Týden 14

Přednáška

Pravděpodobnostní algoritmy

Přiblížili jsme si elementární základy zachycené v sekci 10.4.
Speciálně jsme se věnovali 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. Vydá-li (nějaký) jeho běh NE, tak sice víme jistě, že k není prvočíslo, ale vydá-li ANO pro dané k třeba při miliónkrát opakovaném provedení, nemůžeme si vůbec být jisti, že k je prvočíslem. (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 (k čemuž se ještě vrátíme na cvičení).

Šifrovací systém s veřejným klíčem; RSA

Probrali jsme RSA algoritmus zachycený následujícím schématem a diskutovali jsme jednotlivé kroky, korektnost algoritmu, atd.

1. Zvol 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 $x = b_1 b_2 \dots b_n$, 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 $\{2, 3, \dots, n^2\}$.
- C_1 pak spočte $s = Number(x) \bmod p$ (kde $Number(x)$ je číslo s binárním zápisem x, tedy $b_1 b_2 \dots b_n$).
- C_1 pošle dvojici (p, s) počítači C_2.
- C_2 spočte $q = Number(y) \bmod p$ 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!".

Partie textu k prostudování

Část 10.4. (pravděpodobnostní algoritmy).

Cvičení

Příklad 14.1

Je prostor k diskusi zápočtové písemky z minulého týdne. Příští týden proběhne prověření referátů, takže teď je i poslední možnost na cvičení zkonzultovat případné nejasnosti z učiva semestru, které bude prověřovat zkouška.

Příklad 14.2

Následující tvrzení je známo jako „Malá Fermatova věta“.
Tvrzení. Jestliže p je prvočíslo, tak pro každé $a, 0 < a < p$, platí

$$a^{p-1} \equiv 1 \pmod p$$

.

(Když p není prvočíslo, tak to neplatí, jak byste se měli být schopni sami snadno přesvědčit.)
Přesvědčte se, že tvrzení platí pro $p = 11$. Přitom si uvědomte, jak je užitečné tzv. opakované umocňování. Můžete postupovat vyplněním následující tabulky; přitom využijte, že $x^{10} = x^8 \cdot x^2$, tedy $x^{10} \mod 11 = (x^8 \mod 11) \cdot (x^2 \mod 11) \mod 11$.

x	x^2 mod 11	x^4 mod 11	x^8 mod 11	x^{10} mod 11
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Pak vyplňte podobnou tabulku pro neprvočíslo 15.

x	x^2 mod 15	x^4 mod 15	x^8 mod 15	x^{14} mod 15
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				

Uvedená pozorování nabízejí zvážit jistý (polynomiální) pravděpodobnostní algoritmus k testování prvočíselnosti (velkých čísel). Jak vypadá tento algoritmus?

(Poznámka. Ten algoritmus „téměř“ funguje, „ošálí“ jej ale tzv. Carmichaelova čísla; naprosto korektní pravděpodobnostní algoritmus využívá o něco hlubší poznatky z teorie čísel.)

(Další příklady jsou nepovinné.)

Příklad 14.3

Jedním krokem v RSA algoritmu je “Spočítej součiny $n = pq$ a $\Phi(n) = (p-1)(q-1)$”. Pro (extrémně malá) $p = 3$, $q = 5$ bychom měli $n = 15$ a $\Phi(n) = 8$. Zjistěte počet čísel z množiny $\{1, 2, \ldots, 15\}$, která jsou nesoudělná s 15 (největší společný dělitel takového čísla a čísla 15 je 1). Ověřte také, že tato čísla vytvářejí grupu vzhledem k násobení modulo 15. Umíte teď vysvětlit, co je uvedené $\Phi(pq) = (p-1)(q-1)$ pro obecná prvočísla p, q ?

Příklad 14.4

Připomeňte si randomizovaný protokol z přednášky.
- Kvalifikovaně odhadněte počet bitů v binárních prezentacích p a s a porovnejte praktický úkol komunikace (zaslání přes oceán) čísel p, s s úkolem zaslání celého obsahu $x = b_1 b_2 \ldots b_n$.
- Vysvětlete, proč je operace zvolení náhodného prvočísla p (a vypočtení s) na současných počítačích zvládnutelné.
Pomůže vám připomenutí toho, co je známo o "hustotě prvočísel": když $\pi(n)$ označuje počet prvočísel v intervalu $[1 \ldots n]$, tak

$$\frac{\pi(n)}{n} \doteq \frac{1}{\ln n}$$

- Charakterizujte situaci, kdy se protokol mýlí.
- Odhadněte seshora počet prvočísel ve faktorizaci čísla $|Number(x) - Number(y)|$.
- Vyvoďte omezení pro pravděpodobnost, že se protokol mýlí, v případě obecného n a pro konkrétní $n = 10^{16}$.