15/11/2016

ΙΣΟΤΙΜΙΕΣ, ΙΣΟΔΥΝΑΜΙΑ, modulo m

$a, b \in \mathbb{Z}$ $\quad a \equiv b \mod m \Leftrightarrow m / a-b$

$a-b = km$

$k \in \mathbb{Z}$

$a \equiv b \mod m$. Σχέση ισοδυναμίας

κλάσεις ισοδυναμίας

$\mathbb{Z}$ - Ξένη ένωση των κλάσεων ισοδυναμίας

ΚΛΑΣΕΙΣ ΙΣΟΔΥΝΑΜΙΑΣ

$[0]m = \{k_0 m / k_0 \in \mathbb{Z}\} \subseteq \mathbb{Z}$
$[1]m = \{k_1 m - 1 / k_1 \in \mathbb{Z}\} \subseteq \mathbb{Z}$

$[m-1]m = \{k_{m-1} m + m-1 / k_{m-1} \in \mathbb{Z}\} \subseteq \mathbb{Z}$

Δηλαδή οι κλάσεις χαρακτηρίζονται από τα υπόλοιπα της διαίρεσης με το m.

$\mathbb{Z}_m$ = Το σύνολο των κλάσεων $= \{[0]m, [1]m, \ldots, [m-1]m\}$

$\mathbb{Z} = [0]m \sqcup [1]m \sqcup \ldots \sqcup [m-1]m$

Ορίζουμε δυο πράξεις:

$\oplus : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$

το ορίζουμε εμείς

$([i]_m, [j]_m) \Rightarrow [i]_m \oplus [j]_m = [i+j]m$

$[i+km]m \oplus [j+lm]m = [i+j+km+lm]m$

$[i]m = [i+km]m \Leftrightarrow i + km \equiv i \mod m$

$[j]m = [j+lm]m$

ισχύει $[i+j]m = [i+j+km+lk]m$ ΝΑΙ

γιατί $i+j+km+lm \equiv i+j \mod m \Leftrightarrow$

$\Leftrightarrow i+j+km+lm-(i+j) =$ πολ/σιο του m

Άρα η πράξη $\oplus$ είναι καλά ορισμένη

[60]

Βλέπουμε ότι $\mathbb{Z}_m$ εφοδιάζεται με μια πράξη πρόσθεσης $\oplus$

πχ. $[1]_6 + [2]_6 = [3]_6$
$[7]_6 + [3]_6 = [15]_6$ $\quad 15 = 3 + 2 \cdot 6 \equiv 3 \mod 6$

Ερώτημα: Η πράξη $\oplus$ είναι προσεταιριστική, έχει ουδέτερο στοιχείο, υπάρχει ο αντίθετος

Προσεταιριστικότητα: Πρέπει $([i]_m \oplus [j]_m) \oplus [m]_m$
$([i]_m \oplus [j]_m) \oplus [k]_m = [(i+j)+k]_m$
$[i]_n \oplus ([j]_n \oplus [k]_n) = [i+(j+k)]_n$ ισχύει

Ουδέτερο: $[i]_m \oplus [m]_m = [i+m]_m = [i]_m$
$[m]_m = [0]_m$
$[0]_m \oplus [i]_m = [i]_m$

Αντίθετος: $[i]_m \oplus [m-i]_m = [0]_m = [m]_m$

πχ $[2]_6 + [4]_6 = [6]_6 = [0]_6$

Αντίθετη κλάση της $[i]_m$ είναι η $[m-i]_m$

Πίνακας της πρόσθεσης mod 6

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]					
[4]						
[5]						

Το σύνολο $\mathbb{Z}_m$ εφοδιάζεται με πράξεις πολ/σμού

$$[a]_m \odot [b]_m = [a\cdot b]_m$$

$$[a+km] \odot [b+\ell m] = [(a+km)\cdot(b+\ell\cdot m)]_m$$

$$(a+km)\cdot(b+\ell m) = ab + a\ell m + bk\cdot m + k\cdot\ell\cdot m^2 =$$

$$= ab + \underbrace{(a\ell + b\cdot k + k\ell\cdot m)}_{\text{πολ/σιο}}\cdot m \equiv ab \bmod m$$

$$[ab]_m = [(a+km)\cdot(b+\ell\cdot k)]_m$$

πρώτα μεταξύ τους

το 1 και 5 έχουν μόνο αντίστροφο γιατί έχουν ΜΚΔ το 1

Πίνακας του πολ/σμού mod 6

		[0]	[1]	[2]	[3]	[4]	[5]
ουδέτερο μοναδικό	[0]	[0]	[0]	[0]	[0]	[0]	[0]
$(1,6)=1$	[1]	[0]	[1]	[2]	[3]	[4]	[5]
$(2,6)=2>1$	[2]	[0]	[2]	[4]	[0]	[2]	[4]
$(3,6)=3>1$	[3]	[0]	[3]	[0]	[3]	[0]	[3]
$(4,6)=2>1$	[4]	[0]	[4]	[2]	[0]	[4]	[2]
	[5]	[0]	[5]	[4]	[3]	[2]	[1]

$[a]_m \odot [b]_m$

$(5,6)=1$

Η πράξη $\odot$ είναι προσεταιριστική: $([a]_m \odot [b]_m)\odot[c]_m = [(a\cdot b)\cdot c]$

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

Η κλάση $[1]_m$ είναι μοναδιαίο: $[a]_m \odot [1]_n = [a]_m = [1]_m \odot [a]_m$

Αντίστροφος ΕΞΑΡΤΑΤΑΙ

$\boxed{62}$

οποιοδήποτε δεν έχει μηδέν έχει αντίστροφο

Πίνακας του πολ/σμου mod 5.

⊙	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[2]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

αντίστροφος: $[1]_5 \odot [1]_5 = [1]_5$

$[0]_5 \odot [3]_5 = [1]_5$

$[3]_5 \odot [2]_5 = [1]_5$

$[4]_5 \odot [4]_5 = [1]_5$

Αντίστροφος του $[a]_m$ θα συμβολίζεται $[a]_m^{-1}$ ΟΧΙ $\cancel{\frac{1}{[a]_m}}$

$[1]_5^{-1} = [1]_5$

$[2]_5^{-1} = [3]_5$

$[3]_5^{-1} = [2]_5$

$[4]_5^{-1} = [4]_5$

$[4]_6^{-1} = ???$ $[2]_6^{-1} = ???$

$[5]_6^{-1} = [5]_6$, $[3]_6^{-1} = ?$

Παρατηρούμε ότι το $\mathbb{Z}_5$ και το $\mathbb{Z}_6$ έχουν διαφορετική συμπεριφορά ως προς τους αντιστρόφους

Ερώτημα: Πότε το $[a]_m$ θα έχει αντίστροφο;

ΠΡΟΤΑΣΗ: Υπάρχει ο αντίστροφος του $[a]_m$ ανν $(a,m)=1$

Αποδ. ($\Rightarrow$) Έστω ότι $\exists [b]_m$ με $[a]_m \odot [b]_m = [1]_m$

Άρα: $[ab]_m = [1]_m \Leftrightarrow ab - 1 = km \Leftrightarrow ab - km = 1$

Αν είχαμε $(a,m) = d \Rightarrow d / a, m \Rightarrow d / ab, km \Rightarrow d/1$

Αντίστροφα ($\Leftarrow$) Έχουμε ότι $(a,m)=1$

$$\overset{\text{Ευκλείδη}}{\Longleftrightarrow} \exists b \text{ και } k \in \mathbb{Z} \text{ με } ab + km = 1$$

$$(ab + km) \equiv 1 \mod m \Leftrightarrow$$

$$ab \equiv 1 \mod m \Leftrightarrow [ab]_m = [1]_m \Leftrightarrow$$

$$[a]_m \cdot [b]_m = [1]_m \Leftrightarrow [a]_m = [b]_m$$

ΠΟΡΙΣΜΑ: Αν m = πρώτος τότε υπάρχει αντίστροφος $[a]_m^{-1}$ για $a \not\equiv 0 \mod m$
όταν m = πρώτος θα γράφουμε p

πεπερασμένο $\mathbb{Z}_p$	$\mathbb{Z}_m$ → άπειρο
p πρώτος	m όχι πρώτος
πολύ καλό	προβληματικός
Σώμα	ο πολ/σμός

Μοιάζει με $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$

Εφαρμογή 1) Αν p πρώτος, $p>3 \Rightarrow p^2+2$ σύνθετος

Ο p θα έχει μορφή $p = k\cdot 3 + u$ $\quad u = 1$ ή 2, όχι 0

$p = 3k+1 \Rightarrow$

$p^2 = (3k+1)^2 = 9k^2+6k+1$

$p^2+2 = 9k^2+6k+3 = 3(3k^2+2k+1)$ σύνθετος

$p = 3k+2 \Rightarrow p^2 = 9k^2+12k+4 \Rightarrow p^2+2 = 9k^2+12k+6$ σύνθετος

2) Αν $n \in \mathbb{N}$, τότε $2^{2n}+5$ είναι σύνθετος

$(2^{2n}+5) \mod 3$

Στο mod 3, επειδή 3 πρώτος το $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ οι πράξεις συμπεριφέρονται καλά, όπως τις γνωρίζουμε από τους πραγματικούς

Δηλαδή αν $a \equiv b \mod p \Rightarrow a^n \equiv b^n \mod p$

$2^2 = 4 \equiv 1 \mod 3 \Rightarrow (2^2)^n \equiv 1^n \mod 3 \Rightarrow 2^{2n} \equiv 1 \mod 3 \Rightarrow 2^{2n}+5 \equiv 1+5 \mod 3 \equiv 0 \mod 3$

$\Leftrightarrow 3 / 2^{2n}+5$ σύνθετος

64

Εφαρμογή: Η εξίσωση $3x^2+2=y^2$ δεν έχει ακέραιες λύσεις
έχει άπειρες πραγματικές

<u>Ακέραιες λύσεις</u> : $3x_0^2+2=y_0^2 \quad x_0, y_0 \in \mathbb{Z}$

$(3x_0^2+2) \bmod 3 \equiv 2 \Rightarrow$

$y_0^2 \equiv 2 \bmod 3 \equiv -1 \bmod 3$

$y_0 \bmod 3 \Rightarrow y_0^2 \bmod 3$

$y_0 \bmod 3 \to [0]_3 \to y_0^2 \bmod 3 = [0]_3$

$\to [1]_3 \to \quad = [1]_3$

$\to [2]_3 \to \quad [2^2]_3 = [1]_3 \quad \neq [2]$;

Δεν υπάρχει ακέραιος y_0 ώστε $3x_0^2+2=y_0^2$