TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Teemu Lehtonen

Alkulukujen teoriaa ja Goldbachin otaksuma

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Maaliskuu 2004

Sisältö

1 Johdanto

Kuten työn otsikosta voi jo arvata, tämä työ käsittelee alkulukuja ja yhtä niihin liittyvää ratkaisematonta ongelmaa, Goldbachin otaksumaa. Alkulukuteoria on jaettu neljään osioon (pohjustusta, alkulukujen määrä, alkulukujen sijoittuminen ja alkulukujen tuottaminen), joilla pyritään antamaan kattava käsitys siitä, mitä alkuluvut ovat ja siitä, mitä niistä tänä päivänä tiedetään. Goldbachin otaksumaa koskeva kappale on jaettu kahteen osioon (otaksuman historia ja otaksumasta), joista ensimmäinen esittää nimensä mukaan otaksumaan liittyvän historian ja toinen otaksumaa hieman tarkemmin, lähinnä antaen hieman tietoa siitä, miten otaksumaa on pyritty todistamaan. Mitään varsinaisia osatodistuksia tai hyvin pitkälle vietyjä tietokonepohjaisia suuntaa antavia todistuksia ei työssä kuitenkaan esitetä, niiden laajuuden ja monimutkaisuuden vuoksi.

Työssä on pyritty siihen, että jokainen sen lukija pystyy ymmärtämään niin itse teorian kuin sen todistuksetkin. Liian syvälle menevät todistukset on työn eri vaiheissa jätetty pois, ja näin pääpaino on pyritty pitämään juuri niiden lauseiden todistuksissa, jotka työn aiheiden kannalta eniten kiinnostavat. Jokaisen todistamattoman lauseen todistus on kuitenkin saatavilla lähdeteoksesta, johon lauseen perässä viitataan. Mikäli määritelmissä tai lauseissa ei erikseen mainita mihin lukujoukkoon niissä esiintyvät muuttujat kuuluvat, on syytä olettaa niiden kuuluvan kokonaislukuihin.

Alkuluvut ovat siis positiivisia kokonaislukuja, jotka ovat jaollisia ainoastaan luvulla 1 ja itsellään (ks. 5), ja Goldbach otaksui seuraavasti:

> Jokainen parillinen kokonaisluku ≥ 4 voidaan esittää kahden alkuluvun summana. (ks. 36)

Mikäli alkulukujen historia ei ole tuttu, esitetään seuraavaksi pääpiirteittäin, mistä kaikki on saanut alkunsa:
Ei ole selvinnyt, oliko jo babylonialaisilla käsitystä alkuluvuista, mutta ensimmäiset, jotka tutkivat alkulukuja ja niiden ominaisuuksia perusteellisesti, olivat antiikin Kreikan matemaatikot. Jo ennen 400 eKr, pythagorialaiset ottivat alkuluvut käyttöön numeroina, jotka voitiin järjestää vain yhteen riviin, eikä mihinkään muuhun suuruusjärjestykseen. Noin 300 eKr Eukleides puhui alkulukujen erilaisista ominaisuuksista teoksessaan *Elements* esittäen esimerkiksi todistuksen sille, että alkulukuja on ääretön määrä (ks. 10). Eratosthe-

nen seula (ks. 42) kuvailtiin 200 eKr, ilmeisesti Platonin ajatuksia seuraten. 1600-luvun alussa kehitettiin erilaisia metodeja tekijöihin liittyen ja tehtiin erilaisia otaksumia alkulukuja tuottavista kaavoista. Pierre Fermat ehdotti, että $2^{2^n}+1$ olisi alkulukujen alkulähde, ja Marin Mersenne sanoi sen olevan 2^p+1, missä p on alkuluku (ks. 12). Vuonna 1752 Christian Goldbach osoitti, että mikään tavallinen polynomi ei voi tuottaa vain alkulukuja (ks. 33), tosin Leonard Euler näytti, että n^2+n+41 tekee niin, kun $n<40$ (ks. 32). Alkaen 1800-luvun paikkeilta analyyttisessä arvioinnissa alkulukujen jakaumasta tehtiin mittava työ. Siitä sai alkunsa hidas työ suurien tiettyjen alkulukujen löytämiseksi; $2^{31}-1$ todettiin alkuluvuksi vuonna 1750 ja $2^{127}-1$ vuonna 1876. ($2^{2^5}+1$ todettiin yhdistetyksi vuonna 1732, ja nykyään tiedetään kaikkien lukujen $2^{2^n}+1$, kun $n \leq 32$, olevan yhdistettyjä.) Tämän jälkeen alkaen vuodesta 1950 elektronisten tietokoneiden avulla on pystytty löytämään useita uusia isoja alkulukuja. Kahden viime vuosisadan aikana suurimman tunnetun alkuluvun pituus merkkeinä on kasvanut, historiallisen karkeasti, eksponentiaalisesti. Tämä johtuu siitä, että suurimpia alkulukuja etsitään juuri Mersennen kaavalla (ks. 12). Tänä päivänä suurin tunnettu alkuluku on yli 6 miljoonaa numeroa pitkä ($2^{20996011}-1$ [6]).

Tänä päivänä, kun olemme siirtyneet ja siirrymme edelleen yhä vahvemmin tietokoneistettuun aikakauteen, uusien suurien alkulukujen löytäminen on saanut aivan uuden merkityksen. Koska tietokoneet ovat verkossa, turvattu tiedonsiirto on saanut hyvin tärkeän roolin. Kryptologia ja tarkemmin kryptografia eli salakirjoituksen teoria on tullut erittäin riippuvaiseksi juuri isoista alkuluvuista. Niiden avulla pystytään salaamaan tekstiä niin, että edes tietokoneet eivät pysty laskemaan tarvittavia lukuja viestin luvattomaan avaamiseen. Tunnetumpia salakirjoitustekniikoita, jotka tarvitsevat suuria alkulukuja, ovat RSA ja El-Gamel.

Se, miksi valitsin työni aiheeksi juuri alkuluvut, johtaa juurensa hyvin kaukaa. Siihen sen tarkemmin menemättä mainittakoon ainakin se, että matematiikkaa lukeneena ei voi olla törmäämättä siihen, mihin kaikkeen matematiikan eri osa-alueita tarvitaan. Hyvänä esimerkkinä on juuri edellä mainittu kryptologia, jonka kehitys nojaa hyvin vahvasti juuri alkuluvuista hankittuun tietoon. Alkuluvut ovat muutenkin matematiikan se alue, mistä ei tiedetä vielä lähellekkään niin paljon kuin ehkä olisi mahdollista. Alkuluvut sisältävät salaisuuksia, joita matemaatikot ovat yrittäneet selvittää vuosisatoja pääsemättä minkäänlaiseen todelliseen läpimurtoon. Siitä hyvänä esimerkkinä on

juuri Goldbachin otaksuma, joka tuntuu ajatuksena hyvin yksinkertaiselta ja uskottavalta, mutta kuitenkaan sitä ei ole pystytty vielä todistamaan. Tämä on mielestäni erittäin mielenkiintoinen osa-alue matematiikasta, ja sitä tulisikin tutkia aina vain voimakkaammin panostuksin, jotta totuus alkulukujen takaa voitaisiin vihdoin saada esille.

Mikäli alkuluvut kiinnostavat aiheena voisi tässä työssä käytetyn kirjallisuuden lisäksi mainita ainakin kirjan *Prime Numbers: A Computational Perspective* (R.Crandall ja C.Pomerance, 2001). Se on hyvin kattava teos alkuluvuista ja niihin liittyvistä tiedossa olevista asioista. Teoksessa käsitellään teorian lisäksi myös tietokoneiden ottamista mukaan laskentaan. Siinä on pyritty myös siihen, että asiat tuotaisiin esille jokaisen ymmärtämällä tavalla. Mikäli myös Goldbachin otaksuma herättää kiinnostusta, on syytä tutustua kirjaan *Goldbach Conjecture* (Wang Yuan, 1984). Siinä on lähestytty Goldbachin otaksumaa todistamalla ensin, että jokainen pariton kokonaisluku on kolmen alkuluvun summa. Tämän jälkeen todistetaan, että jokainen parillinen kokonaisluku on kahden melkein alkuluvun summa (ks. 47) ja viimeisenä, että jokainen parillinen kokonaisluku on alkuluvun ja melkein alkuluvun summa.

2 Alkuluvuista

2.1 Pohjustusta

Aivan aluksi on syytä määritellä alkuluvut:

Määritelmä 2.1.1 *Kokonaislukua p (> 1) sanotaan* ***alkuluvuksi****, mikäli sen ainoat positiiviset jakajat ovat* 1 *ja* p*. Kokonaisluku, joka on suurempi kuin* 1 *mutta ei ole alkuluku, on* ***yhdistetty****.* [1, s. 40]

Huomautus Yhdistetty luku a voidaan esittää tulona bc $(1 < b, c < a)$.

Merkintä Alkulukujen joukkoa merkitään symbolilla $\mathbf{P}$.

Esimerkki 2.1.1 Luvut 2, 3, 5, 7 ja 11 ovat alkulukuja. Luvut 4, 6 ja 9 ovat yhdistettyjä.

Huomautus Luku 2 on ainoa parillinen alkuluku.

Esimerkki 2.1.2 Todista, että luku $a^4 - 2^4$ ei ole alkuluku aina, kun $a > 1$.

Ratkaisu Kirjoitetaan $a^4 - 2^4$ muodossa

$$\begin{aligned} a^4 - 2^4 &= (a^2)^2 - 4^2 \\ &= (a^2 - 4)(a^2 + 4). \end{aligned}$$

Koska $a > 1$, niin $a^2 - 4 > 1$ ja $a^2 + 4 > 1$. Siis $a^4 - 2^4$ ei ole alkuluku, vaan se on yhdistetty luku.

Alkulukujen perusteoriaan kuuluu oleellisena myös *aritmetiikan peruslause.* Seuraavaksi esitetään lauseita, joita tarvitaan peruslauseen todistamisessa.

Lause 2.1.1 (Eukleideen lemma) *Jos* $a \mid bc$ *ja* $\text{syt}(a, b) = 1$, niin $a \mid c$. [1, s. 24]

Todistus Sivuutetaan.

Lause 2.1.2 *Jos p on alkuluku ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.* [1, s. 41]

Todistus Mikäli $p \mid a$, niin lause on suoraan tosi. Valitaan siis, että $p \not| a$. Koska p on alkuluku, niin sen ainoat jakajat ovat 1 ja p. Siis $\text{syt}(a, p) = 1$. (Yleisesti alkuluvun p ja kokonaisluvun a suurin yhteinen tekijä $\text{syt}(a, p) = 1$ tai $\text{syt}(a, p) = p$.) Nyt Eukleideen lemmasta seuraa suoraan, että $p \mid b$. □

Esimerkki 2.1.3 Yleisesti tiedetään, että 3 on alkuluku ja että $3 \mid 30$. Tiedetään myös, että $30 = 6 \cdot 5$. Siis $3 \mid 6 \cdot 5$ ja edelleen $3 \mid 6$. Näin ollen 3 jakaa ainakin toisen tulon tekijän.

Huomautus Lause 2.1.2 voidaan helposti yleistää myös tuloihin, joissa on enemmän kuin kaksi tekijää.

Seuraus 1 Jos p on alkuluku ja $p \mid a_1 a_2 a_3 \cdots a_n$, niin $p \mid a_k$, kun $1 \leq k \leq n$. [1, s. 41]

Todistus Todistus perustuu induktioon n:n suhteen, missä n on tulon tekijöiden lukumäärä. Kun $n = 1$, niin lause on selvästi tosi. Kun taas $n = 2$, niin todistus menee lauseen 2.1.2 mukaisesti. Induktio-oletus on, että $n > 2$ ja että silloin kun p jakaa jonkin tulon, jossa on vähemmän kuin n tekijää, niin se jakaa ainakin yhden tulon tekijöistä. Oletetaan, että $p \mid a_1 a_2 a_3 \cdots a_n$. Nyt Lauseen 2.1.2 mukaan $p \mid a_n$ tai $p \mid a_1 a_2 a_3 \cdots a_{n-1}$. Mikäli $p \mid a_n$, niin lause on todistettu. Jos taas $p \mid a_1 a_2 a_3 \cdots a_{n-1}$, niin induktio-oletuksen mukaan $p \mid a_k$ jollain luvun k arvolla, kun $1 \leq k \leq n - 1$. Siis, joka tapauksessa p jakaa jonkin tulon $a_1 a_2 a_3 \cdots a_n$ tekijöistä. □

Esimerkki 2.1.4 Yleisesti tiedetään, että 5 on alkuluku ja että $5 \mid 200$. Tiedetään myös, että $200 = 10 \cdot 10 \cdot 2$, ja edelleen $5 \mid 10$. Näin ollen 5 jakaa ainakin yhden tulon tekijöistä.

Seuraus 2 Jos $p, q_1, q_2, q_3, \ldots, q_n$ ovat kaikki alkulukuja ja $p \mid q_1 q_2 q_3 \cdots q_n$, niin $p = q_k$ jollain luvun k arvolla, kun $1 \leq k \leq n$. [1, s. 41]

Todistus Seurauksen 1 perusteella voidaan todeta, että $p \mid q_k$ jollain luvun k arvolla, kun $1 \leq k \leq n$. Koska q_k on alkuluku, se on jaollinen vain luvulla 1 tai itsellään. Koska $p > 1$ (p on alkuluku), niin täytyy olla, että $p = q_k$. □

Esimerkki 2.1.5 Yleisesti tiedetään, että 7 on alkuluku ja että $7 \mid 70$. Tiedetään myös, että $70 = 7 \cdot 5 \cdot 2$ ja edelleen $7 \mid 7$. Näin ollen 7 on yksi alkuluvuista koostuvan tulon tekijöistä.

Edellä esitettyjen lauseiden ja seurausten avulla saamme käyttöön tarvittavat tiedot aritmetiikan peruslauseen todistamiseen.

Lause 2.1.3 (Aritmetiikan peruslause) *Jokainen kokonaisluku $n > 1$ voidaan esittää alkulukujen tulona. Saatu tulo on yksikäsitteinen, tekijöiden järjestystä lukuun ottamatta.* [1, s. 42]

Todistus Valitaan mielivaltainen kokonaisluku n. (Sen täytyy olla alkuluku tai yhdistetty luku.) Mikäli n on alkuluku, niin lause on todistettu. Olkoon n siis yhdistetty luku. Nyt on olemassa kokonaisluku d siten, että $d \mid n$, kun $1 < d < n$. Kaikkien mahdollisten lukujen d joukosta valitaan pienin (hyvän järjestyksen periaate) ja merkitään sitä symbolilla p_1.

> **Hyvän järjestyksen periaate:** Jokainen positiivisia kokonaislukuja sisältävä epätyhjä joukko sisältää aina pienimmän alkion; on olemassa kokonaisluku a, joka kuuluu joukkoon S siten, että $a \leq b$ aina, kun $b \in S$.

Nyt p_1 täytyy olla alkuluku, koska muuten myös sillä olisi tekijä q, $1 < q < p_1$. Silloin $q \mid p_1$ ja $p_1 \mid n$, josta seuraisi, että $q \mid n$. Tämä olisi ristiriidassa alkuperäisen valinnan kanssa, jonka mukaan p_1 on pienin n:n jakaja ($p_1 > 1$). Nyt voidaan kirjoittaa $n = p_1 n_1$, missä p_1 on alkuluku ja $1 < n_1 < n$. Mikäli n_1 on alkuluku, niin lause on todistettu. Mikäli se ei ole, niin n_1 voidaan edellä käytettyä keinoa toistamalla kirjoittaa muotoon $n_1 = p_2 n_2$ (p_2 alkuluku). Siis

$$n = p_1 p_2 n_2, \qquad 1 < n_2 < n_1.$$

Mikäli n_2 on alkuluku, niin lause on todistettu. Mikäli se ei ole, niin n_2 voidaan kirjoittaa muotoon $n_2 = p_3 n_3$ (p_3 alkuluku). Siis

$$n = p_1 p_2 p_3 n_3, \qquad 1 < n_3 < n_2.$$

Vähenevä jono

$$n > n_1 > n_2 > \cdots > 1$$

ei voi jatkua äärettömästi, joten äärellisen määrän askeleita jälkeen n_{k-1} on alkuluku. Merkitaan sitä symbolilla p_k. Näin on päästy luvun n *alkutuloesitykseen*

$$n = p_1 p_2 \cdots p_k.$$

Täytyy vielä todistaa, että saatu alkutuloesitys on yksikäsitteinen. Aloitetaan olettamalla, että kokonaisluku n voidaan esittää alkulukujen tulona kahdella eri tavalla,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \ , \qquad r \leq s,$$

missä p_i ja q_j $(1 \leq i \leq r$ ja $1 \leq j \leq s)$ ovat kaikki alkulukuja suuruusjärjestyksessä,

$$p_1 \leq p_2 \leq \cdots \leq p_r \ , \qquad q_1 \leq q_2 \leq \cdots \leq q_s.$$

Koska p_1 on luvun n tekijä, niin $p_1 \mid q_1 q_2 \cdots q_s$. Nyt lauseen 2.1.2 seurauksen 2 mukaan $p_1 = q_k$ jollain k:n arvolla $(1 \leq k \leq s)$, eli $p_1 \geq q_1$. Samalla periaatteella saadaan myös, että $q_1 \geq p_1$. Tästä seuraa, että $p_1 = q_1$. Ne voidaan siis supistaa pois,

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Nyt toistamalla sama prosessi saadaan, että $p_2 = q_2$. Ja edelleen

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s.$$

Jatkamalla vastaavasti ja olettaen, että $r < s$ päädytään lopulta tilanteeseen

$$1 = q_{r+1} q_{r+2} \cdots q_s,$$

mikä on mahdotonta, sillä $q_j > 1$ kaikilla j:n arvoilla. Siis $r = s$ ja

$$p_1 = q_1, \quad p_2 = q_2, \ldots, p_r = q_r.$$

Siis luvun n alkutuloesitykset ovat samat, eli alkutuloesitys on yksikäsitteinen. □

Esimerkki 2.1.6 Luvun 75460 esitys alkulukujen tulona on

$$75460 = 2 \cdot 2 \cdot 5 \cdot 7 \cdot 7 \cdot 7 \cdot 11.$$

Yleensä kirjoitetaan muotoon

$$75460 = 2^2 \cdot 5 \cdot 7^3 \cdot 11.$$

Määritelmä 2.1.2 *Luvun $a > 1$* ***kanoninen alkutekijäesitys*** *on muotoa*

$$a = {p_1}^{a_1} {p_2}^{a_2} \cdots {p_n}^{a_n},$$

missä $p_1, p_2, \ldots, p_n$ ($p_1 < p_2 < \cdots < p_n$) ovat luvun a alkulukutekijät ja $a_1, a_2, \ldots, a_n > 0$. Kanoniseksi alkutekijäesitykseksi sanotaan myös esitystä

$$a = \prod_{p \in \boldsymbol{P}} p^{a(p)},$$

missä p käy läpi kaikki alkuluvut ja $a(p) \geq 0$. [3, s. 22]

2.2 Alkulukujen määrä

Tässä kappaleessa esitetään kaksi alkulukujen määrään läheisesti liittyvää lausetta. Ensimmäinen niistä on ehdottomasti merkittävin ja toinen antaa meille edes jonkinlaisen käsityksen siitä, montako alkulukua on ennen tiettyä lukua.

2.2.1 Alkulukujen äärettömyys

Lause 2.2.1 (Eukleides) *Alkulukuja on ääretön määrä.* [1, s. 47]

Todistus Tehdään vastaoletus, että alkulukuja on äärellinen määrä. Olkoot ne $p_1,\ p_2, \ldots,\ p_n$. Merkitään $P = 1 + p_1 p_2 \cdots p_n$. Lauseen 2.3 mukaan, jokainen kokonaisluku voidaan esittää alkulukujen tulona. P on kokonaisluku. On siis oltava sellainen i, $1 < i < n$, että $p_i \mid P$ (Koska $p_1 p_2 \cdots p_n$ sisälsi kaikki alkuluvut). Tiedetään myös, että $p_i \mid p_1 p_2 \cdots p_n$. Siis $p_i \mid P - p_1 p_2 \cdots p_n$ ($a \mid b,\quad a \mid c \ \Rightarrow\ a \mid b - c$), eli $p_i \mid 1$. Tämä on kuitenkin mahdotonta, sillä $p_i > 1$. Siis vastaoletus on väärin, eli alkulukuja on ääretön määrä. □

2.2.2 Alkuluvun p_n arviointi

Lause 2.2.2 *Jos p_n on n. alkuluku, niin $p_n \leq 2^{2^{n-1}}$.* [1, s. 49]

Todistus Todistus perustuu induktioon luvun n suhteen. Selvästi epäyhtälö on totta, kun $n = 1$. Induktio-oletus on, että $n > 1$ ja että epäyhtälö on totta kaikilla kokonaisluvuilla lukuun n asti. Seuraavaksi tarkastellaan epäyhtälön toteutumista luvulla $n+1$. Selvästi alkulukujen tulo kasvaa kohti ääretöntä nopeammin kuin alkuluvut itse. Voidaan siis merkitä:

$$\begin{aligned} p_{n+1} &\leq p_1 p_1 \cdots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdot 2^{2^2} \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\cdots+2^{n-1}} + 1. \end{aligned}$$

Tarkastellaan seuraavaksi summaa $1+2+2^2+\cdots+2^{n-1}$. Kyseessä on geometrisen sarjan osasumma, jonka ensimmäinen termi on 1 ja kahden peräkkäisen termin suhde on 2. Siis sarjan summa on

$$\frac{1(1-2^n)}{1-2} = 2^n - 1.$$

Alkuperäinen epäyhtälö saadaan siis muotoon

$$p_{n+1} \leq 2^{2^n-1} + 1.$$

Koska $2^{2^n-1} \geq 1$ kaikilla luvun n arvoilla, niin

$$\begin{aligned} p_{n+1} &\leq 2^{2^n-1} + 2^{2^n-1} \\ &\leq 2 \cdot 2^{2^n-1} \\ &\leq 2^{2^n-1+1} \\ &\leq 2^{2^n}. \end{aligned}$$

Nyt siis epäyhtälö pätee myös luvulla $n+1$. Siis induktioperiaatteen perusteella lause on tosi. □

Seuraus Kun $n \geq 1$, niin on oltava ainakin $n+1$ alkulukua, jotka ovat pienempiä kuin 2^{2^n}.

Todistus Lauseesta 2.2.2 saadaan suoraan, että $p_1, p_2, \ldots, p_{n+1}$ ovat kaikki pienempiä kuin 2^{2^n}. □

Esimerkki 2.2.1 Ratkaise, montako alkulukua ainakin on oltava ennen lukua 1024.

Ratkaisu Ratkaistaan ensin n;

$$\begin{aligned} 1024 &= 2^{2^n} \\ \log(1024) &= 2^n \cdot \log(2) \\ 2^n &= \frac{\log(1024)}{\log(2)} \\ n \cdot \log 2 &= \log\left[\frac{\log(1024)}{\log(2)}\right] \\ n &\approx 3. \end{aligned}$$

Seurauksen perusteella tiedetään, että alkulukuja ennen lukua 1024 on oltava ainakin 4.

Kuten esimerkistä voi huomata, niin annettu lause ei anna varsinaisesti mitään uutta tietoa alkulukujen määrästä. Sitä voidaan kuitenkin käyttää hyväksi, kun halutaan todistetusti esittää alkulukujen vähimmäismäärä tietyllä välillä.

2.2.3 Alkulukulause

Fermat'n ja Mersennen luvut

$$F_n = 2^{2^n} + 1, \qquad n \geq 0, \qquad [1, s.\ 226]$$
$$M_n = 2^n - 1, \qquad n \geq 1, \qquad [1, s.\ 215]$$

ovat niin harvassa, että vaikka ne kaikki olisivat alkulukuja, niin silti alkulukujen jakaumasta yleisesti tiedettäisiin hyvin vähän. Paljon hedelmällisempi tutkielma, tosin empiirinen, oli 1792 Gaussin alulle panema. Hän käytti apunaan Johann Lambertin muutama vuosi aiemmin julkaisemaa alkulukujen taulukkoa, johon oli listattu kaikki lukua 102000 pienemmät alkuluvut. Perinteisesti merkitään, että $\pi(x)$ tarkoittaa lukua x pienempien alkulukujen määrää. Gauss pohti miten $\pi(x)$ kasvaa luvun x suhteen. Hän aloitti laskemalla alkulukujen määriä tietyn pituisissa peräkkäisissä etäisyyksissä ja sai aikaan seuraavan taulukon, missä $\Delta(x) = [\pi(x) - \pi(x - 1000)]/1000$:

x	$\pi(x)$	$\Delta(x)$
1000	168	0,168
2000	303	0,135
3000	430	0,127
4000	550	0,120
5000	669	0,119
6000	783	0,114
7000	900	0,117
8000	1007	,107
9000	1117	,110
10000	1229	0,112

Alkulukujen "tiheys" peräkkäisissä etäisyyksissä näytti olevan hitaasti vähenevä, keskimääräisesti, joten Gauss otti vastavuoroisesti funktion $\Delta(x)$ ja vertasi sitä moneen alkeisfunktioon. Muuttujan x luonnolliselle logaritmille saadaan seuraava taulukko:

x	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000
$\Delta(x)$	0,168	0,135	0,127	0,120	0,119	0,114	0,117	0,107	0,110	0,112
$\frac{1}{\log x}$	0,145	0,132	0,125	0,121	0,117	0,115	0,113	0,111	0,110	0,109

Yllättävän hyvä yhteensopivuus tuki voimakkaasti arvausta, että $\Delta(x)$ on suunnilleen $1/\log x$. Koska $\Delta(x)$ on jänteen kaltevuus funktion $y = \pi(x)$ kuvaajassa, niin hypoteettisen likimääräisen yhtäsuuruuden $\Delta(x) \approx 1/\log x$ tulisi olla integroitu saavuttamaan $\pi(x)$ itse, ja siten Gauss oletti, että

$$\pi(x) = \int_2^x \frac{dt}{\log t}.$$

Tätä integraalia, joka ei ole alkeisfunktio, on yleensä merkitty symbolilla $li(x)$; sen arvot on helppo laskea, ja viimeaikaiset laskennat funktiolle $\pi(x)$ tuottavat seuraavan vertailun (missä $li(x)$ on pyöristetty lähimpään kokonaislukuun):

x	$\pi(x)$	$li(x)$	$li(x) - \pi(x)$	$\pi(x)/li(x)$
10^3	168	178	10	0,94382
10^4	1229	1246	17	0.98636
10^5	9592	9630	38	0.99605
10^6	78498	78628	230	0.99835
10^7	664579	664918	339	0.99949
10^8	5761455	5762209	754	0.99987
10^9	50847534	50849235	1701	0.99997
10^{10}	455052512	455055614	3102	0.99999

Mitä Gauss halusi arvellessaan, että $li(x)$ on hyvä arvio funktiolle $\pi(x)$ isoilla luvun x arvoilla, ei oletettavasti ollut, että erotus $li(x) - \pi(x) \to 0$ eikä se

että $li(x) - \pi(x)$ pysyy rajallisena, vaan se että suhteellinen virhe

$$\frac{li(x) - \pi(x)}{\pi(x)} \to 0$$

tulee pieneksi tai että

$$\lim_{x\to\infty} \frac{\pi(x)}{li(x)} = 1. \tag{1}$$

Hän teki tämän oletuksen 1793, kun hän oli vasta 15-vuotias, mutta silti se todistettiin vasta yli 100 vuotta myöhemmin J. Hammondin ja C. de la Vallée Poussinin toimesta (riippumattomasti 1896). Ei ole vaikea huomata, että raja-arvo (1) implikoi raja-arvon

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1. \tag{2}$$

Koska näillä on niin keskeinen osa alkulukujen teoriassa, niin raja-arvo (1) tai perinteisemmin raja-arvo (2) tunnetaan *alkulukulauseena.* [3, s. 4–5]

Esimerkki 2.2.2 Laske, montako alkulukua, integraalin $li(x)$ mukaan, on pienempiä kuin 100. (Tarkka arvo on 25.)

Ratkaisu Sijoitetaan $x = 100$ integraaliin

$$li(x) = \int_2^x \frac{dt}{\log t}$$

ja integroidaan muuttujan t suhteen. Vastaukseksi saadaan, että ennen lukua sata on $29,081$ alkulukua. Siis vastaus on 29.

2.3 Alkulukujen jakautuminen

Tässä kappaleessa esitetään kaksi lausetta, joiden avulla saadaan tietoa alkulukujen sijainneista. Ensimmäisenä on lause, joka tarjoaa hyvän mahdollisuuden rajata alkuluku kahden kokonaisluvun väliin. Toisena on lause, jolla pystytään tutkimaan, ovatko kaksi kokonaislukua, joiden erotus on 2, alkulukuja.

2.3.1 Bertrandin hypoteesi

Aivan ensimmäisenä esitetään kolme apulausetta, joita tarvitaan ensimmäisen lauseen todistamiseen. Niitä ei kuitenkaan todisteta, koska niiden todistukset ovat erittäin vaativia ja laajoja ja koska pääpaino halutaan pitää lauseessa, joka kiinnostaa eniten.

Lemma 2.3.1 *Jos* $n \geq 3$ *ja* $\frac{2}{3}n < p \leq n$, *niin* $p \not| \binom{2n}{n}$. [3, s. 160]

Todistus Sivuutetaan.

Lemma 2.3.2 *Kun* $n \geq 2$, *niin jokaista alkulukua* $p \leq 2n$ *kohti on olemassa yksikäsitteinen kokonaisluku* r_p *siten, että* $p^{r_p} \leq 2n < p^{r_p+1}$ *ja että*

$$\frac{(2n)!}{(n!)^2} \Bigg| \prod_{p \leq 2n} p^{r_p}. \qquad [3, \text{ s. } 149]$$

($\prod_{p \leq 2n} p^{r_p} = {p_1}^{r_1} {p_2}^{r_2} \cdots {p_m}^{r_m}$, ks. Määritelmä 2.1.2)

Todistus Sivuutetaan.

Lemma 2.3.3 *Jokaiselle positiiviselle kokonaisluvulle* n, $\prod_{p \leq n} p < 4^n$. [3, s. 160]

Todistus Sivuutetaan.

Nyt olemme saaneet tarvittavat tiedot ensimmäisen lauseen todistamiseen.

Lause 2.3.1 *Jokaista positiivista kokonaislukua* n *kohti on olemassa alkuluku* p *siten, että* $n < p \leq 2n$. [3, s. 161]

Todistus Selvästi lause on tosi, kun $n = 1$ tai $n = 2$. Oletetaan, että se ei ole tosi jollain tietyllä kokonaisluvulla $n \geq 3$. Lemma 2.3.1 sanoo, että jokaisen alkuluvun, joka jakaa luvun $\binom{2n}{n}$, täytyy olla pienempi tai yhtä suuri kuin $\frac{2}{3}n$. Olkoon p sellainen alkuluku, ja oletetaan, että

$$p^e \Bigg\| \binom{2n}{n}.$$

$\Big($Merkinnällä $p^e \Big\| \binom{2n}{n}$ tarkoitetaan $\binom{2n}{n} = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_n}^{e_n}$. [3, s. 22]$\Big)$
Nyt Lemmasta 2.3.2 seuraa, että kun

$$\binom{2n}{n} \Bigg\| \prod_{p \leq 2n} p^{r_p}, \qquad \text{missä} \qquad p^{r_p} \leq 2n < p^{r_p+1},$$

niin $p \leq 2n$. $\Big($Huomaa, että $\binom{2n}{n} = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{(n!)^2}.\Big)$ Nyt mikäli $e \geq 2$, niin $p \leq \sqrt{2n}$ (Mikäli e suurenee, niin p pienenee.). Siis luvun $\binom{2n}{n}$ alkutuloesityksessä on enintään $[\sqrt{2n}]$ alkulukua, joiden eksponentti on suurempi kuin 1. Joka tapauksessa $p^e < 2n$ (Lemma 2.3.1). Siis

$$\binom{2n}{n} \leq (2n)^{[\sqrt{2n}]} \cdot \prod_{p \leq \frac{2}{3}n} p.$$

(Huomaa, että $[\sqrt{2n}]$ on alkulukujen lukumäärä.)
Koska luku $\binom{2n}{n}$ on $2n+1$ termeistä suurin lausekkeen $(1+1)^{2n}$ sarjakehitelmässä (Huomaa, että $(1+1)^{2n} = 4^n$.), niin

$$4^n < (2n+1)\binom{2n}{n} \qquad \left(\Rightarrow \frac{4^n}{2n+1} < \binom{2n}{n} \right),$$

joten

$$\frac{4^n}{2n+1} < (2n)^{\sqrt{2n}} \cdot \prod_{p \leq \frac{2}{3}n} p.$$

Nyt Lemman 2.3.3 mukaan

$$\frac{4^n}{2n+1} < (2n)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n},$$

ja koska $2n+1 < 4n^2$ (kun $n \geq 3$), niin

$$\frac{4^n}{4n^2} < 2n^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n}.$$

Seuraavaksi sievennetään tämä epäyhtälö:

$$\begin{aligned} 4^n &< 2n \cdot 2n \cdot 2n^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \\ 4^n &< 2n^{\sqrt{2n}+2} \cdot 4^{\frac{2}{3}n} \\ 4^{\frac{n}{3}} &< 2n^{\sqrt{2n}+2}. \end{aligned}$$

Ottamalla tästä logaritmi saadaan

$$\frac{n \log 4}{3} < (\sqrt{2n}+2) \log (2n).$$

Tämä epäyhtälö ei pidä paikkaansa, kun $n > 512$. Siis lukujen n ja $2n$ välissä on alkuluku, kun $n > 512$. Mutta nyt alkulukujonossa

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 557$$

jokainen luku on pienempi kuin kaksi kertaa sitä edeltävä luku, joten ehdon täyttävä alkuluku on olemassa myös kaikille kokonaisluvuille $n \leq 512$. Siis ehdon täyttävä alkuluku on olemassa kaikille kokonaisluvuille $n \geq 1$. □

Esimerkki 2.3.1 Olkoon $n = 50$. Siis $2n = 100$. Nyt esimerkiksi

$$50 < 61 \leq 100.$$

2.3.2 Alkulukukaksoset

Seuraavaksi tutkitaan alkulukuja, jotka ovat kahden kokonaisluvun päässä toisistaan.

Määritelmä 2.3.1 *Jos p ja $p+2$ ovat alkulukuja, niin niitä kutsutaan **alkulukukaksosiksi**.* [4, s. 199]

Esimerkki 2.3.2 *Pienimmät alkulukukaksoset ovat* $(3,5)$, $(5,7)$, $(11,13)$ *ja* $(17,19)$.

Seuraavaksi esitettävällä lauseella voidaan siis tutkia, ovatko kaksi kokonaislukua, joiden erotus on 2, alkulukuja. Lause ei kuitenkaan sovellu kyseisten alkulukujen etsintään.

Lause 2.3.2 *Kun $n \geq 2$, niin kokonaisluvut n ja $n+2$ ovat alkulukukaksoset, jos ja vain jos*

$$4[(n-1)!+1]+n \equiv 0 \qquad [\text{mod } n(n+2)]. \qquad [4, \text{ s. } 199]$$

Todistus Mikäli kongruenssi on voimassa, niin $n \neq 2$ ja $n \neq 4$, ja edelleen (mod $n(n+2)$) edellyttää, että luvun $4[(n-1)!+1]+n$ täytyy olla aina jaollinen luvulla n. Koska $n \neq 2$, niin tästä seuraa, että luvun $(n-1)!+1$ täytyy aina olla jaollinen luvulla n. Siis

$$(n-1)!+1 \equiv 0 \qquad (\text{mod } n).$$

> **Wilsonin lause:** Jos p on alkuluku, niin $(p-1)! \equiv -1$ (mod p). [4, s. 19]

Nyt Wilsonin lauseen perusteella n on alkuluku.
Edelleen (mod $n(n+2)$) edellyttää myös, että lvun $4[(n-1)!+1]+n$ täytyy olla aina jaollinen luvulla $(n+2)$. Koska

$$\begin{aligned} 4[(n+1)!+1]+n &= 4(n-1)!+4+n \\ &= [4(n-1)!+2]+(n+2), \end{aligned}$$

niin tästä seuraa, että luvun $4(n-1)!+2$ on oltava jaollinen luvulla $(n+2)$. Siis

$$4(n-1)!+2 \equiv 0 \qquad (\text{mod } n+2).$$

Nyt kertomalla tämä luvulla $n(n+1)$ (Kertominen ei muuta jaollisuutta.) saadaan, että

$$\begin{aligned} n(n+1)[4(n-1)!+2] &= (n^2+n)[4(n-1)!+2] \\ &= 4n^2(n-1)!+2n^2+4n(n-1)!+2n \\ &= (4n^2+4n)(n-1)!+2n^2+2n \\ &= 4n(n+1)(n-1)!+2n^2+2n \\ &= 4(n+1)!+2n^2+2n \\ &= 4[(n+1)!+1-1]+2n^2+2n \\ &= 4[(n+1)!+1]+2n^2+2n-4 \\ &= 4[(n+1)!+1]+(n+2)(2n-2). \end{aligned}$$

Siis

$$4[(n+1)!+1]+(n+2)(2n-2) \equiv 0 \qquad (\text{mod } n+2).$$

Koska jälkimmäinen yhteenlaskettava on jaollinen luvulla $(n+2)$, voidaan päätellä, että $4[(n+1)!+1]$ on jaollinen luvulla $(n+2)$.

Siis (Koska $n \neq 2$, voidaan kerroin 4 jättää pois.)

$$\begin{aligned} (n+1)!+1 &\equiv 0 \qquad (\text{mod } n+2) \\ (n+2-1)! &\equiv -1 \qquad (\text{mod } n+2). \end{aligned}$$

Eli Wilsonin lauseen perusteella $(n+2)$ on alkuluku.

Seuraavaksi todistetaan käänteinen puoli. Nyt, koska n ja $(n+2)$ ovat alkulukuja, niin $n \neq 2$ ja (Wilsonin lauseen perusteella)

$$\begin{aligned} (n-1)!+1 &\equiv 0 \qquad (\text{mod } n) \\ (n+1)!+1 &\equiv 0 \qquad (\text{mod } n+2). \end{aligned}$$

Mutta nyt

$$\begin{aligned} n(n+1) &= n^2+2n \\ &= n^2+2n-2+2 \\ &= (n+2)(n-1)+2, \end{aligned}$$

ja edelleen

$$(n+1)! = (n-1)!(n+1)n.$$

Nyt yhdistämällä nämä tulokset saadaan, että

$$\begin{aligned} (n+1)! &= (n-1)![(n+2)(n-1)+2] \\ &= 2(n-1)!+(n-1)(n+2)(n-1)!, \end{aligned}$$

ja edelleen

$$(n+1)!+1 = 2(n-1)!+1+(n-1)(n+2)(n-1)!.$$

Nyt koska $(n+1)! + 1 \equiv 0 \pmod{n+2}$, niin edellisestä saadaan, että

$$\begin{aligned} 2(n-1)! + 1 &= k(n+2) \quad (3) \\ 2[2(n-1)! + 1] &= 2k(n+2), \quad (4) \end{aligned}$$

missä k on kokonaisluku.
Koska $(n-1)! + 1 \equiv 0 \pmod{n}$ ja koska

$$\begin{aligned} 2(n-1)! + 1 &= k(n+2) \\ 2(n-1)! + 1 + 1 &= k(n+2) + 1 \\ 2[(n-1)! + 1] &= (2k+1) + kn, \end{aligned}$$

niin täytyy olla, että

$$2k + 1 \equiv 0 \qquad (\text{mod } n).$$

Saadaan siis, että

$$\begin{aligned} (2k+1)(n+2) &\equiv 0 \qquad [\text{mod } n(n+2)] \\ 2k(n+2) + (n+2) &\equiv 0. \end{aligned}$$

Nyt yhtälön (4) perusteella

$$\begin{aligned} 2[2(n-1)! + 1] + (n+2) &\equiv 0 \qquad [\text{mod } n(n+2)] \\ 4(n-1)! + 2 + (n+2) &\equiv 0 \\ 4[(n-1)! + 1] + n &\equiv 0. \end{aligned}$$

□

Esimerkki 2.3.3 Selvitä, onko luku 29 alkulukukaksosten ensimmäinen jäsen.

Ratkaisu Sovelletaan lausetta 2.3.2 eli tutkitaan, onko

$$4[(n-1)! + 1] + n \equiv 0 \qquad [\text{mod } n(n+2)]$$

voimassa, kun $n = 29$.

Siis

$$\begin{aligned} 4[(29-1)!+1]+29 &\equiv 0 && [\text{mod } 29(29+2)] \\ 4(30488834461171386050150400000 0+1)+29 &\equiv 0 && [\text{mod } 29\cdot 31] \\ 4(3048883446117138605015040000 01)+29 &\equiv 0 && [\text{mod } 899] \\ 12195533784468554420060160000 33 &\equiv 0 && [\text{mod } 899]. \end{aligned}$$

Nyt $121955337844685544200601600000 9 - 0$ on jaollinen luvulla 899, joten kongruenssi pitää paikkansa. Siis luku 29 on alkulukukaksosten ensimmäinen jäsen. (Alkulukupari on siis $(29, 31)$.)

2.3.3 Alkulukujen välit

Alkulukukaksosissa alkuluvut ovat mahdollisimman lähellä toisiaan. On kuitenkin mahdollista löytää peräkkäisiä alkulukuja, jotka ovat mielivaltaisen kaukana toisistaan. Seuraavassa tyydytään kuitenkin tietoon siitä, että sellaisia alkulukuja on yleensä olemassa.

Lause 2.3.3 *Jokaista positiivista kokonaislukua n kohti on olemassa n perättäistä yhdistettyä lukua.*[1, s. 52]

Todistus Todistamiseen riittää käsitellä n:ää perättäistä kokonaislukua

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1).$$

Selvästi kyseessä on n kokonaislukua ja ne ovat peräkkäisiä. Nyt voidaan huomata, että ne ovat myös yhdistettyjä, sillä

$$\begin{aligned} (n+1)!+2 &= (n+1)\cdot n\cdots 3\cdot 2\cdot 1+2 \\ &= 2\cdot[(n+1)\cdot n\cdots 3\cdot 1]+2 \\ &= 2\cdot[(n+1)\cdot n\cdots 3\cdot 1+1], \end{aligned}$$

ja vastaavasti $(n+1)!+3$ ja niin edelleen. □

Siis lauseesta seuraa, että on olemassa kaksi alkulukua siten, että niiden välissä on ääretön määrä yhdistettyjä lukuja.

Esimerkki 2.3.4 Etsi viisi peräkkäistä yhdistettyä lukua.

Ratkaisu Sovelletaan lauseen 2.3.3 todistusta. Valitaan ensimmäiseksi luvuksi $(n+1)!+2$, missä n on nyt 5. Saadaan siis

$$\begin{aligned}(5+1)!+2 &= 6!+2\\ &= 2(6\cdot 5\cdot 4\cdot 3\cdot 1+1)\\ &= 721.\end{aligned}$$

Lauseen 2.3.3 todistuksesta seuraa siis, että 5 perättäistä yhdistettyä lukua ovat $721, 722, 723, 724$ ja 725. Tietysti muitakin viiden peräkkäisen yhdistetyn luvun jonoja on olemassa.

2.3.4 Alkulukujen etäisyydet

Tässä kappaleessa käsitellään alkulukupareja, joissa kumpikin alkuluku on tietyllä etäisyydellä halutusta positiivisesta kokonaisluvusta. Mielenkiintoiseksi aiheen tekee se, että mikäli voitaisiin todistaa, että Lauseessa 2.3.6 esitetty kongruenssi pitää paikkansa kaikilla positiivisilla kokonaisluvuilla n, niin Goldbachin otaksuma tulisi todistetuksi.

Aloitetaan kahdella lauseella, joita tarvitaan myöhemmin Lauseen 2.3.6 todistuksessa.

Lause 2.3.4 (Kiinalainen jäännöslause) *Olkoon $m_1, m_2, \ldots, m_r$ pareittain suhteellisia alukulukuja ja positiivisia kokonaislukuja. Silloin kongruenssiryhmällä*

$$\begin{aligned}x &\equiv a_1 \pmod{m_1},\\ x &\equiv a_2 \pmod{m_2},\\ &\vdots\\ x &\equiv a_r \pmod{m_r},\end{aligned}$$

on yksikäsitteinen ratkaisu modulo $M = m_1 m_2 \cdots m_r$. [1, s. 144]

Todistus Sivuutetaan.

Lause 2.3.5 *Jos n on yhdistetty luku, $n \geq 6$, niin*

$$(n-1)! \equiv 0 \pmod{n}.$$

Todistus Lauseen kongruenssi tarkoittaa sitä, että kertoma $(n-1)!$ on jaollinen luvulla n. Aritmetiikan peruslauseen (ks. 7) perusteella riittää tarkastella kahta eri tapausta.
1. $n = p^k$, missä $k \geq 2$. (Oletuksesta $n \geq 6$ seuraa, että $p^k \neq 4$.)
2. $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, missä $p_i \neq p_j$, aina kun $i \neq j$ ja $i, j \leq r$. Myös $a_l \geq 1$, kun $l = 1, 2, \ldots, r$ ja $r \geq 2$.
Todistetaan tapaus 1.
Alkuluku p on yksi kertoman $(n-1)!$ tekijöistä, koska $k \geq 2$. Myös tulo $(p-1)p^{k-1}$ on yksi kertoman $(n-1)!$ tekijöistä, sillä $(p-1)p^{k-1} < p^k - 1$. Ainut tapaus, jolloin $(p-1)p^{k-1}$ voi olla yhtä suuri, kuin p on silloin, kun $k = 2$ ja $(p-1) = 1$. Siis ainut tapaus on $2^2 = 4$. Lauseessa oletetaan, että luvun n tulee olla suurempi kuin 6, joten voimme jättää huomioimatta luvun n arvon 4. Nyt koska sekä luku $(p-1)p^{k-1}$ että luku p kuuluvat kertomaan $(n-1)!$, niin yhdeksi kertoman tekijäksi voidaan erottaa p^k. Siis $n \mid (n-1)!$.
Todistetaan tapaus 2.
Koska jokaisen kokonaisluvun alkutuloesitys on yksikäsitteinen, niin jokainen luku $p_i^{a_i} \neq p_j^{a_j}$, kun $i \neq j$. Edelleen jokainen luku $p_q^{a_q} < p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} - 1$, kun $q \in \{1, 2, \ldots, r\}$. Nyt siis kaikki luvut $p_1^{a_1}, p_2^{a_2}, \ldots, p_r^{a_r}$ ovat kertoman $(n-1)!$ tekijöitä. Siis $n \mid (n-1)!$. □

Nyt voidaan todistaa Lause 2.3.6.

Lause 2.3.6 *Kun $n \geq 4$ ja $0 < k \leq n-3$, niin kokonaisluvut $n-k$ ja $n+k$ ovat kumpikin alkulukuja jos ja vain jos kongruenssi*

$$[(n+k)-1]! + (n+k)^{n-k-1}[(n-k)-1]! \equiv -1 \qquad [\text{mod } (n-k)(n+k)]$$

on ratkeava.

Todistus Oletetaan, että luvut $n-k$ ja $n+k$ ovat alkulukuja. Nyt Wilsonin lauseen (ks. 18) perusteella ne ovat alkulukuja jos ja vain jos seuraavat kongruenssit pitävät paikkansa:

$$\begin{aligned} [(n-k)-1]! &\equiv -1 \qquad (\text{mod } n-k), \\ [(n+k)-1]! &\equiv -1 \qquad (\text{mod } n+k). \end{aligned}$$

Nyt kiinalaisen jäännöslauseen (ks. 22) mukaan tällä kongruenssiparilla on olemassa yksikäsitteinen ratkaisu modulo $(n-k)(n+k)$. Tässä tapauksessa muuttujan x arvo on tunnettu ja se on -1.

Ratkaisu: $M = (n-k)(n+k)$, $M_1 = (n+k)$ ja $M_2 = (n-k)$. Ratkaistaan y_1 ja y_2:

$$\begin{aligned} (n+k)y_1 &\equiv 1 \pmod{n-k}, \\ (n-k)y_2 &\equiv 1 \pmod{n+k}. \end{aligned}$$

Siis

$$\begin{aligned} y_1 &\equiv (n+k)^{n-k-2} \pmod{n-k}, \\ y_2 &\equiv (n-k)^{n+k-2} \pmod{n+k}. \end{aligned}$$

Nyt

$$-1 \equiv (n-k)(n-k)^{n+k-2}[(n+k)-1]! + (n+k)(n+k)^{n-k-2}[(n-k)-1]! \pmod{(n-k)(n+k)}.$$

Eli

$$-1 \equiv (n-k)^{n+k-1}[(n+k)-1]! + (n+k)^{n-k-1}[(n-k)-1]! \pmod{(n-k)(n+k)}.$$

Merkitään tätä kongruenssia symbolilla (a).

Seuraavaksi osoitetaan, että kongruenssi

$$(n-k)^{n+k-1}[(n+k)-1]! \equiv [(n+k)-1]! \pmod{(n-k)(n+k)}$$

pitää paikkansa. Tämä on helpoin osoittaa tarkastelemalla erotuksen

$$(n-k)^{n+k-1}[(n+k)-1]! - [(n+k)-1]!$$

jaollisuutta luvuilla $n-k$ ja $n+k$. Nyt erotus voidaan kirjoitaa muodossa

$$[(n-k)^{n+k-1} - 1][(n+k)-1]!.$$

Fermat'n pieni lause Jos p on alkuluku ja $p \not| a$, niin

$$a^{p-1} \equiv 1 \pmod{p}.$$

[4, s. 16]

Nyt Fermat'n pienen lauseen perusteella tulon vasemmanpuoleinen tekijä on jaollinen luvulla $n+k$, sillä se on alkuluku ja $(n-k, n+k) = 1$. Edelleen tulon oikeanpuoleinen tekijä on jaollinen luvulla $n-k$, sillä se on yksi kertoman tekijöistä.
Kongruenssi (a) voidaan kirjoittaa siis seuraavaan muotoon:

$$[(n+k)-1]! + (n+k)^{n-k-1}[(n-k)-1]! \equiv -1 \qquad [\text{mod } (n-k)(n+k)].$$

Seuraavaksi todistetaan sama toiseen suuntaan:
Oletetaan, että

$$[(n+k)-1]! + (n+k)^{n-k-1}[(n-k)-1]! \equiv -1 \qquad [\text{mod } (n-k)(n+k)].$$

Merkitään tätä kongruenssia symbolilla (c). Osoitetaan ensin, että luvun $n+k$ täytyy olla alkuluku. Voidaan helposti huomata, että tulo $(n+k)^{n-k-1}[(n-k)-1]!$ on kongruentti nollan kanssa modulo $n+k$, joten se voidaan poistaa kongruenssista (c), joka saadaan seuraavaan muotoon:

$$[(n+k)-1]! \equiv -1 \qquad [\text{mod } (n+k)].$$

Nyt Wlsonin lauseen perusteella tämä kongruenssi on ratkeava jos ja vain jos $n+k$ on alkuluku.
Seuraavaksi osoitetaan, että myös luvun $n-k$ tule olla alkuluku. Jälleen on helppo nähdä, että kertoma $[(n+k)-1]!$ on kongruentti nollan kanssa modulo $n-k$, joten kongruenssi (c) saadaan muotoon

$$(n+k)^{n-k-1}[(n-k)-1]! \equiv -1 \qquad [\text{mod } (n-k)].$$

Nyt lisäämällä ja vähentämällä lukuun $n+k$ luku k, saadaan kongruenssi muotoon

$$(n-k+2k)^{n-k-1}[(n-k)-1]! \equiv -1 \qquad [\text{mod } (n-k)].$$

Ja edelleen muotoon

$$[(n-k)^{n-k-1} + \cdots + (2k)^{n-k-1}][(n-k)-1]! \equiv -1 \qquad [\text{mod } (n-k)].$$

Nyt kertomalla tämä tulo auki saadaan kongruenssi muotoon

$$\begin{aligned}(n-k)^{n-k-1}[(n-k)-1]! \;&+\; \cdots \\ &+\; (2k)^{n-k-1}[(n-k)-1]! \equiv -1 \;[\text{mod } (n-k)].\end{aligned}$$

Tiedetään, että summattavista kaikki muut paitsi $(2k)^{n-k-1}[(n-k)-1]!$ ovat kongruentteja nollan kanssa modulo $n-k$, joten kongruenssi saadaan muotoon

$$(2k)^{n-k-1}[(n-k)-1]! \equiv -1 \ [\text{mod } (n-k)].$$

Nyt Lauseen 2.3.5 perusteella jos luku $n-k$ on yhdistetty ja ≥ 6, niin $[(n-k)-1] \equiv 0$. Siis jos luku $n-k$ on yhdistetty, niin $0 \equiv -1 \bmod n-k$. Tämä ei voi koskaan pitää paikkaansa. Erikseen täytyy vielä tarkastella tapaus $n-k=4$, koska lause 2.3.5 ei kata sitä. Merkitään $n-k=4$. Saadaan, että

$$\begin{aligned}
(2k)^{4-1}(4-1)! &\equiv -1 \quad (\text{mod } n-k) \\
(2k)^3 3! &\equiv -1 \quad (\text{mod } n-k) \\
2^3 k^3 6 &\equiv -1 \quad (\text{mod } n-k) \\
48k^3 &\equiv -1 \quad (\text{mod } n-k)
\end{aligned}$$

Nyt koska luku $48k^3$ on aina jaollinen luvulla 4, niin luku $48k^3+1$ ei voi koskaan olla jaollinen luvulla 4. (Kaksi peräkkäistä kokonaislukua ei koskaan ole jaollinen samalla kokonaisluvulla > 1.)

Luku $n-k$ ei siis voi olla yhdistetty, joten sen täytyy olla alkuluku. $\square$

2.4 Alkulukujen tuottaminen

Tässä kappaleessa on tarkoitus tutkia hieman, minkä muotoisina alkuluvut positiivisten kokonaislukujen seassa esiintyvät ja onko mahdollista löytää keinoa, jolla ne voitaisiin erottaa, ilman jokaisen luvun läpikäymistä erikseen.

2.4.1 Alkulukujen muodot

Tutkittaessa alkulukujen muotoja on syytä aloittaa jakoalgoritmista, jonka perusteella jokainen positiivinen kokonaisluku voidaan yksikäsitteisesti ilmaista jossain seuraavista muodoista

$$4n \qquad 4n+1 \qquad 4n+2 \qquad 4n+3,$$

missä $n \geq 0$. Selvästi kokonaisluvut $4n$ ja $4n+2 = 2(2n+1)$ ovat kumpikin parillisia. Siksi kaikki parittomat kokonaisluvut jakautuvat kahteen sarjaan, ensimmäinen sisältää kaikki muotoa $4n+1$ olevat ja toinen muotoa $4n+3$ olevat kokonaisluvut.

Kysymys kuuluukin, miten nämä alkulukujen kaksi eri tyyppiä jakaantuvat positiivisten kokonaislukujen joukkoon. Aluksi on syytä katsoa, kuinka muutamat ensimmäiset parittomat alkuluvut jakaantuvat näihin sarjoihin. Ylärivillä ovat muotoa $4n+3$ olevat ja alarivillä ovat muotoa $4n+1$ olevat alkuluvut suuruusjärjestyksessä:

3	7	11	19	23	31	43	47	59	67	71	79	83
5	13	17	29	37	41	53	61	73	89.			

Tässä vaiheessa voisi hyvin ajatella, että muotoa $4n+3$ olevia alkulukuja on runsaammin kuin muotoa $4n+1$ olevia. Jotta saisimme enemmän tietoa asiasta, otamme käyttöön funktion $\pi_{a,b}(x)$ (vertaa alkulukuteoria s. 12), joka laskee muotoa $p = an+b$ olevat alkuluvut, jotka eivät ylitä lukua x. Katsomalla esimerkiksi yllä olevaa taulukointia voimme huomata, että $\pi_{4,1}(89) = 10$ ja $\pi_{4,3}(89) = 13$.

Tsebysev huomautti kuuluisassa kirjeessä vuonna 1853, että $\pi_{4,1}(x) \leq \pi_{4,3}(x)$ pienillä luvun x arvoilla. Hän antoi epäsuorasti myös ymmärtää, että hänellä oli todistus siitä, että epäyhtälö pätee aina. Vuona 1914, J.E. Littlewood

osoitti, että epäyhtälö ei pidä paikkaansa äärettömän monella luvun x arvolla, mutta hänen metodinsa ei antanut mitään viitteitä siitä, millä luvun x arvolla näin ensimmäisen kerran tapahtuisi. Se osoittautuikin hyvin vaikeaksi löytää. Vasta vuonna 1957 tietokoneiden avulla pystyttiin osoittamaan, että $x = 26861$ on pienin alkuluku, jolla $\pi_{4,1}(x) > \pi_{4,3}(x)$; $\pi_{4,1}(x) = 1473$ ja $\pi_{4,3}(x) = 1472$. Tämä on yksittäinen tapaus, sillä seuraava alkuluku, jolla käänteisyys ilmaantuu, on $x = 616841$. Huomattavan arvoista on se, että $\pi_{4,1}(x) > \pi_{4,3}(x)$ 410 miljoonalla perättäisellä kokonaisluvulla x, jossakin lukujen 18540000000 ja 18950000000 välissä.

Muotoa $3n \pm 1$ olevien alkulukujen käyttäytyminen antoi jo enemmän laskennallista haastetta: epäyhtälö $\pi_{3,1}(x) \leq \pi_{3,2}(x)$ pitää paikkansa kaikilla luvuilla x aina lukuun 608981813029 asti.

Tämä antaakin meille mieluisan mahdollisuuden tehdä uudestaan Eukleideen metodin esitys, jolla hän todisti alkulukujen äärettömyyden (ks. 10). Hänen argumenttinsa pieni muokkaus paljastaa, että on olemassa ääretön määrä muotoa $4n + 3$ olevia alkulukuja. Lähestymme todistusta yksinkertaisen lemman avulla.

Lemma 2.4.1 *Kahden tai useamman muotoa $4n + 1$ olevan kokonaisluvun tulo on edelleen muotoa $4n + 1$.*

Todistus On riittävää tarkastella vain kahden kokonaisluvun tuloa. Merkitään, että $k = 4n + 1$ ja $k' = 4m + 1$. Kertomalla nämä yhteen saamme

$$\begin{aligned} kk' &= (4n + 1)(4m + 1) \\ &= 16nm + 4n + 4m + 1 \\ &= 4(4mn + n + m) + 1, \end{aligned}$$

mikä oli haluttu muoto. □

Tästä pääsemmekin lauseeseen 2.4.1.

Lause 2.4.1 *Muotoa $4n + 3$ olevia alkulukuja on ääretön määrä.*

Todistus Ristiriitaa ennakoiden oletetaan, että muotoa $4n + 3$ olevia alkulukuja on äärellinen määrä; merkitään niitä $q_1, q_2, \ldots, q_s$. Merkitään, että

positiivinen kokonaisluku

$$N = 4q_1 \cdot q_2 \cdots q_s - 1 = 4(q_1 \cdot q_2 \cdots q_s - 1) + 3,$$

ja olkoon $r_1 r_2 \cdots r_t$ sen alkutuloesitys. Koska N on pariton kokonaisluku, niin $r_k \neq 2$, kaikilla luvun k arvoilla, ja siksi jokainen r_k on joko muotoa $4n+1$ tai $4n+3$ oleva alkuluku. Lemma 2.4.1 sanoo, että jokainen muotoa $4n+1$ olevien alkulukujen tulo on edelleen muotoa $4n+1$. Nyt siis, koska N on selvästi muotoa $4n+3$, täytyy sen alkutuloesityksen sisältää ainakin yksi r_i, joka on muotoa $4n+3$. Mutta nyt r_i ei voi olla yksi alkuluvuista $q_1, q_2, \ldots, q_s$, sillä se johtaisi ristiriitaan $r_i \mid 1$. Tämä on helppo todistaa:

> Nyt siis r_i jakaa luvun N. Jos r_i olisi yksi muotoa $4n+3$ olevista alkuluvuista $q_1, q_2, \ldots, q_s$, niin
>
> $$\frac{N}{r_i} = \frac{4q_1 \cdot q_2 \cdots q_s - 1}{r_i} = \frac{4q_1 \cdot q_2 \cdots q_s}{r_i} - \frac{1}{r_i},$$
>
> eli r_i jakaisi luvun 1.

Ainoa päätelmä onkin, että muotoa $4n+3$ olevia alkulukuja täytyy olla ääretön määrä. □

[1, s. 54–56]

2.4.2 Alkulukuja sarjasta

Nyt kun olemme juuri voineet huomata, että muotoa $4n+3$ olevia alkulukuja on ääretön määrä, niin on järjellistä kysyä, onko muotoa $4n+1$ olevia alkulukuja myös ääretön määrä. Tämä vastaus on hyvin todennäköisesti myönteinen, mutta ennen kuin se voidaan todistaa, on meidän odotettava tarvittavan mateaattisen koneiston kehittymistä. Molemmat näistä tuloksista ovat P.G.L Dirichlet'n merkittävän teorian, alkuluvut aritmeettisissa sarjoissa (julkaistu 1837), erikoistapauksia. Todistus on aivan liian vaikea esitettäväksi tässä, joten täytyy tyytyä pelkkään toteamukseen.

Lause 2.4.2 Dirichlet'n lause: *Mikäli a ja b ovat molemmat positiivisia kokonaislukuja ja* $\text{syt}(a,b) = 1$*, niin aritmeettinen sarja*

$$a, a+b, a+2b, a+3b, \ldots$$

sisältää äärettömän monta alkulukua.

Dirichlet'n lause kertoo meille esimerkiksi sen, että on olemassa äärettömän monta alkulukua, jotka päättyvät numeroihin 999, kuten 1999, 1000999, ... Nämä saadaan aritmeettisesta sarjasta, jonka määrittää $1000n + 999$, missä $\text{syt}(1000, 999) = 1$.

Ei ole kuitenkaan olemassa aritmeettista sarjaa $a, a + b, a + 2b, \ldots$, joka sisältäisi ainoastaan alkulukuja. Tämä on helposti todistettavissa. Oletetaan, että sarjan jäsen $a + nb$ on $= p$, p on alkuluku. Nyt jos $n_k = n + kp$, kun $k = 1, 2, 3, \ldots$,niin silloin sarjan n_k jäsen on

$$a + n_k b = a + (n + kp)b = (a + nb) + kpb = p + kpb = p(1 + kb).$$

Saadaan siis, että n_k:s termi $a + n_k b$ on jaollinen luvulla p. Tästä seuraa, että sarjan täytyy sisältää äärettömän monta yhdistettyä lukua.

Vanha, mutta edelleen ratkaisematon, kysymys on se, onko olemassa mielivaltaisen pitkää, mutta äärellistä sarjaa, joka sisältäisi ainoastaan alkulukuja (ei välttämättä kuitenkaan peräkkäisiä). Pisin sarja, mikä tähän päivään mennessä on löydetty, koostuu 22 alkuluvusta:

$$11410337850553 + 4609098694200n, \qquad 0 \leq n \leq 21.$$

Termien välisen erotuksen eli differenssin alkutuloesitys on

$$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 1033,$$

joka on jaollinen luvulla 9699690 ja on alle 22 alkuluvun tulo. Tästä pääs-täänkin lauseeseen 2.4.3.

Lause 2.4.3 *Jos kaikki aritmeettisen sarjan*

$$p, p + d, \ldots, p + (n - 1)d \qquad n > 2$$

termit ovat alkulukuja, niin differenssi d on jaollinen kaikilla alkuluvuilla $q < n$.

Todistus Oletetaan, että alkuluku q on $< n$, ja tehdään vastaoletus $q \not| d$. Väitetään, että q ensimmäistä sarjan

$$p, p + d, p + 2d, \ldots, p + (q - 1)d \tag{5}$$

termiä saavat aikaan eri jakojäännökset, kun ne jaetaan luvulla q. Muuten täytyisi olla kaksi kokonaislukua j ja k, $0 \leq j < k \leq q-1$, siten, että termit $p+jd$ ja $p+kd$ saisivat aikaan saman jakojäännöksen jaettaessa luvulla q. Tästä seuraisi, että q jakaisi niiden erotuksen $(p+kd)-(p+jd) = (k-j)d$. Mutta nyt koska q ei jakanut lukua d eli $\text{syt}(q,d) = 1$, niin Eukleideen lemmasta (ks. 5) seuraa, että $q \mid k-j$, mikä on mahdotonta epäyhtälön $k-j \leq q-1$ suhteen.

Koska q eri, yhtälöstä (5) tuotettua, jakojäännöstä on saatu q kokonaisluvusta $0, 1, \ldots, q-1$, niin yhden noista jakojäännöksistä täytyy olla nolla (vain kun $q \not| d$). Seuraa siis, että $q \mid p+td$ jollain t:llä, $0 \leq t \leq q-1$. Epäyhtälöstä $q < n \leq p \leq p+td$ seuraa, että luvun $p+td$ täytyy olla yhdistetty. (Jos p olisi pienempi kuin n, niin yksi sarjan termeistä olisi $p+pd = p(1+d)$.) Nyt olemme siis tulleet ristiriitaan, koska sarjan kaikki termit eivät voi olla alkulukuja. Täytyy siis olla, että $q \mid d$. □

On otaksuttu, että olisi olemassa äärellisen (mutta muutoin mielivaltaisen) pituinen aritmeettinen sarja, joka muodostuisi peräkkäisistä alkuluvuista. Esimerkkinä sellaisista sarjoista, jotka sisältävät 3 ja 4 alkulukua, ovat 47, 53, 59, ja 251, 257, 263, 269 (näissä kummassakin alkulukujen erotus on siis 6).

Vähän aikaa sitten löydettiin 10 peräkkäisen alkuluvun pituinen sarja, jossa jokainen termi ylittää edeltäjänsä vain 210:llä; pienimmässä näistä alkuluvuista on 93 numeroa. 11 termin pituisen aritmeettisen sarjan löytäminen on todennäköisesti ulottumattomissa vielä jonkin aikaa. Mikäli rajoitus siitä, että alkulukujen täytyy olla peräkkäisiä, poistetaan, niin 11 termin pituisia aritmeettisia sarjoja voidaan löytää jo paljon helpommin. Esimerkkinä yhtälö

$$110437 + 13860n, \qquad 0 \leq n \leq 10.$$

[1, s. 56–57]

2.4.3 Alkulukuja funktiosta

Täydellisyydestä kiinnostuneena on hyvä tutkia myös toista kuuluisaa ongelmaa, joka on pystynyt vastustamaan kaikkein määrätietoisimpiakin yrityksiä ratkaista se. Jo vuosisatoja matemaatikot ovat yrittäneet löytää yksinkertaista kaavaa, joka tuottaisi kaikki alkuluvut, tai, epäonnistuttuaan siinä, kaa-

vaa, joka tuottaisi pelkästään alkulukuja. Ensi silmäykseltä toivomus näyttää hyvin vaatimattomalta: löytää funktio $f(n)$, jonka lähtöjoukko on vaikka ei-negatiiviset kokonaisluvut ja jonka maalijoukko jokin kaikkien alkulukujen ääretön osajoukko. Monia vuosia uskottiin hyvin laajalti, että toisen asteen polynomi

$$f(n) = n^2 + n + 41$$

tuottaisi vain alkulukuja. Euler osoitti sen kuitenkin vääräksi vuonna 1772. Kuten seuraava taulukko todistaa, väitös pitää paikkansa, kun $n = 0, 1, 2, \ldots, 39$.

n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	14	251	28	853
1	43	15	281	29	911
2	47	16	313	30	971
3	53	17	347	31	1033
4	61	18	383	32	1097
5	71	19	421	33	1163
6	83	20	461	34	1231
7	97	21	503	35	1301
8	113	22	547	36	1373
9	131	23	593	37	1447
10	151	24	641	38	1523
11	173	25	691	39	1601
12	197	26	743		
13	223	27	797		

Kuitenkin tämä provosoiva otaksuma ei enää pidä paikkaansa luvun n arvoilla 40 ja 41, jolloin kummankin tekijä on 41. Nimittäin

$$f(40) = 40^2 + 40 + 41 = 40 \cdot 41 + 41 = 41^2$$

ja

$$f(41) = 41^2 + 41 + 41 = 41 \cdot 41 + 42 = 41 \cdot 43.$$

Seuraava arvo $f(42) = 1847$ on kuitenkin taas alkuluku. Itse asiassa 100 ensimmäisellä kokonaisluvulla tämä niin kutsuttu Eulerin polynomi tuottaa 86 alkulukua. Vaikka se alkaa varsin hyvin tuottaa alkulukuja, on olemassa kuitenkin muita toisenasteen polynomeja, kuten

$$g(n) = n^2 + n + 27941,$$

joka alkaa tuottaa alkulukuja paremmin kuin $f(n)$, kun luvun n arvot kasvavat. Esimerkiksi, kun n on välillä $0 \leq n \leq 10^6$, niin $g(n)$ tuottaa 286129 eri alkulukua, kun vastaavasti sen kuuluisa kilpailija $f(n)$ tuottaa 261081 eri alkulukua.

On kuitenkin osoitettu, että mikään muotoa n^2+n+q oleva polynomi, missä q on alkuluku, ei pysty parempaan kuin Eulerin polynomi, kun puhutaan alkulukujen tuottamisesta peräkkäisillä luvun n arvoilla. Tosiaankin, lähes tähän päivään asti ei ole ollut tiedossa minkäänlaista toisenasteen polynomia, joka tuottaisi enemmän kuin 40 alkulukua peräkkäin. Polynomi

$$h(n) = 103n^2 - 3945n + 34381,$$

joka löydettiin 1988, tuottaa 43 erilaista alkulukua, kun $n = 0, 1, 2, \ldots, 42$. Tämänhetkinen ennätyksenhaltija tässä sarjassa,

$$k(n) = 36n^2 - 810n + 2753,$$

on tuloksiltaan vielä hieman parempi, koska se tuottaa alkuluvun 45 peräkkäisellä luvun n arvolla.

Ei ole mikään vahinko, että edellä mainitut funktiot eivät ole vain alkulukuja tuottavia. On nimittäin helppo todistaa, että ei ole olemassa epäjatkuvaa kokonaislukukertoimista polynomia $f(n)$, joka tuottaisi vain alkulukuja kokonaisluvuilla n. Todistetaan tämä seuraavaksi. Oletetaan, että tällainen polynomi $f(n)$ olisi olemassa, ja väitetään niin, kunnes pääsemme ristiriitaan. Olkoon

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0,$$

missä kaikki kertoimet $a_0, a_1, \ldots, a_k$ ovat kokonaislukuja ja $a_k \neq 0$. Sovitulla muuttujan n arvolla (olkoon $n = n_0$) $p = f(n_0)$ on alkuluku (koska

$f(n)$ on alkuluku kaikilla muuttujan n arvoilla). Nyt, jos t on mikä tahansa kokonaisluku, niin käymme läpi seuraavan yhtälön:

$$\begin{aligned} f(n_0 + tp) &= a_k(n_0 + tp)^k + \cdots + a_1(n_0 + tp) + a_0 && (6)\\ &= (a_k n_0^k + \cdots + a_1 n_0 + a_0) + pQ(t) && (7)\\ &= f(n_0) + pQ(t) && (8)\\ &= p + pQ(t) && (9)\\ &= p(1 + Q(t)), && (10) \end{aligned}$$

missä $Q(t)$ on muuttujan t polynomi, jolla on kokonaislukukertoimet.

(6)→(7): Kun yhtälön (6) oikeanpuoleinen lauseke kerrotaan auki, ainoat termit, jotka eivät sisällä lukua p, ovat muotoa $a_i n_0^i$. Tämä nähdään suoraan Newtonin binomikaavasta

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Esimerkiksi

$$\begin{aligned} a_k(n_0 + tp)^k &= a_k\left[n_0^k + \binom{k}{1} n_0^{k-1} tp + \cdots + (tp)^k\right]\\ &= a_k n_0^k + a_k k n_0^{k-1} tp + \cdots + a_k (tp)^k\\ &= a_k n_o^k + p(a_k k n_0^{k-1} t + \cdots + a_k t^k p^{k-1}), \end{aligned}$$

missä termeistä, jotka eivät sisällä lukua p muodostuu $a_k n_0^k$. Näistä ei lukua p sisältävistä termeistä muodostuu lausekkeen (7) summan vasen summattava. Kaikki loput termit sisältävät siis luvun p, joten niistä voidaan ottaa se yhteiseksi tekijäksi. Tämän tulon toista tekijää on merkitty symbolilla $Q(t)$.

Tästä laskutoimituksesta voidaan todeta, että $p \mid f(n_0 + tp)$. Koska oletuksesta johtuen $f(n)$ voi tuottaa vain alkulukuja, niin $f(n_0 + tp) = p$ millä tahansa kokonaisluvulla t (eli funktion f tulisi saada alkuluku p äärettömän monta kertaa). Koska k-asteinen polynomi voi saada saman arvon vain k kertaa, olemme päässeet haluttuun ristiriitaan.

Viime vuodet ovat ovat olleet menestyksellisiä alkulukuja tuottavien funktioiden etsinnässä. W.H. Mills todisti vuonna 1945, että on olemassa sellainen positiivinen reaaliluku r, että funktio $f(n) = [r^{3^n}]$ tuottaa alkulukuja, kun $n = 1, 2, 3, \ldots$ (sulut viittavat katto-funktioon). Tarpeetonta on varmaan sanoa, että tämä on vain olemassa oleva teoria ja että muuttujan r todellisesta arvosta ei tiedetä mitään. Millsin funktio ei tuota kaikkia alkulukuja.[1, s. 57–59]

3 Goldbachin otaksuma

Tässä luvussa on tarkoitus tutustua Goldbachin otaksuman historiaan ja otaksumaan yleensä. Otaksuma on edelleen todistamatta, joten luonnollisesti tässäkään työssä ei pätevää todistusta tulla esittämään.

> **Goldbachin otaksuma:** Jokainen parillinen kokonaisluku ≥ 4 voidaan esittää kahden alkuluvun summana.

3.1 Otaksuman historia

Esittelemme Goldbachin otaksuman varhaista historiaa luettelomaisesti Dicksonin kirjan [2, s. 421–424] mukaisesti. Tapahtumat sijoittuvat 1700-luvun alkupuolelta 1900-luvun alkupuolelle.

Christian Goldbach (1690-1764) otaksui, että jokainen luku N, joka on kahden alkuluvun summa, on niin monen alkuluvun summa, mukaan lukien luku 1, kuin vain haluaa (lukuun N asti) ja että jokainen luku > 2 on kolmen alkuluvun summa.

L. Euler huomautti, että ensimmäinen otaksuma voidaan vahvistaa havainnosta, että jokainen parillinen luku on kahden alkuluvun summa. Otaksumansa Goldbach kertoi Eulerille kirjeessään vuonna 1742. Euler uskoi myös toisen otaksuman pitävän paikkansa, kuitenkaan hän ei sitä todistanut. Siitä seuraisi, että jos n on parillinen, niin $n, n-2, n-4, \ldots$ ovat kahden alkuluvun summia ja edelleen n on $3, 4, 5, \ldots$ alkuluvun summa.

R. Descartes totesi, että jokainen parillinen luku on 1:n, 2:n tai 3:n alkuluvun summa.

E. Waring uskoi Goldbachin otaksuman olevan oikein ja lisäsi, että jokainen pariton luku on joko alkuluku tai kolmen alkuluvun summa.

L. Euler totesi, ilman todistusta, että jokainen muotoa $4n + 2$ oleva luku on kahden muotoa $4n + 1$ olevan alkuluvun summa, ja todisti tämän jokaiselle luvulle $4n + 2 \leq 110$.

A. Desboves todisti, että jokainen parillinen luku lukujen 2 ja 10000 välissä on kahden alkuluvun summa vähintään kahdella eri tavalla. Jos parillinen

luku on kahden parittoman luvun summa, niin se on yhtäaikaisesti kahden muotoa $4n+1$ olevan alkuluvun summa ja kahden muotoa $4n-1$ olevan alkuluvun summa.

J. J. Sylvester totesi, että määrä, jolla suuri parillinen luku n voidaan esittää kahden alkuluvun summana, on suunnilleen alkulukujen $< n$ lukumäärän neliön suhde lukuun n, ja siksi osamäärä, n jaettuna luvun n luonnollisen logaritmin neliöllä, on äärellinen.

F. J. E. Lionnet merkitsi muuttujalla x määrää, kuinka monella eri tavalla $2a$ voitiin ilmaista kahden parittoman alkuluvun summana, muuttujalla y määrää, kuinka monella eri tavalla $2a$ voitiin ilmaista kahden, toisistaan eriävän, parittoman yhdistetyn luvun summana, muuttujalla z parittomien alkulukujen $< 2a$ määrää ja muuttujalla q suurinta kokonaislukua $\leq a/2$. Hän todisti, että $q + x = y + z$ ja väitti olevan hyvin todennäköistä, että jollain luvun $2a$ arvoilla $q = y + z$, missä $x = 0$.

Esimerkki 3.1.1 Lasketaan, pitääkö yhtälö $q + x = y + z$ paikkansa, kun $2a = 20$.

Ratkaisu Ratkaistaan x, y, z ja q:

$$\begin{aligned} x &= 2 && (3+17, 7+13) \\ y &= 0 && \\ z &= 7 && (3,5,7,11,13,17,19) \\ q &= 5 && (a = 10 \rightarrow a/2 = 5). \end{aligned}$$

Nyt siis

$$\begin{aligned} q + x &= y + z \\ 5 + 2 &= 0 + 7 \\ 7 &= 7, \end{aligned}$$

siis yhtälö $q + x = y + z$ pitää paikansa, kun $2a = 20$.

N.V. Bougaief huomautti, että jos $M(n)$ merkitsee määrää, kuinka monella

eri tavalla n voidaan esittää kahden alkuluvun summana, ja jos θ_i merkitsee i alkulukua > 1, niin

$$\sum_i (n - 3\theta_i) M(n - \theta_i) = 0.$$

Esimerkki 3.1.2 Lasketaan, pitääkö yhtälö $\sum_i (n-3\theta_i)M(n-\theta_i) = 0$ paikkansa, kun $n = 10$.

Ratkaisu Lasketaan summattavat:

$$\begin{aligned}
i = 1: &\quad (10 - 3 \cdot 2)M(10 - 2) = \quad 4 \cdot 1 = 4 \\
i = 2: &\quad (10 - 3 \cdot 3)M(10 - 3) = \quad 1 \cdot 1 = 1 \\
i = 3: &\quad (10 - 3 \cdot 5)M(10 - 5) = \quad -5 \cdot 1 = -5 \\
i = 4: &\quad (10 - 3 \cdot 7)M(10 - 7) = \quad -11 \cdot 0 = 0.
\end{aligned}$$

Enempää ei tarvitse laskea, sillä tulon tekijä $M(n-\theta_i)$ on suuremmilla indeksin i arvoilla 0, joten tulo $(n - 3\theta_i)M(n - \theta_i)$ on nolla. Näin ollen summaksi saadaan

$$4 + 1 + (-5) + 0 = 0.$$

Siis yhtälö $\sum_i (n - 3\theta_i)M(n - \theta_i) = 0$ pitää paikkansa, kun $n = 10$.

G. Cantor vahvisti Goldbachin otaksuman lukuun 1000 asti. Hänen taulukkonsa antaa jokaisen parillisen luvun, < 1000, kaikkien mahdollisten kahden alkuluvun summien määrän ja listaa pienemmän alkuluvun.

V. Audry vahvisti otaksuman luvusta 1002 lukuun 2000.

R. Haussner varmisti otaksuman lukuun 10000 asti ja toi julki tulokset, joita hänen taulukoidensa tutkinta tarkkaili lukuun 5000 asti. Taulukoita on kolme. Ensimmäinen taulukko antaa määrän v, jolla jokainen parillinen luku n, lukuun 3000 asti, voidaan jakaa kahden alkuluvun summaksi $x + y$, ja luvun x arvot ($x \leq y$), kuten Cantorin taulukko. Toinen taulukko antaa määrän v jokaiselle luvulle n siten, että $2 < n < 2000$; tämä taulukko ja pidemmälle menneet laskennat mahdollistivat hänen toteamuksensa siitä, että Goldbachin teoria on totta, kun $n < 10000$. Olkoon $P(2n + 1)$ niiden parittomien

alkulukujen määrä, jotka ovat $\leq 2n+1$, ja olkoon

$$\xi(2p+1) = P(2p+1) - 2P(2p-1) + P(2p-3), \tag{11}$$

$P(-1) = P(-3) = 0$. Nyt määrä, jolla $2n$ voidaan jakaa kahden alkuluvun x ja y $(x \leq y)$ summaksi, on

$$\sum_{p=0}^{n-1} P(2n-2p-1)\xi(2p+1). \tag{12}$$

Esimerkki 3.1.3 Osoita, että summalauseke (12) pitää paikkansa, kun $n = 6$.

Ratkaisu Muodostetaan taulukko siten, että ensimmäiseen sarakkeeseen sijoitetaan luvun p arvot, toiseen summalauseen tulon vasemmanpuoleinen tekijä ja kolmanteen tulon oikeanpuoleinen tekijä eli yhtälön (11) vasemman puoleinen lauseke. Nyt siis $n = 6$ ja siten p saa arvot nollasta viiteen.

p	$P(2n-2p-1)$	$\xi(2p+1)$
0	$P(11) = 5$	1
1	$P(9) = 4$	0
2	$P(7) = 4$	0
3	$P(5) = 3$	0
4	$P(3) = 2$	-1
5	$P(1) = 1$	1

Seuraavaksi lasketaan summalauseke (12). Saadaan

$$\begin{aligned}\sum_{p=0}^{n-1} P(2n-2p-1)\xi(2p+1) &= 5\cdot 1 + 4\cdot 0 + 4\cdot 0 + 3\cdot 0 + 2\cdot -1 + 1\cdot 1 \\ &= 5+0+0+0-2+1 \\ &= 4.\end{aligned}$$

Saadaan siis, että luku 12, $2\cdot n$, voidaan jakaa kahden alkuluvun summaksi neljällä "eri" tavalla, jotka ovat

$$\begin{aligned} 1 &+ 11 \\ 5 &+ 7 \\ 7 &+ 5 \\ 11 &+ 1. \end{aligned}$$

Nyt jos $\epsilon = 1$ tai $\epsilon = -1$ rippuen siitä, onko n alkuluku vai ei, niin

$$v = \frac{1}{2}\sum_{p=1}^{n-1} P(2n-2p-1)\xi(2p+1) + \frac{\epsilon}{2}.$$

Kolmas taulukko antaa luvun p ja luvun ϵ arvot jokaiselle parittomalle luvulle $2p+1 < 5000$.

P. Stäckel totesi, että Lionnetin argumentti ei ole aukoton, ja merkitsi symbolilla G_{2n} kaikkia luvun $2n$ eri osituksia kahden alkuluvun summina (siten, että $p+q$ ja $q+p$ lasketaan kahtena eri osituksena). Jos P_k on kaikkien parittomien alkulukujen määrä luvusta 1 lukuun k, niin silloin

$$\begin{aligned} \sum_{n=1}^{\infty} G_{2n}x^{2n} &= \left(\sum x^p\right)^2 \\ &= (1-x^p)^2\left(\sum_{v=0}^{\infty} P_{2v+1}x^{2v+1}\right)^2, \end{aligned}$$

missä p käy läpi kaikki parittomat alkuluvut.

> **Eulerin ϕ-funktio:** Jokaiselle kokonaisluvulle $n \geq 1$, $\phi(n)$ on niiden kokonaislukujen a, $1 \leq a < n$, lukumäärä, jotka täyttävät ehdon $\text{syt}(a,n) = 1$. [4, s. 25]

Arviot symbolin G_{2n} saamille arvoille suurilla luvun n arvoilla Eulerin ϕ-funktiota (phi-funktio) apuna käyttäen ovat

$$\frac{P(2n)^2}{\phi(2n)}$$

ja

$$\frac{[P(2n-\sqrt{2n})-P(\sqrt{2n})]^2}{n-\sqrt{2n}}\cdot\frac{n}{\phi(2n)}.$$

Erimielisyyttä Sylvesterin kanssa on huomattavissa; vertaa Landau s. 37. On todettu, että Goldbachin teorian paikkansapitävyys on hyvin todennäköistä (mutta ei todistettu).

Sylvester totesi, että mikä tahansa parillinen kokonaisluku $2n$ on kahden alkuluvun summa, toinen $> \frac{n}{2}$ ja toinen $< \frac{3n}{2}$, joten on mahdollista löytää kaksi alkulukua, joiden erotus on pienempi kuin mikä tahansa annettu luku (n) ja joiden summa on kaksi kertaa niin iso kuin annettu luku.

F. J. Studnicka tutki Sylvesterin lausuntoa.

Sylvester totesi, että jos N on parillinen ja $\lambda,\ldots,\omega$ ovat ne θ alkulukua, jotka ovat $> \frac{1}{4}N$ ja $< \frac{3}{4}N$ (poislukien $\frac{1}{2}N$ jos se on alkuluku), niin lukumäärä, jolla N voidaan muodostaa kahden näiden alkuluvun summana, on luvun x^N kerroin lausekkeessa

$$\frac{(\frac{1}{1-x^\lambda}+\cdots+\frac{1}{1-x^\omega})^r}{r(r-1)\theta^{r-2}} \qquad (r\geq 2).$$

E. Landau huomautti, että Stäckelin arvio luvulle G_n on

$$G_n=\frac{n^2}{\log^2 n\phi(n)},$$

ja osoitti, että summan $\sum_{n=1}^{x} G_n$ todellinen arvio on $\frac{1}{2}x^2/\log^2 x$. Pidemmällä analyysillä hän todisti, että jos me käytämme Stäckelin symbolia G_n summan muodostamiseen, niin emme saa oikeata kertaluokkaa vastauksena.

L. Ripert tutki tiettyjä suuria parillisia lukuja.

E. Maillet todisti, että jokainen parillinen luku ≤ 350000 (tai 10^6 tai $9\cdot 10^6$) on, kun puuttuvia on korkeintaan 6 (tai 8 tai 14), kahden alkuluvun summa.

A. Cunningham varmisti Goldbachin teorian kaikille luvuille 200 miljoonaan asti, jotka ovat muotoja

$$(4 \cdot 3)^n, \quad (4 \cdot 5)^n, \quad 2 \cdot 10^n, \quad 2^n(2^n \neq 1), \quad a \cdot 2^n, \quad 2a^n, \quad (2a)^n, \quad 2(2^n \neq a),$$

kun $a = 1, 3, 5, 7, 9, 11$. Hän supisti Haussnerin kaavan muuttujalle v muotoon, joka on kätevämpi laskemiselle.

J. Merlin tarkasteli operaatiota $A(b, a)$, jossa kokonaislukujen luonnollisesta sarjasta pyyhittäisiin pois kaikki luvut muotoa $ax + b$. Seuraus siitä, että läpiviedään operaatioiden $A(r_1, p_1)$, $A(r_i, p_i)$, $A(r_i', p_i)$, $i = 2, \ldots, n$, missä p_n on n alkuluku > 1, kahdesta sarjasta yksi, on sama kuin konstruoisi Eratosthenen seulan lukuun p_n asti.

> **Eratosthenen seula:** Kirjoitetaan kaikki kokonaisluvut peräkkäin lukuun p_n asti. Vedetään yli kaikki parilliset luvut, jotka ovat suurempia kuin 2. Jatketaan sievennystä vetämällä yli kaikki luvut $(> p)$, jotka ovat jaollisia pienimmälle ei yli vedetyllä luvulla p. Riittää kun tätä jatketaan lukuun p siten, että $p^2 < p_n$.[4, s. 14]

On todettu, että jokaista $vp_n \log p_n$ pituista väliä kohden on olemassa vähintään yksi luku, jota ei pyyhitä pois, mikäli v on riippumaton luvusta n. Siitä on sanottu seuraavan, että luvun a ollessa riittävän suuri, on olemassa kaksi alkulukua, joiden summa on $2a$. Tiettyjen olettamuksien ollessa voimassa, on olemassa ääretön määrä lukuja n siten, että $p_{n+1} - p_n = 2$ (ks.17).

M. Vecchi merkitsi n. paritonta alkulukua symbolilla p_n ja sanoi lukujen p_h ja p_{h+a} kuuluvan samaan järjestykseen, jos ${p_h}^2 > p_{h+a}$. Silloin $2n$ (> 132) on kahden samaan järjestykseen kuuluvan alkuluvun summa $[\frac{1}{2}(\phi+1)]$ tavalla, jos ja vain jos on olemassa ϕ lukua $\not> n - p_{m+1} + 1$ ja ei ole esitettävissä yhdelläkään tavalla muodoista

$$a_i + 3x, \ b_i + 5x, \ldots, \ l_i + p_m x \qquad (i = 1, 2),$$

missä p_{m+1} on pienin alkuluku p, jolla $p^2 + p > 2n$, ja missä tunnetut termit $a_i, b_1, \ldots$ ovat parittomia alkulukuja koskevat jäännökset, jotka esiintyvät luvun x kertoimina. [2, s. 421–424]

3.2 Otaksumasta

Vaikka alkulukuja on ääretön määrä (ks. 10), niiden jakautuminen positiivisten kokonaislukujen seassa on hyvin mystinen. Jakautumisesta löytyy nimittäin jatkuvasti vihjeitä tai aivan kuin varjoja siitä, että ne jakautuisivat tietyn säännön mukaisesti. Kuitenkin todellinen kaava, joka kuvaisi täydellisesti niiden säännönmukaisuutta, on edelleen epämääräinen. Peräkkäisten alkulukujen välinen ero voi olla hyvin pieni, kuten pareissa 11 ja 13, 17 ja 19, tai jopa 1000000000061 ja 1000000000063. Samaan aikaan kokonaislukujen joukosta voidaan löytää mielivaltaisen pitkiä jaksoja, jotka eivät sisällä ainoatakaan alkulukua.

Kysymys, onko alkulukukaksosia (ks. 17) ääretön määrä, on edelleen vastaamatta. Numeeriset todisteet johtavat epäilyihin myönteisestä päätelmästä. Elektroniset tietokoneet ovat löytäneet 152892 alkulukukaksosta, jotka ovat pienempiä kuin 30000000, ja 20 kaksosta lukujen 10^{12} ja $10^{12} + 10000$ välistä, mikä viittaa siihen, että ne yleistyvät, kun positiiviset kokonaisluvut kasvavat kooltaan. Monta todella suurista luvuista muodostuvaa esimerkkiä alkulukukaksosista on jo olemassa. Suurimmat tunnetut alkuluvut, jotka muodostavat alkulukukaksoset, ovat kumpikin 24099 merkkiä pitkiä. Ne ovat

$$665551035 \cdot 2^{80025} \pm 1.$$

Tämä alkulukupari löydettiin vuonna 2000.

Perättäiset alkuluvut voivat siis olla hyvin lähellä toisiaan tai, kuten jo edellä mainitusta voidaan päätellä, erittäin kaukana toisistaan, eli kahden alkuluvun välissä saattaa olla mielivaltaisen suuri aukko (ks. 21). Näiden laskettavissa olevien välien avulla voidaan siis saada jonkinlainen käsitys siitä, millä tavalla alkuluvut ovat kokonaislukujen sekaan sijoittuneet. Ensimmäiset tietyn pituiset alkulukujen väliset aukot, missä kaikki kahden alkuluvun väliin jäävät luvut ovat yhdistettyjä, ovat olleet tietokoneilla tehtyjen etsintöjen kohde. Esimerkiksi on olemassa 778:n suuruinen aukko (ts. $p_{n+1} - p_n = 778$), joka tulee alkuluvun 42842283925351 jälkeen. Näin isoa aukkoa ei esiinny minkään pienemmän alkuluvun jälkeen. Suurin, laskennallisesti todettu, kahden perättäisen alkuluvun välissä oleva aukko on 1092:n pituinen, jossa on 1091 yhdistettyä lukua välittömästi alkuluvun

$$4095343750096572397 21$$

jälkeen. Mielenkiintoista on se, että edes tietokoneilla laskemalla ei ole pystytty löytämään kaikkia eripituisia aukkoja, jotka ovat pienempiä kuin 1091. Pienin puuttuva aukko on 796. Otaksuma on, että on olemassa alkulukujen välinen aukko (pituudeltaan $2k-1$ peräkkäistä yhdistettyä lukua kahden alkuluvun välissä) jokaiselle parilliselle kokonaisluvulle $2k$.

Tästä päästäänkin toiseen alkulukuja koskevaan ratkaisemattomaan otaksumaan, nimittäin Goldbachin otaksumaan. Jokainen parillinen kokonaisluku voidaan esittää kahden alkuluvun summana. (Palauta mieleen nykyinen versio otaksumasta sivulta 36). Uskoaksemme, että tämä on yleensä mahdollista, on syytä tarkkailla ensin pienimpiä parillisia kokonaislukuja ja pyrkiä esittämään ne kahden alkuluvun summana. Seuraavassa esityksessä on hyvä muistaa, että aikanaan myös lukua 1 pidettiin alkulukuna ja siksi myös Goldbach aloitti parillisten lukujen käsittelyn luvusta 2 seuraavasti:

$$
\begin{aligned}
2 &= 1+1 \\
4 &= 2+2 = 1+3 \\
6 &= 3+3 = 1+5 \\
8 &= 3+5 = 1+7 \\
10 &= 3+7 = 5+5 \\
12 &= 5+7 = 1+11 \\
14 &= 3+11 = 7+7 = 1+13 \\
16 &= 3+13 = 5+11 \\
18 &= 5+13 = 7+11 = 1+17 \\
20 &= 3+17 = 7+13 = 1+19 \\
22 &= 3+19 = 5+17 = 11+11 \\
24 &= 5+19 = 7+17 = 11+13 = 1+23 \\
26 &= 3+23 = 7+19 = 13+13 \\
28 &= 5+23 = 11+17 \\
30 &= 7+23 = 11+19 = 13+17 = 1+29.
\end{aligned}
$$

Viidentoista ensimmäisen parillisen kokonaisluvun tarkastelu antaa uskoa siihen, että otaksuma olisi oikein.

Numeerista tietoa siitä, että Goldbachin otaksuma olisi totta, on uskomattoman paljon. Tietokoneiden avulla on voitu varmistaa otaksuman paikkansa-

pitävyys kaikille parillisille kokonaisluvuille, jotka ovat pienempiä kuin $6 \cdot 10^{16}$. Esimerkki tällaisesta ohjelmasta, joka laskee summattavat alkuluvut parillisille kokonaisluvuille, löytyy internetistä [5]. (Ohjelma laskee summattavat luvuille, jotka ovat $\leq 4 \cdot 10^6$. Ohjelman kooodi ks. Liite1.) Kun kokonaisluvut suurenevat, niin tavat, jolla luku $2n$ voidaan esittää kahden alkuluvun summana, lisääntyvät. Esimerkiksi luvulle 100000000 on löydettävissä 219400 erilaista tapaa. Vaikka tämä perustelee ajatusta siitä, että Goldbach oli otaksumassaan oikeassa, on se kuitenkin kaukana matemaattisesta todistuksesta, ja kaikki yritykset todistaa otaksuma ovat olleet täysin epäonnistuneita. Yksi tunnetuimmista lukuteoreetikoista viime vuosisadalla, G.H. Hardy, puheessaan Kööpenhaminan Matemaattiselle Yhdistykselle vuonna 1921 totesi, että Goldbachin otaksuma näytäisi olevan "...todennäköisesti yhtä vaikea kuin mikä tahansa ratkaisematon ongelma matematiikassa". Nykyään tiedetään, että jokainen parillinen kokonaisluku on kuuden tai vähemmän alkuluvun summa.

Huomaamisen arvoista on se, että mikäli Goldbachin otaksuma on oikein, niin silloin jokaisen parittoman kokonaisluvun suuremman kuin 7, täytyy olla kolmen parittoman alkuluvun summa. Jotta tämä nähtäisiin valitaan pariton kokonaisluku n, jonka on oltava suurempi kuin 7, jolloin $n-3$ on parillinen ja suurempi kuin 4. Nyt mikäli $n-3$ voitaisiin esittää kahden alkuluvun summana, niin silloin n voitaisiin esittää kolmen alkuluvun summana:

$$\begin{aligned} n-3 &= p_1 + p_2, \\ n &= p_1 + p_2 + 3. \end{aligned}$$

Toinen mielenkiintoinen seuraus siitä, että Goldbachin otaksuma olisi oikein, on se, että silloin jokaista kokonaislukua, $n \geq 3$, vastaisi kokonaisluku $k \geq 0$ siten, että $n+k$ ja $n-k$ olisivat molemmat alkulukuja. Tämä seuraa siitä, että jokainen parillinen kokonaisluku on muotoa $2n$, ja jotta se voitaisin esittää kahden alkuluvun summana, on näiden alkulukujen oltava kummankin yhtä kaukana luvusta n. Mielenkiintoista onkin nyt tutkia, mitä nämä luvun k arvot ovat, kun tarkastelemme parillisia kokonaislukuja. Kuten hyvin muistamme, parillisilla luvuilla ei ole välttämättä yksikäsitteistä tapaa esittää niitä kahden alkuluvun summana (ks. 44), joten seuraavaan taulukkoon on valittu aina pienin mahdollinen lukua n vastaava k (Taulukosta on jätetty pois kokonaisluvut jotka ovat muotoa $2p$, p on alkuluku, eli tapaukset, joissa $k = 0$). Seuraavaa taulukkoa tarkastellessa on syytä kiinnittää huomio siihen,

kuinka luvun k arvot noudattavat tiettyä kaavaa (sanomattakin on selvää, että kaava ei jatku loputtomiin, vaan se edustaa vain yhtä osaa parillisista luvuista).

$2n$	n	k	$n-k$	$n+k$	$2n$	n	k	$n-k$	$n+k$
12	6	1	5	7	72	36	5	31	41
16	8	3	5	11	76	38	9	29	47
18	9	2	7	11	78	39	2	37	41
20	10	3	7	13	80	40	3	37	43
24	12	1	11	13	84	42	1	41	43
28	14	3	11	17	88	44	3	41	47
30	15	2	13	17	90	45	2	43	47
32	16	3	13	19	92	46	15	31	61
36	18	1	17	19	96	48	5	43	53
40	20	3	17	23	98	49	12	37	61
42	21	2	19	23	100	50	3	47	53
44	22	9	13	31	102	51	8	43	59
48	24	5	19	29	104	52	9	53	61
50	25	6	19	31	108	54	7	47	61
52	26	3	23	29	110	55	12	43	67
54	27	4	23	31	112	56	3	53	59
56	28	9	19	37	114	57	4	53	61
60	30	1	29	31	116	58	15	43	73
64	32	9	23	31	120	60	1	59	61
66	33	4	29	37	124	62	9	53	71
68	34	3	31	37	126	63	4	59	67
70	35	6	29	41	128	64	3	61	67

Tämänmittaisesta taulukosta voidaan löytää useita pieniä jaksoja, joissa k noudatta tiettyä kaavaa. Taulukosta voidaan kuitenkin löytää myös yk-

si suhteellisen laaja tiettyä kaavaa noudattava jakso. Tarkastellessamme väliä $30 \leq 2n \leq 90$ voimme huomata, että luvun k arvot noudattavat tiettyä kaavaa keskipisteenään $2n = 60$, josta ylös- ja alaspäin lähtevät luvun k arvot ovat samoja. Alkaen luvusta $2n = 92$ luvun k arvot näyttäisivät saavan hyvin epämääräisiä arvoja. Jotta suurempia kaavamaisuuksia voitaisiin tällä tavalla löytää, vaatisi se jo tietokonaiden mukaan ottamista etsintään.

Edellä mainitut seuraamukset eivät kuitenkaan johdata meitä otaksuman matemaattiseen todistukseen, ja niin kauan kuin otaksuma pysyy todistamattomana, on asiaa lähestyttävä toisesta suunnasta.

Ensimmäinen todellinen edistyminen otaksuman suhteen lähes 200 vuoteen tehtiin Hardyn ja Littlewoodin toimesta 1922. Tietyn todistamattoman hypoteesin pohjalta, niin sanotun yleistetyn Riemannin hypoteesin, he näyttivät, että jokainen riittävän suuri pariton luku on kolmen alkuluvun summa. Vuonna 1937 venäläinen matemaatikko I. M. Vinogradov onnistui poistamaan todistuksesta sen riippuvuuden yleistetystä Riemannin hypoteesista ja näin myös antamaan tälle tulokselle ehdottoman todistuksen; toisin sanoen hän todisti, että jokainen pariton kokonaisluku, suurempi kuin jokin käytännössä laskettavissa oleva n_0, voidaan esittää kolmen parittoman alkuluvun summana. Siis

$$n = p_1 + p_2 + p_3 \qquad (n \text{ pariton ja riittävän suuri}).$$

Vinogradov ei osannut päättää, kuinka suuri luvun n_0 tulisi olla, mutta Borozdkin (1956) todisti, että $n_0 < 3^{3^{15}}$. Vuonna 1989 luvun n_0 raja väheni luvuksi 10^{43000}. Siitä seurasi suoraan, että jokainen parillinen kokonaisluku jostain pisteestä eteenpäin on joko kahden tai neljän alkuluvun summa. Siksi riittääkin, että kysymykseen vastataan jokaisen parittoman kokonaisluvun n osalta välillä $9 \leq n \leq n_0$. Tämä vastaaminen, annetulla kokonaisluvulla, olisi vain yksitoikkoista laskemista, mutta valitettavasti n_0 on niin suuri, että se ylittää tämän päivän elektronisten tietokoneiden kyvyt.

Toinen ongelma, läheisessä yheydessä Goldbachin otaksumaan, on se, onko jokainen parillinen luku kahden melkein alkuluvun summa.

> **Melkein alkuluku** on luku, jolla on vain tietty määrä alkulukutekijöitä; mitä vähemmän tekijöitä on, sitä tarkempi arvio luku on, ja sitä parempia tuloksia luvulla saadaan.

Ensimmäinen tämänkaltainen teoria oli Brunin aikaansaannos (1920). Hän osoitti, että jokainen riittävän suuri parillinen luku voidaan esittää kahden termin summana, jossa kummallakin on korkeintaan 9 alkulukutekijää. Myöhemmin Buchstab (1940) paransi tulosta 4 alkulukutekijään.

Vuonna 1948 unkarilainen matemaatikko Rényi osoitti, että jokainen suuri parillinen kokonaisluku n on alkuluvun ja melkein alkuluvun summa:

$$n = p + p_1 p_2 \cdots p_r \qquad (n \text{ parillinen ja riittävän suuri}).$$

Rényin todistuksessa r on erittäin suuri. Mikäli voitaisiin osoittaa, että todistuksessa $r = 1$, niin silloin Goldbachin otaksuma tulisi todistettua suurille luvuille n. Wangin (1959) myöhempi työ mahdollisti käyttämään lukua $r \leq 4$, kun taas A.I Vinogradov (1965) edelleen vähensi arvion lukuun $r \leq 3$. Chen Jing-Run (1966) on päässyt lähimmäksi otaksuman todistamista kuin kukaan muu, kun hän pääsi tulokseen $r \leq 2$; toisin sanoen, jostain pisteestä eteenpäin jokainen parillinen kokonaisluku on alkuluvun ja enintään kahden alkuluvun tulon summa. Chenin alkuperäinen todistus oli hyvin pitkä, mutta vuonna 1973 hän paranteli argumenttiaan ja vähensi sen pituuden 20 sivuun.

Vahvojen todisteiden vuoksi meidän on helppo uskoa Goldbachin otaksuman paikkansa pitävyys. On kuitenkin mahdollista, että se ei ole totta. Vinogradov osoitti, että jos $A(x)$ on parillisten lukujen $n \leq x$, jotka eivät ole kahden alkuluvun summa, määrä, niin

$$\lim_{x \to \infty} A(x)/x = 0.$$

Tämä mahdollistaa päätelmän, että "melkein kaikki" parilliset kokonaisluvut toteuttavat otaksuman. Kuten Edmund Landau hyvin osuvasti sanoi, "Goldbachin otaksuma ei pidä paikkaansa melkein 0%:ssa kaikista parillisista kokonaisluvuista; tämä *melkein* 0% ei tietenkään sulje pois mahdollisuutta, että on olemassa äärettömän monta poikkeusta.".[1, s. 51–54]

Viitteet

[1] Burton, David M.: *Elementary Number Theory, Fifth Edition.* R. R. Donnelley & Sons Company/Crawfordsville, IN, 2002.

[2] Dickson, Leonard Eugene: *History of The Theory of Numbers, Volume 1, Divisibility And Primality.* Chelsea Publishing Company, New York, 1971.

[3] LeVeque, William J.: *Fundamentals of Number Theory.* Addison-Wesley Publishing Company, Inc., 1977.

[4] Ribenboim, Paulo: *The Book of Prime Number Records, Second Edition.* R. R. Donnelley & Sons, Harrisonburg, Virginia, 1989.

[5] Teemu Lehtosen kotisivu. Linkki ohjelma (toteutettu javalla) [Viitattu 4.10.2003].
URL http://www.lehtoset.net/teemu/mat.html

[6] The Great Internet Mersenne Prime Search Home Page [Viitattu 27.9.2003].
URL http://www.mersenne.org

Liite1

Ohjelma, joka laskee annetulle positiiviselle parilliselle kokonaisluvulle alkuluvut, joiden summa annettu luku on. Ohjelma on java-koodia.

```
import In;
class Goldbach{
  static int luku;
  static int jako;
  static char odota;
  public static void main(String[] args){
        esittely();
        odota = 'k';
        while(odota == 'k'){
            vastaanotaSyöte();
            lasketaanSummattavat();
            System.out.println("Haluatko jatkaa (k)kyllä vai (e)ei?");
            odota = In.lueChar();
        }
  }
  public static void esittely(){
      System.out.print("Teemu Lehtonen\n3.10.2003\n\n");
  }
  public static void vastaanotaSyöte(){
      System.out.println("Anna jokin positiivinen parillinen
      kokonaisluku >7.");
      luku = In.lueInt();
      jako = luku/2;
  }
  public static void lasketaanSummattavat(){
        for(int i=1; i<jako; i++){
              int erotus = jako-i;
              int t = alkulukuTesti(erotus);
              if(t==1){
                    int summa = jako+i;
                    int u = alkulukuTesti(summa);
                    if(u==1){
                          System.out.println("Luku " +luku +" on
                                              alkulukujen " +erotus +"
                                              ja " +summa +" summa.\n");
                          i = jako;
                    }
              }
        }
  }
  public static int alkulukuTesti(int x){
      int index = 2;
      int laskuri = 0;
      while(laskuri == 0){
            int a = x % index;
            if(a == 0 && x == index){
                  return 1;
            }
            else if(a == 0 && x != index){
                  return 0;
            }
            else
```

```
                index = index + 1;
      }
      return 0;
  }
}
```

Edellisessä tarvittava In.java tiedosto:

```
import java.io.*;
public class In{
    static BufferedReader stdin = new BufferedReader
                        (new InputStreamReader(System.in));
    static final int lippu = 81;

    public static int lueInt(){
       int luku = 0;
       String rivi;
       while(true){
          try{
             do{
                rivi = stdin.readLine();
             }while(rivi.length()==0);
             stdin.mark(lippu);
            stdin.reset();
            luku = Integer.parseInt(rivi);
            break;
          }catch(IOException e){
               System.out.println("Virhesyöte");
                        System.exit(1);
          }
          catch(NumberFormatException e2){
              System.out.println("Virhe luvun syötössä - anna uudestaan.");
          }
       } //while
       return luku;
    }

    public static float lueFloat(){
       float liuku = 0.0F;
       String rivi;
       while(true){
          try{
              do{
                 rivi = stdin.readLine();
              }while(rivi.length()==0);
          stdin.mark(lippu);
          stdin.reset();
          liuku =Float.valueOf(rivi).floatValue();
          break;
        }catch(IOException e){
              System.out.println("Virhesyöte");
              System.exit(1);
        }
        catch(NumberFormatException e2){
           System.out.println("Virhe luvun syötössä - anna uudestaan.");
        }
```

```
      } //while
      return liuku;
   }

   public static String lueRivi(){
      String rivi = "";
      try{
         rivi = stdin.readLine();
         stdin.mark(lippu);
         stdin.reset();
      }catch(IOException e){
          System.out.println("Virhesyöte");
          System.exit(1);
      }
      return rivi;
   }

   public static char lueChar(){
       String rivi;
       try{
          rivi = stdin.readLine();
          if(rivi.length() > 0){
             stdin.mark(lippu);
             stdin.reset();
             return rivi.charAt(0);
          }
       }catch(IOException e){
           System.out.println("Virhesyöte");
           System.exit(1);
       }
       return '\0';
   }
}
```