Harjoitukset 6 **Lukuteoria**
tiistai 25.10.2011 16.00-17.30 MaD-302

1. *Ratkaise kongruenssiryhmä:*

a) $\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 5 \pmod 7 \\ x \equiv 8 \pmod{15} \end{cases}$ b) $\begin{cases} 2x \equiv 3 \pmod 9 \\ 4x \equiv 6 \pmod{10} \\ 6x \equiv 9 \pmod{11} \end{cases}$

2. *Todista kiinalaisen jäännöslauseen avulla, että kaikille $k \in \mathbb{N}$ on olemassa k peräkkäistä lukua $a+1, \ldots, a+k$ joista yksikään ei ole neliövapaa.*

3. *Laske $\varphi(10)$, $\varphi(100)$ ja $\varphi(10!)$.*

4. *a) Millä luvuilla n on $\varphi(n)$ pariton?*
b) Millä luvuilla n on $\varphi(n) = \varphi(2n)$?

5. *Määrää lukujen* 3, 7 *ja* 11 *kertaluku* $\pmod{20}$.

6. *Löydä ainakin yksi primitiivinen juuri modulo* 14.

7. 2 *on primitiivinen juuri modulo* 101. *Määrää* $ord_{101}(2^{32})$.

8. 2 *on primitiivnen juuri modulo* 19. *Laske ensin, kuinka monta primitiivistä juurta modulo* 19 *on olemassa ja määrää sen jälkeen nämä primitiiviset juuret.*

9. *Olkoon r primitiivinen juuri modulo m ja olkoon $(m, a) = 1$. Osoita, että seuraavat ehdot ovat yhtäpitäviä:*
(1) *a on primitiivinen juuri* $\pmod m$.
(2) *Kaikille $\varphi(m)$:n alkutekijöille p pätee:* $a^{\varphi(m)/p} \not\equiv 1 \pmod m$.

10. *Rakenna indeksitaulukko modulille* 13. *Vertaa taulukkoon.*

11. *Mitkä seuraavista kongruensseista ratkeavat?*
a) $x^4 \equiv 17 \pmod{67}$
b) $x^4 \equiv 18 \pmod{67}$
c) $x^5 \equiv 17 \pmod{67}$
Ratkaise ne käyttämällä tietoa, että 2 on primitiivnen juuri $\pmod{67}$.