11/05/15.

# Ισοτιμίες

**Ορισμός**: Έστω $n \geq 1$, και $a, b \in \mathbb{Z}$. Οι $a, b$ καλούνται ισότιμοι mod $n \Leftrightarrow n \mid (a-b)$. Τότε θα γράφουμε $a \equiv b \pmod n$. Έτσι:

$$\boxed{a \equiv b \pmod n \Leftrightarrow n \mid (a-b)} \quad (*)$$

**Παραδείγματα**: $17 \equiv -7 \pmod 8$ και $6 \not\equiv 11 \pmod 3$

- $\forall a \in \mathbb{Z}: a \equiv 0 \pmod n \Leftrightarrow n \mid a$
- $\forall a \in \mathbb{Z}: a \equiv 0 \pmod 2 \Leftrightarrow a$: άρτιος
- $\forall a \in \mathbb{Z}: a \equiv 1 \pmod 2 \Leftrightarrow a$: περιττός
- $\left.\begin{matrix} a \equiv b \pmod m \\ m \mid n \end{matrix}\right\} \Rightarrow \left.\begin{matrix} n \mid (a-b) \\ m \mid n \end{matrix}\right\} \Rightarrow$

$$\Rightarrow m \mid (a-b) \Rightarrow \boxed{a \equiv b \pmod m}$$

**Πρόταση**: Έστω $a, b \in \mathbb{Z}$ και $n \in \mathbb{N}$. Τότε:

$a \equiv b \pmod n \Leftrightarrow$ οι $a, b$ αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το $n$.

δηλ οι $a, b$ είναι ισοϋπόλοιποι mod $n$.

**Απόδειξη**: ($\Leftarrow$) Έστω ότι οι $a, b$ είναι ισοϋπ. mod $n$. $\Rightarrow$

$$\left.\begin{matrix} a = q_1 \cdot n + r \\ b = q_2 \cdot n + r \end{matrix}\right| \text{ όπου } 0 \leq r < n$$

R

Τότε : $\alpha-b=(q_1-q_2)\cdot n \Rightarrow n \mid (\alpha-b) \Rightarrow \alpha \equiv b \pmod n$

($\Rightarrow$) Έστω ότι $\alpha \equiv b \pmod n \Rightarrow n \mid (\alpha-b) \Rightarrow (\alpha-b)=k\cdot n,\ k\in\mathbb{Z}$.

$\Rightarrow \alpha = b+kn$

$b=q\cdot n+r,\ 0\le r<n$ $\Rightarrow \alpha = q\cdot n+r+n=(k+q)n+r$, $0\le r<n$

Άρα οι $\alpha, b$ είναι ισοϋπόλοιποι mod n.

$\longleftrightarrow$

**Πρόταση:** Η σχέση "$\equiv_n$" ισοτιμίας mod n στο σύνολο $\mathbb{Z}$:

$\alpha \equiv b \pmod n \Leftrightarrow n \mid (\alpha-b)$

είναι μια σχέση ισοδυναμίας.

**Απόδειξη:** ① $\forall \alpha\in\mathbb{Z} : \alpha \equiv \alpha \bmod(n) \Leftrightarrow$

$\Leftrightarrow n \mid \alpha-\alpha=0$ (ισχύει)

② $\forall \alpha, b\in\mathbb{Z} : \alpha \equiv b \pmod n \Rightarrow$

$\Rightarrow n \mid (\alpha-b) \Rightarrow n \mid -(\alpha-b) \Rightarrow$

$\Rightarrow b \equiv \alpha \pmod n$

③ $\forall \alpha, b, c\in\mathbb{Z}$ τ.ώ. $\left.\begin{matrix}\alpha\equiv b \pmod n\\ b\equiv c \pmod n\end{matrix}\right| \Rightarrow$

$\Rightarrow \left.\begin{matrix}n\mid \alpha-b\\ n\mid b-c\end{matrix}\right| \Rightarrow n \mid (\alpha-b)+(b-c) \Rightarrow n \mid \alpha-c \Rightarrow \alpha \equiv c \pmod n$

Άρα η σχέση ισοτιμίας (mod n) είναι σχέση ισοδυναμίας επί του $\mathbb{Z}$.

$\longleftrightarrow$

$X\neq\emptyset,\ R\subseteq X\times X$ :

Το R σχ. ισ. στο X :

$\Leftrightarrow$

- $\forall x\in X : (x,x)\in R \Rightarrow xRx$
- $\forall x,y\in X : (x,y)\in R \Rightarrow (y,x)\in R$
- $\forall x,y,z\in X$ : $\left.\begin{matrix}(x,y)\in R\\ (y,z)\in R\end{matrix}\right| \Rightarrow (x,z)\in R$

⊛ **Πρόταση:** Έστω $n\ge 1$ και $a, b, c\in\mathbb{Z}$, και $f(x)=c_0+c_1x+\dots+c_kx^k,\ \mathbb{Z}[x]=$ {σύνολο των πολυωνύμων με ακέραιους συντελεστές}.

① $\left.\begin{matrix}\alpha\equiv b \pmod n\\ c\equiv d \pmod n\end{matrix}\right\} \Rightarrow \begin{matrix}(\alpha+c)\equiv(b+d) \pmod n\\ \alpha c\equiv bd \pmod n\end{matrix}$

② $\alpha\equiv b \pmod n \Rightarrow (\alpha+c)\equiv(b+c) \pmod n$

③ $\alpha\equiv b \pmod n \Rightarrow \forall k\ge 1 : \alpha^k\equiv b^k \pmod n$

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

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

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

Τότε: $\left.\begin{matrix} a-b = k \cdot n \\ c-d = \lambda \cdot n \end{matrix}\right| \lambda, k \in \mathbb{Z}. \Rightarrow \left.\begin{matrix} a = kn+b \\ c = \lambda \cdot n + d \end{matrix}\right\} \Rightarrow$

$\Rightarrow a \cdot c = b \cdot d + (b \cdot \lambda + kd + k\lambda \cdot n) \cdot n \Rightarrow$

$\Rightarrow n \mid ac - b \cdot d \Rightarrow \boxed{ac \equiv bd \pmod n}$

② $\left.\begin{matrix} c \equiv c \pmod n \\ a \equiv b \pmod n \end{matrix}\right| \Rightarrow \boxed{a+c = b+c \pmod n}$

③ Με αρχή Μαθ. Επαγωγής:

$k=1$ : $a \equiv b \pmod n$ δηλ. $a^1 = b^1 \pmod n$ (ισχύει) $\left.\right\} \overset{①}{\Rightarrow}$

Επαγ. Υποθ: $a^k = b^k \pmod n$

$\Rightarrow a^k \cdot a^1 \equiv b^k \cdot b^1 \pmod n \Rightarrow \boxed{a^{k+1} \equiv b^{k+1} \pmod n}$

④ $a \equiv b \pmod n$, τότε λόγω των ①, ②, ③:

$\left.\begin{matrix} a^m \equiv b^m \pmod n, \forall m \geq 1 \\ c_m a^m = c_m b^m \pmod n, \forall m \geq 1 \end{matrix}\right\} \Rightarrow$

$\Rightarrow c_0 + c_1 a^1 + \ldots + c_k a^k \equiv c_0 + c_1 b^1 + \ldots + c_k b^k \pmod n \Rightarrow$

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

⟷

• $\mathcal{R}$: σχέση ισοδ. στο $X$.

$[x]_{\mathcal{R}} = \{y \in X \mid (y,x) \in \mathcal{R}\} = \{y \in X \mid y \mathcal{R} x\}$

↓

κλάση ισοδυναμίας του $x \in X$

• $[x]_{\mathcal{R}} = [y]_{\mathcal{R}} \Leftrightarrow x \mathcal{R} y$

• $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$ ή $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset$.

Η συλλογή υποσυνόλων $\{[x]_R \subseteq X \mid x \in X\}$ αποτελεί διαμέριση του $X$ και συμβολίζεται με $X/R$ και καλείται το σύνολο-πηλίκο του $X$ ~~προς~~ ως προς τη σχέση $R$.

• Θεωρούμε τη σχέση ισοδυναμίας "$\equiv_n$": $\forall a, b \in \mathbb{Z}$:

$$a \equiv b \pmod n \Leftrightarrow n \mid a-b.$$

$\forall \alpha \in \mathbb{Z}$: $[\alpha]_n = \{x \in \mathbb{Z} \mid x \equiv \alpha \pmod n\} = \{x \in \mathbb{Z} \mid n \mid x-\alpha\} =$

↑ κλάση ισοδ. (mod n) του $\alpha \in \mathbb{Z}$.

$$= \{x \in \mathbb{Z} \mid x - \alpha = k \cdot n, k \in \mathbb{Z}\} =$$

$$= \{x \in \mathbb{Z} \mid x = \alpha + k \cdot n, k \in \mathbb{Z}\} =$$

= όλοι οι ακέραιοι οι οποίοι αφήνουν το ίδιο υπόλοιπο με το $\alpha$, όταν διαιρεθούν με το $n$.

Θεωρούμε το σύνολο πηλίκο: $\mathbb{Z}_n = \{[\alpha]_n \subseteq \mathbb{Z} \mid \alpha \in \mathbb{Z}\}$

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

**Απόδειξη**: Προφανώς: $\{[0]_n, [1]_n, \dots, [n-1]_n\} \subseteq \mathbb{Z}_n$. ①

Έστω $[\alpha]_n \in \mathbb{Z}_n$. Από την ευκλείδεια διαίρεση του $\alpha$ με το $n$: $\alpha = q \cdot n + r$, $0 \le r < n \Rightarrow \alpha - r = q \cdot n \Rightarrow$

$\Rightarrow n \mid \alpha - r \Rightarrow \alpha \equiv r \pmod n \Rightarrow [\alpha]_n = [r]_n$, $0 \le r < n \Rightarrow$

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

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

Από ①, ② $\Rightarrow$

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

**Παράδειγμα**: $\alpha = 13^{23} \cdot 17^{41}$ και $n = 8$. Βρείτε το υπόλοιπο της διαίρεσης του $\alpha$ με το $n$.

• $13 \equiv 5 \pmod 8 \Rightarrow 13^2 \equiv 5^2 \pmod 8 \equiv 25 \pmod 8 \equiv$

$$\equiv 1 \pmod 8$$

Τότε $13^{23} = 13^{2 \cdot 11 + 1} = 13^{2 \cdot 11} \cdot 13^1 = (13^2)^{11} \cdot 13 \equiv$

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

$27 \equiv 3 \pmod 8 \Rightarrow 27^2 = 3^2 \pmod 8 \Rightarrow 27^2 \equiv 1 \pmod 8$

$27^{41} = 27^{2 \cdot 20 + 1} = 27^{2 \cdot 20} \cdot 27^1 = (27^2)^{20} \cdot 27 \equiv 1^{20} \cdot 27 \pmod 8 \equiv$

$\equiv 27 \pmod 8 \equiv 3 \pmod 8$

Άρα $\left.\begin{matrix} 13^{23} = 5 \pmod 8 \\ 27^{41} = 3 \pmod 8 \end{matrix}\right\} \Rightarrow \alpha = 13^{23} \cdot 27^{41} = 3 \cdot 5 \pmod 8 = 7 \pmod 8.$

Άρα $[\alpha]_8 = [7]_8$ κ' το υπόλοιπο της διαίρεσης του $\alpha$ με το 8 είναι 7.

⟷

**Παράδειγμα:** Να βρεθεί το υπ. του $\alpha = 3^{4n+2} + 2 \cdot 4^{3n+1}$, $n \in \mathbb{N}$ με το 17.

**Λύση:** $3^4 = 81 \equiv 13 \pmod{17} \Rightarrow 3^{4n+2} = 3^{4n} \cdot 3^2 =$

$= (3^4)^n \cdot 9 \equiv 13^n \cdot 9 \pmod{17}$ ①

$4^3 = 64 = 13 \pmod{17} \Rightarrow 4^{3n+1} = 4^{3n} \cdot 4 = (4^3)^n \cdot 4 \equiv$

$\equiv 13^n \cdot 4 \pmod{17} \Rightarrow 2 \cdot 4^{3n+1} \equiv 8 \cdot 13^n \pmod{17}$ ②

①, ② $\Rightarrow 3^{4n+2} + 2 \cdot 4^{3n+1} \equiv (9 \cdot 13^n + 8 \cdot 13^n) \pmod{17} \equiv$

$\equiv 17 \cdot 13^n \pmod{17} \equiv 0 \pmod{17} \Rightarrow$

$\Rightarrow \alpha \equiv 0 \pmod{17} \Leftrightarrow 17 \mid \alpha$

⟷

**Παράδειγμα:** $\forall a, b \in \mathbb{Z}$, $p$: πρώτος. Τότε:

$(a+b)^p \equiv a^p + b^p \pmod p$ (*)

$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} \cdot b^p$, όπου $\binom{p}{k} = \frac{p!}{k!(p-k)!}$

$= a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k$. Θ.δ.ο. $\binom{p}{k} \equiv 0 \pmod p$

$1 \le k \le p-1$.

Τότε $p! = \binom{p}{k} k!\,(p-k)!$

$p \mid p! \Rightarrow p \mid \binom{p}{k} k!\,(p-k)!$

Επειδή $k < p : p \nmid k!$

Όμοια $p \nmid (p-k)!$

Άρα επειδή $p$: πρώτος $\Rightarrow \boxed{p \mid \binom{p}{k}}$

Τότε $(a+b)^p = a^p + b^p + \underbrace{\sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k}_{\text{επειδή } \binom{p}{k} \equiv 0 \pmod p} \equiv a^p + b^p \pmod p$