

1341a

Ecuații de gradul I în \mathbb{Z}_n

Ex 1) $5x + 3 = 1 \text{ în } \mathbb{Z}_7$

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

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

$$3 \cdot 5 \cdot x = 5 \cdot 3 \Rightarrow \underline{x = 1}$$

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

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

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

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

$$4x = 8$$

Rezolv prin încercări

$$\Rightarrow \begin{array}{l} x = 2 \\ \underline{x = 7} \end{array}$$

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

Matricea coeficienilor: $A = \begin{pmatrix} 3 & 2 \\ 5 & -3 \end{pmatrix} \in M_2(\mathbb{Z}_{11})$

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

\Rightarrow Sist. Cramer \Rightarrow solutie unica.

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

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

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

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

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

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

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

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

\Rightarrow sist. NU este Cramer

$$\begin{cases} 3x+y=4 \\ 2x+2y=3 \end{cases} \Rightarrow \begin{cases} 6x+2y=8 \\ 2x+2y=3 \end{cases}$$

(-)

$$4x=5 \quad | \cdot 4^{-1} \text{ nu exista}$$

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

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

$$\Rightarrow S = \emptyset$$

Ec. de gradul al II-lea

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

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

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

$\exists \sqrt{6}$ in \mathbb{Z}_7 ?

x	0	1	2	3	4	5	6
x^2 mod 7	0	1	4	2	2	4	1

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

$$\underline{\text{Ex:}} \quad 5x^2 + 3x + 2 = 4 \quad \text{in } \mathbb{Z}_{11}$$

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

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

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

$$a = b^2$$

$$\Delta = 9 + 40 = 49 = 7^2 + 5 = 5$$

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

x	0	1	2	3	4	5	6	7	8	9	10
$x^2 \text{ mod } 11$	0	1	4	9	5			5			

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

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

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

$$x_3 = (-3 + 7) \cdot 10^{-1} = 4 \cdot 10 = 40 = 7 \quad \text{--- } 40 = 3 \cdot 11 + 7 = 7$$

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



NU E NECESAR

Logaritmi în \mathbb{Z}_n

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

Ex: $\log_3 5 \in \mathbb{Z}_7$ $\log_3 5 = a \Leftrightarrow \underline{\underline{3^a = 5 \pmod{7}}}$

a	0	1	2	3	4	5	6	7	8	9	...		
$3^a \pmod{7}$	1	3	2	6	4	5	1	3	2	6	4	5	...

$$3^3 = 3^2 \cdot 3 = 2 \cdot 3$$

$$\Rightarrow 3^5 = 5 \pmod{7}$$

$$3^4 = 3^3 \cdot 3 = 6 \cdot 3$$

$$\Rightarrow \log_3 5 = 5 \in \mathbb{Z}_7$$

Teorema lui Lagrange pt grupuri

G grup, $\#G = n$ \rightarrow cel mai mic t al $g^t = e$

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

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: $\log_3 2 \in \mathbb{Z}_{11}$ $3^a = 2 \in \mathbb{Z}_{11}$

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

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

2) $\log_3 2$ nu exista in \mathbb{Z}_{11} .

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

$$A = \begin{pmatrix} 2 & -1 & 0 \\ 1 & 2 & -1 \\ -2 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}_5)$$

$A^{-1} = ?$

daca exista

Teorema: A este inversabila in $M_n(\mathbb{Z}_t)$

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

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

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

$(-1)^{\text{linie} + \text{colana}}$

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

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

$$\Rightarrow A^{-1} = \begin{pmatrix} 4 & 2 & 2 \\ 2 & 4 & 4 \\ 3 & 4 & 0 \end{pmatrix} \in M_3(\mathbb{Z}_5)$$

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

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

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

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

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

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

Algoritmi criptografici

I Flux (stream cipher)

II Pe blocuri (block cipher)

1) Caesar

2) Afin

3) Hill

A	B	C	D	E	F	G
0	1	2	3	4	5	6
H	I	J	K	L	M	N
7	8	9	10	11	12	13
O	P	Q	R	S	T	U
14	15	16	17	18	19	20
V	W	X	Y	Z		
21	22	23	24	25		

Adaug $\underbrace{\quad}_{26}$ $\underbrace{\quad}_{27}$ $\underbrace{\quad}_{28}$

\Rightarrow lucrăm în \mathbb{Z}_{29}

Caesar - flux: o cheie pt tot mesajul

Ec. de criptare: $m + K = c$, $\forall m \in \text{Mesaj}$
K cheie
 $c \in \text{Cod}(afm)$

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



Ec de decriptare: $m = C - K$ ✓

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

Ex: Mesaj: MARTI ; $K = 13$

$$[M, A, R, T, i] \rightarrow [12, 0, 17, 19, 8] \xrightarrow{+K} \xrightarrow{+13}$$

$$[25, 13, 30, 32, 21] \xrightarrow{\text{mod } 26} [25, 13, 4, 6, 21]$$

→ ZNB DV

Concluzie: MARTI $\xrightarrow[+13]{\text{Caesar}}$ ZNB DV.

Decriptare: $[Z, N, B, D, V] \rightarrow [25, 13, 4, 6, 21] \xrightarrow[-K]{-13}$

$$\rightarrow [12, 0, -12, -10, 8] \xrightarrow{\text{mod } 26} [12, 0, 14, 16, 8] \rightarrow$$

→ MARTI ✓

Caesar pe blocuri fără padding

o cifră/bloc

≤ 1 bloc mai scurt

Ex: Mesaj: LABORATOR ; $b = 5$

→ LABOR ; $K_1 = 7$

ATOR ; $K_2 = 15$

$$[L, A, B, O, R] \rightarrow [11, 0, 1, 14, 17] \xrightarrow{+K_1} \xrightarrow{+7} [18, 7, 8, 21, 24]$$

→ SHIVY

$$[A, T, O, R] \rightarrow [0, 19, 14, 17] \xrightarrow[+15]{+K_2} [15, 34, 29, 32]$$

$$\xrightarrow{\text{mod } 29} [15, 5, 0, 3] \rightarrow \text{PFAD}$$

LABORATOR \rightarrow SHIVY PFAD

Caesar pe blocuri cu padding random
toate blocurile de aceeași
lungime, dar cu zgomot

Ex: Mesaj: MARTI, $b=3 \Rightarrow$

MAR ; $K_1=11$

TiE ; $K_2=12$

\hookrightarrow padding
random

$$[M, A, R] \rightarrow [12, 0, 17] \xrightarrow[+11]{+K_1} [23, 11, 28] \rightarrow \text{XL?}$$

$$[T, i, E] \rightarrow [19, 8, 4] \xrightarrow[+12]{+K_2} [31, 20, 16] \xrightarrow{\text{mod } 29} [2, 20, 16]$$

$$\rightarrow [C, U, Q]$$

MARTiE \rightarrow XL? CUQ
 \hookrightarrow zgomot

Examen: Criptare folosind Caesar-flux

mesaj = nume de familie, cheia = primul prenume
(sau invers).

Mesaj: MANEA

cheia: ADRIAN

$$\begin{array}{rcccccc} & M & A & N & E & A \\ & 12 & 0 & 13 & 4 & 0 \\ + & \left[\begin{array}{c} A & D & R & i & A \\ \rightarrow 0 & 3 & 17 & 8 & 0 \end{array} \right. \\ \hline & 12 & 3 & 30 & 12 & 0 \text{ mod } 29 \\ & 12 & 3 & 1 & 12 & 0 \\ & M & D & B & M & A \\ \hline \end{array}$$

Cifru afiu - flux

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

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

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

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

$$\xrightarrow{\text{mod } 29} [14, 7, 0, 6, 2] \rightarrow \text{OHAGC}$$

Decryption: OHAGC $\rightarrow [14, 7, 0, 6, 2] \xrightarrow{-K_2 \cdot K_1^{-1}} \begin{matrix} -7, \cdot 3^{-1} \\ -7, \cdot 10 \end{matrix}$

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

$$70 = 58 + 12$$

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

$$-50 = -58 + 8 = 8$$

MARTI

Hill - flux

Ec. de criptare:
$$\begin{pmatrix} \text{Matrice de} \\ \text{criptare} \end{pmatrix} \cdot \begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = \begin{pmatrix} C \\ 0 \\ D \end{pmatrix}$$

\downarrow $\in M_3(\mathbb{Z}_{29})$ $\swarrow \searrow$ $\in M_{3,1}(\mathbb{Z}_{29})$

Ec. de decriptare:
$$\begin{pmatrix} M \\ E \\ S \\ A \\ J \end{pmatrix} = \begin{pmatrix} \text{Matrice de} \\ \text{criptare} \end{pmatrix}^{-1} \cdot \begin{pmatrix} C \\ 0 \\ D \end{pmatrix}$$

Ex: $Message = A \cdot \Sigma_i$

$$M_C = \begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix}$$

$$\det M_C = 1 - 4 + 2 + 1 = 0$$

$\Rightarrow M_C$ nu este inversabilă
 \Rightarrow nu se poate realiza decriptarea!

$$\begin{pmatrix} A \\ Z \\ i \end{pmatrix} = \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 2 & 1 \\ 0 & 1 & 1 \\ -2 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 25 \\ 8 \end{pmatrix} = \begin{pmatrix} 58 \\ 33 \\ 17 \end{pmatrix} \bmod 29 = \begin{pmatrix} 0 \\ 4 \\ 17 \end{pmatrix} \begin{matrix} A \\ E \\ R \end{matrix}$$

Decriptare: $\det MC = 2$; $(\det MC)^{-1} = 2^{-1} = 15$

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

$$MC^{-1} = (\det MC)^{-1} \cdot MC^* = 15 \cdot \begin{pmatrix} -2 & 3 & 1 \\ -2 & 3 & 1 \\ 2 & -3 & -1 \end{pmatrix}$$

Exerciții

1. Criptati numele de familie cu cheia dată de luna de naștere, folosind Caesar flux - Decriptare.
2. Criptati primul prenume folosind Caesar pe blocuri, $b=3$. Cheie = ultimele cifre numele din nr. de telefon. Decriptare.
3. Criptati orașul de naștere cu cifrul afin - flux, $K1$ = luna de naștere, $K2$ = ziua de naștere.

4. Hill: Mesaj: YES

$$MC = \begin{pmatrix} -1 & 0 & 2 \\ 1 & 1 & -1 \\ 2 & 1 & 0 \end{pmatrix}.$$