Υπενθύμιση: Έστω $n \geq 2$ κ' $a \in \mathbb{Z}$ με $ΜΚΔ(a,n)=1$. Ο $ord_n(a)$ = ο ελάχιστος θετικός ακέραιος k ώστε $a^k \equiv 1 \bmod n$.

Δείξαμε ότι $ord_n(a) \mid \phi(n)$

Δείξαμε ότι αν $a \equiv b \bmod n$, τότε $ord_n(a) = ord_n(b)$.

Άρα ορίζεται κ' η τάξη (modulo n) στοιχείων του $U(\mathbb{Z}/n)$ κ' ισχύει $ord([a]_n) = ord_n(a)$

Δείξαμε ότι αν $l>0$ $ord_n(a^l) = \dfrac{d}{ΜΚΔ(l,d)}$, όπου $d = ord_n(a)$

Για αν $ΜΚΔ(l,d)=1$, $ord_n(a^l) = ord_n(a)$, ενώ αν $ΜΚΔ(l,d)>1$, $ord_n(a^l) < ord_n(a)$

Υπενθύμιση: Ο a (με $ΜΚΔ(a,n)=1$) λέγεται ΑΡΧΙΚΗ Ή ΠΡΩΤΑΡΧΙΚΗ ΡΙΖΑ modulo n αν $ord_n(a) = \phi(n)$

(Πχ) $n=3, a=2$, τότε $ΜΚΔ(a,n)=1$
$\phi(n)=\phi(3)=3(1-\frac{1}{3})=2$ κ' $ord_n(a)=ord_3(2)=2=\phi(n)$
Συνεπώς το $a=2$ είναι αρχική ρίζα mod 3

(Πχ) $n=8, a=7$ τότε $ΜΚΔ(a,n)=ΜΚΔ(7,8)=1$
$\phi(n)=\phi(8)=\phi(2^3)=2^3(1-\frac{1}{2})=\frac{2^3}{2}=2^2=4$
Έχουμε $7^2=49\equiv 1 \mod 8$ Συνεπώς, $ord_8(7)=2$
κ' $2\neq\phi(n)$ Άρα το a όχι αρχική ρίζα mod 8

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

(Πχ) $\nexists$ αρχικές ρίζες modulo 8 ενώ υπάρχουν modulo 11^{2020} από το θεώρημα.
Επίσης υπάρχουν modulo $2\cdot 11^{2020}$, ενώ δεν υπάρχουν modulo $4\cdot 11^{2020}$

Πρόταση: Έστω $n\geq 2$ κ' ικανοποιεί το θεώρημα κ' $a\in\mathbb{Z}$ με $ΜΚΔ(a,n)=1$ αρχική ρίζα modulo n. Τότε:
1
τα στοιχεία $\{a^k : 1\leq k\leq\phi(n)$ κ' $ΜΚΔ(k,\phi(n))\}$ είναι αρχικές ρίζες modulo n. Είναι ανά δύο ασύμβατα modulo n κ' αν b αρχική ρίζα modulo n, $\exists$ μοναδικό k με $1\leq k\leq\phi(n)$ κ' $ΜΚΔ(k,\phi(n))=1$, ώστε $[b]_n=[a^k]_n$. Σαν συνέπεια, υπάρχουν ακριβώς $\phi(\phi(n))$ αρχικές ρίζες modulo n ασύμβατες modulo n ανά 2

Απόδειξη: Έχουμε $\#U(\mathbb{Z}/n)=\phi(n)$ κ' $ord[a]_n=ord_n(a)=\phi(n)$
Συνεπώς, από προτάσεις $U(\mathbb{Z}/n)=\{a^k : 1\leq k\leq\phi(n)\}$.
Από πρόταση, $ord(a^k)=\frac{\phi(n)}{ΜΚΔ(k,\phi(n))}$

Συνεπώς, $ord[a^k]_n=\phi(n)$ αν $ΜΚΔ(k,\phi(n))=1$. Από αυτό προκύπτουν οι ισχυρισμοί

(Πχ) Έστω $n=11$ Βρείτε όλες τις αρχικές ρίζες modulo 11
Βήμα 1º: Υπολογίζουμε (με δοκιμές) μια αρχική ρίζα modulo 11
Για το $[2]_n=[2]_{11}$ Έχουμε $ΜΚΔ(2,11)=1$
$\phi(11)=11(1-\frac{1}{11})=10$ με σύνολο διαιρετών του $\phi(11)$ το $S=\{1,2,5,10\}$

Άρα $ord[2]_{11} \notin S$. Έχουμε $[2^2]_{11} = [4]_{11} \neq [1]_{11}$

$[2^4]_{11} = ([16]_{11}) = [5]_{11} \neq [1]_{11}$, άρα
$[2^5]_{11} = [2^4]_{11}[2]_{11} = [5]_{11}[2]_{11} = [10]_{11} \neq [1]_{11}$

Συνεπώς, αφού $ord[2]_{11} \in S$ κ' $ord([2]_{11}) \neq 1, 2, 5$ έπεται $ord[2]_{11} = 10 = \phi(11)$.
Συνεπώς, το 2 είναι αρχική ρίζα (modulo 11)

Βήμα 2ο: Υπολογίζουμε τα κ με $1 \leq \kappa \leq \overset{10}{\phi(11)}$ κ' ΜΚΔ$(\kappa, \phi(11))$
Αυτοί είναι $\kappa = 1, \kappa = 3, \kappa = 7, \kappa = 9$

Βήμα 3ο: Υπολογίζουμε $[2^1]_{11} = [2]_{11}$
$[2^3]_{11} = [8]_{11}$, $[2^7]_{11} = [2^4]_{11}[2^3]_{11} = [5]_{11}[-3]_{11} = [-15]_{11} = [-4]_{11} = [7]_{11}$
$[2^9]_{11} = [2^7]_{11}[2^2]_{11} = [7]_{11}[4]_{11} = [28]_{11} = [6]_{11}$

Συνεπώς, από την πρόταση οι αρχικές ρίζες mod 11 είναι οι 2, 8, 7, 6 καθώς κ' κάθε ακέραιος b με $[b]_{11} \in \{[2]_{11}, [6]_{11}, [7]_{11}, [8]_{11}\}$

ΑΣΚΗΣΗ (ΘΕΜΑ 2018)

Ν.δ.ο. 41 είναι πρώτος. Ν.δ.ο. ο 6 είναι αρχική ρίζα modulo 41
(i) Βρείτε όλους τους φυσικούς x, ώστε $x \leq 70$ κ' $ord_{41}(6^x) = 20$
(ii) Βρείτε όλους τους φυσικούς y, ώστε $6^{5y} \equiv 1 \pmod{41}$

Λύση: 41 πρώτος. (βρίσκουμε το $\sqrt{41}$ το οποίο είναι < 7 κ' δείχνουμε ότι κανένας αριθμός μέχρι το 6 ή 7 δεν διαιρεί το 41)

Αφού 41 πρώτος, $\phi(41) = 41\left(1 - \frac{1}{41}\right) = 40$. Οι διαιρέτες του $40 = 2^3 \cdot 5$ είναι $\{1, 2, 4, 5, 8, 10, 20, 40\}$
Με πράξεις δείχνουμε $[2^m]_{41} \neq [1]_{41}$ για $m = 1, 2, 4, 5, 8, 10, 20$
Άρα $ord_{41}(6) = 40 = \phi(41)$
Από θεωρία, για ακέραιο $x \geq 1$ $ord_{41}(6^x) = \frac{40}{ΜΚΔ(40, x)}$
Συνεπώς, $ord_{41}(6^x) = 20$ όταν ΜΚΔ$(40, x) = 2$
Έχουμε $40 = 2^3 \cdot 5$
Επομένως, ΜΚΔ$(40, x) = 2 \Leftrightarrow \begin{cases} 2 \mid x \\ 4 \nmid x \\ 5 \nmid x \end{cases}$

1 / τα πολλαπλάσια του 4
2 : / τα πολλαπλάσια του 5

$2, \cancel{4}, 6, \cancel{8}, \cancel{10}, \cancel{12}, 14, \cancel{16}, 18, \cancel{20}, 22, \cancel{24}, 26, \cancel{28}, \cancel{30}, \cancel{32}, 34, \cancel{36}, 38, \cancel{40}, 42, \cancel{44}, 46, \cancel{48}, \cancel{50},$
$\cancel{52}, 54, \cancel{56}, 58, \cancel{60}, 62, \cancel{64}, 66, \cancel{68}, \cancel{70}$

Μένουν $x = 2, 6, 14, 18, 22, 26, 34, 38, 42, 46, 54, 58, 62, 66$

(ii) (Υπενθύμιση: Έστω $n \geq 2$ κ' $a \in \mathbb{Z}$ με $\text{ΜΚΔ}(a, n) = 1$. Θέτουμε $d = ord_n(a)$.
Έστω $m, m' \geq 0$ ακέραιοι)
Τότε $a^m \equiv a^{m'} \bmod n$ αν $m \equiv m' \bmod d$
(όπου $a^0 = 1$ από ορισμό)

Άρα από υπενθύμιση
$6^{5y} \equiv 1 \bmod 41 \Leftrightarrow 6^{5y} \equiv 6^0 \bmod 41$
$\Leftrightarrow 5y \equiv 0 \bmod ord_{41}(6) \Leftrightarrow 5y \equiv 0 \bmod 40$
$\Leftrightarrow y \equiv 0 \bmod 8 \Leftrightarrow 8 \mid y$.

Άρα το σύνολο των φυσικών y με την ιδιότητα $6^{5y} \equiv 1 \bmod 41$ είναι ακριβώς το σύνολο $\{k8 \mid k \in \mathbb{N}\}$