06-12-16

Ισοτιμίες

↳ **Ορισμός:** Αν $a,b \in \mathbb{Z}$ λέμε ότι οι a,b είναι ισότιμοι mod n και γράφουμε συμβολικά $a \equiv b \pmod n \iff n \mid a-b$

(Αν οι a,b δεν είναι ισότιμοι mod n, γράφουμε $a \not\equiv b \pmod n$)

Παραδείγματα: 1) $17 \equiv -7 \pmod 8$, διότι $8 \mid 17-(-7) = 24$

2) $6 \not\equiv 11 \pmod 3$, διότι $3 \nmid 6-11 = -5$

↳ **Βασικές Ισιότητες**

1) $a \equiv 0 \pmod n \iff n \mid a$

2) $a \equiv 0 \pmod 2 \iff 2 \mid a \iff a$: άρτιος

3) $a \equiv 1 \pmod 2 \iff 2 \mid a-1 \iff \exists k \in \mathbb{Z} : a-1 = 2k \Rightarrow a = 2k+1$
$\iff a$: περιττός

4) $\forall a,b \in \mathbb{Z} : a \equiv b \pmod 1$

5) $\left.\begin{matrix} a \equiv b \pmod n \\ m \mid n \end{matrix}\right\} \Rightarrow a \equiv b \pmod m$ διότι: $\left.\begin{matrix} n \mid a-b \\ m \mid n \end{matrix}\right\} \Rightarrow$
$\Rightarrow m \mid a-b \Rightarrow a \equiv b \pmod m$

↳ [Πρόταση: Έστω $n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Τότε: $a \equiv b \pmod n \iff$

$\iff a, b$ έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με το n

Απόδειξη: "$\Leftarrow$" Έστω ότι οι a, b έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με το n

Άρα, $\exists\, q_1, q_2 \in \mathbb{Z}$ και $r \in \mathbb{N} \cup \{0\}$ έτσι ώστε:

$$\begin{cases} a = n \cdot q_1 + r & 0 \le r < n \\ b = n \cdot q_2 + r \end{cases}$$

Τότε $a - b = n(q_1 - q_2) \Rightarrow n \mid a - b \Rightarrow a \equiv b \pmod n$

"$\Rightarrow$" Έστω ότι $a \equiv b \pmod n \Rightarrow n \mid a - b \Rightarrow$

$\Rightarrow \exists\, q \in \mathbb{Z} : a - b = n \cdot q \Rightarrow a = b + nq$ (1)

Από την Ευκλείδεια Διαίρεση του b με το n:

$b = n \cdot k + r$, $0 \le r < n$ (2)

(1), (2) $\Rightarrow a = n \cdot k + r + n \cdot q = n(k+q) + r$, $0 \le r < n$ (3)

(2), (3) $\Rightarrow$ Οι a, b έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με το n.

[Μια μικρή επανάληψη στις σχέσεις]

Έστω $X \neq \emptyset$. Μια σχέση επί του X είναι ένα υποσύνολο $R \subseteq X \times X = \{(x_1, x_2) \mid x_i \in X,\ i = 1, 2\}$

Αν $x,y \in X$ τότε τα x,y σχετίζονται μέσω της $R \Leftrightarrow$

$\Leftrightarrow (x,y) \in R$ και τότε θα γράφαμε xRy

Μια σχέση R επί ενός συνόλου X καλείται σχέση ισοδυναμίας $\Leftrightarrow$ ικανοποιεί τις ακόλουθες ιδιότητες:

1) Ανακλαστική: $\forall x \in X \; : xRx$

2) Συμμετρική: $\forall x,y \in X \; : xRy \Longleftrightarrow yRx$

3) Μεταβατική: $\forall x,y,z \in X$: Αν $\left.\begin{matrix} xRy \\ yRz \end{matrix}\right\} \Rightarrow xRz$

$\forall x \in X$, η κλάση ισοδυναμίας του x ως προς R είναι το σύνολο:

$$[x]_R = \{y \in X \mid yRx\} = \{y \in X \mid xRy\}$$

Το σύνολο $X/R = \{[x]_R \subseteq X \mid x \in X\}$ καλείται

σύνολο πηλίκο του X ως προς τη σχέση ισοδυναμίας R

Για τις κλάσεις ισοδυναμίας των στοιχείων του X ισχύουν οι ακόλουθες ιδιότητες:

1) $\forall x \in X : [x]_R \neq 0$, διότι $x \in [x]_R$

2) $\forall x,y \in X$. Είτε $[x]_R = [y]_R$

είτε $[x]_R \cap [y]_R = \phi$

3) $X = \bigcup_{x \in X} [x]_R$

Επιπλέον $\forall x, y \in X : [x]_R = [y]_R \iff$

$x \in [y]_R \iff y \in [x]_R \iff xRy$

↳ Πρόταση: Έστω $n \in \mathbb{N}$. Τότε ορίζοντας για κάθε $a, b \in \mathbb{Z} : aRb \iff a \equiv b \pmod n$, αποκτούμε μια σχέση ισοδυναμίας επί του $\mathbb{Z}$

Απόδειξη: 1) $\forall a \in \mathbb{Z} : a \equiv a \pmod n$, διότι: $n \mid a - a = 0$

Άρα $\forall a \in \mathbb{Z} : aRna$

2) $a, b \in \mathbb{Z}$ και αν $a \equiv b \pmod n \Rightarrow n \mid a - b \Rightarrow n \mid b - a \Rightarrow$

$\Rightarrow b \equiv a \pmod n$

Δηλαδή: $\forall a, b \in \mathbb{Z} : aRnb \Rightarrow bRna$

3) $\forall a, b, c \in \mathbb{Z} : \left.\begin{array}{l} a \equiv b \pmod n \Rightarrow n \mid a - b \\ b \equiv c \pmod n \Rightarrow n \mid b - c \end{array}\right\} \Rightarrow$

$\Rightarrow n \mid (a - b) + (b - c) \Rightarrow n \mid a - c$

Άρα: $a \equiv c \pmod n$

Συνεπώς, $\left.\begin{array}{l} aRnb \\ bRnc \end{array}\right\} \Rightarrow aRnc$

Άρα, η σχέση R_n είναι σχέση ισοδυναμίας

Έστω η σχέση ισοτιμίας (mod n) επί του $\mathbb{Z}$ και $a \in \mathbb{Z}$

$[a]_n$: κλάση ισοδυναμίας του a ως προς την R

Η $[a]_n$ καλείται κλάση ισοτιμίας (mod n) του a

$$[a]_n = \{b \in \mathbb{Z} \mid b \equiv a \pmod n\} = \{b \in \mathbb{Z} \mid n \mid b-a\} =$$

$$= \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : b-a = k \cdot n\} = \{b \in \mathbb{Z} \mid \exists k \in \mathbb{Z} : b = a + kn\} =$$

$$= \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$$

Πχ: $[-2]_n = \{-2 + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$

$[-1]_n = \{-1 + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$

$[0]_n = \{kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$

$[1]_n = \{1 + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$

$[2]_n = \{2 + kn \in \mathbb{Z} \mid k \in$ }

⋮

↳ Πόσες διαφορετικές κλάσεις ισοτιμίας mod n υπάρχουν στο $\mathbb{Z}$;

Το σύνολο πηλίκο του $\mathbb{Z}$ ως προς τη σχέση ισοτιμίας mod n θα συμβολίζεται $\mathbb{Z}_n$

$$\mathbb{Z}_n = \{[a]_n \subseteq \mathbb{Z} \mid a \in \mathbb{Z}\}$$

↳ Ισχυρισμός: $Z_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$

Προφανώς $\{[0]_n, [1]_n, \dots, [n-1]_n\} \subseteq Z_n$

Έστω $\alpha \in Z$. Τότε $\alpha = nq + r$, $0 \le r < n \Rightarrow$

$\Rightarrow \alpha - r = nq \Rightarrow n \mid \alpha - r \Rightarrow \alpha \equiv r \pmod n \Rightarrow$

$\Rightarrow [\alpha]_n = [r]_n \in \{[0]_n, [1]_n, \dots, [n-1]_n\}$

Άρα, ο ισχυρισμός είναι αληθής

Αν $r_1, r_2 \in Z$, $0 < r_1, r_2 \le n-1$ και $[r_1]_n = [r_2]_n$

Θα έχουμε $r_1 \equiv r_2 \pmod n \Rightarrow n \mid r_1 - r_2$

Αν $r_1 - r_2 \neq 0 \Rightarrow n \le r_1 - r_2 < n$. Άτοπο

Συνεπώς, $\boxed{r_1 = r_2}$

Άρα, $[r_1]_n = [r_2]_n$, $0 \le r_1, r_2 \le n-1$ $\Rightarrow r_1 = r_2$

Άρα, $|Z_n| = n$

↳ Πρόταση: Έστω $n \ge 1$, $a, b, c, d \in Z$ και

$f(x) = c_0 + c_1 x + \dots + c_k x^k$, $c_0, c_1, \dots, c_k \in Z$

1) $\left.\begin{array}{l} a \equiv b \pmod n \\ c \equiv d \pmod n \end{array}\right\} \Rightarrow \begin{array}{l} a+c \equiv b+d \pmod n \\ a \cdot c \equiv b \cdot d \pmod n \end{array}$

2) $a \equiv b \pmod n \Rightarrow a+c \equiv b+c \pmod n$
και
$a \cdot c \equiv b \cdot c \pmod n$

3) $a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n \quad \forall \; k \geq 1$

4) $a \equiv b \pmod n \Rightarrow f(a) \equiv f(b) \pmod n$.

Απόδειξη: 1) Έστω $\left.\begin{array}{l} a \equiv b \pmod n \Rightarrow n \mid a-b \\ c \equiv d \pmod n \Rightarrow n \mid c-d \end{array}\right\} \Rightarrow$

$\Rightarrow n \mid (a+c)-(b+d) \Rightarrow a+c \equiv b+d \pmod n$

Επιπλέον: $a-b = kn$, για κάποιο $k \in \mathbb{Z}$

$c-d = \lambda n$, -11- $\lambda \in \mathbb{Z}$

$\left.\begin{array}{l} a = b+kn \\ c = d+\lambda n \end{array}\right\} \Rightarrow ac = bd + n(b\lambda + kd + nk\lambda)$
$\Rightarrow n \mid ac-bd \Rightarrow ac \equiv bd \pmod n$

2) $\left.\begin{array}{l} a \equiv b \pmod n \\ c \equiv c \pmod n \end{array}\right\} \Rightarrow \begin{array}{l} a+c \equiv b+c \pmod n \\ a \cdot c \equiv b \cdot c \pmod n \end{array}$

3) Έστω ότι $a \equiv b \pmod n \Rightarrow a^1 \equiv b^1 \pmod n$

Επαγωγική Υπόθεση: $a^{k-1} \equiv b^{k-1} \pmod n$, $k \geq 2$

Από την ①: $\alpha^{k-1}\cdot\alpha \equiv b^{k-1}\cdot b \pmod n \Rightarrow \alpha^k \equiv b^k \pmod n$

4) Έστω $f(x) = c_0 + c_1 x + \dots + c_k x^k$

$\alpha \equiv b \pmod n$

Από την 3) $\Rightarrow \forall m \geq 1 : \alpha^m \equiv b^m \pmod n$ ② $\Rightarrow$

$\Rightarrow \forall c_i \in Z : c_i \alpha^i \equiv c_i b^i \pmod n$

$i = 0, \dots, k$

Τότε από την ①: $c_0 + c_1\alpha + \dots + c_k \alpha^k \equiv c_0 + c_1 b + \dots + c_k b^k \pmod n$

$\Rightarrow f(\alpha) \equiv f(b) \pmod n$

Παράδειγμα: Να βρεθεί το υπόλοιπο της διαίρεσης

$$\frac{13^{23}\cdot 27^{41}}{8}$$ ⊛

$\cdot\ 13 \equiv 5 \pmod 8 \Rightarrow 13^{23} \equiv 5^{23} \pmod 8$

Όμως $5^2 \equiv 1 \pmod 8$

Άρα: $13^{23} \equiv 5^{23} \pmod 8 \Rightarrow 5^{23} = 5^{2\cdot 11+1} = (5^2)^{11}\cdot 5^1 \pmod 8$

$\Rightarrow 13^{23} \equiv 1^{11}\cdot 5^1 \pmod 8 \equiv 5 \pmod 8$

Συνεπώς $13^{23} \equiv 5 \pmod 8$

• $27 \equiv 3 \pmod 8 \rightarrow 27^{41} \equiv 3^{41} \pmod 8 \equiv 3^{2\cdot 20+1} \pmod 8 \equiv$

$\equiv (3^2)^{20} \cdot 3^1 \pmod 8 \equiv 1^{20} \cdot 3^1 \pmod 8 \equiv 3 \pmod 8$

Άρα, $27^{41} \equiv 3 \pmod 8$

Συνεπώς, $13^{23} 27^{41} \equiv 5 \cdot 3 \pmod 8 \equiv 15 \pmod{18} \equiv 7 \pmod 8$

$\Rightarrow$ Υπόλοιπο διαίρεσης της ⊛ είναι το 7.

↳ Παρατήρηση: Τελευταίο ψηφίο ενός αριθμού =

= Υπόλοιπο διαίρεσης αριθμού με το 10

$\forall \alpha \geq 1 : \alpha = \alpha_k \cdot 10^k + \alpha_{k-1} \cdot 10^{k-1} + \ldots + \alpha_1 \cdot 10 + \alpha_0$

$0 \leq \alpha_i \leq 9 \quad , i = 0, \ldots k$

Υπόλοιπο διαίρεσης του α με το $10 = \alpha_0$

Παράδειγμα: 7777^{5555}

Το τελευταίο ψηφίο είναι ένας αριθμός $r, 0 \leq r \leq 9$

έτσι ώστε $7777^{5555} = r \pmod n$