Profesor Blaga Mirela-Gabriela

Clase de resturi modulo n

O mulţime specială de obiecte matematice este mulţimea claselor de resturi modulo n, pe care s-au definit două operaţii algebrice, numite adunarea şi înmulţirea modulo n.

Rezultatele provin din Teorema împărţirii cu rest în mulţimea numerelor întregi.

Teoremă. Fiind dat un număr natural n, nenul, pentru orice număr întreg a există numerele unice q, număr întreg şi r număr natural, mai mic decât n, astfel încât $a = nq + r$.

Exemplu. La împărţirea numărului întreg 5 la numărul întreg pozitiv 3, obţinem $5 = 3 \cdot 1 + 2$, unde $a = 5, n = 3, q = 1$ şi $r = 2$, $0 \leq 2 < 3$.

1) Numărul q este câtul şi r este restul împărţirii numărului a la n.

Exemplu. $5 = 3 \cdot 1 + 2$, unde $a = 5, n = 3$, câtul $q = 1$ şi restul $r = 2$, $0 \leq 2 < 3$

2) Notaţia folosită este $r = a \; mod \; n$ şi se citeşte "$a \; modulo \; n$".

Exemplu. $2 = 5 \; mod \; 3$

3) Presupunând că împărţim toate numerele întregi la n, resturile obţinute sunt mai mari sau egale cu 0, dar mai mici sau egale cu $n - 1$, rezultă că există n tipuri de numere întregi, care formează n submulţimi, disjuncte două câte două, a căror reuniune formează mulţimea $\mathbb{Z}$.

Exemplu. $2 = 8 \; mod \; 3$, $1 = 7 \; mod \; 3$, $0 = 6 \; mod \; 3$

4) În general, pentru n, submulţimile sunt de forma $nk, nk + 1, nk + 2, \ldots , nk + (n - 1)$, unde $k \in \mathbb{Z}$.

Exemplu. Pentru $n = 3$ avem submulţimile $3k, 3k + 1, 3k + 2, k \in \mathbb{Z}$.

5) Clasa de resturi modulo n a lui a este mulţimea $\hat{a} = \{a + nk \mid k \in \mathbb{Z}\}$.

Exemplu. Pentru $n = 3$ avem $\hat{2} = \{\ldots, -1, 2, 5, \ldots\}, \hat{1} = \{\ldots, 1, 4, 7, \ldots\}, \hat{0} = \{\ldots, 0, 3, 6, \ldots\}$.

6) Mulţimea claselor de resturi modulo n este $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ \ldots, \ \widehat{n-1}\}, n \in \mathbb{N}^*$.

Exemplu. $\mathbb{Z}_3 = \{\hat{0}, \hat{1}, \hat{2}\}$

7) Adunarea modulo n: $\hat{a} + \hat{b} = \widehat{a + b}$

Exemplu. $\hat{2}, \hat{4} \in \mathbb{Z}_5 \quad \hat{2} + \hat{4} = \widehat{2 + 4} = \hat{1}$ pentru că $6 = 5 \cdot 1 + 1$

8) Înmulţirea modulo n: $\hat{a} \cdot \hat{b} = \widehat{a \cdot b}$

Exemplu. $\hat{2}, \hat{4} \in \mathbb{Z}_5 \quad \hat{2} \cdot \hat{4} = \widehat{2 \cdot 4} = \hat{3}$ pentru că $8 = 5 \cdot 1 + 3$

9) Tabla lui Cayley pentru adunarea modulo 3 este

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{0}$	$\hat{1}$

10) Tabla lui Cayley pentru înmulţirea modulo 3 este

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{1}$