Φυλ 8 ασκ 2

Έστω $k \geq 2$. Δ.ο. $\exists$ k το πλήθος διαδοχικοί ακέραιοι ≥ 2, κάθε ένας από τους οποίους διαιρείται από τετράγωνο ακεραίου >1.

Λύση: Έχουμε δει ότι το σύνολο των πρώτων είναι άπειρο. Έστω $p_1, \dots, p_k$ k διακεκριμένοι πρώτοι (δηλ. $p_i \neq p_j$) για $i \neq j$

Θεωρούμε το σύστημα

$$\begin{cases} x \equiv 0 \bmod p_1^2 \\ x \equiv -1 \bmod p_2^2 \\ x \equiv -2 \bmod p_3^2 \\ x \equiv -(k-1) \bmod p_k^2 \end{cases}$$

Αφού για $i \neq j$ πρώτοι με $p_i \neq p_j$, έχουμε $\text{ΜΚΔ}(p_i^2, p_j^2)=1$. Συνεπώς από το Κινέζικο Θεώρημα Υπολοίπων το σύστημα έχει λύση στο $\mathbb{Z}$ και μάλιστα $\exists$ λύση x με $x \geq 2$

→ Τότε $x \equiv 0 \bmod p_1^2 \Rightarrow p_1^2 \mid x$

$x \equiv -1 \bmod p_2^2 \Rightarrow p_2^2 \mid x+1$

$x \equiv -2 \bmod p_3^2 \Rightarrow p_3^2 \mid x+2$

$x \equiv -3 \bmod p_4^2 \Rightarrow p_4^2 \mid x+3$

$\vdots$

$x \equiv -(k-1) \bmod p_k^2 \Rightarrow p_k^2 \mid x+(k-1)$

- Συνεπώς, κάθε ένας από τους k διαδοχικούς ακεραίους $x, x+1, x+2, \dots, x+(k-1)$ διαιρείται από τετράγωνο ακεραίου >1

- Συνεπώς, κανένας από τους $x, x+1, \dots, x+(k-1)$ δεν είναι πρώτος. Άρα δείξαμε.

Πρόταση: Έστω $k \geq 2$. Τότε $\exists$ k διαδοχικοί ακέραιοι $x, x+1, \dots, x+k-1$ με την ιδιότητα κανένας από αυτούς δεν είναι πρώτος, δηλαδή όλοι είναι σύνθετοι

Απόδειξη: $(x=(k+1)!+2$. Τότε $2 \mid x, 3 \mid x+1, 4 \mid x+2, \dots)$

ΤΑΞΗ ΣΤΟΙΧΕΙΟΥ ΤΟΥ $U(\mathbb{Z}/n)$

Υπενθύμιση: Έστω $n\geq 1$ κ' $a,b\in\mathbb{Z}$ με $a\equiv b \bmod n$. Τότε $a^2\equiv b^2 \bmod n$, $a^3\equiv b^3 \bmod n$ κ' γενικά $a^k\equiv b^k \bmod n$. Για κάθε $k\geq 1$.

Υπενθύμιση: (Θ Euler-Fermat) Έστω $n\geq 1$ ακέραιος κ' $a\in\mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$. Τότε $a^{\phi(n)}\equiv 1 \bmod n$

Ορισμός: Έστω $n\geq 1$ κ' $a\in\mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$. Θέτουμε $L=\{k\in\mathbb{N} : a^k\equiv 1 \bmod n\}$. Από υπενθύμιση $\phi(n)\in L$ άρα $L\neq\emptyset$. Συνεπώς, $\exists$ ελάχιστο στοιχείο του L, που το συμβολίζουμε $\text{ord}[a]_n$ κ' το λέμε τάξη του a modulo n

ΠΑΡΑΤΗΡΗΣΗ: Από υπενθύμιση αν $a,b\in\mathbb{Z}$ με $a\equiv b \bmod n$, τότε για $k\geq 1$ $a^k\equiv 1 \bmod n$, ανν $b^k\equiv 1 \bmod n$. Άρα $\text{ord}([b]_n)=\text{ord}([a]_n)$

Συνεπώς, έχει νόημα να αναφερόμαστε κ' στην τάξη του $[a]_n\in U(\mathbb{Z}/n)$ που εξ' ορισμού είναι η τάξη το a modulo n.

Π.χ. $n=5$, $a=4$. Υπολόγισε την $\text{ord}([4]_5)$

Λύση: Αφού $\text{ΜΚΔ}(4,5)=1$, η $\text{ord}([4]_5)$ ορίζεται

Έχουμε $([4]_5)^1=[4]_5\neq[1]_5$

$([4]_5)^2=[16]_5=[1]_5$

Άρα $\text{ord}([4]_5)=2$

Π.χ. $n=6$. Υπολόγισε το $U(\mathbb{Z}/6)$ κ' τις τάξεις των στοιχείων του

Λύση: Έχουμε $U(\mathbb{Z}/6)=\{[1]_6,[5]_6\}$

Φανερά, $\text{ord}([1]_6)=1$

$([5]_6)^1\neq[1]_6$.

$([5]_6)^2=[25]_6=[1]_6$

Άρα $\text{ord}([5]_6)=2$

Πχ $n=8$. Υπολόγισε το $U(\mathbb{Z}/8)$ κ' τις τάξεις των στοιχείων του

$U(\mathbb{Z}/8)=\{[1]_8,[3]_8,[5]_8,[7]_8\}$ $\text{οτd}([1]_8)=1$

Έχουμε $([3]_8)^2=[1]_8$, άρα $\text{οτd}([3]_8)=2$

Επίσης, $([5]_8)^2=[1]_8$, άρα $\text{οτd}([5]_8)=2$

Επιπλέον $[7]_8=[-1]_8$, άρα $([7]_8)^2=([-1]_8)^2=[1]_8$

Συνεπώς, $\text{οτd}([7]_8)=2$

ΠΑΡΑΤΗΡΗΣΗ $\#U(\mathbb{Z}/8)=\phi(8)=4$, αλλά το $U(\mathbb{Z}/8)$ δεν έχει στοιχείο τάξης $\phi(8)$ από τον παραπάνω υπολογισμό

Πρόταση: Έστω $n\geq 1$. Τότε $[1]_n\in U(\mathbb{Z}/n)$ κ' $\text{οτd}([1]_n)=1$

Απόδειξη: $\text{ΜΚΔ}(1,n)=1$, άρα $[1]_n\in U(\mathbb{Z}/n)$.
Αφού $([1]_n)^1=[1]_n$, άρα $\text{οτd}([1]_n)=1$

Πρόταση: Έστω $n\geq 3$. Τότε $\text{οτd}([n-1]_n)=\text{οτd}([-1]_n)=2$

Απόδειξη: Αφού $n-1\equiv -1 \bmod n$ έχουμε $\text{οτd}([n-1]_n)=\text{οτd}([-1]_n)$
Έχουμε $([-1]_n)^1=[-1]_n\neq[1]_n$, γιατί $n\geq 3$, άρα $n\nmid 2$

Επιπλέον $([-1]_n)^2=[1]_n$. Άρα $\text{οτd}([-1]_n)=2$

Πρόταση: Έστω $n\geq 2$ κ' $a\in\mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1$, τότε $\text{οτd}([a]_n)\mid\phi(n)$

Απόδειξη: Έστω ότι δεν ισχύει. Αφού $\text{οτd}([a]_n)\leq\phi(n)$ έχουμε $\text{οτd}([a]_n)<\phi(n)$
Από Ευκλείδεια Διαίρεση υπάρχουν $q\geq 1$ κ' r με $1\leq r\leq \text{οτd}([a]_n)-1$, ώστε $\phi(n)=q\cdot\text{οτd}([a]_n)+r$

Συνεπώς $([a]_n)^{\phi(n)}=([a]_n)^{q\,\text{οτd}([a]_n)+r}$

$\longrightarrow [a^{\phi(n)}]_n=[a^{q\cdot\text{οτd}([a]_n)}]_n[a^r]_n$

Euler → Fermat $[1]_n = \left([a]_n^{ord([a]_n)}\right)^q [a^r]_n \Rightarrow [1]_n = ([1]_n)^q [a^r]_n \Rightarrow$

$[a^r]_n = [1]_n \Rightarrow a^r \equiv 1 \mod n$ (αντίφαση, γιατί $1 \le r \le (ord([a]_n)-1)$)

(Π.χ.) Έστω $n \in \mathbb{N}$ με $\phi(n) = 10$ κ' $a \in \mathbb{Z}$ με ΜΚΔ$(a,n) = 1$. Το σύνολο των θετικών διαιρετών του $10 = 2^1 \cdot 5^1$ είναι $\{1, 2, 5, 10\}$. Συνεπώς, $ord([a]_n) \in \{1, 2, 5, 10\}$

(Π.χ.) Βρείτε την τάξη του $[7]_{11}$

Λύση: Αφού 11 πρώτος, $\phi(11) = 11 - 1 = 10$. Φανερά ΜΚΔ$(7,11) = 1$, άρα η τάξη $[7]_{11}$ ορίζεται. Από προηγούμενο π.χ. $ord([7]_{11}) \in \{1, 2, 5, 10\}$

$[7]_{11} \neq [1]_{11}$, άρα $ord([7]_{11}) \neq 1$

$([7]_{11})^2 = [49]_{11} = [5]_{11} \neq [1]_{11}$, άρα $ord([7]_{11}) \neq 2$.
$([7]_{11})^4 = ([7^2]_{11})^2 = ([5]_{11})^2 = [25]_{11} = [3]_{11}$
άρα $([7]_{11})^5 = ([7]_{11})^4 \cdot [7]_{11} = [3]_{11}[7]_{11} = [21]_{11}$
$= [10]_{11} \neq [1]_{11}$. Άρα $ord([7]_{11}) \neq 5$.
Συνεπώς, $ord([7]_{11}) = 10$