06/12/2016

$ord_n(a) = k$ ελάχιστος ώστε $a^k \equiv 1 \mod n$

<u>ΠΡΟΤΑΣΗ</u>

$n > 1$ φυσικός και $a, b \in \mathbb{Z}^*$ με $(a,n)=1$

$a \equiv b \mod n \Rightarrow ord_n(a) = ord_n(b)$

<u>Απόδειξη</u>

$a \equiv b \mod n$ και $(a,n)=1 \Rightarrow (b,n)=1$

$ord_n(a) = k \Rightarrow a^k \equiv 1 \mod n \Rightarrow b^k \equiv 1 \mod n$

Έστω $ord_n(b) = l \neq k$

Υποθέτουμε ότι $l < k$.

$k = \pi l + u$ με $u < l$

$a^k \equiv b^k \mod n \Rightarrow 1 \equiv (b^l)^\pi b^u \mod n \Rightarrow$

$\Rightarrow b^u \equiv 1 \mod n$ με $\underline{u < l}$

αδύνατο

άρα, $ord_n(a) = ord_n(b)$

<u>ΠΡΟΤΑΣΗ</u>

$a \in \mathbb{Z}^*$, $n > 1$ φυσικός με $(a,n)=1$. Αν $ord_n(a) = s$, τό

1) $a^m \equiv a^k \mod n \Rightarrow \underline{m \equiv k \mod s}$

2) $a^m \equiv 1 \mod n \Rightarrow s | m$

<u>Απόδειξη</u>

1) Υποθέτουμε ότι δεν ισχύει η (+).

$m - k = \pi s + u$ με $u < s$

$a^{m-k} = a^{\pi s + u} \Rightarrow a^{m-k} = a^{\pi s} \cdot a^u \mod n$

$a^{m-k} = a^u \mod n \Rightarrow a^m (a^k)^{-1} \equiv a^u \mod n \xRightarrow{(++)}$

$1 \equiv a^u \mod n$ με $u < s$. <u>Άτοπο</u>

Άρα, $m \equiv k \mod s$

2) $a^m \equiv 1 \bmod n \Rightarrow a^m \equiv a^s \bmod n \Rightarrow m \equiv s \bmod s \equiv 0 \bmod s$
$\Rightarrow s | m$

Πόρισμα
$ord_n(a) | \varphi(n)$
Όταν θέλουμε να βρούμε τάξεις εξετάζουμε τους διαιρέτες του $\varphi(n)$.

$a^m \equiv a^k \bmod n$
$\Rightarrow m \equiv k \bmod s$
$s = ord_n(a)$

Π.χ. Να βρεθεί $ord_{11}(8^{1998})$

$\varphi(11) = 11 - 1 = 10$
Άρα, Euler $\Rightarrow 8^{10} \equiv 1 \bmod 11$
Πιθανόν να υπάρχει $s < 10$ με $s | 10$ ώστε
$ord_{11} 8 = s$ $\quad s|10 \Rightarrow s = 1, 2, 5, 10$

$8^2 = 64 \bmod 11 = -2$
$8^5 = 8^2 \cdot 8^2 \cdot 8 \equiv (-2)(-2) \cdot 8 \bmod 11 =$
$32 \bmod 11 \equiv -1 \bmod 11 \Rightarrow ord_{11}(8) = 10$
$8^{1998} = 8^{199 \cdot 10 + 8} \equiv 1 \cdot 8^8 \bmod 11$
$\equiv 8^5 \cdot 8^3 \equiv 8^5 \cdot 8^2 \cdot 8 \bmod 11 =$
$= (-1) \cdot (-2) \cdot 8 \equiv 16 \bmod 11$
$\equiv 5 \bmod 11$

$ord_{11}(5) = \cancel{1}, \cancel{2}, 5, \cancel{10}$

$5^2 \equiv 3 \bmod 11 \quad 5^2 \cdot 5 \cdot 5 \equiv 3 \cdot 3 \cdot 5 \equiv 1 \bmod 5$

$ord_{11}(5) = 5 = ord_{11}(8^{1999})$

Συστήματα Γραμμικών Εξισώσεων

$ax \equiv b \bmod n$

1) $(a,n)=1 \mid b \Rightarrow$ Έχει μοναδική λύση

2) $(a,n)=\delta \neq 1$ Αν $\delta \mid b \Rightarrow$ έχει λύσεις

$\frac{a}{\delta}x \equiv \frac{b}{\delta} \bmod \frac{n}{\delta}$ έχει μοναδική λύση $x_0 \bmod \frac{n}{\delta}$

$\Rightarrow$ Γενική λύση : $x_0, x_0+\frac{n}{\delta}, x_0+\frac{2n}{\delta}, \dots, x_0+\frac{(\delta-1)n}{\delta}$ $\bmod n$

Ζητάμε τη λύση ενός συστήματος

$x \equiv 2 \bmod 3 \Rightarrow x = 2+3k$ (+)

$x \equiv 1 \bmod 5 \Rightarrow 2+3k \equiv 1 \bmod 5$

$\Rightarrow 3k \equiv 4 \bmod 5$

$(3,5)=1 \Rightarrow$ Μοναδική

$\Rightarrow \exists [3]_5^{-1} = [2]_5$

$3k \equiv 4 \bmod 5 \Rightarrow 2\cdot 3k \equiv 2\cdot 4 \bmod 5 \Rightarrow k \equiv 8 \bmod 5 \equiv 3 \bmod 5$

$k = 3+5\ell$ (++)

(+) και (++) $\Rightarrow$

$x = 2+3k = 2+3(3+5\ell) = 11+3\cdot 5\ell$

$x = 11+3\cdot 5\cdot \ell$

$3\cdot 5 = [3,5]$

$x \equiv 11 \bmod [3,5] \equiv 11 \bmod 15$

Εφαρμογή στο Κινέζικο Θεώρημα

$x \equiv 2 \bmod 3 \longleftarrow m_1 = 3$
$x \equiv 1 \bmod 5 \longleftarrow m_2 = 5$

$M = [3,5] = 3 \cdot 5 = 15$

$\frac{M}{m_1} = m_2$

$(m_1, m_2) = 1 \Rightarrow \exists$ αντίστροφος m_2 στο $\bmod m_1$
Ονομάζουμε τον αντίστροφο c_1

$c_1 \frac{M}{m_1} \equiv 1 \bmod m_1$

$\frac{M}{m_2} = m_1$ και $c_2 \frac{M}{m_2} \equiv 1 \bmod m_2$

$x = \left(c_1 \frac{M}{m_1} a_1 + c_2 \frac{M}{m_2} a_2 \right) \bmod M$

$c_1 \cdot 5 \equiv 1 \bmod 3 \Rightarrow c_1 \cdot 2 \equiv 1 \bmod 3 \Rightarrow c_1 \equiv 2 \bmod 3$
$c_2 \cdot 3 \equiv 1 \bmod 5 \qquad c_2 = 2$
$x = (2 \cdot 5 \cdot 2 + 2 \cdot 3 \cdot 1) \bmod 15$
$x \equiv 26 \bmod 15 \equiv 11 \bmod 15$

Επαλήθευση

$11 \bmod 3 \equiv 2$ ✓ γιατί $x \equiv 2 \bmod 3$
$11 \bmod 5 \equiv 1$ ✓ $\qquad x \equiv 1 \bmod 5.$

Θεώρημα (Κινέζικο Θεώρημα) SOS

Έστω ότι οι φυσικοί $m_1, \dots, m_k$ είναι πρώτοι ανά δύο, $(m_i, m_j) = 1$ για $i \neq j$.
Τότε το σύστημα
$$\left.\begin{array}{l} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \vdots \\ x \equiv a_k \bmod m_k \end{array}\right\} (+)$$

έχει μοναδική λύση $\bmod (m_1, \dots, m_k)$. Δηλαδή υπάρχει x_0 με $x_0 \equiv a_i \bmod m_i$ και αν x_0' είναι επίσης λύση τότε $x_0 \equiv x_0' \bmod (m_1, \dots, m_k)$.

$m_1 m_2 \dots m_k = ΕΚΠ(m_1, \dots, m_k)$

Απόδειξη Αλγόριθμος εύρεσης λύσης

$M = m_1 \dots m_k = ΕΚΠ(m_1, \dots, m_k)$ γιατί είναι πρώτοι μεταξύ τους.

Για κάθε i βρίσκουμε c_i ως εξής:
(++) $c_i \frac{M}{m_i} \equiv 1 \bmod m_i$. Αυτά τα c_i υπάρχουν γιατί

$$\left(\frac{M}{m_i}, m_i\right) = 1$$

Ορίζουμε το x_0

$$x_0 = \left(a_1 c_1 \frac{M}{m_1} + a_2 c_2 \frac{M}{c_2} + \dots + a_k c_k \frac{M}{m_k}\right) \bmod M$$

Να εξετάσουμε ότι είναι πράγματι λύση
Πρέπει να ικανοποιεί τις (+).

Για $i=1$
$$x_0 \bmod m_1 \equiv \left(a_1 c_1 \frac{M}{m_1} + a_2 c_2 \frac{M}{m_2} + \dots + a_k c_k \frac{M}{m_k}\right) \bmod m_1$$

$$\equiv \underbrace{a_1 c_1 \frac{M}{m_1} \bmod m_1}_{(*)} + \cancel{a_2 c_2 \frac{M}{m_2} \bmod m_1}^{\to 0} + \cancel{\dots} + \cancel{a_k c_k \frac{M}{m_k} \bmod m_1}^{\to 0}$$

$$\equiv a_1$$

$$\equiv a_1 1 \bmod m_1$$

$$\frac{M}{m_i} \bmod m_i \equiv \boxed{\frac{m_1 m_2 \dots m_k}{m_i}} \bmod m_i \equiv 0$$

Υποθέτουμε ότι έχουμε και άλλη μία λύση $\bmod M$ x_0 και x_0' $\Big|$ $x_0 \equiv a_i \bmod m_i$ $\quad \forall i = 1, \dots, k$

$x_0' \equiv a_i \bmod m_i$

$x_0 - x_0' \equiv 0 \bmod m_i \Rightarrow m_i \mid x_0 - x_0'$ για όλα τα $i = 1, \dots, k$.

$(m_i, m_j) = 1$

Άρα $m_1 m_2 \dots m_k \mid x_0 - x_0' \Leftrightarrow x_0 - x_0' \equiv 0 \bmod M$

$\Leftrightarrow x_0 \equiv x_0' \bmod M$

Π.Χ. Να λυθεί το σύστημα

$$x \equiv 2 \bmod 3$$
$$x \equiv 3 \bmod 5$$
$$x \equiv 2 \bmod 7$$

$$M = 3 \cdot 5 \cdot 7 = 105$$

$c_1 \frac{M}{m_1} \equiv 1 \bmod 3 \Rightarrow c_1 \frac{\cancel{3} \cdot 5 \cdot 7}{\cancel{3}} \bmod 3 \equiv c_1 \cdot 2 \bmod 3 \Rightarrow c_1 \equiv 2 \bmod 3$

$c_2 \frac{M}{m_2} \equiv 1 \bmod 5 \Rightarrow c_2 \frac{3 \cdot 5 \cdot 7}{5} \bmod 5 \equiv c_2 \cdot 1 \cdot \bmod 5 \Rightarrow c_2 = 1 \bmod 5$

$c_3 \frac{N}{m_3} \equiv 1 \bmod 7 \Rightarrow c_3 \frac{3\cdot 5\cdot 7}{7} \bmod 7 \equiv c_3 \cdot 1 \bmod 7 \Rightarrow c_3 \equiv 1 \bmod 7$

$x_0 \equiv \left(a_1 c_1 \frac{N}{m_1} + a_2 c_2 \frac{N}{m_2} + a_3 c_3 \frac{N}{m_3}\right) \bmod N$

$x_0 \equiv (2\cdot 2\cdot 5\cdot 7 + 3\cdot 1\cdot 3\cdot 7 + 2\cdot 1\cdot 3\cdot 5) \bmod 105 \equiv 23 \bmod 105$

Π.Χ. Να λυθεί το σύστημα.

Δεν μπορεί να εφαρμόσω το Κινέζικο θεώρημα γιατί (8,12) δεν είναι πρώτοι μεταξύ τους

$x \equiv 3 \bmod 8$
$x \equiv 7 \bmod 12$

Έχει λύση;

Αν x_0 είναι λύση $\quad x_0 \equiv 3 \bmod 8$
$\quad x_0 \equiv 7 \bmod 12$

$$\left.\begin{array}{l} x_0 = 3+8k \\ x_0 = 7+12l \end{array}\right\} \Rightarrow \begin{array}{l} 7-3 = 12l-8k \\ 4 = 12l - 8k \end{array}$$

Επειδή $(8,12) \mid 3-7$ έχουμε λύση.

$$\left.\begin{array}{l} x = 3+8k \\ x = 7+12l \end{array}\right\} \Rightarrow 3+8k = 7+12l \Rightarrow 12l' + 8k = 4$$ και λύνουμε τη Διοφαντική

Λύνεται γιατί $(12,8) \mid 4$

$l_0' = 1 \quad k_0 = -1$

$12 - 8 = 4$

$$\left.\begin{array}{l} l' = 1+8t \\ k = 1-12t \end{array}\right\} (**)$$

$(*)$ και $(**) \Rightarrow x = 3+8(-1-12t) = 3-8-8\cdot 12t = -5-8\cdot 12t$

$\Rightarrow \boxed{x = -5-8\cdot 12t}$

Επαλήθευση

$-5-8\cdot 12t \bmod 8 \equiv 3$ ✓

$-5-8\cdot 12t \bmod 12 \equiv 7$ ✓