13429)

Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $5x+3=1$ în $\mathbb{Z}_{11}$

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

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

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

$x = 4$

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

Rezolv prin încercări

x	0	1	2	3	4	5	6	7	8	9
$6x \bmod 10$	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: $A = \begin{pmatrix} 3 & 2 \\ 5 & -3 \end{pmatrix} \in M_2(\mathbb{Z}_7)$

$\det A = -9-10 = -19 = -14-5 = -5 = 2 \in U(Z_7) \Rightarrow$

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

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

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

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

$18+6y+2y = 1$

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

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

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

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

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

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

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

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

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

$(-)$

$5y = -3 = 7$

Rezolv prin încercări

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

$\Rightarrow 5y = 7$ nu se poate în Z_{10}

$\Rightarrow S = \phi$.

Ec. de gradul II

Ex: $2x^2 - 3x + 1 = 0$ în Z_5

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

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

$\exists \sqrt{\Delta} \in Z_5$? $\sqrt{1} \in \{1, 4\}$

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

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

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

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

↑ 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 $\mathbb{Z}_7$

$\mathbb{Z}_7=\{0,1,2,3,4,5,6\}$ $\quad P(\mathbb{Z}_7)=\{0,1,4,2\}\neq 3$

(↑ 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 $\mathbb{Z}_7$

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

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

↳ $\operatorname{ord} 2 = 3$

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

Teorema lui Lagrange pt grupuri

G grup, $\#G = n$.

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

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

Lucrăm <u>multiplicativ</u> 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	3	4	5	6	7	8	9	10
3^a în $\mathbb{Z}_{11}$	1	3	9	5	4	1					1

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

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

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

$\log_3 5 = 3$ în $\mathbb{Z}_{11}$

Inverse matriceale $M_3(Z_n)$

Teoremă $A \in M_n(Z_t)$ este inversabilă $\Leftrightarrow$ $\det A \in U(Z_t)$

Ex: $A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \in M_3(Z_5)$ $A^{-1} = ?$ dacă există

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

Ex: $A = \begin{pmatrix} 3 & 1 & 2 \\ -1 & 0 & -2 \\ 1 & 1 & 1 \end{pmatrix} \in M_3(Z_7)$

$\det A = -2 - 2 + \underbrace{6+1}_{0} = -4 = 3 \in U(Z_7)$

$\Rightarrow$ există A^{-1}

$(\det A)^{-1} = 3^{-1}$ în $Z_7 = 5$ $\quad (-1)^{\text{linie+col.}}$

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

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

$\Rightarrow A^{-1} = \begin{pmatrix} 3 & 5 & 4 \\ 2 & 5 & 6 \\ 2 & 4 & 5 \end{pmatrix} \in M_3(Z_7)$

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

Algoritmi criptografici

I Flux (stream cipher)

II Pe blocuri (block cipher)

1) Caesar
2) Afin
3) Hill

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

I	J	K	L	M	N	O	P
8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X
16	17	18	19	20	21	22	23

Y	Z
24	25

Adaug $\sqcup$ (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

$C \in Cod\ (Cifru)$

$Enc(m) = m + k$

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

$Dec(c) = c - K$

Exemplu: Mesaj = MARTI

Cheia = 11

$[M, A, R, T, i] \to [12, 0, 17, 19, 8] \xrightarrow[+11]{+K}$

$[23, 11, 28, \underline{30}, 19] \xrightarrow[mod\ 29]{} [23, 11, 28, 1, 19]$

→ XL?BT

Concluzii: $MARTI \xrightarrow[+11]{Caesar} XL?BT$

Decriptare $[x, L, ?, B, T] \longrightarrow [23, 11, 28, 1, 19]$

$\xrightarrow[-11]{-K} [12, 0, 17, \underline{-10}, 8] \xrightarrow[mod\ 29]{} [12, 0, 17, 19, 8] \to$

→ MARTI ✓

Caesar pe blocuri: o cheie pt fiecare bloc

a) Fără padding: ≤ 1 bloc mai scurt

Ex: Mesaj: NOIEMBRIE, b = 6 ⇒ NOIEMB ; K1 = 15
RIE ; K2 = 21

[N, O, I, E, M, B] → [13, 14, 8, 4, 12, 1] $\xrightarrow[+15]{+K1}$

→ [28, 29, 23, 19, 27, 16] $\xrightarrow{\text{mod } 29}$ [28, 0, 23, 19, 27, 16]

→ ?AXT.Q

[R, I, E] → [17, 8, 4] $\xrightarrow[+24]{+K2}$ [38, 29, 25] $\xrightarrow{\text{mod } 29}$

[9, 0, 25] → JAZ

NOIEMBRIE → ?AXT.QJAZ

b) Cu padding random: toate blocurile au aceeași lungime

Ex: Mesaj: MARTI, b = 3 ⇒ MAR ; K1 = 5
TIE ; K2 = 7
↳ padding random

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

[T, I, E] → [19, 8, 4] $\xrightarrow[+7]{+K2}$ [26, 15, 11] → _PL

MARTIE → RFW_PL

Ex. suplimentar

Examen: Criptați cu Caesar numele de familie cu cheia = primul prenume (sau invers).

Ex: NF: MANEA

P: ADRIAN

	M	A	N	E	A
	12	0	13	4	0
+	A	D	R	I	A
→	0	3	17	8	0

12 3 30 12 0 mod 29

↓

12 3 1 12 0

M D B M A

Cifrul afin

Ec. de criptare: $m \cdot K1 + K2 = C$, $\forall m \in Mesaj$
$k1, k2$ chei
$C \in Cod$

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

Flux: Mesaj: MARTI; K1 = 3; K2 = 7

$[M, A, R, T, I] \rightarrow [12, 0, 17, 19, 8] \xrightarrow[\cdot 3 + 7]{\cdot K1 + K2} [43, 7, 58, 64, 31]$

$\xrightarrow{mod\ 29} [14, 7, 0, 6, 2] \rightarrow$ O H A G C

Descriptare: $(OHAGC] \to [14,7,0,6,2] \xrightarrow{-K2;K]^{-1}} \begin{matrix} -7\cdot 3^{-1} \\ -7,\cdot 10 \end{matrix}$

$[70,0,-70,-10,-50] \xrightarrow{\text{mod } 29} [12,0,17,19,8]$

$\to$ MARTi

$-70 = -58 - 12 = -12 = 17$

$-50 = -29 - 21 = -21 = 8$

Hill - flux

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

$\in \mathcal{M}_3(\mathbb{Z}_{29})$ $\qquad$ $\in \mathcal{M}_{3,1}(\mathbb{Z}_{29})$

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

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

$\det A = 2 - 2 - 1 = -1 = 28 \in U(\mathbb{Z}_{29})$

$\begin{pmatrix} Y \\ E \\ S \end{pmatrix} = \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix}$

$$\begin{pmatrix} -1 & 0 & 1 \\ 2 & 1 & 0 \\ 1 & -1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 4 \\ 18 \end{pmatrix} = \begin{pmatrix} -6 \\ 52 \\ -16 \end{pmatrix} \bmod 29 = \begin{pmatrix} 23 \\ 23 \\ 13 \end{pmatrix} = \begin{matrix} X \\ X \\ N \end{matrix}$$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 28^{-1} \cdot \begin{pmatrix} -2 & -1 & -1 \\ 4 & 1 & 2 \\ -3 & -1 & -1 \end{pmatrix}$$

$$28 = 4$$

$$28 \cdot \begin{pmatrix} -2 & -1 & -1 \\ 4 & 1 & 2 \\ -3 & -1 & -1 \end{pmatrix} = \begin{pmatrix} -56 & -28 & -28 \\ 112 & 28 & 56 \\ -84 & -28 & -28 \end{pmatrix}$$

$$\text{Mesaj} = \begin{pmatrix} -56 & -28 & -28 \\ 112 & 28 & 56 \\ -84 & -28 & -28 \end{pmatrix} \cdot \begin{pmatrix} 23 \\ 23 \\ 13 \end{pmatrix} = \begin{matrix} 24 \\ 4 \\ 18 \end{matrix} \begin{matrix} Y \\ E \\ S \end{matrix}$$

Exerciții

1. Caesar flux, mesaj = nume de familie, cheie = luna de naștere. Descriptare.
2. Caesar pe blocuri, mesaj = prenume, b = 3, cheie: ultimele cifre ale nr. de telefon. Descriptare.
3. Afin flux, mesaj = orașul de naștere, k1 = luna de naștere, k2 = ziua de naștere. Descriptare.

4. Hill, Mesaj = OPT, MC = $\begin{pmatrix} -1 & 2 & -1 \\ 0 & 1 & -1 \\ 2 & -2 & 1 \end{pmatrix}$. Decriptare.