18/1/2015

Έστω $n>1$ και $a\in\mathbb{Z}$. Αν $(a,n)=1$, τότε ορίζεται η τάξη του $a$ mod $n$ να είναι ο φυσικός

$$ord_n(a)=\min\{k\in\mathbb{N} \mid a^k\equiv 1 \pmod n\}$$

Υπενθυμίζουμε από το Θεώρημα του Euler ότι: $a^{\varphi(n)}\equiv 1 \pmod n$

ΠΡΟΤΑΣΗ: Αν $(a,n)=1$, και $k\in\mathbb{N}: a^k\equiv 1 \pmod n$, τότε: $ord_n(a)\mid k$

ΠΟΡΙΣΜΑ: Αν $(a,n)=1$, τότε: $ord_n(a)\mid \varphi(n)$

ΠΡΟΤΑΣΗ (Θετικό Κριτήριο για το αν αριθμός είναι πρώτος)

Έστω $n>1$ και $a\in\mathbb{Z}$. Υποθέτουμε ότι: $a^{n-1}\equiv 1 \pmod n$ και

$a^d\not\equiv 1 \pmod n$, $\forall d\mid n-1$ και $d\neq n-1$. Τότε $n$: πρώτος

Απόδειξη:

Επειδή $a^{n-1}\equiv 1 \pmod n \Rightarrow n\mid a^n-1 \Rightarrow \exists k\in\mathbb{Z}: a^{n-1}-1=kn \Rightarrow$

$a^{n-1}-kn=1 \Rightarrow a(a^{n-2})+(-k)n=1 \Rightarrow (a,n)=(a^{n-1},n)=1$. Άρα ορίζεται η $ord_n(a)$

Τότε θα είχαμε: $ord_n(a)\mid n-1$ (1). Όμως $a^d\not\equiv 1 \pmod n$: $\forall d\mid n-1$, $d\neq n-1$ (2)

Από τις (1), (2) $\Rightarrow ord_n(a)=n-1$

$ord_n(a)\mid\varphi(n)$ $\Rightarrow n-1\mid\varphi(n) \Rightarrow n-1\le\varphi(n)$.

Όμως $\varphi(n)\le n-1$ και άρα: $\varphi(n)=n-1$. Τότε όμως ο μόνος διαιρέτης του $n$ είναι ο μοναδιαίος $\Rightarrow$ $n$: πρώτος

---

- Έστω $a,b\in\mathbb{Z}$ και $a\equiv b \pmod n$. Αν $(a,n)=1 \Rightarrow (b,n)=1$ και ισχύει ότι: $ord_n(a)=ord_n(b)$. Έστω αν $(a,n)=1$ και $a=qn+r$, $0\le r\le n-1$, τότε $(r,n)=1$ και $ord_n(a)=ord_n(r)$

ΠΑΡΑΔΕΙΓΜΑ:

$ord_{33}(38) = ;$

Επειδή $(33, 38) = 1 \Rightarrow$ ορίζεται η τάξη $ord_{33}(38)$

Επειδή $38 \equiv 5 \pmod{33}$, έπεται ότι: $ord_{33}(38) = ord_{33}(5)$

Άρα η τάξη θα είναι διαιρέτης του $\varphi(33) = \varphi(3 \cdot 11) = \varphi(3)\varphi(11) = 2 \cdot 10 = 20$.

Άρα $ord_{33}(5) \in \{1, 2, 4, 5, 10, 20\}$

- $5^1 \equiv 5 \not\equiv 1 \pmod{33}$
- $5^2 = 25 \equiv -8 \pmod{33} \not\equiv 1 \pmod{33}$
- $5^4 \equiv (-8)(-8) \equiv 64 \pmod{33} \equiv -2 \pmod{33} \not\equiv 1 \pmod{33}$
- $5^5 \equiv 5(-2) \equiv -10 \pmod{33} \not\equiv 1 \pmod{33}$
- $5^6 \equiv (-10)(-10) \equiv 100 \equiv 1 \pmod{33}$

Επειδή $10 = \min\{k \in \mathbb{N} \mid 5^k \equiv 1 \pmod{33}\} \Rightarrow ord_{33}(5) = ord_{33}(38) = 10$

**ΟΡΙΣΜΟΣ**: Αν $n \in \mathbb{N}$, $n > 1$ και αν $a \in \mathbb{Z}$ έτσι ώστε $(a, n) = 1$, τότε:

$a$: πρωταρχική ρίζα mod $n$ $\Leftrightarrow ord_n(a) = \varphi(n)$

- $n = 2$. Τότε ο ακέραιος $a = 1$ είναι πρωταρχική ρίζα mod 2
- $n = 3$ Τότε $(2, 3) = 1$ και $2^1 \equiv 2 \not\equiv 1 \pmod{3}$

  $2^2 = 4 \equiv 1 \pmod{3} \Rightarrow ord_3(2) = 2 = \varphi(3) \Rightarrow 2$: πρωταρχ. ρίζα mod 3
- $n = 4$. Τότε $(3, 4) = 1$ και $3^1 \equiv 3 \not\equiv 1 \pmod{4}$

  $3^2 = 9 \equiv 1 \pmod{4} \Rightarrow ord_4(3) = 2 = \varphi(4) \Rightarrow 3$: πρωταρχική ρίζα mod 4

$n = 5$. Τότε $(2, 5) = 1$ και: $2^1 \equiv 2 \not\equiv 1 \pmod{5}$

$2^2 \equiv 4 \not\equiv 1 \pmod{5}$

$2^3 \equiv 8 \not\equiv 1 \pmod{5}$

$2^4 \equiv 16 \equiv 1 \pmod{5} \Rightarrow ord_5(2) = 4 = \varphi(5) \Rightarrow 2$ πρωταρχική ρίζα mod 5.

• $n=8$ Πιθανές επιλογές $a \in \mathbb{Z} : (a,8)=1$ είναι οι $1, 3, 5, 7$

$\begin{cases} 3^1 \equiv 3 \not\equiv 1 \pmod 8 \\ 3^2 = 9 \equiv 1 \pmod 8 \end{cases} \Rightarrow ord_8(3)=2$

$\begin{cases} 5^1 \equiv 5 \not\equiv 1 \pmod 8 \\ 5^2 = 25 \equiv 1 \pmod 8 \end{cases} \Rightarrow ord_8(5)=2$

$7^1 \equiv 7 \not\equiv 1 \pmod 8$

$7^2 \equiv 49 \equiv 1 \pmod 8 \Rightarrow ord_8(7)=2$

$\varphi(8)=\varphi(2^3)=2^3-2^2=8-4=4$ Άρα επειδή $ord_8(1), ord_8(3), ord_8(5), ord_8(7) \neq 4 = \varphi(8) \Rightarrow$

$\Rightarrow$ δεν υπάρχουν πρωταρχικές ρίζες $(\bmod 8)$

Ψάχνουμε πρωταρχικές ρίζες $a \pmod n$, αναζητούμε ακεραίους $a \in \mathbb{Z} : (a,n)=1$ και $1 \le a \le n-1$ και $ord_n(a)=\varphi(n)$. Άρα οι πιθανές πρωταρχικές ρίζες $(\bmod n)$ θα είναι οι αντιπρόσωποι $a$ των διακεκριμένων κλάσεων υπολοίπων $[a]_n$, όπου $(a,n)=1$

δηλαδή $U(\mathbb{Z}_n)=\{[a]_n \in \mathbb{Z}_n \mid (a,n)=1\}$

ΠΡΟΤΑΣΗ: Έστω $n>1$ και $a \in \mathbb{Z} : (a,n)=1$. Τότε $a$: πρωταρχική ρίζα $(\bmod n) \Leftrightarrow$ το σύνολο $\{1, a, a^2, \dots, a^{\varphi(n)-1}\}$: αναγκαίο σύστημα υπολοίπων $(\bmod n)$

Απόδειξη:

"$\Rightarrow$". Έστω $a$: πρωταρχική ρίζα $(\bmod n)$. Επειδή $(a,n)=1 \Rightarrow (a^k,n)=1$, $1 \le k \le \varphi(n)-1$

Αν $a^i \equiv a^j \pmod n$ και $i \neq j$, $1 \le i,j \le \varphi(n)-1$ $\Rightarrow$ χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $i>j$ και τότε $a^{i-j} \equiv 1 \pmod n \Rightarrow ord_n(a) \mid i-j$, $ord_n(a)=\varphi(n)$ $\Rightarrow \varphi(n) \mid i-j \Rightarrow \varphi(n) \le i-j$

είναι αναγκαίο σύστημα υπολοίπων $(\bmod n)$

"$\Leftarrow$": Αν το $\{1, a, a^2, a^{\varphi(n)-1}\}$ αναγκαίο σύστημα υπολοίπων $(\bmod n)$. Τότε από το θεώρημα του Euler: $a^{\varphi(n)} \equiv 1 \pmod n$. Αν $a^d \equiv 1 \pmod n$, τότε το αναγκαίο σύστημα υπολοίπων και $d < \varphi(n)$ $(\bmod n)$ θα ήταν το $\{1, a, \dots, a^{d-1}\}$ αυτό είναι άτοπο διότι $d < \varphi(n)$. Άρα $\varphi(n) = \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod n\} = ord_n(a) \Rightarrow$ $a$: πρωταρχική ρίζα.

**ΠΟΡΙΣΜΑ:** Αν $a$: πρωταρχική ρίζα mod $n$, τότε:

$$U(\mathbb{Z}_n) = \{[1]_n, [a]_n, \dots, [a^{\varphi(n)-1}]_n\}$$

---

1: πρωταρχική (mod $n$) $\Rightarrow n=1$ ή 2

δηλαδή: 1: πρωταρχική ρίζα (mod $n$) $\Leftrightarrow ord_n(1) = \varphi(n) \Leftrightarrow 1 = \varphi(n) \Leftrightarrow n=1$ ή $n=2$

**ΘΕΩΡΗΜΑ:** Έστω $n \in \mathbb{N}$. Τότε:

Υπάρχουν πρωταρχικές ρίζες (mod $n$) $\Leftrightarrow n=2$ ή $n=4$ ή $n=p^m$, ή $n=2p^m$

($p$: περιττός πρώτος, $p$: περιττός πρώτος)

---

**ΠΡΟΤΑΣΗ:** Έστω $n>1$ και $a \in \mathbb{Z}: (a,n)=1$. Αν $k \geq 1$, τότε:

$$ord_n(a^k) = \frac{ord_n(a)}{(ord_n(a), k)}$$

**Απόδειξη:**

Επειδή $(a,n)=1 \Rightarrow (a^k,n)=1 \Rightarrow$ ορίζεται η τάξη $ord_n(a^k)$. Έστω $r = ord_n(a)$

Έστω $d = (ord_n(a), k) = (r,k)$. Θέλω $ord_n(a^k) = \frac{r}{(r,k)}$

$$d=(r,k) \Rightarrow \begin{cases} d \mid r \Rightarrow r = d \cdot r' \\ d \mid k \Rightarrow k = d k' \end{cases} \text{ και } (r',k')=1$$

① $(a^k)^{r/d} = a^{k\frac{r}{d}} = a^{r\frac{k}{d}} \equiv 1^{k/d} \equiv 1 \pmod n \Rightarrow$ **$(a^k)^{r/d} \equiv 1 \bmod n$** ①

② Έστω ότι: $(a^k)^m \equiv 1 \pmod n \Rightarrow a^{km} \equiv 1 \pmod n \Rightarrow$

$\Rightarrow r \mid km \Rightarrow \not\exists r' \mid \not\exists k' m \Rightarrow r' \mid k' \cdot m \Big| \Rightarrow r' \mid m \Rightarrow \frac{r}{d} \mid m \Rightarrow \frac{r}{d} \leq m$ ($(r',k')=1$)

①, ② $\Rightarrow ord_n(a^k) = \frac{r}{d} = \frac{r}{(r,k)} = \frac{ord_n(a)}{(ord_n(a),k)}$

---

**ΠΡΟΤΑΣΗ:**

Έστω $n \geq 2$, και υποθέτουμε ότι υπάρχει πρωταρχική ρίζα (mod $n$). Τότε το πλήθος των πρωταρχικών ριζών (mod $n$) είναι: $\varphi(\varphi(n))$

**Απόδειξη**

Έστω $a$: πρωταρχική ρίζα (mod $n$). Τότε το σύνολο $\{1, a, a^2, \dots, a^{\varphi(n)-1}\}$: ανοφέτο σύστημα υπολοίπων (mod $n$) και $U(\mathbb{Z}_n) = \{[1]_n, [a]_n, \dots, [a^{\varphi(n)-1}]_n\}$

Ⓐ

$\forall k = 1, \dots, \varphi(n)-1$ : $a^k$ πρωταρχική ρίζα $(\bmod n) \Leftrightarrow \text{ord}_n(a^k) = \varphi(n) \Leftrightarrow$

$\Leftrightarrow \dfrac{\text{ord}_n(a)}{(\text{ord}_n, k)} = \varphi(n) \Leftrightarrow \dfrac{\varphi(n)}{(\varphi(n), k)} = \varphi(n)$

**ΠΡΟΤΑΣΗ**: Έστω $n>1$ και $a \in \mathbb{Z}$ : $(a,n)=1$. Αν $k \geq 1$, τότε

$$\text{ord}_n(a^k) = \frac{\text{ord}_n(a)}{(\text{ord}_n[a], k)}$$

**ΠΟΡΙΣΜΑ**: Αν $n \geq 2$ και υπάρχουν πρωταρχικές ρίζες $(\bmod n)$, τότε οι πρωταρχικές ρίζες $(\bmod n)$ είναι : $a^k$, $(k, \varphi(n)) = 1$, όπου : $a$ : πρωταρχική ρίζα $(\bmod n)$ και σε πλήθος $\varphi(\varphi(n))$.

---

**ΠΑΡΑΔΕΙΓΜΑ**: $\boxed{n=10}$ $n=10=2\cdot 5 \Rightarrow$ υπάρχουν πρωταρχικές ρίζες $(\bmod 10)$ οι οποίες σε πλήθος είναι

$\varphi(\varphi(10)) = \varphi(4) = 2 \Rightarrow$ υπάρχουν ακριβώς πρωταρχικές ρίζες $(\bmod 10)$

$\{1, 3, 7, 9\}$ : αναγκαίο αλγόριθμο υπολοίπων $(\bmod 10)$

$3^1 \equiv 3 \not\equiv 1 (\bmod 10)$

$3^2 = 9 \not\equiv 1 (\bmod 10)$

$3^3 \equiv 3^2 \cdot 3^2 = 9 \cdot 9 \equiv 81 \equiv 1 (\bmod 10)$

Η μία είναι το 3. Η άλλη δεν είναι η $3^k$, $(k, \varphi(10)) = 1 \Rightarrow$

$(k,4)=1 \Rightarrow k=3$

Άρα $\text{ord}_{10}(3) = 4 = \varphi(10) \Rightarrow 3$ : πρωταρχική ρίζα $(\bmod 10)$

$3^3 = 27 \equiv 7 \bmod 10$

η δεύτερη είναι το 7.