7. cvičení

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

2. Spočítejte v $\mathbb{Z}[i]$ (pomocí Eukleidova algoritmu nebo normy)
(a) $\mathrm{NSD}(5+7i, 3-i)$, (b) $\mathrm{NSD}(6-7i, 7+i)$, (c) $\mathrm{NSD}(8+5i, 4+i)$.

3. Dokažte pro prvočíslo p, že
(a) je prvočinitelem v oboru $\mathbb{Z}[i]$, právě když $p \equiv 3 \pmod 4$,
(b) je-li $p \equiv 1 \pmod 4$, pak existují prvočinitele $a+bi, a-bi \in \mathbb{Z}[i]$, pro které $p = (a+bi)(a-bi)$.
(Návod: dokažte a využijte tvrzení $(p-1)! \equiv -1 \pmod p$)

4. Určete v oboru $\mathbb{Z}[i]$ rozklad čísel $3, 5, 6, 7, 20, 21, 101, 157$ na prvočintele.

Řešení:

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

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

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

2. (a) $1+i$, (b) $2+i$, (c) 1

3. Pokud $p = (a+bi)(a-bi) = a^2+b^2$, pak je právě jedno z čísel, například a liché, proto $p \equiv 1 \pmod 4$. Protože $\nu(p) = p^2$, je prvočíslo součinem nejvýše dvou prvočinitelů (s normou p), proto pokud $p \equiv 3 \pmod 4$, je p prvočinitel.

   Jestliže $p \equiv 1 \pmod 4$, pak je $\frac{p-1}{2}$ sudé a proto

   $$-1 \equiv (p-1)! \equiv \prod_{i=1}^{\frac{p-1}{2}} i(-i) \equiv (\frac{p-1}{2})^2 \pmod p,$$

   tedy existuje c splňující $p/c^2+1 = (c+i)(c-i)$. Hledané $a+bi$ je $\mathrm{NSD}(p, c+i)$ v $\mathbb{Z}[i]$.

4. $3, 5 = (2+i)(2-i)$, $6 = (1+i)(1-i)\cdot 3$, 7, $20 = (1+i)^2(1-i)^2(2+i)(2-i)$, $21 = 3\cdot 7$, $101 = (10+i)(10-i)$, $157 = (11+6i)(11-6i)$