Diofantoksen yhtälön ratkaisut

Matias Mäkelä
Matemaattisten tieteiden tutkinto-ohjelma
Oulun yliopisto
Kevät 2017

Sisältö

Johdanto

Tämän tutkielman pääasiana on Diofantoksen yhtälön $ax + by = c$ ratkaiseminen ja ratkaisujen olemassaolo. Sitä ennen esitellään suurin yhteinen tekijä ja Eukleideen algoritmi, joitten avulla saadaan Diofantoksen yhtälön tarkastelu tehtyä. Lisäksi käsitellään lineaarisen kongruenssiyhtälön ratkaisemista ja ratkaisujen olemassaoloa. Tutkielmassa on käytetty lähteenä teosta [1].

1 Suurin yhteinen tekijä

Lause 1. *Olkoot a ja b kokonaislukuja, joista ainakin toinen on nollasta eroava. Jos d on suurin sellainen positiivinen kokonaisluku, että $d|a$ ja $d|b$, niin on olemassa sellaiset kokonaisluvut x ja y, että $d = ax + by$.*

Todistus. Olkoon epätyhjä joukko $A = \{ax+by \mid a, b, x, y \in \mathbb{Z},\ ax+by > 0\}$. Olkoon d' joukon A pienin alkio, joten on olemassa sellaiset x_1 ja y_1, että $d' = ax_1 + by_1$. Lisäksi on olemassa alkiot q ja r, joilla

$$a = d'q + r,\ 0 \leq r < d'.$$

Osoitetaan, että $d' \mid a$. Toisin sanoen, tulemme näyttämään, että $r = 0$. Tehdään vastaoletus $r \neq 0$, jolloin

$$r = a - d'q = a - (ax_1 + by_1)q.$$

Tällöin

$$r = a(1 - x_1q) + b(-y_1q).$$

Oletuksen nojalla tiedämme, että $r \neq 0$. Täten on selvää, että $r > 0$ ja $r = ax_2 + by_2$, jossa $x_2 = 1 - x_1$ ja $y_2 = -y_1q$. Tämän pitäisi kuitenkin olla mahdotonta oletuksen nojalla, sillä d' on joukon A pienin alkio. Täten $r = 0$, josta seuraa $d' \mid a$. Samoin voidaan osoittaa, että $d' \mid b$. Siis d' on alkioiden a ja b yhteinen jakaja.

Olkoon m kokonaislukujen a ja b yhteinen tekijä. Siten $m \mid ax_1 + by_1$ ja täten $m \mid d'$, mistä seuraa, että $m \leq d'$. Näin d' on suurin kokonaislukujen a ja b yhteisistä tekijöistä eli

$$d' = d = ax + by \text{ kaikilla } x, y \in \mathbb{Z}.$$

□

Huomautus 1. Edellisen lauseen positiivinen kokonaisluku d on yksikäsitteinen. Jos on kaksi positiivista kokonaislukua d_1 ja d_2 näillä omaisuuksilla, niin $d_1 \leq d_2$ ja $d_2 \leq d_1$. Täten $d_1 = d_2$.

Edellisestä lauseesta seuraa tulos:

Seuraus 2. Jokaisella kokonaisluvulla e, joilla on $e \mid a$ ja $e \mid b$, seuraa $e \mid d$.

Määritelmä 1. Olkoon a ja $b \in \mathbb{Z}$, missä ainakin toinen kokonaisluvuista ei ole nolla. Kokonaislukua $d > 0$ kutsutaan alkioiden a ja b *suurimmaksi yhteiseksi tekijäksi* (jota merkitään $d = \text{syt}(a, b)$) jos ja vain jos $d \mid a$ ja $d \mid b$ sekä kaikilla positiivisilla kokonaisluvuilla e, joilla on $e \mid a$ ja $e \mid b$, pätee $e \mid d$.

Lause 3. *Olkoon $d = \text{syt}(a_1, a_2, \ldots, a_n)$, missä a_1, a_2, …, $a_n \in \mathbb{Z}$. Tällöin*

$$\text{syt}\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right) = 1.$$

Todistus. On selvää, että $d|a_1$, $d|a_2$, …, $d|a_n$. Täten

$$a_1 = k_1 d, a_2 = k_2 d, \ldots, a_n = k_n d, \tag{1}$$

missä $k_1 \in \mathbb{Z}$ jokaisella $i = 1, 2, \ldots, n$. Olkoon

$$\text{syt}\left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right) = d' > 1.$$

Vastaavasti saadaan

$$d' \mid \frac{a_1}{d}, d' \mid \frac{a_2}{d}, \ldots, d' \mid \frac{a_n}{d}.$$

Tästä seuraa, että on olemassa $k_1', k_2', \ldots, k_n'$, joille

$$\frac{a_1}{d} = k_1' d', \frac{a_2}{d} = k_2' d', \ldots, \frac{a_n}{d} = k_n' d'. \tag{2}$$

Tällöin yhtälöryhmien (1) ja (2) nojalla saadaan

$$a_1 = k_1' d' d, a_2 = k_2' d' d, \ldots, a_n = k_n' d' d.$$

Täten,

$$d'd \mid a_1, d'd \mid a_2, \ldots, d'd \mid a_n.$$

Siten, $dd'|d$, mikä on mahdotonta sillä $d' > 1$. Täten $d' = 1$. □

Lause 4. *Olkoon a, b ja $c \in \mathbb{Z}$ ja $a|bc$. Jos $\text{syt}(a, b) = 1$, niin $a|c$.*

Todistus. Jos $\text{syt}(a, b) = 1$, niin

$$1 = ax + by, \text{ missä } x, y \in \mathbb{Z}.$$

Täten

$$c = acx + bcy.$$

Koska $a|acx$ ja $a|bcy$, niin $a|c$. □

2 Eukleideen algoritmi

Olkoon a ja b kokonaislukuja. Yksi tapa kokonaislukujen a ja b suurimman yhteisen tekijän tuottamiseen on löytää pienin luku joukosta

$$A = \{ax + by \mid a, b, x, y \in \mathbb{Z},\ ax + by > 0\}.$$

On kuitenkin olemassa paljon tehokkaampi keino suurimman yhteisen tekijän löytämiseen. Sitä kutsutaan *Euklidiseksi algoritmiksi* ja seuravassa näytämme, miten se toimii.

Jos haluamme tuottaa suurimman yhteisen tekijän $\text{syt}(a, b)$, ilman että menettäisimme oletuksen $b \leq a$. Siis $\text{syt}(a, b) = \text{syt}(b, r)$, missä r on jakojäännös alkiosta a jaettuna alkiolla b. Tämä tapahtuu, koska $a = bq + r$ tai $r = a - bq$, jollakin kokonaisluvulla q ja siten $\text{syt}(a, b) \mid r$. Lisäksi $\text{syt}(a, b) \mid b$. Täten suurimman yhteisen tekijän määritelmän nojalla saadaan

$$\text{syt}(a, b) \mid \text{syt}(b, r). \tag{3}$$

Samoin, koska $a = bq + r$, saamme $\text{syt}(b, r) \mid b$ ja $\text{syt}(b, r) \mid a$. Täten

$$\text{syt}(b, r) \mid \text{syt}(a, b). \tag{4}$$

Yhtälöryhmistä (3) ja (4) saadaan yhtälö $\text{syt}(a, b) = \text{syt}(b, r)$. Jos $b = a$, niin $\text{syt}(a, b) = \text{syt}(a, 0) = \text{syt}(0, b) = a = b$ ja algoritmi päättyy. Yleensä saadaan kuitenkin

$$\text{syt}(a, b) = \text{syt}(b, r_1) = \text{syt}(r_1, r_2) = \cdots = \text{syt}(r_{n-1}, r_n) = \text{syt}(r_n, 0) = r_n,$$

missä

$$\begin{gathered}
a = bq_1 + r_1, b \leq a \\
b = r_1 q_2 + r_2, 0 \leq r_1 < b \\
r_1 = r_2 q_3 + r_3, 0 \leq r_2 < r_1 \\
\vdots \\
r_{n-2} = r_{n-1} q_n + r_n, 0 \leq r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} + 0, 0 \leq r_n < r_{n-1}.
\end{gathered}$$

Tällöin r_n on lukujen a ja b suurin yhteinen tekijä.

Esimerkki 1. Olkoot kokonaisluvut 1234 ja 250 ja lasketaan niiden suurin yhteinen tekijä. Tällöin Eukleideen algoritmin avulla

$$1234 = 4 \cdot 250 + 234, 250 \leq 1234$$

$$250 = 1 \cdot 234 + 16, 0 \leq 234 < 250$$

$$234 = 14 \cdot 16 + 10, 0 \leq 16 < 234$$

$$16 = 1 \cdot 10 + 6, 0 \leq 10 < 16$$

$$10 = 1 \cdot 6 + 4, 0 \leq 6 < 10$$

$$6 = 1 \cdot 4 + 2, 0 \leq 4 < 6$$

$$4 = 2 \cdot 2 + 0 \leq 2 < 4.$$

Tällöin Eukleideen algoritmin nojalla $\text{syt}(1234, 50) = 2$.

3 Diofantoksen yhtälön ratkaisut

Lause 5. *Olkoon a, b ja c kokonaislukuja, joista ainakin a tai b ovat erisuuria kuin nolla. Jos $d = \text{syt}(a, b)$ ja $d \mid c$, niin Diofantoksen yhtälöllä*

$$ax + by = c$$

on äärettömän monta ratkaisua

$$x = x_0 + \frac{b}{d}n, \; y = y_0 - \frac{a}{d}n,$$

missä n on kokonaisluku ja (x_0, y_0) on yhtälön ratkaisu. Jos d ei jaa kokonaislukua c, niin Diofantoksen yhtälöllä

$$ax + by = c$$

ei ole ratkaisua.

Todistus. Tapaus 1. Jos $d \mid c$, niin on olemassa kokonaisluku k, jolla $c = kd$. Koska d on kokonaislukujen a ja b suurin yhteinen tekijä, Lauseen 1 mukaan on olemassa kokonaisluvut k_1 ja k_2, joilla saadaan yhtälö

$$d = k_1 a + k_2 b,$$

ja siten

$$c = kk_1 a + kk_2 b.$$

Tällöin on ainakin yksi pari kokonaislukuja $x_0 = kk_1$ ja $y_0 = kk_2$, jotka ovat Diofantoksen yhtälön ratkaisuja. Pitää osoittaa, että on äärettömän monta ratkaisua ja varsinkin muodossa

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 + \frac{a}{d}n,$$

jossa (x, y) on Diofantoksen yhtälön mielivaltainen ratkaisu. Tällöin meillä on

$$ax + by = c$$

ja

$$ax_0 + by_0 = c.$$

Täten

$$a(x - x_0) + b(y - y_0) = 0$$

eli

$$a(x - x_0) = b(y_0 - y),$$

joten

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{5}$$

Täten

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0).$$

Koska

$$\text{syt}(\frac{a}{d}, \frac{b}{d}) = 1,$$

niin

$$\frac{b}{d} \mid (x - x_0).$$

On siis olemassa kokonaisluku n, jolla saadaan yhtälö

$$x = x_0 + n\frac{b}{d}. \tag{6}$$

Tehdään oletus, että b ei ole nolla. Tällöin yhtälöiden (5) ja (6) nojalla saadaan

$$\frac{a}{d} \cdot n \cdot \frac{b}{d} = \frac{b}{d}(y_0 - y)$$

eli

$$\frac{a}{d}n = y_0 - y$$

eli

$$y = y_0 - \frac{a}{d}n.$$

Tapauksessa $a \neq 0$ menetelmä on samanlainen ja päättyy samaan tulokseen. Tällöin kiinnitetylle kokonaisluvulle n saadaan pari (x, y), missä

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n,$$

joka on yhtälön $ax + by = c$ ratkaisu. Jos t on sellainen kokonaisluku, että

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t,$$

niin

$$\begin{aligned} c &= a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) \\ &= ax_0 + \frac{ab}{d}t + by_0 - \frac{ba}{d}t \\ &= ax_0 + by_0, \end{aligned}$$

mikä pitää paikkansa. Täten Diofantoksen yhtälöllä $ax + by = c$ on ääretön määrä ratkaisua

$$x = x_0 + \frac{b}{d}n, \quad y = y_0 - \frac{a}{d}n,$$

missä n on kokonaisluku.

Tapaus 2. Oletetaan, että d ei jaa lukua c. Kuitenkin $d \mid a$ ja $d \mid b$, joten

$$d \mid ax + by,$$

joten $d \mid c$, mikä on ristiriita. Tässä tapauksessa Diofantoksen yhtälöllä $ax + by = c$ ei ole yhtään ratkaisua. □

Esimerkki 2. Olkoon kokonaisluvut $a = 12$, $b = 21$ ja $c = 100$. Tällöin $\text{syt}(12, 21) = 3$. Kuitenkaan kokonaisluku 3 ei jaa kokonaislukua 100, joten Diofantoksen yhtälöllä

$$12x + 21y = 100$$

ei ole ratkaisua.

Esimerkki 3. Olkoon kokonaisluvut $a = 18$, $b = 28$, ja $c = 24$. Tällöin $\text{syt}(18, 28) = 2$. Nyt $2 \mid 24$ eli Diofantoksen yhtälöllä

$$18x + 28y = 24,$$

on äärettömän monta ratkaisua

$$x = x_0 + 14n, \; y = y_0 - 9n,$$

missä n on kokonaisluku.

4 Lineaarisen kongruenssiyhtälön ratkaisut

Lause 6. *Olkoon a ja b kokonaislukuja ja m luonnollinen luku. Jos $d = \text{syt}(a, m)$ ja $d \mid b$, niin lineaarisella kongruenssiyhtälöllä*

$$ax \equiv b \pmod{m}$$

on d kappaletta pareittain erilaisia ratkaisuja modulo m. Jos d ei jaa kokonaislukua b, niin lineaarisella kongruenssiyhtälöllä ei ole ratkaisua.

Huomautus 2. Kaksi ratkaisua x_1 ja x_2 ovat erilaiset jos ja vain jos ne eivät ole ekvivalentteja toistensa kanssa modulo m.

Todistus. Tapaus 1. Jos $d \mid b$, niin lineaarisella kongruenssiyhtälöllä $ax \equiv b \pmod{m}$ on ratkaisu, jos Diofantoksen yhtälöllä

$$ax - my = b \tag{7}$$

on ratkaisu. Yhtälöllä (7) on äärettömän monta ratkaisua

$$x = x_0 - \frac{m}{d}n,$$

missä (x_0, y_0) on yhtälön (7) ratkaisu. Aiomme osoittaa, että äärettömän monesta lineaarisen kongruenssiyhtälön

$$ax \equiv b \pmod{m}$$

ratkaisuista ainostaan pareittain erilaisia ovat d kappaletta. Huomataan, että kaikki kokonaisluvut

$$x_0, x_0 - \frac{m}{d}, x_0 - 2\frac{m}{d}, \cdots, x_0 - (d-1)\frac{m}{d}$$

ovat lineaarisen kongruenssiyhtälön $ax \equiv b \pmod{m}$ ratkaisuja. Nämä ratkaisut ovat parettain erilaiset, sillä jos olisi sellaiset ratkaisuparit, jossa

$$x_0 - n_1\frac{m}{d} \equiv x_0 - n_2\frac{m}{d} \pmod{m},$$

missä n_1 ja n_2 ovat kokonaislukuja sekä $1 \leq n_1 < n_2 \leq d-1$, niin

$$n_1\frac{m}{d} \equiv n_2\frac{m}{d} \pmod{m}$$

eli

$$m \mid (n_1 - n_2)\frac{m}{d}.$$

Tästä seuraa, että

$$d \mid (n_1 - n_2),$$

joka on ristiriita, sillä $1 \leq n_1 < n_2 \leq d-1$. Tällöin ratkaisut

$$x_0, x_0 - \frac{m}{d}, x_0 - 2\frac{m}{d}, \cdots, x_0 - (d-1)\frac{m}{d}$$

ovat parettain erilaiset. Aiomme nyt todistaa, että lineaarisella kongruenssiyhtälöllä $ax \equiv b \pmod{m}$ ei ole muita kuin pareittain erilaiset ratkaisut.

Olkoon kokonaisluku k lineaarisen kongruenssiyhtälön ratkaisu, mutta erilainen kuin aikaisemmat. Tällöin

$$ak \equiv b \pmod{m},$$

kun tiedämme, että $ax_0 \equiv b \pmod{m}$ on myös voimassa. Tällöin saadaan

$$ak \equiv ax_0 \pmod{m}. \tag{8}$$

Koska $\text{syt}(a, m) = d$, niin

$$a = \lambda_1 d, \ m = \lambda_2 d,$$

missä λ_1 ja λ_2 ovat kokonaislukuja. Yhtälön (8) nojalla saadaan

$$\lambda_1 dk \equiv \lambda_1 dx_0 \pmod{\lambda_2 d}.$$

Täten

$$\lambda_2 \mid \lambda_1(k - x_0).$$

Koska $\text{syt}(\lambda_1, \lambda_2) = 1$, niin

$$\lambda_2 \mid (k - x_0).$$

Tällöin on olemassa sellainen kokonaisluku ν, että

$$k = x_0 + \nu\lambda_2.$$

Jakoalgoritmilla saadaan

$$\nu = dq + r,$$

missä q ja r, $0 \leq r < d$, ovat kokonaislukuja. Tästä saadaan

$$\begin{aligned} k &= x_0 + d\lambda_2 q + \lambda_2 r \\ &= x_0 + mq + \frac{m}{d}r \end{aligned} \tag{9}$$

ja täten

$$mq = k - (x_0 + \frac{m}{d}r).$$

Näin

$$k \equiv x_0 + \frac{m}{d}r \pmod{m},$$

missä $0 \leq r \leq d-1$. Tällöin k ei ole yhtälölle uusi pareittain erilainen ratkaisu, mikä on ristiriidassa oletuksen kanssa. Tämä todistaa väitteen, että lineaarisella kongruenssilla

$$ax \equiv b \pmod{m}$$

on d kappaletta pareittain erilaisia ratkaisuja modulo m.

Tapaus 2. Jos d ei jaa kokonaislukua b, niin Diofantoksen yhtälöllä

$$ax - my = b$$

ei ole ratkaisua. Täten lineaarisella kongruenssilla

$$ax \equiv b \pmod{m}$$

ei ole myöskään ratkaisua. □

Huomautus 3. Silloin, kun $\text{syt}(a, m) = 1$, lineaarisella kongruensilla $ax \equiv b \pmod{m}$ on yksikäsitteinen ratkaisu.

Esimerkki 4. Olkoot kokonaisluvut $a = 7$ ja $b = 11$ sekä luonnollinen luku $m = 21$. Tällöin $\text{syt}(7, 21) = 3$, mutta kokonaisluku 7 ei jaa kokonaislukua 11. Tällöin lineaarisella kongruenssilla $7x \equiv 11 \pmod{21}$ ei ole yhtään ratkaisua.

Esimerkki 5. Olkoot kokonaisluvut $a = 8$ ja $b = 12$ sekä luonnollinen luku $m = 20$. Tällöin $\text{syt}(8, 20) = 4$ ja $4 \mid 12$. Tällöin lineaarisella kongruenssilla $8x \equiv 12 \pmod{20}$ on 4 kappaletta pareittain erilaisia ratkaisuja.

Lähdeluettelo

[1] Michael Th. Rassias: *Problem-Solving and Selected Topics in Number Theory; In the Spirit of the Mathematical Olympiads*, Spinger, 2011.