

1342a)

Ecuatii de gradul I în \mathbb{Z}_n

Ex: $5x + 3 = 1$ în \mathbb{Z}_{11}

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

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

$$\underbrace{9 \cdot 5x}_{=1} = \underbrace{9 \cdot 9}_{=1} \Rightarrow x = 81 = 7 \cdot 11 + 4 = 4$$

$x = 4$

Ex: $6x + 5 = 2$ în \mathbb{Z}_{10}

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

$$6x = 7 \quad | \cdot \underbrace{6^{-1}}_{\text{NU exista în } \mathbb{Z}_{10}} \text{ pt } \text{ca } \gcd(6, 10) = 2$$

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

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

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

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

\Rightarrow system Cramer \Rightarrow solution unique

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

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

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

$$18 + 6y + 2y = 1$$

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

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

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

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

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

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

$5 \notin U(\mathbb{Z}_{10}) \Rightarrow$ system not Cramer
 $\Rightarrow S = \emptyset$ non # $S = \infty$

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

(-)

$$5y = -3 = 7$$

Rezolvăm prin încercări

x	0	1	2	3	4	5	6	7	8	9
$5x \text{ mod } 10$	0	5	0	5	0	5	0	5	0	5

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

$$\Rightarrow S = \emptyset.$$

Ex. de gradul II

$$\underline{\text{Ex.}}: 2x^2 - 3x + 1 = 0 \text{ în } \mathbb{Z}_5$$

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

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

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

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

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

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

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

$m \in N \vee n \in E$

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

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

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

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

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

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

↑
pătrată

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

Logaritmi în \mathbb{Z}_n

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

Ex: $\log_2 3 \in \mathbb{Z}_7$

$$\log_2 3 = a (\Leftrightarrow) \underline{2^a = 3} \in \mathbb{Z}_7$$

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

$\hookrightarrow \text{ord } 2 = 3$

$\Rightarrow \log_2 3$ 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 calculăm $a^0, a^1, a^2, a^3, \dots, a^{n-1} = 1$

Ex: $\log_3 5$ în \mathbb{Z}_{11}

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

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

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

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

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

Inverse matriceale $M_3(\mathbb{Z}_n)$

Teorema $A \in M_n(\mathbb{Z}_t)$ este inversabilă \Leftrightarrow

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

Ex: $A = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}_5)$ $A^{-1} = ?$
dacă există

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

Ex: $A = \begin{pmatrix} 3 & 1 & 2 \\ -1 & 0 & -2 \\ 1 & 1 & 1 \end{pmatrix} \in M_3(\mathbb{Z}_7)$

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

\Rightarrow există A^{-1}

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

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

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

$$\Rightarrow A^{-1} = \begin{pmatrix} 3 & 5 & 4 \\ 2 & 5 & 6 \\ 2 & 4 & 5 \end{pmatrix} \in M_3(\mathbb{Z}_7)$$

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

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 $\underline{\quad}$ \cdot $?$
 26 27 28

\Rightarrow lucrăm în \mathbb{Z}_{29}

Caesar - flux \rightarrow o cheie pt tot mesajul

Ecuația de criptare: $m + K = C, \forall m \in \text{Mesaj}$

$$\text{Enc}(m) = m + K$$

Ec. de decriptare: $m = C - K$ \rightarrow K cheie
 $C \in \text{Cod (Cifru)}$

$$\text{Dec}(c) = c - K$$

Exemplu: Mesaj = MARTI

Cheie = 11

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

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

\rightarrow XL?BT

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

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

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

\rightarrow MARTI \checkmark

Caesar pe blocuri: o cheie pt fiecare bloc

a) Fără padding: ≤ 1 bloc mai scurt

Ex: Mesaj: NOIEMBRIE \Rightarrow NOIEMB ; $K_1 = 15$
 $b = 6$ RIE ; $K_2 = 21$

$[N, O, I, E, M, B] \rightarrow [13, 14, 8, 4, 12, 1] \xrightarrow{+K_1, +15}$

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

$\rightarrow ? \text{ AXT.Q}$

$[R, I, E] \rightarrow [17, 8, 4] \xrightarrow{+K_2, +21} [38, 29, 25] \xrightarrow{\text{mod } 29}$

$[9, 0, 25] \rightarrow ? \text{ AZ}$

NOIEMBRIE $\rightarrow ? \text{ AXT.Q} ? \text{ AZ}$

b) Cu padding random: toate blocurile au aceeași lungime

Ex: Mesaj: MARTI \Rightarrow MAR ; $K_1 = 5$
 $b = 3$ TIE ; $K_2 = 7$

\rightarrow padding random

$[M, A, R] \rightarrow [12, 0, 17] \xrightarrow{+K_1, +5} [17, 5, 22] \rightarrow \text{RFW}$

$[T, I, E] \rightarrow [19, 8, 4] \xrightarrow{+K_2, +7} [26, 15, 11] \rightarrow \text{LPL}$

MARTIE $\rightarrow \text{RFW_LPL}$

Ex. suplimentar

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

Ex. NF: MANEA

P: ADRIAN

$$\begin{array}{rcccccc} & M & A & N & E & A \\ + & \left[\begin{array}{c} 12 \\ A \\ \rightarrow 0 \end{array} \right. & \left[\begin{array}{c} 0 \\ D \\ 3 \end{array} \right. & \left[\begin{array}{c} 13 \\ R \\ 17 \end{array} \right. & \left[\begin{array}{c} 4 \\ I \\ 8 \end{array} \right. & \left[\begin{array}{c} 0 \\ A \\ 0 \end{array} \right. \end{array}$$

$$\hline 12 \quad 3 \quad 30 \quad 12 \quad 0 \pmod{29}$$

↓

$$12 \quad 3 \quad 1 \quad 12 \quad 0$$

$$M \quad D \quad B \quad M \quad A$$

Cifrul afîn

$$\text{Ec. de criptare: } m \cdot K_1 + K_2 = c, \quad \forall m \in \text{Mesaj}$$

K_1, K_2 chei
 $c \in \text{Cod}$

$$\text{Ec. de decriptare: } m = (c - K_2) \cdot K_1^{-1}$$

Flux: Mesaj: MARTI; $K_1 = 3$; $K_2 = 7$

$$[M, A, R, T, i] \rightarrow [12, 0, 17, 19, 8] \xrightarrow{\cdot \frac{K_1 + K_2}{\cdot 3 + 7}} [43, 7, 58, 64, 31]$$

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

Decriptare: $(OHAGC) \rightarrow [14, 7, 0, 6, 2] \xrightarrow{\substack{-K2; K1^{-1} \\ -7 \cdot 3^{-1} \\ -7, \cdot 10}}$

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

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

$\rightarrow \text{MARTI}$

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

Hill - flux

Ec. de criptare: $\left(\begin{array}{c} \text{Matrice de} \\ \text{criptare} \end{array} \right) \cdot \left(\begin{array}{c} M \\ E \\ S \\ A \\ J \end{array} \right) = \left(\begin{array}{c} C \\ 0 \\ D \end{array} \right)$

\downarrow
 $\in \mathcal{M}_3(\mathbb{Z}_{29})$

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

Ec. de decriptare: $\left(\begin{array}{c} M \\ E \\ S \\ A \\ J \end{array} \right) = \left(\begin{array}{c} \text{Matrice de} \\ \text{criptare} \end{array} \right)^{-1} \cdot \left(\begin{array}{c} C \\ 0 \\ D \end{array} \right)$

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

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

$$\left(\begin{array}{c} Y \\ E \\ S \end{array} \right) = \left(\begin{array}{c} 24 \\ 4 \\ 18 \end{array} \right)$$

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

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

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

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

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

Exerciții

1. Caesar flux, mesaj = nume de familie, cheie = luna de naștere. Decriptare.
2. Caesar pe Ylowrî, mesaj = prenume, b = 3, cheie: ultimele cifre numele din nr. de telefon. Decriptare.
3. Afin flux, mesaj = orașul de naștere, K1 = luna de naștere, K2 = ziua de naștere

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