1342b

Aritmetică modulară (în $\mathbb{Z}_n$)

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

$(\mathbb{Z}_n, +, \cdot)$ inel comutativ

$\rightarrow (\mathbb{Z}_n, +)$ grup comutativ

$\rightarrow (\mathbb{Z}_n^*, \cdot)$ monoid comutativ

$U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid x$ este inv. față de „$\cdot$"$\}$

$U(\mathbb{Z}_n) \neq \mathbb{Z}_n$

Ex: $\mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$

$-3 =$ opusul lui $3 = x$ pt care $x + 3 = 0$

$-3 = 4$

$3^{-1} =$ inversul lui $3 = y$ pt care $3 \cdot y = 1$

$3^{-1} = 5$ pt că $3 \cdot 5 = 15 = 1$.

Teoremă: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{cmmdc}(x, n) = 1\}$

Obs: $(U(\mathbb{Z}_n), \cdot)$ grupul unităților

$\mathbb{Z}_{10}$ $\quad U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$

4^{-1} nu există

$3^{-1} = 7$ pt că $3 \cdot 7 = 21 = 1 \mod 10$

$\mathbb{Z}_{26}$ $\qquad$ $\mathbb{Z}_{29}$

A	B	C	D	...	Z	␣	.	?
0	1	2	3		25	26	27	28

$5x + 2 = 1$ în $\mathbb{Z}_7$

$5x = -1 \quad | \cdot 5^{-1} = 3$

$5^{-1} \cdot 5 \cdot x = (-1) \cdot 5^{-1}$

$x = (-1) \cdot 3 = -3 = 4$

$3x^2 + x - 2 = 0$ în $\mathbb{Z}_{11}$

$\Delta = 1 - 4 \cdot (-2) \cdot 3 = 1 + 24 = 25 = 3$

$\sqrt{a} = b \iff a = b^2$

$\sqrt{3}$ în $\mathbb{Z}_{11} = \{5, 6\} = \{5, -5\}$

$$x_{1,2} = \left(-1 \pm \sqrt{\Delta}\right) \cdot 6^{-1}$$

$$\sqrt{3} = 5 \Rightarrow x_1 = (-1+5) \cdot 6^{-1} = 4 \cdot 2 = 8$$

$$x_2 = (-1-5) \cdot 6^{-1} = -6 \cdot 2 = -12$$

$$= -\underset{0}{11} - 1 = -1 = 10.$$

$$\Rightarrow x \in \{8, 10\}$$

Logaritmul discret

$$\log_a b = c \Rightarrow a^c = b$$

$\log_2 3$ în $\mathbb{Z}_5 = x \Leftrightarrow 2^x = 3$ în $\mathbb{Z}_5$

$$2^0 = 1;\ 2^1 = 2;\ 2^2 = 4;\ 2^3 = 8 = 3$$

$\Rightarrow \log_2 3 = 3$ în $\mathbb{Z}_5$

D-H: $\underbrace{\log_{7131} 5247}_{x}$ în $\mathbb{Z}_{21733}$

$$\Rightarrow 7131^x = 5247 \bmod 21733$$

Teorema lui Lagrange

$(G, \cdot)$ grup, $\# G = n$

$\forall g \in G, \; g^n = e.$

9^{52} în $\mathbb{Z}_{11}$

$$9^{52} = (9^2)^{26} = (81)^{26} = 4^{26} = (4^2)^{13}$$

$$= 5^{13} = (5^2)^6 \cdot 5 = 3^6 \cdot 5 = (3^3)^2 \cdot 5$$

$$= 5^2 \cdot 5 = 3 \cdot 5 = 4.$$

$A \in \mathcal{M}_n(\mathbb{Z}_t) \qquad A^{-1} = (\det A)^{-1} \cdot A^* \text{ există}$

$\Leftrightarrow (\det A)^{-1} \text{ există} \Leftrightarrow \text{cmmdc}(\det A, t) = 1.$

Cifruri bazate pe $\mathbb{Z}_n$

$\mathbb{Z}_{29}$

A	B	C	D	...	Z	␣	.	?
0					25	26	27	28

cifruri

1) flux (stream): aceeași cheie pt tot mesajul
2) pe blocuri (block): 1 cheie / bloc
   a) cu padding: toate blocurile au aceeași lungime
   b) fără padding, ≤ 1 bloc mai scurt

Caesar

$c = m + K$ în $\mathbb{Z}_{29}$

Flux: Ec. de criptare: Cod = Mesaj + Cheie

Ec. de decriptare: Mesaj = Cod − Cheie

Ex: Mesaj: LUNI ; Cheia = 35

$$[L, U, N, I] \to [11, 20, 13, 8] \xrightarrow[+35]{+K}$$

$$[46, 55, 48, 43] \xrightarrow{\% 29} [17, 26, 19, 14]$$

$$\to [R, ␣, T, O] : R␣TO$$

Decriptarea:

$[R, L, T, O] \to [17, 26, 19, 14] \xrightarrow[-35]{-k}$

$[-18, -9, -16, -21] \xrightarrow{\% 29} [11, 20, 13, 8]$

$\to$ LUNI.

Pe blocuri: fără padding:

Mesaj: NOIEMBRIE

Bloc: 5 $\Rightarrow$ b1: NOIEM K1: 10

b2: BRIE K2: 15

$[N, O, I, E, M] \to [13, 14, 8, 4, 12] \xrightarrow{+10}$

$\to [23, 24, 18, 14, 22] \to$ XYSOW

$[B, R, I, E] \to [1, 17, 8, 4] \xrightarrow{+15} [16, 32, 23, 19]$

$\xrightarrow{\% 29} [16, 3, 23, 19] \to$ QDXT

NOIEMBRIE $\to$ XYSOW QDXT

cu padding:

Mesaj: NOIEMBRIE

Bloc: 5 ⇒ NOIEM   K1: 10

BRIEM   K2: 15

NOIEM → XYSOW

BRIEM → QDXT.

12+15=27

NOIEMBRIEM → XYSOWQDXT.

Afin: Ec. de criptare: Cod = Mesaj · K1 + K2

$c = mk_1 + k_2$

Ec. de decriptare: mesaj = (Cod − K2) · $K1^{-1}$

$m = (c - K2)\, k_1^{-1}$

Ex: Mesaj: LUNI   Flux.

K1 = 5 ; K2 = 11

$[L, U, N, I] \to [11, 20, 13, 8] \xrightarrow[\cdot 5+11]{\cdot K1+K2}$

$[66, 111, 76, 51] \xrightarrow{\% 29} [8, 24, 18, 22]$

$[i, Y, S, W]$

LUNI $\rightarrow$ iYSW.

Decriptare: 5^{-1} în $\mathbb{Z}_{29} = 6$

$[8, 24, 18, 22] \xrightarrow{-11 \cdot 6} [11, 20, 13, 8] \rightarrow$ LUNI.

Hill

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

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

Ex: Mesaj: Joi $\rightarrow \begin{pmatrix} J \\ o \\ i \end{pmatrix} \rightarrow \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$

$MC: \begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 1 \\ 0 & -5 & 2 \end{pmatrix}$

$$\begin{pmatrix} 1 & -1 & 3 \\ 2 & -2 & 1 \\ 0 & -5 & 2 \end{pmatrix} \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 19 \\ -2 \\ -54 \end{pmatrix} \% 29$$

$$\begin{pmatrix} 19 \\ 27 \\ 4 \end{pmatrix} = T \cdot E$$

$$-54 = \underset{\overset{\shortparallel}{0}}{-58} + 4 = 4$$

$$\det MC = \begin{vmatrix} 1 & -1 & 3 \\ 2 & -2 & 1 \\ 0 & -5 & 2 \end{vmatrix} = -4 - 30 + 5 + 4 = -25$$

$$= 4$$

4^{-1} in $\mathbb{Z}_{29} = 22$

$4^{-1} = x \Leftrightarrow 4x = 1$ in $\mathbb{Z}_{29}$

1 in $\mathbb{Z}_{29} = \{30, 59, \underline{\underline{88}}, \dots\}$

$$A^t = \begin{pmatrix} 1 & 2 & 0 \\ -1 & -2 & -5 \\ 3 & 1 & 2 \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} 1 & -13 & 5 \\ -4 & 2 & +5 \\ -10 & +5 & 0 \end{pmatrix}$$

$$\Rightarrow A^{-1} = 4^{-1} \cdot A^* = 22 \cdot \begin{pmatrix} 1 & -13 & 5 \\ -4 & 2 & 5 \\ -10 & 5 & 0 \end{pmatrix}$$

$$22 \cdot \begin{pmatrix} 1 & -13 & 5 \\ -4 & 2 & 5 \\ -10 & 5 & 0 \end{pmatrix} \begin{pmatrix} 19 \\ 27 \\ 4 \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} \begin{matrix} J \\ O \\ I \end{matrix}$$

Hill afin

Ec. de criptare: $\begin{pmatrix} C \\ O \\ D \end{pmatrix} = MC_1 \cdot \begin{pmatrix} M \\ S \\ J \end{pmatrix} + MC_2$

Ec. de decriptare: $\begin{pmatrix} M \\ S \\ J \end{pmatrix} = MC_1^{-1} \left(\begin{pmatrix} C \\ O \\ D \end{pmatrix} - MC_2 \right)$

Teste de primalitate

Algoritmi (teoreme):

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

OUTPUT: A/F dacă n este prim

Dacă n nu este prim (= compus), se poate găsi un <u>martor</u> (= „motiv" pt care n nu este prim)

1) <u>Exact</u> = Determinist: sigur, ineficient

2) <u>Probabilist</u> : rapid, nu sigur

Dacă n prim $\Rightarrow$ <u>Probabil</u> prim

n compus $\Rightarrow$ Sigur compus, martor

<u>I Testul direct</u>

Pentru $d \in \{2, \dots, n-1\}$:

dacă $n \,\%\, d = 0 \Rightarrow n$ compus

<u>Ex</u>: $n = 11$:

Dacă $11 \,\%\, 2 = 0$ NU

$11 \,\%\, 3 = 0$ NU

- - - -

$11 \,\%\, 10 = 0$ NU

$\Rightarrow 11$ prim

<u>II Ciurul (Sita) lui Eratostene</u>

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: $\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$

III Testul Fermat

Mica Teoremă a lui Fermat:

$$n \text{ prim} \Rightarrow a^{n-1} = 1 \text{ în } \mathbb{Z}_n, \quad \forall a \in \mathbb{Z}_n^*$$

obs: Dacă $\exists a \in \mathbb{Z}_n^*$ a.î. $a^{n-1} \neq 1$ în $\mathbb{Z}_n \Rightarrow$

$\Rightarrow n$ compus și a martor

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

$1^6 = 1$ ok

$2^6 = 64 = 1$ ok

$3^6 = (3^2)^3 = 2^3 = 8 = 1$ ok

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

$5^6 = (5^2)^3 = 4^3 = 2^6 = 1$ ok

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

$\Rightarrow \forall a \in \mathbb{Z}_7^*$, $a^6 = 1$ în $\mathbb{Z}_7 \Rightarrow 7$ prim.

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

$1^8 = 1$ ok

$2^8 = (2^4)^2 = 5^2 = 25 = 7 \neq 1 \Rightarrow 9$ compus,
2 martor

Varianta exactă (deterministă)

Varianta probabilistă: Aleg un număr de mostre pt. $a \in \mathbb{Z}_n^*$

Ex: $n = 27409$ cu 3 mostre alese aleatoriu

$\Rightarrow a_1 = 9731 \Rightarrow 9731^{27408} = 1$ în $\mathbb{Z}_{27409}^*$ ✓

$a_2 = 20195 \Rightarrow 20195^{27408} = 1$ în $\mathbb{Z}_{27409}^*$ ✓

$a_3 = 13582 \Rightarrow 13582^{27408} = 1$ în $\mathbb{Z}_{27409}^*$ ✓

$\Rightarrow n = 27409$ PROBABIL prim

$$prob = \frac{3}{27408}$$

Simbolul Jacobi

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

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

Ex: $\left(\frac{3}{7}\right) = ?$

- $7 \nmid 3$
- 3 este pătrat în $\mathbb{Z}_7^*$?

Pătratele din $\mathbb{Z}_7^* = \{1, 4, 2\} \not\ni 3$ $\Rightarrow$

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

Ex: $\left(\frac{31}{5}\right) = ?$

$5 \nmid 31$

Pătratele din $\mathbb{Z}_5^*$ $= \{1, 4\}$

$31 = 1$ în $\mathbb{Z}_5$ $\in \{1, 4\}$ $\Rightarrow \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$

Teorema Solovay-Strassen

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

$\forall b \in \mathbb{Z}_n^*$.

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

$\forall b \in \{1,2,3,4,5,6\}$

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

$2^{\frac{7-1}{2}} = 2^3 = 8 = 1$; $\left(\frac{2}{7}\right) = 1$ pt că 2 este pătrat $(2 = 3^2)$ OK

Pătratele din $\mathbb{Z}_7^* = \{1, 4, 2\}$

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

$4^{\frac{7-1}{2}} = 4^3 = 2^6 = (2^3)^2 = 1$; $\left(\frac{4}{7}\right) = 1$ pt că $4 = 2^2$ OK

$5^{\frac{7-1}{2}} = 5^3 = 25 \cdot 5 = 4 \cdot 5 = 6$; $\left(\frac{5}{7}\right) = -1 = 6$ OK

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

$\Rightarrow n = 7$ prim.

$n = 9$ $\quad b^{\frac{9-1}{2}} = \left(\frac{b}{9}\right)$ în $\mathbb{Z}_9$, $\forall\, b \in \mathbb{Z}_9^*$

$1^{\frac{9-1}{2}} = 1^4 = 1$, $\left(\frac{1}{9}\right) = 1$ pt că $1 = 1^2$ ok

Pătratele din $\mathbb{Z}_9^* = \{1, 4, 0, 7\}$

$2^{\frac{9-1}{2}} = 2^4 = 16 = 7$; $\left(\frac{2}{7}\right) = -1 = 8 \Rightarrow$

$\Rightarrow 2^{\frac{9-1}{2}} \neq \left(\frac{2}{7}\right) \Rightarrow$ 9 nu e prim
2 este martor

Varianta deterministă (exactă)

Var. probabilistă: aleg martor pt $b \in \mathbb{Z}_n^*$