Algoritmy na polynomech — Cvičení 5

ondrej.jezil@email.cz

November 2023

1 Teoretická část

Gröbnerovy báze

1. Ukažte, že problém určit zda polynom $p(\overline{x})$ náleží danému ideálu $I \leq \mathbb{Q}[\overline{x}]$ je **coNP**-těžký?

Bezčtvercová faktorizace polynomů

2. Spočtěte bezčtvercovou faktorizaci polynomu $x^5 + 2x^4 - 2x^3 - 4x^2 + x + 2$ nad $\mathbb{Z}[x]$.

3. Spočtěte bezčtvercovou faktorizaci polynomu $x^7 + x^6 - x^5 - x^4 - x^3 - x^2 + x + 1$ nad $\mathbb{Z}[x]$.

4. Spočtěte bezčtvercovou faktorizaci polynomu $x^6 + x^4 + x^2 + 1$ nad $\mathbb{Z}_2[x]$.

5. Spočtěte bezčtvercovou faktorizaci polynomu $x^7 + x^6 + x^4 + x^3 + x + 1$ nad $\mathbb{Z}_3[x]$.

6. Nechť $\mathbf{R}$ je gaussovský obor charakteristiky 0 a nechť f je primitivní polynom z $\mathbf{R}[x_1, ..., x_m]$. Dokažte:

   - f je bezčtvercový $\iff \gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = 1$;
   - Pokud $f = \prod_{i=1}^{k} h_i^i$ je bezčtvercový rozklad, potom

   $$\gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = \prod_{i=1}^{k} h_i^{i-1}.$$

   Aplikujte toto tvrzení na návrh algoritmu pro bezčtvercovou faktorizaci polynomů více proměnných nad gausovskými obory charakteristiky 0.

7. Formulujte a dokažte analogické tvrzení jako v minulé úloze, ale pro kladnou charakteristiku.