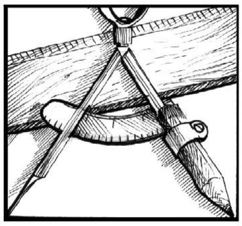


Diofantoksen ongelmat

Kalevi Suominen
Professori, matematiikan laitos, Helsingin yliopisto

1. *Etsittävä kaksi lukua, joista ensimmäisen kuution ja toisen luvun summa on sama kuin lukujen summan kuutio.*

2. *Jaettava annettu luku kahteen osaan, joiden tulo on erään luvun kuution ja itse luvun erotus.*

Nämä tehtävät ovat esimerkkejä yli sadasta antiikin matematiikan ongelmasta, jotka kreikkalainen matemaatikko Diofantos kokosi nimellä "*Aritmetiikka*" tunnettuun tehtäväkokoelmaansa. Teos on säilynyt vain osaksi, eikä sen historiaa tunneta. Itse Diofantos eli Egyptin Aleksandriassa luultavasti roomalaisajan loppuolella, erään arvion mukaan 200-luvulla.

Yhteistä kaikille Diofantoksen ongelmille on, että niissä luvuilla tarkoitetaan rationaalilukuja; reaalilukuja ei tehtäviä laadittaessa vielä tunnettu. Siksi niiden ratkaisemiseen on käytettävä erilaisia keinoja kuin nykyisin tavanmukaisissa tehtävissä.

Esimerkiksi tehtävä 1 on nykyaikaisin merkinnöin helppo muotoilla yhtälöksi

$$x^3 + y = (x+y)^3. \tag{1}$$

Tämä on kolmannen asteen algebrallinen yhtälö kahden tuntemattoman, x:n ja y:n suhteen. Se toteutuu aina, kun $y = 0$, mutta on selvää, että Diofantos ei etsinyt tällaista ratkaisua. Jos luvulle x annetaan jokin kiinteä, riittävän pieni arvo, voidaan y aina valita niin, että yhtälö toteutuu. Mitään takeita ei kuitenkaan ole siitä, että saatu ratkaisu olisi rationaalinen. Asiaa ei auta, vaikka y valittaisiin ensin rationaaliseksi ja sitten ratkaistaisiin x.

Vaikka tehtävä siis vaikuttaakin aluksi helpolta, kun siinä asetetaan vain yksi ehto kahdelle tuntemattomalle, niin tällainen vapaus osoittautuukin ratkaisun suurimmaksi esteeksi! Itse asiassa voidaan ajatella, että ratkaisujen rationaalisuus on lisäehto, joka vastaa vähintään yhtä yhtälöä. Tämä on luonteenomaista kaikille Diofantoksen ongelmille.

Ratkaisut

Diofantoksen esittämät ratkaisut perustuvat siihen, että asetetaan uusia ehtoja tuntemattomien välille, kunnes yhtälöitä on yhtä monta kuin tuntemattomia. Silloin ratkaisuja jää vain äärellinen määrä. Jos ehdot on vielä valittu siten, että ratkaisu on yksikäsitteinen, niin sen löytäminen ei edes vaadi juurenottoa ja tulos on rationaalinen.

Esimerkiksi yhtälöstä (1) saadaan sijoituksella $y = 2x - 1$ kolmannen asteen yhtälö

$$0 = 26x^3 - 27x^2 + 7x. \tag{2}$$

Tällä on kolme ratkaisua: Triviaali juuri $x = 0$, arvoa $y = 0$ vastaava toinen juuri $x = 1/2$ ja lopuksi etsitty juuri $x = 7/13$. Ratkaisu on rationaalinen, koska se on oleellisesti yksikäsitteinen, kun arvoja $x = 0$ ja $y = 0$ vastaavia erikoistapauksia ei lasketa.

Tehtävä 2 voidaan käsitellä samalla tavoin. Jos annettu luku on 6, kuten Diofantos olettaa esimerkissään, ja sen osat ovat x ja $6-x$, niin ratkaistavaksi tulee yhtälö

$$y^3 - y = x(6-x). \tag{3}$$

Lisäehdon $y = 3x - 1$ avulla voidaan eliminoida y, ja jäljelle jää yhtälö

$$27x^3 - 26x^2 = 0. \tag{4}$$

Kun kaksinkertaista triviaalia juurta $x = 0$ ei oteta huomioon, saadaan ratkaisuksi $x = 26/27$, joka ainoana epätriviaalina juurena on välttämättä rationaalinen.

Edellä käsitellyt tehtävät osoittavat, että Diofantoksen ongelmien ratkaisu on helppoa – ainakin sen jälkeen, kun on keksitty sopiva lisäehto tuntemattomien välille. Eteen tuleekin väistämättä kysymys, miten tällainen ehto löydetään. Diofantoksen kirja ja muut antiikin lähteet eivät anna mitään viitteitä yleisestä menetelmästä, vain suuren joukon yksittäisiä esimerkkejä.

Geometrinen tulkinta

Diofantoksen ongelmien ratkaisuperiaatteen ymmärtämiseksi on hyödyllistä tulkita yhtälöt geometrisesti. Kahden tuntemattoman yhtälöt, kuten esimerkiksi (1) ja (3), kuvaavat algebrallisia tasokäyriä. Usein tuntemattomia on useampia, mutta samalla myös ehtoja on enemmän ja ne esittävät edelleen algebrallista käyrää jossakin korkeampiulotteisessa avaruudessa.

Ensimmäinen vaihe Diofantoksen ongelman ratkaisussa on tavallisesti käyrän jakaminen komponentteihinsa. Esimerkiksi kumpikin yhtälöistä (1) ja (3) on kolmatta astetta, mutta niiden esittämät käyrät ovat oleellisesti erilaiset. Jälkimmäinen on jaoton, kun taas edellinen jakautuu kahdeksi komponentiksi: suoraksi $y = 0$ ja ellipsiksi

$$3x^2 + 3xy + y^2 = 1. \tag{5}$$

Tehtävä yksinkertaistuu, kun kutakin komponenttia tarkastellaan erikseen. Niinpä edellä yhtälön $y = 0$ ratkaisut ovat triviaaleja eivätkä kelpaa vastaukseksi; tutkittavaksi jää siten vain ellipsi (5).

Rationaaliset pisteet

Algebrallisilla käyrillä on yleensä ääretön määrä pisteitä, joiden koordinaatit ovat reaalilukuja. Myös sellaisia pisteitä on paljon, joiden toinen koordinaatti on rationaalinen. Pisteitä, joiden kumpikin koordinaatti on rationaalinen, on sen sijaan usein vain äärellinen määrä. Tällaisia pisteitä sanotaan käyrän *rationaalisiksi pisteiksi*. Geometrisesti tarkasteltuna Diofantoksen ongelma on siis sama kuin *algebrallisen käyrän rationaalisten pisteiden määrittäminen*.

Kun ratkaistaan kahden tuntemattoman yhtälöitä, myös jokainen lisäehto tuntemattomien välillä esittää tasokäyrää. Esimerkiksi tehtävän 1 ratkaisussa ehto $y = 2x - 1$ kuvaa suoraa. Lisäehdon toteuttavat ratkaisut ovat siten samat kuin käyrien yhteiset pisteet. Diofantoksen ongelman ratkaisemiseksi on siis asetettava lisäehto siten, että *käyrien leikkauspisteet ovat rationaaliset*.

Ensi näkemältä tämä ajatus ei juuri vaikuta käyttökelpoiselta. Kun ollaan vasta etsimässä rationaalisia pisteitä, miten niitä voitaisiin käyttää hyväksi? Tilanne ei kuitenkaan ole toivoton. Käytännössä on usein mahdollista löytää eräitä "ilmeisiä" rationaalisia pisteitä, jotka eivät kelpaa etsityiksi ratkaisuiksi. Tällaisia ovat tyypillisesti käyrän leikkauspisteet koordinaattiakselien kanssa. Esimerkiksi yhtälöllä (5) on ilmeiset rationaaliset ratkaisut $x = 0$ ja $y = \pm 1$.

Triviaalien, ilmeisten ratkaisujen lisäksi tarvitaan tietenkin vielä kelvollisiakin ratkaisuja. Miten voidaan taata, että tällaiset toistaiseksi tuntemattomatkin käyrien leikkauspisteet olisivat rationaalisia? Ongelman ratkaisee seuraava tulos:

Jos kahden käyrän leikkauspisteet ovat rationaaliset mahdollisesti yhtä pistettä lukuunottamatta, niin ne kaikki ovat rationaalisia.

Tämän todistamiseksi tarvitsee vain eliminoida toinen tuntemattomista. Tällöin saadaan yhden tuntemattoman polynomiyhtälö, ja sen juuret mahdollisesti yhtä lukuunottamatta ovat rationaaliset. Koska juurien summa on rationaalinen, on viimeinenkin juuri välttämättä rationaalinen.

Ratkaisuperiaate

Edellä esitetyn perusteella voidaan nyt ilmaista *Diofantoksen ongelmien ratkaisuperiaate*: Etsitään ongelmaan liityvän käyrän "ilmeiset" rationaaliset pisteet ja asetetaan lisäehtoa vastaava käyrä kulkemaan niistä mahdollisimman monen kautta. Jos tämä on mahdollista tehdä siten, että yhtä lukuunottamatta kaikki käyrien leikkauspisteet ovat näitä rationaalisia pisteitä, niin myös viimeinenkin leikkauspiste on rationaalinen.

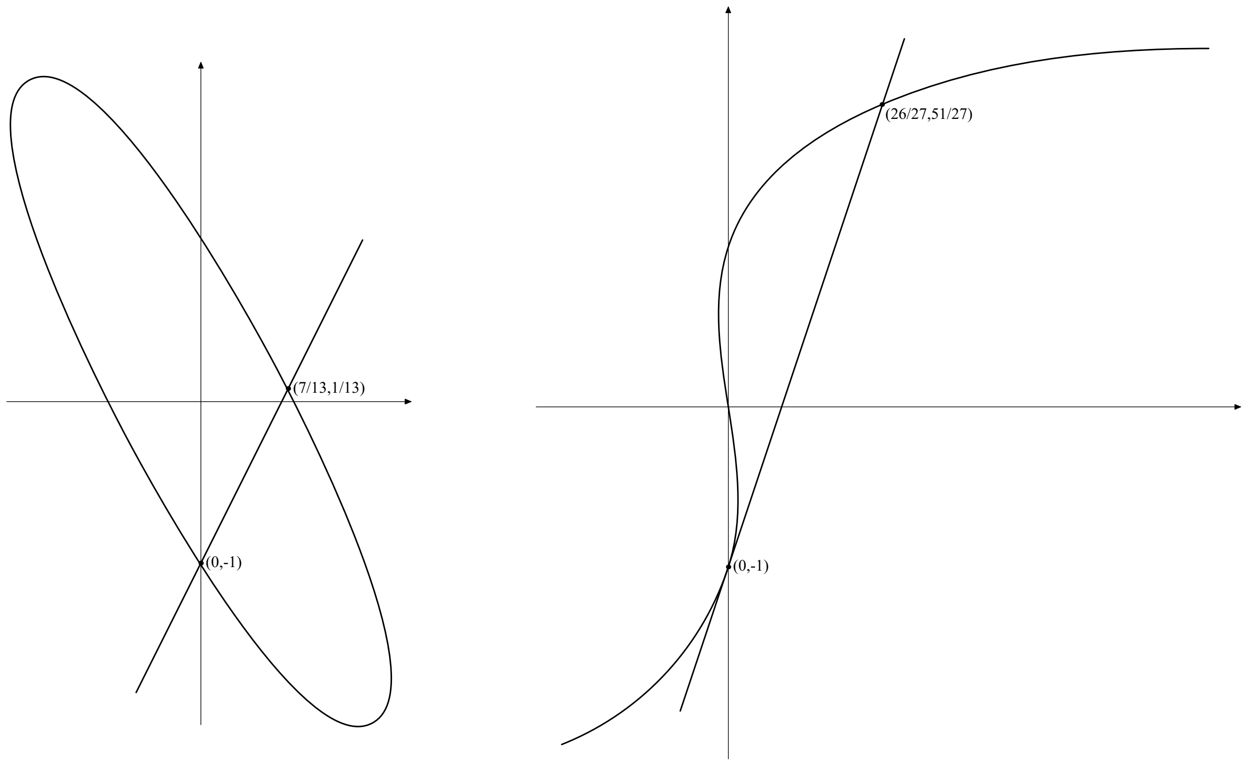
Esimerkiksi tehtävän 1 ratkaisussa asetettiin lisäehto $y = 2x - 1$. Se kuvaa suoraa, joka kulkee ellipsin (5) triviaalin rationaalisen pisteen $(0, -1)$ kautta. Tämän ohella se leikkaa ellipsin vain yhdessä pisteessä, kuten jo edellä nähtiin, ja tämä piste $(7/13, 1/13)$ on myös rationaalinen.

Tarkastelu osoittaa lisäksi, että suoran kulmakerroin voidaan valita vapaasti. Siihen käy mikä tahansa rationaaliluku. Näin ellipsillä on ääretön määrä rationaalisia pisteitä, jotka voidaan esittää rationaalisen parametrin avulla. Algebrallisia käyriä, joilla on tämä ominaisuus, sanotaan *rationaalisiksi käyriksi*. Moniin Diofantoksen esittämiin ongelmiin liittyvät käyrät ovat rationaalisia, ja siten niillä on paljon ratkaisuja Diofantoksen kuvaamien lisäksi.

Tehtävä 2 osoittautuu oleellisesti erilaiseksi. Aluksi havaitaan, että käyrä (3) leikkaa y-akselin rationaalisissa pisteissä $(0, \pm 1)$ ja $(0, 0)$. Jos nyt asetetaan lisäehto, joka kuvaa esimerkiksi pisteen $(0, -1)$ kautta kulkevaa suoraa, niin tämä leikkaa käyrän (3) vielä kahdessa pisteessä. Nämä leikkauspisteet toteuttavat toisen asteen yhtälön, ja siten ne eivät yleensä ole rationaalisia.

Ongelma ratkeaa, kun suora valitaan kulkemaan kahden rationaalisen pisteen kautta. Ratkaisun kannalta on tärkeää huomata, että näiden ei tarvitse olla eri pisteitä. Kahden käyrän leikkauspiste voi näet olla moninkertainen, kun käyrät sivuavat toisiaan. Niinpä käyrän (3) tapauksessa lisäehdon kuvaajaksi voidaan valita tangentti pisteessä $(0, -1)$. Tämän yhtälö on $y = 3x - 1$, jota jo edellä käytettiin. Vastaava menettely on mahdollinen myös muiden rationaalisten pisteiden $(0, 0)$ ja $(0, 1)$ kohdalla. Näin saaduista rationaalisista pisteistä voidaan edelleen johtaa uusia joko tangenttien avulla tai sitten kahden eri pisteen kautta kulkevilla sekanteilla.

Tehtävän 2 tapauksessa lisäehtojen valinnassa on siis paljon vähemmän valinnan vapautta kuin tehtävässä 1. Yhtälön (3) kuvaama käyrä on esimerkki ns. *elliptisestä käyrästä*. Nimi tulee siitä, että käyrän pisteitä voidaan esittää *elliptisillä funktioilla*; itse käyrä ei ole ellipsi. Tällaisen käyrän rationaalisten pisteiden joukko ei välttämättä ole ääretön.



Kuva 1: Tehtävien 1 ja 2 ratkaisut annetuilla lisäehdoilla, yhtälö (5) vasemmalla ja yhtälö (3) oikealla.

Lisätehtäviä.

1. Etsittävä Diofantoksen ongelman 1. kaikki rationaaliset ratkaisut.

2. Etsittävä Diofantoksen ongelman 2. ratkaisu, kun annettu luku ei ole 6.

3. Etsittävä useita rationaalisia pisteitä käyrältä (3).

4. Etsittävä kaksi lukua, joiden summan suhde niiden neliöiden summaan on annettu luku.

5. Etsittävä kaksi lukua, joiden summa on sama kuin niiden kuutioiden summa.