1342b

Wednesday, 30 October, 2024 8:01

1342b

1342b

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

- $(\mathbb{Z}_n, +)$ grup comutativ
- $(\mathbb{Z}_n - \{0\}, \cdot)$ monoid → nu orice element este inversabil

Ex: $(\mathbb{Z}_7, +, \cdot)$

$2+3=5 \Leftrightarrow 16+17=12 \Leftrightarrow 23+3=5$ etc (în $\mathbb{Z}_7$) modulo 7, mod 7

$2 = \{7k+2 \mid k \in \mathbb{Z}\} = \{2, 9, 16, 23, \dots\}$

$3 = \{7k+3 \mid k \in \mathbb{Z}\} = \{3, 10, 17, 24, \dots\}$

$5 = \{7k+5 \mid k \in \mathbb{Z}\} = \{5, 12, 19, 26, \dots\}$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ → reprezentanți

0 = element neutru la $+$ $\Rightarrow x+0=x, \forall x \in \mathbb{Z}_7$

Notez $-x$ simetricul (inversul) lui x față de „+"

$-x$ se mai numește opusul lui x.

Def: $-x = y \Leftrightarrow y+x=0$

$-2 = y \Leftrightarrow y+2 = 0 = \{7k \mid k \in \mathbb{Z}\} \Rightarrow y=5$

Obs: $\underbrace{-2 = 0-2 = 7-2}_{0\text{ = multipli de } 7} = 14-2 = \dots$ pt că

Înmulțirea: $2 \cdot 3 = 6 \Leftrightarrow 9 \cdot 24 = 13 \Leftrightarrow 16 \cdot 10 = 34$ etc

Def: x^{-1} = simetricul lui x față de „$\cdot$" = invers

Obs: $(\mathbb{Z}_n, +, \cdot)$ inel $\Rightarrow x^{-1}$ nu există pentru orice x.

Def: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{există } x^{-1}\}$ = unități

Teoremă: x este unitate în $\mathbb{Z}_n \Leftrightarrow \text{cmmdc}(x, n) = 1$

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

Obs: Dacă n este număr prim $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n - \{0\} = \mathbb{Z}_n^*$

Cum calculez x^{-1}?

Ex: În $\mathbb{Z}_7$, $U(\mathbb{Z}_7) = \mathbb{Z}_7^*$ pt că 7 prim.

$2^{-1} = y \Leftrightarrow 2 \cdot y = 1 \leftarrow$ el. neutru la „$\cdot$"

$\Downarrow$

$y = 4$ pt că $2 \cdot 4 = 8 = 1$.

Ecuații de gradul I

1) $5x+2=1$ în $\mathbb{Z}_7 = \{0, 1, \dots, 6\}$

$\Downarrow$

$5x = 1-2 = -1 = 6 \mid \cdot 5^{-1} = 3$

$3 \cdot 5 \cdot x = 6 \cdot 3$

$x = 18 = 4 \Rightarrow \underline{x=4 \text{ este soluție.}}$

2) $3x+1=7$ în $\mathbb{Z}_9 = \{0, 1, 2, \dots, 8\}$

$3x = 7-1 = 6 \mid \cdot 3^{-1}$ NU EXISTĂ ÎN $\mathbb{Z}_9$ pt că $\text{cmmdc}(3,9) = 3 \neq 1$

$\Rightarrow 3 \notin U(\mathbb{Z}_9)$

Rezolv prin încercări:

$x=0$ NU; $x=1$ NU; $\underline{x=2 : \text{OK}}$; $x=3$ NU; $x=4$: NU; $\underline{x=5 : \text{OK}}$;

$x=6$: NU; $x=7$ NU; $\underline{x=8 : \text{OK}}$

Ecuații de gradul II

Ex: $2x^2 - 5x + 1 = 0$ în $\mathbb{Z}_7 = \{0, 1, \dots, 6\}$

$\Delta = (-5)^2 - 4 \cdot 1 \cdot 2 = 25 - 8 = 17 = 3$

Există $\sqrt{\Delta}$? Dacă $\sqrt{\Delta} = y \Leftrightarrow \Delta = y^2$

Există $\sqrt{3}$ în $\mathbb{Z}_7 \Leftrightarrow$ există $a \in \mathbb{Z}_7$ a.î. $a^2 = 3$.

a	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1

în $\mathbb{Z}_7$

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

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

$\Delta = 25 - 24 = 1$

Există $\sqrt{1}$ în $\mathbb{Z}_{11}$?

a	0	1	2	3	4	5	6	7	8	9	10
a^2	0	1	4	9	5	3	3	5	9	4	1

$\Rightarrow \sqrt{1} \in \{1, 10\}$ dar $10 = -1$

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

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

Dacă lucram cu $\sqrt{1} = 10$: $x_1 = (5+10)\cdot 2^{-1} = 15\cdot 6 = 90 = 2$

$x_2 = (5-10)\cdot 2^{-1} = (-5)\cdot 6 = 6\cdot 6 = 36 = 3$

Ex: $3x^2 + x + 4 = 2$ în $\mathbb{Z}_8$

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

$\Delta = 1 - 4\cdot 2\cdot 3 = 1 - \overset{0}{24} = -23 = -\overset{0}{16} - 7 = -7 = 1$

$\sqrt{1}$ în $\mathbb{Z}_8$ este 1 sau 7

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

6^{-1} NU EXISTĂ în $\mathbb{Z}_8$ (cmmdc$(6,8)=2$)

$\Rightarrow$ Ec. nu are soluții.

Sisteme liniare (2×2)

! Dacă det matricei sistemului **nu** este element inversabil $\Rightarrow$ rezolv prin încercări.

Altfel, aplic reducere sau substituție.

Ex: $\begin{cases} 2x + 3y = 1 \\ x - 5y = 2 \end{cases}$ în $\mathbb{Z}_7$ $\quad U(\mathbb{Z}_7) = \mathbb{Z}_7^*$

! $A = \begin{pmatrix} 2 & 3 \\ 1 & -5 \end{pmatrix}$ $\det A = -10 - 3 = -13 = -6 = 1$ ok

Reducere: $\begin{cases} 2x + 3y = 1 \\ x - 5y = 2 \mid \cdot 2 \end{cases} \Rightarrow \begin{cases} 2x + 3y = 1 \\ 2x - 10y = 4 \end{cases}$ (−)

$13y = -3 \Rightarrow 6y = 4 \mid \cdot 6^{-1}$ ($6^{-1} = 6$)

$y = 24 = 3$

$x - 5\cdot 3 = 2$

$x = 2 + 15 = 17 = 3$

Substituție: $\begin{cases} 2x + 3y = 1 \\ x - 5y = 2 \Rightarrow x = 2 + 5y \end{cases}$ $\Rightarrow 2(2+5y) + 3y = 1$

$4 + 10y + 3y = 1$

$13y = -3 = 4 \Rightarrow y = 3$

$x = 2 + 5\cdot 3 = 3$

Inverse matriceale

În $\mathbb{R}$, M este inversabilă $\Leftrightarrow \det M \neq 0$

În $\mathbb{Z}_n$, M este inversabilă $\Leftrightarrow \det M \in U(\mathbb{Z}_n)$

Ex: $A = \begin{pmatrix} 2 & 3 \\ 0 & 5 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}_7)$ $\quad A^{-1} = ?$ dacă există

$\det A = 10 = 3 \in U(\mathbb{Z}_7) \Rightarrow$ există A^{-1}

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

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

$A^{-1} = (\det A)^{-1}\cdot A^* = 3^{-1}\cdot A^* = 5\cdot\begin{pmatrix} 5 & -3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 25 & -15 \\ 0 & 10 \end{pmatrix}$

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

Verificare: $A\cdot A^{-1} = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$A^{-1}\cdot A$

Cifruri elementare

Setup:

A	B	C	D	E	F	G	H	I	J	K
0	1	2	3	4	5	6	7	8	9	10
L	M	N	O	P	Q	R	S	T	U	V
11	12	13	14	15	16	17	18	19	20	21
W	X	Y	Z	␣	.	?				
22	23	24	25	26	27	28				

Alfabetul englezesc conduce la $\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$

DAR 26 nu este nr prim $\Rightarrow$

$U(\mathbb{Z}_{26}) \subsetneq \mathbb{Z}_{26}^*$ (există elemente/litere neinversabile/indescifrabile)

Completăm alfabetul la $\mathbb{Z}_{29}$, 29 prim $\Rightarrow U(\mathbb{Z}_{29}) = \mathbb{Z}_{29}^*$.

Cifrul Caesar (flux = stream cipher)

Ecuația de criptare: text clar + cheie = cod $(\underset{\text{mesaj}}{m} + \overset{\text{key}}{k} = \underset{\text{cod}}{c})$

Ecuația de decriptare: cod - cheie = text $(c - k = m)$

Exemplu: mesaj: "Salut" ; cheie: 17

Criptarea: $[S, A, L, U, T] \longrightarrow [18, 0, 11, 20, 19] \xrightarrow[+17]{+k}$

$\longrightarrow [35, 14, 28, 37, 36] \xrightarrow[\text{mod } 29]{} [6, 17, 28, 8, 7]$

$\rightarrow$ GR?IH

SALUT $\xrightarrow{+17}$ GR?IH (Caesar)

SALUT $\xrightarrow{+17}$ GR?ÎH (Caesar)

Decriptarea : GR?ÎH $\to [6, 17, 28, 8, 7] \xrightarrow[-17]{-K}$

$\to [-11, 0, 11, -9, -10] \xrightarrow[\text{mod } 29]{} [18, 0, 11, 20, 19]$

$\to$ SALUT

Variație : Caesar pe blocuri

a) fără padding

b) cu padding random

a) Împart mesajul în blocuri de lungime b (dată) și folosesc câte o cheie pt fiecare bloc.

Ex: mesaj: TOAMNA , bloc: 4

$\Rightarrow b_1$: TOAM , b_2 : NA

chei: $K_1 = 15$; $K_2 = 6$

Criptarea : Blocul 1 : $[T, O, A, M] \to [19, 14, 0, 12] \xrightarrow[+15]{+K_1}$

$\to [34, 29, 15, 27] \xrightarrow[\text{mod } 29]{} [5, 0, 15, 27] \to [F, A, P, .]$

Blocul 2 : $[N, A] \to [13, 0] \xrightarrow[+6]{+K_2} [19, 6] \to [T, G]$

TOAMNA $\to$ FAP.TG (Caesar, 2 blocuri)

b) Cu padding random : toate blocurile vor avea aceeași lungime

b) Cu padding random: toate blocurile vor avea aceeași lungime

Ex: mesaj: CAIET, blocuri de lungime 4

b_1: CAIE $\Rightarrow K_1 = 7$

b_2: TMZ? $\Rightarrow K_2 = 10$ etc.

Obs1: Dacă 2 car. identice se găsesc în blocuri diferite $\Rightarrow$ ele se vor codifica diferit $\Rightarrow$ securitate ++

Obs2: Nu putem elimina padding-ul fără a ști mesajul inițial.

Cifrul afin

Varianta flux:

Ec. de criptare: text · cheie1 + cheie2 = cod

$m \cdot K1 + K2 = C$

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

Ex: $m = AZi$; $K1 = 5$; $K2 = 6$

$[A, Z, i] \rightarrow [0, 25, 8] \xrightarrow[\cdot 5 + 6]{\cdot K1 + K2} [6, 131, 46] \rightarrow$

$\xrightarrow[mod\,29]{} [6, 15, 17] \rightarrow [G, P, R]$

$AZi \rightarrow GPR$ (afin, flux)

Decriptarea: $[G, P, R] \rightarrow [6, 15, 17] \xrightarrow[-6 \cdot 5^{-1}]{-K_2 \cdot K_1^{-1}} [0, 54, 66] \xrightarrow{mod\,29}$

$-6, \cdot 6$

5^{-1} în $Z_{29} = 6$

$\rightarrow [0, 25, 8] \rightarrow AZi$

2) Varianta pe blocuri cu/fără padding

! câte 2 chei/bloc.

Ex: mesaj: CARTE, blocuri de lungime 3

b_1: CAR $K1=3$ $K2=5$

b_2: TE␣ $K3=6$ $K4=8$

Blocul 1: $[C, A, R] \to [2, 0, 17] \xrightarrow[\cdot 3+5]{\cdot K1+K2} [11, 5, 56] \xrightarrow[mod\ 29]{} [11, 5, 27]$

$\to$ LF.

Blocul 2: $[T, E, ␣] \to [19, 4, 26] \xrightarrow[\cdot 6+8]{\cdot K3+K4} [122, 32, 164]$

$\xrightarrow[mod\ 29]{} [6, 3, 19] \to$ GDT

CARTE␣ $\to$ LF.GDT

Cifrul Hill

Flux: Ecuația de criptare: cheie · mesaj = cod, unde
cheie este matrice
mesaj, cod = vectori

Ec. de decriptare: mesaj = $\text{cheie}^{-1} \cdot \text{cod}$

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

Cheie (matrice de criptare): $K = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & -2 & 0 \end{pmatrix}$

Criptarea: $KM = C$

Criptarea: $KM = C$

$$\begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 2 \\ -1 & -2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix} = \begin{pmatrix} 24 \\ 30 \\ -37 \end{pmatrix} \bmod 29 = \begin{pmatrix} 24 \\ 1 \\ 21 \end{pmatrix} \begin{matrix} Y \\ B \\ V \end{matrix}$$

$-37 = -29 - 8 = -8$

Joi $\longrightarrow$ YBV (Hill)

Decriptarea $\det K = -2 - 1 + 8 = 5 \in U(\mathbb{Z}_{29})$

$(\det K)^{-1} = 5^{-1} = 6.$

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

$$K^{-1} = (\det K)^{-1} \cdot K^* = 6 \cdot \begin{pmatrix} 4 & 2 & 3 \\ -2 & -1 & -4 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 24 & 12 & 18 \\ -12 & -6 & -24 \\ 6 & 18 & 12 \end{pmatrix}$$

Mesaj: $K^{-1} \cdot C = \begin{pmatrix} 24 & 12 & 18 \\ -12 & -6 & -24 \\ 6 & 18 & 12 \end{pmatrix} \cdot \begin{pmatrix} 24 \\ 1 \\ 21 \end{pmatrix} = \begin{pmatrix} 9 \\ 14 \\ 8 \end{pmatrix}$