ΙΣΟΤΙΜΙΕΣ

14/12/2015

Έστω $n>1$

ΟΡΙΣΜΟΣ: Αν $a,b\in\mathbb{Z}$, τότε ο a καλείται ισότιμος με τον b $\bmod n = n|a-b$

Τότε θα γράφαμε $a\equiv b \bmod n$. Αν ο a δεν είναι ισότιμος με τον b $\bmod n$, δηλαδή $n\nmid a-b$, τότε θα γράφαμε $a\not\equiv b \bmod n$

$$\boxed{a\equiv b \bmod n \Leftrightarrow n|a-b}$$

ΠΑΡΑΔΕΙΓΜΑ

① $17\equiv -7 \bmod 8$, διότι $8|17-(-7)=24$

② $6\not\equiv 11 \bmod 3$ διότι $3\nmid 6-11=-5$

ΠΑΡΑΔΕΙΓΜΑ

① $\forall a\in\mathbb{Z}: a\equiv a \bmod n$, διότι $n|a-a=0$

② $\forall a\in\mathbb{Z}: a\equiv 0 \bmod 2 \Leftrightarrow 2|a-0=a \Leftrightarrow a$: άρτιος

③ $\forall a\in\mathbb{Z}: a\equiv 1 \bmod 2 \Leftrightarrow 2|a-1 \Leftrightarrow a$: περιττός

④ $\forall a,b\in\mathbb{Z}: a\equiv b \bmod 1$, διότι $1|a-b$

⑤ $\forall a,b\in\mathbb{Z}: \left.\begin{matrix} a\equiv b \bmod n \\ m|n \end{matrix}\right| \Longrightarrow a\equiv b \bmod m$, διότι: $\left.\begin{matrix} n|a-b \\ m|n \end{matrix}\right| \Rightarrow m|a-b \Rightarrow a\equiv b \bmod m$

ΠΡΟΤΑΣΗ

Αν $a,b\in\mathbb{Z}$, τότε: $a\equiv b \bmod n \Leftrightarrow$ οι a,b αφήνουν το ίδιο υπόλοιπο όταν διαιρεθούν με το n.

Απόδειξη

"$\Rightarrow$" Έστω $a\equiv b \bmod n \Rightarrow n|a-b \Rightarrow a-b=k\cdot n$, για κάποιο $k\in\mathbb{Z} \Rightarrow a=b+kn$

Από τον Ευκλείδια Διαίρεση του b με το n: $b=qn+r$, όπου: $0\le r<n$ $\Rightarrow$

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

"$\Leftarrow$" Θα έχουμε: $a = q_1 n + r$, $0 \le r < n$ και $b = q_2 n + r$, $0 \le r < n$.

Τότε $a - b = q_1 n + r - q_2 n - r \Rightarrow$

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

Υπενθύμιση: Έστω X: τυχόν σύνολο. Τότε μια σχέση ισοδυναμίας "$\sim$" στο σύνολο X είναι ένας τρόπος να συσχετίσουμε δύο τυχόντα στοιχεία, $x, y \in X$, γράφοντας $x \sim y$ αν τα x, y σχετίζονται μέσω της $\sim$, έτσι ώστε να ικανοποιούνται τρεις ιδιότητες:

1. $\forall x \in X: x \sim x$ (ανακλαστική ιδιότητα)
2. $\forall x, y \in X: x \sim y \Rightarrow y \sim x$ (συμμετρική ιδιότητα)
3. $\forall x, y, z \in X: \left.\begin{matrix} x \sim y \\ y \sim z \end{matrix}\right| \Rightarrow x \sim z$ (μεταβατική ιδιότητα)

ΠΡΟΤΑΣΗ

Η σχέση ισοτιμίας $\equiv$ ή $\equiv_n$ στο σύνολο $\mathbb{Z}$ των ακεραίων είναι μια σχέση ισοδυναμίας.

Απόδειξη:

1. $\forall a \in \mathbb{Z}: a \equiv a \pmod n$, ισχύει και άρα ισχύει η ανακλαστική ιδιότητα.
2. Έστω $a, b \in \mathbb{Z}$ και έστω ότι $a \equiv b \bmod n \Rightarrow n \mid a - b \Rightarrow n \mid b - a \Rightarrow b \equiv a \bmod n$. Άρα ισχύει η συμμετρική ιδιότητα.
3. Έστω $a, b, c \in \mathbb{Z}$ και υποθέτουμε: $\left.\begin{matrix} a \equiv b \bmod n \\ b \equiv c \bmod n \end{matrix}\right| \Rightarrow \left.\begin{matrix} n \mid a - b \\ n \mid b - c \end{matrix}\right| \Rightarrow n \mid a - b + b - c \Rightarrow$

$\Rightarrow n \mid a - c \Rightarrow a \equiv c \bmod n$. Άρα ισχύει και η μεταβατική ιδιότητα.

Άρα η σχέση ισότητας ισοτιμίας $\bmod n$ είναι μια σχέση ισοδυναμίας στο $\mathbb{Z}$

□

ΒΑΣΙΚΕΣ ΙΔΙΟΤΗΤΕΣ ΤΗΣ ΣΧΕΣΗΣ ΙΣΟΤΙΜΙΑΣ mod n:

Έστω $a,b,c,d \in \mathbb{Z}$ και έστω $f(x)=c_0+c_1x+\dots+c_mx^m$ ένα πολυώνυμο με ακέραιους συντελεστές.

① $\left.\begin{matrix} a\equiv b \bmod n \\ c\equiv d \bmod n \end{matrix}\right\} \Rightarrow \begin{matrix} a+c\equiv b+d \bmod n \\ a\cdot c\equiv bd \bmod n \end{matrix}$

② $a\equiv b \bmod n \Rightarrow \left\{\begin{matrix} a+c\equiv b+c \bmod n \\ a\cdot c\equiv b\cdot c \bmod n \end{matrix}\right.$

③ $a\equiv b \bmod n$, τότε $\forall k\geq 1: a^k\equiv b^k \bmod n$

④ $a\equiv b \bmod n$, τότε: $f(a)\equiv f(b) \bmod n$

Απόδειξη

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

$\boxed{\begin{matrix} a-b=k\cdot n \\ c-d=\lambda n \end{matrix}}$, για κάποιο $k\in\mathbb{Z}$, για κάποιο $\lambda\in\mathbb{Z}$ Τότε: $(a+c)-(b+d)=n(k+\lambda) \Rightarrow n\mid (a+c)-(b+d) \Rightarrow$

$\Rightarrow a+c\equiv (b+d) \bmod n$

$\boxed{\begin{matrix} a=b+kn \\ c=d+\lambda n \end{matrix}} \Rightarrow ac=bd+n(b\lambda+kd+k\lambda n) \Rightarrow n\mid ac-bd \Rightarrow ac\equiv bd \bmod n$

② $a\equiv b \bmod n$, τότε $a+c\equiv b+c \bmod n$, διότι: $\left.\begin{matrix} a\equiv b \bmod n \\ c\equiv c \bmod n \end{matrix}\right| \overset{①}{\Rightarrow} \left\{\begin{matrix} a+c\equiv b+c \bmod n \\ a\cdot c\equiv b\cdot c \bmod n \end{matrix}\right.$

③ Η απόδειξη με την Αρχή Μαθηματικής Επαγωγής

Για $k=1$: $a\equiv b \pmod n$ από την υπόθεση.

Επαγωγική Υπόθεση: $a^k \equiv b^k \bmod n$, $a \equiv b \bmod n$ $\Big| \xrightarrow{①} a^{k+1} \equiv b^{k+1} \bmod n$

Άρα $a^k \equiv b^k \bmod n$, $\forall k \geq 1$

Ⓐ Έστω ότι $a \equiv b \bmod n \xrightarrow{②} a^k \equiv b^k \bmod n$

$\forall k \geq 0$. Επίσης από το ② $\Rightarrow c_i a^i \equiv c_i b^i \bmod n$, $\forall i = 0, 1, \dots, m$

Από το ① $\Rightarrow c_0 + c_1 a^1 + c_2 a^2 + \dots + c_m a^m \equiv c_0 + c_1 b^1 + c_2 b^2 + \dots + c_m b^m \pmod n$

Άρα: $f(a) = f(b) \bmod n$

ΠΡΟΤΑΣΗ: Έστω $a, b, k \in \mathbb{Z}$, όπου $k \neq 0$ και $d = (k, n)$. Τότε:

$ka \equiv kb \bmod n \iff a \equiv b \bmod \left(\frac{n}{d}\right)$

$d = (k, n) \Rightarrow \begin{matrix} d \mid k \\ \text{και} \\ d \mid n \end{matrix} \Rightarrow$

$k = d \cdot k'$, $n = d \cdot n'$ } ⊛, $(k', n') = 1$

Απόδειξη: "$\Rightarrow$" Έστω ότι $ka \equiv kb \bmod n \Rightarrow n \mid ka - kb \Rightarrow$

$\Rightarrow n \mid k(a-b) \xRightarrow{⊛} d \cdot n' \mid d \cdot k'(a-b) \Rightarrow n' \mid k'(a-b)$ } ΛΗΜΜΑ

$(n', k') = 1$ } ΕΥΚΛΕΙΔΗ $\Rightarrow n' \mid a-b \Rightarrow a \equiv b \bmod n' \Rightarrow$

$\Rightarrow a \equiv b \bmod \frac{n}{d}$.

"$\Leftarrow$" Έστω ότι $a \equiv b \bmod \frac{n}{d} \Rightarrow$

$\Rightarrow n \mid d(a-b) \Rightarrow n \mid ak'(a-b) \Rightarrow$

$\Rightarrow n \mid k(a-b) \Rightarrow n \mid ka - kb \Rightarrow ka \equiv kb \pmod n$

ΠΟΡΙΣΜΑ: Αν $a, b, k \in \mathbb{Z}$ και $(k, n) = 1$. Τότε $\boxed{ka \equiv kb \bmod n \iff a \equiv b \bmod n}$

Έστω $a \in \mathbb{Z}$. Από τον Ευκλείδια Διαίρεση του a με το n: $a = qn + r$, όπου $0 \leq r < n$, $a = qn + r \equiv r \bmod n$ διότι: $a - r = q \cdot n \Rightarrow n \mid a - r \Rightarrow$

$\Rightarrow \boxed{a \equiv r \bmod n}$, r: υπόλοιπο της διαίρεσης του a με το n.

$r = 0, 1, 2, \dots, n-1$

ΠΑΡΑΔΕΙΓΜΑ: Έστω $A=13^{23}\cdot 27^{41}$. Να βρεθεί το υπόλοιπο της διαίρεσης του A με το 8. Θέτουμε στο παρακάτω αθέλεια $n=8$

$13=8+5\equiv 5 \bmod 8 \Rightarrow 13^{23}=5^{23} \bmod 8$

$5^2=25=3\cdot 8+1\equiv 1 \bmod 8$. Τότε $5^{23}=5^{2\cdot 11+1}=5^{2\cdot 11}\cdot 5=(5^2)^{11}5\equiv 1^{11}5\equiv 5 \bmod 8\equiv 5 \bmod 8$

Άρα: $\boxed{13^{23}\equiv 5 \bmod 8}$ (1)

$27=3\cdot 8+3\equiv 3 \bmod 8 \Rightarrow 27^{41}\equiv 3^{41} \bmod 8$

$3^2=9=24+1\equiv 1 \bmod 8$. Άρα $3^{41}=3^{2\cdot 20+1}=(3^2)^{20}\cdot 3\equiv 1^{20}\cdot 3 \bmod 8\equiv 3 \bmod 8$

Άρα: $\boxed{27^{41}\equiv 3 \bmod 8}$ (2) Από τις (1), (2) $\Rightarrow A=13^{23}\cdot 27^{41}\equiv 5\cdot 3 \bmod 8 \Rightarrow$

$\Rightarrow A=15 \bmod 8\equiv 7 \bmod 8$. Άρα: $A=7 \bmod 8$. Άρα το υπόλοιπο της διαίρεσης του A με το 8 είναι 7.

ΠΑΡΑΔΕΙΓΜΑ: $\forall n\in\mathbb{N}: 17 \mid 3^{4n+2}+2\cdot 4^{3n+1}$ δηλαδή:

$3^{4n+2}+2\cdot 4^{3n+1}\equiv 0 \bmod 17$

$3^4=81\equiv 13 \bmod 17 \Rightarrow 3^{4n}\equiv 13^n \bmod 17$. Άρα $3^{4n+2}\equiv 3^{4n}\cdot 3^2\equiv 13^n\cdot 9 \bmod 17$

$\Rightarrow \boxed{3^{4n+2}\equiv 13^n\cdot 9 \bmod 17}$ (1)

$4^3=64\equiv 13 \bmod 17 \Rightarrow 4^{3n}\equiv 13^n \bmod 17$. Άρα $4^{3n+1}=4^{3n}\cdot 4\equiv 13^n\cdot 4 \bmod 17 \Rightarrow$

$\Rightarrow \boxed{2\cdot 4^{3n+1}\equiv 13^n\cdot 8 \bmod 17}$ (2)

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

$\equiv 0 \bmod 17$

Άρα $3^{4n+2}+2\cdot 4^{3n+1}\equiv 0 \bmod 17 \Rightarrow 17 \mid 3^{4n+2}+2\cdot 4^{3n+1}$