13416

Aritmetică în $\mathbb{Z}_n$

Ecuații de gradul I → CAESAR AFIN

Ex: $5x+1=3$ în $\mathbb{Z}_7$

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

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

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

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

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

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

$3x = 0$

$\Rightarrow x = 0$

$5 \cdot 0 - y = 2 \Rightarrow y = -2 = 5$

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 Z_7

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

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

$= -2 = 5$

$\exists \sqrt{5}$ în Z_7? $\sqrt{5} = y \Leftrightarrow y^2 = 5$

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ $P(Z_7) = \{0, 1, 4, 2\} \neq 5$

↑ pătratele

$\Rightarrow \nexists \sqrt{5}$ în $Z_7 \Rightarrow$ nu are soluții.

Ex: $X^2 - 5X + 7 \overset{\text{în } Z_{11}}{=} 1 \Leftrightarrow X^2 - 5X + 6 = 0$ în Z_{11}

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

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

2^{-1} în $Z_{11} = 6$

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

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

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

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

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

Inverse matriceale → HILL

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

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

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

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

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

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

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

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

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

Logaritm discret → DIFFIE-HELLMAN

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

Ex: $\log_2 5$ în $\mathbb{Z}_7$

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

x	0	1	2	3	4	5	6
2^x	1	2	4	1	2	4	1

$\neq 5$

→ $\text{ord}\, 2 = 3$

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

Teorema lui Lagrange pt grupuri

G grup finit, cu n elemente.

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

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 $\mathbb{Z}_{11}$

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

Sol 1: 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

$\neq 2$

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

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

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

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

↑

Văd puterile de puteri ale lui 3

Algoritmi criptografici

Caesar, Afin, Hill } flux (stream cipher)

pe blocuri (block cipher)
- cu padding random
- fără padding

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Adaug ␣ . ? (26, 27, 28) $\Rightarrow$ lucrăm în $\mathbb{Z}_{29}$

Caesar - flux: o cheie pt tot mesajul

Ecuația de criptare: $m + K = C$, $\forall m \in$ Mesaj, K cheie $\rightarrow C \in$ Cod(Cifru)

Ec. de decriptare: $m = C - K$

$Enc(m) = m + K$; $Dec(c) = C - K$

Ex: Mesaj: LABORATOR
cheie: K = 15

[L, A, B, O, R, A, T, O, R] ⟶ [11, 0, 1, 14, 17, 0, 19, 14, 17]

$\xrightarrow[+15]{+K}$ [26, 15, 16, 29, 32, 15, 34, 29, 32] $\xrightarrow{\text{mod } 29}$

[26, 15, 16, 0, 3, 15, 5, 0, 3] → ␣PQADPEAD

Concluzie: LABORATOR $\xrightarrow[\text{Caesar}]{+15}$ ␣PQADPEAD.

Decriptare: [␣, P, Q, A, D, P, E, A, D] → [26, 15, 16, 0, 3, 15, 5, 0, 3]

$\xrightarrow[-15]{-K}$ [11, 0, 1, -15, -12, 0, -10, -15, -12] $\xrightarrow{\text{mod } 29}$

[11, 0, 1, 14, 17, 0, 19, 14, 17] ⟶ LABORATOR

Caesar pe blocuri, fără padding

o cheie/bloc

cel mult un bloc mai scurt

Ex: Mesaj: LABORATOR
bloc: 5

⇒ LABOR, K1 = 15
ATOR, K2 = 11

[L, A, B, 0, R] → ␣PQAD

[A, T, 0, R] → [0, 19, 14, 7] $\xrightarrow[+11]{+K2}$ [11, 30, 25, 18] $\xrightarrow{\text{mod } 29}$

[11, 1, 25, 18] → LBZS

LABORATOR $\xrightarrow[\text{pe blocuri}]{\text{Caesar}}$ ␣PQADLBZS

Caesar pe blocuri, cu padding random

Ex. Mesaj: MARTI → MAR
TIE → padding random

Bloc: 3

K1=5; K2=10

[M, A, R] → [12, 0, 17] $\xrightarrow[+5]{+K1}$ [17, 5, 22] → RFW

[T, I, E] → [19, 8, 4] $\xrightarrow[+10]{+K2}$ [29, 18, 14] $\xrightarrow{\text{mod } 29}$ [0, 18, 14]

→ ASO

MARTIE → RFWASO

padding lasă neschimbat

Cifrul afin - varianta flux

Ec. de criptare: $m \cdot K1 + K2 = C$, $\forall m \in Mesaj$

$K1, K2$ chei

$c \in Cod$

Ec. de decriptare: $m = (C - K2) \cdot K1^{-1}$

Ex: Mesaj: CRIPTO ; $K1 = 7$; $K2 = 13$

$[C, R, I, P, T, O] \rightarrow [2, 17, 8, 15, 19, 14] \xrightarrow[\cdot 7 + 13]{\cdot K1 + K2}$

$[27, 132, 69, 118, 146, 111] \xrightarrow{mod\ 29}$

$[27, 16, 11, 2, 1, 24] \rightarrow [., Q, L, C, B, Y]$

$132 = 116 + 16 = 16$

$4 \cdot 29 = 116$

$\rightarrow .QLCBY$

Decriptare: $[., Q, L, C, B, Y] \rightarrow [27, 16, 11, 2, 1, 24]$

$\xrightarrow[-13 \cdot 25]{-13 \cdot 7^{-1}} [350, 75, -50, -275, -300, 275] \xrightarrow{mod\ 29}$

$[2, 17, 8, 15, 19, 14] \rightarrow CRIPTO.$

Hill - Flux

Ec. de criptare : $\begin{pmatrix} \text{Matrice de} \\ \text{criptare} \end{pmatrix} \cdot \begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = \begin{pmatrix} C \\ O \\ D \end{pmatrix}$

Ec. de decriptare : $\begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = \begin{pmatrix} \text{Matrice de} \\ \text{criptare} \end{pmatrix}^{-1} \cdot \begin{pmatrix} C \\ O \\ D \end{pmatrix}$

Matrice de criptare $\in M_3(Z_{29})$, inversabilă

Mesaj, Cod $\in M_{3,1}(Z_{29})$

Ex: Mesaj: YES ; Mat. cr. $= \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ -2 & 0 & 1 \end{pmatrix} = A$

$\det(A) = -1 - 8 + 2 = -7 = 22$

$\begin{pmatrix} Y \\ E \\ S \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$; $\begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ -2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix} = \begin{pmatrix} -24+8+18 \\ 4+36 \\ -48+18 \end{pmatrix}$

$= \begin{pmatrix} 2 \\ 40 \\ -30 \end{pmatrix} \bmod 29 = \begin{pmatrix} 2 \\ 11 \\ 28 \end{pmatrix} = CL?$

Decriptare $A^{-1} = ?$

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

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 22^{-1} \cdot \begin{pmatrix} 1 & -2 & 3 \\ -4 & 1 & 2 \\ 2 & -4 & -1 \end{pmatrix} = 4 \cdot \begin{pmatrix} 1 & -2 & 3 \\ -4 & 1 & 2 \\ 2 & -4 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 4 & -8 & 12 \\ -16 & 4 & 8 \\ 8 & -16 & -4 \end{pmatrix}$$

$$\text{Mesaj} = \begin{pmatrix} 4 & -8 & 12 \\ -16 & 4 & 8 \\ 8 & -16 & -4 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 11 \\ 28 \end{pmatrix} = \begin{pmatrix} Y \\ E \\ S \end{pmatrix}$$

Ex de examen: Criptați cu Caesar-flex numele de familie, ca cheia = prenume (sau invers).

Mesaj: MANEA
Cheia: ADRIAN

M	A	N	E	A	← m
+	+	+	+	+	
A	D	R	I	A	← k

12	0	13	4	0
+ 0	3	17	8	0
12	3	30	12	0

→ 12, 3, 1, 12, 0 = ...

Tema: 1) Criptați cu Caesar - flux + decriptare

Mesaj: Numele de familie

Cheia: Luna nașterii.

2) Criptați cu Caesar pe blocuri fără padding

Mesaj: Prenume; b=3; Chei: ultimele cifre ale numărului din nr. de telefon.

+ decriptare

3) Criptați cu afin - flux, Mesaj = Orașul de naștere, K1 = luna de naștere, K2 = ziua de naștere

+ decriptare

---

4) Hill: Mesaj: Joi; $MC = \begin{pmatrix} -2 & 1 & 0 \\ 2 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}$.

+ decriptare.