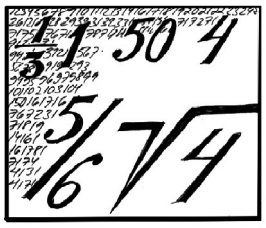

# Alkulukujen tiheydestä lukiolaisille

***Alex Karrila***
Matematiikan ja systeemianalyysin laitos, Aalto-yliopisto
alex.karrila@gmail.com

***Seppo J. Karrila***
Faculty of Science and Industrial Technology, Prince of Songkla University, Surat Thani, Thailand
seppo.karrila@gmail.com

**Tiivistelmä**

Tässä kirjoitelmassa todistetaan seuraavat alkulukujen tiheyttä lukusuoralla kuvailevat tulokset: Merkitään korkeintaan $N$:n suuruisten alkulukujen määrää $\pi(N)$. Tällöin kaikille $N \geq 2$ pätee

$$\pi(N) \leq (2\ln 2 + 1)\frac{N}{\ln N}. \tag{1}$$

Erityisesti siis alkulukujen osuus $\pi(N)/N$ kaikista kokonaisluvuista $N$:ään asti lähestyy nollaa kun $N$ kasvaa rajatta. Todistetaan myös alaraja alkulukujen tiheydelle: kaikille $N \geq 2$ pätee

$$\pi(N) \geq \frac{\ln 2}{2} \cdot \frac{N}{\ln N}. \tag{2}$$

Todistukset ovat toisistaan loogisesti riippumattomat. Kumpikaan ei vaadi logaritmia monimutkaisempia työkaluja, ja ne voisivat yhdessä tai erikseen soveltua esitettäväksi esimerkiksi lukiolaisesitelmään tai lukion lukuteorian kurssilla.

## Perusteita

Merkitään *luonnollisten lukujen joukkoa* $\{1, 2, 3, \ldots\}$ kirjaimella $\mathbb{N}$. Viitataan jatkossa muuttujamerkinnöillä $k$, $m$, $N$ ja $n$ aina $\mathbb{N}$-arvoiseen muuttujaan.

*Alkuluvut* $\mathbb{P} = \{2, 3, 5, 7, 11, 13, \ldots\}$ ovat yhtä suurempia luonnollisia lukuja, jotka ovat jaollisia vain itsellään ja ykkösellä. Alkulukumuuttujaa merkitään tässä kirjoitelmassa aina kirjaimella $p$ (engl. *prime number*).

*Alkulukulaskuri* $\pi : \mathbb{N} \to \mathbb{N} \cup \{0\}$ on funktio, jonka arvo pisteessä $N \in \mathbb{N}$ kertoo, kuinka monta korkeintaan $N$:n suuruista alkulukua on olemassa,

$$\pi(N) = \#\{p \in \mathbb{P} \ : \ p \leq N\}.$$

Esimerkiksi siis $\pi(6) = 3$ ja $\pi(11) = 5$.

Jo muinaiset kreikkalaiset tiesivät, että alkulukuja on äärettömän monta, eli

$$\pi(N) \longrightarrow \infty, \qquad \text{kun } N \to \infty,$$

ja Eukleideen todistus alkulukujen äärettömyydestä kuuluu lukion lukuteorian kurssin vakiomateriaaliin. Mutta miten nopeasti tai hitaasti alkulukulaskuri $\pi(N)$ kasvaa $N$:n mukana? Vaikuttaa esimerkiksi järkeenkäyvältä, että alkulukuja olisi (keskimäärin) aina vain harvemmassa, eli

$$\frac{\pi(N)}{N} \longrightarrow 0, \qquad \text{kun } N \to \infty. \tag{3}$$

Tässä artikkelissa todistetaan yhtälön (1) yläraja $\pi(N)$:lle, josta seuraa myös raja-arvo (3). Lisäksi todistetaan alaraja (2) $\pi(N)$:lle.

Epäyhtälöt (1)–(2) tunnetaan *Chebyshevin estimaattina*, ja ne ovat heikennetty versio *alkulukulauseesta*, joka toimi sadan vuoden ajan lukuteorian kehityksen pontimena. Sikäli onkin huomattavaa, että epäyhtälöiden (1)–(2) todistukset ovat suhteellisen yksinkertaiset. Tämän kirjoitelman tarkoituksena on tuoda näitä yksinkertaisia todistuksia yleisempään tietoisuuteen.

## Ylärajan (1) todistus

Tässä luvussa todistetaan tiivistelmässä esitelty epäyhtälö (1).

### Logaritminen alkulukukulaskuri

Todistuksessa avainasemassa on Chebyshevin theta-funktio, jota voidaan ajatella logaritmisesti painotettuna alkulukukulaskurina.

**Määritelmä 1.** Määritellään *Chebyshevin theta-funktio* $\vartheta : \mathbb{N} \to \mathbb{R}$ kaavalla

$$\vartheta(N) = \sum_{\substack{p\in\mathbb{P}\\ p\le N}} \ln p = \ln\left(\prod_{\substack{p\in\mathbb{P}\\ p\le N}} p\right). \tag{4}$$

Esimerkiksi siis $\vartheta(10) = \ln(2\cdot 3\cdot 5\cdot 7)$. Varsinaisen alkulukukulaskurin $\pi$ rajoittaminen epäyhtälössä (1) perustuu logaritmisen alkulukukulaskurin $\vartheta$ rajoittamiseen:

**Propositio 2.** *Kaikilla $N \in \mathbb{N}$ pätee*

$$\vartheta(N) \le (2\ln 2)N.$$

Erotetaan Proposition 2 todistuksesta seuraava aputulos.

**Lemma 3.** *Parillisille luvuille $(2m)$, $m \in \mathbb{N}$, pätee*

$$\prod_{\substack{p\in\mathbb{P}\\ m<p\le 2m}} p \le \binom{2m}{m} \le 2^{2m},$$

*ja parittomille luvuille $(2m+1)$ pätee*

$$2\prod_{\substack{p\in\mathbb{P}\\ m+1<p\le 2m+1}} p \le 2\binom{2m+1}{m+1} \le 2^{2m+1}.$$

*Todistus.* Parilliset luvut $2m$, vasen epäyhtälö: binomikerroin

$$\binom{2m}{m} = \frac{(2m)!}{m!m!}$$

on kokonaisluku. Sen alkutekijät voidaan päätellä tutkimalla kertomien $(2m)!$ ja $m!$ alkutekijöitä. Alkuluvut $p \in \mathbb{P}$, joille $m < p \le 2m$, ovat alkutekijöinä kertomassa $(2m)!$, ja ne eivät ole alkutekijöinä kertomassa $m!$. Näin ollen kaikki alkuluvut $p \in \mathbb{P}$, $m < p \le 2m$, ovat alkutekijöinä binomikertoimessa $\binom{2m}{m}$. Tämä todistaa vasemman epäyhtälön. Oikea epäyhtälö: $(2m)$:n alkion joukolla on $2^{2m}$ osajoukkoa ja $\binom{2m}{m}$ osajoukkoa, joissa on tasan $m$ alkiota.

Parittomat luvut $(2m+1)$: oikean epäyhtälön todistamiseksi huomataan, että

$$2\binom{2m+1}{m+1} = \frac{(2m+1)!}{(m+1)!m!} + \frac{(2m+1)!}{m!(m+1)!} = \binom{2m+1}{m+1} + \binom{2m+1}{m}.$$

Muilta osin todistus on kuten parillisille luvuille. □

*Proposition 2 todistus.* Induktio. Kun $N = 1$ saadaan $\vartheta(1) = 0$, eli väite pätee. Oletetaan, että väite pätee theta-funktiolle $\vartheta(\cdot)$ argumenteilla $1, 2, \ldots, (N-1)$ ja osoitetaan, että se pätee tällöin myös argumentilla $N$. Käsitellään parilliset ja parittomat $N$ erikseen. Parilliselle $N = 2m$ saadaan

$$\begin{aligned}
&\vartheta(2m) - \vartheta(m)\\
&(\text{Määritelmä 1}) = \ln\left(\prod_{\substack{p\in\mathbb{P}\\ m<p\le 2m}} p\right)\\
&(\text{Lemma 3}) \le \ln(2^{2m}) = 2m\ln 2.
\end{aligned}$$

Näin ollen saadaan $\vartheta(2m) \le \vartheta(m) + 2m\ln 2$, jolloin induktio-oletuksesta $\vartheta(m) \le (2\ln 2)m$ seuraa

$$\vartheta(N) = \vartheta(2m) \le 4m\ln 2 = (2\ln 2)N.$$

Parittomille $N = 2m+1$ todistus seuraa samaan tapaan tutkimalla erotusta $\vartheta(2m+1) - \vartheta(m+1)$. □

### Tavallinen alkulukukulaskuri

Proposition 2 mukaan logaritmisesti painotetun alkulukujen laskurin $\vartheta(N)$ kasvua rajoittaa suora $(2\ln 2)N$. Mitä tämä kertoo alkulukujen tiheydestä? Tutkitaan ensin vertailun vuoksi logaritmisen luonnollisten lukujen laskurin

$$S(N) = \sum_{n=1}^{N} \ln n$$

kasvua, joka on alla olevan proposition mukaan nopeampaa kuin minkään suoran $[vakio]\cdot N$.

**Propositio 4.** *Kaikille $N \in \mathbb{N}$ pätee*

$$S(N) \geq N \ln N - N.$$

*Todistus.* Verrataan summaa integraaliin:

$$\begin{aligned} S(N) &= \sum_{n=1}^{N} \ln n = \sum_{n=2}^{N} \ln n \\ &= \sum_{n=2}^{N} \int_{x=n-1}^{n} \ln n \; dx \\ &\geq \sum_{n=2}^{N} \int_{x=n-1}^{n} \ln x \; dx \\ &= \int_{x=1}^{N} \ln x \; dx \\ &= N \ln N - N + 1 \\ &\geq N \ln N - N. \end{aligned}$$

□

Yläraja (1) seuraa nyt suoraviivaisesti yhdistämällä Propositiot 2 ja 4.

**Lause 5.** *Kaikille $N \in \mathbb{N}$ pätee*

$$\pi(N) \ln N \leq (2 \ln 2 + 1)N.$$

*Todistus.* Tutkitaan erotusta

$$S(N) - \vartheta(N) = \sum_{\substack{n=1 \\ n \notin \mathbb{P}}}^{N} \ln n.$$

Yhtäältä y.o. logaritmisummassa on $N - \pi(N)$ termiä, kukin korkeintaan $\ln N$, joten

$$S(N) - \vartheta(N) \leq (N - \pi(N)) \ln N. \tag{5}$$

Toisaalta Propositioiden 2 ja 4 perusteella

$$S(N) - \vartheta(N) \geq N \ln N - N - (2 \ln 2)N. \tag{6}$$

Väite seuraa nyt yhdistämällä ylä- ja alarajat (5) ja (6). □

## Alarajan (2) todistus

Todistetaan alaraja (2).

**Lause 6.** *Kaikille $N \geq 2$ pätee*

$$\pi(N) \geq \frac{\ln 2}{2} \cdot \frac{N}{\ln N}.$$

Siinä missä ylärajan (1) todistuksen ydin, Lemma 3, oli alkulukujen logaritmien $\ln p$ rajoittaminen binomikertoimen logaritmilla $\ln \binom{2m}{m}$, perustuu alarajan (2) todistus $\ln \binom{2m}{m}$:n rajoittamiseen alkulukujen logaritmien $\ln p$ avulla.

Erotetaan todistuksesta kaksi aputulosta. Alla käytetään *lattiafunktiomerkintää* $\lfloor x \rfloor$, jolla tarkoitetaan reaaliluvulle $x$ suurinta kokonaislukua $\ell$, jolle $\ell \leq x$.

**Lemma 7.** *Kaikille $n \in \mathbb{N}$ pätee*

$$\ln(n!) = \sum_{\substack{p \in \mathbb{P} \\ p \leq n}} \left( \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots \right) \ln p.$$

Huomaa, että $\lfloor n/p^k \rfloor = 0$, kun $k$ on niin suuri, että $p^k > n$. Yllä sulkeissa olevat summat ovat siis ei-nollien termien $\lfloor n/p^k \rfloor$ summia, joissa $k$ on tarpeeksi pieni.

*Lemman 7 todistus.* Tutkitaan kertoman $n! = 1 \cdot 2 \cdot \ldots \cdot n$ alkutekijöitä sen tekijöiden $1, 2, \ldots, n$ avulla. Kaikki alkutekijät $p$ ovat korkeintaan $n$, joten saadaan

$$\ln(n!) = \sum_{\substack{p \in \mathbb{P} \\ p \leq n}} m_p \ln p,$$

jossa $m_p \in \mathbb{N}$ kertoo kuinka monta kertaa alkutekijä $p$ esiintyy $(n!)$:n alkulukuhajotelmassa. Kertoman $n!$ tekijöiden $1, 2, \ldots, n$ joukossa on $p$:llä jaollisia lukuja $\lfloor n/p \rfloor$ kappaletta, joista $p^2$:lla jaollisia on $\lfloor n/p^2 \rfloor$ kappaletta jne., joten saadaan

$$m_p = \left( \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots \right).$$

□

**Lemma 8.** *Kaikille $m \in \mathbb{N}$ ja $p \in \mathbb{P}$ pätee*

$$\begin{aligned} &\left( \left\lfloor \frac{2m}{p} \right\rfloor + \left\lfloor \frac{2m}{p^2} \right\rfloor + \ldots \right) - 2 \left( \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \ldots \right) \\ &\qquad \leq \frac{\ln(2m)}{\ln p}. \end{aligned} \tag{7}$$

*Todistus.* Erotus $\lfloor 2m/p^k \rfloor - 2 \lfloor m/p^k \rfloor$ on joko 1 tai 0, vastaten tapauksia, joissa reaaliluvun $m/p^k$ desimaalikehitelmän desimaaliosa on $\geq 0.5$ tai $< 0.5$. Toisaalta erotuksen kumpikin termi on nolla, jos pätee $p^k > 2m$. Erotus voi siis olla 1, vain jos pätee

$$p^k \leq 2m \Leftrightarrow k \leq \ln(2m)/\ln p.$$

Näin ollen summassa (7) on (sopivasti uudelleenjärjesteltynä) enintään $\ln(2m)/\ln p$ ei-nollaa termiä, kukin enintään 1. Väite seuraa. □

[1] Alaraja (8) ei ole tiukka suurille $m$. Arvioimalla kertomien logaritmeja ylhäältä ja alhaalta Proposition 4 tapaan saataisiin suurille $m$ parempi alaraja epäyhtälöön (8) ja siten myös epäyhtälöön (2).

*Lauseen 6 todistus.* Todistetaan ensin epäyhtälö parillisille luvuille $N = 2m$. Tutkitaan binomikerrointa $\binom{2m}{m}$. Yhtäältä saadaan[1]

$$\ln\binom{2m}{m} = \ln\left(\frac{2m}{m}\cdot\frac{2m-1}{m-1}\cdot\ldots\cdot\frac{m+1}{1}\right) \geq \ln(2^m) = m\ln 2. \tag{8}$$

Toisaalta yhdistämällä Lemmat 7 ja 8 saadaan

$$\begin{aligned}\ln\binom{2m}{m} &= \ln((2m)!) - 2\ln(m!)\\ \text{(Lemma 7)} &= \sum_{\substack{p\in\mathbb{P}\\ p\leq 2m}}\left(\left\lfloor\frac{2m}{p}\right\rfloor + \left\lfloor\frac{2m}{p^2}\right\rfloor + \ldots\right)\ln p\\ &\quad - \sum_{\substack{p\in\mathbb{P}\\ p\leq m}} 2\left(\left\lfloor\frac{m}{p}\right\rfloor + \left\lfloor\frac{m}{p^2}\right\rfloor + \ldots\right)\ln p\\ \text{(Lemma 8)} &\leq \sum_{\substack{p\in\mathbb{P}\\ p\leq m}}\frac{\ln(2m)}{\ln p}\ln p + \sum_{\substack{p\in\mathbb{P}\\ m<p\leq 2m}}\ln p\\ &\leq \pi(2m)\ln(2m); \end{aligned} \tag{9}$$

viimeisessä epäyhtälössä summattiin $\pi(2m)$ kappaletta korkeintaan $\ln(2m)$:n suuruisia termejä. Väite parilliselle $N = 2m$ seuraa nyt yhdistämällä yhtälöt (8) ja (9).

Parittomille luvuille $N \geq 3$ epäyhtälö seuraa, kun sen tiedetään pätevän parilliselle luvulle $(N+1)$:

$$\pi(N) = \pi(N+1) \geq \frac{\ln 2}{2}\cdot\frac{(N+1)}{\ln(N+1)} \geq \frac{\ln 2}{2}\cdot\frac{N}{\ln N};$$

yllä alussa käytettiin havaintoa, että $(N+1)$ ei parillisena lukuna ole alkuluku ja lopussa havaintoa, että funktio $x \mapsto x/\ln x$ on kasvava kun $x \geq 3$. □

## Kirjallisuutta ja historiaa

Chebyshev todisti ensimmäisenä yhtälöiden (1)–(2) tyyppiset ylä- ja alarajat alkulukulaskurille sekä esitteli theta-funktionsa vuonna 1852 [3]. Erilaisia moderneja, enemmän tai vähemmän tässä esitetyn kaltaisia todistuksia löytyy lukuisista lukuteorian oppimateriaaleista (esim. [1]).

Tämän artikkelin tuloksia vahvempi ja huomattavasti vaikeampi on *alkulukulause*

$$\frac{\pi(N)}{N/\ln N} \longrightarrow 1, \qquad \text{kun } N \to \infty,$$

joka voidaan muotoilla yhtäpitävästi (kts. esim. [1]) theta-funktion avulla

$$\frac{\vartheta(N)}{N} \longrightarrow 1, \qquad \text{kun } N \to \infty.$$

Esimerkiksi Proposition 2 mukaan siis $\vartheta(N)/N \leq 2\ln 2 \approx 1.4$ kaikilla $N$. Alkulukulauseen eri muotoiluja ennustivat tosiksi 1700-luvun lopulta alkaen esimerkiksi ajan suurimmat matemaatikot Legendre [6] ja Gauss [4]. Chebyshev tutki ongelmaa 1850-luvun alussa ja todisti estimaattinsa ja eräitä muita lukuteorian tuolloin avoimia kysymyksiä, mutta ei alkulukulausetta [2, 3]. Riemann taas kirjoitti aiheesta vuonna 1859, missä yhteydessä hän esitteli työkaluksi kuuluisan zeta-funktionsa [7]. Alkulukulause pysyi avoimena lopulta noin sata vuotta, kunnes vuonna 1896 de la Vallée Poussin [8] ja Hadamard [5] julkaisivat riippumattomat todistukset, molemmat perustuen Riemannin zeta-funktioon.

Alkulukujen jakautuminen lukusuoralle on yhä lukuteorian tutkimuksen ydinalueita. Esimerkiksi yksi lukuteorian suurimmista ratkaisemattomista ongelmista on todistaa *alkulukuparien konjektuuri*: jos merkitään $i$:nnettä alkulukua $p_i$, niin uskotaan olevan olemassa äärettömän monta peräkkäisten alkulukujen paria $(p_i, p_{i+1})$, joille $(p_{i+1} - p_i) = 2$, kuten $(3,5)$, $(5,7)$ tai $(41,43)$. Huomaa, että yhdistämällä epäyhtälöt (1) ja (2) saadaan $\pi(7N) - \pi(N) > 0$ kaikilla tarpeeksi suurilla $N$; toisin sanoen $(p_{i+1} - p_i) \leq 6p_i$ kaikilla tarpeeksi suurilla $i$. Toisaalta raja-arvosta (3) seuraa, että mille tahansa $m$ on olemassa peräkkäisten alkulukujen pareja $(p_i, p_{i+1})$, joille $(p_{i+1} - p_i) \geq m$.

Suomalainen lukuteorian tutkimus on saanut viime aikoina kansainvälistä tunnustusta, kenties huomattavimpana Kaisa Matomäen syksyllä 2018 saama New Horizons in Mathematics -palkinto. Lukuteorian tutkimusta ja opetusta eri painotuksilla löytyy useimmilta suomalaisilta matematiikan laitoksilta.

## Viitteet


[1] T. M. Apostol. *Introduction to analytic number theory* (luvut 4.4–4.5), 1976.

[2] P. L. Chebyshev. Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donnée. *J. math. pures appl.*, nro 17, 1852.[2]

[3] P. L. Chebyshev. Mémoire sur les nombres premiers. *J. math. pures appl.*, nro 17, 1852.[3]


[2] Saatavilla: `https://archive.org/details/oeuvresdepltche01chebrich/page/n39`

[3] Saatavilla: `https://archive.org/details/oeuvresdepltche01chebrich/page/n61`

[4] Saatavilla: `https://gdz.sub.uni-goettingen.de/id/PPN236018647`

[4] Gaussin omista muistiinpanoista löytyvä muotoilu, väitetysti jo vuodelta 1791, mainitaan Gaussin kootuissa teoksissa. C. F. Gauss. *Werke* (nidos 10, sivu 11), 1863.[4]

[5] J. Hadamard. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bull. Soc. Math. France*, nro 24, 1896.[5]

[6] A. M. Legendre. *Essai sur la théorie des nombres* (osa 4, luku 8), 1808.[6]

[7] B. Riemann. Über die Anzahl der Primzahlen unter einer gegebener Größe. *Monatsberichte der Berliner Akademie*, marraskuu 1859.[7]

[8] C. J. de la Vallée Poussin. Recherches analytiques sur la théorie des nombres: Première partie: La fonction $\zeta(s)$ de Riemann et les nombres premiers en général. *Ann. Soc. scient. Bruxelles*, nro 20, 1896.[8]

[5] Saatavilla: `http://www.numdam.org/article/BSMF_1896__24__199_1.pdf`

[6] Saatavilla: `https://gallica.bnf.fr/ark:/12148/bpt6k42612x/f80.image.texteImage`

[7] Saatavilla: `https://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/`

[8] Saatavilla: `https://archive.org/details/recherchesanaly00pousgoog/page/n9`