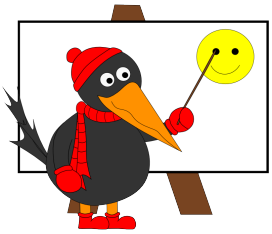
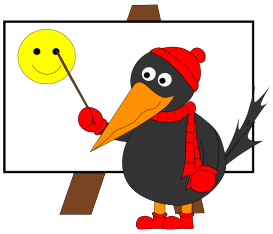


Pomocný text

POLYNOMY



Tato série bude o polynomech a to zejména o polynomech jedné proměnné (pokud nebude uvedeno explicitně, že jde o polynom více proměnných). Formálně je někdy polynom jedné proměnné chápán jako konečná posloupnost reálných čísel (sčítání a násobení polynomů pak definujeme jako operace na posloupnostech), lze jej ale brát i jako zobrazení p, které reálnému číslu x přiřazuje číslo

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

Číslo n nazýváme *stupněm polynomu*, čísla a_i koeficienty, každý z výrazů $a_i x^i$ je *členem*. Koeficient a_n nazýváme *vedoucím koeficientem*, člen $a_n x^n$ *vedoucím členem*. Definičním oborem je celá množina $\mathbb{R}$. Je-li stupeň polynomu lichý, je oborem hodnot opět celá množina $\mathbb{R}$, je-li sudý, je oborem hodnot množina $\langle a, \infty)$ pro nějaké reálné a. Pokud je a_n rovno jedné, nazveme polynom *normovaným* neboli *monickým*.

Pokud jsou p a q polynomy a existuje polynom r takový, že $p = q \cdot r$, pak řekneme, že polynom q dělí polynom p. Pokud takový polynom neexistuje, lze najít právě jednu dvojici polynomů r, s takovou, že s má menší stupeň než q a $p = rq + s$. V takovém případě polynom r nazveme *částečným podílem* a s *zbytkem po dělení* polynomu p polynomem q.

Euklidův algoritmus a Bezoutova rovnost

Podobně jako u přirozených čísel můžme definovat největšího společného dělitele polynomů p a q jako polynom, který dělí p i q a je dělitelný všemi ostatními polynomy s touto vlastností.

Tento polynom lze najít algoritmem podobným tomu pro reálná čísla: vyjdeme z polynomů p, q a v každém kroku polynom s větším stupněm nahradíme jeho zbytkem po dělení s menším stupněm. Poslední nenulový polynom d, který tímto algoritmem dostaneme, je největším společným dělitelem polynomů p a q. Pokud budeme v každém kroku psát i částečné podíly, jsme schopni vyjádřit d ve tvaru $f \cdot p + g \cdot q$, kde f a g jsou polynomy. Například pro polynomy $x^4+x^3-5x^2-3x+6$ a x^4-5x^2+4 provedeme následující dělení:

$$\begin{aligned} x^4+x^3-5x^2-3x+6 &= 1\cdot(x^4-5x^2+4)+(x^3-3x+2)\\ x^4-5x^2+4 &= x\cdot(x^3-3x+2)+(-2x^2-2x+4)\\ x^3-3x+2 &= \left(-\frac{1}{2}x+\frac{1}{2}\right)(-2x^2-2x+4)+0 \end{aligned}$$

Největším společným dělitelem[1] je proto polynom $-2x^2-2x+4$, který lze vyjádřit jako

$$\begin{aligned} &(x^4-5x^2+4)-x\cdot(x^3-3x+2)=\\ &\quad=(x^4-5x^2+4)-x\cdot[(x^4+x^3-5x^2-3x+6)-(x^4-5x^2+4)]=\\ &\quad=(1+x)(x^4-5x^2+4)-x(x^4+x^3-5x^2-3x+6) \end{aligned}$$

Faktorizace polynomu

Pokud existují nekonstantní polynomy q, r takové, že jejich koeficienty leží v množině M a $p = q \cdot r$, nazveme polynom p *reducibilním nad* M, v opačném případě *iredcibilním nad* M. Není-li uvedeno, nad kterou množinou má být reducibilní, uvažujeme reducibilitu nad $\mathbb{R}$. Polynomy obsahující pouze absolutní člen se nazývají konstantní.

Věta 1. *Každý polynom stupně alespoň 3 je reducibilní nad* $\mathbb{R}$.

Toto tvrzení je ekvivalentní se základní větou algebry, kterou zmíníme v textu o komplexních číslech. Lze jej formulovat také tak, že jediné ireducibilní polynomy nad $\mathbb{R}$ jsou konstantní, lineární a kvadratické se záporným diskriminantem.

Je-li polynom p dělitelný polynomem $x - c$, nazveme $x - c$ kořenovým činitelem p a číslo c kořenem p. Kořen polynomu lze definovat také jako číslo, které daný polynom zobrazuje na nulu.

Hledat kořeny polynomů stupňů 1 a 2 znamená řešit lineární resp. kvadratickou rovnici, pro stupně 3 a 4 musíme použít Cardanovy vzorce (ty jsou bohužel nad rámec tohoto textu), pro stupeň 5 a více algoritmus neexistuje. Ukážeme si ale několik technik, jak hledat kořeny polynomu.

Odštěpení racionálních kořenů

Jde o techniku využitelnou pouze u polynomů s celočíselnými koeficienty. Pomocí následujícího tvrzení najdeme kandidáty na racionální kořeny.

Věta 2. *Je-li racionální číslo* $\frac{r}{s}$ *kořenem polynomu* $p(x) = a_n x^n + \cdots + a_0$ *s celočíselnými koeficienty, pak* $r \mid a_0$ *a* $s \mid a_n$.

[1] Podobně jako u celých čísel je největší společný dělitel určen jednoznačně až na znaménko, také u polynomů je určen jednoznačně, ovšem až na násobek libovolnou nenulovovou reálnou konstantou.

Takto máme pouze omezenou množinu čísel r i s, kandidátů na racionální kořeny je konečně mnoho. Abychom se vyhnuli ověřování všech, můžeme množinu zúžit následujícím tvrzením.

Věta 3. *Je-li racionální číslo $\frac{r}{s}$ kořenem polynomu $p(x) = a_n x^n + \cdots + a_0$ s celočíselnými koeficienty, pak pro každé přirozené číslo m platí $r - ms \mid p(m)$.*

Zejména tedy $r + s \mid p(-1)$ a $r - s \mid p(1)$.

Abychom si v následující ukázce usnadnili zápis dělení polynomů[2] použijeme speciální metodu pro dělení polynomem tvaru $x - c$: takzvané Hornerovo schéma. Jde o tabulku, v jejímž prvním řádku jsou koeficienty polynomu $a_n, \ldots, a_0$. Před druhý řádek zapíčeme číslo c. Pak do druhého řádku dopisujeme postupně čísla b_i pod a_i tak, že $b_n = a_n$ a pro $i < n$ $b_i = a_i + cb_{i+1}$. Jakmile doplníme celý řádek, jsou $b_n, \ldots, b_1$ koeficienty částečného podílu a b_0 zbytek po dělení (zbytek po dělení $x - c$ je roven funkční hodnotě v bodě c). Pokud vyjde b_0 nulové, můžeme výsledný podíl vzít za nový výchozí polynom a zkusit ho vydělit jiným polynomem tvaru $x - c$.

Příklad 1. *Najděte všechny racionální kořeny polynomu* $2x^6 + 5x^5 - 7x^4 - 18x^3 + 10x^2 + 16x - 8$.

Využitím věty 2 máme, že zlomek $\frac{r}{s}$ může být kořenem pouze pokud $r|8$ a $s|2$. Množina připustných zlomků po zkrácení je $\{\pm 1, \pm 2, \pm 4, \pm 8, \pm\frac{1}{2}\}$. Dle 3 navíc musí být $r+s|-6$ a $r-2s|96$, což nám zužuje množinu kandidátů na $\{1, -2, -4, \frac{1}{2}\}$. Nyní pomocí Hornerova schematu zkusíme tyto kořeny odštěpovat:

	2	5	-7	-18	10	16	-8
1	2	7	0	-18	-8	8	**0**
1	2	9	0	-9	-17	**-9**	
-2	2	3	-6	-6	4	**0**	
-2	2	-1	-4	2	**0**		
$\frac{1}{2}$	2	0	-4	**0**			

Jak je vidět, každého kandidáta je potřeba zkoušet několikrát, neboť může být násobným kořenem. U jedničky jsme to provedli, u dalších kořenů ne (z důvodů úspory místa). Polynom se nám podařilo rozložit na $(x-1)(x+2)^2(x-\frac{1}{2})(2x^2-4)$, dále jej již nad $\mathbb{Q}$ rozložit nelze.

Polynom s celočíselnými koeficienty nazveme *primitivním*, pokud neexistuje prvočíslo takové, že by dělilo všechny jeho koeficienty.

Věta 4 (Gaussovo lemma)**.** *Nechť f, g jsou primitivní polynomy. Pak $h = f \cdot g$ je také primitivní.*

Indukcí podle stupně polynomu h dokážeme, že pokud prvočíslo p dělí koeficienty h, dělí i koeficienty jednoho z polynomů f, g. Pokud je h konstantní, jsou f i g konstantní, tvrzení platí dle Základní věty aritmetiky.

[2]Běžný zápis je stejný jako u dělení reálných čísel – tedy dost prostorově náročný.

Předpokládejme, že věta platí pro polynomy stupně k, a dokažme ji pro polynom h stupně $k+1$. Důkaz provedeme obměnou. Vedoucí koeficient h je dělitelný p, proto p musí dělit vedoucí koeficient f nebo g (BÚNO předpokládejme první možnost, tedy že vedoucí člen f je roven tpx^r pro nějaká celá t, r). Číslo p pak dělí koeficienty $h - tpx^r g = (f - tpx^r)g$, který má stupeň k. Z indukčního předpokladu pak p dělí buď koeficienty g nebo $f - tpx^r$, a proto i f. Tím je indukční krok hotov.

Snadno nahlédneme, že každý polynom s racionálními koeficienty lze (až na znaménko) zapsat jednoznačně ve tvaru $r \cdot f$, kde r je racionální číslo a f primitivní polynom.

Eisensteinovo kritérium

Věta 5. *Nechť $f = a_n x^n + \cdots + a_0$ je polynom s celočíselnými koeficienty a prvočíslo p má následující vlastnosti: $p \mid a_{n-1}$,$p \mid a_{n-2}$, $\ldots p \mid a_0$, dále $p^2 \nmid a_0$ a konečně $p \nmid a_n$. Pak f je ireducibilní nad $\mathbb{Q}$.*

Budeme dokazovat Eisensteinovo kritérium v trochu zesílené podobě: Pokud f je polynom s celočíselnými koeficienty a existuje prvočíslo p a index i takový, že $p \mid a_{i-1}$,$p \mid a_{i-1}$, $\ldots p \mid a_1$, $p \mid a_0$, $p^2 \nmid a_0$ a $p \nmid a_n$, pak stupeň polynomu s racionálními koeficienty, který dělí f, je alespoň t. Pak f je ireducibilní nad $\mathbb{Q}$.

Nejprve si uvědomíme, že tvrzení stačí dokázat pro primární polynomy f (jakýkoliv jiný polynom $\overline{f} = t \cdot f$ je reducibilní, pokud je f reducibilní). Pro spor předpokládejme, že $f = \overline{g} \cdot \overline{h}$, kde $\overline{g}, \overline{h}$ jsou polynomy s racionálními koeficienty. Tyto polynomy lze jistě zapsat ve tvaru $\overline{g} = \frac{1}{r} g$, $\overline{h} = \frac{1}{s} h$, kde g, h jsou primární polynomy a r, s racionální čísla. Náš předpoklad přepíšeme jako $rsf = g \cdot h$. Proto rsf musí být primární, takže $|rs| = 1$. Protože $f_0 = g_0 h_0$ je číslo dělitelné p v právě první mocnině, je právě jeden z koeficientů g_0, h_0 dělitelný p. BÚNO předpokládejme první možnost. Protože je $f_1 = g_0 h_1 + g_1 h_0$ i $g_0 h_1$ dělitelné p, musí platit $p \mid g_1 h_0$ a tudíž $p \mid g_1$. Takto pokračujeme dál, až zjistíme, že všechny koeficienty $g_0, g_1, \ldots, g_{i-1}$ jsou dělitelné p a protože je g primární, musí mít stupeň alespoň i.

Příklad 2. *Rozložte polynom $(x+1)^4 + 1$ nad $\mathbb{Q}$.*

Polynom rozepíšeme jako $x^4 + 4x^3 + 6x^2 + 4x + 2$. Vidíme, že prvočíslo 2 dělí všechny koeficienty krom prvního a 4 nedělí poslední, proto daný polynom nad $\mathbb{Q}$ dále rozložit nelze.

Odštěpení násobných kořenů

Derivací polynomu $p(x) = a_n x^n + \cdots + a_0$ nazveme polynom $P'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$. Tuto definici lze přijmout jako fakt bez toho, že bychom věděli cokoliv o derivacích obecně. Zajímavou vlastností derivací je to, že pokud má p kořen k násobnosti $t > 1$, má p' kořen k násobnosti $t - 1$. Proto polynom d, který spočítáme jako největší společný dělitel polynomů p a p', má za kořeny právě ta čísla, která jsou násobnými kořeny p. Polynom $\frac{p}{d}$ má stejné kořeny jako p, ale jednonásobné.

Polynomy a teorie čísel

V mnoha úlohách, v nichž vystupují polynomy s celočíselnými koeficienty, využijeme poznatky z teorie čísel. Asi nejhojněji využívaným tvrzením je následují věta:

Věta 6. *Nechť p je polynom s celočíselnými koeficienty. Pak pro libovolná dvě celá čísla j, k platí*

$$j - k \mid p(j) - p(k).$$

Důkaz této věty není těžký, stačí si uvědomit, že

$$\begin{aligned} p(j) - p(k) &= a_1(j-k) + a_2(j^2 - k^2) + \cdots + a_n(j^n - x^n) = \\ &= (j-k)[a_1 + a_2(j+k) + \cdots + a_n(j^{n-1} + kj^{n-2} + \cdots + k^{n-1})], \end{aligned}$$

odtud z celočíselnosti koeficientů ihned plyne dokazované tvrzení.

Příklad 3. *Je dán polynom P stupně alespoň 1 s celočíselnými koeficienty. Dokažte, že posloupnost $|P(1)|, |P(2)|, |P(3)|, \ldots$ obsahuje nekonečně mnoho složených čísel.*

Vezměme k takové, že $P(k) \notin \{-1, 0, 1\}$ (protože jde o nekonstantní polynom, nevyhoví této podmínce pouze konečně mnoho čísel). Položme $P(k) = y$. Z předešlé věty jsou všechny členy posloupnosti $P(k)$, $P(k+y)$, $P(k+2y)$ dělitelné y. Protože je P nekonstantní, obsahuje tato posloupnost i jiné násobky y než $0, y, -y$ a ta musí být složená.

Příklad 4. *Pro polynom P platí $P(4) = -1$, $P(6) = 1$. Najděte všechny racionální kořeny tohoto polynomu víte-li, že nějaké má.*

Uvažme polynom $Q(x) = P(x+4)$. Pro něj platí $Q(0) = -1$, aby byl zlomek $\frac{r}{s}$ kořenem polynomu, muselo by být podle věty 3 $r \mid -1$, tedy $r = \pm 1$. Analogicky pokud je $\frac{u}{v}$ kořenem polynomu $R(x) = P(x+6)$, je $u = \pm 1$. Proto je-li q racionálním kořenem P, jsou $q-4$ i $q-6$ zlomky tvaru $\frac{1}{k}$, kde k je celé. Protože se liší o 2 a každý je v absolutní hodnotě nejvýše 1, je jediná možnost $q - 4 = 1$, $q - 6 = -1$, $q = 5$. Víme, že 5 je kořen polynomu. Pro úplnost dodejme, že jakýkoliv polynom tvaru $(x-5)^{2n+1}$ vyhoví zadání. Na tomto příkladu jsme chtěli ukázat, že se v některých úlohách vyplácí polynom v proměnné x převést na polynom v proměnné $x-t$ (takové t se nazývá středem polynomu). Koeficienty takto upraveného polynomu lze napočítat Hornerovým schématem, z nějž je získáme jako zbytky po dělení $x - t$. Není těžké rozmyslet, proč to funguje.

Polynomy více proměnných

Polynom k proměnných lze brát jako polynom, v němž koeficienty nejsou reálná čísla, ale polynomy $k-1$ proměnných. Jde tedy o výrazy typu

$$p(x_1, \ldots, x_k) = a_1 x_1^{e_{1,1}} \cdots x_k^{e_{1,k}} + \cdots + a_n x_1^{e_{n,1}} \cdots x_k^{e_{n,k}}.$$

Symetrické polynomy

Symetrické polynomy jsou takové polynomy, které nezmění svou hodnotu záměnou proměnných. Každý symetrický polynom k proměnných lze získat sčítáním a násobením tzv. *elementárních symetrických polynomů* σ_1, σ_2, ..., kde σ_t je součet součinů všech možných t-tic proměnných, tj.

$$\begin{aligned}\sigma_1(x_1,\ldots,x_k) &= x_1 + x_2 + \cdots + x_k\\ \sigma_1(x_1,\ldots,x_k) &= x_1x_2 + x_1x_3 + \cdots + x_{k-1}x_k\\ &\cdots\\ \sigma_k(x_1,\ldots,x_k) &= x_1x_2\cdots x_k\end{aligned}$$

Při řešení rovnic, v nichž vystupují polynomy symetrické nebo symetrickým podobné, se často převod na symetrické polynomy využije.

Příklad 5. *Řešte soustavu rovnic*

$$\begin{aligned}x + y &= 3\\ x^5 + y^5 &= 33\end{aligned}$$

Hodnoty symetrických polynomů označíme $s = x + y$, $p = xy$. Pak

$$\begin{aligned}x^5 + y^5 =& s(s^4 - 5p(s^2 - p)))\\ 33 =& 3(81 - 5p(9 - p)))\\ 70 =& 5p(9 - p))\\ 14 =& p(9 - p).\end{aligned}$$

Odtud $p = 2$ nebo $p = 7$. V prvním případě $x = 1$, $y = 2$ nebo naopak, ve druhém případě $x, y = \frac{7\pm\sqrt{35}}{2}$.

Symetrické polynomy se vyskytují také ve známých Viètových vztazích. Pokud má polynom $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ kořeny $x_1, x_2, \ldots, x_n$, pak $a_{n-1} = -\sigma_1(x_1,\ldots,x_n)$, $a_{n-2} = \sigma_2(x_1,\ldots,x_n)$, obecně $a_{n-k} = (-1)^k\sigma_k(x_1,\ldots,x_n)$. Příklady na symetrické polynomy lze najít například v knize J. Herman, R. Kučera, J. Šimša: Metody řešení matematických úloh.