

Παράδειγμα 1 85-11

$$a \cdot b \equiv 0 \pmod{m} \Rightarrow a \equiv 0 \pmod{m}$$

OXI $m=5$ $a \cdot b \equiv 0 \pmod{5} \Rightarrow$ ή $a \equiv 0 \pmod{5}$ ή $a \neq 0 \pmod{5}$ $\mu\epsilon$ $a \neq b \not\equiv 0 \pmod{5}$
 $b \equiv 0 \pmod{5}$

$$1 \cdot a \equiv 0 \pmod{5}$$

$$2 \cdot a \equiv 0 \pmod{5} \Rightarrow a \equiv 0 \pmod{5} \text{ ή } 2^{-1} \pmod{5}$$

$$\text{ή } 2 \pmod{5} \text{ ή } 2 \equiv 1 \pmod{5}$$

$$3 \cdot 2 \equiv 1 \pmod{5}$$

$$3 \cdot a \equiv 0 \pmod{5} \Rightarrow$$

$$3 \cdot 2a \equiv 3 \cdot 0 \pmod{5} \Rightarrow a \equiv 0 \pmod{5} \text{ (αριθμός και 3 το 2)}$$

$$4 \cdot a \equiv 0 \pmod{5}$$

$$2 \cdot 3a \equiv 2 \cdot 0 \pmod{5} \Rightarrow a \equiv 0 \pmod{5} \text{ (αριθμός και 2 το 3)}$$

$$\Rightarrow 4 \cdot 4a \equiv 4 \cdot 0 \pmod{5} \Rightarrow a \equiv 0 \pmod{5}$$

$$a \cdot b \equiv 0 \pmod{4} \Rightarrow 2 \cdot 2 \equiv 0 \pmod{4}$$

Πρόταση:

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

$$1) a^n \equiv b^n \pmod{m} \text{ ΟΧΙ ΑΝΑΠΟΔΑ } 1^2 \equiv (-1)^2 \pmod{m}$$

$$2) a \pm b \equiv (a \pm b) \pmod{m} \text{ ΝΑΝΤΑ}$$

$$3) a \cdot b \equiv b \cdot a \pmod{m}, 2 \cdot 6 \equiv 6 \cdot 2 \pmod{12}$$

Απόδ. $a \equiv b \pmod{m} \Rightarrow a - b = km$

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

$$a^n - b^n \equiv 0 \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$$

$$2) a - b = km \Rightarrow a \pm b \pm b - b = km \Rightarrow (a \pm b) - (b \pm b) = km \Rightarrow$$

$$(a \pm b) \equiv (b \pm b) \pmod{m}$$

$$3) a \cdot b - b \cdot a = (a - b) \cdot b = km \cdot b \Rightarrow a \cdot b - b \cdot a \equiv 0 \pmod{m} \Rightarrow a \cdot b \equiv b \cdot a \pmod{m}$$

$Z_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$ ορίζεται πράξη και πολ/μο

Η πράξη είναι καλή

Ο πολ/μος (πλευρά προσεγγίζει) είναι καλός ή κακός
αν το m είναι πρώτος ή σύνθετος

Ορισμός: Μια κλάση $[a]_m$ θα λέμε ότι είναι αντιστρέψιμη
ή έχει αντιστροφή, αν υπάρχει κλάση $[b]_m$ ώστε

$$[a]_m \odot [b]_m = [1]_m$$

$$\text{Γράφουμε } a \cdot b \equiv 1 \pmod{m}$$

Προσοχή: Δεν υπάρχει πάντα. Όπως $[2]_4$ δεν έχει

• Πότε έχει:

Πρόταση: Η κλάση $[a]_m$ είναι αντιστρέψιμη απ-ν $(a, m) = 1$

Απόδ.

" $\Leftarrow$ " Έστω $(a, m) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ με $ax + my = 1$

$$ax \pmod{m} + my \pmod{m} = 1 \pmod{m} \Rightarrow ax \equiv 1 \pmod{m}$$

$$\Rightarrow [a]_m^{-1} = [x]_m$$

" $\Rightarrow$ " Έστω ότι υπάρχει b με $[b]_m \odot [a]_m = [1]_m \Leftrightarrow$

$$a \cdot b \equiv 1 \pmod{m} \Leftrightarrow a \cdot b - 1 = km \Leftrightarrow a \cdot b - km = 1 \Leftrightarrow (a, m) = 1$$

Πόρισμα: 1) Έστω $a, b \in \mathbb{Z}$ και $(a, m) = 1$

Αν $a \cdot b \equiv 0 \pmod{m}$, τότε $b \equiv 0 \pmod{m}$

2) Έστω $a, b \in \mathbb{Z}^*$. Αν $a \cdot b \equiv 0 \pmod{m}$, τότε

$$b \equiv 0 \pmod{\frac{m}{(a, m)}}$$

Απόδ

$$1) (a, m) = 1 \Rightarrow \exists [x]_m \text{ με } [a]_m \odot [x]_m = [1]_m$$

$$\begin{aligned} \text{Αρα } a \cdot \beta &\equiv 0 \pmod{m} \Rightarrow \beta \cdot a \equiv \beta \cdot 0 \pmod{m} \Rightarrow \\ &\Rightarrow 1 \cdot \beta \equiv 0 \pmod{m} \Rightarrow \beta \equiv 0 \pmod{m} \end{aligned}$$

$$2) a \cdot \beta \equiv 0 \pmod{m} (\Rightarrow a \cdot \beta = km \Rightarrow \frac{a}{(a, m)} \beta = k \frac{m}{(a, m)})$$

$$\Rightarrow \frac{a}{(a, m)} \beta \equiv 0 \pmod{\frac{m}{(a, m)}} \quad \text{Επειδή } \left(\frac{a}{(a, m)}, \frac{m}{(a, m)} \right) = 1$$

$$\Rightarrow \text{Ανο το προηγούμενο } \beta \equiv 0 \pmod{\frac{m}{(a, m)}}$$

Π.Χ1

Να βρεθούν οι αντιστρέψιμες κλάσεις mod 6

$$[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6$$

$$\begin{matrix} \uparrow \\ \text{oxi} \end{matrix} \quad \text{NAI} \quad \text{oxi} \quad \text{oxi} \quad \text{oxi} \quad \text{NAI}$$

$$(2, 6) = 2, \quad (3, 6) = 3, \quad (4, 6) = 2$$

Π.Χ1

Να βρεθεί οι αντιστρέψιμη κλάση $10 \pmod{33}$

Υπάρχει γιατί $(10, 33) = 1$ Θα τη βρούμε με τον αλγόριθμο του Ευκλείδη

$$\left. \begin{aligned} 33 &= 3 \cdot 10 + 3 \Rightarrow 3 = 33 - 3 \cdot 10 \\ 10 &= 3 \cdot 3 + 1 \Rightarrow 1 = 10 - 3 \cdot 3 \end{aligned} \right\} \Rightarrow L = 10 - 3(33 - 3 \cdot 10) = -3 \cdot 33 + 10 \cdot 10$$

$$\text{Αρα } [10]_{33}^{-1} = [10]_{33}^{-1}$$

Παρατήρηση: Αν a & p είναι πρώτοι, τότε κάθε μη-μηδενική κλάση είναι αντιστρέψιμη.

$$1 \leq a \leq p-1 \Rightarrow (a, p) = 1 \Rightarrow \exists [a]_p^{-1}$$

Ορισμός: Συνάρτηση Euler

$\varphi: \mathbb{N}^+ \rightarrow \mathbb{N}^+$ με $\varphi(n)$ = το πλήθος των αριθμών από το 1 μέχρι το n οι οποίοι είναι πρώτοι με τον n .

Π.χ]

$$\begin{array}{ccccccc} \varphi(1) = 1 & , & \varphi(2) = 1 & , & \varphi(3) = 2 & , & \varphi(4) = 2 & , & \varphi(5) = 4 \\ & & 1, \cancel{2} & & 1, 2, \cancel{3} & & 1, \cancel{2}, 3, \cancel{4} \end{array}$$

► Άρα $\varphi(p) = p - 1$ για p πρώτος.

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

$$1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}$$

$$\varphi(8) = 4, \quad \varphi(2^3) = 2^2 = \varphi(2) \cdot 2^{3-1}$$

$$1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}$$

$$\varphi(9) = 6, \quad \varphi(3^2) = 2 \cdot 3^1$$

$$1, \cancel{2}, \cancel{3}, 4, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}$$

Πρόταση:

1) $\varphi(p) = p - 1$ για p πρώτος

2) $\varphi(p^k) = \varphi(p) p^{k-1}$ για p πρώτος

3) $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$ για p και q πρώτοι

Απόδ

1) Προφανές

2) Να βρεθούν οι αριθμοί y τέτοιοι οι οποίοι είναι πρώτοι με τον p^k

$$(p^k, a) = 1 \Rightarrow a \text{ δεν διαιρείται με το } p$$

$$1 \leq \dots, a \dots \leq p^k$$

Βρες αυτούς που διαιρούνται με το p και από άλλους αγαιρέ τους.

$$\beta = p p', \quad 1 \leq p' \leq p$$

$$p^2 - p = y(p^2)$$

Υπολοι είναι p^2 το οποίο διαιρείται με το p είναι p . Άρα $y(p^2) = p^2 - p$.

Με αναγωγή δείχνουμε:

$$y(p^k) = y(p) p^{k-1}$$

3) $y(p, q)$ p, q πρώτοι
όλοι είναι $p \neq q$

Αν $(p, q) \neq 1 \Rightarrow$ Άρα ο p θα διαιρείται είτε από p είτε από q

$$\left\{ \begin{array}{l} p = p p', \quad 1 \leq p' \leq q \\ p = q p'', \quad 1 \leq p'' \leq p \end{array} \right.$$

$$p \cdot q - q - (p-1) = (p-1)(q-1) = y(p) y(q)$$

Π.χ $p=3 \quad q=11 \quad y(3 \cdot 11)$

$$y(3) = 2 \quad y(11) = 10$$

Να βρούμε αυτούς που διαιρούνται με το 11

Αυτοί που το διαιρούν θα είναι τις μορφής $11p', 1 \leq p' \leq 3$
όμοιος $3p'', 1 \leq p'' \leq 11$

$$3 \cdot 11 - 3 - 10$$

$$= 3(11-1) - 10 = 3(11-1) - (11-1)$$

$$= (3-1)(11-1) = (11-1)(3-1) = 20 = y(11) y(3)$$

Θεωρήμα: Χάρης απόδειξη

Αν m και n θετικοί φυσικοί με $(m, n) = 1$, τότε

$$\varphi(m, n) = \varphi(m) \cdot \varphi(n)$$

Πρόταση: Έστω n οποιαδήποτε αριθμό του n να είναι?

$$n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$$

$$\text{τότε } \varphi(n) = \varphi(p_1) p_1^{k_1-1} \cdot \varphi(p_2) p_2^{k_2-1} \dots \varphi(p_l) p_l^{k_l-1} =$$

$$= (p_1 - 1) p_1^{k_1-1} \cdot (p_2 - 1) p_2^{k_2-1} \dots (p_l - 1) p_l^{k_l-1} = n \prod_{i=1}^l (1 - 1/p_i)$$

Π.Χ (π) $\varphi(2^4 \cdot 3 \cdot 5^2 \cdot 17^{20}) = \varphi(2) \cdot 2^3 \cdot \varphi(3) \cdot 3^0 \cdot \varphi(5) \cdot 5^1 \cdot \varphi(17) \cdot 17^{19}$
 $= 2^3 \cdot 5 \cdot 17^{19} \cdot 2 \cdot 4 \cdot 16$
 $= 2^{3+1+2+4} \cdot 5 \cdot 17^{19} = 2^{10} \cdot 5 \cdot 17^{19}$