MFK-M310 Johdatus lukuteoriaan ja sen sovelluksiin
Tentti 18.12.2023

Ratkaise kaikki tehtävät. Muista kirjoittaa ratkaisuihisi riittävästi perusteluja ja välivaiheita. Voit käyttää laskinta tukenasi, mutta laskimella ei saa ratkaista yhtälöitä tai laskea kongruensseja suoraan. Laskujesi välivaiheet tulee olla kirjoitettuna niin, että olisi uskottavaa, että ne olisi laskettu ilman laskinta.

1. (a) Määritä Eukleideen algoritmilla lukujen 315 ja 141 suurin yhteinen tekijä.
   (b) Laske $\varphi(250)$
   (c) Olkoon n positiivinen kokonaisluku. Määrittele kongruenssi modulo n.

2. Ratkaise kongruenssiyhtälöryhmä

$$\begin{cases} x \equiv 3 \pmod{11}, \\ x \equiv 5 \pmod{12}. \end{cases}$$

3. Käytetään RSA-salausta alkuluvuilla $p = 7$ ja $q = 11$.
   (a) Kuinka monta mahdollista salauseksponenttia e on välillä $1 \leq e \leq \varphi(pq)$? (3p)
   (b) Käytetään salauseksponenttia $e = 53$. Määritä avauseksponentti d ja avaa viesti 5. (9p)

4. Osoita, että $n^7 - n$ on jaollinen luvulla 14 kaikilla kokonaisluvuilla n.

5. (a) Onko luku 5 primitiivinen juuri modulo 23?
   (b) Osoita, että $\ln 2$ on irrationaaliluku. (Tässä ln on luonnollinen logaritmi.) Voit olettaa tunnetuksi, että Neperin luku e on transkendenttinen luku.