Να επιλυθεί η εξίσωση

$$x^2 \equiv 410 \bmod 847$$

ΛΥΣΗ

Έχουμε, ότι:

$$847 = 11^2 \cdot 7$$

Επομένως,

$$x^2 \equiv 410 \bmod 847 \iff \begin{cases} x^2 \equiv 410 \bmod 7 & (1) \\ x^2 \equiv 410 \bmod 11^2 & (2) \end{cases}$$

(1): $x^2 \equiv 410 \bmod 7 \equiv (50 \cdot 7 + 60) \bmod 7 \equiv$

$\equiv 60 \bmod 7 \equiv 4 \bmod 7.$

(Το 4 ΤΥ $\iff 4^{\frac{7-1}{2}} = 4^3 = 1 \bmod 7$ έχει λύση)

Εφόσον, $7 = 4 \cdot 1 + 3$ και 4 ΤΥ $\Rightarrow$

$\Rightarrow 4^{1+1} = 4^2 \equiv 16 \bmod 7 \equiv 2 \bmod 7$ λύση της εξίσωσης $x^2 \equiv 410 \bmod 7$

Άρα, μια ακόμα λύση της ίδιας εξίσωσης είναι η $x \equiv -2 \bmod 7 \equiv 5 \bmod 7$

(2): Επιλύουμε, πρώτα την $x^2 \equiv 410 \bmod 11$ όπου έαν έχει 2 λύσεις τότε και η $x^2 \equiv 410 \bmod 11^2$ θα έχει 2 λύσεις.

Πιο απλά: $x^2 \equiv (30 \cdot 11 + 80) \bmod 11 \Rightarrow$

$\Rightarrow x^2 \equiv 80 \bmod 11 \Rightarrow x^2 \equiv 3 \bmod 11$

(Το 3 ΤΥ $\Leftrightarrow 3^{\frac{11-1}{2}} = 3^5 \equiv 81 \cdot 3 \bmod 11 \equiv 1 \bmod 11$)

Άρα, έχει λύση.

Εφόσον, $n = 4(2)+3$ και 3 ΤΥ $\Rightarrow$

$\Rightarrow 3^{2+1} = 3^3 \equiv 27 \bmod 11 \equiv 5 \bmod 11$ είναι λύση

της εξίσωσης $x^2 \equiv 410 \bmod 11$

Άρα, μια ακόμα λύση της ίδιας εξίσωσης

είναι η $x \equiv -5 \bmod 11 \equiv 6 \bmod 11$

(Βεβαίως η λύση $x \equiv 5 \bmod 11$ θα μπορούσε να

βρεθεί και μέσω παραγώντων)

Για την $x^2 \equiv 410 \bmod 11^2$ η διαδικασία είναι:

$(5 + k \cdot 11)^2 \equiv (5^2 + 11 \cdot 10k + 11^2 k^2) \bmod 11^2 \equiv 410 \bmod 11^2 \Rightarrow$

(όπου $410 \equiv 47 \bmod 11^2$)

$\Rightarrow (11 \cdot 10k + 11^2 k^2) \equiv 22 \bmod 11^2 \Rightarrow$

$\Rightarrow (10 \cdot k + \cancel{11 k^2}^{0}) \equiv 2 \bmod 11 \Rightarrow$

$\Rightarrow 10k \equiv 2 \bmod 11 \Rightarrow$

$\Rightarrow k \equiv 2 \cdot 10^{-1} \bmod 11 \quad (*)$

Από, Ευκλείδειο Αλγόριθμο:

$11 = 5 \cdot 2 + 1 \Rightarrow 1 = 11 - 5 \cdot 2 \Rightarrow 1 \equiv (-5) 2 \bmod 11 \Rightarrow$

$\Rightarrow 1 \equiv \boxed{6} 2 \bmod 11 \rightsquigarrow 10^{-1} \equiv 6 \bmod 11$

Άρα, $k \equiv 2 \cdot 6 \bmod 11 \equiv 12 \bmod 11 \equiv 1 \bmod 11$

Άρα, $x_1 \equiv (5 + 1 \cdot 11) \bmod 11^2 \equiv 17 \bmod 11^2$

ομοια, κανουμε για τη λύση $x \equiv 6 \bmod 11$

$(6 + \lambda 11)^2 \bmod 11^2 \equiv \ldots\ldots \quad \lambda \equiv \ldots\ldots \rightsquigarrow x_2 \equiv \ldots$