

Lukuteoria 2007
Kirjalliset tehtävät 2

6. Olkoon $n = p_1^{t_1} \cdots p_r^{t_r}$ parittoman luvun $n > 1$ kanoninen esitys ja olkoon $\text{sy}(a, n) = 1$. Osoita, että kongruenssilla

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

on ainakin yksi ratkaisu jos $\left[\frac{a}{p_i}\right] = 1$ kaikilla $i = 1, \dots, r$.

[Vihje! Käytä hyväksi Kirjallisten tehtävien 1 tehtävää 5 ja muodosta yhtälöryhmä vastaavaan tapaan kuin Lauseessa 7.2.2.]

7. Olkoon $n = pq$, missä p ja q ovat erilliset parittomat alkuluvut. Olkoon $\text{sy}(a, n) = 1$ siten, että $x_0^2 \equiv a \pmod{n}$ ja

$$\begin{aligned} x_0 &\equiv x_1 \pmod{p}, & 0 \leq x_1 \leq p, \\ x_0 &\equiv x_2 \pmod{q}, & 0 \leq x_2 \leq q. \end{aligned}$$

Osoita, että yhtälöparien

$$\begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv x_2 \pmod{q} \end{cases}$$

ja

$$\begin{cases} x \equiv x_1 \pmod{p} \\ x \equiv -x_2 \pmod{q} \end{cases}$$

ratkaisut ovat ei-kongruentit modulo n .

[Vihje! Tee antiteesi.]

8. Olkoot p ja $q = 4p + 1$ alkulukuja ja oletetaan, että $\left[\frac{a}{q}\right] = -1$. Osoita, että a on välttämättä primitiivijuuri modulo q jos $\text{ord}_q a \neq 4$.

[Vihje! Sulje pois "väärät" kertalukuehdokkaat, ks. Lemma 6.1.1.]

9. Osoita: Jos p on pariton alkuluku, niin

$$\left[\frac{-3}{p}\right] = \begin{cases} 1, & \text{kun } p \equiv 1 \pmod{6} \\ -1, & \text{kun } p \equiv -1 \pmod{6}. \end{cases}$$

[Vihje! Tarkastele kummassakin tilanteessa tapaukset $p \equiv 1 \pmod{4}$ ja $p \equiv 3 \pmod{4}$ erikseen määrittämällä kussakin tapauksessa symbolit $\left[\frac{3}{p}\right]$ ja $\left[\frac{-1}{p}\right]$ resiprookkilain ja Tehtävän 4 (Harjoitus 12) avulla.]

10. Todista Seurauksen 7.3.2 väite tapauksessa $p \equiv \pm 3 \pmod{8}$.

[Vihje! Imitoi tapauksen $p \equiv \pm 1 \pmod{8}$ todistusta.]

Huom! Tehtävien ratkaisut on palautettava viimeistään pe 14.12. Kirjallisia tehtäviä käsitellään maanantaina 3.12 luentoajalla siinä määrin kun luentojen päättämiseltä jää aikaa. **Keski-viikkona 5.12 klo 12.15 salissa M4** järjestetään ohjattu harjoitus, jossa kirjallisia tehtäviä on mahdollisuus tehdä. Tämä korvaa viimeisen puuttuvan luennon.