Matematika 4, 7. travnja 2021.

Modularna aritmetika: aritmetika modulo neki prirodni broj

$m, n, p \in \mathbb{Z}$, $p \neq 0$

$m \equiv n \pmod p \overset{def}{\iff} \exists k \in \mathbb{Z},\ m = n + k \cdot p$

npr. $3 \equiv 11 \pmod 8$ ← sa i bez zagrade

$\equiv_h$ $3 \equiv 3 \pmod 8$

$3 \equiv 27 \pmod 8$

jednakost modulo p je relacija ekvivalencije na skupu cijelih brojeva

$H \subset G$ normalna podgrupa tj. $\forall h \in H \forall g \in G,\ ghg^{-1} \in H$

$g \sim_H g' \iff gH = g'H$ tj. $\exists h \in H,\ gh = g'$

$G/H = \{ [g] \mid g \in G \}$

Ako je G Abelova, npr. $\mathbb{Z}$, tada $ghg^{-1} = h$, dakle

Svaka podgrupa je normalna

$p\mathbb{Z} = \{ m \in \mathbb{Z} \mid m \equiv 0 \pmod p \} = \{ 0, \pm p, \pm 2p, \pm 3p, \dots \}$ je podgrupa Abelove grupe $(\mathbb{Z}, +, 0)$

$\exists k,\ m - 0 = kp,\ k \in \mathbb{Z}$

$m = kp$

$m \sim_{p\mathbb{Z}} n \iff m \equiv n \bmod p$

$\mathbb{Z}/p\mathbb{Z} = \{ [0], [1], [2], \dots, [p-1] \}$

$p\mathbb{Z}$

suprotni element od [m] je [p-m] jer [m]=[p-m] = [p] = [0]

$\forall m \in \mathbb{Z} \forall p > 0 \exists! k \in \mathbb{N}_0 \exists! n \in \{0, 1, 2, \dots, p-1\}$

$m = kp + n$ (matematika 1)

$27 = 8 \cdot 3 + 3 \Rightarrow 27 \equiv 3 \pmod 8$

$0 \leq 3 < 8$

$27 = 8 \cdot 2 + 11$ parcijalno dijeljenje

ostatak $> p - 1 = 7$

MNOŽENJE

$(\mathbb{Z}, \cdot, 1)$ je zatvoreno na $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

asocijativno, komutativno, ima neutr. elem. 1 } monoid

$\forall m\ \exists m^{-1}$ ne! nema inverza

$(\mathbb{Z}, +, 0, \cdot, 1)$ komutativan prsten: Abelova grupa za zbrajanje, monoid za množenje i distributivnost

$(\mathbb{Z}/\mathbb{Z}p, +, \cdot, 0, 1)$ također prsten, prsten klasa ostataka mod p

$\mathbb{Z}/p\mathbb{Z} = \{ [0], [1], [2], \dots, [p-1] \}$

Množenje $[m] \cdot [n] = [m \cdot n]$ je dobro definirano jer

$\{m + k\,p \mid k \in \mathbb{Z}\} \cdot \{n + k'p \mid k \in \mathbb{Z}\}$ je skup svih elemenata

ujedno i asocijativno, komutativno i s neutralnim elementom [1]

oblika $(m + k \cdot p)(n + k' \cdot p) = m \cdot n + k \cdot p \cdot n + k' \cdot p \cdot m + k \cdot k' \cdot p \cdot p$

$= m \cdot n + (k \cdot n + k' \cdot m + k \cdot k' \cdot p) \cdot p = m \cdot n \pmod p$

$p=4$ nema inverze

$[2]\cdot[2]=[0]$

$2\cdot 2 = 4 \equiv 0 \pmod 4$

Postoji li m takav da

$0\cdot m \equiv 1 \pmod p$, $p=4$

$0 \equiv 1 \pmod 4$?

$0-1 = 4\cdot p$

$4p = -1$ ne

$[2]^{-1}$ ne postoji

$2n \equiv 1 \bmod 4$

$2n=1$ X

$2n=5$ X

$2n=9$ X

$2n=13$ X

↑ neparni brojevi

$-[2]_4=[4]_4$

$-[m]=[p-m]$

$\mathbb{Z}/p\mathbb{Z}$ je polje ji svaki element $\neq[0]$ ima inverz

p prost broj

$p=5$

$\mathbb{Z}/5\mathbb{Z} = \{[0],[1],[2],[3],[4]\}$

ima inverz samo $[0]$

$[0]\cdot[m]=[1]$

$m \in \{0,1,2,3,4\}$

$\mathbb{Z}/p^n\mathbb{Z}$ p prost

$5k\cdot(5k'+m) = 1+5k''$ $[m]^{-1}=[n]$

$1 = 5(k\cdot(5k'+m)-k'')$ nema rješenja, $[0]^{-1}$ ne postoji

$\forall m \neq 0$ postoji li m' $[m]\cdot[m]^{-1}=[1]$

$(m+5k)(n+5k') = 1+5k''$

$m\cdot n - 1 \equiv 0 \pmod 5$

$m=1$ $1\cdot n - 1 \equiv 0 \pmod 5$

$n=1$

$m=2$ $2\cdot n - 1 \equiv 0 \pmod 5$

$2n \equiv 1 \pmod 5$

$2n = 6 \Rightarrow n=3$

„$[2]^{-1}$"

$[2]\cdot[3]=[1]$

$6 \equiv 1 \bmod p$

$m=3$ $3\cdot n - 1 \equiv 0 \pmod 5$

$3n = 1+5k$, $k=1$

$3n=6$, $n=2$

$[3]\cdot[?]=[1]$

„$[3]^{-1}$"

$[4]\cdot[4]=[1]$

$4\cdot n - 1 \equiv 0 \pmod 5$

$4n = 1+5k$

$k=0$ $4n=1$ X

$k=1$ $4n=6$ X

$k=2$ $4n=11$ X

$k=3$ $4n=16$

$n=4$ „ $1 \bmod 5$

$4\cdot 4 = 16 \equiv 1 \bmod 5$