13/12/2018

Παρατήρηση Έστω (*) $ax \equiv b \bmod n$ ισοτιμία που έχει λύση στο $\mathbb{Z}$ (ισοδύναμα $\text{ΜΚΔ}(a,n) \mid b$). Έβαλε αλγόριθμο που υπολογίζει $e, m \in \mathbb{Z}$ ώστε η (*) έχει ίδιες λύσεις με την ισοτιμία $x \equiv e \bmod n$. Άρα το σύνολο λύσεων της (*) είναι

$S = \{e + t \cdot m \mid t \in \mathbb{Z}\}$ δηλαδή S κλάση ισοτιμίας $\bmod m$.

Άρα αν έχω m το πλήθος διαδοχικοί ακέραιοι, ακριβώς ένας από αυτούς είναι λύση του (*). (Υπενθυμίζουμε $m = \frac{n}{\text{ΜΚΔ}(a,n)}$)

Άρα αν μας δίνουν συστήματα από ισοτιμίες:

$$(\Sigma) \begin{cases} a_1 x \equiv b_1 \bmod n_1 \\ \\ a_l x \equiv b \bmod n \end{cases}$$

Βήμα 1ο Για κάθε μια $a_i x \equiv b_i \bmod n_i$ ελέγχουμε αν $\text{ΜΚΔ}(a_i, n_i) \mid b_i$.

Περίπτωση 1 Υπάρχει ένα i ώστε $\text{ΜΚΔ}(a_i, b_i) \nmid b_i$. Τότε η $a_i x \equiv b_i \bmod n_i$ από την πρόταση ΔΕΝ έχει λύσεις στο $\mathbb{Z}$. Άρα το (Σ) δεν έχει λύσεις στο $\mathbb{Z}$.

Πρόταση 2. Για κάθε i, n ισοτιμίες $a_i x \equiv b_i \bmod n$, έχει λύση στο $\mathbb{Z}$. Τότε υπολογίζουμε e_i, m_i όπως προηγουμένως, και από το (ε) είναι ισοδύναμο με το σύστημα

$$(\varepsilon') \begin{cases} x \equiv e_1 \bmod m_1 \\ x \equiv e_2 \bmod m_2 \\ x \equiv e_r \bmod m_r \end{cases}$$

Κινέζικο Θεώρημα: Υποθέτουμε ότι στο (ε') ισχύει $\text{ΜΚΔ}(m_i, m_j) = 1$ για κάθε $i \neq j$.

Θέτουμε $M = m_1 m_2 \dots m_r$, $M_i = \frac{M}{m_i}$. Υπολογίζουμε $t_i \in \mathbb{Z}$ με $t_i M_i \equiv 1 \bmod m_i$, λύνοντας την ισοτιμία $M_i x \equiv 1 \bmod m_i$. Το σύνολο λύσεων του (ε') είναι το εξής:

$$S = \left\{ \sum_{i=1}^{r} (t_i e_i M_i) + t M \mid t \in \mathbb{Z} \right\}$$

(Αφού $S \neq \emptyset$, λοιπόν S άπειρο σύνολο) Επιπλέον S κλάσεις υπολοίπων modulo $m_1, m_2 \dots m_r$. Αφού σε κάθε σύνολο M διαδοχικών ακεραίων, υπάρχει ακριβώς μία λύση του ε'.

Παράδειγμα

Να βρείτε τον μικρότερο φυσικό, μεγαλύτερο του 4000 που είναι λύση του συστήματος (Σ) $\begin{cases} x \equiv -3 \bmod 11 \\ -2x \equiv 4 \bmod 23 \\ 6x \equiv 15 \bmod 45. \end{cases}$

Λύση $-2x \equiv 4 \bmod 23$ είναι ισοδύναμη (γιατί $ΜΚΔ(11, 23) = 1$).

$11(-2)x \equiv 11 \cdot 7 \bmod 23 \Leftrightarrow -22x \equiv 77 \bmod 23 \Leftrightarrow x \equiv 8 \bmod 23$

γιατί $[-22]_{23} = [1]_{23}$ και $77 = 3 \cdot 23 + 8$ (Επίσης $ΜΚΔ(-2, 23) = 1$)

$6x \equiv 15 \bmod 45$. Θέτουμε $d = ΜΚΔ(6, 45) = 3$. Έχουμε $3 | 15$.

Συνεπώς η (*) είναι ισοδύναμη με την $\frac{6}{d} x \equiv \frac{15}{d} \bmod \frac{45}{d}$

δηλ. την $2x \equiv 5 \bmod 15$ (**)

Αφού $([2]_{15})^{-1} = [8]_{15}$.

Η (**) είναι ισοδύναμη με $8 \cdot 2x \equiv 8 \cdot 5 \bmod 15$, δηλαδή με την

$x \equiv 40 \bmod 15$, δηλ. $x \equiv 10 \bmod 15$.

Συνεπώς το (2) είναι ισοδύναμο με το (Σ')

$$(\Sigma') \begin{cases} x \equiv -3 \bmod 11 \\ x \equiv 8 \bmod 23 \\ x \equiv 10 \bmod 15 \end{cases}$$

Έχουμε $m_1 = 11$, $m_2 = 23$, $m_3 = 15$. Ισχύει $ΜΚΔ(m_1, m_2) = 1$

$ΜΚΔ(m_1, m_3) = 1$, $ΜΚΔ(m_2, m_3) = 1$.

Συνεπώς το Κινέζικο Θεώρημα Υπολοίπων εφαρμόζεται στο (Σ').

Έτσι έχουμε $e_1 = -3$, $e_2 = 8$, $e_3 = 10$,

$M = m_1 m_2 m_3 = 11 \cdot 23 \cdot 15 = 3795$ $\quad M_1 = \frac{M}{m_1} = 23 \cdot 15 = 345$

$M_2 = \frac{M}{m_2} = m_1 m_3 = 11 \cdot 15 = 165$ $\quad M_3 = \frac{M}{m_3} = 11 \cdot 23 = 253$

i) Έτσι θα βρούμε

$M_1 x \equiv 1 \bmod 11 \Leftrightarrow 345x \equiv 1 \bmod 11$

ΦΥΛΛΑΔΙΟ 8 - ΑΣΚΗΣΗ 2

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

Παρατήρηση: Έστω $n \geq 2$ ακέραιος, με πρωτογενή ανάλυση $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ με p_i πρώτους, $p_i \neq p_j$ για $i \neq j$ και $\alpha_i > 0$. Τότε ο n διαιρείται από τετράγωνο ακέραιου αριθμού > 1 αν και μόνο αν υπάρχει i με $\alpha_i \geq 2$.

~~2~~, ~~3~~, ~~4~~, ~~5~~, ~~6~~, ~~7~~, ~~8~~, ~~9~~, ~~10~~, ~~11~~, ~~12~~, ~~13~~, ~~14~~, ~~15~~, ~~16~~

Απόδειξη (Για $k = 5$, η γενική περίπτωση το ίδιο επιχείρημα)

Έστω p_1, p_2, p_3, p_4, p_5 5 διακριτοί πρώτοι

Αν με $m \in \mathbb{Z}$, $m \equiv 0 \bmod p_i^2 \Leftrightarrow p_i^2 \mid m$

Θεωρούμε το σύστημα

$$(\Sigma) \begin{cases} x \equiv 0 \bmod p_1^2 \Leftrightarrow p_1^2 \mid x \\ x \equiv -1 \bmod p_2^2 \Leftrightarrow p_2^2 \mid x+1 \\ x \equiv -2 \bmod p_3^2 \Leftrightarrow p_3^2 \mid x+2 \\ x \equiv -3 \bmod p_4^2 \Leftrightarrow p_4^2 \mid x+3 \\ x \equiv -4 \bmod p_5^2 \Leftrightarrow p_5^2 \mid x+4 \end{cases}$$

Άρα αν το συστημα (*) έχει ακεραια λυση $x \in \mathbb{Z}$, οι 5 διαδοχικοι ακεραιοι $x, x+1, x+2, x+3, x+4$ έχουν την ιδιοτητα που θελουμε. Έχει το (*) λυση; Έχουμε $m_1 = p_1^2$, $m_2 = p_2^2$, $m_3 = p_3^2$, $m_4 = p_4^2$, $m_5 = p_5^2$. Αφου p_1, p_5 διαδοχικοι ανα δυο πρωτοι για $i \neq j$ $\text{ΜΚΔ}(p_i^2, p_j^2) = 1$. Συνεπως για $i \neq j$ $\text{ΜΚΔ}(m_i, m_j) = 1$. Επομενως, το Κιν. Θεωρημα υπολοιπων, μας δινει ότι υπαρχει $x \in \mathbb{Z}$ λυση του (*).

Β' Τροπος: (Επιλυση Διοφ. Γραμ. Εξισωσεων)

Παραδειγμα 1:
$$(*) \begin{cases} x \equiv 3 \bmod 15 \\ x \equiv 2 \bmod 10 \end{cases}$$

Το Κινεζικο Θεωρημα υπολοιπων ΔΕΝ εφαρμοζεται γιατι $m_1 = 15$, $m_2 = 10$ $\Rightarrow \text{ΜΚΔ}(10, 15) = 5 \neq 1$.

Έστω $x \in \mathbb{Z}$ λυση του (*). Τοτε $x \equiv 2 \bmod 10 \Rightarrow 10 \mid x-2 \Rightarrow$ υπαρχει $t \in \mathbb{Z}$ με $x = 2 + 10t$.

Επομενως, η εξισωση $x \equiv 3 \bmod 15 \Leftrightarrow (2+10t) \equiv 3 \bmod 15$.

$\Rightarrow 10t \equiv 1 \bmod 15$ ← Αδυνατη ισοτιμια γιατι $\text{ΜΚΔ}(10, 15) = 5 \nmid 1$.

Άρα το (*) δεν εχει λυση στο $\mathbb{Z}$.

Παραδειγμα 2
$$(*) \begin{cases} x \equiv 7 \bmod 15 \\ x \equiv 2 \bmod 10 \end{cases}$$

Το Κινεζικο Θεωρημα υπολοιπων ΔΕΝ εφαρμοζεται γιατι $\text{ΜΚΔ}(10, 15) = 5 \neq 1$.

Έστω $x \in \mathbb{Z}$ λυση του (*). Τοτε $x \equiv 2 \bmod 10 \Rightarrow 10 \mid x-2 \Rightarrow$ υπαρχει $t \in \mathbb{Z}$ με $x = 2 + 10t$.

Η πρωτη εξισωση $x \equiv 7 \bmod 15$ γινεται $2 + 10t \equiv 7 \bmod 15$, δηλ. $10t \equiv 5 \bmod 15$ (A)

Θεωρουμε $d = \text{ΜΚΔ}(10, 15) = 5$. Έχουμε $d \mid 5$. Συνεπως η (A) ειναι ισοδυναμη με την $\frac{10}{d} t \equiv \frac{5}{d} \bmod \frac{15}{d}$, δηλ. την $2t \equiv 1 \bmod 3$

που είναι ισοδύναμη (που έχουν ίδιο υπόλοιπο με το 2) με την $t \equiv 2 \bmod 3$

Άρα, υπάρχει $s \in \mathbb{Z}$ με $t = 2 + 3s$

Άρα $x = 2 + 10t \Rightarrow x = 2 + 10(2 + 3s) = 22 + 30s$

Άρα το σύνολο λύσεων του (2) είναι

$$S = \{22 + 30s \ : s \in \mathbb{Z}\}$$