

1. Määää ryhmän \mathbb{Z}_{13}^* alkioiden Legendren symbolien arvot.

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

a) Määää

$$\log_{\beta}(-1).$$

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

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

3. Määää sellainen β , että

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

(Lyhyet perustelut.)

4. 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.)

5. Olkoot $n \in \mathbb{Z}^+$ ja

$$n - 1 = mj, \quad m = \prod_{i=1}^s p_i^{k_i}, \quad p_i \in \mathbb{P}, \quad m \perp j, \quad \sqrt{n} \leq m.$$

Oletetaan vielä, että jokaista $i = 1, \dots, s$ kohti on olemassa sellainen a_i , että

$$a_i^{n-1} \equiv 1 \pmod{n} \quad \text{ja} \quad \text{syt}(a_i^{\frac{n-1}{p_i}} - 1, n) = 1.$$

Osoita, että $n = p \in \mathbb{P}$.