Lukuteoria
Harjoitus 5/2007

1. Olkoot $a_1 \equiv a_2 \pmod{m}$ ja $b_1 \equiv b_2 \pmod{m}$. Osoita, että $a_1 x \equiv b_1 \pmod{m}$ jos ja vain jos $a_2 x \equiv b_2 \pmod{m}$.

2. Muinainen kiinalainen kenraali laski sotajoukkonsa taistelun jälkeen järjestämällä joukot eripituisiin riveihin ja laskemalla kussakin tapauksessa viimeiseen riviin jäävien sotilaiden lukumäärän. Oletetaan, että ennen taistelua sotajoukon lukumäärä oli 1200 miestä ja taistelun jälkeen viimeiseen riviin jäi 1 mies kun joukot järjestyivät seitsemän riveihin, 11 miestä kun joukot järjestyivät yhdentoista riveihin ja 3 miestä kun joukot järjestyivät 30 riveihin. Selvitä Kiinalaisen jäännöslauseen (Lause 3.3.2) kaavan avulla, kuinka monta miestä kenraalilla oli käytössä taistelun jälkeen.

3. Etsi pienin positiivinen luvun 11 monikerta, jolla on jakojäännös 1 jaettaessa millä hyvänsä luvuista 2,3,5 tai 7. [Vihje! Esitä annettu yhtälöryhmä yhtälöparina Lemman 3.3.5 avulla.]

4. Ratkaise muinainen intialainen munaongelma iteraatiomenetelmällä: Laatikosta poistetaan munia 2,3 ja 4 kappaletta kerrallaan, jolloin jäljelle jäävien munien lukumäärät ovat (vastaavassa järjestyksessä) 1,2 ja 3. Edelleen poistettaessa 5 munaa kerrallaan, ei lopulta jäljelle jää yhtään. Mikä on pienin munien lukumäärä, joka laatikossa on voinut olla?

5. Olkoot $m_1, m_2 \in \mathbf{N}$ ja olkoot $a_1, a_2 \in \mathbf{Z}$ siten, että yhtälöparilla

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

on ratkaisu $x \in \mathbf{Z}$. Osoita, että $\operatorname{syt}(m_1, m_2) \mid (a_1 - a_2)$.

6. Olkoot $m_1, m_2 \in \mathbf{N}$ ja olkoot $a_1, a_2 \in \mathbf{Z}$ siten, että $\operatorname{syt}(m_1, m_2) \mid (a_1 - a_2)$. Osoita, että yhtälöparilla

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

on ratkaisu joka on yksikäsitteinen modulo $\operatorname{pym}(m_1, m_2)$.

7. Olkoon $A = \{ x_1, \ldots, x_m \}$ t.j.s. mod m ja olkoon r_i luvun x_i jakojäännös modulo m, $i = 1, \ldots, m$. Osoita, että $\{ r_1, \ldots, r_m \} = \{ 0, 1, \ldots, m-1 \}$.

8. Osoita Fermat'n pienen lauseen avulla: Jos p on alkuluku, niin

$$a^p \equiv a \pmod{p}$$

kaikilla $a \in \mathbf{Z}$.