

Pr. (generică)

Seminar 8

22.11.2021

Calculati restul împărțirii lui a^b la c , unde a, b, c sunt numere naturale care care.

Mai târziu $a^b \pmod{c}$

Ex $2021^{2021} \pmod{22}, 2022^{2022} \pmod{22}$

TEMA

$\overbrace{2021}^{2021} \pmod{\mathbb{Z}_{22}}$

(• $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$)
($n \geq 2$)

$$\begin{aligned} 2021 &\stackrel{2021}{=} 19 \pmod{22} \equiv (-3) \stackrel{2021}{=} 19 \pmod{22} \\ &\equiv -3 \pmod{22} \\ &\equiv -(-3)^{404} \cdot 3 \pmod{22} \\ &\equiv -(-3)^{202} \cdot 3 \pmod{22} \\ &\equiv -3 \pmod{22} \end{aligned}$$

$$3^5 = \frac{243}{22} \pmod{22}$$

($a \equiv 1 \pmod{n}$)
↓ restul împ. lui
alături

$$\begin{array}{r} 2021 \\ 198 \\ \hline 22 \\ 18 \\ \hline 4 \\ 22 \\ \hline 18 \\ \hline 1 \end{array}$$

T. Euler ($a, n) = 1$)
 $a^{\varphi(n)} \equiv 1 \pmod{n}$

$$\varphi(22) = 22 \cdot \frac{1}{2} \cdot \frac{10}{11} = 10$$

Dem $-3 \stackrel{2021}{=} 19 \pmod{22} \equiv$
 $\equiv -3 \stackrel{10 \cdot 202 + 1}{=} 19 \pmod{22} \equiv$
 $\equiv -(-3)^{202} \cdot 3 \pmod{22} \equiv -3 \pmod{19} \pmod{22}$

Euler +

Pabz Fie $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$. Def. pe G legea $x * y = \{x+y\}$ ($\{x+y\}$ înseamnă parte fracțională a lui $x+y$). Arăta că $(G, *)$ este un grup abelian.

"*" - asociativă: $a * (b * c) = a * \{b+c\} = \{a+\{b+c\}\}$ (1)

$$\{x\} = x - [x]$$

$$(a * b) * c = \{a+b\} * c = \{\{a+b\} + c\}$$
 (2)

$$\begin{aligned} \{a+\{b+c\}\} &= a + \underline{\{b+c\}} - \underline{\{a+\{b+c\}\}} = a + b + c - \{b+c\} \\ &= a + b + c - \{b+c\} - (\{a+b+c\} - \{b+c\}) = \end{aligned}$$

$$\begin{aligned} &= a + b + c - \{a+b+c\} = \{a+b+c\} \\ &= a + b + c - \{a+b+c\} = \{a+b+c\} \end{aligned}$$

$$[x - \bar{x}] = [x]^k$$

Analog se arată că $\{\{a+b\} + c\} = \{a+\{b+c\}\}$

$$\Rightarrow (1) = (2) \quad \forall a, b, c \in G$$

$\Rightarrow " * "$ e asociativă

"*" e comutativă!

$$x * 0 = \{x+0\} = \{x\} = x = 0 * x \quad (\forall x \in G) \Rightarrow 0 \text{ e element neutru pt *} \quad x \in \{0, 1\}$$

Fie $x, y \in G$ a.i. $x * y = 0 \Rightarrow 3x + y = 0 \Rightarrow x + y \in \mathbb{Z}$
 $x, y \in [0, 1] \Rightarrow 0 \leq x + y \leq 2$

$$\Rightarrow x + y \in \{0, 1\}$$

Dc $x + y = 0 \Rightarrow x = -y = 0$ (0 este inversul lui 0)

Dc $x + y = 1 \Rightarrow y = 1 - x$ (x este inversul lui $1-x$ ($\forall x \in G \setminus \{0\}$))

$\Rightarrow U(G) = G \Rightarrow (G, *)$ e grup abelian

Prb 3 "Calculati" toate morfismele de grupuri dintre:

$(\mathbb{Z}, +)$ și $(\mathbb{Z}, +)$; $(\mathbb{Z}, +)$ și $(\mathbb{Q}, +)$; $(\mathbb{Q}, +)$ și $(\mathbb{Z}, +)$

$(\mathbb{Z}_m, +)$ și $(\mathbb{Z}_n, +)$; $(\mathbb{Z}_m, +)$ și $(\mathbb{Z}_{m'}, +)$ unde $m, n \in \mathbb{N}$, $m, m' \geq 2$.

(Determinam morfismele de grupuri $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$ a.i. f să fie fct. continuă)

$f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ morfism de gr. $\Rightarrow f(x+y) = f(x) + f(y)$

$(\Rightarrow f(0) = 0)$ $\begin{array}{l} \cancel{x=y=1} \\ \cancel{x=2, y=1} \\ \cancel{x \in \mathbb{Z}, y \in \mathbb{N}} \end{array}$ $\begin{array}{l} f(2) = f(1) + f(1) = 2f(1) \\ f(3) = f(2) + f(1) = 2f(1) + f(1) = 3f(1) \\ \text{dsm. că } f(n) = nf(1) \end{array}$ $\begin{array}{l} f(x_1 + \dots + x_n) \\ f(x_1) + \dots + f(x_n) \end{array}$

Prim ind. după $n \in \mathbb{N}$ se

$$n \in \mathbb{N}^* \quad f(-n) = ? \quad \begin{array}{l} f(0) = f(n+(-n)) \\ \parallel \\ 0 \end{array} \quad \begin{array}{l} \Downarrow \\ f(n) + f(-n) = 0 \end{array} \Rightarrow$$

$$f(-n) = -f(n) = -nf(1)$$

$$\Rightarrow f(k) = kf(1) \Leftrightarrow k \in \mathbb{Z} \Rightarrow f \in \text{perf. det. de } f|_{\mathbb{N}}$$

Toate morf. de gr. de la $(\mathbb{Z}, +)$ în $(\mathbb{Z}, +)$ sunt date: $a \in \mathbb{Z}$

$$f_a: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +) \quad f_a(k) = ka \quad (\forall k \in \mathbb{Z})$$

Generalizare Fie $(G, +)$ un grup abelian. Morfisme de grupuri

de la $(\mathbb{Z}, +)$ în $(G, +)$ sunt date de:
 $(a \in G$ oricare)

$$f_a: (\mathbb{Z}, +) \rightarrow (G, +) \quad f_a(k) = ka \quad (\forall k \in \mathbb{Z})$$

$$(k \in \mathbb{N}^* \quad ka = \underbrace{a + \dots + a}_{k \text{ ori}} \quad ; \quad k < 0, k \in \mathbb{Z} \quad ka = \underbrace{(-a) + \dots + (-a)}_{-k \text{ ori}})$$

Fie $h: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}, +)$ morf. de grupuri. $h(x+y) = h(x) + h(y)$

La fel ca mai sus

$$h(k) = kh(1) \quad (\forall k \in \mathbb{Z})$$

$$(\exists x, y \in \mathbb{Q})$$

Ex $h\left(\frac{1}{2} + \frac{1}{2}\right) = h(1)$
 $x=y=\frac{1}{2}$ $h\left(\frac{1}{2}\right) + h\left(\frac{1}{2}\right) = 2h\left(\frac{1}{2}\right)$

$$\Rightarrow h\left(\frac{1}{2}\right) = \frac{1}{2}h(1)$$

Fie $g \in \mathbb{Q}^*$ $\Rightarrow g = \frac{a}{b}$ $b \neq 0, a \in \mathbb{Z}, b \in \mathbb{N} \quad (a, b) = 1$

$$h\left(b \cdot \frac{a}{b}\right) = h\left(\underbrace{\frac{a}{b} + \dots + \frac{a}{b}}_{b \text{ ori}}\right) \stackrel{\substack{\text{morf} \\ (b \in \mathbb{N})}}{=} h\left(\frac{a}{b}\right) + \dots + h\left(\frac{a}{b}\right) = b h\left(\frac{a}{b}\right)$$

$$\stackrel{||}{\Rightarrow} h(a) = \underbrace{ah(1)}_{a \in \mathbb{Z}}$$

$$h(g) = g h(1) \quad (\forall g \in \mathbb{Q})$$

$$bh\left(\frac{a}{b}\right) = ah(1) \Rightarrow h\left(\frac{a}{b}\right) = \frac{a}{b}h(1) \stackrel{\substack{a \in \mathbb{Q}^* \\ b \in \mathbb{N}}}{\text{oarecare}}$$

\Rightarrow Orice morfism de gr. de la $(\mathbb{Q}, +)$ în $(\mathbb{Q}, +)$ este de forma
 $f_a: (\mathbb{Q}, +) \rightarrow (\mathbb{Q}, +) \quad h_a(g) = ag \quad (\forall g \in \mathbb{Q}) \quad (a = h(1))$

Q1 Există o generalizare identică cu cea de mai sus în

casul $(\mathbb{Z}, +)$? **NU**

Def. morfismele de grupuri între 2 grupuri oarecare?

Q2 Există morfisme de grupuri între 2 grupuri oarecare. Funcție

Obs Fie $(G_1, *)$, (G_2, \circ) 2 grupuri oarecare. Funcție **DA**
 $\varphi: (G_1, *) \rightarrow (G_2, \circ)$ $\varphi(g) = s_{G_2} \quad (\forall g \in G_1)$ este un morfism
de grupuri, numit și morfismul trivial.

Singurul morfism de grupuri de la $(\mathbb{Q}, +)$ în $(\mathbb{Z}, +)$ e

morfismul trivial. \dagger

Fie $\varphi: (\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +)$ un morfism de grupuri \Rightarrow
 $\Rightarrow \varphi = h_a$ cu $a \in \mathbb{Z}$ (deoarece $h_a(1) = a \in \mathbb{Z}$) $\begin{pmatrix} \text{morf.} \\ \text{trivial} \\ \text{et } h_a \end{pmatrix}$

Dacă $a \neq 0$ $\varphi\left(\frac{1}{2a}\right) = h_a\left(\frac{1}{2a}\right) = \frac{a}{2a} = \frac{1}{2} \notin \mathbb{Z} \Rightarrow$

\Rightarrow Nu există morfism de activitate de la $(\mathbb{Q}, +)$ în $(\mathbb{Z}, +)$.

Fie $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$

f continuă.

$$f(x+y) = f(x) + f(y) \quad \forall x, y \in \mathbb{R}$$

P Orice nr. real poate fi scris ca limita unei siruri de nr. rationale.

La fel $f(q) = \lim_{n \rightarrow \infty} f(q_n)$ unde $q_n \in \mathbb{Q}$.

Fie $a \in \mathbb{R}$ și $(q_m)_m$ un sir de nr. reale. a.i. $\lim_{m \rightarrow \infty} q_m = a$.

$$\lim_{m \rightarrow \infty} f(q_m) = f\left(\lim_{m \rightarrow \infty} q_m\right) = f(a)$$

$\| q_m \in \mathbb{Q}$

continuă

$$\Rightarrow f(a) = a f(1)$$

$$\lim_{n \rightarrow \infty} (q_n f(1)) = f(1) \cdot \left(\lim_{n \rightarrow \infty} q_n\right) = f(1) \cdot a$$

$\| a \in \mathbb{R}$