NO:
DATE: 11/01/16

Η γραμμική ισοτιμία: $a-x \equiv b \pmod n$ (*)

① Η (*) έχει μοναδική λύση, αν $(a,n)=1$, και η μοναδική λύση είναι η $x_0 \equiv b \cdot c \pmod n$, όπου c είναι ακέραιος ($c \in \mathbb{Z}$): $[a]_n^{-1} = [c]_n$ $[(a,n)=1 \Rightarrow \exists\, c \in \mathbb{Z}\ x' \in \mathbb{Z} : a \cdot c + x'n = 1]$.

② Έχει τουλάχιστον μία λύση $\Leftrightarrow \delta = (a,n) \mid b$. Αν $\delta = (a,n) \mid b$ και x_0 μια λύση της (*), τότε όλες οι ανά δύο αναδότιμες λύσεις της (*) είναι: $x_0, x_0 + \frac{n}{\delta}, x_0 + 2\frac{n}{\delta}, \ldots, x_0 + (\delta-1)\frac{n}{\delta}$

Πως βρίσκουμε την x_0; Η (*) είναι ισοδύναμη με τη γραμμική ισοτιμία $\frac{a}{\delta} \cdot x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}}$ (**)

Αν x_0 είναι η μοναδική λύση $\bmod \frac{n}{\delta}$ της (**), τότε η x_0 είναι μια λύση της (*) $\bmod n$.

Άσκηση: (*) $\underset{a}{10}\, x \equiv \underset{b}{6} \pmod{\underset{n}{14}}$.

Λύση: Έστω $\delta = (10,14) = 2 \mid 6 \Rightarrow$ η (*) έχει τουλάχιστον μία λύση.

Τότε θεωρούμε τη γραμμική ισοτιμία:
$\frac{10}{2} x \equiv \frac{6}{2} \pmod{\frac{14}{2}}$ δηλαδή: $5x \equiv 3 \pmod 7$ (**)

Η (**) έχει μοναδική λύση $\pmod 7$
$(5,7)=1 \xrightarrow[\text{Euler}]{\text{Θεώρημα}} 5^{\varphi(7)} \Rightarrow \pmod 7 \Rightarrow 5^6 \equiv 1 \pmod 7$

$\Rightarrow [5]_7^6 = [1]_7 \Rightarrow [5]_7^5 \cdot [5]_7 \equiv [1]_7 \Rightarrow$

NO:
DATE:

$[5]_7^{-1} = [5]_7^5 = [5^5]_7$. Όμως $5^5 = 5\cdot5\cdot5\cdot5\cdot5 = 25\cdot25\cdot5$
$\equiv 4\cdot4\cdot5 \equiv 16\cdot5 \equiv 2\cdot5 \equiv 10 \equiv 3 \bmod 7$. Άρα.
$[5]_7^{-1} \equiv [3]_7$. Τότε:
$x_0 = 3\cdot3 = 9 \bmod 7 \Rightarrow x_0 = 2 \pmod 7$: μοναδική λύση του (**).
Τότε όλες οι ανά δύο ανισότιμες λύσεις της (**) είναι:
$2,\ 2+1\cdot\underbrace{7}_{\delta} = 2+\underbrace{14}_{2} = 9$

ΣΥΣΤΗΜΑΤΑ ΓΡΑΜΜΙΚΩΝ ΙΣΟΤΙΜΙΩΝ

Να βρεθεί ένας ακέραιος ο οποίος όταν διαιρεθεί με τους φυσικούς αριθμούς $m_1, m_2, \dots, m_r$, να αφήνει υπόλοιπο: $a_1, a_2, \dots, a_r$, αντίστοιχα. Αυτό το οποίο ζητείται είναι μια κοινή λύση των γραμμικών ισοτιμιών: $x \equiv a_1 \pmod{m_1} \dots x \equiv a_r \pmod{m_r}$
Ένα σύστημα γραμμικών ισοτιμιών είναι της μορφής:

$$(\Sigma)\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_k \cdot x \equiv b_k \pmod{m_k} \end{cases}$$

Μια λύση του (Σ) είναι ένας $x_0 \in \mathbb{Z}$ ο οποίος είναι λύση κάθε ισοτιμίας του (Σ).

Παράδειγμα: Το σύστημα γραμμικών ισοτιμιών:

$\begin{cases} x = 0 \pmod 2 \\ x = 1 \pmod 2 \end{cases}$ → δεν έχει καμία ακέραια λύση

NO:
DATE:

Κινέζικο Θεώρημα Υπολοίπου

Θεωρούμε το σύστημα γραμμικών ισοτιμιών:

$$(\Sigma)\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

και υποθέτουμε ότι $(m_i, m_j) = 1$, $1 \le i \ne j \le r$.

Τότε το (Σ) έχει τουλάχιστον μια λύση που είναι μοναδική $(\mod m_1 \cdot m_2 \cdots m_r)$

Απόδειξη: Θέτουμε: $M = m_1 m_2 \cdots m_r$ και $M_i = \frac{M}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_r$ $1 \le i \le r$

Θεωρούμε τις γραμμικές ισοτιμίες: $M_i X \equiv 1 \pmod{m_i}$
Επειδή $(m_i, m_j) = 1$, $\forall\, 1 \le i \ne j \le r \Rightarrow$
$(M_i, m_i) = 1$, $\forall i = 1, \dots, r$ [Αν $(M_i, m_i) = d_i \ge 1$, τότε έστω $p \mid d_i$, όπου p: πρώτος. Τότε: $p \mid M_i$ και $p \mid m_1 \cdots m_{i-1} m_{i+1} \cdots m_r \Rightarrow p \mid m_i$ κ' $p \mid M_j$, όπου $j \ne i \Rightarrow$ $p(m_i, m_j) \Rightarrow$ άτοπο]

Επειδή $(M_i, m_i) = 1$, $1 \le i \le r \Rightarrow$ η γραμμική ισοτιμία: $M_i X = 1 \pmod{m_i}$, $1 \le i \le r$ έχει μοναδική λύση την b_i, $1 \le i \le r$. Θέτουμε:

$$X_0 = \sum_{i=1}^{r} M_i b_i a_i = M_1 b_1 a_1 + \dots + M_r b_r a_r$$

Θα δείξουμε ότι ο ακέραιος x_0 είναι η μοναδική λύση του $(\Sigma) \mod m_1 m_2 \cdots m_r$

NO:
DATE:

Για κάθε $j = 1, \dots, r$ με $j \neq i$: $M_i \equiv 0 \pmod{m_j}$

(διότι $M_i = m_1 m_2 \dots m_{i-1} m_{i+1} \dots m_r$) $\Rightarrow$

$M_i b_i a_i \equiv 0 \pmod{m_j}$, αν $j \neq i$ $\longrightarrow$

$M_i b_i a_i \equiv a_i \pmod{m_j}$, αν $j = i$

Τότε $x_0 = M_1 b_1 a_1 + \dots + M_r b_r a_r \equiv a_i \pmod{m_i}$
$\forall i = 1, \dots, r$.

Άρα ο ακέραιος x_0 είναι λύση του (Σ)

Έστω x_1 μια άλλη λύση του (Σ) Τότε: $x_0 \equiv a_i \pmod{m_i}$ $\Rightarrow$
$x_1 \equiv a_i \pmod{m_i}$, $\forall i = 1, \dots, r$.

$x_1 \equiv x_0 \pmod{m_i} \Rightarrow m_i \mid x_1 - x_0$ $\Rightarrow m_1 m_2 \dots m_r \mid x_1 - x_0 \Rightarrow$
$1 \leq i \leq r$

$x_1 \equiv x_0 \pmod{m_1 \dots m_r}$.

ΠΑΡΑΔΕΙΓΜΑ

(Σ) $\begin{cases} x \equiv 2 \pmod 3 \\ x = 3 \pmod 5 \\ x = 2 \pmod 7 \end{cases}$ $\quad \begin{matrix} a_1 = 2 \\ a_2 = 3 \\ a_3 = 2 \end{matrix} \quad \begin{matrix} m_1 = 3 \\ m_2 = 5 \\ m_3 = 7 \end{matrix}$

$M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$.

$M_1 = \frac{M}{m_1} = 35$, $M_2 = \frac{M}{m_2} = 21$, $M_3 = \frac{M}{m_3} = 15$

NO:
DATE:

$M_1 X \equiv 1 \pmod{m_1}$
$M_2 X \equiv 1 \pmod{m_2}$
$M_3 X \equiv 1 \pmod{m_3}$

$\Rightarrow$

$35x \equiv 1 \pmod 3$
$21x \equiv 1 \pmod 5$
$15x \equiv 1 \pmod 7$

$\Rightarrow$

$2x \equiv 1 \pmod 3$
$x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 7$

$\Rightarrow$

$b_1 = 2 \pmod 3$
$b_2 = 1 \pmod 5$
$b_3 = 1 \pmod 7$

$x_0 = M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 = 35 \cdot 2 \cdot 2 + 21 \cdot 3 \cdot 1 + 15 \cdot 2 \cdot 1 = 233 \Rightarrow 0 < x \in \mathbb{Z} : x_0 = 233$ είναι η μοναδική λύση του $(\Sigma) \bmod m_1 m_2 m_3$ δηλαδή $\bmod 105 \Rightarrow x_0 = 23 \pmod{105}$

ΘΕΩΡΗΜΑ: Θεωρούμε το ακόλουθο σύστημα γραμμικών ισοτιμιών:

(Σ)
$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_r \pmod{m_r}$

Θέτουμε $d_{ij} = (m_i, m_j)$, $1 \le i \ne j \le r$
Αν $d_{ij} \mid a_i - a_j$, $\forall i, j = 1, \dots, r$, με $i \ne j$ τότε το (Σ) έχει λύση που είναι μοναδική $(\bmod [m_1, m_2, \dots, m_r])$

ΠΑΡΑΔΕΙΓΜΑ: Θεωρούμε το ακόλουθο σύστημα:

(Σ)
$x \equiv 7 \pmod{18}$ $a_1 = 7$ $m_1 = 18$ $d_{12} = (m_1, m_2) = (18, 15) = 3$
$x \equiv 10 \pmod{15}$ $a_2 = 10$ $m_2 = 15$ $d_{13} = (m_1, m_3) = (18, 14) = 2$
$x = 1 \pmod{14}$ $a_3 = 1$ $m_3 = 14$ $d_{23} = (m_2, m_3) = (15, 14) = 1$

$d_{12} = 3 \mid -3 = a_1 - a_2$ ✓
$d_{13} = 2 \mid 6 = a_1 - a_3$ ✓
$d_{23} = 1 \mid 9 = a_2 - a_3$ ✓

Από το Θεώρημα $\Rightarrow$ το (Σ) έχει μοναδική λύση $(\bmod [18, 15, 14]) = (\bmod 630)$

NO:
DATE:

• $x \equiv 7 \pmod{18} \Rightarrow 18 \mid x-7 \Rightarrow x-7 = 18t$, για κάποιο $t \in \mathbb{Z}$.
Τότε: $x = 18t + 7$, $t \in \mathbb{Z}$

$x \equiv 10 \pmod{15} \Rightarrow 18t + 7 = 10 \pmod{15} \Rightarrow 18t \equiv 3 \pmod{15}$:
Μια λύση αυτής είναι:

$$\frac{18}{3}t = \frac{3}{3} \pmod{\frac{15}{3}} \Rightarrow 6t \equiv 1 \pmod{5} \Rightarrow t \equiv 1$$

η μοναδική λύση της $6t = 1 \pmod 5$

Τότε: $x = 18 \cdot 1 + 7 = 25$ και άρα η $x = 25$ είναι η μοναδική λύση των 2 πρώτων εξισώσεων
$\pmod{[18, 15]} = \pmod{90}$ Τότε: $x \equiv 25 \pmod{90} \Rightarrow$
$x \equiv 1 \pmod{14}$

Ομοίως λύνουμε με τον ίδιο τρόπο
Η κοινή λύση είναι $x = 295 \pmod{[90, 14]} \Rightarrow$
$x = 295 \pmod{630}$
Άρα μοναδική λύση του (Σ) είναι $\pmod{630}$