Lukuteoria 2007
Kirjalliset tehtävät 1

1. Olkoon $p > 2$ alkuluku ja $k \in \mathbf{N}$. Osoita, että kongruensin

$$x^2 \equiv 1 \pmod{p^k}$$

ainoat ratkaisut ovat $x \equiv 1 \pmod{p^k}$ ja $x \equiv -1 \pmod{p^k}$.

[Vihje! Vertaa Harjoitus 3, Tehtävä 3.]

2. Osoita, että

$$\sum_{d \in \mathbf{N}, d \mid n} \phi(d) = n.$$

[Vihje! Ks. Rosen: Elementary number theory and its applications, Theorem 6.7, s. 212.]

3. Olkoon $a \in \mathbf{Z}$ pariton ja $k \geq 3$. Osoita, että

$$a^{\frac{\phi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Mitä väite kertoo luvun 2^k primitiivijuurista?

[Vihje! Todista oikeanpuolen kongruenssi induktiolla k:n suhteen. Kirjoita induktio-oletus $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ muodossa $a^{2^{k-2}} = 1 + n2^k$ ja korota toiseen.]

4. Olkoon p alkuluku, jolle $p \equiv 1 \pmod{4}$. Perustele Seurauksen 6.3.2 avulla, miksi kongruenssilla $x^2 \equiv -1 \pmod{p}$ on täsmälleen kaksi ei-kongruenttia ratkaisua modulo p.

[Vihje! Jos $x^4 \equiv 1 \pmod{p}$, niin $x^2 \equiv 1 \pmod{p}$ tai $x^2 \equiv -1 \pmod{p}$.]

5. Olkoon $p > 2$ alkuluku ja $\text{syt}(a, p) = 1$. Osoita, että kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu jos ja vain jos kongruenssilla $x^2 \equiv a \pmod{p^k}$ on ratkaisu kaikilla $k \in \mathbf{N}$.

[Vihje! Todista väite vasemmalta oikealle induktiolla seuraavasti: Jos $x_0^2 \equiv a \pmod{p^k}$, niin $x_0^2 = a + np^k$ jollekin $n \in \mathbf{Z}$. Olkoon y lineaarisen kongruenssin $2x_0 y \equiv -n \pmod{p}$ ratkaisu. Totea, että tällöin $x_1 := x_0 + yp^k$ toteuttaa kongruenssin $x^2 \equiv a \pmod{p^{k+1}}$.]

Huom! Tehtävien ratkaisut on palautettava viimeistään pe 14.12. Kunkin tehtävän ratkaisu arvostellaan asteikolla $\frac{1}{2}$, $\frac{1}{4}$, 0. Maksimissaan ratkaisuista (yhteensä 10 tehtävää Kirjallisten tehtävien 2 kanssa) voi saada 5 bonuspistettä välikokeisiin eli 2.5 bonuspistettä loppukokeeseen. Nämä pisteet annetaan siis tavanomaisten demohyvityspisteiden lisäksi.