

28/05/15.

Τάξεις Στοιχείων
Πρωταρχικές ρίζες

Av $\alpha, n \in \mathbb{N}$ όπου $n \geq 1$ και $(\alpha, n) = 1$, τότε: Θεώρημα Euler:
 $\alpha^{\varphi(n)} \equiv 1 \pmod{n}$

Πρόβλημα: Είναι ο $\varphi(n)$ ο μικρότερος k : $\alpha^k \equiv 1 \pmod{n}$

Απάντηση: Όχι, δίδω: Έστω $\alpha=2, n=15$. Τότε $(\alpha, n) = (2, 15) = 1$.

$$\text{Τότε: } \varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8.$$

$$\text{Τότε } 2^8 \equiv 1 \pmod{15}$$

$2^1 = 2 \not\equiv 1 \pmod{15}$	Άρα $2^8 \equiv 1 \pmod{15}$
$2^2 = 4 \not\equiv 1 \pmod{15}$	
$2^3 = 8 \not\equiv 1 \pmod{15}$	
$2^4 = 16 \equiv 1 \pmod{15}$	

Ορισμός: Έστω $\alpha, n \in \mathbb{N}$, όπου $n \geq 1$ και $(\alpha, n) = 1$. Τότε: η τάξη του $\alpha \pmod{n}$ ορίζεται να είναι:
$$\text{ord}_n(\alpha) \stackrel{\text{def}}{=} \min \{ k \in \mathbb{N} / \alpha^k \equiv 1 \pmod{n} \} \stackrel{\text{def}}{=} \text{τάξη } \alpha \pmod{n}$$

Το α : πρωταρχική ρίζα $\pmod{n} \Leftrightarrow \text{ord}_n(\alpha) = \varphi(n)$.

Π.χ.: $\text{ord}_{55}(12) = ?$; Επειδή $(12, 55) = 1$, ορίζεται η $\text{ord}_{55}(12)$.
 $12^{\varphi(55)} \equiv 1 \pmod{55}$

$$12^1 = 12 \not\equiv 1 \pmod{55}$$

$$12^2 = 144 \not\equiv 1 \pmod{55} \rightarrow \equiv 34 \pmod{55}$$

$$12^3 \equiv 12 \cdot 34 \pmod{55} \equiv 23 \not\equiv 1 \pmod{55}$$

$$12^4 \equiv 12 \cdot 23 \pmod{55} \equiv 276 \pmod{55} \equiv 1 \pmod{55}$$

$$\begin{aligned} \text{ord}_{55}(12) &= 4 \\ 12^4 &\equiv 1 \pmod{55} \Rightarrow \\ &\Rightarrow 12^{40} \equiv 1 \pmod{55} \end{aligned}$$

Παραδείγματα: $\text{ord}_{15}(7) = ?$

$$(7, 15) = 1 \Rightarrow \text{Ford}_{15}(7) \quad \left| \begin{array}{l} 7^1 = 7 \not\equiv 1 \pmod{15} \\ 7^2 = 49 \equiv 4 \pmod{15} \\ 7^3 = 4 \cdot 7 \equiv 28 \equiv -2 \pmod{15} \not\equiv 1 \pmod{15} \\ 7^4 \equiv (-2) \cdot 7 \equiv -14 \equiv 1 \pmod{15} \end{array} \right.$$

Άρα $\text{ord}_{15}(7) = 4 \cdot 7 = 28 = \varphi(15)$

Άρα $\nexists$ OXI απαρ. ρ_i/α .

Πρόταση: Έστω $\alpha, n \in \mathbb{Z}$, $n \geq 1$ & ϵ έστω $(\alpha, n) = 1$. Έστω $r = \text{ord}_n(\alpha)$

① $\alpha^k \equiv \alpha^l \pmod{n} \Leftrightarrow k \equiv l \pmod{r}$

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

③ $\forall m, k : 0 \leq m \neq k \leq r-1 \Rightarrow \alpha^m \not\equiv \alpha^k \pmod{n}$

④ $b \equiv \alpha \pmod{n} \Rightarrow \text{ord}_n(\alpha) = \text{ord}_n(b)$

$\Rightarrow b \in \langle \alpha \rangle_n$
 $\Rightarrow \text{ord}_n(b) =$
 $= \text{ord}_n(\alpha)$

Απόδειξη: ① $(\Rightarrow)$ Έστω $\alpha^k \equiv \alpha^l \pmod{n} \Rightarrow n | \alpha^k - \alpha^l$ (*)

Χωρίς βλάβης ως γενικότερας, έστω $k \geq l$, τότε $k = l + h$

Εκεί. Διαίρεση: $\mu = k - l = r \cdot q + s, 0 \leq s < r$ (**)

(*) : $n | \alpha^k - \alpha^l \Rightarrow \alpha^k - \alpha^l = n \cdot m \Rightarrow \alpha^{l+h} - \alpha^l = n \cdot m \Rightarrow$
 $\Rightarrow \alpha^l (\alpha^h - 1) = n \cdot m \Rightarrow n | \alpha^l (\alpha^h - 1)$

$\Rightarrow n | \alpha^h - 1 \Rightarrow \alpha^h \equiv 1 \pmod{n}$ (***) $\left| \begin{array}{l} (n, \alpha) = 1 \Rightarrow (n, \alpha^l) = 1 \end{array} \right| \Rightarrow$

$\Rightarrow (\alpha^r)^q \cdot \alpha^s \equiv 1 \pmod{n} \Rightarrow 1^q \cdot \alpha^s \equiv 1 \pmod{n} \Rightarrow \alpha^s \equiv 1 \pmod{n}$

$\Rightarrow \boxed{s=0}$

Άρα: (**) $\Rightarrow k - l = r \cdot q \Rightarrow r | k - l \Rightarrow k \equiv l \pmod{r}$

($\Leftarrow$) Αν $k \equiv l \pmod{r} \Rightarrow k - l = r \cdot q, q \in \mathbb{Z}$. Τότε $\alpha^k \equiv \alpha^{l+r \cdot q} = \alpha^l \cdot (\alpha^r)^q \equiv \alpha^l \pmod{n}$

② Από το ①, για $l=0 \Rightarrow \alpha^k \equiv 1 \pmod{n} \Leftrightarrow k \equiv 0 \pmod{r} \Leftrightarrow r | k$

③ Έστω ότι $\alpha^m \equiv \alpha^k \pmod{n}$ ① $\Rightarrow m \equiv k \pmod{r} \Rightarrow r | m - k$

Άρα $\alpha^m \not\equiv \alpha^k \pmod{n}$ $\Rightarrow r \nmid m - k \Rightarrow r \leq m - k$:
 Απορ. διότι $m + k \leq r - 1$

④ Έστω $b \equiv \alpha \pmod{n} \Rightarrow$
 $\Rightarrow \forall k \geq 1 : b^k \equiv \alpha^k \pmod{n} \Rightarrow \alpha^k \equiv 1 \pmod{n} \Leftrightarrow b^k \equiv 1 \pmod{n}$. Τότε $\text{ord}_n(\alpha) = \min\{x \in \mathbb{N} / \alpha^x \equiv 1 \pmod{n}\}$
 (23) $= \min\{x \in \mathbb{N} / b^x \equiv 1 \pmod{n}\} = \text{ord}_n(b)$

Πρόταση: Έστω $\alpha, n \in \mathbb{Z}, n \geq 1, (\alpha, n) = 1$. Τότε: $\text{ord}_n(\alpha) \mid \varphi(n)$

Απόδειξη: Γνωρίζουμε ότι: $\alpha^k \equiv 1 \pmod{n} \Leftrightarrow n \mid k$
 Θεώρημα Euler: $\alpha^{\varphi(n)} \equiv 1 \pmod{n} \parallel \Rightarrow n \mid \varphi(n)$.

Παράδειγμα: Δυνατές τάξεις στοιχείων $\pmod{21}$

Από το ΠΟΡΙΣΜΑ οι δυνατές τάξεις θα είναι οι διαιρέτες του $\varphi(21) = \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = 2 \cdot 6 = 12$.
 Δηλαδή θα είναι: 1, 2, 3, 4, 6, 12

Παράδειγμα: $\text{ord}_{33}(38)$; $(38, 33) = 1 \Rightarrow \exists \text{ord}_{33}(38)$

$$38 \equiv 5 \pmod{33} \Rightarrow \text{ord}_{33}(38) = \text{ord}_{33}(5)$$

$$\varphi(33) = \varphi(3 \cdot 11) = \varphi(3) \cdot \varphi(11) = 2 \cdot 10 = 20.$$

$$\text{Αρα } \text{ord}_{33}(5) \mid \varphi(33) = 20 \Rightarrow$$

$$\Rightarrow \text{μοżliκές τιμές: } 1, 2, 4, 5, 10, 20.$$

$$5^1 = 5 \not\equiv 1 \pmod{33}$$

$$5^2 = 25 \equiv -8 \pmod{33}$$

$$5^4 \equiv (-8) \cdot (-8) \equiv 64 \pmod{33} \equiv (-2) \pmod{33}$$

$$5^5 \equiv (-2) \cdot 5 \equiv (-10) \pmod{33}$$

$$5^{10} \equiv (-10) \cdot (-10) = 100 \equiv 1 \pmod{33} \Rightarrow 5^{10} \equiv 1 \pmod{33} \Rightarrow \boxed{\text{ord}_{33}(5) = 10}$$

Θεώρημα: Έστω $\alpha, n \in \mathbb{Z}, n \geq 1$, και $(\alpha, n) = 1$. Τότε:

$$\text{ord}_n(\alpha^k) = \frac{\text{ord}_n(\alpha)}{(\text{ord}_n(\alpha), k)}, \quad \forall k \geq 1.$$

Απόδειξη: Έκτιθέμεν $(\alpha, n) = 1 \Rightarrow$

$$\Rightarrow (\alpha^k, n) = 1, \quad \forall k \geq 1 \Rightarrow \exists \text{ord}_n(\alpha^k)$$

Θέτουμε $r = \text{ord}_n(\alpha)$, $d = (r, k)$. ΘΑΘ $\text{ord}_n(\alpha^k) = \frac{r}{d} \Leftrightarrow$

$$\Leftrightarrow \begin{cases} (\alpha^k)^{\frac{r}{d}} \equiv 1 \pmod{n} \\ \text{Αν } (\alpha^k)^m \equiv 1 \pmod{n} \end{cases}$$

$$\Rightarrow \frac{r}{d} \leq m.$$

$$d = (r, k) \Rightarrow d | r \Rightarrow r = dr' / r', k' \in \mathbb{Z} : (r', k') = 1.$$

$$\cdot (\alpha^k)^{\frac{r}{d}} = \alpha^{k \cdot \frac{r}{d}} = (\alpha^r)^{\frac{k}{d}} = (\alpha^r)^{k'} = 1^{k'} = 1 \pmod{n}$$

$$\cdot \text{Έστω ότι } (\alpha^k)^m \equiv 1 \pmod{n} \Rightarrow \alpha^{km} \equiv 1 \pmod{n} \Rightarrow r | km \Rightarrow dr' = dk'm \Rightarrow$$

$$\Rightarrow r' / k' m \parallel d r' / m \Rightarrow \frac{r}{d} / m \Rightarrow \frac{r}{d} \leq m.$$

$$\forall \alpha \left[\text{ord}_n(\alpha^r) = \frac{r}{d} \right]$$

0 $\alpha \in \mathbb{Z}$ είναι πρωταρχική π.π. $\alpha \pmod{n} \Leftrightarrow (\alpha, n) = 1$ ή $\text{ord}_n(\alpha) = \phi(n)$

Παράδειγμα: ① $n=2$, $\forall \alpha : (\alpha, 2) = 1$, δηλ α : περιζωός $\Rightarrow \alpha = 2k+1, k \in \mathbb{N}$
~~και~~ $\alpha^1 \equiv 1 \pmod{2}$ και $1 = \phi(2) \Rightarrow \text{ord}_2(\alpha) = \phi(2) = 1$.
 $\Rightarrow \alpha$: πρωταρχική π.π. α
 $\hookrightarrow$ περιζωός.

$n=4$ $\Rightarrow$ Επειδή κάθε $k \in \mathbb{Z}$, ανήκει σε μία από τις
κλάσεις ισοτιμίας $[0]_4, [1]_4, [2]_4, [3]_4$ και $\forall b \in [\alpha]_n$:
 $\text{ord}_n(\alpha) = \text{ord}_n(b)$ αρκεί να βρούμε τις τάξεις των $1, 3$.
γιατί $(0, 4) \neq 1, (2, 4) \neq 1$.

$$1^1 \equiv 1 \pmod{4} \Rightarrow \text{ord}_4(1) = 1 \neq 2 = \phi(4)$$

$$3^1 \not\equiv 1 \pmod{4}, 3^2 = 9 \equiv 1 \pmod{4} \Rightarrow \text{ord}_4(3) = 2 = \phi(4) \Rightarrow 3: \text{πρωτ. π.π. } \alpha \pmod{4}.$$

$$\boxed{n=12}. U(\mathbb{Z}_{12}) = \{ [\alpha]_{12} \mid (\alpha, n) = 1 \} = \{ [1]_{12}, [5]_{12}, [7]_{12}, [11]_{12} \}$$

$$1^1 \equiv 1 \pmod{12} \Rightarrow \text{ord}_{12}(1) = 1 \neq 4 = \phi(12)$$

$$5^1 \not\equiv 1 \pmod{12}, 5^2 = 25 \equiv 1 \pmod{12} \Rightarrow \text{ord}_{12}(5) = 2 \neq 4 = \phi(12)$$

$$\text{ord}_{12}(7) = 2, \text{ord}_{12}(11) = 2, \text{Άρα } \forall \alpha \in U(\mathbb{Z}_{12}): \text{ord}_{12}(\alpha) = 1 \text{ ή } 2$$

και άρα $\nexists$ πρωτ. π.π. $\alpha \pmod{12}$.

Βολικό Πρόβλημα: Περιγραφή του συνόλου: $U(\mathbb{Z}_n) = \{ [k]_n \mid (k, n) = 1 \}$.

Θα είναι βολικό: αν $\exists \alpha \in \mathbb{Z} : \forall [k]_n \in U(\mathbb{Z}_n) : [k]_n = [\alpha^k]_n$
 δηλ αν: $U(\mathbb{Z}_n) = \{ [\alpha^k]_n \mid k = 0, 1, \dots, \varphi(n)-1 \}$ $\lambda \in \mathbb{N}$.

Θα δείξω ότι τέτοιος ακέραιος α υπάρχει $\Leftrightarrow$ το α : πρωτ. π/κ $\pmod{n}$.

Πρόταση: Έστω $\alpha, n \in \mathbb{Z}, n \geq 1, (\alpha, n) = 1$. Τότε: α : πρωτ. π/κ $\pmod{n} \Leftrightarrow$
 $\Leftrightarrow \{ 1, \alpha, \alpha^2, \dots, \alpha^{\varphi(n)-1} \} : \alpha$. G.U. $\pmod{n}$.

Απόδειξη: α : πρωτ. π/κ $\pmod{n} \Leftrightarrow (\alpha, n) = 1$ και
 το $\varphi(n) = \min_{k \in \mathbb{N}} k : \alpha^k \equiv 1 \pmod{n} \Leftrightarrow$

$\{ \alpha_1, \dots, \alpha_k \}$ α . G.U. $\pmod{n} \Leftrightarrow$
 $k = \varphi(n)$
 $\alpha_i \not\equiv \alpha_j \pmod{n}$
 αν $1 \leq i \neq j \leq k$

$\Leftrightarrow 1, \alpha, \alpha^2, \dots, \alpha^{\varphi(n)-1}$ είναι α και 2 αλληλοπρώτοι $\pmod{n} \Leftrightarrow$
 $\Leftrightarrow \{ 1, \alpha, \alpha^2, \dots, \alpha^{\varphi(n)-1} \} \alpha$. G.U. $\pmod{n}$.

Πρόταση 2: α : πρωτ. π/κ $\pmod{n} \Leftrightarrow U(\mathbb{Z}_n) = \{ [1]_n, [\alpha]_n, \dots, [\alpha]^{\varphi(n)-1} \}$

α : πρωτ. π/κ $\pmod{n} \Leftrightarrow (\alpha, n) = 1$ και $\text{ord}_n(\alpha) = \varphi(n) \Leftrightarrow$

$\Leftrightarrow [\alpha]_n \in U(\mathbb{Z}_n)$ και $\text{ord}_n([\alpha]_n) = \varphi(n)$

Πρωτ. π/κ $\pmod{n} = \{ \alpha \in \mathbb{Z} \mid (\alpha, n) = 1 \text{ κ' } \text{ord}_n(\alpha) = \varphi(n) \}$

Αν α : πρωτ. π/κ $\pmod{n}$, τότε: $U(\mathbb{Z}_n) = \{ [1]_n, [\alpha]_n, \dots, [\alpha^{\varphi(n)-1}]_n \} =$
 $= \{ [\alpha^k]_n \mid k = 0, 1, \dots, \varphi(n)-1 \}$

Π.Χ: ① $n=8$: $U(\mathbb{Z}_8) = \{ [1]_8, [3]_8, [5]_8, [7]_8 \}$

~~4(8)=4~~ $\varphi(8)=4$ | Δυνατά ζώγια $\pmod{8}$ = διαίρετες του $\varphi(8)=4 : 1, 2, 4$

$3^1 \equiv 3 \pmod{8} \neq 1 \pmod{8} \Rightarrow \text{ord}_8(3) = 2 \neq 4 = \varphi(8)$
 $3^2 = 9 \equiv 1 \pmod{8} \Rightarrow \text{ord}_8(3) = 2 \neq 4 = \varphi(8)$
 $5^2 = 25 \equiv 1 \pmod{8} \Rightarrow \text{ord}_8(5) = 2 \neq 4 = \varphi(8)$
 $7^2 = 49 \equiv 1 \pmod{8} \Rightarrow \text{ord}_8(7) = 2 \neq 4 = \varphi(8)$ $\Rightarrow \nexists$ πρωτ. π/κ $\pmod{8}$

(9) $n=10$: $\varphi(\mathbb{Z}_{10}) = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$
 $\varphi(10) = 4$. • $\text{ord}_{10}(1) = 1$. // Διωνές 2 & 5 στοιχείων mod 10 είναι οι διευρέες του $\varphi(10)=4$ δηλ: 1, 2, 4.
 $3^2 = 9 \equiv (-1) \pmod{10}$
 $3^4 \equiv (-1)(-1) \pmod{10} \equiv 1 \pmod{10}$ } $\Rightarrow \text{ord}_p(3) = 4 = \varphi(10) \Rightarrow 3: \text{πρωτ. πηλ.} \pmod{10}$
 $\{[3^k]_{10} \mid k=1, 2, 3, 4\} = \{[3]_{10}, [9]_{10}, [7]_{10}, [1]_{10}\} = \varphi(\mathbb{Z}_{10})$

$7^1 \equiv 7 \pmod{10}$
 $7^2 \equiv 9 \pmod{10} \equiv (-1) \pmod{10}$
 $7^4 \equiv (-1)(-1) \pmod{10} \equiv 1 \pmod{10}$ } $\Rightarrow \text{ord}_{10}(7) = 4 = \varphi(10) \Rightarrow 7: \text{πρωτ. πηλ.} \pmod{10}$
 $9^2 = 81 \equiv 1 \pmod{10} \Rightarrow \text{ord}_{10}(9) = 2 \neq 4 = \varphi(10) \Rightarrow 9: \text{οχι! πρωτ. πηλ.}$

Θεώρημα: $\exists$ πρωταρχικές π ηλ. $\pmod{p}$ $\Leftrightarrow n=2, 4, p^w$ ή $2 \cdot p^w$: p : πρῶτος πηλός.
 (mod n) $\Rightarrow \exists$ πρωτ. πηλ. $\pmod{p}$, $\forall p$: πρῶτος.

Θεώρημα: Έστω $n \geq 2$ και υποδ. δν $\exists$ πρωτ. πηλ. $\pmod{n}$.
 Το πλήθος τους είναι: $\varphi(\varphi(n))$. Είναι άρα α : πρωτ. πηλ. $\pmod{n} \Rightarrow$ όλες οι πρωτ. πηλ. είναι οι εξής:
 α^k , όπου $(k, \varphi(n)) = 1$, $k \in \mathbb{N}$.

Απόδειξη: Έστω α : πρωτ. πηλ. $\pmod{n}$ $\Rightarrow \varphi(\mathbb{Z}_n) = \{[\alpha]_n, \dots, [\alpha^{\varphi(n)}]_n\}$
 Ο αρέσμος x : πρωτ. πηλ. $\pmod{n}$ $\Rightarrow [x]_n \in \varphi(\mathbb{Z}_n)$
 $\Leftrightarrow [x]_n = [\alpha^k]$, $k=1, \dots, \varphi(n)$ και $\text{ord}_n(x) = \varphi(n)$
 και $\text{ord}_n(\alpha^k) = \frac{\text{ord}_n(\alpha)}{(\text{ord}_n(\alpha), k)} = \frac{\varphi(n)}{(\varphi(n), k)}$. Άρα α^k : πρωτ. πηλ. $\Leftrightarrow \text{ord}_n(\alpha^k) = \varphi(n) \Leftrightarrow (\varphi(n), k) = 1$. Τέτοια στοιχεία υπάρχουν σε πλήθος: $\varphi(\varphi(n))$.

Παράδειγμα: $\boxed{n=11}$, $U(\mathbb{Z}_{11}) = \{[1]_{11}, [2]_{11}, \dots, [10]_{11}\}$

$\varphi(11) = 10$ (αφού 11: πρώτος).

$\text{ord}_{11}(2) = 10$ ((Διότι) ισχύει $2^k \not\equiv 1 \pmod{11}$ & είναι διαιρετός του $\varphi(11) = 10 = 1, 2, 5, 10$).

$2^1 = 2 \equiv 2 \pmod{11}$

$2^2 \equiv 4 \pmod{11}$

$2^5 \equiv (-1) \pmod{11}$

$2^{10} \equiv (-1)(-1) \pmod{11} \equiv 1 \pmod{11} \Rightarrow \text{ord}_{11}(2^{10}) = 10 = \varphi(11) \Rightarrow 2^{10}$: new-
 πύκ $\pmod{11}$

Υπάρχουν $\varphi(\varphi(11)) = \varphi(10) = 4$ new πύκ $\pmod{11}$.

Όλες οι new πύκ $\pmod{11}$ θα είναι: 2^k , όπου $(k, 10) = 1 \Rightarrow$

$\underline{k=1} \Rightarrow 2^1 = 2$ | $\underline{k=7} \Rightarrow 2^7 \equiv 7 \pmod{11}$ | $\underline{k=3} \Rightarrow 2^3 = 8$ | $\underline{k=9} \Rightarrow 2^9 \equiv 6 \pmod{11}$

άρα $U(\mathbb{Z}_{11}) = \{[2^k]_{11} \mid k=1, \dots, 10\} = \{[8^k]_{11} \mid k=1, \dots, 10\} =$
 $= \{[7^k]_{11} \mid k=1, \dots, 10\} = \{[6^k]_{11} \mid k=1, \dots, 10\}$

συνολικά 4

