

DISZKRÉT MATEMATIKA II ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2026. február 19.

Tartalom

Bemelegítés

Diofantoszi egyenletek

A kongruencia fogalma

A kongruenciareláció tulajdonságai

Lineáris kongruencia

Lépj be!

- wifi hálózat (SSID): Kiss Arpad terem GUEST
- jelszó: 12345678
- coospace: Diszkrét matematika 2. ea. színtér



Ki van a képen?



(A)



(B)



(C)

CS teszt: 1. előadás - képek



Ki van a képen?



alexandriai Diophantos
200(?) – 284(?)



Gyula
2018 – ???



Pierre de Fermat
1607(?) – 1665

Tartalom

Bemelegítés

Diofantoszi egyenletek

A kongruencia fogalma

A kongruenciareláció tulajdonságai

Lineáris kongruencia

Kétismeretlenes lineáris diofantoszi egyenlet

$$ax + by = c$$

- a, b, c adott egész számok, $a, b \neq 0$
- x, y ismeretlen egész számok

Tudnunk kell:

- Van-e megoldás?
- Hogyan találunk meg egy megoldást?
- Hogyan találjuk meg az összes megoldást?

Mely répákat tudja megenni Gyula?

$$a = 44$$

$$b = 32$$



CS teszt: 1. előadás - répák



Euklideszi algoritmus

```
def lnko(a,b):  
    while b != 0:  
        a,b = b,a%b  
    return a
```

Példa

Futtassuk le az euklideszi algoritmust az $a = 44$, $b = 32$ számokra.

$$\begin{aligned}44 &= 1 \cdot 32 + 12 &\implies 12 &= a - b \\32 &= 2 \cdot 12 + 8 &\implies 8 &= b - 2(a - b) = -2a + 3b \\12 &= 1 \cdot 8 + 4 &\implies 4 &= (a - b) - (-2a + 3b) = 3a - 4b \\8 &= 2 \cdot 4 + 0\end{aligned}$$

Tétel

Két egész szám lnko-ja mindig előáll a két szám „lineáris kombinációjaként”:

$$\forall a, b \in \mathbb{Z} \quad \exists x, y \in \mathbb{Z}: \quad ax + by = \text{lnko}(a, b).$$

Hova juthat el Gyula?

- Azt már tudjuk, hogy a 4-esnél lévő répát el tudja érni: $4 = 3a - 4b$.
- Ha már a 4-esnél van, ugyanezzel a trükkel eljut 8-ba is:
 $8 = 2 \cdot (3a - 4b) = 6a - 8b$.
- Ha már a 8-asnál van, ugyanezzel a trükkel eljut 12-be is:
 $12 = 3 \cdot (3a - 4b) = 9a - 12b$.
- ...

Tehát az összes 4-gyel osztható számhoz el tud jutni Gyula.

Más számhoz pedig nem juthat el, mert

$$4 \mid 44, 32 \implies 4 \mid 44x + 32y.$$

Konklúzió: A Gyula által elérhető számok halmaza:

$$\{44x + 32y : x, y \in \mathbb{Z}\} = \{c \in \mathbb{Z} : 4 \mid c\}.$$

Hogyan jut el Gyula a 20-as répához?

Az euklideszi algoritmusból megkaptuk, hogy

$$44 \cdot 3 + 32 \cdot (-4) = 4.$$

Szorozzunk be 5-tel, hogy 20 legyen a jobboldalom:

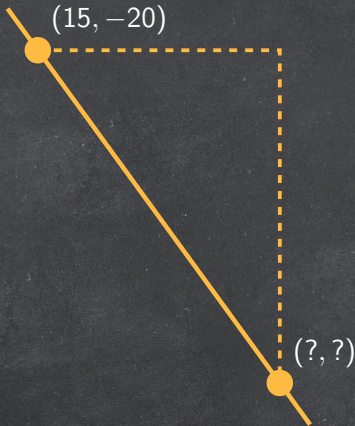
$$44 \cdot 15 + 32 \cdot (-20) = 20.$$

Tehát $x_0 = 15$, $y_0 = -20$ egy megoldása az egyenletnek.

Ez 35 ugrást jelent. Elég fárasztó lesz...

Ábrázoljuk: $44x + 32y = 20$

Mi a $(15, -20)$ ponttól jobbra lévő első rácspont az egyenesen?



CS teszt: 1. előadás - rácspon



$$\text{Ábrázoljuk: } 44x + 32y = 20$$

A $44x + 32y = 20$ egyenletű egyenesen a $(15, -20)$ ponttól jobbra lévő t -edik rácspont:

$$(15 + t \cdot 8, -20 - t \cdot 11).$$

A $44x + 32y = 20$ diofantoszi egyenlet **általános megoldása**:

$$x_t = 15 + 8t, \quad y_t = -20 - 11t, \quad \text{ahol } t = \dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

Foglaljuk táblázatba a megoldásokat.

t	$\dots$	-4	-3	-2	-1	0	1	2	$\dots$
x_t	$\dots$	-16	-9	-1	7	15	23	31	$\dots$
y_t	$\dots$	24	13	2	-9	-20	-31	-42	$\dots$

A „legjobb” megoldást $t = -2$ esetén kapjuk: $x = -1, y = 2$.

Kétismeretlenes lineáris diofantoszi egyenlet

$$ax + by = c$$

- a, b, c adott egész számok, $a, b \neq 0$
- x, y ismeretlen egész számok

Tudnunk kell:

- Akkor és csak akkor van megoldás, ha $\text{Inko}(a, b) \mid c$.
- Euklideszi alg. $\rightsquigarrow a \cdot _ + b \cdot _ = \text{Inko}(a, b) \rightsquigarrow ax + by = c$
- Ha (x_0, y_0) egy partikuláris megoldás, akkor az általános megoldás:

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

Tartalom

Bemelegítés

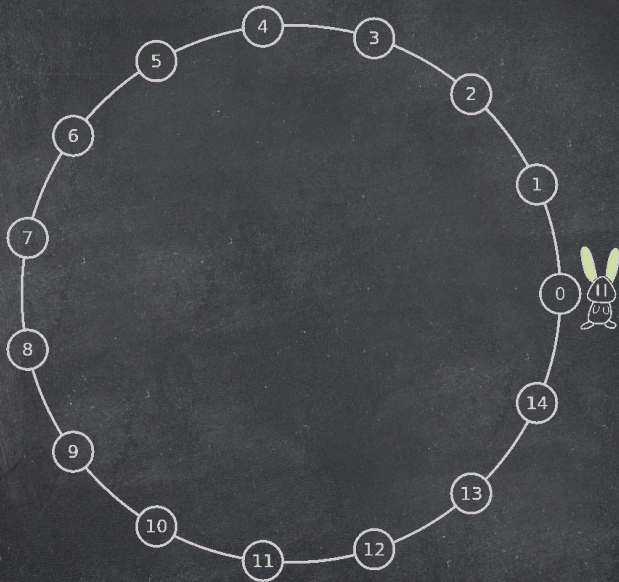
Diofantoszi egyenletek

A kongruencia fogalma

A kongruenciareláció tulajdonságai

Lineáris kongruencia

Hol lesz Gyula 1512 ugrás után?



Gyula-ekvivalencia

Kérdés

Hol lesz Gyula 1512 ugrás után?

Válasz

$1512 = 100 \cdot 15 + 12 \implies$ a 12-esnél lesz.

Tehát 1512 és 12 ekvivalensek Gyula ugrálása szempontjából:

$$1512 \equiv 12 \pmod{15}.$$

Kérdés

Ugyanott lesz-e Gyula 239 ugrás után, mint 539 ugrás után?

Válasz

$539 - 239 = 300 = 20 \cdot 15 \implies$ igen, ugyanott lesz (de hol?).

Tehát 239 és 539 ekvivalensek Gyula ugrálása szempontjából:

$$239 \equiv 539 \pmod{15}.$$

A kongruencia fogalma

Rögzítünk egy $m \geq 2$ egész számot (**modulus**), és csak arra vagyunk kíváncsiak, hogy adott szám(ok) milyen maradékot ad(nak) m -mel osztva.

Formálisan ezt egy ekvivalenciarelációval tudjuk leírni:

Definíció

Tetszőleges a, b egész számok esetén azt mondjuk, hogy **a kongruens b -vel modulo m** , ha ugyanazt a maradékot adják m -mel osztva.

Definíció

Tetszőleges a, b egész számok esetén azt mondjuk, hogy **a kongruens b -vel modulo m** , ha $m \mid a - b$.

Tétel

A fenti két definíció ekvivalens.

Jelölés: $a \equiv b \pmod{m}$.

Példák

- $2026 \stackrel{?}{\equiv} 1234 \pmod{3}$

Igaz, mert $2026 \equiv 1 \pmod{3}$ és $1234 \equiv 1 \pmod{3}$.

- $2026 \stackrel{?}{\equiv} -666 \pmod{10}$

Hamis, mert $2026 \equiv 6 \pmod{10}$ és $-666 \equiv -6 \equiv 4 \pmod{10}$,
tehát nem ugyanazt adják maradékul 10-zel osztva.

- $2572 \stackrel{?}{\equiv} -28 \pmod{13}$

Igaz, mert $2572 - (-28) = 2572 + 28 = 2600$, ami osztható 13-mal.

Igazak-e az alábbi kongruenciák?

(A) $2026 \stackrel{?}{\equiv} 666 \pmod{100}$

(B) $1111 \stackrel{?}{\equiv} 1814 \pmod{7}$

(C) $38 \stackrel{?}{\equiv} -17 \pmod{11}$

CS teszt: 1. előadás - kongruenciák



Igazak-e az alábbi kongruenciák?

(A) $2026 \stackrel{?}{\equiv} 666 \pmod{100}$ Hamis

(B) $1111 \stackrel{?}{\equiv} 1814 \pmod{7}$ Hamis

(C) $38 \stackrel{?}{\equiv} -17 \pmod{11}$ Igaz

Tartalom

Bemelegítés

Diofantoszi egyenletek

A kongruencia fogalma

A kongruenciareláció tulajdonságai

Lineáris kongruencia

Lehet így számolni a maradékokkal?

✓ 12345 négyet ad maradékul 7-tel osztva

✓ 6789 hatot ad maradékul 7-tel osztva

✓ $4 \cdot 6 = 24$, ami hármát ad maradékul 7-tel osztva

??? következésképp $12345 \cdot 6789$ hármát ad maradékul 7-tel osztva

✓ $12345 = 7k + 4$

✓ $6789 = 7\ell + 6$

✓ $24 = 7t + 3$

??? következésképp

$$\begin{aligned} 12345 \cdot 6789 &= (7k + 4) \cdot (7\ell + 6) = \\ &= 7 \cdot (\dots) + 24 = \\ &= 7 \cdot (\dots) + 3 \quad \checkmark \end{aligned}$$

Lehet így számolni a maradékokkal!

Tétel (a kongruencia tulajdonságai)

Tetszőleges a, a_1, a_2, b, b_1, b_2 egész számok és $m \geq 2$ modulus esetén teljesülnek a következők:

1. $a \equiv a \pmod{m}$;
2. $(a \equiv b \pmod{m} \text{ és } b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$;
3. $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$;
4.
$$\left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies \begin{array}{l} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m} \text{ és} \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}. \end{array}$$

Vigyázat!

Az osztással óvatosságnak kell lenni, pl. $24 \equiv 54 \pmod{10}$, de ha leosztunk 6-tal, akkor azt kapjuk, hogy $4 \equiv 9 \pmod{10}$, ami már nem igaz!

$$6 \cdot 4 \equiv 6 \cdot 9 \pmod{10} \not\Rightarrow 4 \equiv 9 \pmod{10}$$

Hogyan kell óvatosnak lenni?

Tétel (a kongruencia tulajdonságai, folyt.)

5. Ha $a \neq 0$, akkor

$$a \cdot b \equiv a \cdot c \pmod{m} \iff b \equiv c \pmod{\frac{m}{\text{Inko}(a, m)}}.$$

6. Ha a és m relatív prímek, akkor

$$a \cdot b \equiv a \cdot c \pmod{m} \iff b \equiv c \pmod{m}.$$

A kongruencia reklámja

Feladat

Mutassuk meg, hogy $2^{n+2} + 3^{2n+1}$ osztható 7-tel minden $n \in \mathbb{N}_0$ esetén.

Megoldás teljes indukcióval

- **Kezdőlépés:** $n = 0$ esetén $2^{n+2} + 3^{2n+1} = 7$. ✓
- **Indukciós lépés:** tfh. $7 \mid 2^{n+2} + 3^{2n+1}$, ez az indukciós hipotézis (IH); célunk belátni, hogy $7 \mid 2^{n+3} + 3^{2n+3}$.

Alakítsuk át az utóbbi kifejezést, hogy fel tudjuk használni (IH)-t:

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

Itt mindkét tag osztható 7-tel, így maga az összeg is osztható 7-tel. ✓

Megoldás kongruenciával

$$2^{n+2} + 3^{2n+1} = 4 \cdot 2^n + 3 \cdot 9^n \equiv 4 \cdot 2^n + 3 \cdot 2^n = 7 \cdot 2^n \equiv 0 \pmod{7} \quad \checkmark$$

Tartalom

Bemelegítés

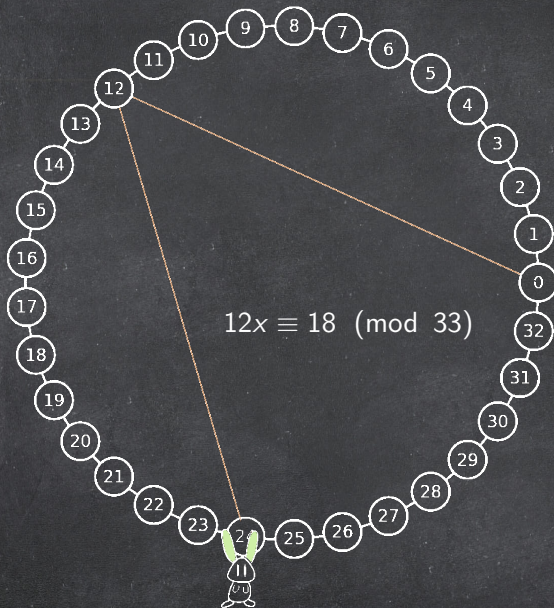
Diofantoszi egyenletek

A kongruencia fogalma

A kongruenciareláció tulajdonságai

Lineáris kongruencia

Hány ugrással jut el Gyula a 18-ba?



Lineáris kongruencia

$$ax \equiv b \pmod{m}$$

- a, b, m adott egész számok, $a \neq 0$, $m \geq 2$
- x ismeretlen egész szám

Tudnunk kell:

- Van-e megoldás?
- Hogyan találunk meg egy megoldást?
- Hogyan találjuk meg az összes megoldást?

Hány ugrással jut el Gyula a 18-ba?

Példa

Oldjuk meg a $12x \equiv 18 \pmod{33}$ lineáris kongruenciát.

Megoldás (kongruenciákkal számolva óvatosan)

Rögtön le tudunk osztani 6-tal ($\text{Inko}(6, 33) = 3$):

$$12x \equiv 18 \pmod{33} \iff 2x \equiv 3 \pmod{11}.$$

Írjunk a jobb oldalon 3 helyett 14-et:

$$2x \equiv 3 \pmod{11} \iff 2x \equiv 14 \pmod{11}.$$

Most le tudunk osztani 2-vel ($\text{Inko}(2, 11) = 1$):

$$2x \equiv 14 \pmod{11} \iff x \equiv 7 \pmod{11}.$$

Tehát először a 7. ugrásnál jut 18-ba (aztán a 18., 29., stb. ugrásoknál is).

Hány ugrással jut el Gyula a 18-ba?

Példa

Oldjuk meg a $12x \equiv 18 \pmod{33}$ lineáris kongruenciát.

Megoldás (diofantoszi egyenletre visszavezetve)

A kongruenciát átfogalmazhatjuk diofantoszi egyenletre:

$$12x \equiv 18 \pmod{33} \iff 12x = 33y + 18 \quad (\exists y \in \mathbb{Z}).$$

A $12x - 33y = 18$ diofantoszi egyenlet egy megoldása: $x_0 = 18, y_0 = 6$.

Az általános megoldás:

$$\begin{aligned} x &= 18 + \frac{33}{\text{lko}(12, 33)} \cdot t = 18 + 11t, \\ y &= 6 + \frac{12}{\text{lko}(12, 33)} \cdot t = 6 + 4t \end{aligned} \quad (t \in \mathbb{Z}).$$

Az x -re kapott képlet azt jelenti, hogy $x \equiv 18 \pmod{11}$.

Lineáris kongruencia

$$ax \equiv b \pmod{m}$$

- a, b, m adott egész számok, $a \neq 0$, $m \geq 2$
- x ismeretlen egész szám

Tudnunk kell:

- Akkor és csak akkor van megoldás, ha $\text{Inko}(a, m) \mid b$.
- A kongruencia ekvivalens az $ax - my = b$ diofantoszi egyenlettel, és ezt meg tudjuk oldani euklideszi algoritmussal.
- Ha x_0 egy partikuláris megoldás, akkor az általános megoldás:

$$x \equiv x_0 \pmod{\frac{m}{\text{Inko}(a, m)}}.$$