

9/12/15

Τότε $\text{ord}_n(a) = S \Leftrightarrow S$ ο μικρότερος πολλαπλάσιος του $\phi(n)$ ώστε $a^S \equiv 1 \pmod{n}$

Πρωταρχική ρίζα: α πρωταρχική ρίζα $\pmod{n}$ αν $\text{ord}_n(a) = \phi(n) \Rightarrow$ κάθε αντιστρέφεται κλάση $\pmod{n}$ να γράφεται σαν S όπου $a^S \equiv x \pmod{n}$ αν x αντιστρέφεται, τότε $f(x) = a^x \pmod{n}$

Π.χ. $\text{ord}_{36}(5) = ?$

$(5, 36) = 1 \Rightarrow 5$ είναι αντιστρέφεται κλάση

$$\phi(36) = \phi(2^2 \cdot 3^2) = 2\phi(2) \cdot 3\phi(3) = 12$$

$$\text{ord}_{36}(5) \mid 12 \Rightarrow \text{ord}_{36}(5) = 2, 3, 4, 6, 12$$

$$5^2 = 25 \not\equiv 1 \pmod{36}$$

$$5^3 = 125 \equiv 17 \pmod{36}$$

$$5^4 \equiv 17 \cdot 5 \pmod{36} = 85 \pmod{36} \equiv 13 \pmod{36}$$

$$5^5 \equiv 13 \cdot 5 \pmod{36} = 65 \pmod{36} \equiv 29$$

$$5^6 \equiv 29 \cdot 5 \pmod{36} \equiv 1 \pmod{36}$$

$$\text{άρα } \text{ord}_{36}(5) = 6$$

$$\text{ord}_{11}(3) = 10$$

$$\varphi(11) = 10 \Rightarrow 8 \text{ primitive root mod } 11$$

$$3 \bmod 11 = 3, 3^2 \bmod 11 = 9, 3^3 \bmod 11 = 27 \bmod 11 = 5, 3^4 \bmod 11 = 15 \bmod 11 = 4, 3^5 \bmod 11 = 12 \bmod 11 = 1$$

$$3^2 \bmod 11 = 9, 3^4 \bmod 11 = 4, 3^5 \bmod 11 = 1$$

$$3^4 \bmod 11 = 4, 3^5 \bmod 11 = 1$$

$$3^5 \bmod 11 = 1, 3^{10} \bmod 11 = 1$$

$$3^{10} \bmod 11 = 1$$

$$\text{ord}_{11}(8) = 10$$

$$8^{10} \bmod 11 = 1 \Rightarrow 2015 = 201 \cdot 10 + 5$$

$$8^{2015} \bmod 11 = (8^{10})^{201} \cdot 8^5 \bmod 11 = 1 \cdot 8^5 \bmod 11$$

$$\text{ord}_{11}(8) = 10$$

$$8^{10} \bmod 11 = 1 \Rightarrow 2015 = 201 \cdot 10 + 5$$

$$(8^5)^2 \bmod 11 = 1 \Rightarrow \text{ord}_{11}(8^5) = 2$$

Συνάρτηση Γραμμικών Τυποτήτων

1. $x \cdot 2x \equiv 1 \pmod{3}$

$(2, 3) = 1 \Rightarrow 2$ αντιστροφή $\Rightarrow \exists b \text{ τέτοια } 2b \equiv 1 \pmod{3}$
 $\Rightarrow b = 2$

$2x \equiv 1 \pmod{3} \Rightarrow 2 \cdot 2x \equiv 2 \cdot 1 \pmod{3} \Rightarrow$

$\boxed{x \equiv 2 \pmod{3}} \Rightarrow \boxed{x = 2 + 3k} \quad k \in \mathbb{Z}$

2. x Να βρούμε το σύνολο όλων αριθμών

$2x \equiv 1 \pmod{3} \Leftrightarrow x \equiv 2 \pmod{3}$

$3x \equiv 3 \pmod{5} \wedge 3^{-1} \pmod{5} \quad 3^{-1} = 2 \pmod{5} \Rightarrow 2 \cdot 3x \equiv 2 \cdot 3 \pmod{5}$

$4x \equiv 3 \pmod{5} \Rightarrow x \equiv 1 \pmod{5}$

$\hookrightarrow \exists 4^{-1} \pmod{7} \quad 4^{-1} = 2 \pmod{7} \Rightarrow 2 \cdot 4x \equiv 2 \cdot 3 \pmod{7}$
 $\Rightarrow x \equiv 6 \pmod{7}$

Το γενικευμένο σύνολο είναι το σύνολο x τέτοιο

$x \equiv 2 \pmod{3} \Leftrightarrow x = 2 + 3k$

$x \equiv 1 \pmod{5} \Leftrightarrow 2 + 3k = 1 + 5\lambda \Rightarrow 2 + 3k \equiv 1 \pmod{5}$

$x \equiv 6 \pmod{7}$

$\Rightarrow$

• $x \equiv 2 \pmod{3} \Leftrightarrow x = 2 + 3k$

• $x \equiv 1 \pmod{5} \Leftrightarrow 2 + 3k = 1 + 5\lambda \Rightarrow 2 + 3k \equiv 1 \pmod{5}$

$\Rightarrow 3k \equiv -1 \pmod{5} \equiv 4 \pmod{5}$

$\Rightarrow 2 \cdot 3 \equiv 6 \pmod{5} \Rightarrow k \equiv 3 \pmod{5}$

$k \equiv 3 \pmod{5} \Rightarrow k = 3 + 5\lambda \xrightarrow{+} x = 2 + 3(3 + 5\lambda) = 11 + 15\lambda \quad (+)$

• $x \equiv 6 \pmod{7}$

$x = 11 + 15\lambda \quad \left\{ \begin{array}{l} \Rightarrow 11 + 15\lambda \equiv 6 \pmod{7} \Rightarrow 15\lambda \equiv -5 \pmod{7} \equiv 2 \pmod{7} \\ x \equiv 6 \pmod{7} \end{array} \right.$

$15\lambda \equiv 2 \pmod{7} \Rightarrow \lambda \equiv 2 \pmod{7} \Rightarrow \lambda = 2 + 7\delta, \delta \in \mathbb{Z}$

$$(7) \Rightarrow x = 11 + 15\lambda = 11 + 15(2 + 7\lambda) = 11 + 30 + 105\lambda$$

$$\text{Γενοίκεται } x = 41 + 105\lambda, \lambda \in \mathbb{Z}$$



$$x \equiv 41 \pmod{105}$$

Όχι, πιο μικρό modulo
πιο μικρό είναι!

$$\text{Ερμ. } \Pi(3, 5, 7) = 105$$

Γενική Περίπτωση

Να ληθεί το σύστημα

$$a_1 x \equiv b_1 \pmod{n_1}$$

$$a_2 x \equiv b_2 \pmod{n_2}$$

$$a_k x \equiv b_k \pmod{n_k}$$

$$x \equiv c_1 \pmod{n_1}$$

$$\Rightarrow x \equiv c_2 \pmod{n_2}$$

$$x \equiv c_k \pmod{n_k}$$

$$a_1 x \equiv b_1 \pmod{n_1}$$

$$2x \equiv 4 \pmod{6}$$

$$2x - 4 \equiv 6\lambda \Rightarrow x - 2 \equiv 3\lambda \quad x \equiv 2 \pmod{3}$$

Η εξίσωση $a_i x \equiv b_i \pmod{n_i}$ έχει λύση αν
(a_i, n_i) / b_i

Θεώρημα (Κινέζικο)

Έστω ότι οι φυσικοί $n_1, \dots, n_k$ είναι πρώτοι ανά δύο,
(n_i, n_j) $\neq 1$). Τότε το σύστημα έχει μοναδική λύση
 $\pmod{n_1 n_2 \dots n_k}$. Ανάσκη αν x_0 είναι μία λύση τότε
κάθε $a \equiv x_0 \pmod{n_1 n_2 \dots n_k}$ είναι λύση.

Απόδειξη

$$\text{Επειδή } (n_i, n_j) = 1 \ (i \neq j) \Rightarrow$$

$$\text{Εχουμε } (n_1^2, \dots, n_k) = n_1 \cdot n_2 \cdot \dots \cdot n_k = N$$

$$\text{Για κάθε } i \text{ ισχύει } \left(\frac{N}{n_i}, n_i \right) = 1 \Rightarrow$$

(γιατί)

$$\exists d_i \text{ με } d_i \frac{N}{n_i} \equiv 1 \pmod{n_i} \quad (1)$$

Θα δείξουμε ότι το $x_0 = d_1 \frac{N}{n_1} c_1 + d_2 \frac{N}{n_2} c_2 + \dots + d_k \frac{N}{n_k} c_k$ είναι λύση του συστήματος.

Αντικαθιστώντας το έχουμε

$$x_0 \equiv c_1 \pmod{n_1}$$

$$x_0 \pmod{n_i} = \left(d_1 \frac{N}{n_1} c_1 + d_2 \frac{N}{n_2} c_2 + \dots + d_k \frac{N}{n_k} c_k \right) \pmod{n_i}$$

$$\equiv d_i \frac{N}{n_i} \pmod{n_i} \equiv 1 c_i \pmod{n_i} \equiv c_i \pmod{n_i}$$

Άρα την ικανοποιεί.

Η λύση του συστήματος είναι $x_0 \pmod{N}$.

Ας υποθέσουμε ότι η x' είναι μία άλλη λύση.

Άρα ισχύει $x' \equiv c_i \pmod{n_i}$ για όλα τα i .

$x' - x_0 \equiv 0 \pmod{n_i}$ για όλα τα i και

$$(n_1, n_2) = 1 \Rightarrow$$

$$x' - x_0 \equiv 0 \pmod{N} \Leftrightarrow x' \equiv x_0 \pmod{N}$$

π.χ. $N = 105$, αν δίνονται, το σύστημα

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$\text{Για να έχει λύση } (3, 5) = 1 = (5, 7) = (3, 7)$$

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

$$\frac{N}{n_1} = \frac{105}{3} = 35 \pmod{3} \equiv d_1 \cdot 2 \pmod{3} \equiv d_1 = 2$$

$$d_2 \frac{N}{n_2} = d_2 21 \pmod{5} \equiv d_2 \pmod{5} \quad d_2 = 1$$

$$d_3 \frac{N}{n_3} = d_3 15 \pmod{7} \equiv d_3 \pmod{7} \quad d_3 = 1$$

$$x_0 \equiv d_1 \cdot \frac{N}{n_1} c_1 + d_2 \cdot \frac{N}{n_2} c_2 + d_3 \cdot \frac{N}{n_3} c_3$$

$$= 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 2$$

$$= 140 + 63 + 30 = 233$$

$$\text{Άρα } x_0 \equiv 233 \pmod{105} \equiv 23 \pmod{105}$$

$$\text{Να βρούμε το } x \equiv 3 \pmod{6}$$

$$x \equiv 7 \pmod{12}$$

Δεν εφαρμόζουμε το Κινέζικο!

$$x \equiv 3 \pmod{6} \Leftrightarrow x = 3 + 6k$$

$$3 + 6k \equiv 7 \pmod{12} \Rightarrow 6k \equiv 4 \pmod{12}$$

$$(6, 12) = 6 \mid 4 \xrightarrow{\frac{4}{6}} 2k \equiv 1 \pmod{3}$$

$$2k \equiv 1 \pmod{3} \Rightarrow 2 \cdot 2k \equiv 2 \pmod{3} \Rightarrow$$

$$k \equiv 2 \pmod{3} \Rightarrow k = 2 + 3s$$

$$x = 3 + 6k = 3 + 6(2 + 3s) = 15 + 18s$$

$$x = 15 + 18s \quad \eta \quad x \equiv 15 \pmod{18}$$

$$\text{Το } 18 = \text{Ε.Κ.Π.}(6, 12)$$

Θεώρημα (χρησις ασκήσεως)

Έστω το σύστημα $x \equiv a_i \pmod{n_i} \quad i=1, \dots, k$

Αυτό έχει λύση $\Leftrightarrow (n_1, \dots, n_k) \mid a_i - a_j$ για όλα τα i, j . Αν το είναι για λύση, τότε υπάρχει λύση $x \pmod{\text{Ε.Κ.Π.}(n_1, \dots, n_k)}$

Π.χ. Να βρούμε, αν δίνεται, το σύστημα:

$$x \equiv 11 \pmod{21}$$

$$x \equiv 4 \pmod{10}$$

$$x \equiv 2 \pmod{12}$$

Δεν μπορούμε να εφαρμόσουμε το Κινημα

$$(2, 10) \mid 11-4 \quad \checkmark$$

$$(2, 12) = 3 \mid 11-2 = 9 \quad \checkmark$$

$$(10, 12) = 2 \mid 4-2 = 2 \quad \checkmark$$

Έχουμε άρα B.p.c. > μν!

$$\text{EKΠ}(2, 10, 12) = \text{EKΠ}(3, 2, 3) = 2^2 \cdot 3 \cdot 2$$

$$\begin{array}{l} x \equiv 11 \pmod{21} \\ x \equiv 4 \pmod{10} \end{array} \xrightarrow[\text{Κινημα}]{\text{ME}} \begin{array}{l} N = 21 \cdot 10 \dots \text{όχι } 110 \pmod{21} \equiv 1 \Rightarrow d_1 = 19 \\ 21 = 2 \cdot 10 + 1 \Rightarrow 1 = 21 - (2) \cdot 10 \end{array}$$

$$d_2 \cdot 21 \equiv 1 \pmod{10} \Rightarrow d_2 = 1$$

$$x_0 = 19 \cdot 10 \cdot 11 + 1 \cdot 21 \cdot 4 = 19 \cdot 110 + 84 = 2090 + 84 = 2174$$

$$x \equiv 2174 \pmod{210} \equiv 74 \pmod{210}$$

$$x \equiv 2 \pmod{12}$$

$$x = 2 + 12k \equiv 74 \pmod{210} \Rightarrow 12k \equiv 72 \pmod{210}$$

$$6k \equiv 36 \pmod{105}$$

$$2k \equiv 12 \pmod{35}$$

$$18 \cdot 2k \equiv 18 \cdot 12 \pmod{35}$$

$$k \equiv 18 \cdot 12 \pmod{35}$$

$$k \equiv 18 \cdot 12 + 35t$$

$$\begin{array}{l} x = 2 + 12k \\ k = 18 \cdot 12 + 35t \end{array} \xrightarrow{\quad} \begin{array}{l} x = 2 + 12(18 \cdot 12 + 35t) \end{array}$$

$$x_0 = 2 + 12^2 \cdot 18 + 35 \cdot 12t \quad t \in \mathbb{Z}$$