ΓΡΑΜΜΙΚΕΣ ΙΣΟΤΙΜΙΕΣ

Έστω $n>1$ κ' $a,b\in\mathbb{Z}$. Θεωρούμε την εξίσωση (για $x\in\mathbb{Z}$)

$$ax \equiv b \bmod n \quad (*)$$

Με άλλα λόγια, το $x\in\mathbb{Z}$ είναι λύση της $(*)$ αν $n \mid ax-b$.

Π.χ. Το 1 είναι λύση της $4x\equiv 1 \bmod 3$, ενώ το 2 δεν είναι, γιατί

$$[4\cdot 2]_3 = [2]_3 \neq [1]_3$$

Πρόταση: Έστω $x,y\in\mathbb{Z}$ με $x\equiv y \bmod n$. Τότε το x είναι λύση της $(*)$ αν το y είναι λύση της $(*)$.

Απόδειξη: $x\equiv y \bmod n \Rightarrow [x]_n=[y]_n \Rightarrow [a]_n[x]_n=[a]_n[y]_n$
$\Rightarrow [ax]_n=[ay]_n \Rightarrow ax\equiv ay \bmod n$

Άρα $ax\equiv b \bmod n$ αν $ay\equiv b \bmod n$

Ορισμός: Λέμε ότι το $x\in\mathbb{Z}$ λύση της $(*)$ αν $ax\equiv b \bmod n$
Λέμε το $[x]_n\in\mathbb{Z}_n$ —||— αν $ax\equiv b \bmod n$

ΕΡΩΤΗΜΑΤΑ: (1): Πότε η $ax\equiv b \bmod n$ έχει λύση στο $\mathbb{Z}_n$;
(2) Αν έχει λύση στο $\mathbb{Z}_n$, πόσες έχει;

Π.χ. Η $6x\equiv 1 \bmod 4$ δεν έχει λύση στο $\mathbb{Z}_n$ ούτε στο $\mathbb{Z}$, γιατί αν $x\in\mathbb{Z}$,
$6x-1$ περιττός, άρα $2\nmid 6x-1$ άρα $4\nmid 6x-1$

Πρόταση: Έστω $n\geq 2$ $a,b\in\mathbb{Z}$. Υποθέτουμε $\text{ΜΚΔ}(a,n)\nmid b$.
Τότε η ισοτιμία $ax\equiv b \bmod n$ ΔΕΝ έχει λύση στο $\mathbb{Z}$, άρα ούτε στο $\mathbb{Z}_n$.

Απόδειξη: Έστω ότι $\exists x\in\mathbb{Z}$ με $ax\equiv b \bmod n$.
Άρα $n\mid ax-b$, συνεπώς $\exists k\in\mathbb{Z}$ με $ax-b=kn$, άρα $b=ax-kn$ $(*)$
Θέτουμε $d=\text{ΜΚΔ}(a,n)$. Αφού $d\mid a$ κ' $d\mid n \overset{(**)}{\Rightarrow} d\mid b$, αντίφαση

Πρόταση: Έστω $n \geq 2$, $a, b \in \mathbb{Z}$ με $\text{μκδ}(a,n)=1$.
Έστω $c \in \mathbb{Z}$ με $([a]_n)^{-1} = [c]_n$. Τότε η ισοτιμία

$$ax \equiv b \bmod n$$

έχει μοναδική λύση στο $\mathbb{Z}_n$, την $[cb]_n$

(Παρατήρηση: Αφού $\text{μκδ}(a,n)=1$, ξέρουμε $[a]_n \in U(\mathbb{Z}/n)$, δηλαδή $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμο)

Απόδειξη: **Βήμα 1ο:** ΙΣΧΥΡΙΣΜΟΣ Το $cb \in \mathbb{Z}$ της (*)

Πράγματι, $[a \cdot cb]_n = [a]_n[c]_n[b]_n = [a]_n([a]_n)^{-1}[b]_n = [1]_n[b]_n =$
$= [b]_n$

άρα $a(cb) \equiv b \bmod n$

Βήμα 2ο: ΙΣΧΥΡΙΣΜΟΣ Έστω $k \in \mathbb{Z}$ λύση της (*). Τότε $[k]_n = [cb]_n$

Απόδειξη:

$ak \equiv b \bmod n \Rightarrow [ak]_n = [b]_n \Rightarrow [a]_n[k]_n = [b]_n \Rightarrow$

$\Rightarrow ([a]_n)^{-1}[a]_n[k]_n = ([a]_n)^{-1}[b]_n \Rightarrow$

$\Rightarrow [1]_n[k]_n = [c]_n[b]_n \Rightarrow [k]_n = [cb]_n$

ΠΑΡΑΤΗΡΗΣΗ: Η $[cb]_n \in \mathbb{Z}_n$ είναι η μοναδική λύση στο $\mathbb{Z}_n$, σύμφωνα με την πρόταση. Το σύνολο λύσεων στο $\mathbb{Z}$ είναι το εξής:

$$\{cb + t \cdot n \mid t \in \mathbb{Z}\}$$

Πχ Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ κ' στο $\mathbb{Z}_5$ της ισοτιμίας $3x \equiv 1 \bmod 5$

Λύση:

Έχουμε $\text{μκδ}(3,5) = 1$ κ' $([3]_5)^{-1} = [2]_5$

Συνεπώς, από την πρόταση

(1) Στο $\mathbb{Z}_5$ έχει μοναδική λύση στο $\mathbb{Z}$, την $[2]_5[1]_5 = [2]_5$

(2) Από την παρατήρηση, στο $\mathbb{Z}$, το σύνολο λύσεων είναι $\{2 + t \cdot 5 \mid t \in \mathbb{Z}\} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\} = [2]_5$

ΕΡΩΤΗΜΑ: Τι γίνεται για την $ax \equiv b \bmod n$ όταν $ΜΚΔ(a,n) \mid b$, αλλά $ΜΚΔ(a,n) > 1$;

Υπενθύμιση: 1) Η ισοτιμία $ax \equiv b \bmod n$ είναι αδύνατη για $x \in \mathbb{Z}$ αν $ΜΚΔ(a,n) \nmid b$

2) Αν $ΜΚΔ(a,n) = 1$, η παραπάνω ισοτιμία έχει μοναδική λύση στο $\mathbb{Z}_n$ κ' άπειρες στο $\mathbb{Z}$.

Ορισμός: Δύο ισοτιμίες $ax \equiv b \bmod n$ κ' $a'x \equiv b' \bmod n'$ λέγονται ισοδύναμες, αν έχουν τις ίδιες λύσεις στο $\mathbb{Z}$.

Πρόταση: Έστω $n \geq 2$, $a, b \in \mathbb{Z}$ με $ΜΚΔ(a,n) > 1$ κ' $ΜΚΔ(a,n) \mid b$.
Τότε η ισοτιμία $ax \equiv b \bmod n$ είναι ισοδύναμη με την $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d}$, όπου $d = ΜΚΔ(a,n)$.

Απόδειξη: Έστω $x \in \mathbb{Z}$ με $ax \equiv b \bmod n$. Άρα $n \mid ax - b$. Άρα $\exists k \in \mathbb{Z}$ με
$ax - b = kn \quad (*)$
Αφού $d \mid a$ κ' $d \mid b$ κ' $d \neq 0$, η $(*) \Rightarrow \frac{a}{d}x - \frac{b}{d} = k\frac{n}{d}$
Άρα $\frac{n}{d} \mid \frac{a}{d}x - \frac{b}{d}$, συνεπώς $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d}$

Έστω τώρα $x \in \mathbb{Z}$ με $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d}$. Άρα $\frac{n}{d} \mid \frac{a}{d}x - \frac{b}{d}$. Άρα $\exists k \in \mathbb{Z}$
με $\frac{a}{d}x - \frac{b}{d} = k\frac{n}{d} \Rightarrow ax - b = kn \Rightarrow n \mid ax - b \Rightarrow ax \equiv b \bmod n$

π.χ. Η ισοτιμία $2x \equiv 12 \bmod 4$ έχει $d = ΜΚΔ(a,n) = ΜΚΔ(2,4) = 2 \mid b = 12$
Άρα από πρόταση είναι ισοδύναμη με την ισοτιμία
$\frac{2}{d}x \equiv \frac{12}{d} \bmod \frac{4}{d}$, δηλαδή την $x \equiv 6 \bmod 2$.

Αλγόριθμος: Έστω $n \geq 2$ $a, b \in \mathbb{Z}$ με $ΜΚΔ(a,n) > 1$ κ' $ΜΚΔ(a,n) \mid b$.
Επίλυση ισοτιμίας $ax \equiv b \bmod n$ για $x \in \mathbb{Z}$
Βήμα 1ο: Θέτουμε $a' = \frac{a}{ΜΚΔ(a,n)}$, $b' = \frac{b}{ΜΚΔ(b,n)}$, $c' = \frac{c}{ΜΚΔ(c,n)}$ κ'

Έχουμε την ισοδύναμη ισοτιμία $a'x \equiv b' \bmod n'$

Βήμα 2º: Αφού από πρόταση $ΜΚΔ(a', n') = 1$, εφαρμόζουμε πρόταση
Άρα έχω $c' \in \mathbb{Z}$ με $a'c' \equiv 1 \bmod n'$ (ισοδύναμα $([c']_{n'}) = ([a']_{n'})^{-1}$
Τότε το σύνολο λύσεων της ισοτιμίας στο $\mathbb{Z}$ είναι το εξής:
$\{c'b' + tn' \mid t \in \mathbb{Z}\}$

Επιπλέον στο $\mathbb{Z}_n$ η αρχική ισοτιμία έχει ακριβώς $ΜΚΔ(a, n)$ λύσεις, τις εξής:
$\{[c'b']_n, [c'b' + n']_n, [c'b' + 2n']_n, \ldots, [c'b' + (d-1)n']_n\}$,

όπου $d = ΜΚΔ(a, n)$

(1) Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ κ' το $\mathbb{Z}_{12}$ της ισοτιμίας $3x \equiv 6 \bmod 12$

Λύση: Έχουμε $a = 3, b = 6, n = 12$. $d = ΜΚΔ(a, n) = 3 \mid 6 = b$.

Θέτουμε $a' = \frac{a}{d} = \frac{3}{3} = 1$, $b' = \frac{b}{d} = 2$, $n' = \frac{12}{3} = 4$
Βήμα 1º: Θεωρούμε την ισοδύναμη ισοτιμία
$a'x \equiv b' \bmod n'$, ισοδύναμα $1x \equiv 2 \bmod 4$
Βήμα 2º: Έχουμε $([1]_4)^{-1} = [1]_4$, θέτουμε $c' = 1$
Από τον Αλγ. το σύνολο λύσεων στο $\mathbb{Z}$ είναι
$\{2 + t\,4 \mid t \in \mathbb{Z}\} = \{\ldots, -10, -6, -2, 2, 6, 10 \ldots\}$
Στο $\mathbb{Z}_{12}$ η ισοτιμία έχει $d = 3$ λύσεις τις εξής:
$[2]_{12}, [6]_{12}, [10]_{12}$

Φυλ 8 ασκ 3. Για $c \in \mathbb{Z}$ με $0 \le c \le 20$ έχει η ισοτιμία $12x \equiv c \bmod 30$
λύση στο $\mathbb{Z}$. Όταν έχει, πόσες ανισότιμες λύσεις $(\bmod 30)$ υπάρχουν;
Λύση: Έχουμε $d = ΜΚΔ(12, 30) = ΜΚΔ(12, 30 - 2 \cdot 12) = ΜΚΔ(12, 6) =$
$= ΜΚΔ(12 - 2 \cdot 6, 6) = ΜΚΔ(0, 6) = 6$
Έχει λύση ανν $d \mid c$, ισοδύναμα $6 \mid c$, ισοδύναμα $c \in \{0, 6, 12, 18\}$
Από Αλγόριθμο έχει, για $c \in \{0, 6, 12, 18\}$ $ΜΚΔ(a, n) = d = 6$ λύσεις στο $\mathbb{Z}_{30}$.

ΚΙΝΕΖΙΚΟ ΘΕΩΡΗΜΑ ΥΠΟΛΟΙΠΩΝ

Έστω ότι έχουμε το σύστημα ισοτιμιών (για $x \in \mathbb{Z}$)

$$(\mathcal{E}) \begin{cases} a_1 x \equiv b_1 \bmod n_1 \\ a_2 x \equiv b_2 \bmod n_2 \\ \vdots \\ a_s x \equiv b_s \bmod n_s \end{cases}$$

όπου $a_i, b_i, n \in \mathbb{Z}$ με $n_i \geq 1$

Βήμα 1ο: Αν $\exists\, i$ με $\text{ΜΚΔ}(a_i,n_i) \nmid b_i$ το $(\mathcal{E})$ είναι αδύνατο.

Βήμα 2ο: Υποθέτουμε ότι $\text{ΜΚΔ}(a_i,n_i) \mid b_i \ \forall i$

Από τα παραπάνω έχουμε το ισοδύναμο σύστημα

$$\frac{a_1}{\text{ΜΚΔ}(a_1,n_1)} x \equiv \frac{b_1}{\text{ΜΚΔ}(a_1,n_1)} \bmod \frac{n}{\text{ΜΚΔ}(a_1,n_1)}$$

$$\frac{a_2}{\text{ΜΚΔ}(a_2,n_2)} x \equiv \frac{b_2}{\text{ΜΚΔ}(a_2,n_2)} \bmod \frac{n}{\text{ΜΚΔ}(a_2,n_2)}$$

$$\vdots$$

$$\frac{a_s}{\text{ΜΚΔ}(a_s,n_s)} x \equiv \frac{b_s}{\text{ΜΚΔ}(a_s,n_s)} \bmod \frac{n_s}{\text{ΜΚΔ}(a_s,n_s)}$$

Βήμα 3ο: Για $i = 1,2,\dots,s$ υπολογίζουμε $c_i \in \mathbb{Z}$ λύση της ισοτιμίας

$$\frac{a_i}{\text{ΜΚΔ}(a_i,n_i)} x \equiv 1 \bmod \frac{n_i}{\text{ΜΚΔ}(a_i,n_i)}$$

με άλλα λόγια $[c_i]_{\frac{n_i}{\text{ΜΚΔ}(a_i,n_i)}} = \left[\frac{a_i}{\text{ΜΚΔ}(a_i,n_i)}\right]^{-1}_{\frac{n_i}{\text{ΜΚΔ}(a_i,n_i)}}$

$$(\mathcal{E}'') \begin{cases} x \equiv c_1 \dfrac{b_1}{\text{ΜΚΔ}(a_1,n_1)} \bmod \dfrac{n_1}{\text{ΜΚΔ}(a_1,n_1)} \\ \vdots \\ x \equiv c_s \dfrac{b_s}{\text{ΜΚΔ}(a_s,n_s)} \bmod \dfrac{n_s}{\text{ΜΚΔ}(a_s,n_s)} \end{cases}$$

(Πχ) $6x \equiv 3 \mod 15$

$2x \equiv 4 \mod 8$

· Για την $6x \equiv 3 \mod 15$ $(*_1)$, έχουμε $d_1 = ΜΚΔ(a_1, n_1) = ΜΚΔ(6, 15) = 3$ κ' $3|3$

Άρα $(*_1)$ ισοδύναμη (από πρόταση) με $\left(\frac{6}{3}\right)x \equiv \left(\frac{3}{3}\right) \mod \left(\frac{15}{3}\right)$

δηλ. $2x \equiv 1 \mod 5$ $(*_2)$

Έχουμε $c_1 = 3$ άρα η $(*_2)$ είναι ισοδύναμη με την $x \equiv 3 \mod 5$

Για την $2x \equiv 4 \mod 8$, έχουμε $ΜΚΔ(2,8) = 2|4$, άρα είναι ισοδύναμη με την

$\frac{2}{2}x \equiv \frac{4}{2} \mod \frac{8}{2}$, δηλαδή $x \equiv 2 \mod 4$

Άρα το αρχικό σύστημα είναι ισοδύναμο με το

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 2 \mod 4 \end{cases}$$

Έστω ότι $n_i \geq 2$ κ' $c_i \in \mathbb{Z}$ κ' έχουμε το σύστημα

$$\begin{cases} x \equiv c_1 \mod n_1 \\ x \equiv c_2 \mod n_2 \\ \vdots \\ x \equiv c_s \mod n_s \end{cases}$$

Επιπλέον υπόθεση: $ΜΚΔ(n_i, n_j) = 1$ $\forall i \neq j$

(χωρίς απόδειξη)

Θεώρημα: Υποθέτουμε ότι έχουμε το σύστημα (Σ) κ' επιπλέον υπόθεση

$ΜΚΔ(n_i, n_j) = 1$ για $i \neq j$

Θέτουμε $N = n_1 n_2 \cdots n_s$

$N_i = \frac{N}{n_i}$, για $i = 1, 2, \dots, s$

Υπολογίζουμε $b_i \in \mathbb{Z}$ με $b_i N_i \equiv 1 \mod n_i$, λύνοντας την $N_i x \equiv 1 \mod n_i$

Τότε το σύνολο λύσεων του (Σ) στο $\mathbb{Z}$ είναι ΑΠΕΙΡΟ κ' είναι το εξής:

$$S = \left\{ \left(\sum_{i=1}^{s} b_i N_i c_i \right) + tN \mid t \in \mathbb{Z} \right\}$$

Φυλ 8 ασκ 4 (παραλλαγή) Δ.ο. ∃ ακέραιος κ, που είναι πολλαπλάσιο του 11 κ' είναι υπόλοιπο 1 όταν διαιρείται με τους αριθμούς 2,3,5 κ' 7.

Λύση: Θεωρούμε το σύστημα (γραμμικών) ισοτιμιών

$$\begin{cases} x \equiv 0 \bmod 11 \\ x \equiv 1 \bmod 2 \\ x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 5 \\ x \equiv 1 \bmod 7 \end{cases}$$

Έχουμε $n_1 = 11, n_2 = 2, n_3 = 3, n_4 = 5, n_5 = 7$. Φανερά ΜΚΔ$(n_i, n_j) = 1$ για $i \neq j$.
Άρα από Κινέζικο Θεώρημα υπολοίπων ∃ ακέραια λύση του συστήματος

Θεώρημα: Έστω $n_i \geq 2$, $c_i \in \mathbb{Z}$. Θεωρούμε το σύστημα

$$(\Sigma) \begin{cases} x \equiv c_1 \bmod n_1 \\ x \equiv c_2 \bmod n_2 \\ \vdots \\ x \equiv c_s \bmod n_s \end{cases}$$

Το (Σ) έχει λύση στο $\mathbb{Z}$ αν $\forall i \neq j$ ΜΚΔ$(n_i, n_j) \mid c_i - c_j$

π.χ.
$x \equiv 3 \bmod 6$
$x \equiv (7+\kappa) \bmod 9$
Για ποια κ με $0 \leq \kappa \leq 10$ έχει το σύστημα λύση στο $\mathbb{Z}$;

Λύση: Από το θεώρημα αν
ΜΚΔ$(6,9) \mid (7+\kappa) - 3$, ισοδύναμα αν $3 \mid (4+\kappa)$, ισοδύναμα αν $\kappa \in \{2, 5, 8\}$