



WILLANSIN KAAVA

Saaga Järvinen

LuK-tutkielma
Maaliskuu 2026

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

Tarkastaja:

FM, DI Mikko Jaskari

Turun yliopiston laatu järjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck-järjestelmällä.

TURUN YLIOPISTO, Matematiikan ja tilastotieteen laitos

LuK-tutkielma

Pääaine: Matematiikka

Tekijä: Saaga Järvinen

Otsikko: Willansin kaava

Ohjaaja: FM, DI Mikko Jaskari

Sivumäärä: 10 sivua

Aika: Maaliskuu 2026

Tässä LuK-tutkielmassa käsitellään alkulukujen generoimista Willansin kaavalla. Lukija johdatellaan aiheen pariin esittelemällä Eratostheneen seula, jonka jälkeen johdetaan Willansin kaava, jolla voidaan määrittää haluttua järjestyslukua vastaava alkuluku. Tämän lisäksi esitetään laskuesimerkki viidennen alkuluvun laskemisesta.

Asiasanat: alkuluvut, Willansin kaava, Eratostheneen seula, Wilsonin lause

Sisällys

| | | |
|----------|--|----------|
| 1 | Johdanto | 1 |
| 2 | Eratostheneen seula | 1 |
| 3 | Willansin kaava alkuluvun p_n generoimiseksi | 3 |
| 3.1 | Willansin kaavan johtaminen | 3 |
| 3.2 | Esimerkki Willansin kaavan käyttämisestä | 7 |
| 4 | Yhteenveto | 9 |
| | Viitteet | 9 |

1 Johdanto

Määritellään luonnolliset luvut alkamaan luvusta 1. Alkuluvuksi kutsutaan luonnollista lukua, joka ei ole jaollinen muilla luvuilla kuin itsellään ja luvulla 1 ja joka on suurempi kuin luku 1, koska luku 1 ei sovitusti ole alkuluku. Alkuluvut voidaan määritellä täsmällisemmin seuraavasti.

Määritelmä 1. Luonnollinen luku $p > 1$ on alkuluku, jos sen ainoat positiiviset tekijät ovat 1 ja p .

Jos luonnollinen luku ei ole alkuluku, sitä kutsutaan yhdistetyksi luvuksi. Jokainen luonnollinen luku voidaan aritmetiikan peruslauseen mukaan esittää yksikäsitteisesti alkulukujen tulona lukuun ottamatta alkulukujen järjestystä tulossa. Toisin sanoen kaikki luonnolliset luvut koostuvat alkuluvuista. [3] Alkulukujen esiintymiseen taas liittyy niin kutsuttu alkulukufunktio, jota merkitään $\pi(x)$. Alkulukufunktion arvona saadaan lukua x pienempien tai yhtäsuurien alkulukujen lukumäärä. [4]

Alkulukuja etsitään sekä laskennallisesta kiinnostuksesta niitä kohtaan että käytännön sovelluksia varten. Eräs esimerkki alkulukujen käytännön sovelluksista ovat salausjärjestelmät, kuten julkisen avaimen salausalgoritmi RSA, jossa tarvitaan erityisesti suuria alkulukuja. [5] Ensimmäisten alkulukujen määrittäminen on vielä suhteellisen helppoa, koska käsiteltävät luvut ovat pieniä. Myöhemmin uusien alkulukujen löytäminen on käynyt hitaaksi niiden kasvaessa valtavan suuriksi. [1]

Alkulukuja voidaan etsiä erilaisten tietokoneella suoritettavien lukuja testaavien algoritmien avulla. Esimerkiksi Great Internet Mersenne Prime Search (GIMPS) tarjoaa nettisivuillaan ladattavaksi ohjelman, jolla voi suorittaa erästä tällaista algoritmia ja etsiä niin kutsuttuja Mersennen alkulukuja. Uuden alkuluvun löytäminen voi kuitenkin kestää useita kuukausia tietokoneelta, sillä algoritmi on kovin työläs suorittaa eikä testattava luku aina ole alkuluku. [8]

Mielenkiintoa kuitenkin herättää kysymys siitä, onko olemassa kaavaa, jolla alkulukuja voisi suoraan generoida. Tunnetulla Eratostheneen seulalla, joka esitellään tutkielman toisessa luvussa, voidaan määrittää uusia alkulukuja, kun pienemmät alkuluvut tiedetään. Alkulukujen suora generointi kuitenkin vaatii Eratostheneen seulaa monimutkaisempaa algoritmia, mistä päästäänkin kolmannessa luvussa esiteltävään Willansin kaavaan järjestyslukua n vastaavan alkuluvun generoimiseksi.

2 Eratostheneen seula

Tutustutaan ensin yksinkertaiseen tapaan määrittää alkulukuja käsin. Kyseessä on Eratostheneen seula, joka on noin vuosina 276–194 jaa eläneen kreikkalaisen matemaatikon Eratostheneen luoma algoritmi alkulukujen löytämiseen. [2] Algoritmi toimii niin, että ensin kirjataan ylös kaikki lukua 1 suuremmat luonnolliset luvut haluttuun lukuun asti, minkä jälkeen poistetaan lukujen joukosta ne luvut, joiden tekijöinä on muita lukuja.

Etsitään esimerkkinä kaikki alkuluvut lukuun 50 asti. Kirjataan luvut esimerkiksi taulukon 1 tapaan.

| | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |

Taulukko 1: Eratostheneen seula: kaikki luonnolliset luvut väliltä [2,50].

Tämän jälkeen lähdetään liikkeelle ensimmäisestä alkuluvusta, eli luvusta 2, ja vedetään taulukosta yli kaikki sen moninkerrat. Esimerkki tästä on esitetty taulukossa 2.

| | | | | | | | | | |
|----|---------------|----|---------------|----|---------------|----|---------------|----|---------------|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |

Taulukko 2: Eratostheneen seula: luvun 2 moninkerrat yliviivattu.

Yliviivatut luvut voidaan poistaa taulukosta, koska ne eivät voi olla alkulukuja, sillä luku 2 on niiden kaikkien tekijä. Tämän jälkeen tarkastellaan taulukon seuraavaa lukua, jota ei ole poistettu, eli lukua 3, ja yliviivataan kaikki sen moninkerrat kuten taulukossa 3 on esitetty.

| | | | | | | | | | |
|---------------|---|---------------|--|---------------|--|----|--|---------------|--|
| | 2 | 3 | | 5 | | 7 | | 9 | |
| 11 | | 13 | | 15 | | 17 | | 19 | |
| 21 | | 23 | | 25 | | 27 | | 29 | |
| 31 | | 33 | | 35 | | 37 | | 39 | |
| 41 | | 43 | | 45 | | 47 | | 49 | |

Taulukko 3: Eratostheneen seula: luvun 2 moninkerrat poistettu ja luvun 3 moninkerrat yliviivattu.

Tästä eteenpäin voitaisiin jatkaa samalla menetelmällä ja seuraava tarkasteltava luku olisi luku 5. Kaikkia alkulukuja valittuun lukuun n asti ei kuitenkaan tarvitse tarkastella. Koska yhdistetyn luvun voi ilmaista muodossa $n = ab$, voi pienempi tekijöistä olla korkeintaan \sqrt{n} . Eli seulassa riittävää on tarkastella luonnolliset luvut, jotka ovat tätä pienempiä. Tässä esimerkissä riittävää on tarkastella lukua 7 pienemmät tai yhtäsuuret alkuluvut, koska $\sqrt{50} = 7,08$. Kun kaikkien tarvittavien alkulukujen moninkerrat on käyty läpi ja poistettu taulukosta, jää jäljelle vain lukua n pienemmät alkuluvut. Lukua 50 pienemmät alkuluvut on esitetty taulukossa 4.

| | | | | | | | | | |
|----|---|----|--|---|--|----|--|----|--|
| | 2 | 3 | | 5 | | 7 | | | |
| 11 | | 13 | | | | 17 | | 19 | |
| | | 23 | | | | | | 29 | |
| 31 | | | | | | 37 | | | |
| 41 | | 43 | | | | 47 | | | |

Taulukko 4: Eratostheneen seula: kaikki alkuluvut väliltä $[2,50]$.

Algoritmina Eratostheneen seula on yksinkertainen ja toimiva. Sen avulla ei kuitenkaan voida suoraan generoida alkulukuja, sillä algoritmi vaatii ensin pienempien alkulukujen määrittämistä.

3 Willansin kaava alkuluvun p_n generoimiseksi

Seuraavaksi esitellään Willansin kaava järjestyslukua n vastaavan alkuluvun generoimiseksi.

Määritelmä 2. Merkitään järjestyslukua n vastaavaa alkulukua p_n , kun indeksointi aloitetaan luvusta 1. Tällöin kolmea ensimmäistä alkulukua merkittäisiin $p_1 = 2$, $p_2 = 3$ ja $p_3 = 5$.

Kaavan johtaminen perustuu englantilaisen matemaatikon John Wilsonin esittämään ja hänen mukaansa nimettyyn tulokseen liittyen alkulukuihin. Päälähteenä tämän luvun kirjoittamiseen on käytetty C. P. Willansin omaa julkaisua kaavastaan vuodelta 1964.[7].

3.1 Willansin kaavan johtaminen

Seuraavaksi esitettävä Wilsonin lause ja sen todistus pohjautuvat lähteeseen [6].

Lause 1 (Wilson). *Luonnollinen luku $p > 1$ on alkuluku, jos ja vain, jos*

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

Todistus. Oletetaan, että p on alkuluku. Kaikki jakojäännökset $a \not\equiv 0 \pmod{p}$ ovat jäännösluokkarenaan \mathbb{Z}/\mathbb{Z}_p alkioita. Tällöin kertoma $(p - 1)!$ on jäännösluokkarenaan kaikkien alkioiden tulo. Jos

$$a \not\equiv a^{-1} \pmod{p} \quad \text{eli} \quad a^2 \not\equiv 1 \pmod{p},$$

niin luvut a ja niiden käänteisalkiot molemmat kuuluvat jäännösluokkarenaan. Kun alkiot ja niiden käänteisalkiot ryhmitellään pareiksi, ne kumoutuvat pois ja saadaan

$$(p - 1)! \equiv \prod_{a^2 \equiv 1 \pmod{p}} a \pmod{p}.$$

Jäljelle siis jäävät vain alkioit, joille pätee $a^2 \equiv 1 \pmod{p}$. Ehto $a^2 \equiv 1 \pmod{p}$ pätee, jos ja vain jos $p|(a-1)(a+1)$. Koska p on alkuluku, se jakaa vain toisen näistä tekijöistä, eli joko $p|(a-1)$ tai $p|(a+1)$. Toisin sanoen $a \equiv \pm 1 \pmod{p}$, josta seuraa, että

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

Osoitetaan lauseen toimivuus vielä toiseen suuntaan vastaoletuksen avulla. Oletetaan, että p ei ole alkuluku, mutta toteuttaa $(p-1)! \equiv -1 \pmod{p}$. On siis olemassa jokin luku b , jolle pätee $1 < b < p$, ja joka jakaa luvun p . Nyt

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

Toisaalta

$$(p-1)! \equiv -1 \pmod{p}$$

eli

$$(p-1)! + 1 \equiv 0 \pmod{p},$$

ja $b | p$ niin myös

$$(p-1)! + 1 \equiv 0 \pmod{b}.$$

Nyt

$$-1 \equiv (p-1)! \equiv 0 \pmod{b},$$

jolloin $b | 1$. Tämä pätee vain, jos $b = 1$. Päädytään siis ristiriitaan oletuksen $1 < b < p$ kanssa, jolloin vasta oletus ei päde ja saadaan, että

$$(p-1)! \equiv -1 \pmod{p},$$

jos ja vain, jos p on alkuluku.

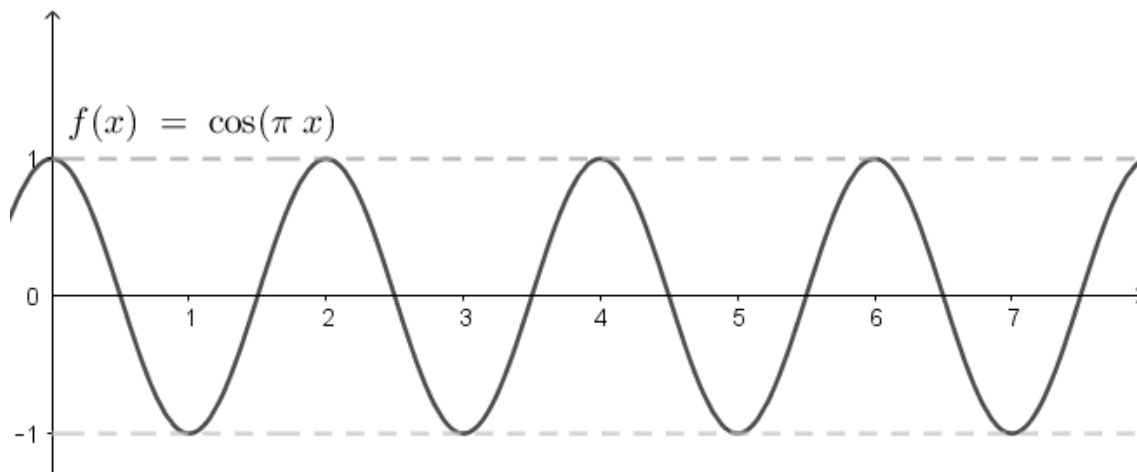
□

Johdetaan tästä seuraavaksi Willansin kaava alkuluvun p_n generoimiseksi. Wilsonin lauseesta saadaan, että luku

$$\frac{(x-1)! + 1}{x} \tag{1}$$

on kokonaisluku, jos ja vain, jos $x = 1$ tai x on alkuluku.

Otetaan seuraavaksi käyttöön kosinifunktio. Funktio $\cos \pi x$ saa arvoja väliltä $[-1, 1]$ niin, että arvoksi saadaan 1 tai -1 , kun x on kokonaisluku. Tätä ominaisuutta on havainnollistettu kuvassa 1.



Kuva 1: Funktion $f(x) = \cos(\pi x)$ kuvaaja.

Koska lausekkeen (1) arvo on kokonaisluku aina, kun $x = 1$ tai x on alkuluku, on lausekkeen

$$\cos \pi \frac{(x-1)! + 1}{x} \quad (2)$$

arvo silloin 1 tai -1 , kun $x = 1$ tai x on alkuluku. Tällöin korottamalla lauseke (2) toiseen potenssiin saadaan tapauksille $x = 1$ ja x on alkuluku arvoksi vain luku 1 ja yhdistetyn luvun arvoksi luku väliltä $[0, 1)$. Nyt kaava on johdettu muotoon

$$\left(\cos \pi \frac{(x-1)! + 1}{x} \right)^2. \quad (3)$$

Seuraavaksi hyödynnetään lattiafunktiota.

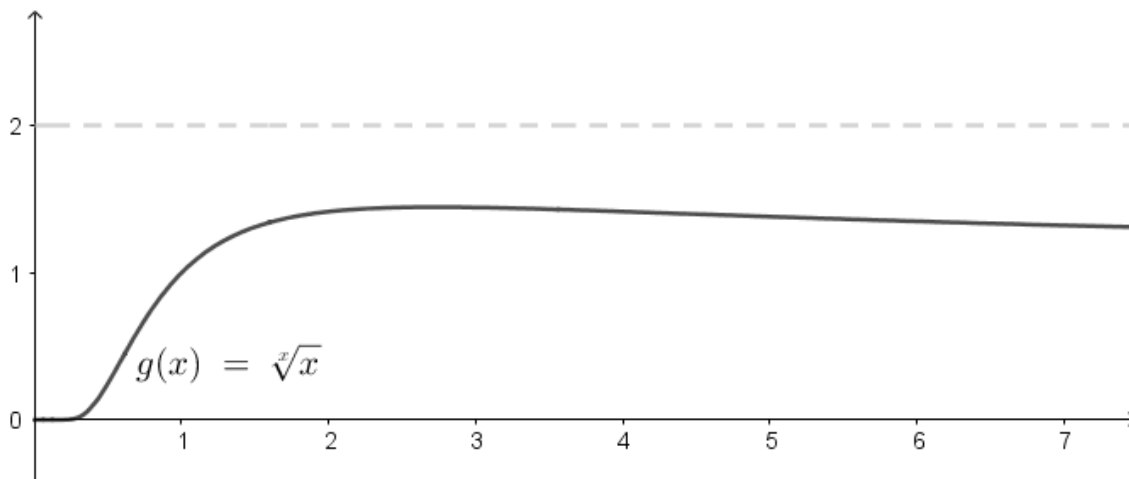
Määritelmä 3. Lattiafunktiolla tarkoitetaan funktiota $f(x) = \lfloor x \rfloor$, joka saa arvokseen suurimman kokonaisluvun, joka on pienempi tai yhtäsuuri kuin x .

Ottamalla lattiafunktio lausekkeesta (3) saadaan välin $[0, 1)$ arvot nolaksi. Tämä yksinkertaistaa yhdistetyn luvun tapauksen. Tässä kohtaa siis

$$\left[\left(\cos \pi \frac{(x-1)! + 1}{x} \right)^2 \right] = \begin{cases} 1, & \text{kun } x = 1 \text{ tai } x \text{ on alkuluku} \\ 0, & \text{kun } x \text{ on yhdistetty luku.} \end{cases}$$

Summaamalla lausekkeen arvoja luvusta 1 luonnolliseen lukuun m saadaan siis summa, jonka termeinä on vain lukuja 1 ja 0. Koska tapauksen $x = 1$ jälkeen jokainen summan termi, jonka arvo on 1, merkitsee alkulukua, summan arvo antaa lukumäärän, jossa on lukua m pienemmät alkuluvut mukaan lukien luku 1. Eli, kun summasta vähennetään luku 1, saadaan lukua m pienempien alkulukujen täsmällinen määrä. Kaava on nyt muotoa

$$-1 + \sum_{x=1}^m \left[\left(\cos \pi \frac{(x-1)! + 1}{x} \right)^2 \right].$$



Kuva 2: Funktion $g(x) = \sqrt[x]{x}$ kuvaaja.

Merkitään kaavan tätä osaa alkulukufunktiona

$$\pi(m) = -1 + \sum_{x=1}^m \left[\left(\cos \pi \frac{(x-1)! + 1}{x} \right)^2 \right]$$

lopullisen kaavan johtamisen yksinkertaistamiseksi.

Määritellään seuraavaksi apufunktio A_n . Olkoon

$$A_n(a) = \left\lfloor \sqrt[n]{\frac{n}{1+a}} \right\rfloor, \text{ jossa } n = 1, 2, \dots \text{ ja } a = 0, 1, 2, \dots$$

Jos $a < n$, niin $1 \leq \frac{n}{1+a} \leq n$. Tästä seuraa, että $1 \leq \sqrt[n]{\frac{n}{1+a}} \leq \sqrt[n]{n}$, eli $1 \leq \sqrt[n]{\frac{n}{1+a}} \leq \sqrt[n]{n} < 2$. Tätä ominaisuutta on havainnollistettu kuvassa 2.

Jos $a \geq n$, niin $0 < \frac{n}{1+a} < 1$, josta seuraa, että $0 < \sqrt[n]{\frac{n}{1+a}} < 1$. Funktiolle siis pätee

$$A_n(a) = \begin{cases} 1, & \text{kun } a < n \\ 0, & \text{kun } a \geq n. \end{cases}$$

Kun funktiot A_n ja π yhdistetään, saadaan

$$A_n(\pi(m)) = \left\lfloor \left(\frac{n}{\sum_{x=1}^m \left[\left(\cos \pi \frac{(x-1)! + 1}{x} \right)^2 \right]} \right)^{1/n} \right\rfloor,$$

jolle pätee

$$A_n(\pi(m)) = \begin{cases} 1, & \text{kun } m < p_n \\ 0, & \text{kun } m \geq p_n. \end{cases}$$

Kun ylläolevan funktion arvolla m antamia arvoja lasketaan yhteen, saadaan summa, jossa on vain nollia ja ykkösiä. Jokainen m , joka on pienempi kuin p_n antaa

summaan luvun 1. Kun $m \geq p_n$, saadaan tästä eteenpäin summaan vain nollia. Funktion antamia arvoja täytyy siis summata riittävän pitkälle, jotta summaan saadaan kaikki ykköset ennen nollia. Tämä on Willansin kaavassa ratkaistu niin, että summa käy luvusta $m = 1$ lukuun $m = 2^n$ asti. Sillä kaikille luonnollisille luvuille n pätee $p_n \leq 2^n$.

Koska sisemmän summan arvo on lukua m pienempien alkulukujen määrä luku 1 mukaan lukien, saadaan ulomman summan arvoksi $p_n - 1$. Summaan täytyy vielä lisätä luku 1, jotta saadaan tuloksena p_n . Nyt kaava on saatu johdettua lopulliseen muotoonsa

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left(\frac{n}{\sum_{x=1}^m \left[\left(\cos \pi \frac{(x-1)!+1}{x} \right)^2 \right]} \right)^{1/n} \right].$$

3.2 Esimerkki Willansin kaavan käyttämisestä

Willansin kaavan havainnollistamiseksi lasketaan vaiheittain viides alkuluku eli p_5 . Viidettä alkulukua laskiessa uloimmassa summassa m käy läpi arvot luvusta 1 lukuun $2^5 = 32$. Tällöin myös sisemmän summan x käy vähitellen läpi arvot luvusta 1 lukuun 32.

Aloitetaan laskemalla kosinilausekkeen arvoja. Neljä ensimmäistä kosinilausekkeen arvoa ovat

$$\begin{aligned} \cos \pi \frac{(1-1)!+1}{1} &= \cos \pi \frac{1+1}{1} = \cos 2\pi = 1, \\ \cos \pi \frac{(2-1)!+1}{2} &= \cos \pi \frac{1+1}{2} = \cos \pi = -1, \\ \cos \pi \frac{(3-1)!+1}{3} &= \cos \pi \frac{2+1}{3} = \cos \pi = -1 \quad \text{ja} \\ \cos \pi \frac{(4-1)!+1}{4} &= \cos \pi \frac{6+1}{4} = \cos \frac{7}{4}\pi = 0,7071 \dots \end{aligned}$$

Arvojen laskemista jatkettaisiin vastaavasti lukuun $x = 32$ asti.

Kun saatujen arvojen neliöistä otetaan lattiafunktio, saadaan

$$\begin{aligned} \left[\left(\cos \pi \frac{(1-1)!+1}{1} \right)^2 \right] &= [1^2] = 1, \\ \left[\left(\cos \pi \frac{(2-1)!+1}{2} \right)^2 \right] &= [(-1)^2] = 1, \\ \left[\left(\cos \pi \frac{(3-1)!+1}{3} \right)^2 \right] &= [(-1)^2] = 1 \quad \text{ja} \\ \left[\left(\cos \pi \frac{(4-1)!+1}{4} \right)^2 \right] &= [0,7071^2] = 0. \end{aligned}$$

Näistä ensimmäisen luvun 1 jälkeen jokainen 1 merkitsee alkulukua ja jokainen 0 yhdistettyä lukua.

Näiden summattavien lukujen lukumäärä riippuu luvun m arvosta. Kun $m = 1$, summaan tulee vain ensimmäisen lausekkeen antama arvo. Kun $m = 2$, saadaan summaan lausekkeen kaksi ensimmäistä arvoa. Kun $m = 3$, saadaan vastaavasti 3 ensimmäistä arvoa. Tätä jatketaan, kunnes m on käynyt läpi kaikki arvot luvusta 1 lukuun 32. Lasketaan näkyviin summa, kun $m = 32$. Tästä summasta pystytään näkemään myös luvun m muilla arvoilla saadut summat ottamalla huomioon vain siihen asti saadut luvut. Kun $m = 32$, summaksi saadaan

$$\begin{aligned} & \sum_{x=1}^{32} \left[\left(\cos \pi \frac{(x-1)!+1}{x} \right)^2 \right] \\ & = 1 + 1 + 1 + 0 + 1 + 0 + 1 + 0 + 0 + 0 + 1 + 0 + 1 + 0 + 0 + 0 \\ & \quad + 1 + 0 + 1 + 0 + 0 + 0 + 1 + 0 + 0 + 0 + 0 + 0 + 1 + 0 + 1 + 0 \\ & = 12. \end{aligned}$$

Myös ulommassa summassa saadaan summattavaksi vain lukuja 1 ja 0. Summaan tuleva luku on 1 silloin, kun lukua m pienempien alkulukujen määrä luku 1 mukaan lukien on pienempi tai yhtä suuri kuin luku n . Tämän rajan jälkeen jokainen summaan saatava luku on 0. Tässä vaiheessa siis tutkitaan sisemässä summassa olevia lukuja. Summan termejä laskettaessa saadaan

$$\begin{aligned} & \sum_{m=1}^{2^5} \left[\left(\frac{5}{\sum_{x=1}^m \left[\left(\cos \pi \frac{(x-1)!+1}{x} \right)^2 \right]} \right)^{1/5} \right] \\ & = \left[\left(\frac{5}{1} \right)^{1/5} \right] + \left[\left(\frac{5}{2} \right)^{1/5} \right] + \dots + \left[\left(\frac{5}{5} \right)^{1/5} \right] + \left[\left(\frac{5}{6} \right)^{1/5} \right] + \dots + \left[\left(\frac{5}{12} \right)^{1/5} \right] \\ & = \underbrace{1 + 1 + \dots + 1}_{10 \text{ kpl}} + \underbrace{0 + \dots + 0}_{22 \text{ kpl}}. \end{aligned}$$

Arvoksi saadaan siis $p_5 - 1$, eli

$$\sum_{m=1}^{2^5} \left[\left(\frac{5}{\sum_{x=1}^m \left[\left(\cos \pi \frac{(x-1)!+1}{x} \right)^2 \right]} \right)^{1/5} \right] = 10.$$

Lopuksi summaan lisätään luku 1. Viidenneksi alkuluvuksi saadaan siis

$$\begin{aligned}
p_5 &= 1 + \sum_{m=1}^{2^5} \left[\left(\frac{5}{\sum_{x=1}^m \left[\left(\cos \pi \frac{(x-1)!+1}{x} \right)^2 \right]} \right)^{1/5} \right] \\
&= 1 + 10 = 11.
\end{aligned}$$

4 Yhteenveto

Käytännössä Willansin kaava on algoritmi, johon voidaan syöttää mikä tahansa järjestysluku n ja josta saadaan tuloksena sitä vastaava alkuluku. Kaavalla voidaan siis täsmällisesti määrittää mikä tahansa alkuluku.

Kaava kuitenkin koostuu yhdestä kertomasta ja kahdesta summasta, jotka molemmat kasvavat nopeasti valtavan pitkiksi luvun n kasvaessa. Tämän vuoksi kaava on jopa tietokoneelle turhan työläs tapa etsiä uusia isoja alkulukuja, ja on siksi melko hyödytön. Willans itse myös toteaa julkaisussaan ettei kaava sovellu ratkaisemaan alkulukuihin liittyviä ongelmia. Toisaalta kaava on vastaus kysymykseen siitä, onko olemassa kaavaa, jolla generoida mikä tahansa alkuluku p_n . [7]

Viitteet

- [1] Jeremiah Bartz, Prime numbers have fascinated mathematicians for centuries—technology is revolutionizing the search, <https://phys.org/news/2025-06-prime-fascinated-mathematicians-centuries-technology.html> viitattu 3.11.2025
- [2] Bressoud, D. M. (1989). Factorization and Primality Testing. In Undergraduate Texts in Mathematics. Springer New York. <https://doi.org/10.1007/978-1-4612-4544-5>
- [3] Crandall, Richard E., and Pomerance, Carl. Prime Numbers: A Computational Perspective. Springer, 2005.
- [4] Elliott, J. (2020). Harmonic numbers and the prime counting function (Version 3). arXiv. <https://doi.org/10.48550/ARXIV.2002.02188>
- [5] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. <https://doi.org/10.1145/359340.359342>
- [6] Alexander Walker, A Generalization of Wilson’s Theorem (due to Gauss), <https://awwalker.com/2017/02/05/a-generalization-of-wilsons-theorem-due-to-gauss/> viitattu 4.11.2025
- [7] Willans, C. P. (1964). On Formulae for the Nth Prime Number. The Mathematical Gazette, 48(366), 413–415. <https://doi.org/10.2307/3611701>

[8] <https://www.mersenne.org/> viitattu 3.11.2025