Diofantoksen yhtälö

Diofantos (antiikin kreikkalainen) tutki kokonaislukukertoimisia yhtälöitä, joista tällä kurssilla tarkastellaan 1. asteen muotoisia

$$ax + by = c$$

yhtälöitä. Diofantoksen yhtälöitä ovat myös esim. $x^n + y^n = z^n$. Tärkeää on havaita, että Diofantoksen yhtälön $ax + by = c$ *kertoimet* a, b *ja* c *ovat kokonaislukuja* $(\neq 0)$ ja *ratkaisuiksi hyväksytään vain kokonaisluvut*.

Esimerkki Aiemmin on saatu tulos $12 = 3 \cdot 84 - 2 \cdot 120$ eli

$$84 \cdot \overbrace{3}^{x} + 120 \cdot \overbrace{(-2)}^{y} = 12.$$

Onko muita ratkaisuja x, y?
Kyllä on, osoittautuu, että esimerkiksi luvut $x = -117$ ja $y = 82$ toteuttavat yhtälön, jolloin

$$84 \cdot (-117) + 120 \cdot 82 = -9\,828 + 9\,840 = 12.$$

Lause, Diofantoksen yhtälö $ax + by = c$:
Olkoon syt$(a, b) = 1$ ja olkoon x_0, y_0 Diofantoksen yhtälön

$$(1) \qquad ax + by = c$$

ns. *yksityisratkaisu*. Tämän yhtälön *yleinen ratkaisu* on

$$(2) \qquad \begin{cases} x = x_0 + b \cdot t \\ y = y_0 - a \cdot t \end{cases}, \qquad t \in \mathbb{Z},$$

missä t on mielivaltainen kokonaisluku.
Toisin sanoen: Jos x ja y ovat muotoa (2), niin ne toteuttavat yhtälön (1) ja käänteisesti; Jokainen yhtälön (1) ratkaisu on muotoa (2).

Todistus Hetken kuluttua.

Huomautus **1)** Sytin ei tarvitse olla 1 → tähän palataan.
2) Kohdan (2) x:n ja y:n lausekkeissa pitää nimenomaan kertoimet a ja b ”olla ristikkäin alkup. yht. nähden ja eri etumerkit”, syy selviää.

Esimerkki(jatkuu) Jaetaan yhtälö $84 \cdot x + 120 \cdot y = 12$ luvulla 12,

$$\Longrightarrow \qquad 7x + 10y = 1$$

Siis $a = 7$, $b = 10$ ja $c = 1$. Eukleideen algoritmilla saatiin $x_0 = 3$ ja $y_0 = -2$.
Koska nyt $\text{syt}(7, 10) = 1$, voidaan edellisen lauseen nojalla kirjoittaa yleinen ratkaisu, saadaan

$$\begin{cases} x = 3 + 10 \cdot t \\ y = -2 - 7 \cdot t \end{cases}, \qquad t \in \mathbb{Z}.$$

Tulos voidaan tarkistaa antamalla muuttujalle $t \in \mathbb{Z}$ eri arvoja. Kun
$t = 0$, niin $7 \cdot 3 + 10 \cdot (-2) = 21 - 20 = 1$, OK
$t = 1$, niin $7 \cdot (3 + 10) + 10 \cdot (-2 - 7) = 91 - 90 = 1$, OK
$t = -8$, niin $7 \cdot (3 - 80) + 10 \cdot (-2 + 56) = -539 + 540 = 1$, OK

Lauseen todistus
Jos x ja y ovat muotoa (2), niin $\quad (2) \quad \begin{cases} x = x_0 + b \cdot t \\ y = y_0 - a \cdot t \end{cases}, \qquad t \in \mathbb{Z}$

$$\begin{aligned} ax + by &= a(x_0 + bt) + b(y_0 - at) \\ &= ax_0 + abt + by_0 - bat \\ &= ax_0 + by_0 = c, \end{aligned}$$

joten ne toteuttavat yhtälön (1). Tässä näkyy Huom./kohta 2:n syy.

Lauseen todistus(jatkuu) Jos käänteisesti $x\ (\neq x_0)$ ja $y\ (\neq y_0)$ toteuttavat yhtälön (1), niin $ax + by = c$. Oletuksen nojalla on voimassa myös yhtälö $ax_0 + by_0 = c$, joten

$$c - c = ax + by - ax_0 - by_0 = 0$$

josta edelleen

$$a(x - x_0) = -b(y - y_0) \quad \Longrightarrow \quad \frac{x - x_0}{y - y_0} = -\frac{b}{a}.$$

Koska $\text{syt}(a, b) = 1$, oikea puoli ei enää supistu, joten vasemman puolen osoittaja ja nimittäjä ovat oikean puolen osoittajan ja nimittäjän *sama monikerta*. Tämä tarkoittaa sitä, että löytyy sellainen $t \in \mathbb{Z}$, että

$$\begin{cases} x - x_0 = bt \\ y - y_0 = -at \end{cases} \quad \Longrightarrow \quad \begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases}.$$

Siis x ja y ovat muotoa (2).

Yleisesti on todettava, ettei Diofantoksen yhtälöllä ole aina ratkaisua.
Esimerkki Mitä voit sanoa Diofantoksen yhtälön $2x + 4y = 3$ ratkaisun olemassaolosta?

Esimerkki(jatkuu) Diofantoksen yhtälön $2x + 4y = 3$ vasen puoli on aina jaollinen luvulla 2, kun taas oikea puoli ei ole jaollinen 2:lla. Näin ollen ratkaisua ei ole olemassa millään x ja y. Toisaalta tätä yhtälöä ei voida esittää sellaisena Diofantoksen yhtälönä $ax + by = c$, jossa $\text{syt}(a, b) = 1$. On siis aihetta otaksua ratkaisun olemassaolon liittyvän jollakin tavoin $\text{syt}(a, b)$:ään.

Lause, Diofantoksen yhtälön $ax + by = c$ ratkeavuus:
Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu (ja edellisen lauseen nojalla ∞ monta ratkaisua) **jos ja vain jos** luku c on $\text{syt}(a, b)$:n monikerta.

Todistus Olkoon $\text{syt}(a, b) = d$. Tällöin

$$\begin{cases} a = dm \\ b = dn \end{cases}, \quad \text{missä } \text{syt}(m, n) = 1.$$

Muutoin olisi $ds > d$ yhteinen tekijä. Todistus on **jos ja vain jos**, joten

"⟹" vain jos -suunta Jos Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu x_0, y_0, yhtälön $ax_0 + by_0 = c$ vasen puoli on jaollinen luvulla d, joten oikea puolikin on jaollinen luvulla d. Siis c on d:n monikerta.

"⟸" jos-suunta Jos c on luvun d monikerta eli $c = dp$ jollakin $p \in \mathbb{Z}$, niin Diofantoksen yhtälö $ax + by = c$ saa muodon

$$dmx + dny = dp \quad \Leftrightarrow \quad mx + ny = p.$$

Koska $\text{syt}(m, n) = 1$, löytyy Eukleideen algoritmilla sellaiset luvut x_0, y_0, että $mx_0 + ny_0 = 1$.
Nyt

$$\begin{aligned} apx_0 + bpy_0 &= dmpx_0 + dnpy_0 \\ &= dp(mx_0 + ny_0) = dp \cdot 1 = dp = c. \end{aligned}$$

Siis yhtälöllä $ax + by = c$ on ratkaisu $\begin{cases} x = px_0 \\ y = py_0 \end{cases}$. Itse asiassa ääretömän monta ratkaisua, edellinen lause:

$$\begin{cases} x = px_0 + nt \\ y = py_0 - mt \end{cases}, \quad t \in \mathbb{Z}.$$

Esimerkki Ratkaise Diofantoksen yhtälö $18x + 14y = 4$. Tässä on kaksi eri tapaa ratkaista yhtälö.

Aluksi, koska $\text{syt}(18, 14) = 2$ ja luku 4 on jaollinen luvulla 2 on ratkaisu olemassa.

TAPA 1: Yhtälö $18x + 14y = 4$ voidaan kirjoittaa muodossa $9x + 7y = 2$. Etsitään aluksi luvut x_0, y_0 siten, että $9x_0 + 7y_0 = 1$. Eukleideen algoritmi ja syt:n lauseke antavat:

$$\begin{aligned} 9 &= 7 \cdot 1 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned} \quad \longrightarrow \quad \begin{aligned} 1 &= 7 \cdot 1 - 2 \cdot 3 \\ &= 7 \cdot 1 - (9 - 7 \cdot 1) \cdot 3 \\ &= 7 \cdot 4 - 9 \cdot 3 \\ &= 9 \cdot (-3) + 7 \cdot 4 \end{aligned}$$

Siis, yhtälön $9x_0 + 7y_0 = 1$ yksityisratkaisu on $\begin{cases} x_0 = -3 \\ y_0 = 4 \end{cases}$ ja yleinen ratkaisu on muotoa $\begin{cases} x = -3 + 7t \\ y = 4 - 9t \end{cases}$, $t \in \mathbb{Z}$. Näin ollen yhtälön $18x + 14y = 4$, eli yhtälön $9x + 7y = 2$ yksityisratkaisu on $\begin{cases} x_0 = -6 \\ y_0 = 8 \end{cases}$ ja ylei-nen ratkaisu on $\begin{cases} x = -6 + 7t \\ y = 8 - 9t \end{cases}$, $t \in \mathbb{Z}$.

Tarkastellaan vielä lopuksi miksi kertoimet $a = 9$ ja $b = 7$ menevät ns. ristiin yleisessä ratkaisussa.

Huomautus

$$9 \cdot x + 7 \cdot y = 2$$

$$9 \cdot (-6 + 7t) \qquad 7 \cdot (8 - 9t)$$

$$9 \cdot 7t = 63 \cdot t \qquad 7 \cdot (-9t) = -63 \cdot t$$

Nämä osiot kumoavat toisensa kaikilla muuttujan $t \in \mathbb{Z}$ arvoilla. Siksi pitää nimenomaan kertoimet mennä ristiin ja etumerkit olla eri, jotta kumoutuminen tapahtuisi.

Eli vaikka eri ratkaisulukuparit x_0, y_0 toteuttavat yhtälön, niin ne ovat sidoksissa toisiinsa.

TAPA 2: Tarkastellaan vain yhtälöä $18x + 14y = 4$. Yksityisratkaisu x_0, y_0 ensin ja yleinen ratkaisu saadaan suoraan muodosta

$$\begin{cases} x = x_0 + \dfrac{b}{\text{syt}(a,b)} \cdot t \\ y = y_0 - \dfrac{a}{\text{syt}(a,b)} \cdot t \end{cases} \Rightarrow \begin{cases} x = -6 + \dfrac{14}{2} \cdot t = -6 + 7t \\ y = 8 - \dfrac{18}{2} \cdot t = 8 - 9t \end{cases}, t \in \mathbb{Z}$$

Yksityisratkaisussa määritetään sytin lauseke, tässä $2 = 18 \cdot ? \pm 14 \cdot ?$.