22/11/2018

Ισοτιμία modulo n
$a \equiv b \bmod n$ αν και μόνο αν $n \mid a-b$

Θεώρημα Έστω $\gamma, n \in \mathbb{N}$ και $a, b \in \mathbb{Z}$. Ισχύει $a \equiv b \bmod n$ αν και μόνο αν $\gamma a \equiv \gamma b \bmod n$

Απόδειξη $a \equiv b \bmod n \Leftrightarrow n \mid a-b \Leftrightarrow \gamma n \mid \gamma(a-b) \Leftrightarrow$
$\Leftrightarrow \gamma n \mid \gamma a - \gamma b \Leftrightarrow \gamma a \equiv \gamma b \bmod n$

Θεώρημα Έστω $a, b, \gamma \in \mathbb{Z}$ και $n \in \mathbb{N}$. Αν $\gamma a \equiv \gamma b \bmod n$ και $\mu\kappa\delta(\gamma, n) = 1$, τότε $a \equiv b \bmod n$

$n \equiv n \bmod n$

Απόδειξη $\mu\kappa\delta(\gamma, n) = 1 \overset{\text{ευκλείδης}}{\Longrightarrow} 1 = k\gamma + \lambda n$

$1 \equiv k\gamma + \lambda n \bmod n \Leftrightarrow 1 \equiv k\gamma \bmod n$, $k\gamma \equiv 1 \bmod n$

$\left.\begin{array}{l} \gamma a \equiv \gamma b \bmod n \\ k \equiv k \bmod n \end{array}\right\} \Rightarrow \underbrace{k\gamma a}_{1} \equiv \underbrace{k\gamma} b \bmod n \Rightarrow 1a \equiv 1b \bmod n \Rightarrow$
$\Rightarrow a \equiv b \bmod n$

Θεώρημα Έστω $d=$ μκδ(a,n) Αν $a\equiv b \bmod n$, τότε $d=$ μκδ(b,n)

Απόδειξη $d=$ μκδ(a,n). Έστω $\delta=$ μκδ(b,n)

$a\equiv b \bmod n \Leftrightarrow n \mid a-b \Leftrightarrow a-b=\lambda n$

$d\mid a$, $d\mid n$: $d \mid 1\cdot a + (-\lambda)\cdot n = b$, $d\mid n$, $d\mid b$

d: κοινός διαιρέτης των b, n, άρα διαιρεί και τον μκδ(b,n), δηλαδή $d\mid\delta$

$[2]_6=\{b \mid b\equiv 2 \bmod 6\}$
$=\{\dots -4, 2, 8, 14, 20, \dots\}$
Ο μκδ είναι ο ίδιος για όλη την κλάση!

$\delta=$ μκδ$(b,n) \Rightarrow \delta\mid b$, $\delta\mid n$; $\delta \mid 1\cdot b + \lambda\cdot n = a$, $\delta\mid n$; $\delta\mid a$, $\delta\mid n$ $\Rightarrow \delta \mid$ μκδ$(a,n)=d$, $\delta\mid d$

Συνεπώς $d\mid\delta$, $\delta\mid d \Rightarrow \delta=d$

Δακτύλιος των κλάσεων υπολοίπων modulo n

$n\in\mathbb{N}$, $a\equiv b \bmod n \Leftrightarrow n\mid a-b$ (σχέση ισοδυναμίας)

$[a]_n=\{b\in\mathbb{Z} \mid a\equiv b \bmod n\}$ → κλάση ισοδυναμίας modulo n του a

$\mathbb{Z}_n=\{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$ → περιέχει η σειρά

↳ δακτύλιος των κλάσεων υπολοίπων modulo n

$(\mathbb{Z}_n, +, \cdot)$

$[a]_n+[b]_n=[a+b]_n$

$[a]_n[b]_n=[ab]_n$

Ιδιότητες

$([a]_n+[b]_n)+[\gamma]_n=[a+b]_n+[\gamma]_n=[(a+b)+\gamma]_n=$

$= [a+(\beta+\gamma)]_n = [a]_n + [\beta+\gamma]_n = [a]_n + ([\beta]_n + [\gamma]_n)$.

Ισχύει η προσεταιριστική ιδιότητα

① $([a]_n + [\beta]_n) + [\gamma]_n = [a]_n + ([\beta]_n + [\gamma]_n)$

② $[a]_n + [0]_n = [a]_n$

③ $[a] + [-a]_n = [0]_n$

④ $[a]_n + [\beta]_n = [\beta]_n + [a]_n$

⑤ $([a]_n [\beta]_n)[\gamma]_n = [a]_n([\beta]_n [\gamma]_n)$

⑥ $([a]_n + [\beta]_n)[\gamma]_n = [a]_n[\gamma]_n + [\beta]_n[\gamma]_n$

⑦ $[a]_n([\beta]_n + [\gamma]_n) = [a]_n[\beta]_n + [a]_n[\gamma]_n$

⑧ $[a]_n[\beta]_n = [\beta]_n[a]_n$

⑨ $[a]_n[1]_n = [a]_n$

Από (1) εως (3): ομάδα
Από (1) εως (4): αβελιανή ομάδα
Από (1) εως (7): δακτύλιος
Από (1) εως (8): μεταθετικός δακτύλιος

Ορισμός Το $[a]_n \in \mathbb{Z}_n$ ονομάζεται αντιστρέψιμο αν υπάρχει $[\beta]_n \in \mathbb{Z}_n$, τέτοιο ώστε $[a]_n[\beta]_n = [1]_n$

Θεώρημα Ένα στοιχείο $[a]_n \in \mathbb{Z}_n$ είναι αντιστρέψιμο αν και μόνο αν $\mu\kappa\delta(a,n)=1$

Παράδειγμα $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$
Αντιστρέψιμα στοιχεία του $\mathbb{Z}_6$:
$U(\mathbb{Z}_6) = \{[1]_6, [5]_6\}$
$[1]_6[1]_6 = [1]_6$
$[5]_6[5]_6 = [1]_6$

Απόδειξη ($\Rightarrow$) $[a]_n$ αντιστρέψιμο $\Rightarrow$ υπάρχει $[b]_n \in \mathbb{Z}_n$, τέτοιο ώστε $[a]_n[b]_n = [1]_n \Rightarrow [ab]_n = [1]_n \Rightarrow ab \equiv 1 \bmod n \Rightarrow$
$\Rightarrow n \mid ab-1 \Rightarrow ab-1 = \lambda n$
Έστω $d = \mu\kappa\delta(a,n) \Rightarrow \begin{matrix} d \mid a \\ d \mid n \end{matrix} \Big\} \; d \mid ba + (-\lambda)n = 1 \Rightarrow d \mid 1 \Rightarrow$
$\Rightarrow d = 1$

($\Leftarrow$) $\mu\kappa\delta(a,n)=1 \overset{\text{ευκλείδου}}{\Longrightarrow} 1 = \kappa a + \lambda n, \; \kappa, \lambda \in \mathbb{Z}$
$[1]_n = [\kappa a + \lambda n]_n$
$[\kappa a + \lambda n]_n = [1]_n$
$[\kappa a]_n = [1]_n \Rightarrow [\kappa]_n[a]_n = [1]_n$.
Άρα, $[a]_n \in \mathbb{Z}_n$ αντιστρέψιμο.

Φυλλάδιο #6
Άσκηση 4 Δείξτε ότι η κλάση υπολοίπων $[10]_{21}$ είναι αντιστρέψιμη ως στοιχείο του $\mathbb{Z}_{21}$ και βρείτε την αντίστροφη κλάση.

$\mu\kappa\delta(10,21)=1 \Rightarrow [10]_{21}$ είναι αντιστρέψιμη
$21 = 2 \cdot 10 + 1, \; 1 = 21 - 2 \cdot 10$
$1 \equiv 21 - 2 \cdot 10 \bmod 21$
$1 \equiv -2 \cdot 10 \bmod 21$
$[1]_{21} = [-2]_{21}[10]_{21}$
Άρα, η αντιστρέψιμη κλάση του $[10]_{21}$ είναι η $[-2]_{21} = [19]_{21}$

Φυλλάδιο #6

Άσκηση 5 Δείξτε ότι η κλάση $[69]_{155}$ δεν είναι αντιστρέψιμη ως στοιχείο του $\mathbb{Z}_{155}$.

$\text{ΜΚΔ}(69, 155) =$

$155 = 2 \cdot 69 + 31$
$69 = 2 \cdot 31 + 0$
Άρα $\text{ΜΚΔ}(69, 155) = 31 \neq 1$
Άρα η κλάση $[69]_{155}$ δεν είναι αντιστρέψιμη.

Κριτήρια Διαιρετότητας

Έστω $a = a_m \cdot 10^m + \dots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 =$
$= (a_m \dots a_2 a_1 a_0)_{10}$, $0 \leq a_i \leq 9$
↳ δεκαδικό σύστημα

και $s(a) = a_m + \dots + a_2 + a_1 + a_0$
$g(a) = (-1)^m a_m \dots + a_2 - a_1 + a_0$ (τα πρόσημα εναλλάξ)
Τότε:
(i) $9 | a$ αν και μόνο αν $9 | s(a)$
(ii) $3 | a$ αν και μόνο αν $3 | s(a)$
(iii) $11 | a$ αν και μόνο αν $11 | g(a)$
(iv) $5 | a$ αν και μόνο αν $5 | a_0$
(v) $2 | a$ αν και μόνο αν $2 | a_0$

Απόδειξη (i) $9 | a \iff a \equiv 0 \bmod 9$
$a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \bmod 9$, $10 \equiv 1 \bmod 9$
$\iff a_m \cdot 1^m + a_{m-1} \cdot 1^{m-1} + \dots + a_2 \cdot 1^2 + a_1 \cdot 1 + a_0 \equiv 0 \bmod 9$

$\iff s(a) \equiv 0 \bmod 9 \iff 9 | s(a) - 0 \iff 9 | s(a)$

(iii) $11 \mid a \iff a \equiv 0 \bmod 11 \iff$

$\iff a_m 10^m + \dots + a_2 10^2 + a_1 \cdot 10 + a_0 \equiv 0 \bmod 11 \quad , 10 \equiv -1 \bmod 11$

$\iff a_m (-1)^m + \dots + a_2 (-1)^2 + a_1 (-1) + a_0 \equiv 0 \bmod 11$

$\iff f(a) \equiv 0 \bmod 11 \iff 11 \mid f(a) - 0 \iff$

$\iff 11 \mid f(a)$