13.42b

Ecuații, sisteme, matrice în $\mathbb{Z}_n$

CAESAR
AFIN

Ec. de gradul I

Ex: $2x+5=3$ în $\mathbb{Z}_7$

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

sau $2x=-2 \Rightarrow x=-1=6$

$2x=5$ 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 $\mathbb{Z}_{10}$

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

Teoremă a este inversabil în $\mathbb{Z}_n \Leftrightarrow$ cmmdc$(a,n)=1$

$5x=9$ 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 soluții

Sisteme liniare

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

Matricea sistemului $A=\begin{pmatrix} 2 & 3 \\ 5 & -1 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_7)$

$\det A=-2-15=-17=\underset{0}{-14}-3=-3=4\in U(\mathbb{Z}_7)$

$\Rightarrow$ sist. este Cramer $\Rightarrow$ are sol. unică

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

$(+)$

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

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

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

$A=\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_{10})$; $\det A = 4-6=-2=8$

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

$(8 \cdot 5 = 0$ în $\mathbb{Z}_{10})$

$\Rightarrow$ <u>Sist NU este Cramer</u>.

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

$\Rightarrow \underline{x=-7=3}$ ✓

$x+2y=4 \Rightarrow 3+2y=4 \Rightarrow 2y=1 \Rightarrow y=2^{-1}$ NU există în $\mathbb{Z}_{10}$ ✗

$\Rightarrow$ <u>Sist. nu are soluții</u>.

Ec. de gradul II

Ex: $x^2+3x-1=0$ în $\mathbb{Z}_5$

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

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

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

$\mathbb{Z}_5=\{0,1,2,3,4\}$; $P(\mathbb{Z}_5)=\{0,1,4\}\not\ni 3$

pătrate

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

Ex: $x^2-5x+7=1$ în $\mathbb{Z}_{11}$

$x^2-5x+6=0$ în $\mathbb{Z}_{11}$ $\qquad 2^{-1}$ în $\mathbb{Z}_{11}=6$

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

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

$\exists\sqrt{1}$ în $\mathbb{Z}_{11}$ DA $\Rightarrow \sqrt{1}\in\{1,\underset{}{\overset{-1}{\overset{\shortparallel}{10}}}\}$

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

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

Dacă iau $\sqrt{1}=10$ — Nu sînt necesare!!

$x_3=(5+10)\cdot 2^{-1}=15\cdot 6=4\cdot 6=2$

$x_4=(5-10)\cdot 2^{-1}=-5\cdot 6=-30=-22-8=-8=3$

Inverse matriceale $\longrightarrow$ 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

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

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

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

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

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

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

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

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

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

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

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

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

Logaritmul discret $\longrightarrow$ DIFFIE-HELLMAN

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

Ex.: $\log_3 2$ în $\mathbb{Z}_7$

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

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

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

Ex.: $\log_3 2$ în $\mathbb{Z}_{11}$

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

Sol1: Calculez puterile lui 3 mod 11

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

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

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

Teorema lui Lagrange pt grupuri

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

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

În particular, $g^n = e$, el. neutru.

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

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

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

$3^{10} = 59049$

Caut puteri ale lui 3 (dacă există)

Algoritmi criptografici

Caesar
Afin } flux
Hill } pe blocuri < cu padding random / fără padding

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: ␣ (26), . (27), ? (28) $\Rightarrow$ Lucrăm în $\mathbb{Z}_{29}$

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

- Ec. de criptare: $m + K = c$, $\forall\, m \in$ Mesaj, K = cheie, $c \in$ Cod (cifru)
- Ec. de decriptare: $m = c - K$

Ex: Mesaj: MIERCURI ; K=11

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

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

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

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

(Caesar, flux)

Decriptare:

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

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

$\rightarrow$ MIERCURI.

Pe blocuri – fără padding

$\downarrow$ câte o cheie pt. fiecare bloc

$\downarrow$ cel mult un bloc mai scurt

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

$[M, i, E, R, C] \to [12, 8, 4, 17, 2] \xrightarrow[+12]{+K1} [24, 20, 16, 29, 14]$

$\xrightarrow[mod\ 29]{} [24, 20, 16, 0, 14] \to [Y, U, Q, A, O] \to YUQAO$

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

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

Concluzie: MIERCURI $\to$ YUQAOGDX

Caesar pe blocuri cu padding random

toate blocurile de aceeași lungime

+ zgomot

Ex. Mesaj: MARTI

bloc: 3 $\Rightarrow$ MAR

TI E $\to$ padding random

$K1 = 10$; $K2 = 15$

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

$\to [W, K, .] \to WK.$

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

$\to FXT$

MARTIE → WK.FXT

Cifrul afin - Flux

Ec. de criptare: $m \cdot K1 + K2 = c$, $\forall m \in$ Mesaj

K1, K2 chei

$c \in$ Cod

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

Ex: Mesaj: AZi ; K1 = 11 ; K2 = 17

$[A, Z, i] \to [0, 25, 8] \xrightarrow[\cdot 11 + 17]{\cdot K1 + K2} [17, 292, 105]$

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

$AZi \xrightarrow{\text{afin}} RCS$

Decriptare: $[R, C, S] \to [17, 2, 18] \xrightarrow[-17 \cdot 8]{-K2 \cdot K1^{-1}} [0, -120, 8]$

$\xrightarrow[\text{mod } 29]{} [0, 25, 8] \to AZi$.

$-120 = \underset{\overset{\shortparallel}{0}}{-116} - 4 = -4 = 25$

Hill: Flux

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

Matricea de criptare $\in \mathcal{M}_3(\mathbb{Z}_{29})$

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

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

Ex: Mesaj: URA ; $MC = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & 2 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{Z}_{29})$

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

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

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

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

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

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

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

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

$$\begin{pmatrix} ? \\ R \\ 0 \end{pmatrix} = \begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix} \longrightarrow \underbrace{21}_{-8} \cdot \begin{pmatrix} -4 & -2 & 3 \\ -2 & -1 & -4 \\ 1 & -5 & 2 \end{pmatrix} \underbrace{\begin{pmatrix} 28 \\ 17 \\ 14 \end{pmatrix}}_{\begin{pmatrix} -1 \\ -12 \\ -15 \end{pmatrix}} = \begin{pmatrix} 20 \\ 17 \\ 0 \end{pmatrix}$$

<u>Examen</u>: Criptați cu Caesar flux numele de familie cu cheia prenumele (sau invers).

NF: MANEA = Mesaj
P : ADRIAN = Chei

$$\begin{array}{ccccc} M & A & N & E & A \\ + & + & + & + & + \\ A & D & R & I & A \end{array}$$

$$\begin{array}{ccccc} 12 & 0 & 13 & 4 & 0 \\ + & + & + & + & + \\ 0 & 3 & 17 & 8 & 0 \\ \hline 12 & 3 & 30 & 12 & 0 \end{array} \xrightarrow[\text{mod } 29]{} 12\ 3\ 1\ 12\ 0$$

$\downarrow$

MDBMA

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

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

3) Afin flux, Mesaj: Orașul nașterii
cheie 1 = luna nașterii, cheie 2 = ziua nașterii
+ decriptare

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

Teste de primalitate

INPUT: $n \in \mathbb{N}$ (n impar)

OUTPUT: n prim/compus

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

- Varianta deterministă = sigură
  + 100% certitudine
  - ineficientă
- Varianta probabilistă
  - probabilitate
  + rapidă
  +/- sigur compus/probabil prim

Ciurul lui Eratostene - Variantă sigură

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

OUTPUT: lista de nr prime $\leq n$

Ex: $n = 25$

$\boxed{2}$ $\boxed{3}$ $\cancel{4}$ $\boxed{5}$ $\cancel{6}$ $\boxed{7}$ $\cancel{8}$ $\cancel{9}$ $\cancel{10}$ $\boxed{11}$ $\cancel{12}$ $\boxed{13}$

$\cancel{14}$ $\cancel{15}$ $\cancel{16}$ $\boxed{17}$ $\cancel{18}$ $\boxed{19}$ $\cancel{20}$ $\cancel{21}$ $\cancel{22}$ $\boxed{23}$ $\cancel{24}$

$\cancel{25}$ OUTPUT: 2, 3, 5, 7, 11, 13, 17, 19, 23 prime ≤ 25

Testul Fermat – Varianta deterministă

Mica Teoremă Fermat

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

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

Exemplu: $n = 7 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_7, \ a^6 = 1$ în $\mathbb{Z}_7$

$a = 1 \Rightarrow 1^6 = 1$ ✓

$a = 2 \Rightarrow 2^6 = 64 = 63 + 1$ ✓

$a = 3 \Rightarrow 3^6 = (3^2)^3 = (9)^3 = 2^3 = 8 = 7 + 1$ ✓

$a = 4 \Rightarrow 4^6 = (2^6)^2 = 1^2 = 1$ ✓

$a = 5 \Rightarrow 5^6 = (-2)^6 = 2^6 = 1$ ✓

$a = 6 \Rightarrow 6^6 = 2^6 \cdot 3^6 = 1 \cdot 1 = 1$ ✓

$\Rightarrow 7$ este sigur prim (cf. Fermat)

Exemplu: $n = 9 \overset{?}{\Rightarrow} \forall a \in \mathbb{Z}_9, \ a^8 = 1$ în $\mathbb{Z}_9$

$a = 1 \Rightarrow 1^8 = 1$ ✓

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

$\Rightarrow n = 9$ nu este prim, $a = 2$ martor (witness)

Fermat - probabilist

Testez (aleatoriu) mostre $a \in \mathbb{Z}_n$ dacă

$$a^{n-1} = 1 \text{ în } \mathbb{Z}_n.$$

Exemplu: $n = 17$, $t = 3$ mostre, $a \in \{3, 4, 5\}$

- $a = 3 \Rightarrow 3^{16} = 1$ în $\mathbb{Z}_{17}$

$$(3^4)^4 = (81)^4 = (-4)^4 = 2^8 = (2^4)^2 = 16^2 = (-1)^2 = 1 \checkmark$$

- $a = 4 \Rightarrow 4^{16} = 1$ în $\mathbb{Z}_{17}$

$$(4^4)^4 = (2^8)^4 = 1^4 = 1 \checkmark$$

- $a = 5 \Rightarrow 5^{16} = 1$ în $\mathbb{Z}_{17}$

$$(5^3)^5 \cdot 5 = 125^5 \cdot 5 = 6^5 \cdot 5 = 2^5 \cdot 3^5 \cdot 5$$

$$= 2^4 \cdot 2 \cdot 3^4 \cdot 3 \cdot 5 = 16 \cdot 81 \cdot 2 \cdot 15 = (-1) \cdot (-4) \cdot 2 \cdot (-2) = -16 = 1 \checkmark$$

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

Simbolul Jacobi

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

n impar

Ex: $\left(\frac{2}{7}\right) = ?$ $\quad 7 \nmid 2$

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

în $\mathbb{Z}_7^*$

2 este pătrat în $\mathbb{Z}_7 \Rightarrow \left(\frac{2}{7}\right) = 1$

Ex: $\left(\frac{12}{3}\right) = 0$ pt că $3 \mid 12$

Ex: $\left(\frac{3}{5}\right) = -1$

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

în $\mathbb{Z}_5$

Testul Solovay-Strassen-Sigma

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

Ex: $n=7 \overset{?}{\Rightarrow} b^{\frac{7-1}{2}} = b^3 = \left(\frac{b}{7}\right), \forall b \in \mathbb{Z}_7$?

$\cdot\ b=1 \Rightarrow 1^3 = \left(\frac{1}{7}\right)$

$1 = 1$ pt că $1=1^2$ în $\mathbb{Z}_7$

$\cdot\ b=2 \Rightarrow 2^3 = \left(\frac{2}{7}\right)$

$8=1 \quad 1$ pt că $2=3^2$ în $\mathbb{Z}_7$

$\cdot\ b=3 \Rightarrow 3^3 = 27 = 6 = -1$

$\left(\frac{3}{7}\right) = -1$

x	1	2	3	4	5	6
x^2	1	4	1	2	4	1

$\cdot\ b=4 \Rightarrow 4^3 = 2^6 = 64 = 63+1 = 1$

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

$\cdot\ b=5 \Rightarrow 5^3 = 25\cdot 5 = 4\cdot 5 = 20 = 6 = -1$

$\left(\frac{5}{7}\right) = -1$

$\cdot\ b=6 \Rightarrow 6^3 = 2^3\cdot 3^3 = 1\cdot(-1) = -1$

$\left(\frac{6}{7}\right) = -1$

$\Rightarrow n=7$ sigur prim (Solovay-Strassen)

Ex: $n=15 \Rightarrow b^{\frac{15-1}{2}} = \left(\frac{b}{15}\right), \forall b \in \mathbb{Z}_{15}^*$

$\qquad\quad \| $

$\qquad\; b^7$

• $b=1 \Rightarrow 1^7 = 1$; $\left(\frac{1}{15}\right) = 1$ pt că $1 = 1^2$

• $b=2 \Rightarrow 2^7 = 2^4 \cdot 2^3 = 16 \cdot 8 = 1 \cdot 8 = 8$

$\left(\frac{2}{15}\right) \neq 8 \Rightarrow 2$ martor $\Rightarrow n=15$ compus.

<u>Varianta probabilistă</u>

Aleg t mostre $b \in \mathbb{Z}_n^*$, $b^{\frac{n-1}{2}} = \left(\frac{b}{n}\right)$ în $\mathbb{Z}_n$

$\Rightarrow$ răspuns
- sigur nu (dacă găsesc martor)
- probabil da ($p = \frac{t}{n-1}$).