mezinárodní
korespondenční
seminář

iksko.org

Aritmetické vlastnosti polynomů

Matěj Doležálek

Abstrakt. Na polynomy klasicky nahlížíme jako na funkce, které shodou okolností mají hezký předpis. Nový úhel pohledu se však otevírá, začneme-li místo toho s polynomy zacházet jako s formálními výrazy, do kterých se shodou okolností dá dosazovat. To nám umožní zkoumat jejich číslo teoretické vlastnosti jako dělitelnost, ireducibilitu nebo třeba násobnost kořenů. Tímto přístupem trochu zabrousíme do vysokoškolské teorie, ale získané nástroje dobře upotřebíme ke zdolání olympiádních úloh.

Definice. *Oborem integrity* rozumíme množinu R, v níž se dá sčítat, odečítat a násobit podle všech obvyklých pravidel (včetně toho, že součin nenulových prvků je nenulový). Obor integrity K, v němž se navíc dá dělit každým nenulovým prvkem, nazveme *těleso*.

Úmluva. Není-li řečeno jinak, budeme pro obecnost označovat písmenem R libovolný obor integrity a písmenem K libovolné těleso. Pokud se s těmito pojmy nekamarádíš, můžeš si s klidným svědomím konkrétněji představovat obor celých čísel $\mathbb{Z}$ a tělesa (což jsou zároveň také obory integrity) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a $\mathbb{Z}_p$ pro prvočísla p.

Obory polynomů

Definice. *Polynomem* nad R rozumíme výraz tvaru

$$f = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0,$$

kde n je nezáporné celé číslo a $c_i \in R$, tyto prvky nazýváme *koeficienty* f. *Stupněm* nenulového f (značíme $\deg f$) rozumíme největší k takové, že $c_k \neq 0$, a stupeň nulového polynomu dodefinováváme jako $-\infty$.

Polynomy lze sčítat po členech a násobit pomocí distributivity a vztahů $x^k \cdot x^\ell = x^{k+\ell}$. Toto jim dává strukturu oboru integrity, který značíme $R[x]$.

Cvičení. Pro polynomy f, g nad oborem integrity platí

$$\deg(f+g) \leq \max\{\deg f, \deg g\} \quad \text{a} \quad \deg(f \cdot g) = \deg f + \deg g.$$

Poznámka. Koeficient c_0 nazýváme *absolutní člen*. Koeficient $c_{\deg f}$ polynomu $f \neq 0$ se nazývá *vedoucí koeficient* a někdy se značí $\operatorname{lc} f$. Polynom s vedoucím koeficientem 1 se nazývá *monický*.

Definice. V oboru integrity R říkáme, že a *dělí* b (značíme $a \mid b$), pokud existuje c takové, že $b = ac$. Dále říkáme, že a je kongruentní b modulo m (značíme $a \equiv b \pmod m$), pokud $m \mid a - b$. Prvek d nazveme *největším společným dělitelem* prvků a, b, pokud $d \mid a$, $d \mid b$ a zároveň pro každé c splňující $c \mid a$, $c \mid b$ platí i $c \mid d$.

Speciálně tyto obecné definice používáme i v oborech polynomů $R[x]$.

Tvrzení (dělení se zbytkem). Je-li K těleso, pak pro libovolná $f, g \in K[x]$, $g \neq 0$ lze zvolit $q, r \in K[x]$ tak, že $f = qg + r$ a zároveň $\deg r < \deg g$.

Tvrzení (Bézoutova identita). Je-li K těleso a $d \in K[x]$ je největším společným dělitelem $f, g \in K[x]$, pak existují $a, b \in K[x]$ taková, že $af + bg = d$.

Dosazování a kořeny

Definice. Je-li $f = c_n x^n + \cdots + c_1 x + c_0 \in R[x]$ a máme další polynom $g \in R[x]$, můžeme jej *dosadit* do f a obdržet tak

$$f(g) = c_n g^n + \cdots + c_1 g + c_0 \in R[x].$$

Speciálně můžeme dosazovat prvky $a \in R$. Prvek $r \in R$ splňující $f(r) = 0$ nazýváme *kořenem* polynomu f.

Tvrzení. Jsou-li $f, a, b \in R[x]$, pak v $R[x]$ platí $a - b \mid f(a) - f(b)$. Ekvivalentně, pokud $a \equiv b \pmod{m}$, pak i $f(a) \equiv f(b) \pmod{m}$.

Cvičení. Je-li $r \in R$ kořenem polynomu $f \in R[x]$, pak $x - r \mid f$.

Definice. Říkáme, že $r \in R$ je kořenem *násobnosti* m polynomu f, jestliže platí $(x - r)^m \mid f$.

Tvrzení. Nenulový polynom stupně n nad oborem integrity má v tomto oboru nanejvýš n kořenů včetně násobnosti.

Cvičení. Pokud se polynomy f, g stupně nanejvýš n nad oborem integrity shodují v alespoň $n + 1$ bodech, pak $f = g$.

Věta (základní věta algebry). Polynom $f \in \mathbb{C}[x]$ stupně n má v $\mathbb{C}$ přesně n kořenů včetně násobnosti.

Tvrzení. Jsou-li $x_1, \ldots, x_n \in R$ kořeny (včetně násobnosti) polynomu $f \in R[x]$ stupně n, pak

$$f = a(x - x_1) \cdots (x - x_n)$$

pro nějaké $a \in R$.

Tvrzení (Viètovy vztahy). Je-li v předchozím tvrzení $f = c_n x^n + \cdots + c_1 x + c_0$, pak pro $0 \leq k \leq n$ platí

$$(-1)^k c_k = c_n \cdot \sum_{\substack{J \subseteq \{1,\ldots,n\} \\ |J| = k}} \prod_{i \in J} x_i.$$

Věta (rational root theorem). Je-li racionální číslo $\frac{p}{q}$ v základním tvaru kořenem celočíselného polynomu $c_n x^n + \cdots + c_1 x + c_0$, pak platí $p \mid c_0$ a $q \mid c_n$.

Cvičení. Racionální kořen monického celočíselného polynomu už musí být celé číslo.

Tvrzení. Je-li $f \in \mathbb{C}[x]$ nekonstantní, pak pro $|z| \to \infty$ nastává i $|f(z)| \to \infty$. Neformálně řečeno: nekonstantní polynomy při zvětšování argumentu utíkají do nekonečna.

Definice. *(Formální) derivací* polynomu

$$f = \sum_{k=0}^{n} c_k x^k \in R[x]$$

rozumíme polynom

$$f' = \sum_{k=1}^{n} k c_k x^{k-1} \in R[x].$$

Tvrzení. Formální derivace splňuje obvyklé vztahy pro analýznickou derivaci, např.

$$(f+g)' = f' + g', \qquad (f \cdot g)' = f' \cdot g + f \cdot g' \qquad \text{a} \qquad (f(g))' = f'(g) \cdot g'.$$

Tvrzení (detekce násobných kořenů). Je-li r kořenem násobnosti $m > 1$ polynomu f, pak je také kořenem násobnosti $m-1$ polynomu f'.

Ireducibilita

Definice. Prvek $u \in R$ oboru integrity nazveme *jednotkou*, pokud $u \mid 1$. Nenulový prvek $q \in R$ nazveme *ireducibilním*, pokud není to jednotka a jeho jsou děliteli až na přenásobení jednotkou pouze 1 a q. Nenulový prvek $p \in R$ nazveme *prvočinitelem*, pokud to není jednotka a navíc $p \mid ab$ implikuje $p \mid a$ nebo $p \mid b$ pro libovolná $a, b \in R$.

Poznámka. O ireducibilitě vždy mluvíme nad konkrétním oborem: kupříkladu polynom $2x^2 + 2$ není ireducibilní nad $\mathbb{Z}$, zatímco nad $\mathbb{Q}$ a $\mathbb{R}$ ireducibilní je a nad $\mathbb{C}$ opět není.

Tvrzení. Je-li K těleso, pak je každý ireducibilní polynom v $K[x]$ nutně také prvočinitelem.

Tvrzení (kořeny chodí spolu). Nechť jsou $K \subseteq L$ tělesa a $f, g \in K[x]$ polynomy. Pokud je f ireducibilní nad K a má s g společný kořen v L, pak už v $K[x]$ platí $f \mid g$.

Poznámka. Předchozí tvrzení typicky využijeme s $K = \mathbb{Q}$, $L = \mathbb{C}$.

Cvičení. Nahlédni, že ireducibilní polynom $f \in \mathbb{Q}[x]$ nemůže mít násobný komplexní kořen.

Definice. Polynom $c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ nazveme *primitivním*, pokud $\gcd(c_0, c_1, \ldots, c_n) = 1$.

Věta (Gaussovo lemma). Primitivní polynom $f \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}$, právě když je ireducibilní nad $\mathbb{Q}$.

Věta (Eisensteinovo kritérium). Nechť je $f = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ primitivní polynom. Pokud pro nějaké prvočíslo p platí

(i) $p \mid c_i$ pro $0 \leq i \leq n-1$,
(ii) $p \nmid c_n$,
(iii) $p^2 \nmid c_0$,

pak je f ireducibilní nad $\mathbb{Z}$.

Věta (rozšířený Eisenstein). Nechť je $f = c_n x^n + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ primitivní polynom. Pokud pro nějaké prvočíslo p a přirozené číslo k platí

(i) $p \mid c_i$ pro $0 \leq i \leq k-1$,
(ii) $p \nmid c_k$,
(iii) $p^2 \nmid c_0$,

pak je f násobkem ireducibilního polynomu stupně alespoň k.

Úlohy

Úloha 1. Je dán polynom $f \in \mathbb{Z}[x]$ stupně n a přirozená čísla k, m. Nahlédni, že pokud žádné z čísel

$$f(k), \quad f(k+1), \quad \ldots, \quad f(k+m-1)$$

není násobkem m, pak f nemá celočíselný kořen.

Úloha 2. Komplexní číslo $\alpha \neq 0$ je kořenem polynomu $f \in \mathbb{Q}[x]$. Najdi polynom $g \in \mathbb{Q}[x]$, jehož kořenem je $\frac{1}{\alpha}$.

Úloha 3. Lze zvolit reálná a, b, c tak, aby každý ze tří polynomů

$$ax^2 + bx + c, \qquad bx^2 + cx + a, \qquad cx^2 + ax + b$$

měl dva různé reálné kořeny?

Úloha 4. Královské vojsko táhne krajinou po křivce, která má tvar grafu polynomu f s celočíselnými koeficienty. Boleslav si cestu zkrátil po úsečce mezi body $A = [a, f(a)]$ a $B = [b, f(b)]$, kde $a, b \in \mathbb{Z}$. Všiml si navíc, že délka této úsečky byla celé číslo. Dokaž, že Boleslav táhl ve směru rovnoběžném s osou x.

Úloha 5. Nahlédni, že polynom

$$1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

nemá násobný kořen.

Úloha 6. Nahlédni, že $x^a - 1 \mid x^b - 1$, právě když $a \mid b$.

Úloha 7. Pro polynom $f \in \mathbb{Z}[x]$ má rovnice $|f(x)| = 1$ alespoň tři různá celočíselná řešení. Dokaž, že potom f nemá celočíselný kořen.

Úloha 8. Nahlédni, že $nx^{n+1} - (n+1)x^n + 1$ má násobný kořen.

Úloha 9. Lucienovi se zdálo o nenulovém polynomu $f \in \mathbb{Z}[x]$ s nezápornými celočíselnými koeficienty. Áďa se může ptát na celá čísla z a Lucien jí vždy odpoví hodnotu $f(z)$. Kolik nejméně otázek Áďa potřebuje, aby zaručeně uhodla Lucienův polynom? (PraSe–36–4p–6)

Úloha 10. Monický polynom $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in \mathbb{Z}[x]$ má všechny kořeny celočíselné a po dvou nesoudělné. Dokaž, že $\gcd(c_0, c_1) = 1$.

Úloha 11. Polynom $f \in \mathbb{Z}[x]$ má sudý stupeň a všechny koeficienty liché. Může mít racionální kořen?

Úloha 12. Polynomy $f, g, h \in \mathbb{R}[x]$ splňují $x^2 + x + 1 \mid f$ a zároveň

$$f(x) = g\left(x^3\right) + x \cdot h\left(x^3\right).$$

Dokaž, že $x - 1$ dělí g i h.

Úloha 13. Jsou dána $a, b, c, d \in \mathbb{Z}$ taková, že ad je liché a bc sudé. Nahlédni, že $ax^3 + bx^2 + cx + d$ má (klidně komplexní) iracionální kořen.

Úloha 14. Reálný polynom $ax^4 + bx^3 + 1$ je násobkem $(x-1)^2$. Urči a, b.

Úloha 15. Pro každé prvočíslo p je polynom $x^{p-1} + x^{p-2} + \cdots + x + 1$ ireducibilní nad $\mathbb{Z}$.

Úloha 16. Najdi všechny dvojice přirozených čísel (m, n) takové, že

$$1 + x + \cdots + x^m \mid 1 + x^n + \cdots + x^{mn}.$$

(USAMO 1977)

Úloha 17. Jsou dány polynomy $f, g \in \mathbb{Z}[x]$, které jsou v $\mathbb{Z}[x]$ nesoudělné. Nahlédni, že posloupnost $a_n = \gcd(f(n), g(n))$ je periodická.

Úloha 18. Najdi všechny polynomy $f \in \mathbb{Z}[x]$, jež splňují $f(n) \mid n! + 2$ pro každé $n \in \mathbb{N}$. (PraSe–41–4p–7)

Úloha 19. Nekonečnou posloupnost $c_0, c_1, \ldots$ přirozených čísel nazvěme *krutopřísnou*, pokud je pro každé $n \in \mathbb{N}$ polynom

$$c_nx^n + \cdots + c_1x + c_0$$

ireducibilní nad $\mathbb{Z}$. Najdi krutopřísnou posloupnost, v níž se vyskytují jen dva navzájem různé prvky. (PraSe–40–3s–2)

Úloha 20. Pro která $k \in \mathbb{Z}$ lze zvolit $a, b \in \mathbb{Z}$ tak, aby polynomy

$$x^5 - kx + 1 \qquad \text{a} \qquad x^2 - ax - b$$

měly společný komplexní kořen?

Úloha 21. Polynom $f \in \mathbb{Z}[x]$ má tu vlastnost, že pro libovolná přirozená m, n má kongruence $f(x) \equiv n \pmod{m}$ řešení. Dokaž, že f je lineární.

Úloha 22. Polynom $f \in \mathbb{Z}[x]$ a čísla $a \in \mathbb{Z}$, $k \in \mathbb{N}$ splňují

$$\underbrace{f(\cdots f(}_{k\text{-krát}} a) \cdots) = a.$$

Dokaž, musí platit i $f(f(a)) = a$.

Úloha 23. Najdi všechny polynomy $f \in \mathbb{Z}[x]$, které splňují $n \mid f(2^n)$ pro každé $n \in \mathbb{N}$.

Úloha 24. Dokaž, že pro přirozené $n > 1$ je polynom $x^n + 5x^{n-1} + 3$ ireducibilní nad $\mathbb{Z}$. (IMO 1993)

Úloha 25. Pro které polynomy $f \in \mathbb{Z}[x]$ platí pro $a, b \in \mathbb{Z}$ implikace

$$a \mid b \implies f(a) \mid f(b)?$$

Úloha 26. Jsou dána $a, b, c, d, e, f \in \mathbb{N}$ taková, že pro $S = a + b + c + d + e + f$ platí $S \mid abc + def$ a zároveň $S \mid ab + bc + ca - de - ef - fd$. Dokaž, že S je složené číslo. (ISL 2005 N3)

Úloha 27. Jsou-li pro $a, b, c \in \mathbb{Z}$ obě čísla $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ i $\frac{a}{c} + \frac{b}{a} + \frac{c}{b}$ celá, dokaž, že $|a| = |b| = |c|$.

Úloha 28. Je dáno zobrazení $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$, jež splňuje:

(i) Pro libovolný polynom $f \in \mathbb{Z}[x]$ je $\varphi(f + 1) = \varphi(f) + 1$.
(ii) Pokud pro polynomy $f, g \in \mathbb{Z}[x]$ platí $f \mid g$, pak i $\varphi(f) \mid \varphi(g)$.

Dokaž, musí existovat $z \in \mathbb{Z}$ takové, že $\varphi(f) = f(z)$ pro každé $f \in \mathbb{Z}[x]$.
(PraSe–40–3s–3)

Úloha 29 (Schurova věta). Pro nekonstantní $f \in \mathbb{Z}[x]$ existuje nekonečně mnoho prvočísel p, která dělí nějakou nenulovou hodnotu $f(n) \neq 0$ pro nějaké $n \in \mathbb{N}$.

Úloha 30. Budiž dán nekonstantní polynom $f \in \mathbb{Z}[x]$ a přirozená čísla n, k. Nahlédni, že existuje $a \in \mathbb{N}$ takové, že každé z čísel $f(a), f(a+1), \ldots, f(a+n-1)$ má alespoň k různých prvočíselných dělitelů.

Úloha 31. Je dán polynom $f \in \mathbb{Z}[x]$ splňující $f(n) > n$ pro každé $n \in \mathbb{N}$. Definujme nekonečnou posloupnost celých čísel pomocí $a_1 = 1$, $a_{i+1} = f(a_i)$. Dokaž, že pokud je pro každou $m \in \mathbb{N}$ nějaký člen a_i násobkem m, pak je $f = x + 1$.
(Iran TST 2004)

Úloha 32. Je dán polynom $f \in \mathbb{Z}[x]$ stupně $n > 1$. Dokaž, že lze zvolit $g \in \mathbb{Z}[x]$ tak, aby $f(g(x))$ byl reducibilní nad $\mathbb{Z}$.

Úloha 33. Jsou-li $a_1, \ldots, a_n$ navzájem různá celá čísla, dokaž, že polynom

$$(x - a_1) \cdots (x - a_n) - 1$$

je ireducibilní nad $\mathbb{Z}$.

Úloha 34. Pro monické ireducibilní polynomy $f, g \in \mathbb{Z}[x]$ platí, že $f(n)$ a $g(n)$ mají stejné množiny prvočíselných dělitelů pro všechna kromě konečně mnoha $n \in \mathbb{N}$. Dokaž, že $f = g$.

Úloha 35. Pro které polynomy $f \in \mathbb{Z}[x]$ platí, že jsou-li $a, b \in \mathbb{Z}$ nesoudělná, pak jsou i $f(a)$, $f(b)$ nesoudělná? (Iran 2004)

Úloha 36. Je dán polynom $f = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + 1$, v němž všechna c_i jsou nezáporná celá čísla a navíc platí $c_{n-i} = c_i$. Dokaž, že existuje nekonečně mnoho dvojic (a, b) přirozených čísel takových, že $a \mid f(b)$ a zároveň $b \mid f(a)$.
(*i*KS 2–N5)

Úloha 37. Pro která k platí, že splňuje-li $f \in \mathbb{Z}[x]$ nerovnosti $0 \leq f(a) \leq k$ pro $a \in \{0, \ldots, k+1\}$, pak už $f(0) = f(1) = \cdots = f(k+1)$. (ISL 1997)

Úloha 38. Pro která n lze zvolit navzájem různá celá čísla $a_1, \ldots, a_n$ tak, aby polynom

$$(x - a_1) \cdots (x - a_n) + 1$$

byl reducibilní nad $\mathbb{Z}$?

Úloha 39. Mějme polynom $f \in \mathbb{Z}[x]$ s alespoň dvěma různými celočíselnými kořeny a označme $A = \{f(a) \mid a \in \mathbb{Z}\}$. Ukaž, že pokud v A leží m po sobě jdoucích přirozených čísel, pak tato čísla nejsou menší než $\frac{m!}{2}$.

Úloha 40. Mějme funkci $f : \mathbb{Z} \to \mathbb{R}$, k níž existuje polynom p takový, že pro každá $a, b \in \mathbb{Z}$ platí nerovnost $|f(a)| < p(a)$ a rozdíl $f(a) - f(b)$ je celočíselným násobkem $a - b$. Dokaž, že pro jistý polynom $q \in \mathbb{R}[x]$ platí $f(a) = q(a)$ pro všechna $a \in \mathbb{Z}$.
(PraSe 34–2j–8)

Literatura a zdroje

[1] Filip Sládek: *Artimetické vlastnosti polynómov*, sborník *i*KS, 2013.
[2] Danil Koževnikov: *Aritmetické vlastnosti polynomů*, Paseky, 2018.
[3] Fíla Čermák, Matěj Doležálek: *Teorie nejen čísel*, PraSečí seriál, 2020/2021.

Hinty

Hint 1. Modulo m.
Hint 2. Jak vypadá $f\left(\frac{1}{x}\right)$?
Hint 3. Diskriminanty.
Hint 4. Rozdíl argumentů dělí rozdíl hodnot.
Hint 5. Nevypadá derivace nějak hezky?
Hint 6. Odmocniny z jedničky.
Hint 7. Rozdíl argumentů dělí rozdíl hodnot.
Hint 8. Derivace.
Hint 9. Desítková (nebo jakákoliv jiná poziční) soustava.
Hint 10. Viètovy vztahy.
Hint 11. Rational root theorem a modulo 2.
Hint 12. Kořeny $x^2 + x + 1$.
Hint 13. Pokud má všechny kořeny racionální, vyvoď spor skrz rational root theorem a Viètovy vztahy.
Hint 14. Derivace a dosazení.
Hint 15. Posuň argument.
Hint 16. Odmocniny z jedničky.
Hint 17. Gaussovo lemma a Bézout.
Hint 18. $f(n)$ by nemělo mít malé dělitele, ale přitom hodnoty polynomu modulo cokoliv jsou periodické.
Hint 19. Eisenstein v obráceném pořadí.
Hint 20. $x^2 \equiv ax + b$. Pozor na pečlivý rozbor případů, mělo by vyjít $k \in \{-1, 0, 2\}$.
Hint 21. Co se stane, když je $a - b$ vlastní dělitel $f(a) - f(b)$?
Hint 22. Rozdíl argumentů dělí rozdíl hodnot, opakovaně.
Hint 23. Malý Fermat.
Hint 24. Rozšířený Eisenstein.
Hint 25. $f(2x) - 2^{\deg f} f(x)$.
Hint 26. $(x + a)(x + b)(x + c) - (x - d)(x - e)(x - f)$.
Hint 27. Vyrob polynom, který o příslušných číslech něco hezkého poví.
Hint 28. Zvol $z = \varphi(x)$.
Hint 29. Předpokládej, že je jen konečně mnoho takových prvočísel, omez valuace a vyvoď spor s tím, že nekonstantní polynomy utíkají do nekonečna.
Hint 30. Schur + čínská zbytková věta.
Hint 31. Rozdíl argumentů je dělitelem rozdílu hodnot. Co když to bude vlastní dělitel?
Hint 32. $g(x) - x \mid f(g(x)) - f(x)$.
Hint 33. Uvaž rozklad a dosazuj a_i.
Hint 34. Zkombinuj úlohu o společných dělitelích hodnot nesoudělných polynomů s Schurovou větou.
Hint 35. Pokud $f(0) \neq 0$, využij prvočísla $p \nmid f(0)$.
Hint 36. $(a, b) \mapsto \left(b, \frac{f(b)}{a}\right)$.
Hint 37. Vytkni kořeny z $f(x) - f(0)$.
Hint 38. Uvaž rozklad a dosazuj a_i.

Hint 39. Uvědom si, jak mohou být uspořádány vzory uvažované m-tice a vyrob polynom s mnoha kořeny.

Hint 40. Interpoluj v dostatečně mnoha bodech, pak ukaž rovnost ve všech dostatečně velkých bodech.