Cvičení 24. 5. 2013

Ukážeme si, jak určit d ze znalosti (e, N) pokud N je součinem dvou podobně velkých prvočísel a tajný exponent je malý, konkrétně $0 < d < \frac{1}{3}N^{1/4}$ (útok pochází od M. Wienera).

Věta 1 (Legendre, 1798)**.** Nechť $a, b, c, d \in \mathbb{N}$ jsou taková, že

$$\left|\frac{a}{b} - \frac{c}{d}\right| < \frac{1}{2d^2}.$$

Potom zlomek $\frac{c}{d}$ je některý z konvergentů řetězového zlomku pro a/b (viz demonstrace na tabuli).

Pro nás bude dnes důležité, že konvergenty řetězového zlomku pro a/b se dají snadno spočítat a je jich řádově $\log_2 b$.

Víme, že existuje k, že $ed - k\varphi(N) = 1$ v $\mathbb{Z}$. Budeme předpokládat:

- $N = pq$ pro $q < p < 2q$
- $0 < e < \varphi(N)$
- $0 < d < \frac{1}{3}N^{1/4}$

Příklad 1. Dokažte, že $|N - \varphi(N)| < 3\sqrt{N}$.

Příklad 2. Dokažte, že

$$\left|\frac{e}{N} - \frac{k}{d}\right| \leq \frac{3k}{d\sqrt{N}}.$$

Příklad 3. Dokažte, že

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Příklad 4. Ukažte, jak z předchozího příkladu a Legendreovy věty efektivně spočíst d.

Příklad 5. Zjistěte d, pokud znáte $e = 7915$, $N = 12091$ a víte, že N je součinem dvou podobně velkých prvočísel a $d < 1/3\sqrt[4]{N}$. Postup: Najděte řetězový zlomek pro e/N, jeden z konvergentů bude mít tvar k/d, kde platí $ed - k\varphi(N) = 1$. Potom je třeba testovat, které z nalezených d skutečně funguje.