13/12/2018

Άσκηση Βρείτε όλες τις λύσεις του συστήματος:

$$\begin{cases} 2x \equiv 14 \bmod 10 \\ 5x \equiv 5 \bmod 15 \\ 3x \equiv 2 \bmod 8 \end{cases}$$

$2x \equiv 14 \bmod 10$, $\mu\kappa\delta(2,10) = 2 \mid 14$ (μια λύση μόδιο 5, δυο λύσεις μόδιο 10)

$$x \equiv 7 \bmod 5$$

$5x \equiv 5 \bmod 15$, $\mu\kappa\delta(5,15) = 5 \mid 5$ (μια λύση μόδιο 3, πέντε λύσεις μόδιο 15)

$$x \equiv 1 \bmod 3$$

$3x \equiv 2 \bmod 8$, $\mu\kappa\delta(3,8) = 1 \mid 2$ (μια μοναδική λύση μόδιο 8)

$$x \equiv 6 \bmod 8$$

$\begin{cases} x \equiv 7 \bmod 5 \\ x \equiv 1 \bmod 3 \\ x \equiv 6 \bmod 8 \end{cases}$ $\quad \mu\kappa\delta(5,3)=1$, $\mu\kappa\delta(3,8)=1$, $\mu\kappa\delta(5,8)=1$ Εφαρμόζω κινέζικο θεώρημα

$M = 5 \cdot 3 \cdot 8 = 120$

$b_1 M_1 = 1 \bmod m_1$

$b_1\, 3 \cdot 8 \equiv 1 \bmod 5$

$b_1\, 3 \cdot 3 \equiv 1 \bmod 5$

$b_1\, 9 \equiv 1 \bmod 5$

$b_1(-1) \equiv 1 \bmod 5$

$b_1 \equiv -1 \bmod 5$

$b_2 M_2 \equiv 1 \bmod m_2$

$b_2\, 5 \cdot 8 \equiv 1 \bmod 3$

$b_2(-1)(-1) \equiv 1 \bmod 3$

$b_2 \equiv 1 \bmod 3$

$b_3 M_3 \equiv 1 \bmod m_3$

$b_3\, 5 \cdot 3 \equiv 1 \bmod 8$

$b_3 \cdot 15 \equiv 1 \bmod 8$

$b_3(-1) \equiv 1 \bmod 8$

$b_3 \equiv -1 \bmod 8$

a_i	M_i	b_i
7	$3 \cdot 8$	-1
1	$5 \cdot 8$	1
6	$3 \cdot 5$	-1

$x \equiv a_1 M_1 b_1 + a_2 M_2 b_2 + a_3 M_3 b_3 \bmod M$

$\equiv 7 \cdot 3 \cdot 8(-1) + 1 \cdot 5 \cdot 8(1) + 6 \cdot 3 \cdot 5(-1 \bmod 3 \cdot 5 \cdot 8$

$\equiv -21 \cdot 8 + 40 - 90 \bmod 120$

$\equiv -168 - 50 \bmod 120$

$\equiv -218 \bmod 120$

$\equiv 22 \bmod 120$

Άρα $x = 22 + 120\lambda$, $\lambda \in \mathbb{Z}$

Άσκηση Να λυθεί το σύστημα: $\begin{cases} x \equiv 7 \bmod 15 \\ x \equiv 2 \bmod 20 \\ x \equiv 8 \bmod 14 \end{cases}$

μκδ(15,5) = 5 ≠ 1 άρα δεν μπορώ να εφαρμόσω κινέζικο θεώρημα

$x \equiv 7 \bmod 15 \Rightarrow x = 7 + 15y$ και προσπαθώ να βρω το y. Πάω

$\left.\begin{matrix} x \equiv 2 \bmod 20 \\ x \equiv 8 \bmod 14 \end{matrix}\right\} \Rightarrow \begin{matrix} 7+15y \equiv 2 \bmod 20 \\ x \equiv 8 \bmod 14 \end{matrix}$ στη 2η ισοτιμία και κάνω αντικατάσταση

$7 + 15y \equiv 2 \bmod 20$

$15y \equiv -5 \bmod 20$ μκδ(15,20) = 5/5 άρα το σύστημα

$15y \equiv 15 \bmod 20$ έχει λύση.

$3y \equiv 3 \bmod 4$ μκδ(3,4) = 1 το 3 είναι αντιστρέψιμο

$y \equiv 1 \bmod 4$

$\begin{cases} x = 7 + 15y \\ y \equiv 1 \bmod 4 \Rightarrow y = 1 + 4z \\ x \equiv 8 \bmod 14 \end{cases}$ και τώρα ψάχνω το z $\Rightarrow$

$\Rightarrow x = 7 + 15y \Rightarrow x = 7 + 15(1 + 4z) \Rightarrow x = 7 + 15 + 60z \Rightarrow$

$x = 22 + 60z$

$x \equiv 8 \bmod 14$

$22 + 60z \equiv 8 \bmod 14 \Rightarrow 60z \equiv -14 \bmod 14$ μκδ(60,14) = 2/14 άρα το σύστημα έχει λύσεις

$60z \equiv -14 \bmod 14$

$30z \equiv -7 \bmod 7$

$2z \equiv 0 \bmod 7$

$z \equiv 0 \bmod 7 \Rightarrow z = 0 + 7\omega$

$x = 22 + 60z \Rightarrow x = 22 + 60(0 + 7\omega)$

$\Rightarrow x = 22 + 420\omega, \ \omega \in \mathbb{Z}$

Η λύση του αρχικού συστήματος: $x \equiv 22 \bmod 420$

Παράδειγμα Έστω $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $\mu\kappa\delta(a,n)=1$, Euler $a^{\phi(n)} \equiv 1 \bmod n$

$$\left.\begin{array}{l} a=2,\ n=31 \\ \mu\kappa\delta(2,31)=1 \end{array}\right\} \xrightarrow{Euler} \begin{array}{l} 2^{\phi(31)} \equiv 1 \bmod 31 \\ 2^{30} \equiv 1 \bmod 31 \end{array}$$

$\phi(31)=30$ διότι 31: πρώτος

$\phi(p)=p-1$ όταν p: πρώτος

$\phi(1)=1$

$\phi(p_1^{a_1}\cdots p_s^{a_s}) = p_1^{a_1-1}(p_1-1)\cdots p_s^{a_s-1}(p_s-1)$

$2^1 \equiv 2 \bmod 31$

$2^2 \equiv 4 \bmod 31$

$2^3 \equiv 8 \bmod 31$

$2^4 \equiv 16 \bmod 31$

$2^5 \equiv 32 \bmod 31$

$\equiv 1 \bmod 31$, $ord_{31}(2)=5$

$2^{2018} \equiv 2^{5\lambda+3} \bmod 31$

$\equiv (2^5)^{\lambda} \cdot 2^3 \bmod 31$

$\equiv 1^{\lambda} \cdot 8 \bmod 31$

$\equiv 8 \bmod 31$

Ορισμός Έστω $n \geq 1$ φυσικός αριθμός και a ακέραιος με $\mu\kappa\delta(a,n)=1$. Ονομάζουμε τάξη του a modulo n τον ελάχιστο φυσικό αριθμό s, τέτοιο ώστε:

$a^s \equiv 1 \bmod n$ και το συμβολίζουμε με $s = ord_n(a)$

- $ord_n(1)=1$, η τάξη του 1 είναι πάντοτε ο αριθμός 1.
- Το μοναδικό στοιχείο που έχει τάξη 1 είναι το 1.

$2^1 \equiv 2 \bmod 6$

$2^2 \equiv 4 \bmod 6$

$2^3 \equiv 8 \bmod 6$

$\equiv 2 \bmod 6$

$2^4 \equiv 4 \bmod 6$

$2^5 \equiv 8 \bmod 6$

$\equiv 2 \bmod 6$

$2^s \equiv 1 \bmod 6 \rightarrow$ Δεν μπορεί ποτέ να συμβεί αυτό

Πρόταση Έστω n, s φυσικοί και a ακέραιος.
Αν $a^s \equiv 1 \bmod n$, τότε μκδ$(a,n)=1$

Έστω $d=(a,n)$ $\qquad a^s = 1+\lambda n$

$\Rightarrow d \mid a$
$ d \mid n$ $\Rightarrow d \,\big/\, \boxed{a^{s-1}}\, a + \boxed{-\lambda}\, n = 1 \Rightarrow d = 1$

Παράδειγμα Βρείτε την τάξη του 2 μόδιο 17
μκδ$(2,17)=1$, άρα το 2 έχει τάξη μόδιο 17

$2^1 \equiv 2 \bmod 17$
$2^2 \equiv 4 \bmod 17$
$2^3 \equiv 8 \bmod 17$
$2^4 \equiv 16 \bmod 17$
$2^5 \equiv 32 \bmod 17$
$\equiv 15 \bmod 17$

$2^6 \equiv 30 \bmod 17$
$\equiv 13 \bmod 17$
$2^7 \equiv 26 \bmod 17$
$\equiv 9 \bmod 17$
$2^8 \equiv 18 \bmod 17$
$\equiv 1 \bmod 17$

Η τάξη έχει να κάνει με το μόδιο

Άρα: $ord_{17}(2) = 8$

Παράδειγμα Βρείτε την τάξη του 3 μόδιο 17
μκδ$(3,17)=1$ άρα το 3 έχει τάξη μόδιο 17.

$3^1 \equiv 3 \bmod 17$
$3^2 \equiv 9 \bmod 17$
$3^3 \equiv 27 \bmod 17$
$\equiv 10 \bmod 17$
$3^4 \equiv 3 \cdot 3^3 \bmod 17$
$\equiv 30 \bmod 17$
$\equiv 13 \bmod 17$
$3^5 \equiv 39 \bmod 17$
$\equiv 5 \bmod 17$
$3^6 \equiv 15 \bmod 17$
$3^7 \equiv 45 \bmod 17$
$\equiv 11 \bmod 17$

$3^8 \equiv 33 \bmod 17$
$\equiv -1 \bmod 17$
$3^9 \equiv -3 \bmod 17$
$\equiv 14 \bmod 17$
$3^{10} \equiv 3^2 \cdot 3^8 \bmod 17$
$\equiv -9 \bmod 17$
$\equiv 8 \bmod 17$
$3^{11} \equiv 3^3 \cdot 3^8 \bmod 17$
$\equiv -10 \bmod 17$
$\equiv 7 \bmod 17$

$3^{12} \equiv 3^4 \cdot 3^8 \bmod 17$
$\equiv -13 \bmod 17$
$\equiv 4 \bmod 17$
$3^{13} \equiv 3^5 \cdot 3^8 \bmod 17$
$\equiv -5 \bmod 17$
$\equiv 12 \bmod 17$
$3^{14} \equiv -15 \bmod 17$
$\equiv 2 \bmod 17$
$3^{15} \equiv -11 \bmod 17$
$\equiv 6 \bmod 17$
$3^{16} \equiv 1 \bmod 17$

Άρα $ord_{17}(3) = 16$

$(a,17)=1$

mod17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
mod17	3^0	3^{14}	3^1	3^{12}	3^5	3^{15}	3^{11}	3^{10}	3^2	3^3	3^7	3^{13}	3^4	3^9	3^6	3^8

$13 \cdot 15 \equiv 3^4 \cdot 3^6 \bmod 17$ (η ιδέα του λογαρίθμου)

$\equiv 3^{10} \bmod 17$ Διακριτός Λογάριθμος

$\equiv 8 \bmod 17$

$13^{27} \equiv (3^4)^{27} \bmod 17$

$\equiv 3^{108} \bmod 17$

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

$\equiv 4 \bmod 17$

ο εκθέτης δουλεύει με βάση την τάξη

η βάση δουλεύει με βάση το μόδιο

Ορισμός: Έστω n φυσικός και a ακέραιος με μκδ$(a,n)=1$. Τότε το a ονομάζεται αρχική (πρωταρχική) ρίζα αν η τάξη του a μόδιο n είναι ίση με τη μέγιστη δυνατή, δηλαδή:

$$\boxed{ord_n(a)=\phi(n)}$$

Παράδειγμα
- Το $ord_{17}(3)=16=\phi(17)$. Άρα το 3 είναι αρχική ρίζα μόδιο 17
- Το $ord_{17}(2)=8$. Άρα το 2 δεν είναι αρχική ρίζα μόδιο 17.

Άσκηση S.O.S. Βρείτε όλες τις αρχικές ρίζες μόδιο 6.

$(a,6)=1$

$ord_6(a)=\phi(6)$

$\phi(6)=2$

$5^1 \equiv 5 \bmod 6$

$5^2 \equiv 1 \bmod 6$

~~0mod6~~ μκδ$(0,6)=6$

1mod6 μκδ$(1,6)=1$

~~2mod6~~ μκδ$(2,6)=2$

~~3mod6~~ μκδ$(3,6)=3$

~~4mod6~~ μκδ$(4,6)=2$

5mod6 μκδ$(5,6)=1$

Άρα $ord_6(5)=2 = \phi(6)$

Άρα το 5 είναι αρχική ρίζα.

Παράδειγμα Βρείτε όλες τις αρχικές ρίζες μόδιο 8.

$(a,8)=1$

$ord_8(a)=\phi(8)$

$\phi(8)=4$

$1^1\equiv 1 \mod 8$ $\quad ord_8(1)=1$

$3^1\equiv 3 \mod 8$

$3^2\equiv 9 \mod 8$

$\equiv 1 \mod 8$ $\quad ord_8(3)=2$

$5^1\equiv 5 \mod 8$

$5^2\equiv 25 \mod 8$

$\equiv 1 \mod 8$ $\quad ord_8(5)=2$

$7^1\equiv 7 \mod 8$

$7^2\equiv 1 \mod 8$ $\quad ord_8(7)=2$

Άρα δεν υπάρχουν αρχικές ρίζες μόδιο 8.