Επαλήθευση

$-5-8\cdot 12t \bmod 8 \equiv 3$ ✓

$-5-8\cdot 12t \bmod 12 \equiv 7$ ✓

13/12/2016

Κινέζικο Θεώρημα

Έστω ότι οι φυσικοί $m_1, \dots, m_k$ είναι πρώτοι ανά δύο $(m_i, m_j)=1$

Τότε το σύστημα

$$\left.\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_k \bmod m_k \end{aligned}\right\} \text{ έχει μοναδική λύση } \bmod [m_1, \dots, m_k]$$

$\bmod m_1 \dots m_k$

Ερώτημα: Αν (m_i, m_j) δεν είναι όλα 1

Θεώρημα (χωρίς απόδειξη)

Δίνεται το σύστημα $x \equiv a_1 \bmod m_1$

$\vdots$

$x \equiv a_k \bmod m_k$

Το σύστημα έχει μοναδική λύση $\bmod [m_1, \dots, m_k]$ αννν $(m_i, m_j) \mid a_i - a_j$ για όλα τα i και j

(Ο αλγόριθμος είναι πολύπλοκος)

Π.χ. $x \equiv 3 \bmod 8$

$x \equiv 7 \bmod 12$

Λύση

$(8,12)=4 \mid 3-7=-4$

υπάρχει λύση

$x \equiv 3 \bmod 8 \iff x = 3 + 8k$ (+)

$3 + 8k \equiv 7 \bmod 12 \Rightarrow 8k \equiv 4 \bmod 12$

$2k \equiv 1 \bmod 3 \Rightarrow 2 \cdot 2k \equiv 2 \cdot 1 \bmod 3$

$(2,3) = 1 \Rightarrow [2]^{-1} = [2]$

$k \equiv 2 \bmod 3 \iff k = 2 + 3l$ (++)

(+) και (++) $\Rightarrow x = 3 + 8k = 3 + 8(2 + 3l) = 3 + 16 + 24l$

$x \equiv 19 \bmod 24$

<u>π.χ.</u>

$x \equiv 11 \bmod 21$

$x \equiv 4 \bmod 10$

$x \equiv 2 \bmod 12$

<u>Λύση</u>

$$\left.\begin{array}{l} (21,10) = 1 \mid 11-4 \\ (21,12) = 3 \mid 11-2 = 9 \\ (10,12) = 2 \mid 4-2 = 2 \end{array}\right\} \Rightarrow$$ άρα, έχει λύση

$(21,10) = 1$

$c_1 \frac{21 \cdot 10}{21} \equiv 1 \bmod 21 \iff c_1 \cdot 10 \equiv 1 \bmod 21$

$21 = 2 \cdot 10 + 1$

$2 \cdot 10 \equiv -1 \bmod 21$

$(-2) \cdot 10 \equiv 1 \bmod 21$

$19 \cdot 10 \equiv 1 \bmod 21$

$c_2 \frac{21 \cdot 10}{10} \equiv 1 \bmod 10 \Rightarrow c_2 21 \equiv 1 \bmod 10 \Rightarrow c_2 = 1$

$x_0 \equiv (11 \cdot 19 \cdot 10 + 4 \cdot 1 \cdot 21) \bmod 210 \equiv 2090 + 84 = 2174 \bmod 210 \equiv 74 \bmod 210$

$x \equiv 74 \bmod 210 \Rightarrow x = 74 + 210k$ (+)

$x \equiv 2 \bmod 12 \Rightarrow 74 + 210k = 2 \bmod 12$

$\cancel{72} + 10k \equiv 0 \bmod 12$

$6k \equiv 0 \bmod 12 \Rightarrow 6k = 12s \Rightarrow k = 2s$ (++)

$x = 74 + 210(2s) = 74 + 420s$

$x \equiv a_1 \bmod m_1$ $\vdots$ $x \equiv a_k \bmod m_k$	$b_1 x \equiv a_1 \bmod m_1$ $\vdots$ $b_k \cdot x \equiv a_k \bmod m_k$	$(b_i, m_i) = 1 \Rightarrow \exists\, b_i^{-1} \bmod m_i$ $x \equiv a_1' \bmod m_1$ $\vdots$ $x \equiv a_k' \bmod m_k$

<u>π.χ.</u> Να λυθεί το σύστημα

$x \equiv 2 \bmod 6$

$2x \equiv 8 \bmod 20$

<u>Λύση</u>

$2x \equiv 8 \bmod 20 \Rightarrow x \equiv 4 \bmod 10$

$(2, 20) = 2$

Λύσεις 4, $4 + \frac{20}{2} = 14 \bmod 20$

Έχουμε δύο συστήματα

$x \equiv 2 \bmod 6$

$x \equiv 4 \bmod 20$

και

$x \equiv 2 \bmod 6$

$x \equiv 14 \bmod 20$

$x \equiv 2 \bmod 6$
$x \equiv 4 \bmod 20$
$x = 4 + 20k$

$4 + 20k \equiv 2 \bmod 6$
$2k \equiv -2 \bmod 6$
$2k \equiv 4 \bmod 6$
$k \equiv 2 \bmod 3$
$k = 2 + 3l.$