

ΚΙΝΗΤΙΚΟ ΘΕΩΡΗΜΑ:

Έστω m_1, m_2, \dots, m_r ανά δύο πρώτοι και γυνοί αριθμοί

Έστω $m = m_1 \cdot m_2 \cdot \dots \cdot m_r$. Αν a_1, a_2, \dots, a_r είναι αυθαίρετοι

τότε υπάρχει αυθαίρετος x που αντίζει στην υπόθεση

$$(a_1 \beta_1 \frac{m}{m_1} + a_2 \beta_2 \frac{m}{m_2} + \dots + a_r \beta_r \frac{m}{m_r}) \pmod{m} \text{ θα είναι λύση του συστήματος:}$$

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

όπου $\beta_1, \beta_2, \dots, \beta_r$ οι αντίστοιχοι αντίστροφτοι των αντίστοιχων υπόθετων των $\frac{m}{m_1} \pmod{m_1}, \frac{m}{m_2} \pmod{m_2}, \dots, \frac{m}{m_r} \pmod{m_r}$

ΠΑΡΑΔΕΙΓΜΑ:

Να εντοχθεί το σύστημα:

$$x \equiv 4 \pmod{7}$$

$$x \equiv 9 \pmod{11}$$

$$x \equiv 4 \pmod{13}$$

Λύση

Παρατηρούμε ότι $(7, 11) = (11, 13) = (7, 13) = 1$

Άρα, μπορεί να εφαρμοσθεί το κινητικό θεώρημα.

$$m = [7, 11, 13] = 7 \cdot 11 \cdot 13 = 7(10+1)(10+3) = 7(100+30+10+3) = 7 \cdot 143 = 1001$$

Θα υπολογίσουμε τα $\beta_1, \beta_2, \beta_3$ ενός και στο θεώρημα.

$$\bullet \frac{m}{m_1} \beta_1 = \frac{7 \cdot 11 \cdot 13}{7} \beta_1 = 143 \cdot \beta_1 \equiv 1 \pmod{7} \Rightarrow 3 \cdot \beta_1 \equiv 1 \pmod{7} \Rightarrow \beta_1 = 5$$

$$\bullet \frac{m}{m_2} \beta_2 = \frac{7 \cdot 11 \cdot 13}{11} \beta_2 = 91 \cdot \beta_2 \equiv 1 \pmod{11} \Rightarrow 3 \beta_2 \equiv 1 \pmod{11} \Rightarrow \beta_2 = 4$$

$$\bullet \frac{m}{m_3} \beta_3 = \frac{7 \cdot 11 \cdot 13}{13} \beta_3 = 77 \cdot \beta_3 \equiv 1 \pmod{13} \Rightarrow 12 \beta_3 \equiv 1 \pmod{13} \quad (1)$$

$$(12, 13) = 1 \rightsquigarrow 13 = 1 \cdot 12 + 1 \Rightarrow 1 = 13 - 12 \Rightarrow [1]_{13} = [12]_{13} \cdot [-1]_{13} \Rightarrow$$

$$\Rightarrow [1]_{13} = [12]_{13} \cdot [12]_{13} \text{ Άρα, } ([12]_{13})^{-1} = [12]_{13}$$

Και άρα, (1) είναι:

$$\beta_3 \equiv 12 \pmod{13} \Rightarrow \beta_3 = 12 \text{ . Έτσι, σύμφωνα με το θεώρημα:}$$

$$x_0 \equiv (143 \cdot 5 \cdot 4 + 91 \cdot 4 \cdot 9 + 77 \cdot 12 \cdot 4) \pmod{1001} \equiv (2860 + 3276 + 3696) \pmod{1001} \equiv 9832 \pmod{1001} \equiv 67 \pmod{1001}$$