ΓΡΑΜΜΙΚΕΣ ΙΣΟΤΙΜΙΕΣ

ΘΕΩΡΗΜΑ: Η εξίσωση $ax \equiv b \bmod n$ έχει λύση στους ακεραίους αν.κ.α. $(a,n) \mid b$. Τότε, οι λύσεις θα δίνονται από τα παρακάτω:

$$x_0,\ x_0 + \frac{n}{(a,n)},\ x_0 + \frac{2n}{(a,n)},\ \dots,\ x_0 + \frac{((a,n)-1)n}{(a,n)}$$

όπου x_0 μια λύση της εξίσωσης

ΠΑΡΑΔΕΙΓΜΑ:

Να λυθεί η εξίσωση

$540x \equiv 120 \bmod 420$

ΛΥΣΗ

$(540, 420) = (60 \cdot 9, 60 \cdot 7) = 60(9,7) = 60$.

Ή αν δεν μπορούμε να το διαπιστώσουμε με το "μάτι" εφαρμόζουμε τον ευκλείδειο αλγόριθμο

$540 = 1 \cdot 420 + 120 \iff 120 = 540 - 420$

$420 = 3 \cdot 120 + 60 \iff 60 = 420 - 3 \cdot 120$

$120 = 2 \cdot 60 + 0$

Έτσι, $60 = 420 - 3 \cdot 120 = 420 - 3 \cdot (540 - 420) =$

$= 420 + 3 \cdot 420 - 3 \cdot 540 = 4 \cdot 420 - 3 \cdot 540$

Πολλαπλασιάζοντας με το 2, παίρνουμε:

$120 = 8 \cdot 420 - 6 \cdot 540 \Rightarrow 120 \equiv (8 \cdot 420 - 6 \cdot 540) \bmod 420$

$\Rightarrow 120 \equiv -6 \cdot 540 \bmod 420 \Rightarrow x_0 = -6$ μια λύση της

Τουτέστιν, όλες οι λύσεις θα δίνονται από τους τύπους

$$\left(-6,\ -6 + \frac{420}{60},\ -6 + \frac{2 \cdot 420}{60},\ \dots,\ -6 + \frac{59 \cdot 420}{60}\right) =$$

$$= (-6,\ -6 + 7,\ -6 + 14,\ \dots,\ -6 + 7 \cdot 59) =$$

$$= (-6,\ 1,\ 8,\ \dots,\ -6 + 7 \cdot 59).$$

ΘΕΩΡΗΜΑ: Εαν $(a,n)=1$ τοτε η εξίσωση $ax \equiv b \bmod n$ έχει λύση στο $\mathbb{Z}$ την: $x \equiv b \cdot a^{\varphi(n)-1} \bmod n$.

ΠΑΡΑΔΕΙΓΜΑ:

Να λυθεί η εξίσωση:

$7x \equiv 3 \bmod 10$

ΛΥΣΗ

Παρατηρούμε ότι $(10,7)=1 \mid 3$

Άρα, επιδέχεται λύση και μάλιστα μοναδική τη λύση:

$$x \equiv 3 \cdot 7^{\varphi(10)-1} \bmod 10 \quad (1)$$

$$\varphi(10) = \varphi(5 \cdot 2) = \varphi(5) \cdot \varphi(2) = 5-1 = 4.$$

Άρα, (1) είναι:

$$x \equiv 3 \cdot 7^{4-1} \bmod 10 \equiv 3 \cdot 7^3 \bmod 10 \quad (2)$$

όπου $7^2 = 49 \equiv 9 \bmod 10$

Άρα, η (2) γίνεται:

$$x \equiv 3 \cdot 7 \cdot 9 \bmod 10 \equiv 1 \cdot 9 \bmod 10 \equiv 9 \cdot \bmod 10.$$