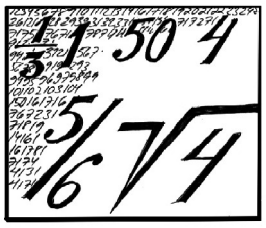

Näennäisen triviaalit temput matematiikassa

Anne-Maria Ernvall-Hytönen
Helsingin yliopisto

Tässä tekstissä on tarkoitus käsitellä kahta harvinaisen triviaalilta tuntuvaa ajatusta:

1. Jos summaan lisätään nolla, ei summan arvo muutu.
2. Ykkönen on pienin positiivinen kokonaisluku. (Toisinaan tämä on myös hyödyllistä muotoilla muotoon "Kahden peräkkäisen kokonaisluvun erotus on yksi.")

Kumpikin väite on täysin triviaali. Niillä voi kuitenkin saada yllättävän paljon aikaiseksi. En pysty kirjoittamaan yleistä teoriaa siitä, miten näitä tulisi käyttää – lähinnä ideana on ensimmäisen kohdan kanssa se, että yritetään muokata lauseketta sellaiseen muotoon, jota on helpompi käsitellä esimerkiksi vähentämällä siitä joku luku ja lisäämällä sama luku toiseen kohtaan lauseketta. Toinen kohta taas usein soveltuu esimerkiksi kokonaislukujen joukossa arviointiin. Näitä ideoita onkin helpoin valottaa esimerkein.

Summan arvo ei muutu, jos lisätään nolla

Polynomien arviointi

Halutaan selvittää, mikä on polynomin $p(x) = x^2 + 6x$ pienin mahdollinen arvo reaalilukujen joukossa. Tämän voisi tehdä derivoimalla, mutta ei tehdä nyt sitä, vaan täydennetään neliöksi:

$$p(x) = x^2 + 6x = x^2 + 6x + 9 - 9 = (x-3)^2 + 9.$$

Nollan lisääminen tehtiin lisäämällä ja vähentämällä yhdeksän. Tämä tehtiin, koska siten saatiin polynomiin siisti neliölauseke ja lisäksi vakio. Nyt on helppo nähdä, että $p(x) \geq 9$ ja lisäksi 9 todella on sen pienin arvo, sillä $p(3) = 9$.

Kongruenssin laskusäännön todistaminen

Todistetaan seuraavaksi, että jos $a \equiv b \pmod{n}$ ja $c \equiv d \pmod{n}$, niin $ac \equiv bd \pmod{n}$. Kirjoitetaan kongruessi ensin jaollisuuden avulla. Oletukset ovat $n \mid a - b$ ja $n \mid c - d$. Väitetään, että $n \mid ac - bd$. Nyt on hyödyllistä vähentää ja lisätä termi ad, jolloin saadaan

$$ac - bd = ac - ad + ad - bd = a(c-d) + d(a-b).$$

Koska $c - d$ ja $a - b$ ovat oletusten nojalla jaollisia luvulla n, on erotus $ac - bd$ jaollinen luvulla n.

Yllä oleva olisi yhtä hyvin voitu tehdä myös vähentämällä ja lisäämällä termi bc:

$$ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d).$$

Oleellista on lisätä ja vähentää jokin sellainen termi, jonka avulla erotus saadaan esitettyä muodossa, jossa on selkeästi luvulla n jaollisia termejä.

Jaollisuus ja induktio

Osoitetaan induktiolla, että $6^n - 1$ on jaollinen viidellä, kun $n \geq 0$. Tämän pystyisi helposti tekemään kongruenssien avulla, mutta tehdään todistus nyt induktiolla niin, että saadaan jälleen yksi esimerkki siitä, miten nollan lisääminen voi olla hyödyllistä.

Induktion alkuaskel: Kun $n = 0$, saadaan $6^0 - 1 = 0$, joka on jaollinen viidellä. Alkuaskel on siis kunnossa.

Induktio-oletus: Oletetaan, että väite pätee, kun $n = k$, eli luku $6^k - 1$ on jaollinen viidellä.

Induktioväite: Väitetään, että $6^{k+1} - 1$ on jaollinen viidellä.

Todistetaan nyt induktioväite. Tärkeää on päästä käyttämään induktio-oletusta. Tämä voidaan tehdä monella eri tavalla. Otetaan nyt yksi esimerkki:

$$6^{k+1} - 1 = 6^{k+1} - 6^k + 6^k - 1.$$

Lisäämällä ja vähentämällä termi 6^k saadaan lausekkeeseen osa, joka on suoraan induktio-oletuksesta. Lisäksi pitää vielä käsitellä lausekkeen alkuosa. Kirjoitetaan

$$6^{k+1} - 6^k = 6^k(6 - 1) = 5 \cdot 6^k,$$

joka on triviaalisti jaollinen viidellä. On siis saatu

$$6^{k+1} - 1 = 5 \cdot 6^k + 6^k - 1,$$

missä ensimmäinen termi oikealla on triviaalisti viidellä jaollinen ja loppuosa on induktio-oletuksen nojalla viidellä jaollinen. Väite on todistettu.

Wienerin hyökkäys RSA-kryptojärjestelmään

RSA-kryptojärjestelmästä olen kirjoittanut aiemminkin. Eräs hyökkäys järjestelmää kohtaan tunnetaan Wienerin hyökkäyksenä. Sen matemaattinen pohja on itse asiassa ketjumurtolukujen teoriassa. Luvun ketjumurtokehitelmästä katkaisemalla saatavia lukuja kutsutaan konvergenteiksi. Esimerkiksi siis luvun

$$3 + \frac{1}{2 + \frac{1}{4}}$$

konvergentteja ovat luvun itsensä lisäksi myös luvut 3 ja $3 + \frac{1}{2}$. Näille pätee erilaisia hyviä ominaisuuksia. Erityisesti niillä voidaan approksimoida lukuja poikkeuksellisen hyvin. Eräs hyödyllinen tulos on seuraavanlainen: Jos

$$\left|\xi - \frac{r}{s}\right| \leq \frac{1}{2s^2},$$

niin $\frac{r}{s}$ on luvun ξ *konvergentti*. Luvun konvergentit on laskettavissa tehokkaasti. Käytännössä RSA:ssa on kyse siitä, että on julkinen eksponentti e, salainen eksponentti d ja modulo n. Salaus onnistuu, jos tiedetään e ja n, ja salauksen purkaminen puolestaan, jos tiedetään d ja n. Julkinen eksponentti ja modulo ovat julkisia. Modulo n jakautuu kahden keskenään erisuuren alkuluvun tuloksi $n = pq$, ja nämä alkutekijät ovat salaisia. Salaisen eksponentin d saa laskettua, jos tietää nämä tekijät. Toisaalta, jos saa selvitettyä salaisen eksponentin, niin myös luvun n saa jaettua tekijöihin. Lukujen välinen yhteys on tämä:

$$ed \equiv 1 \pmod{\varphi(n)},$$

missä $\varphi(n) = (p-1)(q-1)$ on Eulerin φ-funktion arvo. Yllä oleva yhtälö voidaan siis kirjoittaa muodossa

$$ed - k\varphi(n) = 1$$

jollain k. Kyseessä on Diofantoksen yhtälö, jossa on käytännössä kolme tuntematonta. Jos saadaan selville $\varphi(n)$, saadaan selville myös p ja q ja voidaan ratkaista d. Jos saadaan selville d, tiedetään salainen eksponentti, jolloin salatut viestit voidaan purkaa. Kolmen tuntemattoman Diofantoksen yhtälölle on liikaa ratkaisuja, eli pelkän yhtälön tuijottelu ei ole hyvä idea. Jos tehdään oletus, että luvun n alkutekijät eivät ole keskenään kovin erisuuruisia, eli $p < q < 2p$, niin voidaan arvioida

$$\begin{aligned} n - \varphi(n) &= pq - (p-1)(q-1) \\ &= p + q - 1 \leq p + q < 3p < 3\sqrt{n}, \end{aligned}$$

jolloin luvut n ja $\varphi(n)$ ovatkin hyvin lähellä toisiaan. Oletetaan lisäksi, että $1 < e < \varphi(n)$, jolloin $k < d$. Lisäksi oletetaan $d \leq \frac{1}{3}n^{1/4}$ (eli tämä hyökkäys toimii, jos d on verrattain pieni). Tarkastellaan nyt erotusta

$$\left|\frac{e}{n} - \frac{k}{d}\right|.$$

Tämä on läheistä sukua sille, että yhtälö

$$ed \equiv 1 \pmod{\varphi(n)}$$

jaettaisiin puolittain luvuilla d ja $\varphi(n)$, jolloin saataisiin yhtälö

$$\frac{e}{\varphi(n)} - \frac{k}{d} = \frac{1}{d\varphi(n)}.$$

Helpointa on kuitenkin käyttää muotoa $ed - k\varphi(n) = 1$ ja sitä kautta hyödyntää lausekkeen ja yhtälön läheistä yhteyttä. Nyt voidaankin kirjoittaa

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \left|\frac{ed - nk}{dn}\right| = \left|\frac{ed - k\varphi(n) + k\varphi(n) - nk}{dn}\right|.$$

Olemme jälleen lisänneet termiin keskelle nollan lisäämällä ja vähentämällä saman termin. Tavoite oli yllä mainittua yhtälöä hyödyntämällä saada osa lausekkeesta arvioitua pieneksi ja sen jälkeen jatkaa loppuosan kanssa:

$$\begin{aligned} \left|\frac{ed - k\varphi(n) + k\varphi(n) - nk}{dn}\right| &= \left|\frac{1 + k\varphi(n) - nk}{dn}\right| \\ &\leq \left|\frac{k\varphi(n) - nk}{dn}\right|. \end{aligned}$$

Epäyhtälö perustuu siihen, että osoittajassa oli suuri negatiivinen osa ja pieni positiivinen, jolloin positiivinen voitiin arvioida pois. Koska $k < d$, voidaan arvioida

$$\left|\frac{k\varphi(n) - nk}{dn}\right| \leq \left|\frac{\varphi(n) - n}{n}\right| \leq \frac{3\sqrt{n}}{n} = \frac{3}{\sqrt{n}} \leq \frac{1}{2d^2},$$

jolloin $\frac{k}{d}$ saadaan laskemalla luvun $\frac{e}{n}$ konvergentit.

Tässä tilanteessa nollan lisäämisen voi nähdä kahdella (yhteenkietoutuvalla) tavalla: sen avulla saatiin osoittajaan kaksi erotusta, joista kumpikin osattiin käsitellä. Näin myös saatiin erotus yhdistettyä tunnettuun yhtälöön.

Ykkönen on pienin positiivinen kokonaisluku: kuinka tätä käytetään

Polynomit rationaalipisteissä

Tiedämme, että polynomilla $p(x) = x^2 - 2$ ei ole rationaalisia nollakohtia, vaan nollakohdat ovat $x = \pm\sqrt{2}$. Omalla laillaan luonnollinen kysymys onkin, miten lähelle nollaa päästään, jos lasketaan polynomin arvo jossain rationaalilukupisteessä. Selvää on, että ilman tarkempia rajoituksia voi todeta olevan mahdollista päästä mielivaltaisen lähelle nollaa. Jos nimittäin otetaan rationaaliluku u, jolla pätee $\sqrt{2} < u < \sqrt{2} + 10^n$, eli voidaan kirjoittaa $u = \sqrt{2} + \varepsilon$, niin

$$\begin{aligned} p(u) = p(\sqrt{2} + \varepsilon) &= (\sqrt{2} + \varepsilon)^2 - 2 \\ &= 2 + 2\sqrt{2}\varepsilon + \varepsilon^2 - 2 = 2\sqrt{2}\varepsilon + \varepsilon^2. \end{aligned}$$

Kun ε on hyvin pieni, saadaan polynomin arvo hyvin pieneksi. Lasketaan seuraavaksi raja, joka riippuu vain rationaaliluvun nimittäjästä. Olkoon $\frac{r}{s}$ rationaaliluku, joka on sievennetyssä muodossa. Nyt

$$\left|p\left(\frac{r}{s}\right)\right| = \left|\left(\frac{r}{s}\right)^2 - 2\right| = \left|\frac{r^2 - 2s^2}{s^2}\right|.$$

Tiedetään, että arvo ei voi olla nolla. Osoittajassa on kokonaislukujen tuloja ja erotuksia. Siispä osoittaja on kokonaisluku. Koska se ei ole nolla, on sen pakko olla itseisarvoltaan vähintään yksi. Siispä

$$\left|p\left(\frac{r}{s}\right)\right| = \left|\frac{r^2 - 2s^2}{s^2}\right| \geq \frac{1}{s^2}.$$

Lukijalle jätetään harjoitustehtäväksi osoittaa, että jos p on n. asteen polynomi, jolla ei ole rationaalisia nollakohtia, niin

$$\left|p\left(\frac{r}{s}\right)\right| \geq \frac{1}{s^n},$$

kun r ja s ovat kokonaislukuja ja $s \neq 0$.

Jaollisuustehtävä matematiikkaolympialaisista

Vuonna 1992 kansainvälisissä matematiikkaolympialaisissa oli seuraava tehtävä:

Määritä kaikki kokonaisluvut a, b ja c, $1 < a < b < c$, joille $(a-1)(b-1)(c-1)$ on luvun $abc - 1$ tekijä.

Jos $(a-1)(b-1)(c-1)$ on luvun $abc - 1$ tekijä, niin

$$\frac{abc - 1}{(a-1)(b-1)(c-1)}$$

on kokonaisluku. Arvioidaan

$$1 < \frac{abc - 1}{(a-1)(b-1)(c-1)} < \frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1}.$$

Funktio $f(x) = \frac{x}{x-1} = 1 + \frac{1}{x-1}$ on laskeva ykköstä suurempien lukujen joukossa, joten lauseke $\frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1}$ on mahdollisimman suuri, kun luvut a, b ja c ovat mahdollisimman pieniä. Tämä toteutuu, kun $a = 2$, $b = 3$ ja $c = 4$. Tässä on huomionarvoista, että tällaista arviota ei voitaisi tehdä, jos emme tietäisi lukujen olevan kokonaislukuja. Nyt

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} < \frac{2}{2-1} \cdot \frac{3}{3-1} \cdot \frac{4}{4-1} = 4.$$

Täytyy siis olla

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} = 2$$

tai

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} = 3.$$

Aloitetaan jälkimmäisestä tapauksesta. Huomaamme nimittäin, että osamäärä pienenee aika nopeasti, kun luvut kasvavat, jolloin intuitiivisesti tuntuu uskottavalta, että tämä tapaus on helpompi.

Jos $a \geq 3$, niin $b \geq 4$ ja $c \geq 5$, jolloin

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} < \frac{3}{3-1} \cdot \frac{4}{4-1} \cdot \frac{5}{5-1} = \frac{5}{2} < 3.$$

Tämä ei siis ole mahdollista. On oltava $a = 2$. Nyt siis

$$2bc - 1 = 3(2-1)(b-1)(c-1) = 3(b-1)(c-1).$$

Koska vasen puoli on pariton, on oikeankin puolen oltava pariton. Siispä b ja c ovat parillisia. Testataan pienimmällä mahdollisella luvun b arvolla: $b = 4$. Nyt

$$2 \cdot 4c - 1 = 3(4-1)(c-1),$$

eli

$$8c - 1 = 9(c-1),$$

josta ratkaistaan $c = 8$. Nyt on löydetty yksi ratkaisu. Osoitetaan seuraavaksi, että ei voi olla $b > 4$. Jos näin olisi, niin olisi vähintään $b = 6$ ja $c = 8$, jolloin olisi

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} < \frac{2}{2-1} \cdot \frac{6}{6-1} \cdot \frac{8}{8-1} = \frac{96}{35} < 3.$$

Jos siis osamäärä on kolme, on ainoa ratkaisu $a = 2$, $b = 4$ ja $c = 8$.

Siirrytään nyt toiseen tapaukseen, eli siihen, että osamäärä on kaksi. Nyt

$$abc - 1 = 2(a-1)(b-1)(c-1),$$

jolloin oikea puoli on parillinen. Jotta vasen puoli on myös parillinen, ovat a, b ja c parittomia. On siis $a \geq 3$, $b \geq 5$ ja $c \geq 7$.

Osoitetaan ensimmäiseksi, että ei voi olla $a > 3$. Jos näin olisi, niin olisi $a \geq 5$, $b \geq 7$ ja $c \geq 9$, ja tällöin

$$\frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{5}{4} \cdot \frac{7}{6} \cdot \frac{9}{8} = \frac{105}{64} < 2.$$

Siis on oltava $a = 3$. Testataan tapaus $b = 5$:

$$3 \cdot 5 \cdot c - 1 = 2(3-1)(5-1)(c-1),$$

eli

$$15c - 1 = 16(c-1),$$

jolloin $c = 15$ ja yksi ratkaisu on löytynyt. Osoitetaan vielä, että muita ratkaisuja ei ole. Riittää osoittaa, että ei voi olla $b > 5$. Jos näin olisi, olisi $b \geq 7$ ja $c \geq 9$, jolloin voisimme arvioida

$$\frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{3}{2} \cdot \frac{7}{6} \cdot \frac{9}{8} = \frac{63}{32} < 2,$$

eli ratkaisuja ei löydy. Ainoat ratkaisut ovat siis jo aiemmin löydetyt $a = 2$, $b = 4$ ja $c = 8$ sekä $a = 3$, $b = 5$ ja $c = 15$.

Tässä tehtävässä oleellista oli vedota kahteen itsestäänselvyyteen:

- Jos osamäärä on kahden peräkkäisen kokonaisluvun välissä, ei se voi olla kokonaisluku.
- Koska a, b ja c olivat kokonaislukuja ja keskenään erisuuria, kasvatti pienimmän luvun kasvattaminen usein myös kahta seuraavaa.

Luvun e irrationaalisuus

Osoitetaan Neperin luku e irrationaaliseksi. Olen kirjoittanut tästä aiemminkin, mutta aiemmin lähinnä irrationaalisuuden näkökulmasta, enkä niinkään todistuksen ideoita ajatellen. Tehdään vastaoletus: e on rationaalinen. Nyt siis $e = \frac{a}{b}$ joillakin positiivisilla kokonaisluvuilla a ja b. Tiedämme, että

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Sijoitetaan luvun e paikalle $e = \frac{a}{b}$ ja kerrotaan yhtälö puolittain jonkin sopivan positiivisen kokonaisluvun kertomalla $n!$. Nyt siis

$$an! = bn! \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Oikean puolen summa voidaan jakaa kahteen osaan:

$$bn! \sum_{k=0}^{\infty} \frac{1}{k!} = bn! \sum_{k=0}^{n} \frac{1}{k!} + bn! \sum_{k=n+1}^{\infty} \frac{1}{k!}.$$

Koska

$$bn! \sum_{k=0}^{n} \frac{1}{k!} = b \sum_{k=0}^{n} \frac{n!}{k!}$$

on varmasti kokonaisluku, on luvun

$$bn! \sum_{k=n+1}^{\infty} \frac{1}{k!} = an! - bn! \sum_{k=0}^{n} \frac{1}{k!}$$

oltava kahden kokonaisluvun erotuksena myös kokonaisluku. Lähdetään arvioimaan:

$$\begin{aligned} 0 < bn! \sum_{k=n+1}^{\infty} \frac{1}{k!} &= b \sum_{k=n+1}^{\infty} \frac{n!}{k!} \\ &= b \left(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots \right) \\ &\leq b \sum_{k=1}^{\infty} \frac{1}{(n+1)^k} \\ &= \frac{b}{(n+1)} \cdot \frac{1}{1 - \frac{1}{n+1}} = \frac{b}{n} < 1, \end{aligned}$$

kun valitaan $n > b$. Koska nollan ja ykkösen välissä ei ole kokonaislukuja, ei tämän lausekkeen arvo voi olla kokonaisluku. Väite on todistettu.

Loppusanat

Näillä ideoilla on varsin paljon käyttöä erilaisten matemaattisten ongelmien ratkaisussa. Esimerkiksi luvun e transkendenttimittaa arvioitaessa arvioidaan lineaarimuotoja, joille lähinnä saadaan ala-arvioksi, että ne varmasti ovat nollasta poikkeavia ja kokonaislukuarvoisia.