

18/05/15

(*) Θεώρημα Wilson (*)

Έστω $p > 1$. τότε:

p : πρώτος $\Leftrightarrow (p-1)! \equiv (-1) \pmod{p}$ (*)

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

Απόδειξη: ($\Leftarrow$) Έστω ότι ισχύει η (*) δηλ $p \mid (p-1)! + 1$ ①
 Έστω ότι p : πρώτος $\Rightarrow \exists d, d' \in \mathbb{N}$, όπου $1 < d, d' < p$
 Τότε $d \mid p \Rightarrow d \mid (p-1)! + 1$

$d < p \Rightarrow d \leq p-1 \Rightarrow d \mid (p-1)!$ } $\Rightarrow d \mid (p-1)! + 1 - (p-1)! \Rightarrow$

Άρα p : πρώτος.

$\Rightarrow d \mid 1$ Απονοδίου ② ($d > 1$)

($\Rightarrow$) Έστω ότι p : πρώτος. Αν $p=2$, τότε $(p-1)! \equiv 1 \pmod{p}$

Αλλά για $p=2 \Rightarrow 2 \mid 1 - (-1) = 2$ (φανερό)

$\forall$ mod. ότι $p \geq 3$. Θα δείξουμε ισχύοντα ότι:

$$[(p-1)!]_p = [-1]_p \text{ δηλαδή:}$$

$$[1 \cdot 2 \cdot \dots \cdot (p-1)]_p = [-1]_p \Leftrightarrow$$

$$\Leftrightarrow [1]_p \cdot [2]_p \cdot \dots \cdot [p-1]_p = [-1]_p$$

Επειδή p : πρώτος, $\forall \alpha = 1, \dots, p-1 : (\alpha, p) = 1 \Rightarrow$

$\Rightarrow$ οι κλάσεις (mod p): $[1]_p, [2]_p, \dots, [p-1]_p$: αλληλοπρώτες.

Άρα $\forall \alpha = 1, \dots, p-1, \exists b = 1, \dots, p-1 : [\alpha]_p \cdot [b]_p = [1]_p$

• Αν $\alpha \neq b$, τότε το άνωτερο $[1]_p [2]_p \cdot \dots \cdot [p-1]_p = [1]_p$
 Θα εμφανιστούν $[\alpha]_p, [b]_p$ με $[\alpha]_p \cdot [b]_p = 1$

• Αν $\alpha = b \Rightarrow [\alpha]_p \cdot [\alpha]_p = [1]_p \Rightarrow [\alpha^2]_p = [1]_p$

Cert $[\alpha^2]_p = [1]_p \Rightarrow \alpha^2 \equiv 1 \pmod{p} \Rightarrow p \mid \alpha^2 - 1 \Rightarrow p \mid (\alpha+1)(\alpha-1) \Rightarrow$
 $\Rightarrow p \mid \alpha-1$ ή $p \mid \alpha+1$.

Av $p \mid \alpha-1 \Rightarrow p \leq \alpha-1$ $\left| \begin{array}{l} \text{κ'} \\ \alpha \leq p-1 \end{array} \right|$ ΑΓΟΡΟ ΣΙΩΝ $p \geq 3$.

Αρα $p \mid \alpha+1 \Rightarrow p \leq \alpha+1 \Rightarrow \alpha \geq p-1$
 Επίσης $\alpha \leq p-1 \Rightarrow \boxed{\alpha = p-1}$

$$[2]_p \cdot [3]_p \cdots [p-2]_p \equiv [1]_p \Rightarrow$$

$$\Rightarrow [1]_p [2]_p \cdots [p-1]_p = [p-1]_p = [-1]_p \Rightarrow$$

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

Φύλλο διαότ

Αγκ ①: Υπολ. της διαίρεσης $\frac{251^{143}}{7}$.

Av $\alpha, n \in \mathbb{N} \Rightarrow$ αν $\alpha \equiv b \pmod{n}$ κ' $0 \leq b \leq n-1$ τότε
 το b είναι το υπόλοιπο της διαίρεσης του α με το n .

Λύση: $251 \equiv b \pmod{7}$. Επίσης $251 = 35 \cdot 7 + 6$. Τότε $251 \equiv 6 \pmod{7} \Rightarrow$
 $\Rightarrow 251^{143} \equiv 6^{143} \pmod{7}$. Όπως $6 \equiv -1 \pmod{7}$

$$\text{Αρα } 251^{143} \equiv (-1)^{143} \pmod{7} \equiv -1 \pmod{7} \equiv 6 \pmod{7}.$$

Αγκ ⑥: Av $n > 1$, τότε n : πρώτος $\Leftrightarrow (n-2)! \equiv 1 \pmod{n}$

Ανδ: ($\Rightarrow$) Έστω ότι n : πρώτος. Τότε από Θ. Wilson:

$$(n-1)! \equiv -1 \pmod{n} \Rightarrow n \mid (n-1)! + 1 \quad (1)$$

$$\text{Cert } (n-1)! + 1 = (n-2)!(n-1) + 1 = (n-2)! \cdot n - (n-2)! + 1 =$$

$$= n \cdot (n-2)! - [(n-2)! - 1]$$

$$\textcircled{1} \Rightarrow \left. \begin{array}{l} n \mid n(n-2)! - [(n-2)! - 1] \\ n \mid n(n-2)! \end{array} \right\} \Rightarrow n \mid (n-2)! - 1 \Rightarrow (n-2)! \equiv 1 \pmod{n}$$

$$\Leftrightarrow \left. \begin{array}{l} \text{Έστω ότι } (n-2)! \equiv 1 \pmod{n} \Rightarrow n \mid (n-2)! - 1 \\ \text{Όπως } n \nmid n(n-2)! \end{array} \right\} \Rightarrow n \mid n(n-2)! - [(n-2)! - 1] =$$

$$= (n-1)! + 1 \Rightarrow$$

$$\Rightarrow (n-1)! \equiv -1 \pmod{n} \quad \text{Θ. Wilson} \Rightarrow n: \text{πρώτος}$$

A6k ⑦: ① $2^{20} \equiv 1 \pmod{41}$

Ans: $2^1 \equiv 2 \pmod{41}$
 $2^2 \equiv 4 \pmod{41}$
 $2^3 \equiv 8 \pmod{41}$

$2^4 \equiv 16 \pmod{41}$

$2^5 \equiv 32 \pmod{41} \equiv -9 \pmod{41} \Rightarrow$

$\Rightarrow (2^5)^2 \equiv (-9)^2 \pmod{41} \Rightarrow$

$\Rightarrow 2^{10} \equiv 81 \pmod{41} \equiv -1 \pmod{41} \Rightarrow$

$\Rightarrow 2^{20} \equiv (-1)^2 \pmod{41} \equiv 1 \pmod{41}$

sol. $\frac{a}{m}$: $[a]_n = [b]_n$, $0 \leq b \leq n-1$
 $a \equiv b \pmod{n}$

② $2^{50} \pmod{7}$

$(2, 7) = 1 \Rightarrow \overset{\text{Euler}}{2^{\phi(7)}} \equiv 1 \pmod{7} \Rightarrow$

$\Rightarrow 2^6 \equiv 1 \pmod{7} \Rightarrow (2^6)^8 \equiv 1^8 \pmod{7} \Rightarrow 2^{48} \equiv 1 \pmod{7} \Rightarrow 2^{50} = 2^{48} \cdot 2^2 \equiv$
 $\equiv 4 \pmod{7}$

③ sol. $\frac{41^{65}}{7}$

Ans:

$41 \equiv 42 - 1 = 6 \cdot 7 - 1 \Rightarrow 41 \equiv (-1) \pmod{7} \Rightarrow$

$\Rightarrow 41^{65} \equiv (-1)^{65} \pmod{7} \equiv -1 \pmod{7} \equiv 6 \pmod{7}$

④ sol. $\frac{\sum_{k=1}^{100} k!}{12} = \frac{1! + 2! + \dots + 100!}{12}$

Ans: $1! + 2! + 3! + 4! + \dots + 100! \equiv (9+0) \pmod{12} \equiv 9 \pmod{12}$
 $9 \pmod{12} \text{ or } 9 \pmod{12}$

A6k ①⑦

Ans:

(a) $3^{999,999,999} \pmod{17}$, (b) $2^{1,000,000} \pmod{17}$

(a) $(3, 17) = 1 \Rightarrow \text{Euler}$

$3^{\phi(17)} \equiv 1 \pmod{17} \Rightarrow$

$999,999,999 = 6 \cdot 166,666,666 + 3$

$\Rightarrow 3^{999,999,999} = 3^{6 \cdot 166,666,666 + 3} = (3^6)^{166,666,666} \cdot 3^3$

$\equiv 1 \cdot 3^3 \pmod{17} \equiv -1 \pmod{17} \equiv 16 \pmod{17}$

(b) $(2, 17) = 1 \Rightarrow \text{Euler}$

$2^{\phi(17)} \equiv 1 \pmod{17} \Rightarrow$

$1,000,000 = 16 \cdot 62,500$

$\Rightarrow 2^{1,000,000} = (2^{16})^{62,500}$

$\equiv 1^{62,500} \pmod{17} \equiv 1 \pmod{17}$

Κάθε αριθμός $n \geq 1$ γράφεται μοναδικά: $\alpha = d_m 10^m + d_{m-1} 10^{m-1} + \dots + d_2 10^2 + d_1 10^1 + d_0$
 Το τελευταίο δεκαδικό ψηφίο των α είναι το α_0 .
 $0 \leq d_i \leq 9, i=1, \dots, m$.

Αν $\alpha \in \mathbb{N}$, τότε τελευταίο δεκαδικό ψηφίο του α είναι ένας αριθμός b : $\alpha \equiv b \pmod{10}, 0 \leq b \leq 9$.

Ασκ. (18): Να βρεθεί το τελευταίο δεκ. ψηφίο των αριθμών:
 (α) 3^{1000} , (β) $7^{999.999}$, (γ) $9^{333.333}$.

Λύση:
 (α) $(3, 10) = 1 \Rightarrow$ Euler $3^{\varphi(10)} \equiv 1 \pmod{10} \Rightarrow 3^4 \equiv 1 \pmod{10} \Rightarrow$
 $\Rightarrow 3^{1000} = 3^{4 \cdot 250} = (3^4)^{250} \equiv 1^{250} \pmod{10} \equiv 1 \pmod{10} \Rightarrow$ τελευταίο ψηφίο είναι το 1.

(β) $7^{999.999} \pmod{10}$

$(7, 10) = 1 \Rightarrow$ Euler $7^{\varphi(10)} \equiv 1 \pmod{10} \Rightarrow 7^4 \equiv 1 \pmod{10}$

$999.999 = 4 \cdot 249999 + 3$ και τότε $7^{999.999} \equiv (7^4)^{249999} \cdot 7^3 \equiv 1^{249999} \cdot 7^3 \equiv 343 \pmod{10} \equiv 3 \pmod{10} \Rightarrow$ τελευταίο ψηφίο $\rightarrow 3$.

Ασκ. (16): (α) Να δειχθεί $11/10! + 1 \equiv 13/12! + 1$, (β) Να βρεθούν τα υπολ. των διαιρετών $\frac{16!}{19} \frac{5! \cdot 25!}{31}$

Λύση (α) Τα 11, 13 είναι πρώτοι

οπότε από Θ. Wilson έχουμε τα γινόμενα.

(β) ① Θα υπολ. των κλειν 16ουφίας $[16!]_{19}$

Θ. Wilson για $p=19$: $18! \equiv (-1) \pmod{19} \Rightarrow$

$\Rightarrow 16! \cdot 17 \cdot 18 \equiv 18 \pmod{19} \Rightarrow 16! \cdot (-2) \cdot (-1) \equiv 2 \cdot 9 \pmod{19} \Rightarrow$

$\Rightarrow 2 \cdot 16! \equiv 2 \cdot 9 \pmod{19} \Rightarrow 19 \mid 2 \cdot 16! - 2 \cdot 9 = 2(16! - 9) \Rightarrow$

$\Rightarrow 19 \mid 16! - 9 \Rightarrow 16! \equiv 9 \pmod{19}$

Υπόλοιπο: 9

$$\begin{aligned}
 & \textcircled{2} \quad \frac{5! 25!}{31}, \quad (5! 31!) \pmod{31} \quad \Bigg| \quad \text{O. Wilson: Ha } p=31: \\
 & \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad \qquad 30! \equiv -1 \pmod{31} \\
 & \quad \underbrace{(5! 25!) \pmod{31}}_{\substack{\uparrow \quad \nwarrow \quad \nearrow \quad \nwarrow \quad \nearrow \\ (-30) \pmod{31} \quad (-29) \pmod{31} \quad (-28) \pmod{31} \quad (-27) \pmod{31} \quad (-26) \pmod{31}}} \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 25! \pmod{31} \equiv \\
 & \equiv (-30)(-29)(-28)(-27)(-26) \cdot 25! \pmod{31} \equiv \\
 & \equiv -30! \pmod{31} \equiv -(-1) \pmod{31} \equiv 1 \pmod{31}.
 \end{aligned}$$

O. Wilson

$A_p \propto$ to unobtaino einu: 1.