Tietojenkäsittelyteoria, kevät 2000
Harjoitus 9, to 23.3. klo 10–12 sali MaD381

1. Osoita, että universaalihajautusta käytettäessä minkä tahansa avaimen x kanssa törmäävien muiden avainten $y \neq x$ määrän odotusarvo on alle 1.

2. Hajautin $h : [N] \to [m]$ on *täydellinen* joukolle $S \subseteq [N]$, jos kaikilla $x, y \in S$, $x \neq y$, on $h(x) \neq h(y)$. Osoita, että jos $S \subseteq [N]$, $|S| = n$, on esitettävien avainten joukko ja hajautin $h : [N] \to [m]$ valitaan satunnaisesti jostakin universaalista hajautinperheestä, niin todennäköisyys että h on itse asiassa täydellinen joukolle S on vähintään $(1 - n^2/m)$.

3. Testaa ainakin 75% varmuudella onko 103 alkuluku, käyttäen (a) Solovayn–Strassenin, (b) Millerin–Rabinin algoritmia.

4. Toinen seuraavista tehtävistä:

   (a) Osoita, että jos $n > 2$ on pariton yhdistetty luku, niin todennäköisyys että Solovayn–Strassenin testi kelpuuttaa sen "mahdollisena alkulukuna" on alle 1/2.

   (b) Osoita, että jos $n > 4$ on pariton yhdistetty luku, niin todennäköisyys että Millerin–Rabinin testi kelpuuttaa sen "mahdollisena alkulukuna" on alle 1/2.

   (Kirjallisuuden käyttö tämän tehtävän apuna on sallittua ja suotavaa. Molempia testejä käsitellään ainakin teoksissa Knuth, *Seminumerical Algorithms* ja von zur Gathen & Gerhard, *Modern Computer Algebra.* Solovayn–Strassenin testin oikeellisuustodistus, joka on helpompi, löytyy useista muistakin lähteistä, esim. Motwani & Raghavan, *Randomized Algorithms* ja Salomaa, *Public Key Cryptography.*)

5. Osoita, että jos NP $\subseteq$ BPP, niin NP = R. (*Vihje:* SATin totuusarvoasetuksen oikeellisuuden voi tarkastaa.)

Huom.: Yliopiston rehtorinvaalin takia kurssilla ei ole luentoa torstaina 23.3.