Harjoitukset 1 **Lukuteoria**
tiistai 20.9.2011 16-18 MaD-302
An English version is due soon

1. *Esitä seuraavat luvut kymmenjärjestelmässä:*
   (a) 10011_2,
   (b) 1203_4,
   (c) $A0C_{16}$.

   Esitä luku
   (d) 111 *kaksijärjestelmässä,*
   (e) 117_8 *kaksijärjestelmässä,*
   (f) 230 16-*järjestelmässä.*

2. *Laske*
   (a) $1110_2 + 101_2$,
   (b) $230_4 - 101_2$, *anna vastaus kaksijärjestelmässä,*
   (c) $32_4 \cdot 23_4$.

3. *Olkoon* $k \in \mathbb{N}$, $k > 1$.
   (a) *Määrää kantaluku* k, *kun tiedetään, että* $28 = 124_k$.
   (b) *Laske* $101_k + 101_{k^2}$.

4. *Todista malliksi jaollisuuden ominaisuuksista:*
   Olkoot $n, m, d \in \mathbb{Z}$.
   (a) *Jos* $d \,|\, n$ *ja* $n \,|\, m$, *niin* $d \,|\, m$.
   (b) *Jos* $d \,|\, n$ *ja* $d \,|\, m$, *niin* $d \,|(an + bm)$ *kaikilla* $a, b \in \mathbb{Z}$.

   Ja todista edelleen induktiolla:
   (c) *Olkoot* $m \in \mathbb{Z} \setminus \{0\}$ *ja* $n \in \mathbb{N}$. *Jos* $a_i \in \mathbb{Z}$ *ja* $m \,|\, a_i$ *kaikilla* $i = 1, 2, \ldots n$, *niin*
   $$m \,|(c_1a_1 + c_2a_2 + \cdots + c_na_n)$$
   kaikilla $c_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$.

5. *Olkoot* $m \in \mathbb{Z} \setminus \{0\}$ *ja* $n \in \mathbb{N}$, $n \geq 2$. *Näytä, että jos* $a_i \in \mathbb{Z}$, $m \,|\, a_i$ *kaikilla* $i = 1, 2 \ldots n - 1$ *ja* $m \not| \; a_n$, *niin*
$$m \not| \; (a_1 + a_2 + \cdots + a_n).$$

6. *Ovatko seuraavat väitteet totta? Todista tai keksi vastaesimerkki.*
   (a) *Jos luku* $k \in \mathbb{Z}$ *on jaollinen* 5:*llä, niin* $(k + 5)^{10}$ *on jaollinen* 5:*llä.*
   (b) *Olkoot* $a, b, c, d \in \mathbb{Z}$, $a \,|\, b$ *ja* $c \,|\, d$. *Tällöin* $(a + c) \,|(b + d)$.
   (c) *Olkoot* a, b, n *kokonaislukuja, joille* $a^2 \,|\, n$, $b^2 \,|\, n$ *ja* $a^2 \leq b^2$. *Tällöin* $a \,|\, b$.
   (1) *Olkoot* $a, b \in \mathbb{N}$ *ja* $c \in \mathbb{N}$. *Tällöin* $c \,|\, a$ *ja* $c \,|\, b$ *jos ja vain jos* $c \,|\, \mathrm{syt}(a, b)$.

KÄÄNNÄ

Tehtäviin (7) ja (8) tarvitaan Eukleideen algoritmi.
Eukleideen algoritmi. Kahden luvun a ja b s.y.t. eli (a, b) voidaan määrittää näin: Oletetaan esimerkiksi, että $a \geq b > 0$. Muodostetaan jono lukuja (jakojäännöksiä!) r_j siten, että valitaan $r_0 = a,\ r_1 = b$ ja kirjoitetaan yleisesti jakoalgoritmin mukaan

$$r_{j-2} = r_{j-1}q_{j-1} + r_j, \quad 0 \leq r_j < r_{j-1}, j = 2, 3, \ldots, n+1.$$

Ensimmäiset kolme yhtälöä ovat

$$a = bq_1 + r_2,$$
$$b = r_2q_2 + r_3.$$
$$r_2 = r_3q_3 + r_4.$$

Koska yleisesti on $(a, b) = (a + kb, b)$, niin

$$d = (a, b) = (a - bq_1, b) = (r_2, b), \text{ eli } (r_0, r_1) = (r_1, r_2).$$

Jatkamalla samoin nähdään, että

$$d = (r_j, r_{j+1}), \quad \forall\ j = 0, 1, \ldots, n.$$

Mutta koska $r_{n+1} = 0$, on $(r_n, r_{n+1}) = r_n$. Täten

$$d = r_n,$$

mikä onkin Eukleideen algoritmin idea. Lisäksi esitys $d = ax + by$ saadaan käymällä läpi laskelmat lopusta alkuun.

Esimerkki.
Lasketaan (252,198):
$252 = 1 \cdot 198 + 54$
$198 = 3 \cdot 54 + 36$
$54 = 1 \cdot 36 + 18$
$36 = 2 \cdot 18$
Siis $(252, 198) = 18 = 54 - 36 = \ldots = 4 \cdot 252 - 5 \cdot 198$.

7. *a) Laske* $(1492, 1066)$ *Eukleideen algoritmilla.*

8. *Etsi luvut* $x, y \in \mathbb{Z}$*, joille* $(1492, 1066) = 1492x + 1066y$.

9. *etsi luvut* $a, b, c \in \mathbb{Z}$ *joille*
(1) $a \,|\, c$ *ja* $b \,|\, c$ *mutta* $ab \not| \, c$,
(2) $a \,|\, bc$ *mutta* $a \not| \, c$.