Kriptografija in računalniška varnost – 2. domača naloga (do srede 25. nov., 2009)

---

1. Naj bodo a, b in n naravna števila za katere velja $b \leq a \leq n$.

   (a) Dokaži, da je časovna zahtevnost običajnega deljenja velikih števil pri katerem računamo števili q (kvocijent) in r (ostanek) za kateri velja

   $$a = qb + r, \quad 0 \leq r < b,$$

   $\mathcal{O}((\log_2 b)(\log_2 q)$ bitnih operacij.

   Spomnimo se, da pri Evklidovem algoritmu za računanje največjega skupnega delitelja $D(a, b)$ števil a in b najprej delimo a z b. Če je ostanek enak 0, potem je $D(a, b) = b$, sicer pa delimo zadnji delitelj z zadnjim ostankom in to ponavljamo vse dokler ne pridemo do ostanka 0. Potem je zadnji od nič različen ostanek največji skupni delitelj števil a in b. Ta proces lahko predstavimo z naslednjimi enačbami

   $$\begin{aligned}
   a &= q_1 b + r_1, \quad 0 < r_1 < b, \\
   b &= q_2 r_1 + r_2, \quad 0 < r_2 < r_1, \\
   r_1 &= q_3 r_2 + r_3, \quad 0 < r_3 < r_2, \\
   &\vdots \\
   r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}, \quad 0 < r_{k-1} < r_{k-2}, \\
   r_{k-2} &= q_k r_{k-1} + r_k, \quad 0 < r_k < r_{k-1}, \\
   r_{k-1} &= q_{k+1} r_k + 0
   \end{aligned}$$

   in je $D(a, b) = r_k$.

   (b) Dokaži, da je $r_{i+2} < \frac{1}{2} r_i$ za vsak $1 \leq i \leq k - 2$.

   (c) Iz (b) izpelji, da je časovna zahtevnost Evklidovega algoritma $\mathcal{O}((\log_2 n)^3)$ bitnih operacij.

2. (a) Za število a in zaporedje $q_1, \ldots, q_{k+1}$ iz 1. naloge dokaži, da velja $\Pi_{i=1}^{k+1} q_i \leq a$.

   (b) Dokaži, da je časovna zahtevnost Evklidovega algoritma $\mathcal{O}((\log_2 n)^2)$ bitnih operacij (to je seveda boljša ocena kot v 1. nalogi).

3. (a) Naj bo $n = pq$, kjer sta p in q različni lihi praštevili in $ed \equiv 1 (\text{mod } \varphi(n))$. RSA enkripcijska funkcija je $E(x) = x^e \bmod n$, RSA dekripcijska funkcija pa je $D(x) = x^d \bmod n$. Na predavanjih smo se prepričali, da je $D(E(x)) = x$ za $x \in \mathbb{Z}_n^*$. Pokaži, da ista trditev velja za vsak $x \in \mathbb{Z}_n$.

   (b) Dokaži, da imamo pri poljubnem RSA sistemu vsaj 9 čistopisov za katere je $E_k(M) = M$.

4. Spomnimo se naslednjih lastnosti Legendrovega simbola. Če p sta q lihi praštevili, potem je

(A) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

(B) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

(C) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$

Naj bo $n \geq 3$ liho naravno število.

(a) Pokaži, da za lihi naravni števili n_1 in n_2 velja

$$\frac{n_1 n_2 - 1}{2} \equiv \frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \pmod 2.$$

Od tod izpelji $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

(b) Pokaži, da za lihi naravni števili n_1 in n_2 velja

$$\frac{n_1^2 n_2^2 - 1}{8} \equiv \frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \pmod 2.$$

Od tod izpelji $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

(c) Pokaži, da za liho naravno število $a \geq 3$, velja $\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{(a-1)(n-1)/4}$.

(d) S pomočjo lastnosti Jacobijevih simbolov izračunaj $\left(\frac{43691}{65537}\right)$.