Bârdilă Mihai-Andrei, Gr. 1, An 1, INFO ID, 22.01.2022

EXAMEN SAI

1) a) $\overline{100}^{-1} = ?$ în $(\mathbb{Z}_{149}, +)$

$\bar{a}^{-1} = (-\bar{a}) \Rightarrow \overline{100}^{-1} = -\overline{100}$

$\overline{100}^{-1} = \overline{49}$ inv = $\overline{49}$

b) $\overline{100}^{-1} = ?$ în $(U(\mathbb{Z}_{149}), \cdot)$

$149 = 100 \cdot 1 + 49$

$100 = 49 \cdot 2 + 2$

$49 = 2 \cdot 24 + 1$

$2 = 1 \cdot 2 + 0$

$\Rightarrow \frac{A}{B} = 49 + \frac{1}{2 + \frac{1}{1}}$

$\frac{A}{B} = 49 + \frac{1}{3} = \frac{148}{3}$

$\frac{n}{a} - \frac{A}{B} = \frac{(-1)^{Nr.op+1}}{a \cdot B}$

$\frac{149}{100} - \frac{148}{3} = \frac{(-1)^4}{100 \cdot 3} \Rightarrow \frac{149 \cdot 3}{=0} - \overline{148} \cdot 100 = 1 \pmod{149}$

$-\overline{147} \cdot \overline{100} = 1 \Rightarrow$ inv lui $\overline{100}$ în $(U(\mathbb{Z}_{149}), \cdot) = \overline{148}$

c) inversa $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ în $(S_4, \circ)$

$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \\ 1 & 2 & 3 & 4 \end{pmatrix}$

$= \begin{pmatrix} 2 & 1 & 4 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ ordonez

$\Rightarrow \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ (inversa)

2) a) $x \in \{0, 1, 2, 3, \dots, 69\}$

a ?

$$\begin{cases} x \equiv 0 \pmod 2 \Rightarrow x \in \{0,2,4,6,8,10,12,\dots,68\} \\ x \equiv 1 \pmod 5 \Rightarrow x \in \{6,16,26,36,46,56,66\} \\ x \equiv 3 \pmod 7 \Rightarrow x \in \{66\} \end{cases}$$

$\Rightarrow x = 66 \equiv 0 \pmod 2 \equiv 1 \pmod 5 \equiv 3 \bmod (7)$

c) ultimele 2 cifre 83^{81} ?

2 cifre $\Rightarrow$ calculez în $\mathbb{Z}_{100}$, aplic Euler

$(83, 100) = 1 \Rightarrow 83^{\varphi(100)} \equiv 1 \pmod{100}$

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

$\Rightarrow \overline{83}^{40} \equiv 1 \bmod (100)$

$\overline{83}^{81} = \overline{83}^{80+1} = \overline{83}^{80} \cdot \overline{83} = \overline{1} \cdot \overline{83}$

$\overline{83}^{81} = \overline{83} \cdot 1 \pmod{100} \Rightarrow$ ultimele 2 cifre sunt 83

b) $16! + 1$ în $\mathbb{Z}_{19}$

$\overline{16!} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \overline{4} \cdot \overline{5} \cdot \dots \cdot \overline{16}$ în $\mathbb{Z}_{19}$

$= \overline{6} \cdot \overline{20} \cdot \overline{42} \cdot \overline{72} \cdot \overline{110} \cdot \overline{156} \cdot \overline{210} \cdot \overline{16}$

$= \overline{6} \cdot \overline{1} \cdot \overline{4} \cdot \overline{15} \cdot \overline{15} \cdot \overline{4} \cdot \overline{1} \cdot \overline{16}$

$= \overline{24} \cdot \overline{15} \cdot \overline{60} \cdot \overline{16}$

$= \overline{5} \cdot \overline{15} \cdot \overline{3} \cdot \overline{16}$

$= \overline{5} \cdot (\overline{-4}) \cdot \overline{3} \cdot (\overline{-3}) = (\overline{-20}) \cdot (\overline{-9}) = (\overline{-1}) \cdot (\overline{-9}) = \overline{9}$ în $\mathbb{Z}_{19}$

$16! \equiv 9 \pmod{19}$

$\Rightarrow 16! + 1 = 10$ în $\mathbb{Z}_{19}$

3. a) $\det \begin{vmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{5} & \bar{6} & \bar{7} \\ \bar{8} & \bar{2} & \bar{15} \end{vmatrix} = ?$ din $M_3(\mathbb{Z}_{17})$

Sarrus $\Rightarrow$ $\begin{vmatrix} \bar{1} & \bar{1} & \bar{1} \\ \bar{5} & \bar{6} & \bar{7} \\ \bar{8} & \bar{2} & \bar{15} \\ \bar{1} & \bar{1} & \bar{1} \\ \bar{5} & \bar{6} & \bar{7} \end{vmatrix}$ $\Rightarrow \det = \bar{1}\cdot\bar{6}\cdot\bar{15} + \bar{5}\cdot\bar{2}\cdot\bar{1} + \bar{8}\cdot\bar{1}\cdot\bar{7} - \bar{1}\cdot\bar{6}\cdot\bar{8} - \bar{7}\cdot\bar{2}\cdot\bar{1} - \bar{15}\cdot\bar{1}\cdot\bar{5}$

$\det = \bar{90} + \bar{10} + \bar{56} - \bar{48} - \bar{14} - \bar{75}$

$= \bar{156} - \bar{48} - \bar{14} - \bar{75}$

$= \bar{108} - \bar{14} - \bar{75} = \bar{94} - \bar{75} = \bar{19} \equiv 2 \pmod{17}$

$\Rightarrow \det = \bar{2}$

c) rădăcinile lui $x^3 - 1$ în $\mathbb{Z}_{97}$

$x^3 - 1 = 0$

$(x-1)(x^2+x+1) = 0$

fie $x - 1 = 0$ fie $x^2 + x + 1 = 0$

i) $x - 1 = 0 \Rightarrow x = 1$

ii) $x^2 + x + \bar{1} = \bar{0} \quad |\cdot 4$

$\bar{4}x^2 + \bar{4}x + \bar{4}$

$(a+b)^2 = a^2 + 2ab + b^2$ $\Rightarrow (2x+1)^2 + \bar{3} = \bar{0}$

$(2x+1)^2 = -\bar{3}$

$\Rightarrow (2x+1)^2 = \bar{94} \pmod{97}$

$\Rightarrow$ rădăcina lui $x^3 - 1$ în $\mathbb{Z}_{97}$ este 1

4) c) nr prime p.t. $5^{p-1} + 3^{p-2} + 2^{p-3} \equiv 42 \pmod p$

Mica Teoremă a lui Fermat: p - prim, $p \nmid a \in \mathbb{Z}$, $p \nmid a$ $\Rightarrow a^{p-1} \equiv 1 \pmod p$

$5^{p-1} + 3^{p-1-1} + 2^{p-1-2} \equiv 42 \ (p)$

$5^{p-1} + \frac{3^{p-1}}{3} + 2^{p-1} : 2^2 \equiv 42 \ (p)$

$1 + \frac{1}{3} + \frac{1}{4} \equiv 42 \ (p)$

$12 + 4 + 3 \equiv 42 \cdot 12 \ (p)$

$19 \equiv 504 \ (p)$

$p \mid 504 - 19 \Rightarrow p \mid 482$

$p \in \{1, 2, 241, 482\}$ | $\Rightarrow$ numerele prime $p \in \{241\}$

nr prime | $\Rightarrow p = 241$