ΘΕΩΡΗΜΑ (Αριθμητική των Υπολοίπων)

Εστω το σύστημα
$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \end{cases}$$
Τότε αυτό έχει λύση αν-ν $(m_1, m_2) \mid a_1 - a_2$

Αν x_0 μια λύση του, τότε κάθε λύση του θα είναι της μορφής $x_0 \bmod [m_1, m_2]$.

(Το θεώρημα αυτό βεβαίως μπορεί να εφαρμοσθεί και στη γενική μορφή του με n-εξισώσεις).

ΠΑΡΑΔΕΙΓΜΑ 1ο:

Λύστε το παρακάτω σύστημα:
$$\begin{cases} x \equiv 10 \bmod 13 \\ x \equiv 16 \bmod 17 \end{cases}$$

ΛΥΣΗ

Πρώτον ελέγχουμε:

$(17, 13) = 1 \mid (16-10) = 6$

Άρα, πράγματι έχει λύση

$x \equiv 10 \bmod 13 \Rightarrow x = 10 + 13 \cdot k \Rightarrow 10 + 13k \equiv 16 \bmod 17 \Rightarrow$

$\Rightarrow 13k \equiv 6 \bmod 17 \quad (*)$

Σκοπός μας είναι να βρούμε εκείνο το k ώστε να ισχύει η σχέση $(*)$

Αρκεί, να απαλείψουμε τον αριθμό 13 μπρος από το k

Αυτό, θα γίνει μέσω της αντίστροφης κλάσης

$13^{-1} \cdot 13k \equiv 6 \cdot 13^{-1} \bmod 17$. Ποιο είναι όμως το $13^{-1} \bmod 17$;

Μέσω του Ευκλείδειου Αλγορίθμου, αφού $(17, 13) = 1$ τότε

$17 = 1 \cdot 13 + 4$ και $13 = 3 \cdot 4 + 1 \Rightarrow 1 = 13 - 3 \cdot 4 = 13 - 3(17 - 13) =$

$= 13 - 3 \cdot 17 + 3 \cdot 13 = 4 \cdot 13 - 3 \cdot 17 \Rightarrow 1 = 4 \cdot 13 - 3 \cdot 17 \Rightarrow$

$\underset{\cancel{3 \cdot 17}\,0}{\overset{[\,]_7}{\Longrightarrow}} [1]_7 = [4]_7 \cdot [13]_7$, Άρα $([13]_7)^{-1} = [4]_7$)

Συνεπώς, στην παραπάνω σχέση είναι:

$$k \equiv 6 \cdot 4 \bmod 17 \equiv 24 \bmod 17 \equiv 7 \bmod 17$$

Άρα, $x = 10 + 13 \cdot k = 10 + 13 \cdot 7 = 101$

Επομένως, οι ακέραιοι $x \equiv 101 \bmod [13, 17] \equiv$

$\equiv 101 \bmod (13 \cdot 17) \equiv 101 \bmod 221$ είναι οι λύσεις!!!

ΠΑΡΑΔΕΙΓΜΑ 2ο

Να λύσετε το σύστημα:

$3x \equiv 7 \bmod 23$

$15x \equiv 12 \bmod 18$ (Αν θέλουμε για ευκολία $\frac{15}{3}x \equiv \frac{12}{3} \bmod \frac{18}{3} \Rightarrow 5x \equiv 4 \bmod 6$)

ΛΥΣΗ

Οι συντελεστές μπροστά από τις μεταβλητές εμποδίζουν να εφαρμοστεί το προηγούμενο θεώρημα.

Λύνουμε ξεχωριστά τις παραπάνω γραμμικές ισοτιμίες.

- $(3,23)=1$ τότε η 1η θα έχει μοναδική λύση την:

$x \equiv 7 \cdot 3^{\varphi(23)-1} \bmod 23 \equiv 7 \cdot 3^{21} \bmod 23$. (1)

$3^{21} = 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^3 \cdot 3^3 = 27 \cdot 27 \cdot 27 \cdot 27 \cdot 27 \cdot 27 \equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \bmod 23$

$4^7 = (4 \cdot 4)(4 \cdot 4)(4 \cdot 4)4 = 16 \cdot 16 \cdot 16 \cdot 4 = 256 \cdot 16 \cdot 4 \equiv 3 \cdot 16 \cdot 4 \bmod 23 \equiv 8 \bmod 23$

Άρα, η (1) γίνεται:

$x \equiv 7 \cdot 8 \bmod 23 \equiv 56 \bmod 23 \equiv 10 \bmod 23$.

- $(15,18) = (3 \cdot 5, 3 \cdot 6) = 3 \cdot (5,6) = 3 \cdot 1 = 3 \mid 12$ ← έχει λύση (όχι μοναδική)

Μια προφανής λύση είναι η: $x_0 \equiv 2 \bmod 18$

Άρα, το σύνολο των λύσεων θα είναι

$\{x_0, x_0 + \frac{n}{(a,n)}, x_0 + \frac{2n}{(a,n)}\} = \{2, 2+\frac{18}{3}, 2+\frac{36}{3}\} = \{2, 8, 14\}$

Συνεπώς, ο ακέραιος x_0' είναι λύση του συστήματος αν.ν x_0' ανήκει στην τομή των κλάσεων

($10 \bmod 23$ και $2 \bmod 18$) ή ($10 \bmod 23$ και $8 \bmod 18$) ή ($10 \bmod 23$ και $14 \bmod 18$)

Άρα, καλούμεθα να λύσουμε τα ακόλουθα συστήματα:

$\begin{cases} x \equiv 10 \bmod 23 \\ x \equiv 2 \bmod 18 \end{cases}$ και $\begin{cases} x \equiv 10 \bmod 23 \\ x \equiv 8 \bmod 18 \end{cases}$ και $\begin{cases} x \equiv 10 \bmod 23 \\ x \equiv 14 \bmod 18 \end{cases}$

Έτσι, αναγόμαστε στο "Παράδειγμα 1".

Αφού, $(23,18) \mid 10-2=8$ και μάλιστα $(23,18)=1$ (μοναδική λύση)

$x \equiv 10 \bmod 23 \Rightarrow x = 10 + 23k \Rightarrow 10 + 23k \equiv 2 \bmod 18 \Rightarrow 23k \equiv -8 \bmod 18$

$\Rightarrow 23k \equiv 10 \bmod 18$ όπου $([23]_{18})^{-1} = [2]_{18}$ (από Ευκλ. αλγόριθμο)

Άρα, $k \equiv 20 \bmod 18 \Rightarrow k \equiv 2 \bmod 18$. Επομένως, $x = 10 + 23 \cdot 2 = 56$

Άρα, οι λύσεις του συστήματος θα είναι οι ακέραιοι μορφής:

$x_0' \equiv 56 \bmod (18 \cdot 23) \equiv 56 \bmod 414$ · όμοια και για τα άλλα δύο συστήματα έχουμε: $x_0' \equiv 332 \bmod 414$ και $x_0' \equiv 194 \bmod 414$ αντίστοιχως με τον ίδιο τρόπο. (όπου $18 \cdot 23 = [18,23]$ το ΕΚΠ).

ΠΑΡΑΔΕΙΓΜΑ 3º:

Να λυθεί το ακόλουθο σύστημα:

$x \equiv 10 \bmod 16$

$x \equiv -15 \bmod 175$

$x \equiv 6 \bmod 49$

ΛΥΣΗ

Εφόσον $(m_1, m_2) = (16, 175) = 1$

$175 = 10 \cdot 16 + 15$

$16 = 1 \cdot 15 + \boxed{1}$

και $(m_2, m_3) = (175, 49) = 7 \mid (-15-6) = -21$

$175 = 3 \cdot 49 + 28$

$49 = 1 \cdot 28 + 21$

$28 = 1 \cdot 21 + \boxed{7}$

και $(m_1, m_3) = (16, 49) = 1$

Το σύστημα θα έχει λύση στο modulo $[16, 49, 25]$ = modulo $(16 \cdot 49 \cdot 25)$ = modulo 19600

Πρώτα, λύνουμε το σύστημα των δύο πρώτων εξισώσεων

$$\begin{cases} x \equiv 10 \bmod 16 \\ x \equiv -15 \bmod 175 \end{cases}$$

το οποίο έχει λύση και μάλιστα μοναδική αφού $(16, 175) = 1$

Έπειτα, $x \equiv 10 \bmod 16 \Rightarrow x = 10 + 16 \cdot k \Rightarrow 10 + 16k \equiv -15 \bmod 175 \Rightarrow$

$\Rightarrow 16k \equiv 150 \bmod 175$. Ψάχνουμε το $([16]_{175})^{-1}$

$1 = 16 - 15 = 16 - (175 - 10 \cdot 16) = 11 \cdot 16 - 175 \Rightarrow [1]_{175} = [11]_{175} \odot [16]_{175}$

Άρα, $([16]_{175})^{-1} = [11]_{175}$

Επομένως, $k \equiv (11 \cdot 150) \bmod 175 \equiv (1500 + 150) \bmod 175 \equiv$

$\equiv 1500 \bmod 175 \oplus 150 \bmod 175 \equiv 100 \bmod 175 \oplus 150 \bmod 175 \equiv$

$\equiv 250 \bmod 175 \equiv 75 \bmod 175$

Συνεπώς, $x = 10 + 16 \cdot 75 = 10 + 1200 = 1210$

Άρα, η λύση αυτού του συστήματος είναι η εξής:

$x \equiv 1210 \bmod [16, 175] \equiv 1210 \bmod 2800$

Όμοια, αν λύσουμε το σύστημα

$$\begin{cases} x \equiv 1210 \bmod 2800 \\ x \equiv 6 \bmod 49 \end{cases}$$

Θα βρεθεί η λύση $x \equiv 9610 \bmod [49, 2800] \Rightarrow$

$\Rightarrow x \equiv 9610 \bmod 19600$ όπου είναι λύση του αρχικού μας συστήματος