6. cvičení (10. dubna 2008)

Co jsme dělali?

Pověděli jsme si, jak funguje Fermatův a Rabin-Millerův test prvočíselnosti a co to je (silné) pseoudoprvočíslo v nějaké bázi. Také jsme si připomněli, jak funguje systém RSA.

Příklady

1. Najdi všechna $a \in \mathbb{Z}$ taková, že N je silné pseudoprvočíslo v bázi a, kde a) $N = 15$, b) $N = 9$.

2. Dokaž, že $561 = 3 \cdot 11 \cdot 17$ je Carmichaelovo číslo.

3. Můj modul pro RSA je 33, veřejný klíč je 7. Přišla mi zakódovaná zpráva 1, 2, 27, 10. Dekóduj ji.

4. Dokaž, že 49 je silné pseudoprvočíslo v bázi a pro nějaké $a \not\equiv \pm 1 \pmod{49}$.

5. Ať jsou $p \neq q$ prvočísla. Dokaž, že pq není Carmichaelovo číslo.

6. Dokaž, že $N = 2^{2k+1} + 1$, $k \in \mathbb{N}$, je silné pseudoprvočíslo v bázi a právě tehdy, když $a \equiv \pm 1 \pmod{N}$

7. Najdi nejmenší N, které je silné pseudoprvočíslo v bázi a pro nějaké $a \not\equiv \pm 1 \pmod{N}$.

8. Ať $(\varphi(N), N - 1) = 2$. Je možné, aby N bylo silné pseudoprvočíslo v bázi a pro nějaké $a \not\equiv \pm 1 \pmod{N}$?