Pravděpodobnostní algoritmy

Přiblížili jsme si elementární základy zachycené v sekci 10.4., ilustrované na problému prvočíselnosti. Uvědomili jsme si, že algoritmus

> *Máš-li testovat prvočíselnost zadaného (např. několikasetmístného) k, projdi všechna $a, 1 < a < k$, a zjišťuj, zda Divides(a, k) (tedy zda $(k \mod a) = 0$) ...*

je exponenciální (ve velikosti zápisu k). (A to i při přímočarých vylepšeních, při nichž zkoumáme jen lichá $a \leq \sqrt{k}$ apod.)
Také jsme si všimli, že pravděpodobnostní algoritmus

> *Vygeneruj náhodné a (řekněme liché $a, 1 < a \leq \sqrt{k}$); jestliže Divides(a, k), return NE, jinak return ANO.*

nám moc nepomůže. (Např. pro velké číslo $m = pq$, kde p, q jsou prvočísla, je náhodná trefa jednoho z dělitelů p, q téměř nemožná.)
Pak jsme naznačili, že (malá) Fermatova věta je základem podstatně lepšího algoritmu.

Šifrovací systém s veřejným klíčem; RSA

(Mj. motivace zkoumání problému prvočíselnosti.)

Algoritmus vytvoření soukromého a veřejného klíče:

1. Vygeneruj dvě náhodná různá (velká, např. 200-místná) prvočísla p, q.
2. Spočítej součiny $n = pq$ a $\Phi(n) = (p-1)(q-1)$.
3. Urči (malé) e tž. $\gcd(e, \Phi(n)) = 1$ (gcd označuje největší společný dělitel).
4. Vypočti d tž. $de \equiv 1 \pmod{\Phi(n)}$.
5. Zveřejni dvojici (e, n); šifrovací funkce je $enc(m) = m^e \bmod n$.
6. Drž v tajnosti (d, n); dešifrovací funkce je $dec(m) = m^d \bmod n$.

Randomizovaný komunikační protokol ("fingerprinting")

Diskutovali jsme následující protokol mající za úkol prověřit, zda obsah jisté databáze velikosti např. 10^{16} bitů uložené na počítači $C1$ (např. v USA) je stejný jako u její kopie udržované na počítači $C2$ (např. v Evropě).

- Obsah databáze na C_1 je $x = b_1 b_2 \ldots b_n$, kde b_i jsou bity (prvky množiny $\{0, 1\}$); máme zajištěno, že vždy platí $b_1 = 1$.
- C_1 zvolí náhodné prvočíslo p z množiny $\{2, 3, \ldots, n^2\}$.
- C_1 pak spočte $s = \mathit{Number}(x) \bmod p$ (kde $\mathit{Number}(x)$ je číslo s binárním zápisem x, tedy $b_1 b_2 \ldots b_n$).
- C_1 pošle dvojici (p, s) počítači C_2.
- C_2 spočte $q = \mathit{Number}(y) \bmod p$ pro svůj obsah databáze y. Jestliže $s = q$, pak C_2 sdělí "OK, naše kopie jsou stejné", a jinak C_2 sdělí "Pozor! Naše kopie jsou různé!".