17/12/2018

Ορισμός Έστω a,n ακέραιοι με $n>1$ και $(a,n)=1$. Ο μικρότερος φυσικός αριθμός s, τέτοιος ώστε $a^s \equiv 1 \bmod n$ ονομάζεται τάξη του a modulo n.

$$\operatorname{ord}_n(a)=s$$

Πρόταση Αν $a \equiv b \bmod n$ και $(a,n)=1$, τότε $\operatorname{ord}_n(a)=\operatorname{ord}_n(b)$

Απόδειξη Έστω $\operatorname{ord}_n(a)=s_1$ και $\operatorname{ord}_n(b)=s_2$

$$\operatorname{ord}_n(a)=s_1 \Rightarrow \left.\begin{array}{l} a^{s_2} \equiv 1 \bmod n \\ a \equiv b \bmod n \end{array}\right\} \Rightarrow b^{s_2} \equiv 1 \bmod n \Rightarrow \operatorname{ord}_n(b)=s_2 \leq s_1 \Rightarrow$$

$$\Rightarrow (s_2 \leq s_1)$$

$\left.\begin{array}{l} ord_n(\beta) = s_2 \Rightarrow \beta^{s_2} \equiv 1 \bmod n \\ a \equiv \beta \bmod n \end{array}\right\} \Rightarrow a^{s_2} \equiv 1 \bmod n \Rightarrow ord_n(a) = s_1 \leq s_2$

$\Rightarrow (s_1 \leq s_2)$

Άρα $s_1 = s_2 \Rightarrow ord_n(a) = ord_n(\beta)$

#Άσκηση 8

Άσκηση 7 Βρείτε τις τάξεις των ακεραίων 3, 5, 7, 9 modulo 16

Λύση

$3^1 \equiv 3 \bmod 16$

$3^2 \equiv 9 \bmod 16$

$3^3 \equiv 27 \bmod 16$

$\equiv 11 \bmod 16$

$3^4 \equiv 33 \bmod 16$

$\equiv 1 \bmod 16$ (Άρα $ord_{16}(3) = 4$)

$5^1 \equiv 5 \bmod 16$

$5^2 \equiv 25 \bmod 16$

$\equiv 9 \bmod 16$

$5^3 \equiv 5^2 \cdot 5 \bmod 16$

$\equiv 45 \bmod 16$

$\equiv 13 \bmod 16$

$5^4 \equiv 5^3 \cdot 5 \bmod 16$

$\equiv 5^2 \cdot 5^2 \bmod 16$

$\equiv 81 \bmod 16$

$\equiv 1 \bmod 16$ (Άρα $ord_{16}(5) = 4$)

$7^1 \equiv 7 \bmod 16$

$\equiv -9 \bmod 16$

$7^2 \equiv (-9)^2 \bmod 16$

$\equiv 81 \bmod 16$

$\equiv 1 \bmod 16$

(Άρα $ord_{16}(7) = 2$)

$9^2 \equiv 9 \bmod 16$

$9^2 \equiv 81 \bmod 16$

$\equiv 1 \bmod 16$ (Άρα $ord_{16}(9) = 2$)

Ορισμός: Έστω $(a,n) = 1$ Το a ονομάζεται αρχική ρίζα modulo n αν $ord_n(a) = \varphi(n)$

$\varphi(16) = \varphi(2^4) = 2^{4-1}(2-1) = 2^3 \cdot 1 = 8$

Άρα δεν υπάρχουν αρχικές ρίζες modulo 16.

#Φυλλάδιο 8

Άσκηση 8 Βρείτε τις τάξεις των στοιχείων της $U(\mathbb{Z}_{10})$

Λύση

$U(\mathbb{Z}_{10}) = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$

$\phi(10) = \phi(2\cdot 5) = 2^{1-1}(2-1)\cdot 5^{1-1}(5-1) = 4$ → τάξη στοιχείου

$ord_{10}([1]_{10}) = ord_{10}(1) = 1$

$1^1 \equiv 1 \bmod 10$

→ Άρα $ord_{10}(3) = \phi(10)$, δηλαδή το 3 είναι αρχική ρίζα modulo 10

$ord_{10}([3]_{10}) = ord_{10}(3) = 4$

$3^1 \equiv 3 \bmod 10$ $\quad 3^2 \equiv 9 \bmod 10$ $\quad \equiv -1 \bmod 10$

$3^3 \equiv 3^2 \cdot 3 \bmod 10$ $\quad \equiv (-1)\cdot 3 \bmod 10$ $\quad \equiv -3 \bmod 10$

$3^4 \equiv 3^2 \cdot 3^2 \bmod 10$ $\quad \equiv (-1)(-1) \bmod 10$ $\quad \equiv 1 \bmod 10$

Euler: $3^4 = 3^{\phi(10)} = 3 \bmod 10$

$ord_{10}([7]_{10}) = ord_{10}(-3) = 4$

$(-3)^1 \equiv -3 \bmod 10$ $\quad (-3)^2 \equiv 9 \bmod 10$ $\quad \equiv -1 \bmod 10$

$(-3)^3 \equiv (-3)^2(-3) \bmod 10$ $\quad \equiv 3 \bmod 10$

$(-3)^4 \equiv (-3)^2(-3)^2 \bmod 10$ $\quad \equiv 1 \bmod 10$

Άρα το 7 (ή το −3) είναι αρχική ρίζα modulo 10

$ord_{10}([9]_{10}) = ord_{10}(-1) = 2$

$(-1)^1 \equiv -1 \bmod 10$

$(-1)^2 \equiv 1 \bmod 10$

Φυλλάδιο 9

Άσκηση 2 $n \geq 3$, $(n-2, n) = 1$ και $\text{ord}_n(n-1) = 2$

Λύση $(n-2, n) = (-2, n) = (2, n) = 1$ επειδή $n-2$ είναι ίσο σ' όλο με το 2

$\text{ord}_n([n-2]_n) = \text{ord}_n(n-1) = \text{ord}_n(-1) = 2$

$(-1)^1 \equiv -1 \bmod n$ Αν $(-1) \equiv 1 \bmod n \Rightarrow n \mid -1-1 = -2 \Rightarrow$

$\neq 1 \bmod n$ $\Rightarrow n = 1$ ή $n = 2$

$(-1)^2 \equiv 1 \bmod n$ Όμως $n \geq 3$.

Θεώρημα Έστω $a, n \in \mathbb{Z}$ με $n > 1$ και $(a, n) = 1$. Αν $\text{ord}_n(a) = s$, τότε:

(i) $a^\lambda \equiv a^\kappa \bmod n \Leftrightarrow \lambda \equiv \kappa \bmod s$

(ii) $a^\lambda \equiv 1 \bmod n \Leftrightarrow s \mid \lambda$ (SOS) ‼ ‼

(iii) Οι αρέσκοι $1, a, a^2, \ldots, a^{s-1}$ είναι ανά δύο ανίσοι modulo n

Απόδειξη (i) $a^\lambda \equiv a^\kappa \bmod n \Rightarrow a^\lambda - a^\kappa \equiv 0 \bmod n \Rightarrow$

$\Rightarrow a^\kappa (a^{\lambda-\kappa} - 1) \equiv 0 \bmod n$

$(a, n) = 1 \overset{\text{ορισμός}}{\Rightarrow} \beta \cdot a \equiv 1 \bmod n$

$\Rightarrow \beta^\kappa \cdot a^\kappa (a^{\lambda-\kappa} - 1) \equiv \beta^\kappa \cdot 0 \bmod n$

$\Rightarrow a^{\lambda-\kappa} - 1 \equiv 0 \bmod n$

$\Rightarrow a^{\lambda-\kappa} \equiv 1 \bmod n$

$\lambda - \kappa = qs + r$, $0 \leq r < s$. 1η περίπτωση: $r \neq 0$

2η περίπτωση: $r = 0$

• 1η περίπτωση: $r \neq 0$, $0 \leq r < s \Rightarrow 1 \leq r < s \Rightarrow r \in \mathbb{N}$

$a^{\lambda-\kappa} \equiv 1 \bmod n$

$a^{qs+r} \equiv 1 \bmod n \Rightarrow a^{qs} \cdot a^r \equiv 1 \bmod n \Rightarrow (a^s)^q \cdot a^r \equiv 1 \bmod n \Rightarrow$ $\Rightarrow 1$, διότι αν ύψωση a

$\Rightarrow 1^q \cdot a^r \equiv 1 \bmod n \Rightarrow a^r \equiv 1 \bmod n$ Άτοπο!

$1 < r < s = \text{ord}_n(a)$

Άρα $r = 0$, δηλαδή $\lambda - \kappa = qs \Rightarrow s \mid \lambda - \kappa \Rightarrow \lambda \equiv \kappa \bmod s$

(ii) $a^\lambda \equiv 1 \bmod n \Leftrightarrow s \mid \lambda$

$a^\lambda \equiv 1 \bmod n \Leftrightarrow a^\lambda \equiv a^0 \bmod n \Leftrightarrow \lambda \equiv 0 \bmod s \Leftrightarrow s \mid \lambda - a \Leftrightarrow$

$s \mid \lambda$

(iii) Οι αριθμοί $0, 1, a, a^2, \dots, a^{s-1}$ είναι ανισοϋπολοιποι modulo n
Άρα οι δυνάμεις του $a^0, a^1, a^2, \dots, a^{s-2}$ είναι ανισοϋπολοιποι modulo n.

Πορισμα Euler

Έστω $a, n \in \mathbb{Z}$ με $n > 1$ και $(a,n) = 1$. Τότε:

$$\text{ord}_n(a) \mid \phi(n)$$

(η τάξη οποιουδήποτε στοιχείου διαιρεί το $\phi(n)$)

Απόδειξη

$(a,n) = 1 \overset{\text{Euler}}{\Rightarrow} a^{\phi(n)} \equiv 1 \bmod n$

$\text{ord}_n(a) \mid \phi(n)$

Άσκηση Βρείτε μια αρχική ρίζα modulo 23 ($\text{ord}(a) = 22$)

Λύση Έστω $(a, 23) = 1$, τότε $\text{ord}(a) \mid \phi(23) = 22 \Rightarrow$

$\Rightarrow \text{ord}(a) \mid 22$

$\Rightarrow \text{ord}(a) \in \{1, 2, 11, 22\}$

$2^1 \equiv 2 \bmod 23$

$2^2 \equiv 4 \bmod 23$

$2^3 \equiv 8 \bmod 23$

$2^4 \equiv 16 \bmod 23$

$2^5 \equiv 32 \bmod 23$

$\equiv 9 \bmod 23$

$2^{11} \equiv 2^5 \cdot 2^5 \cdot 2 \bmod 23$

$\equiv 9 \cdot 9 \cdot 2 \bmod 23$

$\equiv 9 \cdot 18 \bmod 23$

$\equiv 9(-5) \bmod 23$

$\equiv -45 \bmod 23 \Rightarrow$

$2^{11} \equiv 1 \bmod 23$

$\text{ord}_{23}(2) \in \{1, 2, 11, 22\}$

Άρα $\text{ord}_{23}(2) = 11$

Άρα το 2 δεν είναι αρχική ρίζα

$ord_{23}(3) \in \{1, 2, 11, 22\}$

$3^1 \equiv 3 \bmod 23$

$3^2 \equiv 9 \bmod 23$

$3^3 \equiv 27 \bmod 23$

$\equiv 4 \bmod 23$

$3^{11} \equiv 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^2 \bmod 23$

$\equiv 4 \cdot 4 \cdot 4 \cdot 9 \bmod 23$

$\equiv 16 \cdot 36 \bmod 23$

$\equiv 16 \cdot 13 \bmod 23$

$\equiv 208 \bmod 23$

$\equiv 208 - 230 \bmod 23$

$\equiv -22 \bmod 23$

$\equiv 1 \bmod 23$

Άρα $ord_{23}(3) = 11$

Άρα το 3 δεν είναι πρωταρχική ρίζα

$ord_{23}(5) \in \{1, 2, 11, 22\}$

$5^1 \equiv 5 \bmod 23$

$5^2 \equiv 25 \bmod 23$

$\equiv 2 \bmod 23$

$5^{11} \equiv 5^2 \cdot 5^2 \cdot 5^2 \cdot 5^2 \cdot 5^2 5 \bmod 23$

$\equiv 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \bmod 23$

$\equiv 4 \cdot 4 \cdot 10 \bmod 23$

$\equiv 160 \bmod 23$

$\equiv 160 - 161 \bmod 23$

$\equiv -1 \bmod 23$

Άρα $ord_{23}(5) = 22$

Άρα το 5 είναι αρχική ρίζα modulo 23.