1342a - Aritmetică modulară (în Z_n)

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$(Z_n, +, \cdot)$ inel comutativ

$\rightarrow (Z_n, +)$ grup comutativ

$\rightarrow (Z_n, \cdot)$ monoid comutativ

Ex: $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$0 = \{0, \pm 7, \pm 14, \pm 21, \pm 28, \ldots\} = \{7k \mid k \in Z\}$

$1 = \{1, 8, 15, 22, 29, \ldots\} = \{7k+1 \mid k \in Z\}$

$-a$ = opusul elementului a

= simetricul față de $+$

$-3 = x \Leftrightarrow x + 3 = 0 \Rightarrow -3 = 4$

a^{-1} = inversul el. a

= simetricul față de $\cdot$.

$3^{-1} = y \Leftrightarrow 3y = 1 \Rightarrow y = 3^{-1} = 5 \Rightarrow 5^{-1} = 3$

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

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

↑ grupul unităților $(U(\mathbb{Z}_n), \cdot)$ grup com.

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

Ex: $U(\mathbb{Z}_7) = \mathbb{Z}_7^* = \mathbb{Z}_7 - \{0\}$

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

$3^{-1} = 7 \Rightarrow 7^{-1} = 3 \; ; \; 9^{-1} = 9$

Ec. de gradul I

$2x + 5 = 1$ în $\mathbb{Z}_7$

$2x = 1 - 5 = -4 \longrightarrow x = -2 = 5$

$\downarrow$

$2x = 3 \quad | \cdot 2^{-1} \Leftrightarrow \underbrace{2^{-1} \cdot 2}_{1} \cdot x = 2^{-1} \cdot 3$

$1 \cdot x = x = 4 \cdot 3 = 12 = 5$

$2x + 5 = 1$ în $\mathbb{Z}_6$ nu are soluție.

$U(\mathbb{Z}_6) = \{1, 5\} \neq 2$

Ec de gradul al II-lea

$3x^2 - 2x + 4 = 1$ în $\mathbb{Z}_7$

$3x^2 - 2x + 3 = 0$

$\Delta = 4 - 4 \cdot 3 \cdot 3 = 4 - 36 = -32 = -28 - 4 \overset{!!}{=} 0$

$= -4 = 3$

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

$\sqrt{3} = a$ în $\mathbb{Z}_7 \Leftrightarrow a^2 = 3$ în $\mathbb{Z}_7$

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

$\Rightarrow \sqrt{3}$ nu există în $\mathbb{Z}_7 \Rightarrow$ ec. nu are sol.

$x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{11}$

$\Delta = 25 - 4 \cdot 6 = 1$

$\sqrt{1} \in \{1, 10\} = \{1, -1\}$

$x_{1,2} = (5 \pm \sqrt{1}) \cdot 2^{-1} = (5 \pm 1) \cdot 6$

$x_1 = 6 \cdot 6 = 3\ ;\ x_2 = 4 \cdot 6 = 2$

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

Logaritmul discret

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

$\log_2 3$ în $\mathbb{Z}_5$ $= x \in \mathbb{Z}_5$, $2^x = 3$ 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 $\mathbb{Z}_7$ nu există

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

Teorema lui Lagrange (pt grupuri)

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

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

Obs: $(\mathbb{Z}_p^*, \cdot)$ grup

p nr prim

În plus, $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

În $\mathbb{Z}_{11}$, $4^{50} = ?$

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

$5^5 = 5^2 \cdot 5^2 \cdot 5 = 3 \cdot 3 \cdot 5 = 1$

$3 \cdot 3 = 4$

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

$A^{-1} = (\det A)^{-1} \cdot A^*$ există $\Leftrightarrow$

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

$\Leftrightarrow$, $\det A \in U(\mathbb{Z}_t)$.