Lukuteorian helmiä lukiolaisille

Jukka Pihko
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

0. Taustaa

Sain 24.4.2007 Marjatta Näätäseltä sähköpostiviestin, jonka aihe oli "Fwd: yhteistyökurssi, Jukka, kiinnostaako?" Eteenpäin lähetetyn viestin olivat allekirjoittaneet Ressun lukion matematiikan opettajat Hilkka Taavitsainen, Mika Spåra ja Susanna Moksunen. Sen sisältönä oli ehdotus matematiikan kurssin järjestämiseksi Ressun lukiossa, tarkoituksena tarjota oppilaille mielenkiintoista matematiikkaa lukiokurssien ulkopuolelta. Mahdollisena aiheena mainittiin mm. lukuteoria. Hetkeäkään harkitsematta nielaisin syötin ja ilmoitin olevani halukas pitämään lukuteorian kurssin. Olen nimittäin usein ajatellut, että olisi hauskaa päästä esittelemään alaani koululaisille, mutta tähän suuntaavat pyrkimykseni oli aina enemmän tai vähemmän tylysti tyrmätty sillä seurauksella että olin jo kokonaan luopunut toivosta.

Hilkka Taavitsainen kutsui minut koululle 3.5.2007 ideoimaan kurssin sisältöä. Paikalla olivat myös muut edellä mainitut opettajat. Minulla oli valmis ehdotus kurssin ydinkohdista: Lagrangen lause neljän neliön summista (joka sanoo, että jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliön summana) ja Fermat'n Suuren Lauseen tapaus $n = 4$. Näistä edellinen on suurimpia suosikkejani: pidin siitä dosenttikoeluennon vuonna 1994. Mitä taas tulee jälkimmäiseen, niin se on ollut mielessäni sopivana aiheena Solmu-lehden kirjoitukseen, jota minulta on joskus pyydetty mutta jota en ole saanut aikaiseksi. Opettajilla ei ollut mitään ehdotustani vastaan vakuutettuani, että kyseiset melko 'kovat' tulokset voidaan todistaa suhteellisen helposti (vaikka ei ihan lyhyesti) lukuteorian peruskäsitteiden avulla. Palaverimme päättyi siihen, että Hilkka Taavitsainen lainasi minulle koulussa käytetyn oppikirjan [5] ja lupasin palata kurssin tarkempaan sisältöön tutustuttuani teokseen tarkemmin.

Kirjassa [5] mainitaan Aritmetiikan peruslause (joka sanoo, että jokainen ykköstä suurempi kokonaisluku voidaan esittää alkulukujen tulona, vieläpä tekijöiden järjestystä vaille yksikäsitteisesti), mutta jostakin syystä sitä ei todisteta. Kuten tulemme näkemään, todistus ei ole kovinkaan vaikea, mutta tätä lausetta, joka todella on nimensä veroinen, ei voi mitenkään pitää itsestään selvänä. Samassa kirjassa mainitaan myös täydelliset luvut ja Mersennen alkuluvut, mutta ei kerrota, että niiden välillä vallitsee läheinen yhteys. Koska kirjassa mainitaan Lagrangen lause (ilman todistusta) ja Fermat'n Suuri Lause ((tietenkin!) ilman todistusta), niin saatoin todeta, että kurssini, jonka pääkohdat olisivat 1) Aritmetiikan peruslauseen todistus, 2) Täydelliset luvut, Mersennen alkuluvut ja niiden välinen

yhteys, 3) Lagrangen lause neljän neliön summista ja 4) Fermat'n Suuri Lause tapauksessa $n = 4$, lähes saumattomasti liittyi Ressun lukiossa käytettyyn oppikirjaan [5]. Huomattakoon, että kurssin sisältö muodostui subjektiivisten mieltymysten ja sattuman vaikutusten tuloksena; jonkun toisen pitämä lukuteorian kurssi olisi todennäköisesti ollut täysin erilainen.

Kurssille piti sitten vielä keksiä vetävä nimi ja iskulauseita, joiden avulla sitä voisi mainostaa. Nimen "Lukuteorian helmiä" lainasin Khintsinin tunnetusta teoksesta [12]. Iskulauseita olivat mm. "koulukurssin ylittävää mutta kaikille ymmärrettävää lukuteoriaa" ja "kurssilla tehdään sukelluksia matematiikan historiaan". Viimeksi mainitulla tarkoitin sitä, että matematiikan ohessa kertoisin myös aiheeseen liittyvistä matemaatikoista. Näitä tarinoita en ole ottanut tähän mukaan, jottei esityksestä tulisi liian laaja. Sen sijaan viittaan netissä olevaan helppokäyttöiseen MacTutor-arkistoon [8], josta lukija saa tarvittaessa tietoja (ja kuvia) matemaatikoista. Eräässä toisessa mielessä (jos ajattelemme matemaattisia käsitteitä ja tuloksia) kurssilla oltiin itse asiassa sukelluksissa matematiikan historiassa lähes koko ajan 1700-luvulla ja sitä varhaisemmalla ajalla; vain sillöin tällöin nousimme pintaan, kurkistamaan periskoopista mitä nykyään tapahtuu. Tätä 'aihe'-historiaa käsittelen esityksessäni jonkin verran.

Syksyllä 2007 pidetylle "Lukuteorian helmiä"-kurssille ilmoittautui 14 oppilasta, joista kymmenkunta jaksoi seurata loppuun saakka. Osa oppilaista oli sellaisia, jotka eivät olleet suorittaneet "Lukuteoria ja logiikka"-kurssia. Minun oli siis aloitettava aivan peruskäsitteistä. Käytettävissä oli 13 tuntia (missä yksi tunti sisälsi 75 minuuttia). Tunteja oli kolme viikossa, joten jos ajatellaan että ensimmäinen tunti kului kurssin esittelyyn, niin kurssin neljälle kohdalle oli kullekin viikko varattuna. Aika riitti (omasta mielestäni) hyvin: sain sanottua sen mitä olin suunnitellut.

Kurssin päätyttyä mieleeni juolahti, että kurssimateriaali saattaisi kiinnostaa Solmun lukijoita. Sen lukeminen ei edellytä lukuteorian tuntemista, mutta vaatii ehkä hieman vaivannäköä. Tarkoitukseni on esittää yksityiskohtaiset todistukset, paitsi silloin kun asia on itsestään selvä tai kun todistus olisi samanlainen kuin joku aikaisemmin (tai myöhemmin) esitetty. Mitään yleiskuvaa lukuteoriasta en yritäkään antaa; kurssin nimeenkin viitaten tarkoitukseni on ainoastaan esitellä muutama tarkkaan valittu hieno tulos. (Luvussa 2 tämä on Eukleideen ja Eulerin antama karakterisointi parillisille täydellisille luvuille.) Luonnollisesti on eduksi, jos lukijalla on perustiedot lukuteoriasta tai käytettävissä [5] tai jokin vastaava lukion kirja (kahteen sellaiseen viitataan Apiolan Solmu-artikkelissa [2], joka on oheislukemisena myös paikallaan). Tukeudun esityksessäni pääasiassa Burtonin oppikirjaan [4], johon perustuvaa kurssia "Johdatus alkeelliseen lukuteoriaan" olen kolme kertaa luennoinut Helsingin yliopistossa. Tätä kirjaa voin suositella (ensimmäiseksi) jatkolukemiseksi sellaisille, joiden tiedonnälkää tämä Ressun lukiossa pitämäni kurssi ei saa tyydytetyksi; muitakin hyviä oppikirjoja on mainittu viitteissä.

Loppukevennyksen antakoon matemaatikko ja kirjailija Klaus Vala (1930–2000). Teoksessa *Nikolai Kval* [16] hän kirjoittaa kertomuksen "Kaksi, kolme ..." päätteeksi

sivulla 87: ”Arvelen kuitenkin voivani päätellä mihin suuntaan maailmankuulu baijerilainen olutkulttuuri on menossa. Olen nimittäin opiskellut joskus niinkin turhaa asiaa kuin lukuteoriaa. Kaikki me haksahdamme elämämme aikana joihinkin hullutuksiin.”

1. Aritmetiikan peruslauseen todistus

Induktioperiaatteen tavallinen ja 'vahva' muoto

Käytän muuten standardimerkintöjä, mutta **positiivisten kokonaislukujen joukolle** käytän merkintää $\mathbb{N}^*$. Toisin sanoen $\mathbb{N}^* = \mathbb{N}\backslash\{0\} = \{1, 2, 3, \dots\}$.

Induktioperiaatteen (johon lukija toivottavasti on törmännyt aikaisemminkin) taustalla on **hyvinjärjestysperiaatteeksi** joskus sanottu

Luonnollisten lukujen minimiominaisuus: Jokaisessa $\mathbb{N}$:n epätyhjässä osajoukossa on **pienin luku**.

Olkoon $n_0 \in \mathbb{N}$ kiinteä. Tarkastellaan muotoa

$$P(n) \text{ on tosi kaikilla } n \geq n_0 \tag{1.1}$$

olevaa väitettä, missä $P(n)$ on jokin luonnollisen luvun n ominaisuus. Jos todistetaan molemmat kohdat

1° $P(n_0)$ on tosi.
2° Olkoon $n > n_0$. Oletuksesta ('induktio-oletus')

$$P(n-1) \text{ on tosi}$$

seuraa, että $P(n)$ on tosi,

niin tällöin (1.1) on todistettu. Tämä on 'tavallinen' induktioperiaate. Kohta 1° on nimeltään **alkuaskel** ja kohta 2° on nimeltään **induktioaskel**. Hyppään tavallisen induktioperiaatteen todistuksen yli, koska se on hyvin samanlainen kuin 'vahvan' induktioperiaatteen (johon lukija kenties ei ole aikaisemmin törmännyt) todistus, jonka esitän. Korvataan edelläolevassa tarkastelussa kohta 2° kohdalla

$(2')^\circ$ Olkoon $n > n_0$. Oletuksesta ('vahva iduktio-oletus')

$$P(k) \text{ on tosi kun } n_0 \leq k \leq n-1$$

seuraa, että $P(n)$ on tosi.

'Vahva' induktioperiaate sanoo, että jos todistetaan molemmat kohdat 1° ja $(2')°$, niin tällöin (1.1) on todistettu.

'Vahvan' induktioperiaatteen todistus. Tehdään vastaoletus: (1.1) ei ole voimassa. Olkoon $T = \{n \geq n_0 \mid P(n) \text{ on epätosi}\}$. Tällöin vastaoletuksesta seuraa, että T on epätyhjä. Luonnollisten lukujen minimiominaisuudesta seuraa, että joukossa T on pienin alkio; olkoon se n. Koska kohta 1° on todistettu, on oltava $n > n_0$. Koska n on T:n pienin alkio, niin $P(k)$ on tosi kun $n_0 \leq k \leq n-1$. Koska $(2')°$ on todistettu, niin $P(n)$ on tosi. Tämä on ristiriita (RR) sen kanssa, että $n \in T$. □

Huomautus 1.1. Ehdossa 2° voitaisiin yhtä hyvin olettaa, että $n \geq n_0$, tehdä induktio-oletus '$P(n)$ on tosi' ja todistaa, että '$P(n+1)$ on tosi'. (Vastaavat muutokset voitaisiin tehdä myös ehdossa $(2')°$.) Pidän kuitenkin tässä esityksessä tiukasti kiinni alkuperäisestä muotoilusta 'turhan sanahelinän' välttämiseksi (vrt. [2]): koska aina mennään '$n-1$:stä n:ään' (n:n paikalla voi tietenkin olla joku toinen kirjain), niin ei ole tarpeen erikseen sanoa, mikä on induktio-oletus. 'Tavallisen' induktioperiaatteen käyttöä harjoitellaan tässä kurssissa usein; 'vahvaa' induktiota ainoastaan kerran (juuri Aritmetiikan peruslauseen yhteydessä). Jos muuta ei sanota, kyse on siis aina 'tavallisesta' induktiosta. Luku n_0 käy ilmi kulloinkin todistettavan väitteen muotoilusta. Tässä kurssissa useimmiten $n_0 = 1$. Kohta 1° on aina muistettava käsitellä, vaikka se useimmiten onkin helppo.

Todettakoon vielä, että 'vahva' induktio on siinä mielessä nimensä veroinen, että sitä voidaan joskus menestyksellä käyttää sellaisissa tilanteissa, missä 'tavallinen' induktio ei pure.

Kokonaislukujen jaollisuus

Määritelmä 1.2. Olkoot $a, b \in \mathbb{Z}$. Sanotaan, että a **jakaa** b:n (merk. $a|b$), jos on olemassa $c \in \mathbb{Z}$ siten, että $b = ac$. Sanotaan myös, että a on b:n **tekijä**. Merk. $a \nmid b$, jos a ei jaa b:tä.

Seuraavaan lauseeseen on koottu ne jaollisuuteen liittyvät perusasiat, joita tarvitaan jatkossa. Lauseessa esiintyvät luvut ovat kokonaislukuja, mikäli erikseen ei muuta sanota.

Lause 1.3. *Jaollisuudella on seuraavat ominaisuudet:*
(1) $a|0$, $1|a$, $a|a$.
(2) Jos $a|b$ *ja* $b|c$, *niin* $a|c$.
(3) Jos $a|b$, *niin* $(-a)|b$ *ja* $a|(-b)$.
(4) Jos $a|b$ *ja* $b \neq 0$, *niin* $|a| \leq |b|$.
(5) Jos $a|b$ *ja* $a|c$, *niin* $a|(b \pm c)$.
(6) Jos $a|b$ *ja* $a|c$, *niin* $a|(bx + cy)$ *mielivaltaisille* x, y.

(7) Jos $a|b_i$, $i = 1, \ldots, n$, *niin*

$$a|(b_1x_1 + \cdots + b_nx_n) \text{ mielivaltaisille } x_i, i = 1, \ldots, n$$

(8) Oletetaan, että $a, b \in \mathbb{N}^*$. *Jos* $a|b$ *ja* $b|a$, *niin* $a = b$. *Erityisesti jos* $a|1$, *niin* $a = 1$.

(9) Jos $b \in \mathbb{N}^*$, *niin* b*:llä on vain äärellinen määrä tekijöitä.*

Tod. Kohdat (1)–(6) ovat itsestään selviä ja jätetään lukijan tarkistettaviksi.

Todistetaan (7) 'tavallisella' induktiolla, vrt. Huomautus 1.1.
1° $n = 1$: Olkoon $b_1 = ac$ ja olkoon x_1 mielivaltainen kokonaisluku. Tällöin $b_1x_1 = a(cx_1)$, joten $a|(b_1x_1)$. Tämä oli alkuaskel. (Tässä olisi voitu käyttää myös kohtaa (6), valitsemalla esim. $b = b_1 = c,\ x = x_1,\ y = 0$.)
2° Olkoon $n > 1$. Koska nyt $a|(b_1x_1 + \cdots + b_{n-1}x_{n-1})$ (induktio-oletus) ja $a|b_n$ (oletus), niin kohdan (6) nojalla (valitsemalla $b = (b_1x_1 + \cdots + b_{n-1}x_{n-1}),\ c = b_n,\ x = 1,\ y = x_n$) saadaan $a|(b_1x_1 + \cdots + b_nx_n)$. Tämä oli induktioaskel.

(8) seuraa heti kohdasta (4), koska nyt $a \leq b$ ja $b \leq a$. Erikoistapauksessa $b = 1$ käytetään apuna kohtaa (1).

(9) seuraa myös heti kohdasta (4). □

Lause 1.4. *(Jakoyhtälö) Olkoon* $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. *Tällöin on olemassa yksikäsitteiset kokonaisluvut* q *ja* r, *missä* $0 \leq r < b$ *siten, että* $a = qb + r$. *Lisäksi pätee:* $b|a \Leftrightarrow r = 0$.

Tod. A) Olemassaolo: Jos $x \in \mathbb{R}$, merkitään $[x]$:llä suurinta kokonaislukua, joka on $\leq x$. Pätee siis

$$[x] \leq x < [x] + 1. \tag{1.2}$$

Olkoon nyt $q = [a/b]$ ja $r = a - qb$. Tällöin $q, r \in \mathbb{Z}$ ja $a = qb + r$. On vielä todistettava, että $0 \leq r < b$. Nyt (1.2):stä seuraa (kun $x = a/b$) $q \leq a/b < q + 1$, josta (kertomalla luvulla $b > 0$) saadaan $qb \leq a < qb + b$, josta edelleen r:n määritelmän nojalla haluttu tulos.

B) Yksikäsitteisyys: Oletetaan, että $a = qb + r = q'b + r'$, missä $0 \leq r' < b$. Saadaan yhtälö $b(q - q') = r' - r$, mistä edelleen $b|q - q'| = |r' - r|$. Tästä seuraa, että b jakaa luvun $|r' - r|$. Jos olisi $r' \neq r$, niin tällöin olisi $0 < |r' - r| < b$, mikä on RR Lauseen 1.3 kohdan (4) kanssa. On siis oltava $r' = r$. Koska $q - q' = (r' - r)/b$, seuraa tästä myös $q' = q$.

C) Viimeinen väite on itsestään selvä. □

Huomautus 1.5. Olkoon $n \in \mathbb{N}^*$, $n \geq 2$ ja olkoot $d_1 = 1 < \cdots < d_t = n$ luvun n **positiiviset tekijät** (joita on vain äärellinen määrä, vrt. Lause 1.3 (9)). Lauseen 1.3 kohdasta (3) seuraa, että n:llä ja $-n$:llä on samat tekijät,

nimittäin luvut $\pm d_1, \ldots, \pm d_t$. Esimerkiksi ± 6:n tekijät ovat ± 1, ± 2, ± 3 ja ± 6. Jos siis olemme kiinnostuneita jonkun luvun tekijöistä, niin riittää tuntea positiiviset tekijät. Tämän johdosta, jälleen välttääksemme turhaa sanahelinää, sanalla 'tekijä' tarkoitan jatkossa aina 'positiivista tekijää'.

Olkoon $a, b \in \mathbb{N}^*$. Lukujen a ja b **suurin yhteinen tekijä**, merk. $syt(a, b)$ on varmasti olemassa, koska ainakin 1 on yhteinen tekijä ja yhteisiä tekijöitä on vain äärellinen määrä. Symboleja käyttäen määritelmä saa muodon

Määritelmä 1.6. Olkoon $a, b, d \in \mathbb{N}^*$. Tällöin $d = syt(a, b)$ jos seuraavat ehdot ovat voimassa:
(1) $d|a$ ja $d|b$,
(2) jos luvulle $c \in \mathbb{N}^*$ pätee $c|a$ ja $c|b$, niin $c \leq d$.

Tärkeä erikoistapaus on se, missä $syt(a, b) = 1$. Silloin sanotaan, että a ja b ovat **keskenään jaottomat**.

Lause 1.7. *Olkoon $a, b \in \mathbb{N}^*$ ja $d = syt(a, b)$. Tällöin on olemassa $x, y \in \mathbb{Z}$ siten, että*

$$d = ax + by \tag{1.3}$$

Tod. Olkoon esimerkiksi $a \geq b$. Lisäksi voidaan olettaa, että $b \not| a$, koska jos $b|a$, niin selvästi $d = syt(a, b) = b$ ja (1.2):ssa voidaan valita $x = 0$ ja $y = 1$. Erityisesti nyt $a > b$. Käytetään **Eukleideen algoritmia**: Jakoyhtälö (Lause 1.4) antaa

$$a = q_1 b + r_1, \text{ missä } 0 < r_1 < b \text{ (oletettiin, että } b \not| a.)$$

Soveltamalla uudelleen jakoyhtälöä saadaan seuraavaksi

$$b = q_2 r_1 + r_2, \text{ missä } 0 \leq r_2 < r_1.$$

Jos $r_2 = 0$ niin lopetetaan. Muussa tapauksessa jatketaan samaan tyyliin ja äärellisen monen askeleen jälkeen saadaan yhtälöt

$$\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b \\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned}$$

Osoitetaan, että $d = r_n$, viimeinen nollasta eroava jakojäännös. Ensinnäkin pätee $r_n \in \mathbb{N}^*$. Toiseksi pätee $r_n|a$ ja $r_n|b$. Tämä nähdään menemällä yhtälöissä alhaalta ylöspäin. Viimeisestä yhtälöstä nähdään nimittäin, että $r_n|r_{n-1}$, viimeistä edellisestä (Lause 1.3 (6)) että $r_n|r_{n-2}$ jne. Kolmanneksi nähdään, että jos $c \in \mathbb{N}^*$

toteuttaa ehdot $c|a$ ja $c|b$, niin $c|r_n$. Tämä taas nähdään menemällä yhtälöissä ylhäältä alaspäin. Ensimmäisestä yhtälöstä nähdään, että $c|r_1$, toisesta saadaan $c|r_2$ jne., viimeistä edellisestä lopulta $c|r_n$. Tästä seuraa (Lause 1.3 (4)), että $c \leq r_n$. Luku r_n toteuttaa siis määritelmän 1.6 ehdot (1) ja (2), joten $r_n = d = syt(a, b)$.

Yhtälön (1.2) luvut x ja y löydetään nyt menemällä taas alhaalta ylöspäin. Tämä on mukavinta näyttää **esimerkin** avulla. Olkoon $a = 12378$ ja $b = 3054$. Eukleideen algoritmi antaa yhtälöt

$$\begin{aligned} 12378 &= 4 \cdot 3054 + 162, \\ 3054 &= 18 \cdot 162 + 138, \\ 162 &= 1 \cdot 138 + 24, \\ 138 &= 5 \cdot 24 + 18, \\ 24 &= 1 \cdot 18 + 6, \\ 18 &= 3 \cdot 6 + 0. \end{aligned}$$

Nyt siis tiedetään, että $syt(12378, 3054) = 6$. Saadaan

$$\begin{aligned} 6 &= 24 - 18 \quad \text{(toiseksi viimeiseltä eli 5. riviltä)} \\ &= 24 - (138 - 5 \cdot 24) \quad \text{(4. riviltä)} \\ &= 6 \cdot 24 - 138 \\ &= 6(162 - 138) - 138 \quad \text{(3. riviltä)} \\ &= 6 \cdot 162 - 7 \cdot 138 \\ &= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \quad \text{(2. riviltä)} \\ &= 132 \cdot 162 - 7 \cdot 3054 \\ &= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \quad \text{(1. riviltä)} \\ &= 132 \cdot 12378 - 535 \cdot 3054. \end{aligned}$$

Nähdään siis, että $6 = syt(12378, 3054) = 12378x + 3054y$, missä $x = 132$ ja $y = -535$. □

Seuraus 1.8. *Olkoon $a, b \in \mathbb{N}^*$ ja $d = syt(a, b)$. Tällöin pätee*
(2') Jos $c \in \mathbb{N}^*$ toteuttaa ehdot $c|a$ ja $c|b$, niin $c|d$.

Tod. Lauseen 1.7 nojalla on olemassa $x, y \in \mathbb{Z}$ siten, että

$$d = ax + by.$$

Väite seuraa nyt Lauseen 1.3 kohdasta (6). □

Seuraus 1.9. *Olkoon $a, b \in \mathbb{N}^*$. Tällöin a ja b ovat keskenään jaottomat silloin ja vain silloin kun on olemassa $x, y \in \mathbb{Z}$ siten, että $1 = ax + by$.*

Tod. A) Oletetaan, että a ja b ovat keskenään jaottomat. Määritelmän mukaan se tarkoittaa sitä, että $syt(a, b) = 1$. Lukujen x ja y olemassaolo seuraa nyt Lauseesta 1.7.

B) Oletetaan, että $1 = ax + by$ joillakin $x, y \in \mathbb{Z}$. Olkoon $d = syt(a, b)$ Koska $d|a$ ja $d|b$, niin $d|(ax + by)$ Lauseen 1.3 kohdan (6) nojalla. Tästä seuraa, että $d|1$, joten $d = 1$ Lauseen 1.3 kohdan (8) nojalla. Siis $syt(a, b) = 1$, joten a ja b ovat keskenään jaottomat. □

Seuraus 1.10. *Olkoon $a, b \in \mathbb{N}^*$. Jos $syt(a, b) = d$, niin $syt(a/d, b/d) = 1$.*

Tod. Todetaan aluksi, että $a/d, b/d \in \mathbb{N}^*$, koska $d|a$ ja $d|b$. Lauseen 1.7 nojalla on olemassa $x, y \in \mathbb{Z}$ siten, että $d = ax + by$. Kun tämä yhtälö jaetaan puolittain d:llä, saadaan yhtälö $1 = (a/d)x + (b/d)y$. Väite seuraa nyt Seurauksesta 1.9. □

Neljännessä luvussa tarvitsemme vastaavan tuloksen kolmen luvun suurimmalle yhteiselle tekijälle:

Lause 1.11. *Olkoon $a, b, c \in \mathbb{N}^*$. Jos $syt(a, b, c) = d$, niin $syt(a/d, b/d, c/d) = 1$.*

Se saadaan todistetuksi samaan tapaan kuin Seuraus 1.10 (käyttäen apuna Lauseen 1.3 kohtaa (7) kun $n = 3$), kunhan seuraava lause todistetaan ensin (vrt. Lause 1.7):

Lause 1.12. *Olkoon $a, b, c \in \mathbb{N}^*$ ja $d = syt(a, b, c)$. Tällöin on olemassa $x, y, z \in \mathbb{Z}$ siten, että*

$$d = ax + by + cz. \tag{1.4}$$

Todistetaan ensin

Lemma 1.13. *$syt(a, b, c) = syt(syt(a, b), c)$.*

Tod. Olkoon $d = syt(a, b, c)$, $d' = syt(a, b)$ ja $d^* = syt(d', c)$. On siis todistettava, että $d = d^*$.

A) Koska $d|a$ ja $d|b$, niin $d|d'$ (Seuraus 1.8). Koska $d|d'$ ja $d|c$, niin $d|d^*$ (Seuraus 1.8). Tästä seuraa, että $d \leq d^*$ (Lause 1.3 (4)).

B) Koska $d^*|d'$ ja $d'|a$, niin $d^*|a$ (Lause 1.3 (2)). Aivan samoin nähdään, että $d^*|b$. Koska $d^*|c$, niin d^* on a:n, b:n ja c:n yhteinen tekijä, joten $d^* \leq d$.

Kohdista A) ja B) seuraa, että $d = d^*$. $\square$

Lauseen 1.12 todistus. Käytetään edellisen todistuksen merkintöjä ja kaksi kertaa Lausetta 1.7. On siis olemassa $x', y', x^*, y^* \in \mathbb{Z}$ siten, että $d' = ax' + by'$ ja $d^* = d'x^* + cy^*$. Tästä seuraa, että $d = d^* = (ax' + by')x^* + cy^* = ax + by + cz$, missä $x = x'x^* \in \mathbb{Z}$, $y = y'x^* \in \mathbb{Z}$ ja $z = y^* \in \mathbb{Z}$. $\square$

Esimerkki 1.14. Olkoon tehtävänä löytää luvut $x, y, z \in \mathbb{Z}$ siten, että

$$syt(198, 288, 512) = 198x + 288y + 512z.$$

Käytetään lauseen 1.12 todistuksen merkintöjä ja etsitään ensin luvut $x', y' \in \mathbb{Z}$ siten, että $d' = syt(198, 288) = 198x' + 288y'$. Eukleideen algoritmilla (vrt. Lauseen 1.7 todistus)

$$\begin{aligned} 288 &= 1 \cdot 198 + 90, \\ 198 &= 2 \cdot 90 + 18, \\ 90 &= 5 \cdot 18 + 0, \end{aligned}$$

josta $d' = 18 = 198 - 2 \cdot 90 = 198 - 2(288 - 198) = 3 \cdot 198 - 2 \cdot 288$; voidaan siis valita $x' = 3$, $y' = -2$.

Seuraavaksi etsitään luvut $x^*, y^* \in \mathbb{Z}$ siten, että $d^* = syt(18, 512) = 18x^* + 512y^*$. Nyt saadaan

$$\begin{aligned} 512 &= 28 \cdot 18 + 8, \\ 18 &= 2 \cdot 8 + 2, \\ 8 &= 4 \cdot 2 + 0, \end{aligned}$$

josta $d^* = 2 = 18 - 2 \cdot 8 = 18 - 2(512 - 28 \cdot 18) = 57 \cdot 18 - 2 \cdot 512$; voidaan siis valita $x^* = 57$, $y^* = -2$.

Lopuksi saadaan

$$syt(198, 288, 512) = 2 = 198x + 288y + 512z,$$

missä $x = 3 \cdot 57 = 171$, $y = (-2) \cdot 57 = -114$ ja $z = -2$.

Huomautus 1.15. Olkoon $a, b, c \in \mathbb{N}^*$. Jos $syt(a, b) = 1$, niin tästä seuraa luonnollisesti (tai Lemmasta 1.13) myös $syt(a, b, c) = 1$. Käänteinen ei päde: esimerkiksi $syt(6, 10, 15) = 1$, mutta $syt(6, 10) = 2$, $syt(6, 15) = 3$ ja $syt(10, 15) = 5$.

Matkallamme kohti Aritmetiikan peruslauseen todistusta tärkeän etapin muodostaa seuraava tulos.

Lause 1.16. *(Euleideen Lemma) Olkoon $a, b, c \in \mathbb{N}^*$. Jos $syt(a, b) = 1$ ja $a|bc$, niin $a|c$.*

Tod. Lauseen 1.7 perusteella on olemassa $x, y \in \mathbb{Z}$ siten, että $1 = ax + by$. Kertomalla puolittain luvulla c saadaan

$$c = 1 \cdot c = (ax + by)c = a(cx) + (bc)y.$$

Koska $a|a$ ja oletuksen nojalla $a|bc$, niin (Lause 1.3 (6)) a jakaa oikeanpuolisen lausekkeen. Tästä seuraa, että $a|c$. □

Alkuluvut

Olkoon $n \in \mathbb{N}^*$, $n > 1$ ja d luvun n tekijä. Sanomme, että d on n:n **aito tekijä**, jos $1 < d < n$.

Määritelmä 1.17 Olkoon $p \in \mathbb{N}^*$, $p > 1$. Sanomme, että p on **alkuluku**, jos sillä ei ole aitoja tekijöitä. Toisin sanoen sen ainoat (positiiviset) tekijät ovat 1 ja p. Jos $n > 1$ ei ole alkuluku, niin se on **yhdistetty**.

Käytämme **alkulukujen joukolle** merkintää $\mathbb{P}$. Esimerkiksi $2 \in \mathbb{P}$, koska luvulla 2 ei voi olla aitoja tekijöitä siitä yksinkertaisesta syystä, että ei ole ylipäätään yhtään kokonaislukua d siten, että $1 < d < 2$.

Edelleen laskut

$$3 = 1 \cdot 2 + 1, \qquad 5 = 2 \cdot 2 + 1,$$
$$5 = 1 \cdot 3 + 2,$$
$$5 = 1 \cdot 4 + 1,$$

$$7 = 3 \cdot 2 + 1,$$
$$7 = 2 \cdot 3 + 1,$$
$$7 = 1 \cdot 4 + 3,$$
$$7 = 1 \cdot 5 + 2,$$
$$7 = 1 \cdot 6 + 1$$

osoittavat, että 3, 5 ja 7 ovat alkulukuja. Koska $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$ ja $10 = 2 \cdot 5$ ovat yhdistettyjä lukuja, niin olemme saaneet tuloksen

$$\{p \in \mathbb{P} \mid p \leq 10\} = \{2, 3, 5, 7\}. \tag{1.5}$$

Seuraava tulos ilmoittaa erään alkulukujen tärkeimmistä ominaisuuksista.

Lause 1.18. *Jos $p \in \mathbb{P}$, $a, b \in \mathbb{N}^*$ ja $p|ab$, niin $p|a$ tai $p|b$.*

Tod. Jos $p|a$, niin väite on voimassa. Oletetaan nyt, että $p \not| a$. Koska $syt(p, a)$ on alkuluvun p tekijä, niin on oltava $syt(p, a) = 1$ tai $syt(p, a) = p$. Viimeksi mainittu vaihtoehto ei käy, koska siitä seuraisi $p|a$, joka on vastoin tehtyä oletusta. On siis oltava $syt(p, a) = 1$. Eukleideen Lemma (Lause 1.16) antaa nyt tuloksen $p|b$. □

Seuraus 1.19. *Olkoon $p \in \mathbb{P}$ ja $a_1, \ldots, a_n \in \mathbb{N}^*$. Jos $p|a_1 \cdots a_n$, niin $p|a_i$ jollakin $i \in \{1, \ldots, n\}$.*

Tod. Todistetaan väite induktiolla luvun $n \in \mathbb{N}^*$ suhteen.
1° $n = 1$: Tämä tapaus on selvä (väite on sama kuin oletus!).
2° Olkoon $n > 1$. Koska $p|(a_1 \cdots a_{n-1})a_n$, niin lauseesta 1.18 seuraa, että

$$p|a_1 \cdots a_{n-1} \text{ tai } p|a_n.$$

Ensimmäisestä vaihtoehdosta seuraa induktio-oletuksen avulla, että $p|a_i$ jollakin $i \in \{1, \ldots, n-1\} \subset \{1, \ldots, n\}$. Toinen vaihtoehto vie suoraan maaliin. □

Seuraus 1.20. *Olkoon $p, q_1, \ldots, q_n \in \mathbb{P}$. Jos $p|q_1 \cdots q_n$, niin $p = q_i$ jollakin $i \in \{1, \ldots, n\}$.*

Tod. Edellisestä tuloksesta seuraa, että $p|q_i$ jollakin $i \in \{1, \ldots, n\}$. Koska $q_i \in \mathbb{P}$ ja $p > 1$, niin $p = q_i$. □

Lause 1.21. *Olkoon $n \in \mathbb{N}^*$, $n > 1$. Tällöin on olemassa $p \in \mathbb{P}$ siten, että $p|n$. (Sanotaan, että p on luvun n* **alkutekijä***).*

Tod. Tarkastellaan joukkoa $S = \{d \in \mathbb{N}^* \mid d|n \text{ ja } d > 1\}$. S ei ole tyhjä, koska $n \in S$. Olkoon p joukon S pienin alkio (luonnollisten lukujen minimiominaisuus). Koska $p \in S$, niin $p|n$ ja $p > 1$. Jos p olisi yhdistetty, niin sillä olisi aito tekijä d, jolle pätee siis $d|n$ ja $1 < d < p$. Koska $d|p$ ja $p|n$, niin $d|n$ (Lause 1.3 (2)). Tästä seuraa, että $d \in S$, mikä on RR, koska $d < p$ ja p on S:n pienin alkio. Pätee siis $p \in \mathbb{P}$ ja lause on todistettu. □

Lause 1.22. *(Eukleides) Alkulukuja on ääretön määrä.*

Tod. Tehdään vastaoletus: $\mathbb{P} = \{p_1 \ldots, p_n\}$, missä $n \in \mathbb{N}^*$. (Muistetaan, että $2 \in \mathbb{P}$ (vrt. (1.5)) joten $\mathbb{P} \neq \emptyset$.) Tarkastellaan lukua $N = p_1 \cdots p_n + 1 \in \mathbb{N}^*$. Koska $N > 1$, niin on olemassa $p \in \mathbb{P}$, $p|N$ (Lause 1.21). Vastaoletuksesta seuraa, että $p = p_i$ jollakin $i \in \{1, \ldots, n\}$. Tästä seuraa RR: $p|N$, mutta toisaalta N:n määritelmästä seuraa, että jos N jaetaan p_i:llä, niin jakojäännös on 1, joten $p_i \not| N$ eli siis $p \not| N$. (Lause 1.4). □

Huomautus 1.23. Edellistä Eukleideen lausetta alkulukujen äärettömästä määrästä ei tarvita seuraavana esitettävän Aritmetiikan peruslauseen todistuksessa. (Lausetta 1.21 **voitaisiin** käyttää, mutta ei tässä käytetä.) Sitä kuitenkin tarvitaan seuraavassa luvussa antamassa pohjaa kysymykselle Mersennen alkulukujen lukumäärästä. Myös monet muut alkulukujen arvoitukset liittyvät Eukleideen lauseeseen. Ei esimerkiksi tiedetä, onko olemassa äärettömän monta 'kaksoisparia' $(p, p+2)$, missä sekä $p \in \mathbb{P}$ että $p+2 \in \mathbb{P}$, siis esimerkiksi $(3,5)$ ja $(5,7)$. Voidaan myös kysyä (mutta vastausta ei tunneta) onko $n^2+1 \in \mathbb{P}$ äärettömän monella $n \in \mathbb{N}^*$. Edelleen voidaan kysyä (mutta vastausta ei tunneta) onko kahden peräkkäisen neliön välissä aina alkuluku, toisin sanoen, jos $n \in \mathbb{N}^*$ on annettu, onko aina olemassa $p \in \mathbb{P}$ siten, että $n^2 < p < (n+1)^2$.

Tällaisia 'mahdottoman' vaikeilta vaikuttavia, alkulukuihin liittyviä kysymyksiä on paljon muitakin, mutta haluan lopettaa tämän huomautuksen siihen rohkaisevaan seikkaan, että matemaatikot onnistuvat joskus **ratkaisemaankin** (eikä vain esittämään) vaikeita ongelmia. Esimerkiksi vain muutama vuosi sitten Ben Green ja Terence Tao todistivat yhteistyönään, että joukko $\mathbb{P}$ sisältää mielivaltaisen pitkiä aritmeettisia (äärellisiä) jonoja, toisin sanoen, jos $n \in \mathbb{N}^*$ on annettu, niin on olemassa (parillinen) luku $d \in \mathbb{N}^*$ ja $p_i \in \mathbb{P}$, $i = 1, \ldots, n$ siten, että $p_{i+1} - p_i = d$ kun $i = 1. \ldots, n-1$. (Osittain juuri tämän työn ansiosta Terence Tao sai vuonna 2006 kansainvälisessä matemaatikkokongressissa Madridissa 'matematiikan Nobelin palkinnoksi' usein sanotun Fieldsin mitalin.) Lisätietoja kaipaava lukija voi mennä tutustumaan Terence Taon kotisivuihin [10].

Lause 1.24. *(Aritmetiikan peruslause) Olkoon $n \in \mathbb{N}^*$, $n > 1$.*

(a) Luku n voidaan kirjoittaa alkulukujen tulona, siis muodossa $n = p_1 \cdots p_r$, missä luvut p_i ovat alkulukuja (eivät välttämättä keskenään erisuuria). Tässä termi 'alkulukujen tulo' sisältää myös sen tapauksen, että tekijöitä on vain yksi (silloin kun n on alkuluku).

(b) Luvun n esitys alkulukujen tulona on tekijöiden järjestystä vaille yksikäsitteinen. Tarkemmin sanottuna: jos

$$n = p_1 \cdots p_r = q_1 \cdots q_s, \text{ missä } p_1 \leq \cdots \leq p_r \text{ ja } q_1 \leq \cdots \leq q_s, \tag{1.6}$$

missä myös luvut q_j ovat alkulukuja, niin $r = s$ ja $p_i = q_i$ kaikilla $i \in \{1, \ldots, r\}$.

Tod. (a) Todistetaan tämä kohta 'vahvalla' induktiolla luvun n suhteen.
1° $n = 2$: Tämä on selvä, koska 2 on alkuluku. Tämä oli alkuaskel.
$(2')^\circ$ Olkoon $n > 2$. Jos n on alkuluku, niin asia on selvä. Jos taas n on yhdistetty, niin voidaan kirjoittaa $n = n_1 n_2$, missä $1 < n_1 < n$ ja $1 < n_2 < n$. Vahvasta induktio-oletuksesta seuraa, että n_1 ja n_2 ovat alkulukujen tuloja. Tästä seuraa, että myös n on alkulukujen tulo. Tämä oli induktioaskel, joten kohta (a) on todistettu.

(b) Todistetaan tämä kohta 'tavallisella' induktiolla luvun r suhteen.
1° $r = 1$: Koska $n = p_1$ on alkuluku, täytyy olla $s = 1$ (koska muutoin q_1 olisi n:n aito tekijä) ja edelleen $p_1 = n = q_1$. Alkuaskel on todistettu.
2° Olkoon $r > 1$ ja oletetaan, että (1.6) on voimassa. Tällöin n on yhdistetty, joten on oltava myös $s > 1$. Koska $p_r | q_1 \cdots q_s$, niin (Seuraus 1.20) $p_r = q_j$ jollakin

$j \in \{1, \ldots, s\}$. Aivan samoin saadaan $q_s = p_i$ jollakin $i \in \{1, \ldots, r\}$. Tästä seuraa (1.6):n epäyhtälöiden nojalla, että

$$p_r = q_j \leq q_s = p_i \leq p_r.$$

Tässä täytyy olla kummankin '$\leq$'-merkin paikalla olla '=', koska muuten seurauksena olisi $p_r < p_r$, RR. Saadaan siis tulos $p_r = q_s$. Tästä seuraa (1.6):n nojalla supistamalla

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1},$$

josta induktio-oletuksen nojalla $r - 1 = s - 1$ ja $p_i = q_i$ kaikilla $i \in \{1, \ldots, r-1\}$. Mutta nyt pätee myös $r = s$ ja (koska $p_r = q_s = q_r$) lopulta $p_i = q_i$ kaikilla $i \in \{1, \ldots, r\}$. Tämä oli induktioaskel, joten kohta (b) on todistettu. □

Seuraavat kaksi tulosta seuraavat välittömästi Aritmetiikan peruslauseesta.

Seuraus 1.25. *Jos $n \in \mathbb{N}^*$, $n > 1$, niin voidaan kirjoittaa*

$$n = p_1^{k_1} \cdots p_t^{k_t}, \ \textit{missä}\ p_i \in \mathbb{P}, \quad k_i \in \mathbb{N}^*\ \textit{ja}\ p_i \neq p_j\ \textit{kun}\ i \neq j. \tag{1.7}$$

Tämä esitys, luvun n **alkutekijähajoitelma**, *on yksikäsitteinen alkulukupotenssien $p_i^{k_i}$ järjestystä vaille.*

Seuraus 1.26. *Jos $n \in \mathbb{N}^*$, $n > 1$, niin on olemassa yksikäsitteinen esitys, luvun n* **kanoninen alkutekijähajoitelma**

$$n = p_1^{k_1} \cdots p_t^{k_t}, \ \textit{missä}\ p_1 < \cdots < p_t. \tag{1.8}$$

Konkreettisissa tapauksissa, kun luku n tunnetaan, käytetään yleensä kanonista hajoitelmaa (1.8), teoreettisemmissa yhteyksissä (esim. todistuksissa) hajoitelma (1.7) on usein kätevämpi. Esimerkiksi luvun 17640 kanoninen alkutekijähajoitelma on

$$17640 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2.$$

Minun on tässä vaiheessa turhaa ruveta hehkuttamaan Aritmetiikan peruslauseen tärkeyttä. Lukija tulee nimittäin sen itsekin toteamaan: käytämme tätä työkalua ahkerasti kaikissa seuraavissa luvuissa.

2. Täydelliset luvut, Mersennen alkuluvut ja niiden välinen yhteys

Täydelliset luvut

Määritelmä 2.1. Jos $n \in \mathbb{N}^*$, merkitään $\sigma(n)$:llä n:n **tekijöiden summaa**.

Esimerkki 2.2. $\sigma(6) = 1 + 2 + 3 + 6 = 12$ (vrt. Huomautus 1.5). Määritelmästä seuraa heti, että $\sigma(p) = p + 1$ kaikilla $p \in \mathbb{P}$.

Tarkoitus on seuraavaksi todistaa kaava, jonka avulla $\sigma(n)$ voidaan laskea, kun tunnetaan n:n alkutekijähajoitelma. Sitä varten tarvitsemme kaksi seuraavaa tulosta (joita voimme käyttää muihinkin tarkoituksiin).

Lemma 2.3. *Olkoon $x \in \mathbb{R}\backslash\{1\}$ ja $n \in \mathbb{N}^*$. Tällöin*

$$1 + x + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}. \tag{2.1}$$

Tod. Käytetään induktiota n:n suhteen.
1° $n = 1$: Koska $x^2 - 1 = (x - 1)(x + 1)$, niin

$$1 + x = \frac{x^2 - 1}{x - 1}, \text{ OK.}$$

2° Olkoon $n > 1$. Tällöin

$$1 + x + \cdots + x^n = (1 + x + \cdots + x^{n-1}) + x^n = \frac{x^n - 1}{x - 1} + x^n = \frac{x^{n+1} - 1}{x - 1}. \quad \square$$

Lause 2.4. *Olkoon $n \in \mathbb{N}^*$, $n > 1$. Jos $n = p_1^{k_1} \cdots p_r^{k_r}$ on n:n alkutekijähajoitelma, niin n:n tekijät ovat täsmälleen ne luvut $d \in \mathbb{N}^*$, jotka ovat muotoa*

$$d = p_1^{a_1} \cdots p_r^{a_r},$$

missä $0 \leq a_i \leq k_i$ $(i = 1, \ldots, r)$.

Tod. A) Huomaa, että tekijä $d = 1$ saadaan valitsemalla $a_1 = \cdots = a_r = 0$ ja $d = n$ saadaan valitsemalla $a_i = k_i$ $(i = 1, \ldots, r)$. Olkoon nyt d aito tekijä, jolloin voidaan kirjoittaa $n = dd'$, missä $d > 1$ ja $d' > 1$. Lausutaan (Aritmetiikan peruslause) sekä d että d' (ei välttämättä keskenään erisuurten) alkulukujen tulona:

$$d = q_1 \cdots q_s, \qquad d' = t_1 \cdots t_u,$$

missä siis $q_i, t_j \in \mathbb{P}$. Tällöin yhtälön

$$p_1^{k_1} \cdots p_r^{k_r} = q_1 \cdots q_s t_1 \cdots t_u$$

kumpikin puoli on n:n esitys alkulukujen tulona, joten (jälleen Aritmetiikan peruslauseen nojalla) jokaisen alkuluvuista q_i ja t_j on oltava joku alkuluvuista p_i. Tästä seuraa, että voidaan kirjoittaa

$$d = q_1 \cdots q_s = p_1^{a_1} \cdots p_r^{a_r}, \quad d' = t_1 \cdots t_u = p_1^{b_1} \cdots p_r^{b_r},$$

missä jokaisella $i \in \{1, \ldots, r\}$ pätee $a_i, b_i \in \mathbb{N}$, $a_i + b_i = k_i$ ja siten $0 \leq a_i \leq k_i$.

B) Kääntäen jokainen luku $d = p_1^{a_1} \cdots p_r^{a_r}$ $(0 \leq a_i \leq k_i)$ on n:n tekijä. Jos nimittäin määritellään $d' = p_1^{k_1 - a_1} \cdots p_r^{k_r - a_r}$, niin koska $k_i - a_i \geq 0$ kaikilla i, pätee $d' \in \mathbb{N}^*$ ja edelleen $n = dd'$. $\square$

Lause 2.5. *Olkoon $n \in \mathbb{N}^*$, $n > 1$ ja $n = p_1^{k_1} \cdots p_r^{k_r}$. Tällöin*

$$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Tod. Tarkastellaan tuloa

$$(1 + p_1 + \cdots + p_1^{k_1}) \cdots (1 + p_r + \cdots + p_r^{k_r}).$$

Kun tämä tulo kirjoitetaan auki, niin syntyy summa, jossa jokainen termi on saatu siten, että otetaan yksi luku jokaisesta sulkulausekkeesta ja ne kerrotaan keskenään. Lauseen 2.4 perusteella näin saadut termit ovat täsmälleen luvun n tekijät. Näin ollen

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{k_1}) \cdots (1 + p_r + \cdots + p_r^{k_r})$$

ja väite seuraa soveltamalla Lemmaa 2.3. $\square$

Esimerkki 2.6. Luvun $180 = 2^2 \cdot 3^2 \cdot 5$ tekijät ovat Lauseen 2.4 nojalla luvut

$$2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3},$$

missä $a_1 = 0, 1, 2$; $a_2 = 0, 1, 2$; $a_3 = 0, 1$. Tulokseksi saadaan luvut

$$1, 2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180.$$

Näiden summan pitäisi siis olla sama (tarkista!) kuin Lauseen 2.5 antama tulos

$$\sigma(180) = \frac{2^3 - 1}{2 - 1} \frac{3^3 - 1}{3 - 1} \frac{5^2 - 1}{5 - 1} = 7 \cdot 13 \cdot 6 = 546.$$

Seuraus 2.7. *Funktio σ on* **multiplikatiivinen**, *toisin sanoen se toteuttaa ehdon*

$$Jos\ syt(m,n)=1,\ \ niin\ \sigma(mn)=\sigma(m)\sigma(n). \tag{2.2}$$

Tod. Oletetaan, että $syt(m,n)=1$. Jos $m=1$ tai $n=1$, niin (2.2):n jälkimmäinen yhtälö on varmasti voimassa (koska $\sigma(1)=1$). Voidaan siis olettaa, että $m>1$ ja $n>1$. Olkoot m:n ja n:n alkutekijähajoitelmat $m=p_1^{k_1}\cdots p_r^{k_r}$ ja $n=q_1^{t_1}\cdots q_s^{t_s}$. Koska m ja n ovat keskenään jaottomat, niin $p_i\neq q_j$ kaikilla i,j. Tästä seuraa, että

$$mn=p_1^{k_1}\cdots p_r^{k_r}q_1^{t_1}\cdots q_s^{t_s}$$

on luvun mn alkutekijähajoitelma. Lauseen 2.5 nojalla saadaan nyt

$$\sigma(mn)=\frac{p_1^{k_1+1}-1}{p_1-1}\cdots\frac{p_r^{k_r+1}-1}{p_r-1}\frac{q_1^{t_1+1}-1}{q_1-1}\cdots\frac{q_r^{t_s+1}-1}{q_s-1}=\sigma(m)\sigma(n).\quad\square$$

Määritelmä 2.8 Luku $n\in\mathbb{N}^*$ on **täydellinen** jos $\sigma(n)=2n$. (Koska $\sigma(n)=2n \Leftrightarrow n=\sigma(n)-n$, voitaisiin yhtä hyvin sanoa, että luku n on täydellinen, jos se on itseään pienempien tekijöidensä summa.)

Esimerkiksi 6 on täydellinen luku, koska (vrt. Esimerkki 2.2 tai Lause 2.5) $\sigma(6)=12=2\cdot 6$ (myös $6=1+2+3$). Antiikin aikana tunnettiin kolme muutakin täydellistä lukua, nimittäin luvut 28, 496 ja 8128.

Eukleides todisti, että jos summa

$$1+2+2^2+2^3+\cdots+2^{k-1}=p$$

on alkuluku, niin $2^{k-1}p$ on täydellinen luku (välttämättä parillinen). Esimerkiksi $1+2+4=7$ on alkuluku, joten $4\cdot 7=28$ on täydellinen luku (kuten edellä mainittiin). Koska

$$1+2+2^2+2^3+\cdots+2^{k-1}=2^k-1 \text{ (Lemma 2.2)},$$

niin Eukleideen tulos voidaan pukea muotoon

Lause 2.8. *(Eukleides) Jos $2^k-1\in\mathbb{P}$ $(k>1)$, niin $n=2^{k-1}(2^k-1)$ on parillinen täydellinen luku.*

Tod. Koska $k-1\geq 1$, niin n on parillinen. Merkitään $p=2^k-1$ (alkuluku oletuksen nojalla). Koska p on lisäksi pariton, on $syt(2^{k-1},p)=1$. Funktion σ multiplikatiivisuuden (Seuraus 2.7) ja Esimerkin 2.2 nojalla saadaan nyt (käyttämällä myös Lausetta 2.5)

$$\sigma(n)=\sigma(2^{k-1})\sigma(p)=(2^k-1)(p+1)=2^k(2^k-1)=2n,$$

joten n on täydellinen. $\square$

Kääntäen pätee

Lause 2.9. *(Euler) Jos n on parillinen täydellinen luku, niin $n = 2^{k-1}(2^k - 1)$, missä $k > 1$ ja $2^k - 1 \in \mathbb{P}$.*

Tod. Koska n on parillinen, niin se voidaan esittää muodossa $n = 2^{k-1}m$, missä $k > 1$ ja m on pariton (tässäkin voi käyttää Aritmetiikan peruslausetta). Tällöin (koska $syt(2^{k-1}, m) = 1$ ja koska n on täydellinen)

$$\begin{aligned} \sigma(n) &= \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m) = 2n = 2^k m, \text{ joten} \\ \sigma(m) &= \frac{2^k m}{2^k - 1} = \frac{(2^k - 1)m + m}{2^k - 1} = m + \frac{m}{2^k - 1}. \end{aligned} \tag{2.3}$$

Koska $\sigma(m) \in \mathbb{N}^*$, niin yhtälöstä (2.3) seuraa, että $\frac{m}{2^k-1}$ on kokonaisluku, mistä taas seuraa, että $2^k - 1$ on luvun m tekijä, mistä lopulta seuraa, että myös $\frac{m}{2^k-1}$ on luvun m tekijä. Lisäksi $\frac{m}{2^k-1} < m$, koska $k > 1$, joten erityisesti pätee $m > 1$.

Yhtälöstä (2.3) nähdään nyt, että $\sigma(m)$ on kahden keskenään erisuuren m:n tekijän summa. Koska $\sigma(m)$ on määritelmän mukaan m:n **kaikkien** tekijöiden summa, niin tämä merkitsee, että m:llä ei ole muita tekijöitä. Luvulla $m > 1$ on siis vain kaksi tekijää, josta seuraa, että m on alkuluku ja pienempi tekijä $\frac{m}{2^k-1} = 1$. Pätee siis $m = 2^k - 1 \in \mathbb{P}$ ja väite on todistettu. □

Mersennen alkuluvut

Määritelmä 2.10. Kun $n \in \mathbb{N}^*$, merk. $M_n = 2^n - 1$ ja sanotaan, että M_n on **Mersennen luku**. Jos $M_n \in \mathbb{P}$, niin sanotaan, että M_n on **Mersennen alkuluku**.

Lemma 2.11. *Jos M_n on Mersennen alkuluku, niin $n \in \mathbb{P}$.*

Tod. Jos $M_n \in \mathbb{P}$, niin täytyy olla $n > 1$. Tehdään vastaoletus: n on yhdistetty. Tällöin voidaan kirjoittaa $n = rs$, missä $1 < r < n$ ja $1 < s < n$. Tästä seuraisi (Lemma 2.3), että

$$M_n = 2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1) \tag{2.4}$$

olisi yhdistetty, mikä on RR. □

Esimerkki 2.12. Katsotaan, miten kaava (2.4) toimii käytännössä pienillä yhdis-

tetyillä luvuilla n:

$$\begin{aligned}
M_4 = 15 &= 3 \cdot 5 && (r = 2, s = 2),\\
M_6 = 63 &= 3 \cdot 21 && (r = 2, s = 3),\\
&= 7 \cdot 9 && (r = 3, s = 2),\\
M_8 = 255 &= 3 \cdot 85 && (r = 2, s = 4),\\
&= 15 \cdot 17 && (r = 4, s = 2),\\
M_{10} = 1023 &= 3 \cdot 341 && (r = 2, s = 5),\\
&= 31 \cdot 33 && (r = 5, s = 2),\\
M_{12} = 4095 &= 3 \cdot 1365 && (r = 2, s = 6),\\
&= 7 \cdot 585 && (r = 3, s = 4),\\
&= 15 \cdot 273 && (r = 4, s = 3),\\
&= 63 \cdot 65 && (r = 6, s = 2).
\end{aligned}$$

Huomautus 2.13. Lemman 2.11 käänteinen tulos ei päde. Esimerkiksi $11 \in \mathbb{P}$, mutta $M_{11} = 2047 = 23 \cdot 89$.

Kun Lemma 2.11 yhdistetään Lauseisiin 2.8 ja 2.9, saadaan Eukleideen ja Eulerin tulokset lausuttua muodossa

Lause 2.14. *(Parilliset täydelliset luvut) Olkoon $n \in \mathbb{N}^*$ parillinen. Tällöin*

$$n \text{ on täydellinen } \Leftrightarrow n = 2^{p-1}M_p, \text{ missä } p \in \mathbb{P} \text{ ja } M_p \in \mathbb{P}. \quad \square$$

Edellinen tulos osoittaa, että jos halutaan tuntea parilliset täydelliset luvut, niin riittää tuntea Mersennen alkuluvut. Aikaisemmin mainitut parilliset täydelliset luvut 6, 28, 496 ja 8128 vastaavat Lauseen 2.14 välityksellä neljää pienintä Mersennen alkulukua $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ ja $M_7 = 127$. Ei tiedetä, onko Mersennen alkulukuja ääretön määrä. Ei myöskään tiedetä, onko **parittomia** täydellisiä lukuja olemassa.

Munkki Marin Mersenne, jonka suuri merkitys matematiikan historiassa perustuu ennenkaikkea hänen laajaan kirjeenvaihtoonsa muiden matemaatikkojen (Fermat, Descartes,...) kanssa, antoi (ilman todistusta) vuonna 1644 (yllättävän vähän virheitä sisältävän) listan alkuluvuista M_p, missä $p \leq 257$. Vasta vuonna 1947 tämä 'Mersennen lista' saatiin täydellisesti korjattua. Tällä hetkellä Mersennen alkulukuja tunnetaan 44 kappaletta (kts. [6]). Mersennen alkuluvuista löytyy myös Burtonin kirjasta [4] paljon lisää. Tässä haluan mainita vain sen seikan, että kun Laura Nickel ja Curt Noll todistivat yhdessä vuonna 1978, että $M_{21701} \in \mathbb{P}$, he olivat 18-vuotiaita koululaisia.

Jotta lukija saisi hieman harjoitusta funktion σ arvojen laskemisessa, annan tämän luvun lopuksi vielä yhden määritelmän ja pari harjoitustehtävää.

Määritelmä 2.14. Pari (m, n), missä $m, n \in \mathbb{N}^*$ ja $m \neq n$, muodostaa **ystävällisen lukuparin**, jos

$$\sigma(m) = m + n = \sigma(n).$$

Ei tiedetä, onko ystävällisiä lukupareja ääretön määrä. (Niitä tunnetaan nykyisin miljoonia!)

Tehtävä 2.15. Osoita, että alla luetellut luvut muodostavat ystävällisen lukuparin:
(a) $220 = 2^2 \cdot 5 \cdot 11$ ja $284 = 2^2 \cdot 71$ (Pythagoras, noin 500 e.a.a);
(b) $17296 = 2^4 \cdot 23 \cdot 47$ ja $18416 = 2^4 \cdot 1151$ (Fermat, 1636);
(c) $9363584 = 2^7 \cdot 191 \cdot 383$ ja $9437056 = 2^7 \cdot 73727$ (Descartes, 1638).

Tehtävä 2.16. Vuonna 1886 16-vuotias italialainen poika Nicolo Paganini (ei pidä sekoittaa kuuluisaan kaimaan, joka oli säveltäjä ja viuluvirtuoosi ja eli vuosina 1782–1840) ilmoitti, että luvut $1184 = 2^5 \cdot 37$ ja $1210 = 2 \cdot 5 \cdot 11^2$ muodostavat ystävällisen lukuparin. Osoita, että hän oli oikeassa.

Viitteessä [3] on ystävällisessä muodossa lisätietoja ystävällisistä lukupareista.

Huomautus 2.17. Funktio σ vaikuttaa viattomalta. Lukija, joka haluaa hämmästyä, tutustukoon artikkeliin [13].

3. Lagrangen lause neljän neliön summista

Kongruenssi

Seuraava määritelmä ja siihen liittyvä kätevä merkintä on Gaussin teoksessa *"Disquisitiones Arithmeticae"* (1801) aivan alussa.

Määritelmä 3.1. Olkoon $n \in \mathbb{N}^*$ kiinteä. Sanotaan, että kokonaisluvut a ja b ovat **kongruentteja modulo** n, merk.

$$a \equiv b \pmod{n},$$

jos $n|(a - b)$. Muussa tapauksessa sanotaan, että a ja b ovat **epäkongruentteja modulo** n ja merk.

$$a \not\equiv b \pmod{n}.$$

Tarvitsemme jatkossa ainoastaan kongruenssin **perusominaisuuksia**, joita käymme nyt tarkastelemaan.

Huomautus 3.2. Olkoon $a \in \mathbb{Z}$ mielivaltainen ja $n \in \mathbb{N}^*$ Määritelmässä 3.1 esiintyvä kiinteä luku. Jakoyhtälöstä saadaan

$$a = qn + r, \text{ missä } 0 \leq r < n.$$

Kongruenssin määritelmästä seuraa nyt heti, että $a \equiv r \pmod{n}$. Tämä on yksinkertainen, mutta hyödyllinen havainto! Tästä (tai suoraan määritelmästä) seuraa myös, että $a \equiv 0 \pmod{n}$ silloin ja vain silloin, kun $n|a$. Helposti huomataan, että a on **parillinen** täsmälleen silloin kun $a \equiv 0 \pmod{2}$ ja **pariton** täsmälleen silloin kun $a \equiv 1 \pmod{2}$.

Lause 3.3. *Olkoot $a, b \in \mathbb{Z}$. Tällöin $a \equiv b \pmod{n}$ silloin ja vain silloin, kun a:lla ja b:llä on sama jakojäännös, kun ne jaetaan n:llä.*

Tod. A) Oletetaan, että $a \equiv b \pmod{n}$, josta seuraa, että $a = b + kn$ jollakin $k \in \mathbb{Z}$. Olkoon r jakojäännös, kun b jaetaan n:llä: $b = qn + r$, missä $0 \leq r < n$. Tällöin

$$a = b + kn = (qn + r) + kn = (q + k)n + r,$$

mistä nähdään, että a:lla on sama jakojäännös kuin b:llä.

B) Oletetaan nyt, että voidaan kirjoittaa $a = q_1 n + r$ ja $b = q_2 n + r$ (samalla jakojäännöksellä r). Tällöin

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n,$$

mistä nähdään, että $n|(a - b)$. Määritelmän nojalla tämä merkitsee sitä, että $a \equiv b \pmod{n}$. □

Esimerkki 3.4. Yhtälöistä

$$-56 = (-7)9 + 7 \text{ ja } -11 = (-2)9 + 7$$

seuraa Lauseen 3.2 nojalla, että $-56 \equiv -11 \pmod{9}$. Itse asiassa $(-56) - (-11) = (-5)9$.

Kongruenssista $-31 \equiv 11 \pmod{7}$ taas seuraa, että luvuilla -31 ja 11 on sama jakojäännös, kun ne jaetaan 7:llä; itse asiassa

$$-31 = (-5)7 + 4, \qquad 11 = 1 \cdot 7 + 4.$$

Seuraavaan lauseeseen on koottu ne kongruenssin ominaisuudet, joita tarvitaan jatkossa.

Lause 3.5. *Olkoon $n \in \mathbb{N}^*$ kiinteä ja a, b, c, d jne. mielivaltaisia kokonaislukuja.*
(1) $a \equiv a \pmod{n}$.
(2) Jos $a \equiv b \pmod{n}$, *niin* $b \equiv a \pmod{n}$.
(3) Jos $a \equiv b \pmod{n}$ *ja* $b \equiv c \pmod{n}$, *niin* $a \equiv c \pmod{n}$.
(4) Jos $a \equiv b \pmod{n}$ *ja* $c \equiv d \pmod{n}$, *niin* $a + c \equiv b + d \pmod{n}$ *ja* $ac \equiv bd \pmod{n}$.
(5) Jos $a_i \equiv b_i \pmod{n}$ *kun* $i = 1, \ldots, k$, *niin* $a_1 + \cdots + a_k \equiv b_1 + \cdots + b_k \pmod{n}$ *ja* $a_1 \cdots a_k \equiv b_1 \cdots b_k \pmod{n}$.
(6) Jos $a \equiv b \pmod{n}$, *niin* $a + c \equiv b + c \pmod{n}$ *ja* $ac \equiv bc \pmod{n}$.
(7) Jos $a \equiv b \pmod{n}$, *niin* $a^k \equiv b^k \pmod{n}$ *kaikilla* $k \in \mathbb{N}^*$.

Tod. (1) ja (2) seuraavat välittömästi jaollisuuden perusominaisuuksista (Lause 1.3).

(3) Oletuksesta seuraa, että $a - b = hn$ ja $b - c = kn$, missä $h, k \in \mathbb{Z}$. Tästä seuraa, että

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n,$$

joten $a \equiv c \pmod{n}$.

(4) Kirjoitetaan nyt $a - b = k_1 n$ ja $c - d = k_2 n$, missä $k_1, k_2 \in \mathbb{Z}$. Saadaan

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= k_1 n + k_2 n = (k_1 + k_2)n,\end{aligned}$$

joten $a + c \equiv b + d \pmod{n}$. Mitä tulee toiseen väitteeseen, niin

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n.$$

Tästä nähdään, että $n|(ac - bd)$, josta seuraa, että $ac \equiv bd \pmod{n}$.

(5) Todistetaan ensimmäinen väite induktiolla k:n suhteen.
1° $k = 1$: Tämä on selvä (ei ole mitään todistamista!).
2° Olkoon $k > 1$. Induktio-oletuksesta seuraa, että $a_1 + \cdots + a_{k-1} \equiv b_1 + \cdots + b_{k-1} \pmod{n}$. Koska lisäksi oletuksen nojalla $a_k \equiv b_k \pmod{n}$, seuraa induktioaskel kohdasta (4).

Kohdan (5) jälkimmäinen väite todistetaan samoin.

(6) seuraa erikoistapauksena kohdasta (4), koska (1):n nojalla $c \equiv c \pmod{n}$.

(7) voidaan tulkita (5):n jälkimmäisen väitteen erikoistapaukseksi, kun valitaan $a_1 = \cdots = a_k = a$ ja $b_1 = \cdots = b_k = b$. (7) voidaan myös todistaa induktiolla k:n suhteen, kuten lukija voi helposti todeta. □

Määritelmä 3.6. Olkoon $n \in \mathbb{N}^*$ Määritelmässä 3.1 esiintyvä kiinteä luku. Olkoon $a \in \mathbb{Z}$ mielivaltainen. Joukkoa

$$[a] = [a]_n = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}$$

sanotaan a:n **jäännösluokaksi modulo** n.

Lause 3.7. *Olkoon $n \in \mathbb{N}^*$ kuten Määritelmässä 3.6. Jäännösluokat $[i]$, $i = 0, 1, \ldots, n-1$ ovat keskenään pistevieraita epätyhjiä joukkoja ja jokainen $a \in \mathbb{Z}$ kuuluu johonkin niistä.*

Tod. A) Olkoon $i \in \{0, 1, \ldots, n-1\}$. Tällöin $[i] \neq \emptyset$, koska $i \in [i]$ (Lause 3.5 (1)).

B) Olkoon $i, j \in \{0, 1, \ldots, n-1\}$, $i \neq j$. Tehdään vastaoletus: $[i] \cap [j] \neq \emptyset$. Tällöin on olemassa $x \in [i] \cap [j]$. Tästä seuraisi, että $x \equiv i \pmod{n}$ ja $x \equiv j \pmod{n}$, josta Lauseen 3.5 kohtien (2) ja (3) perusteella seuraisi $i \equiv j \pmod{n}$. Lauseesta 3.3 seuraisi nyt (koska i ja j ovat omia jakojäännöksiään, kun ne jaetaan n:llä) $i = j$, mikä on RR.

C) Viimeinen väite seuraa heti Huomautuksesta 3.2. □

Esimerkki 3.8. Jos $n = 2$, niin (vrt. Huomautus 3.2)

$$[0] = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{2}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \text{ (parilliset luvut)},$$
$$[1] = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{2}\} = \{\ldots, -3, -1, 1, 3, 5, \ldots\} \text{ (parittomat luvut)}.$$

Jos $n = 3$, niin

$$[0] = \{3k \mid k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\},$$
$$[1] = \{3k + 1 \mid k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\},$$
$$[2] = \{3k + 2 \mid k \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Lokeroperiaate

Seuraava tulos, joka on äärimmäisen yksinkertainen, on usein hyödyllinen. Se on nimeltään **(Dirichlet'n) lokero- tai laatikkoperiaate**.

Lause 3.9. *Jos n esinettä sijoitetaan lokeroihin, joiden lukumäärä on $k < n$, niin jossakin lokerossa on ainakin 2 esinettä.*

Tod. Tehdään vastaoletus: jokaisessa lokerossa on korkeintaan yksi esine. Tällöin selvästikin esineiden lukumäärä n olisi korkeintaan k, mikä on RR. □

Lagrangen lauseen todistus

Tarkoituksena on siis todistaa

Lause 3.10. *(Lagrange, 1770) Olkoon $n \in \mathbb{N}^*$ Tällöin on olemassa $x_i \in \mathbb{Z}$, $i = 1, \ldots, 4$ siten, että $n = x_1^2 + \cdots + x_4^2$.*

Ennen todistuksen alkua tarkastelemme ensin lyhyesti tilannetta ennen Lagrangea. Kyseisen lauseen on ilmeisesti ensimmäisenä muotoillut Bachet, toimittamansa Diofantoksen *Aritmetiikka*-teoksen latinankielisessä laitoksessa 1621 (samassa teoksessa, jonka marginaaleihin Fermat teki kuolemattomia huomautuksiaan). Lagrange puhuukin 'Bachet'n lauseesta'. Bachet tarkisti, että luvut $1, \ldots, 325$ voidaan esittää neljän neliön summina, mutta myönsi, että yleinen todistus ei ole hänen ulottuvillaan. Fermat väitti marginaalissa, että hänellä on hallussaan todistus, jonka hän aikoo liittää suunnittelemaansa lukuteoriaa käsittelevään kirjaan. Valitettavasti tämä kirja ei koskaan ilmestynyt!

Todistus, joka seuraavassa esitetään, on käytännöllisesti katsoen kokonaan Eulerin käsialaa. Euler oli tehnyt tärkeän perustyön (josta Lagrange antaa täyden tunnustuksen), mutta häneltä puuttui se (ratkaiseva) seikka, että jokainen **alkuluku** voidaan esittää neljän neliön summana. Lagrange todisti tämän puuttuvan palan aika monimutkaisella tavalla, käyttäen hyväksi tunnettua yhtälöä

$$\boxed{\boxed{2+2=4,}}$$

tarkemmin sanottuna käyttäen apuna **kahden** neliön summia, katso [14]. Euler keksi hieman myöhemmin yksinkertaisemman todistuksen tälle puuttuvalle palalle.

Lemma 3.11. *(Euler) Jos $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$ ja $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$, niin*

$$\begin{aligned} mn =& (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &+ (a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2. \end{aligned}$$

Tod. Raaka lasku! $\square$

Lemma 3.12. *(Euler) Jos $p \in \mathbb{P}\backslash\{2\}$, niin kongruenssilla*

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

on ratkaisu x_0, y_0 missä $0 \leq x_0 \leq (p-1)/2$ ja $0 \leq y_0 \leq (p-1)/2$.

Tod. Todistuksen ideana on tarkastella kahta joukkoa:

$$\begin{aligned} S_1 &= \left\{1 + 0^2, 1 + 1^2, 1 + 2^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2\right\}, \\ S_2 &= \left\{-0^2, -1^2, -2^2, \ldots, -\left(\frac{p-1}{2}\right)^2\right\}. \end{aligned}$$

Osoitetaan, että mitkään kaksi joukon S_1 (eri) alkiota eivät voi olla kongruentteja modulo p. Tehdään vastaoletus: joillakin $0 \leq x_1 < x_2 \leq (p-1)/2$ pätee $1 + x_1^2 \equiv 1 + x_2^2 \pmod{p}$. Tästä seuraisi ensinnäkin (Lause 3.5 (6)) $x_1^2 \equiv x_2^2 \pmod{p}$ ja edelleen $x_2^2 - x_1^2 \equiv 0 \pmod{p}$. Pätee siis

$$(x_2 - x_1)(x_2 + x_1) \equiv 0 \pmod{p},$$

josta, koska p on alkuluku, seuraa että $p|(x_2 - x_1)$ tai $p|(x_2 + x_1)$ (Lause 1.18). Kumpikin näistä ehdoista on RR Lauseen 1.3 (4) kanssa, koska $0 < x_2 - x_1 \leq (p-1)/2 < p$ ja $0 < x_2 + x_1 \leq (p-1)/2 + (p-1)/2 = p - 1 < p$.

Aivan samanlainen päättely osoittaa, että myös joukon S_2 alkiot ovat keskenään epäkonguentteja modulo p.

Joukoissa S_1 ja S_2 on yhteensä $2\big(1 + (p-1)/2\big) = p + 1$ kokonaislukua. Käytetään nyt lokeroperiaatetta (Lause 3.9), missä 'esineet' ovat nämä $p + 1$ kokonaislukua ja 'lokerot' ovat jäännösluokat modulo p, joita on p kappaletta (vrt. Lause 3.7). Lokeroperiaatteen nojalla jokin jäännösluokka sisältää kaksi kyseistä kokonaislukua, jotka ovat siis kongruentteja modulo p. Ylläolevan nojalla toisen luvuista on oltava S_1:ssä ja toisen S_2:ssa. On siis olemassa x_0, $0 \leq x_0 \leq (p-1)/2$ ja y_0, $0 \leq y_0 \leq (p-1)/2$ siten, että

$$1 + x_0^2 \equiv -y_0^2 \pmod{p},$$

mistä väite seuraakin välittömästi. □

Seuraus 3.13. *Jos $p \in \mathbb{P}\backslash\{2\}$, niin on olemassa $k \in \mathbb{N}^*$, $k < p$ siten, että kp on neljän neliön summa.*

Tod. Lemman 3.12 nojalla on olemassa $x_0, y_0 \in \mathbb{N}$,

$$0 \leq x_0 < p/2, \qquad 0 \leq y_0 < p/2$$

siten, että

$$x_0^2 + y_0^2 + 1^2 + 0^2 = kp$$

jollakin $k \in \mathbb{Z}$. Lukujen x_0 ja y_0 koolle annetuista rajoituksista seuraa, että

$$0 < kp = x_0^2 + y_0^2 + 1 < p^2/4 + p^2/4 + 1 < p^2,$$

josta $0 < k < p$ ja väite on todistettu. □

Huomautus 3.14. Jos edellisessä tuloksessa olisi vaadittu vain $k \leq p$ eikä $k < p$ niin voitaisiin valita $k = p$: $pp = p^2 + 0^2 + 0^2 + 0^2$. Tästä ei kuitenkaan olisi meille mitään hyötyä!

Esimerkki 3.15. Jos $p = 17$, niin Lemman 3.12 joukot S_1 ja S_2 ovat

$$S_1 = \{1, 2, 5, 10, 17, 26, 37, 50, 65\}$$

ja

$$S_2 = \{0, -1, -4, -9, -16, -25, -36, -49, -64\}.$$

Modulo 17, joukon S_1 alkiot ovat $1, 2, 5, 10, 0, 9, 3, 16, 14$, kun taas joukon S_2 alkiot ovat $0, 16, 13, 8, 1, 9, 15, 2, 4$. Lemma 3.12 kertoo meille, että joku alkio $1 + x^2$ joukosta S_1 on kongruentti modulo 17 jonkun alkion $-y^2 \in S_2$ kanssa. Useista vaihtoehdoista voidaan valita esimerkiksi

$$1 + 5^2 \equiv 9 \equiv -5^2 \pmod{17}$$

eli toisin sanoen $1 + 5^2 + 5^2 \equiv 0 \pmod{17}$. Tästä seuraa, että Seurauksessa 3.13 voidaan valita $k = 3$:

$$3 \cdot 17 = 1^2 + 5^2 + 5^2 + 0^2.$$

Nyt olemme valmiit todistamaan ratkaisevan tuloksen:

Lause 3.16. *(Lagrange) Jokainen alkuluku p on neljän neliön summa.*

Tod. (Euler) Väite pätee alkuluvulle $p = 2$, koska $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Oletetaan nyt, että $p \in \mathbb{P}\backslash\{2\}$. Olkoon $k \in \mathbb{N}^*$ **pienin** alkio, jolla kp on neljän neliön summa; olkoon vaikka

$$kp = x^2 + y^2 + z^2 + w^2.$$

Tällöin pätee $k < p$ (Seuraus 3.13). Jos osoitamme, että $k = 1$, niin tällöin väite on todistettu. Tehdään vastaoletus: $k > 1$. Jaetaan tarkastelu kahteen osaan sen mukaan, onko k parillinen vai pariton.

A) k **parillinen**. Tällöin myös kp on parillinen, josta seuraa, että luvuista x, y, z, w, joko kaikki ovat parillisia tai kaikki parittomia tai sitten niistä kaksi on parillista ja kaksi paritonta. Koska niiden järjestyksellä ei ole väliä, voidaan siis olettaa, että

$$x \equiv y \pmod{2} \text{ ja } z \equiv w \pmod{2}.$$

Tästä seuraa, että jos määritellään

$$a = (x - y)/2, \quad b = (x + y)/2, \quad c = (z - w)/2, \quad d = (z + w)/2,$$

niin tällöin $a, b, c, d \in \mathbb{Z}$ ja

$$(k/2)p = a^2 + b^2 + c^2 + d^2,$$

mikä on RR k:n määritelmän kanssa, koska $k/2 \in \mathbb{N}^*$ ja $k/2 < k$.

B) k **pariton**. Nyt voidaan valita $a, b, c, d \in \mathbb{Z}$ siten, että

$$a \equiv x \pmod{k}, b \equiv y \pmod{k}, c \equiv z \pmod{k}, d \equiv w \pmod{k}$$

ja

$$|a| < k/2, |b| < k/2, |c| < k/2, |d| < k/2.$$

(Esimerkiksi a:n löytämiseksi voidaan menetellä siten, että etsitään ensin jakojäännös r kun x jaetaan k:lla. Sitten valitaan $a = r$ tai $a = r - k$ sen mukaan, onko $r < k/2$ tai $r > k/2$. Huomaa, että tapaus $r = k/2$ ei tule kyseeseen, koska k on pariton.)

Kongruenssin perusominaisuuksia käyttämällä (Lause 3.5) saadaan

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k}$$

ja siten

$$a^2 + b^2 + c^2 + d^2 = nk$$

jollakin $n \in \mathbb{N}$. Lukujen a, b, c, d koolle annetuista rajoituksista seuraa, että

$$0 \leq nk = a^2 + b^2 + c^2 + d^2 < 4(k/2)^2 = k^2.$$

Jos olisi $n = 0$, niin tällöin olisi oltava $a = b = c = d = 0$, mikä on mahdotonta, koska siitä seuraisi että k jakaisi jokaisen luvuista x, y, z, w, josta seuraisi, että luku k^2 jakaisi jokaisen luvuista x^2, y^2, z^2, w^2 ja siis myös niiden summan, joka on kp. Tästä taas seuraisi, että $k|p$, mikä ei käy päinsä, koska p on alkuluku ja $1 < k < p$. On siis oltava $n \in \mathbb{N}^*$. Lisäksi ehdosta $nk < k^2$ seuraa, että $n < k$.

Yhdistämällä aikaisemmat tulokset saadaan

$$\begin{aligned} k^2np = (kp)(nk) &= (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) \\ &= r^2 + s^2 + t^2 + u^2, \end{aligned}$$

missä (Lemma 3.11)

$$\begin{aligned} r &= xa + yb + zc + wd, \\ s &= xb - ya + zd - wc, \\ t &= xc - yd - za + wb, \\ u &= xd + yc - zb - wa. \end{aligned}$$

On tärkeää huomata, että k jakaa jokaisen luvuista r, s, t, u. Jos tarkastellaan esimerkiksi lukua r, niin saadaan

$$r = xa + yb + zc + wd \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{k}.$$

Samoin nähdään, että $s \equiv t \equiv u \equiv 0 \pmod{k}$. Tämä johtaa esitykseen

$$np = (r/k)^2 + (s/k)^2 + (t/k)^2 + (u/k)^2,$$

missä r/k, s/k, t/k, u/k ovat kokonaislukuja. Koska $n \in \mathbb{N}^*$ ja $n < k$, tämä on RR k:n määritelmän kanssa.

On siis oltava $k = 1$ ja lause on todistettu. □

Huomautus 3.17. Lauseen 3.16 todistus on siinä mielessä **konstruktiivinen**, että siinä esitettyä menetelmää voitaisiin käyttää esityksen $p = x^2 + y^2 + z^2 + w^2$ löytämiseen. Ensin löydetään Seurauksen 3.13 menetelmällä **jokin** $k < p$ siten, että kp on neljän neliön summa. Sitten 'pienennetään' k:ta kohtien A) ja/tai B) menetelmällä (tarvittaessa useita kertoja), kunnes lopuksi saadaan p esitetyksi neljän neliön summana.

Esimerkki 3.18. Olkoon $p = 17$. Esimerkissä 3.15 saatiin

$$3 \cdot 17 = x^2 + y^2 + z^2 + w^2,$$

missä $x = 1$, $y = 5$, $z = 5$, $w = 0$. Koska $k = 3$ on pariton, käytetään Lauseen 3.16 todistuksen kohdan B) menetelmää. Nyt voidaan valita $a = 1$, $b = -1$, $c = -1$, $d = 0$, josta saadaan

$$a^2 + b^2 + c^2 + d^2 = 3 = nk, \text{ missä } n = 1.$$

Lemmasta 3.11 saadaan $r = -9$, $s = -6$, $t = -6$, $u = 0$ ja edelleen $r/k = -3$, $s/k = -2$, $t/k = -2$, $u/k = 0$. Lopuksi saadaan

$$17 = (-3)^2 + (-2)^2 + (-2)^2 + 0^2.$$

Lagrangen kuuluisa lause neljän neliön summista saadaan nyt helposti:

Lauseen 3.10 todistus. Olkoon $n \in \mathbb{N}^*$. Jos $n = 1$, niin asia on selvä: $1 = 1^2 + 0^2 + 0^2 + 0^2$. Voidaan siis olettaa, että $n > 1$. Aritmetiikan peruslauseen nojalla voidaan kirjoittaa

$$n = p_1 \cdots p_k,$$

missä $p_1, \ldots, p_k$ ovat alkulukuja (eivät välttämättä keskenään erisuuria). Käytetään induktiota k:n suhteen.
1° $k = 1$: Tällöin $n = p_1$ on alkuluku, joten väite seuraa Lauseesta 3.16.
2° Olkoon $k > 1$. Induktio-oletuksen nojalla $p_1 \cdots p_{k-1}$ on neljän neliön summa ja Lauseen 3.16 nojalla p_k on neljän neliön summa. Tästä seuraa Lemman 3.11 avulla, että myös $n = (p_1 \cdots p_{k-1})p_k$ on neljän neliön summa. □

Täydentäviä tarkasteluja: kahden ja kolmen neliön summat, Waringin Probleema

Seuraavassa hahmottelen (pääosin ilman todistuksia), perspektiivin luomiseksi, tilannetta Lagrangin lausetta 'ennen' ja 'jälkeen.' Lukija voi halutessaan huoleti

hypätä suoraan neljänteen eli viimeiseen lukuun, koska nyt esitettyjä tarkasteluja ei siellä käytetä hyväksi.

Todetaan aluksi, että jokaiselle $p \in \mathbb{P}\backslash\{2\}$ pätee joko $p \equiv 1 \pmod 4$ tai $p \equiv 3 \pmod 4$. Tämä seuraa välittömästi Huomautuksesta 3.2.

Seuraava lause antaa välttämättömän ja riittävän ehdon sille, että $n \in \mathbb{N}^*$ on **kahden** kokonaisluvun neliön summa.

Lause 3.19. *Olkoon $n \in \mathbb{N}^*$. Tällöin seuraavat ehdot ovat yhtäpitävät:*
(1) n on kahden neliön summa, ts. $n = x_1^2 + x_2^2$ joillakin $x_1, x_2 \in \mathbb{Z}$.
(2) Jos $p|n$, missä $p \equiv 3 \pmod 4$, niin p:n eksponentti n:n alkutekijähajoitelmassa (1.7) on **parillinen**.

Hahmottelen seuraavassa todistuksen suunnan '(2) $\Rightarrow$ (1)'. Yksityiskohtien ja suunnan '(1) $\Rightarrow$ (2)' suhteen viittaan Burtonin kirjaan [4].

Suunnan '(2) $\Rightarrow$ (1)' todistus perustuu seuraavalle tulokselle, joka lukijan on helppo tarkistaa:

Lemma 3.19. *Jos $m = a^2 + b^2$ ja $n = c^2 + d^2$, niin $mn = (ac + bd)^2 + (ad - bc)^2$.* □

Äskeisestä tuloksesta seuraa helposti induktion avulla, että jos luvut $n_1, \ldots, n_k$ ovat kahden neliön summia, niin myös niiden tulo on kahden neliön summa.

Alkuluku 2 on kahden neliön summa: $2 = 1^2 + 1^2$. Jokainen alkulukupotenssi p^k, missä $k = 2t$ on parillinen, on neliö ja siten myös kahden neliön summa: $p^k = (p^t)^2 + 0^2$. Tästä havaitaan, että jos n toteuttaa ehdon (2), niin n on kahden neliön summa, kunhan vielä todistetaan

Lause 3.20. *(Fermat, Euler) Olkoon $p \in \mathbb{P}$, $p \equiv 1 \pmod 4$. Tällöin p on kahden neliön summa.*

Fermat ilmoitti Mersennelle 25.12.1640 päivätyssä kirjeessään todistaneensa em. lauseen, jonka ensimmäinen **julkaistu** todistus on peräisin Eulerilta runsas sata vuotta myöhemmin.

Huomautus 3.21. Mikään alkuluku $p \equiv 3 \pmod 4$ ei voi olla kahden neliön summa. Yleisemmin pätee: mikään luku $n \equiv 3 \pmod 4$ ei voi olla kahden neliön summa. Tämä seuraa helposti siitä, että koska parillisten lukujen neliöt ovat $\equiv 0 \pmod 4$ ($(2k)^2 = 4k^2$) ja parittomien lukujen neliöt ovat $\equiv 1 \pmod 4$ ($(2k+1)^2 = 4(k^2 + k) + 1$), jokainen kahden neliön summa on $\equiv 0, 1, 2 \pmod 4$.

Mitä tulee **kolmen** neliön summiin, niin seuraavan tuloksen todisti ensimmäisenä Legendre vuonna 1798.

Lause 3.22. *(Legendre) Olkoon $n \in \mathbb{N}^*$. Seuraavat ehdot ovat yhtäpitävät:*
(1) n on kolmen neliön summa.
(2) $n \neq 4^k(8m+7)$, missä $k, m \in \mathbb{N}$.

Tässä tapauksessa hahmottelen suunnan '(1) $\Rightarrow$ (2)', joka on aika helppo (yksityiskohdissa viittaan taas Burtonin kirjaan [4]). Koska jokainen neliö on $\equiv 0, 1, 4 \pmod 8$ (riittää tarkastella lukuja i^2, missä $i = 0, 1, \ldots, 7$), seuraa samaan tapaan kuin Huomautuksessa 3.21, että mikään kolmen neliön summa ei voi olla $\equiv 7 \pmod 8$. Tämä antaa tapauksen $k = 0$ eli alkuaskeleen, kun suunta '(1) $\Rightarrow$ (2)' todistetaan induktiolla k:n suhteen.

Suunta '(2) $\Rightarrow$ (1)' on aika vaikea, viittaan Landaun kirjaan [15].

Jos ajattelemme kahden neliön summia (Lause 3.19) ja kolmen neliön summia (Lause 3.22), niin Lagrangen lause neljän neliön summista (Lause 3.10) näyttäytyy ikäänkuin erään tien **päätepisteenä**. Toisaalta samainen lause edustaa erään toisen tien **alkupistettä**, tien, jota vielä tänäkään päivänä ei ole valmiiksi rakennettu. Voidaan nimittäin kysyä (tämä kysymys tehtiinkin minulle Ressun lukiossa!), mitä tapahtuu, jos **neliöiden** sijasta tarkastellaankin **kuutioita**, **neljänsiä potensseja** jne.

Kirjassaan *Meditationes Algebraicae* (1770) Edward Waring mainitsi ilman todistusta, että jokainen $n \in \mathbb{N}^*$ voidaan esittää neljän neliön, yhdeksän kuution, yhdeksäntoista neljännen potenssin jne. summana. **Waringin Probleemaksi** ruvettiin kutsumaan (aluksi) seuraavaa kysymystä (myöhemmin muutakin siihen liittyvää, josta tulee vielä puhe):

Kysymys 3.23. (Waringin probleema) Olkoon $k \in \mathbb{N}^*$, $k \geq 2$. Onko olemassa sellainen luku $s(k)$, että jokainen $n \in \mathbb{N}^*$ voidaan esittää muodossa

$$n = x_1^k + \cdots + x_{s(k)}^k \quad \text{joillakin } x_i \in \mathbb{N}?$$

Tämä kysymys osoittautui vaikeaksi. Vasta vuonna 1909 Hilbert onnistui vastaamaan kysymykseen myöntävästi. (Khintsinin kirjasta [12] löytyy Linnikiltä peräisin oleva todistus, joka on metodisesti Hilbertin todistusta yksinkertaisempi, mutta ei kovin helppo sekään.) Hilbertin tulos mahdollistaa seuraavan määritelmän.

Määritelmä 3.24. Olkoon $k \in \mathbb{N}^*$, $k \geq 2$. Tällöin $g(k)$ on **pienin** sellainen luku, että jokainen $n \in \mathbb{N}^*$ voidaan esittää muodossa

$$n = x_1^k + \cdots + x_{g(k)}^k \quad \text{joillakin } x_i \in \mathbb{N}.$$

Seuraava tehtävä olisi luonnollisesti määrittää $g(k)$:n arvo. Koska lukua 7 ei voida lausua kolmen neliön summana (tämä seuraa Lauseesta 3.22, mutta lukija voi sen helposti todeta suoraan, koska ainoastaan neliöitä 0^2, 1^2 ja 2^2 voidaan nyt käyttää), niin Lagrangen lauseesta neljän neliön summille seuraa, että $g(2) = 4$.

Kun $k \in \mathbb{N}^*$, $k \geq 2$, merkitään

$$I(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2.$$

Vuonna 1772 Euler todisti seuraavan tuloksen ja esitti konjektuurin, että $g(k) = I(k)$ kaikilla k.

Lause 3.25. *(Alaraja $g(k)$:lle)*

$$g(k) \geq I(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2, \quad k = 2, 3, \ldots .$$

Tod. Tässä käytetään 'hakasulkufunktion' $[x]$ perusominaisuutta (1.2). Olkoon $n = 2^k[(\frac{3}{2})^k] - 1$. Koska $[x] < x$ kun x ei ole kokonaisluku, pätee $n < 2^k(\frac{3}{2})^k - 1$, toisin sanoen $n < 3^k - 1$. Luvun $g(k)$ määritelmästä seuraa, että

$$n = x_1^k + \cdots + x_{g(k)}^k$$

joillakin luonnollisilla luvuilla x_i, $i = 1, 2, \ldots, g(k)$. Jokaisen luvuista x_i on oltava pienempi kuin 3. Oletetaan, että a kpl. luvuista x_i on kakkosia, b kpl. on ykkösiä ja c kpl. nollia. Tällöin $n = 2^k a + b$ ja $g(k) = a + b + c$.

Koska $2^k a \leq n < 2^k[(\frac{3}{2})^k]$, niin $a < [(\frac{3}{2})^k]$, toisin sanoen $a \leq [(\frac{3}{2})^k] - 1$. Koska $b = n - 2^k a$, niin $a + b = n - (2^k - 1)a$. Koska

$$(2^k - 1)a \leq (2^k - 1)\left(\left[\left(\frac{3}{2}\right)^k\right] - 1\right) = (2^k - 1)\left[\left(\frac{3}{2}\right)^k\right] - (2^k - 1),$$

niin saadaan

$$\begin{aligned} n - (2^k - 1)a &\geq n - (2^k - 1)\left[\left(\frac{3}{2}\right)^k\right] + (2^k - 1) \\ &= 2^k\left[\left(\frac{3}{2}\right)^k\right] - 1 - 2^k\left[\left(\frac{3}{2}\right)^k\right] + \left[\left(\frac{3}{2}\right)^k\right] + 2^k - 1 \\ &= \left[\left(\frac{3}{2}\right)^k\right] + 2^k - 2 = I(k). \end{aligned}$$

Koska $g(k) \geq a + b$ ja $a + b = n - (2^k - 1)a \geq I(k)$, niin $g(k) \geq I(k)$. $\square$

Huomautus 3.26. Lauseen 3.25 todistuksen olen ottanut oppikirjasta [1], jossa on Waringin Probleemaa käsittelevä luku. Tätä lukua (ja kirjaa muutenkin) voin

suositella, mutta sitä lukiessa on otettava huomioon kirjan ilmestymisvuosi 1972. Vuonna 1909 Wieferich julkaisi todistuksen sille, että $g(3) = I(3) = 9$ ja Kempner täydensi todistuksessa olleen puutteen 1912. Kirjassa [1] nämä seikat mainitaan, ja lisäksi esitetään mm. yksinkertainen todistus heikommalle tulokselle (Maillet, 1895) $g(3) \leq 21$. Mutta vasta 1986 intialainen Balasubramanian ja ranskalaiset Deshouillers ja Dress todistivat yhteistyönään, että $g(4) = I(4) = 19$. Todistus on erittäin vaikea. Lukija voi katsella kolmikon kahta portrettia netistä [9] (kravattikaulainen matemaatikko on Jean-Marc Deshouillers). Mitä taas tulee Eulerin konjektuuriin, niin nykyään tiedetään, että se pätee, lukuunottamatta **mahdollisesti** äärellisen montaa poikkeusta.

Vaikka Eulerin konjektuuri $g(k) = I(k)$ saataisiin täydellisesti selvitettyä, ei se kuitenkaan lopettaisi matemaatikkojen työskentelyä Waringin Probleeman parissa. On esimerkiksi todistettu, että ainoastaan luvut 23 ja 239 vaativat yhdeksän kuutiota, muut voidaan esittää kahdeksan kuution summana. Tämä ilmiö antaa aiheen seuraavalle määritelmälle:

Määritelmä 3.27. Olkoon $G(k)$ **pienin** luku siten, että **jollakin** $n_0 \in \mathbb{N}^*$ pätee

$$n \geq n_0 \Rightarrow n = x_1^k + \cdots + x_{G(k)}^k \quad \text{joillakin } x_i \in \mathbb{N}.$$

Määritelmistä 3.24 ja 3.27 seuraa heti, että $G(k) \leq g(k)$. Koska on olemassa äärettömän monta lukua (esimerkiksi luvut $8m + 7$, vrt. Lause 3.22) jotka eivät ole kolmen neliön summia, saadaan tulos $G(2) = 4$. Ainoastaan yksi toinen G:n arvo tunnetaan, $G(4) = 16$, muiden lukujen k kohdalla täytyy tyytyä erilaisiin arvioihin. Kun Ressun lukiossa sanoin, että näistä kahdesta täsmällisestä tuloksesta ei suinkaan pidä päätellä, että aina olisi $G(k) = k^2$, minulta kysyttiin, voidaanko **todistaa**, että $G(k) \neq k^2$ kun $k \notin \{2, 4\}$. Siihen en osannut suoralta kädeltä vastata, mutta konsultoituani Wikipedian artikkelia "Waring's problem" [7] saatoin seuraavalla tunnilla helposti antaa vastauksen

Lause 3.28. *$G(k) < k^2$ kun $k \notin \{2, 4\}$.*

Tod. Se, että $G(k) < k^2$ kun $k \notin \{2, 4\}$, $k \leq 20$, seuraa taulukosta, jossa on ilmoitettu yläraja luvulle $G(k)$:

k	3	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$G(k) \leq$	7	17	21	33	42	50	59	67	76	84	92	100	109	117	125	134	142

Arvoilla $k > 20$ voidaan käyttää Vinogradovin tulosta vuodelta 1947: $G(k) \leq k(3 \ln k + 11)$. Pätee nimittäin

$$k(3 \ln k + 11) < k^2 \Leftrightarrow 3 \ln k + 11 < k \Leftrightarrow k \geq 20,$$

kuten lukija voi helposti todeta esim. muodostamalla funktion $f(x) = x - 3 \ln x - 11$ ja tutkimalla sen käyttäytymistä derivaatan $f'(x) = 1 - 3/x$ avulla. $\square$

4. Fermat'n Suuri Lause tapauksessa n=4

Pythagoraan kolmikot

Tässä viimeisessä luvussa päämääränä on todistaa Fermat'n Suuri Lause tapauksessa $n = 4$, toisin sanoen

Lause 4.1. *(Fermat) Yhtälöllä*

$$x^n + y^n = z^n, \tag{4.1}$$

missä $n = 4$, ei ole ratkaisua $x, y, z \in \mathbb{N}^*$.

Lähdemme liikkeelle tarkastelemalla yhtälöä (4.1) kun $n = 2$:

Määritelmä 4.2. Olkoon $x, y, z \in \mathbb{N}^*$. Kolmikko (x, y, z) on **Pythagoraan kolmikko**, jos

$$x^2 + y^2 = z^2. \tag{4.2}$$

Pythagoraan kolmikko (x, y, z) on **primitiivinen**, jos $syt(x, y, z) = 1$.

Esimerkki 4.3. $(3, 4, 5)$ on primitiivinen Pythagoraan kolmikko.

Olkoon (x, y, z) Pythagoraan kolmikko ja olkoon $d = syt(x, y, z)$. Kirjoitetaan $x = dx_1$, $y = dy_1$ ja $z = dz_1$. Tällöin

$$x_1^2 + y_1^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = z_1^2$$

ja lisäksi $syt(x_1, y_1, z_1) = 1$ (Lause 1.11). Tästä seuraa, että (x_1, y_1, z_1) on **primitiivinen** Pythagoraan kolmikko. Tämä tarkastelu osoittaa, että riittää tuntea primitiiviset Pythagoraan kolmikot: kaikki muut Pythagoraan kolmikot saadaan kertomalla primitiivisen kolmikon alkiot jollain luvulla $k \in \mathbb{N}^*$.

Tarkastelemme seuraavassa siis lähemmin primitiivisiä Pythagoraan kolmikkoja (p.P.k.). Nämä hallitaan täydellisesti: tulemme todistamaan lauseen, jossa annetaan kaavat kaikkien p.P.k. muodostamiseksi. Tämä vaatii kuitenkin jonkin verran valmisteluja.

Lemma 4.5. *Jos (x, y, z) on primitiivinen Pythagoraan kolmikko, niin luvuista x ja y toinen on parillinen ja toinen pariton. (Tällöin z on selvästi pariton.)*

Tod. A) Jos x ja y olisivat molemmat parillisia, niin tällöin (4.2):n nojalla myös z olisi parillinen. Mutta tällöin $2|x$, $2|y$ ja $2|z$, mikä on RR oletuksen $syt(x, y, z) = 1$ kanssa.

B) Jos x ja y olisivat molemmat parittomia, niin tällöin olisi $x^2 \equiv 1 \pmod 4$ ja $y^2 \equiv 1 \pmod 4$, josta seuraisi

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4.$$

Tämä on kuitenkin mahdotonta, koska jokainen neliö on kongruentti joko 0:n tai 1:n kanssa modulo 4.

Väite seuraa heti A):sta ja B):stä. □

Huomautus 4.6. Hyödyllinen huomio (jota jatkossa käytetään useasti) on se, että jos (x, y, z) on p.P.k., niin luvut x, y ja z ovat **parittain keskenään jaottomia**, toisin sanoen $syt(x, y) = syt(x, z) = syt(y, z) = 1$ (vrt. Huomautus 1.5). Olkoon esim. $syt(x, y) = d > 1$. Tällöin on olemassa $p \in \mathbb{P}$ siten, että $p|d$ (Lause 1.21 tai Aritmetiikan peruslause). Koska $d|x$ ja $d|y$, niin $p|x$ ja $p|y$ (Lause 1.3 (2)). Tästä seuraa, että pätee myös $p|x^2$ ja $p|y^2$, josta (4.2):n nojalla seuraa, että $p|z^2$. Koska p on alkuluku, saadaan $p|z$, ja on saatu RR oletuksen $syt(x, y, z) = 1$ kanssa. Aivan samalla tavalla todistetaan, että $syt(x, z) = syt(y, z) = 1$.

Lemmasta 4.5 seuraa helposti, että ei ole olemassa sellaista p.P.k. (x, y, z), jossa x, y ja z olisivat kaikki alkulukuja. Olkoon esimerkiksi x parillinen. Jos x olisi alkuluku, täytyisi siis olla $x = 2$. Tällöin olisi $4 = 2^2 = z^2 - y^2 = (z - y)(z + y)$, josta seuraisi, että $z - y = 1$ ja $z + y = 4$. Laskemalla yhteen kaksi viimeistä yhtälöä saadaan $2z = 5$, josta seuraisi, että 5 on parillinen luku, RR.

Sellaisia p.P.k. (x, y, z), joissa kaksi luvuista x, y, z on alkulukuja, ovat esimerkiksi $(3, 4, 5)$, $(11, 60, 61)$ ja $(19, 180, 181)$. Ei tiedetä onko tällaisia kolmikkoja äärettömän monta.

Tarvitsemme pian tulosta, joka sanoo että jos kahden keskenään jaottoman luvun tulo on neliö, niin luvut itsekin ovat neliöitä. Muotoilemme tuloksen koskemaan yleisemmin n:nsiä potensseja, koska todistus menee ihan samoin kuin neliöiden tapauksessa.

Lemma 4.7. *Olkoon $a, b, c, n \in \mathbb{N}^*$, $syt(a, b) = 1$ ja $ab = c^n$. Tällöin a ja b ovat n:nsiä potensseja, toisin sanoen on olemassa $a_1, b_1 \in \mathbb{N}^*$ siten, että $a = a_1^n$ ja $b = b_1^n$.*

Tod. Selvästikin voidaan olettaa, että $a > 1$ ja $b > 1$. Olkoot a:n ja b:n alkutekijähajoitelmat $a = p_1^{k_1} \cdots p_r^{k_r}$ ja $b = q_1^{t_1} \cdots q_s^{t_s}$. Koska a ja b ovat keskenään jaottomat, niin (vrt. Seurauksen 2.7 todistus) luvun ab alkutekijähajoitelma on

$$ab = p_1^{k_1} \cdots p_r^{k_r} q_1^{t_1} \cdots q_s^{t_s}.$$

Oletetaan, että luvun c alkutekijähajoitelma on $c = u_1^{e_1} \cdots u_h^{e_h}$. Tällöin oletuksesta $ab = c^n$ seuraa

$$p_1^{k_1} \cdots p_r^{k_r} q_1^{t_1} \cdots q_s^{t_s} = u_1^{ne_1} \cdots u_h^{ne_h}.$$

Aritmetiikan peruslauseesta seuraa, että alkuluvut $u_1, \dots u_h$ ovat samat kuin alkuluvut $p_1, \dots, p_r, q_1, \dots, q_s$ (jossakin järjestyksessä) ja edelleen, että $ne_1, \dots, ne_h$ ovat samat kuin eksponentit $k_1, \dots, k_r, t_1, \dots, t_s$ (vastaavassa järjestyksessä). Tästä päättelemme, että jokainen eksponenteista k_i ja t_j on jaollinen n:llä, mistä seuraa, että jos määritellään

$$a_1 = p_1^{k_1/n} \cdots p_r^{k_r/n}, \quad b_1 = q_1^{t_1/n} \cdots q_s^{t_s/n},$$

niin tällöin $a_1^n = a$ ja $b_1^n = b$ kuten haluttiin. □

Seuraavaa tulosta tarvitsemme vasta vähän myöhemmin, ja kuten Lemmaa 4.7, sitäkin vain erikoistapauksessa $n = 2$.

Lemma 4.8. *Olkoon $a, b, n \in \mathbb{N}^*$. Jos $a^n | b^n$, niin $a | b$.*

Tod. Voidaan olettaa, että $a > 1$ ja $b > 1$. (Jos $a = 1$, niin ilman muuta $a|b$. Jos taas $b = 1$, niin $b^n = 1$, jolloin on oltava $a^n = 1$, josta seuraa, että $a = 1$.) Olkoon $b = p_1^{k_1} \cdots p_r^{k_r}$ luvun b alkutekijähajoitelma. Tällöin

$$b^n = p_1^{nk_1} \cdots p_r^{nk_r}$$

ja koska tässä $b > 1$ on mielivaltainen, niin huomataan, että **jos joku luku** (> 1) **on n:s potenssi, niin sen alkutekijähajoitelmassa eksponentit ovat n:llä jaollisia**.

Koska oletuksen nojalla $a^n | b^n$, niin Lauseen 2.4 nojalla

$$a^n = p_1^{t_1} \cdots p_r^{t_r}, \text{ missä } 0 \le t_i \le nk_i, \quad i = 1, \dots, r.$$

Äskeisen havainnon nojalla $t_i = nt_i'$ kun $t_i > 0$; tämä pätee myös jos $t_i = 0$. Tästä seuraa, että

$$a^n = p_1^{nt_1'} \cdots p_r^{nt_r'} = (p_1^{t_1'} \cdots p_r^{t_r'})^n,$$

josta seuraa, että $a = p_1^{t_1'} \cdots p_r^{t_r'}$. Koska $0 \le nt_i' \le nk_i$, $i = 1, \dots, r$, niin pätee myös $0 \le t_i' \le k_i$, josta seuraa Lauseen 2.4 nojalla, että $a|b$. □

Huomautus 4.9. Lemmat 4.7 ja 4.8 ovat triviaaleja, jos $n = 1$. Lemman 4.8 tulos pätee myös kääntäen: jos $a|b$, niin $a^n|b^n$. Tämä nähdään aivan helposti. Jos nimittäin $b = ac$, niin tällöin $b^n = a^n c^n$.

Näiden valmistelujen jälkeen primitiivisten Pythagoraan kolmikkojen karakterisointi sujuu jo melko mukavasti.

Lause 4.10. *Kaikki ratkaisut Pythagoraan yhtälölle*

$$x^2 + y^2 = z^2, \tag{4.2}$$

jotka toteuttavat ehdot

$$x, y, z \in \mathbb{N}^*, \qquad syt(x, y, z) = 1, \qquad 2|x$$

saadaan kaavoilla

$$x = 2st,\ y = s^2 - t^2,\ z = s^2 + t^2$$

missä $s, t \in \mathbb{N}^*$ *toteuttavat ehdot* $s > t$, $syt(s, t) = 1$ *ja* $s \not\equiv t \pmod 2$.

Tod. A) Olkoon (x, y, x) sellainen p.P.k., jossa x on parillinen. Tällöin (Lemma 4.5) y ja z ovat parittomia, joten $z - y$ ja $z + y$ ovat parillisia; olkoon $z - y = 2v$ ja $z + y = 2u$. Yhtälö (4.2) voidaan kirjoittaa uudelleen muodossa

$$x^2 = z^2 - y^2 = (z - y)(z + y),$$

josta seuraa, että

$$(x/2)^2 = \Big(\frac{z - y}{2}\Big)\Big(\frac{z + y}{2}\Big) = vu.$$

Huomaa, että u ja v ovat keskenään jaottomat, koska jos olisi $syt(u, v) = d > 1$, niin tällöin $d|(u - v)$ ja $d|(u + v)$, toisin sanoen $d|y$ ja $d|z$, mikä on RR sen kanssa, että $syt(y, z) = 1$ (Huomautus 4.6). Lemmasta 4.7 (kun $n = 2$) seuraa nyt että u ja v ovat molemmat neliöitä; olkoon vaikka

$$u = s^2, \quad v = t^2,$$

missä $s, t \in \mathbb{N}^*$. Tästä saadaan

$$\begin{aligned} z &= u + v = s^2 + t^2, \\ y &= u - v = s^2 - t^2 > 0 \Rightarrow s > t, \\ x^2 &= 4uv = 4s^2t^2 \end{aligned}$$

ja viimeisestä yhtälöstä edelleen $x = 2st$. Koska jokainen s:n ja t:n yhteinen tekijä jakaa sekä y:n että z:n, niin edellä jo käytetystä ehdosta $syt(y, z) = 1$ seuraa, että $syt(s, t) = 1$. Ei enää tarvita muuta kuin todeta, että jos s ja t olisivat molemmat parillisia tai molemmat parittomia, niin siitä seuraisi että y ja z olisivat molemmat parillisia, mikä on mahdotonta (koska $syt(y, z) = 1$; itse asiassa tiedämme, että y ja z ovat molemmat parittomia). Tästä seuraa, että toinen luvuista s ja t on parillinen ja toinen pariton, mikä tarkoittaa täsmälleen sitä että $s \not\equiv t \pmod 2$.

B) Oletamme nyt kääntäen, että s ja t toteuttavat lauseessa annetut ehdot. Se, että $x = 2st$, $y = s^2 - t^2$ ja $z = s^2 + t^2$ muodostavat Pythagoraan kolmikon (x, y, z) seuraa helposti tarkistettavalla laskulla

$$x^2 + y^2 = (2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2 = z^2.$$

Olkoon $d = syt(x, y, z)$. Oletamme, että $d > 1$ ja tarkastelemme jotakin d:n alkutekijää p. Koska p jakaa parittoman luvun z (oletettiin, että toinen luvuista s, t on parillinen ja toinen pariton, joten luvun $s^2 + t^2 = z$ on oltava pariton), on oltava $p \neq 2$. Koska $p|y$ ja $p|z$, niin $p|(z + y)$ ja $p|(z - y)$, toisin sanoen $p|2s^2$ ja $p|2t^2$. Koska nyt $syt(p, 2) = 1$, niin Eukleideen lemmasta (Lause 1.16) seuraa, että $p|s^2$ ja $p|t^2$. Koska p on alkuluku, saadaan tästä $p|s$ ja $p|t$, mikä on RR oletuksen $syt(s, t) = 1$ kanssa. Tästä seuraa, että täytyy olla $d = 1$ ja siten (x, y, z) on primitiivinen Pythagoraan kolmikko. □

Seuraavassa taulukossa on jokaista arvoa $s = 2, 3, \ldots, 7$ kohti valittu t, joka on s:n kanssa keskenään jaoton, pienempi kuin s ja parillinen täsmälleen silloin kun s on pariton.

s	t	$x = 2st$	$y = s^2 - t^2$	$z = s^2 + t^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85

Taulukossa olevissa p.P.k.:ssa joko x tai y (mutta ei molemmat, vrt. Huomautus 4.6) on jaollinen luvulla 3. Tämä on helppo todistaa yleisesti käyttäen Lausetta 4.10. Jos nimittäin $3|s$ tai $3|t$, niin tällöin selvästi $3|x$. Jos taas $3 \not| s$ ja $3 \not| t$, niin $s \equiv \pm 1 \pmod 3$ ja $t \equiv \pm 1 \pmod 3$, josta seuraa, että

$$s^2 \equiv 1 \pmod 3, \quad t^2 \equiv 1 \pmod 3$$

ja siten

$$y = s^2 - t^2 \equiv 0 \pmod 3,$$

josta nähdään, että $3|y$.

Samaan tapaan voidaan todistaa, että jokaisessa p.P.k.:ssa täsmälleen yksi luvuista x, y ja z on jaollinen luvulla 5. Jätän tämän todistuksen lukijan harteille. Huomattakoon, että tämän pidemmälle ei voida enää mennä samaan suuntaan, mikä seuraa tarkastelemalla kolmikkoa $(3, 4, 5)$.

Määritelmä 4.11. Pythagoraan kolmio on suorakulmainen kolmio, jonka sivujen pituudet ovat kokonaislukuja, toisin sanoen suorakulmainen kolmio, jonka kateetit x, y ja hypotenuusa z muodostavat Pythagoraan kolmikon (x, y, z).

Ennenkuin käymme Fermat'n Suuren Lauseen erikoistapauksen $n = 4$ kimppuun, esitän vielä Lauseen 4.10 geometrisena sovelluksena seuraavan tuloksen.

Lause 4.12. *Pythagoraan kolmion sisäänpiirretyn ympyrän säde r on kokonaisluku.*

Tod. Kateetit x ja y voidaan valita siten, että

$$x = 2kst,\ y = k(s^2 - t^2),\ z = k(s^2 + t^2),\quad \text{missä } k \in \mathbb{N}^*. \tag{4.3}$$

Kolmion ala voidaan laskea kahdella tavalla: 1) kateettien x ja y avulla ja 2) kolmen osakolmion summana, missä osakolmiot saadaan yhdistämällä sisäänpiirretyn ympyrän keskipiste alkuperäisen kolmion kärkiin. Kaikissa osakolmioissa on korkeutena r.

Edelläoleva huomio johtaa sievennettyyn yhtälöön $xy = r(x+y+z)$, josta ratkaisemalla r ja käyttämällä yhtälöitä (4.3) saadaan

$$\begin{aligned} r &= \frac{2k^2st(s^2 - t^2)}{k(2st + s^2 - t^2 + s^2 + t^2)} \\ &= \frac{kt(s^2 - t^2)}{s + t} = kt(s - t), \end{aligned}$$

mikä on kokonaisluku. □

Huomautus 4.13. Pythagoraan kolmion ala on (positiivinen) kokonaisluku. Tämä on selvää, koska tiedämme, että ainakin toinen kateeteista on parillinen luku.

Fermat'n Suuren Lauseen todistus tapauksessa $n = 4$

Vaikka voidaankin pitää epätodennäköisenä, että Fermat olisi todella todistanut Suuren Lauseensa, niin tapauksen $n = 4$ kohdalla tilanne on toinen: seuraavassa esitettävä todistus on olennaisesti Fermat'n oma. Siinä käytetään Fermat'n 'äärettömän laskeutumisen' menetelmää. Antakaamme Fermat'n itse esitellä tämä mainio menetelmä! Vapaasti ja hieman lyhentäen suomennan otteen Fermat'n kirjeestä Carcaville 1659 (vrt. [11, s. 41–45]).

"Kutsun tätä todistusmenetelmää *äärettömäksi laskeutumiseksi*; aluksi käytin sitä ainoastaan negatiivisten väitteiden todistamiseen, esimerkkinä seuraava:

Ei ole olemassa Pythagoraan kolmiota, jonka ala olisi neliö. [Vrt. Huomautus 4.13. Todistus löytyy Burtonin kirjasta [4].]

Epäsuora todistus menee seuraavaan tapaan:

Jos olisi olemassa Pythagoraan kolmio, jonka ala olisi neliö, niin olisi olemassa alaltaan pienempi Pythagoraan kolmio, jolla on sama ominaisuus. Jos on olemassa toinen, pienempi kuin ensimmäinen, jolla on sama ominaisuus, niin samalla päättelyllä olisi olemassa kolmas, pienempi kuin tämä toinen, jolla olisi sama ominaisuus, ja edelleen neljäs, viides, äärettömästi laskeutuen. Mutta jos joku luku on annettu, ei voi olla äärettömän monta sitä pienempää lukua (puhun nyt positiivisista kokonaisluvuista). Tästä päättelemme, että on mahdotonta, että olisi olemassa Pythagoraan kolmio, jonka ala olisi neliö."

Tuttuun tyyliinsä Fermat lisää, että hän ei viitsi kertoa, millä perusteella hän päättelee, että olisi olemassa kyseessä olevan laatuinen pienempi Pythagoraan kolmio, koska selitys olisi liian pitkä ja sitäpaitsi siinä juuri piilee hänen menetelmänsä salaisuus.

Osoittautuu helpommaksi todistaa ensin hieman vahvempi tulos.

Lause 4.14. *(Fermat) Yhtälöllä*

$$x^4 + y^4 = z^2 \tag{4.4}$$

ei ole ratkaisua $x, y, z \in \mathbb{N}^*$.

Tod. Olettakaamme, että yhtälöllä (4.4) on ratkaisu $x_0, y_0, z_0 \in \mathbb{N}^*$. Fermat'n 'äärettömän laskeutumisen' menetelmää soveltaen haluamme osoittaa, että yhtälöllä (4.4) on toinen ratkaisu $x_1, y_1, z_1 \in \mathbb{N}^*$, jossa $z_1 < z_0$. Merkitään $d = syt(x_0, y_0)$. Jaetaan todistus kahteen tapaukseen.

A) $d > 1$. Kirjoitetaan $x_0 = dx_1$ ja $y_0 = dy_1$. Koska

$$d^4(x_1^4 + y_1^4) = z_0^2,$$

nähdään, että $d^4 | z_0^2$ josta (Lemma 4.8 $n = 2$) seuraa, että $d^2 | z_0$. Voidaan siis kirjoittaa $z_0 = d^2 z_1$ ja saadaan

$$x_1^4 + y_1^4 = z_1^2.$$

Lisäksi $z_1 = z_0/d^2 < z_0$, koska oletuksen nojalla $d > 1$.

B) $d = 1$. Nyt siis $syt(x_0, y_0) = 1$, josta Aritmetiikan peruslauseen nojalla seuraa heti myös $syt(x_0^2, y_0^2) = 1$. Tällöin myös $syt(x_0^2, y_0^2, z_0) = 1$ (Huomautus 1.15), joten (x_0^2, y_0^2, z_0) on p.P.k. ja voimme käyttää Lausetta 4.10. Voimme olettaa, että x_0^2 (ja siis myös x_0) on parillinen, jolloin on olemassa Lauseessa 4.10 esiintyvät $s, t \in \mathbb{N}^*$ siten, että

$$\begin{aligned} x_0^2 &= 2st, \\ y_0^2 &= s^2 - t^2, \\ z_0 &= s^2 + t^2. \end{aligned}$$

Jos tässä s olisi sattumalta parillinen, niin saataisiin

$$1 \equiv y_0^2 = s^2 - t^2 \equiv 0 - 1 \equiv 3 \pmod 4,$$

mikä on mahdotonta. Tästä seuraa, että s:n on oltava pariton ja sen seurauksena t on parillinen. Kirjoitetaan $t = 2r$. Tällöin yhtälöstä $x_0^2 = 2st$ tulee $x_0^2 = 4sr$, mikä voidaan kirjoittaa muodossa

$$(x_0/2)^2 = rs.$$

Koska ehdosta $syt(s,t) = 1$ seuraa $syt(s,r) = 1$, niin (Lemma 4.7 $n = 2$) voidaan kirjoittaa $s = z_1^2$, $r = w_1^2$ missä $z_1, w_1 \in \mathbb{N}^*$.

Nyt haluamme käyttää Lausetta 4.10 uudelleen, soveltaen sitä tällä kertaa yhtälöön

$$t^2 + y_0^2 = s^2.$$

Koska $syt(s,t) = 1$, niin pätee myös $syt(t, y_0, s) = 1$, joten (t, y_0, s) on p.P.k. Koska tiedämme, että t on parillinen, saadaan

$$\begin{aligned} t &= 2uv, \\ y_0 &= u^2 - v^2, \\ s &= u^2 + v^2, \end{aligned}$$

missä $u, v \in \mathbb{N}^*$ ovat keskenään jaottomat. Yhtälöstä

$$uv = t/2 = r = w_1^2$$

seuraa, että u ja v ovat molemmat neliöitä (Lemma 4.7 jälleen käytössä). Kirjoitetaan $u = x_1^2$ ja $v = y_1^2$, missä $x_1, y_1 \in \mathbb{N}^*$. Kun nämä sijoitetaan aikaisempaan s:n yhtälöön, niin saadaan

$$z_1^2 = s = u^2 + v^2 = x_1^4 + y_1^4,$$

josta nähdään, että $x_1, y_1, z_1 \in \mathbb{N}^*$ muodostavat (4.4):n ratkaisun. Lisäksi pätee

$$z_1 \leq z_1^2 = s \leq s^2 < s^2 + t^2 = z_0,$$

joten todistus on päättynyt. □

Nyt päästäänkin helposti päämäärään:

Lauseen 4.1 todistus. Jos $x, y, z \in \mathbb{N}^*$ olisi yhtälön

$$x^4 + y^4 = z^4$$

ratkaisu, niin $x, y, z^2 \in \mathbb{N}^*$ olisi yhtälön (4.4) ratkaisu. Tämä olisi RR Lauseen 4.14 kanssa. □

Kiitokset

Ressun lukion rehtori Ari Huovinen, opettajat Hilkka Taavitsainen, Susanna Moksunen, Jarkko Jänis ja Mika Spåra, sekä luonnollisesti myös kurssilleni osallistuneet oppilaat saavat kaikki kauniit kiitokseni.

Viitteet

[1] Agnew, Jeanne: *Explorations in number theory*, Brooks/Cole Publishing Co., 1972.

[2] Apiola, Heikki: Lukuteoriaa ja salakirjoitusta, osa 1, *Solmu* 3/2007, 7–13.

[3] Borho, Walter: Befreundete Zahlen: ein zweitausend Jahre altes Thema der elementaren Zahlentheorie, *Lebendige Zahlen, 5–38, Math. Miniaturen, 1, Birkhäuser, 1981.*

[4] Burton, David M.: *Elementary number theory*, Revised printing, Allyn and Bacon, Inc., 1980. Useita painoksia, esim. 6th. ed., McGraw-Hill, 2005.

[5] Hautajärvi, Ottelin, Wallin-Jaakkola: *Laudatur 11, Lukuteoria ja logiikka*, Otava, 2006.

[6] `http://en.wikipedia.org/wiki/Mersenne_prime`

[7] `http://en.wikipedia.org/wiki/Waring's_problem`

[8] `http://www-history.mcs.st-and.ac.uk/history/`

[9] `http://www.math.u-bordeaux.fr/~dress/g4_19.html`

[10] `http://www.math.ucla.edu/~tao/`

[11] Itard, Jean: *Arithmétique et théorie des nombres*, "Que sais-je?" No. 1093, Presses Universitaires de France, 1963.

[12] Khinchin, A. Y.: *Three pearls of number theory*, Graylock Press, 1952.

[13] Lagarias, Jeffrey C.: An elementary problem equivalent to the Riemann hypothesis, *Amer. Math. Monthly* **109** (2002), no. 6, 534–543.

[14] Lagrange, J. L.: Démonstration d'un théorème d'arithmétique, *Oeuvres III*, 189–201, `http://www.gdz-cms.de/no_cache/dms/load/img/?IDDOC=41080`

[15] Landau, Edmund: *Elementary number theory*, translated by J. E. Goodman, Chelsea Publising Co., 1958.

[16] Vala, Klaus: *Nikolai Kval*, Art House, 1955.