## Lukuteoria ja ryhmät

### Vihjeet 2  kevät 2014

1. Määrää kaikki lukua 110 pienemmät alkuluvut.

   *Vihje.* Kirjoita luvut 1-110 niin, että 1. rivillä on luvut $1, 2, \dots, 10$, 2. rivillä luvut $11, 12, \dots, 20$, 1. sarakkeella on luvut $1, 11, \dots, 101$ ja niin edelleen. Viivaa yli luku 1 ja tämän jälkeen viivaa yli luvulla 2 jaolliset yhdistetyt luvut, sitten luvulla 3 jaolliset yhdistetyt luvut. Mikä on viimeinen alkuluku, millä jaolliset yhdistetyt luvut pitää viivata yli? Jäljelle jää vain alkulukuja.

2. a) Osoita, että jokainen alkuluku $p > 3$ on muotoa $6n \pm 1$, missä $n \in \mathbb{Z}_+$.
   b) Onko lukujen 3, 5 ja 7 lisäksi olemassa muita sellaisia kokonaislukukolmikoita $p$, $p + 2$, $p + 4$, että jokainen näistä kolmesta luvusta on alkuluku?

   *Vihje.* a) Jaa kokonaisuvut luokkiin jakoalgoritmia käyttämällä (Lause 2.2), kun $b = 6$. Mieti, mitkä näistä eri luokista voivat sisältää alkulukuja.
   b) Käytä a)-kohtaa hyväksi. Oleta, että $p$ on alkuluku ja osoita, että $p+2$ ja $p + 4$ eivät molemmat voi olla alkulukuja.

3. Olkoot $n \geq 3$ ja $n^2 + 2$ alkuluku. Osoita, että $3 \mid n$.

   *Vihje.* Tee vastaoletus, että $3 \nmid n$ ja mieti minkälainen esitys luvulla $n$ voi nyt olla jakoalgoritmin avulla (Lause 2.2), kun $b = 3$. Osoita, että nyt $n^2+2$ on yhdistetty luku.

4. Määrää Eukleideen algoritmilla suurin yhteinen tekijä seuraaville luvuille ja esitä se näiden kokonaislukujen lineaarikombinaationa:
   a) 478 ja 212,
   b) 201 ja 1024.
   Esitä luku 3 lukujen 201 ja 1024 lineaarikombinaationa (käytä b-kohtaa apuna).

   *Vihje.* Katso Eukleideen algoritmiin liittyvät luentoesimerkit.

5. a) Olkoot $a$ ja $b$ kokonaislukuja. Oletetaan, että on olemassa sellaiset kokonaisluvut $x$ ja $y$, että $ax + by = 1$. Osoita, että $\mathrm{syt}(a, b) = 1$.
   b) Onko olemassa sellaisia kokonaislukuja $r$ ja $s$, että $1841r + 3647s = 1$?

*Vihje.* a) Merkitse, että $\mathrm{syt}(a, b) = c$. Osoita, että $c \mid ax + by$.
b) Laske $\mathrm{syt}(1840, 3647)$ ja käytä a)-kohtaa apuna perustelussa.

6. Oletetaan, että $k \in \mathbb{Z}_+$. Osoita, että luvut $3k + 2$ ja $5k + 3$ ovat suhteellisia alkulukuja.

   *Vihje.* Laske Eukleideen algoritmilla $\mathrm{syt}(3k + 2, 5k + 3)$.

7. Olkoot $a$ ja $b$ kokonaislukuja, joista ainakin toinen on nollasta eroava.
   a) Olkoot $\mathrm{syt}(a, b) = 1$ sekä $c$ ja $d$ sellaisia kokonaislukuja, että $c \mid a$ ja $d \mid b$. Osoita, että $\mathrm{syt}(c, d) = 1$.
   b) Olkoot $\mathrm{syt}(a, b) = 1$ ja kokonaisluku $c$ sellainen, että $a \mid c$ ja $b \mid c$. Osoita, että $ab \mid c$.
   c) Olkoon $m$ positiivinen kokonaisluku. Osoita, että $\mathrm{syt}(ma, mb) = m\mathrm{syt}(a, b)$.

   *Vihje.* a) Merkitse $\mathrm{syt}(c, d) = e$ ja osoita, että $e \mid a$ ja $e \mid b$. Ota tämän jälkeen suurimman yhteisen tekijän määritelmän 2. kohta avuksi (Määritelmä 2.8).
   b) Esitä luku 1 Lauseen 2.9 tavalla ja kerro tämä esitys puolittain luvulla $c$. Mieti, miten tästä saat, että $ab \mid c$.
   c) Merkitse, että $\mathrm{syt}(a, b) = d$. Osoita, että $md$ toteuttaa Määritelmän 2.8 ehdot. Jälkimmäisessä kohdassa kannattaa käyttää apuna Lausetta 2.9.