

Τετάρτη 16 Δεκεμβρίου 2015

Έστω $n \in \mathbb{N}$. Τότε: $\forall a, b \in \mathbb{Z} : a \equiv b \pmod{n} \Leftrightarrow n \mid a - b$, οί a, b είναι ισοαίμοι $\pmod{n}$

Η σχέση ισοαίμοις $\pmod{n}$ είναι μία σχέση ισοδυναμίας στο $\mathbb{Z}$

Αν X τυχαίο σύνολο και " $\sim$ " είναι μία σχέση ισοδυναμίας επί του X , τότε: $\forall x \in X$, το σύνολο $[x]_{\sim} = \{y \in X \mid y \sim x\}$: η κλάση ισοδυναμίας του $x \in X$. Τότε:

- ① $\forall x \in X : [x]_{\sim} \neq \emptyset$ (όσοι $x \in [x]_{\sim}$)
 - ② $\forall x, y \in X : \text{είτε } [x]_{\sim} \cap [y]_{\sim} = \emptyset \text{ είτε } [x]_{\sim} = [y]_{\sim}$
 - ③ $X = \bigcup_{x \in X} [x]_{\sim}$
- } $\Rightarrow$

$\Rightarrow$ η συλλογή υποσυνόλων $X/\sim = \{[x]_{\sim} \subseteq X \mid x \in X\}$ είναι μία διαμέριση του X . Το σύνολο $X/\sim$ καλείται σύνολο-πηλίκο του X ως προς τη σχέση ισοδυναμίας $\sim$

Έστω $a \in \mathbb{Z}$. Τότε, η κλάση ισοδυναμίας του a ως προς τη σχέση ισοαίμοις $\pmod{n}$ καλείται κλάση ισοαίμοις $\pmod{n}$ και συμβολίζεται με $[a]_n$. Τότε:

$$[a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} = \{x \in \mathbb{Z} \mid n \mid x - a\} = \{x \in \mathbb{Z} \mid x - a = kn, \text{ για κάποιο } k \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x = a + kn, k \in \mathbb{Z}\} \Rightarrow$$
$$\Rightarrow [a]_n = \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$$

Το σύνολο πηλίκο του $\mathbb{Z}$ ως προς τη σχέση ισοαίμοις $\pmod{n}$ θα συμβολίζεται με $\mathbb{Z}_n = \{[a]_n \subseteq \mathbb{Z} \mid a \in \mathbb{Z}\} = \mathbb{Z}/\sim$

Ισοκυρίοις: $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$

Προφανώς: $\{[0]_n, [1]_n, \dots, [n-1]_n\} \subseteq \mathbb{Z}_n$. Έστω $[a]_n \in \mathbb{Z}_n$. Τότε, από την ευκλείδεια διαίρεση τα a με το n θα έχουμε: $a = n \cdot q + r$, $0 \leq r \leq n-1$. Άρα, $\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$
Αν $a, b = 0, 1, \dots, n-1$ και $[a]_n = [b]_n \Rightarrow a \equiv b \pmod{n} \Rightarrow$

$\Rightarrow n | a-b \Rightarrow n \leq a-b$, άτονο (αν $a \neq b$), άρα τα $a, b \leq n-1$

Άρα $a=b$

Άρα το πλήθος των στοιχείων του $\mathbb{Z}_n$ είναι αριθμός n

Για παράδειγμα: $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$$

Ιδιότητες:

① $\forall a \in \mathbb{Z} : [a]_n \neq \emptyset$

② $\forall a, b \in \mathbb{Z} : [a]_n \cap [b]_n = \emptyset$ (ii) $[a]_n = [b]_n$

③ $\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} [a]_n$

$$[a]_n = [b]_n \Leftrightarrow a \in [b]_n \Leftrightarrow b \in [a]_n \Leftrightarrow a \equiv b \pmod{n}$$

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

Θεωρούμε τις εξής απεικονίσεις επί του συνόλου $\mathbb{Z}_n$

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a]_n + [b]_n := [a+b]_n$$

$$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a]_n \cdot [b]_n := [a \cdot b]_n$$

Οι πράξεις που ορίσαμε $+$ και $\cdot$ στο σύνολο $\mathbb{Z}_n$ είναι καλά ορισμένες, δηλαδή:

$$[a]_n = [a']_n \quad \Bigg| \Rightarrow \quad [a]_n + [b]_n = [a']_n + [b']_n, [a+b]_n = [a'+b']_n$$

$$[b]_n = [b']_n \quad \Bigg| \Rightarrow \quad [a]_n [b]_n = [a']_n [b']_n, [ab]_n = [a'b']_n$$

$$\begin{array}{l} \text{Τότε: } a \equiv a' \pmod{n} \\ \quad \quad b \equiv b' \pmod{n} \end{array} \quad \Bigg| \Rightarrow \quad \begin{array}{l} a+b \equiv a'+b' \pmod{n} \\ ab \equiv a'b' \pmod{n} \end{array}$$

$$\Bigg| \Rightarrow \quad \begin{array}{l} [a+b]_n = [a'+b']_n \\ [ab]_n = [a'b']_n \end{array}$$

Αν $n=2$, άρα θα δείαμε στο $\mathbb{Z}_2$, τότε για παράδειγμα

$$[0]_2 = [4]_2$$

$$[1]_2 = [3]_2$$

$$\begin{aligned}\text{Τότε: } [0]_2 + [1]_2 &= [0+1]_2 = [1]_2 \\ [1]_2 + [3]_2 &= [4+3]_2 = [7]_2 = [1]_2\end{aligned}$$

Παράδειγμα: Αν $n=8$ και τότε έστω:

$$[35]_8 + [23]_8 = [35+23]_8 = [58]_8 = [2]_8$$

$$[3]_8 + [7]_8 = [10]_8 = [2]_8$$

Πρόταση: Στο σύνολο $\mathbb{Z}_n$, οι πράξεις $+$, $\cdot$ κλάσεων ισοτιμίας mod n ικανοποιούν τις ακόλουθες ιδιότητες, $\forall x, y, z \in \mathbb{Z}_n$:

① $x + (y + z) = (x + y) + z$

② $x + y = y + x$

③ Υπάρχει μια κλάση ισοτιμίας mod n , η $[0]_n$ είναι αδέτερο στοιχείο ως προς την πρόσθεση
 $x + [0]_n = x = [0]_n + x$

④ $\forall x \in \mathbb{Z}_n : \exists$ η κλάση ισοτιμίας $-x : x + (-x) = [0]_n = (-x) + x$

⑤ $x(y \cdot z) = (xy)z$

⑥ $xy = yx$

⑦ $\begin{cases} x(y+z) = xy + xz \\ (x+y)z = xz + yz \end{cases}$

⑧ Υπάρχει μια κλάση ισοτιμίας mod n , η $[1]_n$ έτσι ώστε
 $x[1]_n = x = [1]_n x$

Το σύνολο $\mathbb{Z}_n$ μαζί με τις πράξεις $+$, $\cdot$ αποτελεί έναν μεταθετικό δακτύλιο με μονάδα.

Πρόβλημα: Στο σύνολο $\mathbb{Z}_n$, τότε για μια κλάση ισοτιμίας $[a]_n$, υπάρχει $[b]_n \in \mathbb{Z}_n : [a]_n \cdot [b]_n = [1]_n$;
 Έστω ότι υπάρχει $[b]_n \in \mathbb{Z}_n : [a]_n \cdot [b]_n = [1]_n \Rightarrow$
 $\Rightarrow [ab]_n = [1]_n \Rightarrow ab = 1 \pmod n \Rightarrow n \mid ab - 1 \Rightarrow ab - 1 = kn,$
 για κάποιο $k \in \mathbb{Z} \Rightarrow \exists k \in \mathbb{Z}, ab + (-k)n = 1 \Leftrightarrow (a, n) = 1$

Άρα: για την $[a]_n, \exists [b]_n \in \mathbb{Z}_n : [a]_n [b]_n = [1]_n \Rightarrow$
 $\Rightarrow (a, n) = 1$

Αντίστροφα, αν $(a, n) = 1 \Rightarrow \exists b, \lambda \in \mathbb{Z}_n : ab + \lambda n = 1 \Rightarrow$
 $\Rightarrow [ab + \lambda n]_n = [1]_n \Rightarrow [ab]_n + [\lambda n]_n = [1]_n \Rightarrow$
 $\Rightarrow [a]_n [b]_n + [\lambda n]_n = [1]_n \Rightarrow [a]_n [b]_n = [1]_n$

Ορισμός: Αν $[a]_n \in \mathbb{Z}_n$, τότε η τάση ισοτιμίας $[a]_n$ λέγεται αναστρέγιμη $\Leftrightarrow \exists [b]_n \in \mathbb{Z}_n : [a]_n [b]_n = [1]_n$ και τότε θα γράφουμε $[b]_n = [a]_n^{-1}$ αντίστροφη τάση ισοτιμίας του $[a]_n$.

Θέτουμε $U(\mathbb{Z}_n) = \{[a]_n \in \mathbb{Z}_n \mid (a, n) = 1\}$: το σύνολο των αναστρέγιμων τάσεων ισοτιμίας mod n. Τότε:
 $|U(\mathbb{Z}_n)| = \phi(n)$

Παράδειγμα: $n = 49$ και άρα θα γράφουμε στο $\mathbb{Z}_{49}$. Θεωρούμε το στοιχείο $[88]_{49}$.

$(88, 49) = 1$ και άρα $[88]_{49} \in U(\mathbb{Z}_n)$. Ποια τάση είναι η $[88]_{49}^{-1}$;

Επειδή $\underbrace{9}_{\lambda} \cdot \underbrace{49}_{n} + \underbrace{(-5)}_b \cdot \underbrace{88}_a = 1 \Rightarrow$

$$\Rightarrow [88]_{49} [-5]_{49} = [1]_{49} \Rightarrow$$

$$\Rightarrow [88]_{49}^{-1} = [-5]_{49} = [44]_{49}$$

$\forall n \geq 2$ η τάση $[0]_n \in \mathbb{Z}_n$ δεν είναι ποτέ αναστρέγιμη. Παρά $[a]_n \in \mathbb{Z}_n, \mu \in [a]_n \neq [0]_n$ είναι αναστρέγιμη;

Πρόταση: Κάθε m - m δεστική σχέση $\text{mod } n$ είναι
αντιστρέψιμη $\Leftrightarrow n$: πρώτος

$$U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{[0]_n\} \Leftrightarrow n: \text{πρώτος}$$

Απόδειξη: $U(\mathbb{Z}_n) = \{[a]_n \in \mathbb{Z}_n \mid (a, n) = 1\} =$

$$= \{[a]_n \in \mathbb{Z}_n \mid \text{οι αριθμοί } a, n \text{ δεν έχουν κανέναν κοινό διαιρέτη παρά μόνο τη μονάδα}\}$$

Αυτά συμβαίνει $\Leftrightarrow n$: πρώτος

$\mathbb{Z}_n$: μεταθετικός δακτύλιος με μονάδα

σώμα: μεταθετικός δακτύλιος με μονάδα, κάθε στοιχείο
διαφορο του μηδέν, είναι αντιστρέψιμο

$\mathbb{Z}_n$: σώμα $\Leftrightarrow n$: πρώτος