1.

gcm es lcm kell, de primtenyezokre bontani lassu ezert be kell ujitani: euklideszi algoritmus

a)

$$a = 13, b = 14$$

a ket szam kozul kivalasztjuk a nagyobbikat, es modoljuk

$$14 \bmod 13 = 1$$

a vegeredmennyel megcsinaljuk ugyanezt

$$13 \bmod 1 = 0$$

a legutolos nem 0 ertek lesz a legnagyobb kozos oszto

$$\mathrm{gcm}(14, 13) = 1$$

lcm pedig

$$\mathrm{lcm}(a, b) = \frac{a \cdot b}{\mathrm{gcm}(14,\ 13)}$$

$$\mathrm{lcm}(14, 13) = \frac{14 \cdot 13}{1} = 182$$

## b)

$$a = 16, b = 37$$

$$37 \bmod 16 = 5$$

$$16 \bmod 5 = 1$$

$$5 \bmod 1 = 0$$

$$\mathrm{gcm}(16, 37) = 1$$

$$\mathrm{lcm}(16, 37) = \frac{16 \cdot 37}{1} = 592$$

celszerubb tablazatban dolgozni (elso ket sorban nincs semmi) a bal oszlop a mod es a jobb az hogy hanyszor van meg

## c)

$$a = 90, b = 111$$

| | |
|---|---|
| 111 | |
| 90 | |
| 21 | 1 |
| 6 | 4 |
| 2 | 3 |
| 0 | 2 |

a nulla feletti szam lesz a gcm

$$\mathrm{gcm}(111, 90) = 3$$

$$\mathrm{lcm}(111, 90) = \frac{111 \cdot 90}{3} = 3330$$

**d)**

| | |
|---|---|
| 219 | |
| 168 | |
| 51 | 1 |
| 15 | 3 |
| 6 | 3 |
| 3 | 2 |
| 0 | 2 |

$$\mathrm{gcm}(219, 168) = 3$$

$$\mathrm{lcm}(219, 168) = \frac{219 \cdot 168}{3} = 12264$$

**f)**

$$a = 756, b = 795$$

| | |
|---|---|
| 795 | |
| 756 | |
| 39 | 1 |
| 15 | 19 |
| 9 | 2 |
| 6 | 1 |
| 3 | 1 |
| 0 | 2 |

$$\mathrm{gcm}(795, 756) = 3$$

$$\mathrm{lcm}(795, 756) = \frac{795 \cdot 756}{3} = 20034$$

## kongruencia

kongruencia ugy mukodik hogy $a, b \in \mathbb{Z} : a \equiv b (\operatorname{mod} n) \quad \text{ha } n \mid a - b$

ekvivalenciarelaciot jelol a $\equiv$ (reflexiv, szimmetrikus, tranzitiv)

- Reflexiv: $a \equiv a (\operatorname{mod} n)$
- Tranzitiv: $a \equiv b, b \equiv c \Rightarrow a \equiv c (\operatorname{mod} n)$
- Szimmetrikus: $a \equiv b \Longleftrightarrow b \equiv a (\operatorname{mod} n)$

ez azert jo mert ezzel egyenletszeruen meg tuduk oldani problemakat

$$a, b, c, m \in \mathbb{Z} \quad m \neq 0$$

$$ab \equiv a \cdot c \pmod{m} \Longleftrightarrow b \equiv c \quad \left(\operatorname{mod} \frac{m}{(a, m)}\right)$$

### 1. pelda

$$2 \equiv 6 \pmod{6} \Longrightarrow 1 \equiv 4 \quad \left(\operatorname{mod} \frac{6}{2} = 3\right)$$

### 2. pelda

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

ennek tobb megoldasa is lehet, ehhez valamiert eleg $n$ proba (ennyi probalkozasbol garantaltam megtalaljuk a megoldast, de nem mindig van szuksegunk mindre)

$$ax \equiv b \pmod{m} \text{ megoldhato} \Longleftrightarrow (a, m) \mid b \text{ es } (a, m) \text{ db inkongurens megoldas van}$$

## 2

Milyen $x \in \mathbb{Z}$ egeszek elegitik ki a kovetkezo kongurenciakat?

### 2/a

$$x \equiv 1 \operatorname{mod} 3$$

probalgassuk vegig nullatol $n$-szer

$$\text{ha } x = 0 \Longrightarrow 0 \not\equiv 1$$

$$\text{ha } x = 1 \Longrightarrow 1 \equiv 1$$

$$\text{ha } x = 2 \Longrightarrow 2 \not\equiv 1$$

1 az egyetlen helyes megoladas $\Longrightarrow x \equiv 1 \operatorname{mod} 3$

### 2/b

$$2x \equiv 1 \operatorname{mod} 3$$

$$2 \cdot 0 \not\equiv 1$$

$$2 \cdot 1 \not\equiv 1$$

$$2 \cdot 2 = 4 \equiv 1$$

$$x = 2 \operatorname{mod} 3$$

## 2/c

$$2x \equiv 1 \bmod 4$$

$$2 \cdot 0 \not\equiv 1$$

$$2 \cdot 1 \not\equiv 1$$

$$2 \cdot 2 \not\equiv 1$$

$$2 \cdot 3 \not\equiv 1$$

$$2 \cdot 4 \not\equiv 1$$

nincs megoldas azert mert a 2 meg a 4 relativ primek de ezt ki lehet deriteni mashogy is ilyen tiltott technikaval

$$(2,4) = 2 \text{ es } 2 \nmid 1 \text{ tehat nincs megolas}$$

## 2/d

$$2x \equiv 2 \bmod 4$$

ketfele modon lehet csinalni

1. ugy ahogy eddig

nezzuk meg hogy van-e egyaltalan megoldas

$$(2,4) = 2 \quad 2|2$$

ketto megolas van, nezzuk meg mik azok

$$2 \cdot 0 = 0 \not\equiv 2$$

$$2 \cdot 1 = 2 \equiv 2$$

$$2 \cdot 2 = 4 \not\equiv 2$$

$$2 \cdot 3 = 6 \equiv 2$$

$$x \equiv 1, x \equiv 3 \bmod 4$$

2. az elejen keplettel le lehet osztani

$$2x \equiv 2 \bmod 4$$

$$x \equiv 1 \bmod \frac{4}{(4,2)} = 2$$

$$x \equiv 1 \bmod 2$$

a ket megoldas ekvivalens

hogy ha van benne valami nem linearis dolog akkor nehez lesz (nem tudjuk megcsinalni az ellenorzest, stb)

meg kell nezni az osszes lehetoseget

$$x^2 \equiv 1 \bmod 5$$

$$0^2 = 0 \not\equiv 1$$

$$1^2 = 1 \equiv 1$$

$$2^2 = 4 \not\equiv 1$$

$$3^2 = 9 \not\equiv 1$$

$$4^2 = 16 \equiv 1$$

$$x \equiv 1 \text{ vagy } x \equiv 4 \bmod 5$$

**3**

$$2 = i \quad w = \frac{1}{2} + \frac{\sqrt{3}}{2} i$$

mely $n \in \mathbb{Z} : z^n = w^n = 1$?

$$z^4 = i^4 = 1 \Longrightarrow z^{4 \cdot 1} = 1$$

$$w^2 = \frac{1}{4} + \frac{2\sqrt{3}}{4} + \frac{3}{4} \cdot (-1) = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$$

$$w^3 = \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right)\left(\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) = -\frac{1}{4} - \frac{\sqrt{3}}{4} i + \frac{\sqrt{3}}{4} i - \frac{3}{4} = -1$$

ebbol ki lehet talani hogy

$$w^6 = 1 \Longrightarrow w^{6 \cdot k} = 1$$

ezzel a tudassal ki lehet talalni azt is hogy

$$z^4 = 1, w^6 = 1 \quad \operatorname{lcm}(6, 4) = 12$$

ez azt jelenti hogy

$$z^{12 \cdot k} = w^{12 \cdot k} = 1$$

## 4

ket dolgot kell bebizonyitani, ZH-n nem kell de egyszer latnia kell mindenkinek

**1. tetel**

$$(ca, cb) = c(a, b)$$

bizonyitas:

$$d = (a, b) \implies d|a, \qquad d|b \implies cd \mid ca, \qquad cd \mid cb \implies cd \mid (ca, cb)$$

$$d = (a, b) \implies d = ax + by \qquad x, y \in \mathbb{Z}$$

$$cd = cax + cby \implies (ca, cb) \mid cd \impliedby d = (a, b)$$

tehat valoban

$$(ca, cb) = c(a, b)$$

□

**2. tetel**

$$(a, b) = (a - b, b)$$

biz:

$$d = (a, b) \implies d = ax + by = ax + by - bx + bx = (a - b)x + b(x + y) \implies (a - b, b) \mid d$$

$$d = (a, b) \implies d \mid a, \qquad d \mid b \implies d \mid (a - b) \implies d \mid b, \qquad d \mid a - b \implies d \mid (a - b, b)$$

tehat valoban

$$(a, b) = (a - b, b)$$

ez a ketto kell hogy meg tudjuk oldani a negyest

### 4/a

$$(2^{13}-1, 2^8-1) = ?$$

elso azonossagot hasznaljuk

$$(2^{13}-1, 2^8-1) = (2^{13}-1-2^8+1, 2^8-1) = (2^{13}-2^8, 2^8-1) = (2^8(2^8-1), 2^8-1) = (2^5-1, 2^8-1)$$

ezt akkor lehet leosztani a bal oldallal ha a jobb oldal relativ primje. ha leosztjuk egy olyan szammal a bal oldalt amivel a jobb relativ prim akkor az eredmenyen ez nem fog valtoztatni, ezert ez szabad.

pl $(6, 2) = 2$, itt leoszthatok harommal: $(2, 2) = 2$

$$(2^5-1, 2^8-1) = (2^5-1, 2^8-1-2^5-1) = (2^5-1, 2^5(2^3-1)) = (2^5-1, 2^3-1) =$$

lehetne tovabb vinni de mar nagyon uncsi

$$= (31, 7) = 1$$

## megjegyzes:

$$(a, b) = 1 \iff \text{relativ prim}$$

### 4/b

hell na i ain doin allat

### 5

eloszor definialjuk a fibonacci sorozatot:

$$F_1 = F_2 = 1, \quad n \geq 1$$

$$F_{n+2} = F_n + F_{n+1}$$

kerdes: bizonyitsd be hogy $(F_{n+1}, F_n) = 1$

bizonyitas:

$$F_{n+2} - F_{n+1} = F_n$$

az elejen hasznalt tablat hasznalva (a jobb oszlopot ignoralva):

| | |
|---|---|
| $F_{n+1}$ | |
| $F_n$ | |
| $F_{n-1}$ | |
| $F_{n-2}$ | |
| ... | |
| 1 | |
| 0 | |

addig mentunk hogy elertunk a sorozat elejehez

legalja 0, az azelotti tag pedig $F_1 = 1$

ezzel igazoltuk hogy $(F_{n+1}, F_n) = 1$