

29/05/15 : Έστω $\alpha, n \in \mathbb{Z}, (\alpha, n) = 1, n \geq 1$, $\text{ord}_n(\alpha) = \min \{k \in \mathbb{N} \mid \alpha^k \equiv 1 \pmod{n}\}$

① $\alpha^k \equiv \alpha^l \pmod{n} \Leftrightarrow k \equiv l \pmod{r}, r = \text{ord}_n(\alpha)$.

② $\alpha^k \equiv 1 \pmod{n} \Leftrightarrow r \mid k$.

- α : πρωτ. π/α $\pmod{n} \Leftrightarrow (\alpha, n) = 1$ και $\text{ord}_n(\alpha) = \varphi(n)$.
- $\exists$ πρωτ. π/α $\pmod{n} \Leftrightarrow n = 2, 4, p^m, 2p^m, m \geq 1, p$: άπρ/πρς άπρ/πρς
- Αν $\exists$ πρωτ. π/α $\pmod{n}$ τότε το σύνθετος τότε θα είναι $\varphi(\varphi(n))$ οι αριθμοί
 είναι $\alpha^k, (k, n) = 1, 1 \leq k \leq n$ κ' α : πρωτ. π/α $\pmod{n}$.

Φύλλαδιο #9

Άσκηση ①: $\alpha, n \in \mathbb{Z}, n \geq 1$, Τότε ο θετ. ακέραιος x είναι άνω
 με 1602105 $\alpha^x \equiv 1 \pmod{n} \Leftrightarrow \text{ord}_n(\alpha) \mid x$.

Εφαρμογή: Να βρεθούν οι x , ώστε $2^x \equiv 1 \pmod{7}$

Άντι: $(\Rightarrow)$ Έστω $x \in \mathbb{N}$ είναι άνω με $\alpha^x \equiv 1 \pmod{n} \Rightarrow$
 $\Rightarrow n \mid \alpha^x - 1$. Αν $d = (\alpha, n) \neq 1$ κ' $d \mid n$
 $\Rightarrow d \mid \alpha^x \Rightarrow d \mid \alpha^x - \alpha^x + 1 \Rightarrow d \mid 1 \Rightarrow d = 1$. Άρα $(\alpha, n) = 1 \Rightarrow$
 $\Rightarrow \text{ord}_n(\alpha)$. Τότε $(\alpha^k \equiv 1 \pmod{n}) \Leftrightarrow \text{ord}_n(\alpha) \mid k \Rightarrow$
 $\Rightarrow \text{ord}_n(\alpha) \mid x$.

$(\Leftarrow)$ Αν $\text{ord}_n(\alpha) \mid x \Rightarrow x = k \cdot r, r = \text{ord}_n(\alpha)$. Τότε $\alpha^x = \alpha^{k \cdot r} \Rightarrow$
 $\Rightarrow \alpha^x = (\alpha^r)^k \equiv 1^k \pmod{n} \equiv 1 \pmod{n}$.

Εφαρμογή: Αν x : άνω με $2^x \equiv 1 \pmod{7} \Rightarrow \boxed{\text{ord}_7(2) \mid x} \text{ ①}$
 $2^1 \equiv 2 \pmod{7} \neq 1 \pmod{7}$
 $2^2 \equiv 4 \pmod{7}$
 $2^3 \equiv 8 \equiv 1 \pmod{7} \Rightarrow \boxed{\text{ord}_7(2) = 3} \text{ ②}$

$\Rightarrow 3 \mid x \Rightarrow x = 3k, k \geq 1$.

Αντίστροφα $2^{3k} \equiv 1 \pmod{7}, \forall k \geq 1$.

Άσκηση ④: Αν $\alpha = 3, 5, 7, 9$ να βρεθεί η τάξη $\text{ord}_{16}(\alpha)$

$$\begin{aligned} \varphi(p^a) &= \\ &= p^a - p^{a-1} \end{aligned}$$

Άντι $(3, 16) = (5, 16) = (7, 16) = (9, 16) = 1 \Rightarrow \text{ord}_{16}(\alpha)$, για $\alpha = 3, 5, 7, 9$.
 $\left. \begin{array}{l} \text{ord}_n(\alpha) \mid \varphi(n) \\ (\alpha, n) = 1 \end{array} \right\} \Rightarrow \text{Άρα } \text{ord}_{16}(\alpha) \mid \varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 16 - 8 = 8 \Rightarrow$
 $\Rightarrow \text{ord}_{16}(\alpha) = 1, 2, 4, 8$.

$\boxed{\alpha = 3}$ $3^1 = 3 \not\equiv 1 \pmod{16}$
 $3^2 = 9 \not\equiv 1 \pmod{16}$
 $3^4 \equiv 1 \pmod{16} \Rightarrow \boxed{\text{ord}_{16}(3) = 4}$

$\boxed{\alpha = 5}$:
 $5^1 \not\equiv 1 \pmod{16}$
 $5^2 = 25 \equiv 9 \pmod{16}$
 $5^4 \equiv 1 \pmod{16} \Rightarrow \boxed{\text{ord}_{16}(5) = 4}$

$$\bullet \boxed{x=7}$$

$$7^1 \not\equiv 1 \pmod{16}$$

$$7^2 = 49 \equiv 1 \pmod{16}$$

$$\boxed{\text{ord}_{16}(7) = 2}$$

$$\bullet \boxed{x=9}$$

$$9^1 = 9 \not\equiv 1 \pmod{16}$$

$$9^2 = 81 \equiv 1 \pmod{16}$$

$$\boxed{\text{ord}_{16}(9) = 2}$$

Άσκηση 7: $\alpha, n \in \mathbb{N}$, τότε: $\text{ord}_{\alpha^n-1}(\alpha) = n$ κ' $n/\varphi(\alpha^n-1)$

Way: Είναι: $(\alpha, \alpha^n-1) = 1$, διότι αν $d = (\alpha, \alpha^n-1)$, τότε $d \mid \alpha$ και $d \mid \alpha^n-1 \Rightarrow d \mid 1 \Rightarrow \boxed{d=1}$.

Ενady $\alpha^n \equiv 1 \pmod{\alpha^n-1}$ τότε θα έχουμε ότι: αν $k < n$ και $\alpha^k \equiv 1 \pmod{\alpha^n-1}$, τότε: $\alpha^n-1 \mid \alpha^k-1 \Rightarrow \alpha^n \leq \alpha^k-1$ ΑΤΟΝΟ διότι $k < n$.

$$\text{Άρα } \boxed{\text{ord}_{\alpha^n-1}(\alpha) = n}$$

και τότε $n \mid \varphi(\alpha^n-1)$

Άσκηση 8: ① Να βρεθούν πρωταρχικές ρίζες mod n , $n=4, 5, 10, 13, 14, 18, 20$

Πρωτ. ρίζα mod n : Ζητείται $\alpha \in \mathbb{N}$:

- ① $1 \leq \alpha \leq n$
- ② $(\alpha, n) = 1$
- ③ $\text{ord}_n(\alpha) = \varphi(n)$

Way: ① $\boxed{n=4}$ $1 \leq \alpha \leq 4$, $(\alpha, 4) = 1 \Rightarrow \alpha = 1 \text{ ή } \alpha = 3$.

$\varphi(4) = 2$ και $\text{ord}_4(3) = 2 = \varphi(4)$, διότι $3^2 = 9 \equiv 1 \pmod{4}$
 $\Rightarrow$ 3: πρωτ. ρίζα.

$\bullet \boxed{n=5}$ $1 \leq \alpha \leq 5$,
 $(\alpha, 5) = 1 \Rightarrow \alpha = 2, 3, 4$.

$2^1 \not\equiv 1 \pmod{5}$
 $2^2 \equiv 4 \not\equiv 1 \pmod{5} \equiv (-1) \pmod{5}$
 $2^4 \equiv (-1)^2 \pmod{5} \equiv 1 \pmod{5} \Rightarrow \text{ord}_2(5) = 4 = \varphi(5) \Rightarrow$
 $\Rightarrow$ 2: πρωτ. ρίζα mod 5.

Το 1: είναι πρωταρχική ρίζα
 $\Leftrightarrow n=1$ ή $n=2$
 διότι έχουμε $\varphi(n)=1$

$\bullet \boxed{n=10}$: $1 \leq \alpha \leq 10 \Rightarrow \alpha = 3, 7, 9$. και $\varphi(10) = 4$.

$$3^1 = 3 \not\equiv 1 \pmod{10}$$

$$3^2 = 9 \equiv (-1) \pmod{10}$$

$$3^4 \equiv 1 \pmod{10}$$

$$\boxed{\text{ord}_{10}(3) = 4} = \varphi(n) \Rightarrow$$

3: πρωτ. ρίζα mod 10.

$\bullet \boxed{n=13}$: $1 \leq \alpha \leq 13 \Rightarrow (\alpha, 13) = 1 \Rightarrow \alpha = 2, \dots, 12$, $\varphi(13) = 12$

$$2^1 \not\equiv 1 \pmod{13}$$

$$2^2 \not\equiv 1 \pmod{13}$$

$$2^3 = 8$$

$$2^4 = 16 \equiv 3 \pmod{13}$$

$$2^6 \equiv 2^3 \cdot 2^3 \equiv 64 \equiv (-1) \pmod{13}$$

$$2^{12} \equiv (-1)^2 \equiv 1 \pmod{13}$$

Παραμένει να βρούμε mod 13 ότι είναι οι διακεκομμένες και $\varphi(13) = 12$: 1, 2, 3, 4, 6, 12.

$$\boxed{\text{ord}_{13}(2) = 12}$$

2: πρωτ. ρίζα.

(30)

• $[n=14]$: $1 \leq \alpha \leq 14$, $(\alpha, 14) = 1$. Totu $\varphi(14) = \varphi(2 \cdot 7) = \varphi(2) \cdot \varphi(7) = 1 \cdot 6 = 6$
 $\Rightarrow \alpha = 3, 5, 9, 11, 13$. // n-ordine α fets: 1, 2, 3, 6. (diap. rev $\varphi(14)$)

$$\begin{aligned} 3^1 &= 3 \not\equiv 1 \pmod{14} \\ 3^2 &= 9 \not\equiv 1 \pmod{14} \\ 3^3 &= 27 \equiv (-1) \pmod{14} \\ 3^6 &= (3^3)^2 \equiv (-1)^2 \equiv 1 \pmod{14} \end{aligned} \quad \Rightarrow \text{ord}_{14}(3) = 6 : \underline{\underline{3: \text{nprw. pi} / \alpha}}$$

$[n=18] \Rightarrow \underline{\underline{5: \text{nprw. pi} / \alpha}}$

$n = 4, 5, 10, 13, 14, 18$
 $\textcircled{3} \textcircled{2} \textcircled{3} \textcircled{2} \textcircled{3} \textcircled{5}$

$[n=4] \Rightarrow 3: \text{nprw. pi} / \alpha$
 $3^k: \text{nprw. pi} / \alpha$ fets $(k, \varphi(4)) = 1 \Rightarrow$
 $\Rightarrow (k, 2) = 1 \Rightarrow \underline{\underline{k=1}}$

$[n=5] : 2: \text{nprw. pi} / \alpha \Rightarrow 2^k: \text{nprw. pi} / \alpha$
 $\forall k \in (k, \varphi(5)) = 1 \Rightarrow \underline{\underline{k=1}}$ $\wedge$ $\underline{\underline{k=3}}$

$[n=10] \Rightarrow 3: \text{nprw. pi} / \alpha \Rightarrow$
 $\Rightarrow 3^k: \text{nprw. pi} / \alpha$ fets $(k, \varphi(10)) = 1, \Rightarrow \underline{\underline{k=1}}$ $\wedge$ $\underline{\underline{k=3}}$
 $\hookrightarrow 3, 7 \pmod{10}$ (nprw. pi fets).

$[n=13] : \text{nprw. pi} / \alpha : 2 \Rightarrow 2^k, (k, \varphi(13)) = 1 \Rightarrow (k, 12) \Rightarrow k = 1, 5, 7, 11$
 $\hookrightarrow 2^1, 2^5, 2^7, 2^{11}$

46464 (10): $n > 1, \alpha, b \in \mathbb{Z}$ cu $(\alpha, n) = (b, n) = 1$ cu $(\text{ord}_n(\alpha), \text{ord}_n(b)) = 1$.
 Totu $\text{ord}_n(\alpha \cdot b) = \text{ord}_n(\alpha) \cdot \text{ord}_n(b)$

Noti: $\exists$ cu $r = \text{ord}_n(\alpha)$
 $s = \text{ord}_n(b)$ cu energ $(\alpha \cdot b, n) = 1 \Rightarrow \exists \text{ord}_n(b \cdot \alpha) = t$.
 $(\alpha \cdot b)^{r \cdot s} = \alpha^{rs} \cdot b^{rs} = (\alpha^n)^s \cdot (b^n)^r \equiv 1^s \cdot 1^r \pmod{n} \equiv 1 \pmod{n} \Rightarrow$
 $\Rightarrow t \mid r \cdot s$ (1)
 $(\alpha \cdot b)^t \equiv 1 \pmod{n} \Rightarrow (\alpha \cdot b)^{t \cdot r} \equiv 1 \pmod{n} \Rightarrow \alpha^{tr} \cdot b^{tr} \equiv 1 \pmod{n} \Rightarrow$
 $\Rightarrow (\alpha^n)^r \cdot b^{tr} \equiv 1 \pmod{n} \Rightarrow b^{tr} \equiv 1 \pmod{n} \Rightarrow s \mid tr \mid \Rightarrow \underline{\underline{s \mid t}}$
 $(s, r) = 1 \Rightarrow \underline{\underline{s \mid t}}$

$$\begin{aligned}
 (a \cdot b)^t &\equiv 1 \pmod{n} \Rightarrow (a^t b^t)^s \equiv 1 \pmod{n} \Rightarrow a^{ts} \cdot (b^t)^s \equiv 1 \pmod{n} \Rightarrow \\
 &\Rightarrow a^{ts} \equiv 1 \pmod{n} \Rightarrow r/t \cdot s \mid r/t \quad (r,s)=1 \quad \boxed{r/t} \textcircled{3}
 \end{aligned}$$

$$\text{Ans } \textcircled{2}, \textcircled{3} \Rightarrow \boxed{r \cdot s / t} \textcircled{4} \quad (r,s)=1$$

$$\textcircled{1}, \textcircled{4} \Rightarrow \boxed{t = r \cdot s}$$

$$a=3 \quad b=7 \quad k' \cdot n = 20 \Rightarrow (3, 20) = 1 = (7, 20)$$

$$\text{ord}_{20}(3 \cdot 7) = \text{ord}_{20}(21) = \text{ord}_{20}(1) = 1.$$

$$\text{Ομως } \text{ord}_{20}(3) = 4 = \text{ord}_{20}(7)$$

$$\alpha \rho \alpha (\text{ord}_{20}(3), \text{ord}_{20}(7)) = 4 \neq 1.$$

$$\delta \eta \lambda \text{ ord}_{20}(3 \cdot 7) = 1 \neq 16 = \text{ord}_{20}(3) \cdot \text{ord}_{20}(7).$$

- ① Διαμεζώμενα - ΜΚΔ, ΕΚΠ. π.χ. $(2^k + 5, 2^7 + 32 + 1)$
- ② Πρώτοι αριθμοί (Νόβ 3 αλληλικοί πρώτοι αριθμοί συσχετισμός heron)
- ③ Επίλυση Διοφαντικών Εξισώσεων
- ④ Αριθ. Συναρτήσεις & νόμος αντιστροφής Möbius.
- ⑤ Επίλυση γραμ. ισοτιμιών. (2ο κεφάλαιο ψηφίο κάποιων αριθμών/υπολοίπων)
- ⑥ Επίλυση γραμ. ισοτ. (Κ.Θ.Υ. ή άλλα γραμ. συστήματα ισοτιμιών)
- ⑦ Γάστρι βρογχίτων - πρώτ. ρίτες.