13426

Ecuații, sisteme, matrice în $\mathbb{Z}_n$

CAESAR
AFIN

Ec. de gradul I

Ex: $2x+5=3$ în $\mathbb{Z}_7$

$2x = 3-5 = -2 = 5$

sau $2x=-2 \Rightarrow \underline{x=-1=6}$

$2x=5$ în $\mathbb{Z}_7 \;\big|\cdot 4 = 2^{-1}$

$2\cdot 4\cdot x = 5\cdot 4 \Rightarrow x = 20 = 6 \Rightarrow \underline{x=6}$

Ex: $5x+2=1$ în $\mathbb{Z}_{10}$

$5x = 1-2 = -1 = 9 \;\big|\cdot 5^{-1}$ NU există în $\mathbb{Z}_{10}$!

Teoremă: a este inversabil în $\mathbb{Z}_n \Leftrightarrow \text{cmmdc}(a,n)=1$

$5x=9$ Rezolvăm prin încercări

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

$\neq 9 \Rightarrow$ Ec. nu are soluții

Sisteme liniare

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

Matricea sistemului $A=\begin{pmatrix} 2 & 3 \\ 5 & -1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_7)$

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

$\Rightarrow$ sist. este Cramer $\Rightarrow$ are sol. unică

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

$$\Rightarrow 17x=7 \Rightarrow 3x=0 \Rightarrow \underline{x=0}$$

$$2x+3y=1 \Rightarrow 3y=1 \mid \cdot 3^{-1}=5 \Rightarrow \underline{y=5}$$

$\underline{Ex}$: $\begin{cases} x+2y=4 \\ 3x+4y=1 \end{cases}$ în $\mathbb{Z}_{10}$

$$A=\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_2(\mathbb{Z}_{10}) \; ; \; \det A = 4-6=-2=8$$

$\det A = 8 \notin U(\mathbb{Z}_{10}) \Rightarrow \det A$ este divizor al lui zero.
$(8 \cdot 5 = 0$ în $\mathbb{Z}_{10})$

$\Rightarrow$ <u>Sist NU este Cramer.</u>

$$\begin{cases} x+2y=4 \mid \cdot 2 \\ 3x+4y=1 \end{cases} \Rightarrow \begin{cases} 2x+4y=8 \\ 3x+4y=1 \end{cases} \Big| -$$

$$\Rightarrow \underline{x=-7=3} \checkmark$$

$x+2y=4 \Rightarrow 3+2y=4 \Rightarrow 2y=1 \Rightarrow y=2^{-1}$ NU există în $\mathbb{Z}_{10}$

$\Rightarrow$ <u>Sist. nu are soluții.</u>

Ec. de gradul II

Ex: $x^2+3x-1=0$ în $\mathbb{Z}_5$

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

$\Delta=b^2-4ac=9+4=13=3$

$\exists\sqrt{3}$ în $\mathbb{Z}_5$? $\sqrt{3}=y \Leftrightarrow y^2=3$ în $\mathbb{Z}_5$ NU

$\mathbb{Z}_5=\{0,1,2,3,4\}$; $P(\mathbb{Z}_5)=\{0,1,4\}\not\ni 3$

pătrate

$\Rightarrow \nexists\sqrt{3}$ în $\mathbb{Z}_5 \Rightarrow$ ec. nu are soluții.

Ex: $x^2-5x+7=1$ în $\mathbb{Z}_{11}$

$x^2-5x+6=0$ în $\mathbb{Z}_{11}$ $\qquad 2^{-1}$ în $\mathbb{Z}_{11}=6$

$a=1$; $b=-5$; $c=6$

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

$\exists\sqrt{1}$ în $\mathbb{Z}_{11}$ DA $\Rightarrow \sqrt{1}\in\{1, \overset{-1}{\overset{\parallel}{10}}\}$

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

$x_2=(5-1)\cdot 2^{-1}=4\cdot 6=24=2$

Dacă iau $\sqrt{1}=10$ $\qquad$ Nu sunt necesare!!

$x_3=(5+10)\cdot 2^{-1}=15\cdot 6=4\cdot 6=2$

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

Inverse matriceale → HILL

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

$\det A = 2 + 1 + 1 = 4 \in U(\mathbb{Z}_5) \Rightarrow \exists A^{-1}$.

$(\det A)^{-1} = 4^{-1} = 4$

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

$A^{-1} = (\det A)^{-1} \cdot A^* = 4 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -2 & 2 & -2 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 4 & -4 \\ -8 & 8 & -8 \\ 4 & 4 & 12 \end{pmatrix}$

$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 4 & 1 \\ 2 & 3 & 2 \\ 4 & 4 & 2 \end{pmatrix}$

Ex.: $A = \begin{pmatrix} 2 & 1 & -1 \\ 1 & -2 & 1 \\ 0 & 2 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$ $A^{-1} = ?$ dacă există

$\det A = -2 \quad -4 = -6 = 1 \in U(\mathbb{Z}_7) \Rightarrow \exists A^{-1}$

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

$A \to A^t = \begin{pmatrix} 2 & 1 & 0 \\ 1 & -2 & 2 \\ -1 & 1 & 0 \end{pmatrix} \to A^* = \begin{pmatrix} -2 & -2 & -1 \\ 0 & 0 & -3 \\ 2 & -4 & -5 \end{pmatrix}$

$$A^{-1} = (\det A)^{-1} \cdot A^{*} = 1 \cdot A^{*} = A^{*} = \begin{pmatrix} -2 & -2 & -1 \\ 0 & 0 & -3 \\ 2 & -4 & -5 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 5 & 5 & 6 \\ 0 & 0 & 4 \\ 2 & 3 & 2 \end{pmatrix}$$

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

Logaritmul discret $\longrightarrow$ DIFFIE-HELLMAN

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

Ex: $\log_3 2$ în $\mathbb{Z}_7$

$\log_3 2 = x \Leftrightarrow 3^x = 2$ în $\mathbb{Z}_7 \Rightarrow \underline{x = 2}$

$3^0 = 1$; $3^1 = 3$; $\underline{3^2 = 9 = 2}$

$$\Rightarrow \boxed{\log_3 2 = 2 \text{ în } \mathbb{Z}_7}$$

Ex.: $\log_3 2$ în $\mathbb{Z}_{11}$

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

Sol1: Calculez puterile lui 3 mod 11

n	0	1	2	3	4	$\boxed{5}$	6	7	8	9	10
$3^n \bmod 11$	1	3	9	5	4	$\boxed{1}$	3	9	5	4	1

$\Rightarrow \operatorname{ord} 3 = 5$ în $\mathbb{Z}_{11}^*$

$\Rightarrow \log_3 2$ nu ex. în $\mathbb{Z}_{11}^*$

Teorema lui Lagrange pt grupuri

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

$\Rightarrow \operatorname{ord} g \mid n$

În particular, $g^n = e$, el. neutru.

! Multiplicativ, lucrăm cu $\mathbb{Z}_n^* \Rightarrow \# \mathbb{Z}_n^* = n-1$

Sol2: Soluția $3^x = 2$ în $\mathbb{Z}_{11}$ este sol. $3^x = 11k+2$

$11k+2 = \{2, 13, 24, 35, 46, 57, \ldots\ldots \sim 3^{10}\}$

$3^{10} = 59049$

Caut puteri ale lui 3 (dacă există)