KÉTISMERETLENES LINEÁRIS DIOFANTOSZI EGYENLETEK

Waldhauser Tamás

SZTE Bolyai Intézet

alexandriai Diophantos

200(?) – 284(?)

Pierre de Fermat

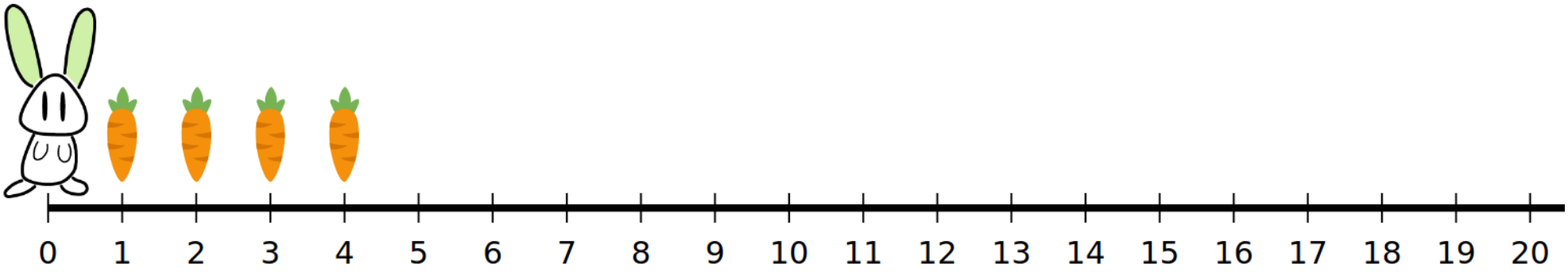
1607(?) – 1665

Sejtés (Fermat, 1637) $\rightarrow$ Tétel (Wiles és Taylor, 1993–1995)

Ha $n \geq 3$, akkor az $x^n + y^n = z^n$ egyenletnek nincs megoldása a pozitív egészek körében.

Bemelegítő feladat

Egy nyúl ugrál a számegyenesen, a nullából indulva. Csak kétféle ugrásra képes: a nagyobb ugrás mérete 36 egység, a kisebb ugrásé 28 egység. Az 1,2,3,4 számoknál lévő répák közül hányat tud megenni?



$36x+28y=1,3$

páros

$36x+28y=2$

4-gyel osztható

$36x+28y=4$

$x=-3, y=4$

$\text{Lnko}(36,28)=4$

Tartalom

Oszthatóság, prímszámok

Legnagyobb közös osztó

Diofantoszi egyenlet

Definíció

Tetszőleges a, b egész számok esetén azt mondjuk, hogy a **osztója** b-nek (b **többszöröse** a-nak), ha van olyan c egész szám, amelyre $b = ac$.
Jelölés: $a \mid b$. Formálisan:

$$a \mid b \iff \exists c \in \mathbb{Z}\colon b = ac.$$

$\Leftrightarrow \frac{b}{a} \in \mathbb{Z}$ Ha $a \neq 0$!

Példák

- $2 \mid 26$, $-2 \mid 26$, $2 \mid -26$, $-2 \mid -26$

$26 = 2 \cdot 13 = (-2) \cdot (-13)$

- $12 \mid -12$, $-12 \mid 12$

$12 = (-12) \cdot (-1)$

- $3 \nmid 1975$, $2021 \nmid 2020$, $2020 \nmid 2021$

- $1 \mid 23$, $-1 \mid 23$

$23 = 23 \cdot 1 = (-23) \cdot (-1)$

- $239 \mid 0$, $0 \mid 0$

$0 = 239 \cdot 0 = 0 \cdot 0$

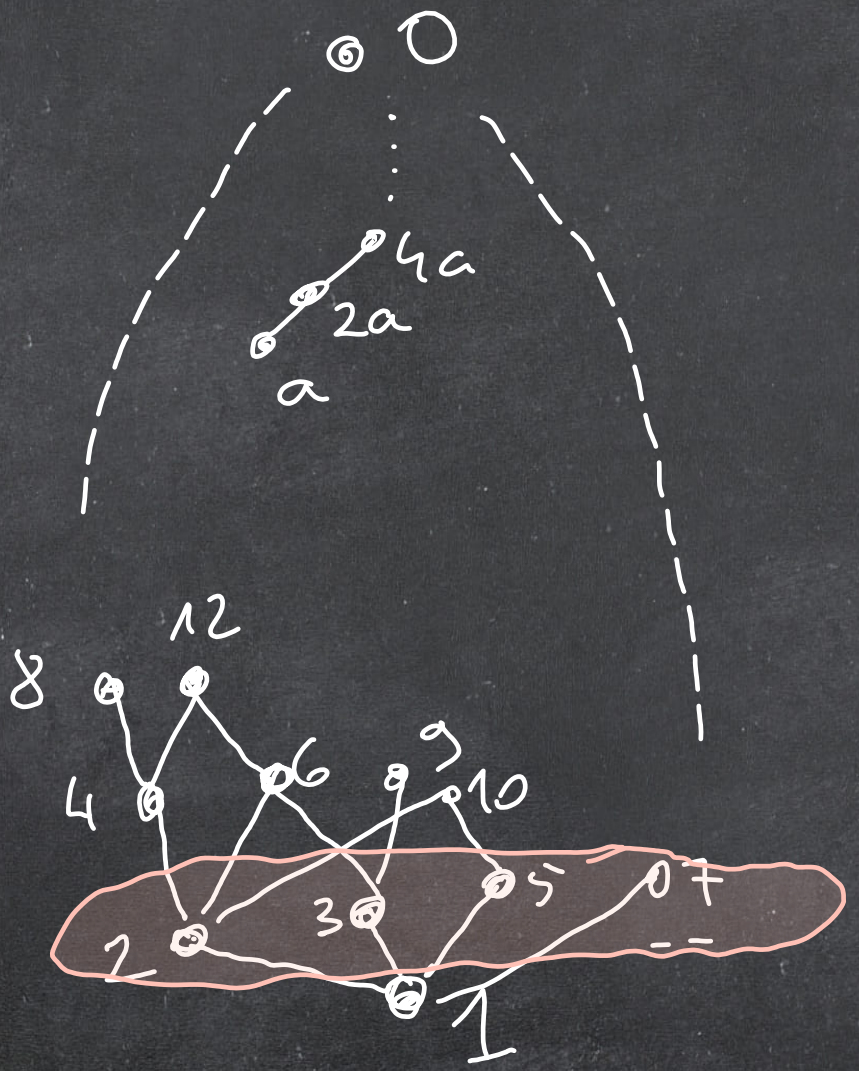
Tétel

Tetszőleges a, b, c egész számok esetén teljesülnek az alábbiak:

1. $a \mid a$; $a = a \cdot 1$
2. $(a \mid b$ és $b \mid c) \implies a \mid c$; $c = b \cdot v = (au) \cdot v = a(uv)$
3. $(a \mid b$ és $b \mid a) \iff b = \pm a$; $a = b \cdot v = (au) \cdot v = a(uv)$ $\Rightarrow 1 = uv$, ha $a \neq 0$
4. $(a \mid b$ és $a \mid c) \implies a \mid b \pm c$; $b \pm c = au \pm av = a(u \pm v)$
5. $a \mid b \iff ac \mid bc$, feltéve, hogy $c \neq 0$; $\exists u: b = au \Leftrightarrow \exists u: bc = acu$
6. $1 \mid a$ és $a \mid 0$. $a = 1 \cdot a$ $0 = a \cdot 0$

Következmény

Az oszthatóság részbenrendezési reláció a nemnegatív egész számok halmazán, vagyis $(\mathbb{N}_0, |)$ részbenrendezett halmaz, amelynek legkisebb eleme 1, legnagyobb eleme 0.



Definíció

A p természetes szám felbonthatatlan (irreducibilis), ha $p > 1$ és csak úgy bontható két természetes szám szorzatára, hogy az egyik tényező 1:

$$\forall a, b \in \mathbb{N}\colon\ p = ab \implies a = 1 \text{ vagy } b = 1.$$

Definíció

A p természetes szám prím(tulajdonságú), ha $p > 1$ és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat valamelyik tényezőjének:

$$\forall a, b \in \mathbb{N}\colon\ p \mid ab \implies p \mid a \text{ vagy } p \mid b.$$

Tétel

A természetes számok körében a felbonthatatlanság és a prímtulajdonság egymással ekvivalens.

Tétel (a számelmélet alaptétele)

Minden (1-nél nagyobb) természetes szám felbontható prímszámok szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.

Tétel (Euklidész)

Végtelen sok prímszám van.

Biz. Tfh. $p_1, \dots, p_n$ az összes prím.

$N = p_1 \cdot \dots \cdot p_n + 1 > 1 \Rightarrow$ van q prímosztója

$\forall i : p_i \nmid N \Rightarrow q \notin \{p_1, \dots, p_n\}$ ↯ ∎

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots$

1 2 2 2 2

Prímszámtétel (Hadamard és de la Vallée Poussin, 1896)

Az n-edik prímszám nagyságrendileg $n \cdot \log n$.

Ikerprímsejtés

Végtelen sokszor előfordul, hogy két szomszédos prím távolsága 2.

Tétel (Zhang, 2013)

Végtelen sokszor előfordul, hogy két szomszédos prím távolsága legfeljebb 70 000 000.

Tétel (Polymath8, 2014)

Végtelen sokszor előfordul, hogy két szomszédos prím távolsága legfeljebb 246.

Tartalom

Oszthatóság, prímszámok

Legnagyobb közös osztó

Diofantoszi egyenlet

Definíció (lnko – első nekifutás)

Azt mondjuk, hogy a d nemnegatív egész szám legnagyobb közös osztója az a és b nemnegatív egész számoknak (jelölés: $d = \text{lnko}(a, b)$), ha

(KO) $d \mid a, b$, és

(LN) $\forall k \in \mathbb{N}_0$ esetén $k \mid a, b \implies k \leq d$.

Példák

- $\text{lnko}(24, 42) = 6$
- $\text{lnko}(24, 0) = 24$
- $\text{lnko}(0, 0) =$ ~~0~~

24 osztói: 1, 2, 3, 4, 6, 8, 12, 24

42 osztói: 1, 2, 3, 6, 7, 14, 21, 42

24 osztói: 1, 2, 3, 4, 6, 8, 12, 24

0 osztói: 0, 1, 2, 3, 4, ...

0 osztói: 0, 1, 2, 3, 4, ...

0 osztói: 0, 1, 2, 3, 4, ...

Definíció (lnko – második nekifutás)

Azt mondjuk, hogy a d nemnegatív egész szám legnagyobb közös osztója az a és b nemnegatív egész számoknak (jelölés: $d = \mathrm{lnko}(a, b)$), ha

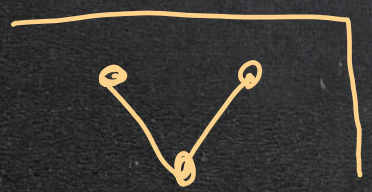
(KO) $d \mid a, b$, és

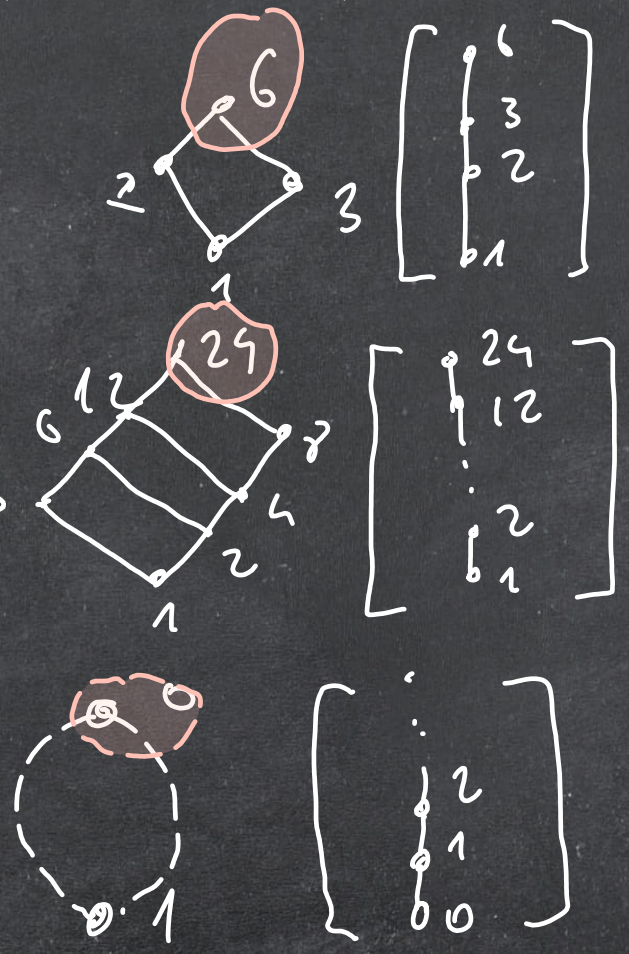
(LN) $\forall k \in \mathbb{N}_0$ esetén $k \mid a, b \implies k \mid d$.

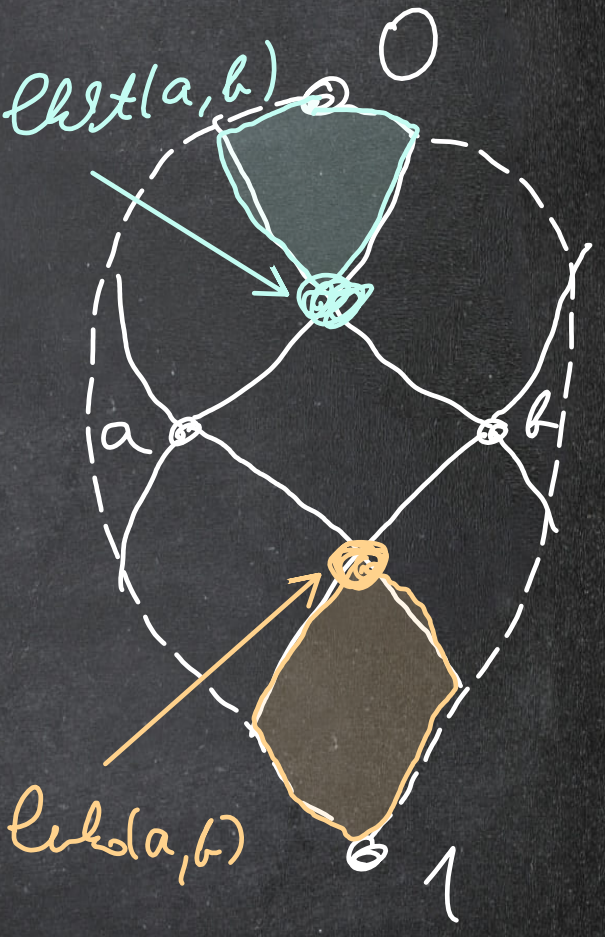
(Nagy!)

Példák

- $\mathrm{lnko}(24, 42) = 6$
- $\mathrm{lnko}(24, 0) = 24$
- $\mathrm{lnko}(0, 0) = 0$







Definíció (lnko – végső változat)

Azt mondjuk, hogy a d egész szám legnagyobb közös osztója az a és b egész számoknak (jelölés: $d = \text{lnko}(a, b)$), ha

(KO) $d \mid a, b$, és

(LN) $\forall k \in \mathbb{Z}$ esetén $k \mid a, b \implies k \mid d$.

Példák

- $\text{lnko}(24, 42) = \pm 6$

$\text{lnko}(24,42)=6$
$\text{lnko}(24,42)=-6$
$\neq) \; 6 = -6$

- $\text{lnko}(24, 0) = \pm 24$

- $\text{lnko}(0, 0) = 0$

Tétel

Bármely két egész számnak létezik legnagyobb közös osztója és legkisebb közös többszöröse; ezek előjeltől eltekintve egyértelműen meghatározottak, és teljesül a következő összefüggés

$$\mathrm{lnko}(a, b) \cdot \mathrm{lkkt}(a, b) = ab.$$

Tétel

Legyen az a és b természetes számok prímhatványtényezős felbontása

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \quad \text{és} \quad b = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}.$$

(Azokat a prímeket, amelyek csak egyik szám felbontásában szerepelnek, a másik számban nulla kitevővel tüntetjük fel.) Ekkor

1. $a \mid b \iff \alpha_i \leq \beta_i$ (minden i-re);
2. $\mathrm{lnko}(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_k^{\min(\alpha_k, \beta_k)}$;
3. $\mathrm{lkkt}(a, b) = p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_k^{\max(\alpha_k, \beta_k)}$.

Egyszerű De Nagyon Fontos Megfigyelés

Teszőleges $a, b \in \mathbb{Z}$ esetén a és b közös osztói ugyanazok, mint $a - b$ és b közös osztói. Következésképp

$$\mathrm{lnko}(a, b) = \mathrm{lnko}(a - b, b).$$

Biz.

$\forall k \in \mathbb{Z}: k \mid a, b \Rightarrow k \mid a-b, b$

$\forall k \in \mathbb{Z}: k \mid a-b, b \Rightarrow k \mid \underbrace{a-b+b}_{a}, b$ ∎

Példa

$\mathrm{lnko}(36, 28) = \mathrm{lnko}(0, 4) = 4$

(EDNF!)

$(36,28) \to (8,28) \to (8,20) \to (8,12) \to (8,4) \to (4,4) \to (0,4)$

$(36,28) \to (8,28) \to (8,4) \to (0,4)$

$-3.$ $-2.$

Euklideszi algoritmus

```
1: function lnko(a, b)
2:     while b ≠ 0 do
3:         (a, b) ← (b, a mod b)
4:     end while
5:     return a
6: end function
```

$(36, 28)$

$(28, 8)$

$(8, 4)$

$(4, 0)$

$36 = 1 \cdot 28 + 8 \Rightarrow 8 = 36 - 28$

$28 = 3 \cdot 8 + 4 \Rightarrow 4 = 28 - 3 \cdot (\underbrace{36 - 28}_{8}) =$

$8 = 2 \cdot 4 + 0$

$= -3 \cdot 36 + 4 \cdot 28 = 4$

$= -3 \cdot a + 4 \cdot b = lkk(a, b)$

Tétel (a maradékos osztás tétele)

Tetszőleges $a, b \in \mathbb{Z}\,(b \neq 0)$ esetén léteznek olyan q és r egész számok, amelyekre $a = q \cdot b + r$ és $0 \leq r < |b|$.

Tétel

Bármely két egész számnak létezik legnagyobb közös osztója, és az előáll a két szám „lineáris kombinációjaként”:

$$\forall a, b \in \mathbb{Z}\ \ \exists u, v \in \mathbb{Z}\colon\ \ au + bv = \mathrm{lnko}(a, b).$$

Bizonyítás (vázlat).

- Az euklideszi algoritmus véges számú lépésben véget ér, mert a maradékok folyamatosan csökkennek.
- Az utolsó nemnulla maradék lesz a legnagyobb közös osztó (EDNFM-nek köszönhetően).
- Sorra minden maradékot fel tudunk írni $a \cdot \_ + b \cdot \_$ alakban.

Következmény

Ha $\text{lnko}(a, b) \neq 0$, akkor $\dfrac{a}{\text{lnko}(a,b)}$ és $\dfrac{b}{\text{lnko}(a,b)}$ relatív prímek.

Biz. $d := \text{lnko}(a,b) \neq 0$

EALG: $au + bv = d \quad /:d$

$$\underbrace{\frac{a}{d}}_{\in\mathbb{Z}} \cdot u + \underbrace{\frac{b}{d}}_{\in\mathbb{Z}} \cdot v = 1$$

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

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

$\in\mathbb{Z}$

$\Rightarrow z \mid 1 \Rightarrow z = \pm 1$ ▨

$$\frac{36}{28} = \frac{36/4}{28/4} = \frac{9}{7} \qquad \frac{a}{b} = \frac{a/\text{lnko}(a,b)}{b/\text{lnko}(a,b)}$$

Következmény (Euklidész lemmája)

Ha $\text{lnko}(a, b) \neq 0$, akkor

$$a \mid bc \implies \frac{a}{\text{lnko}(a, b)} \mid c.$$

Speciálisan, ha a és b relatív prímek, akkor

$$a \mid bc \implies a \mid c.$$

Biz $d := \text{lnko}(a,b) \neq 0$, tfh. $a \mid bc$.

EALG: $au + bv = d \quad / \cdot c$

$acu + bcv = cd \implies a \mid cd \implies \frac{a}{d} \cdot d \mid c \cdot d \overset{d \neq 0}{\implies} \frac{a}{d} \mid c$

(acu: $a \mid$, bcv: $a \mid$)

Példa

Oldjuk meg a $28 \mid 36x$ „egyenletet”.

$28 \mid 36x \iff \frac{28}{\text{lnko}(28,36)} \mid x \iff 7 \mid x \quad x = \ldots, -7, 0, 7, 14, 21, \ldots$

Tartalom

Oszthatóság, prímszámok

Legnagyobb közös osztó

Diofantoszi egyenlet

Definíció

Kétismeretlenes lineáris diofantoszi egyenleten $ax + by = c$ alakú egyenletet értünk, ahol a, b, c adott egész számok ($a, b \neq 0$), és az x, y ismeretleneket is az egész számok körében keressük.

$d := \text{lnko}(a,b) \neq 0$

Célok

1. Döntsük el, hogy van-e megoldás.

   Ha $d \nmid c$, akkor nincs.

   $\underbrace{\underbrace{ax}_{d\mid} + \underbrace{by}_{d\mid}}_{d\mid} = \underbrace{c}_{d\nmid}$.

   Ha $d \mid c$, akkor ... ↘

2. Ha van, akkor találjunk először egy megoldást,

   EALG: $au + bv = d \quad / \cdot \frac{c}{d}$

   $a \cdot u\frac{c}{d} + b \cdot v\frac{c}{d} = c$

   $u\frac{c}{d} = x_0 \qquad v\frac{c}{d} = y_0$

3. majd határozzuk meg az összes megoldást.

Példa

$36x+28y=12$

$$y = \frac{12-36x}{28} = \frac{12}{28} - \frac{36}{28}x = \frac{3}{7} - \frac{9}{7}x$$

EALG: $36\cdot(-3)+28\cdot(4)=4=\mathrm{lnko}(36,28) \mid \cdot 3$

$$36\cdot\underbrace{(-9)}_{x_0}+28\cdot\underbrace{(12)}_{y_0}=12$$

$\vdots$

$(-16,21)=(x_{-1},y_{-1})$

$(-9,12)=(x_0,y_0)$

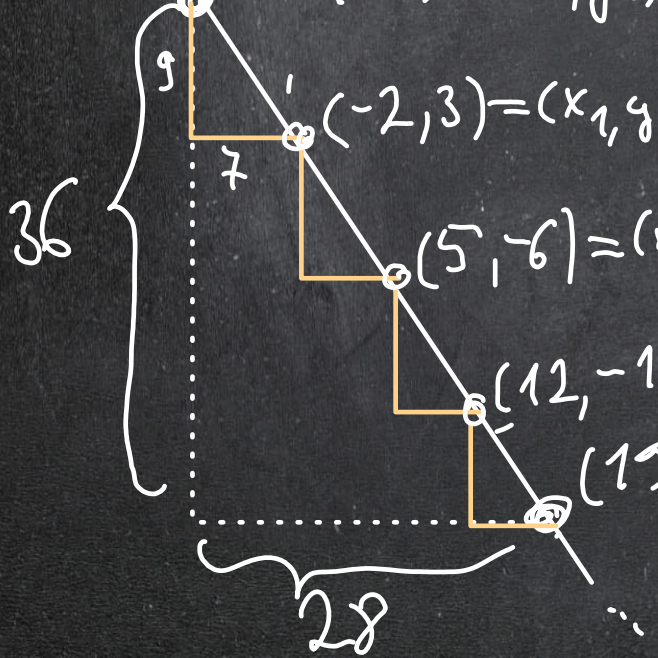
$(-2,3)=(x_1,y_1)$

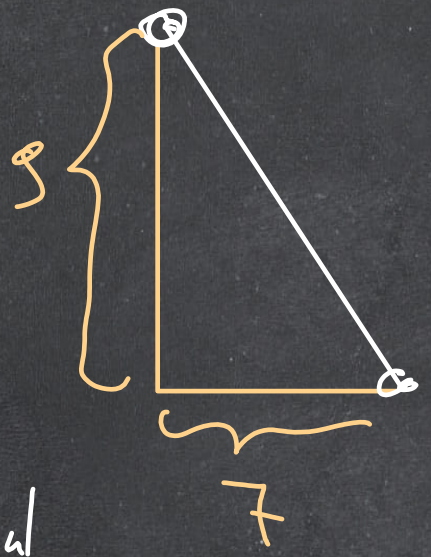
$(5,-6)=(x_2,y_2)$

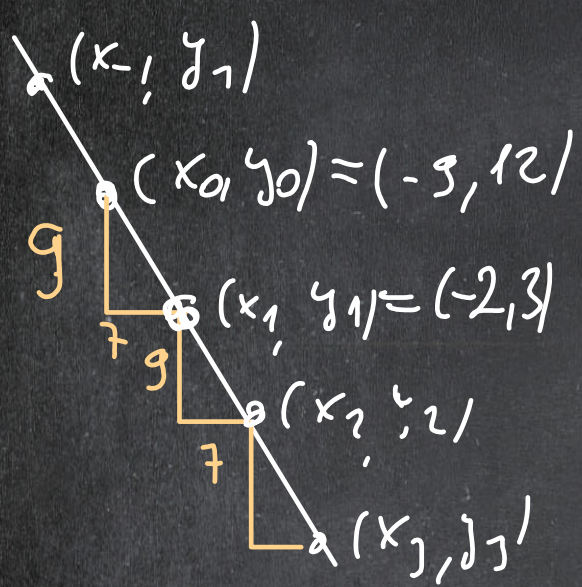
$(12,-15)=(x_3,y_3)$

$(19,-24)=(x_4,y_4)$

$\vdots$







t	...	-1	0	1	2	...
x_t	...	-16	-9	-2	5	...
y_t	...	21	12	3	-6	...

$3(x+2)8y = 12$

a b

Algemeen:

$$x_t = -9 + 7t = x_0 + \frac{b}{\text{ggd}(a,b)} \cdot t$$

$$y_t = 12 - 9t = y_0 - \frac{a}{\text{ggd}(a,b)} \cdot t$$

$$x_t = -2 + 7t$$

$$y_t = 3 - 9t$$

$t \in \mathbb{Z}$

$M = \{ \ldots, (-16, 21), (-9, 12), (-2, 3), (5, -6), \ldots \}$

Tétel

Tekintsük az $ax + by = c$ diofantoszi egyenletet, ahol a, b, c egész számok és $a, b \neq 0$.

- Az egyenletnek akkor és csak akkor van megoldása, ha $\text{lnko}(a, b) \mid c$.
- Ha (x_0, y_0) egy partikuláris megoldás, akkor az általános megoldás:

$$x_t = x_0 + \frac{b}{\text{lnko}(a, b)} t, \quad y_t = y_0 - \frac{a}{\text{lnko}(a, b)} t \quad (t \in \mathbb{Z}).$$

Bizonyítás helyett a megoldás lépései

1. $\text{lnko}(a, b)$ kiszámítása
2. ha $\text{lnko}(a, b) \nmid c$, akkor nincs megoldás; különben gyerünk tovább
3. euklideszi algoritmusból: $au + bv = \text{lnko}(a, b)$
4. beszorzunk azzal, amivel kell: $ax_0 + by_0 = c$
5. felírjuk az általános megoldás képletét
6. kiválogatjuk a feladat szövegének megfelelő megoldásokat