Cvičení 23. 2. 2012

Vzpomeňte si, že každé nenulové celé číslo lze (až na pořadí prvočísel jednoznačně) psát ve tvaru $\pm p_1^{a_1} \dots p_k^{a_k}$, kde $p_1, \dots, p_k$ jsou různá prvočísla. Zápis (m, n) značí největšího společného dělitele čísel m, n (pro dnešek uvažujeme $m, n \in \mathbb{Z} \setminus \{0\}$, tam NSD vždy existuje a je určen jednoznačně až na znaménko).

Platí věta (Bezoutova), že pro $m, n \in \mathbb{Z}$ vždy existují $x, y \in \mathbb{Z}$, že $mx + ny = (m, n)$. Přitom čísla x, y lze najít Euklidovým algoritmem (zhruba: dělíme se zbytkem, dokud to jde).

Cyklická grupa je grupa generovaná jedním prvkem. Každá cyklická grupa je isomorfní celým číslům nebo $\mathbb{Z}_n$ pro nějaké n (speciálně je každá cyklická grupa komutativní).

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

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

Příklad 2. Určete, kolik existuje v grupě G prvků, které ji generují:

1. $G = \mathbb{Z}$
2. $G = \mathbb{Z}_5$
3. $G = \mathbb{Z}_6$
4. $G = \mathbb{Z}_{11}^\star$ (množina $\{1, \dots, 10\}$ s násobením modulo 11)
5. $G = \mathbb{Z}_n$ pro obecné n

Příklad 3. Spočtěte poslední cifru čísla:

1. 2^{100}
2. $99^{98^{97}}$

Příklad 4. Dokažte, že pro každé $n > 2$ najdeme mezi n a $n!$ prvočíslo.

Příklad 5. Najděte všechna n taková, že počet prvočísel v množině

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

je maximální možný.

Příklad 6. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k + 2$.

Příklad 7 (pro pokročilé)**.** Dokažte, že existuje nekonečně mnoho n takových, že $n|2^n + 1$.