Sedmé cvičení

16. listopadu 2012

Okruh $\mathbb{Z}[i]$ je gaussovský. To znamená, že ireducibilní prvky se v něm chovají velmi podobně jako prvočísla v $\mathbb{Z}$.

Užitečný nástroj: Zavedeme si normu $\|a + bi\| = a^2 + b^2$ (druhá mocnina běžné absolutní hodnoty).

Náš cíl: Dokázat, že v $\mathbb{Z}[i]$ jsou ireducibilní prvky právě $\pm p, \pm ip$ pro $p \in \mathbb{N}$ prvočíslo dávající po dělení 4 zbytek 3 a dále všechna u, že $\|u\|$ je prvočíslo.

V řešení úlohy 3 se vám může hodit fakt, že pro $p = 4k + 1$ prvočíslo vždy existuje řešení rovnice $x^2 + 1 = 0$ modulo p.

Příklad 1. Dokažte, že v $\mathbb{Z}[i]$ platí:

a) pokud $u|v$, tak $\|u\|\|v\|$,

b) u je invertibilní, právě když $\|u\| = 1$.

Příklad 2. Dokažte, že pokud je $u \in \mathbb{Z}[i]$ takové, že $\|u\|$ je prvočíslo, tak je u ireducibilní v $\mathbb{Z}[i]$.

Příklad 3. Dokažte, že pokud je p prvočíslo takové, že $p \equiv 3 \pmod 4$, tak jsou $\pm p$, $\pm ip$ ireducibilní v $\mathbb{Z}[i]$.

Příklad 4. Nechť $a + bi$ je ireducibilní prvek $\mathbb{Z}[i]$, $a, b \neq 0$. Dokažte, že:

a) Číslo $a - bi$ je ireducibilní.

b) Pokud $a + bi$ je nesoudělné s 2, tak jsou $a \pm bi$ nesoudělná.

c) Využitím předchozího a faktu, že $\mathbb{Z}[i]$ je gaussovský, dokažte, že $\|a + bi\|$ musí být prvočíslo.

Příklad 5. Dokažte, že pokud $p = 2$ nebo p je prvočíslo takové, že $p \equiv 1 \pmod 4$, tak p není ireducibilní v $\mathbb{Z}[i]$. Rada: Využijte existenci odmocniny z -1 v $\mathbb{Z}_p$.