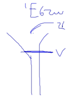
Βασική άλγεβρα
Τετάρτη 8/10/2014

Έστω ν ακέραιος θετικός.



$\alpha = \nu \cdot \pi + \upsilon$

$0 \leq \upsilon < \nu$

$\mathbb{Z}_\nu = \{\hat{0}, \hat{1}, \dots, \widehat{\nu-1}\}$

$\{\zeta \cdot \nu, \zeta \in \mathbb{Z}\}$ $\quad = \{0(\text{mod}\,\nu), 1(\text{mod}\,\nu), \dots, (\nu-1)(\text{mod}\,\nu)\}$

$\{\zeta\nu + 1, \zeta \in \mathbb{Z}\}$ $\quad = \{[0]_\nu, [1]_\nu, \dots, [\nu-1]_\nu\}$

$\vdots$

$\{\zeta\nu + (\nu-1), \zeta \in \mathbb{Z}\}$

<u>Ορισμός</u> Το $\mathbb{Z}_\nu$ το λέμε σύνολο των ακεραίων mod ν

<u>Σκέψεις</u> Για $\nu=1$, $\mathbb{Z}_1 = \{0\} = \{0(\text{mod}\,1)\} = \{[0]_1\}$

Για $\nu=2$, $\mathbb{Z}_2 = \{\underbrace{0(\text{mod}\,2)}_{\text{άρτια}}, \underbrace{1(\text{mod}\,2)}_{\text{περιττά}}\}$

Για $\nu=3$, $\mathbb{Z}_3 = \{0(\text{mod}\,3), 1(\text{mod}\,3), 2(\text{mod}\,3)\}$

<u>Πράξεις στο $\mathbb{Z}_\nu$</u>

$\alpha(\text{mod}\,\nu) + \beta(\text{mod}\,\nu) = (\alpha+\beta)(\text{mod}\,\nu)$

$\alpha+\beta \geq \nu$

$\mathbb{Z}_6$

$15(\text{mod}\,6)$

Αν $\alpha+\beta \geq \nu$ τότε $\alpha+\beta = \nu \cdot \pi + \upsilon$, $0 \leq \upsilon < \nu$

Ισχυρισμός $(\alpha+\beta)\,\text{mod}\,\nu = \upsilon(\text{mod}\,\nu)$

$w \in (\alpha+\beta)\,\text{mod}\,\nu \rightarrow w \Rightarrow \upsilon(\text{mod}\,\nu)$ $\quad \nu \mid w - \alpha - \beta \rightarrow$

$w \mid \upsilon$

$w \in \upsilon(\text{mod}\,\nu) \Longrightarrow w \in (\alpha+\beta)\,\text{mod}\,\nu$ $\quad \nu \mid \upsilon \Rightarrow \nu \mid w - \alpha - \beta$

αν $\alpha(\text{mod}\,\nu) = \alpha'(\text{mod}\,\nu)$

$\beta(\text{mod}\,\nu) = \beta'(\text{mod}\,\nu)$

$\alpha+\beta\,(\text{mod}\,\nu)$ $\quad \alpha'+\beta'(\text{mod}\,\nu)$

$\left.\begin{array}{l} \rightarrow \nu \mid \alpha - \alpha' \\ \nu \mid \beta - \beta' \end{array}\right\} \rightarrow \nu \mid (\alpha+\beta) - (\alpha'+\beta')$

$\Longrightarrow \alpha+\beta(\text{mod}\,\nu) = \alpha'+\beta'(\text{mod}\,\nu)$

Ομοίως $\alpha\beta(\text{mod}\,\nu) = \alpha'\beta'(\text{mod}\,\nu)$

άρα ορίζονται καλά οι πράξεις πολλ. και πρόσθεσης στο $\mathbb{Z}_\nu$.

$(\mathbb{Z}_\nu, +, \cdot)$ δακτύλιος των ακεραίων mod ν

$0(\text{mod}\,\nu)$ είναι το μηδενικό στοιχείο

$1(\text{mod}\,\nu)$ " " το μοναδιαίο στοιχ.

<u>Ορ</u> Το $\alpha(\text{mod}\,\nu) \in \mathbb{Z}_\nu$ ονομάζεται <u>αντιστρέψιμο</u> αν υπάρχει $\beta(\text{mod}\,\nu)$ με $\alpha(\text{mod}\,\nu)\beta(\text{mod}\,\nu) = \beta(\text{mod}\,\nu)\cdot\alpha(\text{mod}\,\nu) = 1(\text{mod}\,\nu)$

<u>$\nu=6$</u>

$\mathbb{Z}_6$

+	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	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

5, 1
6

$\mathbb{Z}_6$

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\{1, 5\}$

$\mathbb{Z}_7$ $\quad \{0, 1, 2, \dots, 6\}$

Πρόταση Αν ν ακέραιος θετικός και $\text{ΜΚΔ}(\alpha,\nu)=1$ τότε το $\alpha(\bmod \nu)\in\mathbb{Z}_\nu$ είναι αντιστρέψιμο

Απόδ Επειδή $\text{ΜΚΔ}(\alpha,\nu)=1$ τότε υπάρχουν $\kappa,\lambda\in\mathbb{Z}$ με

$$\kappa\cdot\alpha+\lambda\nu=1 \Longrightarrow$$

$$(\kappa\alpha+\lambda\nu)(\bmod \nu)=1(\bmod \nu)$$

$$\Longrightarrow \kappa\alpha(\bmod \nu)+\lambda\nu(\bmod \nu)=1(\bmod \nu)$$

$$\Longrightarrow [\kappa(\bmod \nu)][\alpha(\bmod \nu)]+\cancel{[\lambda(\bmod \nu)][\nu(\bmod \nu)]}=1(\bmod \nu)$$

$$\Longrightarrow [\kappa(\bmod \nu)]\cdot[\alpha(\bmod \nu)]=1(\bmod \nu)$$ δηλ

$\alpha(\bmod \nu)$ αντιστρ.

Πρόταση Έστω $\alpha(\bmod \nu)\in\mathbb{Z}_\nu$ αντιστρέψιμο.

Τότε $\text{ΜΚΔ}(\alpha,\nu)=1$

Απόδ Επειδή $\alpha(\bmod \nu)$ αντιστ. $\Rightarrow \exists\, \kappa(\bmod \nu)\in\mathbb{Z}_\nu$ με

$$\alpha(\bmod \nu)\cdot \kappa(\bmod \nu)=1(\bmod \nu)$$

$$\Rightarrow \nu \mid \alpha\kappa-1 \Longrightarrow \alpha\kappa-1=\lambda\cdot\nu,\ \lambda\in\mathbb{Z}$$

$$\Longrightarrow \alpha\kappa+(-\lambda)\nu=1$$

αν $d=\text{ΜΚΔ}(\alpha,\nu)\longrightarrow d\mid\alpha \longrightarrow d\mid\alpha\kappa$

$d\mid\nu \longrightarrow d\mid-\lambda\nu$

$$\longrightarrow d\mid 1 \Rightarrow d=1$$

Ορισμός Το πλήθος των ακεραίων α του συνόλου $\{1,2,\dots,\nu-1\}$ με $\text{ΜΚΔ}(\alpha,\nu)=1$ ονομάζεται τιμή συνάρτησης Euler στη $\varphi(\nu)$

$\varphi(1)=1,\ \varphi(2)=1,\ \varphi(3)=2,\ \varphi(4)=2$

$\varphi(5)=4$

Γενικά υπάρχει τύπος $\varphi(\nu)$ $\quad \varphi(p)=p-1$ p πρώτος

Παρατήρηση στο $\mathbb{Z}_7$

Αντιστρ. στοιχεία $\quad 1(\bmod 7),\ 2(\bmod 7),\dots,6(\bmod 7)$

$1\longrightarrow 4\cdot1=4$

$2\longrightarrow 4\cdot2=1$

$3\sim 4\cdot3=5$

$4\sim 4\cdot4=2$

$5\sim 4\cdot5=6$

$6\sim 4\cdot6=3$

$$1\cdot2\cdot3\cdot4\cdot5\cdot6=4^6\, 6!(\bmod 7) \sim 4^6(\bmod 7)=1(\bmod 7)$$

$6!(\bmod 7)$

$$\Leftrightarrow 7\mid 4^6-1$$

Ερώτημα Αν $\alpha(\bmod \nu)\in\mathbb{Z}_\nu$ αντιστρ. τότε

$$\alpha(\bmod \nu)\cdot x(\bmod \nu)=\alpha(\bmod \nu)\cdot y(\bmod \nu)\Longrightarrow$$

$$x(\bmod \nu)=y(\bmod \nu)$$

Απ. $\exists\, \kappa(\bmod \nu):\ \alpha\cdot\kappa=1(\bmod \nu)$

$$\kappa\cdot\alpha\, x(\bmod \nu)=\kappa\cdot\alpha\, y(\bmod \nu)\Longrightarrow x=y(\bmod \nu)$$

(Μικρό) **Θεώρημα Fermat** Αν p πρώτος, $\alpha\in\mathbb{Z}$ τότε

$$p\mid \alpha^p-\alpha$$

Θεώρημα Euler ν θετικός ακέραιος $\alpha\in\mathbb{Z}$, $\text{ΜΚΔ}(\alpha,\nu)=1$

τότε $\nu\mid \alpha^{\varphi(\nu)}-1$

Απόδειξη Θεωρήματος (μικρού) Fermat

α) Αν $\alpha(\bmod \nu)\in\mathbb{Z}_p$, p πρώτος και $\alpha(\bmod p)$ αντιστρ. τότε

$$\alpha(\bmod p)\cdot x(\bmod p)=\alpha(\bmod p)\cdot y(\bmod p)\longrightarrow$$

$$x(\bmod p)=y(\bmod p)$$ έχει ήδη αποδειχθεί.

β) Αν $\alpha(\bmod p)$, $\beta(\bmod p)$ αντιστρ. τότε $\alpha\beta(\bmod p)$ αντιστ. $\Big\}$ άσκηση

Απόδ

$1(\bmod p)\sim \alpha\cdot(\bmod p)$

$2(\bmod p)\sim \alpha\cdot2(\bmod p)$

$\vdots$

$(p-1)(\bmod p) \quad \alpha(p-1)\bmod p$,

$p\nmid\alpha \Leftrightarrow \text{ΜΚΔ}(\alpha,p)=1$

$$(p-1)!\,\cancel{(\bmod p)}=\alpha^{p-1}\cdot\cancel{(p-1)!}$$

$$p\mid \alpha^{p-1}-1$$