

2018.02.10.

2. Feladat

Diszkrét mat.

21. tétel: Végtelen sok prím van.

Biz.:

Tfh. véges sok prím van. $p_1, p_2, \dots, p_k$

$p_1 p_2 \dots p_k$ számok össze:

$a = (p_1 p_2 \dots p_k) + 1$ legyen.

↑

a -t p_i -vel osztva a maradék 1.

$p_i \nmid a \quad \forall i \in \{1, 2, \dots, k\}$

→ a prím: ez ellentmondás. ✓

→ a nem prím: a prímosztója új prím. ✓

(Euler-Gauss bizonyítás).

Ellentmondás.

22. Tétel:

Biz.:

$(k^2 - 1)$ alakú.

Tfh. véges sok ilyen van. $p_1, p_2, \dots, p_k$

Gyökök újat:

$a = k p_1 \dots p_k p_k - 1$

↑

Ez is $k^2 - 1$ alakú lett.

(2ka.) $p_i \nmid a$ mert $i \in \{1, \dots, k\}$.

• maga a prím. Ellentmondás. ✓

• Ha a nem prím: $\rightarrow \exists k^2 - 1$ alakú prímosztója van.

↓ $\exists k^2 + 1$ alakú prímosztója van. Mindegyik ilyen.

$$(k^2_1 + 1)(k^2_2 + 1) =$$

$$= \underbrace{(k^2_1 k^2_2 + k^2_1 + k^2_2 + 1)}_{k^2} \quad k^2 + 1 \text{ alakú lesz. Ez ellentmondás}$$

(1)

27. Tétel:

(Biz.)

Legyen

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + (n+1)$$

$\begin{matrix} |2 & 13 & 14 & \dots & |n+1 \end{matrix}$

az mind összeget szám és $\frac{n}{2}$ darab van benne.

Kongruenciák:

$$2 \equiv 7 \pmod{5} \quad \text{ugyanannyi a maradék}$$

$$7 = 12 \equiv -3 \equiv 2 \pmod{5}$$

↑ Ez neglepo, de ez van mindig osztható áttel.

KONGRUENCIA:

$$5 \mid 12 - 7$$

$$5 \mid 3 + 2$$

stb.

$$a \equiv b \pmod{m} \quad m \mid b - a$$

vagy $m \mid a - b$

a és b ugyanannyi maradékot ad m -el osztva.
mindegy. $a, b, m \in \mathbb{Z}$.

33. def.

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

$$6x \equiv 2 \pmod{8}$$

$$\downarrow$$

$$6x \equiv 2 \equiv 18 \quad /: 6$$

$$x \equiv 3 \pmod{\frac{8}{\text{lnko}(8,6)}}$$

Megoldható, ha $\text{lnko}(a, m) \mid b$.

$$x \equiv 3 \pmod{4}$$

$$ax \equiv b \pmod{m} \Rightarrow m \mid ax - b$$

$$\exists y \in \mathbb{Z}$$

$$my = ax - b \rightarrow$$

$$\boxed{ax - my = b}$$

diophantosi egyenlet.

②

Tehát:

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

megoldható, ha $\text{lkko}(a, m) \mid b$.

Az előbb tehát azt be is bizonyítottuk.

Vannak kongruencia-rendszerek is.

36 Lemma

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

$$x = \underbrace{q_1}_{\uparrow} m_1 + c_1 = \underbrace{q_2}_{\rightarrow} m_2 + c_2$$

ismételjük.

$$q_1 m_1 - q_2 m_2 = c_2 - c_1$$

ismét diofantoszi egyenlet:

$$\text{lkko}(m_1, m_2) \mid c_2 - c_1.$$

A megoldhatóság feltétele.

Ezt mindig végig kell nézni. Kivéve, ha a modulusz relatív prímek, akkor $\text{lkko}(m_1, m_2) = 1$ és $1 \mid c_2 - c_1$ minden esetben...

Feladat:

$$(1/a)$$

$$1.37/a.$$

$$6x \equiv 4 \pmod{8}$$

megoldható?

$$\text{lkko}(6, 8) = 2 \mid 4 \quad \checkmark$$

Megoldható.

$$6x \equiv 12 \pmod{8}$$

$$x \equiv 2 \pmod{\frac{8}{\text{lko}(6,8)}}$$

2

$$x \equiv 2 \pmod{4}$$

Erreje:

$$\textcircled{c} \quad 88x \equiv 42 \pmod{55}$$

$$\text{lko}(88, 55) = 11$$

$11 \nmid 42$
nem osztható.

Nincs megoldás.

$$\textcircled{c} \quad 9x \equiv 15 \pmod{12}$$

$$9x \equiv 27 \pmod{12} \quad / :3$$

$$\text{lko}(9, 12) = 3$$

az eredeti modulus
számt 3 megoldás van.

$3 \mid 15$ megoldható. ✓

$$x \equiv 3 \pmod{\frac{12}{\text{lko}(9,12)}}$$

$$x \equiv 3 \pmod{4}$$

Rendszer.

1.40/a.

$$x \equiv 7 \pmod{8}$$

$$x \equiv 6 \pmod{7}$$

||

$$x \equiv -1 \pmod{\text{lko}(8,7)}$$

7.8

$\text{lko}(8,7) = 1$ relatív prím

$1 \mid 7-6$ ✓

Ez a Brute-force megoldás.

1.40/e.

$$\begin{aligned} X &= 5z + 3 \\ X &\equiv 3 \pmod{5} \\ X &\equiv 4 \pmod{7} \end{aligned} \quad \begin{aligned} &\Rightarrow \\ &\text{luko}(5, 7) = 1 \mid 3-4 \checkmark \end{aligned}$$

Megoldható, relatív
prímek.

$$5z + 3 \equiv 4 \pmod{7}$$

oldjuk meg.

$$5z \equiv 1 \pmod{7} \quad \checkmark \quad \text{Megoldható, itt is relatív}$$

↓

$$5z \equiv 15$$

$$z \equiv 3 \pmod{\frac{7}{\text{luko}(5,7)}}$$

↓

$$z = 7l + 3$$

$$X = 5z + 3 = 5 \cdot (7l + 3) + 3 =$$

$$= 35l + 18$$

$$X \equiv 18 \pmod{35}$$

1.18. feladat

van a tesitben.

Diophantosi egyenlet van.

$$a) \quad 11x - 8y = 3$$

$$x = y = 1 \text{ megoldás}$$

$$x_0 = 1$$

$$x = x_0 + \frac{-8}{1} \cdot t$$

$$10 \leq x \leq 30$$

2 db van.

$$1, 9, (17, 25) 35$$

(5.)

1.17/2.

$$21x - 15y = 12$$

diophantosi egyenletünk

1. lépés:

$$\text{lnko}(21, 15) \mid 12$$

euklideszi algoritmus:

$$21 = 15 + 6$$

$$15 = 2 \cdot 6 + 3$$

$$\text{lnko}(21, 15) = 3 \quad 3 \mid 12 \checkmark$$

$$6 = 2 \cdot 3 + 0$$

Megoldható.

2. lépés

$$\text{lnko}(21, 15) = 21 \cdot u - 15 \cdot v \text{ alakban}$$

$$3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (21 - 15) = (-2) \cdot 21 + 3 \cdot 15$$

$$6 = 21 - 15$$

$$3 = -2 \cdot (21) - 15 \cdot (-3) \text{ írható fel!}$$

3. lépés

Be kell szerezni még.

$$12 = (-8) \cdot 21 - 15 \cdot (-12) \text{ írható fel}$$

ez egy megoldás

utolsó lépés:

$$x = -8 + \frac{-15}{3} \cdot t$$

$$t \in \mathbb{Z}$$

$$y = -12 - \frac{21}{3} t$$