LUKUTEORIA A

2. Välikoe 23.11.2009 (T. Matala-aho)

EI LASKIMIA, EI PUHELIMIA

1. Olkoon $n = 1105$. Tiedetään, että $n - 1 = 2^4 \cdot 69$ ja

$$2^{2^3 \cdot 69} \equiv 1 \pmod{n}; \quad 2^{2^2 \cdot 69} \equiv 781 \pmod{n}.$$

a) Onko n pseudoalkuluku kannan 2 suhteen?

b) Onko n vahva pseudoalkuluku kannan 2 suhteen?
(Lyhyet perustelut määritelmistä lähtien.)

2. Olkoon $p, q \in \mathbb{P}_{\geq 3}$ ja $q | 2^p - 1$. Näytä, että

$$q = 2kp + 1, \quad \text{jollakin} \quad k \in \mathbb{Z}^+.$$

3. a) Olkoon $q \in \mathbb{P}_{\geq 5}$ ja

$$\left(\frac{3}{q}\right) = -1.$$

Määrää kunnan $\mathbb{Z}_q[\sqrt{3}]$ alkioiden lukumäärä ja alkion $1 + \sqrt{3}$ käänteisalkio.

b) Määrää Dirichlet'n karakteerit (mod 5).

4. Olkoot $p \in \mathbb{P}_{\geq 3}$, $a \in \mathbb{Z}$, $p \nmid a$ sekä

$$R_a = \{r_k | 1 \leq r_k \leq p - 1,\ r_k \equiv ak \pmod{p},\ \ 1 \leq k \leq (p-1)/2\};$$

$$I_a = \{r_k \in R_a |\ (p+1)/2 \leq r_k \leq p - 1\}, \quad s = \# I_a.$$

Osoita, että tällöin

$$\left(\frac{a}{p}\right) = (-1)^s.$$