

JOHDATUS LUKUTEORIAAN (syksy 08)

Loppukoe (pe 19.12)

HUOM. vastaa **vain toiseen** kysymyksistä 5 ja 6.

1. Mikä on luvun 7^{2008} viimeinen numero?
2. (i) Esitä Fermat'in pienen lauseen todistus.
(ii) Millä alkuluvuilla p on olemassa positiivinen eksponentti k , jolle $p|(10^k - 1)$?
3. (i) Määritä Legendren symboli $(503/773)$.
(ii) Laske kunnassa \mathbf{Q}_{17} käänteisalkiot $\overline{12}^{-1}$ ja $\overline{5}^{-1}$.
4. (i) Määrää luvun $\sqrt{5}$ ketjumurtokehitemä.
(ii) Osoita tarkasti, että Pellin yhtälöllä $x^2 - 5y^2 = 1$, on äärettömän monta ratkaisua.
5. Todista Eulerin kriteerio Legendren symbolille: jos p on pariton alkuluku ja a on kokonais-luku, niin
$$(a/p) \equiv a^{(p-1)/2} \pmod{p}.$$
6. (i) Kuvaile, kuinka todistetaan, että alkutekijöihin jako on (oleellisesti) yksikäsitteinen Gaussin kokonaisluvuille. Ei tarvitse esittää kaikkia yksityiskohtia; riittää esim. selittää tarvittavien aputulosten sisältö, todistusten pääidea, ja miten aputuloksia käytetään)