13-12-16

Αν $n \geq 2$, τότε $Z_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$

• Ορισμός: Ένα σύνολο n το πλήθος ακεραίων $x_0, x_1, \dots, x_{n-1}$ καλείται πλήρες σύστημα υπολοίπων mod n $\Leftrightarrow$

$\Leftrightarrow$ Όταν $0 \leq i \neq j \leq n-1$, τότε $x_i \not\equiv x_j \pmod n$

Αν $\{x_0, x_1, \dots, x_{n-1}\}$: π.σ.υ mod n, τότε : $Z_n = \{[x_0]_n, [x_1], \dots, [x_{n-1}]_{n-1}\}$

Επειδή $x_i \not\equiv x_j \pmod n \Rightarrow$ οι κλάσεις υπολοίπων mod n $[x_0]_n, [x_1]_n, \dots, [x_{n-1}]_n$, είναι ανά δύο διαφορετικές

Επειδή απ' την Ευκλείδεια Διαίρεση $[x_i]_n = [r_i]$ όπου r_i : υπόλοιπο της διαίρεσης του x_i με το n και κάθε r_i είναι ένα απ' τα $0, 1, \dots, n-1$, έπεται ότι

$Z_n = \{[x_0]_n, [x_1], \dots, [x_{n-1}]_{n-1}\}$

→ Παράδειγμα: 1) Το σύνολο $\{1, 2, \dots, n\}$: π.σ.υ mod n

(αν $1 \leq i \neq j \leq n$ $i \equiv j \pmod n \Rightarrow n \mid i-j \Rightarrow n \leq i-j$.

Άτοπο, διότι: $i \neq j$ και $i, j \leq n$)

2) Ομοίως, $\{0, 1, 2, \dots, n-1\}$: π.σ.υ. mod n

Πρόταση: Έστω $X=\{x_0,x_1,\dots,x_{n-1}\}$: π.σ.υ mod n και έστω $a,b\in\mathbb{Z}$ έτσι ώστε $(a,n)=1$

Τότε: $Y=\{ax_0+b, ax_1+b,\dots,ax_{n-1}+b\}$: π.σ.υ mod n

Απόδειξη: Αρκεί ν.δ.ο : $0\le i\neq j\le n-1 \Rightarrow ax_i+b\not\equiv ax_j+b \pmod n$

Αν $ax_i+b\equiv ax_j+b \pmod n \Rightarrow n\mid(ax_i+b)-(ax_j+b) \Rightarrow$

$\Rightarrow n\mid ax_i-ax_j \Rightarrow n\mid a(x_i-x_j) \overset{(a,n)=1}{\Rightarrow} n\mid x_i-x_j \Rightarrow x_i\not\equiv x_j \pmod n$

Άτοπο, διότι $i\neq j$ και X: π.σ.υ mod n

Άρα, Y: π.σ.υ (mod n)

- **Παράδειγμα:** Αν $n=8$ τότε $\{0,1,2,\dots,7\}$ και $\{1,2,\dots,8\}$ $\Big\}$ π.σ.υ (mod 8)

Το σύνολο $X=\{14,24,9,-11,34,68,-21,23\}$ π.σ.υ (mod 8)

- $14\equiv 6 \pmod 8$
- $24\equiv 0 \pmod 8$
- $9\equiv 1 \pmod 8$
- $-11\equiv 5 \pmod 8$
- $34\equiv 2 \pmod 8$
- $6\equiv 4 \pmod 8$
- $-21\equiv 3 \pmod 8$
- $23\equiv 7 \pmod 8$

- **Ορισμός:** Έστω οι $\varphi(n)$ το πλήθος ακέραιοι : $x_1,x_2,\dots,x_{\varphi(n)}$ έτσι ώστε:

α) $1\le i\neq j\le\varphi(n) \Rightarrow x_i\not\equiv x_j \pmod n$

β) $(x_i,n)=1$, $1\le i\le\varphi(n)$. Τότε το σύνολο $X=\{x_1,x_2,\dots,x_{\varphi(n)}\}$ καλείται ανάγλυφο σύστημα υπολοίπων mod n

β) $(n, \alpha x_i) = (n,\alpha)(n,x_i) = 1 \cdot 1 = 1$, διαφορετικά αν $d = (n, \alpha x_i)$

τότε:

$$d > 1 \Rightarrow \exists p = \text{πρώτος } \delta\varepsilon \; p \mid d \Rightarrow \begin{cases} p \mid n \\ p \mid \alpha x_i \end{cases} \xrightarrow{p:\text{πρώτος}} p \mid \alpha \text{ ή } p \mid x_i$$

$$\Rightarrow \begin{cases} \text{είτε } (p \mid n \text{ και } p \mid \alpha) \Rightarrow p \mid (n,\alpha) = 1 \\ \text{είτε } (p \mid \alpha \text{ και } p \mid x_i) \Rightarrow p \mid (\alpha, x_i) = 1 \end{cases} \Big\} \text{Άτοπο. Άρα } \underline{d = 1}$$

• Παράδειγμα: Το σύνολο $X = \{1,3,5,7\}$: α.σ.υ $(\text{mod } 8)$

Έστω $11 \in \mathbb{N}$ και $(11,8) = 1$

Τότε το σύνολο $Y = \{11\cdot 1, 11\cdot 3, 11\cdot 5, 11\cdot 7\} = \{11, 33, 55, 77\}$: α.σ.υ. $(\text{mod } 8)$

→ Θεώρημα Euler ←

Αν $\alpha \in \mathbb{Z} : (\alpha, n) = 1$, τότε $\alpha^{\varphi(n)} \equiv 1 \; (\text{mod } n)$

Απόδειξη: Θεωρούμε α.σ.υ $(\text{mod } n)$: $X = \{x_1, x_2, \dots, x_{\varphi(n)}\}$

Επειδή $(\alpha, n) = 1$, έπεται ότι το $Y = \{\alpha x_1, \alpha x_2, \dots, \alpha x_{\varphi(n)}\}$: α.σ.υ $(\text{mod } n)$

Τότε προφανώς $[x_1]_n [x_2]_n \dots [x_{\varphi(n)}]_n =$

$= [\alpha x_1]_n [\alpha x_2]_n \dots [\alpha x_{\varphi(n)}]_n$

Τότε $U_n = \{[x_1]_n, \dots, [x_{\varphi(n)}]_n\} = \{[\alpha x_1]_n, \dots, [\alpha x_{\varphi(n)}]_n\} \Rightarrow$

$\Rightarrow [x_1 x_2 \dots x_{\varphi(n)}]_n = [\alpha x_1 \alpha x_2 \dots \alpha x_{\varphi(n)}]_n \Rightarrow$

$\Rightarrow [x_1 x_2 \dots x_{\varphi(n)}]_n = [\alpha x_1 \alpha x_2 \dots \alpha x_{\varphi(n)}] \Rightarrow$

$\Rightarrow [x_1 x_2 \dots x_{\varphi(n)}]_n = [\alpha^{\varphi(n)} x_1 x_2 \dots x_{\varphi(n)}] \Rightarrow$

$\Rightarrow x_1 x_2 \dots x_{\varphi(n)} \equiv \alpha^{\varphi(n)} x_1 x_2 \dots x_{\varphi(n)} \pmod n$

Επειδή $X = \{x_1, x_2, \dots, x_{\varphi(n)}\} = \text{α.σ.υ} \pmod n \Rightarrow$

$\Rightarrow \forall i = 1, \dots, \varphi(n) : (x_i, n) = 1, (x_1, x_2, \dots, x_{\varphi(n)}) = 1$ $\Rightarrow$

$\Rightarrow \alpha^{\varphi(n)} \equiv 1 \pmod n$

→ Θεώρημα Fermat ←

Έστω p: πρώτος. Τότε: α) Αν $\alpha \in \mathbb{Z}$ και $p \nmid \alpha$, τότε:

$\alpha^{p-1} \equiv 1 \pmod p$

β) $\forall \alpha \in \mathbb{Z} : \alpha^p \equiv \alpha \pmod p$

Απόδειξη: α) Επειδή $p \nmid \alpha$ και p: πρώτος, τότε $(p, \alpha) = 1$ και τότε απ' το Θεώρημα του Euler:

$\left.\begin{array}{l} \alpha^{\varphi(p)} \equiv 1 \pmod p \\ p \text{: πρώτος} \Rightarrow \varphi(p) = p-1 \end{array}\right\} \Rightarrow \alpha^{p-1} \equiv 1 \pmod p$

β) Αν $p \nmid \alpha \overset{\text{Fermat}}{\Rightarrow} \alpha^{p-1} \equiv 1 \pmod p \Rightarrow \alpha^{p-1}\alpha \equiv 1\cdot\alpha \pmod p \Rightarrow$

$\Rightarrow \alpha^p \equiv \alpha \pmod p$

Αν $p \mid \alpha \Rightarrow \alpha \equiv 0 \bmod p \Rightarrow \alpha^p \equiv 0 \pmod p \Rightarrow \alpha^p \equiv \alpha \pmod p$

• Παράδειγμα: $5^{320} \equiv 1 \pmod{561}$

$561 = 3\cdot 11\cdot 17 \Rightarrow (561,5)=1$ { Θεώρημα Euler: $5^{\varphi(561)} \equiv 1 \pmod{561}$

"n

$5=\alpha$

$\varphi(561) = \varphi(3\cdot 11\cdot 17) = \varphi(3)\varphi(11)\varphi(17) = 2\cdot 10\cdot 16 = 320$. Άρα, $5^{320} \equiv 1 \pmod{561}$

• Να υπολογιστεί το υπόλοιπο της διαίρεσης $= \dfrac{5^{1603}}{561}$

Υπενθύμιση: υπόλοιπο διαιρέσεων α με τον αριθμό n είναι ο αριθμός $b = 0, 1, \ldots, n-1$ $\alpha \equiv b \pmod n$

Επειδή $1603 = 5\cdot 320 + 3$,

έχουμε: $5^{1603} = 5^{320\cdot 5+3} = (5^{320})^5 \cdot 5^3 \equiv 1^5 \cdot 5^3 \pmod{561}$

$\Rightarrow 5^{1603} \equiv 125 \pmod{561}$

• Άσκηση: Να δειχθεί ότι: $10 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}$

Λύση: Θα εφαρμόσουμε Euler ή Fermat

$A = 7\cdot 1968^{1968} - 3\cdot 68^{78}$. Θέλουμε να δ.ο $10 \mid A$

Αρκεί να δ.ο $2 \mid A$

$5 \mid A$

• $1968 = \text{άρτιος} \Rightarrow 7 \cdot 1968^{1968} = \text{άρτιος}$

$68 = \text{άρτιος} \Rightarrow 3 \cdot 68^{78} \Rightarrow$

$\Rightarrow A = \text{άρτιος} \Rightarrow 2 | A$ ①

$n | A \wedge m | A \Rightarrow [n,m] | A$

Ιδιαίτερα, αν $(n,m)=1$ τότε $[n,m] = n \cdot m | A$

• $1968 = 5 \cdot 393 + 3 \Rightarrow 1968 = 3 \pmod 5 \Rightarrow 1968^{1968} \equiv 3^{1968} \pmod 5$

Θεώρημα Fermat: για $\left.\begin{matrix} p=5 \\ \alpha=3 \end{matrix}\right\} \Rightarrow \alpha^{\varphi(5)} \equiv 1 \pmod 5 \Rightarrow$

$\Rightarrow 3^4 \equiv 1 \pmod 5$. Τότε $1968 = 4 \cdot 492$

Άρα: $3^{1968} \equiv 3^{4 \cdot 492} \equiv (3^4)^{492} \equiv 1^{492} \pmod 5$

Συνεπώς, $1968^{1968} \equiv 1 \pmod 5 \Rightarrow 7 \cdot 1968^{1968} \equiv 7 \pmod 5 \equiv 2 \pmod 5$

Παρόμοια, $68^{78} \equiv 4 \pmod 5$

Άρα, $3 \cdot 68^{78} \equiv 12 \pmod 5 \equiv 2 \pmod 5$

$A = 7 \cdot 1968^{1968} - 3 \cdot 68^{78} \equiv (2-2) \pmod 5 \equiv 0 \pmod 5 \Rightarrow 5 | A$ ②

①,② $\xrightarrow{(2,5)=1}$ $2 \cdot 5 = 10 | A$

• Άσκηση: $\forall n \in \mathbb{Z}$: $2730 | n^{13} - n$. $2730 = 2 \cdot 35 \cdot 7 \cdot 13$

Αρκεί νδο: $p | n^{13} - n$, $\forall p = 2,3,5,7,13$

Τότε επειδή οι 2,3,5,7,13 είναι πρώτοι ανά δύο, έχουμε ότι $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730 | n^{13} - n$

• $p=2$: $\begin{cases} n=\text{άρτιος} \Rightarrow n^{13}=\text{άρτιος} \Rightarrow n^{13}-n=\text{άρτιος} \Rightarrow 2 \mid n^{13}-n \\ n=\text{περιττός} \Rightarrow n^{13}=\text{περιττός} \Rightarrow n^{13}-n=\text{άρτιος} \Rightarrow 2 \mid n^{13}-n \end{cases} \Rightarrow$

$\Rightarrow 2 \mid n^{13}-n$

$\rightsquigarrow$ Θεώρημα Fermat : $\forall \alpha \in \mathbb{Z}, \forall p$: πρώτος : $\alpha^p \equiv \alpha \pmod p$

• $p=3$. Τότε $n^{13} \equiv n^{3\cdot 4+1} = (n^3)^4 n \equiv n^4 \cdot n \equiv n^5 \equiv n^3 n^2 \equiv nn^2 \equiv$

$\equiv n^3 \equiv n \pmod 3$

• $p=5 \Rightarrow \dots \Rightarrow n^{13} \equiv n \pmod 5$

• $p=7 \Rightarrow \dots \Rightarrow n^{13} \equiv n \pmod 7$

• $p=13 \Rightarrow \dots \Rightarrow n^{13} \equiv n \pmod{13}$

Απ' τις παραπάνω σχέσεις $\Rightarrow \forall p=2,3,5,7,13 : p \mid n^{13}-n$

Άρα $2730 = 2\cdot 3\cdot 5\cdot 7\cdot 13 \mid n^{13}-n$

$\rightsquigarrow$ Θεώρημα Wilson

Αν $p>1$, τότε p: πρώτος $\Leftrightarrow (p-1)! \equiv -1 \pmod p$

Απόδειξη: "$\Leftarrow$" Έστω ότι: $(p-1)! \equiv -1 \pmod p \Rightarrow p \mid (p-1)!$

Υποθέτουμε ότι p: σύνθετος $\Rightarrow \exists\, d \mid p$ και $1<d<p$

Επειδή $\begin{matrix} d \mid p \\ d<p \end{matrix} \Rightarrow d \le p-1 \Rightarrow d = 1,2,\dots,(p-1)$ και τότε $d \mid (p-1)!$

Επειδή $\left.\begin{matrix} d|p \\ p|(p-1)!+1 \end{matrix}\right\} \Rightarrow d|(p-1)!+1 \left.\begin{matrix} \\ d|(p-1)! \end{matrix}\right\} \Rightarrow d|1 \Rightarrow d=1$: άτοπο διότι $d>1$

Άρα, p: πρώτος

"$\Rightarrow$" Έστω ότι p: πρώτος

→ Αν $p=2$, τότε : $(2-1)! - 1! = 1 \equiv -1 \pmod 2$

Συνεπώς μπορούμε να υποθέσουμε ότι $p \geq 3$

$U_p = \{[1]_p, [2]_p, \dots, [p-1]_p\}$: αντιστρέψιμες κλάσεις ισοτιμίας $(\mathrm{mod}\, p)$

!→ Πρόβλημα: Για ποιες κλάσεις ισοτιμίας $[k]_p, k=1,\dots,p-1$ ισχύει ότι: $[k]_p^{-1} = [k]_p$

Μια τέτοια κλάση είναι η $[1]_p$, διότι
$[1]_p[1]_p = [1]_p \Rightarrow [1]_p^{-1} = [1]_p$

Έστω $2 \leq k \leq p-1$ και υποθέτουμε ότι:

$[k]_p^{-1} = [k]_p \Leftrightarrow [k]_p[k]_p = [1]_p \Rightarrow [k^2]_p = [1]_p \Rightarrow$

$\Rightarrow k^2 \equiv 1 \pmod p \Rightarrow p | k^2 - 1 \Rightarrow p|(k-1)(k+1) \xrightarrow{p=\text{πρώτος}}$

$\Rightarrow p|k-1$ ή $p|k+1$ → Αν $p|k-1 \Rightarrow p \leq k-1 \Rightarrow p+1 \leq k \leq p-1$: Άτοπο

Άρα $p \nmid k-1$

Άρα, αναγκαστικά $p|k+1 \Rightarrow p \leq k+1 \Rightarrow p-1 \leq k \leq p-1 \Rightarrow$

$\Rightarrow k = p-1$

• Συνεπώς, οι μόνες κλάσεις ισοτιμίας $[k]_p$ $[k]_p \cdot [k]_p = [k]_p$ είναι $[1]_p$ και $[p-1]_p$

• Οι κλάσεις ισοτιμίες (mod p) για τις οποίες $[k]_p^{-1} \neq [k]_p$ θα είναι: $[2]_p, \dots, [p-2]_p$

Τότε: $[2]_p \cdots [p-2]_p = [1]_p$, διότι οι κλάσεις ισοτιμίας $[2]_p, \dots, [p-2]_p$ σ' αυτό το γινόμενο εμφανίζονται ως ζεύγη $[k]_p$ και $[k]_p^{-1}$ όπου $[k]_p \neq [k]_p^{-1}$

$[1]_p, [2]_p, \dots, [p-2]_p = [1]_p \Rightarrow [1 \cdot 2 \cdots (p-2)]_p = [1]_p \Rightarrow$

$\Rightarrow 1 \cdot 2 \cdot 3 \cdots p-2 \equiv 1 \pmod p \Rightarrow$

$\Rightarrow (p-2)! \equiv 1 \pmod p \Rightarrow (p-2)!(p-1) \equiv (p-1) \pmod p \Rightarrow$

$\Rightarrow (p-1)! \equiv -1 \pmod p$