

6) Ένας αριθμός διαμετρεμένος με το 4 είναι της μορφής
 $n = 4k + u$, $u = 0, 1, 2, 3$

Τώρα, το $n = 4k$ δεν είναι πρώτος

το $n = 4k + 2$ " " " "

Τώρα, το $n = 4k + 1$ δεν χωρίζεται εάν είναι πρώτος

το $n = 4k + 3$ " " " " "

Άλλοι πρώτοι μορφής $4k + 3$

Υποθέτουμε ότι οι πρώτοι μορφής $4k + 3$ είναι
πεπερασμένοι αριθμούς

$p_0 = 3, p_1, p_2, \dots, p_k$

Έστω $4p_1 p_2 \dots p_k + 3 \in \mathbb{N}$ και αναλύεται σε

γινόμενο $4p_1 p_2 \dots p_k + 3 = q_1 q_2 \dots q_r$ με

q_i πρώτοι μορφής $4m + 1$ ή $4m + 3$

Ας είναι $q_1 = 2 \Rightarrow q_1 \nmid 3$ Αδύνατον (Αρα, $q_1 \neq 2$)

Ας είναι $q_1 = 3 \Rightarrow 3 \mid 4p_1 \dots p_k \Rightarrow 3 \mid p_i$ $\forall i$ εκ των οποίων. Αδύνατον
επειδή p_i πρώτος > 3

Έστω q_i πρώτος μορφής $4k + 3 \Rightarrow \exists j$ ώστε $q_i = p_j$
 $\Rightarrow p_j \mid 4p_1 \dots p_k \Rightarrow p_j \mid 3$ με $p_j > 3$ Αδύνατον

Αρα, $q_1, \dots, q_r$ είναι πρώτοι μορφής $4m + 1$

$$q_1, q_2, \dots, q_k = (4m_1+1)(4m_2+1)\dots(4m_k+1) = 4A+1$$

$$\text{Αρα, } 4p_1 p_2 \dots p_k + 3 = 4A+1 \Rightarrow 4p_1 p_2 \dots p_k + 2 = 4A \Rightarrow$$

$$\Rightarrow 4 \mid 4p_1 \dots p_k \Rightarrow 4 \mid 2 \text{ Αδύνατον}$$

7) Οα περίοδοι $\text{ord}_{17}(3) \mid \varphi(17) = 16$

$$1, 2, 4, 8, 16$$

$$3, 9, 13, -1, 1$$

$$81 \bmod 17 \equiv 13 \bmod 17$$

$$13 \cdot 13 \bmod 17 \equiv 168 \bmod 17 \equiv 16 \bmod 17 \equiv -1 \bmod 17 \equiv 16 \bmod 17$$

Το 3 συν. είναι γεννητική ρίζα mod 17

$$\{3^0=1, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, 3^{13}, 3^{14}, 3^{15}\}$$

$$\{ \overset{|||}{1}, \overset{|||}{3}, \overset{|||}{9}, \overset{|||}{10}, \overset{|||}{13}, \overset{|||}{5}, \overset{|||}{15}, \overset{|||}{11}, \overset{|||}{16}, \overset{|||}{14}, \overset{|||}{8}, \overset{|||}{7}, \overset{|||}{4}, \overset{|||}{12}, \overset{|||}{2}, \overset{|||}{6} \}$$

8) $7^n \equiv 4 \bmod 17$

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

$$4 \equiv 3^{12} \bmod 17 \Rightarrow 3^{11n} \equiv 3^{12} \bmod 17 \Rightarrow 11n \equiv 12 \bmod 16$$

$\text{ord}_{17}(3) = 16$ (1)

Η (1) έχει μοναδική λύση εάν $(11, 16) = 1$

Ζητάμε $\alpha \bmod 16$ ώστε $11\alpha \equiv 1 \bmod 16$

$$11 \cdot 3 \equiv 33 \bmod 16 \equiv 1 \bmod 16$$

$$11n \equiv 12 \bmod 16 \Rightarrow 3 \cdot 11n \equiv 36 \bmod 16 \Rightarrow n \equiv 4 \bmod 16 \Leftrightarrow$$

$$\Leftrightarrow n = 4 + 16k$$

9) Εστω $(2^n + 3^n) \equiv 0 \bmod 17 \Rightarrow 2^n \equiv -3^n \bmod 17$

$$n \text{ περιττός} \Rightarrow -3^n \equiv (-3)^n \bmod 17$$

$$2 \equiv 3^{14} \bmod 17 \Rightarrow 2^n \equiv 13^{14n} \bmod 17$$

$$-3^n \equiv -1 \cdot 3^n \equiv 3^8 \cdot 3^n \bmod 17 \equiv 3^{8+n} \bmod 17$$

$$\Rightarrow 3^{14n} \equiv 3^{8+n} \bmod 17 \Rightarrow 14n \equiv (8+n) \bmod 16 \Rightarrow$$

$$\Rightarrow 13n \equiv 8 \bmod 16 \Rightarrow 13^{-1} \bmod 16$$

$$(13, 16) = 1$$

$$n \equiv -1 \cdot 3^{-1} \cdot 8 \pmod{16} \equiv 5 \cdot 8 \pmod{16} \equiv 8 \pmod{16}$$

Αρα, $n \not\equiv 8 \pmod{16}$. Δηλ. για $n \not\equiv 8 \pmod{16}$ ισχύει $2^n + 3^n \equiv 0 \pmod{17}$

ΚΙΝΕΖΙΚΟ ΘΕΩΡΗΜΑ

Εάν $(a, n) = 1$ τότε η εξίσωση $ax \equiv b \pmod{n}$ έχει μοναδική λύση $\pmod{n}$:

$$x \equiv a^{q(n)-1} \cdot b \pmod{n}$$

Αν $(a, n) = \delta$ τότε η εξίσωση $ax \equiv b \pmod{n}$ έχει λύση αν-ν $\delta | b$. Αν x_0 είναι μία λύση τότε οι λύσεις δίνονται από:

$$x_0, x_0 + \frac{n}{\delta}, x_0 + \frac{2n}{\delta}, \dots, x_0 + \frac{(\delta-1)n}{\delta} \pmod{n}$$

Λύση:

Να λυθεί το σύστημα

$$x \equiv 2 \pmod{3} \quad (1)$$

$$x \equiv 1 \pmod{5} \quad (2)$$

Λύση

Εστω x_0 μία λύση $\Rightarrow x_0 \equiv 2 \pmod{3} \equiv 1 \pmod{5}$

$$x_0 = 2 + 3k \Rightarrow 0 = (2-1) + 3 - 5\lambda \Rightarrow 0 = 1 + 3k - 5\lambda \Rightarrow$$

$$x_0 = 1 + 5\lambda \Rightarrow -3k + 5\lambda = -1 \quad (3, 5) = 1 \text{ Άρα υπάρχουν}$$

Για των (1) $x_0 \in \{2, 2+3, 2+2 \cdot 3, 2+3 \cdot 3, \dots\} = A$

Για των (2) $x_0 \in \{1, 1+5, 1+2 \cdot 5, 1+3 \cdot 5, \dots\} = B$

Δηλ $x_0 \in A \cap B$.

$$x \equiv 2 \pmod{3} \Rightarrow \boxed{x = 2 + 3k} \quad (3)$$

$$3k + 2 \equiv 1 \pmod{5} \Rightarrow 3k \equiv -1 \pmod{5} \Rightarrow 3k \equiv 4 \pmod{5} \Rightarrow 2 \cdot 3k \equiv 2 \cdot 4 \pmod{5}$$

$$\Rightarrow (3, 5) = 1 \Rightarrow \exists 3^{-1} \pmod{5}$$

$$6k \equiv 8 \pmod{5} \Rightarrow k \equiv 3 \pmod{5} \Rightarrow k = 3 + 5m, m \in \mathbb{Z}$$

$$(3) \rightarrow x = 2 + 3(3 + 5m) = 2 + 9 + 15m = 11 + 15m$$

Οπου $\text{Εκν } [3, 5] = 15$ Η λύση βρίσκεται $\pmod{[3, 5]}$

$$\left[\frac{3, 5}{3} \right] C_1 \equiv 1 \pmod{3} \Rightarrow 5C_1 \equiv 1 \pmod{3} \Rightarrow 2C_1 \equiv 1 \pmod{3} \Rightarrow C_1 \equiv 2 \pmod{3}$$

$$\frac{[3,5]}{5} C_2 \equiv 1 \pmod{5} \Rightarrow 3 C_2 \equiv 1 \pmod{5} \Rightarrow C_2 \equiv 2 \pmod{5}$$

$$X_0 = \frac{[3,5]}{3} a_1 + \frac{[3,5]}{5} C_2 \cdot d_2 = 5 \cdot 2 \cdot 2 + 3 \cdot 2 \cdot 1 =$$

$$\equiv 26 \pmod{[3,5]} \equiv 26 \pmod{15} \equiv 11 \pmod{15}$$

Αναπαράδειγμα (για το κινέζικο θεωρήμα)

Να λυθεί το σύστημα:

$$x \equiv 3 \pmod{8}$$

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

Λύση

$$x \equiv 3 \pmod{8} \Rightarrow x = 8k + 3$$

$$x \equiv 7 \pmod{12} \Rightarrow 8k + 3 \equiv 7 \pmod{12} \Rightarrow 8k \equiv 4 \pmod{12} \Rightarrow$$

$$\Rightarrow 8k = 4 + 12\lambda \Rightarrow 2k = 3\lambda + 1 \Rightarrow 2 \cdot 2k = 2 \cdot 1 \pmod{3}$$

$$4k \equiv 2 \pmod{3} \Rightarrow k \equiv 2 \pmod{3} \Rightarrow k = 2 + 3\lambda'$$

$$2k = 2(2 + 3\lambda') = 4 + 6\lambda' = 1 + 3 + 6\lambda' = 1 + 3(1 + 2\lambda')$$

$$\text{Άρα, } x = 3 + 8k = 3 + 8(2 + 3\lambda') = 3 + 16 + 3 \cdot 8\lambda' = 19 + 24\lambda'$$

$$\text{Ή } 24 = [8, 12]$$

Κινέζικο Θεώρημα Υπολοίπων:

Έστω ότι οι φυσικοί $m_1, \dots, m_k$ είναι πρώτοι ανά δύο (δηλ. $(m_i, m_j) = 1$ για $i \neq j$). Τότε το σύστημα

$$\begin{array}{l|l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_k \pmod{m_k} \end{array} \quad \left| \begin{array}{l} \text{Έχει μοναδική λύση} \\ \pmod{[m_1, \dots, m_k]} = \pmod{(m_1, \dots, m_k)} \end{array} \right.$$

Αν x_0 λύση, τότε λύση θα είναι $x_0 \pmod{(m_1, \dots, m_k)}$

Απόδειξη

Επειδή $(m_i, m_j) = 1 \Rightarrow [m_1, \dots, m_k] = m_1 \dots m_k = M$. Τότε

για κάθε $\frac{M}{m_i}$ θα $\exists c_i$ ώστε $\frac{M}{m_i} c_i \equiv 1 \pmod{m_i}$

ΟΔΟ $x_0 \in \mathbb{Z}$ τότε με

$$x_0 = \frac{M}{m_1} c_1 d_1 + \dots + \frac{M}{m_k} c_k d_k \text{ αποτελεί λύση του συστήματος}$$

$\text{mod } M$. Εξ επαγωγής αν το x_0 αποτελεί λύση

$$x_0 \equiv a_i \pmod{m_i} \Rightarrow \left(\frac{M}{m_1} c_1 d_1 + \dots + \frac{M}{m_k} c_k d_k \right) \pmod{m_i} \quad (1)$$

$$\text{Αλλά, } \left(\frac{M}{m_i} = \frac{m_1 \dots m_i \dots m_k}{m_i} \right) \pmod{m_i} \equiv 0 \Rightarrow \left(\frac{M}{m_i} = \frac{m_1 \dots m_i \dots m_k}{m_i} \right) \pmod{m_i} \neq 0$$

Άρα, (1) όλα μηδενίζονται εκτός του $\frac{M}{m_i} c_i d_i$, άρα

$$M \text{ (1) λύση με: } \frac{M}{m_i} c_i d_i \pmod{m_i} \equiv 1 \cdot a_i \pmod{m_i} \equiv a_i \pmod{m_i}$$

Δηλ.ο x_0 επαληθεύει κάθε εξίσωση

Άρα λύση.

Έστω x_0' μια άλλη λύση $\text{mod } M$

$$\left. \begin{array}{l} x_0 \equiv a_i \pmod{m_i} \\ x_0' \equiv a_i \pmod{m_i} \end{array} \right\} \Rightarrow \left. \begin{array}{l} x_0 - x_0' \equiv 0 \pmod{m_i} \\ \text{για όλα τα } m_i \\ (m_i, m_j) = 1 \end{array} \right\} \Rightarrow x_0 - x_0' \equiv 0 \pmod{M}$$

πχ

Να λυθεί το σύστημα:

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

$$x \equiv 1 \pmod{5}$$

$$x \equiv 6 \pmod{7}$$

Λύση

Παρατηρούμε ότι $(3,5)=1=(5,7)=(3,7)$

Άρα, εφαρμόζεται το Θ. του Κινέζου

$$[3,5,7]=3 \cdot 5 \cdot 7 = 105 = M$$

Θα βρούμε τα c_1, c_2, c_3 όπως στο θεωρήμα

$$\bullet \frac{M}{m_1} c_1 = \frac{3 \cdot 5 \cdot 7}{3} c_1 \equiv 1 \pmod{3} \Rightarrow 35 c_1 \equiv 1 \pmod{3} \Rightarrow$$

$$\Rightarrow 2 \cdot c_1 \equiv 1 \pmod{3} \Rightarrow c_1 = 2$$

$$\bullet \frac{M}{m_2} c_2 = 1 \pmod{5} \Rightarrow 37 c_2 \equiv 1 \pmod{5} \Rightarrow c_2 = 1$$

$$\bullet \frac{M}{m_3} C_3 \equiv 1 \pmod{7} \Rightarrow 3 \cdot 5 C_3 \equiv 1 \pmod{7} \Rightarrow C_3 = 1$$

$$X_0 = \frac{M}{m_1} C_1 a_1 + \frac{M}{m_2} C_2 a_2 + \frac{M}{m_3} C_3 a_3 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 1 + 15 \cdot 1 \cdot 6 =$$

$$= 140 + 21 + 90 = 251 \Rightarrow X_0 \equiv 251 \pmod{105} \equiv 41 \pmod{105}$$

Επαλήθευση:

$$41 \equiv 2 \pmod{3} \quad \text{ωχρη}$$

$$41 \equiv 1 \pmod{5} \quad \text{ωχρη}$$

$$41 \equiv 6 \pmod{7} \quad \text{ωχρη}$$

ΘΕΩΡΗΜΑ: Το σύστημα

$$\left. \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{array} \right\} \text{ έχει λύση αν } \forall (m_i, m_j) \mid a_i - a_j \quad \forall i, j$$

Αν x_0 μια λύση, τότε κάθε λύση θα είναι της μορφής
 $x_0 \pmod{M}$ όπου $M = [m_1, \dots, m_k]$

Πχ

Να λυθεί το σύστημα:

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

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

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

ΛΥΣΗ

Δεν εφαρμόζεται το Θ. λυνέται στις 3 mod; $((21, 12) = 3 \neq 1)$

Αλλά, εφαρμόζεται σε 2 από αυτές

Για τις $x \equiv 11 \pmod{21}$ όπου $(21, 10) = 1$

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

$$M = [21, 10] = 210$$

Θα υπολογίσουμε C_1, C_2 ώστε $\frac{M}{m_1} C_1 \equiv 1 \pmod{m_1}$ & $\frac{M}{m_2} C_2 \equiv 1 \pmod{m_2}$

$$10 C_1 \equiv 1 \pmod{21} \quad (\rightarrow \text{ευκλ. αλγ. } 21 = 10 \cdot 2 + 1 \Rightarrow 1 = 21 - 10 \cdot 2)$$

