Aritmeettinen derivaatta

Veera Rosama

Matematiikan pro gradu -tutkielma

Helsingin yliopisto
Matematiikan ja tilastotieteen laitos
Syksy 2013

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto Fakultet/Sektion – Faculty	Laitos/Institution– Department	
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos	
Tekijä/Författare – Author		
Rosama Veera		
Työn nimi / Arbetets titel – Title		
Aritmeettinen derivaatta		
Oppiaine /Läroämne – Subject		
Matematiikka		
Työn laji/Arbetets art – Level	Aika/Datum – Month and year	Sivumäärä/ Sidoantal – Number of pages
Pro-gradu tutkielma	9.12.2013	28

Tiivistelmä/Referat – Abstract

Tutkielman tarkoituksena on tutkia aritmeettista derivaattaa. Aritmeettinen derivaatta on määritelty vasta muutamia kymmeniä vuosia sitten, vaikka sen alkuperä saattaa hyvinkin olla kaukana historiassa. Luvun n aritmeettinen derivaatta n' perustuu luvun alkutekijöihin jakoon. Alun perin aritmeettisessa derivaatassa on ollut kyse juuri luonnollisten lukujen ominaisuuksista ja jaosta alkutekijöihin. Tekijöihin jaon avulla voidaan selvittää yksiselitteinen muoto derivaatan lausekkeelle ja laajentaa tätä koskemaan myös negatiivisia kokonaislukuja. Myöhemmin käsitettä on laajennettu koskemaan sekä rationaalilukuja, että joitain irrationaalilukuja.

Tutkielman alussa esitellään yleisiä määritelmiä, joita käytetään myöhemmin hyväksi. Tämän jälkeen määritellään aritmeettinen derivaatta luonnollisilla luvuilla käyttäen hyväksi Leibnizin sääntöä tulon derivaatalle. Määrittelyn jälkeen tutkitaan aritmeettisen derivaatan ominaisuuksia. Luvussa tutkitaan myös osamäärän derivaattaa sekä laajennetaan määritelmä negatiivisille kokonaisluvuille.

Seuraavassa luvussa on tarkoitus laajentaa aritmeettisen derivaatan määritelmää koskemaa myös rationaalilukuja. Luvussa löydetään yleinen laskukaava aritmeettisen derivaatan laskemiselle sekä pohditaan myös raja-arvon $\lim_{x\to a} x'$ olemassaoloa. Määritelmän laajennusta jatketaan logaritmin derivaattaan, potenssien derivaattaan sekä myös joidenkin irrationaalilukujen derivaattaan.

Viimeisissä luvuissa keskitytään aritmeettisen derivaatan soveltamiseen. Ensin tutkitaan eräitä differentiaaliyhtälöitä ja keskitytään lähinnä ratkaisuiden lukumäärien selvittämiseen. Lopuksi esitellään kaksi käsitettä: Sophie Germainin alkuluku ja Cunninghamin ketju. Näiden kahden ominaisuuksia valotetaan hieman aritmeettisen derivaatan avulla. Viimeisenä tutkielmassa esitellään vielä muutama avoin tutkimusongelma.

Avainsanat – Nyckelord – Keywords

Aritmeettinen derivaatta, alkuluku, Sophie Germainin alkuluku, Cunninghamin ketju

Säilytyspaikka – Förvaringställe – Where deposited

Kumpulan kampuskirjasto

Muita tietoja – Övriga uppgifter – Additional information

Sisältö

1. Johdanto

Tämän tutkielman tarkoituksena on tutkia aritmeettista derivaattaa. Aritmeettinen derivaatta on määritelty vasta muutamia kymmeniä vuosia sitten, vaikka sen alkuperä saattaa hyvinkin olla kaukana historiassa. Luvun n aritmeettinen derivatta n' perustuu vahvasti luvun alkutekijöihin. Alunperin on nimenomaan ollut kyse luonnollisten lukujen ominaisuuksista ja jaosta alkutekijöihin. Tekijöihin jaon avulla voidaan selvittää yksiselitteinen muoto derivaatan lausekkeelle ja laajentaa tätä koskemaan myös negatiivisia kokonaislukuja. Myöhemmin käsitettä on laajennettu koskemaan sekä rationaalilukuja, että joitain irrationaalilukuja.

Tutkielman alussa esitellään yleisiä määritelmiä, joita käytetään myöhemmin hyväksi. Tämän jälkeen määritellään aritmeettinen derivaatta luonnollisilla luvuilla sekä tutkitaan aritmeettisen derivaatan ominaisuuksia. Luvussa tutkitaan myös osamäärän derivaattaa sekä negatiivisten kokonaislukujen derivointia.

Seuraavassa luvussa on tarkoitus laajentaa aritmeettisen derivaatan määritelmää koskemaan myös rationaalilukuja. Luvussa pohditaan myös raja-arvon $\lim_{x\to a} x'$ olemassaoloa. Määritelmän laajennusta jatketaan logaritmin derivaattaan, potenssien derivaattaan sekä joidenkin irrationaalilukujen derivaattaan. Tarkoituksena on myös tutkia ratkaisuja joihinkin differentiaaliyhtälöihin ja keskittyä nimenomaan ratkaisuiden lukumäärien selvittämiseen.

Lopussa on vielä tarkoituksena tutkia Sophie Germainin lukujen ja Cunninghamin ketjujen ominaisuuksia aritmeettisen derivaatan avulla. Viimeisenä pohditaan vielä avoimia ongelmia.

2. Yleistä

Luvussa esitellään tutkielmassa yleisesti käytettyjä ominaisuuksia ja määritelmiä. Tutkielman läpi luonnollisten lukujen symbolilla $\mathbb{N}$ tarkoitetaan lukujoukkoa $\{0, 1, 2, ...\}$.

2.1. Alkuluvut. Alkuluku p on luonnollinen luku $p > 1$, joka ei ole jaollinen muilla positiivisilla kokonaisluvuilla kuin luvuilla 1 ja p. Vastaavasti ne positiiviset kokonaisluvut, jotka eivät ole alkulukuja, ovat yhdistettyjä lukuja. Luvun 1 alkulukuihin kuulumisesta on historian saatossa käyty kiivasta keskustelua. Loppujen lopuksi luvun 1 ei katsota kuuluvan alkulukuihin, sillä alkuluvuilla on useita ominaisuuksia, joita luvulla 1 ei ole. Alkulukuja on loputon määrä, eli ne muodostavat jonon $2, 3, 5, 7, 11, \ldots$

2.2. Luvun alkutekijöihin jako. Jokainen yhdistetty luku voidaan jakaa alkulukutekijöihinsä. Yhdistetty luku voidaan siis ilmoittaa kahden tai useamman alkuluvun tulona. Esimerkiksi yhdistetty luku 8 voidaan esittää tulona $2 \cdot 2 \cdot 2$, missä kaikki kolme lukua ovat alkulukuja. Puolialkuluku on yhdistetty luku, joka voidaan esittää tulona kahdesta alkuluvusta. Esimerkiksi luku 6 on puolialkuluku, sillä se voidaan esittää tulona $2 \cdot 3$. Mitään yksinkertaista alkutekijöihinjakoalgoritmia ei ole olemassa. Vaikeimpia alkutekijöihin jaettavia lukuja ovat suuret puolialkuluvut, sillä kahden tarpeeksi suuren alkuluvun metsästäminen voi kestää kauan.

2.3. Ryhmä. Ryhmä on algebrallinen systeemi, jossa on määritelty yksi laskutoimitus.

Määritelmä 1. Olkoon G epätyhjä joukko. Paria $(G, \circ)$ sanotaan ryhmäksi, jos seuraavat ehdot ovat voimassa:

G0. $\circ$ on joukossa G määritelty laskutoimitus, ts. $a \circ b \in G \qquad \forall a, b \in G$;
G1. $(a \circ b) \circ c = a \circ (b \circ c) \qquad \forall a, b, c \in G \qquad$ (liitäntälaki);
G2. on olemassa sellainen G:n alkio e (ns. neutraalialkio), että

$$e \circ a = a \circ e = a \quad \forall a \in G;$$

G3. jokaista G:n alkiota a kohti on olemassa sellainen G:n alkio a^{-1} (ns. käänteisalkio), että

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Jos lisäksi laskutoimitus on kommutatiivinen, eli vaihdannainen, sanotaan että $(G, \circ)$ on kommutatiivinen ryhmä eli Abelin ryhmä.

Jäännösluokat $\mod m$ muodostavat additiivisen Abelin ryhmän $(\mathbb{Z}_m, +)$, kun yhteenlasku määritellään $\overline{a} + \overline{b} = \overline{a + b}$. Nolla-alkiona on $\overline{0}$ ja alkion $\overline{a}$ vasta-alkiona $\overline{-a}$.

Esimerkki 2. Ryhmä $\mathbb{Z}_3$ on siis joukko $\{\overline{0}, \overline{1}, \overline{2}\}$. Yhteenlasku toimii siis $\overline{2} + \overline{0} = \overline{2}$ ja $\overline{2} + \overline{1} = \overline{3} = \overline{0}$.

Alkion sanotaan virittävä ryhmän, jos kaikki ryhmän jäsenet voidaan lausua kyseisen alkion monikertoina. Eli äskeisen esimerkin ryhmän virittää esimerkiksi alkio $\overline{1}$, sillä $\overline{2} = \overline{1} + \overline{1}$ ja $\overline{0} = \overline{1} + \overline{1} + \overline{1}$.[**4**]

2.4. Rengas. Rengas on nyt kahden laskutoimituksen systeemi.

Määritelmä 3. Kolmikkoa $(R, +, \cdot)$ sanotaan renkaaksi, jos se täyttää ehdot:

R1. $(R, +)$ on Abelin ryhmä;

R2. kertolasku $\cdot$ on joukossa R määritelty laskutoimitus;
R3. $a(bc) = (ab)c \quad \forall a, b, c \in R$;
R4. joukossa R on sellainen alkio 1, että

$$a \cdot 1 = 1 \cdot a = a \qquad \forall a \in \mathbb{R};$$

R5. $a(b + c) = ab + ac, \quad (a + b)c = ac + bc \quad \forall a, b, c \in R.$

Jos kertolasku on lisäksi kommutatiivinen, sanotaan, että R on kommutatiivinen rengas.[**5**]

2.5. Bertrandin postulaatti. Bertrandin postulaatti on lause, jonka mukaan jokaiselle positiiviselle kokonaisluvulle $n > 3$ on olemassa ainakin yksi alkuluku p, jolle pätee

$$n < p < 2n - 2.$$

Heikompi muotoilu tästä on, että jokaiselle positiiviselle kokonaisluvulle $n > 1$ on olemassa ainakin yksi alkuluku p, jolle pätee

$$n < p < 2n.$$

Yksi Bertrandin postulaatin seurauksia on, että alkuluvut mukaanlukien luku 1 muodostavat täydellisen jonon. Jokainen positiivinen kokonaisluku voidaan esittää summana alkuluvuista ja luvusta 1 käyttäen jokaista lukua aina vain kerran.

3. Aritmeettinen derivaatta

Tässä luvussa määritellään arimeettinen derivaatta, sekä osoitetaan, että derivaatta on hyvinmääritelty.

Määritelmä 4. Aritmeettinen derivaatta $n' : \mathbb{N} \to \mathbb{N}$ määritellään käyttäen kahta pääsääntöä, joissa p olkoon mikä tahansa alkuluku sekä a ja b mitä tahansa luonnollisia lukuja. Tällöin

$$p' = 1 \text{ ja } (ab)' = a'b + ab'.$$

Jälkimmäinen aritmeettisen derivaatan määritelmän säännöistä tunnetaan paremmin Leibnizin sääntönä.

Esimerkki 5. Määritetään luvun 8 aritmeettinen derivaatta.

$$\begin{aligned} 8' &= (4 \cdot 2)' = 4' \cdot 2 + 4 \cdot 2' = (2 \cdot 2)' \cdot 2 + 4 \cdot 1 \\ &= (2' \cdot 2 + 2 \cdot 2') \cdot 2 + 4 = (2 + 2) \cdot 2 + 4 = 8 + 4 = 12. \end{aligned}$$

Lause 6. *$1' = 0$ sekä $0' = 0$.*

Todistus. Käytämme hyväksi todistuksessa Leibnizin sääntöä, jonka perusteella

$$1' = (1^2)' = (1 \cdot 1)' = 1 \cdot 1' + 1' \cdot 1 = 2 \cdot 1' \Leftrightarrow 1' = 0,$$

$$0' = (2 \cdot 0)' = 2 \cdot 0' + 2' \cdot 0 = 2 \cdot 0' \Leftrightarrow 0' = 0.$$

□

Seuraavaksi tulee todistaa, että aritmeettinen derivaatta on hyvinmääritelty.

Lause 7. *Derivaatta n' on hyvinmääritelty jos ja vain jos pätee: kun*

$$n = \prod_{i=1}^{k} p_i^{n_i} \text{ on alkutekijöihinsä jaettu luonnollinen luku, niin}$$

$$n' = n \sum_{i=1}^{k} \frac{n_i}{p_i}.$$

TODISTUS. Jotta derivaatta on hyvinmääritelty, tulee sen olla yksiselitteisesti määritelty. Koska $1' = 0$, pitää enää todistaa, että yhtälö $n' = n \sum_{i=1}^{k} \frac{n_i}{p_i}$ on johdonmukainen.

Tätä varten todistetaan lause.

LAUSE 8. *Ratkaisut funktionaaliseen yhtälöön* $L : \mathbb{N} \to S$,

$$L(a) + L(b) = L(ab),$$

jossa S *on mielivaltainen rengas, jonka laskutoimituksina on* $+$ *ja* $\cdot$, *saadaan muodossa*

$$L(n) = \sum_{i=1}^{k} \alpha f(p_i),$$

missä $f : \mathbb{P} \to S$ *on mikä tahansa funktio alkuluvuilta* S*:lle.*

TODISTUS. Ensin osoitetaan, että jokainen yhtälön $L(a) + L(b) = L(ab)$ ratkaisu on muotoa $L(n) = \sum_{i=1}^{k} \alpha f(p_i)$.

L:n määritelmästä seuraa, että $L(\prod_{i=1}^{k} a_i) = \sum_{i=1}^{k}(a_i)$ sekä $L(a^b) = bL(a)$. Olkoon $n = \prod_{i=1}^{k} p_i^{\alpha_1}$ mielivaltainen kokonaisluku. Nyt

$$L(n) = L(\prod_{i=1}^{k} p_i^{\alpha_1}) = \sum_{i=1}^{k} L(p_i^{\alpha_1}) = \sum_{i=1}^{k} \alpha_i L(p_i).$$

Määritellään $f : \mathbb{P} \to Sf(p) = L(p)$ jokaiselle alkuluvulle p. Tällöin $L(n) = \sum_{i=1}^{k} \alpha_i f(p_i)$.

Seuraavaksi osoitetaan, että jokaiselle funktiolla $f : \mathbb{P} \to S$ on olemassa $L(n) = \sum_{i=1}^{k} \alpha_i f(p_i)$ ratkaisuna yhtälöön $L(a) + L(b) = L(ab)$.

Olkoon $a = \prod_{i=1}^{k} p_i^{\alpha_1}$ ja $b = \prod_{i=1}^{k} p_i^{\beta_1}$ yhtälössä $L(a)+L(b) = L(ab)$.Tällöin

$$
\begin{aligned}
L(a) + L(b) &= L(\prod_{i=1}^{k} p_i^{\alpha_1}) + L(\prod_{i=1}^{k} p_i^{\beta_1}) = \sum_{i=1}^{k} L(p_i^{\alpha_i}) + \sum_{i=1}^{k} L(p_i^{\beta_i}) \\
&= \sum_{i=1}^{k} \alpha_i L(p_i) + \sum_{i=1}^{k} \beta_i L(p_i) = \sum_{i=1}^{k} (\alpha_i + \beta_i) L(p_i) \\
&= \sum_{i=1}^{k} (\alpha_i + \beta_i) f(p_i) = L(\prod_{i=1}^{k} p_i^{\alpha_i+\beta_i}) = L(ab).
\end{aligned}
$$

Siis saimme yksikäsitteisen ratkaisun. □

Nyt siis meillä on yksikäsitteinen määritelmä derivaatalle, eli määrittelemämme funktio on hyvinmääritelty. □

Nyt kun tiedetään, että aritmeettinen derivaatta voidaan laskea kaavalla $n' = n \sum_{i=1}^{k} \frac{n_i}{p_i}$, voimme laskea alun esimerkin uudelleen.

Esimerkki 9.

$$8' = (2^3)' = 8 \cdot \frac{3}{2} = 12.$$

4. Ominaisuuksia

Seuraavaksi tutkitaan aritmeettisen derivaatan ominaisuuksia. Tärkeää aritmeettisessa derivaatassa on huomata, että lineaarisuus ei päde yleisesti. Joillakin yksittäistapauksilla pätee $(a+b)' = a' + b'$, mutta yleisesti yhtälö ei pidä paikkaansa. Helppo esimerkki lineaarisuuden puuttumisesta on

$$\begin{aligned} (2+3)' &= 5' = 1 \\ 2' + 3' &= 1 + 1 = 2. \end{aligned}$$

Lineaarisuuden puuttumisesta seuraa myös se, että $(ab)'' \neq a'' + 2a'b' + b''$. Tutkitaan siis ensiksi, mitä lineaarisuuden voimassaolosta seuraa.

Lause 10. *Jos $(a+b)' = a' + b'$, niin kaikille $k \in \mathbb{N}$ pätee $(ka+kb)' = (ka)' + (kb)'$.*

Todistus. Oletetaan $(a+b)' = a' + b'$. Tällöin

$$\begin{aligned} (ka+kb)' &= (k(a+b))' = k'(a+b) + k(a+b)' = k'a + k'b + k(a+b)' \\ &= k'a + k'b + ka' + kb' = k'a + ka' + k'b + kb' = (ka)' + (kb)'. \end{aligned}$$

□

Sama pätee myös epäyhtälöille sekä voimme laajentaa ne koskemaan lineaarikombinaatioita,

$$(a+b)' \geq a' + b' \Rightarrow (ka+kb)' \geq (ka)' + (kb)',$$

$$(a+b)' \leq a' + b' \Rightarrow (ka+kb)' \leq (ka)' + (kb)',$$

$$(\sum \gamma_i a_i)' = \sum \gamma_i (a_i)' \Rightarrow (k \sum \gamma_i a_i)' = \sum \gamma_i (ka_i)'.$$

Näiden todistaminen noudattaa edellisen lauseen todistuksen kaavaa.

Tästä on suoraan johdettavissa seurauksia.

Seuraus 11. $(3k)' = k' + (2k)'$, $(2k)' \leq 2k'$, $(5k)' \neq (2k)' + (3k)'$, $(5k)' = (2k)' + 3k'$.

Lause 12. *Kaikille $k > 1, k \in \mathbb{N}$, jos $n' \geq n$, niin $(kn)' > kn$.*

TODISTUS. Olkoon $k > 1, k \in \mathbb{N}$ ja $n' \geq n$. Nyt

$$(kn)' = k'n + kn' > kn' \geq kn.$$

$\square$

LAUSE 13. *Kun $n' \geq n$, niin kaikille luonnollisille luvuille $k > 1$ pätee $(kn)' > kn$.*

TODISTUS. Oletetaan $n' \geq n$ ja $k > 1$. Nyt $(kn)' = k'n + kn' > kn' \geq kn$. $\square$

LAUSE 14. *Jos $n = p^p m$, missä p on alkuluku ja $m \in \mathbb{N}$ ja $n > 1$, niin $n' = p^p(m + m')$ ja $\lim_{k\to\infty} n^{(k)} = \infty$.*

TODISTUS. Oletetaan, että $n = p^p m$. Nyt Leibnizin säännön sekä lauseen 7 mukaan

$$n' = (p^p)'m + p^p m' = p^p \cdot \frac{p}{p} m + p^p m' = p^p(m + m').$$

Alkuoletusten mukaisesti $n > 1$ sekä $k \geq 1$. Nyt on selkeästi nähtävissä, että $n \leq n'$ sekä yleisemmin $n^{(k)} \geq n + k$. $\square$

Lause pätee siis, jos alkuluvun p eksponentti on sama kuin luku itse. Helposti on kuitenkin huomattavissa, että sitä voidaan soveltaa tilanteeseen, jossa eksponentti on suurempi kuin luku itse. Tutkitaan siten tapausta, jossa p:n eksponentti on pienempi kuin itse luku.

LAUSE 15. *Olkoon luonnollinen luku n jaollinen luvulla p^k, missä p on alkuluku ja k on p:n suurin mahdollinen potenssi, $0 < k < p$. Tällöin n' on* *jaollinen luvulla p^{k-1} ja $k-1$ on p:n suurin mahdollinen potenssi, jolla tämä pätee. Lisäksi kaikki luvut $n, n', n'', \ldots, n^{(k)}$ ovat eri lukuja.*

TODISTUS. Olkoon $n = p^k m$. Nyt

$$n' = kp^{k-1}m + p^k m' = p^{k-1}(km + pm').$$

Selkeästi n' on jaollinen luvulla p^{k-1}. Termi $km + pm'$ ei ole jaollinen luvulla p, sillä $0 < k < p$, joten $k-1$ on suurin mahdollinen p:n potenssi, jolla n' on jaollinen. □

Seuraavaksi tutkitaan negatiivisten kokonaislukujen derivointia.

MÄÄRITELMÄ 16. Negatiivisen kokonaisluvun aritmeettinen derivaatta lasketaan säännöllä $(-n)' = -(n')$, missä $n \in \mathbb{N}$.

LAUSE 17. *Aritmeettinen derivaatta on yksiselitteisesti määritelty koko kokonaislukujen joukossa.*

TODISTUS. Aloitetaan todistaminen selvittämällä luvun -1 derivaatta. Käytetään hyväksi tietoa, että $(-1)^2 = 1$ sekä lausetta 6, joiden mukaan

$$(-1)^2 = 1 \Rightarrow ((-1)^2)' = 1' \Leftrightarrow 2 \cdot (-1) \cdot (-1)' = 0 \Leftrightarrow (-1)' = 0.$$

Käytetään tätä tietoa nyt hyväksi negatiivisten kokonaislukujen derivoinnissa. Olkoon k positiivinen kokonaisluku. Tällöin

$$(-k)' = (-1 \cdot k)' = (-1)'k + (-1)k' = 0 + (-1)k' = -(k').$$

Näin ollen siis aritmeettinen derivaatta on pariton funktio. □

Seuraavaksi tutkitaan osamäärän derivointisääntöä. Jos haluamme Leibnizin säännön pätevän kokonaisvaltaisesti, tulee myös osamäärän derivointisäännön olla voimassa.

Lause 18. $(\frac{a}{b})' = \frac{a'b-ab'}{b^2}$.

Todistus. Lauseen 6 mukaan $1' = 0$. Oletetaan, että $n \neq 0$. Nyt

$$(\frac{n}{n})' = 1' \Leftrightarrow (n \cdot \frac{1}{n})' = 0 \Leftrightarrow n' \cdot \frac{1}{n} + n \cdot (\frac{1}{n})' = 0,$$

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

Näin ollen saamme

$$(\frac{a}{b})' = a' \cdot \frac{1}{b} + a \cdot (\frac{1}{b})' = \frac{a'}{b} - \frac{ab'}{b^2} = \frac{a'b}{b^2} - \frac{ab'}{b^2} = \frac{a'b-ab'}{b^2}.$$

Osamäärän derivaatan tulee olla myös yksiselitteisesti määrätty, joten tutkitaan, onko äskeisen lauseen derivaatta hyvinmääritelty. Tämä tehdään osoittamalla, että $(\frac{ac}{bc})' = (\frac{a}{b})'$. Nyt

$$\begin{aligned}
(\frac{ac}{bc})' &= \frac{(ac)'bc - ac(bc)'}{(bc)^2} = \frac{(a'c+ac')bc - ac(b'c+bc')}{(bc)^2} \\
&= \frac{a'bc^2 + abcc' - ab'c^2 - abcc'}{(bc)^2} = \frac{c^2(a'b-ab')}{b^2c^2} \\
&= \frac{a'b-ab'}{b^2} = (\frac{a}{b})'.
\end{aligned}$$

Näin ollen siis myös osamäärän derivaatta on hyvinmääritelty. $\square$

5. Aritmeettisen derivaatan laajennukset

Tutkitaan vielä lisää aritmeettisen derivaatan ominaisuuksia. Laajennetaan sen käsitettä rationaaliluvuille, logaritmin derivaatalle, potenssin derivoinnille sekä joillekin irrationaaliluvuille.

5.1. Rationaaliluvun derivaatta. Aloitetaan positiivisista rationaaliluvuista. Helpointa on määritellä rationaaliluvun derivaatta Lauseen 7 osoittamalla tavalla.

Määritelmä 19. Olkoon $x = \prod_{i=1}^{k} p_i^{x_i}$ rationaaliluvun x jako alkutekijöihin, jossa jotkut eksponentit x_i voivat olla negatiivisia. Nyt

$$x' = x \sum_{i=1}^{k} \frac{x_i}{p_i}$$

Esimerkki 20.

$$\frac{1}{6} = \frac{1}{2} \cdot \frac{1}{3} = 2^{-1} \cdot 3^{-1},$$

$$(\frac{1}{6})' = \frac{1}{6}(\frac{-1}{2} + \frac{-1}{3}) = \frac{1}{6}(-\frac{3}{6} - \frac{2}{6}) = \frac{1}{6} \cdot (-\frac{5}{6}) = -\frac{5}{36}.$$

Tutkitaan nyt rationaaliluvun derivaatan ominaisuuksia. Tavoitteena on osoittaa, että rationaaliluvun derivaatta on rajoittamaton. Aloitetaan todistamalla, että aritmeettinen derivaatta on epäjatkuva jokaisessa pisteessä.

Lause 21. *Jokaiselle alkuluvulle $p > 3$ pätee $(\frac{p}{p+1})' < 0$ ja $(\frac{p-1}{p})' > \frac{1}{2}$.*

Todistus. Aloitetaan todistaminen jälkimmäisestä osasta. Käytetään osamäärän derivaattaa hyväksi,

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

Koska $p > 3$, niin $p-1$ on parillinen. Nyt siis $p-1 = 2m, m > 1$, joten

$$(p-1)' = (2m)' = 2'm + 2m' \geq m + 2 = \frac{p-1}{2} + 2.$$

Nyt siis $(p-1)' \geq \frac{p-1}{2} + 2$, joten

$$(\frac{p-1}{p})' = \frac{p(p-1)' - (p-1)p'}{p^2} \geq \frac{p(\frac{p-1}{2}+2) - (p-1)}{p^2} = \frac{p^2 - p + 2p + 2}{2p^2}$$

$$= \frac{p^2 + p + 2}{2p^2} > \frac{p^2}{2p^2} = \frac{1}{2}.$$

Siis $(\frac{p-1}{p})' > \frac{1}{2}$.

Seuraavaksi todistetaan lauseen ensimmäinen osa. Käytetään myös tässä hyödyksi osamäärän derivaattaa,

$$(\frac{p}{p+1})' = \frac{(p+1)p' - p(p+1)'}{(p+1)^2}.$$

Edelleen $p+1$ on parillinen, joten samalla päättelyketjulla kuin yllä $(p+1)' > \frac{p+1}{2} + 2 > \frac{p+1}{2}$ ja

$$(\frac{p}{p+1})' = \frac{(p+1)p' - p(p+1)'}{(p+1)^2} < \frac{(p+1) - p\frac{p+1}{2}}{(p+1)^2}.$$

Ottaen huomioon alkuoletuksen $p > 3$ saadaan $\frac{p}{2} > 1$, joten $\frac{p}{2}(p+1) > (p+1)$. Näin ollen

$$(\frac{p}{p+1})' < \frac{(p+1) - p\frac{p+1}{2}}{(p+1)^2} < 0.$$

Näin ollen siis, kun $p > 3$, pätee $(\frac{p}{p+1})' < 0$ ja $(\frac{p-1}{p})' > \frac{1}{2}$. $\square$

Käytetään nyt edellistä lausetta hyväksi ja todistetaan rationaaliluvun aritmeettinen derivaatta rajoittamattomaksi, kun rationaaliluku x lähestyy toista rationaalilukua a.

LAUSE 22. $\lim_{x\to a} x'$ *ei ole olemassa millään* $a \in \mathbb{Q}$.

TODISTUS. Määritelmän 16 mukaan $(-x)' = -x'$, joten voidaan rajoittautua tutkimaan pelkästään ei-negatiivisia lukuja. Lauseen 21 mukaan nyt siis pätee $(\frac{p}{p+1})' < 0$ ja $(\frac{p-1}{p})' > \frac{1}{2}$, kun $p > 3$. Otetaankin tutkittavaksi luvut $a\frac{p-1}{p}$ ja $a\frac{p}{p+1}$. Havaitaan heti, että kun p kasvaa rajatta, molemmat luvut lähestyvät arvoa a. Tällöin

$$\lim_{p\to\infty}(a\frac{p-1}{p})' = \lim_{p\to\infty}(a'\frac{p-1}{p} + (\frac{p-1}{p})'a) > \lim_{p\to\infty}(a'\frac{p-1}{p} + \frac{1}{2}a) = a' + \frac{1}{2}a$$

ja

$$\lim_{p\to\infty}(a\frac{p}{p+1})' = \lim_{p\to\infty}(a'\frac{p}{p+1} + a(\frac{p}{p+1})') < \lim_{p\to\infty} a'\frac{p}{p+1} = a'.$$

Näin ollen siis yleistettynä saadaan $\lim_{x\to a} x' > a' + \frac{1}{2}a$ ja $\lim_{x\to a} x' < a'$. Tästä nähdään suoraan, että raja-arvoa ei ole olemassa, kun $a \neq 0$. Osoitetaan vielä, että raja-arvoa $\lim_{x\to 0} x'$ ei ole olemassa. Määritellään kaksi funktiota $\mathbb{Z}_+ \to \mathbb{Z}_+$:

$$\begin{aligned} a(x) &= \log_2(2 + \sum_{k=1}^{x}\frac{1}{p_k}), \text{ missä } p_i \text{ on i:nnes alkuluku,} \\ p(x) &= \text{pienin alkuluku, joka on suurempi kuin } a(x)\textstyle\prod_{m=1}^{x} p_m. \end{aligned}$$

$p(x)$:lle pätee näin ollen $a(x)\prod_{m=1}^{x} p_m \leq p(x) < 2a(x)\prod_{m=1}^{x} p_m$. Tämä pätee, sillä Bertrandin postulaatin mukaisesti lukujen n ja $2n$ välistä löytyy aina alkuluku. Huomataan myös, että sarja $\sum_{k=0}^{x}\frac{1}{p_k}$ hajaantuu. Näin ollen $\lim_{x\to\infty} a(x) = \infty$.

Tutkitaan nyt jonoa, jonka yleinen termi on

$$\frac{\prod_{m=1}^{x} p_m}{p(x)}.$$

Havaitaan, että tämä jono lähestyy lukua 0, kun x:ää kasvatetaan rajatta. Koska $a(x)\prod_{m=1}^{x} p_m \leq p(x) < 2a(x)\prod_{m=1}^{x} p_m$, pätee nyt

$$\lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{2a(x)\prod_{m=1}^{x} p_m} \leq \lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{p(x)} < \lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{a(x)\prod_{m=1}^{x} p_m},$$

$$\lim_{x\to\infty} \frac{1}{2a(x)} \leq \lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{p(x)} < \lim_{x\to\infty} \frac{1}{a(x)}.$$

Havaitaan siis, että jonoa molemmin puolin rajoittavat funktiot lähestyvät molemmat lukua 0, jolloin myös jono itse lähestyy lukua 0, kun x kasvaa rajatta.

Määritelmän 19 mukaan voidaan luoda jonon yleisen termin derivaatan lauseke

$$(\frac{\prod_{m=1}^{x} p_m}{p(x)})' = \frac{\prod_{m=1}^{x} p_m}{p(x)}(\sum_{k=1}^{x} \frac{1}{p_k} - \frac{1}{p(x)}).$$

Määritetään nyt tämän jonon raja-arvo:

$$\begin{aligned}
\lim_{x\to\infty}(\frac{\prod_{m=1}^{x} p_m}{p(x)}(\sum_{k=1}^{x} \frac{1}{p_k} - \frac{1}{p(x)})) &= \lim_{x\to\infty}(\frac{\prod_{m=1}^{x} p_m}{p(x)}(\sum_{k=1}^{x} \frac{1}{p_k}) - \frac{\prod_{m=1}^{x} p_m}{p(x)}(\frac{1}{p(x)})) \\
&= \lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{p(x)}(\sum_{k=1}^{x} \frac{1}{p_k}).
\end{aligned}$$

Rajoittavien funktioiden avulla saadaan

$$\lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{2a(x)\prod_{m=1}^{x} p_m}(\sum_{k=0}^{x} \frac{1}{p_k}) \leq \lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{p(x)}(\sum_{k=1}^{x} \frac{1}{p_k}) < \lim_{x\to\infty} \frac{\prod_{m=1}^{x} p_m}{a(x)\prod_{m=1}^{x} p_m}(\sum_{k=0}^{x} \frac{1}{p_k}),$$

$$\lim_{x\to\infty}\frac{\sum_{k=0}^{x}\frac{1}{p_k}}{2\log_2(\sum_{k=0}^{x}\frac{1}{p_k})}\leq\lim_{x\to\infty}\frac{\prod_{m=1}^{x}p_m}{p(x)}(\sum_{k=1}^{x}\frac{1}{p_k})<\lim_{x\to\infty}\frac{\sum_{k=0}^{x}\frac{1}{p_k}}{\log_2(\sum_{k=0}^{x}\frac{1}{p_k})}.$$

Koska molemmat rajoittavat funktiot kasvavat rajatta, niin tekee myös jono. Näin ollen x' hajaantuu, kun x lähestyy lukua 0.

$\square$

5.2. Logaritmin derivaatta. Aritmeettinen derivaatta ei täytä aina lineaarisuutta, joten emme voi myöskään olettaa, että tulon logaritmi olisi yhtä suuri kuin tulontekijöiden logaritmien summa. Määritellään seuraavaksi logaritmin derivaatta $ld(x)$.

MÄÄRITELMÄ 23. Jos $x=\prod_{i=1}^{k}p_i^{x_i}$, missä p_i:t ovat eri alkulukuja ja x_i:t ovat kokonaislukuja, niin

$$ld(x)=\sum_{i=1}^{k}\frac{x_i}{p_i},\quad ld(-x)=ld(x),\quad ld(0)=\infty.$$

Määritelmä voidaan siis esittää muodossa

$$ld(x)=\frac{x'}{x}.$$

LAUSE 24. *Kaikille rationaaliluvuille pätee $ld(xy)=ld(x)+ld(y)$.*

TODISTUS. Käytetään hyväksi edellistä määritelmää, jolloin

$$ld(xy)=\frac{(xy)'}{xy}=\frac{x'y+xy'}{xy}=\frac{x'}{x}+\frac{y'}{y}=ld(x)+ld(y).$$

$\square$

5.3. Potenssin derivaatta. Seuraavaksi laajennetaan aritmeettisen derivaatan määritelmä koskemaan potenssin derivointia.

LAUSE 25. *Olkoon x ja y rationaalilukuja ja x positiivinen. Nyt pätee*

$$(x^y)' = yx^{y-1}x' = \frac{yx'}{x}x^y = yx^y ld(x).$$

TODISTUS. Jos $x = \prod_{i=1}^k p_i^{x_i}$, niin määritelmän 19 mukaisesti

$$(x^y)' = (\prod_{i=1}^k p_i^{yx_i})' = x^y \sum_{i=1}^k \frac{yx_i}{p_i} = yx^{y-1}x \sum_{i=1}^k \frac{x_i}{p_i} = yx^{y-1}x'.$$

□

Erityisesti alkuluvuille p pätee nyt $(p^p)' = p \cdot p^{p-1} \cdot p' = p \cdot p^{p-1} = p^p$.

SEURAUS 26. *Olkoon a, b, c, d rationaalilukuja niin, että $a^b = c^d \quad (a, c$ positiivisia$)$. Silloin*

$$\begin{aligned} b \cdot ld(a) &= d \cdot ld(c), \\ a'bc &= c'ad. \end{aligned}$$

Erityisesti, jos $a = b, c = d$, saadaan $a^a = c^c$, jolloin $a' = c'$.

5.4. Joidenkin irrationaalilukujen derivaatta. Laajennetaan nyt aritmeettisen derivaatan määritelmä koskemaan myös joitain irrationaalilukuja.

LAUSE 27. *Olkoon $\{p_1, \ldots, p_k\}$ jono eri alkulukuja sekä $\{x_1, \ldots, x_k\}$ jono rationaalilukuja. Nyt $P = \prod_{i=1}^k p_i^{x_i} = 1$ jos ja vain jos $x_1 = x_2 = \cdots = x_k = 0$.*

TODISTUS. Lause on selvästi totta, jos kaikki x_i:t ovat kokonaislukuja. Jos jokainen x_i on rationaaliluku mutta ei kokonaisluku, valitaan luonnollinen luku m siten, että $y_i = mx_i \in \mathbb{Z}$. Nyt $P^m = 1$, jolloin $y_i = 0$. Näin ollen myös $x_i = 0$. $\square$

Äskeisen lauseen nojalla voimme laajentaa aritmeettisen derivaatan määritelmää.

MÄÄRITELMÄ 28. Luvun x, $\quad x \in \mathbb{R}$, aritmeettinen derivaatta x' voidaan laskea

$$x' = x \sum_{i=1}^{k} \frac{x_i}{p_i},$$

kun x voidaan kirjoittaa tulona $x = \prod_{i=1}^{k} p_i^{x_i}$, missä p_i on alkuluku ja x_i on rationaaliluku.

ESIMERKKI 29. Ratkaistaan reaaliluvun $\sqrt{3}$ aritmeettinen derivaatta,

$$(\sqrt{3})' = (3^{\frac{1}{2}})' = 3^{\frac{1}{2}} \frac{\frac{1}{2}}{3} = \frac{\sqrt{3}}{6}.$$

6. Differentiaaliyhtälöitä

Seuraavaksi ratkaistaan muutamia differentiaaliyhtälöitä. Käytämme alussa vain positiivisia kokonaislukuja mutta myöhemmin otamme myös rationaaliluvut käyttöön.

6.1. $n = n'$.

LAUSE 30. *$n = n'$ jos ja vain jos $n = p^p$, missä p on mikä tahansa alkuluku.*

TODISTUS. Oletetaan ensin, että $n = p^p$. Nyt lauseen 7 mukaan $n' = p^p \cdot \frac{p}{p} = p^p = n$. Oletetaan sitten, että $n = n'$. Koska n on luonnollinen luku, se on jaollinen alkuluvulla p. Nyt lauseen 15 mukaan n on jaollinen luvulla p^p tai sitten $n \neq n'$. Jälkimmäinen on ristiriidassa oletuksen kanssa, joten n

on jaollinen p^p:llä. Eli $n = p^p m$. Lauseen 14 mukaan nyt $n' = p^p m + p^p m'$. Oletusten mukaan nyt pätee

$$n' = n \Leftrightarrow p^p m + p^p m' = p^p m \Leftrightarrow p^p m' = 0 \Leftrightarrow m' = 0$$

Nyt lauseen 6 ja oletusten mukaan $m = 1$. Eli $n = p^p$. □

6.2. $n' = a$. Ensiksi toteamme, että suora seuraus lauseesta 6 on se, että differentiaaliyhtälöllä $n' = 0$ on vain yksi positiivinen kokonaislukuratkaisu $n = 1$. Lisäksi aritmeettisen derivaatan määritelmän mukaan $p' = 1$ kaikille alkuluvuille. Näin ollen yhtälölle $n' = 1$ ratkaisuna toimivat ainoastaan kaikki alkuluvut. Tämä voidaan perustella Leibnizin säännöllä. Jos $n \in \mathbb{N}$ ei ole alkuluku, se voidaan ilmoittaa tulona ja derivoida Leibnizin sääntöä käyttäen. Näin ollen luvun n derivaatta on aina summa kahdesta tulosta ja on aina siis suurempi kuin 1. Kaikilla muilla tapauksilla $n' = a$ on äärellinen määrä ratkaisuja tai ratkaisuja ei ole olemassa.

LAUSE 31. *Olkoon n mielivaltainen positiivinen kokonaisluku. Nyt n:lle pätee*

$$n' \leq \frac{n \log_2 n}{2}.$$

TODISTUS. Olkoon $n = \prod_{i=1}^{k} p_i^{n_i}$. Tällöin $n \geq \prod_{i=1}^{k} 2^{n_i} \Rightarrow \log_2 n \geq \sum_{i=1}^{k} n_i$. Lauseen 7 mukaan nyt pätee

$$n' = n \sum_{i=1}^{k} \frac{n_i}{p_i} \leq \frac{n \sum_{i=1}^{k} n_i}{2} \leq \frac{n \log_2 n}{2}.$$

□

Lause 32. *Olkoon n luonnollinen luku ja k pienin n:n alkulukutekijä. Nyt pätee*

$$\frac{n \log_k n}{k} \geq n'.$$

Todistus. Olkoon $n = \prod_{i=1}^m p_i^{\alpha_i}$. Nyt lauseen 7 mukaan

$$n' = n \sum_{i=1}^m \frac{\alpha_i}{p_i} \leq n \sum_{i=1}^m \frac{\alpha_i}{k} = \frac{n \sum_{i=1}^m \alpha_i}{k} \leq \frac{n \log_k n}{k}.$$

Yhtäsuuruus pätee vain, jos n on k:n potenssi. □

Lause 33. *Jokaiselle luonnolliselle luvulle n, joka ei ole alkuluku ja voidaan näin ollen jakaa k:hon alkulukutekijään, pätee*

$$n' \geq k n^{\frac{k-1}{k}}.$$

Todistus. Olkoon $n = \prod_{i=1}^k p_i$ luonnollisen luvun n alkutekijöihin jako, jossa jokainen alkulukutekijä voi esiintyä useita kertoja. Nyt

$$n' = n \sum_{i=1}^k \frac{p_i'}{p_i} = n \sum_{i=1}^k \frac{1}{p_i} \geq nk(\prod_{i=1}^k \frac{1}{p_i})^{\frac{1}{k}} = nkn^{-\frac{1}{k}} = kn^{\frac{k-1}{k}}$$

Tästä seurauksena on, että $n' \geq 2\sqrt{n}$. □

Tutkitaan nyt yhtälön $n' = a$ ratkaisuiden lukumääriä.

Seuraus 34. *Jos yhtälöllä $n' = a$ on luonnollisia ratkaisuja, sillä on niitä vain rajallinen määrä, kun $a > 1$.*

Todistus. Koska $a > 1$, n ei voi olla alkuluku. Käytetään nyt hyväksi lausetta 33 ja etenkin sen seurausta $n' \geq 2\sqrt{n}$. Nyt siis $a \geq 2\sqrt{n} \Leftrightarrow \frac{a}{2} \geq \sqrt{n} \Rightarrow \frac{a^2}{4} \geq n$. Siis yhtälön ratkaisu ei voi olla suurempi kuin $\frac{a^2}{4}$. □

Lause 35. *Olkoon p alkuluku ja $a = p + 2$. Nyt $2p$ on ratkaisu yhtälöön $n' = a$.*

Todistus. Oletetaan, että $n = 2p$. Nyt

$$n' = (2p)' = 2'p + 2p' = 1 \cdot p + 2 \cdot 1 = p + 2 = a.$$

Siis $2p$ on ratkaisu yhtälöön $n' = a$, kun $a = p + 2$. □

6.3. $x' = \alpha x$. Otetaan nyt käyttöön rationaaliluvut ja tutkitaan seuraavaksi yhtälön $x' = \alpha x$ ratkaisuiden lukumääriä, kun molemmat x ja α ovat rationaalilukuja. Tarkastellaan siis luvun α mahdollisia arvoja.

Lause 36. *Jokainen rationaaliluku, jonka nimittäjä voidaan esittää erilaisten alkulukujen tulona, $\frac{m}{p_1 p_2 p_3 \cdots p_k}$, voidaan esittää summana $\sum_i \frac{a_i}{p_i}$, missä p_i on alkuluku ja $a_i \in \mathbb{Z}$.*

Todistus. Käytetään todistuksessa hyödyksi induktiota. Kun $k = 1$, tapaus on selvä. Oletetaan nyt, että jokainen muotoa $\frac{m}{p_1 p_2 p_3 \cdots p_k}$ oleva rationaaliluku voidaan esittää summana $\sum_i \frac{a_i}{p_i}$. Osoitetaan nyt, että myös jokainen muotoa $\frac{m}{p_1 p_2 p_3 \cdots p_k p_{k+1}}$ voidaan esittää vastaavanlaisena summana. Tutkitaan seuraavaa summaa:

$$\frac{m}{p_i \cdots p_k p_{k+1}} + \frac{a_{k+1}}{p_{k+1}},$$

jossa a_{k+1} on kokonaisluku, jolle pätee

$$(a_{k+1})(p_1 \ldots p_k) \equiv -m \pmod{p_{k+1}}$$

Tällainen luku on olemassa, sillä kokonaisluvut muodostavat jäännösluokkaryhmän $\pmod{p}$ yhteenlaskun suhteen ja tässä ryhmässä $\mathbb{Z}_p$ jokainen nollasta poikkeava alkio virittää ryhmän. Näin ollen saadaan

$$\frac{m}{p_1 \dots p_k p_{k+1}} + \frac{a_{k+1}}{p_{k+1}} = \frac{m + a_{k+1} p_1 \dots p_k}{p_1 \dots p_{k+1}}.$$

Käytetään nyt tietoa a_{k+1}:stä hyväksi, jolloin tiedetään, että

$$m + a_{k+1} p_1 \dots p_k \equiv 0 \pmod{p_{k+1}}.$$

Näin ollen siis osoittaja on jaollinen luvulla p_{k+1}, jolloin summa on muotoa

$$\frac{m}{p_1 \dots p_k p_{k+1}} + \frac{a_{k+1}}{p_{k+1}} = \frac{m + a_{k+1} p_1 \dots p_k}{p_1 \dots p_{k+1}} = \frac{\left(\frac{m+a_{k+1}p_1 \dots p_k}{p_{k+1}}\right)}{p_1 \dots p_k}.$$

Nyt osoittaja $\frac{m+a_{k+1}p_1 \dots p_k}{p_{k+1}}$ on selkeästi kokonaisluku. Tällöin

$$\frac{m}{p_1 \dots p_{k+1}} = \frac{-a_{k+1}}{p_{k+1}} + \frac{\frac{m+a_{k+1}p_1 \dots p_k}{p_{k+1}}}{p_1 \dots p_k}.$$

Viimeinen luku voidaan esittää summana rationaaliluvuista, joiden nimittäjät ovat alkulukuja, induktio-oletuksen mukaisesti. □

Käytetään seuraavaksi äsken todistettua lausetta hyväksi.

LAUSE 37. *Yhtälöllä $x' = \alpha x$ on ratkaisuja jos ja vain jos α on rationaaliluku, jonka nimittäjä on neliötön.*

TODISTUS. Määritellään ensin lauseessa esiintynyt neliötön nimittäjä. Nimittäjä on neliötön, kun sen tekijänä ei ole minkään määrittelyjoukkoon kuuluvan luvun neliötä.

Osoitetaan ensiksi, että jos yhtälöllä $x' = \alpha x$ on ratkaisuja, niin α:lla on neliötön nimittäjä.

Olkoon $x \in \mathbb{Q}, x = p_1^{x_1} \dots p_k^{x_k} \dots$ ja oletetaan, että $x' = \alpha x$. Nyt määritelmän 19 mukaan

$$\alpha = \frac{x_1}{p_1} + \frac{x_2}{p_2} + \dots + \frac{x_k}{p_k} + \dots.$$

Helposti nähdään, että kun lavennetaan murtoluvut α:n lausekkeessa samannimiseksi ja suoritetaan yhteenlasku, niin yhteisenä nimittäjänä oleva luku on neliötön. Siis α:n jakajassa ei ole alkulukua, jolla on suurempi potenssi kuin 1.

Oletetaan sitten puolestaan, että α:lla on neliötön nimittäjä ja osoitetaan, että yhtälöllä on ratkaisuja.

Lauseen 36 mukaan jokainen rationaaliluku, jolla on neliötön nimittäjä, voidaan esittää summana rationaaliluvuista, joilla on jakajana alkuluku. Näin ollen α voidaan esittää muodossa $\alpha = \frac{x_1}{p_1} + \frac{x_2}{p_2} + \dots + \frac{x_k}{p_k} + \dots$. Tämä viittaa suoraan siihen, että yhtälöllä $x' = \alpha x$ on ratkaisu $p_1^{x_1} \dots p_k^{x_k} \dots$.

□

Todistetaan vielä lause ratkaisujen lukumäärästä.

LAUSE 38. *Jos yhtälöllä $x' = \alpha x$ on yksi ratkaisu, joka ei ole* 0, *niin sillä on loputon määrä ratkaisuja.*

TODISTUS. Lause voidaan muotoilla toisin: jokainen luku α, joka voidaan esittää summana rationaaliluvuista, joilla on jakajana alkuluku, voidaan esittää äärettömän monella eri tavalla.

Olkoon $\alpha = \sum_i \frac{a_i}{p_i}$. Nyt α voidaan esittää muodossa

$$\alpha = \sum_i \frac{a_i}{p_i} + \frac{cp_h}{p_h} - \frac{cp_j}{p_j}, \text{ missä } c \in \mathbb{Z}, a_h = a_j = 0.$$

Tätä lukua α vastaava luku x on $p_1^{a_1} \dots p_h^c \dots p_j^{-c} \dots$. Koska c voi olla mikä tahansa kokonaisluku, on erilaisia vaihtoehtoja lukematon määrä. □

6.4. $n'' = 1$. Tutkitaan vielä toisen kertaluvun derivaattaa $n'' = 1$, missä $n \in \mathbb{Z}_+$. Todetaan ensin muutama seuraus.

SEURAUS 39. *Differentiaaliyhtälöllä $n'' = 1$ on ääretön määrä ratkaisuja luonnolisissa luvuissa.*

Lauseen 35 mukaan nyt voidaan todeta, että $2p$ on ratkaisu yhtälöön, jos p ja $p+2$ ovat alkulukuja. Näin ollen saadaan seuraus.

SEURAUS 40. *On olemassa loputon määrä pareja $p, p+2$, missä p ja $p+2$ ovat alkulukuja.*

SEURAUS 41. *On olemassa loputon määrä kolmikkoja p, q, r, missä p, q, r ovat alkulukuja, siten, että $P = pq + pr + qr$ on alkuluku.*

Seurauksen 41 kolmikko p, q, r tuottaa aina ratkaisun $n = pqr$ yhtälöön $n'' = 1$, sillä $n' = P$. Näin ollen kaikki ratkaisut voidaan kuvata seuraavalla määritelmällä.

MÄÄRITELMÄ 42. Luku n on ratkaisu yhtälöön $n'' = 1$ jos ja vain jos seuraavat ehdot ovat voimassa:

(1) Luku n voidaan esittää tulona eri alkuluvuista $n = \prod_{i=1}^{k} p_i$.
(2) $\sum_{i=1}^{k} \frac{1}{p_i} = \frac{p}{n}$, missä p on alkuluku.
(3) Jos k on parillinen, niin p_i:n pienin alkuluku tulee olla 2.

7. Sophie Germainin alkuluvut ja Cunninghamin ketjut

MÄÄRITELMÄ 43. Alkuluku p on Sophie Germainin alkuluku, jos $2p+1$ on myös alkuluku.

Oletettu seuraus Sophie Germainin alkuluvuille on, että niitä on loputtomasti, mutta tätä ei ole pystytty vielä todistamaan. Tällä hetkellä löydetyistä luvuista suurin on $18543637900515 \cdot 2^{666667} - 1$.

MÄÄRITELMÄ 44. Cunninghamin ketjun muodostaa alkulukujen joukko. Ensimmäisen tyypin Cunninghamin ketju koostuu luvuista $\{p, 2p+1, 2(2p+1)+1, ...\}$, missä kaikki muut paitsi viimeinen luku on Sophie Germainin alkuluku. Toisen tyypin Cunninghamin ketju koostuu 1. tyypin tapaan alkuluvuista $\{p, 2p-1, 2(2p-1)-1...\}$.

Cunninghamin ketju on kokonainen, jos sitä ei voida enää jatkaa. Eli jos sarjan seuraava luku ei ole enää alkuluku, ei sarjaa voida jatkaa.

Tutkitaan nyt Sophie Germainin alkulukujen ja Cunninghamin ketjujen ominaisuuksia aritmeettisen derivaatan avulla. Potenssin derivaatan avulla voidaan nyt todeta, että kaikille alkuluvuille p pätee

$$(2^4p)' = 4 \cdot 2^3p + 2^4p' = 2^4(2p+p') = 2^4(2p+1).$$

Nyt siis, jos p on Sophie Germainin alkuluku, derivaatassa luku $2p+1$ on myös alkuluku. Näin ollen alkulukujen "Sophie Germain" -ominaisuus tulee esille differentiaaliyhtälöissä.

LAUSE 45. *Kaikille positiivisille kokonaisluvuille m pätee $(2^4m)'' \geq 2^4(4m+3)$, ja yhtä suuruus pätee ainoastaan, jos m on Sophie Germainin alkuluku.*

Todistus. Oletetaan ensin, että $m \in \mathbb{N}$, mutta m ei ole alkuluku. Nyt

$$\begin{aligned}
(2^4m)' &= 4 \cdot 2^3 m + 2^4 m' = 2^4(2m + m'), \\
(2^4(2m + m'))' &= 4 \cdot 2^3(2m + m') + 2^4(2m + m')' \\
&= 2^4(4m + 2m') + 2^4(2m + m')' \\
&= 2^4(4m + 2m' + (2m + m')) > 2^4(4m + 3).
\end{aligned}$$

Oletetaan nyt, että $m \in \mathbb{N}$ ja m on alkuluku. Tällöin

$$\begin{aligned}
(2^4m)' &= 2^4(2m + m') = 2^4(2m + 1), \\
(2^4(2m + 1))' &= 4 \cdot 2^3(2m + 1) + 2^4(2m + 1)' \\
&= 2^4(4m + 2 + (2m + 1)') \geq 2^4(4m + 3).
\end{aligned}$$

Helposti nähdään, että viimeisen epäyhtälön yhtäsuuruus pätee ainoastaan, jos $2m + 1$ on alkuluku, eli m on Sophie Germainin alkuluku. $\square$

Seuraus 46. *Yhtälölle $n'' = 4n + 48$, missä $n = 2^4 p$ ja p on alkuluku, on äärettömän monta eri ratkaisua.*

Lause 47. *Jokaiselle Cunninghamin ketjulle, jossa on k termiä, pätee $(2^4m)^{(k)} \geq 2^4(2^k m + 2^k - 1)$ ja yhtäsuuruus pätee vain, jos $\{m, 2m + 1, 4m + 3, ...\}$ ovat alkulukuja.*

Todistus. Todistetaan lause induktion avulla. Cunninghamin ketjulle, jossa on yksi termi, pätee $(2^4m)' = 4 \cdot 2^3 m + 2^4 m' = 2^4(2m + m') \geq 2^4(2m + 1)$. Yhtäsuuruus pitää paikkansa vain ja ainoastaan silloin, kun $m' = 1$ eli m on alkuluku.

Oletetaan, että Cunninghamin ketjulle, jossa on k termiä, pätee $(2^4m)^{(k)} = 2^4(2^km+2^k-1)$. Nyt

$$\begin{aligned}(2^4m)^{(k+1)} &= ((2^4)^{(k)})' \\ &= (2^4(2^km+2^k-1))' \\ &= 4\cdot 2^3(2^km+2^k-1)+2^4(2^km+2^k-1)' \\ &= 2^4(2^{k+1}m+2^{k+1}-2+1) \\ &\geq 2^4(2^{k+1}m+2^{k+1}-1).\end{aligned}$$

Yhtäsuuruus pätee vain ja ainoastaan silloin, kun Cunninghamin ketjun k:nnes termi $2^{k+1}m+2^{k+1}-1$ on alkuluku. □

8. Yhteenveto ja avoimia tutkimusongelmia

Tutkielmassa on nyt onnistuneesti määritelty aritmeettinen derivaatta ensin luonnollisille luvuille ja sitten rationaaliluvuille. Määritelmä on onnistuttu koskemaan myös potenssin derivointia sekä joitain irrationaalilukuja. Aritmeettisen derivaatan ominaisuuksia on tutkittu eri tavoin sekä derivaattaa on onnistuttu rajoittamaan erilaisilla raja-arvon määrityksillä. Tutkielmassa on myös löydetty ratkaisuja erilaisiin differentiaaliyhtälöihin ja tutkittu lukuteorian sovelluksien ominaisuuksia aritmeettisen derivaatan avulla.

Avoimia ja lisätutkimusta vaativia ongelmia voisivat olla esimerkiksi: Onko olemassa sellaista lukua k, että $n^{(k)} = n$, kun $n' \neq n$? Onko olemassa rationaalilukuratkaisua x yhtälöön $x' = a$ jokaisella luvun a arvolla?

Lähdeluettelo

[1] APOSTOL, T.: *Introduction to Analytic Number Theory* New York: Springer-Verlag, 1976

[2] BARBEAU E.J.: *Remarks on an arithmetic derivative* Canadian Mathematical Bulletin. Vol. 4, 1961: 117-122

[3] DAHL N., OLSSON J., LOIKO A.: *Investigations on the properties of the arithmetic derivative* 2011

[4] HARDY, G.H., WRIGHT, EM: *An Introduction to the Theory of Numbers* Oxford University Press, 1980, 5th edition

[5] METSÄKYLÄ T., NÄÄTÄNEN M.: *Algebra* Limes ry, 2. korjattu painos, 2005

[6] NIVEN, I., ZUCKERMAN, H.S.: *An Introduction to the Theory of Numbers* Wiley Textbooks, 1991, 5th edition

[7] STAY M.: *Generalized Number Derivatives* Journal of Integer Sequences, Vol. 8, 2005, Artikkeli 05.1.4

[8] UFNAROVSKI V., ÅHLANDER B.: *How to Differentiate a Number* Journal of Integrer Sequences, Vol. 6, 2003, Artikkeli 03.3.4

[9] WESTRICK L.: *Investigations of the Number Derivative* Massachussetts Institute of Technology, 15.11.2003