Lukuteoria 1
Harjoitus 3, 31.1.2018
Ratkaisuehdotuksia

Tehtävissä 1 ja 2 etsitään kaikki kokonaislukuratkaisut Diofantoksen yhtälölle

$$(*) \qquad 27x + 11y = 3.$$

1. Laske Eukleideen algoritmilla syt$(27, 11)$, ja etsi sitten jokin kokonaislukuratkaisu yhtälölle

$$27x + 11y = \text{syt}(27, 11).$$

Ratkaisu. Eukleideen algoritmilla saadaan

$$\begin{aligned} 27 &= 2 \cdot 11 + 5 \\ 11 &= 2 \cdot 5 + 1, \end{aligned}$$

joten syt(27,11)=1. Peruuttamalla saadaan

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ &= 11 - 2(27 - 2 \cdot 11) \\ &= -2 \cdot 27 + 5 \cdot 11. \end{aligned}$$

Siis eräs ratkaisu tehtävän yhtälölle on $x = -2$, $y = 5$.

2. Etsi edellisen tehtävän avulla jokin kokonaislukuratkaisu yhtälölle $(*)$, ja käytä sitten Lausetta 2.5.3 löytääksesi yhtälön $(*)$ kaikki kokonaislukuratkaisut.

Ratkaisu. Kertomalla yhtälö

$$-2 \cdot 27 + 5 \cdot 11 = 1$$

puolittain luvulla 3 saadaan

$$-6 \cdot 27 + 15 \cdot 11 = 3,$$

joten eräs ratkaisu yhtälölle $(*)$ on $x = -6$, $y = 15$. Lauseen 2.5.3 nojalla yhtälön $(*)$ ratkaisuja ovat täsmälleen lukuparit

$$-6 + 11k, \quad 15 - 27k, \quad k \in \mathbb{Z}.$$

3. Pitävätkö seuraavat väitteet paikkansa? Todista tai keksi vastaesimerkki.
(a) Kahden yhdistetyn luvun summa on yhdistetty luku.
(b) Kahden yhdistetyn luvun tulo on yhdistetty luku.
(c) Kahden alkuluvun summa on alkuluku.
(d) Kahden alkuluvun tulo on alkuluku.

Ratkaisu.
(a) Väärin. Esimerkiksi $4 + 9 = 13$.
(b) Oikein: Jos a ja b ovat yhdistettyjä lukuja, niin ab on jaollinen luvulla a, ja pätee $2 \leq a \leq ab$, sillä $a, b \geq 2$. Siis ab on yhdistetty luku.
(c) Väärin. Esimerkiksi $2 + 2 = 4$.
(d) Väärin, kahden alkuluvun tulo on aina yhdistetty luku.

4. Esitä yhdistetyt luvut 64 ja 99 alkulukujen tuloina.

Ratkaisu. $64 = 2^6$ ja $99 = 3^2 \cdot 11$.

5. Osoita seuraavat väitteet:

(a) Luku 2 on ainoa parillinen alkuluku.

(b) Olkoon p alkuluku. Tällöin se on ainoa alkuluku, joka on jaollinen luvulla p.

Ratkaisu.

(a) Olkoon p alkuluku, $p \neq 2$. Tällöin $p > 2$. Koska luvun p ainoat positiiviset tekijät ovat 1 ja p, se ei ole jaollinen kahdella, eli se on pariton. Siis luku 2 on ainoa parillinen alkuluku.

(b) Olkoon $q \neq p$ jokin toinen alkuluku. Koska Luvun q ainoat tekijät ovat 1 ja q ja on $p \neq 1$ ja $p \neq q$, luku q ei ole jaollinen luvulla p. Siis luku p on ainoa alkuluku joka on jaollinen luvulla p.

6. Luvut 3, 5 ja 7 ovat alkulukuja. Onko olemassa sellaista luonnollista lukua $a > 3$, että luvut a, $a + 2$ ja $a + 4$ ovat alkulukuja?

Ratkaisu. Olkoon $a > 3$ alkuluku. Edellisen tehtävän nojalla se ei ole jaollinen luvulla 3, joten jakojäännöslauseen nojalla se on joko muotoa $3k + 1$ tai $3k + 2$ jollakin $k \in \mathbb{Z}$. Koska $a > 3$, tiedämme vieläpä että $k \geq 1$. Jos a on muotoa $3k + 1$, on $a + 2 = 3k + 3 = 3(k + 1)$, eli luku $a + 2$ on jaollinen kolmella. Koska lisäksi $a + 2 \geq 5$, se on yhdistetty luku.

Jos taas $a = 3k + 2$ jollakin k, on $a + 4 = 3k + 6 = 3(k + 2)$, eli $a + 4$ on yhdistetty luku.

Olemme osoittaneet, että ei ole sellaista alkulukua $a > 3$, että myös luvut $a + 2$ ja $a + 4$ olisivat alkulukuja.

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 $b \mid c$.

Matemaatikkolegenda Paul Erdős (1913-1996) esitti usein tämän kysymyksen tavatessaan jonkun nuoren, matematiikasta kiinnostuneen ihmisen.

Ratkaisuja. (Kaikki ratkaisut ovat kurssin opiskelijoiden esittämiä!)

Ratkaisu 1. (J.V.) Jokainen joukon B luku voidaan ilmaista muodossa $2^d(2k+1)$, missä $k \in \{0, 1, ..., n-1\}$ ja $d \in \mathbb{N}$. (Esimerkiksi $1 = 2^0(2 \cdot 0 + 1)$, $2 = 2^1(2 \cdot 0 + 1)$, $3 = 2^0(2 \cdot 1 + 1)$, $4 = 2^2(2 \cdot 0 + 1)$ jne.)

Koska joukossa C on $n + 1$ eri lukua, on oltava sellaiset luvut $b, c \in C$ ja $k_0 \in \{0, 1, ..., n-1\}$, että $b = 2^{d_1}(2k_0+1)$ ja $c = 2^{d_2}(2k_0+1)$, missä $d_1, d_2 \in \mathbb{N}$. Jos $d_1 \leq d_2$, on $b \mid c$. Jos taas $d_1 \geq d_2$, on $c \mid b$. $\square$

Ratkaisu 2. (E.H.) Olkoon $B_1 = \{1, 2, ..., n\}$ ja $B_2 = \{n + 1, ..., 2n\}$, jolloin $B = B_1 \cup B_2$. Olkoon $C_1 \subset B_1 \cap C$ ja $C_2 = B_2 \cap C$, jolloin $C = C_1 \cup C_2$. On oltava $C_1 \neq \emptyset$ ja $C_2 \neq \emptyset$. Numeroidaan joukkojen C_1 ja C_2 luvut seuraavasti: $C_1 = \{c_1, ..., c_k\}$ ja $C_2 = \{c_{k+1}, ..., c_{n+1}\}$.

Tehdään vastaoletus, että joukossa C ei ole sellaisia lukuja b, c että $b \mid c$. Jokaiselle luvulle $c_j \in C_1$ on sellaiset luvut $b_j \in B_2$ ja $d_j \in \mathbb{N} \setminus \{0\}$ että $b_j = 2^{d_j} c_j$. Vastaoletuksen nojalla on oltava $b_j \notin C_2$ kaikilla $j \in \{1, ..., k\}$. Siis joukossa B_2 on oltava vähintään k kappaletta sellaisia lukuja, jotka eivät kuulu joukkoon C_2. Mutta tämä on mahdotonta, sillä joukossa $C_2 \subset B_2$ on $n - k + 1$ lukua ja joukossa B_2 on n lukua. $\square$

Ratkaisu 3. (A.K.) Viimeisenä on vielä induktiotodistus: Alkuaskel $n = 1$ on selvä. Induktio-oletus: Jos $B = \{1, 2, ..., 2k\}$ ja joukossa $C \subset B$ on $k + 1$ eri lukua, joukossa C on sellaiset luvut b, c että $b \mid c$.

Todistetaan induktioväite: Olkoon $B = \{1, 2, ..., 2k + 2\}$ ja olkoon joukossa $C \subset B$ $k + 2$ eri lukua. Mikäli joukon C luvuista vähintään $k + 1$ lukua on joukosta $\{1, 2, ..., 2k\}$, induktio-oletuksen nojalla väite seuraa. Oletetaan nyt, että joukon C luvuista vain minimimäärä k kappaletta on joukosta $\{1, 2, ..., 2k\}$. Tällöin $(2k + 1) \in C$ ja $(2k + 2) \in C$. Olkoon $C_1 = \{1, 2, ..., 2k\} \cap C$, jolloin siis joukossa C_1 on k eri lukua. Mikäli $(k + 1) \in C_1$, olemme löytäneet vaaditut luvut, sillä myös $(2k + 2) \in C$. Oletetaan seuraavaksi, että $(k + 1) \notin C_1$. Tällöin induktio-oletuksen nojalla joukossa $C_1 \cup \{k+1\}$ on oltava luvut b, c siten että $b \mid c$. Mikäli $b \neq k+1$ ja $c \neq k+1$, on $b, c \in C_1 \subset C$ ja väite seuraa. Mikäli taas $k + 1$ on toinen luvuista b, c, on oltava $k + 1 = c$ (muussa tapauksessa olisi $c \geq 2(k + 1)$, mikä ei ole mahdollista, sillä $c \in \{1, 2, ..., 2k\}$). Koska $k + 1 = c$, luku $b \in C_1 \subset C$ jakaa luvun $k + 1$, joten luku b jakaa myös luvun $(2k + 2) \in C$. Induktioväite on todistettu. $\square$