20.10.2017

# Grupuri de clase de resturi #3

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

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

Scriem $\hat{a} = \hat{b} \Leftrightarrow n \mid (a-b)$

$\equiv$ Relație de echivalență

a) reflexivă $a \equiv a \pmod n$

Dacă $n \mid (a-a) \Leftrightarrow n \mid 0$ adevărat

b) simetrică

$a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

c) tranzitivă

$$\left.\begin{array}{l} a \equiv b \pmod n \\ b \equiv c \pmod n \end{array}\right| \Rightarrow a \equiv c \pmod n$$

Dem

$$\left.\begin{array}{l} n \mid (a-b) \\ n \mid (b-c) \end{array}\right| \overset{(+)}{\Rightarrow} n \mid (a-c) \Rightarrow a \equiv c \pmod n$$

a) $\bar{a} = \bar{a}$

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

c) $\left.\begin{matrix} \bar{a} = \bar{b} \\ \bar{b} = \bar{c} \end{matrix}\right| \Rightarrow \bar{a} = \bar{c}$

Notație $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\bar{0} \le i < j \le n-1 \Rightarrow \bar{i} \neq \bar{j}$

~~R.A.A~~

Dacă $\bar{i} = \bar{j} \Leftrightarrow n \mid (j-i)$, $n \in \mathbb{Z} \Rightarrow$ ~~$(j-i) \mid n$~~

$|j-i| = n \cdot a$, $a \in \mathbb{Z}$

2) $|j-i| = |n| \cdot |a| \le n-1 \Rightarrow n \le n-1$ contradicție

Obs 1) $\left.\begin{matrix} 0 \le i < j \le n-1 \\ \text{~~$A \in \mathbb{N}$~~} \\ i, j \in \mathbb{N} \end{matrix}\right| \Rightarrow \bar{i} \neq \bar{j}$

2) $a \in \mathbb{Z} \Rightarrow \exists\, i \in \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ a.î. $\bar{a} = \bar{i}$

Dem Th împărțirii cu rest $\Rightarrow a = n \cdot q + i$, $q \in \mathbb{Z}$

$\Leftrightarrow n \mid (a-i) \Leftrightarrow \bar{a} = \bar{i}$

# Structura de grup pe $\mathbb{Z}_n$

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

Definim $\bar{a} + \bar{b} = \overline{a+b}$

Este corectă definiția?

$\left.\begin{array}{l} \bar{a} = \bar{a_1} \\ \bar{b} = \bar{b_1} \end{array}\right| \Rightarrow$ ~~$\overline{a+b} = \overline{a_1+b_1}$~~ $\bar{a}+\bar{b} = \bar{a_1}+\bar{b_1}$

$\Rightarrow \bar{a} - \bar{a_1} = \bar{0} \Rightarrow n \mid (a-a_1)$ $\left| \Rightarrow n \mid (a-a_1+b-b_1) \right.$ $\Rightarrow$
$\Rightarrow n \mid (b-b_1)$

$\Leftarrow \bar{a} - \bar{a_1} + \bar{b} - \bar{b_1} = \bar{0} \Leftrightarrow \bar{a} + \bar{b} = \bar{b_1} + \bar{a_1}$

Prop: $(\mathbb{Z}_n, +)$ grup comutativ cu $n$ elemente

- relativ pe $\mathbb{Z}_n$

$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c}$ (asociativitatea pe $\mathbb{Z}$)

$= \overline{a+b} + \bar{c}$

$\bar{a} + \bar{0} = \bar{a}, \forall \bar{a} \in \mathbb{Z}_n$

$a \in \mathbb{Z}$

$a + \bar{a} = -\bar{a} + \bar{a} = \bar{0}$

$\left.\begin{array}{l} \bar{a}+\bar{b} = \overline{a+b} \\ \bar{b}+\bar{a} = \overline{b+a} \end{array}\right| \Rightarrow \bar{a}+\bar{b} = \bar{b}+\bar{a}$

$\Rightarrow (\mathbb{Z}_n, +)$ grup abelian

Teoremă $(G,+)$ grup comutativ $\Rightarrow$ ~~$(G,+) \cong (\mathbb{Z}_n, +)$~~

~~$(G,+) \cong (\mathbb{Z}_n, +) \times (\mathbb{Z}, +)$~~

$G \cong (\mathbb{Z}_{n_1}, +) \times (\mathbb{Z}_{n_2}, +) \times \ldots \times (\mathbb{Z}_{n_k}, +) \times (\mathbb{Z}, +)$

Explicația termenilor

1). $(G, \cdot)$ grup

Spunem că $(G, \cdot)$ este finit generat, dacă $\exists$ o mulțime finită $\{g_1, g_2, \ldots, g_n\} \subseteq G$, (a.î.) ~~el se poate~~ $\forall g \in G$ el se poate scrie $g = h_1 \cdot h_2 \cdot \ldots \cdot h_m$, unde $h_i = g_j$ pt $\forall j \in \overline{1,n}$

$(G_1, *)$, $(G_2, \perp)$ – grupuri

Spunem că $G_1$ este izomorfe cu $G_2$ ($G_1 \cong G_2$)

dacă $\exists\ f: G_1 \to G_2$, $f$ bijectivă

$$f(g_1 * g_2) = f(g_1) \perp f(g_2)$$

Construcție: $(G_1, *)$, $(G_2, \perp)$ e

$(G_1 \times G_2, \circ)$ – grup

Definim $(g_1, g_2) \circ (h_1, h_2) = (g_1 * h_1, g_2 * h_2)$

$(e_1, e_2)$ – elementele neutre

$$(g_1, g_2) \circ (h_1^{-1}, h_2^{-1}) = (e_1, e_2)$$

Definim o altă operație pe $\mathbb{Z}_n$

$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ – demonstrație similară

elementul neutru este $\bar{1}$

Obs $\bar{0}$ nu are invers $\overline{a} \cdot \overline{a} = \bar{0} \cdot \bar{a}$, $\forall \bar{a} \in \mathbb{Z}_n$

e) $(\mathbb{Z}_n, \cdot)$ – monoid

$U(\mathbb{Z}_n) = \{ \bar{a} \mid a \in \mathbb{Z}, (a,n) = 1 \}$

Ex $U(\mathbb{Z}_{12}) = \{ \bar{1}, \bar{5}, \bar{7}, \bar{11} \}$ $\quad \bar{1}\cdot\bar{1} = \bar{1}$, $\bar{5}\cdot\bar{5} = \bar{1}$, $\bar{7}\cdot\bar{7} = \bar{1}$, $\bar{11}\cdot\bar{11} = \bar{1}$

// $\prod_{i=1}^{k} (\mathbb{Z}_{n_i}, +)$ | $|A \times B| = |A| \cdot |B|$

$(\mathbb{Z}_4, +) \times$

$(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +) \simeq (U(\mathbb{Z}_n), \cdot)$

Propoziție $(U(\mathbb{Z}_n), \cdot)$ grup

// folosim lema de dată trecută

$\bar{a} \in U(\mathbb{Z}_n)$
$\bar{b} \in U(\mathbb{Z}_n)$ $\Rightarrow \bar{a}\cdot\bar{b} \in U(\mathbb{Z}_n)$

$\Rightarrow (a,n) = 1$
$\Rightarrow (b,n) = 1$ $\Rightarrow (a\cdot b, n) = 1$

Demonstrat; $\bar{m}\cdot\bar{a} = \bar{m}\cdot\bar{b} \Rightarrow \bar{a} = \bar{b}$, $m, a, b \in \mathbb{Z}_n$

$\Rightarrow \begin{cases} (m,n) = 1 \\ (m,n) = 1 \\ (a,n) = 1 \end{cases}$ $\Rightarrow n \mid (ma - mb) \Rightarrow n \mid m(a-b) \overset{(m,n)=1}{\Rightarrow}$

$\Rightarrow n \mid (a-b) \Rightarrow \bar{a} = \bar{b}$

# Principiul incluziunii și excluderii (P i & e)

$A_1, A_2, \dots, A_n$ mulțimi oarecare

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{j=1}^{n} |A_j| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \dots + (-1)^{n+1} \left|\bigcap_{j=1}^{n} A_j\right|$$

Câte elemente are $P(n)$

$P(n) = \{ m \in \mathbb{N} \mid 0 \le m \le n-1 \mid (m, n) = 1 \} = \varphi(n)$

$n \ge 2 \quad n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}, \quad p_i \ne p_j \ \forall 1 \le i, j \le n$

$|A - B| = |A| - |B|$

$A = \{ k \mid 0 \le k \le n-1, (k, n) \ne 1 \} \Rightarrow \exists p_i \mid k$

$A_i = \{ k \in \mathbb{N} \mid 0 \le k \le n-1, p_j \mid k \}_{j = \overline{1,k}}$

$A = \bigcup_{j=1}^{k} A_j$ o aplicăm în formula (P i & e)

$$\varphi(n) = n - \sum_{j=1}^{k} \frac{n}{p_j} + \sum_{i,j} \frac{n}{p_i p_j} - \sum \frac{n}{p_1 p_2 \cdots p_k} + \dots + (-1)$$