LUKUTEORIA A

1. Välikoe 19.10.2009 (T. Matala-aho)

EI LASKIMIA, EI PUHELIMIA

1. Tarkastellaan ryhmää $\mathbb{Z}_{13}^*$.

   a) määrää alkioiden kertaluvut.

   b) määrää alkioiden yhden alkion generoimat aliryhmät.

   c) määrää ryhmän generaattorit.

   d) määrää neliöt ja epäneliöt.

   e) määrää alkioiden Legendren symbolit.

2. Olkoon $p \in \mathbb{P}_{\geq 3}$ ja $\mathbb{Z}_p^* = \langle \beta \rangle$.

   a) Määrää

$$\log_\beta -1.$$

   b) Olkoon $p \in \mathbb{P} \cap 4\mathbb{Z} + 1$. Ratkaise yhtälö

$$x^2 = -1 \in \mathbb{Z}_p^*.$$

3. Olkoon G ryhmä, $\tau \in G$. Todista, että tällöin

$$\text{ord } \tau = h \quad \Leftrightarrow \quad \tau^h = 1 \quad ja \quad \tau^{\frac{h}{p_i}} \neq 1, \ \forall p_i | h; \ p_i \in \mathbb{P}.$$

4. a) Määrää sellainen β, että

$$\langle \beta \rangle = \mathbb{Z}_{2 \cdot 13^k}^* \quad \forall \ k \in \mathbb{Z}^+.$$

   b) Olkoon $p \in \mathbb{P}$, $p \equiv 1 \pmod 4$ ja

$$\langle r \rangle = \mathbb{Z}_p^*.$$

   Osoita, että

$$\langle -r \rangle = \mathbb{Z}_p^*.$$