Počítačová algebra - 5. cvičení

24. dubna 2020

Problém 1. Ať $f, g \in \mathbb{Z}[x]$, $\deg f = n, \deg g = n-1$, takové, že maximální koeficienty f, g jsou a, b.
Dokažte, že koeficienty $f \operatorname{pmod} g$ jsou nejvýše $4ab^2$.

Řešení. Označme

$$f = \sum_{i=0}^{n} f_i x^i, \quad g = \sum_{i=0}^{n-1} g_i x^i$$

a

$$q_1 x + q_0 := f \operatorname{pdiv} g, \quad r(x) := f \operatorname{pmod} g,$$

tedy

$$g_{n-1}^2 f = (q_1 x + q_0) g + r(x), \quad r = \sum_{i=0}^{n-2} r_i x^i$$

Porovnejme nyní koeficient u x^n:

$$g_{n-1}^2 f_n = q_1 g_{n-1} \implies q_1 = f_n g_{n-1} \implies |q_1| = |f_n| \cdot |g_{n-1}| \leq ab$$

a koeficient u x^{n-1} :

$$g_{n-1}^2 f_{n-1} = q_0 g_{n-1} + q_1 g_{n-2} = q_0 g_{n-1} + f_n g_{n-1} g_{n-2}.$$

Po zkrácení nenulovým g_{n-1} a převedením na druhou stranu rovnosti dostáváme

$$q_0 = g_{n-1} f_{n-1} - f_n g_{n-2} \implies |q_0| \leq |g_{n-1}| \cdot |f_{n-1}| + |f_n| \cdot |g_{n-2}| \leq 2ab.$$

Porovnejme konečně koeficient u $x^i, 0 \leq i \leq n-2$:

$$g_{n-1}^2 f_i = q_1 g_{i-1} + q_0 g_i + r_i \implies |r_i| \leq |g_{n-1}^2| \cdot |f_i| + |q_1| \cdot |g_{i-1}| + |q_0| \cdot |g_i| \leq b^2 a + ab \cdot b + 2ab \cdot b = 4ab^2,$$

přičemž výrazem g_{-1} rozumíme 0.

Problém 2. Ať $f, g \in \mathbb{Z}[x]$, $\deg f = n, \deg g = n-1$, takové, že délky všech jejich koeficientů jsou nejvýše c.
Dokažte, že časová složitost výpočtu $f \operatorname{pmod} g$ je $\mathcal{O}(nc^2)$.

Řešení.
Výpočet $\operatorname{lc}(g) \cdot \operatorname{lc}(g) \to \mathcal{O}(c \cdot c)$,
Výpočet $\operatorname{lc}(g)^2 \cdot f \to \mathcal{O}(n \cdot 2c \cdot c)$,
Výpočet $\operatorname{lc}(g)^2 f \bmod f \to$ zde 2krát provádíme následující:
Podíl vedoucích koeficientů $\to \mathcal{O}(3c \cdot c))$,
přenásobení dělitele tímto podílem $\to \mathcal{O}((n-1) \cdot 3c \cdot c)$,
odečtení $\to \mathcal{O}((n-1) \cdot 4c)$.
Celkem je složitost $\mathcal{O}(nc^2)$.

Problém 3. Spočítejte $\operatorname{res}(f,g)$ pro
a) $f = x^2 + x - 2, g = x + 2, f, g \in \mathbb{Z}[x]$,
b) $f = x^2 - 1, g = x^2 + 1, f, g \in \mathbb{Z}[x]$.

Řešení. a)

$$\operatorname{res}(f,g) = \begin{vmatrix} 1 & 1 & -2 \\ 1 & 2 & \\ & 1 & 2 \end{vmatrix} = 4 - 2 - 2 = 0.$$

b)

$$\operatorname{res}(f,g) = \begin{vmatrix} 1 & 0 & -1 & \\ & 1 & 0 & -1 \\ 1 & 0 & 1 & \\ & 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix} + \begin{vmatrix} 0 & -1 & 0 \\ 1 & 0 & -1 \\ 1 & 0 & 1 \end{vmatrix} = 1 + 1 + 1 + 1 = 4.$$

Problém 4. Dokažte, že polynom $f \in \mathbb{Q}[x]$ má (ve svém rozkladovém nadtělese) vícenásobný kořen, právě když $\operatorname{res}(f,f') = 0$, kde f' je formální derivace f. Co podmínka $\operatorname{res}(f,f') = 0$ říká pro kvadratické polynomy? (Vyjádřete tuto podmínku pomocí koeficientů obecného kvadratického polynomu.)

Řešení.
Z přednášky víme, že $\operatorname{res}(f,f') = 0 \iff f$ a f' jsou soudělné. Ukážeme, že to je právě tehdy když f má násobný kořen ve svém rozkladovém nadtělese.
Ať f má násobný kořen a. Potom $f = (x-a)^2 \cdot g$ pro nějaké g. Derivací získáme

$$f' = 2(x-a)g + (x-a)^2 g' = (x-a)(2g + (x-a)g')$$

a vidíme, že f a f' jsou soudělné.
Ať naopak f má $n = \deg f$ různých kořenů x_i, tedy

$$f = \operatorname{lc}(f) \prod_{i=1}^{n} (x - x_i).$$

Pak

$$f' = \operatorname{lc}(f)(f/(x-x_1) + \cdots + f/(x-x_n))).$$

Všimněme si, že jelikož $\forall i : (x - x_i)$ dělí právě $n-1$ sčítanců v f', nemají f a f' žádného společného dělitele.

Uvažme $f = ax^2 + bx + c$, tedy $f' = 2ax + b$. Pak

$$\operatorname{res}(f,f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = ab^2 + 4ac - 2ab^2 = -a(b^2 - 4ac).$$

Protože $a \neq 0$, vidíme, že f má dvojnásobný kořen $\iff \operatorname{res}(f,f') = 0 \iff b^2 - 4ac = 0$.

Problém 5. Ať $a, b \in R, f, g \in R[x]$, $\deg f = n, \deg g = m$.
Dokažte (z definice, tj. bez Věty 13.4), že $\operatorname{res}(af, bg) = a^m b^n \operatorname{res}(f,g)$.

Řešení. V Sylvesterově matici je m řádků s koeficienty polynomu f a n řádků s koeficienty polynomu g. Jak víme, tak přenásobením řádku konstantou se determinant přenásobí touto konstantou. Z toho plyne tvrzení. Můžeme to zapsat i maticově

$$\operatorname{res}(af, bg) = \det M(af, bg) = \det \operatorname{diag}(\underbrace{a, \dots a}_{m\times}, \underbrace{b, \dots b}_{n\times}) M(f, g) =$$

$$= \det \operatorname{diag}(\underbrace{a, \dots a}_{m\times}, \underbrace{b, \dots b}_{n\times}) \det M(f, g) = a^m b^n \operatorname{res}(f, g).$$