13/1/2016 Θ.Α

Θεωρούμε ένα σύστημα γραμμικών ισοτιμιών

$$(\Sigma)\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \vdots \\ a_n x \equiv b_n \pmod{m_n} \end{cases}$$

Για να έχει λύση το (Σ) θα πρέπει κάθε γραμμική ισοτιμία:

$a_k x \equiv b_k \pmod{m_k}$, $1 \le k \le n$

να έχει λύση, δηλαδή

$\forall k=1,\dots,n: d_k := (a_k, m_k) \mid b_k$ (*)

Υποθέσαμε ότι η σχέση (*) ισχύει $\forall k=1,\dots,n$

Τότε: $b_k = d_k b'_k$, $a_k = d_k \cdot a'_k$, $m_k = d_k \cdot m'_k$, $\forall k=1,\dots,n$. Τότε η γραμμική ισοτιμία $a_k x \equiv b_k \pmod{m_k}$ είναι ισοδύναμη με την $a'_k x \equiv b'_k \pmod{m'_k}$ $\forall k=1,\dots,n$, όπου $(a'_k, m'_k)=1$, $\forall k=1,\dots,n$. Οι γραμμικές ισοτιμίες $a'_k x \equiv b'_k \pmod{m'_k}$ έχουν μοναδική λύση την $x \equiv c_k \pmod{m'_k}$, $\forall k=1,\dots,n$

Τότε το (Σ) είναι ισοδύναμο με το σύστημα γραμμικών ισοτιμιών:

$$(\Sigma')\begin{cases} x \equiv c_1 \pmod{m'_1} \\ x \equiv c_2 \pmod{m'_2} \\ \vdots \\ x \equiv c_n \pmod{m'_n} \end{cases}$$

Αν $d_{ij} = (m'_i, m'_j) \mid c_i - c_j$, $\forall i,j=1,\dots,n$, με $i \neq j$, τότε το (Σ') άρα και το (Σ) έχει μοναδική λύση $\pmod{[m'_1, m'_2, \dots m'_n]}$

ΠΑΡΑΔΕΙΓΜΑ

Θεωρούμε το ακόλουθο σύστημα γραμμικών ισοτιμιών:

$$(\Sigma)\begin{cases} 5x \equiv 6 \pmod 8 \\ 8x \equiv 10 \pmod{14} \\ 10x \equiv 5 \pmod{15} \end{cases}$$

$a_1=5$, $b_1=6$, $m_1=8$, $d_1=(a_1,m_1)=(5,8)=1 \mid 6=b_1$

$a_2=8$, $b_2=10$, $m_2=14$, $d_2=(a_2,m_2)=(8,14)=2 \mid 10=b_2$

$a_3=10$, $b_3=5$, $m_3=15$, $d_3=(a_3,m_3)=(10,15)=5 \mid 5=b_3$

- Η μοναδική λύση της: $5x \equiv 6 \pmod 8$ είναι η: $x \equiv 6 \pmod 8$
- Η ισοτιμία $8x \equiv 10 \pmod{14}$ είναι ισοδύναμη με την: $4x \equiv 5 \pmod 7$ της οποίας η μοναδική λύση είναι η $x \equiv 3 \pmod 7$

-Η ισοδ/ια $10x \equiv 5 \pmod{15}$ είναι ισοδύναμη με την: $2x \equiv 1 \pmod 3$ της οποίας η μοναδική λύση είναι η $x \equiv 2 \pmod 3$

Το (Σ) είναι ισοδύναμο με το σύστημα

$$(\Sigma')\begin{cases} x \equiv 6 \pmod 8 \\ x \equiv 3 \pmod 7 \\ x \equiv 2 \pmod 3 \end{cases}$$

Επειδή $(8,7)=(8,3)=(7,3)=1$ μπορούμε να εφαρμόσουμε το Κινέζικο Θεώρημα υπολοίπων και άρα το (Σ') έχει μοναδική λύση $\pmod{(3\cdot 7\cdot 8)} = \pmod{168}$

$M = 3\cdot 7\cdot 8 = 168$

$M_1 = \frac{M}{m_1} = \frac{3\cdot 7\cdot 8}{8} = 21$

$M_2 = \frac{M}{m_2} = \frac{3\cdot 7\cdot 8}{7} = 24$

$M_3 = \frac{M}{m_3} = \frac{3\cdot 7\cdot 8}{3} = 56$

Θεωρούμε τις γραμμικές ισοτιμίες $M_i X \equiv 1 \pmod{m_i}$, $1 \le i \le 3$

$21X \equiv 1 \pmod 8$
$24X \equiv 1 \pmod 7$
$56X \equiv 1 \pmod 3$

$\Rightarrow$
$5X \equiv 1 \pmod 8 \rightarrow$ μοναδική λύση $c_1 \equiv 5 \pmod 8$
$3X \equiv 1 \pmod 7 \rightarrow$ μοναδική λύση $c_2 \equiv 5 \pmod 7$
$2X \equiv 1 \pmod 3 \rightarrow$ μοναδική λύση $c_3 \equiv 2 \pmod 3$

Η μοναδική λύση $\pmod{168}$ του (Σ') είναι: $21\cdot 5\cdot 6 + 24\cdot 5\cdot 3 + 56\cdot 2\cdot 2 =$
$= 1214 \pmod{168} = 38 \pmod{168}$

ΑΣΚΗΣΗ: $(\Sigma)\begin{cases} 2x \equiv 4 \pmod 8 \\ 3x \equiv 12 \pmod 9 \\ x \equiv 34 \pmod{12} \end{cases}$

$d_1 = (2,8) = 2 \mid 4$ (V) άρα έχει λύση
$d_2 = (3,9) = 3 \mid 12$ (V) άρα έχει λύση
$d_3 = (1,12) = 1 \mid 34$ (V) άρα έχει λύση

$\Rightarrow$

$\Rightarrow$ Το (Σ) είναι ισοδύναμο με το σύστημα:

$$(\Sigma')\begin{cases} x \equiv 2 \pmod 4 \\ x \equiv 4 \pmod 3 \\ x \equiv 10 \pmod{12} \end{cases}$$

$d_{12} = (4,3) = 1 \mid 2-4 = -2$ (V)
$d_{13} = (4,12) = 4 \mid 2-10 = -8$ (V)
$d_{23} = (3,12) = 3 \mid 4-10 = -6$ (V)

Μια λύση των δύο πρώτων ισοτιμιών είναι η $x \equiv 10 (mod 12)$ η οποία συμπίπτει με την τρίτη ισοτιμία. Άρα η $x \equiv 10 (mod 12)$ είναι η μοναδική λύση $(mod 12)$ του $(Σ')$ άρα και του $(Σ)$.

ΑΣΚΗΣΗ: Κάποιος σκέφτεται έναν κρυφό αριθμό x_0, όπου $1 \le x_0 \le 100$ και κάνει γνωστά τα υπόλοιπα των διαιρέσεων του x_0 με τους 3, 5, 7 και ζητάει να βρεθεί ο αριθμός x_0.

Έστω a_1: υπόλοιπο της διαίρεσης του x_0 με το $3 \Rightarrow x_0 \equiv a_1 (mod 3)$
" a_2 " " " " x_0 " $5 \Rightarrow x_0 \equiv a_2 (mod 5)$
" a_3 " " " " x_0 " $7 \Rightarrow x_0 \equiv a_3 (mod 7)$
$\Bigg\}$ $(Σ)$

Άρα ο x_0 είναι λύση του $(Σ)$, για το οποίο ικανοποιούνται οι προϋποθέσεις του ΚΘΥ.

Άρα ο x_0 είναι η μοναδική λύση $(mod 105)$ του $(Σ)$.

$M = 3 \cdot 5 \cdot 7 = 105$

$M_1 = \frac{3 \cdot 5 \cdot 7}{3} = 35$, $\quad 35x \equiv 1 (mod 3) \rightarrow$ μοναδ. λύση $b_1 = 2 (mod 3)$

$M_2 = \frac{3 \cdot 5 \cdot 7}{5} = 21$, $\quad 21x \equiv 1 (mod 5) \rightarrow$ " $b_2 = 1 (mod 5)$

$M_3 = \frac{3 \cdot 5 \cdot 7}{7} = 15$, $\quad 15x \equiv 1 (mod 7)$ " $b_3 = 1 (mod 7)$

Τότε $x_0 = M_1 b_1 a_1 + M_2 b_2 a_2 + M_3 b_3 a_3 =$

$= 35(-1) a_1 + 21 \cdot a_2 \cdot 1 + 15 \cdot 1 \cdot a_3 =$

$= -35 a_1 + 21 a_2 + 15 a_3$

Άρα η μοναδική λύση του $(Σ) (mod 105)$ είναι η $x_0 = -35a_1 + 21a_2 + 15a_3$
$1 \le x_0 \le 100$.

Π.χ. $a_1 = 1, a_2 = 3, a_3 = 3$. Τότε
$x_0 = -35 \cdot 1 + 21 \cdot 3 + 15 \cdot 3 = -35 + 63 + 45 = 73.$

ΤΑΞΕΙΣ ΣΤΟΙΧΕΙΩΝ mod n

Έστω $a \in \mathbb{Z}$ και $n \in \mathbb{N}$, και έστω $(a,n)=1$. Τότε από το ΘΕΩΡΗΜΑ EULER ⇒

⇒ ~~$a^{\varphi(n)} \equiv 1 \pmod n$~~ $\boxed{a^{\varphi(n)} \equiv 1 \pmod n}$

ΠΡΟΒΛΗΜΑ: Εύρεση ο $\varphi(n)$ ο μικρότερος θετικός ακέραιος k: $a^k \equiv 1 \pmod n$;

Αν $a=2$ και $n=15$, τότε από το Θεώρημα Euler: $2^{\varphi(15)} \equiv 1 \pmod{15}$ ⇒

$2^{\varphi(3)\varphi(5)} = 2^{2\cdot 4} = 2^8 \equiv 1 \pmod{15}$

Ορισμός: Αν $a \in \mathbb{Z}$ και $n \in \mathbb{N}$, έστω ώστε: $(a,n)=1$, τότε ο μικρότερος θετικός ακέραιος k: $a^k \equiv 1 \pmod n$ καλείται τάξη του $a \pmod n$ και συμβολίζεται με: $ord_n(a)$

τάξη:
$ord_n(a) = \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod n\}$

$ord_{15}(2)=4$

ΠΡΟΤΑΣΗ: Έστω $a \in \mathbb{Z}$, $n \in \mathbb{N}$ και υποθέτουμε ότι $(a,n)=1$

Συμβολίζουμε: $r = ord_n(a)$

① $a^k \equiv a^\lambda \pmod n \Rightarrow k \equiv \lambda \pmod r$, δηλαδή: $r \mid k-\lambda$

② $a^k \equiv 1 \pmod n \Rightarrow r \mid k$

③ $a^m \not\equiv a^k \pmod n$, όταν $1 \le m \ne k \le r-1$

④ $b \equiv a \pmod n \Rightarrow (b,n)=1$ και $ord_n(a) = ord_n(b)$

όταν $b \in \mathbb{Z}$

Απόδειξη

① Έστω ότι $a^k \equiv a^\lambda \pmod n$ υποθέτουμε ότι $k \ge \lambda$. Τότε:

$n \mid a^k - a^\lambda \Rightarrow n \mid a^\lambda(a^{k-\lambda}-1)$ | ΛΗΜΜΑ ευκλείδου
$(a,n)=1 \Rightarrow (a^\lambda, n)=1$

Με χρήση της Ευκλείδειας Διαίρεσης του $k-\lambda$ με το r, έπεται ότι
$r \mid k-\lambda$ [ΑΣΚΗΣΗ]

(2) $a^k \equiv 1 \pmod n \Rightarrow a^k \equiv a^0 \pmod n \overset{(1)}{\Rightarrow} r \mid k$.

(3) Αν $a^m \equiv a^k \pmod n$, όπου $1 \le m \ne k \le r-1$. Τότε από το (1) $\Rightarrow$
$r \mid m-k \Rightarrow r \le m-k$: αυτό είναι άτοπο, διότι $1 \le m$, $k \le r-1$ και $m \ne k$.

(4) Έστω $b \equiv a \pmod n \Rightarrow (a,n) = (b,n)$. Άρα επειδή $(a,n)=1 \Rightarrow (b,n)=1 \Rightarrow$
ορίζεται η τάξη $\mathrm{ord}_n(b)$. Τότε: $b^k \equiv a^k \pmod n$, $\forall k \ge 1 \Rightarrow$
$\Rightarrow \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod n\} = \min\{k \in \mathbb{N} \mid b^k \equiv 1 \pmod n\} \Rightarrow \mathrm{ord}_n(a) = \mathrm{ord}_n(b)$

ΟΡΙΣΜΟΣ Έστω $a \in \mathbb{Z}_n^{\times} = \{\overline{a} \in \mathbb{Z}_n \mid n \in \mathbb{Z}, (a,n)=1\}$ και έστω ότι 0 α είναι πρωταρχική ρίζα $\pmod n \Leftrightarrow \boxed{\mathrm{ord}_n(a) = \varphi(n)}$