Θεωρία Αριθμών

14/05/15

- $\forall n \geq 1 : \forall a, b \in \mathbb{Z} : a \equiv b \pmod n \Leftrightarrow n \mid a-b$. Τότε " $\equiv_n$ " είναι σχ. ισοδ. στο $\mathbb{Z}$.
- $\forall a \in \mathbb{Z} : [a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod n\} = \{x \in \mathbb{Z} \mid n \mid x-a\} =$
$= \{x \in \mathbb{Z} \mid x = a + kn, k \in \mathbb{N}\} = \{a + kn \mid k \in \mathbb{Z}\}$.
- $\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$.

Πράξεις επί κλάσεων ισοτιμίας

- Πρόσθεση: $\forall [a]_n, [b]_n \in \mathbb{Z} : [a]_n + [b]_n \underset{\text{ορ.}}{=} [a+b]_n$
- Πολλαπλ/μός : -//- : $[a]_n \cdot [b]_n \underset{\text{ορ.}}{=} [a \cdot b]_n$

Οι παραπάνω πράξεις είναι καλά ορισμένες δηλαδή ανεξάρτητες των a, b:

Αν $[a]_n = [a']_n$, $[b]_n = [b']_n$, τότε: $[a+b]_n = [a'+b']_n$, $[a \cdot b]_n = [a \cdot b]_n$

Πράγματι: $\left.\begin{matrix} a \equiv a' \pmod n \\ b \equiv b' \pmod n \end{matrix}\right\} \Rightarrow$ $a+b \equiv (a'+b') \pmod n \Rightarrow [a+b]_n = [a'+b']_n$
$a \cdot b \equiv a' \cdot b' \pmod n \Rightarrow [a \cdot b]_n = [a' \cdot b']_n$.

Πρόταση: Το σύνολο $\mathbb{Z}_n$, εφοδιασμένο με τις πράξεις $+, \cdot$, ικανοποιεί τις ακόλουθες ιδιότητες: $\forall x, y, z \in \mathbb{Z}_n$:

1. $x + (y+z) = (x+y) + z$
2. $x + y = y + x$
3. $x + [0]_n = x$
4. $[x]_n + [-x]_n = [0]_n$
5. $x(y \cdot z) = (xy) \cdot z$
6. $x \cdot y = y \cdot x$
7. $\begin{cases} x(y+z) = xy + xz \\ (x+y) \cdot z = xz + y \cdot z \end{cases}$
8. $[x]_n \cdot [1]_n = [x]_n$.

Ένα σύνολο το οποίο είναι εφοδιασμένο με δύο πράξεις οι οποίες ικανοποιούν τις 1–8 καλείται: Μεταθετικός δακτύλιος με μονάδα

Παράδειγμα: Αν $n = 6$ και $[2]_6 \in \mathbb{Z}_6$:
Ζητάμε $[a]_6 \in \mathbb{Z}_6 : [2]_6 [a]_6 = [1]_6$ διότι θα έπρεπε $[2]_6 [3]_6 \neq [0]_6$ διότι θα έπρεπε
$\Rightarrow [2a]_6 = [1]_6 \Rightarrow$ $6 \mid (2-0) = 2$ Άτοπο
$\Rightarrow 6 \mid 2a - 1 \Rightarrow 2a + 6k = 1 \Rightarrow$
$\Rightarrow 2(a+3k) = 1$ Άτοπο $[2]_6 \cdot [3]_6 = [2 \cdot 3]_6 = [6]_6 = [0]_6 \rightarrow$

$[2]_6, [3]_6 \neq [0]_6$ κ' $[2]_6 \cdot [3]_6 = [0]_6$.

Ορισμός: Μια κλάση ισοτιμίας $[\alpha]_n \in \mathbb{Z}_n$ καλείται αντιστρέψιμη $\Leftrightarrow \exists\, [b]_n \in \mathbb{Z}_n : [\alpha]_n \cdot [b]_n = [1]_n \; (= [b]_n \cdot [\alpha]_n)$

$U(\mathbb{Z}_n) = \{ [\alpha]_n \in \mathbb{Z}_n \mid [\alpha]_n : \text{αντιστρ. κλάση ισοτιμίας} \}$

Πρόταση: ① $[\alpha]_n \in U(\mathbb{Z}_n) \Leftrightarrow (\alpha, n) = 1$

② $|U(\mathbb{Z}_n)| = \varphi(n)$

Απόδειξη: $[\alpha]_n \in \mathbb{Z}_n$, τότε: $[\alpha]_n \in U(\mathbb{Z}_n) \Leftrightarrow \exists\, [b]_n \in \mathbb{Z}_n$:

$: [\alpha]_n \cdot [b]_n = [1]_n \Leftrightarrow \exists\, b \in \mathbb{Z} : [\alpha \cdot b]_n = [1]_n \Leftrightarrow$

$\Leftrightarrow \exists\, b \in \mathbb{Z} : n \mid 1 - \alpha \cdot b \Leftrightarrow \exists\, b \in \mathbb{Z} : 1 = \alpha \cdot b + \kappa n$ (για κάποιο $\kappa \in \mathbb{Z}$)

Άρα $[\alpha]_n \in U(\mathbb{Z}_n) \Leftrightarrow \exists\, b \in \mathbb{Z} : 1 = \alpha \cdot b + \kappa \cdot n$, $\kappa \in \mathbb{Z} \Rightarrow$

$\Leftarrow \boxed{(\alpha, n) = 1}$

② $U(\mathbb{Z}_n) = \{ [\alpha]_n \in \mathbb{Z}_n \mid (\alpha, n) = 1 \} \Rightarrow \boxed{|U(\mathbb{Z}_n)| = \varphi(n)}$

Ορισμός 1: Έστω $[\alpha]_n \in U(\mathbb{Z}_n)$. Τότε $[\alpha]_n \cdot [b]_n = [1]_n$ για κάποια κλάση $[b]_n$ και τότε:

$[b]_n = [\alpha]_n^{-1}$: αντίστροφη κλάση ισοτιμίας του α.

Παράδειγμα: ① $\mathbb{Z}_4 \rightsquigarrow U(\mathbb{Z}_4) = \{ [1]_4, [3]_4 \}$

$[1]_4^{-1} = [1]_4$

$[3]_4^{-1} = [3]_4$

② $U(\mathbb{Z}_{10}) = \{ [1]_{10}, [3]_{10}, [7]_{10}, [9]_{10} \}$

$[7]_{10}^{-1} \cdot [7]_{10} = [1]_{10}$ // $[3]_{10} \cdot [7]_{10} = [21]_{10} = [1]_{10} \Rightarrow$

$\Rightarrow \boxed{[3]_{10} = [7]_{10}^{-1}}$

Παρατήρηση: Έστω $[\alpha]_n \in U(\mathbb{Z}_n)$. Τότε: $(\alpha, n) = 1 \Rightarrow \exists k, \lambda \in \mathbb{Z}: \alpha k + \lambda n = 1$.
Τότε $[\alpha k + \lambda n]_n = [1]_n \Rightarrow [1]_n = [\alpha]_n [k]_n + [\lambda]_n [n]_n \to [0]_n \Rightarrow$
$\Rightarrow [\alpha]_n [k]_n = [1]_n \Rightarrow \boxed{[\alpha]_n^{-1} = [k]_n}$

Παράδειγμα: $[88]_{49} \in U(\mathbb{Z}_n)$, διότι $(88, 49) = 1$
($88 = 2^3 \cdot 11$, $49 = 7^2$)
$[88]_{49}^{-1} = ?$ Από την ευκλείδεια διαίρεση $\Rightarrow$
$\Rightarrow \underset{k}{(-5)} \cdot \underset{\alpha}{88} + \underset{\lambda}{9} \cdot \underset{n}{49} = 1 \Rightarrow [88]_{49}^{-1} = [-5]_{49} = [44]_{49}$
(διότι $49 / 44 - (-5) = 49$)

Συνήθεια Υπολοίπων modn ⟷ (π.6.υ)

Έστω $n \geq 1$.
Ορισμός: Ένα σύνολο ακεραίων $X = \{x_1, x_2, \dots, x_n\}$ καλείται πλήρες σύστημα υπολοίπων modn $(\Leftrightarrow) \forall i, j = 1, \dots, n$:
$i \neq j \Rightarrow x_i \not\equiv x_j \pmod n$ $(\Leftrightarrow)$
$(\Leftrightarrow)$ $x_i \equiv x_j \pmod n \Rightarrow \boxed{i = j}$
Τότε οι κλάσεις ισοτιμίας modn: $[x_1]_n, [x_2]_n, \dots, [x_n]_n$ είναι ανά 2 διαφορετικές. $\Rightarrow \mathbb{Z}_n = \{[x_1]_n, [x_2]_n, \dots, [x_n]_n\}$

Παράδειγμα: ① Το σύνολο $X = \{0, 1, \dots, n-1\}$ είναι π.6.υ. modn
② Το σύνολο $X = \{1, 2, \dots, n\}$ π.6.υ. modn.
③ Έστω $X = \{1^2, 2^2, \dots, (n-1)^2, n^2\}$
Τότε $(n-1)^2 = n^2 - 2n + 1$, $(n-1)^2 \equiv 1 \pmod n$ διότι
$n \mid (n-1)^2 - 1 = n^2 - 2n$ που ισχύει

Πρόταση: Αν $X = \{x_0, x_1, \dots, x_{n-1}\}$ π.6.υ. (modn) και $(\alpha, n) = 1$. Τότε το $Y = \{\alpha x_0 + b, \dots, \alpha x_{n-1} + b\}$ π.6.υ. modn και: $\alpha, b \in \mathbb{Z}$

Απόδειξη: Έστω $i, j = 0, \dots, n-1$ και $i \neq j$. Αν $\alpha x_i + b \equiv (x_j \cdot \alpha + b) \pmod n$
$\Rightarrow n \mid (\alpha x_i + b) - (\alpha x_j + b) \Rightarrow n \mid \alpha(x_i - x_j) \Rightarrow$
$\underset{(\alpha, n) = 1}{\Rightarrow} n \mid x_i - x_j \Rightarrow x_i \equiv x_j \pmod n$ ΑΤΟΠΟ διότι $i \neq j$
και X π.6.υ. modn

Ορισμός: Ένα σύνολο ακεραίων $X=\{x_1,\dots,x_{\varphi(n)}\}$ καλείται ανηγμένο (α.σ.υ.) σύστημα υπολοίπων mod n $\Leftrightarrow$

$\Leftrightarrow \forall\, 1\le i,j\le \varphi(n),\ i\ne j : x_i \not\equiv x_j \pmod n$

ΚΑΙ

$(x_i,n)=1,\ i=1,\dots,\varphi(n).$

$X=\{x_1,\dots,x_n\}$ π.σ.υ. (mod n) τότε $\mathbb{Z}_n=\{[x_1],\dots,[x_n]_n\}$

$X=\{x_1,\dots,x_{\varphi(n)}\}$ α.σ.υ. (mod n) $\Rightarrow U(\mathbb{Z}_n)=\{[x_1]_n,\dots,[x_{\varphi(n)}]_n\}$

Πρόταση: Έστω $X=\{x_1,\dots,x_{\varphi(n)}\}$: α.σ.υ. (mod n) κ' $(\alpha,n)=1$.
Τότε το $Y=\{\alpha x_1,\dots,\alpha x_{\varphi(n)}\}$: α.σ.υ. (mod n)

Απόδειξη: Έστω ότι $1\le i\ne j\le \varphi(n)$ κ' $\alpha x_i\equiv \alpha x_j \pmod n \Rightarrow$
$\Rightarrow n\mid \alpha x_i-\alpha x_j \Rightarrow n\mid \alpha(x_i-x_j)$, $(\alpha,n)=1$ $\Rightarrow n\mid x_i-x_j \Rightarrow$
$\Rightarrow x_i\equiv x_j \pmod n$

ΑΤΟΠΟ διότι $i\ne j$ κ' X: α.σ.υ.

Ο.δ.ο. $(\alpha x_i,n)=1,\ \forall i=1,\dots,\varphi(n)$. Έστω $d=(\alpha x_i,n)>1 \Rightarrow$
$\Rightarrow \exists p$: πρώτος : $p/d \Rightarrow p$: πρώτος $\Rightarrow p/\alpha$ ή p/x_i κ' p/n $\Rightarrow$
$\Rightarrow p/\alpha$ κ' p/n ή p/x_i κ' p/n $\Rightarrow$ άτοπο, διότι $(\alpha,n)=1$ κ' X: α.σ.υ. (mod n).

(*) ΘΕΩΡΗΜΑ (Euler): Έστω $(\alpha, n)=1$. Τότε:

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

Απόδειξη: Θεωρούμε ένα σ.κ.υ.$(\bmod n)$ $X=\{x_1, \dots, x_{\varphi(n)}\}$

Τότε το σύνολο $Y=\{\alpha x_1, \dots, \alpha x_{\varphi(n)}\}$: σ.κ.υ. $(\bmod n)$ (διότι $(\alpha, n)=1$)

Τότε: $U(\mathbb{Z}_n)=\{[x_1]_n, \dots, [x_{\varphi(n)}]_n\}=\{[\alpha x_1]_n, \dots, [\alpha x_{\varphi(n)}]_n\} \Rightarrow$

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

$\Rightarrow [x_1 \cdots x_{\varphi(n)}]_n = [\alpha x_1 \cdots \alpha x_{\varphi(n)}]_n = [\alpha^{\varphi(n)}]_n \cdot [x_1 \cdots x_{\varphi(n)}]_n$ (1)

* X: σ.κ.υ.$(\bmod n) \Rightarrow (x_i, n)=1$, $1 \le i \le \varphi(n) \Rightarrow$

$\Rightarrow (x_1 \cdots x_{\varphi(n)}, n)=1 \Rightarrow [x_1, \dots, x_{\varphi(n)}]_n \in U(\mathbb{Z}_n) \Rightarrow$

$\Rightarrow [x_1 \cdots x_{\varphi(n)}]_n^{-1} [x_1 \cdots x_{\varphi(n)}]_n = [\alpha^{\varphi(n)}]_n [x_1 \cdots x_{\varphi(n)}]_n [x_1 \cdots x_{\varphi(n)}]^{-1}$

$\Rightarrow [1]_n = [\alpha^{\varphi(n)}]_n \Rightarrow \boxed{\alpha^{\varphi(n)} \equiv 1 \pmod n}$

(*) ΘΕΩΡΗΜΑ (Fermat): Αν p: πρώτος κ' $p \nmid \alpha$, τότε:

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

Απόδειξη: p: πρώτος, $p \nmid \alpha \Rightarrow (p, \alpha)=1 \underset{\text{Euler}}{\overset{\Theta.}{\Longrightarrow}} \alpha^{\varphi(p)} \equiv 1 \pmod p \Rightarrow$

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

Πόρισμα: Αν p: πρώτος, τότε $\alpha^p \equiv \alpha \pmod p$

Απόδειξη: (1) Αν $p \nmid \alpha$ τότε από Θ. Fermat $\Rightarrow \alpha^{p-1} \equiv 1 \pmod p \Rightarrow$

$\Rightarrow \boxed{\alpha^p \equiv \alpha \pmod p}$

(2) Αν $p \mid \alpha$ τότε $p \equiv 0 \pmod p \Rightarrow \alpha^p \equiv 0 \pmod p \equiv \alpha \pmod p$

Εφαρμογή: $\alpha, n \in \mathbb{Z}$, $n \ge 1$ } Αν $[\alpha]_n = [r]_n$ όπου $0 \le r \le n-1$ τότε $r \equiv$ υπόλοιπο της διαίρεσης του α με το n.

Παραδείγματα ① Υπολ. διαίρεσης του 5^{320} διά του 561

Θα προσδιορίσουμε την κλάση $[5^{320}]_{561}$, $n=561$, $a=5$

$561 = 3\cdot 11\cdot 17$ επίσης $(561,5)=1$. Θ. Euler $\Rightarrow$

$\Rightarrow 5^{\varphi(561)} \equiv 1 \pmod{561}$

$\varphi(561) = \varphi(3\cdot 11\cdot 17) = 3\cdot 11\cdot 17\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{17}\right) = 320 \Rightarrow$

$\Rightarrow 5^{320} \equiv 1 \pmod{561}$ $\Rightarrow$ υπόλοιπο είναι το 1.

Αντίστοιχα 5^{320} αν έχω 5^{1603}.

* $1603 = 5\cdot 320 + 3$. Επειδή $5^{320} \equiv 1 \pmod{561}$

Άρα $5^{1603} \equiv 5^{320\cdot 5+3} \equiv (5^{320})^5 \cdot 5^3 \equiv 1\cdot 5^3 \equiv 125 \pmod{561}$

② Υπόλοιπο διαίρεσης $10^{6k+4}/7$, $\forall k \geq 1$.

$n=7$, $a=10$ Αφού $(7,10)=1$ Από Θ. Euler $\Rightarrow$

$\Rightarrow 10^{\varphi(7)} \equiv 1 \pmod 7 \Rightarrow 10^6 \equiv 1 \pmod 7 \Rightarrow$

$\Rightarrow 10^{6k} \equiv 1^k \pmod 7 \Rightarrow 10^{6k} \equiv 1 \pmod 7 \Rightarrow$ ($\varphi(7)=6$)

$\Rightarrow 10^{6k}\cdot 10^4 = 10^4 \pmod 7 \Rightarrow 10^{6k+4} \equiv 3^4 \pmod 7 \equiv$

$\equiv 3^2\cdot 3^2 \pmod 7 \equiv 9\cdot 9 \pmod 7 \equiv 2\cdot 2 \pmod 7 \equiv$

$\equiv 4 \pmod 7$ $\Rightarrow$ το υπόλ. είναι 4.

Θεώρημα Wilson ⋆ : Αν $P \in \mathbb{Z}$ $(P>1)$ τότε:

P: πρώτος $\Leftrightarrow (P-1)! \equiv -1 \pmod P$ (⋆)

$\Leftrightarrow P \mid (P-1)! + 1$.

Απόδειξη: ($\Leftarrow$) Έστω $(P-1)! \equiv -1 \pmod P$ Άρα $P \mid (P-1)! + 1$. ①

Έστω ότι P δεν είναι πρώτος. $\Rightarrow P = d\cdot d'$ (όπου $1 < d < P$) $\Rightarrow$

$\Rightarrow d \leq P-1 \Rightarrow d \mid (P-1)!$

$d \mid P$

$d \mid (P-1)! + 1$

$\Rightarrow d \mid (P-1)!$

$d \mid (P-1)! + 1$

$\Rightarrow d \mid 1 \Rightarrow d = 1$ Άτοπο

Άρα P: πρώτος

($\Rightarrow$) (1) Если $p=2$. Тогда $(p-1)! = (2-1)! = 1! \equiv 1$
$-1 \equiv 1 \pmod 2$ $\Rightarrow$ [illegible]

$\Rightarrow$ $\boxed{(p-1)! \equiv -1 \pmod p}$ $p=2$