JOHDATUS LUKUTEORIAAN JA SEN SOVELLUKSIIN

KESKIVIIKON TENTTI

(1) (4p) Todista
$$a^{p^2} \equiv a \pmod{p}$$
kaikilla kokonaisluvuilla a ja alkuluvuilla p.

(2) (a) (3p) Laske Eukleideen algoritmin avulla syt$(126, 56)$.
(b) (3p) Ratkaise Diofantoksen yhtälö $126x + 56y = 42$ ensimmäistä kohtaa hyödyntäen.

(3) (4p) Käytetään RSA:ta julkisella modulolla $n = 59 \cdot 157$. Valitse jokin mahdollinen arvo julkiseksi eksponentiksi $e > 3$ ja kryptaa viesti 10. (Käytä ihmeessä laskinta, esim. Wolfram Alphaa laskujen suorittamiseen.)

(4) (4p) Olkoon 2 primitiivinen juuri modulo p, missä p on alkuluku. Mikä on luvun 8 kertaluku modulo p? Todista, että jos $p \equiv 2 \pmod{3}$, niin myös 8 on primitiivinen juuri.