**Harjoitukset 5** **Lukuteoria**
**tiistai 11.10.2011 16.00-17.30 MaD-302** **HUOMAA AIKA**

1. *Tutki jaollisuuslauseiden avulla, onko luku 123456789 jaollinen*
   (a) *3:lla tai 9:llä,*
   (b) *11:llä.*
   (c) *Entä onko* 476271 *alkuluku? (Älä yritä jakaa!)*

2. *Johda tai etsi sopivat jaollisuuslauseet ja tutki, mitkä luvuista 222222, 600560 ja 3416 ovat jaollisia*
   (i) *4:llä,*
   (ii) *8:lla,*

3. *Algebrasta tiedetään, että*

Määr: *(Äärellisen)* ryhmän kertaluku *on sen alkioiden lukumäärä.*

Määr: *Ryhmän* $G$ alkion $a$ kertaluku *on* $\min\{n \in \mathbb{N} \mid a^n = 1\}$ *(, joka on itse asiassa alkion* $a$ *virittämän aliryhmän* $\langle a \rangle$ *alkioiden lukumäärä.)*

Esimm: *Ryhmän* $\mathbb{Z}_5^* = \{a \in Z_5 \mid a \text{ on kääntyvä}\} = \{1, 2, 3, 4\}$ *kertaluku on 4. Ryhmän* $\mathbb{Z}_{10}^* = \{a \in Z_{10} \mid a \text{ on kääntyvä}\} = \{a \in Z_{10} \mid (a, 10) = 1\} = \{1, 3, 7, 9\}$ *kertaluku on 4. Yleisesti ryhmän* $\mathbb{Z}_n^* = \{a \in Z_n \mid a \text{ on kääntyvä}\}$ *kertaluku on* $\varphi(n)$.

*Alkion* $1 \in \mathbb{Z}_{10}^*$ *kertaluku on 1, koska* $1^1 = 1$.

*Alkion* $3 \in \mathbb{Z}_{10}^*$ *kertaluku on 4, koska* $3^1 = 3 \neq 1$, $3^2 = 9 \neq 1$, $3^3 = 27 = 7 \neq 1$ *ja vasta* $3^4 = 81 = 1$.

*Alkion* $9 \in \mathbb{Z}_{10}^*$ *kertaluku on 2, koska* $9^1 = 9 \neq 1$, *mutta jo* $9^2 = 81 = 1$.

Lagrangen lause: *Ryhmän alkion kertaluku jakaa ryhmän kertaluvun.*

*Todista Eulerin lause vetoamalla Lagrangen lauseeseen.*

4. (a) *Ratkaise lineaarinen kongruenssiyhtälö* $3x \equiv 5 \pmod 7$,
   (b) *Ratkaise lineaarinen kongruenssiyhtälö* $6x \equiv 5 \pmod{12}$.
   (c) *Montako ratkaisua (eri kongruenssiluokkia) on yhtälöllä* $943x \equiv 381 \pmod{2576}$,
   (d) *Montako ratkaisua (eri kongruenssiluokkia) on yhtälöllä* $1375x \equiv 242 \pmod{5625}$*? Perustele.*

5. *Ratkaise lineaarinen kongruenssiyhtälö* $6x \equiv 4 \pmod{10}$ *eri tavoin.*

6. *Kalle ei muista, montako porttia pujotteluradalla on, mutta hän muistaa, että jos porttien määrä jaetaan*
   (i) *kahdella, niin jää yksi portti,*
   (ii) *kolmella, niin jää kaksi porttia,*
   (iii) *seitsemällä, niin ei jää yhtään porttia.*

*Auta Kallea laskemaan :-) montako portteja on.*

7. *Ratkaise kongruenssiryhmä:*

a) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{12} \end{cases}$ b) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 7 \\ x \equiv 7 \pmod{15} \end{cases}$ c) $\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 7 \\ x \equiv 8 \pmod{12} \end{cases}$ d) $\begin{cases} x \equiv 3 \pmod 9 \\ x \equiv 6 \pmod{10} \\ x \equiv 9 \pmod{11} \end{cases}$

KÄÄNNÄ

8. *Olkoot $p$ ja $q$ eri alkulukuja. Osoita, että*

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

*Olkoon $p$ alkuluku. Todista*

(a) $(a+b)^p \equiv a^p + b^p \pmod{p}$, *(Vihje: Käytä Fermat'n lausetta)*
(b) $(a+b)^p \equiv a^p + b^p \pmod{p}$, *(Kielto: Älä käytä Fermat'n lausetta!)*
(c) $a^p \equiv a \pmod{p}$ *eli Fermat'n lause — kohdan (b) avulla.*