

1. Laske kertaluvut

a)  $\text{ord}_{25}(7)$

b)  $\text{ord}_{257}(11)$

2. Olkoon  $a, m \in \mathbb{Z}$ ,  $m > 0$ , siten, että  $\text{syte}(a, m) = 1$ . Osoita, että

$$\text{ord}_m(a) = \text{ord}_m(a'),$$

kun  $a'$  on luvun  $a$  käänteisluku kertolaskun suhteen modulo  $m$ .

3. Ratkaise yhtälöryhmä

$$\begin{cases} [x]_2 = [1]_2 \\ [x]_7 = [4]_7 \\ [x]_9 = [4]_9 \end{cases}$$

4. Laske Legendren symbolit

a)  $\left(\frac{30}{31}\right)$

b)  $\left(\frac{135}{149}\right)$

5. Minkä parittomien alkulukujen suhteen on luku 3 neliönjäännös?

6. Olkoon  $p$  alkuluku siten, että  $p \equiv 3 \pmod{4}$ . Osoita, että jokaiselle neliönjäännökselle  $a$  modulon  $p$  suhteen on yhtälöllä

$$x^2 \equiv a \pmod{p}$$

ratkaisuina täsmälleen  $x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}$ .

7. Ratkaise yhtälö

$$x^2 + 2x + 1 \equiv 0 \pmod{27}$$