Cvičení 22. 2. 2013

Buď R komutativní okruh. Řekneme, že prvek r dělí prvek s (a napíšeme $r|s$), pokud existuje $t \in R$, že $rt = s$. Dělitelnost je reflexivní a tranzitivní relace.

Okruh R je:

- *Obor integrity*, pokud má komutativní násobení a z $rs = 0$ plyne $r = 0$ nebo $s = 0$.
- *Obor integrity hlavních ideálů*, pokud je obor integrity a každý ideál je tvaru rR pro nějaké $r \in R$.
- *Euklidovský*, pokud je obor integrity a (zhruba řečeno) funguje rozumné dělení se zbytkem pro Euklidův algoritmus. Příklady: $\mathbb{Z}$, polynomy nad tělesem, $\mathbb{Z}[i]$.

Platí: Euklid $\Rightarrow$ obor integrity hlavních ideálů. A pro $m, n \in R$ lze hledat $x, y \in R$, že $mx + ny = \mathrm{NSD}(m, n)$ pomocí rozšířeného Euklidova algoritmu.

Příklad 1. Spočtěte pro dané m, n čísla x, y, aby $mx + ny = (m, n)$:

1. $m = 84, n = 33$
2. $m = 168, n = 396$
3. $m = 2^{63} - 1, n = 2^{98} - 1$

Příklad 2. Pro která $n \in \mathbb{N}$ je okruh $\mathbb{Z}_n$ oborem integrity?

Příklad 3. Okruh $\mathbb{Q}[x]$ je euklidovský. Pomocí Euklidova algoritmu najděte největšího společného dělitele polynomů:

1. $p = x^3 + 2x + 1$, $q = x^2 + 3$
2. $p = 4x^4 + 6x^3 + x^2 + 1$, $q = x^2 + 4x + 3$

Příklad 4. Spočtěte pomocí Euklidova algoritmu inverzní prvky k:

1. 5 modulo 11
2. 3 modulo 206
3. 133 modulo 275
4. $x + 2$ modulo $x^2 + 1$ (nad tělesem $\mathbb{Q}$)

5. $x^2 + 2$ modulo $x^3 - 1$ (nad $\mathbb{Q}$)

Příklad 5. Nakreslete uspořádání dělitelností okruhu $\mathbb{Z}_{10}$. Co „divného“ pozorujete oproti oborům integrity?

Příklad 6. Dokažte, že následující podmínky jsou ekvivalentní pro každou dvojici $n \in \mathbb{N}, a \in \mathbb{Z}$:

1. a, n jsou nesoudělná
2. $(a \mod n) \in \mathbb{Z}_n^\star$
3. $i \mapsto ai \pmod n$ je automorfismus grupy $\mathbb{Z}_n$
4. $a\mathbb{Z}_n = \mathbb{Z}_n$

Kreativní úlohy

Příklad 7. Najděte všechna $n \in \mathbb{N}$ taková, že počet prvočísel v množině

$$\{1 + n, 2 + n, \ldots, 10 + n\}$$

je maximální možný.

Příklad 8. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k+2, k \in \mathbb{Z}$.

Příklad 9. Dokažte, že existuje nekonečně mnoho n takových, že $n|2^n + 1$.