10. cvičení

Ve škole:

1. Dokažte, že algoritmus dělení se zbytkem v oboru $\mathbb{Z}[i]$, který pro $u, v \in \mathbb{Z}[i] \setminus 0$ nejprve najde $a, b \in \mathbb{Q}$ splňující $\frac{u}{v} = a + bi$ a na výstupu předloží hodnoty $q = [a] + [b]i \in \mathbb{Z}[i]$ a $z = u - qv$, splňuje podmínku $\nu(z) < \nu(v)$.

2. Vydělte v oboru $\mathbb{Z}[i]$ se zbytkem
(a) $(5 + 7i) : (3 - i)$, (b) $(3 + 2i) : (1 - 2i)$, (c) $(3 + 2i) : (1 + i)$.

3. Dokažte, že je prvočíslo p splňující $p \equiv 3 \pmod 4$ ireducibilním prvkem oboru $\mathbb{Z}[i]$.

4. Spočítejte v oboru $\mathbb{Z}[i]$ ireducibilní rozklady 3, 5, 6, 7, $10 - 6i$, $9 + 3i$,

Úlohy pro samostatné počítání:

5. Spočítejte v oborech $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}_3[x], \mathbb{Z}_5[x]$ ireducibilní rozklady polynomů (a) $x^3 - 2$ a (b) $x^4 - x^2 - 2$.

6. Dokažte, že v oborech $\mathbb{Z}[\sqrt{s}]$ pro $s = -2, 2, 3$ funguje obdoba algoritmu dělení se zbytkem z 1.úlohy. Proč totéž nemůže fungovat pro $s = -3, 5$?

Řešení:

1. $\frac{\|z\|^2}{\|v\|^2} = \|\frac{z}{v}\|^2 = \|\frac{u-qv}{v}\|^2 = \|\frac{u}{v} - q\|^2 = (a-[a])^2 + (b-[b])^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2}$
   $\Rightarrow \nu(z) = \|z\|^2 \leq \frac{1}{2}\|v\|^2 = \frac{1}{2}\nu(v) \Rightarrow \nu(z) < \nu(v)$.

2. (a) $(5+7i) = (1+3i)\cdot(3-i) - 1 - i$,

   (b) $(3+2i) = 2i\cdot(1-2i) - 1$

   (c) $(3+2i) = 2\cdot(1+i) + 1 = 3\cdot(1+i) - i = (2-i)\cdot(1+i) + i = (3-i)\cdot(1+i) - 1$

3. Je-li p liché prvočíslo, které není ireducibilní v $\mathbb{Z}[i]$, pak lze napsat jako součin $p = (a-bi)(c+di)$ pro $a+bi, c+di \in \mathbb{Z}[i]$, které nejsou invertibilní, tedy $\nu(a-bi) \neq 1 \neq \nu(c+di)$. Protože $p^2 = \nu(p) = \nu(a-bi)\nu(c+di) = (a^2+b^2)(c^2+d^2)$, platí, že $p = a^2+b^2 = c^2+d^2$, a tudíž $a = c$ a $b = d$. Protože je p liché, je právě jedno z čísel a, b liché, tedy existují celá k, l, pro něž $p = (2k)^2 + (2l+1)^2 \equiv 1 \pmod 4$.

   To znamená, že pokud $p \equiv 3 \pmod 4$, je p ireducibilní.

4. 3, $5 = (2+i)(2-i)$, $6 = (1+i)(1-i)\cdot 3$, 7, $10-6i = -(1+i)^3\cdot(4+i)$, $9+3i = 3\cdot(1+i)\cdot(2-i)$,

5. (a) $x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}e^{\frac{2\pi i}{3}})(x + \sqrt[3]{2}e^{\frac{2\pi i}{3}})$ v $\mathbb{C}[x]$,
   $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ v $\mathbb{R}[x]$ $x^3 - 2$ je ireducibilní v $\mathbb{Q}[x]$,
   $x^3 - 2 = x^3 + 1 = (x+1)^3$ v $\mathbb{Z}_3[x]$ a $x^3 - 2 = (x+2)(x^2+3x+4)$ v $\mathbb{Z}_5[x]$.
   (b) $x^4 - x^2 - 2 = (x+i)(x-i)(x+\sqrt{2})(x-\sqrt{2})$ v $\mathbb{C}[x]$,
   $x^4 - x^2 - 2 = (x^2+1)(x+\sqrt{2})(x-\sqrt{2})$ v $\mathbb{R}[x]$,
   $x^4 - x^2 - 2 = (x^2+1)(x^2-2)$ v $\mathbb{Q}[x]$,
   $x^4 - x^2 - 2 = (x^2+1)^2$ v $\mathbb{Z}_3[x]$,
   $x^4 - x^2 - 2 = (x+2)(x-2)(x^2-2)$ v $\mathbb{Z}_5[x]$.

6. Obdobným výpočtem zjistíme, že $\nu(r) \leq \frac{3}{4}\nu(v), \frac{1}{2}\nu(v), \frac{3}{4}\nu(v)$, a proto $\nu(r) < \nu(v)$ pro čísla $s = -2, 2, 3$.

   Pro $s = -3, 5$ podobný odhad provést nelze.