1343a - Aritmetică modulară (în $\mathbb{Z}_n$)

$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$

$(\mathbb{Z}_n, +, \cdot)$ 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 lui $a \in \mathbb{Z}_7$

= simetricul față de $+$

$-a = b \Leftrightarrow a + b = 0$

$-3 = x \Leftrightarrow x + 3 = 0$ în $\mathbb{Z}_7 \Rightarrow x = 4$

$\Leftrightarrow -4 = 3$

$-2 = 5$ pt că $2 + 5 = 7 = 0$ în $\mathbb{Z}_7$

a^{-1} = inversul lui $a \in \mathbb{Z}_7$

= simetricul față de $\cdot$

$3^{-1} = x \Leftrightarrow 3 \cdot x = 1$

$x = 5$ pt că $3 \cdot 5 = 15 = 1$

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

$2^{-1} = 4$ pt că $2 \cdot 4 = 8 = 1$

$1^{-1} = 1$

$6^{-1} = 6$

$\Rightarrow (\mathbb{Z}_7 - \{0\}, \cdot)$ grup com.

<u>Teoremă</u>: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \exists x^{-1}\}$

grupul unităților

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

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

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

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$(U(\mathbb{Z}_{10}), \cdot)$ grup com.

Ec. de gradul I în $\mathbb{Z}_n$

$3x + 2 = 1$ în $\mathbb{Z}_7$

$3x = -1$

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

$$\underbrace{5 \cdot 3} \cdot x = -1 \cdot 5$$

$$x = -5 = 2$$

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

$2x - 1 = 5$ în $\mathbb{Z}_{10}$ $\quad U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

$$\Updownarrow$$

$$2x = 6 \quad | \cancel{\cdot 2^{-1}}$$

obs: $x = 3$ din tabla înmulțirii

$\cdot$	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8

Ex. $2x = 3$ în $\mathbb{Z}_{10}$ nu are sol.

Ec. de gradul II

- $2x^2 - 5x + 1 = 3$ în $\mathbb{Z}_7$

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

$$\Delta = (-5)^2 - 4 \cdot 2 \cdot (-2) = 4 + 2 = 6$$

$\sqrt{6}$ în $\mathbb{Z}_7 = a \Leftrightarrow a^2 = 6$

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

$\Rightarrow \sqrt{6}$ nu există în $\mathbb{Z}_7 \Rightarrow$ ec. nu are sol.

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

$\Delta = 25 - 24 = 1$

$\sqrt{\Delta} = \sqrt{1} = \{1, 12\} = \{1, -1\}$

$0 = -26 - 10 = 11$

$x_1 = (5+1) \cdot 2^{-1} = 6 \cdot 7 = 6 \cdot (-6) = -36$
$= -10 = 3$

$x_2 = (5-1) \cdot 2^{-1} = 4 \cdot 7 = 28 = 2$

4^{100} în $\mathbb{Z}_{11} = ?$

$(4^2)^{50} = 5^{50} = (5^2)^{25} = 3^{25} = (3^5)^5 = 1^5 = 1$

$3^5 = 3^2 \cdot \underbrace{3^2 \cdot 3}_{5} = 9 \cdot 5 = 1$

Logaritmul discret

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

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

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

$\log_2 3$ în $\mathbb{Z}_7$ nu există.

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

$\log_a b$ în $\mathbb{Z}_n$

Teorema lui Lagrange pt grupuri

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

Fie $g \in G. \Rightarrow g^n = e.$

$(\mathbb{Z}_7^*, \cdot)$, $g^6 = 1$, $\forall g \in \mathbb{Z}_7^*$

grup.

Inverse matriceale

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

$\det A \in \mathcal{U}(\mathbb{Z}_t) \Leftrightarrow \text{cmmdc}(\det A, t) = 1.$

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