1. přednáška a cvičení (24. února 2009)

Co jsme dělali na přednášce?

Sekce 2.1, 2.3 a 2.4 ze skript.

Co jsme dělali na cvičení?

Připomněli jsme si, že násobení prvkem a nesoudělným s n je automorfismus grupy $\mathbb{Z}_n$. Tento fakt má řadu využití při počítání s kongruencemi.

Také jsme se zabývali grupou $\mathbb{Z}_n^*$. Je to vskutku grupa, tedy například pro každé $a \in \mathbb{Z}_n^*$ existuje právě jedno $b \in \mathbb{Z}_n^*$ takové, že $ab = 1$. Toto b často značíme a^{-1} nebo $\frac{1}{a}$.

A na závěr jsme počítali NSD nejrůznějších čísel (vyjádřených obecně).

Příklady

-1. Dokaž malou Fermatovu větu, neboli tvrzení, že $a^{p-1} \equiv 1 \pmod{p}$ pro prvočíslo p, $p \nmid a$.

0. V závislosti na $k, l \in \mathbb{Z}$ urči $(2kl, k^2 + l^2)$.

1. V závislosti na $k, l \in \mathbb{Z}, (k, l) = 1$ urči $(k - l, k^2 - kl + l^2)$.

2. Popiš všechny generátory grup $\mathbb{Z}, \mathbb{Z}_5, \mathbb{Z}_6$. Kolik jich je obecně?

3. Dokaž, že prvočíslo p dělí čitatele zlomku $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$.

4. V závislosti na $k, l \in \mathbb{Z}$ urči $(3kl, k^2 + l^2)$.

5. Dokaž, že 198 dělí $13^{62} + 29$.

6. V závislosti na $k, l \in \mathbb{Z}$ urči $(3k^2l, k^3 + l^3)$.

7. Ať je l liché číslo. Využitím automorfismu $\varphi_a : i \mapsto ia$ spočti $\sum_{i=0}^{l-1} i \pmod{l}$.

8. V závislosti na $k, l \in \mathbb{Z}, (k, l) = 1$ urči $(k^3 + k^2l - l^3, k^2 + l^2)$.

9. p^2 dělí čitatele zlomku $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ ($p \geq 5$ je prvočíslo).