Harjoitukset 7 **Lukuteoria**
tiistai 1.11.2011 16.00-17.30 MaD-302

1. *Osoita, että kaikille parittomille alkuluvuille p pätee*
   a) $(p-2)! \equiv 1 \pmod{p}$.
   b) $2 \cdot (p-3)! \equiv 1 \pmod{p}$.

Vihje: Ryhmässä kaikki alkiot ovat kääntyviä. Millä alkioilla on $a \neq a^{-1} \in Z_p^*$? Mikä on muiden tulo?

2. *(jatkoa?) Osoita, että kaikille parittomille alkuluvuille p pätee*

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

3. *Määrää kaikki neliönjäännökset* $\pmod{23}$. *Kirjoita näkyviin niiden itseisarvoltaan pienimmät edustajat. Minkä (todistetun) ilmiön huomaat?*

4. *Tutki Eulerin kriteerillä, onko 2 neliönjäännös* $\pmod{17}$. *Entä 5?*

5. *Kuinka monta (epäkongruenttia, tietenkin) ratkaisua on kongruenssilla* $x^2 \equiv 2$
   a) $\pmod{17}$
   b) $\pmod{17^2}$

(Entä c) $\pmod{17^{100}}$*, tai toisaalta* d $\pmod{10}$*?) Vihje: 2,2,(2,0).*

6. *Onko alkiolla 2 neliöjuuri*
   a) *kunnassa* $\mathbb{Z}_{29}$
   b) *kunnassa* $\mathbb{Z}_{31}$
   c) *kunnassa* $\mathbb{Z}_{97}$
   d) *kunnassa* $\mathbb{Z}_{101}$
   e) *kunnassa* $\mathbb{Z}_{111}$?

7. *Laske* $\left(\frac{61}{31}\right)$, $\left(\frac{33}{31}\right)$, $\left(\frac{29}{31}\right)$, $\left(\frac{8}{31}\right)$ *ja* $\left(\frac{128}{821}\right)$.

8. *Laske* $\left(\frac{3}{17}\right)$
   a) *Gaussin lemmalla*
   b) *Eulerin ehdolla.*
   c) *Resiprookkilauseella*

9. *Olkoon p pariton alkuluku ja* $ab \equiv 1 \pmod{p}$. *Osoita, että jos kongruenssilla* $x^2 \equiv a \pmod{p}$ *on ratkaisu, niin myös kongruenssilla* $x^2 \equiv b \pmod{p}$ *on ratkaisu.*