APPROBATUR 3 (MATP170)
Harjoitus 4
Torstai 23.4. 18-20 MaD259
Perjantai 24.4. 10-12 MaD381 ja 12-14 MaD245

JYVÄSKYLÄN YLIOPISTO

---

1. Pätevätkö seuraavat kongruenssiyhtälöt ?

(a) $40 \equiv 13 \pmod 9$
(b) $211 \equiv 12 \pmod 2$
(c) $126 \equiv -46 \pmod 3$
(d) $29 \equiv -4 \pmod 7$
(e) $(10^{10} + 9) \equiv 49 \pmod{10}$
(f) $6^8 \equiv 2 \pmod 9$

2. Muodosta renkaan $\mathbb{Z}_6$ yhteen-ja kertolaskutaulukot.

3. Määrää pienin positiivinen kokonaisluku m siten, että $m \equiv 7^{25} \pmod{11}$.

4. Määrää renkaan $\mathbb{Z}_{12}$ ne alkiot joilla on käänteisalkio, ja ilmoita kunkin käänteisalkio.

5. Ratkaise yhtälö $13x \equiv 9$ renkaassa $\mathbb{Z}_{35}$.

6. Onko luku $(((7^7)^7)^7)^7 + ((7^7)^7)^7$ jaollinen luvulla 10?

7. Olet salakuunnellut Kallen ja Tiinan välistä viestittelyä ja pystynyt päättelemään heidän käyttävän RSA-salausmenetelmää julkisella avainparilla $N = 10001$ ja $e = 5$. Ratkaise näiden avulla purukuavain d, jolla pystyt lukemaan heidän koodaamat viestinsä.

8. (Jatkoa..) Eräänä päivänä saat siepattua Tiinan lähettämän koodatun viestin

5003 6242 2088 6662 8831 8472.

Mitä viestissä sanotaan? (Käytä modululaskennassa apuna vaikka Wolfram Alpha tms. laskentaohjelmaa ja lopuksi muunna saadut numerot kirjaimiksi jotenkin...)

9. Tarkastelemalla tilannetta sopivasti jäännöluokkien avulla näytä, että yhtälöllä $x^2 - 5y^2 = 2$ ei ole kokonaislukuratkaisuja.

10. ISSN on jatkuvasti ilmestyvän tekstijulkaisun kansainvälinen tunnus. Sen avulla tietty lehti, sarja tai muu jatkuva julkaisu voidaan yksiselitteisesti erottaa muista, jopa samannimisistä julkaisuista. ISSN koodit koostuvat kahdesta neljän numeron sarjasta $d_1d_2d_3d_4$-$d_5d_6d_7d_8$, missä viimeinen numero d_8 on niin sanottu tarkistusnumero. Tarkistusnumero toteuttaa kongruenssiyhtälön

$$d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}.$$

Jos $d_8 \equiv 10 \pmod{11}$ niin merkitään d_8 paikalle kirjain X.

(a) Onko koodi 1530-8669 validi ISSN koodi? Entä 1007-120X ? Ellei niin korjaa numero validiksi.

(b) Riittääkö tarkastusnumero paljastamaan kaikki mahdolliset virheet ISSN koodissa? (ts. määrääkö luku d_8 ISSN koodin yksikäsitteisesti?)

Laskuryhmät Ti 18-20 MaD259, Ke 10-12 MaD381 ja 12-14 MaD245