

## Kongresszus

①  $a, b, m \in \mathbb{Z}$   $a \equiv b \pmod{m}$   $m \mid a - b$

Pl.:  $6 \equiv 4 \pmod{2}$ , mert  $2 \mid \frac{6-4}{2}$ .

$22 \equiv -2 \pmod{8}$ , mert  $8 \mid \frac{22+2}{2}$ .

$a'$  kongresszus,  $b'$ -vel, ha  $a'$  és  $b'$   
 $m'$ -mel osztva ugyan azt a maradékot  
 adja.

## Lis-Fermat tétel

⑤ Ha  $p$  prím,  $a \in \mathbb{Z}$  és  $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Ha  $p$  prím és  $a \in \mathbb{Z} \Rightarrow a^p \equiv a \pmod{p}$

Pl.: Ha  $n \nmid n$  nek  $\Rightarrow n^5 - 1$  vagy  $n^5 + 1$   
 osztatható 11-gyel.

$$p \mid a^{p-1} - 1$$

① Igazdul, hogy  $\underbrace{a \equiv b \pmod m}_{\uparrow} \Rightarrow a \cdot c \equiv b \cdot c \pmod m$

$$m \mid a - b \Rightarrow \underbrace{m \mid (a - b) \cdot c}_{\substack{\uparrow \\ m \mid ac - bc}} \Rightarrow ac \equiv bc \pmod m \quad //$$

② Igazdul, hogy  $a \cdot c \equiv b \cdot c \pmod m \Rightarrow a \equiv b \pmod m$ .

$$\begin{aligned} & \underbrace{a \cdot c \equiv b \cdot c}_{\uparrow} \pmod m \\ & m \mid ac - bc \\ & m \mid c(a - b) \cancel{\Rightarrow} m \mid a - b \\ & \text{ellenőrzi: } 6 \mid 3 \cdot 4 \neq 6 \mid 3 \text{ vagy } 6 \mid 4 \\ & \text{vagy miért leme igaz?} \\ & \hookrightarrow \text{ha } (c, m) = 1 \Rightarrow m \mid c(a - b) \Rightarrow m \mid a - b \end{aligned}$$

PL:  $90 \equiv 30 \pmod 4$

$4 \mid 90 - 30 \Rightarrow 4 \mid 60 \checkmark$  A kongruenciát levezethetjük

5-tel, mert  $(4, 5) = 1$

$$90 : 5 \equiv 30 : 5 \pmod 4$$

$$18 \equiv 6 \pmod 4$$

③ Igazdulj, hogy  $a-b \mid a^n - b^n$ .

H/F Mivel  $a-b \mid a-b$ , ezért  $a \equiv b \pmod{a-b}$ .

Szorzási tulajdonság miatt:  $a^n \equiv b^n \pmod{a-b} \Rightarrow$

$$\Rightarrow a-b \mid a^n - b^n. //$$

④ Igazdulj, hogy  $a+b \mid a^{\frac{n}{2}} - b^{\frac{n}{2}}$ .

H/F Mivel  $a-b \mid a^n - b^n$  (3-as feladat), ezért

$$a+b = a - (-b) \quad | a^n - (-b)^n \quad \text{alapján}$$

$$n=2k \text{ helyettesítéssel: } a+b \mid a^{\frac{2k}{2}} - \underbrace{(-b)^{\frac{2k}{2}}}_{b^{2k}}$$

## Lagrange'szongruenciák

Lagrange szabványcikk. Az  $ax \equiv b \pmod{m}$  alakú  
Lagrangei által egyszerűsítéses lineáris lagrangei által  
megoldható.

① Az  $ax \equiv b \pmod{m}$  megoldhatóak feltétele, hogy  
 $d = (a, m) \mid b$ .  $(a, m)$  a legnagyobb  
számra!

Megoldás menete:

$$\text{Az } ax \equiv b \pmod{m} \text{ megoldható} \Leftrightarrow d = (a, m) \mid b$$
$$\Rightarrow \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

A Lagrangei mindenket időben osztathatja a  
modulushoz relatív prímnek.

$$a_1x \equiv b_1 \pmod{m}$$

- ① Reduktálás
- ② konstrukcióval (azaz  $a_1$ -gyel többet szinjük)

$$\textcircled{1} \quad 24x \equiv 13 \pmod{7}$$

① Reduktions  
durch

$$24 = 3 \cdot 7 + 3$$

$$24 \equiv 3 \pmod{7}$$

||  
↓

$$3x \equiv 13 \pmod{7}$$

$$13 = 2 \cdot 7 - 1$$

$$13 \equiv -1$$

||  
↓

$$\boxed{3x \equiv -1 \pmod{7}}$$

$$-1 \equiv -1 + 7$$

$$-1 \equiv 6 \rightarrow \text{ex wdr} \text{ enthält } 3\text{-mal}$$

② Lösung 24-ges

$$3x \equiv 6 \pmod{7} \quad | :3$$

$$x \equiv 2 \pmod{7} \quad (\text{da 7 vere vältig mit } a \\ (\text{da } 7 \text{ und } 3 \text{ teilerf. sind})$$

$\hookrightarrow$  7-tel extra  
2-t adauer manade!l.

$$\underline{\underline{x = 7k + 2 \quad k \in \mathbb{Z}}}$$

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

|| kell  
 $(a, m) \mid b$

$$(2) \quad 24x \equiv 19 \pmod{13}$$

$$\boxed{24} = 2 \cdot 13 - 2 \quad \left. \begin{array}{l} \\ \boxed{24 \equiv -2 \pmod{13}} \end{array} \right\} \text{I.}$$

$$-2x \equiv 19 \pmod{13}$$

$$\boxed{19} = 1 \cdot 13 + 6 \quad \left. \begin{array}{l} \\ \boxed{19 \equiv 6 \pmod{13}} \end{array} \right\} \text{II.}$$

$$-2x \equiv 6 \pmod{13} \quad | :(-2)$$

$$x \equiv -3 \pmod{13} \quad \text{magg} \quad -3+13 \Rightarrow x \equiv 10 \pmod{13} \Rightarrow$$

$$\Rightarrow \underline{\underline{13x+10}} \text{ alekézésre}$$

$$(3) \quad 13x \equiv 11 \pmod{120}$$

$$(a, m) \mid b? \quad (13, 120) \mid 11 \quad \checkmark$$

Nem lehet redukálni.

$$\boxed{11} = \underbrace{120+11}_{13 \nmid 131} \pmod{120} \rightarrow \text{addig tényleg, amíg nem találunk olyan számot, ami osztatható 13-mal.}$$

$$11 \equiv \underbrace{131+120}_{251} \pmod{120}$$

$$11 \equiv 371 \pmod{120} \rightarrow \text{max 13 próbálkozás.}$$

$$11 \equiv 611 \pmod{120}$$

$$\boxed{13} \nmid 611 \pmod{120} / :13$$

$$\underline{\underline{x \equiv 47 \pmod{120}}}$$

$$\textcircled{4} \quad 142x \equiv 6 \pmod{62} \quad | :2 \quad (142, 62) = 2 \mid 6 \quad \checkmark$$

$$86x \equiv 3 \pmod{31}$$

$\Downarrow$  86 - ist 2-fache 3-mal:  $2 \cdot 31 + 24 \Rightarrow 86 \equiv 24 \pmod{31}$

$$24x \equiv 3 \pmod{31} \quad | :3$$

$$8x \equiv 1 \pmod{31} \quad | + 31$$

$(3, 31) = 1$ , gg &  
modulus neu  
wählbar

$\begin{array}{c} \Delta \\ \Downarrow \\ \end{array}$

$$8x \equiv 32 \pmod{31} \quad | :8$$

$$\underline{\underline{x \equiv 4 \pmod{31}}}$$

$$\textcircled{5} \quad 3x \equiv 8 \pmod{13} \quad (3, 13) = 1$$

$$3x \equiv 8+13 \pmod{13}$$

$$3x \equiv 21 \pmod{13} \quad | :3$$

$$\underline{\underline{x \equiv 7 \pmod{13}}}$$

$$\textcircled{6} \quad 12x \equiv 9 \pmod{15} \quad | :3 \quad (12, 15) = 3 \mid 9 \quad \checkmark$$

$$4x \equiv 3 \pmod{5}$$

$$4x \equiv 3+5 \pmod{5}$$

$$4x \equiv 8 \pmod{5} \quad | :4$$

$$\underline{\underline{x \equiv 2 \pmod{5}}} \quad 52+2 \text{ ist kein } \checkmark$$

$$\textcircled{7} \quad 12x \equiv 9 \pmod{18} \quad (12, 18) = 6 \times 3 \text{ viers} \\ (\text{auch}) \mid 6? \quad \text{nugldas.}$$

$$\textcircled{8} \quad 20x \equiv 10 \pmod{25} \quad | : 5 \quad (20, 25) = 5 \mid 10 \quad \checkmark$$

$$4x \equiv 2 \pmod{5} \quad | + 10$$

$$4x \equiv 12 \pmod{5} \quad | : 4$$

$$\underline{x \equiv 3 \pmod{5}} \quad 5 \nmid 3 \text{ also kein Rest}, \\ \text{aber } 2 \in \mathbb{Z}.$$

$$\textcircled{9} \quad 10x \equiv 25 \pmod{35} \quad | : 5 \quad (10, 35) = 5 \mid 10 \quad \checkmark$$

$$2x \equiv 5 \pmod{7}$$

$$2x \equiv 12 \pmod{7} \quad | : 2$$

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

$$x \equiv 6, 13, 20, 27, 34 \pmod{35}.$$

$$\textcircled{10} \quad 90x + 18 \equiv 0 \pmod{138}$$

$$\begin{array}{r|l} 90 & 3 \\ 30 & 3 \\ 10 & 5 \\ 2 & 2 \\ 1 & \end{array} \quad 2 \cdot 3^2 \cdot 5$$

$$\begin{array}{r|l} 138 & 2 \\ 69 & 3 \\ 23 & 23 \\ 1 & \end{array} \quad 2 \cdot 3 \cdot 23$$

$$\text{Wzg} = 2 \cdot 3 = 6 \mid 18 \quad \checkmark$$

$$90x = -18 \pmod{138} \quad | : 6$$

$$15x \equiv -3 \pmod{23} \quad | : 3$$

$$5x \equiv -1 \pmod{23} \quad | + 2 \cdot 23$$

$$5x \equiv 45 \pmod{23} \quad | : 5$$

$$\underline{\underline{x \equiv 9 \pmod{23}}}$$

11 Mi van, ha tel ugy az az?

$$59x \equiv 11 \pmod{120}$$

ne dedikálunk nem több mint  
azt amit 59-val nem tudunk.

Cserélyül le - M-dt: (azaz ugy nevez kapunk 59-val  
számoltatásra számít)

$$11 \equiv 131$$

↓

Euler-Fermat tétel szerint

az  $x$  körülbelül:

$$\begin{aligned} a^{\ell(n)} &\equiv 1 \pmod{n} \\ \ell(n) &= (\bar{p}_1 - 1) \cdots \end{aligned}$$

$$59^{\ell(120)} \equiv 1 \pmod{120}$$

$$\ell(120) = \varphi(2^3 \cdot 3 \cdot 5)$$

$$\ell(120) = \ell(2^3) \cdot \ell(3) \cdot \ell(5)$$

$$\ell(120) = (2^3 - 2^2)(3 - 1)(5 - 1)$$

$$\ell(120) = 4 \cdot 2 \cdot 4 = 32$$

$$59^{32} \equiv 1 \pmod{120}$$

$$| \cdot 59^{31}$$

$$\underbrace{59^{31}}_{\substack{59 \\ \cdot}} \cdot 59x \equiv 11 \cdot \underbrace{59^{31}}_{\substack{59 \\ \cdot}}$$

$$\underbrace{59^{32}}_{\substack{59 \\ \cdot}} x \equiv 11 \cdot 59^{31}$$

$$1 \cdot x \equiv 11 \cdot 59^{31}$$

$$\underline{x \equiv 11 \cdot 59^{31}} \pmod{120}$$

redukáljuk

$$59^{31} = \underbrace{59^2 \cdot 59^2 \cdots 59^2}_{15} \cdot 59$$

$$3481 \equiv 1 \pmod{120}$$

$$59^{31} = 3481 \cdot 3480 \cdots \cdot 59$$

$$3481 = 29 \cdot 120 + 1$$

$$3481 \equiv 1 \pmod{120} \Rightarrow x \equiv 59 \cdot 11 \pmod{120} \Rightarrow \underline{x \equiv 649 \pmod{120}}$$

$$(12) \quad 23x \equiv 63 \pmod{43}$$

(EF. + Etappe !)

$$23^{\ell(43)} \equiv 1 \pmod{43}$$

$$\alpha^{\ell(n)} \equiv 1 \pmod{n}$$

$$\ell(43) = 42 \quad (43-1)$$

$$23^{42} \equiv 1 \pmod{43}$$

Berzonzirkel  $23^{41}$ -mal:

$$\underbrace{23 \cdot 23}_{} \cdot x \equiv 63 \cdot 23^{41} \pmod{43}$$

$$23^{42}x \equiv 63 \cdot 23^{41} \pmod{43}$$

$$1x \equiv 63 \cdot 23^{41} \pmod{43}$$

Deduktionsfaz:

$$23^{41} = \underbrace{23^2 \cdot 23^2 \cdot \dots \cdot 23^2}_{20} \cdot 23$$

$$= 529 \cdot 529 \dots 529 \cdot 23 \quad (\text{a modular arithm})$$

$\underbrace{\text{+}}_{11} \rightarrow$  43-mal arithm 13 ist ad maradék

$$\underbrace{13 \cdot 13 \cdot 13 \dots}_{20} \cdot 23$$

$$\underbrace{13^{20} \cdot 23}_{\substack{13^4 \cdot 13^4 \cdot 13^4 \cdot 13^4 \cdot 13^4 \\ \downarrow \\ 28561}}$$

$$13^4 \cdot 13^4 \cdot 13^4 \cdot 13^4 \cdot 13^4 \cdot 23 \quad \rightarrow 43\text{-mal arithm 9-est ad maradék}$$

$$13 \equiv 9 \pmod{43}$$

$$9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 23 \Rightarrow 23^{41} \equiv 15 \pmod{43}$$

$$\Rightarrow x \in 23 \cdot 15 \equiv 945 \pmod{43} \Rightarrow 945 = 21 \cdot 43 + 42 \Rightarrow \underline{x \equiv 42 \pmod{43}}$$