1342b

## Aritmetică modulară (în $\mathbb{Z}_n$)

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$(\mathbb{Z}_n, +, \cdot)$ inel comutativ

$\rightarrow (\mathbb{Z}_n, +)$ grup comutativ

$\rightarrow (\mathbb{Z}_n^*, \cdot)$ monoid comutativ

$U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid x \text{ este inv. față de } \cdot\}$

$U(\mathbb{Z}_n) \neq \mathbb{Z}_n$

Ex: $\mathbb{Z}_7 = \{0, 1, 2, \dots, 6\}$

$-3$ = opusul lui $3 = x$ pt care $x + 3 = 0$

$-3 = 4$

$3^{-1}$ = inversul lui $3 = y$ pt care $3 \cdot y = 1$

$3^{-1} = 5$ pt că $3 \cdot 5 = 15 = 1$.

Teoremă: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cmmdc}(x, n) = 1\}$

Obs: $(U(\mathbb{Z}_n), \cdot)$ grupul unităților

$Z_{10}$ $U(Z_{10}) = \{1, 3, 7, 9\}$

$4^{-1}$ nu există

$3^{-1} = 7$ pt că $3 \cdot 7 = 21 = 1 \mod 10$

---

$Z_{26}$ $Z_{29}$

| A | B | C | D | ... | Z | ↳ | . | ? |
|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | | 25 | 26 | 27 | 28 |

$5x + 2 = 1$ în $Z_7$

$5x = -1 \quad | \cdot 5^{-1} = 3$

$5^{-1} \cdot 5 \cdot x = (-1) \cdot 5^{-1}$

$x = (-1) \cdot 3 = -3 = 4$

---

$3x^2 + x - 2 = 0$ în $Z_{11}$

$\Delta = 1 - 4 \cdot (-2) \cdot 3 = 1 + 24 = 25 = 3$

$\sqrt{a} = b \Leftrightarrow a = b^2$

$\sqrt{3}$ în $Z_{11} = \{5, 6\} = \{5, -5\}$

$$x_{1,2} = \left(-1 \pm \sqrt{\Delta}\right) \cdot 6^{-1}$$

$\sqrt{3} = 5 \Rightarrow x_1 = (-1+5) \cdot 6^{-1} = 4 \cdot 2 = 8$

$x_2 = (-1-5) \cdot 6^{-1} = -6 \cdot 2 = -12$

$= -11 - 1 = -1 = 10$

$\Rightarrow x \in \{8, 10\}$

---

## Logaritmul discret

$$\log_a b = c \Rightarrow a^c = b$$

$\log_2 3 \in \mathbb{Z}_5 = x \Leftrightarrow 2^x = 3 \in \mathbb{Z}_5$

$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 8 = 3$

$\Rightarrow \log_2 3 = 3 \in \mathbb{Z}_5$

D-H: $\log_{7131}{}_{\underset{x}{\shortparallel}}\ 5247 \in \mathbb{Z}_{21733}$

$\Rightarrow 7131^x = 5247 \bmod 21733$

# Teorema lui Lagrange

$(G, \cdot)$ grup, $\#G = n$

$\forall g \in G, \; g^n = e.$

---

$g^{52}$ în $\mathbb{Z}_{11}$

$g^{52} = (g^2)^{26} = (81)^{26} = 4^{26} = (4^2)^{13}$

$= 5^{13} = (5^2)^6 \cdot 5 = 3^6 \cdot 5 = (3^3)^2 \cdot 5$

$= 5^2 \cdot 5 = 3 \cdot 5 = 4.$

---

$A \in \mathcal{M}_n(\mathbb{Z}_t) \quad A^{-1} = (\det A)^{-1} \cdot A^*$ există

$\Leftrightarrow (\det A)^{-1}$ există $\Leftrightarrow \text{cmmdc}(\det A, t) = 1.$