

Algoritmy na polynomech, cvičení 6

borysek@karlin.mff.cuni.cz

<https://karlin.mff.cuni.cz/~borysek/>

11. prosince 2025

1 Teoretická část

Berlekampův algoritmus

1. Necht $f \in \mathbb{F}_q[x]$ a

$$W = \{h \in \mathbb{F}_q[x]; \deg h < \deg f, h^q \equiv h \pmod{f}\},$$

dokažte přímo, že W je vektorový prostor nad $\mathbb{F}_q$.

2. Použijte Berlekampův algoritmus na spočtení rozkladu

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

Nezapomeňte ověřit, že dané polynomy jsou bezčtevcové, popř. provést bezčtvercovou faktorizaci. Můžete si pomoci **Sagemath**.

3. Pokuste se začít s Berlekampovým algoritmem a zachovat v něm jen ty části, které jsou potřeba k ověření, že polynom z $\mathbb{F}_q[x]$ na vstupu je ireducibilní.
4. Navíc z předchozího cvičení vydedukujte kritérium pro ireducibilitu polynomu stupně 2 nad $\mathbb{F}_q[x]$. Jak se dá tohle kritérium nahlédnout i bez předchozího bodu? Dá se tohle kritérium zobecnit na kritérium toho, že se libovolný polynom z $\mathbb{F}_q[x]$ rozkládá na lineární činitele?
5. Vysvětlete, proč není výhodné používat Berlekampův algoritmus, pokud pouze chcete najít všechny kořeny daného polynomu.

Bonus

1. Dokažte, že $x^4 + 1$ je ireducibilní v $\mathbb{Z}[x]$, ale má netriviální rozklad v $\mathbb{Z}_p[x]$ pro každé prvočíslo p .

2 Výpočetní část

- Ověřte 2 pomocí **Sagemath**.