24.02.2016.

ALGEBRĂ

SEMINAR 1

Inele

$(R, +, \cdot)$

1) $(R, +)$ - grup comut
2) $(R, \cdot)$ - monoid cu unitate (oper e asoc)
3) $a \cdot (b+c) = a \cdot b + a \cdot c \quad \forall a, b, c \in R$
   $(a+b) \cdot c = a \cdot c + b \cdot c \quad$ —//—

$(\mathbb{Z}_m, +, \cdot)$ - inelul claselor de resturi mod. $m \in \mathbb{N}, m \geq 2$.

$\mathbb{Z}_{26}$

Caesar A B C D E F G H I J K L M N O P Q R S T U V W X Y Z.

+3 ATAC → DWDF

$$\boxed{\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n}$$

$(m, n) = 1$.

$(R, +, \cdot)$

$(S, \perp, *)$

$R \times S = \{(r, s) \mid r \in R, s \in S\}$

$(r_1, s_1) \Delta (r_2, s_2) = (r_1 + r_2, s_1 \perp s_2)$

$(r_1, s_1) \circ (r_2, s_2) = (r_1 \cdot r_2, s_1 * s_2)$

$(R \times S, \Delta, \circ)$ - inel.

Ultimele 2 cifre ale lui 2^{39} $\quad 7^{39}$ 7 prim cu 100.

$39 : 4 = 9$ $\quad 2^3 = 8$.

$\frac{36}{3}$

28

$\mathbb{Z}_{100}$

$a \in \mathbb{Z} \quad n \in \mathbb{N}^* \quad (a,n) = 1.$

$a^{\varphi(n)} \equiv 1 \pmod n$

$n \in \mathbb{N}^*$

$a^{|U(\mathbb{Z}_n)|} \equiv 1 \pmod n$

$a \equiv b \pmod n$

$n \mid a - b$

$\bar{a} = \bar{b}$

R inel.

$U(R) = \{ r \in R \mid \exists s \in S \text{ a.î. } r \cdot s = s \cdot r = 1 \}$.

$(U(R), \cdot)$ - grup.

Th. Lagrange.

$(G, \cdot)$ - grup finit. $g \in G \Rightarrow g^{|G|} = e$

$U(\mathbb{Z}_n) = \{ \bar{a} \mid (a,n) = 1 \}$ → el. inversabile.

$$|U(\mathbb{Z}_n)| = \varphi(n) = n \cdot \prod_{p/n} \left(1 - \frac{1}{p}\right)$$

p prim

→ toate nr prime care sunt div cu n.

$|U(\mathbb{Z}_{100})| = 40$

$(7, 100) = 1$ – 7 prim cu 100.

7^{39}.

$7^{|U(\mathbb{Z}_{100})|} \equiv 1 (100)$

$7^{40} \equiv 1 (100)$

$7 \cdot 7^{39} \equiv 1 (100)$

7^{39} sunt 43

$a \overset{n}{\equiv} b$

$a \equiv b \pmod n$

$a \equiv b (n)$

7
43
2 1
2 8
3 0 1

$\mathbb{Z}_{100} \simeq \mathbb{Z}_4 \times \mathbb{Z}_{25}$ | – pt 2^{39}.

– să fie prime între ele.

$2^{39} \overset{4}{\equiv} 0$

$2^{39} \overset{25}{\equiv} 2^{19} \overset{25}{\equiv} 13.$

$(2, 25) = 1$

$|U(\mathbb{Z}_{25})| = 20.$

$|U(\mathbb{Z}_{25})| \equiv 1 (25)$

$1 \equiv 2^{20} = 2 \cdot 2^{19}$

2^{39} sunt 88.

$\begin{cases} 2^{39} \overset{4}{\equiv} 0 \\ 2^{39} \overset{25}{\equiv} 13 \end{cases}$ – luăm din cât 0,99 pt că suntem în $\mathbb{Z}_{100}$.

13, 38, 63, 88

apoi îl alegem pe cel care : 4 dă rest 0, adică 88.

2

sau $2^{39} = 25k+13 \overset{4}{\equiv} 0$. $\quad k \overset{4}{\equiv} 3$.

$k+1 \overset{4}{\equiv} 0$

$2^{39} = 25k+13$.

$= 25(4s+3)+13 = 100s+88$.

Ultimele 3 cifre

$2^{39} \overset{8}{\equiv} 0$

$2^{39} \overset{125}{\equiv} 2^4 \cdot 2^{35} \equiv 16 \cdot (-7) = -112 \overset{125}{\equiv} 13$

$2^7 = 128 \overset{125}{\equiv} 3$.

ordinul lui 2 modulo 125.

$2^{35} = (2^7)^5 \equiv 3^5 = 243 \overset{125}{\equiv} -7$.

$2^{39} = 125k + 13 \overset{8}{\equiv} 0$.

$5k+5 \overset{8}{\equiv} 0$.

$k+1 \overset{8}{\equiv} 0$.

$k \overset{8}{\equiv} 7$.

$1 \equiv 2^{20} = 2 \cdot (2^{19})$

$125 \cdot 7 = 875$

$875 \cdot 13 = 888$

(th) $|U(\mathbb{Z}_n)| = n \cdot \prod_{\substack{p \text{ prim} \\ p \mid n}} \left(1 - \frac{1}{p}\right)$ - fct. lui Euler.

$\varphi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = \frac{400}{10} = 40$.

$(a, n) = 1$.
$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$ - euler.

Dacă n prim.
$|U(\mathbb{Z}_n)| = n-1$. Mica Th. a lui Fermat.
$a^{n-1} \equiv 1 (n)$

$U(\mathbb{Z}) = \{\pm 1\}$ $\quad \mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$

$U(\mathbb{Z}[i]) =$

$u \in U(\mathbb{Z}[i])$ $\quad u = a+bi$, $a, b \in \mathbb{Z}$
$\exists\, c, d \in \mathbb{Z}$, a.î. $(a+bi)(c+di) = 1$.

↳ el. inversabil.

$|a+bi| = \sqrt{a^2+b^2}$

$|a+bi|^2 = a^2+b^2$.

am lucrat cu modul.

$(a^2+b^2)(c^2+d^2) = 1$. $\Rightarrow a^2+b^2 = 1$.

4 soluții: $a=0$, $b=\pm 1$ $\quad a=\pm 1$, $b=0$.

$U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$.

$i \cdot (-i) = 1$.

$(-1)(-1) = 1$.

$\varepsilon = \dfrac{-1+i\sqrt{3}}{2}$

$U(\mathbb{Z}[\varepsilon]) = ?$

$(\mathbb{Z}[\varepsilon], +, \cdot)$ - inel.

$\mathbb{Z}[\varepsilon] = \{ a + b\varepsilon \mid a, b \in \mathbb{Z} \}$.

să verif dacă este Part. Stab. față de „$\cdot$"

$(a+b\varepsilon)(c+d\varepsilon) = ac + \varepsilon(ad+bc) + \varepsilon^2 \cdot bd\,(-1-\varepsilon)$

$a, b, c, d \in \mathbb{Z}$

$\varepsilon^2 = \frac{1-3-2i\sqrt{3}}{4} = \frac{-1-i\sqrt{3}}{2} = -\varepsilon - 1$

$= \underline{ac - bd} + (\underline{ad + bc - bd})\varepsilon$

nr întreg nr. întreg.

$(a+b\varepsilon)(c+d\varepsilon) = 1$.

$|a + b\varepsilon|^2 = |a + b\frac{-1+i\sqrt{3}}{2}|^2 = \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} = \underline{a^2 - ab + b^2}$

e nr. întreg.

$(a+b\varepsilon)^2 - (c+d\varepsilon)^2 = 1$.

$(a - ab + b^2)(c^2 - cd + d^2) = 1$.

Dacă înmulțim cu 4 $\Rightarrow$ $(a - \frac{b}{2})^2 + \frac{3b^2}{4} = 1 \mid \cdot 4$.

$(2a - b)^2 + 3b^2 = 4$. e pozit.

Dacă $b = 0$ $\boxed{a = \pm 1}$

$2a - b = \pm 2$

Dacă $\boxed{b = 1}$.

$2a - 1 = \pm 1 \Rightarrow \boxed{a = 1 \text{ sau } 0}$

$\boxed{\begin{array}{l} b = -1. \\ a = 0, -1 \end{array}}$

5

· câte elem sunt inversabile? — asta e cerința.

$U(\mathbb{Z}[\varepsilon]) = \{ \pm 1, \pm\varepsilon, \pm\varepsilon^2 \}$.

$(1+\varepsilon) = -\varepsilon^2$.

$(-1-\varepsilon) = \varepsilon^2$

Alt ex.:

$$\mathbb{Z}[\sqrt[3]{2}] = \{ a + b\sqrt[3]{2} + c\sqrt[4]{4} \mid a, b, c \in \mathbb{Z} \}$$

$\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$

$\sqrt[3]{2} \cdot \sqrt[3]{4} = 2$.

$\sqrt[3]{4} \cdot \sqrt[3]{4} = 2\sqrt[3]{2}$

} cred că e T.S.

$U(\mathbb{Z}[\sqrt[3]{2}]) = ?$

exemplu:

de $u \in U(\mathbb{Z}[\sqrt[3]{2}])$ / el. invers!

$u \neq \pm 1$

Folosim: $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$

Dacă luăm $(\sqrt[3]{2})^3 + (-1)^3 = 1$.

$(\sqrt[3]{2} - 1)(\sqrt[3]{4} + \sqrt[3]{2} + 1)$

$U(\mathbb{Z}[\sqrt[3]{2}]) = \{ \pm (\sqrt[3]{2} - 1)^n \mid n \in \mathbb{Z} \}$.

---

alt ex.:

$u \in U(\mathbb{Z}[\sqrt{17}]) = ?$

$u \neq \pm 1$.

$\mathbb{Z}[\sqrt{17}] = \{ a + b\sqrt{17} \mid a, b \in \mathbb{Z} \}$.

$(\sqrt{17} + 4)(\sqrt{17} - 4) = 1$ → deci produsul a cere de forma $a + b\sqrt{17}$ să dea unu.

Să arătăm

$$U(\mathbb{Z}[\sqrt{17}]) = \{ \pm(4+\sqrt{17})^n \mid n \in \mathbb{Z} \}$$

$u \neq \pm 1$.

$u \in U(\mathbb{Z}[\sqrt{13}])$

$u \neq \pm 1$.

~~$2\sqrt{3} \cdot 2\sqrt{3} = 4$~~

$a^2 - 13b^2 = \pm 1$. fără $b = 0$.

pt $b = 1$ avem 14, 12

$b = 2$ avem 53, 51.

$b = 3$ avem 118, 116

$b = 4$ avem 207, 209.

$18^2 + 1 = 13 \cdot 5^2$ Deci $(5\sqrt{13} + 18)(5\sqrt{13} - 18) = 1$.

Ec. Pell.

$x^2 - dy^2 = 1$. $d \in \mathbb{N}$ $\sqrt{d} \notin \mathbb{N}$

$$\sqrt{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

$$\sqrt{6} = 2 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$$

$\sqrt{6}+2$.

$$\rightsquigarrow \frac{1}{\sqrt{6}-2} = a_1 + \cfrac{1}{a_2 + \ddots}$$

$$a_1 = \left[\frac{\sqrt{6}+2}{2} \right] = 2$$

$$\frac{\sqrt{6}+2}{2} - 2 = \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}$$