

ΣΥΣΤΗΜΑΤΑ (ΜΕΘΟΔΟΣ ΕΠΙΛΥΣΗΣ)

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ \vdots \\ a_k x \equiv b_k \pmod{m_k} \end{cases} \quad (1)$$

Εξετάζουμε εάν υπάρξει μία από τις εξισώσεις

$a_i x \equiv b_i \pmod{m_i}$, $i=1, \dots, k$ έχει λύση. $\Leftrightarrow (a_i, m_i) \mid b_i$

Αν $(a_i, m_i) = 1 \Rightarrow$ μοναδική λύση

Αν $(a_i, m_i) = \delta$ και $\delta \mid b_i$ τότε αν x_0 μία λύση, τότε οι λύσεις δίνονται από :

$$x_0, x_0 + \frac{m_i}{\delta}, x_0 + \frac{2m_i}{\delta}, \dots, x_0 + \frac{(\delta-1)m_i}{\delta} \pmod{m_i}$$

Υποθέτουμε ότι το αρχικό σύστημα (1) έχει λύση

διστά $(a_i, m_i) = \delta_i \mid b_i$

Μετασχηματίζουμε των (1) στο :

$$(2) \left(\begin{array}{c} \frac{a_1}{\delta_1} x \equiv \frac{b_1}{\delta_1} \pmod{\frac{m_1}{\delta_1}} \\ \vdots \\ \frac{a_k}{\delta_k} x \equiv \frac{b_k}{\delta_k} \pmod{\frac{m_k}{\delta_k}} \end{array} \right) \xRightarrow{\left(\frac{a_i}{\delta_i}, \frac{m_i}{\delta_i} \right) = 1} \exists \left(\frac{a_i}{\delta_i} \right)^{-1}$$

Το (2) δίνεται:

$$(3): \begin{pmatrix} x \equiv \left(\frac{a_1}{\delta_1}\right)^{-1} \frac{b_1}{\delta_1} \pmod{\frac{m_1}{\delta_1}} \\ \vdots \\ x \equiv \left(\frac{a_k}{\delta_k}\right)^{-1} \frac{b_k}{\delta_k} \pmod{\frac{m_k}{\delta_k}} \end{pmatrix}$$

Το (3) έχει λύση εάν:

$$\left(\frac{m_i}{\delta_i}, \frac{m_j}{\delta_j}\right) \mid \left[\left(\frac{a_i}{\delta_i}\right)^{-1} \frac{b_i}{\delta_i} - \left(\frac{a_j}{\delta_j}\right)^{-1} \frac{b_j}{\delta_j} \right] \quad \forall i, j$$

• Αν $\left(\frac{m_i}{\delta_i}, \frac{m_j}{\delta_j}\right) = 1$ τότε έχουμε (και βρίσκουμε) λύση από το κινεζικό θεωρήμα

• Αν $\left(\frac{m_i}{\delta_i}, \frac{m_j}{\delta_j}\right) > 1$ και όχι μια λύση

τότε οι λύσεις δίνονται από:

$$x_0 \pmod{\left[\frac{m_1}{\delta_1}, \frac{m_2}{\delta_2}, \dots, \frac{m_k}{\delta_k}\right]} = M = \frac{m_1}{\delta_1} \cdot \frac{m_2}{\delta_2} \cdot \dots \cdot \frac{m_k}{\delta_k}$$

Λύση από τον αλγόριθμο του Κινέζου:

$$\left(\frac{M}{\delta_1} c_1 \left(\frac{a_1}{\delta_1}\right)^{-1} \frac{b_1}{\delta_1} + \dots + \frac{M}{\delta_k} c_k \left(\frac{a_k}{\delta_k}\right)^{-1} \frac{b_k}{\delta_k} \right) \pmod{M}$$

ΠΧ

Να λυθεί το σύστημα

$$3x \equiv 7 \pmod{23}$$

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

ΜΕΤ

$(3, 7) = 1 \Rightarrow$ Η 1^η εξίσωση έχει μοναδική λύση

Βεβαιώστε την αντιστρεψιμότητα κλάσης $3^{-1} \equiv 8 \pmod{23}$

Διότι $8 \cdot 3 \equiv 1 \pmod{23}$

$$3x \equiv 7 \pmod{23} \Rightarrow 8 \cdot 3x \equiv 8 \cdot 7 \pmod{23} \Rightarrow x \equiv 10 \pmod{23}$$

$$\text{Λύσεις } x \in \{10, 10 \pm 23, 10 \pm 2 \cdot 23, \dots\}$$

Για να εφιστώσῃ:

$$(15, 18) = 3 \mid 12 \Rightarrow \text{Άρα ἔχει λύση}$$

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

$$\text{Οπου } (5, 6) = 1 \Rightarrow \text{Μοναδική}$$

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

$$\text{Λύσεις } x \in \{2, 2 \pm 6, 2 \pm 12, \dots\}$$

Λύσεις του συστήματος

$$x \in \{10, 10 \pm 23, 10 \pm 2 \cdot 23, \dots\} \cap \{2, 2 \pm 6, 2 \pm 12, \dots\}$$

Αρτοί-Πεπτοί Αριθμοί (έναντι)

Αρτοί Αριθμοί

Θα εξετάσουμε εάν

$$10 \pm 2k \cdot 23 = 2 \pm 6\lambda \Rightarrow \begin{cases} 10 = 2 \pm 6k \Rightarrow 8 = \pm 6k \\ \frac{8}{2} + 2 \frac{k}{2} \cdot 23 = \frac{6}{2} \lambda \Rightarrow 4 + 23k = 3\lambda \end{cases}$$

Προηγμένη λύση $(1, 9) = (k, \lambda)$ και μοναδική

οπου $(23, 6) = 1 \mid 10 - 2 = 8$ έχουμε λύση με το θ. του κινέζου.

ΤΕΤΡΑΓΩΜΙΚΑ ΥΠΟΛΟΙΠΑ:

$$ax^2 + \beta x + \gamma = 0 \Rightarrow a(x^2 + \frac{\beta}{a}x + \frac{\gamma}{a}) = 0 \Rightarrow, a \neq 0$$

$$\Rightarrow a \left(x^2 + 2 \frac{\beta}{2a} x + \left(\frac{\beta}{2a} \right)^2 - \left(\frac{\beta}{2a} \right)^2 + \frac{\gamma}{a} \right) = 0 \Rightarrow$$

$$\Rightarrow a \left(\left(x + \frac{\beta}{2a} \right)^2 - \frac{\beta^2 - 4a\gamma}{4a^2} \right) = 0 \Rightarrow$$

$$\Rightarrow a \left(\left(x + \frac{\beta}{2a} \right)^2 - \frac{\Delta}{4a^2} \right) = 0 \quad (1)$$

• Πάνω στο $\mathbb{R}$, αν $-\Delta > 0$ δεν έχει λύση

• Πάνω στο $\mathbb{C}$, αν $-\Delta > 0$ έχει λύση

Ναι έχει διάφορα τετράγωνα:

Αν υπάρχει E ώστε $E^2 \equiv \Delta$, τότε
 $a \cdot \left[\left(x + \frac{\beta}{2a} \right)^2 - \left(\frac{E}{2a} \right)^2 \right] = 0 \Rightarrow a \left(x + \frac{\beta}{2a} - \frac{E}{2a} \right) \left(x + \frac{\beta}{2a} + \frac{E}{2a} \right) = 0 \quad (1)$

$$y = x + \frac{\beta}{2a} \quad \text{και} \quad z = \left(\frac{E}{2a} \right)^2$$

Αρα, (1) $\rightarrow a(y^2 - z) = 0$ με z δεδομένο

Αυτό που ^{δεν} γινώριζαμε είναι εάν $z = \left(\frac{E}{2a} \right)^2$ δηλαδή

γραφεται ως τέλειο τετράγωνο

Η λύση εξαρτάται από τη λύση της $ay^2 - az = 0$

Δηλ. θέλουμε να λύσουμε την $y^2 = E$

Στας μιγαδικούς, κάθε μιγαδικός γραφεται ως τέλειο τετράγωνο.

Στη θεωρία αριθμών μας ενδιαφέρει η λύση της

$\alpha x^2 + \beta x + \gamma \equiv 0 \pmod{m}$, όπου ανάγεται στη λύση

της $ay^2 - az \equiv 0 \pmod{m}$. Αν $(a, m) = 1 \Rightarrow$ η εξίσωση

γίνεται $y^2 \equiv E \pmod{m}$ και θα εξετάσουμε εάν

οι εξισώσεις της μορφής αυτής έχουν λύση. Το

ερώτημα είναι "μπορεί μια δεδομένη υψωση να γραφεί

σαν τέλειο τετράγωνο μιας άλλης;"

Πχ

στο $\mathbb{Z}_3$: Το 1 γραφεται σαν τέλειο τετράγωνο

Το 2 δεν γραφεται σαν τέλειο τετράγωνο

(δηλ. δεν υπάρχει υψωση ώστε το τετράγωνό της να δίνει 2)

Αρα, αν σου ζητούσε λύσεις:

$$x^2 \equiv 2 \pmod{13} \quad \text{Αδύνατο (δεν έχει λύση)}$$

στο $\mathbb{Z}_5$: Το 1 & 4 Γραφονται σαν τέλειο τετράγωνο

$$x^2 \equiv 4 \pmod{5} \quad \text{έχει 2 λύσεις} \rightarrow \{2, 3\}$$

$$x^2 \equiv 1 \pmod{5} \quad \text{έχει 2 λύσεις} \rightarrow \{1, 4\}$$

Το 2 & 3 δεν γράφονται ως τέλεια τετράγωνα
 $x^2 \equiv 2 \pmod{5}$ δεν έχει λύση } στο $\mathbb{Z}_5$
 $x^2 \equiv 3 \pmod{5}$ " " " }

Ποιόθε τα λύση της $x^2 \equiv a \pmod{n}$

1) Έχει λύσεις;

Από τι εξαρτάται;

Μπορούμε να τις βρούμε;

2) Αν έχει λύση τότε πόσες έχει;

Θα μπορούσαμε να βρούμε το τετράγωνο στο $\text{mod } n$

Αντί που γράφονται σαν τετράγωνα (τέλεια) λέγονται
τετραγωνικά υπόλοιπα ενώ τα άλλα μη τετραγωνικά

ΟΡΙΣΜΟΣ: Αν $m \cdot x^2 \equiv a \pmod{p}$ έχει λύση τότε το
 a καλείται τετραγωνικό υπόλοιπο $\pmod{p}$. Αν δεν έχει
λύση τότε το a καλείται μη τετραγωνικό υπόλοιπο
 $\pmod{p}$. (ΤΥ και ΤΜΥ αντιστοίχως)

Παρατήρηση: Αν το a είναι ΤΥ $\pmod{n}$ και d
ικανοποιεί των $x^2 \equiv a \pmod{n}$, τότε και το $(m-d)$
ικανοποιεί επίσης των $x^2 \equiv a \pmod{n}$. Δηλ. αν
έχαμε μία λύση τότε θα είχαμε δύο.

ΘΕΩΡΗΜΑ (ΣΕΛ 1):

Έστω p πρώτος n πτός

Τότε υπάρχει $d \in \mathbb{Z}$ με $d^2 \equiv -1 \pmod{p} \Leftrightarrow p \equiv 1 \pmod{4}$

ΠΟΡΙΣΜΑ: $x^2 \equiv (p-1) \pmod{p}$ έχει λύση $\Leftrightarrow p \equiv 1 \pmod{4}$

ΘΕΩΡΗΜΑ (Κριτήριο του Euler)

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

Τότε

α) Το a είναι ΤΥ $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

β) Το a είναι ΤΜΥ $\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

ΑΠΟΔΕΙΞΗ

α) Εστω ότι υπάρχει a' με $(a')^2 \equiv a \pmod{p} \Rightarrow$

$$\Rightarrow ((a')^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p} \Rightarrow$$

$$\Rightarrow (a')^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p} \Rightarrow 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Αντίστροφα

Εστω $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ και p πρώτος

Αφού p : πρώτος $\Rightarrow \exists$ ηρωταρχική ρίζα $\beta : \text{ord}_p(\beta) = p-1$

Αρα υψοθέτηση θα δίνεται από τη δύναμη του β

Από την υψοθέση $a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow \text{ord}_p(a) \mid \frac{p-1}{2}$

Επίσης, $\exists r \in \mathbb{N} : a \equiv \beta^r \pmod{p} \Rightarrow a \equiv \beta^r \pmod{p} \Rightarrow$

$$\Rightarrow \text{ord}_p(a) = \text{ord}_p(\beta^r) \mid \frac{p-1}{2}$$

$$\text{ord}_p(\beta^r) = \frac{\text{ord}_p(\beta)}{(r, \text{ord}_p(\beta))} = \frac{p-1}{(r, p-1)} \mid \frac{p-1}{2}$$

$$2 \mid (r, p-1) \Rightarrow 2 \mid r \Rightarrow r = 2m$$

$$a \equiv \beta^r \equiv \beta^{2m} \equiv (\beta^m)^2 \pmod{p}$$

↑
λύση

Αρα, έχει λύση

β) Οι λύσεις $x^2 \equiv 1 \pmod{p}$ είναι $m \mid$ και $p-1$

$$(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \pmod{p} \text{ έχει λύσεις}$$

$$\underbrace{a^{\frac{p-1}{2}} \equiv 1}_{\text{από το (α)}} \quad \vee \quad \underbrace{a^{\frac{p-1}{2}} \equiv -1}_{\text{από το (α)}}$$

είναι λύση

δεν είναι λύση

Κριτήριο : Υποθέτουμε ότι:

α) $p = 4n+3$ και β) ο a είναι ΤΥ $\Leftrightarrow n$ επίσημα
 $x^2 \equiv a \pmod{p}$ έχει λύση. Τότε το a^{n+1} είναι λύση
Επιβεβαίωση: Γνωρίζουμε ότι n $x^2 \equiv a \pmod{p}$
έχει λύση $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Γνωρίζουμε το $a^{n+1} \Leftrightarrow$ είναι λύση $\Leftrightarrow (a^{n+1})^2 = a^{2n+2} =$
 $= a \cdot a^{\frac{p-1}{2}} \equiv a \pmod{p} \rightarrow$ Άρα, a^{n+1} είναι επί

Πχ

Να εξετάσσουμε ως προς το αν έχει λύση η επίσημα
 $x^2 \equiv 5 \pmod{19}$

Λύση

Το 5 είναι ΤΥ $\pmod{19}$ αν $5^{\frac{p-1}{2}} \equiv 1 \pmod{19} \Leftrightarrow$

$\Leftrightarrow 5^{\frac{19-1}{2}} \equiv 1 \pmod{19} \Leftrightarrow 5^9 \equiv 1 \pmod{19}$ (Ολο το εξετάσουμε)

$$5^2 \equiv 25 \pmod{19} \equiv 6 \pmod{19}$$

$$5^4 \equiv 36 \pmod{19} \equiv 17 \pmod{19}$$

$$5^8 \equiv 17^2 \pmod{19} \equiv 4 \pmod{19}$$

$$5^9 \equiv 20 \pmod{19} \equiv 1 \pmod{19}$$

Άρα, πράγματι η επίσημα έχει λύση

Εξετάσουμε αν μπορούμε να την βρούμε

$19 = 4 \cdot 4 + 3$ Άρα, η 5^{4+1} λύση πρέπει να είναι.

$$5^5 = 5^4 \cdot 5 \equiv 17 \cdot 5 \pmod{19} \equiv 85 \pmod{19} \equiv 9 \pmod{19}$$

Άρα, η 4 λύση $9 \pmod{19}$ λύση της.