Algoritmy na polynomech — Cvičení 6

ondrej.jezil@email.cz

November 2023

1 Teoretická část

Berlekampův algoritmus

1. Nechť $f \in \mathbb{F}_q[x]$ a
$$W = \{h \in \mathbb{F}_q[x]; \deg h < \deg f, h^q \equiv f\},$$
dokažte přímo, že W je vektorový prostor nad $\mathbb{F}_q$.
2. Použijte Berlekampův algoritmus na spočtení rozkladu $x^4 + 1 \in \mathbb{F}_3[x]$.
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, aby jste 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.

Berlekamp-Henselův agoritmus

1. Nechť máme následující polynomy v $\mathbb{F}_3[x]$: $f = x^2 + 2x + 2$, $g_1 = 2x + 1$, $g_2 = x+1$ a $g_3 = x$. Nechť $\tilde{g}_i = \prod_{j\in\{1,2,3\}\setminus\{i\}} g_j$. Najděte $u_1, u_2, u_3 \in \mathbb{F}_3[x]$ 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. Nechť $f = 5x^3 + 9x^2 - 146x - 120 \in \mathbb{Z}[x]$. Uvažte rozklad:
$$f \equiv (2x + 1)(x + 1)x \pmod 3$$
Užijte Henselovo zdvihání tak, aby jste našli rozklad f modulo 9.
3. Nechť $f = 6x^7+7x^6+4x^5+x^4+6x^3+7x^2+4x+1 \in \mathbb{Z}[x]$. Uvažte rozklad:
$$f \equiv (6x + 3)(x^2 - 7)(x^2 + 7)(x^2 + 9x - 8) \pmod{25}$$
A zkuste využít Zassenhausovu kombinaci faktorů tak, aby jste našli rozklad f v $\mathbb{Z}[x]$. Splňuje 25 mezi předpokládanou v algoritmu?
4. (*) Dokažte, že $x^4 + 1$ je ireducibilní v $\mathbb{Z}[x]$, ale má netriviální rozklad v $\mathbb{F}_p[x]$ pro každé prvočíslo p.