5. cvičení (24. března 2006)

Co jsme dělali?

Připomněli jsme si, že $a\mathbb{Z}_n = (n, a)\mathbb{Z}_n$. A také to, že grupa invertibilních prvků $\mathbb{Z}_p^*$, kde p je prvočíslo, je cyklická, a tedy například pro každé $a \in \mathbb{Z}_p^*$ existuje právě jedno $b \in \mathbb{Z}_p^*$ takové, že $ab = 1$. Toto b často značíme a^{-1} nebo $\frac{1}{a}$.

Také jsme definovali Eulerovu funkci $\varphi(n)$.

Příklady

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

0. Dokaž Malou Fermatovu větu: Pro prvočíslo p a celé číslo a nesoudělné s p platí $a^{p-1} \equiv 1 \pmod{p}$.

1. Dokaž Eulerovu větu: Pro přirozené číslo n a celé číslo a nesoudělné s n platí $a^{\varphi(n)} \equiv 1 \pmod{n}$.

2. Buď p prvočíslo, označme $M = \{1, 2, \ldots, p-1$. Spočti

$$\sum_{I \subseteq M} \prod_{i \in I} \frac{1}{i} \pmod{p}.$$

3. Dokaž, že $13 | 2^{70} + 3^{70}$.

4. Mějme různá prvočísla p a q. Dokaž, že $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

5. Pro složené číslo n platí $(n-1)! \equiv 0 \pmod{n}$.

6. Dokaž Wilsonovu větu: Pro prvočíslo p platí $(p-1)! \equiv -1 \pmod{p}$.

Těžší příklady

1. Každé prvočíslo $p > 5$ dělí nekonečně mnoho čísel tvaru $111 \ldots 1$.

2. Je-li $p > 5$ prvočíslo, má číslo $(p-1)!+1$ aspoň dva různé prvočíselné dělitele.

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

4. Ať je $n > 1$. Čísla n a $n+2$ jsou prvočíselná dvojčata (jsou obě prvočísla), právě když $4((n-1)!+1) + n \equiv 0 \pmod{n(n+2)}$.