**Harjoitukset 4** **Lukuteoria**
**tiistai 11.10.2011 16.00-17.30 MaD-302** **HUOMAA AIKA**

1. *Osoita, että*
*a) minkään kokonaisluvun neiö ei ole muotoa* $4n+2$ *eikä* $4n+3$.
*b) neljän peräkkäisen kokonaisluvun tulo on jaollinen luvulla 24.*
*c)* $k$ *peräkkäisen kokonaisluvun tulo on jaollinen kertomalla* $k!$ .

2. *Olkoon* $x \in \mathbb{R}$, $m \in \mathbb{N}$ *ja* $p \in \mathbb{P}$.
*a) Osoita, että* $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$
*b) Osoita, että* $p^{\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \mid m$, *mutta* $p^{1+\lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots} \nmid m$.
*c) Kuinka moneen nollaan päättyy luvun 169! desimaaliesitys?*
*d) Osoita suoraan määritelmästä, että binomikertoimet* $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ *ovat kokonaislukuja.*

3. *Etsi käänteiset tai osoita ettei ole olemassa*
*a) Luvuille* $1 \ldots 10 \pmod{11}$
*b) Luvuille* $-12 \ldots 12 \pmod{12}$

4. *Johda seitsemän jaollisuusääntö*

$$7 \mid n = \prod a_\mu 10^\mu \iff 7 \mid (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - \ldots$$

5. *a) Kirjoita näkyviin kaksi täydellistä (tjs) ja kaksi ja supistettua (sjs) jäännössysteemiä* $\pmod{20}$.
*b) Olkoon* $\{a_1, a_2, \ldots, a_k\}$ *täydellinen jäännösysteemi (tjs) modulo* $n$. *Määrää pienin positiiviluku, joka on kongruentti* $a_1 + a_2 + \cdots + a_k \pmod{n}$.
*c) Olkoon* $\{a_1, a_2, \ldots, a_k\}$ *supistettu jäännösysteemi (sjs) modulo* $n$. *Määrää pienin positiiviluku, joka on kongruentti* $a_1 + a_2 + \cdots + a_k \pmod{n}$.

6. *Todista, että jäännössysteemeistä voidaan muodostaa uusia seuraavalla tavalla.*
*a) Jos* $(m, n) = 1$, $x$ *käy läpi t.j.s:n* $\pmod{m}$ *ja* $y$ *käy t.j.s:n* $\pmod{n}$, *niin luvut* $xn + my$ *käyvät t.j.s:n* $\pmod{mn}$.
*b) Aivan samanlainen väite pätee myös supistettuihin jäännössysteemeihin nähden.*

7. **Vahvat pseudoalkuluvut ja Millerin testi.** *Sanotaan, että pariton yhdistetty luku* $n$, *jolle* $n-1 = 2^s t$, $2 \nmid t$, *on* **vahva pseudoalkuluku** *kantaluvun* $a$ $(> 1)$ *suhteen, jos joko*

$$a^t \equiv 1 \pmod{n} \tag{1}$$

*tai*

$$a^{2^j t} \equiv -1 \pmod{n} \quad \textit{jollakin } 0 \leq j \leq s-1. \tag{2}$$

*Sanotaan myös, että luku* $n$ **läpäisee Millerin testin kantaluvun a suhteen**, *jos se toteuttaa kongruenssin* (1) *tai* (2).

*Todista, että jokainen pariton alkuluku läpäisee Millerin testin.*

*Näin ollen Millerin testiä voidaan käyttää alkulukutestinä. Se ei kuitenkaan ole varma testi, sillä esimerkiksi* $n = 2047 = 23 \cdot 89$ *on vahva pseudoalkuluku kantaluvun* 2 *suhteen (ja samalla pienin laatuaan). Luku*

$$3215031751 = 151 \cdot 751 \cdot 28351$$

*on pienin vahva pseudoalkuluku kantalukujen* $2, 3, 5$ *ja* $7$ *suhteen. Kuitenkin voidaan todistaa, että vahvan pseudoalkulukukäsitteen suhteen ei ole Carmichaelin lukuja, ts. jokainen yhdistetty luku "paljastuu" yhdistetyksi, kun Millerin testiä toistetaan riittävän monelle kantaluvulle. Tarkemmin sanottuna pariton yhdistetty luku* $n$ *läpäisee Millerin testin korkeintaan* $(n-1)/4$*:lle kantaluvulle väliltä* $[1, n-1]$.

8. *Ratkaise kongruenssi* $x^2 \equiv -1 \pmod{13}$ *Wilsonin lauseen avulla.*