ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

ΤΜΗΜΑ **Β΄**

ΛΥΣΕΙΣ ΑΣΚΗΣΕΩΝ - ΦΥΛΛΑΔΙΟ **8**

ΔΙΔΑΣΚΩΝ: Α. Μπεληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ:
http://users.uoi.gr/abeligia/NumberTheory/NT2016/NT2016.html

Πέμπτη 22 Δεκεμβρίου 2016

Σχόλιο 1. Υπενθυμίζουμε ότι αν $a \in \mathbb{Z}$ και $n \in \mathbb{N}$ είναι τέτοιοι ώστε $(a,n)=1$, τότε η γραμμική ισοτιμία

$$ax \equiv b \,(\mathsf{mod}\, n) \qquad (*)$$

έχει μοναδική λύση

$$x \equiv bk \,(\mathsf{mod}\, n), \qquad \text{όπου} \quad k \in \mathbb{Z} \quad \text{και} \quad ak+ln=1$$

(ένας τέτοιος αριθμός k υπάρχει διότι $(a,n)=1$).

Ισοδύναμα, βλέποντας την παραπάνω γραμμική ισοτιμία ως εξίσωση

$$[a]_n \cdot x = [b]_n$$

στον δακτύλιο $\mathbb{Z}_n$, θα έχουμε ότι η παραπάνω εξίσωση έχει μοναδική λύση στο $\mathbb{Z}_n$

$$x = [b]_n \cdot [a]_n^{-1}, \qquad \text{όπου} \quad [a]^{-1} = [k]_n$$

και όπου: $ak+ln=1$. $\quad\surd$

Σχόλιο 2. Όπως προκύπτει από το Σχόλιο 1, η επίλυση μιας γραμμικής ισοτιμίας

$$ax \equiv b \,(\mathsf{mod}\, n), \qquad \text{όπου} \quad (a,n)=1 \qquad (*)$$

ανάγεται στον προσδιορισμό της αντίστροφης κλάσης $[a]_n^{-1}$ της κλάσης ισοτιμίας $[a]_n$, διότι τότε η μοναδική λύση $x_0 \,(\mathsf{mod}\, n)$ της $(*)$ είναι η $x_0 \equiv bc \,(\mathsf{mod}\, n)$, όπου $[a]_n^{-1} = [c]_n$.

Επειδή $(a,n)=1$,από το Θεώρημα του Euler, έπεται ότι

$$a^{\phi(n)} \;\equiv\; 1 \,(\mathsf{mod}\, n) \quad \Longrightarrow \quad a^{\phi(n)-1} \cdot a \;\equiv\; 1 \,(\mathsf{mod}\, n) \quad \Longrightarrow \quad [a]_n^{\phi(n)-1} \cdot [a]_n = [1]_n$$

και άρα:

$$[a]_n^{-1} = [a]_n^{\phi(n)-1} = [a^{\phi(n)-1}]_n$$

Επομένως η μοναδική λύση της $(*)$ είναι:

$$x_0 \;\equiv\; b \cdot a^{\phi(n)-1} \,(\mathsf{mod}\, n)$$

Γενικότερα αν $a^r \equiv 1 \,(\mathsf{mod}\, n)$ για κάποιον θετικό ακέραιο r, τότε η μοναδική λύση της $(*)$ είναι:

$$x_0 \;\equiv\; b \cdot a^{r-1} \,(\mathsf{mod}\, n)$$

Ένας τέτοιος ακέραιος r υπάρχει πάντα, για παράδειγμα ο $\phi(n)$. Αλλά μπορεί να υπάρχουν και άλλοι ακέραιοι με αυτή την ιδιότητα οι οποίοι μπορεί να είναι μικρότεροι του $\phi(n)$. Για παράδειγμα: επειδή $(3,8)=1$, θα έχουμε $3^{\phi(8)} \equiv 1 \,(\mathsf{mod}\, 8)$, δηλαδή $3^4 \equiv 1 \,(\mathsf{mod}\, 8)$. Όμως $3^2 = 9 \equiv 1 \,\mathsf{mod}\, 8)$. Και στις δύο περιπτώσεις $[3]_8^{-1} = [3^3]_8 = [27]_8 = [3]_8 = [3]_8^{-1}$.

Προφανώς, για την απλούστευση των αναγκαίων πράξεων, στην αναζήτηση θετικού ακεραίου r έτσι ώστε $a^r \equiv 1 \,(\mathsf{mod}\, n)$, αναζητούμε τον μικρότερο δυνατό θετικό ακέραιο r με αυτή την ιδιότητα. Όπως θα δούμε αργότερα, ισχύει: $r \mid \phi(n)$. $\quad\surd$

Σχόλιο 3. Τέλος υπενθυμίζουμε επίσης ότι γενικά η γραμμική ισοτιμία $(*)$ έχει λύση αν και μόνον αν $d \mid b$, όπου $d = (a, n)$.

Αν x_0 είναι μια λύση της $(*)$, τότε υπάρχουν ακριβώς d το πλήθος λύσεις $(\mathsf{mod}\, n)$ της $(*)$, οι εξής:

$$x_0, \quad x_0 + 2\frac{n}{d}, \quad x_0 + 3\frac{n}{d}, \ \cdots, \quad x_0 + (d-1)\frac{n}{d}$$

Η λύση $x_0 \,(\mathsf{mod}\, n)$ προκύπτει από τη μοναδική λύση $x_0 (\mathsf{mod}\, \frac{n}{d})$ της γραμμικής ισοτιμίας

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \ \mathsf{mod}\, \frac{n}{d} \qquad (**)$$

Η ισοτιμία $(**)$ έχει μοναδική λύση διότι $(\frac{a}{d}, \frac{n}{d}) = 1$, και προφανώς η λύση $x_0 \,(\mathsf{mod}\, \frac{n}{d})$ είναι και λύση της $(*)$. $\quad\surd$

• • •

Άσκηση 1. *Να βρεθούν όλες οι λύσεις των παρακάτω ισοτιμιών:*

1. $13\,x \equiv \ \ 71 \,(\mathsf{mod}\, 380)$

2. $91\,x \equiv \ 419 \,(\mathsf{mod}\, 440)$.

Λύση. **1.** Η πρωτογενής ανάλυση του 380 είναι $380 = 2^2 \cdot 5 \cdot 19$. Ιδιαίτερα $(380, 13) = 1$. Επομένως η ισοτιμία $13\,x \equiv \ 71 \,(\mathsf{mod}\, 380)$ έχει μοναδική λύση:

$$x = [71]_{380} \cdot [13]_{380}^{-1}$$

Με χρήση του αλγόριθμου του Ευκλείδη, εύκολα βλέπουμε ότι

$$1 = (-4) \cdot 380 + (117) \cdot 13 \quad \Longrightarrow \quad [1]_{380} = [117]_{380} \cdot [13]_{380} \quad \Longrightarrow \quad [13]_{380}^{-1} = [117]_{380}$$

Τότε θα έχουμε:

$$x = [71]_{380} \cdot [13]_{380}^{-1} = [71]_{380} \cdot [117]_{380} = [8307]_{380} = [327]_{380}$$

Επομένως η μοναδική λύση της εξίσωσης $[13]_{380} \cdot x = [71]_{380}$ είναι η $x = [327]_{380}$. Ισοδύναμα η μοναδική λύση $(\mathsf{mod}\, 380)$ της ισοτιμίας $13\,x \equiv \ 71 \,(\mathsf{mod}\, 380)$ είναι η

$$327 \,(\mathsf{mod}\, 380)$$

2. Οι πρωτογενείς αναλύσεις των 440 και 91 είναι $440 = 2^3 \cdot 5 \cdot 11$ και $91 = 7 \cdot 13$. Ιδιαίτερα $(440, 91) = 1$. Επομένως η ισοτιμία $91\,x \equiv \ 419 \,(\mathsf{mod}\, 440)$ έχει μοναδική λύση:

$$x = [419]_{440} \cdot [91]_{440}^{-1}$$

Με χρήση του αλγόριθμου του Ευκλείδη, εύκολα βλέπουμε ότι

$$1 = 6 \cdot 440 + (-29) \cdot 91 \quad \Longrightarrow \quad [1]_{440} = [-29]_{440} \cdot [91]_{440} \quad \Longrightarrow \quad [91]_{440}^{-1} = [-29]_{440} = [411]_{440}$$

Τότε θα έχουμε:

$$x = [419]_{440} \cdot [91]_{440}^{-1} = [419]_{440} \cdot [411]_{440} = [172209]_{440} = [169]_{440}$$

Επομένως η μοναδική λύση της εξίσωσης $[91]_{440} \cdot x = [419]_{440}$ είναι η $x = [169]_{440}$. Ισοδύναμα η μοναδική λύση $(\mathsf{mod}\, 440)$ της ισοτιμίας $91\,x \equiv \ 419 \,(\mathsf{mod}\, 440)$ είναι η

$$169 \,(\mathsf{mod}\, 440)$$

■

Άσκηση 2. *Να βρεθούν όλες οι λύσεις των παρακάτω ισοτιμιών:*

1. $15\,x \equiv\ 9 \pmod{25}$.
2. $987\,x \equiv\ 610 \pmod{1597}$
3. $980\,x \equiv\ 1500 \pmod{1600}$.

Λύση. **1.** Επειδή $(15, 25) = 5 \nmid 9$, έπεται ότι η γραμμική ισοτιμία $15\,x \equiv\ 9 \pmod{25}$ δεν έχει καμμία λύση.

2. Υπολογίζουμε εύκολα τις πρωτογείς αναλύσεις των αριθμών 987 και 1597:

$$987 = 3 \cdot 7 \cdot 47 \quad \& \quad 1597 = 1597 \quad \Longrightarrow \quad (987, 1597) = 1$$

Επομένως η γραμμική ισοτιμία $987x \equiv 610 \pmod{1597}$ έχει μοναδική λύση $x_0 \pmod{1597}$ την οποία προσδιορίζουμε ως εξής: Θα έχουμε $x_0 \equiv 610 \cdot c \pmod{1597}$, όπου $[c]_{1597} = [987]^{-1}_{1597}$. Για τον προσδιορισμό του ακεραίου c, εργαζόμαστε ως εξής:

Με χρήση του αλγόριθμου του Ευκλείδη, γράφουμε τον αριθμό 1 ως ακέραιο γραμμικό συνδυασμό των αριθμών 987 και 1597:

$$1 = (-377) \cdot 1597 + 610 \cdot 987$$

και τότε θα έχουμε $[987]_{1597} \cdot [610]_{1597} = [1]_{1597}$. Επομένως $[987]^{-1}_{1597} = [610]_{1597}$ και άρα η μοναδική λύση της ισοτιμίας είναι:

$$x_0 \equiv 610 \cdot 610 \pmod{1597} \ \equiv 372100 \pmod{1597} \ \equiv 1596 \pmod{1597}$$

3. Υπολογίζουμε εύκολα τις πρωτογείς αναλύσεις των αριθμών 980 και 1600:

$$980 = 2^2 \cdot 5 \cdot 7^2 \quad \& \quad 1600 = 2^6 \cdot 5^2 \quad \Longrightarrow \quad (980, 1600) = 2^2 \cdot 5 = 20$$

Επειδή $20 \mid 1500$, έπεται ότι η γραμμική ισοτιμία $980x \equiv 1500 \pmod{1600}$ έχει ακριβώς 20 ανα δύο ανισότιμες λύσεις $\pmod{1600}$.

Θα προσδιορίσουμε αυτές τις λύσεις. Η γραμμική ισοτιμία $(*)$ είναι ισοδύναμη με την

$$\frac{980}{20} \cdot x \ \equiv\ \frac{1500}{20} \pmod{\frac{1600}{20}} \quad \Longrightarrow \quad 49 \cdot x \ \equiv\ 75 \pmod{80} \qquad (**)$$

η οποία έχει μοναδική λύση $x_0 \pmod{80}$ την οποία προσδιορίζουμε ως εξής: Θα έχουμε $x_0 \equiv 75 \cdot c \pmod{80}$, όπου $[c]_{80} = [49]^{-1}_{80}$. Για τον προσδιορισμό του ακεραίου c, εργαζόμαστε ως εξής:

Με χρήση του αλγόριθμου του Ευκλείδη, γράφουμε τον αριθμό 1 ως ακέραιο γραμμικό συνδυασμό των αριθμών 49 και 80:

$$1 = 19 \cdot 80 + (-31) \cdot 49$$

και τότε θα έχουμε $[49]^{-1}_{80} = [-31]_{80} = [49]_{80}$. Επομένως η μοναδική λύση της $(**)$ θα είναι

$$x_0 = 75 \cdot 49 \pmod{80} = 3675 \pmod{80} = 75 \pmod{80}$$

Άρα οι λύσεις της αρχικής ισοτιμίας είναι

$$75, \ \ 75 + \frac{1600}{20}, \ \ 75 + 2\frac{1600}{20}, \ \ \cdots, \ \ 75 + 19\frac{1600}{20} \pmod{1600}$$

δηλαδή οι εξής:

$$75, \ \ 155, \ \ 235, \ \ \cdots, \ \ 1595 \pmod{1600}$$ ■

Άσκηση 3. *Να βρεθούν όλες οι λύσεις των παρακάτω ισοτιμιών:*

1. $2\,x \equiv\ 5 \pmod{7}$
2. $3\,x \equiv\ 6 \pmod{9}$.
3. $19\,x \equiv 30 \pmod{40}$

Λύση. **1.** – **Πρώτος τρόπος**: Επειδή $(2,7)=1 \mid 5$ έπεται ότι η ισοτιμία $2\,x \equiv 5 \pmod 7$ έχει μοναδική λύση $\pmod 7$. Άμεσα παρατηρούμε ότι $2 \cdot 6 = 12 \equiv 5 \pmod 7$ και άρα η μοναδική λύση είναι η

$$x \equiv 6 \pmod 7$$

– **Δεύτερος τρόπος**: Έχουμε

$$\begin{aligned} 7 = 2 \cdot 3 + 1 &\implies 1 = (-3) \cdot 2 + 1 \cdot 7 \\ &\implies [1]_7 = [-3]_7 \cdot [2]_7 + [1]_7 \cdot [7]_7 \\ &\implies [1]_7 = [-3]_7 \cdot [2]_7 \\ &\implies [2]_7 \cdot [4]_7 = [1]_7 \\ &\implies [2]_7^{-1} = [4]_7 \end{aligned}$$

Τότε

$$x = [2]_7^{-1} \cdot [5]_7 \implies x = [4]_7 \cdot [5]_7 = [20]_7 \implies x = [6]_7$$

Επομένως η μοναδική λύση της ισοτιμίας $2\,x \equiv 5 \pmod 7$ είναι η $x \equiv 6 \pmod 7$.

– **Τρίτος τρόπος**: Θα εφαρμόσουμε την διαδικασία στο Σχόλιο 1. Επειδή $(2,7)=1$, από το Θεώρημα του Euler, θα έχουμε

$$2^{\phi(7)} \equiv 1 \pmod 7 \implies 2^6 \equiv 1 \pmod 7 \implies [2]_7^{-1} \cdot [2]_7^5 \implies [2]_7^{-1} \cdot [2^5]_7 = [32]_7 = [4]_7$$

και τότε όπως και πριν, η μοναδική λύση της γραμμικής ισοτιμίας είναι:

$$x = 5 \cdot 4, \pmod 7 = 20 \pmod 7 = 6 \pmod 7$$

2. Επειδή $(3,9)=3 \mid 6$ έπεται ότι η ισοτιμία $3\,x \equiv 6 \pmod 9$ έχει 3 λύσεις $\pmod 9$. Αν x_0 είναι μια λύση της $3\,x \equiv 6 \pmod 9$ τότε όλες οι λύσεις είναι οι ακόλουθες:

$$x_0 \pmod 9, \quad x_0 + 1 \cdot \frac{9}{3} = x_0 + 3 \pmod 9, \quad x_0 + 2 \cdot \frac{9}{3} = x_0 + 6 \pmod 9$$

Παρατηρούμε ότι η $x_0 = 2$ είναι προφανώς μια λύση. Επομένως όλες οι λύσεις της ισοτιμίας $3\,x \equiv 6 \pmod 9$ είναι οι εξής:

$$x_0 \equiv 2 \pmod 9, \qquad x_1 \equiv 5 \pmod 9, \qquad x_2 \equiv 8 \pmod 9$$

3. – **Πρώτος τρόπος**: Επειδή $(19,40)=1 \mid 30$ έπεται ότι η ισοτιμία $19\,x \equiv 30 \pmod{40}$ έχει μοναδική λύση $\pmod{40}$. Άμεσα παρατηρούμε ότι $19 \cdot 10 = 190 = 4 \cdot 40 + 30 \equiv 30 \pmod{40}$ και άρα η μοναδική λύση είναι η $x \equiv 10 \pmod{40}$.

– **Δεύτερος τρόπος**: Έχουμε

$$\begin{aligned} 19 = 2 \cdot 9 + 1 &\implies 1 = 19 - 2 \cdot 9 \\ &\implies 1 = 19 - 9 \cdot (40 - 2 \cdot 19) \\ &\implies 1 = -9 \cdot 40 + 19 \cdot 19 \\ &\implies [1]_{40} = [-9]_{40} \cdot [40]_{40} + [19]_{40} \cdot [19]_{40} \\ &\implies [1]_{40} = [19]_{40} \cdot [19]_{40} \\ &\implies [19]_{40}^{-1} = [19]_{40} \end{aligned}$$

Τότε

$$x = [19]_{40}^{-1} \cdot [30]_{40} \implies x = [19]_{40} \cdot [30]_{40} = [570]_{40} = [10]_{40}$$

Συνεπώς η μοναδική λύση της ισοτιμίας $19\,x \equiv 30 \pmod{40}$ είναι η

$$x \equiv 10 \pmod{40}$$

■

Άσκηση 4. *Να βρεθούν όλοι οι θετικοί ακέραιοι b, όπου $0 \leq b < 1001$, για τους οποίους η γραμμική ισοτιμία*

$$154 \cdot x \ \equiv \ b \,(\mathsf{mod}\, 1001) \qquad (*)$$

έχει λύση. Όταν υπάρχει τουλάχιστον μια λύση, πόσες ανισότιμες $(\mathsf{mod}\, 1001)$ *λύσεις υπάρχουν;*

Λύση. Επειδή οι πρωτογενείς αναλύσεις των αριθμών 154 και 1001 είναι $154 = 2 \cdot 7 \cdot 11$ και $1001 = 7 \cdot 11 \cdot 13$, έπεται ότι: $(154, 1001) = 77$.

Επομένως η γραμμική ισοτιμία $(*)$ έχει λύση αν και μόνον αν $77 \mid b$, δηλαδή αν και μόνον αν $b = 77 \cdot k$. Επειδή $0 \leq b < 1001$, θα πρέπει $0 \leq 77 \cdot k < 1001$ και άρα: $0 \leq k < 13$. Επομένως:

$$\text{η ισοτιμία} \quad (*) \quad \text{έχει λύση} \qquad \Longleftrightarrow \qquad b = 77 \cdot k, \ \ k = 0, 1, 2, \cdots, 12$$

Επειδή $(154, 1001) = 77$, για κάθε μια από τις παραπάνω 13 τιμές του b, υπάρχουν ακριβώς 77 ανισότιμες $(\mathsf{mod}\, 1001)$ λύσεις της $(*)$.

Θα προσδιορίσουμε αυτές τις λύσεις, υποθέτοντας ότι $b = 77 \cdot k$, όπου $0 \leq k \leq 12$. Η γραμμική ισοτιμία $(*)$ είναι ισοδύναμη με την

$$\frac{154}{77} \cdot x \ \equiv \ \frac{b}{77} \,(\mathsf{mod}\, \frac{1001}{77}) \qquad \Longrightarrow \qquad 2 \cdot x \ \equiv \ k \,(\mathsf{mod}\, 13) \qquad (**)$$

Η γραμμική ισοτιμία $(**)$ έχει μοναδική λύση $x_0 (\mathsf{mod}\, 13)$ την οποία προσδιορίζουμε ως εξής. Θα έχουμε $x_0 = k \cdot c \,(\mathsf{mod}\, 13)$, όπου $[2]_{13}^{-1} = [c]_{13}$. Από το Θεώρημα του Euler, θα έχουμε:

$$2^{\phi(13)} \equiv 1 \,(\mathsf{mod}\, 13) \quad \Longrightarrow \quad 2^{12} \equiv 1 \,(\mathsf{mod}\, 13) \quad \Longrightarrow \quad [2]_{13}^{-1} = [2^{11}]_{13}$$

$$[2^{11}]_{13} = [2^5 \cdot 2^5 \cdot 2]_{13} = [32 \cdot 32 \cdot 2]_{13} = [32]_{13} \cdot [32]_{13} \cdot [2]_{13} = [6]_{13} \cdot [6]_{13} \cdot [2]_{13} =$$

$$= [36]_{13} \cdot [2]_{13} = [10]_{13} \cdot [2]_{13} = [20]_{13} = [7]_{13}$$

Άρα η μοναδική λύση της **(**)** είναι η

$$x_0 \equiv k \cdot 7 \,(\mathsf{mod}\, 13)$$

Τότε, για κάθε $k = 0, 1, 2, \cdots, 12$, οι λύσεις της $(*)$ (ανα δύο ανισότιμες $(\mathsf{mod}\, 1001)$) είναι:

$$7k, \quad 7k + 2\frac{1001}{77}, \quad 7k + 3\frac{1001}{77}, \ \cdots, \quad 7k + 76\frac{1001}{77}$$

δηλαδή:

$$7k, \quad 7k + 2 \cdot 13, \quad 7k + 3 \cdot 13, \ \cdots, \ 7k + 76 \cdot 13 \quad (\mathsf{mod}\, 1001) \qquad \blacksquare$$

• • •

Σχόλιο 4. Θεωρούμε το ακόλουθο σύστημα γραμμικών ισοτιμιών

$$(\Sigma) \qquad \begin{cases} x \ \equiv \ a_1 \,(\mathsf{mod}\, n_1) \\ x \ \equiv \ a_2 \,(\mathsf{mod}\, n_2) \\ \quad \vdots \\ x \ \equiv \ a_k \,(\mathsf{mod}\, n_k) \end{cases}$$

Αν $(n_i, n_j) = 1$, όπου $1 \leq i \neq j \leq k$, τότε το Κινέζικο Θεώρημα Υπολοίπων πιστοποιεί ότι το (Σ) έχει μοναδική λύση $x_0 \,(\mathsf{mod}\, n_1 \cdot n_2 \cdots n_k)$.

Υπενθυμίζουμε τη διαδικασία εύρεσης της μοναδική λύσης $x_0 \,(\mathsf{mod}\, n_1 \cdot n_2 \cdots n_k)$:

Θέτουμε:

$$M = n_1 \cdot n_2 \cdots n_k, \qquad \& \qquad M_1 = \frac{M}{n_1}, \quad M_2 = \frac{M}{n_2}, \ \cdots, \ M_k = \frac{M}{n_k}$$

Θεωρούμε τις γραμμικές ισοτιμίες:

$$\begin{cases} M_1 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, n_1) \\ M_2 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, n_2) \\ \qquad \vdots \\ M_k \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, n_k) \end{cases}$$

Επειδή $(M_i, n_i) = 1$, $\forall i = 1, 2, \cdots, k$, κάθε μια από τις παραπάνω ισοτιμίες έχει μοναδική λύση

$$b_i \, (\mathsf{mod}\, n_i), \qquad \text{όπου} \ \ 1 \leq i \leq k$$

Τότε η μοναδική λύση $(\mathsf{mod}\, n_1 \cdot n_2 \cdots n_k)$ του (Σ) είναι η:

$$M_1 \cdot b_1 \cdot a_1 + M_2 \cdot b_2 \cdot a_2 + \cdots + M_k \cdot b_k \cdot a_k \ (\mathsf{mod}\, n_1 \cdot n_2 \cdots n_k) \qquad \surd$$

• • •

Άσκηση 5. *Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma) \qquad \begin{cases} x \ \equiv \ 1 \ (\mathsf{mod}\, 5) \\ x \ \equiv \ 2 \ (\mathsf{mod}\, 6) \\ x \ \equiv \ 3 \ (\mathsf{mod}\, 7) \end{cases}$$

Λύση. Επειδή οι αριθμοί 5, 6, και 7 είναι ανά δύο πρώτοι μεταξύ τους, μπορούμε να εφαρμόσουμε το Κινέζικο Θεώρημα Υπολοίπων για την επίλυση του (Σ). Θα έχουμε:

$$a_1 = 1, \qquad a_2 = 2, \qquad a_3 = 3$$

$$n_1 = 5, \qquad n_2 = 6, \qquad n_3 = 7 \qquad \& \qquad M = 5 \cdot 6 \cdot 7 = 210$$

$$M_1 = \frac{M}{n_1} = \frac{210}{5} = 42, \quad M_2 = \frac{M}{n_2} = \frac{210}{6} = 35, \quad M_3 = \frac{M}{n_3} = \frac{210}{7} = 30$$

Σύμφωνα με το Κινέζικο Θεώρημα Υπολοίπων, το σύστημα (Σ) έχει μοναδική λύση $x_0 \, (\mathsf{mod}\, 210)$, την οποία βρίσκουμε ως εξής:

Θεωρούμε τις γραμμικές ισοτιμίες:

$$M_1 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, n_1) \quad \Longrightarrow \quad 42 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, 5) \quad \Longrightarrow \quad 2 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, 5)$$

$$M_2 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, n_2) \quad \Longrightarrow \quad 35 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, 6) \quad \Longrightarrow \quad 5 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, 6)$$

$$M_3 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, n_3) \quad \Longrightarrow \quad 30 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, 7) \quad \Longrightarrow \quad 2 \cdot x \ \equiv \ 1 \ (\mathsf{mod}\, 7)$$

όπου χρησιμοποιήσαμε ότι: $42 \equiv 2 \, (\mathsf{mod}\, 5)$, $35 \equiv 5 \, (\mathsf{mod}\, 6)$, και $30 \equiv 2 \, (\mathsf{mod}\, 7)$.

Εύκολα βλέπουμε ότι οι μοναδικές λύσεις των παραπάνω ισοτιμιών είναι αντίστοιχα:

$$b_1 \ \equiv \ 3 \ (\mathsf{mod}\, 5), \qquad b_2 \ \equiv \ 5 \ (\mathsf{mod}\, 6), \qquad b_3 \ \equiv \ 4 \ (\mathsf{mod}\, 7)$$

Επομένως η μοναδική λύση $(\mathsf{mod}\, 210)$ του (Σ) είναι:

$$\begin{aligned} x_0 \ &\equiv \ M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 \ (\mathsf{mod}\, 210) \\ &\equiv \ 42 \cdot 3 \cdot 1 + 35 \cdot 5 \cdot 2 + 30 \cdot 4 \cdot 3 \ (\mathsf{mod}\, 210) \\ &\equiv \ 836 \ (\mathsf{mod}\, 210) \\ &\equiv \ 206 \ (\mathsf{mod}\, 210) \quad \blacksquare \end{aligned}$$

Άσκηση 6. *Να βρεθούν όλοι οι ακέραιοι αριθμοί οι οποίοι δίνουν υπόλοιπα 1, 2, και 3, όταν διαιρεθούν με τους αριθμούς 4, 3, και 5, αντίστοιχα.*

Λύση. Το πρόβλημα ανάγεται στην επίλυση του ακόλουθου συστήματος γραμμικών ισοτιμιών:

$$(\Sigma) \quad \begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

Επειδή οι αριθμοί 4, 3, και 5 είναι ανά δύο πρώτοι μεταξύ τους, μπορούμε να εφαρμόσουμε το Κινέζικο Θεώρημα Υπολοίπων για την επίλυση του (Σ). Θα έχουμε:

$$a_1 = 1, \qquad a_2 = 2, \qquad a_3 = 3$$

$$n_1 = 4, \quad n_2 = 3, \quad n_3 = 5 \quad \& \quad M = 4 \cdot 3 \cdot 5 = 60$$

$$M_1 = \frac{M}{n_1} = \frac{60}{4} = 15, \quad M_2 = \frac{M}{n_2} = \frac{60}{3} = 20, \quad M_3 = \frac{M}{n_3} = \frac{60}{5} = 12$$

Σύμφωνα με το Κινέζικο Θεώρημα Υπολοίπων, το σύστημα (Σ) έχει μοναδική λύση $x_0 \pmod{210}$, την οποία βρίσκουμε ως εξής:

Θεωρούμε τις γραμμικές ισοτιμίες:

$$\begin{aligned} M_1 \cdot x \equiv 1 \pmod{n_1} &\implies 15 \cdot x \equiv 1 \pmod 4 \implies 3 \cdot x \equiv 1 \pmod 4 \\ M_2 \cdot x \equiv 1 \pmod{n_2} &\implies 20 \cdot x \equiv 1 \pmod 3 \implies 2 \cdot x \equiv 1 \pmod 3 \\ M_3 \cdot x \equiv 1 \pmod{n_3} &\implies 12 \cdot x \equiv 1 \pmod 5 \implies 2 \cdot x \equiv 1 \pmod 5 \end{aligned}$$

όπου χρησιμοποιήσαμε ότι: $15 \equiv 3 \pmod 4$, $29 \equiv 2 \pmod 3$, και $12 \equiv 2 \pmod 5$.

Εύκολα βλέπουμε ότι οι μοναδικές λύσεις των παραπάνω ισοτιμιών είναι αντίστοιχα:

$$b_1 \equiv 3 \pmod 4, \qquad b_2 \equiv 2 \pmod 3, \qquad b_3 \equiv 3 \pmod 5$$

Επομένως η μοναδική λύση $\pmod{60}$ του (Σ) είναι:

$$\begin{aligned} x_0 &\equiv M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 \pmod{60} \\ &\equiv 15 \cdot 3 \cdot 1 + 20 \cdot 2 \cdot 2 + 12 \cdot 3 \cdot 3 \pmod{60} \\ &\equiv 233 \pmod{60} \\ &\equiv 53 \pmod{60} \end{aligned}$$

Άρα οι ακέραιοι οι οποίοι δίνουν υπόλοιπα 1, 2, και 3, όταν διαιρεθούν με τους αριθμούς 4, 3, και 5, αντίστοιχα, είναι όλοι οι ακέραιοι της μορφής:

$$53 + k \cdot 60, \qquad k \in \mathbb{Z}$$

■

Άσκηση 7. *Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma): \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 5 \pmod{11} \end{cases}$$

Λύση. Επειδή οι αριθμοί $2, 3, 5, 7, 11$ είναι ανα δυο πρώτοι μεταξύ τους, τότε από το Κινέζικο Θεώρημα Υπολοίπων έπεται ότι το σύστημα (Σ) έχει μοναδική λυση

$$x_0 \pmod M = x_0 \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11} = x_0 \pmod{2310}$$

Θα έχουμε:

$$a_1 = 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_4 = 4, \quad a_5 = 5$$

$$n_1 = 2, \quad n_2 = 3, \quad n_3 = 5, \quad n_4 = 7, \quad n_5 = 11 \quad \& \quad M = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$$

$$M_1 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{2} = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$$

$$M_2 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{3} = 2 \cdot 5 \cdot 7 \cdot 11 = 770$$

$$M_3 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{5} = 2 \cdot 3 \cdot 7 \cdot 11 = 462$$

$$M_4 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{7} = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

$$M_5 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{11} = 2 \cdot 3 \cdot 5 \cdot 7 = 210$$

και θεωρούμε τις ισοτιμίες:

$$\begin{cases} 1155x \equiv 1 \pmod 2 \\ 770x \equiv 1 \pmod 3 \\ 462x \equiv 1 \pmod 5 \\ 330x \equiv 1 \pmod 7 \\ 210x \equiv 1 \pmod{11} \end{cases}$$

Επειδή $1155 = 2 \cdot 577 + 1$, $770 = 3 \cdot 256 + 2$, $462 = 5 \cdot 92 + 2$, $330 = 7 \cdot 47 + 1$ και $210 = 11 \cdot 19 + 1$, το παραπάνω σύστημα είναι ισοδύναμο με το ακόλουθο:

$$\begin{cases} x \equiv 1 \pmod 2 \\ 2x \equiv 1 \pmod 3 \\ 2x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 7 \\ x \equiv 1 \pmod{11} \end{cases} \quad \Longrightarrow \quad \begin{cases} b_1 \equiv 1 \pmod 2 \\ b_2 \equiv 2 \pmod 3 \\ b_3 \equiv 3 \pmod 5 \\ b_4 \equiv 1 \pmod 7 \\ b_5 \equiv 1 \pmod{11} \end{cases}$$

Άρα η μοναδική λύση $\pmod{2310}$ του (Σ) είναι

$$\begin{aligned} x_0 &= \sum_{i=1}^{5} M_i b_i a_i \\ &= 1155 \cdot 1 \cdot 1 + 770 \cdot 2 \cdot 2 + 462 \cdot 3 \cdot 3 + 330 \cdot 1 \cdot 4 + 210 \cdot 1 \cdot 5 \\ &= 1155 + 3080 + 4158 + 1320 + 1050 \\ &= 10763 \\ &\equiv 1523 \pmod{2310} \quad \blacksquare \end{aligned}$$

Άσκηση 8. *Βρείτε έναν αριθμό ο οποίος είναι πολλαπλάσιο του* 11 *και δίνει υπόλοιπο* 1 *όταν διαιρεθεί με τους αριθμούς* $2, 3, 5,$ *και* 7.

Λύση. Το πρόβλημα ανάγεται στην επίλυση του παρακάτω συστήματος γραμμικών ισοτιμιών:

$$(\Sigma): \begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{7} \end{cases}$$

Επειδή οι αριθμοί $2, 3, 5, 7, 11$ είναι ανα δυο πρώτοι μεταξύ τους, τότε από το Κινέζικο Θεώρημα Υπολοίπων έπεται ότι το σύστημα (Σ) έχει μοναδική λυση

$$x_0 \pmod{M} = x_0 \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11} = x_0 \pmod{2310}$$

Υπολογίζουμε

$$M_1 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{2} = 3 \cdot 5 \cdot 7 \cdot 11 = 1155$$

$$M_2 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{3} = 2 \cdot 5 \cdot 7 \cdot 11 = 770$$

$$M_3 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{5} = 2 \cdot 3 \cdot 7 \cdot 11 = 462$$

$$M_4 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{7} = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

$$M_5 = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{11} = 2 \cdot 3 \cdot 5 \cdot 7 = 210$$

και θεωρούμε τις ισοτιμίες:

$$\begin{cases} 1155x \equiv 1 \pmod{2} \\ 770x \equiv 1 \pmod{3} \\ 462x \equiv 1 \pmod{5} \\ 330x \equiv 1 \pmod{7} \\ 210x \equiv 1 \pmod{11} \end{cases}$$

Επειδή $1155 = 2 \cdot 577 + 1$, $770 = 3 \cdot 256 + 2$, $462 = 5 \cdot 92 + 2$, $330 = 7 \cdot 47 + 1$ και $210 = 11 \cdot 19 + 1$, το παραπάνω σύστημα είναι ισοδύναμο με το ακόλουθο:

$$\begin{cases} x \equiv 1 \pmod{2} \\ 2x \equiv 1 \pmod{3} \\ 2x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases} \implies \begin{cases} b_1 \equiv 1 \pmod{2} \\ b_2 \equiv 2 \pmod{3} \\ b_3 \equiv 3 \pmod{5} \\ b_4 \equiv 1 \pmod{7} \\ b_5 \equiv 1 \pmod{11} \end{cases}$$

Άρα η μοναδική λύση $(\mathsf{mod}\, 2310)$ του (Σ) είναι

$$\begin{aligned} x_0 &= \sum_{i=1}^{5} M_i b_i a_i \\ &= 1155 \cdot 1 \cdot 1 + 770 \cdot 2 \cdot 1 + 462 \cdot 3 \cdot 1 + 330 \cdot 1 \cdot 1 + 210 \cdot 1 \cdot 0 \\ &= 1155 + 1540 + 1386 + 330 \\ &= 4411 \\ &\equiv 2101 \,(\mathsf{mod}\, 2310) \end{aligned}$$

Συνεπώς ο ζητούμενος αριθμός είναι ο 2101. Παρατηρείστε ότι πράγματι $2101 = 11 \cdot 191$, δηλαδή ο αριθμός 2101 είναι πολλαπλάσιο του 11. ■

Άσκηση 9. *Δείξτε ότι για κάθε $k \geq 2$, υπάρχουν k το πλήθος διαδοχικοί ακέραιοι, κάθε ένας από τους οποίους διαιρείται από τετράγωνο αριθμού > 1.*

Λύση. Έστω $p_1, p_2, \cdots, p_k$ διαφορετικοί πρώτοι αριθμοί k σε πλήθος, για παράδειγμα μπορούμε να θεωρήσουμε τους πρώτους k πρώτους αριθμούς. Θεωρούμε το παρακάτω σύστημα γραμμικών ισοτιμιών:

$$(\Sigma): \begin{cases} x \equiv 0 \,(\mathsf{mod}\, p_1^2) \\ x \equiv -1 \,(\mathsf{mod}\, p_2^2) \\ x \equiv -2 \,(\mathsf{mod}\, p_3^2) \\ \quad \vdots \\ x \equiv -k+1 \,(\mathsf{mod}\, p_k^2) \end{cases}$$

Επειδή $(p_i^2, p_j^2) = 1$ για κάθε $1 \leq i \neq j \leq k$, από το Κινέζικο Θεώρημα Υπολοίπων έχουμε ότι το σύστημα (Σ) έχει μοναδική λύση $\mathsf{mod}(p_1 \cdots p_k)^2$. Έστω N η λύση του (Σ). Τότε

$$\begin{cases} N \equiv 0 \,(\mathsf{mod}\, p_1^2) \\ N \equiv -1 \,(\mathsf{mod}\, p_2^2) \\ N \equiv -2 \,(\mathsf{mod}\, p_3^2) \\ \quad \vdots \\ N \equiv -k+1 \,(\mathsf{mod}\, p_k^2) \end{cases} \Longrightarrow \begin{cases} p_1^2 \mid N \\ p_2^2 \mid N+1 \\ p_3^2 \mid N+2 \\ \quad \vdots \\ p_k^2 \mid N+k-1 \end{cases}$$

Συνεπώς οι k διαδοχικοί ακέραιοι $N, N+1, \ldots, N+k-1$ έχουν την ιδιότητα ότι κάθε ένας από αυτούς διαιρείται από τετράγωνο αριθμού > 1. ■

Άσκηση 10. *Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma) \quad \begin{cases} x \equiv 65 \,(\mathsf{mod}\, 99) \\ x \equiv 2 \,(\mathsf{mod}\, 98) \\ x \equiv 51 \,(\mathsf{mod}\, 97) \\ x \equiv 10 \,(\mathsf{mod}\, 95) \end{cases}$$

Λύση. Οι πρωτογενείς αναλύσεις των αριθμών 99, 98, 97, και 95, είναι

$$99 = 3^2 \cdot 11, \qquad 98 = 2 \cdot 7^2, \qquad 97 = 97, \qquad 95 = 5 \cdot 13$$

και άρα οι αριθμοί 99, 98, 97, και 95 είναι ανα δύο πρώτοι μεταξύ τους. Επομένως μπορούμε να εφαρμόσουμε το Κινέζικο Θεώρημα Υπολοίπων, για την επίλυση του (Σ). Θα έχουμε:

$$n_1 = 99, \qquad n_2 = 98, \qquad n_3 = 97, \qquad n_4 = 95$$

$$M = 99 \cdot 98 \cdot 97 \cdot 95 = 89.403.930$$

$$M_1 = \frac{99 \cdot 98 \cdot 97 \cdot 9}{99} = 903.070, \qquad M_2 = \frac{99 \cdot 98 \cdot 97 \cdot 9}{98} = 912.285,$$

$$M_3 = \frac{99 \cdot 98 \cdot 97 \cdot 9}{97} = 921.690, \qquad M_4 = \frac{99 \cdot 98 \cdot 97 \cdot 9}{95} = 941.094$$

Θεωρούμε τις γραμμικές ισοτιμίες:

$$\begin{aligned} M_1 \cdot x \ &\equiv\ 1 \,(\mathsf{mod}\, n_1) \quad \Longrightarrow \quad 903.070 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 99) \\ M_2 \cdot x \ &\equiv\ 1 \,(\mathsf{mod}\, n_2) \quad \Longrightarrow \quad 912.285 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 98) \\ M_3 \cdot x \ &\equiv\ 1 \,(\mathsf{mod}\, n_3) \quad \Longrightarrow \quad 921.690 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 97) \\ M_4 \cdot x \ &\equiv\ 1 \,(\mathsf{mod}\, n_4) \quad \Longrightarrow \quad 941.094 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 95) \end{aligned}$$

Επειδή:

$903.070 = 99 \cdot 9121 + 91, \quad 912.285 = 98 \cdot 9309 + 3, \quad 921.690 = 97 \cdot 9501 + 93, \quad 941.094 = 95 \cdot 9906 + 24$

οι παραπάνω ισοτιμίες γράφονται ισοδύναμα:

$$91 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 99), \quad 3 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 98), \quad 93 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 97), \quad 24 \cdot x \ \equiv\ 1 \,(\mathsf{mod}\, 95),$$

Οι μοναδικές λύσεις των παραπάνω ισοτιμιών (οι οποίες βρίσκονται με την γνωστή διαδικασία) είναι αντίστοιχα:

$$b_1 \ \equiv\ 37 \,(\mathsf{mod}\, 99), \quad b_2 \ \equiv\ 35 \,(\mathsf{mod}\, 98), \quad b_3 \ \equiv\ 24 \,(\mathsf{mod}\, 97), \quad b_4 \ \equiv\ 4 \,(\mathsf{mod}\, 95)$$

Επομένως η μοναδική λύση $(\mathsf{mod}\, 99 \cdot 98 \cdot 97 \cdot 95) = (\mathsf{mod}\, 89.403.930)$ του (Σ) είναι:

$$\begin{aligned} x_0 \ &\equiv\ M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 + M_4 b_4 a_4 \,(\mathsf{mod}\, 89.403.930) \\ &\equiv\ 903.070 \cdot 37 \cdot 65 + 912.285 \cdot 35 \cdot 2 + 921.690 \cdot 24 \cdot 51 + 941.094 \cdot 4 \cdot 10 \,(\mathsf{mod}\, 89.403.930) \\ &\equiv\ 3.397.886.480 \,(\mathsf{mod}\, 89.403.930) \\ &\equiv\ 537.140 \,(\mathsf{mod}\, 89.403.930) \quad \blacksquare \end{aligned}$$

Άσκηση 11. *Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma) \qquad \begin{cases} 51\,x \ \equiv\ 2 \,(\mathsf{mod}\, 38) \\ 3\,x \ \equiv\ 6 \,(\mathsf{mod}\, 9) \end{cases}$$

Λύση. Επειδή $(51, 38) = 1$, έπεται ότι η ισοτιμία $51x \equiv 2 \,(\mathsf{mod}\, 38)$ έχει μοναδική λύση $x_0 \,(\mathsf{mod}\, 38)$, η οποία προσδιορίζεται ως εξής. Θα έχουμε: $x_0 \equiv 2 \cdot c \,(\mathsf{mod}\, 38)$, όπου $[c]_{38} = [51]_{38}^{-1}$. Όμως $[51]_{38} = [13]_{38}$ και άρτα αναζητούμε την αντίστροφή κλάση $[13]_{38}^{-1}$. Παρατηρούμε ότι $[1]_{38} = [39]_{38} = [3 \cdot 13]_{38} = [3]_{38} \cdot [13]_{38}$ και επομένως $[13]_{38}^{-1} = [3]_{38}$. Τότε η μοναδική λύσης της ισοτιμίας $51x \equiv 2 \,(\mathsf{mod}\, 38)$ είναι:

$$2 \cdot 3 \,(\mathsf{mod}\, 38) \equiv 6 \,(\mathsf{mod}\, 38) \qquad (\dagger)$$

Για την δεύτερη ισοτιμία $3x \equiv 6 \,(\mathsf{mod}\, 9)$, θα έχουμε. Επειδή $(3, 9) = 3 \mid 6$, έπεται ότι υπάρχουν 3 ανισότιμες $(\mathsf{mod}\, 9)$ λύσεις, οι οποίες όπως μπορούμε να προσδιορόισουμε εύκολα είναι οι εξής:

$$2 \,(\mathsf{mod}\, 9), \quad 5 \,(\mathsf{mod}\, 9), \quad (8 \,(\mathsf{mod}\, 9) \qquad (\dagger\dagger)$$

Επομένως για να βρούμε τις λύσεις του αρχικού συτήματος (Σ), από τις σχέσεις $(\dagger)$ και $(\dagger\dagger)$, αρκεί να βρούμε τις λύσεις των εξής συστημάτων:

$$(\Sigma_1) \quad \begin{cases} x \ \equiv\ 6 \,(\mathsf{mod}\, 38) \\ x \ \equiv\ 2 \,(\mathsf{mod}\, 9) \end{cases}, \qquad (\Sigma_2) \quad \begin{cases} x \ \equiv\ 6 \,(\mathsf{mod}\, 38) \\ x \ \equiv\ 5 \,(\mathsf{mod}\, 9) \end{cases}, \qquad (\Sigma_3) \quad \begin{cases} x \ \equiv\ 6 \,(\mathsf{mod}\, 38) \\ x \ \equiv\ 8 \,(\mathsf{mod}\, 9) \end{cases}$$

Για το (Σ_1): Επειδή $(38,9)=1$, μπορούμε να εφαρμόσουμε Κινέζικο Θεώρημα Υπολοίπων. Θα έχουμε:

$$a_1=6,\quad a_2=2\qquad\&\qquad n_1=38,\quad n_2=9$$
$$M=38\cdot 9=342,\qquad M_1=\frac{M}{n_1}=9,\qquad M_2=\frac{M}{n_2}=38$$

Θαωρούμε τις ισοτιμίες:

$$\begin{cases} M_1\cdot x\ \equiv\ 1\,(\mathsf{mod}\,n_1)\\ M_2\cdot x\ \equiv\ 1\,(\mathsf{mod}\,n_2)\end{cases}\quad\Longrightarrow\quad\begin{cases} 9\cdot x\ \equiv\ 1\,(\mathsf{mod}\,38)\\ 38\cdot x\ \equiv\ 1\,(\mathsf{mod}\,9)\end{cases}\quad\Longrightarrow\quad\begin{cases} 9\cdot x\ \equiv\ 1\,(\mathsf{mod}\,38)\\ 2\cdot x\ \equiv\ 1\,(\mathsf{mod}\,9)\end{cases}$$

κάθε μία εκ των οποίων έχει μοναδική λύση. Για την δεύτερη η μοναδική λύση $\mathsf{mod}\,9$ είναι προφανώς η $b_2\,(\mathsf{mod}\,9)=5\,(\mathsf{mod}\,9)$. Για την πρώτη, υπολογίζουμε εύκολα ότι $[9]_{38}^{-1}=[17]_{38}$, διότι $[9]_{38}\cdot[17]_{38}=[9\cdot 17]_{38}=[153]_{389}=[38\cdot 4+1]_{38}=[1]_{38}$. Άρα

$$b_1=17\qquad\&\qquad b_2=5$$

Η μοναδική λύση $(\mathsf{mod}\,38\cdot 9)$ του συστήματος (Σ_1) είναι:

$$x_0\equiv M_1{\cdot}b_1{\cdot}a_1{+}M_2{\cdot}b_2{\cdot}a_2\,(\mathsf{mod}\,n_1{\cdot}n_2)\ \equiv\ 9{\cdot}17{\cdot}6{+}38{\cdot}5{\cdot}2\,(\mathsf{mod}\,342)\ \equiv\ 1298\,(\mathsf{mod}\,342)\ \equiv\ 272\,(\mathsf{mod}\,342)$$

Για το (Σ_2): Παρόμοια βρίσκουμε ότι η μοναδική λύση $(\mathsf{mod}\,342)$ του (Σ_2) είναι η:

$$x_1\ \equiv\ 158\ (\mathsf{mod}\,342)$$

Για το (Σ_3): Παρόμοια βρίσκουμε ότι η μοναδική λύση $(\mathsf{mod}\,342)$ του (Σ_3) είναι η:

$$x_2\ \equiv\ 44\ (\mathsf{mod}\,342)$$

Επομένως το αρχικό σύστημα ισοτιμιών (Σ) έχει ακριβώς τρείς λύσεις $(\mathsf{mod}\,342)$, τις εξής:

$$272\ (\mathsf{mod}\,342),\qquad 158\ (\mathsf{mod}\,342),\qquad 44\ (\mathsf{mod}\,342)$$

■

• • •

Σχόλιο 5. Θεωρούμε το ακόλουθο σύστημα γραμμικών ισοτιμιών

$$(\Sigma)\quad\begin{cases} x\ \equiv\ a_1\ (\mathsf{mod}\,n_1)\\ x\ \equiv\ a_2\ (\mathsf{mod}\,n_2)\\ \quad\vdots\\ x\ \equiv\ a_k\ (\mathsf{mod}\,n_k)\end{cases}$$

Υπενθυμίζουμε ότι το σύστημα (Σ) έχει λύση αν και μόνον αν:

$$d_{ij}:=(n_i,n_j)\ \mid\ a_i-a_j,\qquad 1\le i\ne j\le k$$

Αν οι παραπάνω σχέσεις διαιρετότητας ικανοποιούνται, τότε το σύστημα (Σ) έχει μοναδική λύση

$$(\mathsf{mod}[n_1,n_2,\cdots,n_k])\qquad\surd$$

• • •

Άσκηση 12. *Βρείτε όλες τις λύσεις στο* $\mathbb{Z}$ *για το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma)\quad\begin{cases} x\ \equiv\ \ 32\,(\mathsf{mod}\,21)\\ x\ \equiv\ -6\,(\mathsf{mod}\,10)\\ x\ \equiv\ \ \ 2\,(\mathsf{mod}\,12)\end{cases}$$

Λύση. – **Πρώτος τρόπος**: Έχουμε $n_1 = 21 = 3 \cdot 7$, $n_2 = 10 = 2 \cdot 5$, $n_3 = 12 = 2^2 \cdot 3$, $b_1 = 32$, $b_2 = -6$, $b_3 = 2$ και

$$(n_1, n_2) = 1 \mid b_1 - b_2$$
$$(n_1, n_3) = 3 \mid b_1 - b_3$$
$$(n_2, n_3) = 2 \mid b_2 - b_3$$

Άρα από τη Θεωρία το σύστημα (Σ) έχει λύση στο $\mathbb{Z}$ και είναι ισοδύναμο με το παρακάτω σύστημα:

$$\begin{cases} x \equiv 32 \,(\mathsf{mod}\, 3) \\ x \equiv 32 \,(\mathsf{mod}\, 7) \\ x \equiv -6 \,(\mathsf{mod}\, 2) \\ x \equiv -6 \,(\mathsf{mod}\, 5) \\ x \equiv 2 \,(\mathsf{mod}\, 2^2) \\ x \equiv 2 \,(\mathsf{mod}\, 3) \end{cases} \iff \begin{cases} x \equiv 2 \,(\mathsf{mod}\, 3) \\ x \equiv 4 \,(\mathsf{mod}\, 7) \\ x \equiv 0 \,(\mathsf{mod}\, 2) \\ x \equiv -1 \,(\mathsf{mod}\, 5) \\ x \equiv 2 \,(\mathsf{mod}\, 4) \\ x \equiv 2 \,(\mathsf{mod}\, 3) \end{cases}$$

Επειδή η πρώτη ισοτιμία συμπίπτει με την έκτη, και η πέμπτη ισοτιμία συνεπάγεται την τρίτη (πραγματικά: αν $x \equiv 2 \,(\mathsf{mod}\, 4)$, τότε $4 \mid x - 2$, απ' όπου εύκολα βλέπουμε ότι $2 \mid x$, δηλαδή $x \equiv 0 \,(\mathsf{mod}\, 2)$), και τέλος επειδή το ελάχιστο κοινό πολλαπλάσιο των αριθμών $3, 7, 2, 5, 4$ συμπίπτει με το ελάχιστο κοινό πολλαπλάσιο των αριθμών $3, 7, 5, 4$, έπεται ότι το παραπάνω σύστημα είναι ισοδύναμο με το ακόλουθο σύστημα γραμμικών ισοτιμιών:

$$\begin{cases} x \equiv 2 \,(\mathsf{mod}\, 3) \\ x \equiv 2 \,(\mathsf{mod}\, 4) \\ x \equiv -1 \,(\mathsf{mod}\, 5) \\ x \equiv 4 \,(\mathsf{mod}\, 7) \end{cases}$$

Επειδή οι αριθμοί $3, 4, 5, 7$ είναι ανα δυο πρώτοι μεταξύ τους, τότε από το Κινέζικο Θεώρημα Υπολοίπων έπεται ότι το σύστημα (Σ) έχει μοναδική λυση

$$x_0 \,(\mathsf{mod}\, M) = x_0 \,(\mathsf{mod}\, 3 \cdot 4 \cdot 5 \cdot 7) = x_0 \,(\mathsf{mod}\, 420)$$

Ακολουθώντας το συνηθισμένο τρόπο λύσης βρίσκουμε ότι: $x_0 \equiv 74 \,(\mathsf{mod}\, 420)$.

– **Δεύτερος Τρόπος**: Αφού $x \equiv 2 \,(\mathsf{mod}\, 3)$ έχουμε ότι υπάρχει κάποιο t_1 έτσι ώστε $x = 3t_1 + 2$. Τότε αντικαθιστώντας στην ισοτιμία $x \equiv 2 \,(\mathsf{mod}\, 2^2)$ έχουμε

$$3t_1 + 2 \equiv 2 \,(\mathsf{mod}\, 2^2) \implies 3t_1 \equiv 0 \,(\mathsf{mod}\, 4) \implies t_1 \equiv 0 \,(\mathsf{mod}\, 4) \implies t_1 = 4t_2$$

και άρα $x = 12t_2 + 2$. Από την εξίσωση $x \equiv -1 \,(\mathsf{mod}\, 5)$ έχουμε

$$12t_2 + 2 \equiv -1 \,(\mathsf{mod}\, 5) \implies 2t_2 \equiv -3 \,(\mathsf{mod}\, 5) \implies 2t_2 \equiv 2 \,(\mathsf{mod}\, 5) \implies t_2 \equiv 1 \,(\mathsf{mod}\, 5)$$

Συνεπώς $t_2 = 5t_3 + 1$ και άρα $x = 60t_3 + 14$. Τέλος, αντικαθιστώντας στην $x \equiv 4 \,(\mathsf{mod}\, 7)$ έχουμε

$$60t_3 + 14 \equiv 4 \,(\mathsf{mod}\, 7) \implies 4t_3 \equiv 4 \,(\mathsf{mod}\, 7)$$

Για $t_3 = 1$ έχουμε τη λύση $x = 60 \cdot 1 + 14 = 74$.

Πράγματι έχουμε

$$[74]_3 = [60 + 14]_3 = [14]_3 = [2]_3$$

$$[74]_4 = [34]_4 = [32 + 2]_4 = [2]_4$$

$$[74]_5 = [75-1]_5 = [-1]_5$$

$$[74]_7 = [70+4]_7 = [4]_7$$

Συνεπώς η μοναδική λύση του συστήματος (Σ) είναι η $x_0 \equiv 74 \,(\mathsf{mod}\, 420)$.

– **Τρίτος Τρόπος**: Επειδή $32 \equiv 11 \,(\mathsf{mod}\, 21)$, και $-6 \equiv 4 \,(\mathsf{mod}\, 10)$, το αρχικό σύστημα είναι προφανώς ισοδύναμο με το

$$(\Sigma') \quad \begin{cases} x \equiv 11 \,(\mathsf{mod}\, 21) \\ x \equiv 4 \,(\mathsf{mod}\, 10) \\ x \equiv 2 \,(\mathsf{mod}\, 12) \end{cases}$$

Όπως και προηγουμένως το (Σ') έχει λύση η οποία είναι μοναδική $\mathsf{mod}\, 420$. Θεωρούμε τις δύο πρώτες ισοτιμίες

$$(\Sigma'_1) \quad \begin{cases} x \equiv 11 \,(\mathsf{mod}\, 21) \\ x \equiv 4 \,(\mathsf{mod}\, 10) \end{cases}$$

Επειδή $(21, 10) = 1$, από το Κινέζικο Θεώρημα Υπολοίπων, το σύστημα (Σ'_1) έχει μοναδική λύση $\mathsf{mod}\, 210$. Εργαζόμενοι όπως στην Άσκηση 5, βλέπουμε εύκολα ότι η μοναδική λύση $\mathsf{mod}\, 210$ του (Σ'_1) είναι η $x \equiv 74 \,(\mathsf{mod}\, 210)$. Επειδή προφανώς το (Σ') είναι ισοδύναμο με το συστημα

$$(\Sigma'_2) \quad \begin{cases} x \equiv 74 \,(\mathsf{mod}\, 210) \\ x \equiv 2 \,(\mathsf{mod}\, 12) \end{cases}$$

έπεται ότι η μοναδική λύση του (Σ'_2), $\mathsf{mod}[210, 12] = \mathsf{mod}\, 420$, είναι η μοναδική λύση του (Σ) $\mathsf{mod}\, 420$. Παρατηρούμε ότι το $x_0 = 74$ ικανοποιεί την $x \equiv 2 \,(\mathsf{mod}\, 12)$, διότι $74 - 2 = 6 \cdot 12$. Επομένως η μοναδική λύση του (Σ) είναι η

$$x \equiv 74 \,(\mathsf{mod}\, 74)$$ ■

Άσκηση 13. *Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για το σύστημα γραμμικών ισοτιμιών*

$$(\Sigma) \quad \begin{cases} 3x \equiv 6 \,(\mathsf{mod}\, 12) \\ 2x \equiv 5 \,(\mathsf{mod}\, 7) \\ 3x \equiv 1 \,(\mathsf{mod}\, 5) \end{cases}$$

Λύση. Η πρώτη ισοτιμία $3x \equiv 6 \,(\mathsf{mod}\, 12)$ είναι προφανώς ισοδύναμη με την $x \equiv 6 \,(\mathsf{mod}\, 4)$. Επομένως το αρχικό σύστημα (Σ) είναι ισοδύναμο με το σύστημα

$$(\Sigma') \quad \begin{cases} x \equiv 2 \,(\mathsf{mod}\, 4) \\ 2x \equiv 5 \,(\mathsf{mod}\, 7) \\ 3x \equiv 1 \,(\mathsf{mod}\, 5) \end{cases}$$

– Επειδή $(2, 7) = 1$, η δεύτερη ισοτιμία έχει μοναδική λύση $(\mathsf{mod}\, 7)$ και αυτή η λύση είναι προφανώς η $x \equiv 6 \,(\mathsf{mod}\, 7)$.

– Επειδή $(3, 5) = 1$, η τρίτη ισοτιμία έχει μοναδική λύση $(\mathsf{mod}\, 5)$ και αυτή η λύση είναι προφανώς η $x \equiv 2 \,(\mathsf{mod}\, 5)$.

Επομένως το σύστημα (Σ') είναι ισοδύναμο με το σύστημα

$$(\Sigma'') \quad \begin{cases} x \equiv 2 \,(\mathsf{mod}\, 4) \\ x \equiv 6 \,(\mathsf{mod}\, 7) \\ x \equiv 2 \,(\mathsf{mod}\, 5) \end{cases}$$

στο οποίο μπορούμε να εφαρμόσουμε το Κινέζικο Θεώρημα Υπολοίπων, και έτσι το (Σ'') έχει μοναδική λύση $(\mathsf{mod}\, 4 \cdot 7 \cdot 5) = (\mathsf{mod}\, 140)$. Θα έχουμε:

$$a_1 = 2, \quad a_2 = 6, \quad a_3 = 2 \quad \& \quad n_1 = 4, \quad n_2 = 7, \quad n_3 = 5$$

$$M = n_1 \cdot n_2 \cdot n_3 = 4 \cdot 7 \cdot 5 = 140$$

$$M_1 = \frac{M}{n_1} = \frac{140}{4} = 35$$
$$M_2 = \frac{M}{n_2} = \frac{140}{7} = 20$$
$$M_3 = \frac{M}{n_3} = \frac{140}{5} = 28$$

Θεωρούμε τις ακόλουθες ισοτιμίες:

$$\begin{cases} 35 \cdot x \equiv 1 \pmod 4 \\ 20 \cdot x \equiv 1 \pmod 7 \\ 28 \cdot x \equiv 1 \pmod 5 \end{cases} \implies \begin{cases} 3 \cdot x \equiv 1 \pmod 4 \\ 6 \cdot x \equiv 1 \pmod 7 \\ 3 \cdot x \equiv 1 \pmod 5 \end{cases} \implies \begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 6 \pmod 7 \\ x \equiv 2 \pmod 5 \end{cases}$$

Επομένως:

$$b_1 = 3, \qquad b_2 = 6, \qquad b_3 = 2$$

και άρα η μοναδική λύση $\pmod{140}$ του συστήματος (Σ'') είναι η

$$\begin{aligned} x_0 &\equiv M_1 \cdot b_1 \cdot a_1 + M_2 \cdot b_2 \cdot a_2 + M_3 \cdot b_3 \cdot a_3 \pmod{140} \\ &= 35 \cdot 3 \cdot 2 + 20 \cdot 6 \cdot 6 + 28 \cdot 2 \cdot 2 \pmod{140} \\ &\equiv 1042 \pmod{140} \\ &\equiv 62 \pmod{140} \end{aligned}$$

Επομένως το αρχικό σύστρημα (Σ) έχει μοναδική λύση $\pmod{14}$, την εξής:

$$62 \pmod{140}$$

■

Άσκηση 14. *Βρείτε όλες τις λύσεις στο $\mathbb{Z}$ για τα σύστηματα γραμμικών ισοτιμιών*

$$(\Sigma) \quad \begin{cases} 2x \equiv 4 \pmod 6 \\ 4x \equiv 8 \pmod{12} \\ 5x \equiv 10 \pmod{25} \end{cases} \qquad \& \qquad (\Sigma') \quad \begin{cases} x \equiv 7 \pmod 9 \\ x \equiv 2 \pmod{10} \\ x \equiv 3 \pmod{12} \\ x \equiv 6 \pmod{15} \end{cases}$$

Λύση. **1.** Επειδή $(2,6) = 2 \mid 4$, $(4,12) = 4 \mid 8$ και $(5,25) = 5 \mid 10$, έπεται ότι:

$$2x \equiv 4 \pmod 6 \iff x \equiv 2 \pmod 3$$
$$4x \equiv 8 \pmod{12} \iff x \equiv 2 \pmod 3$$
$$5x \equiv 10 \pmod{25} \iff x \equiv 2 \pmod 5$$

Επομένως το σύστημα (Σ) είναι ισοδύναμο με το ακόλουθο σύστημα γραμμικών ισοτιμιών:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases} \iff \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases}$$

Προφανώς η μοναδική λύση $\pmod{15}$ του τελευταίου συστήματος, άρα και του αρχικού, είναι η

$$x_0 \equiv 2 \pmod{15}$$

2. Επειδή $m_{13} = (9,12) = 3 \nmid a_1 - a_3 = 7 - 3 = 4$, έπεται ότι το σύστημα (Σ') δεν έχει ακέραιες λύσεις. ■

Άσκηση 15. *(Πρόβλημα του Branmagupta, 7ος αιώνας μ.Χ.) Όταν παίρνουμε αυγά από ένα καλάθι ανά:* $2, 3, 4, 5, 6$ *κάθε φορά, τότε μένουν αντίστοιχα* $1, 2, 3, 4, 5$ *αυγά στο καλάθι. Όταν όμως παίρνουμε ανά* 7 *τότε δεν μένει κανένα. Να υπολογισθεί ο ελάχιστος αριθμός αυγών που θα πρέπει να περιέχει το καλάθι.*

Λύση. – **Πρώτος τρόπος**: Η απάντηση στο Πρόβλημα του Branmagupta είναι η ελάχιστη θετική λύση του παρακάτω συστήματος γραμμικών ισοτιμιών:

$$(\Sigma): \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 6 \\ x \equiv 0 \pmod 7 \end{cases}$$

Η ισοτιμία $x \equiv 5 \pmod 6$ είναι ισοδύναμη[1] με το σύστημα ισοτιμιών

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

δηλαδή ισοδύναμη με το σύστημα

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$$

Οι παραπάνω δυο ισοτιμίες υπάρχουν ήδη στο γραμμικό σύστημα (Σ) και άρα μπορούν να παραληφθούν. Παρατηρούμε επίσης ότι η ισοτιμία $x \equiv 1 \pmod 2$ προκύπτει από την $x \equiv 3 \pmod 4$ και άρα μπορεί να παραληφθεί. Πράγματι αφού $x \equiv 3 \pmod 4$ έπεται ότι ο x είναι περιττός και άρα η εξίσωση $x \equiv 1 \pmod 2$ ισχύει. Συνεπώς το (Σ) είναι ισοδύναμο με το ακόλουθο σύστημα γραμμικών ισοτιμιών:

$$(\Sigma'): \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}$$

Επειδή οι αριθμοί $3, 4, 5, 7$ είναι ανα δυο πρώτοι μεταξύ τους, τότε από το Κινέζικο Θεώρημα Υπολοίπων έπεται ότι το σύστημα (Σ'), και άρα και το (Σ), έχει μοναδική λυση

$$x_0 \pmod M = x_0 \pmod{3 \cdot 4 \cdot 5 \cdot 7} = x_0 \pmod{420}$$

Ακολουθώντας το συνηθισμένο τρόπο λύσης (βλέπε Άσκηση 7) βρίσκουμε ότι $x_0 = 119$.

– **Δεύτερος τρόπος**: Από την $x \equiv 2 \pmod 3$ έχουμε ότι $x = 3t_1 + 2$ και άρα από την $x \equiv 3 \pmod 4$ έπεται ότι

$$3t_1 + 2 \equiv 3 \pmod 4 \implies 3t_1 \equiv 1 \pmod 4 \implies 3 \cdot (3t_1) \equiv 3 \pmod 4 \implies t_1 \equiv 3 \pmod 4$$

[1] Γενικά, αν $(n_1, n_2) = 1$, τότε: $x \equiv a \pmod{n_1}$ & $x \equiv a \pmod{n_2} \iff x \equiv a \pmod{n_1 n_2}$

Επομένως $t_1 = 4t_2 + 3$ και άρα $x = 3 \cdot (4t_2 + 3) + 2 = 12t_2 + 11$. Τότε από την εξίσωση $x \equiv 4 \pmod 5$ έπεται ότι

$$\begin{aligned} 12t_2 + 11 \equiv 4 \pmod 5 &\implies 2t_2 + 1 \equiv 4 \pmod 5 \\ &\implies 2t_2 \equiv 3 \pmod 5 \\ &\implies 3 \cdot (2t_2) \equiv 9 \pmod 5 \\ &\implies t_2 \equiv 4 \pmod 5 \\ &\implies t_2 = 5t_3 + 4 \end{aligned}$$

και άρα $x = 12 \cdot (5t_3 + 4) + 11 = 60t_3 + 59$. Τέλος από την εξίσωση $x \equiv 0 \pmod 7$ έπεται ότι

$$60t_3 + 59 \equiv 0 \pmod 7 \implies 4t_3 \equiv -3 \pmod 7 \implies 4t_3 \equiv 4 \pmod 7 \implies t_3 \equiv 1 \pmod 7$$

Επομένως $t_3 = 7t_4 + 1$ και άρα

$$x = 420t_4 + 60 + 59 = 420t_4 + 119.$$

Φανερά, για ακέραιο t_4 η ελάχιστη θετική τιμή που παίρνει το x είναι 119 για $t_4 = 0$. Συνεπώς ο ελάχιστος αριθμός αυγών που θα πρέπει να περιέχει το καλάθι είναι 119. ■

Άσκηση 16. *Σε ένα πάρτυ, κάποιος ζητάει από έναν γνωστό του να διαλέξει στην τύχη έναν αριθμό από το 1 μέχρι το 100, και ακολούθως χωρίς να του αναφέρει το αριθμό, του ζητάει να του πει τα υπόλοιπα των διαιρέσεων του αριθμού με τους αριθμούς 3, 5, και 7. Γνωρίζοντας τα υπόλοιπα αυτών των διαιρέσεων, μπορείτε να βρείτε τον κρυφό αριθμό;*

Λύση. Έστω a_1 το υπόλοιπο της διαίρεσης του x_0 με το 3, a_2 το υπόλοιπο της διαίρεσης του x_0 με το 5 και a_3 το υπόλοιπο της διαίρεσης του x_0 με το 7. Τότε ο κρυφός αριθμός x_0, όπου $1 \leq x_0 \leq 100$, είναι η λύση του συστήματος γραμμικών ισοτιμιών:

$$(\Sigma): \begin{cases} x \equiv a_1 \pmod 3 \\ x \equiv a_3 \pmod 5 \\ x \equiv a_3 \pmod 7 \end{cases}$$

Επειδή οι αριθμοί $3, 5, 7$ είναι ανα δυο πρώτοι μεταξύ τους, τότε από το Κινέζικο Θεώρημα Υπολοίπων έπεται ότι το σύστημα (Σ) έχει μοναδική λυση

$$x_0 \pmod M = x_0 \pmod{3 \cdot 5 \cdot 7} = x_0 \pmod{105}$$

Υπολογίζουμε

$$M_1 = \frac{3 \cdot 5 \cdot 7}{3} = 35$$

$$M_2 = \frac{3 \cdot 5 \cdot 7}{5} = 21$$

$$M_3 = \frac{3 \cdot 5 \cdot 7}{7} = 15$$

και έχουμε τις παρακάτω εξισώσεις:

$$\begin{cases} 35x \equiv 1 \pmod 3 \\ 21x \equiv 1 \pmod 5 \\ 15x \equiv 1 \pmod 7 \end{cases} \implies \begin{cases} 2x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 7 \end{cases} \implies \begin{cases} x \equiv -1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 7 \end{cases}$$

Άρα $b_1 = -1$, $b_2 = 1$, $b_3 = 1$ και η λύση είναι η

$$\begin{aligned} x_0 &= M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 \\ &= 35 \cdot (-1) \cdot a_1 + 21 \cdot 1 \cdot a_2 + 15 \cdot 1 \cdot a_3 \\ &= -35a_1 + 21a_2 + 15a_3 \end{aligned}$$

Επομένως ο ζητούμενος κρυφός αριθμός είναι το μικρότερο θετικό υπόλοιπο $(\mathsf{mod}\, 105)$ του αριθμού:

$$-35a_1 + 21a_2 + 15a_3$$ ■

Άσκηση 17. *Επτά ληστές προσπαθούν να μοιράσουν δίκαια τα κλοπιμαία τα οποία αποτελούνται από ράβδους χρυσού. Μετά τη μοιρασιά 6 ράβδοι χρυσού περίσσεψαν και στη διαμάχη που ακολούθησε ένας ληστής σκοτώθηκε. Οι υπόλοιποι έξι ληστές δοκίμασαν να μοιράσουν πάλι τους ράβδους, αλλά πάλι δεν τα κατάφεραν διότι αυτή τη φορά περίσσεψαν 2 ράβδοι. Στη διαμάχη που ακολούθησε ένας ακόμα ληστής σκοτώθηκε. Στη νέα μοιρασιά που ακολούθησε περίσσεψε μια ράβδος χρυσού και μετά τον θάνατο ενός ακόμα ληστή, τελικά οι εναπομείναντες ληστές κατάφεραν να μοιράσουν στα ίσια τους ράβδους χρυσού.*

Ποιός είναι ο ελάχιστος αριθμός ράβδων χρυσού που έκλεψαν οι ληστές;

Λύση. Έστω x ο ζητούμενος αριθμός ράβδων χρυσού που έκλεψαν οι ληστές. Έχουμε

- Επτά ληστές − Πρώτη μοιρασιά: $x \equiv 6\,(\mathsf{mod}\, 7)$
- Έξι ληστές − Δεύτερη μοιρασιά: $x \equiv 2\,(\mathsf{mod}\, 6)$
- Πέντε ληστές − Τρίτη μοιρασιά: $x \equiv 1\,(\mathsf{mod}\, 5)$
- Τέσσερις ληστές − Τελευταία μοιρασιά: $x \equiv 0\,(\mathsf{mod}\, 4)$

Άρα ο ζητούμενος αριθμός ράβδων χρυσού είναι η (μοναδική) λύση $(\mathsf{mod}\, 7 \cdot 6 \cdot 5 \cdot 4)$ του συστήματος γραμμικών ισοτιμιών:

$$(\Sigma): \begin{cases} x \equiv 6\,(\mathsf{mod}\, 7) \\ x \equiv 2\,(\mathsf{mod}\, 6) \\ x \equiv 1\,(\mathsf{mod}\, 5) \\ x \equiv 0\,(\mathsf{mod}\, 4) \end{cases}$$

Ελέγχουμε ότι πράγματι το παραπάνω σύστημα έχει λύση:

$$\begin{gathered} a_1 = 6, \quad a_2 = 2, \quad a_3 = 1, \quad a_4 = 0 \\ m_{12} = (7,6) = 1 \mid a_1 - a_2 = 4 \\ m_{13} = (7,5) = 1 \mid a_1 - a_3 = 6 \\ m_{14} = (7,4) = 1 \mid a_1 - a_4 = 6 \\ m_{23} = (6,5) = 1 \mid a_2 - a_3 = 2 \\ m_{24} = (6,4) = 2 \mid a_2 - a_4 = 2 \\ m_{34} = (5,4) = 1 \mid a_3 - a_4 = 1 \end{gathered}$$

Θεωρούμε το σύστημα

$$(\Sigma'): \begin{cases} x \equiv 6\,(\mathsf{mod}\, 7) \\ x \equiv 2\,(\mathsf{mod}\, 6) \\ x \equiv 1\,(\mathsf{mod}\, 5) \end{cases}$$

και υπολογίζουμε

$$a_1 = 6, \quad a_2 = 2, \quad a_3 = 1$$

$$M = 7 \cdot 6 \cdot 5 = 210, \quad M_1 = \frac{7 \cdot 6 \cdot 5}{7} = 30, \quad M_2 = \frac{7 \cdot 6 \cdot 5}{6} = 35, \quad M_3 = \frac{7 \cdot 6 \cdot 5}{5} = 42,$$

Τότε έχουμε τις παρακάτω εξισώσεις:

$$\begin{cases} 30x \equiv 1 \,(\mathsf{mod}\, 7) \\ 35x \equiv 1 \,(\mathsf{mod}\, 6) \\ 42x \equiv 1 \,(\mathsf{mod}\, 5) \end{cases} \implies \begin{cases} 2x \equiv 1 \,(\mathsf{mod}\, 7) \\ 5x \equiv 1 \,(\mathsf{mod}\, 6) \\ 2x \equiv 1 \,(\mathsf{mod}\, 5) \end{cases} \implies \begin{cases} x \equiv 4 \,(\mathsf{mod}\, 7) \\ x \equiv 5 \,(\mathsf{mod}\, 6) \\ x \equiv 3 \,(\mathsf{mod}\, 5) \end{cases}$$

Επομένως θα έχουμε:

$$b_1 = 4, \quad b_2 = 5, \quad b_3 = 3$$

και τότε από το Κινέζικο Θεώρημα Υπολοίπων έπεται ότι η μοναδική λύση $(\mathsf{mod}\, 210)$ του (Σ') είναι η

$$\begin{aligned} y_0 &= M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 \\ &= 30 \cdot 4 \cdot 6 + 35 \cdot 5 \cdot 2 + 42 \cdot 3 \cdot 1 \\ &= 720 + 350 + 126 \\ &\equiv 1196 \,(\mathsf{mod}\, 210) \\ &\equiv 146 \,(\mathsf{mod}\, 210) \end{aligned}$$

Από το σύστημα (Σ) και την παραπάνω λύση του (Σ') έχουμε το παρακάτω σύστημα:

$$\begin{cases} x \equiv 146 \,(\mathsf{mod}\, 210) \\ x \equiv 0 \,(\mathsf{mod}\, 4) \end{cases}$$

Από τη δεύτερη εξίσωση έπεται ότι $x = 4t$ και άρα από τη πρώτη έχουμε

$$\begin{aligned} 4t \equiv 146 \,(\mathsf{mod}\, 210) &\implies 2t \equiv 73 \,(\mathsf{mod}\, 105) \\ &\implies t = [2]_{105}^{-1} \cdot [73]_{105} = [53]_{105} \cdot [73]_{105} = [3869]_{105} = [89]_{105} \end{aligned}$$

Συνεπώς ο ελάχιστος αριθμός ράβδων χρυσού που έκλεψαν οι ληστές είναι

$$x = 4 \cdot 89 = 356$$

■

Άσκηση 18. *Να βρεθούν όλες οι ακέραιες λύσεις του συστήματος (όχι απαραίτητα γραμμικών) ισοτιμιών:*

$$(\Sigma) \quad \begin{cases} x^2 \equiv 1 \,(\mathsf{mod}\, 3) \\ x \equiv 2 \,(\mathsf{mod}\, 4) \end{cases}$$

Λύση. Για την πρώτη ισοτιμία, θα έχουμε:

$$x^2 \equiv 1 \,(\mathsf{mod}\, 3) \iff 3 \mid x^2 - 1 \iff 3 \mid (x-1) \cdot (x+1) \iff 3 \mid x-1 \text{ ή } 3 \mid x+1 \iff$$

$$\iff x \equiv 1 \,(\mathsf{mod}\, 3) \text{ ή } x \equiv -1 \,(\mathsf{mod}\, 3) \iff x \equiv 1 \,(\mathsf{mod}\, 3) \text{ ή } x \equiv 2 \,(\mathsf{mod}\, 3)$$

Επομένως το αρχικό σύστημα ισοτιμιών (Σ) είναι ισοδύναμο με το ζεύγος συστημάτων

$$(\Sigma_1) \quad \begin{cases} x \equiv 1 \,(\mathsf{mod}\, 3) \\ x \equiv 2 \,(\mathsf{mod}\, 4) \end{cases} \qquad \& \qquad (\Sigma_2) \quad \begin{cases} x \equiv 2 \,(\mathsf{mod}\, 3) \\ x \equiv 2 \,(\mathsf{mod}\, 4) \end{cases}$$

Για την επίλυση των συστημάτων (Σ_1) και (Σ_2) μπορούμε να εφαρμόσουμε Κινέζικο Θεώρημα Υπολοίπων, και να έχουμε ότι η μοναδική λύση $(\mathsf{mod}\, 12)$ του (Σ_1) είναι:

$$10 \,(\mathsf{mod}\, 12)$$

και η μοναδική λύση $(\mathsf{mod}\,12)$ του (Σ_2) είναι:

$$2\ (\mathsf{mod}\,12)$$

Άρα οι μοναδικές λύσεις $(\mathsf{mod}\,12)$ του αρχικού συστήματος (Σ) είναι:

$$10\ (\mathsf{mod}\,12) \quad \& \quad 2\ (\mathsf{mod}\,12)$$

■

Άσκηση 19. *Να βρεθούν όλες οι ακέραιες λύσεις του συστήματος γραμμικών ισοτιμιών:*

$$(\Sigma) \quad \begin{cases} x \equiv 2\,(\mathsf{mod}\,14) \\ x \equiv 16\,(\mathsf{mod}\,21) \\ x \equiv 10\,(\mathsf{mod}\,30) \end{cases}$$

Λύση. Θα έχουμε:

$$a_1 = 2, \quad a_2 = 16, \quad a_3 = 10$$

$$m_{12} = (14, 21) = 7 \mid a_1 - a_2 = -14$$

$$m_{13} = (14, 30) = 2 \mid a_1 - a_3 = -28$$

$$m_{23} = (21, 30) = 3 \mid a_2 - a_3 = 6$$

Επομένως το σύστημα (Σ) έχει μοναδική λύση $(\mathsf{mod}[14, 21, 30]) = (\mathsf{mod}\,210)$.

Από την πρώτη ισοτιμία, έχουμε:

$$x \equiv 2\,(\mathsf{mod}\,14) \implies 14 \mid x - 2 \implies \exists\, k \in \mathbb{Z}: \quad x = 14 \cdot k + 2 \tag{1}$$

Με χρήση της (1), από την δεύτερη ισοτιμία, έχουμε:

$$x \equiv 16\,(\mathsf{mod}\,21) \implies 14 \cdot k + 2 \equiv 16\,(\mathsf{mod}\,21) \implies 14 \cdot k \equiv 14\,(\mathsf{mod}\,21) \implies 2 \cdot k \equiv 2\,(\mathsf{mod}\,3)$$

Η μοναδική λύση $(\mathsf{mod}\,3)$ της τελευταίας ισοτιμίας είναι η $k \equiv 1\,(\mathsf{mod}\,3)$ και επομένως:

$$k \equiv 1\,(\mathsf{mod}\,3) \implies 3 \mid k - 1 \implies \exists\, \lambda \in \mathbb{Z}: \quad k = 3 \cdot \lambda + 1 \tag{2}$$

Με χρήση της (2), η σχέση (1) δίνει:

$$x = 14 \cdot (3 \cdot \lambda + 1) + 2 = 42 \cdot \lambda + 16 \tag{3}$$

Με χρήση της (3), από την τρίτη ισοτιμία, έχουμε:

$$x \equiv 10\,(\mathsf{mod}\,30) \implies 42 \cdot \lambda + 16 \equiv 10\,(\mathsf{mod}\,30) \implies 42 \cdot \lambda + 6 \equiv 0\,(\mathsf{mod}\,30) \implies 30 \mid 42 \cdot \lambda + 6 \implies$$

$$\exists\, \mu \in \mathbb{Z}: \quad 42 \cdot \lambda + 6 = 30 \cdot \mu \implies 7 \cdot \lambda + 1 = 5 \cdot \mu \implies 7 \cdot \lambda \equiv -1\,(\mathsf{mod}\,5) \implies 2 \cdot \lambda \equiv 4\,(\mathsf{mod}\,5)$$

Η μοναδική λύση της τελευταίας ισοτιμίας είναι $\lambda \equiv 2\,(\mathsf{mod}\,5)$, και άρα:

$$\lambda \equiv 2\,(\mathsf{mod}\,5) \implies 5 \mid \lambda - 2 \implies \exists\, \nu \in \mathbb{Z}: \quad \lambda = 5 \cdot \nu + 2 \tag{4}$$

Τότε η (3), με χρήση της (4), δίνει:

$$x = 42 \cdot \lambda + 16 = 42 \cdot (5 \cdot \nu + 2) + 16 = 210 \cdot \nu + 100 \implies x \equiv 100\,(\mathsf{mod}\,210)$$

είναι η μοναδική λύση $(\mathsf{mod}\,210)$ του αρχικού συστήματος. ■

Άσκηση 20. *Να βρεθούν όλες οι ακέραιες λύσεις του συστήματος γραμμικών ισοτιμιών:*

$$(\Sigma) \quad \begin{cases} x \equiv 2\,(\mathsf{mod}\,6) \\ x \equiv 4\,(\mathsf{mod}\,8) \\ x \equiv 2\,(\mathsf{mod}\,14) \\ x \equiv 14\,(\mathsf{mod}\,15) \end{cases}$$

Λύση. Θα έχουμε:

$$a_1 = 2, \quad a_2 = 4, \quad a_3 = 2, \quad a_4 = 14$$
$$m_{12} = (6,8) = 2 \mid a_1 - a_2 = -2$$
$$m_{13} = (6,14) = 2 \mid a_1 - a_3 = 0$$
$$m_{14} = (6,15) = 1 \mid a_1 - a_4 = -12$$
$$m_{23} = (8,14) = 2 \mid a_2 - a_3 = 2$$
$$m_{24} = (8,15) = 1 \mid a_2 - a_4 = -10$$
$$m_{34} = (14,15) = 1 \mid a_3 - a_4 = -12$$

Επομένως το σύστημα (Σ) έχει μοναδική λύση $(\mathsf{mod}[6,8,14,15]) = (\mathsf{mod}\,840)$.

Θεωρούμε τις δύο τελευταίες ισοτιμίες:

$$(\Sigma_1) \quad \begin{cases} x \equiv 2 \,(\mathsf{mod}\,14) \\ x \equiv 14 \,(\mathsf{mod}\,15) \end{cases}$$

Για την επίλυση του συστήματος (Σ_1) μπορούμε να εφαρμόσουμε το Κινέζικο Θεώρημα Υπολοίπων, και τότε μπορούμε να δούμε εύκολα ότι η μοναδική λύση $(\mathsf{mod}\,14 \cdot 15) = (\mathsf{mod}\,210)$ του (Σ_1) είναι:

$$x \equiv 2774 \,(\mathsf{mod}\,210) \quad \Longrightarrow \quad x \equiv 44 \,(\mathsf{mod}\,210) \tag{1}$$

Θεωρούμε τις δύο πρώτες ισοτιμίες:

$$(\Sigma_2) \quad \begin{cases} x \equiv 2 \,(\mathsf{mod}\,6) \\ x \equiv 4 \,(\mathsf{mod}\,8) \end{cases}$$

η πρώτη εκ των οποίων δίνει:

$$x \equiv 2 \,(\mathsf{mod}\,6) \quad \Longrightarrow \quad 6 \mid x - 2 \quad \Longrightarrow \quad \exists\, k \in \mathbb{Z} : \;\; x = 6 \cdot k + 2 \tag{2}$$

Με χρήση της (2), η πρώτη ισοτιμία δίνει:

$$x \equiv 4 \,(\mathsf{mod}\,8) \quad \Longrightarrow \quad 6 \cdot k + 2 \equiv 4 \,(\mathsf{mod}\,8) \quad \Longrightarrow \quad 6 \cdot k \equiv 2 \,(\mathsf{mod}\,8) \quad \Longrightarrow \quad 3 \cdot k \equiv 1 \,(\mathsf{mod}\,4)$$

Η μοναδική λύση της τελευταίας ισοτιμίας είναι

$$k \equiv 3 \,(\mathsf{mod}\,4) \quad \Longrightarrow \quad 4 \mid k - 3 \quad \Longrightarrow \quad \exists\, \lambda \in \mathbb{Z} : \;\; k = 4 \cdot \lambda + 3 \tag{3}$$

Τότε από τις (2) και (3) θα έχουμε:

$$x = 6 \cdot k + 2 \quad \Longrightarrow \quad x = 6 \cdot (4 \cdot \lambda + 3) + 2 \quad \Longrightarrow \quad x = 24 \cdot \lambda + 20 \tag{4}$$

Επομένως η μοναδική λύση $(\mathsf{mod}[6,8]) = (\mathsf{mod}\,24)$ του (Σ_2) είναι η

$$x \equiv 20 \,(\mathsf{mod}(24) \tag{5}$$

Θεωρούμε το σύστημα το οποίο προκύπτει από τις (1) και (5):

$$(\Sigma_3) \quad \begin{cases} x \equiv 44 \,(\mathsf{mod}\,210) \\ x \equiv 20 \,(\mathsf{mod}\,24) \end{cases}$$

η μοναδική λύση του οποίου $(\mathsf{mod}[210,24]) = (\mathsf{mod}\,840)$ είναι προφανώς η $44 \,(\mathsf{mod}\,840)$, διότι ικανοποιεί και τις δύο ισοτιμίες του (Σ_3). Επομένως η μοναδική λύση $(\mathsf{mod}\,840)$ του αρχικού συστήματος είναι:

$$44 \,(\mathsf{mod}\,840)$$

■