26/11/2018

Ο δακτύλιος των κλάσεων υπολοίπων μόδιο n
$Z_n = \{[0]_n, [1]_n, \dots [n-1]_n\}$ → n στοιχεία

Παράδειγμα $[1]_7 = [8]_7 = [71]_7 = [-6]_7$

$[a]_n + [b]_n = [a+b]_n$
$[a]_n \cdot [b]_n = [ab]_n$

$U(Z_n) = \{[a]_n / \text{μκδ}(a,n) = 1\}$
τα αντιστρέψιμα στοιχεία του Z_n
Ο $U(Z_n)$ έχει φ(n) στοιχεία.

Παράδειγμα $Z_{10} = \{[0]_{10}, [1]_{10}, [2]_{10}, [3]_{10}, [4]_{10}, [5]_{10}, [6]_{10}, [7]_{10}, [8]_{10}, [9]_{10}\}$

* Το $[0]_{10}$ είναι ίδιο με το $[10]_{10}$

$U_2 Z_{10} = \{[2020]_{10}, [-9]_{10}, [82]_{10}, [-17]_{10}, [55]_{10}, [-34]_{10}, [107]_{10}, [8]_{10}, [-1]_{10}\}$

$U(Z_n) = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$
$\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = (2-1)(5-1) = 4$

$[1]^{-1}_{10} = [1]_{10}$, $[3]^{-1}_{10} = [7]_{10}$, $[7]^{-1}_{10} = [3]_{10}$, $[9]^{-1}_{10} = [9]_{10}$

Άσκηση Είναι το $[17]_{42}$ αντιστρέψιμο? Αν ναι, ποιος είναι ο αντίστροφος του $[17]_{42}$?

$\mu\kappa\delta(17,42) = 1$
Επομένως, $[17]_{42}$ είναι αντιστρέψιμο.
$42 = 2 \cdot 17 + 8$
$17 = 2 \cdot 8 + 1$
$8 = 8 \cdot 1 + 0$
Γραμμικός συνδυασμός του 1: $1 = 17 - 2 \cdot 8 =$
$= 17 \cdot 2(42 - 2 \cdot 17) =$

$\Rightarrow 1 = 5 \cdot 17 - 2 \cdot 42$
↳ είναι ο αντίστροφος του 17
$1 \equiv 5 \cdot 17 - 2 \cdot 42 \bmod 42$
$1 \equiv 5 \cdot 17 \bmod 42$
$[5]_{42}[17]_{42} = [1]_{42}$
Επομένως, ο αντίστροφος του $[17]_{42}$ είναι ο $[5]_{42}$

$Z_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$
$U(Z_5) = \{[1]_5, [2]_5, [3]_5, [4]_5\}$
* Z_5 → σώμα
Z_p → σώμα αν και μόνο αν p: πρώτος αριθμός

Ορισμός Ονομάζουμε πλήρες σύστημα υπολοίπων modulo n ένα σύνολο από n ακέραιους αριθμούς τέτοιο ώστε $a_i \not\equiv a_j \bmod n$

Παράδειγμα: Πλήρες σύστημα υπολοίπων mod 10
$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\{100, 101, 102, 103, 104, 105, 106, 107, 108, 109\}$

{37, 38, 39, 40, 41, 42, 43, 44, 45, 46}

{73, 41, 2000, 37, 65, 102, 16, 74, -2, 999}

- Σύνηθες πλήρες σύστημα υπολοίπων
{0, 1, 2, ..., n-1}
- {n = 2k+1} (περιττός)
{-k, ..., -2, -1, 0, 1, 2, ..., k}
- {n = 2k} (άρτιος)
{-k+1, ..., -2, -1, 0, 1, 2, ..., k}
- Άλλο σύνηθες πλήρες σύστημα υπολοίπων:
{1, 2, ..., n-1, n}

είναι ίσα

Θεώρημα Αν n είναι ένας φυσικός περιττός αριθμός και {x1, x2, ..., xn} είναι ένα πλήρες σύστημα υπολοίπων, τότε:
{x1 + x2 + ... + xn ≡ 0 mod n}

Απόδειξη x1 + x2 + ... + xn ≡ -k ... -2 -1 + 0 + 1 + 2 + .. + k mod n
≡ 0 mod n

{* 1 + 2 + .. + n ≡ n(n+1)/2 mod n}

1 + 2 + ... + n ≡ n(n+1)/2 mod n
≡ n((n+1)/2) mod n
≡ 0 mod n (καθώς το (n+1)/2 είναι πολλαπλάσιο του n)

Θεώρημα Αν n είναι ένας φυσικός άρτιος αριθμός και $\{x_1, x_2, \dots, x_n\}$ είναι ένα πλήρες διαστήμα υπολοίπων, τότε:

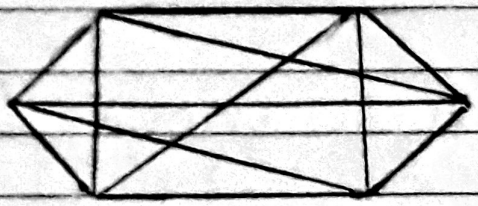
$$x_1 + x_2 + \dots + x_n \equiv \frac{n}{2} \bmod n$$

Απόδειξη

$$\begin{aligned} x_1 + x_2 + \dots + x_n &\equiv 1 + 2 + \dots + n \bmod n \\ &\equiv \frac{n(1+n)}{2} \bmod n \\ &\equiv \frac{n}{2}(n+1) \bmod n \\ &\equiv \frac{n}{2} \cdot 1 \bmod n \\ &\equiv \frac{n}{2} \bmod n \end{aligned}$$

Εκτός ύλης

* κανονικό $2n$-γώνιο (άρτιο πλήθος πλευρών)



Όποια διαδρομή χάμηλων διαλέξαμε, θα κυνδύνευε παράλληλα

(Z_6, Z_2)

$(3,1) + (1,1) + (2,0) = (0,0)$

$(2,1) + (5,1) + (5,0) = (0,0)$

Γενικά (διαδρομή)

$P_1 + P_2 + x_1 = (0,0)$

$P_2 + P_3 + x_2 = (0,0)$

$P_3 + P_4 + x_3 = (0,0)$

$\vdots$

$P_6 + P_1 + x_6 = (0,0)$

$$2\sum_{i=2}^{6} P_i + \sum x_i = (0,0)$$

Σε κάθε διαδρομή Hamilton, το άθροισμα των διευθύνσεων είναι μηδέν
Σxi = (0,0)
Έστω ότι όλες οι διευθύνσεις δεν κινήθηκαν παράλληλα (κινήθηκαν διαφορετικά)
(0,0) + (1,0) + (2,0) + (3,0) + (4,0) + (5,0) = (0,0)
(3,0) = (0,0) άτοπο!
Άρα, οι διευθύνσεις κάποια στιγμή θα κινηθούν παράλληλα

Θεώρημα Αν τα $\{x_1, x_2, \ldots, x_n\}$ είναι ένα πλήρες σύστημα υπολοίπων modulo n και a ακέραιος με $\mu\kappa\delta(a,n)=1$, τότε και $\{ax_1, ax_2, \ldots, ax_n\}$ είναι ένα πλήρες σύστημα υπολοίπων

Παράδειγμα : $\{0,1,2,3,4,5\}$ είναι ένα πλήρες σύστημα υπολοίπων modulo 6
$\mu\kappa\delta(101,6)=1$
$\{0, 101, 202, 303, 404, 505\}$

Απόδειξη $x_i \not\equiv x_j \bmod n$ με $i \neq j$
Το σύνολο $\{ax_1, ax_2, \ldots, ax_n\}$ έχει n στοιχεία και ισχυριζόμαστε ότι $ax_i \not\equiv ax_j \bmod n$, αν $i \neq j$
Έστω ότι $ax_i \equiv ax_j \bmod n$ για $i \neq j$
$\mu\kappa\delta(a,n) = 1 \Rightarrow x_i \equiv x_j \bmod n$, Άτοπο!
Άρα $ax_i \not\equiv ax_j \bmod n$, $i \neq j$
Επομένως, $\{ax_1, ax_2, \ldots, ax_n\}$ είναι ένα πλήρες σύστημα υπολοίπων.

Ορισμός Ονομάζουμε περιορισμένο σύστημα υπολοίπων ένα σύνολο από $\varphi(n)$ σε πλήθος ακεραίους $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ τέτοιους ώστε:
i) $\mu\kappa\delta(a_i, n) = 1$ για κάθε i
ii) $a_i \not\equiv a_j \bmod n$ για $i \neq j$