

1342b/

Ecuații, sisteme, matrice în  $\mathbb{Z}_n$ CAESAR  
AFINEc. de gradul I

Ex:  $2x + 5 = 3$  în  $\mathbb{Z}_7$  <sup>solu</sup>  $2x = -2 \Rightarrow x = -1 = 6$

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

$$2x = 5 \text{ în } \mathbb{Z}_7 \mid \cdot 4 = 2^{-1}$$

$$2 \cdot 4 \cdot x = 5 \cdot 4 \Rightarrow x = 20 = 6 \Rightarrow \underline{x = 6}$$

Ex:  $5x + 2 = 1$  în  $\mathbb{Z}_{10}$

$$5x = 1 - 2 = -1 = 9 \mid \cdot 5^{-1} \text{ nu există în } \mathbb{Z}_{10}!$$

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

$5x = 9$  Rezolvăm prin încercări

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

 $\neq 9 \Rightarrow$  Ec. nu are soluție

Sisteme liniare

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

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

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

$\Rightarrow$  sist. este Cramer  $\Rightarrow$  are <sup>o</sup> sol. unică

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

$$\Rightarrow 17x = 7 \Rightarrow 3x = 0 \Rightarrow \underline{x = 0}$$

$$2x + 3y = 1 \Rightarrow 3y = 1 \cdot 3 = 3 \Rightarrow \underline{y = 1}$$

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

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_2(\mathbb{Z}_{10}); \det A = 4 - 6 = -2 = 8$$

$$\det A = 8 \notin U(\mathbb{Z}_{10}) \Rightarrow \det A \text{ este divizor al lui zero.} \\ (8 \cdot 5 = 0 \text{ in } \mathbb{Z}_{10})$$

$\Rightarrow$  Sist. NU este Cramer.

$$\begin{cases} x + 2y = 4 \cdot 2 \\ 3x + 4y = 1 \end{cases} \Rightarrow \begin{cases} 2x + 4y = 8 \\ \underline{3x + 4y = 1} \end{cases} \begin{array}{l} | \\ - \end{array}$$

$$\Rightarrow \underline{x = -7 = 3} \checkmark$$

$$x + 2y = 4 \Rightarrow 3 + 2y = 4 \Rightarrow 2y = 1 \Rightarrow y = 2^{-1} \text{ NU exista}$$

$\checkmark \left\{ \begin{array}{l} y = 2^{-1} \\ \text{in } \mathbb{Z}_{10} \end{array} \right.$

$\Rightarrow$  Sist. nu are solutie.

## Ex. de gradul I

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

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

$$\Delta = b^2 - 4ac = 9 + 4 = 13 = 3$$

$$\exists \sqrt{3} \text{ în } \mathbb{Z}_5? \quad \sqrt{3} = y \Leftrightarrow y^2 = 3 \text{ în } \mathbb{Z}_5 \text{ NU} \quad \curvearrowright$$

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} ; \quad \underset{\substack{\uparrow \\ \text{pătrate}}}{P(\mathbb{Z}_5)} = \{0, 1, 4\} \neq 3$$

$\Rightarrow \nexists \sqrt{3} \text{ în } \mathbb{Z}_5 \Rightarrow \text{ec. nu are soluții.}$

$$\underline{\text{Ex:}} \quad X^2 - 5X + 7 = 1 \text{ în } \mathbb{Z}_{11}$$

$$X^2 - 5X + 6 = 0 \text{ în } \mathbb{Z}_{11}$$

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

$$2^7 \text{ în } \mathbb{Z}_{11} = 6$$

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

$$\exists \sqrt{1} \text{ în } \mathbb{Z}_{11} \quad \Delta A \Rightarrow \sqrt{1} \in \{1, 10\}$$

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

$$x_2 = (5 - 1) \cdot 2^7 = 4 \cdot 6 = 24 = 2$$

Deci în  $\sqrt{1} = 10$

$$x_3 = (5 + 10) \cdot 2^7 = 15 \cdot 6 = 4 \cdot 6 = 2$$

$$x_4 = (5 - 10) \cdot 2^7 = -5 \cdot 6 = -30 = -22 - 8 = -8 = 3$$

NU sunt necesare!!

## Inverse matriciale $\rightarrow$ HILL

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

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

$$(\det A)^{-1} = 4^{-1} = 4$$

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

$$A^{-1} = (\det A)^{-1} \cdot A^* = 4 \cdot \begin{pmatrix} 1 & 1 & -1 \\ -2 & 2 & -2 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 4 & -4 \\ -8 & 8 & -8 \\ 4 & 4 & 12 \end{pmatrix}$$

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

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

$$\det A = -2 - 4 = -6 = 1 \in U(\mathbb{Z}_7) \Rightarrow \exists A^{-1}$$

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

$$A \rightarrow A^t = \begin{pmatrix} 2 & 1 & 0 \\ 1 & -2 & 2 \\ -1 & 1 & 0 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} -2 & -2 & -1 \\ 0 & 0 & -3 \\ 2 & -4 & -5 \end{pmatrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 1 \cdot A^* = A^* = \begin{pmatrix} -2 & -2 & -1 \\ 0 & 0 & -3 \\ 2 & -4 & -5 \end{pmatrix}$$

$$\Rightarrow A^{-1} = \begin{pmatrix} 5 & 5 & 6 \\ 0 & 0 & 4 \\ 2 & 3 & 2 \end{pmatrix}$$

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

Logarithmus diskret  $\longrightarrow$  DIFFIE-HELLMAN

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

Ex:  $\log_3 2 \in \mathbb{Z}_7$

$$\log_3 2 = x \Leftrightarrow 3^x = 2 \in \mathbb{Z}_7 \Rightarrow \underline{x=2}$$

$$3^0 = 1; 3^1 = 3; \underline{\underline{3^2 = 9 = 2}}$$

$$\Rightarrow \boxed{\log_3 2 = 2 \in \mathbb{Z}_7}$$

$$\text{Ex.: } \log_3 2 \in \mathbb{Z}_{11}$$

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

Sol1: Calculăm puterile lui 3 mod 11

n	0	1	2	3	4	5	6	7	8	9	10
$3^n \bmod 11$	1	3	9	5	4	1	3	9	5	4	1

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

$$\Rightarrow \log_3 2 \text{ nu ex. în } \mathbb{Z}_{11}^*$$

Teorema lui Lagrange pt grupuri

G grup finit cu n elemente,  $g \in G$

$$\Rightarrow \text{ord } g \mid n$$

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

! Multiplicativ, lucrăm în  $\mathbb{Z}_n^* \Rightarrow \# \mathbb{Z}_n^* = n-1$

Sol2: Soluția  $3^x = 2 \in \mathbb{Z}_{11}$  este sol.  $3^x = 11k + 2$

$$11k + 2 = \{2, 13, 24, 35, 46, 57, \dots \sim 3^{10}\}$$

$$59049$$

↑  
Cant puteri ale lui 3  
(dacă există)

# Algoritmi criptografici

Caesar } flux  
Afin } pe blocuri  
Hill }  $\begin{cases} \text{cu padding random} \\ \text{fără padding} \end{cases}$

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

Adăugăm:  $\begin{matrix} \text{L} & \cdot & ? \\ 26 & 27 & 28 \end{matrix} \Rightarrow \text{Lucrăm în } \mathbb{Z}_{29}$

Caesar: Flux (stream cipher) = 0 cheie pt tot mesajul

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

• Ec. de decriptare:  $m = c - K$   $\nearrow c \in \text{Cod (cifru)}$

Ex: Mesaj: MIERCURI ;  $K=11$

$$[M, i, E, R, C, U, R, i] \rightarrow [12, 8, 4, 17, 2, 20, 17, 8] \xrightarrow{+K, +11}$$

$$\rightarrow [23, 19, 15, 28, 13, 31, 28, 19] \xrightarrow{\text{mod } 29}$$

$$\rightarrow [23, 19, 15, 28, 13, 2, 28, 19] \rightarrow \text{XTP?NC?T}$$

$$\text{Conduzi: MIERCURI} \xrightarrow{+11} \text{XTP?NC?T}$$

(Caesar, flux)

Decriptare:

$$[X, T, P, ?, N, C, ?, T] \rightarrow [23, 19, 15, 28, 13, 2, 28, 19] \xrightarrow{-K, -11}$$

$$\rightarrow [12, 8, 4, 17, 2, \underline{-9}, 17, 8] \xrightarrow{\text{mod } 29} [12, 8, 4, 17, 2, 20, 17, 8]$$

$$\rightarrow \text{MIERCURI.}$$

Pe blocuri - făcând padding

↓  
câte o cifră  
pt. fiecare  
bloc

↓  
cel mult un bloc  
mai scurt

Ex: Mesaj: MIERCURI ; bloc=5  $\Rightarrow$  MIERC,  $K_1=12$   
URI,  $K_2=15$



$$[M, i, E, R, C] \rightarrow [12, 8, 4, 17, 2] \xrightarrow[+12]{+K1} [24, 20, 16, 29, 14] \\ \xrightarrow{\text{mod } 29} [24, 20, 16, 0, 14] \rightarrow [\gamma, u, Q, A, o] \rightarrow \gamma u Q A o$$

$$[u, R, i] \rightarrow [20, 17, 8] \xrightarrow[+15]{+K2} [35, 32, 23] \xrightarrow{\text{mod } 29}$$

$$[6, 3, 23] \rightarrow GDX$$

Concluzie: MIERCURI  $\rightarrow \gamma u Q A o GDX$

Caesar pe blocuri cu padding random

toate blocurile de aceeași lungime  
+ zigzagat

Ex. Mesaj: MARTI

bloc: 3  $\Rightarrow$  MAR  
TI E  $\rightarrow$  padding random

$$K1 = 10; K2 = 15$$

$$[M, A, R] \rightarrow [12, 0, 17] \xrightarrow[+10]{+K1} [22, 10, 27] \rightarrow$$

$$\rightarrow [W, k, \cdot] \rightarrow WK.$$

$$[T, i, E] \rightarrow [19, 8, 4] \xrightarrow[+15]{+K2} [34, 23, 19] \xrightarrow{\text{mod } 29} [5, 23, 19]$$

$$\rightarrow FXT$$

MARTIE  $\rightarrow$  WK.FXT

Cifru afin - Flux

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

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

Ex: Mesaj: AZI ;  $K_1 = 11$ ;  $K_2 = 17$

$$[A, Z, i] \rightarrow [0, 25, 8] \xrightarrow{\cdot K_1 + K_2 \atop \cdot 11 + 17} [17, 292, 105]$$

$$\xrightarrow{\text{mod } 29} [17, 2, 18] \rightarrow \text{RCS}$$

AZI afin  $\rightarrow$  RCS

$$\text{decriptare: } [R, c, s] \rightarrow [17, 2, 18] \xrightarrow{\frac{-K_2 \cdot K_1^{-1}}{-17 \cdot 8}} [0, -120, 8]$$

$$\xrightarrow{\text{mod } 29} [0, 25, 8] \rightarrow \text{AZI.}$$

$$-120 = -116 - 4 = -4 = 25$$

"0

Hill : Flux

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

$$\text{Matricea de criptare} \in M_3(\mathbb{Z}_{29})$$

$$\text{Mesaj, Cod} \in M_{3,1}(\mathbb{Z}_{29})$$

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

$$\text{Ex: Mesaj: URA, } MC = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} \in M_3(\mathbb{Z}_{29})$$

$$(U, R, A) \rightarrow \begin{pmatrix} 20 \\ 17 \\ 0 \end{pmatrix}$$

$$\text{Criptarea: } \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 17 \\ 0 \end{pmatrix} = \begin{pmatrix} 57 \\ 17 \\ 14 \end{pmatrix} \text{ mod } 29$$

$$= \begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix} = ?RO$$

Decriptarea:  $A = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} = MC$

$$\det A = -2 - 1 - 8 = -11 = 18 \in U(\mathbb{Z}_{29})$$

$$(\det A)^{-1} = 18^{-1} = 21$$

$$A \rightarrow A^t = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} \rightarrow A^* = \begin{pmatrix} -4 & -2 & 3 \\ -2 & -1 & -4 \\ 1 & -5 & 2 \end{pmatrix}$$

$$A^{-1} = (\det A)^{-1} \cdot A^* = 21 \cdot \begin{pmatrix} -4 & -2 & 3 \\ -2 & -1 & -4 \\ 1 & -5 & 2 \end{pmatrix}$$

$$\begin{pmatrix} ? \\ R \\ 0 \end{pmatrix} = \begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix} \rightarrow 21 \cdot \begin{pmatrix} -4 & -2 & 3 \\ -2 & -1 & -4 \\ 1 & -5 & 2 \end{pmatrix} \begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix} = \begin{pmatrix} 20 \\ 17 \\ 0 \end{pmatrix}$$

$\downarrow$   
 $-8$

$\downarrow$   
 $\begin{pmatrix} -1 \\ -12 \\ -15 \end{pmatrix}$

Examen: Criptat în Caesar flux numele de familie  
cu cheia prenumele (sau invers).

NF: MANĒA = Mesaj

p : ADRIAN = Chei

$$\begin{array}{ccccc} M & A & N & E & A \\ + & + & + & + & + \\ A & D & R & I & A \end{array}$$
$$\begin{array}{r} 12 \\ + \\ 0 \end{array} \quad \begin{array}{r} 0 \\ + \\ 3 \end{array} \quad \begin{array}{r} 13 \\ + \\ 17 \end{array} \quad \begin{array}{r} 4 \\ + \\ 8 \end{array} \quad \begin{array}{r} 0 \\ + \\ 0 \end{array}$$

$12 \ 3 \ 30 \ 12 \ 0 \xrightarrow{\text{mod } 29} 12 \ 3 \ 1 \ 12 \ 0$   
 $\downarrow$

M D B M A

Tema: 1) Caesar flux, Mesaj = numele de familie  
Cheia = luna nașterii  
+ decriptare

2) Caesar pe blocuri, fără padding, Mesaj = numere,  
 Blocuri = 3, Chei = ultimele cifre din nr. telefon  
 + decriptare

3) Afin flux, Mesaj: Inasul nasterii  
cheie 1 = luna nasterii, cheie 2 = ziua nasterii  
+ decriptare

4) Hill, Message =  $foi$  ;  $MC = \begin{pmatrix} 2 & 1 & -1 \\ 2 & 1 & 0 \\ -1 & -2 & -1 \end{pmatrix}$