

ΦΥΜ-ΑΔΚ 3

6) $5x + 55y + 8z + 7w = 2 \quad (1)$

$$\begin{aligned} 5x + 55y &= 5\alpha, \text{ οπου } (5, 55) = 5 \\ 8z + 7w &= \beta \end{aligned}$$

(1): $5\alpha + \beta = 2 \cdot 1$, $(5, 1) = 1/2$ Εχει λύσεις

$$5\alpha + \beta = 1 \text{ οπου } 5 \cdot 1 + 1 \cdot (-4) = 1$$

Λύσεις:

$$\alpha = 1 \cdot 2 + 1 \cdot t \quad \text{και} \quad \beta = (-4) \cdot 2 + 5 \cdot t, \quad t \in \mathbb{Z}$$

$$\left. \begin{aligned} 8z + 7w &= 1 \cdot \beta \\ 8z + 7w &= 1 \\ 8 \cdot 1 + 7(-1) &= 1 \end{aligned} \right\} \text{Λύσεις}$$

$$z = 1 \cdot \beta + 7 \cdot s, \quad s \in \mathbb{Z}$$

$$w = (-1) \cdot \beta - 8s$$

$$z = -8 - 5t + 7s$$

$$w = 8 + 5t - 8s$$

$$5x + 55y = 5\alpha \Leftrightarrow 5x + 55y = 5 \Leftrightarrow 5(-10) + 55 \cdot 1 = 5$$

Άρα,

$$x = (-10)\alpha + 55r = -20 - 10t + 55r$$

$$y = 1 \cdot \alpha - 5r = 2 + t - 5r, \quad r \in \mathbb{Z}$$

Γενικότερα θεωρία:

Εστω $a \in \mathbb{Z}$, τότε

$$Z = [0+a]_m \cup [1+a]_m \cup \dots \cup [m-1+a]_m$$

αλλά όχι με την ίδια σειρά!

ΠΑΡΑΧΗΡΗΣΗ:

Έστω $m_1, \dots, m_k$ φυσικοί μεγαλύτεροι του 1

$$[m_1, \dots, m_k] = m_1 \dots m_k \Leftrightarrow (m_i, m_j) = 1, \forall i \neq j$$

Γενικά:

$$[m_1, \dots, m_k] = \frac{m_1 \dots m_k}{(m_1, \dots, m_k)}$$

ΠΧ1

$$6 \bmod 4 \equiv 2 \quad \left\{ \begin{array}{l} 6 \cdot 10 \bmod 4 \cdot 6 \equiv 60 \bmod 24 \equiv 12 \\ 10 \bmod 6 \equiv 4 \end{array} \right. \quad \text{Αλλά } 2 \cdot 4 = 8 \not\equiv 12$$

$$10 \bmod 6 \equiv 4 \quad \left\{ \begin{array}{l} 2 \cdot 4 = 8 \not\equiv 12 \end{array} \right.$$

Άρα, δω έχουμε δικαίωμα να/ή να των εξισώσεων παρά, μόνο στην περίπτωση όπου οι αριθμοί είναι πρώτοι μεταξύ τους

ΠΧ2

$$\left. \begin{array}{l} 7 \bmod 3 \equiv 1 \\ 10 \bmod 8 \equiv 2 \end{array} \right\} \begin{array}{l} 70 \bmod 24 \equiv 22 \\ \text{Αλλά } 2 \cdot 1 \equiv 2 \not\equiv 22 \end{array}$$

ΠΡΟΤΑΣΗ: Έστω $a \equiv b \bmod m_i$ με $m_i > 1$ φυσικοί

για $i=1, 2, \dots, k$. Τότε,

$$a \equiv b \bmod m_i \quad \forall i \Leftrightarrow a \equiv b \bmod [m_1, \dots, m_k]$$

$$\text{Αντ. } m_1 \dots m_k = [m_1, \dots, m_k] \text{ και } (m_i, m_j) = 1, i \neq j$$

ΠΧ

$$\text{Έστω } a \equiv b \bmod 4 \text{ και } a \equiv b \bmod 27$$

$$\text{Άρα } (27, 4) = 1 \Leftrightarrow a \equiv b \bmod 4 \cdot 27 = b \bmod 108$$

ΑΠΟΔΕΙΞΗ

$$(\Rightarrow) \text{ Έστω, } a \equiv b \bmod m_i, i=1, \dots, k \text{ \& } (m_i, m_j) = 1, i \neq j$$

$$a \equiv b \bmod m_i \Leftrightarrow m_i \mid a-b, \forall i=1, \dots, k$$

$$\text{Θέλω } m_1 \dots m_k \mid a-b$$

$$\text{Αν } m_1 \mid a-b \text{ και } m_2 \mid a-b \Rightarrow m_1 \cdot m_2 \mid a-b$$

$$(\text{διστά ξερατικ'όσα } (m_1, m_2) = 1)$$

Επειδή, $(m_i, m_j) = 1$ και $m_i | a-b \quad \forall i=1, \dots, k$
 $m_1 \dots m_k | a-b \Rightarrow a \equiv b \pmod{m_1 \dots m_k}$

($\Leftarrow$): Γνωρίζουμε ότι

$$m_1 \dots m_k | a-b \Rightarrow m_i | a-b \Rightarrow a \equiv b \pmod{m_i}$$

$$\text{Αλλά, } m_i | m_1 \dots m_k \quad i=1, \dots, k$$

$$\mathbb{Z}_m = \{ [0]_m, [1]_m, \dots, [m-1]_m \}$$

$$\mathbb{Z}_4 = \{ [0]_4, [1]_4, [2]_4, [3]_4 \}$$

Μπορούμε να ορίσουμε πράξεις στο $\mathbb{Z}_4$ ή $\mathbb{Z}_m$,

ΠΡΟΣΘΕΣΗ:

Στο $\mathbb{Z}_m$:

$$[a]_4 \oplus [b]_4 = [c]_4 \text{ μοναδικά}$$

$$[a]_4 = [a+4]_4 = [a-3 \cdot 4]_4$$

Πρέπει η πράξη μας να μην αναπαριστάται ευ γλάστρα
Ορίστηκε στο $\mathbb{Z}_m$ μια πράξη πρόσθετος ως εξής

$$[a]_m \oplus [b]_m = [a+b]_m$$

Πρέπει νδο δεν εξαρτάται από τους αναπαριστάτες

$$[a]_m = [a+km]_m \text{ και } [b]_m = [b+\lambda m]_m$$

$$[a]_m \oplus [b]_m = [a+km]_m \oplus [b+\lambda m]_m \Leftrightarrow$$

$$a+b - (a+b+km+\lambda m) = (-k-\lambda)m = 0 \pmod{m}$$

Άρα, είναι ωστ. Η πράξη $\oplus$ καλά ορισμένη

$\mathbb{Z}_4$

$\oplus$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

ΠΟΛΥΠΛΗΘΙΑΣΜΟΣ:

Στο $\mathbb{Z}_m$:

$$[a]_m \odot [b]_m = [a \cdot b]_m$$

Οπως και προηγουμένως δεν εξαρτάται από τους αναπαριστάτες
και είναι καλά ορισμένη

$\mathbb{Z}_4$:

$\odot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Στο $\mathbb{Z}_4$: $[2]_4 \odot [2]_4 = [0]_4$ αλλά $[2]_4 \neq [0]_4$

Ενώ στο $\mathbb{Q}$: $a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$

$\mathbb{Z}_3$:

$\odot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

• Αν ο πρώτος: $\mathbb{Z}_p$ συνηθίζεται

σχεδόν όπως το $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

• Ενώ αν m σύνθετος: $\mathbb{Z}_m$

συνήθίζεται "ασχημα"

ως προς τον πολλαπλασιασμό

Δηλ. αν $m = ab$ τότε $[a]_m \odot [b]_m = [a \cdot b]_m = [m]_m = [0]_m$

και $[a]_m \neq [0]_m$, $[b]_m \neq [0]_m$

ΕΡΩΤΗΜΑ: Αν $[a]_m \cdot [c]_m = [b]_m \cdot [c]_m$ τότε

μπορούμε να πούμε ότι $[a]_m = [b]_m$?

Στο $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$a \neq 0 \Rightarrow$ Ανστροφος του a . Θα είναι ο αριθμος β

ώστε $a\beta = 1$

Αρα, $\beta = \frac{1}{a} = a^{-1}$

ΑΝΙΣΤΡΟΦΟΣ ΚΑΙ ΑΞΕΙΣ

Στον πίνακα του $\mathbb{Z}_4$, παρατηρούμε ότι

$$([1]_4)^{-1} = [1]_4 \text{ γιατί } [1]_4 \odot [1]_4 = [1]_4$$

$$([2]_4)^{-1} = \text{ΔΕΝ ΥΠΑΡΧΕΙ ΣΤΟ } \mathbb{MOD}_4$$

$$([3]_4)^{-1} = [3]_4 \text{ γιατί } [3]_4 \odot [3]_4 = [1]_4$$

Αλλά στον $\mathbb{Z}_3$ πίνακα, έχει πάντα αντιστροφή.

→ Στον $\mathbb{Z}_4$ θα έχει αντιστροφή όταν οι αριθμοί γινόνται μετὰ ζυγούς.

ΠΡΟΤΑΣΗ: Αν $a \equiv b \pmod{m}$ και $\gamma \in \mathbb{Z}$, τότε:

1) $a^n \equiv b^n \pmod{m}$

2) $a \pm \gamma \equiv b \pm \gamma \pmod{m}$

3) $a \cdot \gamma \equiv b \cdot \gamma \pmod{m}$

ΑΠΟΔΕΙΞΗ

1) ΕΛΘ $a^n - b^n$ διαίρεται από το m

$$a^n - b^n = (a - b) \cdot (a^{n-1} + a^{n-2}b + \dots + b^{n-1})$$

$$m \mid a - b \Rightarrow m \mid a^n - b^n$$

2) $a \pm \gamma \equiv b \pm \gamma \pmod{m} \Leftrightarrow m \mid a \pm \gamma - (b \pm \gamma) = a - b$ ΛΟΓΩ

3) $a \cdot \gamma \equiv b \cdot \gamma \pmod{m} \Leftrightarrow (a - b) \gamma$ διαίρεται από το m

→ ΑΛΛΑ $m \mid a - b \Rightarrow m \mid (a - b) \gamma$

Το σύνολο $\mathbb{Z}_m$ με τις δύο πράξεις $\oplus$ και $\odot$ αποτελεί "δυναμίο" (Μπορεί $[a]_m \neq [0]_m$ και να μην έχει αντιστροφή). Αν p = πρώτος, τότε $\mathbb{Z}_p$ σώμα με αυτές τις πράξεις. Δηλ. συμπεριφέρεται όπως το $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Συστημική: $\forall [a]_p \neq [0]_p \Rightarrow \exists x \text{ αντίστροφο modulo } p$

ΠΡ

Εστω $a \cdot b = 0 \pmod{m}$ και υπάρχει x ώστε $a \cdot x = 1 \pmod{m}$
τότε θα έχουμε $a \cdot b = 0 \pmod{m} \Rightarrow x \cdot a \cdot b = x \cdot 0 \pmod{m} \Rightarrow$
 $\Rightarrow 1 \cdot b = 0 \pmod{m} \Rightarrow b = 0 \pmod{m}$
Η σχέση $a \cdot x = 1 \pmod{m} \Leftrightarrow ax - 1 = km \Leftrightarrow (a, m) = 1 \Leftrightarrow ax - km = 1$

ΘΕΩΡΗΜΑ:

- 1) Εστω $m \in \mathbb{N}^*$ και $a, b \in \mathbb{Z}$ με $(a, m) = 1$. Αν $ab = 0 \pmod{m}$ τότε $b = 0 \pmod{m}$
- 2) Εστω $m \in \mathbb{N}^*$ και $a, b \in \mathbb{Z}^*$. Αν $ab = 0 \pmod{m}$ τότε $b = 0 \pmod{\frac{m}{(a, m)}}$

ΑΝΟΔΕΙΞΗ

- 1) $a \cdot b$ διαίρεται από το m και $(a, m) = 1$
Αρα, $m | b \Rightarrow b = 0 \pmod{m}$
- 2) $m | a \cdot b \Leftrightarrow a \cdot b = km \Leftrightarrow \frac{a}{(a, m)} \cdot b = k \frac{m}{(a, m)} \Rightarrow b = 0 \pmod{\frac{m}{(a, m)}}$

$$\text{Διότι } \left(\frac{a}{(a, m)}, \frac{m}{(a, m)} \right) = 1$$

ΠΡΟΤΗΜΑ:

Αν $m > 1$ φυσικός και $a, b, x \in \mathbb{Z}$. Τότε, $ax = bx \pmod{m}$
αν και $a \equiv b \pmod{\frac{m}{(x, m)}}$. Αν επίσης, $(x, m) = 1$ τότε
 $ax = bx \pmod{m} \Leftrightarrow a = b \pmod{m}$

ΑΝΟΔΕΙΞΗ

- $(\Rightarrow)$ Αν $a \equiv b \pmod{m} \Leftrightarrow ax = bx \pmod{m}$ χωρίς σωθίκες
- $(\Leftarrow)$ $ax - bx$ διαίρεται από το m
 $x(a - b) = 0 \pmod{m}$ από την $(a - b) = 0 \pmod{\frac{m}{(x, m)}} \Rightarrow$
 $\Rightarrow a = b \pmod{\frac{m}{(x, m)}}$. Αν $(x, m) = 1$ έχουμε το $\frac{m}{(x, m)}$ αντιστρέφεται

ΟΡΙΣΜΟΣ: Μια κλάση $[a]_m$ θα καλείται αντιστρέψιμη mod m αν υπάρχει υδάτου $[b]_m$ ώστε $[a]_m \odot [b]_m = [1]_m$
θα γράφεται $([a]_m)^{-1} = [b]_m$

ΠΡΟΤΑΣΗ: Η κλάση $[a]_m$ είναι αντιστρέψιμη $\Leftrightarrow (a, m) = 1$
Είναι μοναδική: Έστω $[b]_m \odot [a]_m = [1]_m =$
 $= [b']_m \odot [a]_m$.

$$\text{οπότε } [b]_m = [b']_m \odot [1]_m = [b']_m \odot [a]_m \odot [b]_m = \\ = [1]_m \odot [b]_m = [b]_m.$$

Πως θα βρισκόμαστε την αντιστροφή;

$$\text{Έστω ότι } (a, m) = 1 \Rightarrow \exists ([a]_m)^{-1} = [b]_m$$

Ευκλείδειος αλγόριθμος:

$$(a, m) = 1 \Rightarrow \exists b \text{ και } x \in \mathbb{Z} \text{ ώστε}$$

$$ab + xm = 1 \Leftrightarrow [ab]_m = [1]_m \Leftrightarrow [a]_m \odot [b]_m = [1]_m$$

$$m=33 \text{ και } a=10$$

$$\text{Άρα } (a, m) = 1 \Rightarrow \exists ([10]_{33})^{-1}$$

$$\begin{cases} 33 = 10 \cdot 3 + 3 \leadsto 3 = 33 - 10 \cdot 3 \\ 10 = 3 \cdot 3 + 1 \leadsto 1 = 10 - 3 \cdot 3 \end{cases} \Rightarrow \begin{cases} 1 = 10 - (33 - 10) \cdot 3 \\ \Rightarrow 1 = -33 \cdot 3 + 10 \cdot 10 \end{cases}$$

$$\leadsto ([10]_{33})^{-1} = [10]_{33} \text{ λογικά ΠΑΝΤΑ αυτό;} \rightarrow \underline{\text{ΟΧΙ!}}$$

$$\text{Έστω } p \text{ πρώτος } \mathbb{Z}_p = \{ [0]_p, [1]_p, \dots, [p-1]_p \}$$

$$\text{Έστω } 1 \leq a \leq p-1 : (a, p) = 1$$

$$\mathbb{Z}_p^* = \{ [1]_p, [2]_p, \dots, [p-1]_p \} \text{ με } p-1 \text{ αντιστοιχίες}$$

$$\text{Αν } a \not\equiv 0 \pmod{p} \Rightarrow \exists [a]_p^{-1} (\mathbb{Z}_p^*, \odot).$$

$$\underline{\text{ΠΡΟΣΟΧΗ!}} \text{ Επειδή } [1]_p \oplus [p-1]_p = [0]_p \notin \mathbb{Z}_p$$

Η πρόσθεση στο $\mathbb{Z}_p^*$ δεν δαδώνει πάντα

Ενώ ο πολλαπλασιασμός δαδώνει για όλα

$$[a]_p, [b]_p \in \mathbb{Z}_p^*$$

$$[a]_p \odot [b]_p = [ab]_p$$

Αν είχαμε $[ab]_p = [0]_p$ τότε $p | ab$ και $p | a$ ή $p | b$
ΑΔΥΝΑΤΟ

$$\text{Και αν } [a]_p \in \mathbb{Z}_p^* \Rightarrow [a]_p^{-1} \in \mathbb{Z}_p^*$$

Παραδειγμα:

Βρείτε όλες τις αντιστροφίμες υποδιότητες mod 8

1, 2, 3, 4, 5, 6, 7

Αν: $(1, 8) = 1$, $(2, 8) = 2$, $(3, 8) = 1$, $(4, 8) = 4$, $(5, 8) = 1$
NAI OXI NAI OXI NAI

$(6, 8) = 2$, $(7, 8) = 1$
OXI NAI

$$[1]_8^{-1} = [1]_8, [3]_8^{-1} = [3]_8, [5]_8^{-1} = [5]_8, [7]_8^{-1} = [7]_8$$

ΟΡΙΣΜΟΣ: Η συνάρτηση του Euler $\varphi: \mathbb{N}^* \rightarrow \mathbb{N}^*$

με τιμή $\varphi(n) =$ το πλήθος των φυσικών μικρότερων του n και πρώτος προς τον n

$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$ (1, 2 < 3 και πρώτοι με το 3)

$\varphi(4) = 2$ (Παρατήρηση: $\varphi(2 \cdot 2) = 2$

αλλά $\varphi(2) \cdot \varphi(2) = 1 \cdot 1 = 1$) $\varphi(5) = 5 - 1 = 4$

$\varphi(6) = 2 = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2$