Φυλ 8 ασκ 7. Βρείτε τις τάξεις mod 16 των 3, 5, 7, 9

<u>Λύση</u>: $16 = 2^4$, άρα $\phi(16) = 2^4(1 - \frac{1}{2}) = 2^3 = 8$

Άρα αν $a \in \mathbb{Z}$ με $\text{ΜΚΔ}(a,16) = 1$, $\text{ord}([a]_{16}) \in \{1, 2, 4, 8\}$

$$[3]_{16} \neq [1]_{16} \qquad [3^2]_{16} = [9]_{16} \neq [1]_{16}$$

$$([3]_{16})^4 = ([9]_{16})^4 = ([-7]_{16})^2 = [(-7)^2]_{16} = [1]_{16}$$

Άρα $\text{ord}([3]_{16}) = 4$

Παρόμοια για τα 5, 7, 9

Φυλ 8 ασκ 9. Έστω $n \geq 2$ κ' $a, b \in \mathbb{Z}$ με $ab \equiv 1 \mod n$

Δ.ο. $\text{ΜΚΔ}(a,n) = 1$, $\text{ord}([a]_n) = \text{ord}([b]_n)$

Παρατήρηση: Ορίζουμε $\text{ord}_n(a) = \text{ord}([a]_n)$

(Ισχύει γενικά αν $u \in U(\mathbb{Z}/n)$, τότε $\text{ord}(u) = \text{ord}(u^{-1})$ όπου $u^{-1} \in U(\mathbb{Z}/n)$ ο αντίστροφος του u)

<u>Λύση</u>: $ab \equiv 1 \mod n \Rightarrow [a]_n[b]_n = [1]_n$

$\Rightarrow [a]_n \in U(\mathbb{Z}/n)$ κ' $[b]_n \in U(\mathbb{Z}/n) \xRightarrow[\text{πρόταση}]{} \text{ΜΚΔ}(a,n) = \text{ΜΚΔ}(b,n) = 1$

Έστω $d_1 = \text{ord}([a]_n)$, $d_2 = \text{ord}([b]_n)$

Έχουμε $([a]_n)^{d_1} = [1]_n \Rightarrow [a]_n^{d_1}([b]_n)^{d_1} = [1]_n([b]_n)^{d_1}$

$\Rightarrow ([ab]_n)^{d_1} = ([b]_n)^{d_1} \Rightarrow ([1]_n)^{d_1} = [b^{d_1}]_n \Rightarrow ([b]_n)^{d_1} = [1]_n$

Συνεπώς $d_2 \leq d_1$

Επίσης $([b]_n)^{d_2} = [1]_n \Rightarrow ([a]_n)^{d_2}([b]_n)^{d_2} = ([a]_n)^{d_2}[1]_n$

$\Rightarrow ([ab]_n)^{d_2} = ([a]_n)^{d_2} \Rightarrow ([a]_n)^{d_2} = [1]_n \Rightarrow d_1 \leq d_2$

Άρα $d_1 = d_2$

<u>Πρόταση</u>: Έστω $n \geq 2$, $a \in \mathbb{Z}$ με $\text{ΜΚΔ}(a,n) = 1$ κ' $k \geq 1$ ακέραιος. Έστω $d = \text{ord}_n(a)$ η τάξη του a modulo n. Τότε $\text{ΜΚΔ}(a^k, n) = 1$ κ'

$$\text{ord}_n(a^k) = \frac{d}{\text{ΜΚΔ}(d,k)}$$

Απόδειξη: Θέλουμε πρώτα ότι $ΜΚΔ(a^k, n) = 1$. Έστω ότι δεν ισχύει. Τότε $ΜΚΔ(a^k,n) \geq 2$, άρα $\exists$ πρώτος p με $p|a^k$ κ' $p|n$. Αφού $k \geq 1$ κ' p πρώτος, από $p|a^k \Rightarrow p|a$. Συνεπώς, $p|a$ κ' $p|n$, άρα $ΜΚΔ(a,n) \neq 1$, αντίφαση.

Θέτουμε $e = \dfrac{d}{ΜΚΔ(d,k)}$ (*)

Αρκεί νδο $(a^k)^e \equiv 1 \bmod n$ κ' ότι αν $f \geq 1$ κ' $(a^k)^f \equiv 1 \bmod n$, τότε $e \leq f$.

Ισχυρισμός 1: $(a^k)^e \equiv 1 \bmod n$

Απόδειξη: Αρκεί νδο $d | ke$. Έχουμε από (*)

$$d = e \cdot ΜΚΔ(d,k). \text{ Αφού } \left.\begin{array}{l} e|e \\ ΜΚΔ(d,k)|k \end{array}\right\} \Rightarrow d = e\,ΜΚΔ(d,k) \,|\, ek.$$

Ισχυρισμός 2: Έστω $f \geq 1$ με $(a^k)^f \equiv 1 \bmod n$. Τότε $e \leq f$.

Απόδειξη: $(a^k)^f \equiv 1 \bmod n \Rightarrow a^{kf} \equiv 1 \bmod n$ κ' αφού d η τάξη του $a \bmod n$, έπεται $d | kf$

$$\Rightarrow \frac{d}{ΜΚΔ(d,k)} \,\Big|\, \frac{k}{ΜΚΔ(d,k)} f \Rightarrow e|f \underset{\substack{f \neq 0 \\ e,f \geq 1}}{\Longrightarrow} e \leq f$$

Πρόταση: Έστω $n \geq 2$, $a \in \mathbb{Z}$ με $ΜΚΔ(a,n) = 1$ κ' $d = ord_n(a)$. Αν $g \geq 1$ κ' $a^g \equiv 1 \bmod n$, τότε $d|g$

Απόδειξη: Έστω ότι δεν ισχύει. Τότε $\exists\, q, r$ με $r > 0$ κ' $q \geq 0$ ώστε $g = qd + r$. Συνεπώς αφού $([a]_n)^d = [1]_n$, έπεται

$([a]_n)^g = ([a^{qd}]_n)[a^r]_n \Rightarrow [a^r]_n = 1$. Άρα $a^r \equiv 1 \bmod n$

κ' αφού $1 \leq r \leq d-1$, έχουμε αντίφαση στο $d = ord([a]_n)$

Πρόταση: Έστω $n \geq 2$, $a \in \mathbb{Z}$ με $ΜΚΔ(a,n) = 1$ κ' $d = ord([a]_n)$. Έστω $k \geq 1$ κ' r το υπόλοιπο της Ευκλ. Διαίρ. του k με το d.

Τότε $[a^k]_n=[a^r]_n$

Απόδειξη: $\exists f\in\mathbb{Z}, f\geq 0$ ώστε $k=fd+r$, άρα

$$[a^k]_n=[a^{fd+r}]_n=[a^{fd}]_n[a^r]=([a^d]_n)^f[a^r]_n=$$
$$=[1]_n[a^r]_n=[a^r]_n$$

π.χ. Έστω $n\geq 2$, $a\in\mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$. Υποθέτουμε $ord([a]_n)=12$.
Υπολογίστε τις τιμές:
$ord([a^2])_n$, $ord([a^3]_n)$, $ord([a^4])_n$, $ord([a^5]_n)$

Λύση. Από πρόταση $ord([a^k]_n)=\dfrac{12}{\text{ΜΚΔ}(12,k)}$

Άρα για $k=2$ $ord([a^2]_n)=\dfrac{12}{\text{ΜΚΔ}(12,2)}=\dfrac{12}{2}=6.$

$$ord([a^3]_n)=\frac{12}{\text{ΜΚΔ}(12,3)}=\frac{12}{3}=4$$

$$ord([a^4]_n)=\frac{12}{\text{ΜΚΔ}(12,4)}=\frac{12}{4}=3$$

$$ord([a^5]_n)=\frac{12}{\text{ΜΚΔ}(12,5)}=\frac{12}{1}=12$$

Παρατήρηση: (Σε απόδειξη σχ. 2)

$$d\mid kf \Rightarrow \frac{d}{\text{ΜΚΔ}(d,k)} \,\Big|\, \frac{k}{\text{ΜΚΔ}(d,k)}f \quad (*)$$

Από πρόταση $\text{ΜΚΔ}\left(\dfrac{d}{\text{ΜΚΔ}(d,k)}, \dfrac{k}{\text{ΜΚΔ}(d,k)}\right)=1$

Άρα από πρόταση, $(*)\Rightarrow \dfrac{d}{\text{ΜΚΔ}(d,k)}\,\Big|\, f$

Παρατήρηση: Έστω $n\geq 2$ κ' $a\in\mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$ κ' $d=ord_n(a)$. Από τις παραπάνω προτάσεις έχουμε $[a]_n, [a^2]_n, \ldots, [a^{d-1}]_n, [a^d]_n=[1]_n$ κ' είναι διαφορετικά ανά δύο στοιχεία του $\mathbb{Z}_n$.
Επίσης, $[a^{d+1}]_n=[a]_n$, $[a^{d+2}]_n=[a^2]_n$, ..., $[a^{d+(d-1)}]_n=[a^{d-1}]_n$
$[a^{2d+1}]_n=[a]_n$, $[a^{2d+2}]_n=[a^2]_n$ κλπ

$[a^{d+d}]_n=[1]_n$

Γεν. αν $k\geq 1$ κ' $1\leq r\leq d$. $[a^{kd+r}]_n=[a^r]_n$

π.χ. $n=5$, $a=2$. Τότε $[a]_5 \neq [1]_5$, $[a^2]_5 = [4]_5 \neq [1]_5$

κ' έχουμε $ord_5(2)=4$ $\quad [a^3]_5=[8]_5=[3]_5$, $[a^4]_5=[1]_5$

κ' $[a^1]_5=[2]_5$, $[a^2]_5=[4]_5$, $[a^3]_5=[3]_5$, $[a^4]_5=[1]_5$

$[a^5]_5=[2]_5$, $[a^6]_5=[4]_5$, $[a^7]_5=[3]_5$, $[a^8]_5=[1]_5$

$[a^9]_5=[2]_5$, $[a^{10}]_5=[4]_5$, $[a^{11}]_5=[3]_5$, $[a^{12}]_5=[1]_5$

$[a^{13}]_5=[2]_5$...

Έστω ότι θέλουμε να υπολογίσουμε το $[a^{2019}]_n$ για $a=2$, $n=5$

Βήμα 1ο: Από τα παραπάνω $ord_5(2)=4$.

Βήμα 2ο: Ευκλ. Διαίρ. του 2019 με την $ord_5(2)$, δηλ. το 4.

Έχουμε $2019=504\cdot 4+3$.

$$\begin{array}{r|l} 2019 & 4 \\ \hline 019 & 504 \end{array}$$

Άρα $[2^{2019}]_5=[2^3]_5=[8]_5=[3]_5$

Ορισμός: Έστω $n\geq 2$ κ' $a\in\mathbb{Z}$ με $ΜΚΔ(a,n)=1$.
Το a λέγεται ΑΡΧΙΚΗ ΡΙΖΑ modulo n
(ή πρωταρχική ρίζα modulo n)
αν $ord_n(a)=\phi(n)$

π.χ. Αν $n=5$, $a=2$ έχουμε $\phi(5)=4$ κ' υπολογίσαμε στο προηγούμενο π.χ. ότι $ord_5(2)=4$. Άρα 2 πρωταρχική ρίζα modulo 5. (γιατί $ord_5(2)=\phi(5)$)

Έστω τώρα $n=5$ κ' $b=4$. Είναι το b αρχική ρίζα modulo 5;

ΟΧΙ, γιατί $[4]_5\neq[1]_5$, αλλά $([4]_5)^2=[16]_5=[1]_5$
Συνεπώς $ord_5(4)=2\neq\phi(5)=4$

π.χ. Έστω $n=8$, άρα $\phi(n)=8(1-\frac{1}{2})=4$
Την προηγούμενη φορά υπολογίσαμε το $U(\mathbb{Z}/8)$ κ' τις τάξεις όλων των στοιχείων του κ' βρήκαμε ότι ποτέ η τάξη δεν είναι 4.
Συνεπώς, δεν $\exists$ αρχικές ρίζες modulo 8

δηλαδή $\forall \alpha \in \mathbb{Z}$ με $ΜΚΔ(\alpha, 8) = 1$, έχουμε $ord_8(\alpha) \neq \phi(8)$

Ερώτημα: Για ποια $n \geq 2$ $\exists$ αρχικές ρίζες modulo n;
Δηλαδή για ποια $n \geq 2$ $\exists \alpha \in \mathbb{Z}$ με $ΜΚΔ(\alpha, n) = 1$ κ' $ord_n(\alpha) = \phi(n)$;

Θεώρημα: (χωρίς απόδειξη).
Έστω $n \geq 2$. Τότε $\exists$ αρχική ρίζα modulo n αν $n=2, n=4, n=p^a$, p περιττός, $a \geq 1$ ή $n = 2p^a$, p περιττός πρώτος, $a \geq 1$.

π.χ 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 2
ΝΑΙ, Ν, Ν, Ν, Ν, Ν, Ο, Ν, Ν, Ν, Ο, Ν, Ν, Ο, Ο, Ν, Ν, Ν, Ο, Ο, Ν, Ν, Ο, Ν

Το τέλος 16/12/19

Άσκηση $\boxed{\text{ΘΕΜΑΤΑ 2018}}$
Βρείτε το μικρότερο φυσικό > του 4.000 που είναι λύση του συστήματος γραμμικών ισοτιμιών.

$$(Σ)\begin{cases} x \equiv -3 \bmod 11 \\ -2x \equiv 7 \bmod 23 \\ 6x \equiv 15 \bmod 45 \end{cases}$$

Λύση $\boxed{\text{Βήμα 1º}}$: $-2x \equiv 7 \bmod 23$. Μέσω της πράξης $([-2]_{23})^{-1} = [11]_{23}$
Άρα ισοδύναμη με $(11)(-2x) = (7 \cdot 11) \bmod 23$
$\Rightarrow x = 77 \bmod 23 \Leftrightarrow x = 8 \bmod 23$ (γιατί $77 = 3 \cdot 23 + 8$)

$\boxed{\text{Βήμα 2º}}$: $6x = 15 \bmod 45$: Έχουμε $ΜΚΔ(6,45) = 3 \mid 15$.
Συνεπώς, ισοδύναμη με $\frac{6}{3}x \equiv \frac{15}{3} \bmod \frac{45}{3}$, δηλαδή $2x \equiv 5 \bmod 15$.

Έχουμε $([2]_{15})^{-1} = [8]_{15}$
Άρα ισοδύναμα με $8 \cdot 2x \equiv 8 \cdot 5 \bmod 15$, δηλαδή $x \equiv 40 \bmod 15$, ισοδύναμα
$x \equiv 10 \bmod 15$

$\rightarrow$ Συνεπώς, το $(Σ)$ έχει τις ίδιες λύσεις με το

$$(\varepsilon')\ \begin{cases} x\equiv -3 \bmod 11 \\ x\equiv 8 \bmod 23 \\ x\equiv 10 \bmod 15 \end{cases}$$

Θέτουμε $n_1=11, n_2=23, n_3=15$

Φανερά $\text{ΜΚΔ}(n_i,n_j)=1=1$ για $i\neq j$

Θέτουμε $N=n_1\cdot n_2\cdot n_3=11\cdot 23\cdot 15=3795$

$N_1=\frac{N}{n_1}=345$. $N_2=\frac{N}{n_2}=165$. $N_3=\frac{N}{n_3}=253$

Υπολογίζουμε $b_1,b_2,b_3\in\mathbb{Z}$ με $b_iN_i\equiv 1 \bmod n_i$. για $i=1,2,3$

→ Μετά τις πράξεις μπορούμε να πάρουμε $b_1=3, b_2=6, b_3=7$. Επομένως, από το Θεώρημα, το σύνολο λύσεων του (ε'), άρα κ' του (ε) είναι το εξής:

$$S=\{(-3)N_1b_1+8N_2b_2+10N_3b_3+t\cdot N \mid t\in\mathbb{Z}\}$$
$$=\{(-3)\cdot 345\cdot 3+8\cdot 165\cdot 6+10\cdot 253\cdot 7+t\cdot 3795 \mid t\in\mathbb{Z}\}$$
$$=\{22525+t\, 3795 \mid t\in\mathbb{Z}\}$$

Θέλουμε $22525+t\cdot 3795>4000 \Rightarrow 3795t>4000-22525\Rightarrow$

$$t>\frac{4000-22525}{3795}\simeq -4{,}8$$

Επομένως, για $t=-4$ που είναι ο ελάχιστος ακέραιος $\geq -4{,}8$ έχουμε τη λύση 7345 που είναι η ζητούμενη.

<u>ΠΑΡΑΤΗΡΗΣΗ</u>: Έστω $m\geq 2$ ακέραιος. Λέμε ότι ο m διαιρείται από τετράγωνο ακεραίου >1, αν $\exists n\in\mathbb{Z}$ με $n\geq 2$ ώστε $n^2|m$

Φανερά, αν $m=p_1^{a_1}\cdots p_r^{a_r}$ η πρωταρχική ανάλυση του m, ο m διαιρείται από τετράγωνο ακεραίου >1, αν $\exists a_i$ με $a_i\geq 2$

$\boxed{\text{π.χ.}}$ Οι $4=2^2, 8=2^3, 9=3^2, 12=2^2\cdot 3$ διαιρούνται από τετράγωνο ακεραίου >1