4. přednáška a cvičení (17. března 2009)

Co jsme dělali na přednášce?

Sekce 2.10 (navíc popis, kdy je $\mathbb{Z}_n^*$ cyklická) a 2.12 (a možná část 2.13) ze skript.

Co jsme dělali na cvičení?

Řešili jsme rovnice rozkladem v $\mathbb{Z}[i]$. Rámcová kostra celého postupu dobrá pro to, aby člověk při řešení na nic nezapomněl, vypadá asi takto:

1. Rozlož jednu stranu rovnice na součin.

2. Dokaž nesoudělnost faktorů (k tomu může být často vhodné zkoumat dělitelnost a soudělnost neznámých).

3. Použij lemma zformulované ve 2. příkladu. Případně jiným způsobem využij jednoznačnosti prvočíselného rozkladu – to je možné, i pokud součinitelé nejsou přímo nesoudělní, ale mají nějakého známého společného dělitele.

4. Ze zjištěných vztahů vyjádři neznámé pomocí (nových) parametrů.

5. Ověř, pro které hodnoty parametrů dostaneme vskutku řešení zadané rovnice (včetně případných dodatečných předpokladů na hodnoty proměnných).

Příklady

0. Vyřeš rovnici $x^2 + y^2 = z^2$.

1. Najdi všechna řešení rovnice $x^2 + 4 = y^3$ taková, že x je liché.

2. Buď R obor s jednoznačným rozkladem na součin prvočinitelů, $a, u, v \in R, (u, v) = 1, n \in \mathbb{N}$. Pokud $uv \| a^n$, existují $b, c \in R$ taková, že $u \| b^n, v \| c^n$.

3. Vyřeš rovnici $y^2 + 1 = x^3$.

4. Vyřeš rovnici $x^4 + y^4 = z^2$.

5. Buď $k \in \mathbb{N}, p \equiv 3 \pmod 4$ prvočíslo. Vyřeš rovnici $16x^2 + y^2 = p^k$ (v závislosti na k, p).

6. $y^2 + 1 = x^p$, $p \geq 3$ prvočíslo.