20-12-16

→ Γραμμικές Ισοτιμίες

Αν $n \geq 2$ και $a, b \in \mathbb{Z}$ τότε κάθε ισοτιμία της μορφής $ax \equiv b \pmod{n}$ (*) καλείται γραμμική ισοτιμία όπου x: ακέραιος προς προσδιορισμό

Ένας ακέραιος x_0 επαληθεύει την (*) $\iff$

$\iff ax_0 \equiv b \pmod{n}$

Αν x_0 επαληθεύει την (*) τότε $\forall y \in \mathbb{Z}: y \equiv x_0 \pmod{n}$ ο y επαληθεύει την (*)

Τότε $n \mid y - x_0 \Rightarrow y - x_0 = kn,\ k \in \mathbb{Z} \Rightarrow y = x_0 + kn$

Άρα, $ay = a(x_0 + kn) = ax_0 + kn = b \pmod{n} \Rightarrow$

$\Rightarrow y$: επαληθεύει την (*)

Έτσι, για λύση της (*) είναι ένας ακέραιος x_0 μαζί με κάθε άλλον ακέραιο στην κλάση ισοτιμίας του x_0, ο οποίος επαληθεύει την (*)

→ Παρατήρηση: Ο ακέραιος x_0 επαληθεύει την (*) $\iff$

$\iff$ ισχύει ότι $[a]_n [x_0]_n = [b]_n$

Άρα οι λύσεις της $ax \equiv b \pmod{n}$ συμπίπτουν με τις λύσεις της $[a]_n [x]_n = [b]_n$ {→ εξίσωση στο $\mathbb{Z}_n$}

→ Παρατήρηση: Γραμμικές Ισοτιμίες δεν έχουν απαραίτητα λύσεις, διότι πχ:

$6x \equiv 1 \pmod 8$ → Δεν έχει λύσεις, διότι αν x_0 την επαληθεύει τότε: $6x_0 \equiv 1 \pmod 8 \Rightarrow$

$\Rightarrow 8 \mid 6x_0 - 1 \Rightarrow 6x_0 - 1 = 8k$, $k \in \mathbb{Z}$ Άτοπο

περιττός ← $6x_0 - 1$, $8k$ → άρτιος

• Παράδειγμα: Έστω η γραμμική ισοτιμία $2x \equiv 1 \pmod 3$

Π.Σ.Υ $\bmod 3 = \{0, 1, 2\}$

• $2 \cdot 0 = 0 \not\equiv 1 \pmod 3$
• $2 \cdot 1 = 2 \not\equiv 1 \pmod 3$
• $2 \cdot 2 = 4 \equiv 1 \pmod 3$ → $x_0 = 2$ επαληθεύει την ⊛

Αν y = άλλος ακέραιος που επαληθεύει την ⊛

$$y \equiv 1 \pmod 3 \Rightarrow \begin{cases} 2x_0 \equiv 1 \pmod 3 \Rightarrow 3 \mid 2x_0 - 1 \\ 2y \equiv 1 \pmod 3 \quad\quad 3 \mid 2y - 1 \end{cases}$$

$$\Rightarrow 3 \mid 2x_0 - 1 - 2y + 1 \xrightarrow{(3,2)=1} 3 \mid x_0 - y \Rightarrow y \equiv x_0 \pmod 3$$

• Πρόταση: Έστω η γραμμική ισοτιμία $ax \equiv b \pmod n$ ⊛

Αν $(a, n) = 1$, τότε η ⊛ έχει μοναδική λύση

Απόδειξη: $(a,n)=1 \Rightarrow [a]_n$: αντιστρέψιμη $\Rightarrow$

$\Rightarrow \exists\, c \in \mathbb{Z} : [a]_n [c]_n = [1]_n \Rightarrow$

$\Rightarrow [ac]_n = [1]_n \Rightarrow ac \equiv 1 \pmod n$

Τότε: $c \cdot a \cdot x \equiv c\,b \pmod n \Rightarrow x \equiv cb \pmod n$

Άρα, αν $(a,n)=1 \Rightarrow$ Η μοναδική λύση της ⊛ είναι η $x = cb \pmod n$, όπου $c \in \mathbb{Z}$.
$[c]_n$: αντίστροφη κλάση ισοτιμίας της $[a]_n$ ($[c]_n = [a]_n^{-1}$)

Παραδείγματα: i) $2x \equiv 10 \pmod 6$ ⊛

Επειδή $10 \equiv 4 \pmod 6 \Rightarrow 2x \equiv 4 \pmod 6$

π.σ.υ $\mod 6 = \{0,1,2,3,4,5\}$

- $2 \cdot 0 = 0 \not\equiv 4 \pmod 6$ ×
- $2 \cdot 1 = 2 \not\equiv 4 \pmod 6$ ×
- $2 \cdot 2 = 4 \equiv 4 \pmod 6$ ✓ → λύση
- $2 \cdot 3 = 6 \not\equiv 4 \pmod 6$ ×
- $2 \cdot 4 = 8 \not\equiv 4 \pmod 6$ ×
- $2 \cdot 5 = 10 \equiv 4 \pmod 6$ ✓ → λύση

Άρα, $x_0 = 2, 5$ λύση της ⊛

ii) $137x \equiv 4 \pmod{102}$ ⊛

Επειδή $137 \equiv 35 \pmod{102} \Rightarrow$ ⊛: $35x \equiv 4 \pmod{102}$

$35 = 5 \cdot 7$

$102 = 2 \cdot 51 = 2 \cdot 3 \cdot 17$

$\Rightarrow (35, 102) = 1$

Άρα, η ⊛ έχει μοναδική λύση (mod 102), την:

$x = 4c \pmod{102}$ ⊛⊛ , $[c]_{102} = [35]_{102}^{-1}$

$$\left.\begin{array}{l} \cdot\ 102 = 2\cdot 35 + 32 \\ 35 = 32 + 3 \\ 32 = 10\cdot 3 + 2 \\ 3 = 2 + 1 \end{array}\right\} \Rightarrow 1 = (-12)\cdot 102 + 35\cdot 35 \Rightarrow$$

$$\Rightarrow [1]_{102} = [-12]_{102}\cdot \cancel{[102]_{102}}^{\,0} + [35]_{102}[35]_{102}$$

Άρα $[35]_{102}^{-1} = [35]_{102}$, συνεπώς $c = 35$ και τότε

⊛⊛ : $x = 4\cdot 35 \pmod{102} \Rightarrow x = 38 \pmod{102}$

• Παράδειγμα : $7x \equiv 8 \pmod{30}$ ⊛

$(7, 30) = 1 \Rightarrow$ η ⊛ έχει μοναδική λύση (mod 30) την $x = 8\cdot c \pmod{30}$, όπου $[c] = [7]_{30}^{-1}$

Απ' το Θεώρημα Euler $\Rightarrow 7^{\varphi(30)} \equiv 1 \pmod{30} \Rightarrow$

$\overset{*}{\Rightarrow} 7^8 \equiv 1 \pmod{30} \Rightarrow 7^7\cdot 7 \equiv 1 \pmod{30} \Rightarrow [7]_{30}^{-1} = [7^7]_{30}$

$*$: $30 = 2\cdot 3\cdot 5 = \varphi(2)\varphi(2)\varphi(5) = 1\cdot 2\cdot 4 = 8$

$$\begin{cases} 7^1 \equiv 7 \pmod{30} & 7^3 \equiv 73 \equiv 13 \pmod{30} \\ 7^2 \equiv 19 \pmod{30} & 7^4 \equiv 91 \equiv 1 \pmod{30} \end{cases}$$

Τότε: $7^7 = 7^4\cdot 7^3 = 7^3 \equiv 13 \pmod{30}$

Άρα $[7]_{30}^{-1} = [13]_{30}$ κι επομένως η λύση της ⊛ είναι η $x = 8\cdot 13 \equiv 14 \pmod{30}$

• **Θεώρημα:** Η γραμμική ισοτιμία $\alpha x \equiv b \pmod{n}$ (*) έχει λύση $\iff$ $\delta = (\alpha, n) \mid b$

Αν $\delta \mid b$ και x_0 λύση της (*), τότε όλες οι ανά δύο ασυσχέτιστες mod n λύσεις της (*) είναι οι εξής:

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

Απόδειξη: "$\Rightarrow$" Έστω ότι x_0 λύση της (*)

Τότε: $\alpha x_0 \equiv b \pmod{n} \Rightarrow n \mid \alpha x_0 - b \Rightarrow \alpha x_0 - b = kn,\ k \in \mathbb{Z}$

Τότε: $\alpha x_0 - kn = b$

Όμως $\delta = (\alpha, n) \mid \alpha \Rightarrow \delta \mid \alpha x_0$

$\delta = (\alpha, n) \mid n \Rightarrow \delta \mid kn$

$\Rightarrow \delta \mid \alpha x_0 - kn \Rightarrow \delta \mid b$

"$\Leftarrow$" Έστω ότι $\delta = (\alpha, n) \mid b \Rightarrow \delta \mid \alpha$, $\delta \mid n$, $\delta \mid b$

Τότε: $\frac{\alpha}{\delta}, \frac{n}{\delta}, \frac{b}{\delta} \in \mathbb{Z}$

Θεωρούμε τη γραμμική ισοτιμία $\frac{\alpha}{\delta} x \equiv \frac{b}{\delta} \left(\mathrm{mod}\ \frac{n}{\delta}\right)$ (**)

όπου $\left(\frac{\alpha}{\delta}, \frac{n}{\delta}\right) = 1$

Αν x_0 λύση της (*) $\Leftrightarrow \alpha x_0 \equiv b \pmod n \Leftrightarrow$

$\Leftrightarrow n \mid \alpha x_0 - b \Leftrightarrow \alpha x_0 - b = \kappa n$, $\kappa \in \mathbb{Z} \Leftrightarrow$

$\Leftrightarrow \frac{\alpha}{\delta} x_0 - \frac{b}{\delta} = \kappa \frac{n}{\delta}$, $\kappa \in \mathbb{Z} \Leftrightarrow$

$\Leftrightarrow \frac{n}{\delta} \mid \frac{\alpha}{\delta} x_0 - \frac{b}{\delta} \Leftrightarrow \frac{\alpha}{\delta} x_0 \equiv \frac{b}{\delta} \left(\mod \frac{n}{\delta} \right) \Leftrightarrow$

$\Leftrightarrow x_0$: λύση της (**)

Έτσι, επειδή $\left(\frac{\alpha}{\delta}, \frac{n}{\delta} \right) = 1 \Rightarrow$ Η (**) έχει μοναδική λύση $\mod \frac{n}{\delta}$ x_0 και σύμφωνα με τις παραπάνω ισοδυναμίες έπεται ότι η x_0 είναι λύση της (*).

Τότε, κάθε ακέραιος της μορφής $x_0 + \kappa \frac{n}{\delta}$ είναι λύση της (**) άρα και της (*)

Έστω ότι $x_0 + \kappa_1 \frac{n}{\delta} \equiv x_0 + \kappa_2 \frac{n}{\delta} \pmod n \Rightarrow$

$\Rightarrow n \mid x_0 + \kappa_2 \frac{n}{\delta} - \left(x_0 + \kappa_1 \frac{n}{\delta} \right) \Rightarrow$

$\Rightarrow n \mid (\kappa_2 - \kappa_1) \frac{n}{\delta} \Rightarrow (\kappa_2 - \kappa_1) \frac{n}{\delta} = n \cdot \lambda$, $\lambda \in \mathbb{Z}$

$\Rightarrow (\kappa_2 - \kappa_1) = \lambda \cdot \delta \Rightarrow \kappa_1 \equiv \kappa_2 \pmod \delta$

Άρα οι ανά δύο ανισοτιμες mod n λύσεις της αρχικής (*) θα είναι: $x_0, x_0+\frac{n}{\delta}, x_0+\frac{2n}{\delta}, \dots, x_0+(\delta-1)\frac{n}{\delta}$

↳ **Παράδειγμα:** $21x \equiv 6 \pmod{33}$ (*)

$\delta=(\alpha,n)=(21,33)=3|6=b$. Άρα, απ' το Θεώρημα η (*) έχει 3 ανισοτιμες ανά δύο (mod 33) λύσεις

Θεωρούμε τη γραμμική ισοτιμία $7x \equiv 2 \pmod{11}$ (**)

Η (**) έχει μοναδική λύση (mod 11) τη $x_0=5 \pmod{11}$

Άρα, το $x_0=5$ είναι λύση της (*) και σύμφωνα με το Θεώρημα όλες οι λύσεις της αρχικής θα είναι: $5, 5+11, 5+2\cdot 11$, δηλαδή: $5, 16, 27 \pmod{33}$

↳ **Παράδειγμα:** $2086x \equiv -1624 \pmod{1729}$

Επειδή $\begin{cases} 2086 \equiv 357 \pmod{1729} \\ -1624 \equiv 105 \pmod{1729} \end{cases}$ => έπεται ότι θα έχουμε τη γραμμική ισοτιμία:

$357x \equiv 105 \pmod{1729}$ (*)

- $1729 = 4\cdot 357 + 301$
- $357 = 301 + 56$
- $301 = 5\cdot 56 + 21$
- $56 = 2\cdot 21 + 14$
- $21 = 14 + (7)$
- $14 = 2\cdot 7$

↱ $(1729, 357) = 7 | 105 \Rightarrow$ Η (*) έχει λύση και μάλιστα θα έχει 7 ανισοτιμες ανά δύο λύσεις (mod 1729)

Τότε: $7 = 19 \cdot 1729 + (-92) \cdot 357 \xrightarrow{\times 15}$

$\Rightarrow 105 = 19 \cdot 15 \cdot 1729 + (-92) \cdot 15 \cdot 357 \Rightarrow$

$\Rightarrow (-92 \cdot 15) \cdot 357 \equiv 105 \pmod{1729} \Rightarrow$

$\Rightarrow x_0 \equiv 349 \pmod{1729}$ Λύση της ⊛ και όλες οι λύσεις της ⊛ θα είναι:

$$349,\ 349 + \frac{1729}{7},\ 349 + 2 \cdot \frac{1729}{7},\ \dots,\ 349 + 6 \cdot \frac{1729}{7}$$