# Algoritmy na polynomech, cvičení 7

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

8. ledna 2026

## 1 Henselovo zdvihání, pomocné lemma

1. Mějme 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 Berlekamp-Henselův algoritmus

1. 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, abyste našli rozklad $f$ modulo 9.

2. 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, abyste našli rozklad $f$ v $\mathbb{Z}[x]$. Splňuje 25 mez předpokládanou v algoritmu? Můžete předpokládat, že tato hodnota stačí.

3. Dokažte jednoznačnost polynomů $u_1, \ldots, u_n$ v tvrzení 17.2.

4. Uvažujme polynom $f = 2x^7 - x^6 - x^4 + 2x^3 - x^2 - 1$. Výstupem Berlekampova algoritmu pro $p = 5$ je rozklad $(2x + 3)(x^2 + 2)(x^2 + 3)(x^2 + 3x + 3)$. Henselovým zdvižením získáme rozklad $f = (2x + 23)(x^2 + 7)(x^2 + 18)(x^2 + 13x + 13)$ modulo 25. Pro jednoduchost předpokládejme, že $k = 2$ stačí. Odsimulujte běh kombinačního algoritmu a spočtěte rozklad polynomu $f$ v $\mathbb{Z}[x]$.

5. Buď $f \in \mathbb{Z}[x]$ bezčtvercový polynom a $p$ prvočíslo takové, že $f \bmod p$ není bezčtvercový. Dokažte, že $p | \mathrm{res}(f, f')$.