802328A LUKUTEORIAN PERUSTEET (5 op)

1. välikoe 26.11.2012 EI LASKIMIA

1. a) Millä luvuilla $n = 2, 3, 4, 5, 6, 7$ pätee

$$\frac{1}{13} \equiv \frac{2}{5} \pmod{n}.$$

b) Näytä, että

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \quad \forall x, y \in \mathbb{R}.$$

2. Määrää alkion $\overline{h} \in \mathbb{Z}_n^*$ käänteisalkio $\overline{h}^{\,-1} \in \mathbb{Z}_n^*$ muodossa $\overline{h}^{\,-1} = \overline{k}$, missä $k \in \{1, 2, ..., n-1\}$, kun
a) $h = 5, \quad n = 101.$
b) $h = 5, \quad n = p \in \mathbb{P}, \quad p \equiv 4 \pmod 5.$

3. Olkoot $p, q \in \mathbb{P}$, $p \neq q$. Todista, että

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

4. a) Olkoon $p \in \mathbb{P}$. Näytä, että

$$p \,\Big|\, \binom{p}{k} \qquad \forall \quad 1 \leq k \leq p-1.$$

b) Olkoon $p \in \mathbb{P}_{\geq 5}$. Todista, että

$$3 || 2^p + 1.$$