

Lukuteoria
Harjoitus 13/2007

1. Etsi Lauseen 7.2.2 todistuksessa esiintyvät luvut $\pm x_1$ ja $\pm x_2$ kongruenssiyhtälön

$$x^2 \equiv 58 \pmod{77}$$

tapauksessa.

2. Ratkaise kongruenssiyhtälö

$$x^2 \equiv 58 \pmod{77}$$

ratkaisemalla neljä yhtälöparia Lauseen 7.2.2 todistuksen tapaan.

3. Luvun $n = 5095$ kanoninen esitys on muotoa $5095 = 5 \cdot 1019$. Etsi kongruenssille

$$x^2 \equiv 1 \pmod{5095}$$

ratkaisu, jolle pätee $x \not\equiv \pm 1 \pmod{5095}$.

4. Olkoon p alkuluku, jolle $p \equiv 3 \pmod{4}$ ja olkoon $q = 2p + 1$ alkuluku. Osoita, että tällöin $q \mid M_p$, missä M_p on Mersennen luku $M_p = 2^p - 1$. (Vihje! Määää Legendren symboli $\left[\frac{2}{q}\right]$ Eulerin kriteerin ja Seurauksen 7.3.2 avulla.)

5. Osoita Tehtävän 4 avulla, että $23 \mid M_{11}$, $47 \mid M_{23}$ ja $503 \mid M_{251}$.

6. Olkoon $p > 2$ alkuluku ja olkoon $a \in \mathbf{Z}$ siten, että $\text{syt}(a, p) = 1$. Jaetaan joukon $\{a, 2a, \dots, \left(\frac{p-1}{2}\right)a\}$ jakojäännökset modulo p kahteen osaan: Olkoot $u_1, \dots, u_s$ ne jäännökset, jotka ovat $> \frac{p}{2}$ ja olkoot $\{v_1, \dots, v_t\}$ ne jäännökset, jotka ovat $< \frac{p}{2}$. Osoita, että

$$\left\{1, \dots, \frac{p-1}{2}\right\} = \{p - u_1, \dots, p - u_s, v_1, \dots, v_t\}.$$

(Vihje! Riittää osoittaa, että joukon $\{p - u_1, \dots, p - u_s, v_1, \dots, v_t\}$ luvut ovat pareittain ei-kongruenteja modulo p .)

7. Osoita: Fermat'n luku $F_m = 2^{2^m} + 1$ on alkuluku, jos

$$3^{\frac{F_m-1}{2}} \equiv -1 \pmod{F_m}.$$

(Vihje! Ks. Lause 6.2.1.)