# Kriptografija in teorija kodiranja – 1. domača naloga

(do torka, 23. marca 2010 – oddaja v asistentov predalček na Jadranski 21)

**Naloge rešujte samostojno. Odgovori in rešitve naj bodo jasne, pregledne in dobro utemeljene!**

1. **Analiza časovne zahtevnosti Evklidovega algoritma.**

   (a) 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.

   (b) 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 $D(a, b) = r_k$. Dokaži, da je $r_{i+2} < \frac{1}{2} r_i$ za vsak $1 \leq i \leq k - 2$ (od tod se hitro izpelje, da je časovna zahtevnost Evklidovega algoritma največ $\mathcal{O}((\log_2 n)^3)$ bitnih operacij).

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

   (d) Dokaži, da je časovna zahtevnost Evklidovega algoritma $\mathcal{O}((\log_2 n)^2)$ bitnih operacij.

2. **RSA sistem.**

   (a) Dokaži, da sta šifriranje in odšifriranje inverzni operaciji. (tj. $(x^e)^d \equiv x \pmod{n}$ za vsak $x \in \mathbb{Z}_n$). Opozorilo: pazi na $x \in \mathbb{Z}_n \backslash \mathbb{Z}_n^*$.

   (b) Dokaži, da imamo vedno vsaj 9 čistopisov za katere je $E_k(M) = M$.

3. **Jacobijevi simboli.**

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

(i) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, (ii) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, (iii) $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$.

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 $\left(\frac{43691}{65537}\right)$.

4. **Mali Fermatov izrek in testiranje praštevilskosti.**

(a) Naj bo $p$ liho praštevilo in $n$ naravno število. Dokaži, da je število rešitev enačbe

$$x^a \equiv 1 \pmod p$$

v $\mathbb{Z}_p$ enako $D(a, p-1)$.

(b) Naj bosta $p$, $q$ lihi praštevili in $n = pq$. Naj bo $f(x)$ polinom s celoštevilčnimi koeficienti. Naj bo $S_n$ (zaporedoma $S_p$ in $S_q$) množica rešitev iz $\mathbb{Z}_n$ (zaporedoma $\mathbb{Z}_p$, $\mathbb{Z}_q$) enačbe $f(x) \equiv 0 \pmod n$ (zaporedoma $\pmod p$, $\pmod q$)).
Dokaži $|S_n| = |S_p| \cdot |S_q|$.

(c) Naj bo $n = pq$ produkt dveh lihih različnih praštevili in $n = pq$ in naj bo $1 \leq a \leq n-1$. Če je $a^{n-1} \not\equiv 1 \pmod n$, potem imenujemo $a$ **Frematova priča** za $n$, sicer pa mu pravimo **Frematov lažnjivec** za $n$. Poišči formulo za število Frematovih lažnjivcev za $n$.

(d) Naj bo $n = 624142660586694101446291308147581805825611279851037995772020202145871$. Preveri ali $n$ je ali ni praštevilo (lahko uporabiš MAPLE/MATEMATICA). Dokaži svoj odgovor in opiši kako bi lahko jaz (zlahka) preveril tvoj dokaz. Kopijo števila $n$ boste našli na domači strani.