

Lukuteoria
Harjoitus 11/2007

1. Osoita, että $\text{ord}_{F_n} 2 \leq 2^{n+1}$, missä $F_n = 2^{2^n} + 1$ on n :s Fermat'n luku eli $n \in \mathbf{N}$.
2. Olkoon $m = a^n - 1$, missä $a > 1$ ja $n > 1$. Osoita, että $\text{ord}_m a = n$.
3. Olkoon $m > 2$ ja olkoon $r \in \mathbf{Z}$ siten, että $\text{syte}(r, m) = 1$. Osoita, että r on primitiivijuuri modulo m jos ja vain jos

$$r^{\frac{\phi(m)}{q}} \not\equiv 1 \pmod{m}$$

kaikille luvun $\phi(m)$ alkutekijöille q .

4. Osoita Tehtävän 3 avulla, että 3 on primitiivijuuri modulo 101.
5. Etsi Tehtävän 4 ja Seurauksen 6.1.8 avulla ainakin kolme primitiivijuurta modulo 101 joukosta $\{50, 51, \dots, 100\}$.
6. Oletetaan, että luvulla $m > 2$ on primitiivijuuri r . Osoita, että

$$\prod_{i=1}^{\phi(m)} r^i \equiv -1 \pmod{m}.$$

[Vihje! Yleistä Wilsonin lauseen todistuksen idea käyttäen hyväksi Lemmaa 6.1.5 ja Huomautusta 6.1.11.]

7. Olkoot $m \in \mathbf{N}$ ja $a, c \in \mathbf{Z}$. Konstruoidaan ns. pseudosatunnaislukujono (x_i) rekursiivisesti valitsemalla $0 \leq x_0 \leq m - 1$ ja

$$x_{i+1} \equiv ax_i + c \pmod{m}, \quad 0 \leq x_{i+1} < m.$$

Osoita, että

$$x_i \equiv a^i x_0 + c \frac{(a^i - 1)}{a - 1} \pmod{m}$$

kaikilla $i \in \mathbf{N}$.

8. Muodosta pseudosatunnaislukujonon luvut $x_1, \dots, x_6$, kun $x_0 = 2$ ja

$$x_{i+1} \equiv 66x_i \pmod{101}, \quad 0 \leq x_{i+1} < 101.$$

Huomautus. Tehtävät 4, 5 ja 8 on tarkoitettu Maplella tehtäviksi.