10/12/2018

Γραμμικές Ισοτιμίες

Πρόταση Έστω a,b,n ακέραιοι με $a \neq 0$ και $n \geq 2$. Υπάρχουν $x \in \mathbb{Z}$ ώστε $ax \equiv b \bmod n$ (*) ($\Leftrightarrow n \mid ax-b$)
Αν ναι, βρείτε όλες τις λύσεις $x \in \mathbb{Z}$ της (*).

Η (*) λέγεται γραμμική ισοτιμία.

Παράδειγμα Βρείτε τα $x \in \mathbb{Z}$ ώστε $2x \equiv 1 \bmod 2$ (**)

Λύση: $2x \equiv 1 \bmod 2 \Leftrightarrow 2 \mid 2x-1$ Άρα για κάθε $x \in \mathbb{Z}$, ο $2x-1$ είναι περιττός άρα $2 \nmid 2x-1$.

Συμπέρασμα: Η ισοτιμία (**) δεν έχει λύσεις στο $\mathbb{Z}$.

Παράδειγμα: Βρείτε τα $x \in \mathbb{Z}$ ώστε $x \equiv 3 \bmod 7$ (***)

Λύση: $x \equiv 3 \bmod 7 \Leftrightarrow$ το υπόλοιπο της Ευκλ. διαιρ. του x με το 7 είναι $\Leftrightarrow x \in \{3+t7 \mid t \in \mathbb{Z}\} =$
$= \{\ldots, 3-2\cdot 7, 3-7, 3, 3+7, 3+2\cdot 7, 3+3\cdot 7 \ldots\}$
$\ldots -11 \quad -4 \quad 10 \quad 17 \quad 24$

Πρόταση: Έστω $n \geq 2$, $b \in \mathbb{Z}$. Το σύνολο λύσεων $a \in \mathbb{Z}$ της ισοτιμίας $x \equiv b \bmod n$ (1) είναι ίσο με $A = \{b+tn : t \in \mathbb{Z}\}$.

Απόδειξη: Έστω $t \in \mathbb{Z}$
Τότε $(b+tn)-b = t \cdot n$, άρα $n \mid (b+t \cdot n)-b \Rightarrow b+tn$ λύση της (1).
Αντίστροφα, έστω $x \in \mathbb{Z}$ λύση της (1). Τότε: $x \equiv b \bmod n \Rightarrow n \mid x-b \Rightarrow$ υπάρχει $t \in \mathbb{Z}$ ώστε $x-b = tn \Rightarrow x = b+tn$. Άρα $x \in A$.

Ορισμός: Έστω $n \geq 2$. Ένα υποσύνολο $S \subseteq \mathbb{Z}$ λέγεται **ΚΛΑΣΗ ΙΣΟΤΙΜΙΑΣ** modulo n αν υπάρχει $b \in \mathbb{Z}$ ώστε $S = \{b + tn : t \in \mathbb{Z}\}$. Με άλλα λόγια αυτό σημαίνει ότι το S περιέχει ακριβώς τους ακεραίους που το υπόλοιπο της Ευκ. Διαίρεσης τους με το n είναι το ίδιο με το υπόλοιπο της Ευκ. Διαιρ. του b με το n.

Παράδειγμα: Οι άρτιοι είναι κλάση ισοτιμίας modulo 2, για $b = 0$ γιατί
$S_2 = \{0 + t2 \mid t \in \mathbb{Z}\}$ Το σύνολο S_2 των περιττών είναι κλάση ισοτιμίας modulo 2, γιατί για $b = 1$ $S_2 = \{1 + 2t \mid t \in \mathbb{Z}\}$
Το σύνολο S_3 των πολλαπλ. του 5 είναι κλάση ισοτιμίας modulo 5, γιατί για $b = 0$ $S_3 = \{0 + t5 : t \in \mathbb{Z}\}$

Παρατήρηση: Η πρόταση λέει ότι το σύνολο λύσεων στο $\mathbb{Z}$ της ισοτιμίας $x \equiv b \bmod n$ είναι ΚΛΑΣΗ ΙΣΟΤΙΜΙΑΣ MODULO n.

Ορισμός: Έστω $a, a', b, b', n, n' \in \mathbb{Z}$ με $a \neq 0$, $a' \neq 0$ $n \geq 2$ και $n' \geq 2$. Οι ισοτιμίες $ax \equiv b \bmod n$ και $a'x \equiv b' \bmod n'$ λέγονται **ΙΣΟΔΥΝΑΜΕΣ** αν έχουν το ίδιο σύνολο λύσεων στο $\mathbb{Z}$.

Παράδειγμα: Οι ισοτιμίες $x \equiv 1 \bmod 2$ και $x \equiv 3 \bmod 2$ είναι ισοδύναμες, γιατί έχουν το ίδιο σύνολο λύσεων στο $\mathbb{Z}$, δηλ. τους περιττούς αριθμούς

Αντίθετα, οι ισοτιμίες $2x \equiv 1 \bmod 3$ και $2x \equiv 2 \bmod 3$ δεν είναι ισοδύναμες, γιατί το $x=2$ είναι λύση της πρώτης, αλλά όχι της δεύτερης.

Πρόταση Έστω $a,b,n \in \mathbb{Z}$ με $a \neq 0$ και $n \geq 2$. Θεωρούμε $d = \text{ΜΚΔ}(a,n)$. Αν d ΔΕΝ διαιρεί το b τότε η ισοτιμία $ax \equiv b \bmod n$ δεν έχει λύσεις στο $\mathbb{Z}$.

Απόδειξη: Έστω ότι δεν ισχύει και $x \in \mathbb{Z}$ λύση. Τότε $ax \equiv b \bmod n$ άρα $n \mid ax-b$, δηλαδή υπάρχει $t \in \mathbb{Z}$ με $ax-b = tn \Rightarrow b = ax - tn$ (2). Τώρα $d \mid a$ και $d \mid n \overset{(2)}{\Rightarrow} d \mid b$ αντίφαση.

Παράδειγμα: Η ισοτιμία $4x \equiv 2 \bmod 8$ δεν έχει (από την πρόταση) λύσεις $x \in \mathbb{Z}$, γιατί $\text{ΜΚΔ}(4,8) = 4$ και 4 ΔΕΝ διαιρεί το 2.

Πρόταση: Έστω $a,b,n \in \mathbb{Z}$ με $a \neq 0$ και $n \geq 2$. Θεωρούμε $d = \text{ΜΚΔ}(a,n)$ υποθέτουμε $d \mid b$.
Τότε, οι ισοτιμίες $ax \equiv b \bmod n$ (1) και $\left(\frac{a}{d}\right)x = \left(\frac{b}{d}\right) \bmod \left(\frac{n}{d}\right)$ (2) είναι ισοδύναμες, δηλ. έχουν το ίδιο σύνολο λύσεων στο $\mathbb{Z}$.

Απόδειξη: Έστω $x \in \mathbb{Z}$ με $ax \equiv b \bmod n \Rightarrow n \mid ax-b \Rightarrow \frac{n}{d} \mid \frac{ax-b}{d} \Rightarrow \frac{n}{d} \mid \frac{a}{d}x - \frac{b}{d} \Rightarrow x$ λύση της (2).

Αντίστροφα, Έστω $x \in \mathbb{Z}$ λύση της (2). Τότε $\frac{n}{d} \mid \frac{ax}{d} - \frac{b}{d} \Rightarrow$

$n \mid ax-b \Rightarrow x$ λύση της (1).

Παρατήρηση: Από γνωστη πρόταση, αφού $d = \text{ΜΚΔ}(a,n)$ έπεται:
$\text{ΜΚΔ}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$

Παραδειγμα: Από πρόταση, η ισοτιμία $3x \equiv b \bmod 9$ είναι ισοδύναμη με την ισοτιμία $\frac{3}{3}x \equiv \frac{b}{3} \bmod \frac{9}{3}$ δηλ $x \equiv \ldots \bmod 3$. Άρα από πρόταση το σύνολο λύσεων της $3x \equiv b \bmod 9$ είναι ίσο με το σύνολο λύσεων της $x \equiv \ldots \bmod 3$, που από πρόταση είναι ίσο με $\{\ldots + t3 \mid t \in \mathbb{Z}\}$

Πρόταση: Έστω $a, b, c, n \in \mathbb{Z}$ με $n \geq 1$ αυτό και $\text{ΜΚΔ}(c,n) = 1$. Τότε οι ισοτιμίες $ax \equiv b \bmod n$ και $cax \equiv cb \bmod n$ είναι ισοδύναμες

Απόδειξη: Έστω $x \in \mathbb{Z}$. Υποθέτουμε $ax \equiv b \bmod n \Rightarrow n \mid ax - b \Rightarrow n \mid c(ax-b) \Rightarrow n \mid acx - bc \Leftrightarrow cax \equiv cb \bmod n$.

Αντίστροφα: έστω $cax \equiv cb \bmod n$. Άρα $n \mid cax - cb \Rightarrow n \mid c(ax-b)$ (*)
Αφού $\text{ΜΚΔ}(n,c) = 1$, n (*) $\Rightarrow n \mid ax - b \Rightarrow ax \equiv b \bmod n$

Ανισοτιμίες: Έστω $a, b, n \in \mathbb{Z}$ με $a \neq 0$ και $n \geq 1$ και (*) n θέλουμε ισοτιμία: $ax \equiv b \bmod n$.
Βήμα - 1ο: Θέτουμε $d = \text{ΜΚΔ}(a,n)$
Αν $d \nmid b$ τότε n (*) αδύνατη στο $\mathbb{Z}$.
Βήμα - 2ο: Υποθέτουμε $d \mid b$ τότε θέτουμε $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $n' = \frac{n}{d}$, και n (*) έχει ίδιο σύνολο λύσεων με την (**) $a'x \equiv b' \bmod n'$.

ΒΗΜΑ 3ο: Αφού $d = ΜΚΔ(a, n)$ έπεται $ΜΚΔ(a', n') = 1$. Άρα, από γνωστό Αλγόριθμο υπολογίζουμε $c' \in \mathbb{Z}$ ώστε $([a']_n)^{-1} = [c']_n$ (δηλ. $a'c' \equiv 1 \bmod n'$).

ΒΗΜΑ 4ο: Από τα παραπάνω το ζητούμενο σύνολο λύσεων στο $\mathbb{Z}$ της (*) είναι το $S = \{c'b' + tn' / t \in \mathbb{Z}\}$.

ΠΑΡΑΤΗΡΗΣΗ: Όταν $d|b$, το σύνολο λύσεων S της (*) είναι **ΚΛΑΣΗ ΙΣΟΤΙΜΙΑΣ** modulo n'

ΠΑΡΑΔΕΙΓΜΑ 8 - ΑΣΚΗΣΗ 1:

(i) $5x \equiv 2 \bmod 8$ (*)

ΒΗΜΑ-1ο: Θέτουμε $d = ΜΚΔ(5, 8) = 1$. Αφού $1|2$ η (*) έχει λύσεις στο $\mathbb{Z}$

ΒΗΜΑ-2ο: Θέτουμε $a' = \frac{a}{d} = \frac{5}{d} = 5$, $b' = \frac{2}{1} = 2$, $n' = \frac{n}{1} = n = 8$

Η (*) γίνεται $5x \equiv 2 \bmod 8$ (**)

ΒΗΜΑ-3ο: Υπολογίζουμε $c' \in \mathbb{Z}$ με $([5]_8)^{-1} = [c']_8$ δηλ. $5c' \equiv 1 \bmod 8$. Με Ευκλ. Αλγορ. (ή δοκιμές) θέτουμε: $c' = 5$

ΒΗΜΑ-4ο: Επομένως η (*) έχει σύνολο λύσεων

$S = \{5 \cdot 2 + t \cdot 8 / t \in \mathbb{Z}\} = \{10 + t \cdot 8 : t \in \mathbb{Z}\} =$

$= \{2 + t \cdot 8 : t \in \mathbb{Z}\} = \{\ldots 2 - 16 = -14, 2 - 8 = -6, 2, 2 + 8 = 10, 2 + 16 = 18, \ldots\}$ = Σύνολο των ακεραίων x που στην Ευκλ. διαιρ. με το 8 αφήνουν υπόλοιπο 2 = Σύνολο των ακεραίων της μορφής $8q + 2$

(ii) $13x \equiv 6 \bmod 26$

ΛΥΣΗ: ΒΗΜΑ - 1ο: Θέτουμε $d = ΜΚΔ(13, 26) = 13$

Έτσαμε $13 \nmid 6$ Συνεπώς η ισοτιμία ΔΕΝ έχει λύσεις στο $\mathbb{Z}$.

(iii) $3x \equiv 9 \bmod 30$

ΛΥΣΗ ΒΗΜΑ - 1ο: Υπολογίζουμε $d = ΜΚΔ(3, 30) = 3$

Έτσαμε $d \mid 9$

ΒΗΜΑ - 2ο: Θέτουμε $a' = \frac{a}{3} = 1$, $b' = \frac{b}{3} = 3$

$n' = \frac{n}{3} = 10$. Άρα η (*) είναι ισοδύναμη με την

$a'x \equiv b' \bmod n'$, δηλ. $x \equiv 3 \bmod 10$ (**)

Επομένως, το σύνολο λύσεων της (*) είναι ίδιο με το σύνολο λύσεων της (**) που είναι το $S = \{3 + t \cdot 10 : t \in \mathbb{Z}\} =$

$= \{\ldots, -57, -47, -37, -27, -17, -7, 3, 13, 23, 33, 43, 53, \ldots\}$

$= \{x \in \mathbb{Z} :$ το υπόλοιπο της Ευκλ. διαιρ. του x με το 10 είναι $3\}$

= το σύνολο των ακεραίων της μορφής $10q + 3$.

ΠΡΟΒΛΗΜΑ 8 - ΑΣΚΗΣΗ 3: Για ποια b, με $0 \le b \le 29$ έχει λύση η ισοτιμία $12x \equiv b \bmod 30$.

ΛΥΣΗ: Θέτουμε $d = ΜΚΔ(12, 30) = ΜΚΔ(2^2 \cdot 3, 2 \cdot 3 \cdot 5) =$

$= ΜΚΔ(2^0 \cdot 3^1 \cdot 5^0, 2^1 \cdot 3^1 \cdot 5^1) = ΜΚΔ(2^{\min(0,1)} \cdot 3^{\min(1,1)} \cdot 5^{\min(0,1)}) = 6$

Συνεπώς, η ισοτιμία έχει λύση αν-ν $6 \mid b$ και αφού

$0 \le b \le 29$, η ισοτιμία έχει λύση αν-ν $b \in \{0, 6, 12, 18, 24\}$