ΦΥΛΛΑΔΙΟ 8 - ΑΣΚΗΣΗ 10.

Έστω a, m ακέραιοι με $a \geq 2$ και $m \geq 2$. Θέτουμε $n = a^m - 1$. Δείξτε

(1) $\text{ΜΚΔ}(a, n) = 1$ και $\text{ord}_n(a) = m$

(2) $m \mid \varphi(a^m - 1)$

ΛΥΣΗ

α' τρόπος

(1) $\text{ΜΚΔ}(a, n) = \text{ΜΚΔ}(a, a^m - 1) = \text{ΜΚΔ}(a, a(a^{m-1} - 1) - a^{m-1} \cdot a) = \text{ΜΚΔ}(a, -1) =$

$= \text{ΜΚΔ}(a, 1) = 1.$

β' τρόπος

Υποθέτουμε $\text{ΜΚΔ}(a, n) > 1$. Τότε υπάρχει πρώτος p με $p \mid \text{ΜΚΔ}(a, n) \Rightarrow$

$$\left.\begin{matrix} p \mid a \\ p \mid n \end{matrix}\right\} \Rightarrow \left.\begin{matrix} p \mid a \\ p \mid a^m - 1 \end{matrix}\right\} \Rightarrow p \mid (-1) \text{ αναίρεση}$$

Άρα $\delta.\delta.$ $\text{ord}_n(a) = m$. Έστω $d = \text{ord}_n(a)$

$\delta.\delta.$ $d = m$, ως εξής. Πρώτα $\delta.\delta.$ $([a]_n)^m = [1]_n$ και

μετά θα δείξουμε ότι αν $k \geq 1$ και $([a]_n)^k = [1]_n \Rightarrow m \leq k$

Έχουμε $([a]_n)^m = ([a^m]_n) = [a^m - 1 + 1]_n =$

$= [a^m - 1]_n + [1]_n = [n]_n + [1]_n = [0]_n + [1]_n = [1]_n.$

Έστω $k \geq 1$ με $([a]_n)^k = [1]_n \Rightarrow [a^k]_n = [1]_n \Rightarrow$

$n \mid a^k - 1$. Αφού $a \geq 2$, $k \geq 1 \Rightarrow a^k \geq 2 \Rightarrow a^k - 1 \geq 1$.

Αφού $n > 0$, $a^k - 1 > 0$, $n \mid a^k - 1 \Rightarrow n \leq a^k - 1$.

(Γιατί $x, y \in \mathbb{Z}$, $x, y > 0$, $x \mid y \xrightarrow{\text{προσ}} x \leq y$)

Άρα $a^m - 1 \leq a^k - 1 \Rightarrow a^m \leq a^k \xrightarrow{a \geq 2} m \leq k$

(γιατί για $a \in \mathbb{R}$, $a > 1$, η συνάρτηση $x \to a^x$ είναι γνησίως αύξουσα)

$\mathbb{R} \to \mathbb{R}$.

(ιι) Γενικά, ισχύει αν $n \geq 2$ και $ΜΚΔ(a,n) = 1$
αν $ορδ_n(a) \mid \varphi(n)$ (από προηγούμενη)
Άρα $m \mid \varphi(n) \Rightarrow \varphi(a^m - 1)$

ΠΡΟΒΛΗΜΑ 9 - ΑΣΚΗΣΗ 7.

(α) Δείξτε ότι το 3 είναι πρωτογενής ρίζα mod 17
(β) Έστω $a \in \mathbb{Z}$ με $ΜΚΔ(a,n) = 1$. Υπολογίστε τον ελάχιστο θετικό ακέραιο n ώστε $3^n \equiv a \bmod 17$
(γ) Λύστε για $x \in \mathbb{Z}$ την ισοτιμία $x^4 \equiv 13 \bmod 17$

ΛΥΣΗ

(α) Έχουμε 17 πρώτος, άρα $\varphi(17) = 16$ και $U(\mathbb{Z}_{17}) = \{[1]_{17}, [2]_{17}, [3]_{17}, \ldots, [16]_{17}\}$
Φανερά $ΜΚΔ(3,17) = 1$. Έστω $d = ορδ_{17}(3)$. Από προηγούμενη
$d \mid \varphi(17) = 16 \Rightarrow d \in \{1, 2, 4, 8, 16\}$
Θα δείξουμε $d = 16$. Για αυτό αρκεί νδο $d \notin \{1, 2, 4, 8\}$
Έχουμε $[3]_{17} \neq [1]_{17}$ $[3^2]_{17} = [9]_{17} \neq [1]_{17}$
$[3^4]_{17} = [8]_{17} = [-9]_{17} = [-4]_{17}$
$[3^8]_{17} = [(3^4)^2]_{17} = [(-4)^2]_{17} = [16]_{17} \neq [1]_{17}$
Άρα $d = 16$ και 3 αρχική ρίζα mod 17

ΠΑΡΑΤΗΡΗΣΗ

Δείξαμε $ορδ_{17}(3) = 16 = \varphi(17) = \# U(\mathbb{Z})_{17}$
Άρα $U(\mathbb{Z}_{17}) = \{([3]_{17})^k$, με $1 \leq k \leq 16\}$
Υπολογισμοί mod 17 $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 10 \equiv -7$
$3^4 \equiv 3 \cdot 3^3 \equiv 3 \cdot 10 \equiv 30 \equiv 13 \equiv -4$ $3^5 \equiv 3(-4) \equiv -12 \equiv 5$
$3^6 \equiv 15 \equiv -2$, $3^7 \equiv -6 \equiv 11$ $3^8 \equiv -18 \equiv -1 \equiv 16$, $3^9 \equiv -3 \equiv 14$
$3^{10} \equiv 3 \cdot (-3) \equiv -9 \equiv 8$ $3^{11} \equiv -7$ $3^{12} \equiv 21 \equiv 4$
$3^{13} \equiv 3 \cdot 4 \equiv 12 \equiv -5$, $3^{14} \equiv 3(-5) \equiv -15 \equiv 2$, $3^{15} \equiv 32 \equiv 6$
$3^{16} \equiv 3 \cdot 6 \equiv 1$
Παρατηρούμε αυτό που ζητούσε $U(\mathbb{Z}_{17}) = \{([3]_{17})^k : 1 \leq k \leq 16\}$

(b) Έστω $a \in \mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$. Βρείτε r, το υπόλοιπο της Ευκλ. Διαίρεσης του a με το 17. Τότε $1 \le r \le 16$ και ο ελάχιστος θετ. ακέραιος k με $3^k \equiv a \bmod 17$ είναι ίσος με τον ελάχιστο θετικό ακέραιο k ώστε $3^k \equiv r \bmod 17$ και επαγόμενο από τους υπολοίπους το εξής

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k	16	19	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Παράδειγμα

Αν $a=2019$ ισχύει $\text{ΜΚΔ}(a,17)=1$; Αν ναι, ποιος είναι ο ελάχιστος θετικός ακέραιος k ώστε $3^k \equiv a \bmod 17$;

Ευκλείδια διαίρεση του 2019 με το 17.

$2019 = 118 \cdot 17 + 13$

Άρα $\text{ΜΚΔ}(2019,17) = \text{ΜΚΔ}(13,17)=1$ και από το πινακάκι $k=4$

(c) Θα λύσουμε για $x \in \mathbb{Z}$ την ισοτιμία $x^4 \equiv 13 \bmod 17$

Αφού $\text{ΜΚΔ}(13,17)=1$, αν $x^4 \equiv 13 \bmod 17 \Rightarrow (x^4,17)=1 \Rightarrow (x,17)=1$

Βήμα 1ο Έστω $x \in \mathbb{Z}$ λύση της (*). Τότε $\text{ΜΚΔ}(x,17)=1$

Υπάρχει μοναδικό $y \in \{1,2,\dots,16\}$ ώστε $x \equiv 3^y \bmod 17$

Από τα παραπάνω $13 \equiv 3^4 \bmod 17$.

Άρα (*) $\Leftrightarrow [x^4]_{17} = [13]_{17} < [3^4]_{17} \Rightarrow [(3^y)^4]_{17} = [3^4]_{17} \Leftrightarrow [3^{4y}]_{17} = [3^4]_{17} \Leftrightarrow 3^{4y} \equiv 3^4 \bmod 17 \Leftrightarrow [3^{4y}]_{17} = [3^4]_{17}$

$\Leftrightarrow 3^{4y} \equiv 3^4 \bmod 17 \Leftrightarrow 4y \equiv 4 \bmod \varphi(17) \Leftrightarrow 4y \equiv 4 \bmod 16 \Leftrightarrow$

$y \equiv 1 \bmod 4$

(Από την πρόταση. Αν $\text{ΜΚΔ}(a,y)=1$, $k_1, k_2 \ge 0$, τότε

$a^{k_1} \equiv a^{k_2} \bmod n \Leftrightarrow k_1 \equiv k_2 \bmod \text{ορδ}_n(a)$)