1341a

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

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

$\mathbb{Z}_n=\{\hat{0},\hat{1},\hat{2},\dots,\widehat{n-1}\}$ , $\hat{k}=\{x\in\mathbb{Z} \mid x$ dă restul $k$ la împ. cu $n\}$

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

$\hat{a}+\hat{b}=\widehat{a+b}$

$\hat{a}\cdot\hat{b}=\widehat{a\cdot b}$

$(\mathbb{Z}_n,+)$ grup comutativ, cu el. neutru $\hat{0}$

$-\hat{a}=$ simetricul lui $a$ față de „+"

$=$ opusul lui $a$

$-\hat{a}=\hat{b} \Rightarrow \hat{a}+\hat{b}=\hat{0}$.

$(\mathbb{Z}_n-\{\hat{0}\},\cdot)$ monoid comutativ

↳ nu neapărat toți $x\in\mathbb{Z}_n$ au simetric la „·"

$\hat{1}=$ el. neutru

$\hat{a}^{-1}=$ simetricul (inversul) lui $\hat{a}$ față de „·" (dacă există)

$\hat{a}^{-1}=\hat{b} \Rightarrow \hat{a}\hat{b}=\hat{1}$ în $\mathbb{Z}_n$.

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

$\widehat{17}=\widehat{14}+\hat{3}=\hat{3}$, $\widehat{14}=\hat{0}$

$-\hat{3}=\hat{a} \Leftrightarrow \hat{3}+\hat{a}=\hat{0} \Rightarrow \hat{a}=\hat{4}$

$-\widehat{38}=-\widehat{35}-\hat{3}=-\hat{3}=\hat{4}$. ($\widehat{35}=\hat{0}$)

$\hat{3}^{-1}=\hat{b} \Leftrightarrow \hat{3}\hat{b}=\hat{1} \Rightarrow b=\hat{5}$ pt că $\hat{3}\cdot\hat{5}=\widehat{15}=\widehat{14}+\hat{1}=\hat{1}$.

$\hat{5}^{-1}=\hat{3}$.

$\hat{6}^{-1}=\hat{6}$ pt că $\hat{6}\cdot\hat{6}=\widehat{36}=\widehat{35}+\hat{1}=\hat{1}$

$\hat{4}^{-1}=\hat{2}=\hat{9}=\widehat{16}=\widehat{23}=\dots$

Ex: $\mathbb{Z}_{20}$  $\hat{3}^{-1}=\hat{7} \Rightarrow \hat{7}^{-1}=\hat{3}$ ; $\widehat{11}^{-1}=\widehat{11}$

$\widehat{10}^{-1}$ nu există

**Def**: $U(\mathbb{Z}_n)=\{x\in\mathbb{Z}_n \mid \exists\, x^{-1}$ în $\mathbb{Z}_n\}$ → grupul unităților

↳ $x$ s.n. unități

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

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

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

În acest caz, $x,y$ s.n. divizori ai lui zero.

Ex: $U(\mathbb{Z}_{10})=\{\hat{1},\hat{3},\hat{7},\hat{9}\}$  $\hat{3}^{-1}=\hat{7} \Rightarrow \hat{7}^{-1}=3$ ; $\hat{9}^{-1}=\hat{9}$

$\hat{4}\notin U(\mathbb{Z}_{10})$ ; $\hat{4}\cdot\hat{5}=\hat{0} \Rightarrow \hat{4},\hat{5}$ divizori ai lui zero

### Ecuații de gradul I în $\mathbb{Z}_n$

Ex: $5x+2=1$ în $\mathbb{Z}_{11}$

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

Ex: $3x-5=4$ în $\mathbb{Z}_{13}$

$3x=9 \mid \cdot 3^{-1}=9 \Rightarrow x=9\cdot 9=81=78+3=3$.

Ex: $2x-1=0$ în $\mathbb{Z}_6$

$2x=1$ → Rezolv prin încercări

$2^{-1}$ nu există în $\mathbb{Z}_6$

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $2x$ | 0 | 2 | 4 | 0 | 2 | 4 |

$\Rightarrow S=\emptyset$

### Sisteme liniare

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

$\det A=-4-5=-9=-2=5\in U(\mathbb{Z}_7)$

$\Rightarrow$ Sol. unică

$\begin{cases}2x+y=3 \mid \cdot 2\\5x-2y=1\end{cases} \Rightarrow \begin{cases}4x+2y=6\\5x-2y=1\end{cases}$ (+) $\Rightarrow$ $9x=7$, $2x=0 \Rightarrow \boxed{x=0}$ ⇓ $\boxed{y=3}$

$2\cdot 0+3=3$ ✓

$5\cdot 0-2\cdot 3=1$ ✓

Ex: $\begin{cases}3x-2y=1\\x+y=2\end{cases}$ $\mathbb{Z}_{10}$  $A=\begin{pmatrix}3 & -2\\1 & 1\end{pmatrix}$ $\det A=5\notin U(\mathbb{Z}_{10})$

$\begin{cases}3x-2y=1\\2x+2y=4\end{cases} \Rightarrow 5x=5 \Rightarrow x=1$ sau $x=5$ sau $x=3\dots$

$x\in\{1,3,5,7,9\}$

pt $\underline{x=1} \Rightarrow y=2-1=1$ ; Verific: $3\cdot 1-2\cdot 1=1$ ✓

$\underline{x=3} \Rightarrow y=2-3=-1=9$ ; Verific: $3\cdot 3-2\cdot 9=-9=1$ ✓

$\underline{x=5} \Rightarrow y=2-5=-3=7$ ; Verific: $3\cdot 5-2\cdot 7=1$ ✓

$\underline{x=7} \Rightarrow y=2-7=-5=5$ ; $3\cdot 7-2\cdot 5=11=1$ ✓

$\underline{x=9} \Rightarrow y=2-9=-7=3$ ; $3\cdot 9-2\cdot 3=21=1$ ✓

$S=\{(1,1),(3,9),(5,7),(7,5),(9,3)\}$.

### Ec. de gradul II în $\mathbb{Z}_n$

Ex: $x^2-5x+3=0$ în $\mathbb{Z}_7$

$\Delta=25-4\cdot 3=13=6$

$\sqrt{6}=?$  $\sqrt{6}=a \Leftrightarrow a^2=6$

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $x^2$ | 0 | 1 | 4 | 2 | 2 | 4 | 1 |

$\Rightarrow \nexists\, \sqrt{6}$ în $\mathbb{Z}_7 \Rightarrow S=\emptyset$.

Ex: $x^2-5x+8=2$ în $\mathbb{Z}_{11}$

$x^2-5x+6=0$

$\Delta=25-24=1$

$\exists\sqrt{1}$? Da, $\sqrt{1}\in\{1,10\}$

Dacă iau $\sqrt{1}=1 \Rightarrow x_1=(5+1)\cdot 2^{-1}=6\cdot 6=36=3$.

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

Dacă iau $\sqrt{1}=10 \Rightarrow x_1=(5+10)\cdot 2^{-1}=\underbrace{15\cdot 6=4}\cdot 6=24=2$

$x_2=(5-10)\cdot 2^{-1}=-5\cdot 6=-30=-22-8=-8=3$.

$x\in\{2,3\}$