Το προηγούμενο μάθημα 19/12/15 είναι στις σελίδες σε. 21/12/15

Γραμμικές Ισοτιμίες

Έστω $n>1$

Τότε μια γραμμική ισοτιμία είναι της μορφής:

$$\boxed{ax \equiv b \bmod n} \quad (1)$$

Λύση της γραμμικής ισοτιμίας (1) είναι $\forall$ ακέραιος $x_0 \in \mathbb{Z}$. η ισοτιμία $ax_0 \equiv b \bmod n$ να ικανοποιείται

Αν $x_0 \in \mathbb{Z}$ είναι μια λύση της (1), τότε $\forall y \in [x_0]_n$ Ο ακέραιος y λύση της (1) δηλ:

$$y \in [x_0]_n \Rightarrow y \equiv x_0 \pmod n \rightarrow n/y-x_0 \Rightarrow$$

$$y - x_0 = \kappa n \text{ για κάποιο } \kappa \in \mathbb{Z} \Rightarrow y = x_0 + \kappa n \quad \kappa \in \mathbb{Z}$$

$$a \cdot y = a(x_0 + kn) = ax_0 + ax \cdot n \equiv b \bmod n$$

Άρα

y λύση της (1)

Άρα

Αν μια γραμμική ισοτιμία (*) έχει λύση τότε έχει άπειρες λύσεις στο $\mathbb{Z}$

Για την γραμμική ισοτιμία (*): $\exists x_0 \in \mathbb{Z} : ax_0 \equiv b \pmod n \Leftrightarrow$

$$\exists x_0 \in \mathbb{Z} : [ax_0]_n = [b]_n \Leftrightarrow \exists x_0 \in \mathbb{Z} :$$

$$[a]_n \cdot [x]_n = [b]_n \Leftrightarrow \text{η εξίσωση } [a]_n \cdot [x]_n = [b]_n$$

στο $\mathbb{Z}_n$ έχει μια λύση την $[x_0]_n$.

Πρόταση

Για κάθε ακέραιο $c \in \mathbb{Z}$ $[c]_n = [a]_n^{-1}$

a) $(a,n)=1 \Rightarrow \exists c,d \in \mathbb{Z}$ $1 = ac + dn \Rightarrow$

$[1]_n = [a]_n[c]_n + [dn]_n \xrightarrow{[a]_n} \Rightarrow$

$\Rightarrow [a]_n[c]_n = [1]_n \Rightarrow [c]_n = [a]_n^{-1}$

b) $(a,n)=1 \xrightarrow[\text{Euler}]{\text{Θεώρημα}} a^{\varphi(n)} \equiv 1 \pmod n \Rightarrow a^{\varphi(n)-1} a \equiv (1 \bmod n) \Rightarrow$

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

η λογαριθμική όλων των (1) είναι $b \cdot a^{\varphi(n)-1} \pmod n$

Παράδειγμα

$$137x \equiv 4 \pmod{102} \quad (1) \iff 35x \equiv 4 \pmod{102} \quad (1)$$

$(35, 102) = (5 \cdot 7,\ 2 \cdot 3 \cdot 17) = 1$

Άρα

η (1) έχει λογαριθμική όλων $\pmod{102}$ την $x_0 \equiv 4c \pmod{102}$,

δηλ

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

Μέσω του Ευκλείδειου Αλγορίθμου $\Rightarrow 1 = 35 \cdot 35 + (-12)102$.

Άρα

Θα έχουμε η λογαριθμική όλων $\pmod{102}$ της (1)

Θα είναι η $x_0 = 4 \cdot 35 \bmod (102) \equiv 140 \pmod{102} =$

$= 38 \pmod{102}$

$\varphi(102) = \varphi(2 \cdot 3 \cdot 17) = \varphi(2)\varphi(3)\varphi(17) = 1 \cdot 2 \cdot 16 = 32$

$35^{\varphi(102)} \equiv 1 \pmod{102} = 35$

$35^{32} \equiv 1 \pmod{102} \Rightarrow [35]_{102}^{-1} = [35^{31}]_{102}$

(Είναι $(a,n)=1 \Rightarrow \exists [a]_n^{-1}$ στο $\mathbb{Z}_n$)

Θέλουμε

αν y άλλη λύση της (1), τότε $y \equiv x_0 \pmod n$

Αλλιώς

$a \cdot x \equiv b \pmod n \Leftrightarrow [a]_n[x]_n = [b]_n$ στο $\mathbb{Z}_n$

Είναι

$(a,n)=1 \Rightarrow \exists [a]_n^{-1} \in \mathbb{Z}_n \quad [a]_n[a]_n^{-1} = [1]_n$

και

έστω ότι $[a]_n^{-1} = [c]_n$ $\left(U(\mathbb{Z}_n) = \{[k]_n \in \mathbb{Z}_n / \overset{1 \le k \le n-1}{(k,n)=1}\}\right)$

Τότε

$[a]_n[x]_n = [b]_n \Rightarrow [c]_n[a]_n[x]_n = [c]_n[b]_n \Rightarrow$

$[x]_n = [bc]_n$ άρα η λύση (ισοδύναμα $[bc]_n$ λύση της $[a]_n[x]_n = [b]_n$ και άρα ο ακέραιος bc λύση της $a \cdot x \equiv b \pmod n$

Αν $y \in \mathbb{Z}$ μια άλλη λύση της (1) $\Rightarrow a \cdot y \equiv b \pmod n \Rightarrow$

$[a]_n[y]_n = [b]_n \Rightarrow [c]_n[a]_n[y]_n = [c]_n[b]_n$

$\Rightarrow [y]_n = [bc]_n = [x_0]_n$.

Άρα

$y \equiv bc \pmod n \Rightarrow$ υπάρχει μοναδική λύση $\pmod n$ της (*)

$\left.\begin{matrix} ax \equiv b \pmod n \\ (a,n)=1 \end{matrix}\right\} \Rightarrow x_0 = b \cdot c \pmod n$ μοναδική λύση, όπου $c \in \mathbb{Z}$

$[c] = [a]_n^{-1}$

Άρα

Γραμμικές ισοτιμίες στο $\mathbb{Z}$ $\equiv$ Εξισώσεις στο $\mathbb{Z}_n$
(λύσεις) (κλάσεις)

Παρατήρηση

Η γραμμική ισοτιμία $6x \equiv 1 \pmod 8$ δεν έχει ακέραιες λύσεις. Διότι αν $x_0 \in \mathbb{Z}$

$$6x_0 \equiv 1 \pmod 8 \Rightarrow 8 \mid 6x-1 \Rightarrow$$

$2 \mid 6x-1$, άτοπο διότι $6x_0 - 1 = 2(3x) - 1$ περιττός

Παρατήρηση

Έστω η γραμμική ισοτιμία $2x \equiv 10 \pmod 6$ (1)

Η (1) γράφεται $2x \equiv 4 \pmod 6$ διότι $10 \equiv 4 \bmod 6$

- $x = 0 \Rightarrow 2 \cdot 0 = 0 \not\equiv 4 \pmod 6$
- $x = 1 \Rightarrow 2 \cdot 1 = 2 \not\equiv 4 \pmod 6$
- $x = 2 \Rightarrow 2 \cdot 2 = 4 \equiv 4 \pmod 6$
- $x = 3 \Rightarrow 2 \cdot 3 = 6 \not\equiv 4 \pmod 6$
- $x = 4 \Rightarrow 2 \cdot 4 = 8 \not\equiv 4 \pmod 6$
- $x = 5 \Rightarrow 2 \cdot 5 = 10 \equiv 4 \pmod 6$

$[2]_6 [x]_6 = [4]_6$

$\mathbb{Z}_6 = \{ [0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6 \}$

Άρα η (1) έχει δύο ανισόβαθμες mod 6 λύσεις τις:

$x_0 = 2$ και $x_0 = 5$

Πρόταση

Αν $(a, n) = 1$, τότε η γραμμική ισοτιμία $ax \equiv b \pmod n$ (1) έχει μοναδική λύση την: $x_0 = b \cdot c$, όπου $[c]_n = [a]_n^{-1}$.

Αν $(a,n)=1 \overset{\text{Euler}}{\Rightarrow} a^{\varphi(n)} \equiv 1 \pmod n \Rightarrow [a]_n^{-1} = [a^{\varphi(n)-1}]_n$

Όπως γενικά υπάρχουν θετικοί ακέραιοι τ:

$\tau < \varphi(n)$ $a^\tau \equiv 1 \pmod n \Rightarrow$

$a \cdot a^{\tau-1} \equiv 1 \pmod n \Rightarrow [a]_n^{-1} = [a^{\tau-1}]_n$

Θεώρημα

Η γραμμική ισοτιμία $ax \equiv b \pmod n$ $(*)$ έχει λύση $\Leftrightarrow \delta = (a,n) \mid b$. Αν $\delta \mid b$ και x_0 είναι μια λύση της $(*)$ τότε όλες οι ανά δύο αντίθετες λύσεις της $(*)$ είναι:

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

Απόδειξη

$(\Rightarrow)$ Έστω ότι x_0 είναι λύση της $(*)$

Τότε:

$$ax_0 \equiv b \pmod n \Rightarrow n \mid ax_0 - b$$

Επειδή

$$\delta = (a,n) \rightarrow \delta \mid n \quad \left.\begin{matrix} \\ n \mid ax_0 - b \end{matrix}\right\} \Rightarrow \delta \mid ax_0 - b \Rightarrow \delta \mid b$$

$$\delta \mid a \Rightarrow \delta \mid ax_0$$

$(\Leftarrow)$ Υποθέτουμε ότι $\delta = (a,n) \mid b$

Τότε

$$\delta \mid a,\ \delta \mid b\ \delta \mid n$$

Τότε

θεωρούμε τη γραμμική ισοτιμία $\frac{a}{\delta} x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}}$ (2

και

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

Τότε η γραμμική ισοτιμία έχει λύσεις όλους (mod $\frac{n}{\delta}$) τους x_0

$ax \equiv b \pmod n \Rightarrow n \mid ax - b \Rightarrow \exists k \in \mathbb{Z} : ax - b = nk$

$\Rightarrow \exists k \in \mathbb{Z} : \frac{a}{\delta} x - \frac{b}{\delta} = \frac{n}{\delta} k \Leftrightarrow$

$\frac{n}{\delta} \mid \frac{a}{\delta} x - \frac{b}{\delta}$, για κάποιο $k \in \mathbb{Z} \Leftrightarrow \frac{a}{\delta} x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}}$

Έστω $\frac{a}{\delta} x_0 \equiv \frac{b}{\delta} \left(\mod \frac{n}{\delta}\right)$, οι παραπάνω ισοδύναμες ⇒ x_0 λύση της (*) $ax_0 \equiv b \pmod n$

• Έστω οι ακέραιοι $x_0 + k\frac{n}{\delta}$, $0 \le k \le \delta - 1$

(λύσεις της αρχικής)

Τότε

$a\left(x_0 + k\frac{n}{\delta}\right) \equiv ax_0 + ak\frac{n}{\delta} \equiv b + k \cdot \frac{an}{\delta} \equiv b \pmod n$

(ακέραιο πολλαπλάσιο του n)

Άρα

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

λύσεις της (*)

Αν

$x_0 + k\frac{n}{\delta} \equiv x_0 + \lambda\frac{n}{\delta} \pmod n \Rightarrow n \mid \left(x_0 + k\frac{n}{\delta}\right) - \left(x_0 + \lambda\frac{n}{\delta}\right) \Rightarrow$

$n \mid (k-\lambda)\frac{n}{\delta} \Rightarrow \delta \mid k - \lambda \Rightarrow \delta \le k - \lambda$

$0 \le k, \lambda \le \delta - 1$ $\Rightarrow k = \lambda$

Άρα

οι λύσεις $x_0 + k\frac{n}{\delta}$, $0 \le k \le \delta - 1$ είναι ανά δύο ανισόδιλες (mod n)

Έστω x_0' μια τυχαία λύση της αρχικής ισοδύναμης (*) τότε η x_0' λύση και η (2).

Επειδή η (2) έχει δοθείσα λύση την x_0, έπεται ότι:

$$x_0' \equiv x_0 \bmod \frac{n}{\delta} \Rightarrow \frac{n}{\delta} \mid x_0' - x_0 \Rightarrow$$

$$\Rightarrow x_0' - x_0 = k\frac{n}{\delta} \Rightarrow x_0' = x_0 + k\frac{n}{\delta}$$

Αλλά

αν διαιρέσουμε το k με το δ θα έχουμε

$k = m\cdot\delta + \tau$, όπου $0 \le \tau \le \delta - 1$. Τότε $x_0' = x_0 + (m\delta + \tau)\frac{n}{\delta}$

$$= x_0 + \frac{m\delta n}{\delta} + \tau\frac{n}{\delta} = x_0 + mn + \tau\frac{n}{\delta} \equiv$$

$$\equiv x_0 + \tau\frac{n}{\delta} \qquad 0 \le \tau \le \delta - 1$$

Άρα

κάθε άλλη λύση x_0' της (*) είναι ίσου/η mod n με μια από τις $x_0 + \tau\frac{n}{\delta}$, $0 \le \tau \le \delta - 1$