Επανάληψη

10/01/2017

$\mathbb{N}$ φυσικοί $+, \cdot$
;;;

$\mathbb{Z}$ ακέραιοι $+, \cdot, -$;;;
όλα κοινά

$\mathbb{Q}$ ρητοί $+, \cdot$
όλα κοινά

Σχέση ισοδυναμίας σε ένα σύνολο A

$\{(a,b) \mid = R \subseteq A \times A \quad a \text{ ισοδύναμο } b\}$
;;;

1) Ανακλαστική $\forall a \in A \Rightarrow aRa$
2) Συμμετρική $\text{Αν } aRb \Rightarrow bRa$
3) Μεταβατική $\text{Αν } aRb \text{ και } bRc \Rightarrow aRc$

Τρεις τις κλάσεις ισοδυναμίας ...

$\bar{a} = [a]_R$ κλάση ισοδυναμίας του a

$\bar{a} = \{b \mid aRb\}$

A διαμερίζεται ως προς R
όταν σε κομμάτια

Ορίζουμε $a \equiv_n b$ αν $a-b$ διαιρείται με το n
↑
σχέση ισοδυναμίας
Δηλαδή $a-b = kn$ με $k \in \mathbb{Z}$

Κλάσεις $= [0]_n, [1]_n, \ldots, [n-1]_n$ δηλαδή οι κλάσεις διαφέρουν από το υπόλοιπο της διαίρεσης με το n.

Ευκλείδης $a = n\pi + \upsilon$ μοναδικά με $a, n, \pi, \upsilon \in \mathbb{Z}$
με $0 \le \upsilon \le |n|$

$\mathbb{Z}_n = \{[0]_n, \dots, [n-1]_n\}$ $\underline{\oplus}$, $\underline{\odot}$
όλα καλά — κάποιες δομές προβληματικές

$\mathbb{Z}_6$ $[2]_6 \odot [3]_6 = [0]_6$

Αν n πρώτος $\Rightarrow$ $\underline{\mathbb{Z}_p}$ όλα καλά

Πρώτοι διαιρέτες μόνο 1 και εαυτός του

Ευκλείδης → άπειροι πρώτοι

$\forall n \in \mathbb{N}$ $n = p_1^{k_1} p_2^{k_2} \dots p_\ell^{k_\ell}$ μοναδικά

Δεν υπάρχει τύπος για τους πρώτους

→ Μ.Κ.Δ. $(a,b) = \delta \iff \exists\, \kappa, \lambda \in \mathbb{Z}$ με $\delta = \kappa a + b\lambda$

$a = b\pi + \upsilon$ $\quad b = \upsilon\pi_1 + \upsilon_1$

$\delta = (a,b) = (b,\upsilon) = (\upsilon,\upsilon_1) = \dots = \delta$

Θα δώσω το κ και λ

Λύση εξισώσεων στο $\mathbb{N}$ ή $\mathbb{Z}$

⊕ $ax \equiv b \bmod n$ έχει μοναδική λύση $\iff (a,n) = 1 \iff$
$\iff \exists$ ο αντίστροφος mod n του a

$[a]_n^{-1} ax \equiv [a]_n^{-1} b \bmod n$

$x \equiv [a]_n^{-1} b \bmod n$

⊕ είχα λύση $(a,n) | b$ είχαμε (a,n) το πλήθος λύσεων

$2a + 3b = 1$ εξαρτε ακέραιες λύσεις

$(2,3) \mid 1$

$(x,y) \mid b$

$a = a_0 + 3k \quad k \in \mathbb{Z}$

Βρες μια : $a_0 = -1 \quad b_0 = 1 \Rightarrow b = b_0 - 2k$

→ Συστήματα : $\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \\ x \equiv a_3 \bmod n_3 \end{cases}$

$(n_1, n_2, n_3) = 1 \Rightarrow$ Κινέζικο Θεώρημα

→ Euler $\varphi(n) =$ πλήθος πρώτων προς το n

$\phi(p) = p - 1$ p πρώτος

$\varphi(p^k) = p^{k-1}(p-1)$

φ πολ/κη

$$\mathbb{Z}_p^* = \{[1]_p, [2]_p, \ldots, [p-1]_p\} = \{[a]_p^k \mid k = 1, 2, \ldots, p-1\} =$$

όλοι αυτοί είναι αντίστροφοι

$$= \langle a \rangle$$

$a =$ πρωταρχική ρίζα mod p

Δεν υπάρχουν πάντα πρωταρχικές ρίζες.

Τάξη του b στο mod n είναι ο ελάχιστος φυσικός k:

$b^k \equiv 1 \bmod n \quad k \mid \phi(n)$

Γραφή φυσικού με βάση κάποιο φυσικό

Βάση το 10 : $380042 =$

$= 3\cdot10^5 + 8\cdot10^4 + 0\cdot10^3 + 0\cdot10^2 + 4\cdot10^1 + 2\cdot10^0$

$(3, 8, 0, 0, 4, 2)$

Με βάση π.χ. 8 Ψηφία : $0, 1, 2, 3, 4, 5, 6, 7$.

Κάθε $n \in \mathbb{N}$ γράφεται μοναδικά

$n = a_n \cdot 8^n + a_{n-1} \cdot 8^{n-1} + \dots + a_0 \cdot 8^0$

$a_n, a_{n-1}, \dots, a_0 \in \{0, 1, 2, 3, 4, 5, 6, 7\}$

$a_n \neq 0$

$10 = 1\cdot10 = 1\cdot2^3 + 2 = 1\cdot2^3 + 0\cdot2^2 + 1\cdot2^1 + 0\cdot2^0$

$(1, 0)$ (βάση 2) $(1, 0, 1, 0)$