13419

Ecuații de gradul I în $\mathbb{Z}_n$

Ex 1) $5x+3=1$ în $\mathbb{Z}_7$

$5x = 1-3 = -2 = 5$

$5x = 5$ în $\mathbb{Z}_7 \mid \cdot 5^{-1} = 3$

$3 \cdot 5 \cdot x = 5 \cdot 3 \Rightarrow x = 1$

Ex 2: $4x + 5 = 3$ în $\mathbb{Z}_{10}$

$4x = 3-5 = -2 = 8 \mid \cdot 4^{-1}$ NU există

$(4,10) = 2 \neq 1$

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

$4x = 8$

Rezolv prin încercări $\mid \Rightarrow x = 2$, $x = 7$

x	0	1	**2**	3	4	5	6	**7**	8	9
$4x$ mod 10	0	4	**8**	2	6	0	4	**8**	2	6

Sisteme liniare

Ex: $\begin{cases} 3x+2y=1 \\ 5x-3y=2 \end{cases}$ în $\mathbb{Z}_{11}$

Matricea sistemului: $A = \begin{pmatrix} 3 & 2 \\ 5 & -3 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_{11})$

$\det A = -9-10 = -19 = -11-8 = -8 = 3 \in U(\mathbb{Z}_{11})$

$\Rightarrow$ S.S.t. Cramer $\Rightarrow$ soluție unică

$$\begin{cases} 3x+2y=1 \\ 5x-3y=2 \Rightarrow 5x = 2+3y \mid \cdot 5^{-1} = 9 \end{cases}$$

$$\Rightarrow x = 9(2+3y) = 18+27y = 7+5y$$

$$3(7+5y)+2y = 1$$

$$21+15y+2y = 1$$

$$10+6y = 1 \Rightarrow 6y = -9 = 2 \mid \cdot 6^{-1} = 2$$

$$\Rightarrow \boxed{y=4} \quad x = 7+5\cdot 4 = 27 = 5$$

$$\boxed{x=5}$$

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

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

$\Rightarrow$ sist. NU este Cramer

$$\begin{cases} 3x+y=4 \mid \cdot 2 \\ 2x+2y=3 \end{cases} \Rightarrow \begin{cases} 6x+2y=8 \\ 2x+2y=3 \end{cases} \quad (-)$$

$4x = 5 \mid \cdot 4^{-1}$ NU există

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

$4x=5$ nu are sol. în $\mathbb{Z}_{10}$.

$\Rightarrow S = \emptyset$

Ec. de gradul al II-lea

Ex: $3x^2 - 2x + 1 = 0$ în $\mathbb{Z}_7$

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

$\Delta = b^2 - 4ac = 4 - 4 \cdot 1 \cdot 3 = -8 = -7 - 1 = -1 = 6$

$\exists \sqrt{6}$ în $\mathbb{Z}_7$?

x	0	1	2	3	4	5	6	
$x^2 \bmod 7$	0	1	4	2	2	4	1	$\neq 6$

$\Rightarrow \nexists \sqrt{\Delta} \Rightarrow$ nu avem sol.

Ex: $5x^2+3x+2=4$ în $\mathbb{Z}_{11}$

$5x^2+3x-2=0$

$a=5;\ b=3;\ c=-2$

$\Delta = 9+40 = 49 = 44+5 = 5$

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

$\exists \sqrt{5}$ în $\mathbb{Z}_{11}$?

x	0	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	0	1	4	9	5			5			

$\sqrt{5} \in \{4, 7\}$

$x_1 = (-b+\sqrt{\Delta})\cdot(2a)^{-1} = (-3+4)\cdot 10^{-1} = 1\cdot 10^{-1} = 10$

$x_2 = (-b-\sqrt{\Delta})\cdot(2a)^{-1} = (-3-4)\cdot 10^{-1} = -7\cdot 10^{-1} = 4\cdot 10$

$= 40 = 33+7 = 7$

$x_3 = (-3+7)\cdot 10^{-1} = 4\cdot 10 = 40 = 7$

$x_4 = (-3-7)\cdot 10^{-1} = -10\cdot 10^{-1} = 1\cdot 10^{-1} = 10$

↑ NU E NECESAR

Logaritmi în $\mathbb{Z}_n$

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

Ex: $\log_3 5$ în $\mathbb{Z}_7$ $\quad \log_3 5 = a \iff 3^a = 5$ în $\mathbb{Z}_7$

a	0	1	2	3	4	5	6	7	8	9 ...
3^a mod 7	1	3	2	6	4	5	1	3	2	6 4 5 ...

$3^3 = 3^2 \cdot 3 = 2 \cdot 3 \Rightarrow 3^5 = 5 \bmod 7$

$3^4 = 3^3 \cdot 3 = 6 \cdot 3 \Rightarrow \log_3 5 = 5$ în $\mathbb{Z}_7$.

Teorema lui Lagrange pt grupuri

G grup, $\#G = n$ → cel mai mic t a.î. $g^t = e$

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

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

Dacă lucrăm multiplicativ $\Rightarrow (\mathbb{Z}_n^*, \cdot)$ grup

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

Ex: $\log_3 2 \in \mathbb{Z}_{11}$ $\quad 3^9 = 2 \in \mathbb{Z}_{11}$

a	0	1	2	3	4	5	6	7	8	9	10
$3^9 \bmod 11$	1	3	9	5	4	1	3	9	5	4	1

$\text{ord}\, 3 = 5 \in \mathbb{Z}_{11}$

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

Inverse matriceale $\mathcal{M}_3(\mathbb{Z}_n)$

$$A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 2 & -1 \\ -2 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_5)$$

$A^{-1} = ?$ dacă există

Teoremă: A este inversabilă în $\mathcal{M}_n(\mathbb{Z}_t)$ $\Leftrightarrow \det A \in U(\mathbb{Z}_t)$

$\det A = 4 - 2 + 1 = 3 \in U(\mathbb{Z}_5)$

$(\det A)^{-1} = 3^{-1} = 2$

$(-1)^{\text{linie + coloană}}$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 2 \cdot \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 2 \\ 4 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 4 \\ 8 & 4 & 0 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 4 \\ 3 & 4 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_5)$$

Obs: $A \cdot A^{-1} = A^{-1} \cdot A = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

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

$\det A = 1 + 4 = 5 \in U(\mathbb{Z}_7) \Rightarrow \exists A^{-1}$

$(\det A)^{-1} = 5^{-1} = 3$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 3 \cdot \begin{pmatrix} 6 & 5 & 2 \\ 5 & 1 & 6 \\ 5 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 18 & 15 & 6 \\ 15 & 3 & 18 \\ 15 & 9 & 18 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 1 & 6 \\ 1 & 3 & 4 \\ 1 & 2 & 4 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7).$$