

## Cvičení 17. 5. 2012

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). Budeme potřebovat teorii kolem řetězových zlomků, kterou vybudujeme až příští hodinu.

**Věta 1** (Legendre, 1798). Necht'  $a, b, c, d \in \mathbb{N}$  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 konvergency řetězového zlomku pro  $a/b$  se dají snadno spočítat a je jich řádově  $\log_2 b$ .

Víme, že existuje  $k$ , že  $ed - k\varphi(N) = 1 \text{ v } \mathbb{Z}$ . 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 spočítat  $d$ .