Polinomi

Jan Pantner (jan.pantner@gmail.com)

30. oktober 2025

Kazalo

Uvod

Zapiski so nastali kot dodatek k predavanju, ki sem ga imel 26. 1. 2024 v okviru priprav na mednarodna matematična tekmovanja v šolskem letu 2023/2024. Izpuščene so rešitve nekaterih nalog, ponekod pa je napisana samo ideja dokaza.

Najprej bomo povedali nekaj splošnih lastnosti polinomov, v drugem delu se bomo posvetili polinomom s celoštevilskimi koeficienti, na koncu pa bomo povedali še nekaj o Lagrangeevi interpolaciji.

Za dobro razumevanje zapiskov je priporočljivo osnovno znanje o funcijskih enačbah, teoriji števil in kompleksnih številih. Pojavi se tudi neenakost med aritmetično in geometrijsko sredino.

Bralcu predlagam, da, preden prebere rešitev katerekoli naloge, najprej poskusi nalogo rešiti sam. Enako velja tudi za dokaze trditev in izrekov.

V primeru kakšne dileme oziroma vprašanja me lahko brez oklevanja kontaktirate na jan.pantner@gmail.com. Zelo verjetno se v zapiskih nahaja tudi kakšna napaka. Če jo opazite, prosim, da mi to sporočite.

1 Osnovne lastnosti

1.1 Definicija in enakost polinomov

Definicija 1.1

Polinom $p(x)$ je funkcija oblike

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0, \qquad a_n \neq 0,$$

kjer je x spremenljivka, konstante $a_n, a_{n-1}, \ldots, a_0$ pa imenujemo *koeficienti*. Številu n pravimu *stopnja* polinoma $p(x)$. Označimo $\deg p = n$. Če je $q(x) = 0$ ničelni polinom, definiramo $\deg q = -\infty$.

Pri nas bodo koeficienti vedno elementi ene od množic $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Z $\mathbb{F}[x]$ označimo množico polinomov s koeficienti iz $\mathbb{F}$. Tako na primer $\mathbb{Q}[x]$ označuje množico polinomov z racionalnimi koeficienti. Seveda velja $\mathbb{Z}[x] \subseteq \mathbb{Q}[x] \subseteq \mathbb{R}[x] \subseteq \mathbb{C}[x]$.

Na naraven način lahko definiramo seštevanje in množenje polinomov. Vsota in produkt polinomov je spet polinom. Naj bo $n \geq m$, $p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ in $n \geq m$, $q(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$. Potem je njuna vsota

$$p(x) + q(x) = a_nx^n + \cdots + a_{m+1}x^{m+1} + (a_n + b_m)x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

njun produkt pa

$$p(x)q(x) = (a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0) \cdot (b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0).$$

Previdni moramo biti pri deljenju, saj kvocient dveh polinomov ni nujno polinom. Naj bo $p(x) = x^3$ in $q(x) = x^2$. Kvocient $p(x)/q(x) = x$ je polinom, $q(x)/p(y) = x^{-1}$ pa ne. O deljenju polinom bomo več povedali v razdelku 1.2.

Poglejmo te pojme na primeru. Polinom $p(x) = 2x^4 - 3x^3 - 4$ je polinom s celoštevilskimi koeficienti, stopnje 4, z vodilnim koeficientom 2 in prostim členom -4. Polinom $q(x) = -2x^4 + \frac{1}{3}x$ pa je polinom z racionalnimi koeficienti, stopnje 4, z vodilnim koeficientom -2 in prostim členom 0. Njuna vsota je

$$p(x) + q(x) = -3x^3 + \frac{1}{3}x - 4,$$

njun produkt pa

$$\begin{aligned} p(x)q(x) &= (2x^4 - 3x^3 - 4)\left(-2x^4 + \frac{1}{3}x\right) \\ &= -4x^8 + 6x^7 + \frac{2}{3}x^5 + 7x^4 - \frac{4}{3}x. \end{aligned}$$

Naloga 1.2

Naj bosta p in q polinoma. Pokažite, da velja

$$\deg(p \cdot q) = \deg p + \deg q \quad \text{in} \quad \deg(p+q) \leq \max\{\deg p, \deg q\}.$$

Rešitev. Pogledamo, kaj se zgodi z vodilnima koeficientoma. □

Definicija 1.3

Polinoma sta enaka, če imata enake koeficiente pri enakih potencah x. Torej, polinoma

$$p(x) = a_n x^n + \cdots + a_1 x + a_0 \quad \text{in} \quad q(x) = b_n x^n + \cdots + b_1 x + b_0$$

sta enaka, če velja $a_n = b_n, a_{n-1} = b_{n-1}, \ldots a_1 = b_1, a_0 = b_0$.

S to preprosto definicija lahko v resnici marsikaj dosežemo. Ko želimo dokazati enakost oziroma neenakost dveh polinomov, se zelo pogosto splača (in ni pretežko) pogledati stopnji, vodilna koeficienta in prosta člena.

Naloga 1.4

Poiščite vse polinome $p \in \mathbb{R}[x]$, za katere velja

$$p(p(x)) = x^2 p(x)$$

za vsako realno število x.

Rešitev. Prepuščena bralcu. □

Trditev 1.5

Naj bosta p in q polinoma. Če se p in q ujemata v vsaj $\max\{\deg(p), \deg(q)\} + 1$ točkah, sta enaka.

Takojšnja posledica te trditve je, da sta polinoma, ki se ujemata v neskončno mnogo točkah, enaka. Med drugim, nam trditev pove tudi, da je polinom stopnje n enolično določen z $n + 1$ točkami.

Naloga 1.6

Poiščite vse polinome $p(x) \in \mathbb{R}[x]$, za katere velja $p(1) = 1$ in

$$p(x^2 + x) = (x + 1)p(x)$$

za vse $x \in \mathbb{R}$.

Rešitev. Če vstavimo $x \mapsto 1$, dobimo $p(2) = 2p(1) = 2$, in če vstavimo $x = 2$, dobimo $p(6) = 3p(2) = 6$. Z indukcijo lahko dokažemo, da velja $p(n^2 + n) = n^2 + n$ za vsako naravno število n. Torej smo pokazali, da se $p(x)$ ujema s polinomom $h(x) = x$ v neskončno mnogo točkah, torej sta $p(x)$ in $h(x)$ enaka. □

Naloga 1.7: MEMO 2017

Poiščite vse pare polinomov (p, q) z realnimi koeficienti, za katere velja

$$p(x + q(y)) = q(x + p(y))$$

za vsa realna števila x in y.

Ta naloga je (tako kot prejšnji dve) primer *polinomske funkcijske enačbe*. To pomeni, da lahko uporabljamo strategije, ki jih poznamo od (splošnih) funkcijskih enačb. Seveda, pa je pomembno imeti v mislih tudi lastnosti polinomov.

Rešitev. Vstavimo $x \mapsto -q(y)$, da dobimo

$$p(0) = q(P(y) - q(y)) \tag{1}$$

Torej je izraz $q(p(y)-q(y))$ konstanten. Označimo $C := p(0)$ in poglejmo koliko vrednosti lahko zazvame $p(y) - q(y)$.

Recimo, da izraz $p(y) - q(y)$ zavzame neskončno različnih vrednosti. Iz (1) sledi, da je polinom q enak konstanti C v neskončno mnogo točkah, torej se s konstantnim polinomom $H(x) = C$ ujema v vsaj $\max\{p(x), h(x)\} + 1$ točkah, torej velja $q = h$. Naša osnovna enačba nam sedaj pove $p(x + C) = C$. Sledi $p(x) = q(x) \equiv C$. Preizkus nam pove, da je C lahko poljubna konstanta.

Druga možnost je, da izraz $p(y) - q(y)$ zazvame končno različnih vrednost. Vendar v tem primeru neko vrednost zazvame neskončno mnogokrat. Ker v neskončno vrednostih c velja $p(y) = q(y) + c$, po naši trditvi sledi, da za vsak y velja $p(y) = q(y) + c$. Hitro lahko preverimo, da primer, ko je $c = 0$, res ustreza pogojem naloge. Dobili smo rešitev $p = q$. Predpostavimo sedaj, da $c \neq 0$. Če to vstavimo v prvotno enačbo, dobimo

$$q(x + q(y)) + c = q(x + q(y) + c).$$

Sedaj vstavimo $x \mapsto x - q(y)$ in dobimo:

$$q(x) + c = q(x + c).$$

Če zapišemo $q(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$, kjer $a_n \neq 0$, dobimo

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

Poglejmo koeficient pred x^{n-1} na obeh straneh. Če je $n \geq 2$, dobimo

$$a_{n-1} = a_{n-1} + nca_n \to nca_n = 0,$$

kar pa ni mogoče. Torej velja $n \in \{0, 1\}$. Primer, ko je $n = 0$, smo že obravnavali. Preostane še $n = 1$, oziroma $q(x) = ax + b$, kjer $a \neq 0$. Dobimo

$$ax + b + c = a(x + c) + b \Rightarrow c = ac \Rightarrow a = 1.$$

Dobili smo $q(x) = x + b$ in $p(x) = x + b + c$ oziroma $q(x) = x + b$ in $p(x) = x + d$, kjer sta b in d poljubni realni števili. Preizkus nam pove, da rešitvi res ustrezata. □

Trditev 1.8

Naj bo $p \in \mathbb{R}[x]$ nekonstanten polinom s pozitivnim vodilnim koeficientom. Potem za dovolj velike $n \in \mathbb{R}$ velja $p(n) > 0$.

Dokaz. Pogledamo absolutno največji koeficient in stopnjo. □

Bralcu predlagam tudi, da razmisli tudi, kaj se zgodi, če je vodilni koeficient negativen, in kaj, ko gre n proti $-\infty$.

1.2 Deljivost polinomov

Povedali smo že, da polinomov v splošnem ne moremo deliti med seboj, vseeno pa lahko definiramo deljenje in deljivost. V tem so si polinomi na primer podobni s celimi števili, ki jih tudi v splošnem ne moremo deliti med seboj.

Definicija 1.9

Polinom $p(x)$ je *deljiv* s polinomom $h(x)$, če obstaja polinom $q(x)$, da velja

$$p(x) = q(x)h(x).$$

Pravimo, da $g(x)$ *deli* $p(x)$.

Izrek 1.10

Za vsak par polinomov p, h obstajata enolično določena polinoma q in r, za katera velja

$$p(x) = q(x)h(x) + r(x)$$

in $\deg r < \deg h$. Polinom $q(x)$ imenujemo *kvocient*, polinom $r(x)$ pa *ostanek*.

Dokaz izreka opustimo, raje si na primeru oglejmo, kaj nam pove. Naj bo $p(x) = x^4 - 2x^3 + x$ in $h(x) = x^2 - x + 2$. V tem primeru velja

$$\frac{x^4 - 2x^3 + x}{x^2 - x + 2} = x^2 - x - 3 + \frac{6}{x^2 - x + 2}$$

oziroma

$$x^4 - 2x^3 + x = (x^2 - x - 3)(x^2 - x + 2) + 6.$$

Kvocient je $q(x) = x^2 - x - 3$, ostanek pa $r(x) = 6$.

Trditev 1.11

Naj bo p polinom. Če za nek a velja $p(a) = 0$, potem $(x - a)$ deli $p(x)$ oziroma obstaja polinom q, da velja

$$p(x) = (x - a)q(x).$$

Trditev velja tudi v nasprotno smer. Če $(x-a)$ deli p, potem lahko zapišemo $p(x) = (x-a)q(x)$ in velja $p(a) = 0$.

1.3 Ničle in razcepnost polinomov

Definicija 1.12

Število z je *ničla* polinoma p, če velja $p(z) = 0$.

Zelo enostavno lahko izračunamo ničlo linearnega polinoma $ax+b$, malo bolj zanimiv pa je primer kvadratnega polinoma ax^2+bx+c. Izkaže se, da sta njegovi ničli podani s *kvadratno formulo*:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

Kot zanimivost lahko povemo, da obstajata eksplicitni formuli tudi za ničle polinomov tretje in četrte stopnje, vendar sta slednji računsko bistveno zahtevnejši. Za polinome višje stopnje pa je celo dokazano, da eksplicitna formula sploh ne more obstajati.

Vemo že, da ima polinom stopnje n kvečjemu n različnih ničel, saj bi sicer bil enak ničelnemu polinomu. Seveda ni nujno, da ima polinom stopnje n res n različnih ničel. Na primer polinom $x^2-2x+1 = (x-1)^2$ ima edino ničlo $x = 1$. Ostane še vprašanje, če se lahko zgodi, da polinom sploh nima ničle. Hitro lahko ugotovimo, da je primer takšnega polinoma vsak neničelni konstantni polinom. Kaj pa v primeru nekonstantnega polinoma? Odgovor podaja naslednji znameniti izrek.

Izrek 1.13: Osnovni izrek algebre

Vsak nekonstanten polinom s kompleksnimi koeficienti ima vsaj eno kompleksno ničlo.

Dokaz izreka opustimo. Obstaja veliko različnih dokazov, vendar vsi močno presegajo nivo teh zapiskov. Izrek je zelo pomemben, vendar je bolj uporaben v naslednji obliki.

Trditev 1.14

Naj bo $p \in \mathbb{C}[x]$ polinom stopnje n. Potem ga lahko zapišemo v obliki

$$p(x) = a(x-x_1)\cdots(x-x_n),$$

kjer so $x_1, \ldots, x_n$ kompleksne ničle polinoma p.

Dokaz. Če je p konstanten polinom, potem je $p(x) = a$, sicer pa ima po osnovnem izreku algebre neko ničlo x_1 in ga lahko zapišemo kot $p(x) = (x-x_1)q(x)$, kjer je $q(x)$ polinom strogo manjše stopnje kot p. Dokaz trditve sledi induktivno. □

Vredno je omeniti, da v takšnem zapisu trditve ničle niso nujno različne. Ekvivalenten zapis trditve bi bil, da lahko vsak polinom napišemo kot

$$p(x) = a(x - x_1)^{\alpha_1} \cdots (x - x_k)^{\alpha_k},$$

kjer so $x_1, \ldots, x_k$ različne ničle polinoma P, naravna števila $\alpha_1, \ldots, \alpha_k$ pa njihove večkratnosti. V tem primeru velja $\alpha_1 + \cdots + \alpha_k = n$.

Naloga 1.15

Naj bo $p \in \mathbb{Z}[x]$ polinom stopnje $n \geq 5$. Recimo, da ima p različne celoštevilske ničle $0, x_2, \ldots x_n$. Poiščite vse celoštevilske ničle polinoma $P(P(x))$.

Rešitev. □

Naloga 1.16

Naj bo $p(x)$ kvadratni polinom. Dokažite, da obstajata kvadratna polinoma $g(x)$ in $h(x)$, za katera velja $p(x)p(x+1) = g(h(x))$.

Lahko bi zapisali $p(x) = ax^2 + bx + c$ in malo premetavali koeficiente. Izkaže se, da je lažje, če pogledamo ničle.

Rešitev. Naj bo $p(x) = a(x - x_1)(x - x_2)$. Potem je

$$\begin{aligned} p(x)p(x+1) &= a^2(x-r)(x-s+1)(x-s)(x-r+1) \\ &= a^2\left(\left[x^2 - (r+s-1)x + rs\right] - r\right)\left(\left[x^2 - (r+s-1)x + rs\right] - s\right). \end{aligned}$$

Torej lahko vzamemo $g(x) = a^2(x-r)(x-s)$ in $h(x) = x^2 - (r+s-1)x + rs$. □

Trditev 1.17

Naj bo $p \in \mathbb{R}[x]$. Če za kompleksno število z velja $p(z) = 0$, potem je tudi $p(\overline{z}) = 0$.

Dokaz. Naj bo $p(x) = a_n x^n + \cdots + a_1 x + a_0$ polinom s celoštevilskimi koeficienti in naj bo $p(z) = 0$, torej

$$a_n z^n + \cdots + a_1 z + a_0 = 0.$$

Konjugiramo obe strani in uporabimo lastnosti konjugiranja, da dobimo

$$\begin{aligned} \overline{a_n z^n + \cdots + a_1 z + a_0} &= \overline{0}, \\ \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} &= 0, \\ \overline{a_n} \cdot \overline{z^n} + \cdots + \overline{a} \cdot \overline{z} + \overline{a_0} &= 0, \\ a_n \overline{z^n} + \cdots + a\overline{z} + a_0 &= 0, \\ a_n \overline{z}^n + \cdots + a\overline{z} + a_0 &= 0. \end{aligned}$$

Torej je tudi $p(\overline{z}) = 0$. □

Trditev 1.18

Naj bo $p \in \mathbb{R}[x]$ polinom lihe stopnje. Potem ima realno ničlo.

Dokaz. Naj bo $p \in \mathbb{R}[x]$ polinom lihe stopnje n. Vemo, da ima n kompleksnih ničel (štetih z večkratnostjo). Ker kompleksne ničle nastopajo v konjugiranih parih, je kompleksnih ničel, ki niso realne sodo, mnogo. Torej je vsaj ena ničla realna. □

Trditev 1.19

Naj bo $p(x) \in \mathbb{Z}[x]$, a_n vodilni koeficient in a_0 prosti člen polinoma p. Če je $\frac{a}{b}$ racionalna ničla polinoma p, potem $a \mid a_0$ in $b \mid b_n$.

Dokaz. Trditev sledi iz

$$\begin{aligned} a_n \left(\frac{a}{b}\right)^n + \cdots + a_1 \left(\frac{a}{b}\right) + a_0 &= 0, \\ a_n a^n + a_{n-1} a^{n-1} b + \cdots + a_1 a b^{n-1} + a_0 b^n &= 0. \end{aligned}$$

□

Definicija 1.20

Polinom $p \in \mathbb{F}[x]$ je *razcepen* v $\mathbb{F}[x]$ natanko tedaj, ko obstajata nekonstantna polinoma $g, h \in \mathbb{F}[x]$, za katera velja $p(x) = g(x)h(x)$. Če polinom ni razcepen v $\mathbb{F}[x]$, pravimo, da je *nerazcepen* v $\mathbb{F}[x]$.

Vemo že, da lahko vsak polinom $p(x)$ zapišemo kot produkt linearnih faktorjev:

$$p(z) = a(z - z_1) \cdots (z - z_n),$$

torej vemo, da je vsak polinom, stopnje vsaj 2, razcepen v $\mathbb{C}[x]$. Prav tako je vsak polinom stopnje vsaj 3 razcepen v $\mathbb{R}[x]$.

V primeru kvadratnega polinoma $ax^2 + bx + c$, lahko povemo, da je nerazcepen v $\mathbb{R}[x]$ natanko tedaj, ko je diskriminanta $b^2 - 4ac$ negativna.

Navedimo še eno trditev, katere uporabo bomo videli v razdelku o polinomih s celoštevilskimi koeficienti.

Trditev 1.21

Če je polinom nerazcepen v $\mathbb{F}[x]$, potem sta v $\mathbb{F}[x]$ nerazcepna tudi polinoma $c \cdot p(x)$ in $p(x + c)$, kjer je c poljubna neničelna konstanta.

1.4 Vietove formule

Trditev 1.22: Vietove formule

Naj bo $p = a_n x^n + \dots a_1 x + a_0$ polinom stopnje n in naj bodo $z_1, \dots z_n$ njegove ničle. Potem za $k \in \{1, 2, \dots, n\}$ velja

$$\sum_{1 \le i_1 < i_2 < \dots < i_k \le n} \left(\prod_{j=1}^{k} z_{i_j} \right) = (-1)^k \frac{a_{n-k}}{a_n}.$$

Poglejmo si trditev na primeru kubičnega polinoma $p(x) = ax^3 + bx^2 + cx + d$, ki ima ničle z_1, z_2 in z_3. Vietove formule nam podajo naslednje enakosti:

$$\begin{aligned} z_1 + z_2 + z_3 &= -\frac{b}{a}, \\ z_1 z_2 + z_2 z_3 + z_3 z_2 &= \frac{c}{a}, \\ z_1 z_2 z_3 &= -\frac{d}{a}. \end{aligned}$$

Naloga 1.23

Poiščite vsoto vseh rešitev (tudi kompleksnih) enačbe

$$x^{2001} + \left(\frac{1}{2} - x \right)^{2001} = 0,$$

če veste, da ni večkratnih ničel.

Rešitev. Ker ni večkratnih ničel, je vsota vseh rešitev enačbe ravno vsota ničel polinoma $p(x) = x^{2001} + (1/2 - x)^{2001}$. Če zapišemo $p(x) = a_n x^n + \dots a_1 x + a_0$, kjer $a_n \neq 0$, je iskana vrednost $-a_{n-1}/a_n$. Uporabimo binomski izrek in dobimo

$$x^{2001} + \left(\frac{1}{2} - x \right)^{2001} = x^{2001} - x^{2001} + \frac{1}{2} \binom{2001}{1} x^{2000} - \binom{2001}{2} \left(\frac{1}{2} \right)^2 x^{1999} + \dots$$

Sledi, da je rešitev

$$\frac{a_{1999}}{a_{2000}} = \frac{\binom{2001}{2} \left(\frac{1}{2} \right)^2}{\frac{1}{2} \binom{2001}{1}} = \frac{2000}{4} = 500.$$

□

Naloga 1.24

Naj bo $p(x) = x^n + a_{n-1} x^{n-1} + \dots a_1 x + a_0$ polinom z neničelnimi celoštevilskimi koeficienti, ki ima n različnih celoštevilskih ničel. Dokažite, da, če so si ničle paroma tuje, potem sta si a_0 in a_1 tuja.

Rešitev. Recimo, da $\gcd(a_0, a_1) \neq 1$. Potem sta a_0 in a_1 deljiva z nekim praštevilom p. Naj bodo $z_1, \ldots, z_n$ ničle polinoma $p(x)$. Vietove formule nam povedo, da $z_1 z_2 \cdots z_n = (-1)^n a_n$. Torej obstaja neka ničla, brez škode za splošnost naj bo to 0, ki je deljiva s p. Po drugi strani pa vemo tudi

$$z_1 z_2 \cdot z_{n-1} + z_1 z_3 z_4 \cdots z_n + \cdots + z_2 z_3 \cdots z_n = (-1)^{n-1} a_{n-1} \equiv 0 \pmod{p}.$$

Ker so vsi členi, ki vsebujejo z_1, deljivi s p, velja tudi $p \mid z_2 z_3 \cdots z_n$. Torej obstaja še neka ničla, poleg z_1, ki je deljiva s p. To pa je v protislovju s tem, da so si ničle paroma tuje. $\square$

Naloga 1.25: Švica 2023

Poiščite vse polinome oblike

$$p(x) = x^{2023} + a_{2022} x^{2022} + \cdots + a_1 x + a_0$$

z realnimi koeficienti, za katere velja $a_{2022} = 0$, $P(1) = 1$, in vse ničle polinoma p so realne in manjše od 1.

Rešitev. Naj bodo $z_1, \ldots, z_{2023}$ ničle od p in $p(x) = (x - z_1)(x - z_2) \cdots (x - z_{2023})$. Pogoj $p(1) = 1$ je ekvivalenten $(1 - z_1)(1 - z_2) \cdots (1 - z_{2023}) = 1$, Vietove formule pa nam povedo $z_1 + z_2 + \cdots + z_{2023} = 0$. Skupaj dobimo

$$(1 - z_1)(1 - z_2) \cdots (1 - z_{2023}) = 1,$$
$$(1 - z_1) + (1 - z_2) + \cdots + (1 - z_{2023}) = 2023.$$

Iz tega sledi

$$\frac{1}{2023} \cdot \sum_{i=1}^{2023} (1 - z_i) = \left(\prod_{i=1}^{2023} (1 - z_i) \right)^{\frac{1}{2023}},$$

kar pa je ravno primer enakosti v neenakosti med aritmetično in geometrijsko sredino (ki jo lahko uporabimo, saj je $1 - z_i > 0$ za vse i). Dobimo $z_1 = z_2 = \cdots = z_{2023} = 0$. Edina rešitev je torej $p(x) = x^{2023}$, ki res zadošča pogojem naloge. $\square$

2 Polinomi s celoštevilskimi koeficienti

2.1 Deljivost

V nadaljevanju bomo malo več pozornosti posvetili polinomom s celoštevilskimi koeficienti. Tu si bomo lahko pomagali z znanjem teorije števil. Naloge so pogosto zelo podobne nalogam iz teorije števil. Daleč najpomembnejši rezultat tega poglavja je sledeči izrek.

Izrek 2.1

Naj bo p polinom s celoštevilskimi koeficienti. Potem za vsaki celi števili a in b velja

$$a - b \mid p(a) - p(b).$$

Dokaz. Naj bo $p(x) = c_n x^n + \cdots + c_1 x + c_0$. Velja

$$p(a) - p(b) = c_n(a^n - b^n) + c_{n-1}(a^{n-1} - b^{n-1}) + c_0(a - b).$$

Upoštevamo, da $(a - b) \mid (a^k - b^k)$ za poljubno naravno število k. $\square$

Naloga 2.2

Naj za polinom $p(x)$ s celimi koeficienti velja $p(3) = 2$. Ali je lahko število $p(2003)$ popoln kvadrat?

Rešitev. Ker ima polinom p cele koeficiente, $x - y$ deli $p(x) - p(y)$, torej

$$2000 \mid p(2003) - p(3) = p(2003) - 2.$$

Sledi

$$p(2003) - 2 \equiv 0 \Rightarrow p(2003) \equiv 2 \pmod 4,$$

torej $p(2003)$ ni popoln kvadrat. $\square$

Naloga 2.3

Naj bo p polinom s celoštevilskimi koeficienti. Dokažite, da ne obstajajo različna cela števila a, b in c, za katera bi veljalo $p(a) = b$, $p(b) = c$ in $p(c) = a$.

Rešitev. Recimo, da taka različna cela števila a, b in c obstajajo. Velja

$$a - b \mid p(a) - p(b), \qquad b - c \mid p(b) - p(c) \quad \text{in} \quad c - a \mid p(c) - p(a).$$

Te tri pogoje lahko združimo v

$$a - b \mid p(a) - p(b) = b - c \mid p(b) - p(c) = c - a \mid p(c) - p(a) = a - b.$$

Dobili smo $a - b \mid b - c \mid c - a \mid a - b$, kar pomeni, da $|a - b| \le |b - c| \le |c - a| \le |a - b|$. Očitno povsod veljajo enakosti, torej

$$|a - b| = |b - c| = |c - a|\,.$$

Brez škode za splošnost lahko predpostavimo, da je a največje med njimi, torej velja

$$a - b = |a - b| = |c - a| = a - c \Rightarrow c = b,$$

kar pa je v protislovju s tem, da so števila a, b in c različna. $\square$

Naloga 2.4: 3. Izbirni test 2020, 1. naloga

Naj bo $n > 1$ naravno število ter naj bo $p(x)$ polinom stopnje n, ki ima celoštevilske koeficiente. Naj bo A množica $n + 1$ zaporednih celih števil. Dokažite, da obstaja število $a \in A$, za katerega za vsako celo število x velja, da $p(x) \neq a$.

Rešitev. Prepuščena bralcu. □

Izrek 2.5: Schur

Naj $f(x) \in \mathbb{Z}[x]$ nekonstanten polinom. Potem obstaja neskončno mnogo praštevil, ki delijo vsaj enega od neničelnih členov zaporedja $f(1)$, $f(2)$, $f(3)$, ...

Dokaz. Naj bo $f \in \mathbb{Z}[x]$ nekonstanten polinom. Če je $f(0) = 0$, potem $p \mid f(p)$, torej smo končali.

Recimo, da $f(0) \neq 0$. Želimo $p(0) = 1$. Definiramo $g(x) := \frac{f(xf(0))}{f(0)}$. Velja $g \in \mathbb{Z}[x]$ in $g(0) = 1$.

Za dovolj velike n vedno velja $g(n) > 0$. Velja $g(n) \equiv 1 \pmod n$ za vsak $n \in \mathbb{N}$. Recimo, da je $\{p_1, \ldots, p_k\}$ končna množica iskanih praštevilskih deliteljev, potem izberemo $n := p_1 \cdots p_l$, in velja $g(n) = kn + 1$ za nek k, torej smo dobili nov praštevilski delitelj, kar je protislovje.

Ker je vsak delitelj $g(n)$ tudi delitelj $f(nf(0))$, smo končali. □

Naloga 2.6: Taiwan 2014

Naj bo k celo število. Poiščite vse polinome $f \in \mathbb{Z}[x]$ za katere za vsako naravno število velja

$$f(n) \mid (n!)^k.$$

Rešitev. Za vsak praštevilski delitelj p od $n!$ zagotovo velja $p \leq n$. Če izberemo tako praštevilo, da $p \mid f(n)$, potem lahko predpostavimo $1 \leq n \leq p$ (če bi bil n večji od p, bi lahko vzeli $n - p$ in bi pogoj deljivosti še vedno veljal). Če velja tudi $p \mid n!$, potem $n = p$, torej $p \mid f(p)$ oziroma $p \mid a_0$, kjer je a_0 prosti člen polinoma.

Če je f nekonstanten polinom, nam Schurov izrek pove, da obstaja neskončno takih praštevil p, torej $a_0 = 0$. Definiramo polinom $q(x) = \frac{f(x)}{x} \in \mathbb{Z}[x]$. Tudi ta polinom zadošča pogojem naloge in velja $\deg q < \deg p$. Na tak način lahko nadaljujemo, dokler ne dobimo konstantega polinoma. To pomeni, da je $f(x)$ oblike cx^a za nek a. Če vstavimo v $f(n) \mid (n!)^k$, dobimo $f(x) = \pm x^b$, kjer je $0 \leq b \leq k$. □

2.2 Razcepnost polinomov s celoštevilskimi koeficienti

Trditev 2.7: Gaussova lema

Če je polinom $p \in \mathbb{Z}[x]$ razcepen v $\mathbb{Q}[x]$, potem je razcepen tudi v $\mathbb{Z}[x]$.

Trditev 2.8: Eisensteinov kriterij

Naj bo

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

polinom s celoštevilskimi koeficienti stopnje $n \geq 1$. Če obstaja tako praštevilo p, da

$$p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}, p \nmid a_n \text{ in } p^2 \nmid a_0,$$

potem je $p(x)$ nerazcepen v $\mathbb{Q}[X]$.

Naloga 2.9

Pokažite, da so polinomi

$$\begin{aligned} p(x) &= 7x^6 + 30x^3 - 6x^2 + 60, \\ q(x) &= \frac{3}{7}x^5 - \frac{7}{2}x^2 - x + 2 \text{ in} \\ r(x) &= x^4 + 1 \end{aligned}$$

nerazcepni v $\mathbb{Q}[x]$.

Rešitev. Za $p(x)$ uporabimo Eisensteinov kriterij za $p = 3$.

Skalarni večkratnik ne vpliva na razcepnost, torej lahko dokažemo nerazcepnost

$$14q(x) = 6x^5 - 49x^2 - 14x + 28.$$

V tem primeru lahko uporabimo Eisensteinov kriterij za $p = 7$.

Če je polinom $h(x)$ nerazcepen, je nerazcepen tudi polinom $h(x+1)$. Poglejmo si torej

$$r(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2.$$

Tu lahko uporabimo kriterij za $p = 2$. □

Naloga 2.10

Naj bo p praštevilo. Pokažite, da je $p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ nerazcepen v $\mathbb{Z}[x]$.

Rešitev. Polinom $p(x+1)$ razvijemo s pomočjo binomskega izreka in uporabimo Eisensteinov kriterij. □

3 Lagrangeeva interpolacija

Vemo že, da je polinom stopnje $n - 1$ natančno določen z n točkami. Preostane pa še vprašanje, kako ta polinom določiti.

Lahko bi ga izračunali tako, da bi rešili sistem $n+1$ enačb.

$$\begin{aligned} a_n x_1^n + \cdots + a_1 x_1 + a_0 &= y_1, \\ a_n x_2^n + \cdots + a_1 x_2 + a_0 &= y_2, \\ &\vdots \\ a_n x_n^n + \cdots + a_1 x_n + a_0 &= y_n. \end{aligned}$$

Tak način bi lahko postal zelo zamuden. Veliko boljši način nam nudi t.i. Lagrangeeva interpolacija.

Izrek 3.1

Naj bodo $(x_1, y_1), \ldots (x_{n+1}, y_{n+1})$ točke v ravnini z različnimi x-koordinatami. Potem obstaja enolično določen polinom $p(x)$ stopnje največ $n-1$, ki poteka skozi te točke. Podan je s formulo

$$p(x) = \sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Bralcu je prepuščen razmislek, da ta formula v splošnem res deluje. Tu si jo bomo pogledali samo na primeru.

Naloga 3.2

Poiščite polinom stopnje 3, za katerega velja $p(1) = 2$, $p(2) = 3$, $p(3) = 4$ in $p(4) = 5$.

Rešitev. Izrek nam pove:

$$\begin{aligned} p(x) = 2 \cdot \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + 3 \cdot \frac{(x-3)(x-4)(x-1)}{(2-3)(2-4)(2-1)} + \\ +4 \cdot \frac{(x-4)(x-1)(x-2)}{(3-4)(3-1)(3-2)} + 5 \cdot \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)}. \end{aligned}$$ □

Za ilustracijo si poglejmo, kaj se zgodi, ko vstavimo $x = 2$:

$$p(2) = 0 + 3 \cdot \frac{(2-3)(2-4)(2-1)}{(2-3)(2-4)(2-1)} + 0 + 0 = 3.$$

Za konec si še poglejmo kako lahko Lagrangeevo interpolacijo uporabimo v nalogi s tekmovanja.

Naloga 3.3: IMO Shortlist 1997

Naj bo p praštevilo in $f \in \mathbb{Z}[x]$ polinom, za katerega velja $f(0) = 0$, $f(1) = 1$ in $f(n) \equiv 0$ ali $f(n) \equiv 1 \pmod{p}$ za vsako celo število n. Dokažite, da je f stopnje vsaj $p-1$.

Rešitev. Če je $p = 2$, f ne more biti konstanten, torej je stopnje vsaj $p - 1 = 1$. Naj bo $p > 2$. Recimo, da je $\deg f \leq p - 2$. Ker imamo nek podatek o vrednostih f v točkah $0, 1, 2, \ldots$, lahko uporabimo Lagrangeevo interpolacijo za točke $0, 1, 2, \ldots, p - 1$, da dobimo

$$f(x) = \sum_{j=0}^{p-1} f(j) \prod_{i \neq j} \frac{x - i}{j - i}.$$

To je polinom stopnje $p - 1$, kar pa je v protislovju z našo predpostavko. Torej je vodilni koeficient enak 0. Dobimo

$$0 = \sum_{j=0}^{p-1} f(j) \prod_{i \neq j} \frac{1}{j - i} = \sum_{j=0}^{p-1} f(j) \cdot \frac{(-1)^{p-1+j}}{j!(p - j - 1)!}.$$

Od tod sledi (obe strani pomnožimo s $(p - 1)!$)

$$\sum_{j=0}^{p-1} (-1)^j \binom{p-1}{j} f(j) = 0.$$

Upoštevamo

$$\binom{p-1}{j} = \frac{(p-1)(p-2)\cdots(p-j)}{j(j-1)\cdots 1} \equiv \frac{(-1)(-2)\cdots(-j)}{j!} \equiv (-1)^j \pmod{p}$$

in dobimo

$$f(0) + f(1) + \cdots + f(p - 1) \equiv 0 \pmod{p}.$$

Ampak, ker je $f(i) \in \{0, 1\} \pmod{p}$, je to nemogoče, razen v primeru, ko bi vedno veljalo $f(i) = 0$, kar pa ni mogoče, ker je $f(1) = 1$. $\square$

Literatura

[1] Aditya Khurmi. *Modern Olympiad Number Theory*. 2020. Pogl. 7, str. 179–209. URL: https://www.academia.edu/44512122/Modern_Olympiad_Number_Theory.

[2] Alexander Remorov. *Polynomials*. 2011. URL: https://alexanderrem.weebly.com/uploads/7/2/5/6/72566533/polynomials.pdf (pridobljeno 24. 1. 2024).