

Celočíselné polynómy

Dominik Rigasz

Úvod

Na prednáške si predstavíme polynómy s celočíselnými koeficientami, a budeme skúmať ich vlastnosti – konkrétne práca s celočíselnými polynómami a deliteľnosťami/kongruenciami, racionálne korene, a pozrieme sa na to, ako sa výsledky, ktoré poznáme z celých čísel dajú zovšeobecniť aj na celočíselné polynómy.

Definícia 1. Polynóm P stupňa n je algebraický výraz tvaru

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

kde x je premenná, a čísla c_i nazývame koeficient. Ak sú všetky koeficienty celé čísla, hovoríme o celočíselnom polynóme.

Navyše, c_n nazývame vedúci koeficient, $c_n x^n$ je vedúci člen, c_0 je absolútny člen. Množinu všetkých celočíselných polynómov značíme $\mathbb{Z}[X]$. Povieme, že polynóm je mnohocký, pokiaľ vedúci koeficient je rovný 1.

Niektoré vlastnosti

Jeden z najdôležitejších výsledkov pri celočíselných polynómoch, ktorý treba vždy držať na pamäti je nasledovné:

Veta 1 (periodicita). *Nech $P \in \mathbb{Z}[X]$. Potom pre ľubovoľné $a, b \in \mathbb{Z}$ platí $a - b \mid P(a) - P(b)$.*

Dôkaz. Pre ľubovoľné k platí $a - b \mid (a - b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1}) = a^k - b^k$, a teda $a - b \mid c_n(a^n - b^n) + c_{n-1}(a^{n-1} - b^{n-1}) + \cdots + c_1(a - b) = P(a) - P(b)$. $\square$

Dôležitý dôsledok tejto vety je nasledovné: Ak $a \equiv b \pmod{m}$, tak aj $P(a) \equiv P(b) \pmod{m}$. Inými slovami, každý polynóm sa modulo m eventuálne zacyklí (preto "periodicita").

Veta 2 (racionálny koreň). *Nech $P(x) = \sum c_i x^i$ je polynóm stupňa n . Nech $\frac{p}{q}$ je jeho koreň, kde p, q sú nesúdeliteľné celé čísla, a $q > 0$ (teda platí $P(p/q) = 0$). Potom $p \mid c_0$ a $q \mid c_n$.*

Dôkaz. Vieme, že $P(p/q) = c_n(p/q)^n + \cdots + c_1(p/q) + c_0 = 0$. Po vynásobení q^n dostávame $c_n p^n + c_{n-1} p^{n-1} q + \cdots + c_1 p q^{n-1} + c_0 q^n = 0$. Všimnime si, že každý člen okrem prvého obsahuje q , a teda musí platiť $q \mid c_n p^n$, vďaka nesúdeliteľnosti $q \mid c_n$. Podobne, každý člen okrem posledného obsahuje p , a teda musí platiť $p \mid c_0 q^n$, vďaka nesúdeliteľnosti $p \mid c_0$. $\square$

Veta o racionálnom koreni nám umožňuje (rýchlo) zistiť, či daný konkrétny celočíselný polynóm má nejaké racionálne korene. Má aj veľa "úlohových" dôsledkov, napríklad: Ak monický polynóm $P \in \mathbb{Z}[X]$ má racionálny koreň r , potom $r \in \mathbb{Z}$.

V celých číslach často uvažujeme množinu prvočíselných deliteľov daného čísla. Podobne pri celočíselných polynómoch môžeme uvažovať množinu všetkých prvočísel, ktoré delia nejakú jeho hodnotu:

Veta 3 (Schur). *Nech $P \in \mathbb{Z}[X]$. Potom existuje nekonečne veľa prvočísel p takých, že $p \mid P(n)$ pre nejaké $n \in \mathbb{Z}$.*

Idea je podobná ako Euklidov dôkaz nekonečnosti prvočísel. Chceli by sme nejak kontrolovať zvyšok čísla $P(n)$ po delení n . Páčilo by sa nám, keby tento zvyšok bol 1, lebo potom ak by $N = p_1 p_2 \cdots p_\ell$ bol súčin všetkých prvočísel deliacich nejakú hodnotu P , tak potom $P(N) \equiv 1 \pmod{N}$, a teda musíme mať nové prvočíslo. Z periodicity však vieme, že zvyšok $P(n)$ po delení n je vlastne iba $P(0)$.

Dôkaz. Ak $P(0) = 0$, potom $n \mid P(n)$, a teda sme hotoví. Nech $P(0) \neq 0$. Teraz definujeme $Q(n) = \frac{P(nP(0))}{P(0)}$. Všimnime si, že $Q \in \mathbb{Z}[X]$, a navyše $Q(0) = 1$. Nakoľko P je nekonštantný tak aj Q je nekonštantný, a teda pre všetky dost veľké n platí $|Q(n)| > 1$. Nech $p_1, \dots, p_\ell$ je súčin všetkých prvočísel, ktoré delia nejakú hodnotu Q , a nech N je ich súčin. Potom $Q(N) \equiv Q(0) = 1 \pmod{N}$, a navyše $|Q(N)| > 1$, teda máme nového prvočíselného deliteľa. Preto Q má nekonečne veľa prvočíselných deliteľov, a teda aj P . $\square$

Ak máme v úlohe celočíselný polynóm, je dobrá šanca, že použijeme deliteľnosti/prvočísla/... Avšak, úlohy s celočíselnými polynómami sú stále úlohy s polynómami, a teda sa zídu aj techniky z algebry:

1. Skúmanie stupňa a rastu polynómu, prípadne počet koreňov, veľkostné odhady.
2. Faktorizácie, delenie polynómov.
3. Vietove vzťahy.

Príklady

Cvičenie 1. Nech P je polynóm. Ak pre každé celé číslo n je $P(n)$ tiež celé číslo, musí byť polynóm P celočíselný? **Hinty:**1

Cvičenie 2. Existuje polynóm $P \in \mathbb{Z}[X]$ taký, že $P(n)$ je prvočíslo pre všetky dost veľké $n \in \mathbb{N}$? **Hinty:**2

Cvičenie 3 (PraSe 41). Nech $P \in \mathbb{Z}[X]$, a nech a, b, c sú celé čísla také, že $P(a) = 1$, $P(b) = 2$, $P(c) = 3$. Ukážte, že b leží medzi číslami a, c . **Hinty:**3

Cvičenie 4. Krivoš má svoj obľúbený polynóm $P \in \mathbb{Z}[X]$, ktorý má aspoň jeden celočíselný koreň. Krivoš povie Iľovi kladné celé číslo k , a Iľo má medzi číslami $P(0), P(1), \dots, P(k-1)$ nájsť násobok k . Podarí sa mu to vždy? **Hinty:**4

Cvičenie 5 (USAMO 1974). Nech $P \in \mathbb{Z}[X]$, a nech a, b, c sú celé čísla také, že $P(a) = b$, $P(b) = c$, $P(c) = a$. Ukážte, že a, b, c nemôžu byť všetky rôzne. **Hinty:**5

Cvičenie 6 (ŠKMO-A 2023/24). Určte počet celočíselných kvadratických polynómov $P(x)$ takých, že pre všetky reálne x platí

$$x^2 + 2x - 2023 < P(x) < 2x^2.$$

Hinty:6

Cvičenie 7 (PraSe 44). Nech $P \in \mathbb{Z}[X]$ je taký, že $P(P(n))$ dáva zvyšok $n - 1$ po delení n pre všetky $n \in \mathbb{N}$. Ukážte, že P nemá celočíselný koreň. **Hinty:**7

Cvičenie 8 (PraSe 41). Nájdite všetky $P \in \mathbb{Z}[X]$ také, že pre všetky $n \in \mathbb{N}$ platí $P(n) \mid n! + 2$. **Hinty:**8

Cvičenie 9 (folklór). Lukáš a Skaloš hrajú hru. Skaloš si najprv vymyslí polynóm $P(x) = a_n x^n + \dots + a_1 x + a_0$, kde a_i je kladné celé číslo pre všetky i . Lukáš sa následne pýta Skaloša na hodnoty $P(x)$, pre ľubovoľné reálne x , a Skaloš mu ich povie. Najmenej koľko otázok potrebuje Lukáš, aby vedel s istotou Skalošov polynóm P ? **Hinty:**9

Cvičenie 10. Nájdite všetky $P \in \mathbb{Z}[X]$ také, že $\text{NSD}(P(n), P(2^n)) = 1$ pre všetky $n \in \mathbb{N}$. **Hinty:**10

Cvičenie 11. Nájdite všetky $P \in \mathbb{Z}[X]$, pre ktoré existuje nekonečná aritmetická postupnosť taká, že žiaden jej člen sa nedá vyjadriť ako $P(x)$ pre nejaké $x \in \mathbb{Z}$. **Hinty:**11

Cvičenie 12 (Israel TST). Nájdite všetky polynómy $P \in \mathbb{Z}[X]$ také, že pre všetky $x \in \mathbb{Z}$ a všetky $n \in \mathbb{N}$ platí

$$n \mid P^n(x) - x.$$

Hinty:12

Cvičenie 13. Nájdite všetky $P \in \mathbb{Z}[X]$ také, že čísla $P(0), P(1), \dots, P(p-1)$ majú rôzne zvyšky modulo p pre všetky dost veľké prvočísla. **Hinty:**13

Cvičenie 14 (Gauss). Polynóm $P \in \mathbb{Z}[X]$ nazveme primitívny, pokiaľ najväčší spoločný deliteľ všetkých jeho koeficientov je 1. Ukážte, že súčin dvoch primitívnych polynómov je tiež primitívny. **Hinty:**14

Cvičenie 15 (IMO 2006/5). Nech $P \in \mathbb{Z}[X]$, kde $\deg P \geq 2$, a nech $k \in \mathbb{N}$. Uvažujme polynóm $Q(x) = P(P(\dots P(x) \dots))$, kde sme zložili P so sebou k -krát. Ukážte, že existuje najviac n celých čísel t takých, že $Q(t) = t$. **Hinty:**15

Cvičenie 16 (ELMO 2019/1). Nech $P \in \mathbb{Z}[X]$, $P(0) = 1$, a nech $c > 1$ je celé číslo. Definujme postupnosť $\{x_n\}$ ako $x_0 = 0$ a $x_{i+1} = P(x_i)$ pre všetky $i \geq 0$. Ukážte, že existuje nekonečne veľa kladných celých čísel n takých, že $\text{NSD}(x_n, n + c) = 1$. **Hinty:**16

Hinty

1. Nemusí.
2. Nie. Vedeli by sme nejako zaručiť $f(\text{niečo}) \mid f(\text{niečo iné})$?
3. Periodicita.
4. Periodicita.
5. Periodicita a odhady.
6. Veľkosť. Obrázok vždy pomôže.
7. Koľko je $P(P(0))$? Periodicita spam.
8. Čo ak by platilo $|P(n)| < N$ a $P(n) \mid P(N)$? Viete pre každé n nájsť také N ?
9. Stačia mu 2 otázky. Prvou hodnotou chce Lukáš nejako zistiť veľkosť koeficientov (približne), tak aby ich z druhej hodnoty vedel určite vyčítať. Ako? Spomeňte si na dekadický zápis.
10. Nech $n = 2^t$. Ak $p \mid P(n)$, potom $p \mid P(n + kp)$. Preto $p \nmid P(2^{n+kp})$ pre všetky k . Zároveň $p \mid P(2^t)$.

11. $P(x), P(x+1), \dots, P(x+d-1)$ musia pokryť všetky zvyšky modulo d , teda všetky musia mať rôzne zvyšky modulo d . Zvoľme x a d také, že $d = P(x+1) - P(x) \geq 2$.
12. Nech $P(x) - x$ je nekonštantný polynóm. Potom existuje nekonečne veľa prvočísel $p \mid P(n) - n$ pre nejaké $n \in \mathbb{N}$. Ak sa pozeráme na P ako funkciu v $\mathbb{Z}_p$, ako musí vyzerat?
13. Čo možno povedať o prvočíselných deliteľoch polynómu $P(x+1) - P(x)$?
14. Nech $(\sum_{i=0}^m a_i x^i)(\sum_{i=0}^n b_i x^i) = \sum_{i=0}^{m+n} c_i x^i$, a nech $p \mid c_i$ pre všetky i . Nech j je najväčší index pre ktorý $p \nmid a_j$, a nech k je najväčší index pre ktorý $p \nmid b_k$. Potom $p \nmid c_{j+k}$.
15. Nech a, b sú dva rôzne pevné body Q . Potom z periodicity $|a - b| = |P(a) - P(b)|$. Preto pre všetky pevné body a, b platí $P(a) + ra = P(b) + rb$, kde $r \in \{\pm 1\}$. Fixnime teraz dva pevné body a, b polynómu Q tak aby $P(a) + ra = P(b) + rb = C$, a uvažujme korene $P(x) + rx - C$.
16. Chceme vedieť kontrolovať NSD. Ktoré čísla majú málo deliteľov? Zvoľte $n + c$ za také čísla. Potom periodicita.

Literatúra a zdroje

1. Modern Olympiad Number Theory (MONT), Aditya Khurmi, 2020.
2. <https://skmo.sk/dokumenty.php>.
3. PraSe archív.