Kriptografija in teorija kodiranja – 1. domača naloga (do torka 3. marca, 2008)

1. Naj bosta a in b naravni števili in $a \geq b$. Dokaži, da je časovna zahtevnost običajnega deljenja velikih števil pri katerem računamo števili q (kvocient) in r (ostanek) za kateri velja

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

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

2. Naj bodo a, b in n naravna števila za katere velja $b \leq a \leq n$. 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 $D(a, b) = r_k$.

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

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

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

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