19/12/2015 Θ.Α.

ΘΕΩΡΗΜΑΤΑ EULER-FERMAT-WILSON

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

Ορισμός: Ένα σύνολο n το πλήθος ακεραίων $x_0, x_1, \dots, x_{n-1}$ καλείται πλήρες σύστημα υπολοίπων modn (π.σ.υ) modn $\overset{\text{ορ}}{\Leftrightarrow}$ $0 \leq i \neq j \leq n-1$, τότε $x_i \not\equiv x_j \pmod n$

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

Επειδή $x_i \not\equiv x_j \pmod n \Rightarrow$ οι κλάσεις υπολοίπων modn: $[x_0]_n, [x_1]_n, \dots [x_{n-1}]_n$ είναι όλες διαφορετικές $0 \leq i \neq j \leq n-1$

Επειδή από την Ευκλείδεια Διαίρεση $[x_i]_n = [r_i]$ όπου r_i: υπόλοιπο στη διαίρεση του x_i με το n, $0 \leq i \leq n-1$, και επειδή κάθε r_i είναι ένα από τα $0, 1, \dots, n-1$ έπεται ότι:

Παράδειγμα: ① Το σύνολο $\{1, 2, \dots, n\}$: π.σ.υ modn [αν $1 \leq i \neq j \leq n$ $i \not\equiv j$ modn $\Rightarrow$ $\Rightarrow n \mid i-j \Rightarrow n \leq i-j$ και αυτό είναι άτοπο διότι $i \neq j$ κ' $i, j \leq n$]

② -11- $\{0, 1, 2, \dots, n-1\}$ -11-

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

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

Απόδειξη: Αρκεί να δείξουμε ότι: $0 \leq i \neq j \leq n-1 \Rightarrow ax_i + b \not\equiv ax_j + b \pmod n$.

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

$$\Rightarrow \left.\begin{matrix} n \mid a(x_i - x_j) \\ (a, n) = 1 \end{matrix}\right\} \Rightarrow n \mid x_i - x_j \Rightarrow x_i \not\equiv x_j \pmod n$$

άτοπο διότι $i \neq j$ και το X: π.σ.υ modn

Άρα Y: π.σ.υ (modn)

ΠΑΡΑΔΕΙΓΜΑ

Αν $n=8$ τότε $\{0,1,2,\dots,7\}$ κ' $\{1,2,\dots,8\}$: π.σ.υ (mod 8)

Το σύνολο $X=\{14^{6}, 24^{0}, 9^{1}, -11^{5}, 34^{2}, 68^{4}, -21^{3}, 23^{7}\}$ π.σ.υ (mod 8)

- $14\equiv 6 \pmod 8$
- $24\equiv 0 \pmod 8$
- $9\equiv 1 \pmod 8$
- $-11\equiv 5 \pmod 8$
- $34\equiv 2 \pmod 8$
- $68\equiv 4 \pmod 8$
- $-21\equiv 3 \pmod 8$
- $23\equiv 7 \pmod 8$

Ορισμός Έστω ότι $\varphi(n)$ το πλήθος ακεραίοι: $x_1, x_2, \dots, x_{\varphi(n)}$ 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 σύνολο υπολοίπων mod n

Θεωρούμε το $\mathbb{Z}_n=\{[0]_n, [1]_n, \dots, [n-1]_n\}$. Συμβολίζοντας τους ορισμούς k, $k=1,2,\dots,n-1$, έτσι ώστε $(k,n)=1$, αποκτούμε ένα α.σ.υ (mod n):

$$X=\left\{k\in\mathbb{N} \;\middle|\; \begin{matrix} 1\le k\le n-1 \\ (k,n)=1 \end{matrix}\right\}$$

ΠΑΡΑΔΕΙΓΜΑ: Αν $n=8 \Rightarrow \mathbb{Z}_n=\{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$

Επειδή $\left\{k\in\mathbb{N} \;\middle|\; \begin{matrix} 1\le k\le 7 \\ (k,8)=1 \end{matrix}\right\}=\{1,3,5,7\} \Rightarrow X=\{1,3,5,7\}$: α.σ.υ. (mod 8)

ΠΡΟΤΑΣΗ: Έστω $X=\{x_1, x_2, \dots, x_{\varphi(n)}\}$: α.σ.υ. (mod n) και έστω $a\in\mathbb{Z}$: $(a,n)=1$.

Τότε το σύνολο $Y=\{ax_1, ax_2, \dots, ax_{\varphi(n)}\}$: α.σ.υ (mod n)

Απόδειξη: Αρκεί νδο:

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

(β) $\forall i=1,\dots,\varphi(n)$: $(ax_i, n)=1$

(α) Έστω ότι $ax_i \equiv ax_j \pmod n \Rightarrow n \mid ax_i - ax_j \Rightarrow n \mid a(x_i - x_j)$

Επειδή $(n,a)=1$, θα έχουμε $n \mid x_i - x_j \Rightarrow x_i \equiv x_j \pmod n$: ΑΤΟΠΟ

διότι $i \neq j$ και τα $x_i, x_j \in X$: α.σ.υ $(\bmod n)$

Άρα ισχύει το α.

(β) $(n, ax_i) = (n,a)(n,x_i) = 1 \cdot 1 = 1$. Διαφορετικά αν $d = (n, ax_i)$, τότε:

$d > 1 \Rightarrow \exists p$ πρώτος με $p \mid d \Rightarrow \begin{cases} p \mid n \\ p \mid ax_i \end{cases} \xrightarrow{p \text{ πρώτος}} p \mid a \text{ ή } p \mid x_i \Rightarrow$

$\Rightarrow$ είτε $(p \mid n$ και $p \mid a) \Rightarrow p \mid (n,a) = 1$ ΑΤΟΠΟ

είτε $(p \mid a$ και $p \mid x_i) \Rightarrow p \mid (a, x_i) = 1$ ΑΤΟΠΟ

Άρα $d = 1$.

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

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 $(\bmod 8)$

ΘΕΩΡΗΜΑ EULER:

Αν $a \in \mathbb{Z}$: $(a,n)=1$, τότε: $\boxed{a^{\varphi(n)} \equiv 1 \pmod n}$

Απόδειξη

Θεωρούμε ένα α.σ.υ $(\bmod n)$:

$X = \{x_1, x_2, \ldots, x_{\varphi(n)}\}$. Επειδή $(a,n)=1$,

έπεται ότι το σύνολο $Y = \{ax_1, ax_2, \ldots, ax_{\varphi(n)}\}$ α.σ.υ $(\bmod n)$

$U_n = \{[k]_n \in \mathbb{Z}_n \mid 1 \le k \le n, (k,n)=1\}$

και αν $\{x_1, x_2, \ldots, x_{\varphi(n)}\}$ α.σ.υ $\bmod n$

τότε $= \{[x_1]_n, \ldots, [x_{\varphi(n)}]_n\}$

Τότε προφανώς: $[x_1]_n [x_2]_n \cdots [x_{\varphi(n)}]_n = [ax_1]_n [ax_2]_n \cdots [ax_{\varphi(n)}]_n$

Τότε $U_n = \{[x_1]_n, \ldots, [x_{\varphi(n)}]_n\} = \{[ax_1]_n, \ldots, [ax_{\varphi(n)}]_n\} \Rightarrow$

$\Rightarrow [x_1 \cdot x_2 \cdots x_{\varphi(n)}]_n = [ax_1\, ax_2 \cdots ax_{\varphi(n)}]_n \Rightarrow [x_1 x_2 \cdots x_{\varphi(n)}]_n =$

$= [a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)}]_n \Rightarrow x_1 x_2 \cdots x_{\varphi(n)} \equiv a^{\varphi(n)} x_1 x_2 \cdots x_{\varphi(n)} \pmod n$

Επειδή $X = \{x_1, x_2, \ldots x_{\varphi(n)}\}$: α.σ.υ $(\bmod n) \Rightarrow \forall i = 1, \ldots, \varphi(n)$: $(x_i, n) = 1$ Τότε $(x_1 x_2 \cdots x_{\varphi(n)}, n) = 1$ $\Rightarrow$

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

ΘΕΩΡΗΜΑ FERMAT:

Έστω p: πρώτος. Τότε:

ⓐ Αν $a \in \mathbb{Z}$ και $p \nmid a$, τότε: $a^{p-1} \equiv 1 \pmod p$

ⓑ $\forall a \in \mathbb{Z}$: $a^p \equiv a \pmod p$

Απόδειξη: ⓐ Επειδή $p \nmid a$ και p: πρώτος, τότε: $(p, a) = 1$ και τότε από το Θεώρημα του Euler: $a^{\varphi(p)} \equiv 1 \pmod p$, p: πρώτος $\Rightarrow \varphi(p) = p-1$ $\Big| \Rightarrow a^{p-1} \equiv 1 \pmod p$

ⓑ Αν $p \nmid a \overset{ⓐ}{\Rightarrow} a^{p-1} \equiv 1 \pmod p \Rightarrow$

$a^{p-1} \cdot a \equiv 1 \cdot a \pmod p \Rightarrow a^p \equiv a \pmod p$

Αν $p \mid a \Rightarrow a \equiv 0 \bmod p \Rightarrow a^p \equiv 0 \pmod p \Rightarrow a^p \equiv a \pmod p$ □

ΠΑΡΑΔΕΙΓΜΑ

$5^{320} \equiv 1 \pmod{561}$

$561 = 3 \cdot 11 \cdot 17$ (= n), $5 = a$ $\Big| \Rightarrow (561, 5) = 1$. ΘΕΩΡΗΜΑ Euler $\Rightarrow 5^{\varphi(561)} \equiv 1 \pmod{561}$

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

Να υπολογιστεί το υπόλοιπο της διαίρεσης: $\frac{5^{1603}}{561}$

Υπόλοιπο διαίρεσης a με τον φυσικό n είναι ο φυσικός $b=0,1,\dots,n-1$: $a \equiv b \pmod n$

Επειδή $1603 = 5\cdot 320 + 3$, θα έχουμε: $5^{1603} = 5^{320\cdot 5+3} =$

$$= \left(5^{320}\right)^5 \cdot 5^3 \equiv 1^5 \cdot 5^3 \pmod{561}$$

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

ΑΣΚΗΣΗ: Να δειχθεί ότι:

$$10 \mid 7\cdot 1968^{1968} - 3\cdot 68^{78}$$

Θα εφαρμόσουμε Euler ή Fermat

$A = 7\cdot 1968^{1968} - 3\cdot 68^{78}$. Θέλουμε να δείξουμε ότι $10 \mid A$ Αρκεί νδο

$2 \mid A$ και $5 \mid A$

$n \mid A$ και $m \mid A \Rightarrow [n,m] \mid A$

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

- 1968 : άρτιος $\Rightarrow 7\cdot 1968^{1968}$: άρτιος κ'

  68 : άρτιος $\Rightarrow 3\cdot 68^{78}$ άρτιος $\Rightarrow$

  $\Rightarrow A$: άρτιος $\Rightarrow 2 \mid A$ (1)

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

ΘΕΩΡΗΜΑ FERMAT: για $\begin{matrix} p=5 \\ a=3 \end{matrix} \Big\} \Rightarrow a^{\varphi(5)} \equiv 1 \pmod 5 \Rightarrow 3^4 \equiv 1 \pmod 5$, Τότε:

$1968 = 4\cdot 492$. Άρα:

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

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

Παρατηρώ $68^{78} \equiv 4 \pmod 5$

Άρα $3\cdot 68^{78} \equiv 12 \bmod 5 = 2 \bmod 5$

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

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

ΑΣΚΗΣΗ: $\forall n \in \mathbb{Z}: 2730 \mid n^{13} - n$ | $2730 = 2\cdot 3\cdot 5\cdot 7\cdot 13$

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

Τότε επειδή οι αριθμοί 2, 3, 5, 7, 13 είναι ανά δύο πρώτοι μεταξύ τους

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

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

Άρα $2 \mid n^{13} - n$

ΘΕΩΡΗΜΑ FERMAT: $\forall a \in \mathbb{Z}, \forall p$: πρώτος: $a^p \equiv a \bmod p$

- $p = 3$: Τότε $n^{13} \equiv n^{3\cdot 4+1} = (n^3)^4 n \equiv n^4 n \equiv n^5 \equiv n^3 n^2 \equiv n n^2 = n^3 \equiv n \pmod 3 \Rightarrow$ $\Rightarrow n^{13} \equiv n \pmod 3$
- $p = 13$ Τότε: $n^{13} \equiv n \pmod{13}$ Παρομοίως για $n = 5$ ή $n = 7$: $n^{13} \equiv n \bmod 5$, $n^{13} \equiv n \pmod 7$

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

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

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

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

Υποθέτουμε p: σύνθετος (δηλ. όχι πρώτος) $\Rightarrow$

$\Rightarrow \exists\, d \mid p$ και $1 < d < p$. Επειδή $\begin{matrix} d \mid p \\ d < p \end{matrix} \Longrightarrow d \le p-1 \Rightarrow$

$\Rightarrow d$ είναι κάποιος από τους $1, 2, \ldots, (p-1)$ και τότε $\Rightarrow d \mid (p-1)!$

Επειδή $d|p$, $p|(p-1)!+1$ $\Rightarrow d|(p-1)!+1$, $d|(p-1)! \Rightarrow d|1 \Rightarrow d=1$ άτοπο διότι $d>1$.

Άρα p: πρώτος

"$\Rightarrow$" Έστω ότι p: πρώτος

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

. Άρα μπορούμε να υποθέσουμε ότι $p \geq 3$

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

ΠΡΟΒΛΗΜΑ: Για ποιες κλάσεις ισοτιμίας $[k]_p$, $k=1,2,\dots,p-1$ 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: $[k]_p^{-1} = [k]_p \Leftrightarrow [k]_p \cdot [k]_p = [1]_p \Rightarrow$

$\Rightarrow [k^2]_p = [1]_p \Leftrightarrow k^2 \equiv 1 \pmod p \Leftrightarrow$

$\Leftrightarrow p | k^2 - 1 \Rightarrow p|(k-1)(k+1) \overset{p:\text{πρώτος}}{\Rightarrow}$ $\begin{cases} p|k-1 \\ \text{ή} \\ p|k+1 \end{cases}$

> $[a]_n$: αντιστρέψιμη $\Leftrightarrow$
> $\exists [b]_n : [a]_n [b]_n = [1]_n$
> $\Leftrightarrow [a \cdot b]_n = [1]_n$
> Τότε $[b]_n = [a]_n^{-1}$

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: $p|k+1 \Rightarrow p \leq k+1 \Rightarrow p-1 \leq k \leq p-1 \Rightarrow$

$\Rightarrow k = p-1$

ΑΡΑ: Οι μόνες αντιστρέψιμες κλάσεις ισοτιμίας $[k]_p$: $[k]_p^{-1} = [k]_p$ είναι $[1]_p$ κ' $[p-1]_p$

Οι κλάσεις ισοτιμίας $(\mod p)$ για τις οποίες $[k]_p^{-1} \neq [k]_p$ θα είναι οι $[2]_p, \ldots, [p-2]_p$. Τότε: $\boxed{[2]_p \cdots [p-2]_p \equiv [1]_p}$, διότι οι κλάσεις ισοτιμίας $[2]_p^{-1}, \ldots, [p-2]_p^{-1}$ σε αυτό το γινόμενο εξαφανίζονται ως εξής:

$[k]_p$ και $[k]_p^{-1}$, όταν $[k]_p \neq [k]_p^{-1}$

$$[1]_p \cdot [2]_p \cdot \ldots \cdot [p-2]_p = [1]_p \Rightarrow [1 \cdot 2 \cdot \ldots \cdot (p-2)]_p = [1]_p \Rightarrow$$

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

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

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