1343b — Aritmetică modulară (în $\mathbb{Z}_n$)

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

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

$\to (\mathbb{Z}_n, \cdot)$ monoid comutativ

Ex: $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$

$-a$ = opusul elem. a

= simetricul în raport cu „+"

$-3 = x$ pt care $3 + x = 0 \Rightarrow -3 = 4$

a^{-1} = inversul elem. a

= simetricul față de „·"

$3^{-1} = x$ pt care $3x = 1 \Rightarrow 3^{-1} = 5 \Rightarrow 5^{-1} = 3$

$2^{-1} = 4 \Rightarrow 4^{-1} = 2$; $6^{-1} = 6$

$\mathbb{Z}_{10} = \{0, 1, \dots, 9\}$

$3^{-1} = 7$; 5^{-1} nu există

Def: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{există } x^{-1}\}$ = grupul unităților

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

$U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$ $\quad$ $3^{-1} = 7 \Rightarrow 7^{-1} = 3$

$1^{-1} = 1$; $9^{-1} = 9$

$(U(\mathbb{Z}_{n}), \cdot)$ grup comutativ.

Ec. de gradul I

- $3x + 2 = 1$ în $\mathbb{Z}_7$

$$3x = 1 - 2 = -1 = 6 \Rightarrow x = 2$$

sau: $3x = -1 \mid \cdot 3^{-1}$

$$3^{-1} \cdot 3 \cdot x = (-1) \cdot 3^{-1}$$

$$x = (-1) \cdot 5 = -5 = 2$$

- $\boxed{4}x - 1 = 5$ în $\mathbb{Z}_{10}$ nu are sol. pt că $4 \notin U(\mathbb{Z}_{10})$.

- $4x + 1 = 5$ în $\mathbb{Z}_{10}$

$4x = 4 \boxed{\Rightarrow} x = 1$ NU

Ec. de gradul II

- $2x^2 - 5x + 1 = 3$ în $\mathbb{Z}_{11}$

$$2x^2 - 5x - 2 = 0$$

$\Delta = 25 - \underbrace{4 \cdot 2 \cdot (-2)} = 3 + 5 = 8$

$\sqrt{8} = a \Leftrightarrow a^2 = 8$

$0^2 = 0$; $1^2 = 1$; $2^2 = 4$; $3^2 = 9$; $4^2 = 5$; $5^2 = 3$; $6^2 = 3$;

$7^2 = 5$; $8^2 = 9$; $9^2 = 4$; $10^2 = 1$

$\Rightarrow \sqrt{8}$ nu există în $\mathbb{Z}_{11}$ $\Rightarrow$ ec. nu are sol.

- $x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{13}$

$\Delta = 25 - 24 = 1 \Rightarrow \sqrt{\Delta} = \{1, 12\} = \{1, -1\}$

$x_{1,2} = (5 \pm \sqrt{1}) \cdot 2^{-1}$

$x_1 = 6 \cdot 7 = 42 = 3$

$x_2 = 4 \cdot 7 = 28 = 2$

$\Rightarrow x \in \{2, 3\}$.

<u>Logaritmul discret</u>

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

$\log_2 3$ în $\mathbb{Z}_5$ $\Rightarrow 2^x = 3$ în $\mathbb{Z}_5$

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

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

$\log_2 3$ în $\mathbb{Z}_7 \Rightarrow 2^x = 3$ în $\mathbb{Z}_7$

$\underbrace{2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;}\ \underbrace{2^3 = 1;\ 2^4 = 2;\ 2^5 = 4}$

$\Rightarrow$ nu există.

$\log_a b$ în $\mathbb{Z}_n \Leftrightarrow a^x = b$ în $\mathbb{Z}_n$, $x \in \{0, 1, \dots, n-1\}$

Teorema lui Lagrange pt grupuri

$(G, \cdot)$ grup, $g \in G$ / $\Rightarrow g^n = e$.

Dacă $\#G = n$

Obs: $(\mathbb{Z}_p^*, \cdot)$ grup $\#\mathbb{Z}_p^* = p - 1$.

p nr. prim

$(\mathbb{Z}_{23}^*, \cdot)$ $\log_5 11$ în $\mathbb{Z}_{23}$

$5^x = 11$ în $\mathbb{Z}_{23}$, $x \in \{0, \dots, 22\}$

4^{100} în $\mathbb{Z}_{11} = ?$

$4^{100} = (4^2)^{50} = (16)^{50} = 5^{50} = (5^2)^{25} = 1^{25} = 1$

$= 3^{25} = (3^5)^5$

$3^5 = \underbrace{3^2 \cdot \underbrace{3^2 \cdot 3}_{5}} = 1$

$A \in \mathcal{M}_n(\mathbb{Z}_t)$

$A^{-1} = (\det A)^{-1} \cdot A^*$ există $\Leftrightarrow$ $\det A$ este element inversabil în $\mathbb{Z}_t$ $\Leftrightarrow$ $\det A \in U(\mathbb{Z}_t) \Leftrightarrow$

$\text{cmmdc}(\det A, t) = 1$