# Algoritmy na polynomech, domácí úkol 2

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

**Řešení posílejte na mail** `borysek@karlin.mff.cuni.cz`

**DEADLINE: 9. ledna 2025**

## 1 Teoretická čast (min. na zápočet- 50 bodů)

### 1.1 Bezčtvercovost

1. **(25 bodů)** Ukažte, že pro monický polynom $f \in \mathbb{F}_q[x]$, a libovolný polynom $h \in \mathbb{F}_q[x]$ takový, že
$$h^q \equiv h \mod f,$$
platí
$$f = \prod_{a \in \mathbb{F}_q} \gcd(f, h - a),$$
i bez předpokladu, že $f$ je bezčtvercový.
2. * **(20 bodů + 15 bonusových)** Co bude výstupem Berlekampova algoritmu, pokud dostane na vstupu monický polynom $f \in \mathbb{F}_q[x]$, který není nutně bezčtvercový?
3. Nechť $\mathbf{R}$ je gaussovský obor charakteristiky 0 a nechť $f$ je primitivní polynom z $\mathbf{R}[x_1, ..., x_m]$. Dokažte:
   - **(7 bodů)** $f$ je bezčtvercový $\iff \gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = 1$;
   - **(8 bodů)** Pokud $f = \prod_{i=1}^{k} h_i^i$ je bezčtvercový rozklad, potom
   $$\gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = \prod_{i=1}^{k} h_i^{i-1}.$$
4. **(8 bodů)** Formulujte a dokažte analogické tvrzení jako v minulé úloze, ale pro konečná tělesa.
5. **(7 bodů)** Aplikujte tvrzení z úlohy 3 na návrh algoritmu pro bezčtvercovou faktorizaci polynomů více proměnných nad gaussovskými obory charakteristiky 0.

### 1.2 Faktorizace polynomů více proměnných

1. Nechť je $\mathbf{R}$ Gaussovský obor a nechť $\phi_d$ je zobrazení z $\mathbf{R}[x_1, \ldots, x_k]$ do $\mathbf{R}[y]$ definované následovně:
$$\phi_d(f) = f(y, y^d, y^{d^2}, \ldots, y^{d^{k-1}}).$$
   - **(12 bodů)** Ukažte, že $\phi_d$ je okruhový homomorfismus a že restrikce $\phi_d$ na množinu
   $$\{f \in \mathbf{R}[x_1, \ldots, x_k]; \deg_{x_i} f < d \text{ pro každé } i\}$$
   je prosté zobrazení. Navíc popište $\mathrm{Im}(\phi_d)$.
   - **(5 bodů)** Uvažte $f = x_1^2x_2 + x_1x_2^2 + x_1 + x_2 \in \mathbb{Z}[x_1, x_2]$ a $\phi_3$ podle definice výše. Zrekonstruujte $f$ z $\phi_3(f)$.
2. **(8 bodů)** Předchozí pozorování je základem Kroneckerova algoritmu. Hlavní myšlenka je místo přímého faktorizování polynomu $f$ faktorizovat $\phi_d(f)$ pomocí Berlekampova-Henselova algoritmu a potom z této faktorizace zrekonstruovat faktorizaci $f$. Použijte tento algoritmus na nalezení ireducibilního rozkladu $f = x^2y^2 + xy^2 - x^2y + y - x - 1 \in \mathbb{Z}[x, y]$. Poznámka: Pro faktorizaci v jedné proměnné můžete použít `SageMath`.

## 2 Výpočetní část (min. na zápočet- 50 bodů)

1. **(15 bodů)** Implementujte bezčtvercovou faktorizaci nad gaussovskými obory charakteristiky 0.
2. **(15 bodů)** Implementujte bezčtvercovou faktorizaci nad konečnými tělesy.
3. **(40 bodů)** Implementujte Berlekampův algoritmus pro $\mathbb{Z}_2[x]$.
4. * **(30 bodů + 35 bonusových bodů)** Implementujte Berlekampův-Henselův algoritmus (zde můžete použít Berlekampův algoritmus zabudovaný v `Sagemath`, Henselovo zdvihání ale implementujte sami).