1342a)

Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $5x+3=1$ în $\mathbb{Z}_{11}$

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

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

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

$x=4$

Ex: $6x+5=2$ în $\mathbb{Z}_{10}$

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

$6x = 7 \quad |\cdot 6^{-1}$ 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: $A = \begin{pmatrix} 3 & 2 \\ 5 & -3 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_7)$

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

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

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

$$x = 3(2+3y) = 6+9y = \underline{6+2y}$$

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

$18+6y+2y=1$

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

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

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

$a^{-1} = \dfrac{1}{a}$ $\qquad a^{-1}\cdot \underline{a} = \dfrac{1}{a}\cdot a = \underline{1}$

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

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

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

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

$$\begin{cases} 2x+3y=5 \\ x+4y=1 \quad | \cdot 2 \end{cases} \Rightarrow \begin{cases} 2x+3y=5 \\ 2x+8y=2 \end{cases} \quad (-)$$

$$5y=-3=7$$

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 $\mathbb{Z}_{10}$

$\Rightarrow S=\emptyset.$

Ec. de gradul II

Ex: $2x^2-3x+1=0$ în $\mathbb{Z}_5$

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

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

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

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

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

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

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

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 $\mathbb{Z}_7$? $\quad \sqrt{3}=n \iff n^2=3$ în $\mathbb{Z}_7$

$\mathbb{Z}_7=\{0,1,2,3,4,5,6\}$ $\quad P(\mathbb{Z}_7)=\{0,1,4,2\}\not\ni 3$

pătrate

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

Logaritmi în $\mathbb{Z}_n$

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

Ex: $\log_2 3$ în $\mathbb{Z}_7$

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

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

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

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

Teorema lui Lagrange pt grupuri

G grup, $\#G = n$.

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

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 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	$\boxed{3}$	4	$\boxed{5}$	6	7	8	9	10
3^a în $\mathbb{Z}_{11}$	1	3	9	$\boxed{5}$	4	$\boxed{1}$					1

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

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

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

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

Inverse matriceale $\mathcal{M}_3(\mathbb{Z}_n)$

Teoremă $A \in \mathcal{M}_n(\mathbb{Z}_t)$ este inversabilă $\Leftrightarrow$

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

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

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

Ex: $A = \begin{pmatrix} 3 & 1 & 2 \\ -1 & 0 & -2 \\ 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$

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

$\Rightarrow$ există A^{-1}

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

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

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

$\Rightarrow A^{-1} = \begin{pmatrix} 3 & 5 & 4 \\ 2 & 5 & 6 \\ 2 & 4 & 5 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_7)$

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 ␣ 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

$Enc(m) = m + K$

K cheie

$C \in$ Cod (Cifru)

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

$Dec(c) = C - K$

Exemplu: Mesaj = MARTI
Cheia = 11

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

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

→ XL?BT

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

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

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

→ 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

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

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

→ ?AXT.Q

$[R, I, E] \rightarrow [17, 8, 4] \xrightarrow[+21]{+K2} [38, 29, 25] \xrightarrow[\text{mod } 29]{}$

$[9, 0, 25] \rightarrow$]AZ

NOIEMBRIE → ?AXT.Q]AZ

b) Cu padding random: toate blocurile au aceeași lungime

Ex: Mesaj: MARTI
b = 3

⇒ MAR ; K1 = 5
TIE ; K2 = 7
↳ padding random

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

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

MARTIE → RFW␣PL

Ex. suplimentar

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

Ex: NF: MANEA

P: ADRIAN

$$
\begin{array}{rccccc}
 & M & A & N & E & A \\
 & 12 & 0 & 13 & 4 & 0 \\
+ & A & D & R & I & A \\
 & 0 & 3 & 17 & 8 & 0 \\
\hline
 & 12 & 3 & 30 & 12 & 0 \ \bmod 29 \\
 & \downarrow & & & & \\
 & 12 & 3 & 1 & 12 & 0 \\
 & M & D & B & M & A
\end{array}
$$

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 ; $K1 = 3$; $K2 = 7$

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

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

Decriptare: (OHAGC) $\to [14, 7, 0, 6, 2] \xrightarrow{-K_2;\cdot K_1^{-1}}$
$-7;\cdot 3^{-1}$
$-7;\cdot 10$

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

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

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

$\to$ MARTI

Hill - flux

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

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

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

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

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

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

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

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

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

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

Exerciții

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

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

Teste de primalitate

INPUT: $n \in \mathbb{N}$

OUTPUT: n prim/compus

1) Ciurul / Sita lui Eratostene
2) Testul Fermat
3) Testul Solovay - Strassen

Teste
- sigure (deterministe)
- probabiliste

Ciurul lui Eratostene

INPUT: $n \in \mathbb{N}$

OUTPUT: lista de nr prime $\leq n$

Ex: $n = 20$

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\boxed{7}$ $\cancel{8}$ $\cancel{9}$ $\cancel{10}$

$\boxed{11}$ $\cancel{12}$ $\boxed{13}$ $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ $\boxed{17}$ $\cancel{18}$ $\boxed{19}$

$\cancel{20}$

Alternativă: Putem decide dacă n este prim.

n = 13 $\quad \boxed{2} \quad \boxed{3} \quad \cancel{4} \quad \boxed{5} \quad \cancel{6} \quad \boxed{7}$

$\cancel{8} \quad \cancel{9} \quad \cancel{10} \quad \boxed{11} \quad \cancel{12} \quad \boxed{13} \leftarrow$ 13 prim

Testul Fermat

Mica Teoremă a lui Fermat (~ sec XVII)

n prim $\Rightarrow a^{n-1} \equiv 1 \bmod n, \forall a \in \{1, \dots, n-1\}$

Echivalent: n prim $\Rightarrow \forall a \in \mathbb{Z}_n^*, a^{n-1} = 1.$

Ex: $n = 7 \Rightarrow \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\forall a \in \mathbb{Z}_7^*, \ a^6 = 1$?

$1^6 = 1$ ok

$2^6 = 64 = 63 + 1 = 1$ ok

$3^6 = (3^2)^3 = 2^3 = 1$ ok

$4^6 = (2^2)^6 = (2^6)^2 = 1$ ok

$5^6 = (-2)^6 = 2^6 = 1$ ok

$6^6 = 2^6 \cdot 3^6 = 1$ ok

$\Rightarrow n = 7$ prim.

Ex: $n=9$ $\quad \mathbb{Z}_9^* = \{1,2,3,4,5,6,7,8\}$

$a^8 = 1$ în $\mathbb{Z}_9^*$, $\forall a \in \mathbb{Z}_9^*$?

$1^8 = 1$ OK

$2^8 = (2^3)^2 \cdot 2^2 = (-1)^2 \cdot 2^2 = 2^2 = 4 \neq 1$

$\Rightarrow n=9$ compus, $a=2$ witness (martor)

Testul Fermat probabilist

Încerc t mostre $a \in \mathbb{Z}_n^*$ și aplic MTF doar pt ele $\Rightarrow$ concluzie cu prob $= \frac{t}{n-1}$.

Ex: $n=17$ $\quad t=3$ $\quad a \in \{12, 5, 10\}$

$a=12 \Rightarrow 12^{16} = 1$ în $\mathbb{Z}_{17}^*$?

$12^{16} = (2^2 \cdot 3)^{16} = 2^{32} \cdot 3^{16} = (2^4)^8 \cdot (3^4)^4$

$= \underbrace{(-1)^8}_{1} \cdot (-4)^4 = 4^4 = (2^2)^4 = (2^4)^2 = (-1)^2 = 1$

OK

$a=5 \Rightarrow 5^{16} = (5^3)^5 \cdot 5 = 6^5 \cdot 5$

$= 2^5 \cdot 3^5 \cdot 5 = \underbrace{2^4}_{(-1)} \cdot 2 \cdot \underbrace{3^4}_{-4} \cdot 3 \cdot 5 = 4 \cdot 2 \cdot 3 \cdot \underbrace{5}_{-2}$

$= 8 \cdot (-2)$

$= -16 = 1$ ok

$a=10 \Rightarrow 10^{16} = 2^{16} \cdot \underbrace{5^{16}}_{1} = (2^4)^4 = (-1)^4 = 1$ ok

$\Rightarrow n=17$ prim probabil, prob $= \frac{3}{16}$.

Simbolul lui Jacobi

n impar, $b \in \mathbb{N}$

Def. $\left(\frac{b}{n}\right) = \begin{cases} 0 & \text{dacă } n \mid b \\ 1 & \text{dacă } b \text{ este pătrat în } \mathbb{Z}_n^* \\ -1 & \text{în rest} \end{cases}$

Ex: $\left(\frac{2}{5}\right) = -1$

x	1	2	3	4
x^2	1	4	4	1

$\mathbb{Z}_5^*$

Ex: $\left(\frac{4}{7}\right)=1$ pt că $4=2^2=5^2$ în $\mathbb{Z}_7$

Ex: $\left(\frac{13}{11}\right)=\left(\frac{2}{11}\right)=-1$

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	4	3	5	9	4	1

$\mathbb{Z}_{11}^*$

Ex: $\left(\frac{21}{3}\right)=0$ pt că $3 \mid 21$

$\quad\Downarrow$

$\left(\frac{0}{3}\right)=0$ pt că $3 \mid 0$

Testul Solovay-Strassen

Teoremă: n prim $\Rightarrow$ $a^{\frac{n-1}{2}}=\left(\frac{a}{n}\right)$ în $\mathbb{Z}_n^*$, $\forall a \in \mathbb{Z}_n^*$.

Ex: $n=7 \overset{?}{\Rightarrow} a^{\frac{7-1}{2}}=a^3=\left(\frac{a}{7}\right)$ în $\mathbb{Z}_7^*$

$a=1 \Rightarrow 1^3=1$; $\left(\frac{1}{7}\right)=1$ pt că $1=1^2$

$a=2 \Rightarrow 2^3=8=1$; $\left(\frac{2}{7}\right)=1$ pt că $2=3^2=4^2$

x	1	2	$\boxed{3}$	4	5	6
x^2	1	4	$\boxed{2}$	2	4	1

$\mathbb{Z}_7^*$

$a=3 \Rightarrow 3^3 = 27 = 6 = -1 \; ; \; \left(\frac{3}{7}\right) = -1$

$a=4 \Rightarrow 4^3 = (2^2)^3 = (2^3)^2 = 1 \; ; \; \left(\frac{4}{7}\right) = 1$ pt că $4 = 2^2 = 5^2$

$a=5 \Rightarrow 5^3 = (-2)^3 = -2^3 = -1 \; ; \; \left(\frac{5}{7}\right) = -1$

$a=6 \Rightarrow 6^3 = 2^3 \cdot 3^3 = 1 \cdot (-1) = -1 \; ; \; \left(\frac{6}{7}\right) = -1$

$\Rightarrow n=7$ prim.

Ex: $n=15 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_{15}^*, \; a^7 = \left(\frac{a}{15}\right)$ în $\mathbb{Z}_{15}^*$

$a=1$ ok

$a=2 \Rightarrow 2^7 = 2^4 \cdot 2^3 = 1 \cdot 2^3 = 8$

$\left(\frac{a}{15}\right) \neq 8, \forall a$

$\Rightarrow a=2$ martor

$n=15$ compus.