# Algebra — cvičení 6

(příklady cihlovou barvou jsme dělali on-line, na doma jsou ty ostatní bez hvězdiček; jeden klidně vynechte)

## Ireducibilita polynomů v gaussovských oborech

1. Najděte všechny racionální kořeny daných polynomů ze $\mathbb{Z}[x]$:
   (a) $2x^3 - x^2 + 3$,
   (b) $4x^7 - 16x^6 + x^5 + 55x^4 - 35x^3 - 38x^2 + 12x + 8$.

2. Rozmyslete si, proč je polynom $f(x) = 2x + 6$ ireducibilní v $\mathbb{Q}[x]$, ale je rozložitelný v $\mathbb{Z}[x]$. Najděte k němu v $\mathbb{Q}[x]$ asociovaný primitivní polynom.

3. Rozmyslete si, proč jsou následující polynomy v příslušných oborech ireducibilní:
   (a) $x^3 + x^2 + x + 3$ v $\mathbb{Z}[x]$,
   (b) $x^4 + x^3 - x + 1$ v $\mathbb{Z}[x]$,
   (c) $4x^3 - 15x^2 + 60x + 180$ v $\mathbb{Z}[x]$,
   (d) $x^5 - 36x^4 + 6x^3 + 30x^2 + 24$ v $\mathbb{Q}[x]$.

4. Spočtěte v oboru $\mathbb{Z}[x, y]$ NSD pro polynomy $6x^2y$ a $15xy^2 + 21x^3y$. (Zaměřte se na zdůvodnění dle Věty 8.3 ze skript.)

5. Najděte v příslušných oborech ireducibilní rozklady daných polynomů:

| | $x^2 - y + 2$ | $x^2 - 2y^2$ | $x^2 + y^2$ | $x^2 + xy + y - 1$ |
|---|---|---|---|---|
| $\mathbb{Q}[x, y]$ | | | | |
| $\mathbb{R}[x, y]$ | | | | |
| $\mathbb{C}[x, y]$ | | | | |

## Čínská věta o zbytcích pro polynomy

6. Vyřešte kongruence:
   (a) $(x^3 + x + 1)f(x) \equiv 1 \pmod{x^4 + x + 1}$ v $\mathbb{Z}_2[x]$,
   (b) $(2x + 1)f(x) \equiv x^3 \pmod{x^2 + 1}$ v $\mathbb{Z}_3[x]$.

7. Najděte všechny polynomy $f \in \mathbb{Q}[x]$ stupně menšího než 3 splňující $f(0) = 1, f(1) = 0, f(2) = 2$
   (a) jako Lagrangeův interpolační polynom,
   (b) pomocí Čínské věty o zbytcích.

8. Najděte polynom $f \in \mathbb{Z}_5[x]$ co nejmenšího stupně, který splňuje

$$\begin{cases} f \equiv x + 1 \pmod{x^2 + 1}, \\ f \equiv x \pmod{x^3 + 1}. \end{cases}$$

## Další příklady

9.* (Další možná metoda pro testování ireducibility; používá se obměněná implikace) Ukažte, že je-li primitivní polynom $f(x) \in \mathbb{Z}[x]$ reducibilní a prvočíslo $p$ nedělí vedoucí koeficient $f(x)$, pak je reducibilní i polynom $\overline{f(x)} \in \mathbb{Z}_p[x]$ získaný vzetím koeficientů $f(x)$ modulo $p$.

10.* Rozhodněte o ireducibilitě polynomu $x^5 + 4x^4 + 2x^3 + 3x^2 - x + 5$ v $\mathbb{Z}[x]$. (Využijte předchozí tvrzení.)

11.* (Ještě jedna možná metoda) Ukažte, že je-li $R$ obor, pak polynom je $f(x) \in \mathbf{R}[x]$ reducibilní právě tehdy, je-li v $\mathbf{R}[x]$ reducibilní polynom $g(x)$ získaný z $f(x)$ lineární substitucí $x \mapsto ax + b$ pro $a, b \in \mathbf{R}$ a $a$ invertibilní v $R$.

12.* S využitím předchozího tvrzení rozhodněte o ireducibilitě následujících polynomů v $\mathbb{Z}[x]$:

(a) $x^3 + 3x^2 + 5x + 5$,

(b) $\frac{x^p-1}{x-1} = \sum_{i=0}^{p-1} x^i$ pro prvočíslo $p$.

13.* Rozmyslete si, proč je polynom $3x^3 + 2x^2 + (4 - 2i)x + (1 + i)$ v $(\mathbb{Z}[i])[x]$ ireducibilní.