

Δευτέρα -14- Δεκεμβρίου 2015

ΠΑΡΑΔΕΙΓΜΑ 1 Δεν εφαρμόζεται το κινέζικο

$$\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 7 \pmod{14} \\ x \equiv 21 \pmod{35} \end{cases} \textcircled{A}$$

ΛΥΣΗ

$$\begin{aligned} x &\equiv 7 \pmod{14} & x &\equiv 21 \pmod{35} \\ x &\equiv 7 \pmod{2} & x &\equiv 21 \pmod{5} \\ x &\equiv 7 \pmod{7} & x &\equiv 21 \pmod{7} \end{aligned}$$

$$\textcircled{A} \Rightarrow x \equiv 5 \pmod{8}$$

$$x \equiv 7 \pmod{2} \equiv 1 \pmod{2} \text{ (λύσεις όπου οι περιττοι)}$$

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

$$x \equiv 21 \pmod{5} \text{ (Επίδω(5,7)=1)}$$

$$x \equiv 21 \pmod{7}$$

($\frac{7}{5}$) Αν έχω $x \equiv 7 \pmod{35}$ δεν θα μπορούσα να γράψω 66 ή 3·12

Κοινές λύσεις από $\textcircled{1}$ και $\textcircled{2} \Rightarrow x \equiv 7 \pmod{2} \equiv 1 \pmod{2}$ δεν χρειάζεται την καλήτητα ή $x \equiv 5 \pmod{8}$.

Άρα, $x \equiv 5 \pmod{8}$ το νέο σύστημα, όπου εφαρμόζεται το κινέζικο
 $x \equiv 21 \pmod{5}$ σύστημα
 $x \equiv 21 \pmod{7}$

ΠΑΡΑΔΕΙΓΜΑ 2

$$3x \equiv 9 \pmod{23}$$

$$15x \equiv 12 \pmod{18}$$

ΛΥΣΗ: Να βγουν οι συντελεστές $3x \equiv 9 \pmod{23}$, 23 πρώτος. Άρα, έχει μοναδική λύση. $8 \cdot 3x \equiv 8 \cdot 9 \pmod{23} \Rightarrow x \equiv 10 \pmod{23}$

$$\begin{cases} x \equiv 2 \pmod{12} \\ x \equiv 4 \pmod{20} \end{cases}$$

$$(12, 20) = 4 \mid 2 - 4 \text{ όχι}$$

$$x \equiv 2 \pmod{12} \Rightarrow x = 2 + 12k$$

$$x \equiv 4 \pmod{20} \text{ βρείτε κ.}$$

$$\text{Εξα λύση αν } (12, 20) = 2 \mid 2 \text{ όχι.}$$

$$\text{II X. } 2x \equiv 4 \pmod{12}$$

$$2x \equiv 8 \pmod{20} \rightarrow \text{λύσε καθεμία}$$

Έχει πολλές λύσεις. Κάθε λύση σου δίνει νέο σύστημα.

Πρέπει να λύσεις ταλακ 1. Αν λύνεται

$$15x \equiv 12 \pmod{18}$$

$$(15, 18) = 3 \mid 12 \text{ έχουμε}$$

Βρες μια $\frac{15}{3}x \equiv \frac{12}{3} \pmod{\frac{18}{3}}$
 $5x \equiv 4 \pmod{6}$

$$5 \cdot 5x \equiv 5 \cdot 4 \pmod{23} \Rightarrow x \equiv 20 \pmod{23} \Rightarrow x \equiv 2 \pmod{6}$$

Μια λύση $2, 2 + \frac{18}{3}, 2 + \frac{2 \cdot 18}{3} \pmod{18}$
 $2, 8, 14 \pmod{18}$

Το εὑρέτημα γίνεται

$$\begin{cases} x \equiv 10 \pmod{23} \\ x \equiv 2 \pmod{18} \end{cases}$$

$$\begin{cases} x \equiv 10 \pmod{23} \\ x \equiv 8 \pmod{23} \end{cases} \Rightarrow x \equiv 10 \pmod{23}$$

$$x \equiv 4 \pmod{18}$$

Αυτά έχουν λύση γιατί $(23, 18) = 1$ και λύνονται με το κινέζικο.

$$x \equiv (G_1 \cdot 8 \cdot 10 + G_2 \cdot 23 \cdot 2) \pmod{23 \cdot 18} \text{ (B)}$$

$$G_1 \cdot 18 \equiv 1 \pmod{23} \text{ και } G_2 \cdot 23 \equiv 1 \pmod{18}$$

Με των Ευκλείδη βρίσκω τα G_1 και G_2

Μετά αντικαθιστώ στον τύπο (B) και έχω μια λύση.

Τετραγωνικά Υπόλοιπα

Λύουμε την $ax \equiv b \pmod{n}$. Πρώτου βαθμού

Να λύσουμε την δεύτερο βαθμια. Στο $\mathbb{R}$: $ax^2 + bx + c = 0$, $a \neq 0$

$$a \left(x^2 + \frac{2b}{2a}x + \frac{c}{a} \right) = 0$$

$$a \left(x^2 + \frac{2b}{2a}x + \left(\frac{b}{2a} \right)^2 - \left(\frac{b}{2a} \right)^2 + \frac{c}{a} \right) = 0$$

$$a \left[\left(x + \frac{b}{2a} \right)^2 - \frac{b^2 - 4ac}{4a^2} \right] = 0$$

Ονομάζουμε:

$$x + \frac{b}{2a} = x'. \text{ Άρα έχουμε } a(x')^2 = \frac{b^2 - 4ac}{4a}, \text{ έχει λύση στο } \mathbb{R}$$

$$\text{Αν } b^2 - 4ac \geq 0$$

Άρα η αρχική μετασχηματίζεται στην $a(x')^2 = b$

$$\text{Να δοθεί } n \quad ax^2 \equiv b \pmod{n}$$

ή $x^2 \equiv b \pmod{n}$ Ποτε δύναται αυτή;

$$x^2 \equiv b \pmod{n}$$

Π.χ | $\mathbb{Z}'_3 = \{0, 1, 2\}$ τετράγωνα $\{0, 1\} =$ Τετραγωνικά Υπόλοιπα.

Το 2 δεν έχει λύση $x^2 \equiv 2 \pmod{3}$

$\mathbb{Z}'_5 = \{0, 1, 2, 3, 4\}$ τετράγωνα $\{0, 1, 4\} =$ Τετραγωνικά Υπόλοιπα

$x^2 \equiv 2 \pmod{5}$ και $x^2 \equiv 3 \pmod{5}$ δεν έχει λύση

$\mathbb{Z}'_7 = \{0, 1, 2, 3, 4, 5, 6\}$ τετράγωνα $\{0, 1, 4, 2\} =$ Τετραγωνικά Υπόλοιπα

Δεν έχουμε λύσεις οι $x^2 \equiv 3 \pmod{7}$, $x^2 \equiv 5 \pmod{7}$, $x^2 \equiv 6 \pmod{7}$

Ορισμός: Αν n είναι συνάρτηση βαθμού $x^2 \equiv b \pmod{n}$ έχει λύση, τότε ο b καλείται τετραγωνικό υπόλοιπο (Τ.Υ.). Αν δεν έχει λύση, καλείται τετραγωνικό μη-υπόλοιπο (Τ.Μ.Υ.).

Π.Χ $1 \pmod{7}, 2 \pmod{7}, 4 \pmod{7}$ είναι Τ.Υ.
 $3 \pmod{7}, 5 \pmod{7}, 6 \pmod{7}$ είναι Τ.Μ.Υ.

Αν x είναι λύση της $x^2 \equiv b \pmod{n}$ τότε και ο $n-x$ είναι επίσης λύση $(n-x) \pmod{n} \equiv -x \Rightarrow (-x)^2 = x^2 \equiv b \pmod{n}$

Αν υπάρχει μια λύση, τότε είναι δύο

Με το Θ. Wilson δείξαμε ότι $x^2 \equiv -1 \pmod{p} \Leftrightarrow p = 4k+1$

Θεώρημα: Κριτήριο του Euler.

Εστω $a \in \mathbb{Z}$ και p πρώτος με $(a, p) = 1$

Τότε α) ο a είναι Τ.Υ. $\pmod{p}$ αν $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

β) ο a είναι Τ.Μ.Υ. $\pmod{p}$ αν $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Αναρτά στο ερώτημα: Λύνεται $x^2 \equiv a \pmod{p}$;

Π.Χ Εξετάστε αν λύνεται $x^2 \equiv 5 \pmod{19}$

Λύνεται $\Leftrightarrow 5^{\frac{19-1}{2}} \equiv 1 \pmod{19}$

$\frac{19-1}{2} = 9$. Βρίσκει $5^9 \pmod{19}$

$5^2 \pmod{19} = 6 \pmod{19} \mid 5^4 \equiv 36 \pmod{19} \equiv -2 \pmod{19} \mid 5^8 \equiv (-2)^2 \pmod{19} = 4 \pmod{19}$

$5^3 \pmod{19} = 11 \pmod{19} \mid 5^9 \equiv 5 \cdot 4 \pmod{19} \equiv 1 \pmod{19}$, Άρα έχει λύση.

Έχει λύση πως θα την βρούμε;

Το $\pmod{19}$ έχει ηρωταρχική ρίζα. Άρα υπάρχει c

με $\text{ord}_{19}(c) = 19-1 = \phi(19)$

Αρα κάθε ~~αριθμός~~ κλάση $\text{mod } 19$ δίνεται από
δυναμική του c
$$S \equiv c^k \text{ mod } 19 \quad \text{και} \quad 1 \leq k \leq 18$$

Το x το οποίο θα είναι λύση της $x^2 \equiv S \text{ mod } 19$ θα είναι :

$$x \equiv c^m \text{ mod } 19$$

Τώρα έχουμε να βρούμε το m γνωρίζοντας το k ώστε

$$x^2 \equiv S \text{ mod } 19 \Leftrightarrow c^{2m} \equiv c^k \text{ mod } 19$$