ΑΣΚΗΣΗ

i) Να βρείτε την τάξη του 3 mod 17 και επειτα να γράψετε τα στοιχεία του $\mathbb{Z}_{17}^*$ σαν δυνάμεις του 3

ii) Να βρείτε τους φυσικούς n, ώστε: $7^n \equiv 4 \bmod 17$

iii) ΝΔΟ $2^n + 3^n \not\equiv 0 \bmod 17$, n: περιττος

ΛΥΣΗ

i) Αναζητούμε το $ord_{17}(3)$.

Γενικως, $ord_{17}(3) \mid \varphi(17) = 17-1 = 16$. (αφού $ord_{17}(3) \leq \varphi(17)$)

Πιθανοί διαιρέτες του 16:

1, 2, 4, 8, 16

$3^1 \longrightarrow 3^2 = 9 \longrightarrow 3^4 \equiv 81 \equiv 13 \longrightarrow 3^8 \equiv 13 \cdot 13 \equiv 169 \equiv 16 \longrightarrow$

$\longrightarrow 3^{16} \equiv 16 \cdot 16 \equiv 256 \equiv 1$ (← Αναγκαστικά εφόσον αποτελεί τον τελευταίο διαιρέτη και μαλιστα $3^{16} = 3^{\varphi(17)}$ απο Θ. Euler $3^{\varphi(17)} \equiv 1 \bmod 17$)

Συνεπώς, το 3 αποτελεί πρωταρχική ρίζα του 17

$$\mathbb{Z}_{17}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$$
$$= \{3^0, 3^{14}, 3^1, 3^{12}, 3^5, 3^{15}, 3^{11}, 3^{10}, 3^2, 3^3, 3^7, 3^{13}, 3^4, 3^9, 3^6, 3^8\}$$

ii) Έχουμε, ότι:

$7^n \equiv 4 \bmod 17$

Αλλά, απο (i) έχουμε: $\begin{cases} 7 \equiv 3^{11} \bmod 17 \\ 4 \equiv 3^{12} \bmod 17 \end{cases}$

Άρα, $3^{11n} \equiv 3^{12} \bmod 17 \overset{ord_{17}(3)=16}{\Longrightarrow} 11n \equiv 12 \bmod 16 \overset{(11,16)=1}{\Rightarrow}$

$\Rightarrow 11^{-1} \cdot 11n \equiv 12 \cdot 11^{-1} \bmod 16 \Rightarrow n = 12 \cdot 11^{-1} \bmod 16$ (1)

Αρκεί, να βρούμε το $11^{-1} \bmod 16$.

$16 = 1 \cdot 11 + 5$

$11 = 2 \cdot 5 + 1 \Rightarrow 1 = 11 - 2 \cdot 5 = 11 - 2(16-11) = 3 \cdot 11 - 2 \cdot 16$

$\Rightarrow 1 \bmod 16 \equiv 3 \cdot 11 \bmod 16 \Rightarrow$

$\Rightarrow 1 \equiv 3 \cdot 11 \bmod 16 \Rightarrow 11^{-1} \equiv 3 \bmod 16$

Άρα, η (1) είναι:

$n \equiv 12 \cdot 3 \bmod 16 \equiv 4 \bmod 16 \Rightarrow n = 16k + 4, k \in \mathbb{N}$

iii) Έστω ότι υπάρχει

$2^n + 3^n \equiv 0 \bmod 17 \Rightarrow 2^n \equiv -3^n \bmod 17 \xRightarrow{n \text{ περιττός}}$

$\Rightarrow 2^n \equiv (-3)^n \bmod 17. \quad (1)'$

Επίσης, $2 \equiv 3^{14} \bmod 17$ (← Από το ερωτ. (i))

Έτσι, $2^n \equiv 3^{14n} \bmod 17$ → $(-1 \equiv 16 \bmod 17)$

Επίσης, $-3^n \equiv -1 \cdot 3^n \equiv 3^8 \cdot 3^n \equiv 3^{8+n} \bmod 17$

Συνεπώς, (1)' θα είναι:

$3^{14n} \equiv 3^{8+n} \bmod 17 \Rightarrow 14n \equiv (8+n) \bmod 16.$

$\Rightarrow 13n \equiv 8 \bmod 16 \Big| \Rightarrow n \equiv 8 \cdot 13^{-1} \bmod 16. \quad (2)$

$(13, 16) = 1$

όπου από ευκλείδειο αλγόριθμο βρίσκουμε ότι $13^{-1} \equiv 5 \bmod 16$

Άρα, (2) είναι:

$n = 8 \cdot 5 \bmod 16 \equiv 8 \bmod 16 \Rightarrow n = 16k' + 8, k' \in \mathbb{N}$

Αυτό, είναι Άτοπο διότι n: περιττός