**Lukuteoria 1**
**Harjoitus 2, 24.1.2018**

**1.** Sinulla on käytössä 16 ja 9 litran vesiämpärit. Onko mahdollista mitata näiden ämpärien avulla kolmanteen astiaan tasan yksi litra vettä? Jos on, kuinka tämän voi tehdä?

**Ratkaisu.** Tehtävän voi ratkaista ilman tämän viikon tietojakin, mutta erään ratkaisuvaihtoehdon tarjoaa Eukleideen algoritmi:

$$\begin{aligned} 16 &= 1 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Siis $\operatorname{syt}(16, 9) = 1$. Peruutetaan:

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 \\ &= 7 - 3(9 - 7) \\ &= 4 \cdot 7 - 3 \cdot 9 \\ &= 4(16 - 9) - 3 \cdot 9 \\ &= 4 \cdot 16 - 7 \cdot 9. \end{aligned}$$

Siis tehtävän saa suoritettua kaatamalla astiaan ensin neljä täyttä 16 litran ämpäriä, ja ottamalla sitten astiasta pois seitsemän yhdeksän litran ämpäriä.

**Huomautus:** Tehtävänannossa ei pyydetty käyttämään Eukleideen algoritmia, joten tehtävän saattoi tehdä myös muilla tavoilla. Mikä tahansa ratkaisu, jolla tehtävän saa suoritettua käyttämällä tai käyttämättä kolmatta astiaa, on ok.

**2.** Lauseen 2.3.4 todistuksessa määritellään $d = \min A$. Osoita, että $d \mid b$.

**Ratkaisu.** Tehdään *vastaoletus*, että $d \nmid b$. Tällöin jakoyhtälön nojalla $b = kd + r$, missä $1 \leq r < d$. Käyttämällä esitystä $d = x_0 a + y_0 b$ saadaan

$$r = b - kd = b - k(x_0 a + y_0 b) = (-kx_0)a + (1 - ky_0)b.$$

Koska $(-kx_0) \in \mathbb{Z}$ ja $(1 - ky_0) \in \mathbb{Z}$, on $r \in A$. Mutta $r < d$, mikä on ristiriita, sillä $d = \min A$. Koska vastaoletus $d \nmid b$ johti ristiriitaan, on $d \mid b$.

**3.** Olkoot $a, b, c \in \mathbb{Z}$, $a \neq 0$. Osoita, että jos $b \mid c$, niin $\operatorname{syt}(a, b) = \operatorname{syt}(a + c, b)$.

**Ratkaisu.** Olkoon $A$ lukujen $a, b$ kaikkien yhteisten tekijöiden joukko, ja olkoon $B$ lukujen $a + c, b$ kaikkien yhteisten tekijöiden joukko. Jos pystytään osoittamaan, että $A = B$, lukupareilla $a, b$ ja $a + c, b$ on samat yhteiset tekijät, jolloin on oltava $\operatorname{syt}(a, b) = \operatorname{syt}(a + c, b)$.

Osoitetaan ensin, että $A \subset B$. Olkoon $e \in A$. Tällöin $e \mid a$ ja $e \mid b$. Koska $b \mid c$, Proposition 2.1.4 (1) nojalla $e \mid c$. Siis saman proposition kakkoskohdan nojalla $e \mid (a + c)$. Koska $e \mid (a + c)$ ja $e \mid b$, on $e \in B$. Siis $A \subset B$.

Osoitetaan seuraavaksi, että $B \subset A$. Olkoon $f \in B$. Tällöin $f \mid (a + c)$ ja $f \mid b$. Jälkimmäisestä tiedosta seuraa jälleen, että $f \mid c$. Koska $f \mid (a + c)$ ja $f \mid c$, Proposition 2.1.4 (2) nojalla $f \mid [(a + c) - c]$, eli $f \mid a$. Siis $f \in A$, joten $B \subset A$. Siis $A = B$, joten todistus on valmis.

**4.** Onko yhtälöllä $16x + 20y = 2$ kokonaislukuratkaisuja? Jos on, anna yksi esimerkki.

**Ratkaisu.** Koska $20 = 16+4$ ja $16 = 4 \cdot 4$, Eukleideen algoritmilla $\operatorname{syt}(20, 16) = 4$. Koska $4 \nmid 2$, Seurauksen 2.3.12 nojalla tehtävän yhtälöllä ei ole kokonaislukuratkaisuja.

**5.** Laske Eukleideen algoritmilla $\operatorname{syt}(123, 456)$.

**Ratkaisu.**

$$\begin{aligned} 456 &= 3 \cdot 123 + 87 \\ 123 &= 87 + 36 \\ 87 &= 2 \cdot 36 + 15 \\ 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3. \end{aligned}$$

Siis $\operatorname{syt}(123, 456) = 3$.

**6.** Etsi edellisen tehtävän avulla jotkin luvut $x, y \in \mathbb{Z}$, joille pätee

$$123x + 456y = \operatorname{syt}(123, 456).$$

**Ratkaisu.** Peruuutetaan edellisen tehtävän Eukleideen algoritmissa:

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 \\ &= 15 - 2(36 - 2 \cdot 15) \\ &= -2 \cdot 36 + 5 \cdot 15 \\ &= -2 \cdot 36 + 5(87 - 2 \cdot 36) \\ &= 5 \cdot 87 - 12 \cdot 36 \\ &= 5 \cdot 87 - 12(123 - 87) \\ &= -12 \cdot 123 + 17 \cdot 87 \\ &= -12 \cdot 123 + 17(456 - 3 \cdot 123) \\ &= -63 \cdot 123 + 17 \cdot 456. \end{aligned}$$

Voidaan siis valita $x = -63$ ja $y = 17$.

**7.** Olkoon $n \in \mathbb{N} \setminus \{0\}$ ja

$$B = \{a \in \mathbb{Z} \ : \ 1 \leq a \leq 2n\} = \{1, 2, 3, ..., 2n\}.$$

Olkoon $C \subset B$ joukko, jossa on $n+1$ eri lukua. Osoita, että on sellaiset luvut $b, c \in C$, että $\operatorname{syt}(b, c) = 1$.

**Ratkaisu.** Jos pystytään osoittamaan, että joukossa $C$ on kaksi peräkkäistä kokonaislukua, väite seuraa Propositiosta 2.3.8.

Osoitetaan induktiolla luvun $n$ suhteen, että jollekin luvulle $a \in C$ pätee $a + 1 \in C$.

*Alkuaskel:* Jos $n = 1$, on $B = \{1, 2\} = C$, joten luvulle $1 \in C$ pätee $1 + 1 \in C$.

*Induktio-oletus:* Jos $n = k$, joukossa $C$ on sellainen luku $a$, että $a + 1 \in C$.

*Induktioväite:* Jos $n = k+1$, joukossa $C$ on sellainen luku $a$, että $a+1 \in C$.

*Induktioväitteen todistus:* Olkoon $n = k + 1$. Tällöin joukossa $C$ on $k + 2$ kokonaislukua väliltä $[1, 2(k + 1)]$. Jos joukkoon $C$ kuuluvat luvut $2k + 1$ ja $2k + 2$, luvulle $2k + 1 \in C$ pätee $(2k + 1) + 1 \in C$. Muussa tapauksessa joukossa $C$ on vähintään $k+1$ eri kokonaislukua väliltä $[1, 2k]$, jolloin induktio-oletuksen nojalla joukossa $C$ on sellainen luku $a$, että $a + 1 \in C$.

Olemme todistaneet induktiolla, että joukossa $C$ on kaksi peräkkäistä kokonaislukua. Proposition 2.3.8 nojalla näiden kahden peräkkäisen kokonaisluvun suurin yhteinen tekijä on 1.

**Huomautus:** Ensimmäisessä harjoitusryhmässä esitettiin myös toinen ratkaisuidea, joka ei käytä induktiota. Idea on lyhyesti kirjoitettuna seuraava: Olkoon $C = \{a_1, a_2, ..., a_{n+1}\}$, missä $a_1 < a_2 < ... < a_{n+1}$. (Joukon $C$ $n + 1$ eri lukua on siis kirjoitettu suuruusjärjestykseen.) Tehdään vastaoletus, että joukossa $C$ ei ole sellaista lukuparia jonka suurin yhteinen tekijä on 1. Tällöin joukossa $C$ ei voi olla kahta peräkkäistä kokonaislukua, joten on

$$a_{j+1} \geq a_j + 2 \quad \text{kaikilla} \quad j \in \{1, 2, ..., n\}.$$

Tällöin $a_{n+1} - a_1 \geq 2n$, mikä on ristiriita, sillä oletuksen $C \subset B$ nojalla on oltava $a_{n+1} - a_1 \leq 2n - 1$.