

BME



BUDAPESTI MŰSZAKI
MATEMATIKA
ÉS GAZDASÁGTUDOMÁNYI
INTÉZET
EGYETEM



Bevezetés az algebraba 1

BMETE92AX23



Egész számok

H406 2017-09-04,06,08,11



Wettl Ferenc

ALGEBRA TANSZÉK

Egész számok és sorozataik

Egész számok és sorozataik

Számok

- Egész számok: $\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, 3, \dots \}$ (Zahlen, \mathbf{Z})
- Pozitív egész számok: $\mathbb{N}^+ = \{ 1, 2, 3, \dots \}$ (Natural, \mathbf{N}^+)
- Nemnegatív egész számok: $\mathbb{N}_0 = \{ 0, 1, 2, 3, \dots \}$ (\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 rendelkező halmazokat **jólrendezett halmazoknak** nevezzük).
- Az egészek halmaza nem jólrendezett halmaz.
- Valós számok halmaza: \mathbb{R} (\mathbf{R}).
- A természetes számok rendelkeznek az **arkhimédészi tulajdonsággal** (Arkhimédészi axióma): Minden $x \in \mathbb{R}$ valós számhoz van olyan n természetes szám, hogy $x < n$.

- D **Racionális számok:** $\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \right\}$, a nem racionális valósokat **irracionális** számoknak nevezzük. (*Quotient*, \mathbf{Q})
- D **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).

T A $\sqrt{2}$ irracionális.

B 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 a

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

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 $a = \sqrt{2}b > b$, hisz $\sqrt{2} > 1$,

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](#))

Egész számok és sorozataik

Egészrész függvény

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

- $\lfloor 0 \rfloor = 0$, $\lfloor -\frac{1}{1000} \rfloor = -1$, $\lfloor 12.81 \rfloor = 12$, $\lfloor -12.81 \rfloor = -13$, $\lfloor \pi \rfloor = 3$,
 $\lfloor -\pi \rfloor = -4$,
- $\{\frac{9}{4}\} = \frac{1}{4}$, $\{-\frac{9}{4}\} = \frac{3}{4}$.

D **Felső egész rész:** $\lceil x \rceil - 1 < x \leq \lceil x \rceil$.

- $\lceil 12.81 \rceil = 13$, $\lceil -12.81 \rceil = -12$, $\lceil \pi \rceil = 4$, $\lceil -\pi \rceil = -3$,
- $0 \leq \{x\} < 1$.

F Igazoljuk, hogy $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = \lfloor 2x \rfloor$

F Igazoljuk, hogy $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$

T 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 $1 \leq a \leq n$, hogy

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

B A **skatulyaelv** szerint a $0, \{x\}, \{2x\}, \dots, \{nx\}$ számok között van kettő, amelyek azonos intervallumba esik a következők közül:

$$[0, \frac{1}{n}), [\frac{1}{n}, \frac{2}{n}), [\frac{2}{n}, \frac{3}{n}), \dots, [\frac{n-1}{n}, 1).$$

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

$$|ax - b| = |(j - i)x - (\lfloor jx \rfloor - \lfloor ix \rfloor)|$$

$$= |jx - \lfloor jx \rfloor - (ix - \lfloor ix \rfloor)|$$

$$= |\{jx\} - \{ix\}| < \frac{1}{n}.$$

T Diofantoszi (diofantikus) approximáció

Tetszőleges x irracionális számhoz végtelen sok olyan b/a tört létezik, melyre

$$\left| x - \frac{b}{a} \right| < \frac{1}{a^2}$$

- m Feltehető, hogy $a > 0$.
- m Ha b/a kielégíti a fenti egyenlőtlenséget, akkor csak véges sok bővítése van, ami ugyancsak kielégíti.
- m Ennél több is igazolható, nevezetesen az is igaz, hogy végtelen sok olyan b/a tört létezik, melyre

$$\left| x - \frac{b}{a} \right| < \frac{1}{2a^2}$$

B A Dirichlet-approximációból

$$\left| x - \frac{b}{a} \right| < \frac{1}{na} \leq \frac{1}{a^2}$$

x irracionális $\rightsquigarrow \exists n'$: $\left| x - \frac{b}{a} \right| > \frac{1}{n'}$. A Dirichlet-approximáció adja a b'/a' törtet.

$$\left| x - \frac{b'}{a'} \right| < \frac{1}{n'a'} \leq \frac{1}{n'} < \left| x - \frac{b}{a} \right|.$$

$\rightsquigarrow \frac{b'}{a'} \neq \frac{b}{a}$, hasonlóan folytatható.

F Hamis-e az állítás racionálisokra?

m $|\sqrt{2} - \frac{7}{5}| \approx 0.0142 < 0.04 = \frac{1}{25}$
 $|\sqrt{2} - \frac{8}{6}| \approx 0.08088 > 0.02\dot{7} = \frac{1}{36}$,
 $|\sqrt{2} - \frac{9}{6}| \approx |-0.085786| > 0.02\dot{7} = \frac{1}{36}$
 $|\pi - \frac{22}{7}| \approx |-0.00126| < 0.0029 < \frac{1}{7^3}$

m **Pi Day**: 3/14, március 14; Pi Approximation Day: 22/7, július 22.

Egész számok és sorozataik

Indukció

- 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 egészeről az 1-gyel nagyobb egészre, akkor igaz minden n -re, melyre $n \geq n_0$.

T **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!
- A teljes indukció egy másik változata következik az előzőből:

T Ha a P állítás „igaz n_0 -ra”, és „ha igaz valamely n esetén minden $n_0, n_0 + 1, \dots, n$ egészre, akkor igaz $n + 1$ -re is”, akkor P igaz minden $n \geq n_0$ egészre.

$$P \quad \sum_{k=1}^n k(k+1) = \frac{n(n+1)(n+2)}{3}$$

M Leosztva 2-vel a következő alakot kapjuk:

$$\sum_{k=1}^n \binom{k+1}{2} = \binom{n+2}{3}$$

(1. mo) teljes indukció: $n = 1$ esetén $\binom{2}{2} = \binom{3}{3}$ ✓

$n \Rightarrow n + 1$:

$$\sum_{k=1}^{n+1} \binom{k+1}{2} = \sum_{k=1}^n \binom{k+1}{2} + \binom{n+2}{2} = \binom{n+2}{3} + \binom{n+2}{2} = \binom{n+3}{3}$$

(2. mo) kombinatorikai: $n + 3$ elemből úgy választhatunk ki kettőt, hogy sorba rakjuk őket, kivesszük az elsőt (az első n elem közül), majd a másik kettőt a sorban hátrébb lévők közül.

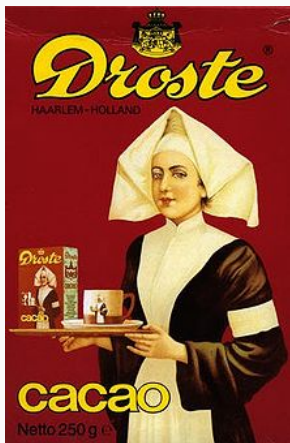
$$F \quad \sum_{k=1}^n k^2 = 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

F Hány éle van egy n -csúcsú fának?

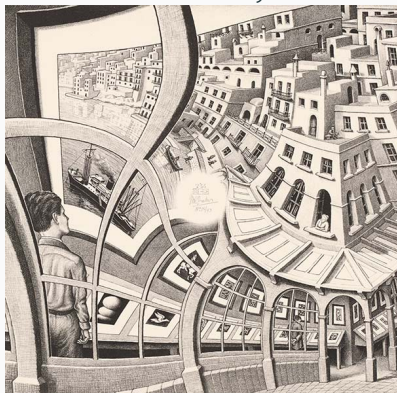
[Útmutatás: hagyjuk el a fa egy tetszőleges élet]

Egész számok és sorozataik

Rekurzió



Escher: Print Gallery



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

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

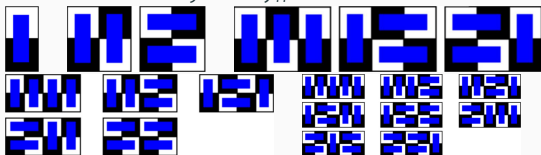
Rekurzió: valamely objektum önhasonló módon való konstrukciója, definíciója, értelmezése.

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

D **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))

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

M Grafikus bizonyítás: f_n .



m [The Fibonacci Quarterly](#) 1963 óta jelenik meg negyedévente.

- F **Általánosított Fibonacci-sorozat:** Legyen $g_n = g_{n-1} + g_{n-2}$, $g_0 = a$, $g_1 = b$. Igazoljuk, hogy $g_n = af_{n-1} + bf_n$.
- F Hány olyan részhalmaza van az $\{1, 2, \dots, n\}$ halmaznak, melyben nincs két szomszédos szám?
- F Hány olyan n -hosszú sorozat képezhető az 1, 2, 3, 4 számokból, melyek 1-gyel kezdődnek, és minden szám pontosan 1-gyel különbözik az előzőtől?
- F Mennyivel egyenlő az alábbi n törtvonalat tartalmazó tört:

$$1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\ddots + \frac{1}{1 + 1}}}}}$$

Egész számok és sorozataik

Lánctörtek*

! $x \in \mathbb{R}$, $a_0 = [x]$, $x_1 = \{x\}$,

$x_1 \neq 0$ esetén $a_1 = \left[\frac{1}{x_1} \right]$, $x_1 = \left\{ \frac{1}{x_1} \right\}$, így $x = a_0 + \frac{1}{a_1 + x_2}, \dots$

$x_n \neq 0$ esetén $a_n = \left[\frac{1}{x_n} \right]$, $x_{n+1} = \left\{ \frac{1}{x_n} \right\}$, így

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n + x_{n+1}}}}}$$

J $x = [a_0, a_1, a_2, \dots, a_n + x_{n+1}]$

ha valamely n -re $x_{n+1} = 0$, akkor $x = [a_0, a_1, a_2, \dots, a_n]$,

egyébként x **végtelen lánctört alakja** $[a_0, a_1, a_2, \dots, a_n, \dots]$,

melynek $[a_0, a_1, a_2, \dots, a_n]$ az n -edik szelete.

P $\sqrt{2}$ lánctört alakja: $\sqrt{2} = [1, 2, 2, 2, \dots]$ (A040000)

M $x = \sqrt{2}$, $a_0 = 1$, $x_1 = \sqrt{2} - 1$, $\frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1)$,
 $a_1 = 2$, $x_2 = \sqrt{2} - 1, \dots$

$$1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots + \frac{1}{2 + \frac{1}{\ddots}}}}}$$

P $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots]$ (A003417),

$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, \dots]$ (A001203),

$\frac{\sqrt{5}+1}{2} = [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \dots]$ (A000012), az aranymetszés aránya (a kisebbik úgy aránylik a nagyobbikhoz, mint a nagyobbik az egészhez).

T Egy szám lánctört alakja pontosan akkor véges, ha a szám racionális.

T Ha az x irracionális szám lánctört alakja $[a_0, a_1, a_2, \dots, a_n, \dots]$, és n -edik szelete $[a_0, a_1, a_2, \dots, a_n] = \frac{r_n}{s_n}$, ahol r_n és s_n relatív prímek, akkor minden n -re

$$\left| x - \frac{r_n}{s_n} \right| < \frac{1}{s_n^2},$$

és bármely két egymást követő szelet legalább egyikére

$$\left| x - \frac{r_n}{s_n} \right| < \frac{1}{2s_n^2}$$

is fennáll.

P π szeletei: $3 = [3]$, $22/7 = [3, 7]$, $333/106 = [3, 7, 15]$,
 $355/113 = [3, 7, 15, 1]$, $103993/33102 = [3, 7, 15, 1, 292]$,
 $104348/33215 = [3, 7, 15, 1, 292, 1], \dots$

Oszthatóság

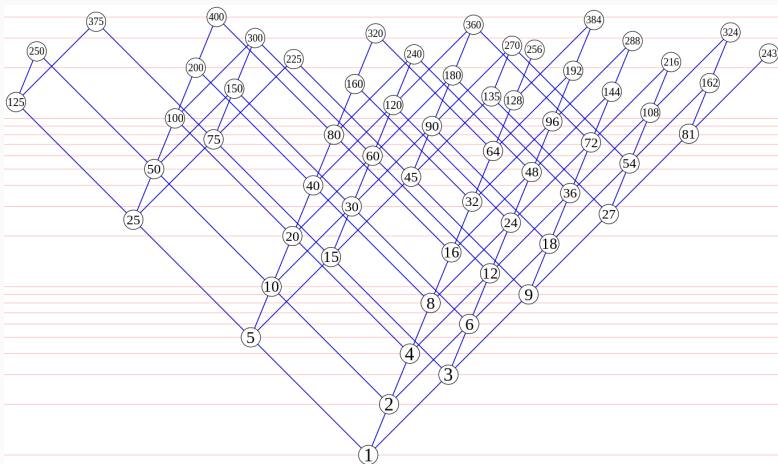
Oszthatóság

Osztó

D Osztó

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.
 - $a \mid 0 \forall a \in \mathbb{Z}$ (0-val is: $0 = b \cdot 0$).
 - a 0 csak a 0-nak osztója,
 - $\pm 1 \mid a \forall a \in \mathbb{Z}$,
 - $a \mid b, b \neq 0 \Rightarrow |a| \leq |b|$,
 - $-5 \mid 15, 5 \mid -15, -5 \mid -15, 2 \mid 0, 0 \mid 0, 7 \nmid 8$,
 - Az oszthatóság hasonlóképp definiálható pl. az egész vagy a valós együtthatós polinomok körében: $x - 1 \mid x^3 - 1$, mert $x^3 - 1 = (x - 1)(x^2 + x + 1)$.
- ? 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)

- F Hány olyan 400-nál kisebb pozitív egész szám van, mely nem osztható a 2, 3, 5 számok egyikével sem?

T 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 (1. mo) teljes indukció: $n = 0$ esetén $7 \mid 3 + 2^2$ ✓

$$n \Rightarrow n + 1: 3^{2n+3} + 2^{n+3} = 2(3^{2n+1} + 2^{n+2}) + 7 \cdot 3^{2n+1}$$

$$(2. mo) 3^{2n+1} + 2^{n+2} = 3 \cdot 9^n + 4 \cdot 2^n = 3 \cdot (9^n - 2^n) + 3 \cdot 2^n + 4 \cdot 2^n$$

és $7 \mid 9^n - 2^n$, $7 \mid 3 \cdot 2^n + 4 \cdot 2^n$.

Oszthatóság

Egység

D Egység

Egységnek nevezzük azokat a számokat, melyek minden számnak osztói.

- Az egészek közt két egység van: 1 , -1 . (Miért?)
- Az egység nem tévesztendő össze az **egységelem**mel, mely egy algebrai struktúra azon e eleme, melyre $ea = a$ minden a -ra.
- ? 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. (Igazolható, hogy más egység nincs).
- M $\pm(1 + \sqrt{2})(-1 + \sqrt{2}) = \pm 1$, így $\pm(1 + \sqrt{2})$ és annak minden nemnegatív egész hatványa is oszt minden $a + b\sqrt{2}$ alakú számot. Hasonlóképp a negatív egész kitevős hatványai is, mivel $1/(1 + \sqrt{2}) = -1 + \sqrt{2}$.

Oszthatóság

Maradékos osztás

T Maradékos osztás nemnegatív maradékkal

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

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

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

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

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

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

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

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

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

Oszthatóság

Számrendszerek

T b -alapú számrendszer

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

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

alakban.

- Az m szám b alapú számrendszerbeli alakját $(a_n a_{n-1} \dots a_1 a_0)_b$ jelöli (a zárójel vagy a b index 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.
 - $26 = 26_{10} = 1A_{16} = 32_8 = 122_4 = 11010_2 = 101_5 = 10_{26}$.
- F Hogyan írunk át b alapú számot és b^k alapúvá és fordítva?
- F Írjuk át a 110111010010001_2 számot 8-as és 16-os, valamint az $AE1F_{16}$ számot 2-es számrendszerbe!

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

$$m = bq_0 + a_0, \quad 0 \leq a_0 < b, \quad q_0 = a_n b^{n-1} + \dots + a_2 b + a_1$$

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b, \quad q_1 = a_n b^{n-2} + \dots + a_3 b + a_2$$

$$q_1 = bq_2 + a_2, \quad 0 \leq a_2 < b, \quad q_2 = a_n b^{n-3} + \dots + a_4 b + a_3$$

⋮

$$q_{n-2} = bq_{n-1} + a_{n-1}, \quad 0 \leq a_{n-1} < b, \quad q_{n-1} = a_n$$

$$q_{n-1} = b \cdot 0 + a_n, \quad 0 < a_n < b$$

A maradékos osztások láncolata addig tart, míg valamely osztás hányadosa 0 nem lesz. Ez véges sok lépésben megtörténik, mert $m > q_0 > q_1 > \dots > q_{n-1} > 0$. Az a_i számok pedig valóban m kívánt előállítását adják, mert

$$((\dots (a_n b + a_{n-1})b + \dots)b + a_1)b + a_0 = a_n b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0 = m.$$

Á Horner-módszer polinom kiértékelésére

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

$$\begin{aligned} & a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \\ &= (\dots ((a_n x + a_{n-1})x + a_{n-2})x + \dots + a_1)x + a_0. \end{aligned}$$

- A polinom kiértékelése egy egyszerű táblázatban követhető:

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

- P** Legyen $p(x) = x^5 - 3x^4 - 6x^3 - 90x + 3$. $p(5) = ?$

- M** A behelyettesítés hosszadalmas ($5^5 = 3125$). Horner-módszer:

	1	-3	-6	0	-90	3
5	1	2	4	20	10	53

Tehát $p(5) = 53$.

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 $X = 1111101001$

$Y = 1101221000$

$Z = 200002$

1001	2		27648	3		6252	5
500	1	$1001 = 2 \cdot 500 + 1$	9216	0		1250	2
250	0	$500 = 2 \cdot 250 + 0$	3072	0		250	0
125	0	$250 = 2 \cdot 125 + 0$	1024	0		50	0
62	1	$125 = 2 \cdot 62 + 1$	341	1		10	0
31	0	$62 = 2 \cdot 31 + 0$	113	2		2	0
15	1	$31 = 2 \cdot 15 + 1$	37	2		0	2
7	1	$15 = 2 \cdot 7 + 1$	12	1			
3	1	$7 = 2 \cdot 3 + 1$	4	0			
1	1	$3 = 2 \cdot 1 + 1$	1	1			
0	1	$1 = 2 \cdot 0 + 1$	0	1			

Közös osztók

Közös osztók

Legnagyobb közös osztó

D Legnagyobb közös osztó (lnko, gcd)

Az $a, b \in \mathbb{Z}$ számok **legnagyobb közös osztója** az a d egész 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 $c \leq d$,
 3. az $a = b = 0$ esetben $d = 0$.
- Jelölések: $d = (a, b)$, $d = \text{lnko}(a, b)$, $d = \text{gcd}(a, b)$ (az angol 'greatest common divisor' kifejezésből)
 - Az első két feltétel 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: $\pm 1, \pm 2, \pm 3, \pm 6$, 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 $(m, 0) = (0, m) = |m|$,
 $(m, mn) = (mn, m) = |m|$,

Közös osztók

Kitüntetett közös osztó

D Kitüntetett közös osztó

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 $c \leq d$ feltételt a $c \mid d$ feltételre cseréltük, vagyis csak az **oszthatóság fogalmát** használjuk, a számok **rendezését nem!**
- Mivel az oszthatóságon egy egységgel való szorzás nem változtat, **itt** 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: $\pm 1, \pm 2, \pm 3, \pm 6$. 6 az az egyetlen nemnegatív szám, mely e számok mindegyikével osztható, tehát 6 a kitüntetett közös osztó.

Közös osztók

Euklideszi algoritmus

T A kitüntetett közös osztó létezése

Bármely két egész számnak létezik kitüntetett közös osztója.

- B 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...

$$r_0 = r_1q_1 + r_2$$

$$r_n \mid r_0 = a$$

$$c \mid r_2 = r_0 - r_1q_1$$

$$r_1 = r_2q_2 + r_3$$

$$r_n \mid r_1 = b$$

$$c \mid r_3 = r_1 - r_2q_2$$

$$r_2 = r_3q_3 + r_4$$

$$r_n \mid r_2$$

$$c \mid r_4 = r_2 - r_3q_3$$

\vdots

$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$

$$r_n \mid r_{n-2}$$

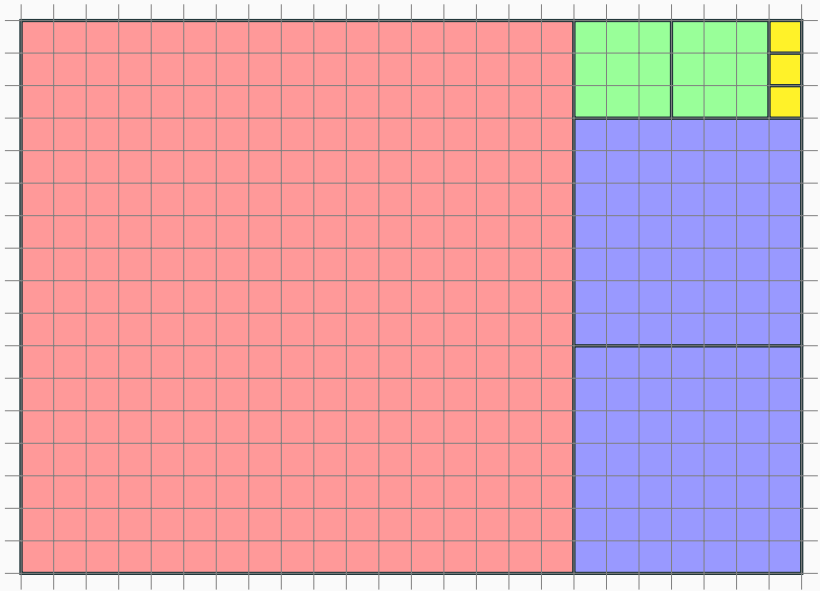
$$c \mid r_n = r_{n-2} - r_{n-1}q_{n-1}$$

$$r_{n-1} = r_nq_n$$

$$r_n \mid r_{n-1}$$

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

- 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 $D \leq d$, D definíciója miatt $d \leq D$, tehát $d = D$.
- A tételbeli algoritmust **euklideszi algoritmusnak** nevezzük. Leegyszerűsítve legyen $r_0 = a$, $r_1 = b$, ahol $a \geq b > 0$. Ismételten végezzük el az $r_k = r_{k+1}q_{k+1} + r_{k+2}$ maradékos osztásokat, ahol $0 \leq r_{k+2} < r_{k+1}$. Az algoritmus leáll, amint valamely maradék 0 nem lesz, azaz ha $r_{n+1} = 0$. Ekkor a kitüntetett közös osztó r_n .
- Az euklideszi algoritmus a legkisebb pozitív maradék helyett a legkisebb abszolút értékűvel is számolható: ekkor $|r_k|$ lesz szigorúan monoton csökkenő.



Lásd még a [Wikipédia Euklideszi algoritmus](#) szócikkét!

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

M $24 = 17 \cdot 1 + 7$ $288 = 204 \cdot 1 + 84$

$17 = 7 \cdot 2 + 3$ $204 = 84 \cdot 2 + 36$

$7 = 3 \cdot 2 + 1$ $84 = 36 \cdot 2 + 12$

$3 = 1 \cdot 3$ $36 = 12 \cdot 3$

Egyszerűen: $(24, 17) = (17, 7) = (7, 3) = (3, 1) = (1, 0) = 1$,

$(288, 204) = (204, 84) = (84, 36) = (36, 12) = (12, 0) = 12$.

P Számítsuk ki $(21, 13)$ értékét minimális absz. ért. maradékkal is!

M $(21, 13) = (13, 8) = (8, 5) = (5, 3) = (3, 2) = (2, 1) = (1, 0) = 1$

$(21, 13) = (13, 5) = (5, 2) = (2, 1) = (1, 0) = 1$.

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

B Az euklideszi algoritmus első egyenletéből r_2 , a következőből r_3, \dots , az utolsó előttiből r_n kifejezhető a és b lineáris kombinációjaként.

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:

$$(1) (24, 17) = 24m + 17n, \quad (2) (288, 204) = 288m + 204n.$$

$$M \quad 24 = 17 \cdot 1 + 7 \quad 7 = 24 - 17$$

$$17 = 7 \cdot 2 + 3 \quad 3 = 17 - 2 \cdot 7 = -2 \cdot 24 + 3 \cdot 17$$

$$7 = 3 \cdot 2 + 1 \quad 1 = 7 - 2 \cdot 3 = 5 \cdot 24 - 7 \cdot 17$$

$$3 = 1 \cdot 3$$

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

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

$$24 = 1 \cdot 24 + 0 \cdot 17$$

$$17 = 0 \cdot 24 + 1 \cdot 17$$

$$7 = 1 \cdot 24 - 1 \cdot 17$$

$$3 = -2 \cdot 24 + 3 \cdot 17$$

$$1 = 5 \cdot 24 - 7 \cdot 17$$

Táblázatban a hányadost is jelölve az első oszlopban:

	24	17		288	204		
	24	1	0	288	1	0	
1	17	0	1	1	204	0	1
2	7	1	-1	2	84	1	-1
2	3	-2	3	2	36	-2	3
3	1	5	-7	3	12	5	-7

Közös osztók

Lineáris diofantoszi egyenletek

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

- Lineáris diofantoszi egyenlet: $ax + by = c$, ($a, b, c \in \mathbb{Z}$)
- Pitagoraszi számhármások: $x^2 + y^2 = z^2$
- Nagy Fermat-tétel (Wiles, 1995): az $x^n + y^n = z^n$ egyenletnek nincs nemtriviális megoldása, 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: $x^2 + y^2 = n$ (van megoldása $\iff n$
prímtényezői közül a $4k - 1$ alakú prímelek páros kitevőn vannak)
- Pell-egyenlet: $x^2 - ny^2 = \pm 1$.

T Tétel

Legyen $d = (a, b)$, $a \neq 0$, $b \neq 0$. Az $ax + by = c$ lineáris diofantoszi egyenlet pontosan akkor oldható meg, ha $d \mid c$. Ekkor az összes megoldás fölírható $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$ alakban, ahol t tetszőleges egész.

B (\Rightarrow) Ha $ax_0 + by_0 = c$, 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 $atm + bnt = c$.

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:

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

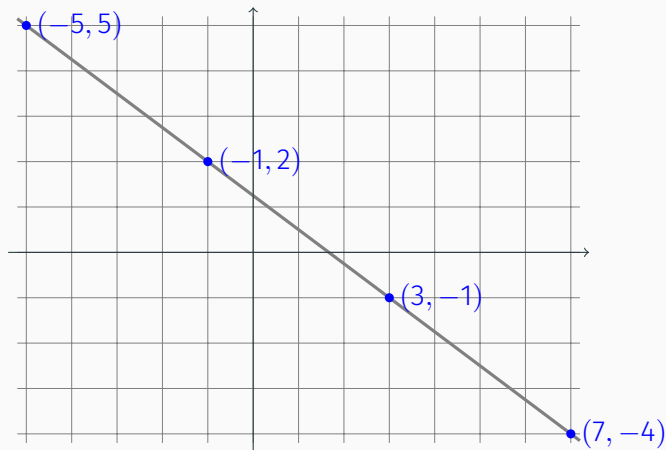
Mivel $(\frac{a}{d}, \frac{b}{d}) = 1$, ezért $\frac{a}{d} \mid (y_0 - y) \rightsquigarrow y = y_0 - \frac{a}{d}t \rightsquigarrow x = x_0 + \frac{b}{d}t$. 40

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 áruért. 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:

$$1 = (24, 17) = 5 \cdot 24 - 7 \cdot 17 \rightsquigarrow 5000 \cdot 24 - 7000 \cdot 17 = 1000.$$

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

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

A lehetséges (x, y) párok: $(36, 8), (19, 32), (2, 56)$.

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