7 Polynomy interpolační i symetrické

Řešení
verze ze dne 31. března 2025.

Cíle cvičení: Zjistíme, že schopnost řešení soustav kongruencí, kterou jsme dříve nabyli pro celá čísla, je dobře aplikovatelná i pro polynomy nad tělesy. Krom toho se blíže seznámíme se symetrickými polynomy a zjistíme, jak pomocí Viètových vzorců pracovat s koeficienty polynomů, aniž bychom přímo našli jejich kořeny.

Úlohy, které bychom určitě měli umět řešit:

Úloha 7.1. Najděte polynom f nejmenšího možného stupně splňující

(a) $f \in \mathbb{Z}_5[x]$, $f \equiv x+1 \pmod{x^2+1}$ a $f \equiv x \pmod{x^3+1}$,

(b) $f \in \mathbb{Q}[x]$, $f(0)=1$, $f(1)=0$, $f(2)=2$,

(c) $f \in \big(\mathbb{Z}_2[\alpha]/(\alpha^2+\alpha+1)\big)[x]$, $f \equiv x \pmod{x^2+\alpha}$, $f \equiv \alpha+1 \pmod{x^2+x}$.

Řešení. (a) Budeme postupovat obdobně jako v 2. sérii při řešení soustav lineárních kongruencí na $\mathbb{Z}$. Obecné řešení druhé kongruence $f \equiv x \pmod{x^3+1}$ tvaru $x+s(x^3+1)$ pro $s \in \mathbb{Z}_5[x]$ dosadíme do první kongruence a ekvivalentně (tentokrát třeba bez explicitního využití Eukleidova algoritmu) upravujeme

$$f \equiv x+s(x^3+1) \equiv x+s(-x+1) \equiv x+1 \pmod{x^2+1},$$

poté odečteme od obou stran kongruence x a dostaneme $s(-x+1) \equiv 1 \pmod{x^2+1}$. Protože $-(1+x)(1-x) = x^2-1 \equiv -2 \pmod{x^2+1}$, vidíme, že

$$-2s \equiv s(x^2-1) \equiv s(-x+1)(-x-1) \equiv (-x-1) \pmod{x^2+1},$$

proto $s \equiv 2(-x-1) \equiv (3x+3) \pmod{x^2+1}$. Jako řešení nejmenšího stupně dostáváme tudíž polynom $f = x+s(x^3+1) = x+(3x+3)(x^3+1) = 3x^4+3x^3+4x+3$.

(b) Můžeme buď úlohu převést na kongruence

$$f \equiv 1 \pmod{x}, \quad f \equiv 0 \pmod{x-1}, \quad f \equiv 2 \pmod{x-2}$$

a pak budeme postupovat obdobně jako v (a), nebo můžeme najít řešení pomocí Lagrangeova interpolačního polynomu (viz důsledek 9.2 ve skriptech):

$$f = 1 \cdot \frac{(x-1)(x-2)}{(0-1)(0-2)} + 0 \cdot \frac{(x-0)(x-2)}{(1-0)(1-2)} + 2 \cdot \frac{(x-0)(x-1)}{(2-0)(2-1)} = \frac{1}{2}(3x^2-5x+2).$$

(c) Přítomností čtyřprvkového tělesa (které zde budeme značit T) se nenecháme vyvést z míry a z první kongruence vyjádříme $f = x+s(x^2+\alpha)$, kde $s \in T[x]$. Dosazení do druhé kongruence způsobí

$$x+s(x^2+\alpha) \equiv \alpha+1 \pmod{x^2+x}$$

neboli

$$s(x+\alpha) \equiv x+\alpha+1 \pmod{x^2+x}$$

(v závorce u s jsme nahradili x^2 za jemu kongruentní x). Nyní můžeme Eukleidovým algoritmem najít inverzní prvek k $x+\alpha$ modulo x^2+x, nebo můžeme díky rozkladu $x^2+x = x(x+1)$ a Čínské zbytkové větě ekvivalentně řešit dvě kongruence

$$\begin{aligned} s(x+\alpha) \equiv s\alpha \equiv \alpha+1 \pmod{x} \quad &\Rightarrow \quad s \equiv (\alpha+1)\cdot\alpha^{-1} = \alpha \pmod{x}, \\ s(x+\alpha) \equiv s(\alpha+1) \equiv \alpha \pmod{x+1} \quad &\Rightarrow \quad s \equiv \alpha\cdot(\alpha+1)^{-1} = \alpha+1 \pmod{x+1}, \end{aligned}$$

odkud snadno vidíme $s \equiv x + \alpha \pmod{x^2 + x}$. Poznamenejme, že takto jsme mohli postupovat díky tomu, že $\mathrm{NSD}_{T[x]}(x, x+1) = 1$. (Trikově jsme se celému tomuto výpočtu mohli vyhnout, pokud bychom si všimli, že $x + \alpha + 1 \equiv x^2 + \alpha + 1 = (x + \alpha)^2 \pmod{x^2 + x}$.) Hledaný polynom nejmenšího stupně tedy je $x + (x + \alpha)(x^2 + \alpha) = x^3 + \alpha x^2 + (\alpha + 1)x + (\alpha + 1)$.

Vsuvka (Gaussův algoritmus aneb kterak vyjádření pomocí elementárních symetrických polynomů nalézti)**.** Nechť R je obor. Máme-li symetrický polynom $f_0 \in R[x_1, \ldots, x_n]$, jehož nejvyšším termem (v lexikografickém uspořádání) je $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ (nezbytně $k_1 \geq k_2 \geq \cdots \geq k_n$) a koeficient u onoho členu je c, pak přejdeme k polynomu

$$f_1 = f_0 - c s_1^{k_1 - k_2} s_2^{k_2 - k_3} \cdots s_{n-1}^{k_{n-1} - k_n} s_n^{k_n},$$

kde s_i je i-tý elementární symetrický polynom v $x_1, \ldots, x_n$. Dále totéž provedeme s polynomem f_1 atd., dokud ještě je co odčítat. Hledané vyjádření je součtem toho, co jsme postupně poodčítali.

Úloha 7.2. Nalezněte vyjádření daných polynomů z $\mathbb{C}[x, y, z]$ pomocí elementárních symetrických polynomů:

(a) $x^2yz + xy^2z + xyz^2$,

(b) $x^3(y + z) + y^3(x + z) + z^3(x + y)$.

Řešení. (a) Lexikograficky nejvyšší člen je x^2yz, odečítáme tedy $s_1^{2-1} s_2^{1-1} s_3^1 = s_1 s_3$ a je okamžitě vidět, že onen zadaný polynom už je ono $s_1 s_3$.

(b) Roznásobíme závorky; lexikograficky nejvyšší člen je x^3y, odečítáme tedy

$$s_1^{3-1} s_2^{1-0} s_3^0 = s_1^2 s_2 = x^3y + x^3z + 2x^2y^2 + 5x^2yz + 2x^2z^2 + xy^3 + 5xy^2z + 5xyz^2 + xz^3 + y^3z + 2y^2z^2 + yz^3,$$

takže nyní máme

$$f_1 = -2(x^2y^2 + y^2z^2 + z^2x^2) - 5(x^2yz + y^2zx + z^2xy).$$

lexikograficky nejvyšší člen je x^2y^2, odečítáme tedy

$$-2s_1^{2-2} s_2^{2-0} s_3^0 = -2s_2^2 = -2(x^2y^2 + y^2z^2 + z^2x^2) - 4(x^2yz + y^2zx + z^2xy),$$

takže

$$f_2 = -(x^2yz + y^2zx + z^2xy).$$

Jako v části (a) nahlédneme, že toto je $-s_1 s_3$, takže hledané vyjádření je $s_1^2 s_2 - 2s_2^2 - s_1 s_3$.

Pro poučení čtenářů zde ještě uvedeme v podstatě tentýž postup, ale zapsaný pomocí symetrických sum $\sum_{\mathrm{sym}}$, což řešení typicky zpřehlední; význam tohoto symbolu bude takový, že bude značit součet všech výrazů získatelných permutací neznámých, tedy např. $\sum_{\mathrm{sym}} x^2y = x^2y + y^2x + y^2z + z^2y + z^2x + x^2z$.

Zadaný symetrický polynom tedy je v tomto značení $\sum_{\mathrm{sym}} x^3y$. Odečíst od něj musíme polynom $s_1^2 s_2$, který je roven

$$\begin{aligned} s_1^2 s_2 = \big(\sum_{\mathrm{sym}} x\big)^2 \big(\sum_{\mathrm{sym}} xy\big) = \big(\sum_{\mathrm{sym}} x^2 + 2\sum_{\mathrm{sym}} xy\big)\big(\sum_{\mathrm{sym}} xy\big) = \big(\sum_{\mathrm{sym}} x^2\big)\big(\sum_{\mathrm{sym}} xy\big) + 2\big(\sum_{\mathrm{sym}} xy\big)^2 = \\ = \big(\sum_{\mathrm{sym}} x^3y + \sum_{\mathrm{sym}} x^2yz\big) + 2\big(\sum_{\mathrm{sym}} x^2y^2 + 2\sum_{\mathrm{sym}} x^2yz\big) = \sum_{\mathrm{sym}} x^3y + 2\sum_{\mathrm{sym}} x^2y^2 + 5\sum_{\mathrm{sym}} x^2yz. \end{aligned}$$

Z části (a) víme, že $\sum_{\mathrm{sym}} x^2yz = s_1 s_3$. Zbývá spočítat, že

$$\sum_{\mathrm{sym}} x^2y^2 = \big(\sum_{\mathrm{sym}} xy\big)^2 - 2\sum_{\mathrm{sym}} x^2yz = s_2^2 - 2s_1 s_3,$$

takže

$$f = s_1^2 s_2 - \big(2\sum_{\mathrm{sym}} x^2y^2 + 5\sum_{\mathrm{sym}} x^2yz\big) = s_1^2 s_2 - (2s_2^2 - 4s_1 s_3 + 5s_1 s_3) = s_1^2 s_2 - 2s_2^2 - s_1 s_3.$$

Úloha 7.3. Označme a, b, c (komplexní) kořeny polynomu $x^3+3x^2+4x-11$. Nechť $f = x^3+rx^2+sx+t \in \mathbb{C}[x]$ je polynom s kořeny $a+b$, $b+c$, $c+a$.

(a) Nahlédněte, že ve skutečnosti $f \in \mathbb{R}[x]$ (dokonce $f \in \mathbb{Z}[x]$),

(b) určete r,

(c) určete t.

Řešení. (a) Není těžké nahlédnout, že permutace a, b, c vede na permutaci $a+b$, $b+c$, $c+a$, takže koeficienty f, které jsou dle Viètových vztahů symetrické polynomy v kořenech f, jsou rovněž symetrické polynomy v a, b, c, tím pádem vyjádřitelné pomocí koeficientů původního polynomu, tedy reálné.

Protože koeficienty f jsou (jakožto polynomy v a, b, c) dokonce prvky $\mathbb{Z}[a,b,c]$, podle základní věty o symetrických polynomech (věta 11.2) je půjde vyjádřit jako prvky $\mathbb{Z}[s_1,s_2,s_3]$ (jinými slovy, v Gaussově algoritmu se „nikde nedělí"). Jelikož jsou hodnoty s_1, s_2, s_3 celá čísla, budou tedy nutně i koeficienty f celá čísla.

(b) Koeficient r je

$$r = -\big((a+b)+(b+c)+(c+a)\big) = -2(a+b+c) = -2\cdot(-3) = 6.$$

(c) Zde platí

$$t = -(a+b)(b+c)(c+a) = -(s_1s_2-s_3) = -\big((-3)\cdot 4-11\big) = 23,$$

kde s_1, s_2, s_3 jsou elementární symetrické polynomy v a, b, c.

A kdyby toho bylo snad málo, máme na přidání:

Úloha 7.4. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně menšího než 3 splňující

$$f \equiv x+1 \pmod{x^2+1}, \qquad f(0) = 3.$$

Řešení. Postupujeme jako v 7.1. První podmínku vyjádříme ve tvaru $f = (x+1)+s(x^2+1)$ pro $s \in \mathbb{Q}[x]$ tu dosadíme do druhé podmínky vyjádřené ve formě kongruence $f \equiv 3 \pmod{x}$:

$$f \equiv (x+1)+s(x^2+1) \equiv 1+s \equiv 3 \pmod{x},$$

tedy $s \equiv 2 \pmod{x}$ a jediné řešení stupně menšího než 3 je $f = (x+1)+2(x^2+1) = 3+x+2x^2$.

Úloha 7.5. Zdůvodněte, proč jsou následující (reálné) polynomy symetrické:

(a) $\prod_{1\le i<j\le n}(x_i-x_j)^2 \in \mathbb{R}[x_1,\dots,x_n]$,

(b) $(x_1+x_2-x_3-x_4)(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4)$.

Řešení. (a) Uvedený součin druhých mocnin můžeme přepsat na $(-1)^{\binom{n}{2}}\prod_{1\le i\ne j\le n}(x_i-x_j)$, odkud už je symetričnost patrná – při permutování neznámých jen permutujeme také všechny uspořádané dvojice neznámých, neboli jen měníme pořadí činitelů v součinu.

(b) Není těžké si rozmyslet, že na to, aby byl polynom symetrický, stačí, aby se neměnil při *transpozicích* proměnných (jelikož každá permutace je složením transpozic). Znaménka v závorkách můžeme chápat jako (všechny tři) možnosti, jak rozdělit čtyři prvky na dvě skupiny po dvou; proto kdykoliv prohodíme dvě proměnné, tak ve výsledku prohodíme ty dvě závorky, ve kterých mají ony proměnné různá znaménka, a ta, ve které mají znaménko stejné, se nezmění.

Úloha 7.6. Najděte izomorfismus mezi okruhy $\mathbb{Z}_5[\alpha]/(\alpha^4-1)$ a $(\mathbb{Z}_5^4,+,-,\cdot,\mathbf{0},\mathbf{1})$ s operacemi definovanými po složkách a $\mathbf{0}=(0,0,0,0)$, $\mathbf{1}=(1,1,1,1)$.

Řešení. Nejprve si uvědomíme, že polynom $x^4 - 1$ má nad $\mathbb{Z}_5$ čtyři kořeny 1, 2, 3, 4, tj. je součinem $\prod_{a\in\mathbb{Z}_5^*}(x-a)$. Z Čínské věty o zbytcích pro polynomy plyne, že zobrazení

$$\rho(f) = (f(1), f(2), f(3), f(4))$$

je bijekce množin $\mathbb{Z}_5[\alpha]/(\alpha^4-1)$ a $\mathbb{Z}_5^4$. Zbývá si rozmyslet, že se dokonce jedná o okruhový izomorfismus, tedy že platí $\rho(0) = (0,0,0,0)$, $\rho(1) = (1,1,1,1)$ a pro všechna $a, b \in \mathbb{Z}_5[\alpha]/(\alpha^4-1)$

$$\rho(a \pm b) = (a(1) \pm b(1), a(2) \pm b(2), a(3) \pm b(3), a(4) \pm b(4)) = \rho(a) \pm \rho(b)$$

$$\rho(a \cdot b) = (a(1) \cdot b(1), a(2) \cdot b(2), a(3) \cdot b(3), a(4) \cdot b(4)) = \rho(a) \cdot \rho(b).$$

Úloha 7.7. Buď p prvočíslo. S pomocí čínské věty o zbytcích pro polynomy ukažte, že polynom $\prod_{a\in\mathbb{Z}_p}(x-a) \in \mathbb{Z}_p[x]$ je roven polynomu $x^p - x$.

Řešení. Oba polynomy mají za kořen každé $a \in \mathbb{Z}_p$ tedy i jejich rozdíl má tuto vlastnost. Ten má ale stupeň $< n$, takový však dle čínské věty o zbytcích existuje jen jeden, čirou náhodou je to právě 0.

Úloha 7.8. Jsou-li α, β, γ (komplexní) kořeny polynomu $x^3 - 3x + 1$, nalezněte polynom, jehož kořeny budou

(a) α^2, β^2, γ^2,

(b) $\alpha + 1$, $\beta + 1$, $\gamma + 1$,

(c) $\frac{1}{\alpha}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$,

(d) $\frac{1}{\alpha+1}$, $\frac{1}{\beta+1}$, $\frac{1}{\gamma+1}$.

(Nápověda: Na (b), (c), (d) nejsou potřeba Viètovy vzorce.)

Řešení. (a) Máme $s_1 = 0$, $s_2 = -3$, $s_3 = -1$. Standardně vyjádříme $\alpha^2\beta^2\gamma^2 = s_3^2 = (-1)^2 = 1$, $\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 = s_2^2 - 2s_1s_3 = (-3)^2 = 9$, $\alpha^2 + \beta^2 + \gamma^2 = s_1^2 - 2s_2 = 6$. Hledaný polynom je tedy $x^3 - 6x^2 + 9x - 1$.

(b) Zde stačí v polynomu nahradit x za $x - 1$, čímž obdržíme $x^3 - 3x^2 + 3$.

(c) Není těžké nahlédnout, že přechod k převráceným hodnotám odpovídá obrácení pořadí koeficientů polynomu, hledaný polynom tedy je $x^3 - 3x^2 + 1$.

(d) Postupujeme stejně jako v (c), jen využijeme již známého výsledku z (b), tedy získáváme polynom $3x^3 - 3x + 1$.

Úloha 7.9. Nechť α, β jsou kořeny reálného polynomu $x^2 + 2x - 2$. Aniž byste určili hodnoty α a β, spočtěte hodnotu $\alpha^6 + \beta^6$. (Nápověda: Buď zatněte zuby a vyjádřete pomocí elementárních symetrických polynomů, nebo zkuste vymyslet rekurenci pro hodnoty $t_n = \alpha^n + \beta^n$.)

Řešení. Přímý algoritmický útok na symetrický polynom $\alpha^6 + \beta^6$ dá $s_1^6 - 6s_1^4s_2 + 9s_1^2s_2^2 - 2s_2^3$, kde $s_1 = \alpha + \beta = -2$ a $s_2 = \alpha\beta = -2$, takže výsledkem je 416. Alternativně si můžeme všimnout, že obecně platí

$$\alpha^n + \beta^n = (\alpha+\beta)(\alpha^{n-1} + \beta^{n-1}) - \alpha^{n-1}\beta - \beta^{n-1}\alpha = (\alpha+\beta)(\alpha^{n-1} + \beta^{n-1}) - \alpha\beta(\alpha^{n-2} + \beta^{n-2}).$$

Položíme-li tedy $t_n = \alpha^n + \beta^n$, máme rekurenci

$$t_n = -2t_{n-1} + 2t_{n-2}$$

s počátečními hodnotami $t_0 = 2$, $t_1 = -2$, pomocí čehož snadno spočteme $t_6 = 416$.

Úloha 7.10 (AIME 2001)**.** Nalezněte součet kořenů komplexního polynomu $x^{2001} + (\frac{1}{2} - x)^{2001}$.

Řešení. Trikové řešení spočívá v tom, že pro každý kořen r uvedeného polynomu je rovněž $\frac{1}{2}-r$ kořenem a $\frac{1}{4}$ jistě kořenem není, tedy se kořeny spárují do dvojic se součtem $\frac{1}{2}$. Jelikož má polynom stupeň 2000, má také (včetně násobnosti) 2000 komplexních kořenů, neboli 1000 dvojic se součtem $\frac{1}{2}$, takže celkový součet je 500.

Alternativně můžeme pomocí binomické věty rozvinout člen $(\frac{1}{2}-x)^{2001}$. Člen nejvyššího stupně, tj. $-x^{2001}$, se odečte, dalším členem bude $2001\cdot\frac{1}{2}\cdot x^{2000}$ a tím ještě následujícím (jehož koeficient udává součet kořenů) je $-\binom{2001}{2}\cdot\frac{1}{4}\cdot x^{1999}$. Součet kořenů tedy je

$$\frac{\binom{2001}{2}\cdot\frac{1}{4}}{2001\cdot\frac{1}{2}}=500.$$

⋆ **Úloha 7.11.** Pro všechna $x,y,z\in\mathbb{R}$ dokažte

$$x^4+y^4+z^4+3x^2y^2+3x^2z^2+3y^2z^2\geq 2x^3y+2x^3z+2xy^3+2xz^3+2y^3z+2yz^3$$

a rozhodněte, kdy nastává rovnost.

Řešení. Všechny členy převedeme na levou stranu, čímž dostaneme nerovnost tvaru $f\geq 0$, kde $f\in\mathbb{R}[x,y,z]$. Nyní rozložíme f na elementární symetrické polynomy a zjistíme

$$f=s_1^4-6s_1^2s_2+9s_2^2=(s_1^2-3s_2)^2.$$

Vidíme, že vskutku $f\geq 0$ pro všechna $x,y,z\in\mathbb{R}$, přičemž rovnost nastává právě za situace $s_1^2=3s_2$. Po rozepsání tato podmínka dostane tvar

$$x^2+y^2+z^2=xy+yz+zx,$$

což lze upravit na

$$(x-y)^2+(y-z)^2+(z-x)^2=0.$$

Vidíme tedy, že rovnost nastane právě když $x=y=z$.