Polinomi nad prstenom cijelih brojeva

Dr. Hasan Jamak

Udruženje matematičara Kantona Sarajevo

Fojnica, 14.01.2017. godine

Sadržaj

Abstract

U ovom predavanju posmatraćemo polinome nad prstenom cijelih brojeva i razmatrati pitanje nesvodljivosti polinoma nad poljem racionalnih brojeva. Upoznaćemo se sa nekim kriterijima nesvodljivosti kao što su:

- Ajzenštajnov kriterij,
- Poopšteni Ajzenštajnov kriterij,
- Redukcioni kriterij i dr.

Uvod

Definicija

Polinom sa cjelobrojnim koeficijentima *je formalni izraz oblika*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

gdje je n nenegativan cio broj, $a_0, a_1, \ldots, a_{n-1}, a_n$ cijeli brojevi. Akao je $n \geq 1$, onda je $a_n \neq 0$. Brojevi $a_0, a_1, \ldots, a_n$ nazivaju se koeficijenti polinoma. Broj a_0 nazivamo ***slobodan član****, a broj a_n nazivamo* ***vodeći koeficijent****. Ako je $a_n \neq 0$, onda kažemo da je n stepen polinoma $P(x)$. Ako je $a_0 \neq 0$ i $a_k = 0$ za svako $k \geq 1$, onda je stepen polinoma nula i taj polinom nazivano* ***konstantan polinom****.*
Ako polinom $P(x)$ ima vodeći koeficijent 1, onda kaženo da je on moničan ili normiran polinom.
Ako su svi koeficijenti polinomi jednaki nula, onda za polinom kažemo da je nula polinom.

Definicija

Za dva polinoma kažemo da su jednaki, ako i samo ako su istog stepena i ako su im odgovarajući koeficijenti jednaki.

Bezuov stav i Hornerova šema

Definicija

Za polinom $P(x)$ sa cjelobrojnim koeficijentima kažemo da je djeljiv polinomom $Q(x)$ ako postoji polinom $R(x)$ takav da je $P(x) = Q(x) \cdot R(x)$.

Teorem

Neka su $P(x)$ i $Q(x)$ polinomi sa cjelobrojnim koeficijentima i $Q(x)$ moničan polinom. Tada postoje polinomi $S(x)$ i $R(x)$ sa racionalnim koeficijentima takvi da je $P(x) = Q(x)S(x) + R(x)$, gdje je $S(x)$ nula polinom, ili polinom stepena manjeg od stepena polinoma $P(x)$.

Polinom $R(x)$ iz prethodnog teorema naziva se **ostatak** pri dijeljenju.

Primjer

Ako je $P(x) = 3x^3 - 2x^2 + 9x - 6$ i $Q(x) = x^2 - x + 2$, onda je $P(x) = (3x + 1)Q(x) + 4x - 8$.

Teorem (Bezuov stav)

Neka $P(x)$ polinom sa racionalnim koeficijentima i x_0 racionalan broj. Ostatak pri dijeljenju polinoma $P(x)$ sa $x - x_0$ jednak je vriojednosti polinoma za $x = x_0$, tj. $P(x_0)$.

Ako je

$$\begin{aligned} P(x) &= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \\ Q(x) &= b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \ldots + b_1 x + b_0 \\ P(x) &= (x - x_0) Q(x) + r, \end{aligned}$$

onda je

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= x_0 b_{n-1} + a_{n-1} \\ &\ldots \\ b_{k-1} &= x_0 b_k + a_k \\ &\ldots \\ b_0 &= x_0 b_1 + a_1 \\ r &= x_0 b_0 + a_0. \end{aligned}$$

To se šematski zapisuje na sljedeći način.

$$\begin{array}{c|ccccc} x_0 & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ \hline & \underbrace{a_n}_{=b_{n-1}} & \underbrace{x_0 b_{n-1} + a_{n-1}}_{=b_{n-2}} & \cdots & \underbrace{x_0 b_1 + a_1}_{=b_0} & \underbrace{x_0 b_0 + a_0}_{=r} \end{array}$$

Primjer

Ostatak pri dijeljenju polinoma $P(x) = x^3 + 3x^2 - 7x + 6$ *sa* $x - 2$ *je* 12, *jer je* $p(2) = 12$. *Provjerimo ovaj rezultat Hornerovom šemom*

2	1	3	-7	6
	1	$2 \cdot 1 + 3 = 5$	$2 \cdot 5 - 7 = 3$	$2 \cdot 3 + 6 = 12$

Pomoću Hornerove šeme možemo dati polinom razložiti po stepenima od $x - x_0$. Ilustrujmo to na sljedećem primjeru.

Primjer

$P(x) = x^5 - 2x^3 - 3x + 1$ $x_0 = -1$.

-1	1	0	-2	0	-3	1
	1	-1	-1	1	-4	**5**
	1	-2	1	0	**-4**	
	1	-3	4	**-4**		
	1	-4	**8**			
	1	**-5**				
	1					

Odavde imami $P(x) = 1(x+1)^5 - 5(x+1)^4 + 8(x+1)^3 - 4(x+1)^2 - 4(x+1) + 5$.

Racionalne nule

Teorem

Neka je $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *polinom sa cijelobrojnim koeficijentima takav da je* $a_n \cdot a_0 \neq 0$. *Ako je racionalan broj*

$$\frac{p}{q},\ p \in \mathbb{Z},\ q \in \mathbb{N}, nzd(p,q) = 1,$$

nula polinoma $P(x)$, *onda*

a) $p \mid a_0,\ q \mid a_n$,

b) $(p - kq) \mid P(k)$ *za svaki cio broj* k.

Primjer

Odredimo racionalne nile polinoma $P(x) = 6x^3 - 11x^2 - 4x + 4$. *Da bi racionalan broj* $\frac{p}{q}$ *bila nula datog polinoma mora* $p \mid 6$ *i* $q \mid 6$. *Zato je* $p \in \{\pm 1, \pm 2, \pm 4\}$ *i* $q \in \{1, 2, 3, 6\}$. *Imamo mnogo mogućnosti za* p/q, *pa ćemo koristiti i činjenicu da* $(p - kq) \mid P(k)$ *za svako* $k \in \mathbb{Z}$. *Najćešće za* k *uzimamo* 1 *i* -1. *Lahko nalazimo* $P(1) = -5$ *i* $P(-1) = -9$. *Kako je* $P(1) \neq 0$ *i* $P(-1) \neq 0$, *to* 1 *i* -1 *nisu nule polinoma. U cilju ispitivanja svih mogućnosti konstruišimo tabelu:*

p	-2	2	-4	4	-1	1	-1	1	-2	2	-1	1
q	1	1	1	1	2	2	3	3	3	3	6	6
p-q	-3	1	-5	3	-3	-1	-4	-2	-5	-1	-7	-5
$(p-q) \mid (-5)$	-	+	+	-	-	+	-	-	+	+	-	+
$(p+q) \mid (-9)$		+	+			+			+	-		-

Iz tabele vidimo da je

$$\frac{p}{q} \in \{-2, -4, \frac{1}{2}, -\frac{2}{3}\}.$$

Primjenom Hornerove šeme nalazimo nule polinoma $z_1 = -2$, $x_2 = \frac{1}{2}$ *i* $x_3 = -\frac{2}{3}$.

Teorem

Sve nule polinom $P(x)$ kod kojeg je vodeći koeficijent jednak 1 su cijeli brojevi ili su iracionalni (realni ili kompleksni) brojevi.

Teorem

Neka je $P(x)$ polinom sa cjelobrojnim koeficijentima. Za svaka dva različita cijela broja u i v vrijedi

$$(u - v) \mid (P(u) - P(v)).$$

Primjer

Da li postoji polinom sa cjelobrojnim koeficijentima takav da je $p(1) = 6$ i $P(4) = 19$? Na osnovu prethodnog teorema, ako takav polinom postoji onda

$$(4 - 1) \mid (P(4) - P(1)),$$

tj. $3 \mid 13.$, *što je nemoguće. Dakle, takav polinom ne postoji.*

Primjer

Postoji li polinom $P(x)$ *sa cjelobrojnim koeficijentima, takav da je* $P(5) = 2005$ *i da je* $P(2005)$ *potpun kvadrat?*
Pretpostavimo da takav polinom postoji. Tada je $P(5) = 2005$ *i* $P(2005) = a^2$ *za neki cio broj a. Na osnovu prethodnog teorema vrijedi*

$$(2005 - 5) \mid (P(2005) - P(5)),$$

tj. $2000 \mid (a^2 - 2005)$. *Odavde slijedi da je a djeljivo sa* 5. *Neka je* $a = 5b$. *Tada* $2000 \mid (25b^2 - 2005)$, *tj.* $400 \mid (5b^2 - 401)$. *Tada je* $5b^2 - 401 = 400k$ *za neki prirodan broj k. To je nemoguće jer* 5 *ne dijeli* 401. *Dakle, ne postoji polinom sa traženim osobinama.*

Nesvodljivost polinoma nad poljem racionalnih brojeva

Definicija

*Za polinom sa racionalnim koeficijentima kažemo da je **nesvodljiv** nad poljem $\mathbb{Q}$ racionalnih brojeva ako se ne može prikazati u obliku proizvoda dva ili više nekonstantnih polinoma sa racionalnim koeficijentima.*

Primjer

Polinom $p(x) = x^2 + 1$ je nesvodljiv nad poljem racionalnih i realnih brojeva, ali nije nesvodljiv nad poljem kompleksnih brojeva, jer je $x^2 + 1 = (x - i)(x + i)$.

Teorem (Ajzenštajnov kriterij)

Neka je

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

Ako postoji prost broj p takav da $p \mid a_i \, (i = 0, 1, \ldots, n-1)$, p ne dijeli a_n i p^2 ne dijeli a_0, onda je polinom $P(x)$ nesvodljiv polinom nad $\mathbb{Q}$.

Primjer

Neka je $P(x) = 4x^4 + 12x^3 - 9x^2 + 3x - 21$. Primjećujemo da su svi koeficijenti, osim vodećeg djeljivi prostim brojem 3 i da $3^2 = 9$ ne dijeli -21, pa je polinom nesvodljiv nad $\mathbb{Q}$.

Primjer

Ispitati nesvodljivost polinoma $P(x) = x^4 + x^3 + x^2 + x + 1$ nad poljem racionalnih brojeva. Da li ovdje možemo primjeniti Ajzenštajnov kriterij? Ne postoji ni jedan prost broj koji dijeli 1, pa na prvi pogled ne možemo. No, ako je polinom $P(ax + b)$, pi čemu su a i b racionalni brojevi i $a \neq 0$, nesvodljiv, onda je i polinom $P(x)$ nesvodljiv. Posmatrajmo polinom $Q(x) = P(x + 1) = x^4 + 5x^3 + 10x^2 + 10x + 5$. Odmah vidimo da možemo primjeniti Ajzenštajnov kriteri i za prost broj uzeti 5. Po Ajzenštajnovom kriteriju polinom je nesvodljiv, pa je i polazni polinom nesvodljiv.

Primjer

Dokažimo da je polinom $P(x) = x^{101} + 101x^{100} + 102$ nesvodljiv nad $\mathbb{Z}$.

Rješenje. Broj 102 nije prost, ali je broj 101, pa direktno ne možemo primjeniti Ajzenštajnov algoritam. Posmatrajmo polinom

$$P(x-1) = (x-1)^{101} + 101(x-1)^{100} + 102.$$

Njega možemo napisati u obliku

$$\begin{aligned} P(x-1) &= x^{101} - \binom{101}{1} x^{100} + \binom{101}{2} x^{99} \\ &- \ldots + \binom{101}{1} x - 1 + 101(x-1)^{100} + 102 \\ &= x^{101} + 101\,T(x) + 101, \end{aligned}$$

gdje je $T(x)$ polinom sa cjelobrojnim koeficijentima stepena 100. Sada možemo primjeniti Ajzenštajnov kriterij za prost broj 101. Lahko se vidi da su ispunjeni uslovi kriterija i polinom je nesvodljiv. $\diamondsuit$

Teorem (Generalizirani Ajzenštajnov kriterij)

Neka je $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ *polinom sa cjelobrojnim koeficijentima. Pretpostavimo da za neki prosti broj* p, $p \mid a_i$ *za neko* $0 \leq i \leq n - m - 1, p \nmid a_{n-m}$ *i* $p^2 \nmid a_0$*. Tada ako* $P(x)$ *ima ima faktorizaciju u* $\mathbb{Z}[x]$*, jedan njegov faktor mora imati stepen manji ili jednak* m*.*

Primjer (IMO 1993)

Neka je $f(x) = x^n + 5x^{n-1} + 3$*, gdje je* $n > 1$ *prirodan broj. Dokazati da je polinom nesvodljiv nad prstenom* $\mathbb{Z}[x]$*.*

Rješenje. Pošto je $P(\pm 1) \neq 0$ i $P(\pm 3) \neq 0$, to polinom nema linearnih faktora. Ovdje prosti broj 3 dijeli sve koeficijente polinom $P(x)$ osim prva dva, pa po Generaliziranom Ajzenštajnovom kriteriju on je nesvodljiv ili ima linearan faktor. Kako nema linearnih faktora to je on nesvodljiv. $\diamondsuit$

Teorem (Redukcioni kriteri)

Neka je $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *polinom sa cjelobrojnim koeficijentima. Neka je* p *prost broj koji ne dijeli* a_n. *Označimo sa* $\overline{P}(x)$ *polinom čiji su koeficijenti kongruentni po modulu* p *koeficijentima polinoma* $P(x)$. *Ako je polinom* $\overline{P}(x)$ *nesvodljiv nad* $\mathbb{Z}_p$, *onda je i polinom* $P(x)$ *nesvodljiv.*

Primjer

Ispitajmo nesvodljivost polinoma $P(x) = x^4 - 2x^3 + 6x^2 + 7x - 1$ *nad* $\mathbb{Z}$. *Primijenimo redukcioni kriterij po modulu* 2. *Tada je* $\overline{P}(x) = x^4 + x + 1$. *U polju* $\mathbb{Z}_2$ *jedini elementi su* 0 *i* 1. *Ako polinom* $x^4 + x + 1$ *nije nesvodljiv, onda on ima linearan ili kvadratan faktor. Kako je* $\overline{P}(0) = \overline{P}(1) = 1 \neq 0$, *to polinom* $\overline{P}(x)$ *nema linearnih faktora. Tada su oba faktora kvadratni. No, kvadratni polinomi nad* $\mathbb{Z}_2$ *su:* x^2, $x^2 + 1$, $x^2 + x$ *i* $x^2 + x + 1$. *Kako proizvod bilo koja dva od ova četiri polinoma ne daje polinom* $x^4 + x + 1$, *to je polinom* $\overline{P}(x$ *nesvodljiv nad* $\mathbb{Z}_2$, *pa je i polinom* $P(x)$ *nesvodljiv.*

Primjer

Neka je p prost broj oblika $4k+3 >$ Dokažsimo da je polinom $P(x) = (x^2+1)^n + p$ nesvodljiv u $\mathbb{Z}[x]$.

Rješenje. Pretpostavimo suprotno, tj. da je $P(x) = Q(x)\,R(x)$, gdje su $Q(x)$ i $R(x)$ nekonstantni polinomi. Posmatrajmo kongruenciju po modulu p. Imamo $\overline{P}(x) = \overline{Q}(x)\overline{R}(x) = (x^2+1)^n$ u $\mathbb{Z}_p[x]$. Kako -1 nije kvadratni ostatak modulo p, to je polinom x^2+1 nesvodljiv u $\mathbb{Z}_p[x]$. Neka je $\overline{Q}(x) = (x^2+1)^k$ i $\overline{R}(x) = (x^2+1)^{n-k}$, pa je $Q(x) = (x^2+1) + pQ_1(x)$ i $R(x) = (x^2+1)^{n-k} + pR_1(x)$, gdje su Q i R polinomi sa cjelobrojnim koeficijentima. Sada imamo

$$(x^2+1)^n + p = \left((x^2+1)^k + Q_1(x)\right)\,\left((x^2+1)^{n-k} + R_1(x)\right).$$

Nakon množenja i sređivanja dobije se

$$(x^2+1)^k R_1(x) + (x^2+1)^{n-k} Q_1(x) + pQ_1(x(R_1(x) = 1. \quad (*)$$

Kako je $k \geq 1$ i $n-k \geq 1$, to je lijeva strana djeljiva x^2+1. Dakle, u prstenu $\mathbb{Z}_p[x]$ jednakost (*) postaje $(x^2+1)^k R_1(x) + (x^2+1)^{n-k} Q_1(x) = 1$, pa x^2+1 dijeli 1 u $\mathbb{Z}_p[x]$. Ovo je nemoguće. Pretpostavka da polinom nije nesvodljiv dovela nas je do kontradikcije, pa nije tačna. $\diamondsuit$

Teorem

Polinomi sa cjelobrojnim koeficijentima stepena dva ili tri su nesvodljivi ako i samo ako nemaju racionalnih nula.

Teorem

Ako postoji prosti broj p koji brojevnom sistemu po bazi b ima prikaz

$$p = a_0 + a_1 b + \ldots + a_{n-1} b^{n-1} + a_n b^n, (0 \leq a_i \leq b-1).$$

Tada je polinom

$$P(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$$

nesvodljiv.

Primjer

Ispitajmo nesvodljivost polinoma $P(x) = x^4 + x^3 + 2x^2 + 1$ *nad* $\mathbb{Z}$. *Posmatrajmo broj* $a = 3^4 + 3^3 + 2 \cdot 3^2 + 1 = 81 + 27 + 18 + 1 = 127$. *Broj* 127 *je prost pa je polinom* $P(x)$ *nesvodljiv.*

Teorem

Neka je $P(x)$ polinom s racionalnih koeficijentima takav da je $u+\sqrt{v}$, $(u, v \in \mathbb{Q})$ i $\sqrt{v} \notin \mathbb{Q}$ jedna njegova nula. Tada je $u-\sqrt{v}$ druga nula tog polinoma.

Primjer

Neka je $P(x) = 2x^3 - 3x^2 + ax + 5$, gdje je a racionalan broj. Odrediti broj a tako da posmatrani polinom ima nulu $u+\sqrt{3}$, gdje je je u racionalan broj. Prema prethodnom teoremu posmatrani polinom kao drugu nulu ima $u-\sqrt{3}$. Tada je

$$S(x) = (x-u-\sqrt{3})(x-u+\sqrt{3}) = (x-u)^2 - 3 = x^2 - 2ux + u^2 - 3$$

faktor polaznog polinoma. Dijeljenjem polinoma $P(x)$ sa $S(x)$ dobije se količnik $2x + 4u - 3$ i ostatak

$$(6u^2 + 6u + 6 + a)x - (4u^3 - 3u^2 - 12u + 4).$$

Kako ostatak dijeljenja mora biti nula polinom, to je

$$\begin{aligned} 6u^2 - 6u + 6 + a &= 0 \\ 4u^3 - 3u^2 - 12u + 4 &= 0, \end{aligned}$$

Druga jednačina ima samo jedno racionalno rješenje $u = 2$. Tada iz prve jednačine slijedi $a = -18$.

Primjer

Neka je $P(x) = (x - a_1)(x - a_2) \cdot \ldots \cdot (x - a_n) + 1$, *gdje su* $a_1, a_2, \ldots, a_n$ *različiti cijeli brojevi. Pokazati*
a) ako je n *neparan broj, onda je* $P(x)$ *nesvodljiv nad* $\mathbb{Z}$;
b) ako je n *paran, onda je* $P(x)$ *nesvodljiv ili je kvadrat nekog polinoma sa cjelobrojnim koeficijentima.*

Rješenje. a) Neka je $n = 2m + 1$ i neka je $P(x) = S(x)T(x)$, pri čemu su S i T polinomi sa cjelobrojnim koeficijentima. Neka je S stepena s, a T stepena t. Tada je $s + t = 2m + 1$, pa je jedan od brojeva s i t veći od m, a drugi manji. Neka je $s > m$. Kako je $P(a_i) = 1$ za svako $i = 1, 2, \ldots 2m + 1$. Tada je $S(a_i)\,T(a_i) = 1$. Dakle, $S(a_i) = T(a_i) = \pm 1$ za svako i. Za polinom $W(x) = S(x) - T(x)$ vrijedi

$$W(a_i) = S(a_i) - T(a_i) = 0 \quad (i = 1, 2, \ldots, n).$$

Kako je $st(S) > m$ i $m \geq st(T) \geq 1$, to je $1 \leq st(S - T) \leq n - 1$. Dakle, polinom $S - T$ u najboljem slučaju može imati $n - 1$ nulu. Vidjeli smo da $S - T$ ima bar n nula, to je jedino moguće ako je $S - T$ nula polinom. Dakle, $S = T$, pa je $P = S^2$. Odavde slijedi $2m + 1 = 2 \cdot st(S)$. Kontradikcija.
b) Neka je $n = 2m$. Pretpostavimo da polinom p nije nesvodljiv. Trebamo pokazati da je $P(x)$ kvadrat nekog polinoma. Neka je $P = S\,T$. Tada je $1 = P(a_i) = S(a_i)\,T(a_i)$. Tada je $S(a_i) = T(a_i) = \pm 1$ za svako i, pa je $st(S) = st(T) = m$. Polinom $W = S - T$ ima $n = 2m$ nula, pri čemu je W nula polinom ili je polinom stepena manjeg od m. Kako polinom W ima $2m$ nula, to je on nula polinom. Dakle, $P = S^2$. $\diamondsuit$

Primjer

Neka je $P(x) = x^4 + ax^3 + bx^2 + cx + d$ polinom sa cjelobrojnim koeficijentima koji ima sve četiri pozitivne nule. Odrediti najveći realan broj k takav da je $(b-a-c)^2 \geq kd$.

Rješenje. Neka su x_1, x_2, x_3, x_4 nule polinoma $P(x)$. Prema Vietovim pravilima imamo

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= -a \\ x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 &= b \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= -c \\ x_1x_2x_3x_4 &= d \end{aligned}$$

Neka je $w = b - a - c$. Na osnovu odnosa aritmetičke i geometrijske sredine imamo

$$\begin{aligned} w &= x_1 + x_2 + x_3 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ &+ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \geq 14\sqrt[14]{(x_1x_2x_3x_4)^{14}} = 14\sqrt{d} \end{aligned}$$

Iz $w \geq kd$ slijedi $14\sqrt{d} \geq kd$, tj. $k \leq 196$. Jednakost vrijedi ako i samo ako je $x_1 = x_2 = x_3 = x_4 = 1$. Tada je $a = -4$, $b = 6$, $c = -4$ i $d = 1$. Dakle, polinom je $P(x) = (x-1)^4$ i $k = 196$. $\diamondsuit$