

1. Ratkaise yhtälöryhmä

$$\begin{cases} [x]_5 = [2]_5 \\ [x]_6 = [3]_6 \\ [x]_7 = [4]_7. \end{cases}$$

2. Ratkaise yhtälöryhmä

$$\begin{cases} [x]_5 = [4]_5 \\ [x]_7 = [1]_7 \\ [x]_9 = [3]_9 \\ [x]_{11} = [2]_{11}. \end{cases}$$

3. Olkoon p pariton alkuluku. Osoita, että -1 on neliönjäännös $(\text{mod } p)$ jos ja vain jos $p = 4n + 1$ jollakin $n \in \mathbb{N}$.

Seuraavien viiden tehtävän tavoitteena on vaiheittain osoittaa seuraava tulos:

Lause Olkoon $n \in \mathbb{N}$, $n \geq 2$. Tällöin on olemassa primitiivinen juuri modulo n täsmälleen silloin kun n on joko 2 , 4 , p^k tai $2p^k$, missä $k \in \mathbb{N}$, $k \geq 1$ ja p on pariton alkuluku.

4. Osoita ettei ole olemassa primitiivistä juurta $(\text{mod } mk)$, kun $m, k \in \mathbb{N}$ ovat siten, että $m, k \geq 3$ ja $\text{sy}(m, k) = 1$. (Vinkki: Sekä $\varphi(m)$ että $\varphi(k)$ ovat parillisia. Hyödynnä tätä tietoa ja käytä esimerkiksi kiinalaista jäännöslausetta.)
5. Todista ettei ole olemassa primitiivistä juurta $(\text{mod } 2^k)$, kun $k > 2$. (Vinkki: Todista induktiolla.)
6. Olkoon p pariton alkuluku. Todista että on olemassa primitiivinen juuri $(\text{mod } p^2)$. (Vinkki: Osoita, että joko a tai $a + p$ on etsitty primitiivinen juuri $(\text{mod } p^2)$, missä a on primitiivinen juuri $(\text{mod } p)$.)
7. Olkoon p pariton alkuluku ja $k \in \mathbb{N}$, $k \geq 3$. Todista että on olemassa primitiivinen juuri $(\text{mod } p^k)$. (Vinkki: Osoita induktiolla, että primitiivinen juuri $(\text{mod } p^2)$ on myös primitiivinen juuri $(\text{mod } p^k)$.)
8. Olkoon p pariton alkuluku ja $k \in \mathbb{N}$, $k \geq 1$. Olkoon lisäksi a primitiivinen juuri $(\text{mod } p^k)$. Osoita todeksi seuraavat väitteet.
- a) Jos a on pariton, on a primitiivinen juuri $(\text{mod } 2p^k)$.
 - b) Jos a on parillinen, on $a + p^k$ primitiivinen juuri $(\text{mod } 2p^k)$.