Algoritmien teoria, kevät 1999

Harjoitus 8, 15.3. klo 10–12 sali MaD380

1. Osoita, että jos $p > 2$ on alkuluku, niin kaikilla a, $1 \leq a < p$, on voimassa $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. (Vrt. luentomuistiinpanojen s. 222.) Käytä hyväksesi seuraavia algebrallisia perustietoja:
   (a) Jos p on alkuluku, niin nollasta poikkeavien kokonaislukujen mod p muodostama ryhmä $\mathcal{Z}_p^* = (\mathcal{Z}_p \setminus \{0\}, \cdot)$ on syklinen, so. jollakin alkiolla $g \in \mathcal{Z}_p^*$ on $\mathcal{Z}_p^* = \{g^k \pmod{p} \mid k \geq 0\}$.
   (b) Kaikilla a, $1 \leq a < p$, on $a^{p-1} \equiv 1 \pmod{p}$ (ns. Fermat'n pieni lause).

2. Testaa luennolla (s. 225) esitetyllä Solovayn–Strassenin algoritmilla ainakin 75% varmuudella, onko 103 alkuluku. (*Huom:* Luentomuistiinpanoissa on valitettavasti virhe s. 224 kohdassa (d): Gaussin resiprookkilause t. "neliönjäännösten käännösyhtälö" pätee vain, kun Jacobin symbolissa $\left(\frac{y}{x}\right)$ luvut y ja x ovat parittomia ja keskenään jaottomia. Jos symbolin "osoittaja" y on parillinen, voidaan sen sijaan soveltaa symbolin multiplikatiivisuuteen perustuvaa sääntöä $\left(\frac{2z}{x}\right) = \left(\frac{2}{x}\right)\left(\frac{z}{x}\right)$.)

3. Johda luentomuistiinpanojen s. 233 esitetty, simuloidun jäähdytyksen asymptoottista konvergenssia kun $T \to 0$ koskeva Seurauslause 2 samalla sivulla esitetystä, algoritmin käyttäytymistä vakiolämpötilassa $T > 0$ koskevasta Lauseesta 1.

4. Tarkastellaan seuraavaa yksinkertaista "säämallia". Säätila annettuna päivänä voi olla joko aurinkoinen (a), pilvinen (p) tai sateinen (s). Seuraavan päivän säätilan todennäköisyysjakauma riippuu edellisen päivän säätilasta seuraavan siirtymämatriisin esittämällä tavalla (rivi-indeksi kuvaa päivän t, sarakeindeksi päivän $t + 1$ säätilaa):

	a	p	s
a	0.5	0.5	0
p	0.5	0.25	0.25
s	0	0.5	0.5

   Totea, että matriisin määrittelemällä "sääprosessilla" on tasapainojakauma, ja määritä se.

5. Hahmottele simuloitua jäähdytystä käyttävä ratkaisumenetelmä NP-täydelliselle solmupeiteongelmalle (engl. VERTEX COVER; luentomuistiinpanojen s. 117). Valitse sopiva kustannusfunktio ja naapurustorakenne. Varmista, että osaat tuottaa annetun kelvollisen ratkaisun satunnaisia naapuriratkaisuja tasaisen jakauman mukaan. Minkälaista jäähdytysaikataulua ongelman ratkaisemiseen n solmun verkossa tulisi käyttää luennolla esitetyn konvergenssilauseen 3 (s. 244) mukaan?