

21/05/15.

Επίλυση Γραμμικών Ισοτιμιών

Έστω $m \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Γραμμική Ισοτιμία είναι κάθε εξίσωση της μορφής:

$$ax \equiv b \pmod{m} \quad (*)$$

Λύση της $(*)$ είναι κάθε αριθμός $x_0 \in \mathbb{Z}$ έτσι ώστε $ax_0 \equiv b \pmod{m}$.

Έστω x_0 λύση της $(*)$. Τότε $ax_0 \equiv b \pmod{m}$

Τότε $\forall y \in \mathbb{Z} : y \equiv x_0 \pmod{m} : ay \equiv b \pmod{m}$ δηλ ο $y \in \mathbb{Z}$ είναι λύση της $(*)$

Διότι $m | y - x_0 \Rightarrow \exists k \in \mathbb{Z} : y - x_0 = k \cdot m \Rightarrow y = x_0 + km \Rightarrow$

$$\Rightarrow ay = (x_0 + km)a = \underbrace{ax_0}_{b \pmod{m}} + \underbrace{akm}_{0 \pmod{m}} \equiv b \pmod{m}$$

Άρα x_0 λύση της $(*) \Rightarrow x_0 + km : \text{λύση της } (*), \forall k \in \mathbb{Z}$.

Έτσι από πάνω και στο εξής, λύση της $(*)$ θα εννοούμε την κλάση ισοτιμίας $[x_0]_m$ του $x_0 \in \mathbb{Z} : ax_0 \equiv b \pmod{m}$.

$$ax \equiv b \pmod{m} \Leftrightarrow [ax]_m = [b]_m \Leftrightarrow [a]_m [x]_m = [\bar{b}]_m$$

Εξίσωση στο σύνολο $\mathbb{Z}_m$

Παράδειγμα: $6x \equiv 1 \pmod{8} \Leftrightarrow 8 | 6x - 1 : 6x - 1 = 8k \Rightarrow$

$$\Rightarrow 6x - 8k = 1 \Rightarrow 2(3x - 4k) = 1 : \text{άτοπο} \Rightarrow$$

$\Rightarrow \nexists x \in \mathbb{Z} : 6x \equiv 1 \pmod{8}$ δεν έχει καμία λύση.

$X \equiv 0 \pmod{2} \Leftrightarrow X$: άρτιος. Στο $\mathbb{Z}_2$ έχουμε τον άρτιο των $[0]_2$
αφού περιγράφει όλους τους άρτιους.

Πρόταση: Έστω η γραμμική ισοτιμία: $\alpha X \equiv b \pmod{n} (*)$. Αν $(\alpha, n) = 1$
τότε η $(*)$ έχει τον άρτιο των $\mathbb{Z}_n$:

~~$X \equiv b \cdot c \pmod{n}$~~ $X \equiv b \cdot c \pmod{n}$, όπου $[c]_n = [\alpha]_n^{-1}$.

Απόδειξη: $(*) \Leftrightarrow [\alpha]_n [X]_n = [b]_n$ ↑
Υπάρχει διότι
 $(\alpha, n) = 1$.
 $(\alpha, n) = 1 \Rightarrow \exists [\alpha]_n^{-1} \in \mathbb{Z}_n : [\alpha]_n \cdot [\alpha]_n^{-1} = [1]_n \Rightarrow$

$\Rightarrow$ Άρα $[\alpha]_n^{-1} [\alpha]_n [X]_n = [\alpha]_n^{-1} [b]_n \Rightarrow$

Αν $[\alpha]_n^{-1} = [c]_n$, όπου $c \in \mathbb{Z}$ και άρα $\} \Rightarrow [X]_n = [c]_n [b]_n = [b \cdot c]_n$

$\Rightarrow b \cdot c$: άρτιος της $(*)$ και αυτή η άρτιος είναι μοναδική.

$(\alpha, n) = 1 \xrightarrow{\text{Θ. Euler}} \alpha^{\varphi(n)} \equiv 1 \pmod{n} \Rightarrow [\alpha^{\varphi(n)}]_n = [1]_n \Rightarrow$

$\Rightarrow [\alpha]_n^{\varphi(n)} = [1]_n \Rightarrow [\alpha]_n^{\varphi(n)-1} = [1]_n \Rightarrow [\alpha]_n^{-1} = [\alpha]_n^{\varphi(n)-1} = [\alpha^{\varphi(n)-1}]_n$

Παράδειγμα: $\begin{matrix} \alpha & b & n \end{matrix} \quad \begin{matrix} 7 & 8 & 30 \end{matrix} \quad (*)$

$(7, 30) = 1 \xrightarrow{\text{Πρόταση}} \eta (*) \text{ έχει μοναδική άρτιο των } \mathbb{Z}_n$:

$[X]_{30} = [7]_{30}^{-1} [8]_{30}$

Θ. Euler $\Rightarrow 7^{\varphi(30)} \equiv 1 \pmod{30}$

Άρα $7^8 \equiv 1 \pmod{30} \Rightarrow 7^7 \cdot 7 \equiv 1 \pmod{30} \Rightarrow 7^7 \equiv 7^{-1} \pmod{30}$. Τότε: $30 = 2 \cdot 3 \cdot 5 \Rightarrow \varphi(30) = \varphi(2 \cdot 3 \cdot 5) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = 1 \cdot 2 \cdot 4 = 8$.

$\Rightarrow [7]_{30}^{-1} = [7^7]_{30} = [7^7]_{30}$

Είναι $7^7 = \underbrace{7 \cdot 7 \cdot 7}_{49 \equiv 19 \pmod{30}} \cdot \underbrace{7 \cdot 7 \cdot 7}_{49 \equiv 19 \pmod{30}} \cdot \underbrace{7 \cdot 7 \cdot 7}_{19 \cdot 7 \equiv 19 \pmod{30}} \equiv 19 \cdot 19 \cdot 19 \cdot 7 \equiv 19 \cdot 7 \equiv 133 \equiv 13 \pmod{30}$

Άρα $[7]_{30}^{-1} = [13]_{30}$

Άρα η $[14]_{30}$ είναι η μοναδική άρτιος της αρίστης.

Εναλλακτικά: Η άρτιος άρτιος της $(*)$ είναι η $(*)$: $X \equiv 14 \pmod{30}$

Τότε $[X]_{30} = [7]_{30}^{-1} [8]_{30} = [13]_{30} [8]_{30} = [104]_{30} = [14]_{30}$.

Παράδειγμα: $137 \cdot x \equiv 4 \pmod{102} \quad (*)$

$[137]_{102} \cdot [x]_{102} = [4]_{102} \quad (*)'$

$[137]_{102} = [102+35]_{102} = \overset{70}{[102]}_{102} + [35]_{102} = [35]_{102} \Rightarrow$

$\Rightarrow (*) \Leftrightarrow (**) \quad 35x \equiv 4 \pmod{102}$. Επειδή $(35, 102) = 1 \Rightarrow$

~~Επειδή~~

$\Rightarrow$ $(**)$ έχει λύση γιατί: $[x]_n = [35]^{-1}_{102} \cdot [4]_{102}$

Τότε $[35]^{-1}_{102} = [35]_{102}$ (από θ. Euler)

Π.χ. $1 = (-12) \cdot 102 + 35 \cdot 35 \Rightarrow$

$\Rightarrow [35]^{-1}_{102} = [35]_{102}$

$(\alpha, n) = 1 \Rightarrow \exists k, \lambda \in \mathbb{Z}:$
 $\alpha k + \lambda n = 1 \Rightarrow$
 $\Rightarrow [\alpha]_n [k]_n + [\lambda]_n [n]_n \overset{70}{=} 1$
 $\Rightarrow [\alpha]_n^{-1} = [k]_n = [1]_n$

Λύση: $[x]_{102} = [35]_{102} \cdot [4]_{102} = [35 \cdot 4]_{102} = [140]_{102} = [38]_{102}$

Λύση με (*): $x \equiv 38 \pmod{102}$

ΘΕΩΡΗΜΑ 1: Η γραμμική Ισοτιμία: $\alpha x \equiv b \pmod{n} \quad (*)$ έχει λύση $\Leftrightarrow$

$\Leftrightarrow \delta = \gcd(\alpha, n) \mid b$. Αν $\delta \mid b$ τότε οι αντί δύο αριθμοί

λύσης της $(*)$ είναι οι $\epsilon\sigma\tau\iota\varsigma$: $x_0, x_0 + \frac{n}{\delta}, x_0 + 2 \cdot \frac{n}{\delta}, \dots, x_0 + (\delta-1) \frac{n}{\delta}$

όπου x_0 : λύση της $(*)$.

Απόδειξη: $(\Rightarrow)$ Έστω x_0 : λύση της $(*) \Rightarrow x_0 \in \mathbb{Z}$ και $\alpha x_0 \equiv b \pmod{n} \Rightarrow$
 $\Rightarrow n \mid \alpha x_0 - b = \alpha x_0 - b = k \cdot n$, για $k \in \mathbb{Z}$.

Όπως $\delta \mid \alpha$ και $\delta \mid n$ $\Rightarrow \delta \mid \alpha x_0 - k \cdot n = \delta \mid b$

$(\Leftarrow)$ Θα έχουμε: $\alpha \cdot x \equiv b \pmod{n} \Leftrightarrow n \mid \alpha x - b \Leftrightarrow \alpha x - b = k \cdot n$
 $\delta = (\alpha, n) \Rightarrow \delta \mid \alpha \Rightarrow \alpha = \delta \cdot \alpha'$
 $\Rightarrow \delta \mid n \Rightarrow n = \delta \cdot n'$
 $\delta \mid b \Rightarrow b = \delta \cdot b'$
 $\Rightarrow \alpha' x - b' = k \cdot n' \Rightarrow \alpha' x \equiv b' \pmod{n'}$

$\Rightarrow \frac{\alpha}{\delta} x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}}$ Επειδή $(\frac{\alpha}{\delta}, \frac{n}{\delta}) = 1$ ⁷⁰ $\Rightarrow$ $(*)$ έχει λύση
 γιατί $(x_0 \bmod \frac{n}{\delta})$

Τότε $x_0 \pmod{n}$ θα είναι και άρα μας $\textcircled{*}$ (έχω ήδη $\{ \in 160 \text{ δυναμίες} \}$
 στο αντίθετο)

$$\forall k=0, \dots, \delta-1: \alpha(x_0 + k \cdot \frac{n}{\delta}) = \alpha x_0 + \alpha k \frac{n}{\delta}$$

$$\text{Επειδή } \delta/\alpha \Rightarrow \frac{\alpha}{\delta} \in \mathbb{Z} \Rightarrow \frac{\alpha \cdot k}{\delta} \in \mathbb{Z}$$

$$\Rightarrow \alpha x_0 + \alpha k \frac{n}{\delta} \equiv (b+0) \pmod{n} \equiv b \pmod{n}$$

Έστω $k, \lambda \in [0, \delta-1]$. και έστω ότι

$$x_0 + k \frac{n}{\delta} \equiv x_0 + \lambda \frac{n}{\delta} \pmod{n} \Rightarrow$$

$$\Rightarrow n/(k-\lambda) \frac{n}{\delta} \Rightarrow (k-\lambda) \frac{n}{\delta} = m \cdot n \Rightarrow (k-\lambda) = m \cdot \delta \Rightarrow$$

$$\Rightarrow \delta/(k-\lambda) \Rightarrow \delta \leq k-\lambda$$

$$\left. \begin{array}{l} \text{Έστω } x_0' \pmod{n} \text{ να είναι άρα μας } \textcircled{*}, \delta \mid \alpha x_0' \equiv b \pmod{n} \\ 0 \leq k, \lambda \leq \delta-1 \end{array} \right\} \Rightarrow \boxed{k=\lambda}$$

$$\frac{\alpha}{\delta} x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}} \textcircled{*}$$

$$\alpha x \equiv b \pmod{n} \textcircled{*}$$

Έστω $x_0' \pmod{n}$ να είναι άρα μας $\textcircled{*}$, $\delta \mid \alpha x_0' \equiv b \pmod{n}$

Τότε η $x_0' \pmod{\frac{n}{\delta}}$ είναι άρα μας $\textcircled{*}$ η οποία έχει

μοναδική λύση $\pmod{\frac{n}{\delta}}$ ως $x_0 \pmod{\frac{n}{\delta}}$. Άρα $x_0 \equiv x_0' \pmod{\frac{n}{\delta}}$

$$\frac{n}{\delta} \mid x_0' - x_0 \Rightarrow x_0' = x_0 + k \frac{n}{\delta}, \text{ για κάποιο } k \in \mathbb{Z}.$$

Εκτελείται Διαίρεση του k με το δ : $k = m \cdot \delta + r, 0 \leq r \leq \delta-1$.

$$\text{Τότε } x_0' = x_0 + k \frac{n}{\delta} = x_0 + (m\delta + r) \frac{n}{\delta} = x_0 + \frac{m\delta n}{\delta} + r \frac{n}{\delta} \equiv$$

$$\equiv x_0 + r \frac{n}{\delta}$$

$$\text{Άρα } x_0' \equiv x_0 + r \frac{n}{\delta} \pmod{n}, 0 \leq r \leq \delta-1.$$

Παράδειγμα: $\frac{21}{3} x \equiv \frac{6}{3} \pmod{\frac{33}{3}} \textcircled{*}$, $\delta = (21, 33) = (3 \cdot 7, 3 \cdot 11) = 3$.

$\delta/b = 3$ $\textcircled{*}$ έχει λύση και: όλες οι λύσεις μας $\textcircled{*}$ θα είναι:

$$x_0, x_0 + \frac{33}{3}, x_0 + 2 \cdot \frac{33}{3} \text{ δηλ: } x_0, x_0 + 11, x_0 + 22$$

~~$x_0 \pmod{n}$~~ $x_0 \pmod{\frac{n}{\delta}}$ είναι η μοναδική άρα μας

$$\frac{\alpha}{\delta} x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}} \text{ δηλ } \frac{21}{3} x \equiv \frac{6}{3} \pmod{\frac{33}{3}} \Rightarrow x \equiv 2 \pmod{11}$$

Τότε $x \equiv 5 \pmod{11}$ είναι η μοναδική άρα μας $\textcircled{*}$

Άρα όλες οι λύσεις

αυτά 2 αντίθετες μας $\textcircled{*}$ είναι: $5 \pmod{33}, 16 \pmod{33}, 27 \pmod{33}$.

Παραίτηση: ① Έστω $m/a, b, n$ και έστω $a' = \frac{a}{m}, b' = \frac{b}{m}, n' = \frac{n}{m}$

Τότε: $ax \equiv b \pmod{n} \Leftrightarrow a'x \equiv b' \pmod{n'}$

Απόδειξη: $ax \equiv b \pmod{n} \Leftrightarrow n/a - b \Leftrightarrow \exists k \in \mathbb{Z}: ax - b = kn \Leftrightarrow$
 $\Leftrightarrow \exists k \in \mathbb{Z}: \frac{a}{m}x - \frac{b}{m} = k \frac{n}{m} \Leftrightarrow \exists k \in \mathbb{Z}: a'x - b' = kn' \Leftrightarrow$
 $\Leftrightarrow n/a' - b' \Leftrightarrow a'x \equiv b' \pmod{n'}$

② Αν $(a, n) = 1$ και $m/a, b$ και $a' = \frac{a}{m}, b' = \frac{b}{m}$. Τότε: $ax \equiv b \pmod{n} \Leftrightarrow a'x \equiv b' \pmod{n}$

Απόδειξη: $ax \equiv b \pmod{n} \Leftrightarrow n/a - b \Leftrightarrow \exists k \in \mathbb{Z}: ax - b = k \cdot n \Leftrightarrow$
 $\Leftrightarrow \frac{a}{m}x - \frac{b}{m} = \frac{k \cdot n}{m} \Leftrightarrow a'x - b' = \frac{k \cdot n}{m} \in \mathbb{Z} \Rightarrow$
 $\Rightarrow m/k \cdot n$
 $m \nmid n$ διότι επειδή m/a θα είχατε ότι $m/(n, a) = 1$.
 Τότε m/k , τότε: $a'x - b' = \left(\frac{k}{m}\right)n \Rightarrow$
 $\Rightarrow \boxed{a'x \equiv b' \pmod{n}}$

Ένα ^{σύνολο} γραμμικών 1602 μιλίων είναι ως topoi:

(Σ): $\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_m x \equiv b_m \pmod{n_m} \end{cases}$ όπου (Σ) είναι ένας ακεραίος x_0 ο οποίος ικανοποιεί ως:
 $a_i x \equiv b_i \pmod{n_i}, i = 1, \dots, m.$

Παράδειγμα: (Σ) : $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 0 \pmod{4} \end{cases}$ Δεν έχει λύση διότι αν x_0 ήταν λύση του (Σ) $\Rightarrow$
 $\Rightarrow x_0 \equiv 1 \pmod{2} \Rightarrow x_0$ περιττός
 και $x_0 \equiv 0 \pmod{4} \Rightarrow x_0$ άρτιος $\Rightarrow$ Ατομή

Να βρεθούν όλοι οι ακεραίοι οι οποίοι ~~είναι~~ δίνουν υπόλοιπα:
 2, 3, 2 όταν διαιρούνται με τους 3, 5, 7 αντίστοιχα.

$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \quad (15)$

⊛ ΚΙΝΗΣΙΚΟ ΘΕΩΡΗΜΑ ΥΠΟΛΟΓΙΣΜΩΝ ⊛

Θεωρούμε το δίδυμο γραμμικών ισολογιών :

$$(\Sigma) : \begin{cases} x \equiv \alpha_1 \pmod{m_1} \\ x \equiv \alpha_2 \pmod{m_2} \\ \vdots \\ x \equiv \alpha_r \pmod{m_r} \end{cases} \quad \text{Αν } (m_i, m_j) = 1 \text{ όπου } 1 \leq i \neq j \leq r$$

τότε το (Σ) έχει λύση, έστω x_0 ,
η οποία είναι μοναδική $\pmod{(m_1, \dots, m_r)}$

Απόδειξη : ① Θέτουμε $M = m_1 \cdot m_2 \cdot \dots \cdot m_r$ και $M_i = \frac{M}{m_i} = m_1 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_r$
 Τότε : $\forall i=1, \dots, r : (m_i, M_i) = 1 \quad \forall i=1, \dots, r$
 διότι $(m_i, m_j) = 1, \forall i \neq j$

Θεωρούμε τις γραμμικές ισολογίες : $M_i \cdot x \equiv 1 \pmod{m_i}, i=1, \dots, r. \quad (*)$
 Επειδή $\forall i=1, \dots, r : (m_i, M_i) = 1 \Rightarrow (*)$ έχει μοναδική λύση $b_i \pmod{m_i}, i=1, \dots, r$.

② Θέτουμε $x_0 = \sum_{i=1}^r M_i b_i = M_1 b_1 + \dots + M_r b_r$

Θ.δ.ο. η x_0 είναι λύση του (Σ) , η οποία είναι μοναδική $\pmod{(m_1, \dots, m_r)}$
 Σημειώνουμε ένα $i=1, \dots, r$. Τότε $\forall j \neq i, j=1, \dots, r : m_j | M_i \Rightarrow$
 $\Rightarrow M_i \equiv 0 \pmod{m_j} \Rightarrow M_i b_i \equiv 0 \pmod{m_j}$
 Για $i=j$: $M_i b_i \equiv \alpha_i \pmod{m_i}$
 $\Rightarrow x_0 = \sum_{i=1}^r M_i b_i \equiv \alpha_i \pmod{m_i}, \forall i=1, \dots, r \Rightarrow x_0$ λύση του (Σ)

③ Έστω x' μια άλλη λύση του $(\Sigma) : x' \equiv \alpha_i \pmod{m_i}, \forall i=1, \dots, r$.
 Επίσης έχουμε $x_0 \equiv \alpha_i \pmod{m_i}, i=1, \dots, r$. Άρα $x' \equiv x_0 \pmod{m_i}, \forall i=1, \dots, r$
 $\Rightarrow m_i | x' - x_0, \forall i=1, \dots, r$
 $\Rightarrow m_1, m_2, \dots, m_r | x' - x_0$
 $(m_i, m_j) = 1, i=1, \dots, r (i \neq j) \Rightarrow m_1 \cdot \dots \cdot m_r | x' - x_0$
 $\Rightarrow x' \equiv x_0 \pmod{(m_1, \dots, m_r)}$
Αντίστροφα : Αν $x' \equiv x_0 \pmod{(m_1, \dots, m_r)}$, θ.δ.ο. x' : λύση του (Σ) .

$$\text{Τότε: } m_1, \dots, m_r \mid x' - x_0 \mid m_1 \dots m_r \mid m \mid m$$

$$x' \equiv x_0 \pmod{m_i} \quad 1 \leq i \leq r \Rightarrow x' \equiv x_0 \pmod{m_1 \dots m_r} \equiv x_0 \pmod{m}$$

$$x' \equiv x_0 \pmod{m}$$

Άρα x' λύση του (Σ) .

Παράδειγμα: $(\Sigma): \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \quad \begin{matrix} d_1 = 2 \\ d_2 = 3 \\ d_3 = 2 \end{matrix} \quad \begin{matrix} m_1 = 3 \\ m_2 = 5 \\ m_3 = 7 \end{matrix}$

$$M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = \frac{3 \cdot 5 \cdot 7}{3} = 35$$

$$M_2 = \frac{3 \cdot 5 \cdot 7}{5} = 21$$

$$M_3 = \frac{3 \cdot 5 \cdot 7}{7} = 15$$

$$35x \equiv 1 \pmod{3} \Rightarrow 2x \equiv 1 \pmod{3}$$

$$21x \equiv 1 \pmod{5} \Rightarrow x \equiv 1 \pmod{5}$$

$$15x \equiv 1 \pmod{7} \Rightarrow x \equiv 1 \pmod{7}$$

Άρα Nov. λύση: $b_1 = 2 \pmod{3}$

$$b_2 \equiv 1 \pmod{5}$$

$$b_3 \equiv 1 \pmod{7}$$

$$x_0 = b_1 M_1 d_1 + b_2 M_2 d_2 + b_3 M_3 d_3 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$$

ο οποίος είναι λύση του (Σ) η οποία είναι το ίδιο mod 105

Δηλ. η γεν. λύση του (Σ) mod 105 είναι η $(23 \pmod{105})$.