Pellin yhtälöstä

Ratkaisun olemassaolo

Olkoon m positiivinen kokonaisluku, joka ei ole neliö. Pellin[1] yhtälö on Diofantoksen yhtälö
$$x^2 - my^2 = 1. \tag{1}$$
Yhtälöllä on triviaaliratkaisut $x = \pm 1$, $y = 0$.

Olkoon q jokin positiivinen kokonaisluku. Tarkastellaan irrationaalilukuja $-k\sqrt{m}$, $k = 1, \ldots, q+1$. Jokaiseen tällaiseen lukuun voidaan lisätä kokonaisluku x_k niin, että
$$0 < x_k - k\sqrt{m} < 1.$$
Näiden väliin $(0, 1)$ kuuluvan $q+1$:n luvun joukossa on laatikkoperiaatteen nojalla aina ainakin kaksi sellaista, esimerkiksi $x_k - k\sqrt{m}$ ja $x_{k'} - k'\sqrt{m}$, joiden keskinäinen etäisyys on pienempi kuin $\dfrac{1}{q}$. Mutta jos asetetaan $x = x_k - x_{k'}$ ja $y = k - k'$, niin
$$0 < |x - y\sqrt{m}| < \frac{1}{q}. \tag{2}$$
Lisäksi $|y| \le q$. Siis
$$\begin{aligned} |x^2 - my^2| &= |x - y\sqrt{m}||x + y\sqrt{m}| \\ &< \frac{1}{q}|x - y\sqrt{m} + 2y\sqrt{m}| \le \frac{1}{q}\left(\frac{1}{q} + 2q\sqrt{m}\right) < 1 + 2\sqrt{m}. \end{aligned} \tag{3}$$
Jokaista epäyhtälön (2) toteuttavaa lukuparia kohden voidaan löytää uusi pari esimerkiksi valitsemalla uusi $q > |x - y\sqrt{m}|$. Kokonaislukupareja, jotka toteuttavat epäyhtälön (3) on siis äärettömän monta. Mutta tämä merkitsee, että jollakin kokonaisluvulla $r < 1 + 2\sqrt{m}$ yhtälöllä
$$x^2 - my^2 = r$$
on äärettömän monta kokonaislukuratkaisua.

Nämä äärettömän monta lukua omaavat vain äärellisen määrän jakojäännöspareja $\bmod r$. On siis luvut x_1, x_2, missä $x_1 \equiv x_2 \bmod r$, ja y_1, y_2, missä $y_1 \equiv y_2 \bmod r$, niin, että
$$x_1^2 - my_1^2 = r, \quad x_2^2 - my_2^2 = r,$$
ja $y_1^2 \ne y_2^2$. Mutta tällöin $x_1y_2 \equiv x_2y_1 \bmod r$ eli $x_1y_2 - x_2y_1 = y'r$, missä y' on kokonaisluku, ja
$$\begin{gathered} r^2 = (x_1^2 - my_1^2)(x_2^2 - my_2^2) = x_1^2x_2^2 + m^2y_1^2y_2^2 - m(x_1^2y_2^2 + x_2^2y_1^2) \\ = (x_1x_2 - my_1y_2)^2 - m(x_1y_2 - x_2y_1)^2 = (x_1x_2 - my_1y_2)^2 - mr^2y'^2. \end{gathered}$$

[1] John Pell (1611–85) oli englantilainen matemaatikko, diplomaatti ja pappi. Ei ole varmaa tietoa siitä, että hän olisi mitenkään ollut tekemisissä Pellin yhtälön kanssa.

Nyt on myös luvun $x_1x_2 - my_1y_2$ oltava r:llä jaollinen, siis muotoa rx', x kokonaisluku. Siis $x'^2 - my'^2 = 1$. Pellin yhtälöllä on siis jokin kokonaislukuratkaisu. Se, että $y' \neq 0$ seuraa yhtälöistä $x_1^2 - my_1^2 = r$, $x_2^2 - my_2^2 = r$; kun näistä eliminoidaan m, saadaan $x_1^2y_2^2 - x_2^2y_1^2 = r(y_2^2 - y_1^2)$. Jos olisi $y' = 0$, olisi $x_1y_2 = x_2y_1$ ja $y_1^2 = y_2^2$, vastoin edellä tehtyjä valintoja.

Ratkaisuja on monta

Olkoon nyt $(a,\, b)$ jokin yhtälön (1) ratkaisu. Tarkastellaan lukuja

$$(a + b\sqrt{m})^k = x_k + y_k\sqrt{m}.$$

Tässä x_k on muotoa $\binom{k}{2j}a^{k-2j}(b\sqrt{m})^{2j}$ olevien termien summa ja y_k muotoa $\binom{k}{2j+1}a^{k-2j-1}(b\sqrt{m})^{2j+1}$ olevien termien summa. Tällöin $(a - b\sqrt{m})^k = x_k - y_k\sqrt{m}$ ja $x_k^2 - my_k^2 = (x_k + y_k\sqrt{m})(x_k - y_k\sqrt{m}) = (a + b\sqrt{m})^k(a - b\sqrt{m})^k = (a^2 - mb^2)^k = 1$. Jokainen pari $(x_k,\, y_k)$ on siis yhtälön (1) ratkaisu. Koska $a + m\sqrt{m} \neq 1$, parit $(x_k,\, y_k)$ eivät ole samoja. Pellin yhtälöllä (1) on siis äärettömän monta ratkaisua.

Olkoon erityisesti $(a,\, b)$ se yhtälön (1) ratkaisu, jolle $a + b\sqrt{m}$ on positiivinen ja mahdollisimman pieni. Kaikki yhtälön (1) ratkaisut ovat silloin lukupareja $(\pm x_k,\, \pm y)$, missä $x_k + y_k\sqrt{m} = (a + b\sqrt{m})^k$. Olkoon $(x,\, y)$, missä x ja y ovat positiivisia, jokin yhtälön (1) ratkaisu. Silloin jollakin k on

$$(a + b\sqrt{m})^k \leq x + y\sqrt{m} < (a + b\sqrt{m})^{k+1}$$

eli

$$1 \leq (x + y\sqrt{m})(a - b\sqrt{m})^k = xx_k - myy_k + (x_ky - y_kx)\sqrt{m} < a + b\sqrt{m}. \tag{4}$$

Mutta koska $(x+y\sqrt{m})(x_k - y_k\sqrt{m})(x - y\sqrt{m})(x_k + y_k\sqrt{m}) = (x^2 - my^2)(a_k - mb_k) = 1$, pari $(xx_k - myy_k,\, yx_k - xy_k)$ on yhtälön (1) ratkaisu. Epäyhtälön (4) ja $a + b\sqrt{m}$:n minimaalisuuden nojalla tämän ratkaisun on oltava triviaaliratkaisu. Yhtälöparista

$$\begin{cases} x_kx - my_ky = 1 \\ -y_kx + x_ky = 0 \end{cases}$$

ratkaistaan $(x_k^2 - my_k^2)y = y_k$ eli $y = y_k$ ja $x = x_k$. Väite on todistettu.

Edellä olevia ajatuksia voi lukea myös niin että kahdesta samasta tai eri yhtälön ratkaisusta $(x,\, y)$ ja $(x',\, y')$ voi muodostaa uuden ratkaisun $(xx' + myy',\, yx' + xy')$, sillä $(xx' + myy')^2 - m(xy' + x'y)^2 = (x^2x'^2 + m^2y^2y'^2 - mx^2y'^2 - mx'^2y^2 = (x^2 - my^2)(x'^2 - my'^2) = 1$. Lähtemällä minimiratkaisusta voidaan näin rakentaa jono ratkaisuja $(x_k,\, y_k)$; voidaan osoittaa, että tässä jonossa ovat kaikki ratkaisut, joissa x ja y ovat positiivisia.

Ratkaisun löytäminen

Pellin yhtälön (1) ratkaisun löytämiseksi voi lähteä tarkastelemaan jonoa $m+1$, $4m+1$, $9m+1$, ...; pienin b, jolla mb^2+1 on neliö, antaa minimiratkaisun. Esimerkiksi yhtälön

$$x^2 - 3y^2 = 1$$

minimiratkaisu on (2, 1). Koska $(2+\sqrt{3})^2 = 7+4\sqrt{3}$ ja $(2+\sqrt{3})^3 = 26+15\sqrt{3}$, ratkaisuja ovat esimerkiksi (7, 4) ja (26, 15) (ja esimerkiksi (137379191137, 79315912984), joka saadaan luvusta $(2+\sqrt{3})^{20}$). m:stä riippuen jonoa mk^2+1 joudutaan tutkimaan välillä kovin pitkään.

Toinen ratkaisualgoritmi perustuu *ketjumurtolukuihin*. Tässä sivuutetaan perustelut. Käytetään lyhennysmerkintää

$$[a_0;\, a_1,\, a_2,\, a_3,\, a_4,\, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\ldots}}}}}.$$

Tässä a_i:t ovat ei-negatiivisia kokonaislukuja. Jokainen positiivinen rationaaliluku voidaan kirjoittaa (Eukleideen algoritmin avulla) päättyväksi ketjumurtoluvuksi, ja jokainen päättyvä ketjumurtoluku on rationaaliluku. Jokainen positiivinen irrationaaliluku A voidaan kirjoittaa yksikäsitteisellä tavalla päättymättömäksi ketjumurtoluvuksi yksinkertaisella algoritmilla: a_0 on A.n kokonaisosa, a_1 A:n desimaaliosan käänteisluvun kokonaisosa jne.

Erityisesti jokainen toisen asteen yhtälön irrationaalinen ratkaisu ja siten jokainen irrationaaliluku $\sqrt{m}$ tuottaa *jaksollisen* ketjumurtoluvun. Kun tarkastellaan $\sqrt{m}$:n ketjumurtolukukehitelmän alkuosaa $A_k = [a_0;\, a_1,\, a_2 \ldots,\, a_k] = \dfrac{p_k}{q_k}$, missä p_k:lla ja q_k:lla ei ole yhteisiä tekijöitä, ominaisuuksia, niin päädytään havaitsemaan, että yhtälön (1) minimiratkaisu on $(p_j,\, q_j)$, missä $j = lh-1$, h $\sqrt{m}$:n jakson pituus, ja $2l = 3-(-1)^h$. Kaikki ratkaisut saadaan pareista $(p_{lhk-1},\, q_{lhk-1})$, $k = 1, 2, \ldots$. Erityisen mukavia ovat luvut $m = n^2+1$. Tällöin $\sqrt{m} = [n; 2n,\, 2n,\, \ldots]$, joten $h = 1$, $m = 2$ ja $j = 1$, josta seuraa, että minimiratkaisu on $(2n^2+1,\, 2n)$. Esimerkiksi yhtälön $x^2 - 50y^2 = 1$ minimiratkaisu on (99, 14). Toisaalta Pellin yhtälöjen ratkaisut saattavat olla melko hankalia. Matematiikan historiassa mainitaan usein Bhaskaran[2] yhtälö $x^2 - 61y^2 = 1$. Luvun $\sqrt{61}$ ketjumurtokehitelmän jakson pituus on 11:

$$\sqrt{61} = [7;\, 1,\, 4,\, 3,\, 1,\, 2,\, 2,\, 1,\, 3,\, 4,\, 1,\, 14,\, \ldots].$$

Minimiratkaisuksi tulee (1766319049, 226153980).

[2] Bhaskara II (1114–85) jatkoi ansiokkaasti Brahmaguptan (598–670) alkuun panemaa Pellin yhtälöiden tutkimusta Intiassa.