Πρόταση: Έστω p πρώτος κ' $n \geq 1$. Τότε $U(\mathbb{Z}/p^n) = \{[a]_{p^n} : 1 \leq a \leq p^n - 1$ κ' $p \nmid a\}$
κ' $\phi(p^n) = p^n - p^{n-1}$

Απόδειξη: Έστω a με $0 \leq a \leq p^n - 1$.
Τότε ΜΚΔ$(a, p^n) = 1$ αν $p \nmid a$. (αφού p πρώτος, $n \geq 1$)

(Απόδειξη: Υποθέτουμε ΜΚΔ$(a, p^n) = 1$ κ' ότι $p \mid a$. Άρα $p \mid a$, $p \mid p^n$ $\} \Rightarrow p \mid$ ΜΚΔ$(a, p^n) = 1$, άτοπο.
Αντίστροφα, υποθέτουμε $p \nmid a$ κ' ΜΚΔ$(a, p^n) \neq 1$. Έστω q πρώτος με $q \mid$ ΜΚΔ$(a, p^n) \Rightarrow$
$q \mid p^n \Rightarrow q \mid p$, άρα $q = p$. Συνεπώς $p \mid a$, άτοπο.
Συνεπώς το $U(\mathbb{Z}/p^n)$ είναι όπως στην πρόταση.
Επειδή $\# \mathbb{Z}/p^n = p^n$ κ' τα πολλαπλάσια b του p με $0 \leq b < p^n$ είναι
$p \cdot 0, p \cdot 1, p \cdot 2, \ldots, p \cdot (p^{n-1} - 1)$ είναι p^{n-1} το πλήθος
Έπεται ότι $\# U(\mathbb{Z}/p^n) = \# \mathbb{Z}/p^n - p^{n-1} = p^n - p^{n-1}$

Παράδειγμα Υπολογίστε $U(\mathbb{Z}/25)$ κ' $\phi(25)$
Λύση $25 = 5^2$. Άρα $\phi(25) = 5^2 - 5^1 = 25 - 5 = 20$
Θέτουμε $B = \{[a]_{25} : 1 \leq a \leq 25$ κ' $5 \mid a\} = \{[5]_{25}, [10]_{25}, [15]_{25}, [20]_{25}, [25]_{25}\}$
κ' $U(\mathbb{Z}/25) = \mathbb{Z}/25 - B$

Πρόταση (χωρίς απόδειξη)
Έστω $n \geq 2$ με πρωτογενή ανάλυση $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$
(όπου p_i πρώτοι, $p_i \neq p_j$ για $i \neq j$ κ' $a_i \geq 1$ ακέραιοι)
Τότε $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right) = (p_1^{a_1} - p_1^{a_1 - 1})(p_2^{a_2} - p_2^{a_2 - 1}) \cdots (p_r^{a_r} - p_r^{a_r - 1})$

ΠΑΡΑΤΗΡΗΣΗ: Το έχουμε δείξει για $r = 1$, δηλαδή n = δύναμη πρώτου.

Παράδειγμα Υπολογίστε το $\phi(52)$
ΛΥΣΗ: Η πρωτογενής ανάλυση του 52 είναι $52 = 2^2 \cdot 13$. Άρα από την πρόταση
$\phi(52) = 52\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{13}\right) = \frac{52 \cdot 1 \cdot 12}{26} = 24$
Δηλαδή υπάρχουν ακριβώς 24 αντιστρέψιμα στοιχεία στο $\mathbb{Z}_{52}$.
Δηλαδή ο αριθμός των ακεραίων a με $1 \leq a \leq 52$ κ' ΜΚΔ$(a, 52) = 1$ είναι ίσος με 24.

ΠΑΡΑΤΗΡΗΣΗ Η πρόταση που μας δίνει τον υπολογισμό του $\phi(n)$ έχει ως συνέπεια το εξής:

Έστω $m\geq 1, n\geq 1$ ακέραιοι με ΜΚΔ$(m,n)=1$. Τότε $\phi(m\cdot n)=\phi(m)\phi(n)$ (*)

Ο λόγος είναι ότι ΜΚΔ$(m,n)=1$ είναι ισοδύναμο με το ότι δεν υπάρχει πρώτος p που να διαιρεί κ' το m κ' τον n. Στην Θεωρία αριθμών, μια συνάρτηση $f: \mathbb{N}\to\mathbb{Z}$ που ικανοποιεί $f(m\cdot n)=f(m)f(n)$ όταν ΜΚΔ$(m,n)=1$ λέγεται ΠΟΛΛΑΠΛΑΣΙΑΣΤΙΚΗ.

Επομένως, η συνάρτηση ϕ του Euler είναι πολλαπλασιαστική!

ΠΑΡΑΤΗΡΗΣΗ: ΠΡΟΣΟΧΗ $\phi(2)=2$, $\phi(4)=2$, γιατί $U(\mathbb{Z}_4)=\{[1]_4,[3]_4\}$.

Άρα $\phi(2\cdot 2)\neq\phi(2)\cdot\phi(2)$, δηλαδή $\phi(m\cdot n)=\phi(m)\phi(n)$ όταν ΜΚΔ$(m,n)=1$ αλλά αν ΜΚΔ$(m,n)\neq 1$ γενικά $\phi(m,n)\neq\phi(m)\phi(n)$.

Φυλ 6 ασκ 4 Δ.ο.

$[10]_{21}\in U(\mathbb{Z}_{21})$ κ' υπολογίστε το $([10]_{21})^{-1}$

Λύση Ευκλείδειος Αλγόριθμος.

$21=2\cdot 10+①$ (*)

Άρα ΜΚΔ$(21,10)=1$, συνεπώς από πρόταση $[10]_{21}\in U(\mathbb{Z}_{21})$

$(*)\Rightarrow 1=(-2)\cdot 10+1\cdot 21\Rightarrow[1]_{21}=[-2]_{21}[10]_{21}=[10]_{21}[-2]_{21}$

Συνεπώς, $([10]_{21})^{-1}=[-2]_{21}=[19]_{21}$

Φυλ 6 ασκ 4 Δ.ο. $[62]_{155}\notin U(\mathbb{Z}_{155})$ ← αφού ΜΚΔ$(62,155)\neq 1$

Λύση: ΜΚΔ$(62,155)=$ ΜΚΔ$(62,155-2\cdot 62)=$ ΜΚΔ$(62,31)=$ ΜΚΔ$(62-2\cdot 31,31)=$

$=$ ΜΚΔ$(0,31)=31\neq 1$

Συνεπώς, από την πρόταση $[62]_{155}$ δεν αντιστρέφεται στο $\mathbb{Z}_{155}$

Πρόταση Έστω $a\in\mathbb{Z}, m\in\mathbb{Z}$ με $m>0$. Θεωρούμε το σύνολο $B=\{a,a+1,a+2,a+3,\dots,a+m\}$

Τότε $\boxed{\#B=m+1}$

Απόδειξη Επαγωγή στο m. Για $m=1$ $B=\{a,a+1\}$ κ' $\#B=2=1+1$

Υπόθεση ισχύει για m κ' $B=\{a,a+1,\dots,a+m,a+m+1\}$

Τότε B είναι η ξένη ένωση $\{a,\dots,a+m\}$ κ' $\{a+m+1\}$, το οποίο από υπόθεση επαγωγής έχει $(m+1)+1$ στοιχεία.

ΠΑΡΑΤΗΡΗΣΗ: Συνεπώς έχουμε n διαδοχικούς ακεραίους που ξεκινάν από $a \in \mathbb{Z}$, αυτοί είναι $\{a, a+1, a+2, \dots, a+n-1\}$.

Ορισμός: Έστω $n \geq 1$. Τότε οι ακέραιοι $a_1, a_2, \dots, a_n$ είναι ΠΛΗΡΕΣ ΣΥΣΤΗΜΑ υπολοίπων modulo n, αν $\mathbb{Z}_n = \{[a_1]_n, [a_2]_n, \dots, [a_n]_n\}$

Π.χ. Έστω $n \geq 1$. Τότε οι ακέραιοι $0, 1, 2, \dots, n-1$ είναι πλήρες σύστημα υπολοίπων modulo n. Το ίδιο κ' οι ακέραιοι $1, 2, 3, \dots, n-1, n$

Π.χ. Έστω $n=3$. Είναι οι 3 ακέραιοι $2, 3, 5$ πλήρες σύστημα υπολοίπων modulo 3;

Λύση: Έχουμε $\{[2]_3, [3]_3, [5]_3\} = \{[2]_3, [0]_3, [2]_3\} = \{[0]_3, [2]_3\} \neq \mathbb{Z}_3$.
Άρα δεν είναι.