

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

a) Määrää ryhmän generaattorit.

b) Ratkaise yhtälö $4x^9 = 7$.

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

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

3. Olkoon $p \in \mathbb{P}_{\geq 3}$. Osoita, että tällöin \mathbb{Z}_p^* on syklinen.

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. 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.