1. cvičení (22. 2. 2007)

Co jsme dělali?

Řekli jsme si, co je to okruh, obor a ideál. Pak jsme si taky připomněli definici dělitelnosti, největšího společného dělitele a nejmenšího společného násobku, větu o dělení se zbytkem a Euklidův algoritmus. No a taky definici prvočísla a tvrzení, že prvočísel je nekonečně mnoho a že každé přirozené číslo jde vyjádřit (až na pořadí) jednoznačně jako součin prvočísel.

Dále Bezoutovu větu, podle níž pro každá a, b existují x a y taková, že $(a,b) = ax + by$, a taky postup, jak tato x a y najít za pomoci Euklidova algoritmu. A nezapomněli jsme ani na tvrzení, že $n \cdot D = a \cdot b$, kde n je nejmenší společný dělitel čísel a, b a D jejich nejmenší společný násobek.

A na závěr jsme se věnovali cyklickým grupám. Nejprve jsme popsali ideály okruhu celých čísel $\mathbb{Z}$ a pak jsme dokázali, že každá cyklická grupa je isomorfní buďto $\mathbb{Z}$ nebo $\mathbb{Z}_n$ (oddíly 2.1 a 2.2 ve skriptech docenta Drápala).

Příklady

0. Spočti $(84, 33)$ a najdi $x, y \in \mathbb{Z}$ taková, že $(84, 33) = 84x + 33y$.

1. Spočti $(168, 238)$ a najdi $x, y \in \mathbb{Z}$ taková, že $(168, 238) = 168x + 238y$.

2. Urči, kolik má cyklická grupa $\mathbb{Z}$ (respektive $\mathbb{Z}_5$, $\mathbb{Z}_6$) generátorů. (Která čísla jsou generátory $\mathbb{Z}_n$ obecně?)

3. Pro každé $n > 2$ existuje prvočíslo, které leží mezi n a $n!$.

4. Najdi všechna $n \in \mathbb{N}$ taková, že mezi čísly $n+1, n+2, \ldots, n+10$ je největší možný počet prvočísel.

5. Spočti $(2^{63} - 1, 2^{98} - 1)$.

6. Pro která n platí $n + 1 | n^2 + 1$?

7. Existuje nekonečně mnoho prvočísel tvaru $3k + 2$.

Těžší příklady

1. Existuje nekonečně mnoho n takových, že $n | 2^n + 1$.

2. Pro každé liché k a přirozené n platí $2^{n+2} | k^{2^n} - 1$.

3. Kolik je $(2^{2^n} + 1, 2^{2^m} + 1)$?

4. Najdi všechny trojice po sobě jdoucích přirozených čísel, z nichž každé je (aspoň první) mocninou prvočísla.

5. Pro každé $k > 1$ existuje nekonečně mnoho n takových, že $2^{2^n} + k$ je složené číslo. Jak je tomu pro $k = 1$?