

25/05/15

$$a \cdot x \equiv b \pmod{n} \quad (*)$$

① $(a, n) = 1 \Rightarrow \eta (*)$ έχει λύν. Άρα υπάρχει $x_0 \equiv b \cdot c \pmod{n}$, όπου $[c]_n = [a]_n^{-1}$

② $\delta = (a, n) \Rightarrow \eta (*)$ έχει ακριβώς δ λύσεις: $x_0, x_0 + \frac{n}{\delta}, \dots, x_0 + (\delta-1) \frac{n}{\delta}$
 όπου $x_0 : n$ του. Άρα μας $\frac{a}{\delta} x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}}$

Φύλλο #8

Άσκηση ② : ① $15x \equiv 9 \pmod{25}$, ③ $980x \equiv 1500 \pmod{1600}$

Λύση: ① $(15, 25) = 5 \nmid 9 \Rightarrow \eta$ ① δεν έχει λύσεις

②: $980 = 2^2 \cdot 5 \cdot 7^2$ και $1600 = 2^6 \cdot 5^2 \Rightarrow (980, 1600) = 20$

Επειδή $20 \nmid 1500 \Rightarrow \eta$ ③ έχει λύσεις και πράγματι
 θα έχει 20 αντίστοιχες λύσεις $\pmod{1600}$

Θεωρούμε τη γραμ. μορφή: $\frac{980}{20} x \equiv \frac{1500}{20} \pmod{\frac{1600}{20}} \Rightarrow$
 $\Rightarrow 49x \equiv 75 \pmod{80}$

Η μοναδική λύση μας ενδιαφέρει θα είναι: $x_0 \equiv 75 \pmod{80}$, όπου:

$[c]_{80} = [49]_{80}^{-1}$. Είναι: $1 = 19 \cdot 80 + (-31) \cdot 49 \Rightarrow [49]_{80}^{-1} = [-31]_{80} =$
 Άρα $c = 49$ τότε: $x_0 \equiv 75 \cdot 49 \pmod{80} = [49]_{80}$

$\Rightarrow x_0 \equiv 3675 \pmod{80} \equiv 75 \pmod{80}$

Άρα όλες οι λύσεις της αρχικής θα είναι:

$75, 75 + \frac{1600}{20}, \dots, 75 + 19 \cdot \frac{1600}{20} \pmod{1600}$

(Σ): $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} : (m_i, m_j) = 1 \text{ αν } 1 \leq i \neq j \leq n.$

Θέτουμε $M = m_1 m_2 \dots m_n$
 $M_i = \frac{M}{m_i}, 1 \leq i \leq n$

b_i : for. λύση στο $M_i x \equiv 1 \pmod{m_i}$

$x \equiv \sum_{i=1}^n M_i b_i \pmod{(m_1, \dots, m_n)}$ είναι η λύση του (Σ) $\pmod{(m_1, \dots, m_n)}$

Άσκηση 7:
$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 5 \pmod{11} \end{cases} \quad (\Sigma)$$

$m_1=2, m_2=3, m_3=5, m_4=7, m_5=11$
 $\alpha_1=1, \alpha_2=2, \alpha_3=3, \alpha_4=4, \alpha_5=5. \Rightarrow$
 $\Rightarrow (m_i, m_j)=1 \text{ αν } i \neq j \leq 5$

$M=2310$, $M_2 = \frac{M}{m_2} = 770, M_4 = 330$
 $M_1 = \frac{M}{m_1} = 1155, M_3 = 462, M_5 = 210$

~~2310x~~ $1155x \equiv 1 \pmod{2} \Rightarrow x \equiv 1 \pmod{2} \leadsto b_1=1$
 $770x \equiv 1 \pmod{3} \Rightarrow 2x \equiv 1 \pmod{3} \leadsto b_2=2$
 $462x \equiv 1 \pmod{5} \Rightarrow 2x \equiv 1 \pmod{5} \leadsto b_3=3$
 $330x \equiv 1 \pmod{7} \Rightarrow x \equiv 1 \pmod{7} \leadsto b_4=1$
 $210x \equiv 1 \pmod{11} \Rightarrow x \equiv 1 \pmod{11} \leadsto b_5=1$

$X_0 \equiv 1155 \cdot 1 \cdot 1 + 770 \cdot 2 \cdot 2 + 462 \cdot 3 \cdot 3 + 330 \cdot 1 \cdot 4 + 210 \cdot 1 \cdot 5 \Rightarrow$
 $\Rightarrow X_0 \equiv 10463 \pmod{2310} \Rightarrow \boxed{X_0 \equiv 1523 \pmod{2310}}$

Άσκηση 6: x_0 : κρυπτός αριθμός, $1 \leq x_0 \leq 100$

Γινόμενοι αριθμοί: α_1 : υπολ. διαμ. του x_0 / ϵ το 3.
 α_2 : -1 / -
 α_3 : -1 / - -1 / - 5. $\Rightarrow$

$$\Rightarrow (\Sigma) \begin{cases} x_0 \equiv \alpha_1 \pmod{3} \\ x_0 \equiv \alpha_2 \pmod{5} \\ x_0 \equiv \alpha_3 \pmod{7} \end{cases} \Rightarrow x_0: \text{αντικαταστήσουμε το } (\Sigma).$$

Επειδή $(3,5)=(3,7)=(5,7)=1 \Rightarrow$ εφάρμοζω Κ.Θ.Υ.

$M=3 \cdot 5 \cdot 7=105$
 $M_1 = 35$
 $M_2 = 21$
 $M_3 = 15$

$$\begin{cases} 35x \equiv 1 \pmod{3} \\ 21x \equiv 1 \pmod{5} \\ 15x \equiv 1 \pmod{7} \end{cases} \Rightarrow \begin{matrix} b_1 = 2 \equiv -1 \pmod{3} \\ b_2 = 1 \\ b_3 = 1 \end{matrix}$$

Αρα
$$X_0 = M_1 b_1 \alpha_1 + M_2 b_2 \alpha_2 + M_3 b_3 \alpha_3 = -35\alpha_1 + 21\alpha_2 + 15\alpha_3$$

$$\Rightarrow \boxed{X_0 = -35\alpha_1 + 21\alpha_2 + 15\alpha_3 \text{ πολλαπλασιάζουμε } (\text{mod } 105)}$$

Εφαρμογή: $x_0 \neq 3$ (κρυπτός), $\alpha_1=1, \alpha_2=3, \alpha_3=3$

$$X_0 = -35 \cdot 1 + 21 \cdot 3 + 15 \cdot 3 = -35 + 108 = 73$$

~~α~~ $\alpha_1=0$
 $\alpha_2=4$
 $\alpha_3=7$

$$\Rightarrow x_0 = -35 \cdot 0 + 21 \cdot 4 + 15 \cdot 7 = 204 \equiv 99 \pmod{105}$$

 (19)

Άσκηση (13): Να υπενθυμίσει ότι ένα καλάνι ανήκει 2, 3, 4, 5, 6 κάθε φορά και να παρατηρήσει ότι είναι: 1, 2, 3, 4, 5 αντίστοιχα κάθε φορά. Αν πάρουμε 7 αυγά, θα είναι τρία στο καλάνι. Να βρεθεί ο ελάχιστος αριθμός αυγών στο καλάνι.

Λύση:
$$(Σ): \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 0 \pmod{7} \end{cases} \Rightarrow \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 0 \pmod{7} \end{cases} \rightarrow \begin{cases} x \equiv 5 \pmod{2} \\ x \equiv 5 \pmod{3} \end{cases} \Rightarrow \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \end{cases}$$

οπότε $(Σ')$:
$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 0 \pmod{7} \end{cases} \xrightarrow{\text{Κ.Θ.Υ.}} n \text{ για } n \text{ είναι } n \text{ } x_0 \equiv 119 \pmod{42}$$

ΘΕΩΡΗΜΑ: Το ελάχιστο γ.π.α. 1602. $(Σ): \begin{cases} x \equiv d_1 \pmod{n_1} \\ \vdots \\ x \equiv d_m \pmod{n_m} \end{cases}$
 έχει λύση $\Leftrightarrow d_{ij} = (n_i, n_j) \mid d_i - d_j$
 $1 \leq i \neq j \leq m$ και τότε η λύση αυτή είναι μοναδική $\pmod{[n_1, \dots, n_m]}$

Παραδείγματα: $(Σ): \begin{cases} x \equiv 7 \pmod{18} \\ x \equiv 10 \pmod{15} \\ x \equiv 1 \pmod{14} \end{cases} \left| \begin{array}{l} d_1 = 7, d_2 = 10, d_3 = 1 \\ n_1 = 18, n_2 = 15, n_3 = 14. \\ d_{12} = (18, 15) = 3 \\ d_{13} = (18, 14) = 2 \quad d_{23} = (15, 14) = 1 \end{array} \right.$

$$d_1 - d_2 = 7 - 10 = -3$$

$$d_1 - d_3 = 7 - 1 = 6$$

$$d_2 - d_3 = 10 - 1 = 9$$

$$d_{12} \mid d_1 - d_2$$

$$d_{13} \mid d_1 - d_3$$

$$d_{23} \mid d_2 - d_3$$

$$(Σ_1): \begin{cases} x \equiv 7 \pmod{18} \\ x \equiv 10 \pmod{15} \end{cases} \Rightarrow$$

$$\Rightarrow 18 \mid x - 7 \Rightarrow x - 7 = 18 \cdot t, \text{ για } t \in \mathbb{Z} \text{ και τότε: } x = 18 \cdot t + 7$$

$$\Rightarrow 18 \cdot t + 7 \equiv 10 \pmod{15} \Rightarrow 18 \cdot t \equiv 3 \pmod{15} \Rightarrow 3t \equiv 3 \pmod{15} \Rightarrow$$

και άρα $x = 18 \cdot 1 + 7 = 25$ $\Rightarrow$ η μοναδική λύση $\pmod{[18, 15]} = 90$

$$\Rightarrow \left\{ \begin{array}{l} x \equiv 25 \pmod{90} \Rightarrow 90 \mid x-25 \Rightarrow x = 90 \cdot s + 25, s \in \mathbb{Z}. \\ (\Sigma_2): \left\{ \begin{array}{l} x \equiv 1 \pmod{14} \end{array} \right\} \Rightarrow \end{array} \right.$$

$$\Rightarrow 90s + 25 \equiv 1 \pmod{14} \Rightarrow 6s \equiv 4 \pmod{14} \Rightarrow \frac{6}{2} \cdot s \equiv \frac{4}{2} \pmod{\frac{14}{2}} \Rightarrow$$

$$\text{Τότε } x = 90 \cdot 3 + 25 = 295 \text{ δίνει τον } (\Sigma) \\ \text{η οποία είναι πολλαδική } \pmod{[8, 15, 14]} = \\ = \pmod{630}.$$

$$\Rightarrow 3s \equiv 2 \pmod{7} \Rightarrow \boxed{s=3}$$

$$(\Sigma): \left\{ \begin{array}{l} \alpha_1 x \equiv b_1 \pmod{m_1} \text{ (1)} \\ \vdots \\ \alpha_m x \equiv b_m \pmod{m_m} \text{ (m)} \end{array} \right. \left| \begin{array}{l} \forall k=1, \dots, m \text{ η γραμ. ισοδύναμη} \\ \text{(X) έχει λύση (C)} \end{array} \right.$$

$\forall$ mod. δυνάμ. οι παραπάνω συστήματα και θέτουμε: $b_k = b'_k \cdot d_k$
 $m_k = m'_k \cdot d_k, d_k = \alpha'_k \cdot d_k, \forall k=1, \dots, m.$

$$\text{Τότε } \alpha_k x \equiv b_k \pmod{m_k} \Leftrightarrow \alpha'_k x \equiv b'_k \pmod{m'_k} \quad \forall k=1, \dots, m$$

Οι τελευταίες ισοδύναμες έχουν πολλαδική λύση $c_k \pmod{m'_k}$

$$\text{Άρα το } (\Sigma) \text{ είναι ισοδύναμο με το } (\Sigma'): \left\{ \begin{array}{l} x \equiv c_1 \pmod{m'_1} \\ \vdots \\ x \equiv c_m \pmod{m'_m} \end{array} \right.$$

Το (Σ') ικανοποιεί ως προς τον ΚΘΥ.

$\delta m) (m'_i, m'_j) = 1, 1 \leq i \neq j \leq m$, και τότε το (Σ') μπορεί να λυθεί με χρήση του ΚΘΥ.

και να βρωτε μια λύση x_0 η οποία είναι πολλαδική $\pmod{(m'_1, \dots, m'_m)}$