

Lukuteoria

25. 10. 2017

4 tuntia

Laskimen käyttö kielletty!

1. Ratkaise kongruenssiryhmä

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{7} \end{cases} .$$

2. (a) Ratkaise $12x \equiv 5 \pmod{317}$ käyttämällä Euklideen algoritmia.

(b) Onko 79 alkuluku? Perustele vastauksesi. Selvitä kongruenssin

$$x^2 + 7x + 7 \equiv 0 \pmod{79}$$

juurten $\pmod{79}$ lukumäärä laskemalla tietty Legendren symboli.

3. Olkoon r pienin positiivinen primitiivinen juuri $\pmod{13}$. Määritä r ja ratkaise

$$6^x \equiv 5 \pmod{13}$$

käyttämällä r -kantaista indeksiä.

4. (a) Laske lukujen $17n + 5$ ja $7n + 2$ pienin yhteinen jaettava.

(b) Osoita, että Eulerin funktio φ on multiplikatiivinen.