Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 11

Polinomi nad beskonačnim poljima

Polinomske funkcije nad beskonačnim poljima (1/2)

Pokazaćemo: Za beskonačna polja važi da $(Pol(F), +, \cdot)$ jeste domen integriteta i da je izomorfan sa $(F[x], +, \cdot)$. Zato ćemo nad beskonačnim poljima umesto $f_p(x)$ pisati samo $p(x)$, tj. nećemo praviti razliku između polinoma i polinomskih funkcija.

Lema

Neka je F beskonačno polje. Tada za $p(x) \in F[x]$ važi $p(x) = 0$ akko $(\forall x \in F) f_p(x) = 0$, tj. svi elementi polja su koreni polinoma $p(x)$.

Dokaz

($\Rightarrow$) *Ako je $p(x) = 0$ tada je $f_p(x) = 0$, za sve $x \in F$.*

($\Leftarrow$) *Neka je $p(x)$ polinom takav da je svako $x \in F$ njegov koren. Za polinom $p(x)$ važi $p(x) = 0$ ili $deg(p(x)) = n$ za $n \geq 0$. Neka je $deg(p(x)) = n$. Tada na osnovu teoreme o maksimalnom broju korena polinoma imamo da $p(x)$ može imati najviše n korena, što je u kontradikciji sa pretpostavkom da su svi elementi polja F koreni polinoma $p(x)$ i da polje F ima beskonačno mnogo elemenata. Dakle, mora važiti $p(x) = 0$.*

Polinomske funkcije nad beskonačnim poljima (2/2)

Teorema

Neka je F beskonačno polje. Polinomi $p(x), q(x) \in F[x]$ su jednaki akko su jednake njihove polinomske funkcije.

Dokaz

($\Rightarrow$) *Ako je $p(x) = q(x)$ tada važi $f_p(x) = f_q(x)$.*

($\Leftarrow$) *Neka je $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, sa $a_n \neq 0$, i $q(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, sa $b_m \neq 0$, i neka je $n \geq m$ (slučaj kada je $n \leq m$ je analogan). Neka je $f_p(x) = f_q(x)$ za svako $x \in F$, odakle imamo $f_p(x) - f_q(x) = 0$, odnosno $(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) - (b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0) = 0$, tj. $a_n x^n + \ldots + a_{m+1}x^{m+1} + (a_m - b_m)x^m + \ldots + (a_1 - b_1)x + (a_0 - b_0) = 0$. Na osnovu prethodne leme sledi da $a_n x^n + \ldots + a_{m+1}x^{m+1} + (a_m - b_m)x^m + \ldots + (a_1 - b_1)x + (a_0 - b_0)$ mora biti nula polinom, odakle sledi $n = m$ (jer smo pretpostavili $a_n \neq 0$) i $a_n = b_n, \ldots, a_0 = b_0$, tj. $p(x) = q(x)$.*

Koreni polinoma nad $\mathbb{C}$

Gaus je krajem *XIX* veka dokazao sledeću teoremu (koju mi dajemo bez dokaza).

Teorema (Osnovni stav algebre)

Svaki polinom stepena većeg od nule nad poljem kompleksnih brojeva ima bar jedan koren u tom polju.

Posledica

Ako je $p(x) \in \mathbb{C}[x]$ *i* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, *za* $n > 0$, *tada postoje* $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ *(koji se mogu ponavljati) takvi da je*

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$$

Dokaz

Imamo da je $p(x) = a_n p_n(x)$, *gde je* $p_n(x)$ *normalizovan polinom stepena n. Na osnovu prethodne teoreme, znamo da* $p(x)_n$ *ima jedan koren u* $\alpha_n \in \mathbb{C}$, *pa iz Bezuovog stava sledi* $p(x) = a_n(x - \alpha_n)p_{n-1}(x)$, *gde je* $p_{n-1}(x)$ *normalizovan polinom stepena* $n - 1$. *Ako sada primenimo prethodnu teoremu na* $p_{n-1}(x)$ *i postupak ponovimo još* $n - 2$ *puta, dobijamo* $p(x) = a_n(x - \alpha_n)\ldots(x - \alpha_1)$.

Kompleksni koreni

Napomena

- *Niti teorema niti posledica ne govore ništa o tome kako naći kompleksne korene, samo kažu da postoje*
- *Iz prethodnih rezultata sledi da je svaki polinom stepena većeg od* 1 *nad poljem kompleksnih brojeva svodljiv*

Napomena

- *Za kvadratni polinom* $ax^2 + bx + c$ *znamo da su koreni* $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$, *odakle sledi da ako su* $a, b, c \in \mathbb{R}$ *i ako je neki kompleksni broj* $\alpha \in \mathbb{C} \setminus \mathbb{R}$ *koren polinoma (diskriminanta je manja od nule) tada je njegov konjugovani* $\overline{\alpha}$ *takođe koren tog polinoma*
- *Sledeća teorema kaže da ovo važi za sve polinome sa realnim koeficijentima*

Konjugovano kompleksni koreni realnih polinoma

Teorema

Neka je $p(x) \in \mathbb{C}[x]$ *i* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, *za* $n > 0$ *i* $\alpha \in \mathbb{C}$ *koren polinoma* $p(x)$. *Ako su koeficijenti polinoma* $p(x)$ *realni brojevi, tj.* $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}$, *tada je i* $\overline{\alpha}$ *koren polinoma* $p(x)$.

Dokaz

Pošto je polje $\mathbb{C}$ *beskonačno, umesto* $f_p(x)$ *pisaćemo samo* $p(x)$. *Na osnovu prethodnih teorema sledi* $p(x) = a_n(x - \alpha_1)\ldots(x - \alpha_n)$, *te iz* $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}$ *imamo*

$$\overline{p(x)} = a_n\overline{x}^n + a_{n-1}\overline{x}^{n-1} + \ldots + a_1\overline{x} + a_0 = p(\overline{x}) = a_n(\overline{x} - \alpha_1)\ldots(\overline{x} - \alpha_n)$$

Sada dobijamo

$$p(x) = \overline{\overline{p(x)}} = \overline{a_n(\overline{x} - \alpha_1)\ldots(\overline{x} - \alpha_n)} = a_n(x - \overline{\alpha_1})\ldots(x - \overline{\alpha_n})$$

Dakle, ako su $\alpha_1, \ldots, \alpha_n$ *koreni polinoma* $p(x)$ *onda su to i* $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$.

Faktorizacija realnih polinoma

Napomena

Primetimo da za sve $\alpha \in \mathbb{C}$ *važi*
$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha} = x^2 - 2Re(\alpha)x + |\alpha|^2$, *te da je ovo polinom sa realnim koeficijentima jer su* $Re(\alpha)$ *i* $|\alpha|$ *realni brojevi.*

Teorema

Ako je $p(x) \in \mathbb{R}[x]$ *i* $deg(p(x)) > 1$ *tada se* $p(x)$ *nad poljem* $\mathbb{R}$ *može zapisati kao proizvod linearnih i/ili kvadratnih polinoma (i konstante).*

Dokaz

Pošto je $\mathbb{R} \subset \mathbb{C}$, *znamo da je*
$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = a_n(x-\alpha_1)\ldots(x-\alpha_n)$, *gde su* $\alpha_1, \ldots, a_n \in \mathbb{C}$. *Ako je* $\alpha_i \in \mathbb{R}$ *onda je* $x - \alpha_i$ *linearni polinom sa realnim koeficijentima. Ako je* $\alpha_i \in \mathbb{C}\backslash\mathbb{R}$ *onda je* $\overline{\alpha_i} = \alpha_j$ *za neko* $j \neq i$, *pa je na osnovu prethodne napomene* $(x-\alpha_i)(x-\alpha_j) = x^2 - 2Re(\alpha_i)x + |\alpha_i|^2$ *kvadratni polinom sa realnim koeficijentima.*

Svodljivost i koreni polinoma nad $\mathbb{R}$

Posledica

Ako je $p(x) \in \mathbb{R}[x]$ *i* $deg(p(x)) \geq 3$ *tada je* $p(x)$ *svodljiv.*

Primer

- *Ako je* $f(x) \in \mathbb{R}[x]$ *i* $f(e^{i\alpha}) = 0$, *za* $\alpha \in \mathbb{R} \setminus \{k\pi \mid k \in \mathbb{Z}\}$ *tada je*
  - $x - e^{i\alpha} \mid f(x)$
  - $x - e^{-i\alpha} \mid f(x)$ *(Konjugovani koren)*
  - $(x^2 - 2x\cos\alpha + 1) \mid f(x)$ *(Proizvod prethodna dva)*
- *Ako je* $f(x) \in \mathbb{R}[x]$ *i* $f(e^{i\alpha}) = 0$, *za* $\alpha \in \mathbb{R}$ *tada je*
  - $x - e^{i\alpha} \mid f(x)$
  - $x - e^{-i\alpha} \mid f(x)$
  - *ali* $(x^2 - 2x\cos\alpha + 1) \mid f(x)$ *ne mora da važi. Npr. za* $\alpha = 0$ *iz* $f(1) = 0$ *ne možemo zaključiti da* $(x^2 - 2x + 1) \mid f(x)$

Višestruki koreni polinoma nad $\mathbb{C}$

Podsećanje: Polinom n-tog stepena nad $\mathbb{C}$ ima n korena. Neki od tih korena se mogu ponavljati - višestruki koreni.

Teorema

Neka su $p(x), q(x) \in \mathbb{C}[x]$. Ako svaki koren od $p(x)$, višestrukosti k, jeste i koren polinoma $q(x)$, višestrukosti veće ili jednake od k, tada polinom $p(x)$ deli polinom $q(x)$.

Napomena: Traženje višestrukih korena može se uraditi deljenjem (ili Hornerovom shemom). Za polinome sa realnim koeficijentima može i pomoću izvoda polinomske funkcije.

Teorema

Koren α reda $k > 2$ polinoma $p(x)$ sa realnim koeficijentima jeste koren reda $k-1$ polinoma $p'(x)$, a takođe je i zajednički koren polinoma $p(x), p'(x), p''(x), \ldots, p^{(k-1)}(x)$ i nije koren polinoma $p^{(k)}(x)$.

Dokaz

Direktna posledica činjenice da je $p(x) = (x-\alpha)^k q(x)$, gde α nije koren polinoma $q(x)$, i $p'(x) = (x-\alpha)^{k-1}\big(kq(x) + (x-\alpha)q'(x)\big)$.

Potencijalni koreni polinoma nad $\mathbb{Q}$

Teorema

Neka je $s(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, gde su svi koeficijenti celi brojevi. Ako je racionalan broj $\frac{p}{q}$ koren polinoma $s(x)$, gde su p i q uzajamno prosti celi brojevi, tada $p \mid a_0$ i $q \mid a_n$.

Dokaz

Ako je $\frac{p}{q}$ koren polinoma $p(x)$ tada važi $a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \ldots + a_1\left(\frac{p}{q}\right) + a_0 = 0$. Ako pomnožimo sa q^{n-1} dobijamo

$$a_n\frac{p^n}{q} + a_{n-1}p^{n-1} + \ldots + a_1 pq^{n-2} + a_0 q^{n-1} = 0$$

U ovoj jednakosti svi sabirci sem prvog su celi brojevi, pa zato i prvi sabirak $a_n\frac{p^n}{q}$ mora biti ceo broj, a pošto su p i q uzajamno prosti, sledi da $q \mid a_n$. Ako sada poslednju jednakost pomnožimo sa $\frac{q}{p}$ dobijamo

$$a_n p^{n-1} + a_{n-1}p^{n-2}q + \ldots + a_1 q^{n-1} + a_0\frac{q^n}{p} = 0$$

Sada slično dobijamo da $p \mid a_0$.

Primer

Zaokruži oznaku polja nad kojima je polinom $s(x) = x^3 + x + 1$ nesvodljiv

$\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$

Primer primene: pogledajte sekciju Tejlorov polinom u knjizi.

Primer

Zaokruži oznaku polja nad kojima je polinom $s(x) = x^3 + x + 1$ nesvodljiv

$$\mathbb{Q} \qquad \mathbb{R} \qquad \mathbb{C}$$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $s(1) \neq 0$ i $s(-1) \neq 0$.

Primer primene: pogledajte sekciju Tejlorov polinom u knjizi.

Primer

Zaokruži oznaku polja nad kojima je polinom $s(x) = x^3 + x + 1$ nesvodljiv

$$\mathbb{Q} \qquad \mathbb{R} \qquad \mathbb{C}$$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $s(1) \neq 0$ i $s(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

Primer primene: pogledajte sekciju Tejlorov polinom u knjizi.

Primer

Zaokruži oznaku polja nad kojima je polinom $s(x) = x^3 + x + 1$ nesvodljiv

$$\mathbb{Q} \qquad \mathbb{R} \qquad \mathbb{C}$$

$\mathbb{Q}$: Potencijalni racionalni koreni su oblika $\frac{p}{q}$ gde $p \mid 1$ i $q \mid 1$. Zato $\frac{p}{q} \in \{1, -1\}$, pa proverom dobijamo $s(1) \neq 0$ i $s(-1) \neq 0$.

$\mathbb{R}$: Svodljiv jer je stepena većeg od 2

$\mathbb{C}$: Svodljiv jer je stepena većeg od 1

Primer primene: pogledajte sekciju Tejlorov polinom u knjizi.

Polinomi nad konačnim poljima

Polinomi nad konačnim poljima

Primer

Za polinome $p(x) = x^2 + x + 1$ *i* $q(x) = x^3 - x$ *date nad poljem* $\mathbb{Z}_3$ *izračunati:*

- $p(x) + q(x)$
- $p(x)q(x)$
- *Podeliti polinom* $q(x)$ *polinomom* $p(x)$
- *Izračunati vrednost polinomske funkcije* $f_q(x)$ *za sve* $x \in \mathbb{Z}_3$
- *Faktorisati* $p(x)$ *nad poljem* $\mathbb{Z}_3$

Napomena: Operacije sa koeficijentima izvodimo u polju $(\mathbb{Z}_3, +, \cdot)$.

Polinomske funkcije nad konačnim poljima

- Nad beskonačnim poljem F važi: ako je $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$ tačno za sve $x \in F$, tada je $a_n = \ldots = a_0 = 0$.
- Nad konačnim poljima ovo nije tačno jer, npr, nad $\mathbb{Z}_3$ važi $x^3 - x = 0$ za sve $x \in \mathbb{Z}_3$.
- Dakle, **nad konačnim poljima postoje različiti polinomi čije su polinomske funkcije jednake**, jer za $p(x) = x^3 - x$ i $q(x) = 0$ nad poljem $\mathbb{Z}_3$ važi $p(x) \neq q(x)$ i $f_p(x) = f_q(x)$.
- Generalno, ako je F polje od m elemenata, tada je $(F \setminus \{0\}, \cdot)$ grupa sa $m - 1$ elemenata, pa je $x^{m-1} = 1$, odakle je $x^m = x$, za sve $x \in F$.

Primer

Zaokruži oznaku polja nad kojima je polinom $p(x) = x^3 + x + 1$ nesvodljiv

$$\mathbb{Z}_2 \qquad \mathbb{Z}_3 \qquad \mathbb{Z}_5 \qquad \mathbb{Z}_7$$

Napomena: Nad konačnim poljima:

- Traženje korena polinoma samo po sebi nije jako zanimljivo (jer možemo direktno da proverimo za sve elemente polja da li su koreni)
- Pitanje nesvodljivosti polinoma jeste zanimljivo (kao što ćemo videti u nastavku)

Primer

Zaokruži oznaku polja nad kojima je polinom $p(x) = x^3 + x + 1$ nesvodljiv

$$\mathbb{Z}_2 \qquad \mathbb{Z}_3 \qquad \mathbb{Z}_5 \qquad \mathbb{Z}_7$$

$\mathbb{Z}_2$: Nesvodljiv jer je $p(0) = 1, p(1) = 1$

Napomena: Nad konačnim poljima:

- Traženje korena polinoma samo po sebi nije jako zanimljivo (jer možemo direktno da proverimo za sve elemente polja da li su koreni)
- Pitanje nesvodljivosti polinoma jeste zanimljivo (kao što ćemo videti u nastavku)

Primer

Zaokruži oznaku polja nad kojima je polinom $p(x) = x^3 + x + 1$ nesvodljiv

$$\mathbb{Z}_2 \qquad \mathbb{Z}_3 \qquad \mathbb{Z}_5 \qquad \mathbb{Z}_7$$

$\mathbb{Z}_2$: Nesvodljiv jer je $p(0) = 1, p(1) = 1$

$\mathbb{Z}_3$: Svodljiv jer je $p(1) = 0$, odakle je $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$

Napomena: Nad konačnim poljima:

- Traženje korena polinoma samo po sebi nije jako zanimljivo (jer možemo direktno da proverimo za sve elemente polja da li su koreni)
- Pitanje nesvodljivosti polinoma jeste zanimljivo (kao što ćemo videti u nastavku)

Primer

Zaokruži oznaku polja nad kojima je polinom $p(x) = x^3 + x + 1$ nesvodljiv

$$\mathbb{Z}_2 \qquad \mathbb{Z}_3 \qquad \mathbb{Z}_5 \qquad \mathbb{Z}_7$$

$\mathbb{Z}_2$: Nesvodljiv jer je $p(0) = 1, p(1) = 1$

$\mathbb{Z}_3$: Svodljiv jer je $p(1) = 0$, odakle je $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$

$\mathbb{Z}_5$: Nesvodljiv jer je $p(0) = 1, p(1) = 3, p(2) = 1, p(3) = 1, p(4) = 4$

Napomena: Nad konačnim poljima:

- Traženje korena polinoma samo po sebi nije jako zanimljivo (jer možemo direktno da proverimo za sve elemente polja da li su koreni)
- Pitanje nesvodljivosti polinoma jeste zanimljivo (kao što ćemo videti u nastavku)

Primer

Zaokruži oznaku polja nad kojima je polinom $p(x) = x^3 + x + 1$ nesvodljiv

$$\textcircled{\mathbb{Z}_2} \qquad \mathbb{Z}_3 \qquad \textcircled{\mathbb{Z}_5} \qquad \textcircled{\mathbb{Z}_7}$$

$\mathbb{Z}_2$: Nesvodljiv jer je $p(0) = 1, p(1) = 1$

$\mathbb{Z}_3$: Svodljiv jer je $p(1) = 0$, odakle je $x^3 + x + 1 = (x + 2)(x^2 + x + 2)$

$\mathbb{Z}_5$: Nesvodljiv jer je $p(0) = 1, p(1) = 3, p(2) = 1, p(3) = 1, p(4) = 4$

$\mathbb{Z}_7$: Nesvodljiv jer je
$p(0) = 1, p(1) = 3, p(2) = 4, p(3) = 3, p(4) = 6, p(5) = 5, p(6) = 6$

Napomena: Nad konačnim poljima:

- Traženje korena polinoma samo po sebi nije jako zanimljivo (jer možemo direktno da proverimo za sve elemente polja da li su koreni)
- Pitanje nesvodljivosti polinoma jeste zanimljivo (kao što ćemo videti u nastavku)

Konstrukcije konačnih polja

Ostaci pri deljenju. Kongruencije

U domenu integriteta $(\mathbb{Z}, +, \cdot)$:

- Delimo brojem n i posmatramo ostatke
- Relacija $\equiv_n$ je relacija ekvivalencije
- Faktor skup $\mathbb{Z}/\equiv_n$, tj. $\mathbb{Z}_n$, ima n elemenata
- $\equiv_n$ je kongrunecija u odnosu na $+$ i $\cdot$
- Faktor prsten $(\mathbb{Z}/\equiv_n, +, \cdot)$ je polje akko je n prost broj

U domenu integriteta $(F[x], +, \cdot)$:

- Delimo polinomom $t(x)$ i posmatramo ostatke
- Relacija $\equiv_t$ je relacija ekvivalencije?
- Faktor skup $F[x]/\equiv_t$, tj. $F[x]/_t$, ima koliko elemenata?
- $\equiv_t$ je kongrunecija u odnosu na $+$ i $\cdot$?
- Faktor prsten $(F[x]/_t, +, \cdot)$ je polje akko je t nesvodljiv polinom?

Nas zapravo interesuje slučaj kada je $F = \mathbb{Z}_p$

Za faktor skup $F[x]/\equiv_t$ pišemo i $F[x]/_t$

Koliko elemenata ima faktor skup $F[x]/_t$?

Podsećanje: Ostatak pri deljenju sa n može biti samo broj iz skupa $\{0, 1, \ldots, n-1\}$. Zato $\mathbb{Z}/\equiv_n$, tj. $\mathbb{Z}_n$, ima n elemenata.

- Kao što smo rekli, nas zanima $\mathbb{Z}_p[x]/_t$, gde je p prost prirodan broj i $t(x) \in \mathbb{Z}_p[x]$
- Ako $\equiv_t$ jeste kongruencija na $\mathbb{Z}_p[x]$ (što ćemo pokazati kasnije), pitanje je: šta sve može biti ostatak pri deljenju polinomom $t(x)$?
- Kada proizvoljan polinom $s(x) \in \mathbb{Z}_p[x]$ podelimo sa $t(x)$, znamo da imamo jedinstvene $q(x), r(x) \in \mathbb{Z}_p[x]$ takve da je $s(x) = q(x)t(x) + r(x)$, pri čemu je $r(x) = 0$ ili je $deg(r(x)) < deg(t(x))$
- Ako je $deg(t(x)) = n$ tada imamo da je ostatak $r(x)$ oblika $r(x) = a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, gde su koeficijenti $a_{n-1}, \ldots, a_1, a_0$ iz skupa $\mathbb{Z}_p$
- Dakle, skup svih ostataka pri deljenju sa $t(x)$ stepena n jeste

$$\mathbb{Z}_p[x]/_t = \{a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \mid a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}_p\}$$

- Pošto $\mathbb{Z}_p$ ima p elemenata, imamo da koeficijent a_i u skupu gore uzima p različitih vrednosti, pa skup ostataka $\mathbb{Z}_p[x]/_t$ ima p^n elemenata.

Primeri

$$\mathbb{Z}_p[x]/_t = \{a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \mid a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Z}_p\}$$

- Na skupu polinoma $\mathbb{Z}_2[x]$ ostaci pri deljenju sa $x^2 + x + 1$ su polinomi oblika $ax + b$, pa imamo 2^2 elemenata

$$\mathbb{Z}_2[x]/_{(x^2+x+1)} = \{0, 1, x, x + 1\}$$

- Na skupu polinoma $\mathbb{Z}_3[x]$ ostaci pri deljenju sa $x^2 + 1$ su polinomi oblika $ax + b$, pa imamo 3^2 elemenata

$$\mathbb{Z}_3[x]/_{(x^2+1)} = \{0, 1, 2, x, 2x, x + 1, x + 2, 2x + 1, 2x + 2\}$$

Relacija $\equiv_t$ jeste kongruencija na $\mathbb{Z}_p[x]$

Podsećanje: Relacija $q \equiv_n s \Leftrightarrow n \mid q - s$ jeste kongruencija na $\mathbb{Z}$ u odnosu na $+$ i $\cdot$

Teorema

Neka je $t(x) \neq 0$. Binarna relacija $\equiv_t$ skupa svih polinoma $\mathbb{Z}_p[x]$ definisana je sa: za sve $q(x), s(x) \in \mathbb{Z}_p[x]$ važi $q(x) \equiv_t s(x)$ akko $t(x) \mid q(x) - s(x)$. Tada je $\equiv_t$ kongurencija u odnosu na sabiranje i množenje polinoma nad $\mathbb{Z}_p$.

Sabiranje i množenje polinoma po modulu $t(x)$

Napomena: Kao što smo kod celih brojeva za klasu broja x u odnosu na relaciju $\equiv_n$ pisali C_x (ili $[x]$), tako ćemo i ovde za klasu polinoma $q(x)$ u odnosu na relaciju $\equiv_t$ pisati C_q (ili $[q(x)]$).

Definicija

Na skupu $\mathbb{Z}_p[x]/\equiv_t$ *definišemo operacije* $+$ *i* $\cdot$ *sa: za sve* $q(x), r(x) \in \mathbb{Z}_p[x]$

$$C_q + C_r = C_{q+r} \qquad i \qquad C_q \cdot C_r = C_{qr}$$

Primer

Na skupu $\mathbb{Z}_2[x]/_{(x^2+x+1)} = \{0, 1, x, x+1\}$ *operacije* $+$ *i* $\cdot$ *su*

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Polje $\mathbb{Z}_p[x]/_t$

Podsećanje: $(\mathbb{Z}_n, +, \cdot)$ je komutativan prsten sa jedinicom.

Teorema

Struktura $(F[x]/_t, +, \cdot)$ *jeste komutativan prsten sa jedinicom.*

Podsećanje: $(\mathbb{Z}_n, +, \cdot)$ je polje akko je n prost broj.

Teorema

Struktura $(\mathbb{Z}_p[x]/_t, +, \cdot)$ *jeste polje ako je* $t(x)$ *nesvodljiv polinom nad poljem* $\mathbb{Z}_p$.

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom $t(x)$ stepena n. Tada je $(\mathbb{Z}_p[x]/_t, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu $t(x)$.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[x]/_{(x^2+x+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[x]/_t, +, \cdot)$*:*

1. $(\mathbb{Z}_2[x]/_{(x+1)}, +, \cdot)$
2. $(\mathbb{Z}_3[x]/_{(x^2+1)}, +, \cdot)$
3. $(\mathbb{Z}_3[x]/_{(x^2+x+1)}, +, \cdot)$
4. $(\mathbb{Z}_5[x]/_{(x^2+1)}, +, \cdot)$

Primer primene: pogledati CRC kodovanje u knjizi.

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom $t(x)$ stepena n. Tada je $(\mathbb{Z}_p[x]/_t, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu $t(x)$.

Primer

Polje od 4 elemenata je $(\mathbb{Z}_2[x]/_{(x^2+x+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[x]/_t, +, \cdot)$*:*

1. $(\mathbb{Z}_2[x]/_{(x+1)}, +, \cdot)$ *(polinom* $x+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[x]/_{(x^2+1)}, +, \cdot)$
3. $(\mathbb{Z}_3[x]/_{(x^2+x+1)}, +, \cdot)$
4. $(\mathbb{Z}_5[x]/_{(x^2+1)}, +, \cdot)$

Primer primene: pogledati CRC kodovanje u knjizi.

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom $t(x)$ stepena n. Tada je $(\mathbb{Z}_p[x]/_t, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu $t(x)$.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[x]/_{(x^2+x+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[x]/_t, +, \cdot)$*:*

1. $(\mathbb{Z}_2[x]/_{(x+1)}, +, \cdot)$ *(polinom* $x+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[x]/_{(x^2+1)}, +, \cdot)$ *(polinom* x^2+1 *je nesvodljiv nad poljem* $\mathbb{Z}_3$*)*
3. $(\mathbb{Z}_3[x]/_{(x^2+x+1)}, +, \cdot)$
4. $(\mathbb{Z}_5[x]/_{(x^2+1)}, +, \cdot)$

Primer primene: pogledati CRC kodovanje u knjizi.

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom $t(x)$ stepena n. Tada je $(\mathbb{Z}_p[x]/_t, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu $t(x)$.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[x]/_{(x^2+x+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[x]/_t, +, \cdot)$*:*

1. $(\mathbb{Z}_2[x]/_{(x+1)}, +, \cdot)$ *(polinom* $x+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[x]/_{(x^2+1)}, +, \cdot)$ *(polinom* x^2+1 *je nesvodljiv nad poljem* $\mathbb{Z}_3$*)*
3. $(\mathbb{Z}_3[x]/_{(x^2+x+1)}, +, \cdot)$ *(1 je koren polinoma* x^2+x+1 *u polju* $\mathbb{Z}_3$*)*
4. $(\mathbb{Z}_5[x]/_{(x^2+1)}, +, \cdot)$

Primer primene: pogledati CRC kodovanje u knjizi.

Kako konstrusati polje od p^n elemenata?

Rešenje: Nad poljem $\mathbb{Z}_p$ naći nesvodljiv polinom $t(x)$ stepena n. Tada je $(\mathbb{Z}_p[x]/_t, +, \cdot)$ polje sa p^n elemenata, gde su $+$ i $\cdot$ sabiranje i množenje polinoma po modulu $t(x)$.

Primer

Polje od 4 elementa je $(\mathbb{Z}_2[x]/_{(x^2+x+1)}, +, \cdot)$.

Primer

Zaokruži broj ispred polja $(\mathbb{Z}_p[x]/_t, +, \cdot)$*:*

1. $(\mathbb{Z}_2[x]/_{(x+1)}, +, \cdot)$ *(polinom* $x+1$ *je nesvodljiv nad poljem* $\mathbb{Z}_2$*)*
2. $(\mathbb{Z}_3[x]/_{(x^2+1)}, +, \cdot)$ *(polinom* x^2+1 *je nesvodljiv nad poljem* $\mathbb{Z}_3$*)*
3. $(\mathbb{Z}_3[x]/_{(x^2+x+1)}, +, \cdot)$ *(1 je koren polinoma* x^2+x+1 *u polju* $\mathbb{Z}_3$*)*
4. $(\mathbb{Z}_5[x]/_{(x^2+1)}, +, \cdot)$ *(2 je koren polinoma* x^2+1 *u polju* $\mathbb{Z}_5$*)*

Primer primene: pogledati CRC kodovanje u knjizi.