

## 1. proseminář (20. února 2007)

### Co jsme dělali?

Tento proseminář se moc nepovedl a přišlo na něj celkem málo lidí, takže jsme na něj později téměř nenavazovali.

Definici dělitelnosti, největšího společného dělitele a nejmenšího společného násobku, větu o dělení se zbytkem a Euklidův algoritmus.

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.

### Příklady

0. Spočti (14, 35).

1. Pro která  $n$   $n + 1 \mid n^2 + 1$ ?

2. Součet čtverců (druhých mocnin) dvou po sobě jdoucích přirozených čísel dává zbytek 1 po dělení 4.

3. Spočti (252, 180). Najdi  $x, y$  tak, aby  $(252, 180) = 252x + 180y$ .

4. V závislosti na  $n$  urči  $(2n - 1, 9n + 4)$ .

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

6. Pro každé prvočíslo  $p$  a přirozené číslo  $k \in \{1, 2, 3, \dots, p - 1\}$  platí  $p \mid \binom{p}{k}$ .

7. Pro všechna  $a, b, c, d \in \mathbb{Z}$ ,  $a \neq c$  platí  $a - c \mid ab + cd$  právě tehdy, když  $a - c \mid ad + bc$ .

8. Spočti  $(2^{63} - 1, 2^{98} - 1)$ .

9. Každé přirozené  $n > 6$  jde napsat jako součet dvou nesoudělných čísel (různých od 1).

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

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

### Těžší příklady

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

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

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  $k = 1$ ?