Πρόταση: Έστω $n \geq 1$ κ' $a, a', b, b' \in \mathbb{Z}$ με $a' \equiv a \bmod n$ κ' $b' \equiv b \bmod n$

Τότε 1) $(a'+b') \equiv (a+b) \bmod n$

2) $a'b' \equiv ab \bmod n$

Απόδειξη: Αφού $a' \equiv a \bmod n$ έχουμε ότι $n \mid a-a'$, άρα $\exists k \in \mathbb{Z}$ με

$a - a' = kn \Rightarrow a = a' + kn$ (1)

Ομοίως, αφού $b' \equiv b \bmod n$, έχουμε ότι $n \mid b-b'$, άρα $\exists l \in \mathbb{Z}$ με

$b - b' = ln \Rightarrow b = b' + ln$ (2)

Προσθέτοντας τις (1), (2) έχουμε $a+b = a'+b' + (k+l)n$. Άρα $(a'+b') \equiv (a+b) \bmod n$

Πολλ/ζοντας τις (1), (2) έχουμε $a \cdot b = (a'+kn)(b'+ln) = a'b' + n(kb' + la' + kln)$

Άρα $n \mid a'b' - ab$, άρα $a'b' \equiv ab \bmod n$

Παρατήρηση: Η πρόταση μας λέει ότι αν $n \geq 1$ κ' $a, a', b, b' \in \mathbb{Z}$ με $[a']_n = [a]_n$ κ' $[b']_n = [b]_n$, τότε ισχύει $[a'+b']_n = [a+b]_n$ κ' $[a'b']_n = [ab]_n$

Ορισμός: Στο $\mathbb{Z}_n$ ορίζουμε πράξεις $+$ κ' $\cdot$ ως εξής.

Έστω $a, b \in \mathbb{Z}$. Ορίζουμε $[a]_n + [b]_n = [a+b]_n$ κ' $[a]_n[b]_n = [ab]_n$

Από την πρόταση είναι καλά ορισμένες.

Πχ $n = 2$ τότε $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$

κ' $[0]_2 + [0]_2 = [0+0]_2 = [0]_2$

$[0]_2 + [1]_2 = [0+1]_2 = [1]_2$

$[1]_2 + [0]_2 = [1+0]_2 = [1]_2$

$[1]_2 + [1]_2 = [1+1]_2 = [2]_2 = [0]_2$

Επίσης, $[0]_2[0]_2 = [0 \cdot 0]_2 = [0]_2$

$[0]_2[1]_2 = [0 \cdot 1]_2 = [0]_2$

$[1]_2[0]_2 = [1 \cdot 0]_2 = [0]_2$

$[1]_2[1]_2 = [1 \cdot 1]_2 = [1]_2$

Π.χ. $n=12$ έχουμε $\mathbb{Z}_{12} = \{[0]_{12}, [1]_{12}, [2]_{12}, [3]_{12}, [4]_{12}, [5]_{12}, [6]_{12}, [7]_{12}, [8]_{12},$
$[10]_{12}, [11]_{12}\}$
$= \{[1]_{12}, [2]_{12}, \dots, [11]_{12}, [12]_{12}\}$

γιατί
$[0]_{12} = [12]_{12}$

Επίσης: $[11]_{12} + [5]_{12} = [11+5]_{12} = [16]_{12} = [4]_{12}$

Πρόταση: Έστω $n \geq 1$ κ' $a, b \in \mathbb{Z}$. Τότε

1) Η πράξη $+$ στο $\mathbb{Z}_n$ είναι προσεταιριστική. Δηλαδή $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n$
2) Το $[0]_n$ είναι ουδέτερο στοιχείο ως προς το $+$. Δηλαδή $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$
3) Το $[-a]_n$ είναι αντίθετο του $[a]_n$ ως προς $+$. Δηλαδή
$$[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$$
4) Η πράξη $+$ είναι μεταθετική. Δηλαδή $[a]_n + [b]_n = [b]_n + [a]_n$

Απόδειξη 1) $([a]_n + [b]_n) + [c]_n = [a+b]_n + [c]_n =$
$= [(a+b)+c]_n = [a+(b+c)]_n$

Η πρόσθεση στο $\mathbb{Z}$ είναι
προσεταιριστική

$= [a]_n + [b+c]_n = [a]_n + ([b]_n + [c]_n)$

2), 3), 4). Παρόμοια (κ' πιο εύκολη) απόδειξη.

Παρατήρηση: Στο $\mathbb{Z}_n$ έχουμε $[-a]_n = [n-a]_n$
γιατί $(n-a) - (-a) = n$ κ' $n \mid n$. Άρα $[-3]_7 = [7-3]_7 = [4]_7$

Π.χ. Υπολογίστε το $A = [3]_7 + [5]_7 + [6]_7 + [2]_7 + [9]_7$

Λύση: $A = ([3]_7 + [5]_7) + ([6]_7 + [2]_7 + [2]_7) =$
$= [8]_7 + [10]_7 = [1]_7 + [3]_7 = [4]_7$

Πρόταση: Έστω $n \geq 1$ κ' $a', a \in \mathbb{Z}$ με $a' \equiv a \bmod n$. Τότε $ΜΚΔ(a', n) = ΜΚΔ(a, n)$
(Δηλαδή αν το n διαιρεί τη διαφορά δύο ακεραίων, αυτοί οι ακέραιοι έχουν ίδιο ΜΚΔ με το n)

Απόδειξη: Αφού $a' \equiv a \bmod n$, έχουμε $n \mid a' - a$, άρα $\exists k \in \mathbb{Z}$ με $(a' - a) = kn$, άρα $a' = a + kn$
Συνεπώς από πρόταση $ΜΚΔ(a', n) = ΜΚΔ(a + kn, n) = ΜΚΔ((a + kn) - kn, n) =$
$= ΜΚΔ(a, n)$

Πόρισμα: Έστω $n \geq 1$, $a \in \mathbb{Z}$ κ' r το υπόλοιπο της Ευκλείδιας Διαίρεσης του a με τον n. Τότε $ΜΚΔ(a, n) = ΜΚΔ(r, n)$

Απόδειξη: Από τον ορισμό του r $\exists k \in \mathbb{Z}$ με $a = kn + r$
Άρα $a - r = kn$, συνεπώς $n \mid a - r$
συνεπώς $a \equiv r \bmod n$. Από την πρόταση $ΜΚΔ(a, n) = ΜΚΔ(r, n)$

Π.χ. Βρείτε το υπόλοιπο της Ευκλείδιας Διαίρεσης του 2019 με το 4 κ' τον $ΜΚΔ(2019, 4)$

Λύση: Έχουμε $2019 = 504 \cdot 4 + 3$
Συνεπώς το υπόλοιπο r είναι 3
κ' από το πόρισμα
$ΜΚΔ(2019, 4) = ΜΚΔ(3, 4) = 1$

$$\begin{array}{r|l} 2019 & 4 \\ \cline{2-2} 019 & 504 \\ 3 & \end{array}$$

Πρόταση: Έστω $n \geq 1$ κ' $a, b, c \in \mathbb{Z}$. Τότε
(i) Ο πολ/σμός στο $\mathbb{Z}/n$ είναι προσεταιριστικός, δηλαδή
$([a]_n [b]_n)[c]_n = [a]_n([b]_n [c]_n)$
(ii) Ο πολ/σμός στο $\mathbb{Z}/n$ είναι μεταθετικός, δηλαδή
$[a]_n [b]_n = [b]_n [a]_n$
(iii) Το $[1]_n$ είναι ουδέτερο στοιχείο του πολ/σμού στο $\mathbb{Z}/n$
δηλαδή $[1]_n [a]_n = [a]_n [1]_n = [a]_n$
(iv) Ο πολ/σμός στο $\mathbb{Z}/n$ είναι δεξιά κ' αριστερά επιμεριστικός ως προς την πρόσθεση στο $\mathbb{Z}/n$, δηλαδή

$[a]_n([b]_n+[c]_n) = [a]_n[b]_n + [a]_n[c]_n$ κ'

$([a]_n+[b]_n)([c]_n) = [a]_n[c]_n + [b]_n[c]_n$

Απόδειξη: (i) $([a]_n[b]_n)[c]_n = [ab]_n[c]_n = [(ab)c]_n$

$= [a(bc)]_n = [a]_n[bc]_n = [a]_n([b]_n[c]_n)$

προσεταιριστικότητα του πολλ/μού στο $\mathbb{Z}$

(ii), (iii), (iv) Παρόμοια απόδειξη

Παρατήρηση: Το $\mathbb{Z}/n$ με τις πράξεις $+$ κ' $\cdot$ λέγεται "Ο δακτύλιος των ακεραίων modulo n".

Ορισμός: Έστω $a \in \mathbb{Z}$. Το στοιχείο $[a]_n \in \mathbb{Z}/n$ λέγεται αντιστρέψιμο στο $\mathbb{Z}/n$ (ως προς τον πολλ/μό) αν $\exists\, b \in \mathbb{Z}$ ώστε

$$[a]_n[b]_n = [b]_n[a]_n = [1]_n$$

Τότε το $[b]_n$ λέγεται αντίστροφο στο $\mathbb{Z}/n$ του $[a]_n$ κ' από την επόμενη πρόταση είναι μοναδικό.

Πρόταση: Έστω $n \geq 1$ κ' $a, b, b' \in \mathbb{Z}$ με $[a]_n[b]_n = [b]_n[a]_n = [1]_n$ κ' $[a]_n[b']_n = [b']_n[a]_n = [1]_n$. Τότε

$$[b]_n = [b']_n$$

Απόδειξη: $[b']_n = [b']_n[1]_n = [b']_n([a]_n[b]_n) = ([b']_n[a]_n)[b]_n$

$= [1]_n[b]_n = [b]_n$

Συμβολισμός: Αν $n \geq 1$ κ' $a \in \mathbb{Z}$ με $[a]_n \in \mathbb{Z}/n$ αντιστρέψιμο, συμβολίζουμε το (μοναδικό από την πρόταση) αντίστροφο στοιχείο του $[a]_n$ στο $\mathbb{Z}/n$ με $([a]_n)^{-1}$.

Π.χ. Έστω $n \geq 1$. Τότε $[1]_n[1]_n = [1]_n$, άρα $([1]_n)^{-1} = [1]_n$

Π.χ. Έχουμε $[2]_3[2]_3=[4]_3=[1]_3$. Συνεπώς $[2]_3$ αντιστρέψιμο στο $\mathbb{Z}_3$ κ' $([2]_3)^{-1}=[2]_3$

Π.χ. $n=11$. Τότε $[2]_{11}[6]_{11}=[6]_{11}[2]_{11}=[12]_{11}=[1]_{11}$.
Συνεπώς $[2]_{11}$ αντιστρ. στο $\mathbb{Z}_{11}$ κ' $([2]_{11})^{-1}=[6]_{11}$
Επίσης $[6]_{11}$ αντιστρ. στο $\mathbb{Z}_{11}$ κ' $([6]_{11})^{-1}=[2]_{11}$.

Π.χ. ΙΣΧΥΡΙΣΜΟΣ: Το στοιχείο $[2]_4$ του $\mathbb{Z}_4$ δεν είναι αντιστρέψιμο.

Απόδειξη: Έστω ότι είναι. Άρα $\exists b\in\mathbb{Z}$ με $[2]_4[b]_4=[1]_4$.
- Άρα $[2b]_4=[1]_4$. Συνεπώς $4\mid(2b-1)$.
- Άρα $\exists k\in\mathbb{Z}$ με $2b-1=4k \Rightarrow 1=2b-4k=2(b-2k)$
- Άρα $2\mid 1$ στο $\mathbb{Z}$. αντίφαση

Ερώτημα: Ποια στοιχεία του $\mathbb{Z}_n$ είναι αντιστρέψιμα κ' αν είναι πως υπολογίζουμε τον (μοναδικό από την πρόταση) αντίστροφο;
Επίσης πόσα είναι αυτά;