Bevezetés az algebrába 1

Egész számok

Wettl Ferenc diái alapján

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 $a = bq$.

Nyilván: ± 1 és $\pm a$ osztója a-nak minden a-ra

D $b \mid a$ esetén b valódi osztója a-nak, ha $b \neq \pm a, \pm 1$.

Á (1) $a \mid 0 \ \forall a \in \mathbb{Z}$ (0-val is: $0 = 0 \cdot 0$).

(2) a 0 csak a 0-nak osztója,

(3) $a \mid b$, $b \neq 0 \Rightarrow |a| \leqslant |b|$,

Mj *Az oszthatóság hasonlóan definiálható pl. az egész vagy a valós együtthatós polinomok körében:* $x - 1 \mid x^3 - 1$, *mert* $x^3 - 1 = (x-1)(x^2 + x + 1)$.

F Hány osztója van a 15-nek $\mathbb{Z}$-ben?

D **Egység**

$u \in \mathbb{Z}$ egység, ha $u \mid a \quad \forall a \in \mathbb{Z}$.

K Á/(3)-ból következik, hogy $\mathbb{Z}$-ben csak ± 1 egység.

Mj Más fogalom az egységelem: $ua = au = a \ \forall a$ ($\mathbb{Z}$-ben az 1).

F1 A páros számok körében, $2\mathbb{Z}$-ben, mit jelent az oszthatóság? 2 osztója-e itt a 6-nak? Van-e egység? Minden számnak van-e osztója?

F2 Mik az egységek a valós együtthatós polinomok körében, $\mathbb{R}[x]$-ben?

F3 Hány olyan 400-nál kisebb pozitív egész szám van, amely nem osztható a 2, 3, 5 számok egyikével sem?

T **Az oszthatóság alaptulajdonságai**

$\forall a, b, c, m, n \in \mathbb{Z}$-re:

(1) $a \mid a$ (reflexív)

(2) $a \mid b$ és $b \mid c \Rightarrow a \mid c$ (tranzitív)

(3) $a \mid b$ és $a \mid c \Rightarrow a \mid mb + nc$

(4) $a \mid b$ és $m \mid n \Rightarrow am \mid bn$

Mj *$\mathbb{R}[x]$-ben is teljesülnek ezek, de $2\mathbb{Z}$-ben nem teljesül a reflexivitás.*

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

m Teljes indukció: $n = 0$ esetén $7 \mid 3 + 2^2$ ✓

$n \Rightarrow n+1$:

$3^{2n+3} + 2^{n+3} = 9 \cdot 3^{2n+1} + 2 \cdot 2^{n+2} = 2(3^{2n+1} + 2^{n+2}) + 7 \cdot 3^{2n+1}$

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. Hasonlóképpen a negatív egész kitevős hatványai is, mivel $1/(1+\sqrt{2}) = -1+\sqrt{2}$.

Itt nem mondhatunk olyat, hogy az osztó valamilyen értelemben kisebb annál, amit oszt: $|1+\sqrt{2}| > 1$.

Osztható ság

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

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

B Kell: $q \in \mathbb{Z}$: $0 \leq a - bq < |b|$, azaz $bq \leq a < bq + |b|$

$$\text{ha } b > 0\text{:} \quad bq \leqslant a < bq + b \quad \Leftrightarrow q \leqslant \tfrac{a}{b} < q + 1 \quad \Leftrightarrow \quad q = \left\lfloor \tfrac{a}{b} \right\rfloor$$

$$\text{ha } b < 0\text{:} \quad bq \leqslant a < bq - b \quad \Leftrightarrow q \geqslant \tfrac{a}{b} > q - 1 \quad \Leftrightarrow \quad q = \left\lceil \tfrac{a}{b} \right\rceil$$

q a fentiek alapján egyértelmű, ezért r is az.

Mj A tételbeli $0 \leqslant r < |b|$ feltétel kicserélhető erre: $-\frac{|b|}{2} < r \leqslant \frac{|b|}{2}$. Ekkor a nemnegatív maradék helyett a legkisebb abszolút értékű maradékot kapjuk.

F Hogyan állítjuk elő itt a q-t?

P Osszuk el maradékosan — nemnegatív, illetve legkisebb abszolút értékű maradékkal — a-t b-vel, ha $|a| = 20$ és $|b| = 7$.

m Nemnegatív maradékkal: $20 = 7 \cdot 2 + 6$, $-20 = 7 \cdot (-3) + 1$, $20 = (-7) \cdot (-2) + 6$, $-20 = (-7) \cdot 3 + 1$.

Legkisebb abszolút értékű maradékkal: $20 = 7 \cdot 3 - 1$, $-20 = 7 \cdot (-3) + 1$, $20 = (-7) \cdot (-3) - 1$, $-20 = (-7) \cdot 3 + 1$.

Osztathatóság

Számrendszerek

T **b-alapú számrendszer**

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

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

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 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.

P $26 = 26_{10} = 1A_{16} = 32_8 = 122_4 = 11010_2 = 101_5 = 10_{26}$.

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

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	2	
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	3
9216	0
3072	0
1024	0
341	1
113	2
37	2
12	1
4	0
1	1
0	1

$Z = 200002$

6252	5
1250	2
250	0
50	0
10	0
2	0
0	2

Mj A b-es és b^k-os számrendszer között egyszerű az áttérés: ha az $m = a_n b^n + a_{n-1} b^{n-1} + \ldots + a_1 b + a_0$ kifejezésben jobbról kezdve k-anként összevonjuk a tagokat, és kiemeljük belőlük a b^k megfelelő hatványát, akkor b^k-as számrendszerben való felírást kapunk, mert az összevont tagokból kapott együttható

$$\begin{aligned} 0 \leq & c_{k-1} b^{k-1} + c_{k-2} b^{k-2} + \ldots + c_1 b + c_0 \\ \leq & (b-1)(b^{k-1} + \ldots + b + 1) = b^k - 1 < b^k. \end{aligned}$$

F Írjuk át az 110111010010001_2 számot 8-as és 16-os, valamint az $AE1F_{16}$ számot 2-es számrendszerbe!

m $110|111|010|010|001 \rightsquigarrow 67221_8$

$110|1110|1001|0001 \rightsquigarrow 6E91_{16}$

$AE1F_{16} \rightsquigarrow 1010|1110|0001|1111 \rightsquigarrow 1010111000011111_2$

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

m A sima behelyettesítés kényelmetlenebb ($5^5 = 3125$). Horner-módszer:

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

Tehát $p(5) = 53$.

F 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

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 (ha van ilyen), azaz ha $c \mid a$ és $c \mid b$, akkor $c \leqslant d$,
3. az $a = b = 0$ esetben $d = 0$.

- Jelölések: $d = (a, b)$, $d = \mathrm{lnko}(a, b)$, $d = \gcd(a, b)$ (az angol 'greatest common divisor' kifejezésből)
- Az első két feltétel bármely két a, b egész szám legnagyobb közös osztóját egyértelműen definiálja, kivéve, ha $a = b = 0$, amikor nincs legnagyobb a közös osztók között.
  A legnagyobb közös osztó — az $a = 0,\ b = 0$ eset kivételével — pozitív, mert az 1 is közös osztó.

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

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

Á Könnyen látható:
Ha $m, n \in \mathbb{Z}$, akkor $(m, 0) = (0, m) = |m|$, $(m, mn) = (mn, m) = |m|$, továbbá $(m, n) = (n, m) = (-m, n)$, ...

Á Legyen $K(a, b)$ az a és b közös osztóinak halmaza. Ekkor minden $n \in \mathbb{Z}$-re $K(a, b) = K(a - nb, b)$, tehát $(a, b) = (a - nb,\ b)$.

B $c \mid a$ és $c \mid b \rightsquigarrow c \mid 1a + (-n)b$ és $c \mid b$.
$c \mid a - nb$, $c \mid b \rightsquigarrow c \mid 1(a - nb) + nb = a$ és $c \mid b$.

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 $c \leqslant d$ 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.
- Ez a definíció a $(0, 0) = 0$ értéket is természetes módon adja.

P 12 és 18 közös osztói: ± 1, ± 2, ± 3, ± 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...

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & K(r_0, r_1) &= K(r_0 - r_1 q, r_1) = K(r_2, r_1) = K(r_1, r_2) \\
r_1 &= r_2 q_2 + r_3 & K(r_1, r_2) &= K(r_2, r_3) \\
r_2 &= r_3 q_3 + r_4 & K(r_2, r_3) &= K(r_3, r_4) \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & K(r_{n-2}, r_{n-1}) &= K(r_{n-1}, r_n) \\
r_{n-1} &= r_n q_n + 0 & K(r_{n-1}, r_n) &= K(r_n, 0)
\end{aligned}
$$

$$K(a, b) =$$

Mivel $K(r_n, 0)$-nak r_n a kitüntetett eleme, azaz, az a nemegatív szám, amelyet az összes többi oszt, $d = r_n$ kitüntetett közös osztója a-nak és b-nek. Az algoritmus véges sok 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 d kitüntetett és a D legnagyobb közös osztó megegyezik: 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, ha valamely $r_{n+1} = 0$. 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, és az algoritmus $\leqslant \log_2 |b|$ lépésben véget ér (a maradék felső becslése feleződik).

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

m

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

Egyszerűen: $(24, 17) = (7, 17) = (7, 3) = (1, 3) = (1, 0) = 1$,
$(288, 204) = (84, 204) = (84, 36) = (12, 36) = (12, 0) = 12$.

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

m $(21, 13) = (8, 13) = (8, 5) = (3, 5) = (3, 2) = (1, 2) = (1, 0) = 1$
$(21, 13) = (-5, 13) = (-5, -2) = (1, -2) = (1, 0) = 1$.

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

Összefoglaljuk a legnagyobb közös osztó legalapvetőbb tulajdonságait:

Á

A lnko elemi tulajdonságai

(1) $(a, b) = (b, a)$ (2) $(a, b) = (-a, b) = (a, -b) = (-a, -b)$ (3) $(a, 0) = |a|$ (4) $(a, b) = (a - mb,\ b)$ (5) $a \mid c$ és $b \mid d \Rightarrow (a, b) \mid (c, d)$

B (1)–(4)-et láttuk korábban.

Az (5)-höz használjuk a kitüntetett közös osztó definiáló tulajdonságát:

$(a, b) \mid a \mid c$ és $(a, b) \mid b \mid d \Rightarrow (a, b) \mid (c, d)$.

Kibővített euklideszi algoritmus

T **Kibővített euklideszi algoritmus**

(a, b) kifejezhető a és b alkalmas $x, y \in \mathbb{Z}$ egészekkel vett lineáris kombinációjaként, azaz felírható $(a, b) = ax + by$ alakban.

B Végezzük el a, b-re az euklideszi algoritmust. Teljes indukcióval bizonyítható, hogy minden r_i felírható $ax + by$ alakban: $r_0 = a = a \cdot 1 + b \cdot 0$ és $r_1 = b = a \cdot 0 + b \cdot 1$ felírható, és ha $j \leq i$-re $r_j = ax_j + by_j$, akkor

$$\begin{aligned} r_{i+1} =& r_{i-1} - r_i q_i = (ax_{i-1} + by_{i-1}) - (ax_i + by_i)q_i = \\ =& a(x_{i-1} - x_i q_i) + b(y_{i-1} - y_i q_i), \end{aligned}$$

tehát $(a, b) = r_n$ is felírható.

K Bármely a, b egészre $\{ax + by \mid x, y \in \mathbb{Z}\} = \{(a, b)c \mid c \in \mathbb{Z}\}$.

B $\subseteq$ ✓, $\supseteq$ ✓

P Kibővített euklideszi algoritmussal határozzuk meg a következő lineáris kombinációk együtthatóit:

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

m

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

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

Mj Mechanikussá tehető az előző számítás, ha egyenlőségek lineáris kombinációit számoljuk:

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

Táblázatosan, az első oszlop előtt kiírva, hogy az adott sor hányszorosát adjuk az előző sorhoz:

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

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

A lnko további tulajdonságai

T **A lnko további tulajdonságai**

(1) $(ac, bc) = c(a, b)$, ha $c > 0$

(2) $(a, b) = d \neq 0 \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$, azaz $\frac{a}{d}$ és $\frac{b}{d}$ relatív prímek.

(3) $c \mid ab$ és $(c, a) = 1 \Rightarrow c \mid b$.

(4) $(a, c) = 1 \Rightarrow (a, bc) = (a, b)$.

B (1) $\left.\begin{array}{l} (a,b) \mid a \rightsquigarrow (a,b)c \mid ac \\ (a,b) \mid b \rightsquigarrow (a,b)c \mid bc \end{array}\right\} \rightsquigarrow \quad (a,b)c \mid (ac, bc)$ másrészt

$(a, b) = ax + by \rightsquigarrow c(a, b) = (ac)x + (bc)y \rightsquigarrow (ac, bc) \mid c(a, b)$

(2) az előzőből ✓

(3) (első biz.) $c \mid ab$, $c \mid cb \rightsquigarrow c \mid (ab, cb) \overset{(1)}{=} (a, c)|b| = |b| \mid b$.

(második) $(c, a) = 1 \rightsquigarrow 1 = cx + ay \rightsquigarrow b = bcx + aby \rightsquigarrow c \mid b$.

(4) $(a, b) \mid (a, bc)$ ✓

$(a, bc) \mid (ab, bc) = |b|(a, c) \mid b$, $(a, bc) \mid a \rightsquigarrow (a, bc) \mid (a, b)$

P Az előző tételt használva számítsuk ki $(12321, 4218)$ értékét!

m $(12321, 4218) \overset{(1)}{=} 3(4107, 1406) \overset{(4)}{=} 3(4107, 703) = 3(-111, 703) = 3(111, 37) = 3(0, 37) = 3 \cdot 37 = 111$

P Egy processzor gyorsan von ki két számot egymásból és oszt páros számot 2-hatvánnyal (a bináris alakjának végén lévő k darab 0-t törölve k hellyel jobbra tolja: ez a 2^k-val való osztásnak felel meg; pl. $11010000_2 = 208$ osztható 2^4-nel, a hányados $1101_2 = 13$). E két művelettel hogy számolható a lnko? Számoljuk ki $(48, 34)$ értékét!

m A következő lépésekkel folyamatosan csökkentjük a számokat:

0. ha induláskor mindkét szám páros: $(2^k a, 2^k b) = 2^k(a, b)$
1. ha csak az egyik szám páros: $(2^k a, b) = (a, b)$ vagy $(a, 2^k b) = (a, b)$
2. ha mindkettő páratlan: $(a, b) = (a - b, b) = (a, b - a)$

$(48, 30) \overset{0.}{=} 2(24, 15) \overset{1.}{=} 2(3, 15) \overset{2.}{=} 2(3, 12) \overset{1.}{=} 2(3, 3) \overset{2.}{=} 2(3, 0) = 2 \cdot 3 = 6$

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 számhármasok: $x^2 + y^2 = z^2$
- 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: $95800^4 + 217519^4 + 414560^4 = 422481^4$)
- Két négyzetszám összege: $x^2 + y^2 = n$ (van megoldása $\iff$ n prímtényezői közül a $4k - 1$ alakú prímek páros kitevőn vannak)
- Pell-egyenlet: $x^2 - ny^2 = \pm 1$.

T **Lineáris diofantoszi egyenlet megoldhatósága és megoldása**

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 $atm + btn = c$.
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:

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

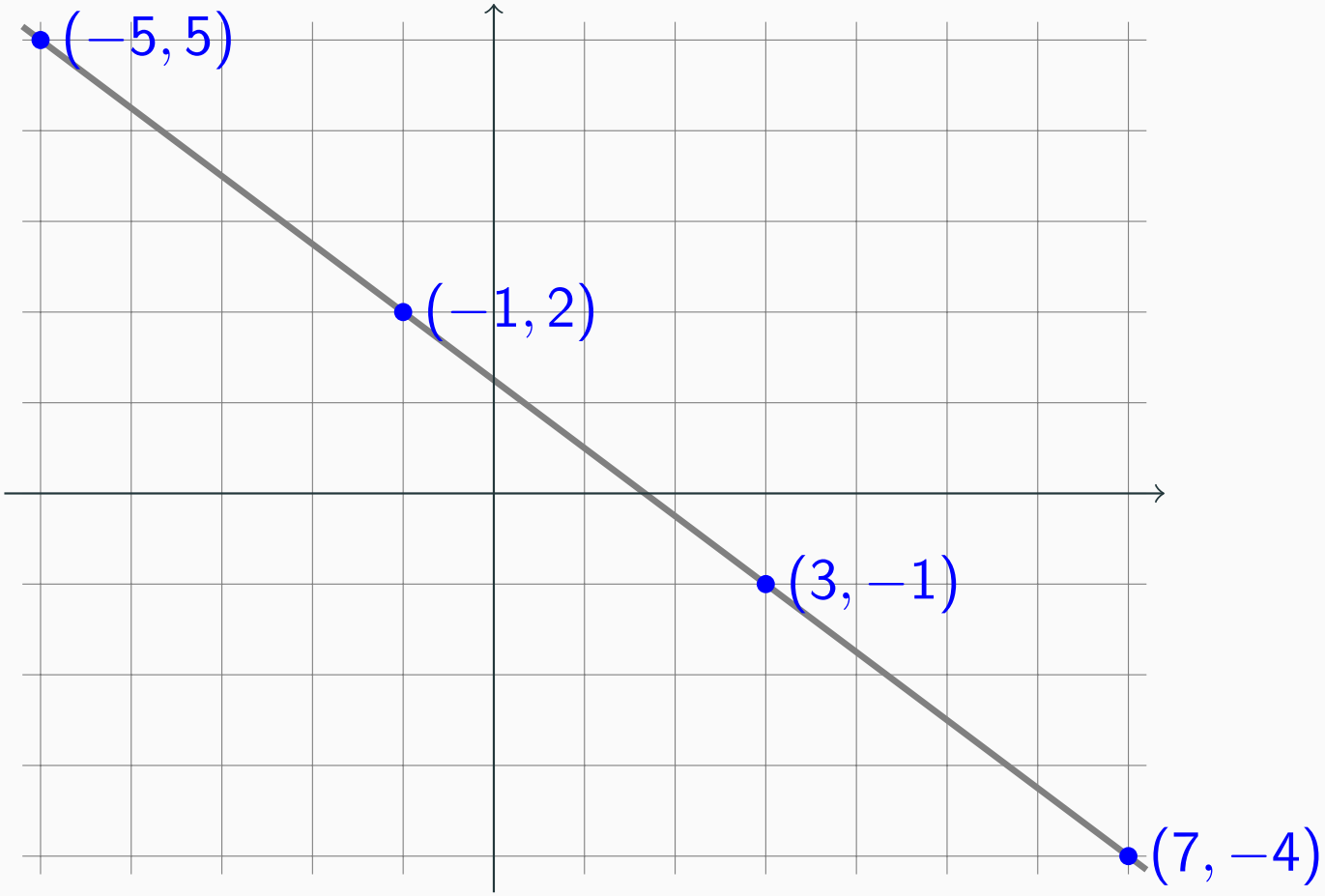
Mivel $(\frac{a}{d}, \frac{b}{d}) = 1$, ezért $\frac{b}{d} \mid (x - x_0) \rightsquigarrow x = x_0 + \frac{b}{d}t \rightsquigarrow y = y_0 - \frac{a}{d}t$.

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 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 $(288, 204) = 12 \mid 12000$.

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

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

A feltételek: $5000 + 17t > -7000 - 24t \geq 0$, azaz
$-\frac{12000}{41} < t \leq -\frac{7000}{24}$, amelynek egész megoldása csak $t = -292$.

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