13.4.16

Aritmetică în $\mathbb{Z}_n$

Ecuații de gradul I $\rightarrow$ CAESAR AFIN

Ex: $5x+1=3$ în $\mathbb{Z}_7$

$5x = 3-1 = 2 \mid \cdot 5^{-1} = 3$

$\underbrace{5\cdot 3}_{1}\cdot x = 2\cdot 3 \Rightarrow \underline{x=6}$

Ex: $6x+2=1$ în $\mathbb{Z}_{10}$

$6x = 1-2 = -1 = 9 \mid \cdot 6^{-1}$ NU există în $\mathbb{Z}_{10}$

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

$6x=9$ rezolv prin încercări

x	0	1	2	3	4	5	6	7	8	9
$6x$	0	6	2	8	4	0	6	2	8	4

$\Rightarrow$ ec. nu are sol.

Sisteme liniare

Ex: $\begin{cases} 2x+3y=1 \\ 5x-y=2 \end{cases}$ în $\mathbb{Z}_7$

Matricea sistemului: $A = \begin{pmatrix} 2 & 3 \\ 5 & -1 \end{pmatrix} \in M_2(\mathbb{Z}_7)$

$\det A = -2 - 15 = -17 = -\underset{\overset{\shortparallel}{0}}{14} - 3 = -3 = 4 \in U(\mathbb{Z}_7)$

$\Rightarrow$ sistem Cramer $\Rightarrow$ sol. unică.

$$\begin{cases} 2x + 3y = 1 \\ 5x - y = 2 \mid \cdot 3 \end{cases} \Rightarrow \begin{cases} 2x + 3y = 1 \\ 15x - 3y = 6 \end{cases} \; (+) \Rightarrow 17x = 7$$

$3x = 0$

$\Rightarrow \underline{x = 0}$

$5 \cdot 0 - y = 2 \Rightarrow \underline{y = -2 = 5}$

Ex: $\begin{cases} 2x + y = 3 \\ 4x + 2y = 1 \end{cases}$ în $\mathbb{Z}_{11}$

$A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_{11}) \Rightarrow \det A = 0 \Rightarrow$ sist. nu este Cramer.

$$\begin{cases} 2x + y = 3 \mid \cdot 2 \\ 4x + 2y = 1 \end{cases} \Rightarrow \begin{cases} 4x + 2y = 6 \\ 4x + 2y = 1 \end{cases} \; (-)$$

$\Rightarrow 0 = 5 \Rightarrow$ incompat.

Def: $a \mid b$ în $X \Leftrightarrow \exists\, c \in X$ a.î. $a \cdot c = b$

Ecuații de gradul II

Ex: $3x^2 - x + 2 = 0$ în $\mathbb{Z}_7$

$a = 3$; $b = -1$; $c = 2$

$\Delta = b^2 - 4ac = 1 - 4 \cdot 2 \cdot 3 = 1 - 24 = -23 = \underset{\overset{\shortparallel}{0}}{-21} - 2$

$= -2 = 5$

$\exists \sqrt{5}$ în $\mathbb{Z}_7$? $\sqrt{5} = y \Leftrightarrow y^2 = 5$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ $\quad P(\mathbb{Z}_7) = \{0, 1, 4, 2\} \not\ni 5$

pătratele

$\Rightarrow \nexists \sqrt{5}$ în $\mathbb{Z}_7 \Rightarrow$ nu are soluții.

Ex: $x^2 - 5x + 7 \overset{\text{în } \mathbb{Z}_{11}}{=} 1 \Leftrightarrow x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{11}$

$a = 1$; $b = -5$; $c = 6$ $\qquad 2^{-1}$ în $\mathbb{Z}_{11} = 6$

$\Delta = b^2 - 4ac = 25 - 24 = 1$

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

$x_1 = (5 + 1) \cdot 2^{-1} = 6 \cdot 6 = 36 = \overset{0}{\overset{\shortparallel}{33}} + 3 = 3$

$x_2 = (5 - 1) \cdot 2^{-1} = 4 \cdot 6 = 24 = \underset{0}{\overset{\shortparallel}{22}} + 2 = 2$

$x_3 = (5 + 10) \cdot 2^{-1} = 15 \cdot 6 = 90 = 88 + 2 = 2$

$x_4 = (5 - 10) \cdot 2^{-1} = -5 \cdot 6 = -30 = -22 - 8 = -8 = 3$

NU e nevoie

Inverse matriceale $\rightarrow$ HILL

Ex: $A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & -1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_5)$ $\quad A^{-1} = ?$ dacă există

$\det A = \underbrace{1+4}_{0} - 1 + 2 = 1 \in U(\mathbb{Z}_5)$

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

$A \rightarrow A^t = \begin{pmatrix} -1 & 0 & 1 \\ 2 & 1 & 1 \\ 1 & 2 & -1 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} -3 & +3 & 3 \\ +2 & 0 & +2 \\ -1 & +3 & -1 \end{pmatrix}$

$A^{-1} = (\det A)^{-1} \cdot A^* = 1 \cdot \begin{pmatrix} -3 & 3 & 3 \\ 2 & 0 & 2 \\ -1 & 3 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 3 \\ 2 & 0 & 2 \\ 4 & 3 & 4 \end{pmatrix}$

$$\boxed{A^{-1} \cdot A = A \cdot A^{-1} = I_3}$$

Ex: $A = \begin{pmatrix} 2 & -1 & 3 \\ 5 & 2 & 1 \\ 7 & 1 & 4 \end{pmatrix}$ în $\mathcal{M}_3(\mathbb{Z}_{11})$ $\quad A^{-1} = ?$ dacă există

$\det A = 16 - 7 + 15 - 42 - 2 + 20$

$= 5 + 4 + 4 + \cancel{2} - \cancel{2} - 2 = 11 = 0 \Rightarrow \nexists A^{-1}$

Logaritm discret → DIFFIE-HELLMAN

Def: $\log_a b = c \Leftrightarrow a^c = b$ (în $\mathbb{R}$, în $\mathbb{Z}_n$)

Ex: $\log_2 5$ în $\mathbb{Z}_7$

$\log_2 5 = x \Leftrightarrow 2^x = 5$ în $\mathbb{Z}_7$

x	0	1	2	$\boxed{3}$	4	5	6
2^x	1	2	4	$\boxed{1}$	2	4	1

$\neq 5$

$\to \operatorname{ord} 2 = 3$

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

Teorema lui Lagrange pt grupuri

G grup finit, cu n elemente.

$\forall g \in G$, $\operatorname{ord} g \mid n$

În particular, $g^n = e$, elem. neutru.

Multiplicativ, lucrăm cu $\mathbb{Z}_n^* = \mathbb{Z}_n - \{0\}$

$\# \mathbb{Z}_n^* = n-1 \Rightarrow \forall x \in \mathbb{Z}_n^*, \; x^{n-1} = 1$

Ex: $\log_3 2$ în $\mathbb{Z}_{11}$

$$\log_3 2 = x \iff 3^x = 2 \text{ în } \mathbb{Z}_{11}$$

Sol1: Calculez puteri

x	0	1	2	3	4	5	6	7	8	9	10	
3^x	1	3	9	5	4	1	3	9	5	4	1	$\neq 2$

$\to$ ord $3 = 5$ în $\mathbb{Z}_{11}$

$$3^4 = 3^3 \cdot 3 = 5 \cdot 3 = 15 = 4$$

$$3^5 = 3^4 \cdot 3 = 4 \cdot 3 = 1$$

$\Rightarrow \log_3 2$ nu există în $\mathbb{Z}_{11}$

Sol2: $3^x = 2$ în $\mathbb{Z}_{11} \iff 3^x = 11K+2$

Enumăr elem. $11K+2$ și caut o putere a lui 3

$$11K+2 = \{2, 13, 24, 35, 46, \ldots, 3^{10} \sim 50{,}000\}$$

$\uparrow$

Caut printre ele puteri ale lui 3