13.11.16

Aritmetică modulară

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

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

$\Leftrightarrow$ 1) $(\mathbb{Z}_n, +)$ grup comutativ

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

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

$(\mathbb{Z}_7, +)$ $-2 = x \Leftrightarrow \underline{x + 2 = 0} \Rightarrow x = 5$

În particular, $-5 = 2$

$(\mathbb{Z}_7, +)$ grup com. $\Leftrightarrow \forall x \in \mathbb{Z}_7$, există $-x$.

$(\mathbb{Z}_7, \cdot)$ $3^{-1} = y \Leftrightarrow 3 \cdot y = 1 \Rightarrow y = 5$

În particular, $5^{-1} = 3$

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

$(\mathbb{Z}_{10}, +, \cdot)$ $-6 = 4$ pt că $6 + 4 = 10 = 0$

6^{-1} nu există.

Teorema: În $\mathbb{Z}_n$, x^{-1} există $\Leftrightarrow$ $\text{cmmdc}(x, n) = 1$.

pt. $\mathbb{Z}_n$ se notează $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \exists x^{-1}\} = \{x \in \mathbb{Z}_n \mid (x, n) = 1\}$

↑ grupul unităților

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

Ec. de gradul I în $\mathbb{Z}_n$

$2x + 5 = 3$ în $\mathbb{Z}_7$

$2x = 3 - 5 = -2$

- $2x = -2 \Rightarrow x = -1 = 6$
- $2x = -2 = 5 \mid \cdot 2^{-1} = 4$

$4 \cdot 2 \cdot x = 4 \cdot 5$

$1 \cdot x = x = 20 = 6$

Ec. de gradul II în $\mathbb{Z}_n$

- $3x^2 - 5x + 1 = 0$ în $\mathbb{Z}_{11}$

$\Delta = 25 - 4 \cdot 1 \cdot 3 = 25 - 12 = 13 = 2$

$\sqrt{2} = ?$ în $\mathbb{Z}_{11}$

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

$\sqrt{2} \in \mathbb{Z}_4$ $\quad \sqrt{2} = a \in \mathbb{Z}_4 \Leftrightarrow a^2 = 2$

$\sqrt{2}$ nu există $\Rightarrow$ Ec. nu are soluții.

- $x^2 + 3x - 4 = 0 \in \mathbb{Z}_7$

$\Delta = 9 + 16 = 25 = 4$

$\sqrt{4} \in \mathbb{Z}_7 = \{2, 5\} = \{2, -2\}$

$x_{1,2} = (-3 \pm \sqrt{\Delta}) \cdot 2^{-1}$

$2^{-1} = 4$

$x_1 = (-3+2) \cdot 4 = -1 \cdot 4 = -4 = 3$

$x_2 = (-3-2) \cdot 4 = -5 \cdot 4 = -20 = \underbrace{-14}_{0} - 6 = 1$

$x_3 = (-3+5) \cdot 4 = 2 \cdot 4 = 8 = 1$

$x_4 = (-3-5) \cdot 4 = -8 \cdot 4 = -32 = \underbrace{-28}_{0} - 4 = 3$

Logaritmul discret

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

$\log_2 5$ în $\mathbb{Z}_7$ nu există

$\exists x \in \mathbb{N}$ cu $2^x = 5$ în $\mathbb{Z}_7$

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

$2^0 = 1$

$(\mathbb{Z}_7^*, \cdot)$

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

$\log_3 5$ în $\mathbb{Z}_7$

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

$3^5 = 5$

$\Rightarrow \boxed{\log_3 5 = 5}$

---

g^{45} în $\mathbb{Z}_{11} = (g^5)^9 = (g^2 \cdot g^2 \cdot g)^9$

$= (81 \cdot 81 \cdot g)^9 = (4 \cdot 4 \cdot g)^9 = 1^9 = 1.$

$5 \quad 1$

Teorema lui Lagrange

G grup cu n elemente, $g \in G$

$\Rightarrow g^n = el.\ neutru.$

$\mathbb{Z}_{29}$

A	B	C	D	...	Z	␣	.	?
0	1	2	3		25	26	27	28

$A \in \mathcal{M}_n(\mathbb{R})$ $A^{-1} = \frac{1}{\det A} \cdot A^*$ ~~ox, 5tq~~

$\Leftrightarrow \det A \neq 0.$