26/11/2018

Έστω $n \geq 1$. Ορίσαμε σχέση ισοδυναμίας στο $\mathbb{Z}$ με αν ισοδυναμεί το b αν $n \mid a-b$ (ισοδυναμεί με $n \mid b-a$). Συμβολίζαμε $\mathbb{Z}_n$ το "σύνολο πηλίκο" δηλ. το σύνολο των κλάσεων ισοδυναμίας, για $a \in \mathbb{Z}$, συμβολίζαμε με $[a]_n \in \mathbb{Z}_n$ το αντίστοιχο στοιχείο του $\mathbb{Z}_n$. Κάθε στοιχείο του $\mathbb{Z}_n$ είναι της μορφής $[a]_n$ για κάποιο (ΟΧΙ ΜΟΝΑΔΙΚΟ) $a \in \mathbb{Z}$. Ισχύει $[a]_n = [b]_n$ αν-ν $n \mid a-b$.

ΠΑΡΑΔΕΙΓΜΑ: $[3]_2 = [1]_2$, γιατί $2 \mid 3-1 = 2$
(3 mod 10 2)

Αλλά $[3]_3 \neq [1]_3$ γιατί $3 \nmid 3-1 = 2$.

Πρόταση: Έστω $n \in \mathbb{N}$. Τα στοιχεία $[0]_n, [1]_n, \dots, [n-1]_n$ είναι διαφορετικά ανά δύο, και κάθε στοιχείο $[a]_n$ του $\mathbb{Z}_n$ είναι ένα από αυτά. Συνεπώς, $\#\mathbb{Z}_n = n$.

Απόδειξη: Έστω i, j με $0 \le i < j \le n-1$. Θ.δ.ο. $[i]_n \neq [j]_n$
(Αρκεί ν.δ.ο. $n \nmid j-i$)
Αφού $1 \le j-i \le n-1 \Rightarrow n$ δεν διαιρεί το $j-i$.
Έστω $a \in \mathbb{Z}$. Από ευκλ. διαίρεση, υπάρχουν $q, r \in \mathbb{Z}$ ώστε
$a = qn + r$ (*) και $0 \le r \le n-1$.
Από (*) $\Rightarrow n \mid a-r \Rightarrow [a]_n = [r]_n$
$n \mid a-b \Leftrightarrow n \mid b-a$.

Πόρισμα: Έστω $n \ge 1$. $a, b \in \mathbb{Z}$ και $a = q_1 n + r_1$ η ευκλ. διαιρ. του a με το n.
$b = q_2 n + r_2$ η ευκλ. διαίρεση του b με το n.
Έτσι έχουμε $[a]_n = [b]_n$ αν-ν $r_1 = r_2$.

Επόμενος Στόχος: Ορίζουμε στο $\mathbb{Z}_n$ πρόσθεση $+$ και πολλαπλασιασμό.

Πρόταση: Έστω $n \ge 1$ και $a, b, c, d \in \mathbb{Z}$. Υποθέτουμε $a = b \bmod n$ (δηλ. $n \mid b-a$) και το $c = d \bmod n$ (δηλ. $n \mid d-c$)
Τότε: (i) $a+c = b+d \bmod n$ (δηλ. $n \mid (a+c)-(b+d)$)
και (ii) $a \cdot c = bd \bmod n$ (δηλ. $n \mid ac-bd$)

Απόδειξη:
(i) Από υπόθεση $n \mid a-b$ και $n \mid c-d$. Επομένως, $n \mid (a-b)+(c-d)$
δηλ. $n \mid (a+c)-(b+d)$.
(ii) Από υπόθεση $n \mid a-b$ και $n \mid c-d$ (*)
$ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d)$
(*) από πρόταση δίνει
$n \mid c(a-b) + b(c-d)$. Συνεπώς $n \mid ac-bd$.

(Η πρόταση λέει: $n|f$ και $n|g \Rightarrow n|xf+yg$ $\forall x,n\in\mathbb{R}$)

Ορισμός: Στο $\mathbb{Z}_n$ ορίζουμε πρόσθεση $[a]_n+[b]_n=[a+b]_n$ και πολλαπλασιασμό $[a]_n\cdot[b]_n=[a\cdot b]_n$

Από την πρόταση οι πράξεις είναι κανονικοί αριθμοί.

Παράδειγμα: $[1]_2+[1]_2=[2]_2=[0]_2$

$[3]_5[4]_5=[12]_5=[2]_5$

Α' τρόπος: $[3]_7\cdot[9]_7=[27]_7=[6]_7=[-1]_7$

Β' τρόπος: $[3]_7\cdot[9]_7=[3]_7[2]_7=[6]_7$

$[2015]_{2018}[2016]_{2018}=[-3]_{2018}[-2]_{2018}=[6]_{2018}$

Παράδειγμα:

$[10]_{12}+[3]_{12}=[13]_{12}=[1]_{12}$

$[11]_{12}+[4]_{12}=[15]_{12}=[3]_{12}$

Πρόταση: Έστω $n\geq 1$.

(1) Η πρόσθεση + στο $\mathbb{Z}_n$ είναι μεταβατική, προσεταιριστική, έχει ουδέτερο στοιχείο το $[0]_n$ και για κάθε $\mathbb{Z}$, το αντίθετο του $[a]_n=[-a]_n$.

Απόδειξη: Έστω $a,b,c\in\mathbb{R}$. Τότε:

Μεταθ.: $[a]_n+[b]_n=[a+b]_n=[b+a]_n=[b]_n+[a]_n$.

Προσετ.: $([a]_n+[b]_n)+[c]_n=[a+b]_n+[c]_n=[(a+b)+c]_n$

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

Ουδετ. το $[0]_n$: $[a]_n+[0]_n=[a+0]_n=[a]_n$

Ομοίως $[0]_n+[a]_n=[a]_n$.

Πρόταση: Έστω $n \geq 1$. Ο πολλαπλασιασμός στο $\mathbb{Z}_n$ είναι μεταθετικός, προσεταιριστικός, έχει ουδέτερο στοιχείο το $[1]_n$. Επίσης, είναι επιμεριστικός ως προς την πρόσθεση στο $\mathbb{Z}_n$.

Απόδειξη: Έστω $a, b, c \in \mathbb{Z}$. Τότε:
$[a]_n [b]_n = [ab]_n = [ba]_n = [b]_n [a]_n$.
$([a]_n [b]_n)[c]_n = [ab]_n [c]_n = [(ab)c]_n = [a(bc)]_n$
$= [a]_n [bc]_n = ([a]_n [b]_n [c]_n)$

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

και παρομοίως: $([b]_n + [c]_n)[a]_n = [b]_n [a]_n + [c]_n [a]_n$.

Ορισμός: Έστω $a \in \mathbb{Z}$. Το στοιχείο $[a]_n \in \mathbb{Z}_n$ λέγεται **ΑΝΤΙΣΤΡΕΨΙΜΟ** αν υπάρχει $b \in \mathbb{Z}$ ώστε $[a]_n [b]_n = [1]_n$.

Πρόταση: Έστω $a, b, b' \in \mathbb{Z}$. Υποθέτουμε ότι $[a]_n [b]_n = [a][b]_n = [1]_n$. Τότε $[b]_n = [b']_n$. Άρα αν $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμο το αντίστροφο του είναι μοναδικό. Θα το συμβολίζουμε $([a]_n)^{-1} \in \mathbb{Z}_n$.

Απόδειξη: Έχουμε: $[b]_n = [b]_n [1]_n = [b]_n [a]_n [b']_n =$
$= [a]_n [b]_n [b']_n = [1]_n [b']_n = [1]_n [b']_n = [b']_n$.

Ερώτημα - 1: Για ποια $a \in \mathbb{R}$ το $[a]_n \in \mathbb{Z}_n$ είναι αντιστρέψιμο;

Ερώτημα - 2: Αν $a \in \mathbb{Z}$ με $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμο πως υπολογίζουμε $b \in \mathbb{Z}$ με $[a]_n[b]_n = [1]_n$

Ερώτημα - 3: Πόσα στοιχεία του $\mathbb{Z}_n$ είναι αντιστρέψιμα;

Παράδειγμα 1: Έστω $n \geq 1$. Το $[1]_n \in \mathbb{Z}_n$ είναι αντιστρέψιμο και $([1]_n)^{-1} = [1]_n$.

Παράδειγμα 2: Το $[3]_5 \in \mathbb{Z}_n$ είναι αντιστρέψιμο και $([3]_5)^{-1} =$
Χρειαζόμαστε ακέραιο b ώστε: $3b = 1 \bmod 5$, δηλαδή το υπόλοιπο της ευκ. διαιρ. του $3b$ με το 5 να είναι 1.
Εύκολα μπορούμε να πάρουμε $b = 2$ και άρα $([3]_5)^{-1} = [2]_5$.
Επίσης, $b = 7$ δουλεύει αλλά $[7]_5 = [2]_5$ στο $\mathbb{Z}_5$.
Πιο γενικά αν $t \in \mathbb{Z}$ μπορούμε να πάρουμε b το $2 + t5$.

Θεώρημα: Έστω $n \geq 2$ και $a \in \mathbb{Z}$. Τότε $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμη αν-ν $\text{ΜΚΔ}(a, n) = 1$.

Απόδειξη: Έστω $a \in \mathbb{R}$ με $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμο. Τότε υπάρχει $b \in \mathbb{Z}$ με $[a]_n[b]_n = [1]_n$, δηλ. $a \cdot b = 1 \bmod n$, δηλ. $n \mid ab - 1$.

Συνεπώς υπάρχει $k \in \mathbb{Z}$ με $kn = ab - 1 \Rightarrow 1 = b \cdot a + (-k)n$ (*)
Έστω $d = \text{ΜΚΔ}(a, n)$. Τότε $d \mid a$ και $d \mid n \overset{(*)}{\Rightarrow} d \mid 1 \Rightarrow d = 1$.

Αντιστροφα, έστω $a \in \mathbb{Z}$ με $ΜΚΔ(a,n) = 1$. Θα δείξουμε ότι $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμη. Αφού $ΜΚΔ(a,n) = 1$ υπάρχουν $x, y \in \mathbb{Z}$ ώστε $1 = xa + ny$ (**)
Θέτουμε $b = x$. Τότε η (**) δίνει:
$1 - ab = yn \Rightarrow n \mid 1 - ab \Leftrightarrow [a]_n [b]_n = [1]_n$
Άρα $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμη, με αντίστροφο, το $[x]_n = [b]_n$.

ΑΛΓΟΡΙΘΜΟΣ: Έστω $n \geq 2$ και $a \in \mathbb{Z}$ με $ΜΚΔ(a,n) = 1$. Ο αλγόριθμος υπολογίζει το $([a]_n)^{-1} \in \mathbb{Z}_n$.

Βήμα - 1ο: Με χρήση ευκλ. αλγορίθμου υπολογίζουμε $x, y \in \mathbb{Z}$ ώστε $1 = x \cdot a + yn$

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

ΠΑΡΑΔΕΙΓΜΑ:

(1) Είναι το $[3]_{15}$ αντιστρέψιμο στο $\mathbb{Z}_{15}$;
Όχι γιατί $ΜΚΔ(3,15) = 3 \neq 1$

(2) Είναι το $[2]_{15}$ αντιστρέψιμο στο $\mathbb{Z}_{15}$;
Ναι από το θεώρημα γιατί $ΜΚΔ(2,15) = 1$
Ποιο είναι το $([2]_{15})^{-1}$;
Έχουμε $2 \cdot 8 = 16 = 1 \bmod 15$
Συνεπώς $([2]_{15})^{-1} = [8]_{15}$.

(3) Ν.δ.ο. $ΜΚΔ(23,25) = 1$ και υπολογίστε το $([23]_{25})^{-1}$.

ΛΥΣΗ: Ευκλ. Αλγόριθμος

$25 = 1 \cdot 23 + 2$ — Άρα ΜΚΔ$(23, 25) = 1$

(*) $23 = 11 \cdot 2 + 1$ — (γιατί 1 το τελευταίο μη μηδενικό υπόλοιπο).

$2 = 2 \cdot 1 + 0$

Επίσης (*) $\Rightarrow 1 = 23 - 11 \cdot 2 = 23 - 11(25 - 23) =$
$= 12 \cdot 23 - 11 \cdot 25$

$x = 12$, $a = 23$

Άρα $([23]_{25})^{-1} = [12]_{25}$.

ΟΡΙΣΜΟΣ: Έστω $n \geq 1$. Θέτουμε $U(\mathbb{Z}_n) = \{[a]_n : 1 \leq a \leq n$ και ΜΚΔ$(a, n) = 1\}$

Συμβολίζουμε (για $n \geq 1$) $\varphi(n) = \# U(\mathbb{Z}_n)$

Λέμε φ είναι η συνάρτηση φ του Euler.

ΠΑΡΑΤΗΡΗΣΗ: Από το θεώρημα, για $b \in \mathbb{Z}$ έχουμε $[b]_n \in U(\mathbb{Z}_n)$ αν-ν $[b]_n$ αντιστρέψιμο στοιχείο του $\mathbb{Z}_n$. Δηλαδή $U(\mathbb{Z}_n) \subseteq \mathbb{Z}_n$ και το $U(\mathbb{Z}_n)$ περιέχει τα αντιστρέψιμα στοιχεία του $\mathbb{Z}_n$ ενώ το $\mathbb{Z}_n \setminus U(\mathbb{Z}_n)$ περιέχει τα ΜΗ ΑΝΤΙΣΤΡΕΨΙΜΑ στοιχεία του $\mathbb{Z}_n$.

ΠΑΡΑΔΕΙΓΜΑ:

$n = 1$: $\mathbb{Z}_n = \{[1]_n\} = U(\mathbb{Z}_n)$ και $\varphi(1) = 1$

$n = 2$: $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ $U(\mathbb{Z}_{n_2}) = \{[1]_2\}$ και $\varphi(2) = 1$.

$n = 3$: $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ $U(\mathbb{Z}_3) = \{[1]_3, [2]_3\}$ και $\varphi(3) = 2$

$n = 4$: $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ $U(\mathbb{Z}_4) = \{[1]_4, [2]_4, [3]_4\}$ και $\varphi(4) = 2$.

$\mathbb{Z}_6 = \{[0]_6 \ldots [5]_6\}$

$U(\mathbb{Z}_6) = \{[1]_6, \ldots, [5]_6\}$ και $\varphi(6) = 2$

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

$U(\mathbb{Z}_7) = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$ και $\varphi(7) = 6$.

Πρόταση: Έστω p πρώτος. Τότε $U(\mathbb{Z}_p) = \{[1]_p, [2]_p, \dots, [p-1]_p\}$ και άρα $\varphi(p) = p-1$.

Απόδειξη: Έστω $a \in \mathbb{Z}$ με $1 \le a \le p-1$. Αφού p πρώτος $\text{ΜΚΔ}(a,p) = 1$. Άρα $[a]_p \in U(\mathbb{Z}_p)$. Επίσης αφού $\text{ΜΚΔ}(0,p) = p$, με $[0]_p \notin U(\mathbb{Z}_p)$. Συν πορισμα $\tau(p) = p-1$.

Πρόταση: Έστω $n = p^k$ με p πρώτο και $k \ge 1$.
Τότε $U(\mathbb{Z}_n) = \mathbb{Z}_n \setminus \{mp : 1 \le m \le p^{k-1}\}$
Συνεπώς, $\varphi(p^k) = p^k - p^{k-1} = n\left(1 - \frac{1}{p}\right)$

Απόδειξη: Έστω $a \in \mathbb{Z}$ με $1 \le a \le n$. Τότε
$\text{ΜΚΔ}(a,n) > 1 \Leftrightarrow \text{ΜΚΔ}(a,p^k) > 1$ (p πρώτος)
$\text{ΜΚΔ}(a,p) > 1 \Leftrightarrow \text{ΜΚΔ}(a,p) = p \Rightarrow p \mid a$.

Παράδειγμα: $p=3$ $k=2$ $1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8, \cancel{9}$
και διαγραφούμε τα πολλαπλάσια του 3
Συνεπώς, $U(\mathbb{Z}_9) = \{[1]_9, [2]_9, [3]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$ και $\varphi(9) = 6 = 3^2 - 3 = 9\left(1 - \frac{1}{3}\right)$

Παράδειγμα: Υπολογίστε το $\varphi(9^2)$. Έχουμε $9 = 3^2 \Rightarrow 9^2 = 3^4$
και 3 πρώτος. Συνεπώς $\varphi(9^2) = \varphi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$.