07-12-16

Previously on Beligiannis

$\forall n \geq 1 : \forall a, b \in \mathbb{Z} : a \equiv b \pmod{n} \iff n \mid a-b$

Η παραπάνω σχέση είναι σχέση ισοδυναμίας στο $\mathbb{Z}$ η οποία καλείται σχέση ισοτιμίας mod n

$\forall a \in \mathbb{Z} : [a]_n = \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$: η κλάση ισοδυναμίας του στοιχείου $a \in \mathbb{Z}$

$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$: σύνολο πηλίκο του $\mathbb{Z}$ ως προς τη σχέση ισοτιμίας mod n

↳ Πρόταση : Έστω ότι $n \geq 1$, $k \in \mathbb{N}$ και $a, b \in \mathbb{N}$

Αν θέσουμε $d = (k, n)$, τότε : $ka \equiv kb \pmod{n} \iff$

$$\iff a \equiv b \left(\mathrm{mod}\ \frac{n}{d}\right)$$

Απόδειξη : $d = (k,n) \Rightarrow \begin{matrix} d \mid k \\ d \mid n \end{matrix}$ $\zeta \Rightarrow \begin{matrix} k = dk' \\ n = dn' \\ (k', n') = 1 \end{matrix}$

" $\Leftarrow$ " Έστω ότι : $a \equiv b \left(\mathrm{mod}\ \frac{n}{d}\right) \Rightarrow$

$$\Rightarrow \frac{n}{d} \mid a-b \Rightarrow n \mid d(a-b)$$

$$\Rightarrow n \mid dk'(a-b) \Rightarrow n \mid k(a-b) = ka - kb \Rightarrow$$

$$\Rightarrow ka \equiv kb \pmod{n}$$

"$\Rightarrow$" Έστω ότι: $k\alpha \equiv kb \pmod n \Rightarrow n \mid k\alpha - kb \Rightarrow$

$\Rightarrow n \mid k(\alpha - b) \Rightarrow d n' \mid d k'(\alpha - b) \Rightarrow$

$\Rightarrow n' \mid k'(\alpha - b)$ $\left.\begin{array}{l} \text{λήμμα} \\ \Rightarrow \text{του} \\ \text{Ευκλείδη} \end{array}\right\}$ $(n', k') = 1$ $\quad n' \mid \alpha - b \Rightarrow \alpha \equiv b \pmod{n'} \Rightarrow$

$\Rightarrow \alpha \equiv b \pmod{\frac{n}{d}}$

Άσκηση: $(\alpha + b)^p \equiv \alpha^p + b^p \pmod p$, αν p: πρώτος και $\alpha, b \in \mathbb{Z}$

Γενικά: $(\alpha+b)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^{p-k} b^k$, όπου

$\binom{p}{k} = \frac{p!}{(p-k)!\,k!} \in \mathbb{Z}$, διότι είναι το πλήθος των τρόπων με τους οποίους επιλέχαμε k πράγματα από p πράγματα $(0 \le k \le p)$

$$(\alpha+b)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^{p-k} b^k = \alpha^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k} b^k$$

Αρκεί νδο: $\sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k} b^k \equiv 0 \pmod p$

Ισοδύναμα αρκεί νδο: $\binom{p}{k} \equiv 0 \pmod p$, $1 \le k \le p-1$

Συμ: $p \mid \binom{p}{k}$

$$\binom{p}{k} = \frac{p!}{(p-k)!\,k!} = \frac{1 \cdot 2 \cdot 3 \cdots (p-k-1)(p-k)(p-k+1)\cdots p}{(p-k)!\,k!}$$

$$= \frac{p(p-1)\cdots(p-k+1)}{k!} \Rightarrow p(p-1)\cdots(p-k+1) = k!\binom{p}{k} \Rightarrow$$

$\Rightarrow p \mid k! \binom{p}{k} \overset{p=\text{πρώτος}}{\Longrightarrow} p \mid k! \text{ ή } p \mid \binom{p}{k}$

Αν $p \mid k! = 1 \cdot 2 \cdot 3 \cdots k \overset{p=\text{πρώτος}}{\Longrightarrow}$

$\Rightarrow \exists \lambda = 1, \ldots, k : p \mid \lambda \Rightarrow p \le \lambda \le k \le p-1$ Άτοπο

Συνεπώς $p \nmid k! \Rightarrow p \mid \binom{p}{k}$

Τότε: $p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k \Rightarrow \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k \equiv 0 \bmod p$

Άρα: $(a+b)^p \equiv a^p + b^p \pmod p$

Έστω $n \ge 1$. Για κάθε $a, b \in \mathbb{Z}$ ορίζουμε πράξεις στο σύνολο $\mathbb{Z}_n$

- $[a]_n + [b]_n = [a+b]_n$: πρόσθεση κλάσεων ισοτιμίας $\bmod n$
- $[a]_n \cdot [b]_n = [a \cdot b]_n$: πολλαπλασιασμός $\bmod n$

↳ Για να είναι "καλά ορισμένες" οι παραπάνω πράξεις θα πρέπει να ισχύουν τα εξής:

- $a \equiv a' \bmod n : [a]_n = [a']_n$
  $b \equiv b' \bmod n : [b]_n = [b']_n$
  $\Rightarrow [a]_n + [b]_n = [a']_n + [b']_n$
  $\Rightarrow [a]_n \cdot [b]_n = [a']_n \cdot [b']_n$

Δηλ: $\begin{cases} [a+b]_n = [a'+b']_n \\ [a \cdot b]_n = [a' \cdot b']_n \end{cases} \Leftrightarrow \begin{cases} a+b \equiv a'+b' \pmod n \\ a \cdot b \equiv a' \cdot b' \pmod n \end{cases}$

$U(Z_n) = \{$αντιστρέψιμες κλάσεις ισοτιμίας mod n$\}$

$U(Z_n) \neq \emptyset$, διότι $[1]_n \in U(Z_n)$

$U(Z_4) = \{[1]_4, [3]_4\}$

- $[2]_4[\alpha]_4 = [1]_4 \Rightarrow [2\alpha]_4 = [1]_4 \Rightarrow 2\alpha \equiv 1 \pmod 4$

$\Rightarrow 4 \mid 2\alpha - 1$, άτοπο διότι: $2\alpha - 1$ περιττός

- $[3]_4[3]_4 = [9]_4 = [1]_4$

↳ Πρόταση: $\forall [\alpha]_n \in Z_n : [\alpha]_n \in U(Z_n) \Leftrightarrow (\alpha, n) = 1$

Απόδειξη: "$\Rightarrow$" Έστω ότι $[\alpha]_n \in U(Z_n) \Rightarrow$

$\Rightarrow \exists\, [b]_n \in Z_n : [\alpha]_n[b]_n = [1]_n \Rightarrow$

$\Rightarrow [\alpha \cdot b]_n = [1]_n \Rightarrow \alpha \cdot b \equiv 1 \pmod n \Rightarrow$

$\Rightarrow n \mid \alpha b - 1 \Rightarrow \exists\, k \in Z : \alpha b - 1 = kn \Rightarrow$

$\Rightarrow \alpha b + (-k)n = 1 \Rightarrow (\alpha, n) = 1$

"$\Leftarrow$" Έστω $(\alpha, n) = 1 \Rightarrow \exists\, b, c \in Z : \alpha b + nc = 1 \Rightarrow$

$\Rightarrow [\alpha b]_n + [nc]_n = [1]_n \Rightarrow [\alpha]_n[b]_n + [n]_n[c]_n = [1]_n \Rightarrow$

$\Rightarrow [\alpha]_n[b]_n = [1]_n \Rightarrow [\alpha]_n \in U(Z_n)$

↳ Πόρισμα: $|U(Z_n)| = \varphi(n)$, φ: συνάρτηση Euler

$$|U(Z_n)| = \left| \{ [\alpha]_n \in Z_n \mid (\alpha, n) = 1 \} \right|$$

• $U(Z_{12}) = \{ [1]_{12}, [5]_{12}, [7]_{12}, [11]_{12} \}$

Παρατήρηση: Έστω p: πρώτος

$U(Z_p) = \{ [1]_p, [2]_p, \dots, [p-1]_p \}$

$|U(Z_p)| = n-1$

• Πόρισμα: Αν $n \geq 1$ τότε: κάθε n-μηδενική κλάση ισοδυναμίας είναι αντιστρέψιμη $\Leftrightarrow n$: πρώτος

Απόδειξη: "$\Leftarrow$" Προκύπτει απ' την Παρατήρηση

"$\Rightarrow$" $\forall [\alpha]_n \in \{ [1]_n, [2]_n, \dots, [n-1]_n \}$

$[\alpha]_n$: αντιστρέψιμη $\Rightarrow (k, \alpha) = 1 \ \forall k = 1, \dots, n-1$

Άρα, n: πρώτος

↳ Παράδειγμα: $[251^{143}]_7 \in U(Z_7)$?

$251 = 35 \cdot 7 + 6 \Rightarrow [251]_7 = [6]_7 \Rightarrow$

$\Rightarrow [251]_7^{143} = [251^{143}]_7 = [6^{143}]_7 \Rightarrow$

$\Rightarrow [251^{143}]_7 = [-1]_7^{143} \Rightarrow [6]_7 \in U(Z_7) \leftrightarrow (6,7) = 1$

Άρα, $[251^{143}]_7 = [6]_7 \in U(Z_7)$

Επειδή $[6]_7[6]_7 = [36]_7 = [1]_7$

Άρα, η αντίστροφη κλάση ισοτιμίας mod 7 της $[6]_7$ είναι η $[6]_7$

Συμβολισμός: Αν $[a]_n \in Z_n$ και $[a]_n[b]_n = [1]_n$

τότε η $[b]_n$ καλείται αντίστροφη κλάση ισοτιμίας mod n της $[a]_n$ και συμβολίζεται με $[a]_n^{-1}$

Πχ: $[6]_7^{-1} = [6]_7$