

ΦΥΛΛΑΔΟ #7

1) $x \equiv U_1 \pmod{3}$

$$x \equiv U_2 \pmod{5}$$

$$x \equiv U_3 \pmod{7}$$

$$x \equiv (-35U_1 + 21U_2 + 15U_3) \pmod{105}$$

Από κινεϊκό θεωρήμα $\exists$ μοναδική λύση

$$\text{και } M = [5, 3, 7] = 3 \cdot 5 \cdot 7 = 105$$

$$5 \cdot 7 C_1 \equiv 1 \pmod{3} \Rightarrow 2C_1 \equiv 1 \pmod{3}$$

$$3 \cdot 7 C_2 \equiv 1 \pmod{5} \Rightarrow C_2 \equiv 1 \pmod{5}$$

$$3 \cdot 5 C_3 \equiv 1 \pmod{7} \Rightarrow C_3 \equiv 1 \pmod{7}$$

Αρα

$$M \equiv (35 \cdot 2U_1 + 21 \cdot 1U_2 + 15 \cdot 1U_3) \pmod{105} \equiv$$

$$\equiv (70U_1 + 21U_2 + 15U_3) \pmod{105} \equiv$$

$$\equiv (-35U_1 + 21U_2 + 15U_3) \pmod{105}.$$

2) α) $7x \equiv 3 \pmod{19}$

$(7, 19) = 1 \leadsto$ μοναδική λύση που έχουμε

(1) $x \equiv 3 \cdot 7^{-1} \pmod{19}$ πρώτος ο αριθμός $7^{-1} \pmod{19}$

$$19 = 2 \cdot 7 + 5 \Rightarrow 7 = 1 \cdot 5 + 2 \Rightarrow 5 = 2 \cdot 2 + 1 \Rightarrow 1 = 5 - 2 \cdot 2 =$$

$$= 5 - 2(7 - 5) = 5 - 2 \cdot 7 + 2 \cdot 5 = 3 \cdot 5 - 2 \cdot 7 =$$

$$= 3(19 - 2 \cdot 7) - 2 \cdot 7 = 3 \cdot 19 - 8 \cdot 7 \Rightarrow [1]_{19} = [-8]_{19} \cdot [7]_{19}$$

Αρα $7^{-1} \equiv -8 \pmod{19} \equiv 11 \pmod{19}$

Αρα, (1) $\rightarrow x \equiv 3 \cdot 11 \pmod{19} \equiv 33 \pmod{19} \equiv 14 \pmod{19}$

β) $12x \equiv 16 \pmod{39}$, οπου $(12, 39) = (3 \cdot 4, 3 \cdot 13) = 3 \mid 16$
 Δεν υπάρχει λύση

γ) $69x \equiv 21 \pmod{99}$, οπου $(69, 99) = (3 \cdot 23, 3 \cdot 33) = 3 \mid 21$
 Δεν υπάρχει λύση (αλλά όχι μοναδική)

$$69x \equiv 21 \pmod{99} \Leftrightarrow 23x \equiv 7 \pmod{33} \quad \leftarrow \underline{\underline{\text{Πιο απλά!}}}$$

Για να βρούμε τον αντιστρόφιο του $23 \pmod{33}$

μέσω του Ευκλείδειου αλγορίθμου, βεβαίως είναι:

$$(23, 33) = 1 \rightsquigarrow 33 = 1 \cdot 23 + 10 \rightsquigarrow 23 = 2 \cdot 10 + 3 \rightsquigarrow 10 = 3 \cdot 3 + 1$$

$$\begin{aligned} 1 &= 10 - 3 \cdot 3 = 10 - 3(23 - 2 \cdot 10) = 7 \cdot 10 - 3 \cdot 23 = 7(33 - 23) - 3 \cdot 23 = \\ &= 7 \cdot 33 - 10 \cdot 23 \Rightarrow 1 = 7 \cdot 33 - 10 \cdot 23 \Rightarrow \end{aligned}$$

$$\Rightarrow [1]_{33} = [-10]_{33} \cdot [23]_{33} \quad \text{οπου} \quad 23 \pmod{33} \equiv -10$$

$$\text{Διαι, } \underline{([23]_{33})^{-1} = [-10]_{33}}.$$

$$\text{Συνεπώς, } x \equiv -10 \cdot 7 \pmod{33} \equiv -70 \pmod{33} \equiv 29 \pmod{33}$$

Διαι το σύνολο των λύσεων μας θα είναι το:

$$\left\{ 29, 29 + \frac{33}{1}, 29 + \frac{2 \cdot 33}{1} \right\} = \{ 29, 62, 95 \}$$

3) α.

Λύστε το παρακάτω σύστημα:

$$\begin{cases} x \equiv 10 \pmod{13} \\ x \equiv 16 \pmod{17} \end{cases}$$

ΛΥΣΗ

Πρώτον ελέγχουμε:

$$(17, 13) = 1 \mid (16 - 10) = 6$$

Άρα, πράγματι έχει λύση

$$\begin{aligned} x &\equiv 10 \pmod{13} \Rightarrow x = 10 + 13 \cdot k \Rightarrow 10 + 13k \equiv 16 \pmod{17} \Rightarrow \\ &\Rightarrow 13k \equiv 6 \pmod{17} (*) \end{aligned}$$

Σκοπός μας είναι να βρούμε ευείκο το k ώστε να ισχύει η σχέση (*).

Άρκει, να αναλύσουμε τον αριθμό 13 προς ατο k . Αυτό, θα γίνει μέσω της αντιστροφής κάποιου

$$13^{-1} \cdot 13k \equiv 6 \cdot 13^{-1} \pmod{17}. \text{ Ποιο είναι όμως το } 13^{-1} \pmod{17},$$

μέσω του Ευκλείδειου Αλγορίθμου, αφού $(17, 13) = 1$ τότε

$$\begin{aligned} 17 &= 1 \cdot 13 + 4 \quad \text{και} \quad 13 = 3 \cdot 4 + 1 \Rightarrow 1 = 13 - 3 \cdot 4 = 13 - 3(17 - 13) = \\ &= 13 - 3 \cdot 17 + 3 \cdot 13 = 4 \cdot 13 - 3 \cdot 17 \Rightarrow 1 = 4 \cdot 13 - 3 \cdot 17 \Rightarrow \end{aligned}$$

$$\xrightarrow{[\cdot]_7} [1]_7 = [4]_7 \cdot [13]_7, \text{ Άρα } ([13]_7)^{-1} = [4]_7$$

Συνεπώς, στην παραπάνω σχέση είναι:

$$k \equiv 6 \cdot 4 \pmod{17} = 24 \pmod{17} \equiv 7 \pmod{17}$$

$$\text{Άρα, } x = 10 + 13 \cdot k = 10 + 13 \cdot 7 = 101$$

$$\text{Επομένως, οι αμέγαλοι } x \equiv 101 \pmod{[13, 17]} \equiv$$

$$\equiv 101 \pmod{(13 \cdot 17)} \equiv 101 \pmod{221} \text{ είναι οι λύσεις!!!}$$

3)

$$B. \begin{cases} 16x \equiv 27 \pmod{41} \\ 23x \equiv 16 \pmod{43} \end{cases}$$

$$16x \equiv 27 \pmod{41} \Rightarrow 48x \equiv 81 \pmod{41} \Rightarrow 7x \equiv -1 \pmod{41} \Rightarrow \\ \Rightarrow \boxed{x \equiv -6 \pmod{41}} \quad (1)$$

$$\text{Evv, } 23x \equiv 16 \pmod{43} \Rightarrow 46x \equiv 32 \pmod{43} \Rightarrow 3x \equiv -1 \pmod{43} \Rightarrow \\ \Rightarrow 314x \equiv -114 \pmod{43} \Rightarrow 42x \equiv -154 \pmod{43} \Rightarrow \\ \Rightarrow -x \equiv -25 \pmod{43} \Rightarrow \boxed{x \equiv 29 \pmod{43}} \quad (2)$$

Enilwate dyadid 21 (1), (2)

ano d. kiveTon exote

$$C_1 = 21 \quad \text{ya} \quad C_2 = 21$$

$$\text{4x } x \equiv 240 \pmod{1763}$$

3)
8.

Να εντοπίσει 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 εφαρμοστεί το κινεϊτικό 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.

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

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

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

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

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

Και άρα, (1) είναι:

$$\beta_3 \equiv 12 \pmod{13} \Rightarrow \beta_3 = 12 \quad \text{Επίσης, συντελεστές του:}$$

$$\begin{aligned} x_0 &\equiv (143 \cdot 5 \cdot 4 + 91 \cdot 4 \cdot 9 + 77 \cdot 12 \cdot 4) \pmod{105} \equiv (2860 + 3276 + 3696) \pmod{105} \\ &\equiv 9832 \pmod{105} \equiv 67 \pmod{105} \end{aligned}$$

ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ

$$(ax^2 + bx + c) \equiv 0 \pmod{p} \text{ ή } (0 \pmod{p})$$

$$ay^2 \equiv b \pmod{p} \text{ (ή } \pmod{p})$$

$$y^2 \equiv b' \pmod{p} \text{ (ή } \pmod{p}) \quad (1)$$

Αν x_0 λύση της (1) τότε $p - x_0$ είναι επίσης λύση

- Η (1) θα έχει 2 λύσεις ή καμία

Η λύση εξαρτάται από το εάν ο b' μπορεί να γραφεί σαν το τετράγωνο ενός άλλου

- Η (1) δεν έχει λύσεις

ο b' καλείται τετράγωνικό υπόλοιπο $\pmod{p}$ αν υπάρχει c ώστε $c^2 \equiv b' \pmod{p}$

Διαφορετικά ο b' καλείται τετράγωνικό $\text{N\acute{o}t\acute{o}$ υπόλοιπο

Πλ

$$\text{Η } x^2 \equiv -1 \pmod{p} \text{ π.η.π. έχει λύση } \Leftrightarrow p = 4k+1$$

ΠΡΟΤΑΣΗ/ΕΦΑΡΜΟΓΗ

Αν $p = 4k+3$ τότε ο a^{kH} αποτελεί λύση της $x^2 \equiv a \pmod{p}$ όταν αυτή έχει λύση. Πώς αντιμετωπίζουμε την $x^2 \equiv b \pmod{p}$;

Δηλ. $m \in \mathbb{N}$ και όχι απαραίτητα πρώτος:

$$m = p_1^{k_1} \dots p_r^{k_r} \Rightarrow x^2 \equiv b \pmod{(p_1^{k_1} \dots p_r^{k_r})} \Rightarrow \begin{cases} x^2 \equiv b \pmod{p_1^{k_1}} \\ \vdots \\ x^2 \equiv b \pmod{p_r^{k_r}} \end{cases}$$

και λύνουμε το δεξί σύστημα $\rightarrow$

(ΜΟΝΟ ΓΙΑ ΕΚΘΕΤΗ 2)

ΠΡΟΤΑΣΗ

Έστω p : πρώτος και $a \in \mathbb{Z}$ με $(a, p) = 1$. Αν $m \neq x \equiv a \pmod{p}$ έχει δύο λύσεις, τότε και $x^2 \equiv a \pmod{p^2}$ έχει επίσης δύο λύσεις. Αν m $x^2 \equiv a \pmod{p}$ δεν έχει λύση, τότε ούτε m $x^2 \equiv a \pmod{p^2}$ έχει λύση.

ΑΠΟΔΕΙΞΗ

$$1 \leq a \leq p^2 - 1 \Rightarrow a = p\pi + u \text{ με } 0 \leq u \leq p-1$$

$$a \pmod{p} = u \pmod{p}$$

$\mathbb{Z}_p^*$ έχει πρωταρχική ρίζα (δηλαδή $\exists r \in \mathbb{Z}_p^* : \text{ord}_p(r) = p-1$)

Γνωρίζουμε ότι m $x^2 \equiv a \pmod{p} \equiv u \pmod{p}$ έχει λύση. Άρα, θα υπάρχει $m \in \mathbb{N}$ ώστε $u = v^{2m} \pmod{p}$. Θεωρούμε το $x_0 = v^m \pmod{p}$ η οποία αποτελεί λύση της $x^2 \equiv u \pmod{p}$.

$$\text{Τότε } (x + kp)^2 = x_0^2 + 2x_0kp + k^2p^2 = (v^{2m} + 2v^m kp) \pmod{p^2}$$

$$2v^m kp + v^{2m} \equiv a \pmod{p^2} \Rightarrow 2v^m kp \equiv \pi p \pmod{p^2} \Rightarrow$$

$$\Rightarrow 2v^m k \equiv \pi \pmod{p^2} \quad (1) \text{ υποθέτουμε ότι } \pi \equiv v^q \pmod{p} \quad (2)$$

$$\text{και } \pi \equiv v^q \pmod{p} \quad (3). \text{ Έτσι, από (1), (2), (3) έχουμε}$$

$$2v^m k \equiv \pi \pmod{p^2} \Rightarrow v^q \cdot v^m \cdot k \equiv v^q \pmod{p^2} \Rightarrow$$

$$\Rightarrow \underline{k \equiv v^{q-m} \pmod{p^2}} \equiv v^q \cdot v^{p-1-q} \cdot v^{p-1-m} \pmod{p^2}$$

ΘΑΔΟ $x_0 + kp$ λύση της $x^2 \equiv u \pmod{p} \equiv a \pmod{p}$.

$$(v^m + v^q \cdot v^{p-1-q} \cdot v^{p-1-m} p)^2 = v^{2m} + 2v^m \cdot v^q \cdot v^{p-1-q} \cdot v^{p-1-m} p + v^{2q} \cdot v^{2(p-1-q)} \cdot v^{2(p-1-m)} p^2 \equiv x \pmod{p^2}$$

$$v^{2m} + v^q p \equiv x \pmod{p^2} \Rightarrow u + \pi p \equiv a \pmod{p^2}$$

$$\Rightarrow (x_0 + kp) \pmod{p^2} \text{ αποτελεί λύση!}$$

πλ

$$x^2 \equiv 15 \pmod{49} \equiv 15 \pmod{7^2}$$

Επιλύουμε πρώτα ενν

$$x^2 \equiv 15 \pmod{7} \equiv 1 \pmod{7} \Rightarrow \text{Λύσεις οι } \pm 1$$

$$(\text{όπου } -1 = 7-1 = 6)$$

Αφού, αν $x^2 \equiv 15 \pmod{7}$ έχει λύση θα έχει

λύση και αν $x^2 \equiv 15 \pmod{49}$. Να τη βρούμε $x_0 = 1$

και θα πάρουμε το $(x_0 + kp)^2 \equiv (1 + k \cdot 7)^2 \pmod{7^2} \equiv 15 \pmod{7^2}$

$$1 + 2 \cdot k \cdot 7 + k^2 \cdot 7^2 \equiv 15 \pmod{7^2} \Rightarrow 2k \cdot 7 \equiv 14 \pmod{7^2} \Rightarrow$$

$$\Rightarrow 2k \equiv 2 \pmod{7} \quad (\text{όπου } (2, 7) = 1 \Rightarrow \exists 2^{-1} \pmod{7})$$

$$\Leftrightarrow k \equiv 1 \pmod{7}.$$

Λύση της $x^2 \equiv 15 \pmod{7^2}$ είναι η $(1 + 7k) \pmod{7^2}$

$$(1 + 7) \pmod{7^2} \equiv 8 \pmod{7^2}$$

$$8^2 \equiv 15 \pmod{49} \sim$$

$$\sim 64 \equiv 15 \pmod{49}.$$

$$\text{Λύση της } x^2 \equiv a \pmod{(p_1^{k_1} \dots p_r^{k_r})} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x^2 \equiv a \pmod{p_1^{k_1}} \\ \vdots \\ x^2 \equiv a \pmod{p_r^{k_r}} \end{cases} \quad \left. \begin{array}{l} \text{Είναι } x_i \text{ μία λύση για κάθε} \\ x^2 \equiv a \pmod{p_i^{k_i}} \end{array} \right\}$$

κάθε έναν του συνιτηζος

$$\left. \begin{array}{l} x \equiv x_1 \pmod{p_1^{k_1}} \\ \vdots \\ x \equiv x_r \pmod{p_r^{k_r}} \end{array} \right\} \text{ είναι λύση της } x^2 \equiv a$$

Επειδή $(p_i^{k_i}, p_j^{k_j}) = 1 \Rightarrow$ Απο το εναλλακτικό ημωδίου το
 $\pmod{(p_1^{k_1} \dots p_r^{k_r})}$.