1342a)

Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $5x+3=1$ în $\mathbb{Z}_{11}$

$5x=1-3=-2=9$

$5x=9 \mid \cdot 5^{-1}=9$

$\underbrace{9\cdot 5}_{1}x=9\cdot 9 \Rightarrow x=81=\overset{0}{77}+4=4$

$\underline{x=4}$

Ex: $6x+5=2$ în $\mathbb{Z}_{10}$

$6x=2-5=-3=7$

$6x=7 \mid \cdot 6^{-1}$ NU există în $\mathbb{Z}_{10}$ pt că $(6,10)=2$

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

Rezolv prin încercări

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

$\Rightarrow$ Ecuația nu are soluție.

Sisteme liniare

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

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

$\det A = -9-10 = -19 = -14-5 = -5 = 2 \in U(\mathbb{Z}_7) \Rightarrow$

$\Rightarrow$ sistem Cramer $\Rightarrow$ soluție unică

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

$x = 3(2+3y) = 6+9y = 6+2y$

$3(6+2y)+2y = 1$

$18+6y+2y = 1$

$4+y = 1 \Rightarrow y = 1-4 = -3 = 4$

$x = 6+2y = 6+2\cdot 4 = 6+8 = 14 = 0.$

$(x,y) \in \{(0,4)\}$

$a^{-1} = \frac{1}{a}$ $\quad a^{-1}\cdot a = \frac{1}{a}\cdot a = 1$

Ex: $\begin{cases} 2x+3y=5 \\ x+4y=1 \end{cases}$ în $\mathbb{Z}_{10}$

$A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix} \in M_2(\mathbb{Z}_{10})$; $\det A = 8-3 = 5$

$5 \notin U(\mathbb{Z}_{10}) \Rightarrow$ sist. nu este Cramer

$\Rightarrow S = \emptyset$ sau $\# S = \infty$

$$\begin{cases} 2x+3y=5 \\ x+4y=1 \mid \cdot 2 \end{cases} \Rightarrow \begin{cases} 2x+3y=5 \\ 2x+8y=2 \end{cases} \quad (-)$$

$$5y=-3=7$$

Rezolv prin încercări

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

$\Rightarrow 5y=7$ nu se poate în $\mathbb{Z}_{10}$

$\Rightarrow S=\emptyset$.

Ec. de gradul II

Ex: $2x^2-3x+1=0$ în $\mathbb{Z}_5$

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

$\Delta=b^2-4ac=9-4\cdot 2=1$

$\exists\sqrt{\Delta}$ în $\mathbb{Z}_5$? $\sqrt{1}\in\{1,4\}$

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

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

$x_3=(3+4)\cdot 4^{-1}=2\cdot 4=3$

$x_4=(3-4)\cdot 4^{-1}=4\cdot 4^{-1}=1$

NU E NEVOIE

Ex: $x^2+2x+3=1$ în $\mathbb{Z}_7$

$x^2+2x+2=0$

$a=1;\ b=2;\ c=2$

$\Delta = 4-4\cdot 2\cdot 1 = -4 = 3$

$\exists\sqrt{3}$ în $\mathbb{Z}_7$? $\quad \sqrt{3}=n \Leftrightarrow n^2=3$ în $\mathbb{Z}_7$

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

pătrate

$\Rightarrow \sqrt{3}$ nu există în $\mathbb{Z}_7$ $\Rightarrow$ ec. nu are soluții.

Logaritmi în $\mathbb{Z}_n$

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

Ex: $\log_2 3$ în $\mathbb{Z}_7$

$\log_2 3 = a \Leftrightarrow \underbrace{2^a=3}$ în $\mathbb{Z}_7$

a	0	1	2	$\boxed{3}$	4	5	6	7	8	...
$2^a \bmod 7$	1	2	4	$\boxed{1}$	2	4	1	...		

$\hookrightarrow$ ord $2=3$

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

Teorema lui Lagrange pt grupuri

G grup, $\#G = n$.

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

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

Lucrăm multiplicativ pt $\log_a b$ $(\mathbb{Z}_n^*, \cdot)$

$\Rightarrow \#\mathbb{Z}_n^* = n-1$

$\Rightarrow$ Pt a calcula $\log_a b$ în $\mathbb{Z}_n$ este suficient să calculez $a^0, a^1, a^2, a^3, \dots, a^{n-1} = 1$

Ex: $\log_3 5$ în $\mathbb{Z}_{11}$

Calculez $3^0, 3^1, 3^2, \dots, 3^{10} = 1$

a	0	1	2	$\boxed{3}$	4	$\boxed{5}$	6	7	8	9	10
3^a în $\mathbb{Z}_{11}$	1	3	9	$\boxed{5}$	4	$\boxed{1}$					1

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

$3^3 = 3^2 \cdot 3 = 9 \cdot 3 = 27 = 5$

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

$\rightarrow \log_3 5 = 3$ în $\mathbb{Z}_{11}$

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

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

$\Leftrightarrow \det A \in U(\mathbb{Z}_t)$

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

$\det A = -1 + 8 - 2 = 5 = 0 \Rightarrow A^{-1}$ nu există

Ex: $A = \begin{pmatrix} 3 & 1 & 2 \\ -1 & 0 & -2 \\ 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$

$\det A = -2 - 2 + \underbrace{6 + 1}_{0} = -4 = 3 \in U(\mathbb{Z}_7)$

$\Rightarrow$ există A^{-1}

$(\det A)^{-1} = 3^{-1}$ în $\mathbb{Z}_7 = 5$ $\qquad (-1)^{\text{linie}+\text{col.}}$

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

$A^{-1} = (\det A)^{-1} \cdot A^* = 5 \cdot \begin{pmatrix} 2 & 1 & -2 \\ -1 & 1 & 4 \\ -1 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 5 & -10 \\ -5 & 5 & 20 \\ -5 & -10 & 5 \end{pmatrix}$

$\Rightarrow A^{-1} = \begin{pmatrix} 3 & 5 & 4 \\ 2 & 5 & 6 \\ 2 & 4 & 5 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$

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