Πρόταση Έστω $n \geq 1$ και $a \in \mathbb{Z}$. Τότε, το στοιχείο $[a]_n \in \mathbb{Z}_n$ είναι αντιστρέψιμο αν και μόνο αν $\text{ΜΚΔ}(a,n) = 1$

Απόδειξη Υποθέτουμε πρώτα ότι $[a]_n$ αντιστρέψιμο και $\text{ΜΚΔ}(a,n) \neq 1$ και θα βρούμε αντίφαση. Αφού $[a]_n$ αντιστρέψιμο, $\exists b \in \mathbb{Z}$ με $[a]_n[b]_n = [1]_n$, άρα $[ab]_n = [1]_n$, συνεπώς $n \mid ab - 1$, συνεπώς $\exists k \in \mathbb{Z}$ με $ab - 1 = kn$, άρα $1 = ab + (-k)n$. Αφού από υπόθεση $\text{ΜΚΔ}(a,n) \neq 1$, $\exists$ πρώτος p με $p \mid \text{ΜΚΔ}(a,n)$. Άρα, p θα είναι $p \mid n$, άρα από (*) $p \mid 1$, αντίφαση.

Αντίστροφα, υποθέτουμε ότι $\text{ΜΚΔ}(a,n) = 1$ και θέλουμε $[a]_n$ είναι αντιστρέψιμο. Αφού $1 = \text{ΜΚΔ}(a,n)$ $\exists z_1, z_2 \in \mathbb{Z}$ με $1 = z_1 a + z_2 n$. Άρα $n \mid 1 - z_1 a \Rightarrow [1]_n = [z_1]_n [a]_n = [a]_n [z_1]_n$. Άρα $[a]_n$ αντιστρ.

ΑΝΤΙΣΤΡΟΦΟΣ ΣΥΝΕΣΗΣ: $([a]_n)^{-1}$ (ως προς $\cdot$)

Έστω $n \geq 1$ κ' $a \in \mathbb{Z}$ με $ΜΚΔ(a,n)=1$.

Βήμα 1ο: Εφαρμόζουμε Ευκλείδειο Αλγόριθμο κ' υπολογίζουμε $z_1, z_2 \in \mathbb{Z}$ με $1 = z_1 a + z_2 n$

Βήμα 2ο: Έχουμε $([a]_n)^{-1} = [z_1]_n$

(π.χ.) $n=5, a=4$

Ευκλείδειος αλγόριθμος: Άρα $z_1=-1, z_2=1$, $ΜΚΔ(4,5)=1$ κ'

$5 = 4+1$

$\Rightarrow 1 = (-1)4 + 1\cdot 5$ $\quad ([4]_5)^{-1} = [z_1]_5 = [-1]_5 = [4]_5$

Συμβολισμός: Έστω $n \geq 1$. Συμβολίζουμε με $U(\mathbb{Z}/n)$ (U=units) το σύνολο των αντιστρέψιμων στοιχείων του $\mathbb{Z}/n$. Επίσης, για $n \geq 1$ ορίζουμε $\phi(n) = \#U(\mathbb{Z}/n)$. Δηλαδή αυτό των πρώτων

$\phi(n) = \#\{a \in \mathbb{Z} : 1 \leq a \leq n$ κ' $ΜΚΔ(a,n)=1\}$

(π.χ.) $\mathbb{Z}/1 = \{[1]_1\}$, $U(\mathbb{Z}/1) = \{[1]_1\}$, $\phi(1)=1$

$\mathbb{Z}/2 = \{[0]_2, [1]_2\}$, $U(\mathbb{Z}/2) = \{[1]_2\}$, $\phi(2)=1$

$\mathbb{Z}/3 = \{[0]_3, [1]_3, [2]_3\}$, $U(\mathbb{Z}/3) = \{[1]_3, [2]_3\}$, $\phi(3)=2$

$\mathbb{Z}/4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ $U(\mathbb{Z}/4) = \{[1]_4, [3]_4\}$, $\phi(4)=2$ (πρώτοι ως προς 8)

$\mathbb{Z}/8 = \{[0]_8, [1]_8, \ldots, [7]_8\}$ $U(\mathbb{Z}/8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$, $\phi(8)=4$

$\mathbb{Z}/12 = \{[0]_{12}, [1]_{12}, \ldots, [11]_{12}\}$ $U(\mathbb{Z}/12) = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$, $\phi(12)=4$

ΠΑΡΑΤΗΡΗΣΗ: Η συνάρτηση ϕ λέγεται ϕ συνάρτηση του Euler

Πρόταση: Έστω p πρώτος τότε $U(\mathbb{Z}/p) = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$ κ' $\phi(p) = p-1$

Με άλλα λόγια, κάθε στοιχείο του $\mathbb{Z}/p$, εκτός του $[0]_p$ είναι αντιστρέψιμο. Άρα το $\mathbb{Z}/p$ σώμα.

Απόδειξη: Γνωρίζουμε $ΜΚΔ(a,p)=p$. Άρα $[a]_p \neq [0]_p$ όχι αντιστρ.

Έστω $a \in \mathbb{Z}$ με $1 < a < p-1$ Αφού p πρώτος $ΜΚΔ(a,p)=1$. Άρα $[a]_p \in U(\mathbb{Z}/p)$