002$

6252	
1250	2
250	0
50	0
10	0
2	0
0	2

Definíció

Az $a, b \in \mathbb{Z}$ számok legnagyobb közös osztója az a d szám, mely

1. közös osztó, azaz $d \mid a$ és $d \mid b$,
2. a közös osztók közül a legnagyobb, azaz ha $c \mid a$ és $c \mid b$, akkor $c \leqslant d$,
3. az $a = b = 0$ esetben $d = 0$.

Jelölések: $d = (a, b)$, $d = \text{lnko}(a, b)$, $d = \gcd(a, b)$ (az angol 'greatest common divisor' kifejezésből)

- A definíció első két feltétele bármely két a, b egész szám legnagyobb közös osztóját egyértelműen definiálja, kivéve ha $a = b = 0$. Ekkor a közös osztók halmaza felülről nem korlátos (a 0 minden egész számmal osztható), ezért nincs a közös osztók közt legnagyobb. A következőkben minden esetre érvényes eredményekhez fogunk jutni a $(0, 0) = 0$ kikötéssel.

P 12 és 18 közös osztói: ± 1, ± 2, ± 3, ± 6, így $(12, 18) = 6$.

P $(12, 6) = (-12, 6) = 6$, $(12, 8) = (-12, -8) = 4$, $(12, 7) = 1$

P Ha $m, n \in \mathbb{Z}$, akkor $(m, 0) = (0, m) = |m|$, $(m, mn) = (mn, m) = |m|$,

Definíció

Az $a, b \in \mathbb{Z}$ számok kitüntetett közös osztója az a $d \in \mathbb{N}_0$ szám, mely

1. közös osztó, azaz $d \mid a$ és $d \mid b$,
2. ha $c \mid a$ és $c \mid b$, akkor $c \mid d$.

- A lényeges változás az előző definícióhoz képest, hogy a $c \leqslant d$ feltételt a $c \mid d$ feltételre cseréltük, vagyis csak az oszthatóság fogalmát használjuk, a számok rendezését nem. A másik változás, hogy – mivel az oszthatóságon egy egységgel való szorzás nem változtat – csak a nemnegatív számokra szorítkozunk ($d \in \mathbb{N}_0$).
- Látni fogjuk, hogy e két fogalom azonos eredményt ad, ezért nem vezetünk be új jelölést.
- E definíció a $(0, 0) = 0$ értéket is természetes módon adja.

P 12 és 18 közös osztói: ± 1, ± 2, ± 3, ± 6. Látjuk, hogy e számok közül a 6 az az egyetlen nemnegatív szám, mely e számok mindegyikével osztható, tehát 6 a kitüntetett közös osztó.

Tétel

Bármely két egész számnak létezik kitüntetett közös osztója.

Bizonyítás.

Ha $b = 0$, akkor $(a, b) = |a|$, ha $b \mid a$, akkor $(a, b) = |b|$. Tegyük fel, hogy $b \nmid a$ és az egységes jelölés érdekében legyen $r_0 = a$, $r_1 = b$. Osszuk el maradékosan a-t b-vel, a maradék legyen r_2, majd b-t osszuk r_2-vel...

$$
\begin{array}{lll}
r_0 = r_1 q_1 + r_2 & r_n \mid r_0 = a & c \mid r_2 = r_0 - r_1 q_1 \\
r_1 = r_2 q_2 + r_3 & r_n \mid r_1 = b & c \mid r_3 = r_1 - r_2 q_2 \\
r_2 = r_3 q_3 + r_4 & r_n \mid r_2 & c \mid r_4 = r_2 - r_3 q_3 \\
\quad\vdots & & \\
r_{n-2} = r_{n-1} q_{n-1} + r_n & r_n \mid r_{n-2} & c \mid r_n = r_{n-2} - r_{n-1} q_{n-1} \\
r_{n-1} = r_n q_n & r_n \mid r_{n-1} &
\end{array}
$$

Tehát $d = r_n$ kitüntetett közös osztó. Az algoritmus véges lépésben véget ér, mivel $r_2 > r_3 > \cdots > r_n > 0$. □

- A kitüntetett közös osztó egyértelmű, ugyanis ha c és d is kitüntetett közös osztó, akkor $c \mid d$ és $d \mid c$ miatt c és d egymás egységszerese, ami c és d nemnegativitása miatt csak $c = d$ mellett lehetséges.
- A kitüntetett és a legnagyobb közös osztó megegyezik. Jelölje d a kitüntetett, D a legnagyobb közös osztót. d definíciója miatt $D \mid d$, így $D \leqslant d$, D definíciója miatt $d \leqslant D$, tehát $d = D$.
- A tételbeli algoritmust euklideszi algoritmusnak nevezzük. Leegyszerűsítve legyen $r_0 = a$, $r_1 = b$, ahol $a \geqslant b > 0$. Ismételten végezzük el az $r_k = r_{k+1}q_{k+1} + r_{k+2}$ maradékos osztásokat, ahol $0 \leqslant r_{k+2} < r_{k+1}$. Az algoritmus leáll, amint valamely maradék 0 nem lesz, azaz ha $r_{n+1} = 0$. Ekkor a kitüntetett közös osztó r_n.

P $(24, 17) =?$, $(288, 204) =?$

M Válasz: $(24, 17) = 1$, $(288, 204) = 12$, ugyanis

$$\begin{aligned} 24 &= 17 \cdot 1 + 7 \\ 17 &= 7 \cdot 2 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 \end{aligned} \qquad \begin{aligned} 288 &= 204 \cdot 1 + 84 \\ 204 &= 84 \cdot 2 + 36 \\ 84 &= 36 \cdot 2 + 12 \\ 36 &= 12 \cdot 3 \end{aligned}$$

T Ha $c > 0$, akkor $(ca, cb) = c(a, b)$.

T Ha $(a, b) = d \neq 0$, akkor $(\frac{a}{d}, \frac{b}{d}) = 1$.

D Az a és b egészeket relatív prímeknek nevezzük, ha $(a, b) = 1$.

K A törtek egyszerűsíthetők. (Fogalmazzuk meg az állítást!)

T $(a + nb, b) = (a, b)$ $(a, b, n \in \mathbb{Z})$

B $c \mid a, b \rightsquigarrow c \mid a + nb$. $c \mid a + nb, b \rightsquigarrow c \mid a + nb - nb = a$

T (a, b) kifejezhető a és b alkalmas $m, n \in \mathbb{Z}$ egészekkel vett lineáris kombinációjaként, azaz kifejezhető $(a, b) = ma + nb$ alakban.

B Az euklideszi algoritmus első egyenletéből r_2, a következőből $r_3, \ldots,$ az utolsó előttiből r_n kifejezhető a és b lineáris kombinációjaként. (Ezt nevezzük kibővített euklideszi algoritmusnak).

K Bármely a, b egészre $\{ma + nb \mid m, n \in \mathbb{Z}\} = \{c(a, b) \mid c \in \mathbb{Z}\}$.

T Ha $c \mid ab$ és $(c, a) = 1$, akkor $c \mid b$.

B (első) $c \mid ab$, $c \mid cb \rightsquigarrow c \mid (ab, cb) = (a, c)b = b$.

B (második) $(c, a) = 1 \rightsquigarrow 1 = mc + na \rightsquigarrow b = mcb + nab \rightsquigarrow c \mid b$.

Példa

Kibővített euklideszi algoritmussal határozzuk meg a következő lineáris kombinációk együtthatóit:
(1) $(24, 17) = 24m + 17n$, *(2)* $(288, 204) = 288m + 204n$.

Megoldás.

$$\begin{aligned} 24 &= 17 \cdot 1 + 7 & 7 &= 24 - 17 \\ 17 &= 7 \cdot 2 + 3 & 3 &= 17 - 2 \cdot 7 = -2 \cdot 24 + 3 \cdot 17 \\ 7 &= 3 \cdot 2 + 1 & 1 &= 7 - 2 \cdot 3 = 5 \cdot 24 - 7 \cdot 17 \\ 3 &= 1 \cdot 3 \end{aligned}$$

Tehát $(24, 17) = 5 \cdot 24 - 7 \cdot 17 = 1$. Az euklideszi algoritmus egyenleteinek 12-vel való szorzása adja a másik feladat megoldását:
$(288, 204) = 5 \cdot 288 - 7 \cdot 204 = 12$. □

Megoldás.

Egyszerűen mechanikussá tehető az előző számítás, ha egyenlőségek lineáris kombinációit számoljuk:

$$\begin{aligned} 24 &= 1 \cdot 24 + 0 \cdot 17 \\ 17 &= 0 \cdot 24 + 1 \cdot 17 \\ 7 &= 1 \cdot 24 - 1 \cdot 17 \\ 3 &= -2 \cdot 24 + 3 \cdot 17 \\ 1 &= 5 \cdot 24 - 7 \cdot 17 \end{aligned}$$

Táblázatban a hányadost is jelölve az első oszlopban (mindkét feladatra):

	24	1	0
1	17	0	1
2	7	1	-1
2	3	-2	3
3	1	5	-7

	288	1	0
1	204	0	1
2	84	1	-1
2	36	-2	3
3	12	5	-7

□

A diofantoszi egyenlet 2- vagy több ismeretlenes egyenlet, melynek csak egész megoldásait keressük.

- Lineáris diofantoszi egyenlet: $ax + by = c$, $(a, b, c \in \mathbb{Z})$
- Pitagorászi számhármasok: $x^2 + y^2 = z^2$
- Nagy Fermat-tétel (Wiles, 1995): $x^n + y^n = z^n$ nem oldható meg, ha $n > 2$.
- $x^3 + y^3 + z^3 = w^3$ $(3^3 + 4^3 + 5^3 = 6^3)$
- $x^4 + y^4 + z^4 = w^4$ (Elkies, 1986: $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$, a legkisebb Frye, 1988: $95800^4 + 217519^4 + 414560^4 = 422481^4$)
- Hardy–Ramanujan-szám: $x^3 + y^3 = z^3 + w^3$ legkisebb nemtriviális megoldása: $1^3 + 12^3 = 9^3 + 10^3 = 1729$.
- Két négyzetszám összege: $x^2 + y^2 = n$ (a $4k - 1$ alakú prímek páros kitevőn)
- Pell-egyenlet: $x^2 - ny^2 = \pm 1$.

Tétel

Legyen $d = (a, b)$. Az $ax + by = c$ lineáris diofantoszi egyenlet pontosan akkor oldható meg, ha $d \mid c$. Ekkor az összes megoldás fölírható $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, ahol t tetszőleges egész.

Bizonyítás.

($\Rightarrow$) Ha $ax_0 + by_0 = c$ megoldás, akkor $d \mid a$, $d \mid b \rightsquigarrow d \mid ax_0 + by_0 = c$.
($\Leftarrow$) Legyen $am + bn = d$. Ha $d \mid c$, azaz $c = td$, akkor $atm + btn = c$.
Ha x_0, y_0 megoldás, akkor $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$ is, ugyanis

$$ax + by = ax_0 + a\frac{b}{d}t + by_0 - b\frac{a}{d}t = ax_0 + by_0 = c.$$

Ha $ax + by = c$ egy tetszőleges megoldás, akkor kivonva a két egyenletet:

$$a(x - x_0) = b(y_0 - y) \rightsquigarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

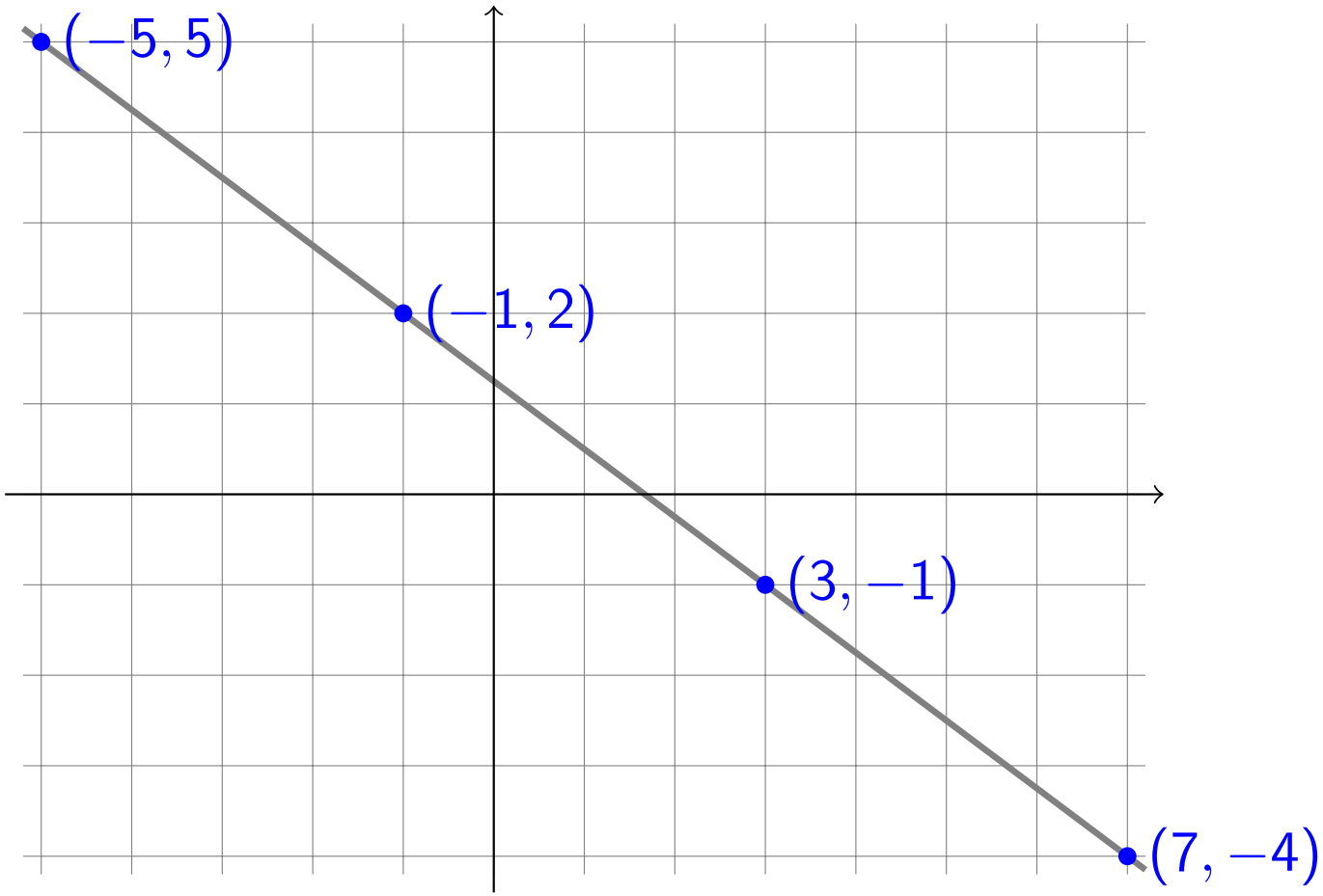
Mivel $(\frac{a}{d}, \frac{b}{d}) = 1$, ezért $\frac{a}{d} \mid (y_0 - y) \rightsquigarrow y = y_0 - \frac{a}{d}t \rightsquigarrow x = x_0 + \frac{b}{d}t$. □

P $3x + 4y = 5$

M $(3, 4) = 1 \mid 5 \rightsquigarrow$ megoldható.

$1 = 4 - 3 \rightsquigarrow 5 = 3 \cdot (-5) + 4 \cdot 5 \rightsquigarrow x = -5 + 4t,\ y = 5 - 3t$

A megoldások geometriai szemléltetése (a $3x + 4y = 5$ egyenes és 4 megoldás):



P Épp 12000€-t fizetett egy cég néhány 288€ és néhány 204€ értékű árúért. Melyikből mennyit vásárolt, ha az elsőből többet vett, mint a másodikból?

M Diofantoszi egyenlet: $288x + 204y = 12000$, ahol $x, y > 0$ egészek.

Megoldható, mert $(288, 204) = 12 \mid 12000$ (hány pozitív közülük?)

A megoldások halmaza megegyezik a $24x + 17y = 1000$ egyenlet megoldásaival (miért?).

Egy megoldást ad a kibővített euklideszi algoritmus:
$1 = (24, 17) = 5 \cdot 24 - 7 \cdot 17 \rightsquigarrow 5000 \cdot 24 - 7000 \cdot 17 = 1000.$

Összes megoldás: $(5000 + 17t)24 + (-7000 - 24t)17 = 1000.$

$5000 + 17t > 0$, azaz $t > -\frac{5000}{17} \approx -294.1$, $-7000 - 24t > 0$, azaz $t < -\frac{7000}{24} \approx -291.7 \rightsquigarrow t = -294, -293, -292.$

A lehetséges $\{x, y\}$ párok: $\{36, 8\}$, $\{19, 32\}$, $\{2, 56\}$.

Tehát az elsőből 36-ot, a másodikból 8-at vásároltak.