Počítačová algebra - cvičení

22. května 2020

Problém 1. Spočítejte $\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2+x-1, 2x^3-x^2-5x-2)$ pomocí modulární metody s jedním prvočíslem.
Pro připomenutí, ať $f = \sum_{i=0}^{m} f_i x^i, g = \sum_{j=0}^{n} g_j x^j, n \leq m$. Pak

$$|\mathrm{mc}(\mathrm{NSD}(f,g))| \leq 2^n \cdot |\,\mathrm{NSD}(f_m, g_n)| \cdot \min\left(\frac{\|f\|_2}{|f_m|}, \frac{\|g\|_2}{|g_n|}\right),$$

kde ztotožňujeme polynom s vektorem koeficientů.

Řešení. Nsd vedoucích koeficientů je $d = 2$, LM mez je

$$LM = 2^2 \cdot 2 \cdot \frac{\sqrt{6}}{2} \leq 2^2 \cdot 2.5 = 10.$$

Volíme $41 = p > 2d \cdot LM$.

$$2x^3 - x^2 - 5x - 2 : 2x^2 - x - 1 = x - 1 \text{ zbytek } -3x - 3,$$

Vezmeme tedy polynom asociovaný se $-3x - 3$ s vedoucím členem $d = 2$, tedy $2x + 2$ a z něj primitivní část, $x + 1$. Protože $x + 1 \in \mathbb{Z}[x]$ dělí oba polynomy ze zadání, je to výsledek.

Problém 2. Spočítejte $\mathrm{NSD}_{\mathbb{Z}[x]}(2x^2-x-1, 2x^3-x^2-5x-2)$ pomocí modulární metody s více prvočísly.

Řešení. Opět $LM \leq 10, d = 2$.
Prvočíslo 2 je nepoužitelné.
Modulo 3:

$$-x^3 - x^2 + x + 1 : -x^2 - x - 1 = x \text{ zbytek } -x + 1$$

$$x^2 + x + 1 : -x + 1 = x - 1 \text{ zbytek } 0$$

Volíme NSD s vedoucím členem $d = 2$: $2x + 1$.
Modulo 5:

$$2x^3 - x^2 - 2 : 2x^2 - x = x \text{ zbytek } x - 2$$

$$2x^2 - x - 1 : x - 2 = 2x + 3 \text{ zbytek } 0.$$

Volíme NSD s vedoucím členem $d = 2$: $2x + 1$. Ještě jsme nepřekročili teoretickou mez, mohli bychom pokračovat na další prvočíslo. Ale vyšel nám stejný mezivýsledek a tak otestujeme, zda se nejedná o finální výsledek. Jedná, protože $2x + 1$ dělí oba polynomy ze zadání.

Problém 3. Pro polynomy $f, g \in \mathbb{Z}[x]$ platí

$$\mathrm{NSD}_{\mathbb{Z}[x]}(f,g) \bmod p \mid \mathrm{NSD}_{\mathbb{Z}_p[x]}(f \bmod p, g \bmod p) \quad \text{a}$$

$$\mathrm{lc}(\mathrm{NSD}_{\mathbb{Z}[x]}(f,g)) \mid \mathrm{NSD}_{\mathbb{Z}}(\mathrm{lc}\, f, \mathrm{lc}\, g).$$

Formulujte a dokažte analogická pozorování pro polynomy ze $\mathbb{Z}[x,y] = (\mathbb{Z}[y])[x]$.

Řešení. Připomeňme si, že pro $f \in \mathrm{R}[x,y]$ je $f \bmod (y-\alpha) = f(x,\alpha)$.
Analogická tvrzení jsou:

1. $\mathrm{NSD}_{\mathbb{Z}[x,y]}(f,g)(x,\alpha) \mid \mathrm{NSD}_{\mathbb{Z}[x]}(f(x,\alpha), g(x,\alpha))$
   Označme $h = \mathrm{NSD}(f,g)$, $f = hu, g = hv$.
   Modulení polynomem $y-\alpha$ neboli dosazení $y = \alpha$ je homomorfismus, tedy
   $$f(x,\alpha) = h(x,\alpha)u(x,\alpha),$$
   $$g(x,\alpha) = h(x,\alpha)v(x,\alpha).$$
   Pak ale $h(x,\alpha)$ je společným dělitelem $f(x,\alpha)$ i tedy $g(x,\alpha)$ takže dělí jejich největšího společného dělitele.

2. $\mathrm{lc}(\mathrm{NSD}_{\mathbb{Z}[x,y]}(f,g)) \mid \mathrm{NSD}_{\mathbb{Z}[x]}(\mathrm{lc}\, f, \mathrm{lc}\, g)$
   Při značení výše $f = hu \implies \mathrm{lc}(f) = \mathrm{lc}(h)\mathrm{lc}(u)$ a
   $g = hv \implies \mathrm{lc}(g) = \mathrm{lc}(h)\mathrm{lc}(v)$.
   Pak $\mathrm{lc}(h)$ je společným dělitelem $\mathrm{lc}(f)$ a $\mathrm{lc}(g)$, takže dělí jejich největšího společného dělitele.

Problém 4. Spočítejte

$$\mathrm{NSD}(y^6 + xy^5 + x^3y - xy + x^4 - x^2, xy^5 - 2y^5 + x^2y^4 - 2xy^4 + xy^4 + xy^2 + x^2y).$$

Řešení. Dosazením $y = 1$ dostaneme

$$1 + x + x^3 - x + x^4 - x^2 = x^4 + x^3 - x^2 + 1 \quad \text{a}$$

$$x - 2 + x^2 - 2x + x + x + x^2 = 2x^2 + x - 2.$$

Druhý polynom má neceločíselné kořeny, je tedy ireducibilní. Zároveň vidíme, že nedělí první polynom, takže jsou nesoudělné. První bod předchozího problému nám dává, že i původní polynomy jsou nesoudělné.

Problém 5. Dokažte z definice, že pro $f, g \in \mathbb{Z}[x], n = \max(\deg f, \deg g)$ s maximálním koeficientem a je

$$\ell(\mathrm{res}(f,g)) = \mathcal{O}(n \log(an)).$$

Řešení. Rezultant je determinant matice s rozměry nejvýše $2n \times 2n$, se vstupy maximálně a. Z definice determinantu tedy

$$|\mathrm{res}| \leq (2n)! \cdot a^{2n} \leq (2na)^{2n},$$

$$\ell(\mathrm{res}) = \mathcal{O}(\log((2na)^{2n})) = \mathcal{O}(2n \log(2na)) = \mathcal{O}(n \log(na)).$$