IPMVFMF 2025-03-18

N

let p liho praštevilo

a.) pokaži, da tvori množica neničelnih kvadratov v $\mathbb{Z}_p$ grupo za množenje moči $\frac{p-1}{2}$.

$\mathbb{Z}_p^* := (\mathbb{Z}_p \setminus \{0\}, \cdot)$

p	kvadrati
3	1
5	1,4

izgleda, da velja.

dokažimo.

oglejmo si $s : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$
$x \mapsto x^2$

hmg $\quad s(g \cdot h) = s(g) \cdot s(h) \quad g, h \in \mathbb{Z}_p^*$

$(g \cdot h)^2 \bmod p = g^2 \bmod p \; h^2 \bmod p$

$ghgh = gghh$

izračunajmo $\ker s$

$$g \in \ker s \iff s(g) = 1$$
$$s(g) = g^2$$

iščemo ničle $g^2 - 1 = (g+1)(g-1)$

nad obsegom ni deliteljev niča

$g \in \{1, -1\} = \ker s$

Po izreku o izomorfizmih

$$|\mathrm{Im}\, s| = \left|\overset{p-1}{\mathbb{Z}_p^*} \Big/ \underset{2}{\ker s}\right| = \frac{p-1}{2}$$

6.) Dokaži, da je polinom x^2+1 nerazcepen v $\mathbb{Z}_p[x]$
$\Leftrightarrow$ p oblike $4k+3$ za neki $k \in \mathbb{N}_0$.

nima nobenih ničel.

opazimo si polinom $x^{p-1}-1$

prejšnjič smo videli, da so ničle tega polinoma vsi elementi za množenje

case: $p = 4k+3$

$$x^{p-1}-1 = x^{(4k+3)-1}+1 = x^{4k+2}+1$$

PDDRAA x^2+1 razcepen in ima ničlo $a \in \mathbb{Z}_p^* \Rightarrow$

$$a^2 = -1 \to (a^2)^{2k+1} = (-1)^{2k+1} \to a^{4k+2} = -1$$

$$a^{4k+2} = 1$$

$\Rightarrow$ polinom je razcepen

case: $p = 4k+1$

$$x^{p-1}-1 = x^{4k+1-1}-1 = x^{4k}-1 =$$

$$= (x^{2k}-1)(x^{2k}+1)$$

Trdimo, da je p razcepen.

$$x^{2k} \in \{-1, 1\}$$

ničle so ravno vsi elementi v $\mathbb{Z}_p^* \Longrightarrow \exists a \in \mathbb{Z}_p^* : a^{2k} = -1$

$\Rightarrow$ a^t reši enačbo $x^2+1=0$

N ———

izrek o deljenju: $p = tq + r$

kvocient ↵ ↳ ostanek

$\deg r < \deg q$ in za p sta t in r enolična.

IZRAČUNAJ kvocienta in ostanka pri deljenju polinoma p s polinomom g.

a.) $p(x) = x^5 + x^3 - x^2 - x$, $g(x) = x^3 + x$ v $\mathbb{Z}_2[x]$

$$x^5 + x^3 - x^2 - x : x^3 + x = x^2$$
$$\underline{x^5 + x^3}$$
$$x^2 + x \text{ ost.}$$

b.) $p(x) = x^5 - x^3 + x + 4$, $g(x) = 2x^3 + x + 1$ v $\mathbb{Z}_5[x]$

$$x^5 - x^3 + x + 4 : 2x^3 + x + 1 = 3x^2 + 3$$
$$3x^3 + 2x^2 + x + 4$$
$$r(x) = 2x^2 + 3x + 1$$

Opomba: V kolobarjih polinomov $K[x]$, kjer K ni obseg, izrek o deljenju ne velja vedno.

(1.) če izberemo $p(x) = x^2 + 1$, $q(x) = 2x + 3$ v $\mathbb{Z}[x]$, izrek odpove. težava: 2 ni obrnljiv el.

$$p(x) = x^2+1 = \underbrace{t(x)}_{ax+b}\cdot(2x+3) + r(x)$$

$\underbrace{}$

$2ax^2 + \dots$

$\neq$

1 za noben $a \in \mathbb{Z}$

$r(x) = r_0$

kvocient v $\mathbb{Z}[x]$ ne obstaja!

(2.) Če izberemo $p(x) = 4x^2+8$, $q(x) = 4x+8$ v $\mathbb{Z}_{12}[x]$. Kvocient ni enolično definiran:

$$(4x+8)(x+1) = 4x^2 + \underbrace{8x+4x}_{=0} + 8 = 4x^2+8 = p(x)$$

$$(4x+8)(x+4) = 4x^2 + \underbrace{8x+16x}_{=0} + \underbrace{32}_{=8} = 4x^2+8 \; p(x)$$

Definicija: Let F obseg in $p,q \in F[x]$. $\gcd(p,q)$ je polinom d, ki zadošča naslednjim pogojem:

$d \mid p \wedge d \mid q \wedge \forall x \in F[x] : (x \mid p \wedge x \mid q) \Rightarrow x \mid d \wedge$

$\wedge$ $\underbrace{\text{vodilni koeficient } p \text{ je } 1}_{\text{monični polinom}}$

Izrek: $\gcd(p,q)$ obstaja in je enolično določen. Poleg tega $\exists$ taki polinoma s in t $\in F[x]$ $\ni$: $s \cdot p + t \cdot q = d$

$\gcd(p,q)$ je moč izračunati z evklidovim algoritmom.

Def.: $r_0 := p$ $r_1 := q$ nato induktivno definiramo polinome

t_i, r_i , $i \geq 2$:

- $r_0 = t_2 r_1 + r_2$
- $r_1 = t_3 r_2 + r_3$

$\vdots$

- $r_m = t_{m+2} \cdot r_{m+1} + \underline{\underline{r_{m+2}}}$ gcd
- $r_{m+1} = t_{m+3} \cdot r_{m+2} + 0$

N izračunaj $d := \gcd(p, q)$ in poišči s in t tako, da je $sp + tq = d$

a.) $\left.\begin{aligned} p(x) &= x^3 + 4x^2 + 3x - 2 \\ q(x) &= x^3 + 3x^2 + 3x + 2 \end{aligned}\right]$ v $\mathbb{Q}[x]$