

Biemne 2021

-1-

Calculate inversul lui 8 în grupul $(\mathbb{Z}_{100}, +)$.

$$\overline{8} + \overline{x} = \overline{0} (\mathbb{Z}_{100}, +) \Rightarrow \overline{x} = \overline{100 - 8} = \overline{92} \Rightarrow \boxed{\overline{x} = \overline{92}}$$

Inversul lui 8 în $(\mathbb{Z}_{100}, +)$ este $\overline{92}$.

mc. b) Inversul lui 3 în grupul $(\mathbb{Z}_{10}, +)$.

$$\overline{3} + \overline{x} = \overline{0} (\mathbb{Z}_{10}, +) \Rightarrow \overline{x} = \overline{10 - 3} = \overline{7} \Rightarrow \boxed{\overline{x} = \overline{7}}$$

a) Calculate inversul lui 8 în grupul $(U(\mathbb{Z}_{103}), \cdot)$.

$$\overline{8} \cdot \overline{x} = \overline{1} (U(\mathbb{Z}_{103}), \cdot)$$

$$\overline{8} \cdot \overline{x} = \overline{1} \cdot \overline{13}$$

$$\begin{array}{l} \overline{104} \cdot \overline{x} = \overline{13} \\ \overline{104} \stackrel{103}{=} \overline{1} \end{array} \Rightarrow \overline{1} \cdot \overline{x} = \overline{13} \Rightarrow \boxed{\overline{x} = \overline{13}}$$

$$\text{verificare: } 13 \cdot 8 = 104 \equiv 1 \pmod{103}$$

pm: $103 = 8 \cdot \boxed{12} + \overline{7}$ Algoritmul lui Euclid

$$\begin{array}{l} 2: \overline{8} = \overline{7} \cdot \boxed{1} + \overline{1} \\ 3: \overline{7} = \overline{1} \cdot \boxed{7} \end{array}$$

$$\frac{A}{B} = 12 + \frac{1}{1} = \frac{13}{1}$$

$$\frac{103}{8} - \frac{13}{1} = \frac{(-1)^3}{8 \cdot 1} = \frac{(-1)}{8}$$

$$103 \cdot \overline{1} - 8 \cdot 13 = (-1) \Rightarrow (-\overline{8}) \cdot \overline{13} = (-1) \cdot (-1)$$

desigur (e multiplu de 103)

$$\begin{array}{c} \overline{8} \cdot \overline{13} = \overline{1} \\ \downarrow \\ x \end{array} \Rightarrow \boxed{\overline{x} = \overline{13}}$$

⇒ Inversul lui 8 în $(U(\mathbb{Z}_{103}), \cdot)$ este $\overline{13}$.

$$\text{verificare: } 13 \cdot 8 = 104 \equiv 1 \pmod{103}.$$

mc.d) Inversul lui 37 în $U(\mathbb{Z}_{100})$.

$$\overline{37} \cdot \overline{x} = \overline{1} \text{ în } U(\mathbb{Z}_{100})$$

$$1: 100 = 37 \cdot \boxed{2} + 26$$

Algoritmul lui Euclid

$$2: 37 = 26 \cdot \boxed{1} + 11$$

$$\frac{A}{B} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1}}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} =$$

$$3: 26 = 11 \cdot \boxed{2} + 4$$

$$4: 11 = 4 \cdot \boxed{2} + 3$$

$$5: 4 = 3 \cdot \boxed{1} + 1$$

$$= 2 + \frac{1}{1 + \frac{3}{7}} = 2 + \frac{1}{\frac{10}{7}} = \frac{10}{2 + \frac{7}{10}} = \frac{10}{2 + \frac{7}{10}} = \frac{10}{\frac{27}{10}} = \frac{10}{27} = \frac{10}{27}$$

$$6: 3 = 1 \cdot 3$$

$$\frac{100}{37} = \frac{27}{10} = \frac{(-1)^6}{37 \cdot 10} \Rightarrow 100 \cdot 10 - 37 \cdot 27 = 1 \Rightarrow$$

desigur (e multiplu de 100)

$$(-37) \cdot (-27) = 1 \Rightarrow \overline{37} \cdot (-\overline{27}) = \overline{1} \Rightarrow \overline{x} = -\overline{27} \stackrel{100}{=} \overline{73}$$

$$\boxed{\overline{x} = \overline{73}}$$

\rightarrow numărul liniar $\overline{37}$ în $U(\mathbb{Z}_{100})^*$ este $\overline{73}$.

$$\text{verificare: } \overline{37} \cdot \overline{73} = \overline{2701} = \overline{1}$$

e) inversul lui $\overline{2}$ în $U(\mathbb{Z}_{31})^*$

$$\overline{2} \cdot \overline{x} = \overline{1} \quad (U(\mathbb{Z}_{31})^*)$$

$$\overline{2} \cdot \overline{x} = \overline{1} \mid \cdot \overline{16}$$

$$\overline{32} \cdot \overline{x} = \overline{16}$$

$$\text{dor } \overline{32} = \overline{1} \text{ în } U(\mathbb{Z}_{31})$$

$$\text{verificare: } 2 \cdot 16 = 32 \equiv 1 \pmod{31}$$

~~Eugen~~ Să luăm $x \in \{9, 1, 2, \dots, 148\}$ cu proprietatea că $\overline{x} + \overline{37} = \overline{0}$ în $(\mathbb{Z}_{149})^*$

$$\overline{x} + \overline{37} = \overline{0} \quad (\mathbb{Z}_{149})^* \Rightarrow \overline{x} = 149 - \overline{37} = \overline{112} \Rightarrow \boxed{\overline{x} = \overline{112}}$$

~~Eugen~~ \rightarrow numărul liniar \overline{x} în $(\mathbb{Z}_{149})^*$ este $\overline{112}$.

f) Să luăm $x \in \{9, 1, 2, \dots, 148\}$ cu proprietatea $\overline{37} \cdot \overline{x} = \overline{1}$ în $(U(\mathbb{Z}_{149}))^*$

$$\overline{37} \cdot \overline{x} = \overline{1} \quad (\text{in } U(\mathbb{Z}_{149})^*)$$

$$\overline{37} \cdot \overline{x} = \overline{1} \mid \cdot \overline{7} \Rightarrow \overline{148} \cdot \overline{x} = \overline{7} \Rightarrow (-1) \cdot \overline{x} = \overline{7} \stackrel{(-1)}{\Rightarrow} \overline{x} = (-\overline{7}) = \overline{145}$$

$$\text{verificare: } \overline{37} \cdot \overline{145} = \overline{5365} \stackrel{149}{=} \overline{1} \vee$$

$$\text{Avem: } 149 = 37 \cdot \overline{145} + 1$$

$$37 = 1 \cdot 37$$

$$\frac{1}{37} = \frac{1}{1}$$

$$\frac{149}{37} - \frac{1}{1} = \frac{(-1)^2}{37 \cdot 1} = \frac{1}{37 \cdot 1} \Rightarrow \underbrace{149 - 1}_{\text{dispare (e multiplu de 149)}} - 1 \cdot 37 = 1 \Rightarrow (-\overline{7}) \cdot \overline{37} = \overline{1} \Rightarrow \overline{x} = (-\overline{7}) = \overline{145}$$

$$\text{verificare: } \overline{37} \cdot \overline{145} = \overline{5365} \stackrel{149}{=} \overline{1}$$

$$\begin{array}{r} 5365 \\ 145 \\ \hline 36 \\ 2895 \\ 895 \\ \hline 1 \end{array}$$

$$\Rightarrow \boxed{\overline{x} = \overline{145}}$$

g) Să luăm acel unic $x \in \{1, 2, \dots, 150\}$ astfel încât $\overline{37} \cdot \overline{x} = \overline{1}$ în $(\mathbb{Z}_{151})^*$.

$$\overline{37} \cdot \overline{x} = \overline{1} \quad (\text{in } (\mathbb{Z}_{151})^*)$$

$$(37, 151) = 1 \Rightarrow \overline{37} \cdot \overline{x} = \overline{1} \mid \cdot \overline{3} \Rightarrow \overline{118} \cdot \overline{x} = \overline{3} \Rightarrow (-3) \cdot \overline{x} = \overline{3} \mid \cdot (-1)$$

$$\overline{118} \stackrel{151}{=} -3$$

$$\Rightarrow \overline{3} \cdot \overline{x} = (-\overline{3}) \stackrel{151}{=} \overline{148} \Rightarrow$$

$$\overline{x} = \overline{148} : \overline{3} = \overline{49} \Rightarrow \boxed{\overline{x} = \overline{49}}$$

$$\text{verifcare: } \widehat{37} \cdot \widehat{59} = \widehat{1813} \stackrel{?}{=} \widehat{151}$$

sau:
 1: $151 = 37 \cdot \boxed{4} + 3$
 2: $37 = 3 \cdot \boxed{12} + 1$
 3: $3 = 1 \cdot 3$

$$\frac{A}{B} = 1 + \frac{1}{12} = \frac{49}{12} \quad \text{reductibil}$$

$$\frac{151}{37} - \frac{49}{12} = \frac{(-1)^3}{37 \cdot 12} \Rightarrow \underbrace{151 \cdot 12 - 49 \cdot 37}_{\text{drop de fermat tipul de 151}} = (-1) \Rightarrow -\widehat{59} \cdot \widehat{37} = (-1) \mid \cdot (-1)$$

$$\begin{array}{r} 1813 \mid 151 \\ 151 \mid 12 \\ \hline 2303 \\ 302 \\ \hline 1 \end{array}$$

Algoritmul lui Euclid

$$\begin{aligned} \widehat{59} \cdot \widehat{37} &= 1 \Rightarrow \\ \widehat{37}^{-1} &= \widehat{59} = \widehat{x} \Rightarrow \\ \boxed{\widehat{x} = \widehat{59}} \end{aligned}$$

\Rightarrow numărul căutat x din $U(\mathbb{Z}_{151})$ este $\widehat{59}$

Găsirea inversului lui $\widehat{61}$ în $U(\mathbb{Z}_{103})$), $\widehat{61} \cdot \widehat{x} = \widehat{1}$
 $\widehat{61} \cdot \widehat{x} = \widehat{1} \quad \text{în } U(\mathbb{Z}_{103})$

$$\widehat{61} \cdot \widehat{x} = \widehat{1}$$

Algoritmul lui Euclid

$$\begin{aligned} 1: \quad 103 &= 61 \cdot \boxed{1} + 42 \\ 2: \quad 61 &= 42 \cdot \boxed{1} + 19 \\ 3: \quad 42 &= 19 \cdot \boxed{2} + 5 \\ 4: \quad 19 &= 5 \cdot \boxed{3} + 4 \\ 5: \quad 5 &= 4 \cdot \boxed{1} + 1 \\ 6: \quad 4 &= 1 \cdot \boxed{4} \end{aligned}$$

$$\begin{aligned} \frac{A}{B} &= 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{5 + \frac{1}{1}}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5}}} = \\ &= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{11}}} = 1 + \frac{1}{1 + \frac{1}{11}} = 1 + \frac{1}{12} = \\ &= 1 + \frac{11}{12} = \frac{23}{12} \quad \text{reductibil} \end{aligned}$$

$$\frac{103}{61} - \frac{23}{16} = \frac{(-1)^6}{61 \cdot 16} = \frac{1}{61 \cdot 16}$$

$$103 \cdot 16 - 23 \cdot 61 = 1 \Rightarrow (-27) \cdot \widehat{61} = \widehat{1} \Rightarrow \text{inversul lui } 61 \stackrel{x}{=} (-27) =$$

drop de (e multiplu de 103)

$$\stackrel{103}{\equiv} \widehat{76} \Rightarrow \boxed{\widehat{x} = \widehat{76}}$$

verificare: $\widehat{61} \cdot \widehat{76} \stackrel{?}{=} \widehat{636} \stackrel{?}{=} \widehat{1} \pmod{103}$

sau: $\widehat{61} \cdot \widehat{x} = \widehat{1} \mid \cdot 2$

$$122 \cdot \widehat{x} = \widehat{2} \Rightarrow 19 \cdot \widehat{x} = \widehat{2} \mid \cdot 5$$

$$\begin{array}{r} 636 \mid 103 \\ 512 \mid 55 \\ \hline 256 \\ 512 \\ \hline 256 \\ \hline 0 \end{array}$$

$$\Rightarrow 55 \cdot \widehat{x} = \widehat{10} \quad \left| :2 \right.$$

$$\widehat{95} \stackrel{103}{\equiv} \widehat{(-8)}$$

$$(-5) \cdot \widehat{x} = \widehat{5} \mid (-1) \Rightarrow 5 \cdot \widehat{x} = (-5) \stackrel{103}{\equiv} \widehat{(-108)} = \widehat{103}$$

$$\Rightarrow \widehat{x} = \widehat{76} \Rightarrow \boxed{\widehat{x} = \widehat{76}}$$

MCJ) $149 \cdot \bar{x} \equiv 1 \pmod{323}$

~~$149 \cdot \bar{x} \equiv 1 \pmod{\mathbb{Z}_{323}}$~~

~~$149 \cdot \bar{x} = 1$~~

Algorithmus mit Euklid

$$\begin{aligned} 1: \quad 323 &= 149 \cdot \boxed{2} + 25 \\ 2: \quad 149 &= 25 \cdot \boxed{5} + 24 \\ 3: \quad 25 &= 24 \cdot \boxed{1} + 1 \\ 4: \quad 24 &= 1 \cdot \boxed{24} \end{aligned}$$

$$323 = 14 \cdot 19$$

$$\varphi(323) = (14-1)(19-1) = 16 \cdot 18 = 288$$

$149 \cdot \bar{x} \equiv 1 \pmod{288}$

$$149 \cdot \bar{x} = 1$$

Algorithmus mit Euklid

$$\begin{aligned} 1: \quad 288 &= 149 \cdot \boxed{1} + 139 \\ 2: \quad 149 &= 139 \cdot \boxed{1} + 10 \\ 3: \quad 139 &= 10 \cdot \boxed{13} + 9 \\ 4: \quad 10 &= 9 \cdot \boxed{1} + 1 \\ 5: \quad 9 &= 1 \cdot \boxed{9} \end{aligned}$$

$$\frac{A}{B} = 2 + \frac{1}{\frac{1}{5} + \frac{1}{1}} = 2 + \frac{1}{\frac{6}{5}} = 2 + \frac{5}{6} = \frac{17}{6}$$

~~$\frac{17}{6}$~~ reduziert

$$\frac{323}{149} - \frac{\frac{17}{6}}{\frac{17}{6}} = \frac{(-1)^5}{149 \cdot 2} = \frac{1}{149 \cdot 2}$$

~~$323 \cdot \frac{6}{149} - 149 \cdot \frac{17}{6} = 1 \Rightarrow (-149) \cdot \frac{17}{6} = 1 \Rightarrow$~~

~~$\text{divide (e multipli de 323)}$~~

$$149 \cdot (-\frac{17}{6}) = 1$$

$$\begin{aligned} \frac{A}{B} &= 1 + \frac{1}{1 + \frac{1}{13 + \frac{1}{1}}} = 1 + \frac{1}{1 + \frac{1}{13}} = \\ &= 1 + \frac{1}{1 + \frac{1}{13}} = 1 + \frac{1}{\frac{14}{13}} = 1 + \frac{13}{14} = \frac{29}{15} \end{aligned}$$

$$\frac{288}{149} - \frac{29}{15} = \frac{(-1)^5}{149 \cdot 15} = \frac{(-1)}{149 \cdot 15}$$

~~$288 \cdot 15 - 29 \cdot 149 = (-1) \cdot (A)$~~

~~$\text{divide (e multipli de 288)}$~~

$$\Rightarrow (-29) \cdot 149 = -1 \pmod{288}$$

$$29 \cdot 149 = 1 \Rightarrow \bar{x} = 29 = \text{dividierend div } 149 \Rightarrow \boxed{\bar{x} = 29}$$

reziproko: $149 \cdot 29 = 4321 = 1 \checkmark$

somit: $149 \cdot \bar{x} \equiv 1 \pmod{288}$

$$149 \cdot \bar{x} = 1 | \cdot 2 \Rightarrow 298 \cdot \bar{x} = 2$$

$$298 \equiv 10$$

$$5 \cdot \bar{x} \equiv 1 \pmod{288}$$

$$\begin{array}{r} 5321 \mid 288 \\ 288 \mid 15 \\ 1451 \mid 15 \\ 1450 \mid 15 \\ \hline = 1 \end{array}$$

$\bar{x} = 29 + 288 \cdot k$
 $\bar{x} = 317 \checkmark$

8.317 eV

$$10 \cdot \bar{x} = 2 | : 2 \Rightarrow \frac{10}{2} = \frac{1}{5} \cdot \bar{x} = 1 \pmod{288}$$

?

Algorithmus Euklid

- 1: $288 = 5 \cdot \boxed{57} + 3$
- 2: $5 = 3 \cdot \boxed{11} + 2$
- 3: $3 = 2 \cdot \boxed{11} + 1$
- 4: $2 = 1 \cdot \boxed{2}$

$$\frac{A}{B} = 57 + \frac{1}{1+\frac{1}{1}} = 57 + \frac{1}{1+1} = 57 + \frac{1}{2} = \frac{115}{2} \quad \text{reduzit.}$$

$$\frac{288}{5} - \frac{115}{2} = \frac{(1)^5}{5 \cdot 2} = \frac{1}{10}$$

$$288 \cdot 2 - 115 \cdot 5 = 1 \quad (\text{A.}) \Rightarrow (-\overline{115}) \cdot \overline{5} = \overline{1} \Rightarrow$$

divide
(remultipliziert mit 288)

$$\Rightarrow \text{Inverses zu } \overline{5} = (-\overline{115}) = \overline{x} \quad \boxed{\overline{x} = \overline{173}} \quad ?$$

K) $67 \cdot \overline{x} \equiv 1 \pmod{840}$

Algorithmus Euklid

- 1: $840 = 67 \cdot \boxed{12} + 36$
- 2: $67 = 36 \cdot \boxed{11} + 31$
- 3: $36 = 31 \cdot \boxed{1} + 5$
- 4: $31 = 5 \cdot \boxed{6} + 1$
- 5: $5 = 1 \cdot \boxed{5}$

$$\frac{A}{B} = 12 + \frac{1}{1+\frac{1}{1+\frac{1}{6}}} = 12 + \frac{1}{1+\frac{1}{6}} = 12 + \frac{13}{7} = 12 + \frac{13}{7} = \frac{163}{13} \quad \text{reduzit.}$$

$$\frac{840}{67} - \frac{163}{13} = \frac{(-1)^5}{67 \cdot 13} = \frac{(-1)}{67 \cdot 13}$$

$$840 \cdot 13 - 163 \cdot 67 = (-1) \quad (\text{A.}) \Rightarrow (-\overline{163}) \cdot \overline{67} \equiv -1 \pmod{840}$$

divide

$$\Rightarrow \overline{x} = \text{Inverses zu } \overline{67} = \overline{163} \Rightarrow \boxed{\overline{x} = \overline{163}}$$

L) $\overline{11} \cdot \overline{x} = \overline{1} \pmod{31}$

$$\begin{aligned} 33 \cdot \overline{x} &= \overline{3} \Rightarrow \overline{2x} = \overline{3} \\ \overline{33} &\equiv \overline{2} \pmod{31} \end{aligned}$$

Sum: $31 = 11 \cdot \boxed{2} + 9$

$$\begin{aligned} 1: \quad 11 &= 9 \cdot \boxed{1} + 2 \\ 2: \quad 9 &= 2 \cdot \boxed{4} + 1 \end{aligned}$$

$$3: \quad 2 = 1 \cdot \boxed{2}$$

$$4: \quad 11 \cdot 4 - 9 \cdot 1 = 1 \quad (\text{A.})$$

$$\overline{2x} \equiv \overline{3} \pmod{31} \quad | : 2$$

$$\Rightarrow \boxed{\overline{x} \equiv \overline{17}} \quad \text{in } U(\mathbb{Z}_{31})$$

$$\frac{A}{B} = 2 + \frac{1}{1+\frac{1}{5}} = 2 + \frac{1}{5} = 2 + \frac{1}{5} = \frac{11}{5} \quad \text{reduzit.}$$

$$\frac{31}{11} - \frac{11}{5} = \frac{(-1)^5}{11 \cdot 5} = \frac{1}{11 \cdot 5}$$

$$\Rightarrow (-\overline{11}) \cdot \overline{15} = \overline{1} \Rightarrow \overline{11} \cdot (-\overline{15}) \equiv \overline{1} \pmod{31}$$

$$\Rightarrow \overline{x} = (-\overline{15}) \stackrel{31}{=} \overline{17} \Rightarrow \boxed{\overline{x} = \overline{17}}$$

verifizieren: $\overline{11} \cdot \overline{17} = \overline{187} = \overline{1} \checkmark$

m) $\widehat{23} \cdot \widehat{x} = 1$ in $U(\mathbb{Z}_{71})$

Algorithmus von Euklid

$$1: \overline{71} = 23 \cdot \overline{3} + \overline{2}$$

$$2: \overline{23} = 2 \cdot \overline{11} + \overline{1}$$

$$3: \overline{2} = 1 \cdot \overline{12}$$

$$\frac{\overline{11}}{\overline{2}} = 3 + \frac{1}{11} = \frac{34}{11}$$

$$\frac{\overline{71}}{\overline{23}} - \frac{34}{11} = \frac{(-1)^3}{23 \cdot 11} = \frac{(-1)}{23 \cdot 11}$$

$$\overline{71} \cdot \overline{11} - 34 \cdot \overline{23} = \overline{(-1)} \quad A. \checkmark$$

divide (e
multipliziert mit $\overline{71}$) \Rightarrow

$$\Rightarrow (-34) \cdot (\widehat{23}) = (-1) | \cdot (-1) \Rightarrow 34 \cdot \widehat{23} = 1 \Rightarrow \widehat{x} = \text{dividende} \text{ div } \widehat{23} = 34$$

$\boxed{\widehat{x} = 34}$

verifizieren: $\widehat{23} \cdot \widehat{34} = \widehat{1}$ | . $\widehat{3}$ in $U(\mathbb{Z}_{71})$

$$\text{son: } \widehat{23} \cdot \widehat{x} = \widehat{1} | \cdot \widehat{3} \Rightarrow (-2) \widehat{x} = \widehat{3} | (-1) \Rightarrow \widehat{2x} = -\widehat{3} \stackrel{!}{=} \widehat{68} | : \widehat{2}$$

$\overline{11}$

$\overline{-2}$

$$\text{verifizieren: } \widehat{23} \cdot \widehat{34} = \widehat{782} = \widehat{1} \checkmark$$

m) $\widehat{163} \cdot \widehat{x} = 1$ in $U(\mathbb{Z}_{2025})$

Algorithmus von Euklid

$$1: 2025 = 163 \cdot \overline{12} + 68$$

$$2: 163 = 68 \cdot \overline{2} + 27$$

$$3: 68 = 27 \cdot \overline{2} + 17$$

$$4: 27 = 17 \cdot \overline{1} + 10$$

$$5: 17 = 13 \cdot \overline{1} + 4$$

$$6: 13 = 1 \cdot \overline{13}$$

$$\frac{\overline{12}}{\overline{2}} = 12 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1}}}} =$$

$$= 12 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} = 12 + \frac{1}{2 + \frac{1}{\frac{5}{2}}} =$$

$$= 12 + \frac{1}{\frac{5}{2} + \frac{2}{5}} = 12 + \frac{1}{\frac{12}{5}} = 12 + \frac{5}{12} =$$

$$\frac{2025}{163} - \frac{149}{12} = \frac{(-1)^6}{163 \cdot 12} = \frac{1}{163 \cdot 12} = \frac{149}{12}$$

$$\underbrace{2025 \cdot 12 - 149 \cdot 163 = 1}_{\text{dividende}} \quad (A) \checkmark \Rightarrow (-149) \cdot \widehat{163} = \widehat{1} \pmod{2025}$$

$$\Rightarrow \hat{x} = (-\hat{b}g) \stackrel{2025}{=} 1875 \quad \boxed{\hat{x} = 1875} \checkmark$$

(2) 2023^{1999} - restul împărțirii la 100. Ultimile 2 cifre.

$$2023^{1999} = 100 \cdot q + r \quad r \in \{0, 1, \dots, 99\} \quad \text{in } \mathbb{Z}_{100}$$

$2023^{1999} \equiv r \pmod{100}$ (100 este divisor, e multiplu de 100).

$$2023^{1999} \equiv 23^{1999}$$

$$2023 \equiv 23 \pmod{100}$$

$$(23, 100) = 1 \Rightarrow 23^{\varphi(100)} \equiv 1$$

$$\begin{array}{r} 2023 \mid 100 \\ 200 \mid 2 \\ \hline 23 \end{array}$$

$$\varphi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$$|\mathbb{U}(\mathbb{Z}_{100})| = 40$$

$$\Rightarrow 23^{40} \equiv 1 \pmod{100} \quad \text{Teorema lui Euler}$$

Algoritmul lui Euclid

$$1: 100 = 23 \cdot 4 + 8$$

$$2: 23 = 8 \cdot 2 + 7$$

$$3: 8 = 7 \cdot 1 + 1$$

$$4: 7 = 1 \cdot 7$$

$$\frac{A}{B} = 4 + \frac{1}{2+1} = 4 + \frac{1}{3} = \frac{13}{3}$$

$$\frac{100}{23} - \frac{13}{3} = \frac{(-1)^4}{23 \cdot 3} = \frac{1}{23 \cdot 3}$$

$$100 \cdot 3 - 23 \cdot 13 = 1 \quad (\text{A}), \Rightarrow$$

dimpotrivă

$$23(-13) \equiv 1 \Rightarrow \bar{x} = -\bar{13} \pmod{100}$$

$$\bar{x} = \boxed{\bar{87}}$$

⇒ ultimele cifre sunt 87

$$\begin{array}{r} 23 \cdot \\ 87 \\ \hline 161 \\ 2001 \end{array}$$

(3) Care sunt ultimele 2 cifre ale lui 193^{197} ?

în $\mathbb{U}(\mathbb{Z}_{100})$

$$(193, 100) = 1 \Rightarrow 193^{\varphi(100)} \equiv 1$$

$$\varphi(100) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40$$

$$\Rightarrow 193^{40} \equiv 1$$

$$\Rightarrow (\widehat{193}^{40})^5 = \widehat{1} \Rightarrow \widehat{193}^{200} = \widehat{1} \Rightarrow \widehat{193}^{197} \cdot \widehat{193}^3 = \widehat{1} \Rightarrow$$

$$\widehat{193}^{197} = (\widehat{193}^{-1})^3 = (\widehat{93}^{-1})^3$$

$$\widehat{193} \equiv \widehat{93} \pmod{100}$$

$$1: 100 = 93 \cdot \boxed{1} + 7$$

$$\frac{\widehat{1}}{\widehat{1}} = 1 + \frac{1}{\widehat{93} + \frac{1}{3}} = 1 + \frac{1}{\frac{40}{3}} = 1 + \frac{3}{40} = \frac{43}{40}$$

$$2: 93 = 7 \cdot \boxed{13} + 2$$

$$\Rightarrow \frac{100}{93} - \frac{43}{40} = \frac{(-1)^7}{93 \cdot 40} = \frac{1}{93 \cdot 40}$$

$$3: 7 = 2 \cdot \boxed{3} + 1$$

$$4: 2 = 1 - \boxed{1}$$

$$100 \cdot 40 - 93 \cdot 43 = 1 \quad (\text{A}) \Rightarrow$$

$$(\widehat{93})^{40} = \widehat{1} \Rightarrow \widehat{93} \cdot (-\widehat{93}) = \widehat{1} \quad \text{droppe}$$

$$\widehat{x} = \widehat{93}^{-1} = (-\widehat{93}) = \widehat{57} \pmod{100}$$

$$(\widehat{193}^{-1})^3 = (\widehat{93}^{-1})^3 = (\widehat{57})^3 = 185 \cdot \widehat{193} \rightarrow \text{ultimale 2. c. fe. sumt } \underline{\widehat{193}}.$$

$$\text{Dau: } \widehat{193}^{197} \text{ in } U(\mathbb{Z}_{100})$$

$$\widehat{193}^{197} = (-\widehat{7})^{197} = -(\widehat{7})^{197} = \widehat{x} \mid \cdot (-\widehat{7})^3 \Rightarrow$$

$$\widehat{193} \equiv \widehat{93} \pmod{100} \equiv (-\widehat{7}) \pmod{100}$$

$$\varphi(100) = 100 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) = 40 \Rightarrow \widehat{193}^{40} = \widehat{1} \Rightarrow \widehat{7}^{40} = \widehat{1}$$

$$(193, 100) = 1$$

$$\Rightarrow \widehat{x} \cdot (-\widehat{7})^3 = \widehat{7}^{200} = (\widehat{7}^{40})^5 = \widehat{1}$$

$$\widehat{x} \cdot (-\widehat{353}) = \widehat{1} \text{ in } U(\mathbb{Z}_{100}) \Rightarrow \widehat{x} \cdot \widehat{57} = \widehat{1} \pmod{100}.$$

$$(-\widehat{353}) = \widehat{57} \pmod{100}$$

$$1: 100 = 57 \cdot \boxed{1} + 43$$

$$2: 57 = 43 \cdot \boxed{1} + 14$$

$$3: 43 = 14 \cdot \boxed{3} + 1$$

$$4: 14 = 1 \cdot \boxed{14}$$

$$\frac{\widehat{1}}{\widehat{1}} = 1 + \frac{1}{\widehat{57} + \frac{1}{3}} = 1 + \frac{1}{\frac{40}{3}} = 1 + \frac{3}{40} = \frac{43}{40} \quad \text{Reductio b2}$$

$$\frac{100}{57} - \frac{43}{57} = \frac{(-1)^7}{57 \cdot 4} = \frac{1}{57 \cdot 4}$$

$$100 \cdot \widehat{4} - 57 \cdot \widehat{4} = 1 \quad (\text{A})$$

$$\Rightarrow (-\widehat{57}) \cdot \widehat{4} = \widehat{1} \Rightarrow$$

$$\widehat{57} \cdot (-\widehat{4}) = \widehat{1} \Rightarrow$$

$$\Rightarrow \widehat{x} = (-\widehat{7}) = \widehat{93} \pmod{100}$$

$$\Rightarrow \widehat{x} = \widehat{93} \Rightarrow$$

curs ④ Care sunt ultimele 2 cifre ale nr. 37^{79} ?

$$\begin{aligned} U(\mathbb{Z}_{100}) & \text{ din teorema lui Euler} \\ (37, 100) = 1 \Rightarrow 37^{\varphi(100)} &= 1 \text{ în } U(\mathbb{Z}_{100}). \Rightarrow 37^{100} = 1 \\ \varphi(100) &= 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40 \\ 37^{79} &= \overbrace{37^{40}}^{=1} \cdot \overbrace{37^{39}}^{=37^{39}} = 37^{39} \end{aligned}$$

$\overbrace{37^{40}}^{=1} = \overbrace{37^{39}}^{=37} \cdot \overbrace{37}^{=1} \Rightarrow 37^{39}$ este înmulțirea în grupul $U(\mathbb{Z}_{100})$.

Calculăm înmulțirea lui 37

- 1: $100 = 37 \cdot \overbrace{2} + 26$
- 2: $37 = 26 \cdot \overbrace{1} + 11$
- 3: $26 = 11 \cdot \overbrace{2} + 4$
- 4: $11 = 4 \cdot \overbrace{2} + 3$
- 5: $4 = 3 \cdot \overbrace{1} + 1$
- 6: $3 = 1 \cdot 3$

$$\begin{aligned} \frac{A}{B} &= 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1}}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3}}} = \\ &= 2 + \frac{1}{1 + \frac{1}{\frac{7}{3}}} = 2 + \frac{1}{\frac{10}{7}} = 2 + \frac{7}{10} = \end{aligned}$$

$$\frac{100}{37} - \frac{27}{10} = \frac{(-1)^6}{37 \cdot 10} = \frac{1}{37 \cdot 10} = \frac{27}{10}$$

$$100 \cdot 10 - 37 \cdot 27 = 1 \quad (\text{A})$$

diagramă

$$\begin{aligned} -37 \cdot 27 &\equiv 1 \pmod{100} \\ 37 \cdot (-27) &\equiv 1 \pmod{100} \\ x = (37)^{-1} &= (-27) = 73 \pmod{100} \\ x &= 73 = \overline{73} \\ \text{ultimele cifre sunt } &\overline{73}. \end{aligned}$$

curs ⑤ Care sunt ultimele 2 cifre ale nr. 194^{194} ?

$$\widehat{194}^{194} = \widehat{94}^{194} = (-6)^{194} = -6 \quad \text{în } U(\mathbb{Z}_{100})$$

$$\widehat{194} = \widehat{94} \pmod{100} = (-6) \pmod{100}$$

$$\widehat{6}^1 = 6$$

$$\widehat{6}^2 = 36$$

$$\widehat{6}^3 = -16$$

$$\widehat{6}^4 = -96$$

$$\widehat{6}^5 = ... 76$$

$$\widehat{6}^6 = ... 56$$

$$\widehat{6}^7 = ... 36$$

Ultimele 2 cifre ale lui 6^n se repetă din 5 în 5 (nu exceptiv în 6^1) \Rightarrow

$$\widehat{6}^{194} = \underbrace{\widehat{6}^{195}}_{\text{diagramă}} \cdot \widehat{6}^2 = \widehat{6}^2 = \widehat{36} \Rightarrow$$

$$\widehat{6}^{194} = -\widehat{36} = \widehat{64} \pmod{100}$$

$$\boxed{x = 64} \quad \text{ultimele 2 cifre} = \widehat{64}$$

Soluție: Notăm $x = \overline{19^{\frac{1}{2}} 19^{\frac{1}{2}}}$ și $19^{\frac{1}{2}} \equiv 2$

$$x = \overline{19^{\frac{1}{2}}} \text{ (fund pol)} \quad r=0 \quad U(\mathbb{Z}_{25}) \xrightarrow{100/4} \overline{U(\mathbb{Z}_{25})}$$

$$\begin{array}{c} 100 \\ \swarrow \\ 25 \end{array}$$

$$U(\mathbb{Z}_{25})$$

$$\overline{19^{\frac{1}{2}}} = \overline{19^{\frac{1}{2}}} = \overline{x} \pmod{25}$$

$$\begin{array}{c} 19^{\frac{1}{2}}/25 \\ \overline{170} \\ \overline{19} \end{array}$$

$$|U(\mathbb{Z}_{25})| = 20$$

$$\varphi(25) = 25\left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20 \Rightarrow \text{T. Euler } \overline{19} \equiv 1$$

$$\overline{x} \cdot \overline{19}^3 = \overline{19}^{200} = (\overline{19}^{20})^{100} = \overline{1} \Rightarrow \overline{x} \cdot \overline{19}^3 \equiv 1 \pmod{U(\mathbb{Z}_{25})}$$

$$\overline{19^{\frac{1}{2}}}$$

$$\begin{array}{c} 361 \\ \swarrow \\ 25 \end{array} \quad \begin{array}{c} 25 \\ \swarrow \\ 111 \end{array} \quad \begin{array}{c} 111 \\ \swarrow \\ 100 \end{array} \quad \begin{array}{c} 66 \\ \swarrow \\ 116 \end{array} \quad \begin{array}{c} 25 \\ \swarrow \\ 2 \end{array}$$

$$\begin{aligned} \overline{361} &= \overline{19}^2 = 36 \pmod{25} = 11 \\ \overline{19}^3 &= \overline{19}^2 \cdot \overline{19} = (-6) \cdot 11 = (-66) = \\ &= (-16) = \overline{9} \pmod{25} \end{aligned}$$

$$\Rightarrow \overline{x} \cdot \overline{9} = \overline{1} \mid \overline{1} \cdot \overline{3} \pmod{U(\mathbb{Z}_{25})} \quad \overline{1} : \overline{2} \Rightarrow \overline{x} = \overline{15} \Rightarrow$$

$$\overline{27} \cdot \overline{x} = \overline{3} \Rightarrow$$

$$\begin{aligned} \overline{2x} &= \overline{3} = \overline{28} \quad \overline{1} : \overline{4} \Rightarrow \overline{x} = \overline{15} \\ &\text{I condiție } x \in \{39, 67, 89, \dots\} \\ &\text{II condiție } x \in \{4, 8, 12, 16, 20, 24, 28, 32, 36, 40, \\ &\quad 44, 64, \dots\} \end{aligned}$$

$$\begin{cases} x = 25k_1 + 14 \\ x = 25k_2 \end{cases}$$

$$\text{deoarece } 100k_2 + 64 = x \Rightarrow \boxed{x = 67} \Rightarrow \text{ultima cifră} = \underline{6}.$$

Care este restul împărțirii lui $2^{97} + 3^{98} + 5^{99}$ la 101?

Test!

$$(2, 101) = 1$$

$$(3, 101) = 1$$

$$(5, 101) = 1$$

$$\varphi(101) = 101 \cdot \left(1 - \frac{1}{101}\right) = 101 \cdot \frac{100}{101} = 100$$

$$\overline{2}^{97} + \overline{3}^{98} + \overline{5}^{99} \equiv \overline{2}^{100} \cdot (\overline{2}^{-1})^3 + \overline{3}^{100} \cdot (\overline{3}^{-1})^2 + \overline{5}^{100} \cdot (\overline{5}^{-1}) =$$

$$= (\overline{2}^{-1})^3 + (\overline{3}^{-1})^2 + (\overline{5}^{-1})^1 \pmod{U(\mathbb{Z}_{101})}$$

Rezolvare se calculează $\overline{2}^{-1}, \overline{3}^{-1}, \overline{5}^{-1}$ în $U(\mathbb{Z}_{101})$

$$\overline{2} \cdot \overline{51} = \overline{102} \equiv \overline{1} \pmod{101} \Rightarrow \overline{2}^{-1} = \overline{51}$$

$$\overline{3} \cdot \overline{34} = \overline{102} \equiv \overline{1} \pmod{101} \Rightarrow \overline{3}^{-1} = \overline{34}$$

$$\overline{5} \cdot \overline{20} = \overline{100} \equiv \overline{-1} \pmod{101} \Rightarrow (\overline{5} \cdot \overline{20})^2 = \overline{1} \Rightarrow$$

$$\Rightarrow \widehat{5}^2 \cdot \widehat{20}^2 = \widehat{1} \Rightarrow \widehat{5}(\widehat{5} \cdot \widehat{20}^2)^{\frac{6}{6}} = \widehat{1} \Rightarrow \widehat{5}^{-1} = x = \widehat{5} \cdot \widehat{20}^2 = \widehat{5} \cdot \widehat{500} \\ = \widehat{2000} = \widehat{81} \pmod{101}$$

$$\begin{array}{r|l} 2000 & 101 \\ \hline 101 & 19 \\ \hline 2990 & \\ 909 & \\ \hline 281 & \end{array}$$

$$\Rightarrow \widehat{2}^{97} + \widehat{3}^{98} + \widehat{5}^{99} = (\widehat{51})^3 + (\widehat{35})^2 + \widehat{81} = \widehat{132651} + \widehat{1156} + \widehat{81} = \widehat{38} + \widehat{45} + \widehat{81} \\ = \widehat{164} = \widehat{63} \Rightarrow$$

$$\begin{array}{r|l} 132651 & 101 \\ \hline 101 & 1313 \\ \hline 2316 & \\ 303 & \\ \hline 2135 & \\ 101 & \\ \hline 2341 & \\ 303 & \\ \hline 238 & \end{array}$$

$$\begin{array}{r|l} 1156 & 101 \\ \hline 101 & 11 \\ \hline 146 & \\ 101 & \\ \hline 45 & \end{array}$$

$$\begin{array}{r|l} 164 & 101 \\ \hline 101 & 1 \\ \hline 63 & \end{array}$$

Rest of Impfaktoren = 63

⑥ Suche minimale $x \in \mathbb{N}_{1,2,\dots,2020}$ a.s. $97 \cdot x \equiv 1 \pmod{2021}$
Da es 1 Euclidsche Teilung $97 \mid \text{dm}(U(\mathbb{Z}_{2021}))$ ist \Rightarrow

$$\widehat{97} \cdot \widehat{x} = \widehat{1} \text{ in } U(\mathbb{Z}_{2021})$$

$(97, 2021) = 1 \Rightarrow 97 \text{ e. invertierbar} \Rightarrow \text{Algorithmus des Euklid}$

$$\begin{aligned} 1: \quad 2021 &= 97 \cdot \boxed{21} + 81 & A &= 20 + \frac{1}{\frac{81}{97} + \frac{1}{5}} = 20 + \frac{1}{\frac{6}{5}} = 20 + \frac{5}{6} = \\ 2: \quad 97 &= 81 \cdot \boxed{1} + 16 & B &= \frac{125}{6} \\ 3: \quad 81 &= 16 \cdot \boxed{5} + 1 & & \\ 4: \quad 16 &= 1 \cdot \boxed{16} & \frac{2021}{97} - \frac{125}{6} &= \frac{(-1)^5}{97 \cdot 6} = \frac{1}{97 \cdot 6} \end{aligned}$$

$$2021 \cdot 6 - 125 \cdot 97 = 1$$

$$12126 - 12125 = 1 \quad (\text{A})$$

$$\underbrace{2021 \cdot 6 - 125 \cdot 97 = 1}_{\text{d.h.}} \Rightarrow (-\widehat{125})(\widehat{97}) = \widehat{1} \Rightarrow (\widehat{97})^{-1} = x = (-\widehat{125}) \pmod{2021}$$

$$(-\widehat{125}) = \widehat{2021 - 125} = \widehat{1896} \pmod{2021}$$

$$\text{Vervf.cke: } \widehat{97} \cdot \widehat{1896} = \widehat{183 \cdot 912} = \widehat{1} \pmod{2021} \vee$$

$$\begin{array}{r|l} 183 \cdot 912 & 2021 \\ \hline 18189 & 91 \\ \hline 22022 & \\ 2021 & \\ \hline 18 & \end{array}$$

(7) Către restul împărțirii la $n = 2^{39} + 3^{39}$ la 51?

$$\begin{cases} (2, 51) = 1 \\ (3, 51) = 1 \\ \varphi(51) = 51 \left(1 - \frac{1}{3}\right) = 51 \cdot \frac{2}{3} = 40 \end{cases} \quad \Rightarrow \hat{2}^{40} = \hat{3}^{40} = 1 \quad \text{în } U(\mathbb{Z}_{51})$$

$$\hat{2}^{39} + \hat{3}^{39} = \hat{2} \cdot \hat{2}^{-1} + \hat{3} \cdot \hat{3}^{-1} = \hat{2} \cdot \hat{2}^{-1} + \hat{1} \cdot \hat{3}^{-1} = \hat{2}^{-1} + \hat{3}^{-1}$$

Trbuie să calculăm $\hat{2}^{-1}$ și $\hat{3}^{-1}$ în $U(\mathbb{Z}_{51})$

$$\begin{aligned} 2 \cdot 20 &\equiv \hat{1} \pmod{51} \Rightarrow 2^2 \cdot 20^2 \equiv 1 \Rightarrow 2(2 \cdot 20^2) \equiv 1 \Rightarrow \\ &\Rightarrow \hat{2}^{-1} = x = 2 \cdot 20 = 2 \cdot 500 = 800 \equiv 21 \pmod{51} \end{aligned}$$

$$\begin{aligned} 3 \cdot \hat{14} &\equiv \hat{2} \equiv 1 \pmod{51} \Rightarrow \hat{3}^{-1} = \hat{14} \\ \Rightarrow \hat{2}^{39} + \hat{3}^{39} &\equiv \hat{2}^{-1} + \hat{3}^{-1} = \hat{21} + \hat{14} = \hat{35} \pmod{51} \\ \Rightarrow m &\equiv 35 \pmod{51} \end{aligned}$$

$$\begin{array}{c|cc} 800 & | & 51 \\ \hline 51 & | & 19 \\ 390 & | & \\ 369 & | & \\ \hline 21 & & \end{array}$$

Restul contine este 35.
Dacă: $\hat{m} = \hat{2}^{39} + \hat{3}^{39} \mid \cdot 6$ (Arithmetica)

$$\begin{aligned} \hat{6m} &\equiv \hat{2}^{39} \cdot \hat{2} \cdot \hat{3} + \hat{3}^{39} \cdot \hat{2} \cdot \hat{3} \Rightarrow \hat{6m} \equiv \hat{1} \cdot \hat{3} + \hat{1} \cdot \hat{2} = \hat{5} \\ \hat{6m} &\equiv \hat{2}^{40} \cdot \hat{3} + \hat{3}^{40} \cdot \hat{2} \Rightarrow \end{aligned}$$

$$\begin{cases} (2, 51) = 1 \\ (3, 51) = 1 \\ \varphi(51) = 51 \left(1 - \frac{1}{3}\right) = 51 \cdot \frac{2}{3} = 40 \end{cases} \quad \Rightarrow \hat{2}^{40} = \hat{3}^{40} = 1 \quad \text{în } U(\mathbb{Z}_{51})$$

$$\hat{6m} \equiv \hat{5} \pmod{51} \equiv -36 \Rightarrow \hat{6} \cdot \hat{m} \equiv -36 \mid :6 \Rightarrow \hat{m} \equiv -36 \equiv 6 \equiv (-6) \equiv 35 \pmod{51}$$

$$\Rightarrow m \equiv 35 \pmod{51} \Rightarrow \text{restul contine este 35.}$$

(8) Către restul împărțirii la $6^{99} + 3^{99} + 2^{99}$ la 101?

$$\begin{cases} \text{Observăm că } (6, 101) = 1 \\ (3, 101) = 1 \\ (2, 101) = 1 \end{cases} \quad \Rightarrow \hat{6}^{100} \equiv \hat{3}^{100} \equiv \hat{2}^{100} \equiv 1 \pmod{101} \quad \text{în } U(\mathbb{Z}_{101})$$

$$\varphi(101) = 101 \left(1 - \frac{1}{101}\right) = 101 \cdot \frac{100}{101} = 100$$

$$\hat{6}^{99} + \hat{3}^{99} + \hat{2}^{99} \equiv \hat{6}^{100} \cdot (\hat{6}^{-1}) + \hat{3}^{100} \cdot (\hat{3}^{-1}) + \hat{2}^{100} \cdot (\hat{2}^{-1}) = \hat{6}^{-1} + \hat{3}^{-1} + \hat{2}^{-1}$$

Trbuie să calculăm $\hat{6}^{-1}$, $\hat{3}^{-1}$ și $\hat{2}^{-1}$ în $U(\mathbb{Z}_{101})$

$$\begin{aligned} \hat{6} \cdot \hat{17} &= \hat{102} \equiv \hat{1} \pmod{101} \Rightarrow \hat{6}^{-1} = \hat{17} \\ \hat{3} \cdot \hat{35} &= \hat{102} \equiv \hat{1} \pmod{101} \Rightarrow \hat{3}^{-1} = \hat{35} \\ \hat{2} \cdot \hat{51} &= \hat{102} \equiv \hat{1} \pmod{101} \Rightarrow \hat{2}^{-1} = \hat{51} \end{aligned}$$

$$\Rightarrow \hat{6}^{99} + \hat{3}^{99} + \hat{2}^{99} = (\hat{6})^{-1} + (\hat{3})^{-1} + (\hat{2})^{-1} = \hat{17} + \hat{35} + \hat{51} = \hat{102} = \hat{1} \text{ in } U(\mathbb{Z}_{101})$$

$\equiv \hat{1} \pmod{101}$

\Rightarrow Restetl. kontat este 1.

son: Notam $m = 6^{99} + 3^{99} + 2^{99} \mid \cdot 6$ 6 = cmmmc ntre 6, 2, 3

$$\Rightarrow 6m = 6^{99} \cdot 6 + 3^{99} \cdot 6 + 2^{99} \cdot 6 = \underbrace{6^{100}}_{=1} + \underbrace{3^{100}}_{=1} \cdot 2 + \underbrace{2^{100}}_{=1} \cdot 3 =$$

$$= 1 + 2 + 3 = 6 \Rightarrow 6m \equiv 6 \pmod{101} \quad \left(\begin{matrix} 6 \mid 101 \\ 6 \equiv 1 \end{matrix} \right) \Rightarrow m \equiv 1 \pmod{101} \Rightarrow$$

\Rightarrow Restul kontat este 1.

R509 Scăză $x \in \{1, 2, \dots, 106\}$ a.s. $17 \cdot x \equiv 1 \pmod{107}$

$$17 \cdot x \equiv 1 \pmod{107}$$

$$17 \cdot x \equiv 1 \mid \cdot \cancel{17}$$

$$\cancel{102}x \equiv \cancel{6} \pmod{107}$$

$$119 \cdot x \equiv 1 \mid \cdot 9 \quad \text{son } 119 \equiv 12 \pmod{107} \quad 12x \equiv 1 \mid \cdot 9 \quad 108x \equiv 63$$

$$119 \cdot 9x \equiv 63$$

$$1071 \cdot x \equiv 63 \pmod{107} \Rightarrow 1 \cdot x \equiv 63 \Rightarrow \boxed{x = 63}$$

$$\begin{array}{c} y \pmod{107} \\ \boxed{x = 63} \pmod{107} \end{array}$$

$$\begin{array}{c} 1071 \mid 107 \\ 107 \mid 1 \\ \hline \cancel{107} \mid 1 \end{array} \quad \begin{array}{l} \text{say: } 107 = 17 \cdot \boxed{6} + 5 \\ 2: 17 = 5 \cdot \boxed{3} + 2 \\ 3: 5 = 2 \cdot \boxed{2} + 1 \\ 4: 2 = 1 \cdot \boxed{2} \end{array}$$

$$\begin{array}{l} \frac{A}{B} = 6 + \frac{1}{3 + \frac{1}{2}} = 6 + \frac{1}{\cancel{2}} = \\ = 6 + \frac{2}{7} = \frac{44}{7} \end{array}$$

$$\frac{107}{17} - \frac{44}{7} = \frac{(-1)^5}{17 \cdot 7} = \frac{1}{17 \cdot 7} \Rightarrow 107 \cdot 7 - 17 \cdot 44 = 1$$

$$749 - 448 = 1 \quad (\text{A}) \checkmark$$

$$\underbrace{107 \cdot 7 - 17 \cdot 44}_{\text{dispare}} \equiv 1 \Rightarrow -17 \cdot 44 \equiv 1 \pmod{107}$$

$$\Rightarrow \overline{17} \cdot (-\overline{44}) \equiv \overline{1} \pmod{107}$$

$$\Rightarrow \overline{x} = \overline{17}^{-1} = -\overline{44} = \overline{(107 - 44)} = \overline{63}$$

$$\Rightarrow \boxed{\overline{x} = \overline{63}}$$

$$\text{adăugare: } 17 \cdot 63 = 1071 = 1 \quad \checkmark$$

1) Cite este inversul lui $\bar{17}$ în corpul \mathbb{Z}_{19} ? (Seară \bar{x} astfel încât $\bar{x} \cdot \bar{17} = \bar{1}$)

In corpul \mathbb{Z}_{19} ,

$\bar{x} \cdot \bar{17} = \bar{1}$ în $\mathbb{U}(\mathbb{Z}_{19})$

Algoritmul lui Euclid

- 1: $19 = 17 \cdot \boxed{1} + 2$
- 2: $17 = 2 \cdot \boxed{8} + 1$
- 3: $2 = 1 \cdot 2$

$$\frac{A}{B} = \bar{1} + \frac{1}{\bar{8}} = \frac{\bar{9}}{\bar{8}}$$

reducere

$$\frac{19}{17} - \frac{9}{8} = \frac{(-1)^3}{17 \cdot 8}$$

$$19 \cdot 8 - 17 \cdot 9 = (-1)$$

$$152 - 153 = (-1) \quad (\text{A.}) \quad \checkmark$$

$$\underbrace{19 \cdot 8 - 17 \cdot 9}_{\text{(diferență)}} = (-1) \pmod{19} \Rightarrow -\bar{17} \cdot \bar{9} = \bar{1} \Rightarrow \bar{17} \cdot \bar{9} = \bar{1} \pmod{19}$$

(secundă)

$$\Rightarrow \cancel{\bar{x} = (\bar{17})^{-1} \equiv \bar{9} \pmod{19}}$$

verificare: $9 \cdot 17 = 153 = 1 \checkmark$

$\boxed{\bar{x} = \bar{9}}$

$$\begin{array}{r} 153 \\ 152 \\ \hline 1 \end{array}$$

$\overset{z=1}{\checkmark}$

2) Cite este restul împărțirii lui 2^{149} la 323 (cifrele sunt cifre românești folosind RST)

cum $n = 323$, $e = 149$ și alfabetul latin de 26 litere

$$n = 323 = 17 \cdot 19 \quad \begin{cases} p = 17 \\ q = 19 \end{cases}$$

$$e = 149$$

$$\varphi(n) = \varphi(323) = (p-1)(q-1) = (17-1)(19-1) = 16 \cdot 18 = 288 \quad \Rightarrow$$

$$\Rightarrow (e, \varphi(323)) = 1$$

$$(149, 288) = 1$$

$$\text{Alfabetul 26 litere} \Rightarrow 26^k < n \leq 26^{k+1} \Leftrightarrow 26^k < 323 \leq 26^{k+1}$$

$$k=0 \Rightarrow 0 < 323 \leq 26^2 = 676$$

$$N = 2 \cdot 26^1 = 2 \quad (\text{trebuie } N \text{ în baza 26}). \quad N^e \equiv 2 \pmod{n} \Leftrightarrow$$

$$\text{Calculăm } 2^{149} \equiv 2 \pmod{323} \text{ din ceea ce în grupă cu grupă cu putință} \\ \text{potrivit lui 2:}$$

$$2^2 \equiv 4 \equiv 4$$

$$2^4 \equiv 4^2 \equiv 16$$

$$2^8 \equiv (16)^2 \equiv 256$$

$$2^{16} \equiv (256)^2 \equiv 290$$

$$2^{32} \equiv (2^{16})^2 \equiv (290)^2 \equiv 120$$

$$2^{64} \overset{323}{\equiv} (120)^2 \overset{323}{\equiv} 188$$

$$2^{128} \overset{323}{\equiv} (188)^2 \equiv 134$$

$$149 = 2^7 + 2^5 + 2^2 + 1 \stackrel{-8}{=} 128 + 16 + 4 + 1$$

$$2^{149} = 2^{128} \cdot 2^{16} \cdot 2^5 \cdot 2^1 \stackrel{32^3}{\equiv} 137 \cdot 290 \cdot 16 \cdot 2 \stackrel{323}{\equiv} 32 \Rightarrow \boxed{Q=32}$$

$Q = 32 \geq 26^\circ \Rightarrow Q \text{ nu } \varphi \text{ de faza XY}$

$$Q = (\overline{xy})_{26} = x \cdot 26^1 + y \cdot 26^0 = 32 = 26 + 6 \Rightarrow \begin{cases} x=1 \rightarrow B \\ y=6 \rightarrow 6 \end{cases} \Rightarrow$$

$$\Rightarrow Q = \overline{B6}, \text{ dec } \boxed{C \xrightarrow{\text{RSA}} BG}$$

③ Să se calculeze $x \in \{9, 1, \dots, 898\}^y$ astfel încât $\begin{cases} x = 31a + 11 \\ x = 29b + 20 \end{cases}, a, b \in \mathbb{N}$.

$$\begin{cases} x = 31a + 11 \\ x = 29b + 20 \end{cases} \Rightarrow 31a + 11 = 29b + 20 \pmod{29}$$

$$\Rightarrow \widehat{31}\widehat{a} + \widehat{11} = \widehat{20} \Rightarrow \boxed{U(\mathbb{Z}_{29})}$$

$$\widehat{31}\widehat{a} = \widehat{20 - 11} = \widehat{9}$$

$$\widehat{31} \cdot \widehat{a} = \widehat{9} \pmod{29} \Rightarrow \widehat{2}\widehat{a} = \widehat{9} = \widehat{38} \Rightarrow \pmod{29}$$

$$\Rightarrow \widehat{a} = \widehat{38}; \widehat{2} = \widehat{9}$$

$$\boxed{\widehat{a} = \widehat{9}} \pmod{29}$$

$$a = 29c + 19$$

$$x = 31a + 11 = 31(29c + 19) + 11 = 899c + 31 \cdot 19 + 11 = 899c + 589 + 11$$

$$\Rightarrow x = 589 + 11 = 600$$

$$\boxed{x = 600}$$

Numele este 600.

$$\text{Verificare: } \begin{cases} 600 = 31 \cdot 19 + 11 = 589 + 11 \\ 600 = 29 \cdot 20 + 20 = 580 + 20 \end{cases} \checkmark$$

④ Să se calculeze rezultatul $2^{147} + 3^{147} + 6^{147}$ la 149.

~~Evident~~ Observație: $(2, 149) = 1$ \Rightarrow Dacă este 7, că nu este

$$\begin{cases} (3, 149) = 1 \\ (6, 149) = 1 \end{cases} \Rightarrow 6^{148} \stackrel{3^{148}}{=} 3^{148} \stackrel{2^{148}}{=} 2^{148} \equiv 1 \pmod{149}$$

În $U(\mathbb{Z}_{149})$

$$\phi(149) = 149 \left(1 - \frac{1}{149}\right) = 148$$

$$2^{147} + 3^{147} + 6^{147} \stackrel{2^{148} \cdot 2^{-1}}{=} 2^{148} + 3^{148} \cdot 3^{-1} + 6^{148} \cdot 6^{-1} =$$

$$= (2^{-1} + 3^{-1} + 6^{-1})^{-1} = 1$$

Pentru să calculăm $2^{-1}, 3^{-1}, 6^{-1}$ în $U(\mathbb{Z}_{149})$

$$2 \cdot \widehat{95} = \widehat{150} \equiv 1 \pmod{149}$$

$$3 \cdot \widehat{50} = \widehat{150} \equiv 1 \pmod{149}$$

$$6 \cdot \widehat{25} = \widehat{150} \equiv 1 \pmod{149}$$

$$\Rightarrow \widehat{2^{147}} + \widehat{3^{147}} + \widehat{6^{147}} = \widehat{2^{-1}} + \widehat{3^{-1}} + \widehat{6^{-1}} \equiv \widehat{95} + \widehat{50} + \widehat{25} = \widehat{150} = \equiv 1 \pmod{149} \Rightarrow \text{Restul contat este } 1$$

Dacă notăm $m = \overbrace{2^{147} + 3^{147} + 6^{147}}^{\text{6 este multimea tuturor } 6, 27, 3} \cdot 6$

$$\Rightarrow 6m = 2^{147} \cdot 2 \cdot 3 + 3^{147} \cdot 2 \cdot 3 + 6^{147} \cdot 6$$

$$\Rightarrow 6m = \underbrace{2^{148}}_{\equiv 1} \cdot 3 + \underbrace{3^{148}}_{\equiv 1} \cdot 2 + \underbrace{6^{148}}_{\equiv 1} = 3 + 2 + 1 = 6$$

$$6m \equiv 6 \pmod{149} \quad \left(\begin{matrix} m \equiv 1 \pmod{149} \\ (6, 149) = 1 \end{matrix} \right) \Rightarrow m \equiv 1 \pmod{149} \Rightarrow \text{Restul contat este } 1$$

Structuri algebrice

Def. $P \subset M$ se numește **parte stabilă** a lui M în raport cu legea „ \circ ” dacă $\forall x, y \in P \Rightarrow x \circ y \in P$

Mulțimea claselor de resturi modulo n

$$Z_n = \left\{ \hat{0}, \hat{1}, \hat{2}, \dots, \hat{n-1} \right\}$$

Operații pe Z_n . Exemplu:

În Z_6 avem $\hat{2} + \hat{5} = \hat{1}$, $\hat{2} \cdot \hat{5} = \hat{4}$

Def. Legea de compozиie „ \circ ” definită pe M se numește **comutativă** dacă $x \circ y = y \circ x$, $\forall x, y \in M$

Def. Legea de compozиie „ \circ ” definită pe M se numește **asociativă** dacă $(x \circ y) \circ z = x \circ (y \circ z)$, $\forall x, y, z \in M$

Def. Legea de compozиie „ \circ ” definită pe M admite **element neutru** dacă există $e \in M$, astfel încăt $x \circ e = e \circ x = x$, $\forall x \in M$

Def. Fie „ \circ ” o lege de compozиie pe M , care admite elementul neutru e . Elementul $x \in M$ se numește **simetrizabil** în raport cu legea „ \circ ” dacă există $x' \in M$, astfel încăt $x \circ x' = x' \circ x = e$

Def. Perechea (M, \circ) se numește **monoid** dacă verifică următoarele axiome:

(M_1) : axioma asociativității;

(M_2) : axioma elementului neutru.

Dacă în plus legea „ \circ ” este comutativă, monoidul se numește **monoid comutativ** sau **abelian**

Def. Perechea (G, \circ) se numește **grup** dacă verifică următoarele axiome:

(G_1) : axioma asociativității;

(G_2) : axioma elementului neutru;

(G_3) : axioma elementelor simetrizabile:

$$\forall x \in G, \exists x' \in G$$

Dacă în plus „ \circ ” este comutativă, grupul se numește **grup comutativ** sau **abelian**

Notația multiplicativă: $x \circ y = xy$

$$\underbrace{x \circ \dots \circ x}_n = x^n$$

Def. Fie (G_1, \circ) și $(G_2, *)$ două grupuri.

Funcția $f : G_1 \rightarrow G_2$ se numește **morfism** dacă $f(x \circ y) = f(x) * f(y)$, $\forall x, y \in G_1$

Funcția $f : G_1 \rightarrow G_2$ se numește **izomorfism** dacă f este morfism și este funcție bijectivă.

Def. $H \subset G$ se numește **subgrup** al grupului (G, \circ) dacă (H, \circ) este grup

Th. Fie (G, \cdot) un grup și $H \subset G$. H este subgrup al lui G dacă și numai dacă $\forall x, y \in H \Rightarrow xy^{-1} \in H$

Subgrupul generat de un element

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

Pro. **Ordinul unui element** a , notat $ord(a)$, este cel mai mic număr natural nenul pentru care $a^n = e$.

Def. Tripletul $(A, \circ, *)$ se numește **inel** dacă sunt verificate axiomele:

(A) : perechea (A, \circ) este grup comutativ;

(A) : perechea $(A, *)$ este monoid

(A) : axioma distributivității:

$$x * (y \circ z) = (x * y) \circ (x * z), \forall x, y, z \in A$$

Dacă în plus legea „ $*$ ” este comutativă inelul se numește **inel comutativ**.

Def. Un inel nenul în care orice element nenul este inversabil se numește **corp**

Def. Fie $(A, \circ, *)$ și (B, \perp, T) două inele

O funcție $f : A \rightarrow B$ se numește **morfism de inele**, dacă:

$$f(x \circ y) = f(x) \perp f(y), \forall x, y \in A$$

$$f(x * y) = f(x) T f(y), \forall x, y \in A$$

$$f(1_A) = 1_B$$

1) Fie $x \circ y = xy - 10x - 10y + 110$

a) Aratati ca $x \circ y = (x-10)(y-10) + 10$

b) Calculati $(e+1) \circ (e-1)$, unde e este elementul neutru al "◦"

c) rezolvați ecuația $x \circ x \circ x = 20$

$$a) (x-10)(y-10) + 10 =$$

$$xy - 10x - 10y + 100 + 10 = x \circ y$$

$$b) xe - 10x - 10e + 110 = x, \forall x$$

$$x(e-11) - 10e + 110 = 0, \forall x.$$

$$\begin{cases} e-11=0 \\ -10e+110=0 \end{cases} \Rightarrow e=11 \Rightarrow (e+1) \circ (e-1) =$$

$$12 \circ 10 = 120 - 120 - 100 + 110 = 10$$

c) Avem succesiv $x \circ x \circ x = 20 \Leftrightarrow$

$$[(x-10)(x-10) + 10] \circ x = 20 \Leftrightarrow$$

$$[(x-10)^2 + 10 - 10](x-10) + 10 = 20 \Leftrightarrow$$

$$(x-10)^3 + 10 = 20 \Leftrightarrow (x-10)^3 = 10 \Leftrightarrow$$

$$x-10 = \sqrt[3]{10} \Leftrightarrow x = \sqrt[3]{10} + 10$$

2) Fie $x * y = x + y + xy$

a) Arătați că „*” este asociativă

b) Arătați că $f(x) = x + 1$ verifică relația

$$f(x * y) = f(x) \cdot f(y)$$

$$c) Calculați $E = 1 * \frac{1}{2} * \frac{1}{3} * \dots * \frac{1}{2010}$$$

$$a) (x * y) * z = (x + y + xy) * z =$$

$$(x + y + xy) + z + (x + y + xy)z =$$

$$x + y + xy + z + xz + yz + xyz =$$

$$x + y + z + xy + xz + yz + xyz \quad (1)$$

$$x * (y * z) = x * (y + z + yz) =$$

$$x + y + z + xy + xz + yz + xyz \quad (2)$$

Din (1) și (2) rezultă că „*” este asociativă

$$b) f(x * y) = f(x + y + xy) = x + y + xy + 1$$

$$f(x) \cdot f(y) = (x+1)(y+1) = xy + x + y + 1$$

c) Folosim rezultatul de la punctual b)

$$f(E) = f(1)f\left(\frac{1}{2}\right)f\left(\frac{1}{3}\right) \dots f\left(\frac{1}{2010}\right) =$$

$$2 \cdot \frac{3}{2} \cdot \frac{4}{3} \cdot \dots \cdot \frac{2011}{2010} = 2011 \Rightarrow E + 1 = 2011 \Rightarrow$$

$$E = 2010$$

3) Fie clasele de resturi Z_7 și Z_6

a) Rezolvați în corpul $(Z_7, +, \cdot)$ ecuația

$$\hat{3}x^2 + \hat{4} = \hat{0}$$

b) Să se determine ordinul elementului $\hat{3}$ în grupul (Z_7^*, \cdot)

c) Să se arate că nu există niciun morfism de grupuri $f : (Z_6, +) \rightarrow (Z_7^*, \cdot)$

a) Verificăm pentru fiecare din cele 7

elemente din Z_7 și obținem soluțiile $\hat{1}$ și $\hat{6}$

$$b) \hat{3}^1 = \hat{3}, \hat{3}^2 = \hat{2}, \hat{3}^3 = \hat{6}, \hat{3}^4 = \hat{4}, \hat{3}^5 = \hat{5},$$

$$\hat{3}^6 = \hat{1} \Rightarrow ord(\hat{3}) = 6$$

c) Dacă există un astfel de morfism, atunci

$$f(e_1) = e_2 \Rightarrow f(\hat{0}) = \hat{1}.$$

$$\text{Dar } f(\hat{0}) = f(\hat{3} + \hat{3}) = (f(\hat{3}))^2 \neq \hat{1}$$

$$4) \text{ Fie } G = \left\{ \begin{pmatrix} x & iy \\ iy & x \end{pmatrix} \mid x, y \in R, x^2 + y^2 \neq 0 \right\}$$

a) Să se arate că G este parte stabilă în raport cu înmulțirea matricelor

b) Să se arate că (G, \cdot) este grup abelian

$$a) \text{ Fie } A = \begin{pmatrix} x & iy \\ iy & x \end{pmatrix} \in G \Rightarrow x^2 + y^2 \neq 0 \Rightarrow$$

$$\det(A) \neq 0, B = \begin{pmatrix} m & in \\ in & m \end{pmatrix} \in G \Rightarrow \det(B) \neq 0$$

$$AB = \begin{pmatrix} xm - yn & i(nx + my) \\ i(nx + my) & xm - yn \end{pmatrix} \in G \text{ deoarece}$$

$$\det(AB) = \det(A)\det(B) \neq 0$$

b) Înmulțirea matricelor este asociativă în general, deci este asociativă și pe G .

Elementul neutru este $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$

deoarece se obține pentru $x = 1$ și $y = 0$

$$A = \begin{pmatrix} x & iy \\ iy & x \end{pmatrix} \in G \Rightarrow \det(A) \neq 0 \Rightarrow$$

A inversabilă.

$$A^{-1} = \begin{pmatrix} \frac{x}{x^2 + y^2} & \frac{-iy}{x^2 + y^2} \\ \frac{-iy}{x^2 + y^2} & \frac{x}{x^2 + y^2} \end{pmatrix} \in G$$

LEMA CHINEZĂ A RESTURILOR

Probleme

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

$$a_1 = 1$$

$$m_1 = 3$$

$$a_2 = 3$$

$$m_2 = 5$$

$$a_3 = 5$$

$$m_3 = 7$$

Stim de ceva că trebuie să restăm;

$$M = m_1 m_2 m_3 = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = \frac{105}{3} = 35 = \underline{\underline{M}}_{m_1}$$

$$M_2 = \frac{105}{5} = \underline{\underline{M}}_{m_2} = 21$$

$$M_3 = \frac{105}{7} = \underline{\underline{M}}_{m_3} = 15$$

$$M_1 y_1 \equiv 1 \pmod{m_1}$$

$$35 y_1 \equiv 1 \pmod{3}$$

$$\overset{1^4}{\cancel{y_1}} - y_1 \equiv 1 \pmod{3} \Rightarrow \underline{\underline{y_1 = 1}} \pmod{3}$$

$$M_2 y_2 \equiv 1 \pmod{m_2}$$

$$21 y_2 \equiv 1 \pmod{5}$$

$$\overset{1^4}{\cancel{y_2}} = 1 \pmod{5}$$

$$M_3 y_3 \equiv 1 \pmod{m_3}$$

$$15 y_3 \equiv 1 \pmod{7}$$

$$\overset{1^4}{\cancel{y_3}} = 1 \pmod{7}$$

$$\Rightarrow e_1 = M_1 y_1 = 35 \cdot (-1) = -35$$

$$e_2 = M_2 y_2 = 21 \cdot 1 = 21$$

$$e_3 = M_3 y_3 = 15 \cdot 1 = 15$$

$$\bar{x} = a_1 e_1 + a_2 e_2 + a_3 e_3 = (-35) + 3 \cdot 21 + 5 \cdot 15 =$$

$$= -35 + 63 + 75 = 103 \pmod{105}$$

$$\Rightarrow \boxed{\bar{x} = 103} \quad \text{Răspunsul este } \underline{\underline{103}}$$

$$\text{Verificare: } 103 \equiv 1 \pmod{3} \quad \checkmark$$

$$103 \equiv 3 \pmod{5} \quad \checkmark$$

$$103 \equiv 5 \pmod{7} \quad \checkmark$$

$$\begin{array}{r} 103 \\ \times 10 \\ \hline 103 \\ \hline \end{array} \quad \begin{array}{r} 103 \\ \times 5 \\ \hline 515 \\ \hline \end{array} \quad \begin{array}{r} 103 \\ \times 9 \\ \hline 927 \\ \hline \end{array} \quad \begin{array}{r} 103 \\ \times 34 \\ \hline 3427 \\ \hline \end{array} \quad \begin{array}{r} 103 \\ \times 7 \\ \hline 721 \\ \hline \end{array} \quad \begin{array}{r} 103 \\ \times 14 \\ \hline 1442 \\ \hline \end{array}$$

Frage:

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

$$x = 3u + 1 = 5v + 3 \pmod{3}$$

$$5v = -2 \pmod{3}$$

$$2v = -2 \Rightarrow v \equiv -1 \pmod{3} \equiv 2 \pmod{3}$$

$$\Rightarrow x = 5v + 3 = 5 \cdot 2 + 3 = 13 \pmod{15}$$

$$\Rightarrow \begin{cases} x \equiv 13 \pmod{15} \\ x \equiv 5 \pmod{7} \end{cases} \Rightarrow \text{Sternen } x = 13 + 15t = 5 + 7a \pmod{7}$$

$$\Rightarrow 15t \equiv (-8) \pmod{7}$$

$$\uparrow \quad t \equiv (-8) \not\equiv (-1) \not\equiv 6$$

$$t \equiv 6 \pmod{7} \Rightarrow t = 6 + 7a$$

$$\text{Sternen } t = 7a + 6 \quad ①$$

$$\Rightarrow x = 13 + 15t \quad ②$$

Einsetzen ① in ② \Rightarrow

$$x = 13 + 15(7a + 6) = 13 + 105a + 15 \cdot 6 = 105a + \underbrace{13 + 15 \cdot 6}_{13 + 90} = 103$$

$$\downarrow \quad x = 13 + 15 \cdot 6 = 90 + 13 = 103 \Rightarrow \boxed{x = 103} \vee$$

verifizieren: $103 \equiv 1 \pmod{3} \vee$

$$103 \equiv 3 \pmod{5} \vee$$

$$103 \equiv 5 \pmod{7}$$

$$\begin{array}{r} 103 | 3 \\ 9 \quad | 34 \\ \hline 13 \end{array} \quad \begin{array}{r} 103 | 5 \\ 10 \quad | 2 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 103 | 7 \\ 103 \quad | 103 \\ \hline 7 \end{array} \quad \begin{array}{r} 103 | 28 \\ 28 \quad | 28 \\ \hline 0 \end{array}$$

Probleme

$$\begin{cases} 2x \equiv 3 \pmod{7} \\ 3x \equiv 5 \pmod{8} \\ 2x \equiv 5 \pmod{9} \end{cases} \quad | \cdot 4 \Rightarrow \begin{cases} 8x \equiv 12 \pmod{7} \\ 9x \equiv 20 \pmod{8} \\ 10x \equiv 20 \pmod{9} \end{cases} \quad \begin{matrix} 1 \pmod{7} \\ 1 \pmod{8} \\ 1 \pmod{9} \end{matrix}$$

$$\Leftrightarrow \begin{cases} x \equiv -2 \pmod{7} \\ x \equiv -1 \pmod{8} \\ x \equiv -2 \pmod{9} \end{cases}$$

$$\begin{array}{ll} a_1 = -2 & m_1 = 7 \\ a_2 = -1 & m_2 = 8 \\ a_3 = -2 & m_3 = 9 \end{array}$$

Grenzen chinesischen Restsatz:

$$M = m_1 m_2 m_3 = 7 \cdot 8 \cdot 9 = 504.$$

$$M_1 = \frac{504}{7} = \underline{\underline{72}} = \frac{M}{m_1}$$

$$M_2 = \frac{M}{m_2} = \frac{504}{8} = \underline{\underline{63}}$$

$$M_3 = \frac{504}{9} = \underline{\underline{56}} = \frac{M}{m_3}$$

$$M_1 y_1 \equiv 1 \pmod{m_1}$$

$$\Rightarrow 72 y_1 \equiv 1 \pmod{7} \quad | \cdot 4 \Rightarrow 288 y_1 \equiv 4 \pmod{7} \Rightarrow \boxed{y_1 = 5} \pmod{7}$$

$$1 \pmod{7}$$

$$M_2 y_2 \equiv 1 \pmod{m_2}$$

$$63 y_2 \equiv 1 \pmod{8}$$

$$\Rightarrow 5 \cdot y_2 \equiv 1 \pmod{8} \Rightarrow \underline{y_2 \equiv -1} \pmod{8}$$

$$M_3 y_3 \equiv 1 \pmod{m_3}$$

$$56 y_3 \equiv 1 \pmod{9} \quad | \cdot 5$$

$$280 y_3 \equiv 5 \pmod{9}$$

$$\Rightarrow \underline{\underline{y_3 \equiv 5}} \pmod{9}$$

$$\Rightarrow e_1 = M_1 y_1 = 72 \cdot 5 = 288$$

$$e_2 = M_2 y_2 = 63 \cdot (-1) = -63$$

$$e_3 = M_3 y_3 = 56 \cdot 5 = 280$$

$$\bar{x} = a_1 e_1 + a_2 e_2 + a_3 e_3 = (-2) \cdot 288 + (-1) \cdot (-63) + (-2) \cdot 280 =$$

$$= -576 + 63 - 560 = -1073 \pmod{504} = -65 \pmod{504}.$$

$$\begin{array}{r|rr} 1073 & 504 \\ 1008 & \hline 65 \end{array}$$

$$\Rightarrow x = 504 - 65 = 439$$

$$\boxed{x=439} \quad \checkmark$$

$$\underline{\text{verifiziere}}: 439 \equiv -2 \pmod{7} \quad \checkmark$$

$$439 \equiv -1 \pmod{8} \quad \checkmark$$

$$439 \equiv -2 \pmod{9} \quad \checkmark$$

$$\begin{array}{r|l} 439 & 7 \\ \hline 52 & 63 \\ \hline 21 & \\ \hline 21 & \\ \hline 0 & \end{array}$$

$$\text{Seriell: } \begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 7 \pmod{8} \\ x \equiv 7 \pmod{9} \end{cases}$$

$$x = 7a + 5 = 8n + 7 \pmod{7}$$

$$8n = -2 \pmod{7}$$

$$\stackrel{4}{\cancel{n}} \equiv -2 \pmod{7} \equiv 5 \pmod{7}.$$

$$\Rightarrow x = 8n + 7 = 8 \cdot 5 + 7 = 47 \pmod{56}$$

$$\begin{cases} x \equiv 47 \pmod{56} \\ x \equiv 7 \pmod{9} \end{cases} \Rightarrow \text{Seriell: } x = 56t + 47 = 9s + 7 \pmod{9}$$

$$\Rightarrow 56t = -40 \pmod{9}$$

$$28t = -20 \pmod{9}$$

$$14t = -10 \pmod{9}$$

$$\stackrel{5}{\cancel{14t}} \equiv -1 \pmod{9} \equiv 8$$

$$-4t = 8 \Rightarrow \boxed{t = -2} \pmod{9}$$

$$\Rightarrow t = 9a - 2$$

$$\Rightarrow x = 56t + 47$$

$$= 56 \cdot (-2) + 47 = 112 + 47 = 65 \pmod{504}$$

$$x = 47 + 56(9a - 2) = 47 + \underbrace{504a}_{\geq 65} - 112 = 504a + \underbrace{47 - 112}_{\geq 65} = 504a - 65 \pmod{504}$$

$$\Rightarrow x = -65 \pmod{504} = \boxed{439}$$

$$= \frac{-65}{504} \pmod{504}$$

$$\underline{\text{verifiziere}}: 439 \equiv 5 \pmod{7} \quad \checkmark$$

$$439 \equiv 7 \pmod{8} \quad \checkmark$$

$$439 \equiv 7 \pmod{9} \quad \checkmark$$

Structuri algebrice

1. Monoid

Fie $(M, *)$, $M \times M \rightarrow M$, $(x, y) \rightarrow x * y$, M -nevidă.

Axiomele monoidului:

M1. $(x * y) * z = x * (y * z) \quad \forall x, y, z \in M$ (asociativitatea);

M2. $\exists e \in M$ astfel încât $x * e = e * x = x, \forall x \in M$ (e element neutru);

dacă **M3.** $x * y = y * x, \forall x, y \in M$ monoidul este comutativ.

Ex: 1. $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) sunt monoizi comutativi;

2. $(F(E), o)$ monoid necomutativ ($F(E)$ este mulțimea funcțiilor $f: E \rightarrow E$, E – nevidă, o – compunerea funcțiilor).

2. Grup

Fie $(G, *)$, $G \times G \rightarrow G$, $(x, y) \rightarrow x * y$, G -nevidă.

Axiomele grupului:

G1. $(x * y) * z = x * (y * z), \forall x, y, z \in G$ (asociativitatea);

G2. $\exists e \in G$ astfel încât $x * e = e * x = x, \forall x \in G$ (e element neutru);

G3. $\forall x \in G \quad \exists x' \in G$ astfel încât $x' * x = x * x' = e$ (x' simetricul lui x);

dacă **G4.** $x * y = y * x, \forall x, y \in G$ grupul este comutativ (sau abelian).

Ex: 1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ – grupuri comutative;

2. (\mathbb{R}_n, \oplus) – grupul resturilor modulo n , comutativ;

3. $(M_n(\mathbb{Z}), +)$ – grupul matricilor pătrate de ordin n cu elemente din \mathbb{Z} ;

4. (K, o) – grupul lui Klein (al simetriilor față de sistemul de coordonate), comutativ;

5. (σ_n, o) – grupul simetric de grad n (al permutărilor de n elemente) nu este comutativ;

Definiția 2.1. Fie $(G, *)$ grup, $H \subset G$, H este subgrup dacă $\forall x, y \in H \Rightarrow x * y \in H$ și $\forall x \in H \Rightarrow x' \in H$ (x' este simetricul lui x în raport cu operația $*$);

Fie grupurile (G_1, \perp) , (G_2, Δ) :

Definiția 2.2. $f: G_1 \rightarrow G_2$ se numește **morfism de grupuri** dacă $f(x \perp y) = f(x) \Delta f(y)$, $\forall x, y \in G_1$.

Definiția 2.3. $f: G_1 \rightarrow G_2$ se numește **izomorfism de grupuri** dacă f este bijectivă și $f(x \perp y) = f(x) \Delta f(y)$, $\forall x, y \in G_1$.

Definiția 2.4. $f: G_1 \rightarrow G_2$ se numește **automorfism (endomorfism)** al grupului G_1 , dacă f este un izomorfism (morfism).

3. Inel

Fie $(A, +, \bullet)$, $A \times A \rightarrow A$, $(x, y) \rightarrow x + y$ și $A \times A \rightarrow A$, $(x, y) \rightarrow x \bullet y$, A nevidă;

Definiția 3.1. $(A, +, \bullet)$ este **inel** dacă:

G. $(A, +)$ este grup abelian;

M. (A, \bullet) este monoid și

D. \bullet este distributivă față de $+$:

$$x \bullet (y + z) = x \bullet y + x \bullet z$$

$$(y + z) \bullet x = y \bullet x + z \bullet x, \forall x, y, z \in A$$

dacă $\mathbf{C}.$ $x \bullet y = y \bullet x \quad \forall x, y \in A,$ inelul este comutativ.

Exemple de inele:

1. $(\mathbb{Z}, +, \cdot)$ – inelul numerelor întregi;
2. $(\mathbb{Z}[i], +, \cdot)$ – inelul întregilor lui Gauss, $\mathbb{Z}[i] = \{z = a + bi \mid a, b \in \mathbb{Z}\}$
3. $(\mathbb{R}_n, \oplus, \otimes)$ – inelul resturilor modulo $n;$
4. $(M_n(A), +, \cdot)$ – inelul matricelor pătratice (cu elemente din inelul $A);$
5. $(\mathbb{Z}_n, +, \cdot)$ – inelul claselor de resturi modulo $n.$

Fie inelele $(A, \perp, *)$ și $(A', \Delta, o):$

Definiția 3.1. $f: A \rightarrow A'$ se numește izomorfism de inele dacă f este bijectivă și $f(x \perp y) = f(x) \Delta f(y), f(x * y) = f(x)o f(y), \forall x, y \in A.$

Definiția 3.2. $(A, +, \bullet)$ este inel fără divizori ai lui zero dacă $x \neq 0, y \neq 0 \text{ implică } x \bullet y \neq 0.$

Definiția 3.3. Un inel comutativ cu cel puțin două elemente și fără divizori ai lui zero se numește domeniu de integritate.

Definiția 3.4. Dacă $(A, +, \cdot)$ este inel, atunci $(A[X], +, \cdot)$ este inelul comutativ al polinoamelor cu coeficienți în A .

$f \in A[X], f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ este forma algebraică a unui polinom de nedeterminată X cu coeficienți în $A:$

- dacă $a_n \neq 0, \text{ grad } f = n$ (a_n – coeficient dominant);
- dacă $a_0 = a_1 = \dots = a_n, f = 0$ (polinom nul), $\text{grad } 0 = -\infty.$

Proprietăți: 1. $\text{grad } (f+g) \leq \max \{\text{grad } f, \text{grad } g\};$

2. $\text{grad } f \cdot g \leq \text{grad } f + \text{grad } g.$

Teoremă. Dacă A este domeniu de integritate atunci $A[X]$ este domeniu de integritate și $\text{grad } f \cdot g = \text{grad } f + \text{grad } g, \forall f, g \in A[X].$

4. Corp

Fie $(K, +, \bullet), KxK \rightarrow K, (x, y) \rightarrow x+y$ și $KxK \rightarrow k, (x, y) \rightarrow x \bullet y, K – nevidă.$

Definiția 4.1. $(K, +, \bullet)$ este corp dacă $(K, +, \bullet)$ este inel, $0 \neq 1$ și $\forall x \in K, x \neq 0 \Rightarrow \exists x^{-1} \in K,$ astfel încât $x \bullet x^{-1} = x^{-1} \bullet x = 1.$

Dacă $x \bullet y = y \bullet x, \forall x, y \in K,$ corpul este comutativ.

Exemple de coruri:

1. $(\mathbb{Q}, +, \cdot)$ – corpul numerelor raționale;
2. $(\mathbb{R}, +, \cdot)$ – corpul numerelor reale;
3. $(\mathbb{C}, +, \cdot)$ – corpul numerelor complexe;
4. $(Q(\sqrt{d}), +, \cdot)$ – corpul numerelor pătratice ($d \in \mathbb{Z}, d – liber de pătrate$);
5. $(\mathbb{Z}_p, +, \cdot)$ – corpul claselor de resturi modulo p ($p \in \mathbb{N}^*, p > 1, p – număr prim$).

Definiția 4.2. Fie corurile $(K, \perp, *)$ și $(K', \Delta, o), f: K \rightarrow K'$ este izomorfism de coruri dacă f este bijectivă, $f(x \perp y) = f(x) \Delta f(y), f(x * y) = f(x) o f(y) \forall x, y \in K.$

Caz general

Fie pe \mathbf{R} operația $x \circ y = axy - abx - aby + b(ab+1)$, $\forall x, y \in \mathbf{R}$. Se cere:

1. Să se arate că, $\forall x, y \in \mathbf{R}$ $x \circ y = a(x-b)(y-b) + b$;
2. Să se arate că $f: \mathbf{R} \rightarrow \mathbf{R}$, $f(t) = a(t-b)$, este funcție bijectivă care verifică totodată $f(x \circ y) = f(x) \cdot f(y)$, $\forall x, y \in \mathbf{R}$;
3. În cazul alegерii $a > 0$ considerând $H = (b; +\infty)$, respectiv în cazul alegерii $a < 0$ considerând $H = (-\infty; b)$, să se arate că, $\forall x, y \in H$, are loc $x \circ y \in H$;
4. În cazul alegерii $a > 0$ considerând $H = (b; +\infty)$, respectiv în cazul alegерii $a < 0$ considerând $H = (-\infty; b)$, să se arate că $f: H \rightarrow \mathbf{R}_+^*$, $f(t) = a(t-b)$, este izomorfism de la $(H; \circ)$ la $(\mathbf{R}_+^*; \cdot)$;
5. Să se arate că, $\forall x, y \in \mathbf{R}$, are loc $x \circ y = y \circ x$;
6. Să se arate că $\exists x, y \in \mathbf{Q} \setminus \mathbf{Z}$ încât $x \circ y \in \mathbf{Z}$;
7. Să se arate că $\exists x, y \in \mathbf{R} \setminus \mathbf{Q}$ încât $x \circ y \in \mathbf{Z}$;
8. Să se arate că $\forall x, y, z \in \mathbf{R}$, are loc $(x \circ y) \circ z = x \circ (y \circ z)$;
9. Să se arate că $\exists e \in \mathbf{R}$ încât, $\forall x \in \mathbf{R}$, verifică $x \circ e = e \circ x = x$;
10. Să se arate că, $\forall x \in \mathbf{R} \setminus \{b\}$, $\exists x' \in \mathbf{R} \setminus \{b\}$ încât $x \circ x' = x' \circ x = \frac{1}{a} + b$;
11. În cazul alegерii $a > 0$, considerând $H = (b; +\infty)$, respectiv în cazul alegерii $a < 0$, considerând $H = (-\infty; b)$, să se determine ce fel de structură este (H, \circ) ;
12. Să se rezolve ecuația $x \circ \left(\frac{1}{a} + b\right) \circ x = a \cdot A \cdot B + C$, $x \in (0, +\infty)$, unde $A = "an" - b - c$, $B = "an" - b + c$, $C = ac^2 + b$, $\forall c \in \mathbf{Z}$;
13. Să se arate că $\exists \theta \in \mathbf{R}$ încât $\forall x \in \mathbf{R}$ verifică $x \circ \theta = \theta \circ x = \theta$;
14. Să se determine valoarea expresiei
 $E = (-"an") \circ (-"an"+1) \circ \dots \circ (-2) \circ (-1) \circ 0 \circ 1 \circ 2 \circ \dots \circ ("an"-1) \circ ("an")$;
15. Să se arate că, $\forall x, y, z \in \mathbf{R}$, $x \circ y \circ z = a^2(x-b)(y-b)(z-b) + b$;
16. Să se rezolve în \mathbf{R} ecuația $("an" x^2 - x + b) \circ (x^2 - "an" x + b) = b$;
17. Să se rezolve în \mathbf{R} ecuația $(b - |b| + d^x) \circ (\log_d x) \circ (b - 1 + C^{x_an}) = b$, $\forall d \in \mathbf{N}$, $d \geq 2$;
18. Să se arate că $\underbrace{A \circ A \circ \dots \circ A}_{de n ori} = a^{n-1} \cdot (A - b)^n + b$, $\forall n \in \mathbf{N}$, A fiind un număr real liber ales, spre exemplu $A = "an"$;
19. Să se determine cel mai mic număr $n \in \mathbf{N}^*$ cu proprietatea $(b+1) \circ (b+2) \circ (b+3) \circ \dots \circ n \geq "an"$;
20. Să se rezolve în \mathbf{R} ecuația $x \circ x \circ x \circ x \circ x = a^4 \cdot A^5 + b$, A fiind un număr real liber ales, spre exemplu $A = "an"$.

Rezolvare

1. Se verifică imediat, prin calcul direct:

$$x \circ y = a(x-b)(y-b) + b = a(xy - bx - by + b^2) + b = axy - abx - aby + b(ab+1)$$
2. Justificarea bijectivității funcției $f: \mathbf{R} \rightarrow \mathbf{R}$, $f(t) = a(t-b)$, este imediată, ca funcție de gradul întâi. Conform cu

Legi de compozitie Bacalaureat 2014-2016

$x \circ y = a(x-b)(y-b) + b \Rightarrow x \circ y - b = a(x-b)(y-b)$ | · a $\Rightarrow a(x \circ y - b) = a(x-b) \cdot a(y-b)$
este chiar cerința, respectiv $f(x \circ y) = f(x) \cdot f(y)$.

3. Fie $x \in H \Rightarrow (x-b) \geq 0$ și $y \in H \Rightarrow (y-b) \geq 0$ și atunci $(x-b)(y-b) \geq 0$, dar cum a este constantă nenulă și de semn prestabilit, apartenența $a(x-b)(y-b) + b = x \circ y \in H$ este justificată.
4. Variația funcției $f : \mathbf{R} \rightarrow \mathbf{R}$, $f(t) = a(t-b)$, studiată anterior, arată imediat că restricția $f : H \rightarrow \mathbf{R}^*$ este bijectivă. Tot din datele anterioare, este evident că H este parte stabilă a structurii $(\mathbf{R}; \circ)$ (item 3) și că are loc proprietatea de morfism +(item 2), izomorfismul fiind astfel demonstrat.
5. Comutativitatea este imediată
6. Luând $x \circ y = a(x-b)(y-b) + b$ și alegând $x-b = \frac{2}{3}$ și $y-b = \frac{3}{2}$, deoarece $b \in \mathbf{Z}$, evident $x, y \in \mathbf{Q} \setminus \mathbf{Z}$ și $x \circ y = a+b \in \mathbf{Z}$.
7. Pe aceeași idee, alegând $x-b = \sqrt{2}-1$ și $y-b = \sqrt{2}+1$, se va obține $x, y \in \mathbf{R} \setminus \mathbf{Q}$ și $x \circ y = a+b \in \mathbf{Z}$. Se observă că alegerea nu este unică, admitând chiar o infinitate de posibilități.
8. Asociativitatea se demonstrează prin calcul
9. Din $x \circ y = a(x-b)(y-b) + b$ și $x \circ e = x$ conduce la $a(x-b)(e-b) + b = x$ din care se obține $e = \frac{1}{a} + b$
10. Dubla egalitate $x \circ x' = x' \circ x = \frac{1}{a} + b$ se reduce de fapt la $x \circ x' = \frac{1}{a} + b$ care se exprimă în forma $a(x-b)(x'-b) + b = \frac{1}{a} + b$, obținând $x' = b + \frac{1}{a^2(x-b)}$ care este în mod evident din $\mathbf{R} \setminus \{b\}$, justificând afirmația din **item 10**.
11. Structura $(H; \circ)$ se dovedește grup comutativ, verificarea proprietăților fiind asigurată de concluzii anterioare.
12. Cum $e = \frac{1}{a} + b$, $x \circ \left(\frac{1}{a} + b \right) \circ x = a \cdot A \cdot B + C$ devine $x \circ x = a \cdot A \cdot B + C$, adică $a(x-b)^2 + b = a \cdot ("an"-b-c) \times ("an"-b+c) + ac^2 + b$. Observând diferența de pătrate, din $a(x-b)^2 = a \cdot [(an-b)^2 - c^2] + ac^2$ se obține $(x-b)^2 = (an-b)^2$ și în final $x = "an"$, în condiția alegерii evidente $2b - "an" < 0 < "an" - b$.
13. Din $x \circ y = a(x-b)(y-b) + b$ se observă $q = b$ cu proprietatea menționată, $x \circ \theta = \theta \circ x = \theta$.
14. Cum $\theta = b$ se regăsește printre „factorii” ce compun expresia E , răspunsul la este $E = \theta = b$.
15. Se obține prin calcul folosind $x \circ y = a(x-b)(y-b) + b$.
16. Ecuația $("an" x^2 - x + b) \circ (x^2 - "an" x + b) = b$ devine $("an" x^2 - x)(x^2 - "an" x) = 0$ și răspunsul va fi $x \in \left\{ 0; "an"; \frac{1}{"an"} \right\}$.
17. Ecuația devine $(d^x - |b|)(\log_d x - b) \left(C_{an}^x - 1 \right) = 0$, deci $x \in \left\{ \log_d |b|; d^b; 0; "an" \right\}$.
18. Izomorfismul conduce imediat la $x_1 \circ x_2 \circ \dots \circ x_n = a^{n-1} \cdot \prod_{k=1}^n (x_k - b) + b$ și astfel identitatea $\underbrace{A \circ A \circ \dots \circ A}_{de\ n\ ori} = a^{n-1} (A - b)^n + b$ este evidentă.

Legi de compozitie Bacalaureat 2014-2016

19. $(b+1) \circ (b+2) \circ (b+3) \circ \dots \circ n = a^{n-b-1} \cdot (n-b)! + b$ și astfel se determină imediat răspunsul.
 20. $x \circ x \circ x \circ x \circ x = a^4 \cdot (x-b)^5 + b$ și $a^4 \cdot (x-b)^5 + b = a^4 \cdot A^5 + b$ soluția $x=A+b$.

Exemplul (corespunzător alegerii $a=1$, $b=5$, $c=5$ și $d=2$)

Fie pe \mathbf{R} operația $x \circ y = xy - 5x - 5y + 30$, $\forall x, y \in \mathbf{R}$. Se cere:

- 1) Să se arate că, $\forall x, y \in \mathbf{R}$, $x \circ y = (x-5)(y-5) + 5$;
- 2) Să se arate că $f : \mathbf{R} \rightarrow \mathbf{R}$, $f(t) = t - 5$, este funcție bijectivă, care verifică totodată $f(x \circ y) = f(x) \cdot f(y)$, $\forall x, y \in \mathbf{R}$.
- 3) Considerând $H = (5; +\infty)$, să se arate că, $\forall x, y \in H$, are loc $x \circ y \in H$;
- 4) Considerând $H = (5; +\infty)$, să se arate că $f : H \rightarrow \mathbf{R}_+^*$, $f(t) = t - 5$, este izomorfism de la $(H; \circ)$ la $(\mathbf{R}_+^*; \cdot)$;
- 5) Să se arate că, $\forall x, y \in \mathbf{R}$, are loc $x \circ y = y \circ x$;
- 6) Să se arate că $\exists x, y \in \mathbf{Q} \setminus \mathbf{Z}$ încât $x \circ y \in \mathbf{Z}$;
- 7) Să se arate că $\exists x, y \in \mathbf{R} \setminus \mathbf{Q}$ încât $x \circ y \in \mathbf{Z}$;
- 8) Să se arate că, $\forall x, y, z \in \mathbf{R}$, are loc $(x \circ y) \circ z = x \circ (y \circ z)$;
- 9) Să se arate că $\exists e \in \mathbf{R}$ încât $\forall x \in \mathbf{R}$ verifică $x \circ e = e \circ x = x$;
- 10) Să se arate că, $\forall x \in \mathbf{R} \setminus \{5\}$, $\exists x' \in \mathbf{R} \setminus \{5\}$ încât $x \circ x' = x' \circ x = 6$;
- 11) Considerând $H = (5; +\infty)$, să se determine ce fel de structură este (H, \circ) ;
- 12) Să se rezolve ecuația $x \circ 6 \circ x = 1999 \cdot 2009 + 30$, $x \in (0, +\infty)$;
- 13) Să se arate că $\exists \theta \in \mathbf{R}$ încât $\forall x \in \mathbf{R}$ verifică $x \circ \theta = \theta \circ x = \theta$;
- 14) Să se determine valoarea expresiei
 $E = (-2009) \circ (-2008) \circ \dots \circ (-2) \circ (-1) \circ 0 \circ 1 \circ 2 \circ \dots \circ 2008 \circ 2009$;
- 15) Să se arate că, $\forall x, y, z \in \mathbf{R}$, $x \circ y \circ z = (x-5)(y-5)(z-5) + 5$;
- 16) Să se rezolve în \mathbf{R} ecuația $(2009x^2 - x + 5) \circ (x^2 - 2009x + 5) = 5$;
- 17) Să se rezolve în \mathbf{R} ecuația $(2^x) \circ (\log_2 x) \circ (4 + C_{2009}^x) = 5$;
- 18) Să se arate că $\underbrace{2009 \circ 2009 \circ \dots \circ 2009}_{\text{de 2009 ori}} = 2004^{2009} + 5$
- 19) Să se determine cel mai mic număr $n \in \mathbf{N}^*$, cu proprietatea $6 \circ 7 \circ 8 \circ \dots \circ n \geq 2009$;
- 20) Să se rezolve în \mathbf{R} ecuația $x \circ x \circ x \circ x \circ x = 2009^5 + 5$

Rezolvare

1. Se calculează $(x-5)(y-5) + 5 = xy - 5x - 5y + 25 + 5 = xy - 5x - 5y + 30 = x \circ y$
2. Funcție de gradul I, bijectivă.

$$f(x \circ y) = f((x-5)(y-5) + 5) = (x-5)(y-5) + 5 - 5 = (x-5)(y-5) = f(x) \cdot f(y).$$
3.
$$\left. \begin{array}{l} x \in H \Rightarrow x > 5 \Rightarrow x - 5 > 0 \\ y \in H \Rightarrow y > 5 \Rightarrow y - 5 > 0 \end{array} \right\} \Rightarrow (x-5)(y-5) > 0 \Rightarrow (x-5)(y-5) + 5 > 5 \Rightarrow x \circ y > 5 \Rightarrow x \circ y \in H$$
4. Calculând $f'(t) = 1 > 0 \Rightarrow f$ este strict crescătoare pe $(5, \infty)$ și deci bijectivă pe $(5, \infty)$. Morfismul este demonstrat la itemul 2.
5. $x \circ y = xy - 5x - 5y + 30 = yx - 5y - 5x + 30 = y \circ x$

Legi de compoziție Bacalaureat 2014-2016

6. Alegem $x-5=\frac{2}{3}$ și $y-5=\frac{3}{2}$ obținem $x=\frac{2}{3}+5=\frac{17}{3}\in\mathbf{Q}\setminus\mathbf{Z}$ și $y=\frac{3}{2}+5=\frac{13}{2}\in\mathbf{Q}\setminus\mathbf{Z}$ și calculăm

$$\frac{17}{3}\circ\frac{13}{2}=\left(\frac{17}{3}-5\right)\left(\frac{13}{2}-5\right)+5=\frac{2}{3}\cdot\frac{3}{2}+5=1+5=6\in\mathbf{Z}.$$

7. Alegem $x-5=\sqrt{2}-1$ și $y-5=\sqrt{2}+1 \Rightarrow x=\sqrt{2}+4\in\mathbf{R}\setminus\mathbf{Q}$ și $y=\sqrt{2}+6\in\mathbf{R}\setminus\mathbf{Q}$ și calculăm
 $(\sqrt{2}+4)\circ(\sqrt{2}+6)=(\sqrt{2}+4-5)\cdot(\sqrt{2}+6-5)+5=$
 $=(\sqrt{2}-1)\cdot(\sqrt{2}+1)+5=2-1+5=6\in\mathbf{Z}.$

8. Asociativitatea:

$$(x\circ y)\circ z=[(x-5)(y-5)+5]\circ z=[(x-5)(y-5)+5-5](z-5)+5=(x-5)(y-5)(z-5)+5$$

$$x\circ(y\circ z)=x\circ[(y-5)(z-5)+5]=(x-5)[(y-5)(z-5)+5-5]+5=(x-5)(y-5)(z-5)+5$$

9. Elemental neutru $x\circ e=x \Rightarrow xe-5x-5e+30=x \Rightarrow xe-5e=6x-30 \Rightarrow e(x-5)=6(x-5) \Rightarrow e=6\in H$.

10. $x\circ x'=6 \Rightarrow xx'-5x-5x'+30=6 \Rightarrow xx'-5x'=5x-24 \Rightarrow x'(x-5)=5x-24 \Rightarrow$

$$x'=\frac{5x-24}{x-5}=\frac{5x-25+1}{x-5}=\frac{5(x-5)-1}{x-5}=5-\frac{1}{x-5}\neq 5 \Rightarrow x'\in\mathbf{R}\setminus\{5\}$$

11. Din 5) H este parte stabilă, din 8) rezultă asociativitatea, din 9) elementul neutru, din 9) elementul simetric și din 5) comutativitatea $\Rightarrow (H,\circ)$ formează o structură de grup comutativ.

12. $x\circ 6\circ x=(x-5)(6-5)(x-5)+5$ și obținem $(x-5)^2+5=1994\cdot 2005+30 \Rightarrow$
 $(x-5)^2=(1999-5)(1999+5)+25 \Rightarrow (x-5)^2=1999^2-25+25 \Rightarrow (x-5)^2=1999^2 \Rightarrow$
 $x+5=\pm 1999 \Rightarrow x_1=1994$ și $x_2=-2004$.

13. Determinăm pe θ astfel încât $\theta-5=0 \Rightarrow \theta=5$. Verificăm: $x\circ 5=(x+5)(\theta-5)+5=5$.

14. Conform itemului 13) $x\circ 5=5$ și în sirul care se compune există numărul 5, deci $E=(-2009)\circ(-2008)\circ\dots\circ(-2)\circ(-1)\circ 0\circ 1\circ 2\dots\circ 2008\circ 2009=5$

15. Exprimarea de la acest punct s-a demonstrat la itemul 8).

16. $(2009x^2-x+5)\circ(x^2-2009x+5)=5 \Rightarrow [(2009x^2-x+5)-5][(x^2-2009x+5)-5]+5=5 \Rightarrow (2009x^2-x)(x^2-2009x)=0 \Rightarrow x(2009x-1)(x-2009)=0 \Rightarrow x\in\left\{0;\frac{1}{2009};2009\right\}$.

17. Conform punctului 15) \Rightarrow

$$(2^x)\circ(\log_2 x)\circ(4+C_{2009}^x)=(2^x-5)(\log_2 x-5)(4+C_{2009}^x-5)+5=5 \Rightarrow$$

$$2^x-5=0 \Rightarrow x_1=\log_2 5$$

$$\log_2 x-5=0 \Rightarrow x_2=2^5$$

$$C_{2009}^x-1=0 \Rightarrow C_{2009}^x=1 \Rightarrow x_3=0$$
 sau $x_4=2009$.

18. Generalizând punctul 8) se obține

$$\underbrace{2009\circ 2009\circ\dots\circ 2009}_{de\ 2009\ ori}=\underbrace{(2009-5)\cdot(2009-5)\cdot\dots\cdot(2009-5)}_{de\ 2009\ ori}+5=2004^{2009}+5$$

19. $6\circ 7\circ 8\circ\dots\circ n=(5+1-5)\cdot(5+2-5)\cdot(5+3-5)\dots\cdot(n-5)+5=1\cdot 2\cdot 3\cdot\dots\cdot(n-5)+5=(n-5)!+5$ se obține $(n-5)!+5\geq 2009 \Rightarrow (n-5)!\geq 2004$. Știm $6!=720$ și $7!=5040$, deci $n=7$.

20. $x\circ x\circ x\circ x\circ x=(x-5)(x-5)(x-5)(x-5)+5=(x-5)^5+5 \Rightarrow (x-5)^5+5=2009^5+5 \Rightarrow$
 $(x-5)^5=2009^5 \Rightarrow x-5=2009 \Rightarrow x=2014$.

Probleme propuse

1. Pe mulțimea numerelor reale se definește legea de compoziție $x \circ y = 3xy + 3x + 3y + 2$.

- a) Arătați că $(-1) \circ 1 = -1$.
- b) Rezolvați în mulțimea numerelor reale ecuația $x \circ x = x$.
- c) Determinați perechile (a,b) de numerele întregi, știind că $a \circ b = 8$.

2. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x \circ y = xy + 3x + 3y + 6.$$

- a) Arătați că $0 \circ (-3) = -3$.
- b) Arătați că $x \circ y = (x+3)(y+3)-3$, pentru orice numere reale x și y .
- c) Arătați că $(-3) \circ x = -3$, pentru orice număr real x .
- d) Verificați dacă $e = -2$ este element neutru al legii de compoziție „ \circ ”.
- e) Calculați $(-2016) \circ (-2015) \circ \dots \circ (-3)$.
- f) Rezolvați în mulțimea numerelor reale ecuația $x \circ x \circ x = 5$.

3. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x * y = xy - x - y + 2.$$

- a) Arătați că $x * y = (x-1)(y-1)+1$, pentru orice numere reale x și y .
- b) Calculați $0 * 1 * 2 * 3$.
- c) Determinați numerele reale a , știind că $a * a * 2016 = 2016$.

4. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x \circ y = 6xy - 2x - 2y + 1.$$

- a) Calculați $1 \circ \frac{1}{3}$
- b) Determinați elementul neutru al legii de compoziție „ \circ ”.
- c) Calculați $\frac{1}{1008} \circ \frac{2}{1008} \circ \frac{3}{1008} \circ \dots \circ \frac{2016}{1008}$

5. Pe mulțimea numerelor reale se definește legea de compoziție $x \circ y = xy + x + y$.

- a) Calculați $(-2) \circ 2$.
- b) Arătați că $x \circ y = (x+1)(y+1)-1$, pentru orice numere reale x și y .
- c) Rezolvați în mulțimea numerelor reale ecuația $x^2 \circ x = -1$.
- d) Verificați dacă legea de compoziție „ \circ ” este asociativă.
- e) Demonstrați că numărul $n \circ n$ este multiplu de 8, pentru orice număr natural par n .
- f) Dați un exemplu de două numere iraționale a și b , pentru care $a \circ b \in \mathbb{N}$.

6. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x * y = xy - 4x - 4y + 20.$$

- a) Arătați că $x * y = (x-4)(y-4)+4$, pentru orice numere reale x și y .
- b) Calculați $1 * 2 * 3 * * 2016$.
- c) Determinați numerele naturale a , b și c , știind că $a < b < c$ și $a * b * c = 66$.

7. Pe mulțimea numerelor reale se definește legea de compoziție $x \circ y = xy + 2x + 2y + 2$.

- a) Arătați că $1 \circ (-2) = -2$.
- b) Demonstrați că $x \circ y = (x+2)(y+2)-2$, pentru orice numere reale x și y .
- c) Determinați numerele reale nenule x , pentru care $x \circ \frac{1}{x} = x$

Legi de compoziție Bacalaureat 2014-2016

8. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x * y = -2xy + 10x + 10y - 45.$$

a) Arătați că $x * y = -2(x - 5)(y - 5) + 5$, pentru orice numere reale x și y .

b) Arătați că $1 * 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * 10 = 5$.

c) Determinați numerele naturale m și n , pentru care $m * n = 27$.

9. Pe mulțimea numerelor reale se definește legea de compoziție dată de

$$x \circ y = -xy + x + y.$$

a) Calculați $1 \circ 2015$.

b) Arătați că $x \circ y = -(x - 1)(y - 1) + 1$, pentru orice numere reale x și y .

c) Rezolvați în mulțimea numerelor reale ecuația $3^x \circ 5^x = 1$.

10. Pe mulțimea numerelor reale se definește legea de compoziție $x \circ y = x + y - 2$.

a) Calculați $(-2) \circ 2$.

b) Arătați că legea de compoziție „ \circ ” este asociativă.

c) Verificați dacă $e = 2$ este element neutru al legii de compoziție „ \circ ”.

d) Determinați numărul real x , știind că $(x + 1) \circ x = 3$.

e) Rezolvați în mulțimea numerelor reale ecuația $9^x \circ 3^x = 0$

f) Arătați că $x^2 \circ \frac{1}{x^2} \geq 0$ pentru orice număr real nenul x .

11. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x * y = xy - 7x - 7y + 56.$$

a) Arătați că $(-7) * 7 = 7$.

b) Arătați că $x * y = (x - 7)(y - 7) + 7$, pentru orice numere reale x și y .

c) Calculați $1 * 2 * 3 * \dots * 2015$.

12. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x \circ y = xy - 3(x + y) + 12.$$

a) Arătați că $x \circ 3 = 3 \circ x = 3$, pentru orice număr real x .

b) Rezolvați în mulțimea numerelor reale ecuația $x \circ x = x$.

c) Calculați $1 \circ 2 \circ \dots \circ 2014$.

13. Pe mulțimea numerelor reale se definește legea de compoziție dată de $x \circ y = x + y - 1$.

a) Calculați $2 \circ 3$.

b) Verificați dacă legea de compoziție „ \circ ” este comutativă.

c) Arătați că legea de compoziție „ \circ ” este asociativă.

d) Determinați numerele reale x pentru care $x^2 \circ x = 11$

e) Arătați că $x \circ (x + 2014) = (x + 1012) \circ (x + 1012)$, pentru orice număr real x .

f) Determinați numărul real nenul x pentru care $x \circ \frac{1}{x} = 1$

14. Pe mulțimea numerelor reale se definește legea de compoziție $x * y = 2(x + y - 1) - xy$.

a) Arătați că $1 * 2 = 2$.

b) Arătați că $x * 2 = 2 * x = 2$ pentru orice număr real x .

c) Rezolvați în mulțimea numerelor reale ecuația $x * x = x$.

15. Pe mulțimea numerelor reale se definește legea de compoziție $x \circ y = 2xy - 3x - 3y + 6$.

a) Calculați $1 \circ 2$.

Legi de compoziție Bacalaureat 2014-2016

b) Arătați că $x \circ y = 2\left(x - \frac{3}{2}\right)\left(y - \frac{3}{2}\right) + \frac{3}{2}$ pentru orice numere reale x și y .

c) Rezolvați în mulțimea numerelor reale ecuația $x \circ x = 2$.

16. Pe mulțimea numerelor reale se definește legea de compoziție $x * y = xy - 5x - 5y + 30$.

a) Arătați că $1 * 5 = 5$.

b) Arătați că $x * y = (x - 5)(y - 5) + 5$ pentru orice numere reale x și y .

c) Rezolvați în mulțimea numerelor reale ecuația $x * x = x$.

17. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x * y = 3x + 3y - xy - 6.$$

a) Calculați $1 * 3$.

b) Arătați că $x * y = 3 - (x - 3)(y - 3)$ pentru orice numere reale x și y .

c) Determinați numerele reale x pentru care $\underbrace{x * x * \dots * x}_{x \text{ de } 2014 \text{ ori}} = x$.

18. Pe mulțimea numerelor întregi se definesc legile de compoziție $x * y = x + y - 3$ și

$$x \circ y = (x - 3)(y - 3) + 3.$$

a) Să se rezolve în mulțimea numerelor întregi ecuația $x * x = x \circ x$.

b) Să se determine numărul întreg a care are proprietatea că $x \circ a = 3$, oricare ar fi numărul întreg x .

c) Să se rezolve sistemul de ecuații $\begin{cases} x * (y + 1) = 4 \\ (x - y) \circ 1 = 5 \end{cases}$, unde $x, y \in \mathbb{Z}$.

19. Pe mulțimea numerelor reale se definește legea de compoziție asociativă

$$x \circ y = 2xy - 6x - 6y + 21.$$

a) Arătați că $x \circ y = 2(x - 3)(y - 3) + 3$, pentru orice numere reale x și y .

b) Arătați că $1 \circ 2 \circ 3 \circ 4 = 3$.

c) Determinați numerele reale x , pentru care $x \circ x \circ x = x$.

20. Pe mulțimea numerelor reale se definește legea de compoziție $x * y = x + y - 5$.

a. Arătați că $(-2) * 7 = 0$.

b. Arătați că legea de compoziție „ $*$ ” este asociativă.

c. Arătați că $(1 * 2) * (8 * 9) = (1 * 9) * (2 * 8)$.

d. Determinați numărul real x , pentru care $(x * x) * x = x$.

e. Determinați numărul real x , pentru care $9^x * 3^x = 7$.

f. Demonstrați că $x^2 * \frac{1}{x^2} \geq -3$, pentru orice număr real nenul x .

Virgil-Mihail Zaharia

STRUCTURI ALGEBRICE: GRUPURI – REGULI DE CALCUL

Prof. Hecser Enikő-Krisztina,

Colegiul Național „Unirea”,

Târgu Mureș, jud. Mureș

În clasa a XII-a noțiunea de lege de compoziție, proprietățile acestora, noțiunea de grup sau de altă structură algebrică se înțelege ușor. La prezentarea regulilor de calcul într-un grup – am putea spune – nu întâmpinăm greutăți, chiar din contră: elevilor li se pare că este o lecție banală cu câteva teoreme evidente care “se cunosc deja”. Confuzia apare din cauza notației și anume: în aproape toate manualele și culegerile utilizate la clasă, grupul este notat – pentru a ușura scrierea-multiplicativ, astfel elevii se gândesc la înmulțire și bagatelizează importanța acestor proprietăți/teoreme. În momentul în care apar problemele/aplicațiile, elevii realizează că aceste exerciții nu sunt deloc ușoare și doar după mai multe probleme abordate în clasă au și ei câteva idei de rezolvare. Deprinderile, tehnicele se formează prin exercițiu, acesta fiind motivul pentru care am ales spre prezentare câteva asemenea probleme.

Problema 1. Fie (G, \cdot) un grup și $a, b \in G$ astfel încât $ab = ba$. Arătați că:

- a) $a^n b = b a^n \quad \forall n \in \mathbb{Z}$
- b) $a^m b^n = b^n a^m \quad \forall m, n \in \mathbb{Z}$

Rezolvare:

a) Se va utiliza metoda inducției matematice pentru $n \in \mathbb{N}$.

Pentru $n = 0$ avem $a^0 b = b a^0 \Leftrightarrow eb = be \Leftrightarrow b = b$ sau pentru $n = 1$: $a^1 b = b a^1 \Leftrightarrow ab = ba$, evident adevărate. Presupunând propoziția adevărată pentru $n = k$, adică $a^k b = b a^k$, putem arăta pentru $n = k + 1$ în felul următor: $a^{k+1} b = a a^k b = a b a^k = b a a^k = b a^{k+1}$. Dacă $n < 0 \Rightarrow -n \in \mathbb{N}$, deci $a^n b = (a^{-1})^{-n} b = b(a^{-1})^{-n} = b a^n$.

b) Ne bazăm pe cele demonstreate anterior și folosim în continuare metoda inducției matematice pentru $n \in \mathbb{N}$. Pentru $n = 0$ avem $a^m b^0 = b^0 a^m \Leftrightarrow a^m e = e a^m \Leftrightarrow a^m = a^m$, adevărat. Dacă presupunem că propoziția este adevărată pentru $n = k$, adică $a^m b^k = b^k a^m$, atunci $a^m b^{k+1} = a^m b^k b = b^k a^m b = b^k b a^m = b^{k+1} a$, ceea ce înseamnă că s-a dovedit propoziția adevărată și pentru $n = k + 1$. Dacă $n < 0 \Rightarrow -n \in \mathbb{N}$, deci $a^m b^n = a^m (b^{-1})^{-n} = (b^{-1})^{-n} a^m = b^n a^m$.

Problema 2. Fie (G, \cdot) un grup și $a, b \in G$ astfel încât $a = b^2, b = a^2$. Arătați că:

- a) dacă $x = aba$, atunci $x^3 = e$
- b) dacă $x = aba^{-1}$, atunci $x^3 = e$
- c) dacă $x = (ab)^n$, atunci $x = e, \forall n \in \mathbb{Z}$.

Rezolvare:

Din ipoteză avem: $b = a^2 = (b^2)^2 = b^4$, de unde $e = b^3$ și analog $a = b^2 = (a^2)^2 = a^4$, de unde $e = a^3$.

- a) $x^3 = (aba)^3 = abaabaaba = aba^2ba^2ba = abbbbba = ab^3b^2a = aeaa = a^3 = e$.
- b) $x^3 = (aba^{-1})^3 = aba^{-1}aba^{-1}aba^{-1} = abebeba^{-1} = ab^3a^{-1} = aea^{-1} = aa^{-1} = e$.
- d) $x = (aa^2)^n = (a^3)^n = e^n = e \quad \forall n \in \mathbb{Z}$.

Problema 3. Fie (G, \cdot) un grup și $a, b, c \in G$ astfel încât $a = b^2, b = c^2, c = a^2$. Arătați că:

- a) dacă $x = abc$, atunci $x = e$.
- b) dacă $x = abc^{-1}$, atunci $x^2 = a^{-1}$ și $x^3 = a^2$.
- c) dacă $x = a^n b^{n+1} c^{n+2}$, atunci $x = a, \forall n \in \mathbb{N}^*$.
- d) dacă $a^m b^n c^p = e$, atunci $a^{3n+5p+6m} = e$.

Rezolvare:

Din ipoteză avem: $a = b^2 = (c^2)^2 = c^4 = (a^2)^4 = a^8 \Rightarrow e = a^7$, analog $b^7 = c^7 = e$. De asemenea $b = c^2 = (a^2)^2 = a^4$.

- a) $x = abc = aa^4a^2 = a^7 = e$.
- b) $x^2 = (abc^{-1})^2 = (aa^4a^{-2})^2 = (a^3)^2 = a^6 = a^{-1}$.
- c) $x^3 = x^2x = a^{-1}abc^{-1} = bc^{-1} = a^4a^{-2} = a^2$.
- c) $x = a^n(a^4)^{n+1}(a^2)^{n+2} = a^{n+4n+4+2n+4} = a^{7n+8} = a^{7n+7}a = (a^7)^{n+1}a = ea = a$.
- d) $a^m b^n c^p = e$, deci $a^m (a^4)^n (a^2)^p = a^{m+4n+2p} = e$, de unde $a^m a^{4n} a^{2p} = a^{7m} a^{7n} a^{7p} \Rightarrow e = a^{6m} a^{3n} a^{5p} \Rightarrow e = a^{6m+3n+5p}$.

Problema 4. Fie (G, \cdot) un grup și $a, b \in G$ astfel încât $ab = e$. Arătați că: $ba = e$.

Rezolvare:

$$ab = e \Rightarrow abb^{-1} = eb^{-1} \Rightarrow ae = b^{-1} \Rightarrow a = b^{-1} \text{ și atunci } ba = bb^{-1} = e.$$

Problema 5. Fie (G, \cdot) un grup în care $x^3 = e$ și $x^2y^2 = y^2x^2, \forall x, y \in G$. Arătați că grupul este comutativ.

Rezolvare:

Dacă în a doua relație din ipoteză alegem $x \mapsto x^2$ și $y \mapsto y^2$, atunci obținem

$$(x^2)^2(y^2)^2 = (y^2)^2(x^2)^2 \Rightarrow x^4y^4 = y^4x^4 \Rightarrow x^3xyy^3 = y^3yxx^3 \Rightarrow exye = eyxe \text{ și deci } xy = yx$$

oricare ar fi elementele $x, y \in G$.

Problema 6. Fie (G, \cdot) un grup cu proprietatea $x^3 = e$ și $(xy)^2 = (yx)^2, \forall x, y \in G$. Arătați că grupul este comutativ.

Rezolvare:

$$e = (xy)^3 = (xy)^2xy = (yx)^2xy \Rightarrow (yx)^2 = (xy)^{-1}. \text{ De asemenea } e = (yx)^3 = (yx)^2yx = (xy)^{-1}(yx) \text{ și deci } xy = yx \text{ oricare ar fi elementele } x, y \in G.$$

Problema 7. Fie (G, \cdot) un grup în care $xy^{-1} = yx^{-1}, \forall x, y \in G$. Arătați că grupul este abelian.

Rezolvare:

Dacă în relația din ipoteză luăm $y \mapsto y^{-1}$, atunci obținem $xy = y^{-1}x^{-1} \Rightarrow xy = (xy)^{-1} \Rightarrow (xy)^2 = e$.

În acest rezultat alegem mai întâi $y = x^2$, după aceea $y = x$ și vom avea

$$\left. \begin{array}{l} y = x^2 \Rightarrow (x^3)^2 = e \Rightarrow x^6 = e \\ y = x \Rightarrow (x^2)^2 = e \Rightarrow x^4 = e \end{array} \right\} \Rightarrow x^2 = e \text{ pentru orice } x \in G.$$

Continuarea acestei rezolvări este o problemă sine stătătoare bine cunoscută:

$$(xy)^2 = e \Rightarrow xyxy = ee \Rightarrow xyxy = x^2y^2 \Rightarrow xyxy = xxyy \Rightarrow yx = xy, \forall x, y \in G.$$

Problema 8. Fie (G, \cdot) un grup și $a, b \in G$ astfel încât $a^5 = b^4 = e$ și $ab = ba^3$.

Arătați că: $ba = a^2b$ și $ab = ba$.

Rezolvare:

Pentru prima cerință: $a^2b = aab = aba^3 = ba^3a^3 = ba^6 = baa^5 = bae = ba$. În cazul celei de-a două relații pornim din $a^2b = ba$ și compunem cu b^3 din stânga, astfel ca să avem

$b^3a^2b = b^4a \Rightarrow b^3a^2b = a$. Urmează ca această relație să fie compusă din dreapta cu b^3 pentru a obține $b^3a^2b^4 = ab^3 \Rightarrow b^3a^2 = ab^3$, ceea ce trebuia demonstrat.

Problema 9. Fie (G, \cdot) un grup și $a, b \in G$ astfel încât $a^6 = e$ și $ab = b^4a$. Arătați că: $b^3 = e$ și $ab = ba$.

Rezolvare:

Pornind din a doua relație din ipoteză putem scrie următorul sir de implicații:

$$\begin{aligned} ab = b^4 a \Rightarrow b^2 ab = b^2 b^4 a \Rightarrow b^2 ab = b^6 a \Rightarrow b^2 ab = a & \quad | \cdot b^2 \Rightarrow b^4 ab = b^2 a \Rightarrow abb = b^2 a \\ \Rightarrow ab^2 = b^2 a & \quad | \cdot b \Rightarrow ab^3 = b^2 ab \Rightarrow ab^3 = b^2 b^4 a \Rightarrow ab^3 = b^6 a \Rightarrow ab^3 = a \Rightarrow b^3 = e. \end{aligned}$$

A doua cerință este banală, și anume $ab = b^4 a \Rightarrow ab = b^3 ba \Rightarrow ab = eba \Rightarrow ab = ba$.

Problema 10. Fie (G, \cdot) un grup și $a, b \in G$ astfel încât $a^6 = b^2 = e$ și $a^3 b = ba$. Arătați că $ab = ba$.

Rezolvare:

Dacă $b^2 = e$, atunci $b = b^{-1}$. Pornind din a doua relație din ipoteză putem obține următorul

$$\begin{aligned} \text{rezultat: } a^3 b = ba & \quad | \cdot b \Rightarrow a^3 b^2 = bab \Rightarrow a^3 = bab \text{ și atunci} \\ e = a^6 = a^3 a^3 = (bab)(bab) & \Rightarrow bab^2 ab = ba^2 b, \text{ deci } ba^2 b = e & \quad | \cdot b \Rightarrow b^2 a^2 b^2 = b^2 \Rightarrow a^2 = e. \text{ Mai} \\ \text{avem doar un singur pas de făcut: } a^3 b = ba & \Leftrightarrow a^2 ab = ba \Leftrightarrow eab = ba \Leftrightarrow ab = ba. \end{aligned}$$

Problema 11. Fie (G, \cdot) un grup. Dacă $x, y \in G$ verifică relațiile $x^3 = e$ și $xyx^{-1} = y^3$, arătați că:

a) $y^{3n} = xy^n x^{-1}, \forall n \in N$

b) $y^{26} = e$

Rezolvare:

a) Se va utiliza metoda inducției matematice. Într-adevăr, pentru $n=1$ este chiar ipoteza, iar dacă presupunem afirmația valabilă pentru $n=k$, atunci este valabilă și pentru $n=k+1$, deoarece putem scrie $y^{3(k+1)} = y^{3k} y^3 = (xy^n x^{-1})(xyx^{-1}) = xy^{n+1} x^{-1}$, ceea ce încheie demonstrația.

b) Dacă în relația dovedită anterior luăm $n=3$, obținem $y^9 = xy^3 x^{-1}$ și folosind iarăși ipoteza putem continua $y^9 = x(xyx^{-1})x^{-1} = x^2 yx^{-2} = x^{-1}yx$ (am utilizat $x^2 = x^{-1}$ și $x^{-2} = x$, relații ce rezultă din $x^3 = e$). Așadar $y^9 = x^{-1}yx$. Tot prin inducție se poate arăta că $y^{9n} = x^{-1}y^n x$ (demonstrație simplă, foarte asemănătoare cu precedenta inducție). Vom încheia rezolvarea alegând $n=3$ în această relație și ținând seama în membrul drept de a doua ipoteză a problemei. Deci obținem succesiv $y^{27} = x^{-1}y^3 x = x^{-1}(xyx^{-1})x = y$, adică $y^{27} = y \Rightarrow y^{26} = e$.

Problema 12. Arătați că dacă într-un grup finit mai mult de jumătate din elementele grupului comută cu toate elementele din grup, atunci grupul este abelian.

Rezolvare:

Deoarece se va utiliza teorema lui Lagrange, reamintim această teoremă: Ordinul oricărui subgrup al unui grup finit divide ordinul grupului.

Notăm grupul din enunț cu (G, \cdot) și să considerăm mulțimea elementelor care comută cu orice element din grup $H = \{x \in G \mid xy = yx, \forall y \in G\}$. Se poate arăta ușor că (H, \cdot) este un grup

comutativ și $(H, \cdot) \leq (G, \cdot)$. Conform ipotezei $|H| > \frac{1}{2}|G| \Leftrightarrow |G| < 2|H|$, dar conform teoremei lui

Lagrange $\exists n \in N^* : |G| = n|H|$, ceea ce înseamnă că $|G| = n|H| < 2|H|$, adică $n < 2$. Evident n nu poate fi altceva decât 1. Deci: $|G| = |H| = |H|$, adică $G = H$ și asta dovedește că (G, \cdot) este grup abelian.

Problema 13. Fie (G, \cdot) un grup comutativ finit cu elementul neutru e . Dacă $x^2 = e$, pentru mai mult de jumătate din elementele grupului, atunci $x^2 = e$, pentru orice $x \in G$.

Rezolvare:

Notăm cu H mulțimea acelor elemente pentru care se verifică egalitatea din ipoteză: $H = \{x \in G \mid x^2 = e\}$ și demonstrăm că $(H, \cdot) \leq (G, \cdot)$. Conform teoremei de caracterizare a submulțimilor verificăm următoarele:

1. $H \neq \emptyset$, deoarece $e \in H$

2. Dacă $x, y \in H$, atunci putem scrie implicațiile: $x, y \in H \Rightarrow x^2 = y^2 = e \Rightarrow (xy^{-1})^2 = x^2(y^{-1})^2 = x^2(y^2)^{-1} = ee = e \Rightarrow xy^{-1} \in H$

Deci într-adevăr $(H, \cdot) \leq (G, \cdot)$.

Dacă notăm ordinul grupului G cu n și ordinul subgrupului H cu k atunci din ipoteză rezultă că $k > \frac{n}{2}$, adică $n < 2k$.

Conform teoremei lui Lagrange: $k \mid n \Rightarrow \exists p \in N : n = pk$. Asemănător cu problema precedentă ajungem la concluzia că $p = 1$, adică $n = k$ și atunci $H = G$, ceea ce înseamnă că egalitatea din ipoteză se verifică pentru toate elementele din G .

Problema 14. Arătați că dacă într-un grup (G, \cdot) avem pentru un anumit n întreg

$(xy)^n = x^n y^n, (xy)^{n+1} = x^{n+1} y^{n+1}, (xy)^{n+2} = x^{n+2} y^{n+2} \quad \forall x, y \in G$, atunci grupul este comutativ.

Rezolvare:

Conform relațiilor din ipoteză, pentru orice două elemente $x, y \in G$, avem

$$x^{n+1}y^{n+1} = (xy)^{n+1} = (xy)^n xy = x^n y^n xy, \text{ așadar } x^{n+1}y^{n+1} = x^n y^n xy, \text{ de unde obținem } xy^n = y^n x.$$

Această egalitate arată că x comută cu y^n și atunci comută cu orice putere întreagă a lui y^n

(Problema 1.). Analog $x^{n+2}y^{n+2} = (xy)^{n+2} = (xy)^{n+1}xy = x^{n+1}y^{n+1}xy$, adică $x^{n+2}y^{n+2} = x^{n+1}y^{n+1}xy$, de unde se obține $xy^{n+1} = y^{n+1}x$, adică x comută cu y^{n+1} și atunci comută cu orice putere întreagă a lui y^{n+1} . Deoarece numerele n și $n+1$ sunt prime între ele, există k, l întregi astfel ca

$$kn + l(n+1) = 1 \text{ și atunci:}$$

$xy = xy^{kn+l(n+1)} = x(y^n)^k (y^{n+1})^l = (y^n)^k x (y^{n+1})^l = (y^n)^k (y^{n+1})^l x = y^{kn+l(n+1)} x = yx$. Relația fiind adevărată pentru orice $x, y \in G$, rezultă că grupul este comutativ.

Problema 15. Fie (G, \cdot) un grup în care are loc implicația $xy^2 = z^2x \Rightarrow y = z$. Demonstrați că:

a) $x^2 \neq e, \forall x \in G - \{e\}$

b) Grupul este abelian.

Rezolvare:

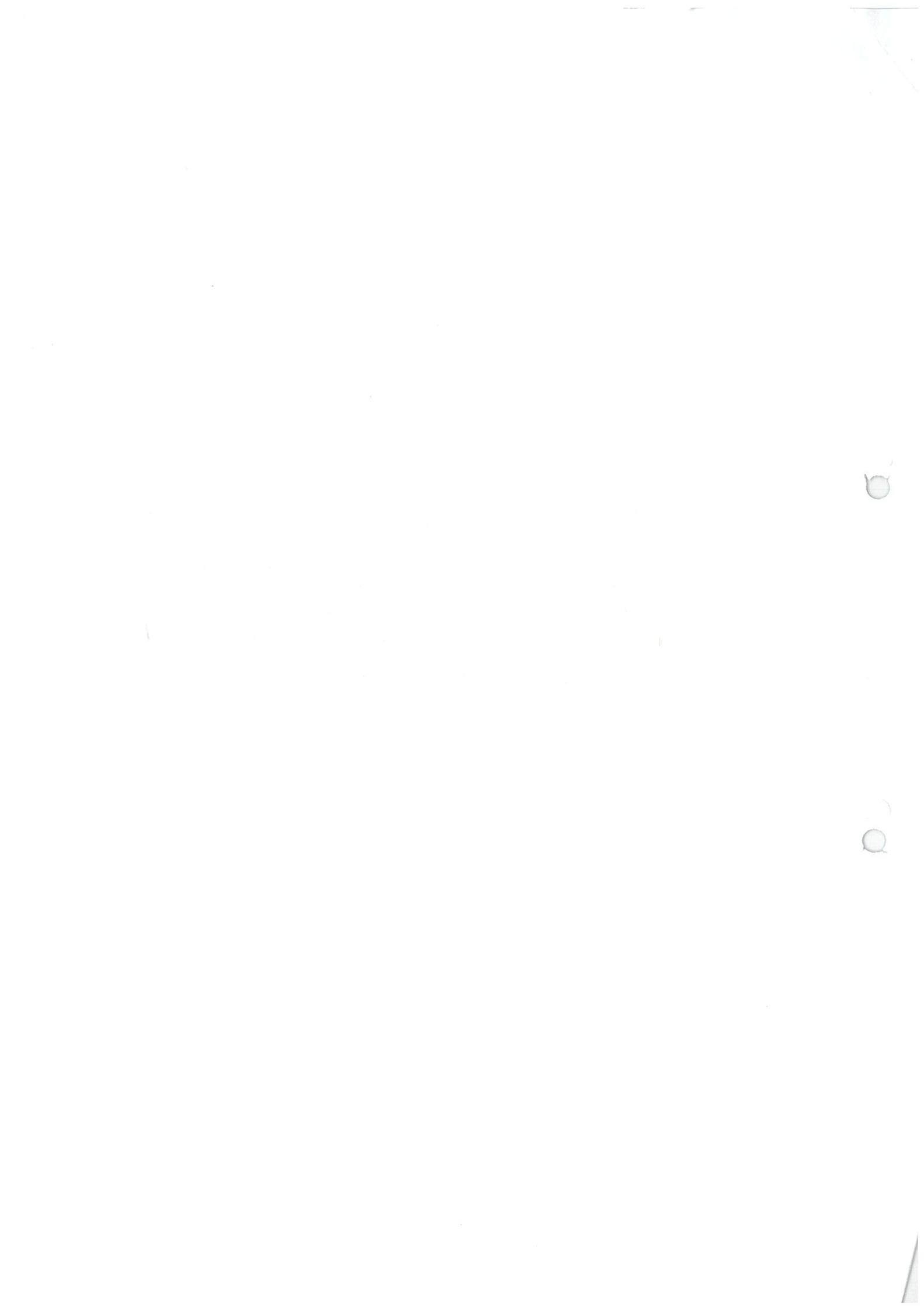
a) Fie $x \in G$ cu $x^2 = e$. Fixând un element $a \in G$, vom avea în mod evident $ax^2 = e^2a$ și atunci pe baza implicației din ipoteză, rezultă $x = e$. Așadar $x^2 = e \Rightarrow x = e$, sau echivalent $x \neq e \Rightarrow x^2 \neq e$.

b) Fie $x, y \in G$ arbitrară. Se poate arăta că $x^{-1}(xy)^2 = (yx)^2 x^{-1}$, deoarece putem scrie succesiv $x^{-1}xyxy = yxyxx^{-1} \Leftrightarrow yxy = yxy$. Din egalitatea $x^{-1}(xy)^2 = (yx)^2 x^{-1}$, folosind implicația din ipoteză, rezultă $xy = yx$, deci grupul este abelian.

Bibliografie:

1. M. Burtea, G. Burtea: Matematică pentru clasa a XII-a, programă M1, Culegere de exerciții și probleme, Editura Carminis Educațional, 2008
2. C. Năstăsescu, M. Tena, G. Andrei, I. Otărășanu: Probleme de structuri algebrice, Editura Academiei Republicii Socialiste România, 1988
3. András Sz., Csapó H., Lukács A.: Matematika a XII osztály számára, Editura Státus, 2002
4. Ion D. Ion, A.P. Ghioca, N.I. Nedea: Manual de algebră pentru clasa a XII-a, Editura Didactică și Pedagogică, 1992
5. Farkas M.: Algebra tankönyv a XII. Osztályosok számára, Editura Erdélyi Tankönyvtanács, 1998

- J 3 I(a) Să se arate că $\{x \in \{1, 2, \dots, 149\} \mid \text{cu proprietatea că } \overline{x} + 3\overline{7} = \overline{0}\}$ este un grup cu proprietatea $(\mathbb{Z}_{149}, +)$.
- J 3 I(b) Să se arate că $\{x \in \{1, 2, \dots, 148\} \mid \text{cu proprietatea că } 3\overline{7} \cdot \overline{x} = \overline{1} \text{ în } (\mathbb{Z}_{149}, \cdot)\}$ este un grup.
- J 3 I(c) Să se arate că restul împărțirii lui $2^{147} + 3^{147} + 6^{147}$ la 149 este 149.
- J 3 II(a) Calculați ord $\overline{3}$ în grupul $(\mathbb{Z}_{61}, +)$.
- J 3 II(b) Calculați ord $\overline{3}$ în grupul (\mathbb{Z}_{61}, \cdot) .
- J 3 II(c) Să se arate că cel mai mare divizor comun impărțitor al numărului $2019^8 + 1$ este 1.
- J 3 III(a) Care sunt redochile polinomului $x^5 - 1$ în corpul $(\mathbb{Z}_{41}, +, \cdot)$?
- J 3 III(b) $x^4 - 4 = x^4 - 4 = x^4 - 5$ în corpul $(\mathbb{Z}_{49}, +, \cdot)$?
- J 3 III(c) Câte soluții are ecuația $T^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}$ în $(\mathbb{Z}_8, +)$?
- J 3 IV(a) Fie (G, \circ) un grup cu proprietatea că $g^2 = e \forall g \in G$. Arătați că 6 este comutativ (e - elementul neutru al grupului G).
- 5 J 3 IV(b) $(R, +, \cdot)$ este un inel cu proprietatea că $x^2 = x, \forall x \in R$. Arătați că inelul este comutativ.



De ce sunt utile polinoamele?

V-am povestit acum ceva vreme despre importanța cheilor publice în criptografie. Istoric, prima astfel de cheie a fost furnizată de ideile matematicienilor Diffie și Hellman. Ideea centrală este furnizată de următorul rezultat din algebră:

Teorema: Dacă p este un număr prim, atunci grupul (\mathbb{Z}_p^*, \cdot) este ciclic. Cu alte cuvinte, în acest grup există un element de ordin $p - 1$.

Schița demonstrației:

Pasul 1: Fie (G, \cdot) un grup comutativ, finit și m ordinul maxim al unui element din G . Atunci g^m este e , elementul neutru al grupului G , pentru orice $g \in G$.

Nu voi da demonstrația completă a acestui rezultat, însă vă voi spune ideea centrală. Trebuie arătat că ordinul lui g divide m , pentru orice $g \in G$. Se presupune că nu ar fi adevărat acest lucru și se construiește un element din G cu ordinul mai mare decât m . Vă sugerez doar cum se găsește contradicția într-un caz concret. Să presupunem că $\text{ord } g = 12$ și $\text{ord } h = 18 = m$. Atunci $\text{ord } g^3 = \frac{12}{(3,12)} = 4$, $\text{ord } h^2 = \frac{18}{(2,18)} = 9$ și

$$\text{ord } (g^3 \cdot h^2) = \text{ord } g^3 \cdot \text{ord } h^2 = 4 \cdot 9 = 36 > 18 = m.$$

Am găsit un element din grup cu ordinul mai mare decât m ; contradicție. Ideea este aceeași și în cazul general.

Pasul 2: Notăm cu m cel mai mare ordin al unui element din grupul (\mathbb{Z}_p^*, \cdot) . Evident că m divide $p - 1$. Noi trebuie să arătăm că $m = p - 1$. Din Pasul 1 știm că $x^m = \bar{1}$, pentru orice $x \in \mathbb{Z}_p^*$. De aici deducem că polinomul

$$X^m - \bar{1} \in \mathbb{Z}_p[X]$$

are cel puțin $p - 1 = |\mathbb{Z}_p^*|$ rădăcini. Dar numărul rădăcinilor este cel mult gradul polinomului, de unde deducem că

$$p - 1 \leq m.$$

Cum m este divizor al lui $p - 1$, rezultă că $m \leq p - 1$. Combinând cele două inegalități, deducem că $m = p - 1$ și enunțul este demonstrat.

Exercițiu : Găsiți acel n pentru care $\bar{2}^n = \bar{3}\bar{1}$ în \mathbb{Z}_{83} .

Comentariu: Ordinul lui $\bar{2}$ în grupul $(\mathbb{Z}_{83}^*, \cdot)$ este 82, ceea ce implică existența numărului n din exercițiu. Ordinul lui $\bar{2}$ în grupul menționat este un divizor al lui 82, deci poate fi 1, 2, 41 sau 82. Cum

$$\bar{2}^{41} = ((\bar{2})^{10})^4 \bar{2} = \bar{2} \cdot \bar{2}^8 = \bar{2} \cdot \bar{37}^2 = \bar{2} \cdot \bar{41} = \bar{82},$$

rezultă imediat că ordinul lui $\bar{2}$ în grupul $(\mathbb{Z}_{83}^*, \cdot)$ este 82

