7/1/2019

Έστω $a \in \mathbb{Z}$ και $n \in \mathbb{N}$ με $\text{μκδ}(a,n)=1$. Τάξη του a modulo n είναι ο μικρότερος φυσικός αριθμός s, τέτοιος ώστε $a^s \equiv 1 \bmod n$

Θεώρημα: Αν $\text{ord}(a)=s$, τότε:

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

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

(iii) $s \mid \varphi(n)$

(iv) Οι αριθμοί $1, a, a^2, \dots, a^{s-1}$ είναι ανισοϋπολοιποι modulo n

Έστω $a \in \mathbb{Z}$ και $n \in \mathbb{N}$ με $\text{μκδ}(a,n)=1$

Το a λέγεται αρχική ρίζα modulo n αν $\text{ord}_n(a) = \varphi(n)$

Αν το a είναι αρχική ρίζα modulo n, τότε οι αριθμοί $1, a, a^2, \dots, a^{\varphi(n)-1}$ είναι ανισοϋπολοιποι modulo n

$\underbrace{1 = a^0, a, a^2, \dots, a^{\varphi(n)-1}}_{\varphi(n) \text{ σε πλήθος}}$ και ανισοϋπολοιποι modulo n

$\text{μκδ}(a,n)=1$

$\text{μκδ}(a^\kappa,n)=1$ (Απόδειξη: Έστω $\text{μκδ}(a^\kappa,n)=d>1 \Rightarrow$ υπάρχει π.χ. του $p \mid d$

$p \mid d, d \mid a^\kappa \Rightarrow p \mid a^\kappa \Rightarrow p \mid \underbrace{aa\dots a}_{\kappa\text{-φορές}} \Rightarrow$

$d \mid n, p \mid n$

$\Rightarrow p \mid \text{μκδ}(a,n)=1$ Άτοπο!

Άρα $d=1$)

Παρατήρηση Αν το a είναι αρχική ρίζα modulo n, τότε το σύνολο $1, a, a^2, \dots, a^{\varphi(n)-1}$ είναι ένα περιορισμένο σύστημα υπολοίπων.

→ Έστω $\text{μκδ}(\beta,n)=1$, τότε υπάρχει κ τέτοιο ώστε $\beta \equiv a^\kappa \bmod n$, $0 \le \kappa \le \varphi(n)-1$

Φυλλάδιο 9

Άσκηση 7: (α) Δείξτε ότι το 3 είναι πρωταρχική ρίζα modulo 17

Διότι $\mu\kappa\delta(3,17)=1 \Rightarrow$ το 3 έχει τάξη modulo 17

$3^2 \equiv 3 \bmod 17$

$3^4 \equiv 3 \cdot 3^3 \bmod 17$
$\equiv 3 \cdot 10 \bmod 17$
$\equiv 30 \bmod 17$
$\equiv 13 \bmod 17$

$3^5 \equiv 3 \cdot 3^4 \bmod 17$
$\equiv 3 \cdot 13 \bmod 17$
$\equiv 39 \bmod 17$
$\equiv 5 \bmod 17$

$3^6 \equiv 3 \cdot 3^5 \bmod 17$
$\equiv 3 \cdot 5 \bmod 17$
$\equiv 15 \bmod 17$

$3^7 \equiv 3 \cdot 3^6 \bmod 17$
$\equiv 3 \cdot 15 \bmod 17$
$\equiv 45 \bmod 17$
$\equiv 11 \bmod 17$

$3^8 \equiv 3 \cdot 3^7 \bmod 17$
$\equiv 3 \cdot 11 \bmod 17$
$\equiv 33 \bmod 17$
$\equiv 16 \bmod 17$

$3^9 \equiv 3 \cdot 3^8 \bmod 17$
$\equiv 3 \cdot 16 \bmod 17$
$\equiv 48 \bmod 17$
$\equiv 14 \bmod 17$

$3^{10} \equiv 3 \cdot 3^9 \bmod 17$
$\equiv 3 \cdot 14 \bmod 17$
$\equiv 42 \bmod 17$
$\equiv 8 \bmod 17$

$3^{11} \equiv 3 \cdot 3^{10} \bmod 17$
$\equiv 3 \cdot 8 \bmod 17$
$\equiv 24 \bmod 17$
$\equiv 7 \bmod 17$

$3^{12} \equiv 3^4 \cdot 3^8 \bmod 17$
$\equiv 13 \cdot (-1) \bmod 17$
$\equiv 4 \bmod 17$

$3^{13} \equiv 3^5 \cdot 3^8 \bmod 17$
$\equiv 5 \cdot (-2) \bmod 17$
$\equiv 19 \bmod 17$

$3^{14} \equiv 3^6 \cdot 3^8 \bmod 17$
$\equiv 15 \cdot (-1) \bmod 17$
$\equiv 2 \bmod 17$

$3^{15} \equiv 3^7 \cdot 3^8 \bmod 17$
$\equiv 11 \cdot (-1) \bmod 17$
$\equiv 6 \bmod 17$

$3^{16} \equiv 3^8 \cdot 3^8 \bmod 17$
$\equiv (-1)(-1) \bmod 17$
$\equiv 1 \bmod 17$

Άρα, ο μικρότερος φυσικός αριθμός s, τέτοιος ώστε $3^s \equiv 1 \bmod 17$ είναι το 16. Άρα το 3 έχει τάξη $16 = \varphi(17)$. Άρα το 3 είναι πρωταρχική ρίζα modulo 17

(β) Για δοθέντα ακέραιο a με $(a,17)=1$, υπολογίστε τον ελάχιστο θετικό ακέραιο k ώστε $3^k \equiv a \bmod 17$

Διότι $1 \equiv 3^{16} \bmod 17$
$2 \equiv 3^{14} \bmod 17$

$3 \equiv 3^1 \bmod 17$

$4 \equiv 3^{12} \bmod 17$

$5 \equiv 3^5 \bmod 17$

$\vdots$

$16 \equiv 3^8 \bmod 17$

(β) Λύστε για x ακέραιο την ισοτιμία $x^4 \equiv 13 \bmod 17$

Λύση Αν x λύση της $x^4 \equiv 13 \bmod 17$, τότε $\mu\kappa\delta(x,17) = 1$

(διαφορετικά $\mu\kappa\delta(x,17) = 17 \Rightarrow x \equiv 0 \bmod 17 \Rightarrow x^4 \equiv 0 \bmod 17 \not\equiv 13 \bmod 17$ άτοπο)

$\Rightarrow x \equiv 3^y \bmod 17$

$(3^y)^4 \equiv 13 \bmod 17 \Leftrightarrow 3^{4y} \equiv 3^4 \bmod 17 \Leftrightarrow 4^y \equiv 4 \bmod(\text{ord}(3)) \Leftrightarrow$

$\Leftrightarrow 4y \equiv 4 \bmod 16^{\cdot d(17)} \Leftrightarrow y \equiv 1 \bmod 4 \Leftrightarrow y = 1 + 4\lambda,\ \lambda \in \mathbb{Z}$

$x = 3^y \bmod 17$

$\equiv 3^{1+4\lambda} \bmod 17$

Για: $\lambda = 0$, $x \equiv 3 \bmod 17$

$\lambda = 1$, $x = 3^5 \bmod 17$

$\equiv 5 \bmod 17$

$\lambda = 2$, $x \equiv 3^9 \bmod 17$

$\equiv 14 \bmod 17$

$\lambda = 3$, $x \equiv 3^{13} \bmod 17$

$\equiv 12 \bmod 17$

$\lambda = 4$, $x \equiv 3^{17} \bmod 17$

$\equiv 3^{1+16} \bmod 17$

$\equiv 3 \bmod 17$

Άρα, οι λύσεις της $x^4 \equiv 13 \bmod 17$ είναι οι:

$\{3 \bmod 17, 5 \bmod 17, 14 \bmod 17, 12 \bmod 17\}$

Θεώρημα: Έστω a ακέραιος και n φυσικός με $\mu\kappa\delta(a,n)=1$
Έστω $\lambda \in \mathbb{Z}$. Τότε:

$$ord(a^\lambda) = \frac{ord(a)}{\mu\kappa\delta(\lambda, ord(a))}$$

Απόδειξη: Έστω $ord(a)=s$, $ord(a^\lambda)=\delta$,

$$\frac{ord(a)}{\mu\kappa\delta(\lambda, ord(a))} = \frac{s}{\mu\kappa\delta(\lambda,s)} = d$$

$ord(a^\lambda)=\delta \Rightarrow (a^\lambda)^\delta \equiv 1 \bmod n \Rightarrow a^{\lambda\delta} \equiv 1 \bmod n$

$ord(a)=s \mid \lambda\delta \Rightarrow s \mid \lambda\delta \Rightarrow d = \frac{s}{\mu\kappa\delta(s,\lambda)} \Big/ \frac{\lambda}{\mu\kappa\delta(s,\lambda)} \cdot \delta$

$$\mu\kappa\delta\left(\frac{s}{\mu\kappa\delta(s,\lambda)}, \frac{\lambda}{\mu\kappa\delta(s,\lambda)}\right) = 1$$

$$d = \frac{s}{\mu\kappa\delta(s,\lambda)} \Big/ \frac{\lambda}{\mu\kappa\delta(s,\lambda)} \cdot \delta \Rightarrow d \mid \delta$$

$(a^\lambda)^d \equiv a^{\lambda d} \bmod n$

$\equiv a^{\lambda \cdot \frac{s}{\mu\kappa\delta(\lambda,s)}} \bmod n$

$\equiv a^{s \cdot \frac{\lambda}{\mu\kappa\delta(\lambda,s)}} \bmod n$

$\equiv (a^s)^{\frac{\lambda}{\mu\kappa\delta(\lambda,s)}} \bmod n$

$\equiv 1^{\frac{\lambda}{\mu\kappa\delta(\lambda,s)}} \bmod n$

$\equiv 1 \bmod n \Rightarrow ord(a^\lambda) \mid d$

$\Rightarrow \delta \mid d$

$d \mid \delta$

$d, \delta \in \mathbb{N}$

Άρα $\delta = d$

$$ord(a^\lambda) = \frac{ord(a)}{\mu\kappa\delta(\lambda, ord(a))}$$

$ord_{17}(3) = 16$

$ord_{17}(2) = ?$

$ord_{17}(2) = ord(3^{14}) = \frac{ord(3)}{\text{μκδ}(14, ord(3))} = \frac{16}{\text{μκδ}(14,16)} = \frac{16}{2} = 8$

$ord_{17}(4) = ord(3^{12}) = \frac{ord(3)}{\text{μκδ}(12, ord(3))} = \frac{16}{\text{μκδ}(12,16)} = \frac{16}{4} = 4$

$ord_{17}(5) = ord(3^5) = \frac{16}{\text{μκδ}(5,16)} = \frac{16}{1} = 16$ Άρα το 5 είναι πρωταρχική ρίζα modulo 17

Άσκηση: Βρείτε όλες τις πρωταρχικές ρίζες modulo 17.

Λύση: Έστω b πρωταρχική ρίζα modulo 17

$ord_{17}(b) = \varphi(17) = 16$

$(b, 17) = 1$

$\Rightarrow b \equiv 3^\lambda \bmod 17$, $1 \le \lambda \le 16$

$16 = ord_{17}(b) = ord_{17}(3^\lambda) = \frac{ord(3)}{\text{μκδ}(\lambda, ord(3))} = \frac{16}{\text{μκδ}(\lambda,16)} \Rightarrow$

$\Rightarrow \text{μκδ}(\lambda,16) = 1$, $1 \le \lambda \le 16$ $\Rightarrow \lambda \in \{1,3,5,7,9,11,13,15\}$

$\varphi(16) = 8$ αριθμοί

Άρα υπάρχουν 8 πρωταρχικές ρίζες modulo 17

$3^1 \equiv 3 \bmod 17$

$3^3 \equiv 10 \bmod 17$

$3^5 \equiv 5 \bmod 17$

$3^7 \equiv 11 \bmod 17$

$3^9 \equiv 14 \bmod 17$

$3^{11} \equiv 7 \bmod 17$

$3^{13} \equiv 12 \bmod 17$

$3^{15} \equiv 6 \bmod 17$

Παρατήρηση: Έστω ότι α είναι πρωταρχική ρίζα modulo n. Τότε όλες οι αντίστοιχες πρωταρχικές ρίζες modulo n είναι της μορφής a^k όπου $1 \le k \le \varphi(n)$ και $\mu\kappa\delta(k, \varphi(n)) = 1$

Παρατήρηση: Έστω ότι υπάρχει πρωταρχική ρίζα modulo n. Τότε υπάρχουν ακριβώς $\varphi(\varphi(n))$ πρωταρχικές ρίζες

Δεν υπάρχουν πάντα πρωταρχικές ρίζες

#Φυλλάδιο 8

Άσκηση 2: Δείξτε ότι για κάθε $k \ge 2$, υπάρχουν k το πλήθος διαδοχικοί ακέραιοι, κάθε ένας από τους οποίους διαιρείται από τετράγωνο αριθμού > 1.

Λύση Για $k = 3$

$$\left.\begin{array}{lll} 2^2 \mid x & x \equiv 0 \bmod 4 & x \equiv 0 \bmod 4 \\ 3^2 \mid x+1 & x+1 \equiv 0 \bmod 9 & x \equiv -1 \bmod 9 \\ 5^2 \mid x+2 & x+2 \equiv 0 \bmod 25 & x \equiv -2 \bmod 25 \end{array}\right\} (\Sigma)$$

$\mu\kappa\delta(4,9) = \mu\kappa\delta(9,25) = \mu\kappa\delta(4,25) = 1$

Άρα το (Σ) έχει λύση από το κινέζικο θεώρημα

Έστω x_0 λύση του (Σ). Τότε $\left.\begin{array}{l} x_0 \equiv 0 \bmod 4 \\ x_0+1 \equiv 0 \bmod 9 \\ x_0+2 \equiv 0 \bmod 25 \end{array}\right\} \Rightarrow \begin{array}{l} 4 \mid x_0 \\ 9 \mid x_0+1 \\ 25 \mid x_0+2 \end{array}$

$p_1, p_2, \dots, p_k$ πρώτοι αριθμοί διαφορετικοί μεταξύ τους.

$$\begin{array}{l} x \equiv 0 \bmod p_1^2 \\ x+1 \equiv 0 \bmod p_2^2 \\ \vdots \\ x+k \equiv 0 \bmod p_k^2 \end{array} \quad (\Sigma)$$

Το (Σ) έχει λύση από το κινέζικο θεώρημα αφού $\mu\kappa\delta(p_i^2, p_j^2) = 1, \forall i, j$

Αν x_0 μια λύση, τότε $\begin{array}{l} p_1^2 \mid x_0 \\ p_2^2 \mid x_0+1 \\ \vdots \\ p_k^2 \mid x_0+k-1 \end{array}$