Cvičení 8. 3. 2012

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. Prvky $a, b \in R$ nazveme *asociované*, pokud $a|b$ a zároveň $b|a$.

Prvek $r \in R$ je *invertibilní*, pokud existuje $s \in R$, že $rs = 1$. Prvek $r \in R \setminus \{0\}$ je *ireducibilní*, pokud r není invertibilní a $r = st$ implikuje $r|s$ nebo $r|t$. Prvek $r \in R \setminus \{0\}$ je *prvočinitel*, pokud není invertibilní a $r|st$ implikuje $r|s$ nebo $r|t$.

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 funguje rozumné dělení se zbytkem: Existuje funkce $\phi : R \to \mathbb{N}_0$, že
  1. $\phi(0) = 0$ a $\phi(x) > 0$ jinak,
  2. $\phi(a) \leq \phi(b)$ kdykoli $a|b$, $b \neq 0$,
  3. (to hlavní) kdykoli $a, b \in R$, $b \neq 0$, tak existují $r, s \in R$, že $\phi(s) < \phi(b)$ a $a = br + s$.

Pokud je okruh R euklidovský, tak funguje Euklidův algoritmus, všechny ireducibilní prvky jsou prvočinitelé a každý prvek $r \in R \setminus \{0\}$ lze psát jako součin prvočinitelů jednoznačně až na pořadí a asociovanost. (Obrácená implikace ale neplatí.)

Příklad 1 (opakování)**.** Dokažte, že $13|2^{70} + 3^{70}$.

Příklad 2. Okruh $\mathbb{R}[x]$ je euklidovský. Pomocí Euklidova algoritmu najděte největšího společného dělitele polynomů:

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

Příklad 3. Rozložte v $\mathbb{R}[x]$ na součin prvočinitelů:

1. $x^2 - 3x + 2$

2. $x^3 + x$

3. $x^4 - 2x^2 + 1$

Příklad 4. Buď R obor integrity. Dokažte, že a, b jsou asociované právě tehdy když existuje invertibilní $r \in R$, že $a = rb$. Co to znamená pro $R = \mathbb{Z}$ a $R = \mathbb{R}[x]$?

Příklad 5. Množina $2\mathbb{Z}$ není okruh (nemá jednotku), ale můžeme na ní definovat dělitelnost. Popište ireducibiliní prvky a prvočinitele $2\mathbb{Z}$ a najděte na $2\mathbb{Z}$ prvek, který nemá jednoznačný rozklad na prvočinitele.

Příklad 6. Dokažte, že $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ je euklidovský obor integrity.

Příklad 7. Dokažte, že v okruhu $\{a + \sqrt{5}b : a, b \in \mathbb{Z}\}$ existuje ireducibilní prvek, který není prvočinitel.

Příklad 8. Buď $p > 2$ prvočíslo. Dokažte, že p dělí čitatele zlomku

$$1 + 1/2 + \cdots + 1/(p-1).$$