Algoritmy na polynomech, cvičení 6

borysek@karlin.mff.cuni.cz
https://karlin.mff.cuni.cz/~borysek/

12. prosince 2024

1 Teoretická část

Berlekampův algoritmus

1. Nechť $f \in \mathbb{F}_q[x]$ a
$$W = \{h \in \mathbb{F}_q[x];\ \deg h < \deg f,\ h^q \equiv h \mod f\},$$
dokažte přímo, že W je vektorový prostor nad $\mathbb{F}_q$.

2. Použijte Berlekampův algoritmus na spočtení rozkladu
   - $x^4 + 1 \in \mathbb{Z}_3[x]$,
   - $x^7 + 2x^5 + 2x^4 + x^3 + 2x + 2 \in \mathbb{Z}_5[x]$,
   - $x^7 + 4x^6 + 2x^5 + 4x^3 + 3x^2 + 4x + 2 \in \mathbb{Z}_5[x]$.

   Nezapomeňte ověřit, že dané polynomy jsou bezčtevrcové, popř. provést bezčtvercovou faktorizaci.

3. Pokuste se začít s Berlekampovým algortmem a zachovat v něm jen ty části, které jsou potřeba k ověření, že polynom na vstupu je ireducibilní. Zkuste to udělat tak, abyste získali algoritmus s lepší časovou složitostí, než je použití Berlekampova algoritmu jako blackboxu.

4. Vysvětlete, proč není výhodné používat Berlekampův algoritmus, pokud pouze chcete najít všechny kořeny daného polynomu.

Henselovo zdvihání, pomocné lemma

5. Nechť máme následující polynomy v $\mathbb{Z}_3[x]$:
$$f = x^2 + 2x + 2,\ g_1 = 2x + 1,\ g_2 = x + 1 \text{ a } g_3 = x.$$
Nechť $\tilde{g}_i = \prod_{j \in \{1,2,3\} \setminus \{i\}} g_j$. Najděte $u_1, u_2, u_3 \in \mathbb{Z}_3[x]$ tak že $f = u_1\tilde{g}_1 + u_2\tilde{g}_2 + u_3\tilde{g}_3$, a $\deg u_i < \deg g_i$, pro všechna $i \in \{1, 2, 3\}$.

2 Výpočetní část

- Ověřte 2 pomocí `Sagemath`.