1342B

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

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

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

$\hat{k} = \{x \in \mathbb{Z} \mid x \text{ dă restul } k \text{ la împ. cu } n\}$

$\hat{k} = \{nq + k \mid q \in \mathbb{Z}\}$, n fixat

- $(\mathbb{Z}_n, +)$ grup comutativ
  $\hat{a} + \hat{b} = \widehat{a+b}$
- $(\mathbb{Z}_n - \{\hat{0}\}, \cdot)$ monoid com.
  ↳ nu neapărat toți $x \in \mathbb{Z}_n - \{0\}$ au invers la înmulțire

Ex: $\mathbb{Z}_5 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}\}$ reprezentanți

$\hat{2} + \hat{2} = \hat{4}$

$\hat{2} + \hat{4} = \hat{6} = \hat{1}$

$\hat{2} \cdot \hat{3} = \hat{6} = \hat{1}$; $\hat{4} \cdot \hat{4} = \hat{16} = \hat{1}$; $\hat{2} \cdot \hat{4} = \hat{8} = \hat{3}$

$\hat{a}^{-1}$ = inversul multiplicativ al lui $\hat{a}$ din $\mathbb{Z}_n$

$-\hat{a}$ = $-$ " $-$ aditiv

Def $\hat{a}^{-1} = \hat{b}$ în $\mathbb{Z}_n \Leftrightarrow \hat{ab} = \hat{1}$ în $\mathbb{Z}_n$

$-\hat{a} = \hat{b}$ în $\mathbb{Z}_n \Leftrightarrow \hat{a+b} = \hat{0}$ în $\mathbb{Z}_n$

Ex: $\mathbb{Z}_{12}$

$-7 = a \Leftrightarrow 7 + a = 0 \Rightarrow a = 5$

$-11 = b \Leftrightarrow 11 + b = 0 \Rightarrow b = 1$

$5^{-1} = c \Leftrightarrow 5c = 1 \Rightarrow c = 5$

$7^{-1} = d \Leftrightarrow 7d = 1 \Rightarrow d = 7$ pt că $7 \cdot 7 = 49 = \overset{0}{\overset{\|}{48}} + 1 = 1$

$11^{-1} = 11$ pt că $11 \cdot 11 = 121 = 120 + 1 = 1$

8^{-1} nu există pt că $8x = 1$ în $\mathbb{Z}_{12}$ nu are sol.

10^{-1} nu există ; $2^{-1}, 4^{-1}, 3^{-1}, 6^{-1}$

Def: $U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \text{există } x^{-1} \text{ în } \mathbb{Z}_n\}$ ← grupul unităților lui $\mathbb{Z}_n$

$x \in U(\mathbb{Z}_n)$ s.u. **unitate**

Obs: $(U(\mathbb{Z}_n), \cdot)$ grup comutativ.

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

Obs1: Dacă n nr prim $\Rightarrow U(\mathbb{Z}_n) = \mathbb{Z}_n - \{0\}$

Obs2: Dacă $x \notin U(\mathbb{Z}_n)$ $\exists y \in \mathbb{Z}_n$ a.î. $xy = 0$, $x, y \neq 0$

↳ x, y s.u. divizori ai lui zero

Ex: În $\mathbb{Z}_{12}$, 4 este divizor al lui zero pt că $4 \cdot 3 = 0$

10 — " — pt că $10 \cdot 6 = 60 = 12 \cdot 5 = 0$.

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

3^{-1} în $\mathbb{Z}_{10} = 7$; $7^{-1} = 3$; $9^{-1} = 9$

Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $5x + 3 = 1$ în $\mathbb{Z}_7$

$5x = 1 - 3 = -2 = 5 \Rightarrow x = 1$

Ex: $3x + 7 = 2$ în $\mathbb{Z}_{13}$

$3x = 2 - 7 = -5 = 8$

$3x = 8 \mid \cdot 3^{-1} = 9 \Rightarrow x = 8 \cdot 9 = 72 = \overset{0}{\overset{\|}{65}} + 7 = 7$

$x = 7$

Ex: $5x - 3 = 7$ în $\mathbb{Z}_{11}$

$5x = 7 + 3 = 10 \mid \cdot 5^{-1} = 9 \Rightarrow x = 10 \cdot 9 = 90 = 88 + 2 = 2$

$x = \hat{2}$

Ex: $4x + 1 = 3$ în $\mathbb{Z}_{10}$ Rezolvăm prin încercări

$4x = 2$ în $\mathbb{Z}_{10}$

4^{-1} nu există!

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

$\Rightarrow x \in \{3, 8\}$

Ecuații de gradul II

Ex: $x^2 + 3x + 1 = 0$ în $\mathbb{Z}_7$

$\Delta = 9 - 4 = 5$

$\sqrt{5} = ?$ în $\mathbb{Z}_7$ $\quad \sqrt{5} = a \Leftrightarrow a^2 = 5$ nu se poate $\Rightarrow \nexists \sqrt{\Delta}$ în $\mathbb{Z}_7$

$S = \emptyset$.

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

Ex: $x^2 - 5x + 6 = 0$ în $\mathbb{Z}_{13}$

$\Delta = 25 - 24 = 1$

$\sqrt{1} \in \{1, 12\}$ pt că $12^2 = 144 = 11 \cdot 13 + 1 = 1$

$(12 = -1)$

Dacă iau $\sqrt{\Delta} = 1$: $x_1 = (5 + 1) \cdot 2^{-1} = 6 \cdot 7 = 42 = 39 + 3 = 3$

$x_2 = (5 - 1) \cdot 2^{-1} = 4 \cdot 7 = 28 = 2$

Dacă iau $\sqrt{\Delta} = 12$: $x_1 = (5 + 12) \cdot 7 = 17 \cdot 7 = 4 \cdot 7 = 2$

$x_2 = (5 - 12) \cdot 7 = (-7) \cdot 7 = 6 \cdot 7 = 42 = 3$