Tartu Ülikool
Loodus- ja täppisteaduste valdkond
Matemaatika ja statistika instituut

Leene Lotta Lüdimois

Dirichlet' karakterid

Matemaatika

Bakalaureusetöö (9 EAP)

Juhendaja: PhD Lauri Tart

Tartu 2024

DIRICHLET' KARAKTERID

Bakalaureusetöö

Leene Lotta Lüdimois

Lühikokkuvõte

Dirichlet' karakterid on teatud aritmeetilised funktsioonid, mille abil saab konstrueerida mitmesuguseid analüütilises arvuteoorias olulisi funktsionaalridu. Näiteks Dirichlet' L-read on tähtsad Dirichlet' teoreemi tõestamisel. Töös tutvustame aritmeetilisi funktsioone, Dirichlet' karaktereid ja tõestame ära ühe olulisema Dirichlet' teoreemi tõestuse vahesammu.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria.

Märksõnad: Dirichlet' read, analüütiline arvuteooria, aritmeetilised funktsioonid, aritmeetiline progressioon, kommutatiivsed rühmad.

DIRICHLET CHARACTERS

Bachelor thesis

Leene Lotta Lüdimois

Abstract

Dirichlet characters are certain arithmetic functions that can be used to construct various function series important in analytic number theory. For example, Dirichlet's L-series are important in proving Dirichlet's theorem. We give an exposition of arithmetic functions, Dirichlet characters and prove an important step in the proof of Dirichlet's theorem.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory.

Key Words: Dirichlet series, analytic number theory, arithmetic functions, arithmetic progression, commutative groups.

Sisukord

Sissejuhatus

Dirichlet' karakterid χ on rühmade homomorfismide kaudu defineeritud multiplikatiivsed ja perioodilised aritmeetilised funktsioonid. Dirichlet' karakterite teooriale pani aluse saksa matemaatik Peter Gustav Lejeune Dirichlet, kes võttis karakterid kasutusele algarvude jaotuse uurimiseks aritmeetilistes jadades. Nendel karakteritel on oluline roll järgmise teoreemi tõestamisel:

Teoreem (Dirichlet' teoreem)**.** *Mistahes ühisteguriteta naturaalarvude a, b korral sisaldab aritmeetiline jada $a + kb$ lõpmata palju algarve.*

Üks olulisi Dirichlet' karakterite kasutusi on Dirichlet L-read $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, mille erijuhu $s = 1$ abil on võimalik tõestada eelnevalt sõnastatud Dirichlet' teoreem. Nimelt põhinevad üht sorti Dirichlet' teoreemi tõestused sellel, et mis tahes reaal- või kompleksarvuliste väärtustega karakteri χ korral $L(1, \chi) \neq 0$. Käesolevas töös tõestame selle omaduse reaalarvuliste väärtustega mitte-peakarakteri χ jaoks.

Bakalaureusetöö kuulub analüütilise arvuteooria valdkonda. Töö on referatiivne ja põhineb Tom M. Apostoli õpikul "Introduction to Analytic Number Theory" [1]. Töös käsitletud Dirichlet' karakterite omadused ja nende abil tõestatavad tulemused on valitud selliselt, et need toetaksid Apostoli õpikus esitatud Dirichlet' teoreemi tõestust.

Lugejalt eeldatakse, et ta on omandanud põhiteadmised arvuteooriast, matemaatilisest analüüsist ja rühmateooriast.

Töö esimeses peatükis korratakse üle olulisemad teadmised arvuteooriast, matemaatilisest analüüsist, rühmateooriast ning süvenetakse edasises vajalikesse Landau sümbolite omadustesse.

Teises peatükis anname ülevaate aritmeetilistest funktsioonidest ning nende omadustest, mida kasutame Dirichlet' karakterite omaduste tõestamisel. Defineerime Dirichlet' korrutise ning tõestame mõned selle omadused, lisaks tõestame mõned asümptootilised hinnangud, näiteks Euleri summa valemi ja Abeli samasuse.

Et Dirichlet' karakterid on lõplike Abeli rühmade karakterite erijuht, tutvume kolmandas peatükis just lõplike Abeli rühmade karakteritega. Defineerime Abeli rühma karakterid, tutvustame nende omadusi, karakterite rühma ning ortogonaalsusseoseid.

Neljas peatükk on Dirichlet' karakteritest. Alustame definitsioonist ja lihtsamatest omadustest, toome mõned näited, tõestame ortogonaalsusseosed ning viimaks tõestame lisaks eelmainitud olulise Dirichlet' teoreemi tõestuse vahetulemuse.

1 Definitsioonid ja abitulemused

Selles peatükis tuletame lugejale meelde mõned töö jaoks vajalikud mõisted ja tulemused arvuteooriast, matemaatilisest analüüsist ning rühmateooriast. Lisaks meenutame Landau sümboleid ning tutuvustame nende olulisemaid omadusi, mida töös kasutame.

1.1 Arvuteooria

Siinsed mõisted pärinevad arvuteooria loengukonspektist [3].

Paneme tähele, et selles töös tähistab märge $[t]$ suurimat täisarvu m, mille korral $m \leq t$.

Definitsioon 1.1. *Euleri funktsioon $\varphi : \mathbb{N} \to \mathbb{N}$ defineeritakse võrdusega*

$$\varphi(n) = |\{x \in \mathbb{N} | 1 \leq x \leq n, (x, n) = 1\}|.$$

Definitsioon 1.2. *Täisarvu d nimetatakse täisarvude a ja b suurimaks ühisteguriks (tähistatakse $d = (a, b)$), kui*

- *$d|a$ ja $d|b$,*
- *iga täisarvu c korral, kui $c|a$ ja $c|b$, siis $c|d$.*

Definitsioon 1.3. *Tähistame sümboliga $\overline{a}$ kõigi selliste täisarvude hulka, mis on kongruentsed täisarvuga a mooduli n järgi, s.o.*

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\},$$

ja nimetame selliseid hulki jäägiklassideks mooduli n järgi.

Paneme tähele, et $\overline{a}$ tähistab käesolevas töös sõltuvalt kontekstist kaaskompleksarvu või jäägiklassi.

1.2 Rühmateooria

Selles peatükis meenutame rühmateooria põhilisi mõisteid, tuginedes loengukonspektidele [2] ja [3].

Definitsioon 1.4. *Mittetühja hulka G koos kahekohalise algebralise tehtega, mida tähistame $\cdot$ abil, nimetatakse rühmaks, kui see rahuldab järgmisi tingimusi:*

- *Kui $a, b \in G$, siis ka $a \cdot b \in G$.*
- *Kui $a, b, c \in G$, siis $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
- *Leidub element $e \in G$ nii, et mistahes $a \in G$ korral $a \cdot e = e \cdot a = a$. Sellist elementi e nimetame ühikelemendiks.*
- *Iga $a \in G$ korral leidub element $b \in G$ nii, et $a \cdot b = b \cdot a = e$. Sellist elementi b tähistame kui a^{-1} ja nimetame a pöördelemendiks.*

Definitsioon 1.5. *Rühma G nimetatakse Abeli rühmaks, kui rühma tehe on kommutatiivne ehk iga $a, b \in G$ korral $a \cdot b = b \cdot a$.*

Definitsioon 1.6 (Alamrühma kriteerium)**.** *Kui G' on rühma G mittetühi alamhulk, siis G' on G alamrühm siis ja ainult siis, kui G' rahuldab järgmisi aksioome:*

- *Kinnisus korrutamise suhtes: Kui $a, b \in G'$, siis ka $ab \in G'$.*
- *Pöördelemendi leidumine: Kui $a \in G'$, siis $a^{-1} \in G'$.*

Definitsioon 1.7. *Lõpliku rühma G järguks nimetatakse tema elementide arvu. Lõpliku rühma G järku tähistatakse $|G|$.*

Definitsioon 1.8. *Olgu G lõplik rühm ja $a \in G$. Vähimat naturaalarvu m, mille korral $a^m = 1$, kus 1 on lõpliku rühma G ühikelement, nimetatakse elemendi a järguks. Tähistame elemendi a järku* $\operatorname{ord}(a)$.

Teoreem 1.9 (Lagrange'i teoreem)**.** *Lõpliku rühma mistahes alamrühma järk on selle rühma järgu jagaja. Muuhulgas lõpliku rühma iga elemendi järk on selle rühma järgu jagaja.*

Järeldus 1.10. *Olgu G lõplik rühm järguga n. Siis iga elemendi $a \in G$ korral*

$$a^n = 1.$$

Definitsioon 1.11. *Mistahes naturaalarvu n korral on*

$$U(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$$

$\varphi(n)$. järku rühm tehte $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ suhtes.

Lemma 1.12. *Kui G on rühm ja $a \in G$, siis $G = aG$, kus $aG = \{ag \mid g \in G\}$.*

Teoreem 1.13. *Ruutmaatriks on pööratav parajasti siis, kui see on regulaarne.*

1.3 Matemaatiline analüüs

Analüüsi osa tugineb loengukonspektile [4]. Meenutame lugejale mõnda olulisemat tulemust, mida edaspidi ka selles töös kasutame.

Lause 1.14. *Olgu funktsioon f lõigus $[a, b]$ integreeruv ja olgu $g : [a, b] \to \mathbb{R}$ selline funktsioon, mis erineb funktsioonist f vaid lõpliku arvu argumendi väärtuste korral. Siis on g lõigus $[a, b]$ integreeruv ning*

$$\int_a^b g(x)dx = \int_a^b f(x)dx. \tag{1.1}$$

Lause 1.15. *Kui iga $x \in [a, b]$ korral $f(x) \leq g(x)$ ja funktsioonid $f, g : [a, b] \to \mathbb{R}$ on integreeruvad, siis $\int_a^b f(x)dx \leq \int_a^b g(x)dx$.*

Lause 1.16. *Kui funktsioonid f ja g on igas lõigus $[a, l]$, kus $l \geq a$, integreeruvad ning iga $x \in [a, \infty)$ korral $0 \leq f(x) \leq g(x)$, siis integraali $\int_a^\infty g(x)dx$ koonduvusest järeldub integraali $\int_a^\infty f(x)dx$ koonduvus.*

Teoreem 1.17 (Cauchy koondumiskriteerium ridade jaoks)**.** *Rida $\sum_{k=1}^{\infty} u_k$ koondub parajasti siis, kui*

$$\forall \varepsilon > 0 \; \exists n \in \mathbb{N} : m > n \geq N \Rightarrow \left| \sum_{k=n+1}^{m} u_k \right| < \varepsilon.$$

Lause 1.18. *Leidugu ridade $\sum_{k=1}^{\infty} u_k$ ja $\sum_{k=1}^{\infty} v_k$ puhul indeks $N \in \mathbb{N}$, et $0 \leq u_k \leq v_k$ iga $k \geq N$ korral. Kui rida $\sum_{k=1}^{\infty} v_k$ koondub, siis koondub ka rida $\sum_{k=1}^{\infty} u_k$.*

1.4 Landau sümbolid

Selles alampeatükis defineerime olulisemad Landau sümbolid ja esitame mõned nende töös kasutatavad omadused. Landau sümbolid võimaldavad võrrelda erinevate jadade käitumist piirprotsessides. Et ülevaatlikku, veel vähem eestikeelset allikat koos tõestustega antud teemal leida on keeruline, anname siinkohal ka vajalike omaduste tõestused.

Definitsioon 1.19. *Olgu $A \subseteq \mathbb{R}$, $B = \mathbb{C}$ või $B = \mathbb{R}$ ja ∞ hulga A kuhjumispunkt. Kui $\alpha : A \to B$ ja $\beta : A \to B$ on mingid funktsioonid, siis kirjutatakse, et $\alpha \in O(\beta)$, kui*

$$\exists K > 0 \; \exists M > 0 : \forall x \in D \; x > M \Rightarrow |\alpha(x)| \leq K|\beta(x)|,$$

kus $|\cdot|$ võib tähistada nii absoluutväärtust kui moodulit.

Lause 1.20. *Suure O notatsioonil on järgmised omadused:*

1. *Kehtib $f(x) = O(f(x))$.*

2. Kehtib $O(O(f(x))) = O(f(x))$.

3. Olgu $f(x) = O(g(x))$ ja k kompleksarv. Siis $kf(x) = O(|k|g(x))$.

4. Olgu $f_1(x) = O(g_1(x))$ ja $f_2(x) = O(g_2(x))$, siis kehtib $f_1(x) + f_2(x) = O(g_1(x) + g_2(x))$.

5. Olgu $f_1(x) = O(g_1(x))$ ja $f_2(x) = O(g_2(x))$, siis $f_1(x)f_2(x) = O(g_1(x)g_2(x))$.

6. Olgu I lõplik hulk. Kui iga $i \in I$ korral $g_i(x) = O(f_i(x))$, siis $\sum_{i \in I} g_i(x) = O\left(\sum_{i \in I} f_i(x)\right)$.

Tõestus. Tõestuse vältel kasutame järgmisi tähistusi. Üldisust kitsendamata olgu I naturaalarvude hulk, $j \in I \cup \{1, 2\}$ ja $f_j(x) = O(g_j(x))$. Sel juhul leiduvad vastavalt definitsioonile 1.19 konstant $K_j > 0$ ja naturaalarv M_j nii, et iga $x > M_j$ korral

$$|f_j(x)| \leq K|g_j(x)|.$$

Lisaks, olgu $f(x) = O(g(x))$, st leiduvad konstant $K > 0$ ja naturaalarv $M > 0$ nii, et iga $x > M$ korral

$$|f(x)| \leq K|g(x)|.$$

1. On lihtne näha, et võrdus kehtib, kui valida definitsioonis 1.19 $K = 1$.

2. Olgu $f_1(x) = O(f_2(x))$, kus $f_2(x) = O(f_3(x))$. Näitame, et siis $f_1(x) = O(f_3(x))$. Et $f_1(x) = O(f_2(x))$ ja $f_2(x) = O(f_3(x))$, siis valides $M := \max\{M_1, M_2\}$ saame, et iga $x > M$ korral

$$|f_1(x)| \leq K_1|f_2(x)| \leq K_1K_2|f_3(x)|$$

ehk $f_1(x) = O(f_3(x))$, nagu soovitud.

3. Kui $f(x) = O(g(x))$, siis

$$|kf(x)| = |k| \cdot |f(x)| \leq |k| \cdot K|g(x)| = K|k||g(x)| \text{ iga } x \geq M \text{ korral.}$$

4. Valime arvud M_3 ja K_3 selliselt, et $M_3 := \max\{M_1, M_2\}$ ning $K_3 := \max\{K_1, K_2\}$. Siis

$$\begin{aligned} |f_1(x) + f_2(x)| &\leq |f_1(x)| + |f_2(x)| \leq K_1 g_1(x) + K_2 g_2(x) \leq K_3 g_1(x) + K_3 g_2(x) \\ &= K_3(g_1(x) + g_2(x)) \text{ iga } x \geq M_3 \text{ korral,} \end{aligned}$$

mis tähendab, et $f_1(x) + f_2(x) = O(g_1(x) + g_2(x))$.

5. Valime $M_3 := \max\{M_1, M_2\}$, siis iga $x \geq M_3$ korral kehtivad mõlemad võrratused ning saame kirjutada:

$$|f_1(x)f_2(x)| = |f_1(x)||f_2(x)| \leq K_1|g_1(x)|K_2|g_2(x)| = K_1K_2|g_1(x)g_2(x)|$$

ning järelikult $f_1(x)f_2(x) = O(g_1(x)g_2(x))$.

6. Kehtigu iga $i \in I$ korral $g_i(x) = O(f_i(x))$. Vaatleme nüüd summat $\sum_i g_i(x)$. Võttes $M := \max\{M_1, M_2, \ldots, M_{|I|}\}$ ja $K := \max\{K_1, K_2, \ldots, K_{|I|}\}$, siis iga $x > M$ korral

$$\left|\sum_{i\in I} g_i(x)\right| \leq \sum_{i\in I} |g_i(x)| \leq \sum_{i\in I} K_i|f_i(x)| \leq \sum_{i\in I} K|f_i(x)| = K\sum_{i\in I} |f_i(x)|.$$

Suure-O notatsiooni definitsiooni kohaselt olemegi saanud, et kehtib $\sum_i g_i(x) = O\left(\sum_i f_i(x)\right)$. □

Definitsioon 1.21. *Olgu $A \subseteq \mathbb{R}$, $B = \mathbb{C}$ või $B = \mathbb{R}$ ja ∞ hulga A kuhjumispunkt. Kui $\alpha : A \to B$ ja $\beta : A \to B$ on mingid funktsioonid, siis kirjutatakse, et $\alpha \in o(\beta)$, kui*

$$\forall K > 0\ \exists M > 0 : \forall x \in D\ x > M \Rightarrow |\alpha(x)| \leq K|\beta(x)|,$$

kus $|\cdot|$ võib tähistada nii absoluutväärtust kui ka moodulit.

Lause 1.22. *Eelnevalt defineeritud o notatsioonil on järgmised omadused:*

1. *Kui $f(x) = o(g(x))$, siis $f(x) = O(g(x))$.*

2. *Kui* $g(x) = O(f(x))$ *ja* $f(x) = o(h(x))$, *siis* $g(x) = o(h(x))$.

3. *Kui* $g(x) = O(f(x))$ *ja* $f(x) = o(1)$, *siis* $g(x) = o(1)$.

Tõestus. 1. Olgu $f(x) = o(g(x))$. Fikseerime $K > 0$. Siis väikese o definitsiooni 1.21 põhjal leidub $M > 0$ nii, et iga $x \in D$ ja $x > M$ korral

$$|\alpha(x)| \leq K|\beta(x)|.$$

Olemegi leidnud definitsiooni 1.19 jaoks sobiva K.

2. Olgu $g(x) = O(f(x))$ ja $f(x) = o(h(x))$. Fikseerime $K > 0$. Peame näitama, et leidub $M > 0$ nii, et iga $x > M$ korral

$$|g(x)| \leq K|h(x)|.$$

Et $g(x) = O(f(x))$, siis leiduvad $K_1 > 0$ ja $M_1 > 0$ nii, et iga $x > M_1$ korral $|g(x)| \leq K_1|f(x)|$. Lisaks seose $f(x) = o(h(x))$ põhjal leidub M_2 nii, et iga $x > M_2$ korral $|f(x)| \leq \dfrac{K}{K_1}|h(x)|$. Võttes nüüd $M := \max\{M_1, M_2\}$, siis iga $x > M$ korral

$$|g(x)| \leq K_1|f(x)| \leq K_1 \cdot \frac{K}{K_1}|h(x)| = K|h(x)|$$

nagu tarvis.

3. Valides omaduses (2) funktsiooniks h sellise funktsiooni, mis on konstantselt 1, saamegi konkreetse omaduse tõestatud. $\square$

2 Aritmeetilised funktsioonid

Selles peatükis anname ülevaate aritmeetilistest funktsioonidest ja nende olulisematest omadustest, mida kasutame töö põhiosas.

Lepime kokku, et edaspidiselt on summade indeksid positiivsed täisarvud, näiteks summa $\sum\limits_{de \leq n} f(d)g(e)$ indeksi korral eeldame, et $d, e \in \mathbb{N}$.
Esmalt defineerime aritmeetilise funktsiooni.

Definitsioon 2.1. *Funktsiooni $f : \mathbb{N} \to K, K \subseteq \mathbb{C}$ nimetatakse aritmeetiliseks funktsiooniks.*

Näiteks Euleri funktsioon φ on aritmeetiline funktsioon.

Definitsioon 2.2. *Aritmeetilist funktsiooni f nimetatakse nõrgalt multiplikatiivseks, kui selle väärtus on vähemalt ühe naturaalarvu korral nullist erinev ja*

$$f(mn) = f(m)f(n), \text{ kui } (m, n) = 1.$$

Kui viimane võrdus kehtib mistahes naturaalarvude m ja n korral, nimetatakse funktsiooni f multiplikatiivseks.

Järgnevalt tutvume Dirichlet' korrutisega, mida kasutatakse eeskätt Dirichlet' ridade uurimisel.

Definitsioon 2.3. *Olgu f ja g aritmeetilised funktsioonid. Nende funktsioonide Dirichlet' korrutiseks nimetame aritmeetilist funktsiooni h kujul*

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Sellist funktsiooni h märgime tähisega $f * g$.

Lemma 2.4. *Olgu $m, n \in \mathbb{N}$. Kui $(m, n) = 1$ ning $a|m$ ja $b|n$, siis $(a, b) = 1$.*

Tõestus. Oletame vastuväiteliselt, et $d := (a, b) > 1$. Kuna $d|a$ ja $d|b$, siis ka $d|m$ ning $d|n$, mis on aga vastuolus eeldusega $(m, n) = 1$. Seega $(a, b) = 1$. □

Lemma 2.5. *Olgu $m, n \in \mathbb{N}$. Kui $(m, n) = 1$, siis saame iga korrutise mn positiivse jagaja c üheselt esitada kujul $c = ab$ nii, et $a, b \in \mathbb{N}$, $a|m$, $b|n$, ja $(a, b) = 1$.*

Tõestus. Olgu c korrutise mn jagaja ning $d = (c, m)$. Definitsiooni 1.2 kohaselt siis $d|c$ ja $d|m$. Järelikult leiduvad sellised täisarvud c' ja m', et $c'd = c$ ja $m'd = m$. Märgime, et $(c', m') = 1$, sest vastasel juhul leiduks suurem ühistegur kui d. Nüüd, et $c|mn$, siis leidub selline täisarv e, et $ce = mn$. Asendame saadud võrduses c ja m eelnevalt avaldatud kujudega ning saame $c'de = m'dn$. Et $d \neq 0$, sest $m > 0$, saame taandada d ning alles jääb $c'e = m'n$. Et $(c', m') = 1$, siis $c'|n$ ning oleme leidnud sellised täisarvud c' ja d, et $c'|n$ ja $d|m$. Lemma 2.4 kohaselt $(c', d) = 1$. Järelikult oleme leidnud sellised naturaalarvud $a = d$ ja $b = c'$, mida vaja.

Näitame, et a ja b on üheselt määratud. Oletame, et leiduvad veel sellised arvud a' ja b', et $c = a'b'$, $a'|m$, $b'|n$ ja $(a', b') = 1$. Sel juhul $c = ab = a'b'$. Et $(m, n) = 1$, $a|m$ ja $b'|n$, siis järelikult $(a, b') = 1$. Kuna $a|c = a'b'$ ja $(a, b') = 1$, siis peab kehtima $a|a'$. Analoogselt, et $a'|m$, $b|n$ ning $(m, n) = 1$, siis $(a', b) = 1$. Kuna $a'|c = ab$ ja $(a', b) = 1$, kehtib $a'|a$. Nüüd et $a|a'$ ja $a'|a$, siis $|a| = |a'|$ ja kuna $a, a' \in \mathbb{N}$, siis järelikult $a = a'$.

Vaatleme uuesti võrdust $ab = a'b'$. Et $a = a' \neq 0$, sest $m > 0$, saame need taandada ja alles jääb $b = b'$. Seega on a ja b üheselt määratud. □

Lause 2.6. *Dirichlet' korrutise korral*

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{db=n} f(d) g(b).$$

Tõestus. Paneme tähele, et $\{(d, n/d) \mid d|n\} = \{(d, b) \mid db = n\}$. □

Teoreem 2.7. *Dirichlet' korrutis on kommutatiivne ja assotsiatiivne.*

Tõestus. Lause 2.6 kohaselt saame kirjutada

$$(f * g)(n) = \sum_{db=n} f(d)g(b).$$

Sellest järeldub $f * g$ kommutatiivsus, sest

$$(f * g)(n) = \sum_{bd=n} f(d)g(b) = \sum_{db=n} g(b)f(d) = (g * f)(n).$$

Assotsiatiivsuse jaoks tähistagu $A := g*k$ ning vaatleme korrutist $f*A = f*(g*k)$:

$$\begin{aligned}(f * A)(n) &= \sum_{a \cdot d=n} f(a)A(d) = \sum_{ad=n} f(a) \sum_{bc=d} g(b)k(c) \\ &= \sum_{abc=n} f(a)g(b)k(c).\end{aligned}$$

Defineerime nüüd $B := f * g$ ja vaatleme korrutist $B * k$:

$$\begin{aligned}(B * k)(n) &= \sum_{dc=n} B(d)k(c) = \sum_{dc=n} k(c) \sum_{ab=d} f(a)g(b) \\ &= \sum_{abc=n} f(a)g(b)k(c)\end{aligned}$$

Seega $f * A = B * k$ ning järelikult on Dirichlet' korrutis assotsiatiivne. □

Lause 2.8. *Kui f on nõrgalt multiplikatiivne, siis $f(1) = 1$.*

Tõestus. Et $(n, 1) = 1$ iga n korral, siis $f(n) = f(1 \cdot n) = f(1)f(n)$. Kuna f ei ole konstantselt 0, siis $f(n) \neq 0$ mingi n korral. Seega $f(1) = 1$. □

Teoreem 2.9. *Kui f ja g on nõrgalt multiplikatiivsed, on ka nende Dirichlet' korrutis $f * g$ nõrgalt multiplikatiivne.*

Tõestus. Näitamaks, et Dirichlet' korrutis $h = f * g$ ei ole konstantselt 0, vaatame korrutist kohal 1 ehk

$$h(1) = \sum_{d|1} f(d)g\left(\frac{1}{d}\right) = f(1)g(1) = 1.$$

Järelikult ei ole h konstantselt 0.

Olgu m, n sellised naturaalarvud, et $(m, n) = 1$. Sel juhul

$$h(mn) = \sum_{c|mn} f(c)g\left(\frac{mn}{c}\right).$$

Et f ja g ise on nõrgalt multiplikatiivsed, saame kasutada lemmat 2.5, et kirjutada $c = ab$. Paneme siinkohal tähele, et lemma 2.4 kohaselt $(a, b) = 1$ ning samamoodi $\left(\frac{m}{a}, \frac{n}{b}\right) = 1$. Seega saame kirjutada

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m,\ b|n \\ (a,b)=1}} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m,\ b|n \\ (a,b)=1}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{\substack{b|n \\ (a,b)=1}} f(b)g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) = h(m)h(n). \end{aligned}$$

Järelikult on Dirichlet' korrutis h nõrgalt multiplikatiivne. $\square$

Definitsioon 2.10. *Defineerime aritmeetilise ühikfunktsiooni u nii, et*

$$u(n) = 1 \textit{ mistahes } n \textit{ korral.}$$

Mõnikord saab osasummasid lähendada integraalidega. Järgmine teoreem annab meile sellisel lähendamisel tekkiva vea täpse avaldise.

Teoreem 2.11 (Euleri summa valem)**.** *Kui funktsioonil f on intervallis $[y, x]$, kus*

$0 < y < x$, *pidev tuletis* f', *siis*

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)([x]-x) - f(y)([y]-y). \quad (2.1)$$

Tõestus. Olgu $m = [y], k = [x]$ ning n ja $n-1$ täisarvud intervallis $[y, x]$. Siis

$$\begin{aligned}\int_{n-1}^{n} [t]f'(t)dt = \int_{n-1}^{n} (n-1)f'(t)dt &= (n-1)(f(n) - f(n-1)) \\ &= (nf(n) - (n-1)f(n-1)) - f(n).\end{aligned}$$

Kasutades seda tähelepanekut saame

$$\begin{aligned}\int_m^k [t]f'(t)dt &= \int_m^{m+1} [t]f'(t)dt + \int_{m+1}^{m+2} [t]f'(t)dt + \ldots + \int_{k-1}^{k} [t]f'(t)dt \\ &= \sum_{n=m+1}^{k} (nf(n) - (n-1)f(n-1)) - \sum_{n=m+1}^{k} f(n) \\ &= -\sum_{n=m+1}^{k} ((n-1)f(n-1) - nf(n)) - \sum_{n=m+1}^{k} f(n) \\ &= -mf(m) + (m+1)f(m+1) - (m+1)f(m+1) \\ &\quad + (m+2)f(m+2) - (m+2)f(m+2) + \ldots \\ &\quad + (k-1)f(k-1) - (k-1)f(k-1) + kf(k) - \sum_{n=m+1}^{k} f(n) \\ &= kf(k) - mf(m) - \sum_{n+1}^{k} f(n) \\ &= kf(k) - mf(m) - \sum_{y<n\leq x} f(n).\end{aligned}$$

Seega

$$
\begin{aligned}
\sum_{y<n\le x} f(n) &= -\int_m^k [t]f'(t)dt + kf(k) - mf(m)\\
&= \left(-\int_y^m [t]f'(t)dt - \int_m^k [t]f'(t)dt - \int_k^x [t]f'(t)dt \right) + kf(k) - mf(m)\\
&\quad + \int_y^m [t]f'(t)dt + \int_k^x [t]f'(t)dt\\
&= -\int_y^x [t]f'(t)dt + kf(k) - mf(m) - \int_m^y [t]f'(t)dt + \int_k^x [t]f'(t)dt\\
&= -\int_y^x [t]f'(t)dt + kf(k) - mf(m) - \int_m^y mf'(t)dt + \int_k^x kf'(t)dt\\
&= -\int_y^x [t]f'(t)dt + kf(k) - mf(m) - mf(y) + mf(m) + kf(x) - kf(k)\\
&= -\int_y^x [t]f'(t)dt + kf(x) - mf(y). \qquad (2.2)
\end{aligned}
$$

Ositi integreerides saame, et

$$\int_y^x tf'(t)dt = tf(t)\Big|_y^x - \int_y^x f(t)dt = xf(x) - yf(y) - \int_y^x f(t)dt$$

ehk järelikult

$$\int_y^x f(t)dt = xf(x) - yf(y) - \int_y^x tf'(t)dt$$

ja

$$\int_y^x tf'(t)dt - xf(x) + yf(y) + \int_y^x f(t)dt = 0.$$

Kombineerides seda võrdusega (2.2) saame, et

$$\begin{aligned}\sum_{y<n\leq x} f(n) &= -\int_y^x [t]f'(t)dt + kf(x) - mf(y)\\ &= -\int_y^x [t]f'(t)dt + [x]f(x) - [y]f(y)\\ &\quad + \left(\int_y^x tf'(t)dt - xf(x) + yf(y) + \int_y^x f(t)dt\right)\\ &= \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)([x]-x) - f(y)([y]-y),\end{aligned}$$

mis ongi võrdus (2.1). □

Märgime siinkohal ära, et Riemanni dzeetafunktsioon on defineeritud kõigi kompleksarvude jaoks, kuid meil on tarvis definitsiooni vaid positiivsete reaalarvude korral. Seega anname selles töös dzeetafunktsiooni definitsiooni järgmiselt.

Definitsioon 2.12. *Riemanni dzeetafunktsioon $\zeta(s)$ on defineeritud võrdustega*

$$\zeta(s) = \begin{cases} \sum_{n=1}^{\infty} \frac{1}{n^s}, & \textit{kui } s > 1, \\ \lim_{x\to\infty} \left(\sum_{n\leq x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right), & \textit{kui } 0 < s < 1. \end{cases}$$

Järgmisena tõestame Euleri summa valemist järelduva asümptootilise valemi üldistatud harmoonilise rea jaoks.

Teoreem 2.13. *Kui $x \geq 1$, $s > 0$ ja $s \neq 1$ siis:*

$$\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s}). \tag{2.3}$$

Tõestus. Võrduse (2.3) tõestamiseks kasutame Euleri summa valemit (2.1). Selleks valime $f(t) = t^{-s}$, kus $s > 0, s \neq 1$. Selle funktsiooni tuletis $f'(t) = -st^{-s-1}$ on $x \geq 1$ korral pidev ning seega pidev ka igas lõigus $[1, x]$. Et saaksime Euleri summa valemit rakendada, peab kehtima $1 < x$, kuid meil on hetkel $1 \le x$, seega vaatame liiget $x = 1$ eraldi. Valemi (2.11) abil saame nüüd kirjutada

$$\sum_{1 \le n \le x} \frac{1}{n^s} = 1 + \sum_{1 < n \le x} \frac{1}{n^s} = 1 + \int_1^x \frac{dt}{t^s} - s \int_1^x \frac{t - [t]}{t^{s+1}} dt - \frac{x - [x]}{x^s} + 0.$$

Märgime siinkohal, et funktsioonid $\frac{t-[t]}{t^{s+1}}$ ja $\frac{1}{t^{s+1}}$ on mõlemad integreeruvad, kui $t \in (0, \infty)$ ning mistahes t korral kehtib $0 \le \frac{t-[t]}{t^{s+1}} \le \frac{1}{t^{s+1}}$. Seega lause 1.16 kohaselt, kuna mistahes $u \in [1, \infty)$ korral $\int_u^\infty \frac{dt}{t^{s+1}} = -\frac{1}{st^s}\Big|_u^\infty = \frac{1}{su^s}$, siis päratu integraal $\int_u^\infty \frac{t-[t]}{t^{s+1}} dt$ koondub. Seega võime kirjutada $\int_1^x \frac{t-[t]}{t^{s+1}} dt = \int_1^\infty \frac{t-[t]}{t^{s+1}} dt - \int_x^\infty \frac{t-[t]}{t^{s+1}} dt$.

Kusjuures kehtib järgmine hinnang

$$0 \le \int_x^\infty \frac{t-[t]}{t^{s+1}} dt \le \int_x^\infty \frac{1}{t^{s+1}} dt = -\frac{1}{st^s}\Big|_x^\infty = \frac{1}{sx^s} = \frac{1}{s} x^{-s}.$$

Järelikult definitsiooni 1.19 ja lause 1.20 kohaselt $\int_x^\infty \frac{t-[t]}{t^{s+1}} dt = \frac{1}{s} O(x^{-s})$.

Lisaks, $0 \le x - [x] \le 1$, kui $x \ge 1$ ning seega ka $0 \le \frac{x-[x]}{x^s} \le \frac{1}{x^s}$. Järelikult $\frac{x-[x]}{x^s} = O\left(\frac{1}{x^s}\right)$.

Arvestades eelnevaid tähelepanekuid, saame

$$\begin{aligned}
\sum_{1 \le n \le x} \frac{1}{n^s} &= \int_1^x \frac{dt}{t^s} + 1 - s \left(\int_1^\infty \frac{t-[t]}{t^{s+1}} dt - \int_x^\infty \frac{t-[t]}{t^{s+1}} dt \right) + O(x^{-s}) \\
&= \frac{t^{-s+1}}{-s+1}\Big|_1^x + 1 - s \int_1^\infty \frac{t-[t]}{t^{s+1}} dt + s \cdot \frac{1}{s} O(x^{-s}) + O(x^{-s}) \\
&= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s \int_1^\infty \frac{t-[t]}{t^{s+1}} dt + O(x^{-s}).
\end{aligned}$$

Seetõttu

$$\sum_{n\le x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+C(s)+O(x^{-s}), \tag{2.4}$$

kus

$$C(s)=1-\frac{1}{1-s}-s\int_1^{\infty}\frac{t-[t]}{t^{s+1}}dt.$$

Kui $s>1$, siis kui $x\to\infty$, läheneb võrduses (2.4) summa $\sum_{n\le x}\frac{1}{n^s}$ Riemanni dzeeta-funktsioonile $\zeta(s)$ ning $x^{1-s}\to 0$ ja $x^{-s}\to 0$. Lisaks, lause 1.22 omaduse (3) tõttu $O(x^{-s})\to 0$ ning seega $C(s)=\zeta(s)$, kui $s>1$.

Kui $0<s<1$, siis $x^{-s}\to 0$ ning seetõttu ka $O(x^{-s})\to 0$ ja võrdusest (2.4) järeldub

$$\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s}\right)=\lim_{x\to\infty}\left(\frac{x^{1-s}}{1-s}+C(s)+O(x^{-s})-\frac{x^{1-s}}{1-s}\right)=C(s)$$

Järelikult $C(s)=\zeta(s)$, kui $0<s<1$. Sellega on ka võrdus (2.3) tõestatud. □

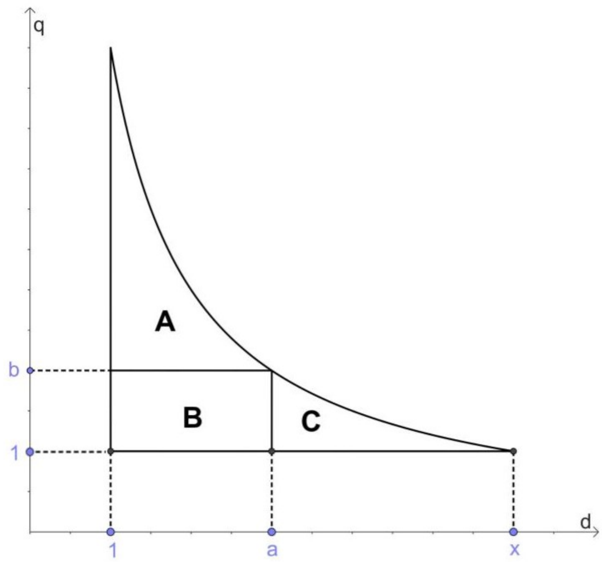
Nüüd tõestame teoreemi, mis võimaldab meil avaldada Dirichlet' korrutisi sisaldavat summat edaspidi vajalikul kujul.

Selleks märgime ära mõned tähistused: Olgu f ja g aritmeetilised funktsioonid ning

$F(x)=\sum_{n\le x}f(n),$

$G(x)=\sum_{n\le x}g(n)$

$H(x)=\sum_{n\le x}(f*g)(n)$, nii et



Joonis 1: Hüperbool

$$H(x) = \sum_{n \le x} \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{\substack{q,d \\ qd \le x}} f(d) g(q).$$

Teoreem 2.14. *Kui a ja b on sellised positiivsed reaalarvud, et $ab = x$, siis*

$$H(x) = \sum_{n \le a} f(n) G\left(\frac{x}{n}\right) + \sum_{n \le b} g(n) F\left(\frac{x}{n}\right) - F(a)G(b). \tag{2.5}$$

Tõestus. Edaspidi nimetame täisarvuliste koordinaatidega koordinaattasandi punkte võrepunktideks. Summa $H(x)$ on võetud üle võrepunktide kujul $qd = n$, kus $n = 1, 2, \ldots, [x]$ ehk $H(x) = \sum_{\substack{q,d \\ qd \le x}} f(d)g(q)$. Antud võrepunktide hulk on kujutatud joonisel 1. Jagame selle summa kaheks osaks, üks üle $A \cup B$ kuuluvate ja teine $B \cup C$ kuuluvate võrepunktide. Piirkonda B jäävad võrepunktid on kahekordselt loetud. Seega saame kasutades eelnevaid tähistusi

$$\begin{aligned}
H(x) &= \sum_{d \le a} \sum_{q \le \frac{x}{d}} f(d)g(q) + \sum_{q \le b} \sum_{d \le \frac{x}{q}} f(d)g(q) - \sum_{d \le a} \sum_{q \le b} f(d)g(q) \\
&= \sum_{d \le a} f(d) \sum_{q \le \frac{x}{d}} g(q) + \sum_{q \le b} g(q) \sum_{d \le \frac{x}{q}} f(d) - \sum_{d \le a} f(d) \sum_{q \le b} g(q) \\
&= \sum_{d \le a} f(d) G\left(\frac{x}{d}\right) + \sum_{q \le b} g(q) F\left(\frac{x}{q}\right) - F(a)G(b) \\
&= \sum_{n \le a} f(n) G\left(\frac{x}{n}\right) + \sum_{n \le b} g(n) F\left(\frac{x}{n}\right) - F(a)G(b),
\end{aligned}$$

mis on sama, mis võrdus (2.5). □

Järgmisena tõestame Abeli samasuse, mille abil saame treppfunktsioone esitada integraalide abil.

Teoreem 2.15 (Abeli samasus)**.** *Olgu $a(n)$ aritmeetiline funktsioon ning tähistame $A(x) = \sum_{n \le x} a(n)$, kui $x \ge 1$, ja $A(x) = 0$, kui $0 < x < 1$. Olgu f funktsioon, millel* *leidub pidev tuletis intervallis* $[y, x]$, *kus* $0 < y < x$. *Siis*

$$\sum_{y<n\le x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt. \tag{2.6}$$

Tõestus. Olgu $k = [x]$ ja $m = [y]$. Et $A(x) = \sum_{n\le x} a(n)$ ja $n \le x$ võtab naturaalarvulisi väärtuseid, siis $A(x) = \sum_{n\le x} a(n) = \sum_{n\le [x]} a(n) = A(k)$ ja $A(y) = A(m)$. Märgime, et $A(n) = a(1) + a(2) + \ldots + a(n-1) + a(n) = A(n-1) + a(n)$ ning seega $a(n) = A(n) - A(n-1)$. Lisaks, et $k = [x]$, siis

$$\begin{aligned} A(k)f(k) &= A(k)(f(x) - f(x) + f(k)) = A(k)f(x) - A(k)(f(x) - f(k)) \\ &= A(k)f(x) - A(k)\int_k^x f'(t)dt = A(k)f(x) - \int_k^x A(k)f'(t)dt \\ &= A(x)f(x) - \int_k^x A(x)f'(t)dt. \end{aligned}$$

Sarnaselt, et $m = [y]$, siis

$$\begin{aligned} A(m)f(m+1) &= A(m)(f(y) + f(m+1) - f(y)) = A(m)f(y) + A(m)\int_y^{m+1} f'(t)dt \\ &= A(y)f(y) + \int_y^{m+1} A(t)f'(t)dt. \end{aligned}$$

Veel, omaduse 1.14 kohaselt $A(n)\int_n^{n+1} f'(t)dt = \int_n^{n+1} A(t)f'(t)dt$, sest funktsioonid $A(n)f'(t)$ ja $A(t)f'(t)$ erinevad üksteisest vahemikus $n \le t \le n+1$ ainult punktis $t = n+1$. Kasutades neid teadmisi, saame

$$
\begin{aligned}
\sum_{y<n\le x} a(n)f(n) &= \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} (A(n)-A(n-1))f(n) \\
&= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1) \\
&= A(m+1)f(m+1) + A(m+2)f(m+2) + \ldots + A(k)f(k) \\
&\quad - A(m)f(m+1) - A(m+1)f(m+2) + \ldots + A(k-1)f(k) \\
&= \sum_{n=m+1}^{k-1} A(n)(f(n)-f(n+1)) + A(k)f(k) - A(m)f(m+1) \\
&= -\sum_{n=m+1}^{k-1} A(n)\int_{n}^{n+1} f'(t)dt + A(k)f(k) - A(m)f(m+1) \\
&= -\sum_{n=m+1}^{k-1} \int_{n}^{n+1} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1) \\
&= -\int_{m+1}^{k} A(t)f'(t)dt + A(x)f(x) - \int_{k}^{x} A(t)f'(t)dt \\
&\quad - A(y)f(y) - \int_{y}^{m+1} A(t)f'(t)dt \\
&= A(x)f(x) - A(y)f(y) - \int_{y}^{x} A(t)f'(t)dt.
\end{aligned}
$$

□

3 Lõplike Abeli rühmade karakterid

Meid huvitavad Dirichlet' karakterid, kuid nende üldised omadused on mugavam tõestada suuremal abstraktsuse astmel. Seega käsitleme siin peatükis lõplike Abeli rühmade karaktereid ning tõestame mõned nende omadused, mida järgmises peatükis kasutada saame.

Definitsioon 3.1. *Olgu G mistahes rühm. Funktsiooni $f : G \to \mathbb{C}$ nimetatakse rühma G karakteriks, kui see on multiplikatiivne, s.t. kui $f(c) \neq 0$ mingi $c \in G$ korral ja iga $a, b \in G$ korral*

$$f(ab) = f(a)f(b).$$

Teoreem 3.2. *Olgu G lõplik rühm ühikelemendiga e. Kui f on rühma G karakter, siis $f(e) = 1$ ja kui iga $a \in G$ korral $a^n = e$, siis $f(a)^n = 1$. See tähendab, et iga $a \in G$ korral on $f(a)$ mingi astme ühejuur.*

Tõestus. Olgu $c \in G$ selline, et $f(c) \neq 0$. Et $ce = c$, siis

$$f(c)f(e) = f(ce) = f(c)$$

ning seega jagades võrduse pooli arvuga $f(c)$ saame $f(e) = 1$. Kui $a \in G$ ja $a^n = 1$, siis $f(a)^n = f(a^n) = f(e) = 1$. Kui n on elemendi a järk rühmas G, siis $f(a)$ on n-nda astme ühejuur. $\square$

Definitsioon 3.3. *Olgu G rühm. Siis konstantne funktsioon $f(a) = 1$ on rühma G karakter. Seda funktsiooni nimetame edaspidi rühma G peakarakteriks.*

Olgu G lõplik rühm, G' selle alamrühm ning a mingi rühma G element. Siis võime tähele panna, et leidub selline $n \in N$ nii, et $a^n \in G'$. Tõepoolest, kui $a \in G'$, siis võtame $n = 1$. Kui nii ei ole, siis võttes $n = \text{ord}(a)$ kehtib $a^n = e \in G'$, aga see võib kehtida ka mõne väiksema n korral. Kuna naturaalarvude hulk on täielikult järjestatud, võime valida vähima sellise arvu n. Seetõttu on mõttekas järgmine definitsioon.

Definitsioon 3.4. *Naturaalarvu n nimetame elmendi $a \in G$ indikaatoriks alamrühmas G', kui see on vähim selline naturaalarv, mille korral $a^n \in G'$.*

Edaspidi vajame järgmist konstruktsiooni.

Teoreem 3.5. *Olgu G' lõpliku Abeli rühma G alamrühm, $G' \neq G$ ning $a \in G$ selline, et $a \notin G'$. Olgu h elemendi a indikaator alamrühmas G'. Siis korrutiste hulk*

$$G'' = \{xa^k : x \in G' \text{ ja } k = 0, 1, 2, \ldots, h-1\}$$

on G alamrühm, mis sisaldab alamrühma G'. Veelgi enam, $h > 1$ ja $|G''| = h|G'|$.

Tõestus. Näitame, et G'' on G alamrühm. Paneme tähele, et $e = ea^0 \in G''$, seega on G' mittetühi hulk. Lisaks märgime, et $h > 1$, sest $a^1 = a \notin G'$.

Veendume, et G'' on kinnine korrutamise suhtes. Valime kaks elemendi hulgast G'', olgu nendeks xa^k ja ya^j, kus $x, y \in G'$ ja $0 \leq k < h$, $0 \leq j < h$. Rühma G kommutatiivsusest $xa^k \cdot ya^j = x \cdot y \cdot a^{k+j}$. Saame summa $k + j$ panna kirja kujul $k + j = qh + r$, kus $0 \leq r < h$ ja $q, r \in \mathbb{Z}$. Seega

$$a^{k+j} = a^{qh+r} = a^{qh}a^r = za^r, \text{ kus } z = a^{qh} = (a^h)^q \in G',$$

sest $a^h \in G'$. Järelikult element $xa^k \cdot ya^j = (xyz)a^r = wa^r$, kus $w = xyz \in G'$ ja $0 \leq r < h$. Seega kuulub see element hulka G'' ja ühtlasi on see hulk kinnine korrutamise suhtes.

Järgmisena näitame, et G'' on kinnine pöördelemendi võtmise suhtes. Valime suvalise $xa^k \in G''$. Kui $k = 0$, siis selle elemendi pöördelement oleks x^{-1}. Et kui $x \in G'$, siis G' kinnisusest pöördelemendi suhtes ka $x^{-1} \in G'$, siis $(xa^k)^{-1} = x^{-1}a^0$ ning see element kuulub alamhulka G'' .

Kui aga $0 < k < h$, siis on pöördelemendiks

$$(xa^k)^{-1} = x^{-1}a^{-k} = (x^{-1}a^{-h})a^{h-k} = ya^{h-k},$$

kus $y = x^{-1}(a^h)^{-1}$. Kuna $x, a^h \in G'$, siis ka $y \in G'$. Lisaks, et $0 < k < h$, siis $0 < h - k < h$. Järelikult $ya^{h-k} \in G''$.

Sellega oleme näidanud, et G'' on G alamrühm ning G'' sisaldab endas alamrühma G', sest iga G' elemendi x saame kirja panna kujule xa^0 ja G'' elementide definitsiooni kohaselt $xa^0 \in G''$.

Näitame, et $|G''| = h|G'|$. Olgu $m = |G'|$. Seega on $x \in G'$ valikuid kokku m ning $0 \leq k < h$ valikuid kokku h. Seega korrutise xa^k moodustamiseks on kokku mh võimalust.

Näitame, et need on kõik erinevad. Vaatleme kaht elementi, $xa^k, ya^j \in G''$ ja oletame, et $xa^k = ya^j$, $0 \leq j \leq k < h$. Siis $a^{k-j} = x^{-1}y$ ja $0 \leq k - j < h$. Et $x^{-1}y \in G'$, peab element a^{k-j} samuti kuuluma alamrühma G', aga kuna h on a indikaator rühmas G', siis ei ole võimalik, et $k - j$ on naturaalarv. Järelikult $k - j = 0$ ehk $k = j$ ning seega ka $x = y$. $\square$

Teeme nüüd kindlaks, mitu karakterit lõplikul Abeli rühmal leidub.

Teoreem 3.6. *Lõplikul n. järku Abeli rühmal on täpselt n erinevat karakterit.*

Tõestus. Tähistame eelmises teoreemis konstrueeritud alamrühma G'' tähisega $\langle G'; a\rangle$ ehk

$$\langle G'; a\rangle = \{xa^k : x \in G' \text{ ja } 0 \leq k < h\}.$$

Meenutame, et a oli selline element, mis ei kuulunud alamrühma G' ning h oli selle indikaator alamrühmas G'. Kasutame seda sama kontrukstsiooni, alustades alamrühmaga $G_1 = \{e\}$, kus e on G ühikelement. Kui nüüd $G_1 \neq G$, siis järelikult leidub rühmas G element a_1, $a_1 \notin G_1$. Saame konstrueerida uue alamrühma, G_2, nii, et $G_2 = \langle G_1; a_1\rangle$. Märgime, et selle alamrühma järk on eelmise teoreemi põhjal $h|G_1|$, kus h on elemendi a_1 indikaator alamrühmas G_1. Kuna $h > 1$, siis $|G_2| > |G_1|$ ja seega $G_1 \subset G_2$. Kui $G_2 \neq G$, siis leidub selline element $a_2 \in G$, mis ei kuulu rühma G_2 ja saame taas koostada uue alamrühma $G_3 = \langle G_2; a_2 \rangle$. Seda mõttekäiku jätkates saame elemendid $a_1, a_2, \ldots, a_t$ ning vastavad alamrühmad $G_1, G_2, \ldots, G_{t+1}$ nii, et

$$G_{r+1} = \langle G_r; a_r \rangle \text{ ja } G_1 \subset G_2 \subset \ldots \subset G_{t+1} = G.$$

Viimase võrduse võime kirjutada, sest rühm G on lõplik ning seega peab see protsess mingi hetk lõppema.

Kasutades sellist alamrühmade ahelat tõestame kogu teoreemi induktsiooniga näidates, et kui väide kehtib alamrühma G_r korral, siis kehtib see ka G_{r+1} korral.

Meil on alamrühmas G_1 ainult üks element ja ka ainult üks karakter, alamrühma G_1 peakarakter. Seega alamrühma järk ja karakterite arv on võrdsed ja teoreem kehtib 1 korral. Olgu nüüd alamrühma G_r järk m ja oletame, et alamrühmal G_r on kokku m karakterit. Tõestame teoreemi väite G_{r+1} jaoks.

Paneme tähele, et $G_{r+1} = \langle G_r; a_r \rangle$. Olgu h elemendi a_r indikaator rühmas G_r. See tähendab, et $a_r^h \in G_r$. Eelmisest teoreemist teame, et $|G_{r+1}| = h \cdot |G_r| = mh$. Peame näitama, et rühmal G_{r+1} leidub täpselt mh karakterit. Selleks näitame, et iga G_r karakteri puhul on täpselt h võimalust jätkata seda rühma G_{r+1} karakteriks ja et rühma G_{r+1} iga karakter on rühma G_r mingi karakteri jätk. Esimesest saame, et rühmal G_{r+1} on kõige vähem mh karakterit, teisest aga, et teisi karaktereid ei ole ehk kokkuvõttes leidubki rühmal G_{r+1} täpselt mh karakterit.

Iga alamrühma G_{r+1} element on kujul xa_r^k, kus $x \in G_r$ ja $0 \leq k < h$. Oletame, et meil on võimalik jätkata G_r karakterit f rühma G_{r+1} karakteriks $\tilde{f}$. Et $\tilde{f}$ on G_{r+1} karakter, on see multiplikatiivne ning järelikult

$$\tilde{f}(xa_r^k) = \tilde{f}(x)(\tilde{f}(a_r))^k.$$

Kuna $x \in G_r$ ja $\tilde{f}$ on karakteri f jätk, siis kehtib $\tilde{f}(x) = f(x)$ ja $\tilde{f}(xa_r^k) = f(x)(\tilde{f}(a_r))^k$. Sellest võrdusest saame, et kui me teame $\tilde{f}(a_r)$ väärtust, saame defineerida $\tilde{f}(xa_r^k)$ ehk saame määrata karakteri $\tilde{f}$ iga G_{r+1} elemendi korral. Uurime $\tilde{f}(a_r)$ kõiki võimalikke väärtuseid. Olgu $c = a_r^h$, sel juhul $c \in G_r$ ning järelikult $\tilde{f}(c) = f(c)$. Karakteri $\tilde{f}$ multiplikatiivsuse tõttu $\tilde{f}(c) = \tilde{f}(a_r^h) = (\tilde{f}(a_r))^h$ ja seega $(\tilde{f}(a_r))^h = f(c)$. Kuna f on juba määratud, siis on meile $f(c)$ väärtus teada, see on kompleksarv. Nii et $\tilde{f}(a_r)$ on üheks arvu $f(c)$ h. juureks. Järelikult on $\tilde{f}(a_r)$ jaoks kõige rohkem h valikut. Selleks, et funktsioon $\tilde{f}$ oleks rühma G_{r+1} karakter on tarvilik defineerida see nii nagu eelnevalt tegime, see tähendab $\tilde{f}(xa_r^k) = f(x)(\tilde{f}(a_r))^k$, kus $\tilde{f}(a_r)$ on $f(a_r^h)$ h. juur. Näitame, et on ka piisav, st iga selliselt defineeritud $\tilde{f}$ on tõepoolest karakter.

Kuna eelmise teoreemi tõestuses näitasime, et iga G'' element esitub üheselt kujul xa^k, siis on $\tilde{f}$ korrektselt defineeritud.

Teame, et $\tilde{f}(a_r)$ valikuid on kokku h ja need on kõik erinevad, sest $f(c) \neq 0$ ning järelikult leidub kompleksarvul $f(c)$ h. juuri täpselt h tükki. Seega on meil karakteri f jätkamiseks karakteriks $\tilde{f}$ ka kokku h võimalust. Kontrollime, kas $\tilde{f}$ on multiplikatiivne. Valime kaks elementi rühmast G_{r+1}, olgu need xa_r^k ja ya_r^j. Jagame arvu $k+j$ jäägiga ja saame $k+j = qh+s$, kus $0 \leq s < h$. Kuna $a_r^h \in G_r$, siis kasutades karakteri f multiplikatiivsust ja $\tilde{f}$ definitsiooni saame

$$\begin{aligned}
\tilde{f}(xa_r^k)\tilde{f}(ya_r^j) &= f(x)(\tilde{f}(a_r))^k \cdot f(y)(\tilde{f}(a_r))^j = f(x)f(y)(\tilde{f}(a_r))^{k+j} \\
&= f(x)f(y)(\tilde{f}(a_r))^{qh+s} = f(xy)(\tilde{f}(a_r))^{qh}(\tilde{f}(a_r))^s \\
&= f(xy)((\tilde{f}(a_r))^h)^q(\tilde{f}(a_r))^s = f(xy)(f(a_r^h))^q(\tilde{f}(a_r))^s \\
&= f(xy)f(a_r^{hq})(\tilde{f}(a_r))^s = f(xya_r^{hq})(\tilde{f}(a_r))^s \\
&= \tilde{f}(xya_r^{hq} \cdot a_r^s) = \tilde{f}(xya_r^{k+j}) = \tilde{f}(xa_r^k \cdot ya_r^j).
\end{aligned}$$

Kuna $G_r \subset G_{r+1}$, siis et f on karakter, leidub selline $c \in G_r$, et $f(c) \neq 0$. Järelikult $\tilde{f}(c) = f(c) \neq 0$ ehk $\tilde{f}$ ei ole konstantselt 0. Seega on $\tilde{f}$ rühma G_{r+1} karakter.

Kõik jätkud on erinevad, sest ühe ja sama karakteri jätkamisel on kõik $\tilde{f}(a_r)$ väärtused erinevad, seega on erinevad ka kõik karakterid, ning kui jätkata erinevaid karaktereid on kõik jätkud erinevad, sest karakterid, mida jätkame, on erinevad.

Seega saame kõiki alamrühma G_r karaktereid, mida on kokku m, jätkata h erineval viisil, et saada G_{r+1} karakterid. Veelgi enam, kui b on mistahes G_{r+1} karakter, siis selle ahend alamrühmale G_r on ka G_r karakter. Nimelt, kuna b on multiplikatiivne hulgal G_{r+1}, siis on ta multiplikatiivne ka tema alamhulgal G_r. Kui mingi $c \in G_{r+1}$ korral $b(c) \neq 0$, siis G_{r+1} konstruktsiooni tõttu $c = xa^k$, kus $x \in G_r$ ja $0 \leq k < h$ ja seega $b(c) = b(xa^k) = b(x)b(a)^k \neq 0$ mistõttu $b(x) \neq 0$. □

Märgime need n erinevat n. järku lõpliku Abeli rühma karakterit tähistega $f_1, f_2, \ldots, f_n$, kus f_1 on peakarakter.

Teoreem 3.7. *Kui karakterite korrutamine on defineeritud kui $(f_i f_j)(a) = f_i(a)f_j(a)$ iga $a \in G$ korral, siis rühma G karakterite hulk moodustab n. järku Abeli rühma G^*, mille ühikelement on peakarakter f_1.*

Tõestus. Karakterite korrutamise kommutatiivsus ja assotsiatiivsus rühmal G^* järeldub kompleksarvude korrutamise kommutatiivsusest ja assotsiatiivsusest. Kui $f, g \in G^*$, siis iga $a, b \in G$ korral

$$(fg)(ab) = f(ab)g(ab) = f(a)f(b)g(a)g(b) = f(a)g(a)f(b)g(b) = (fg)(a) \cdot (fg)(b)$$

ning teoreemi 3.2 kohaselt $(fg)(e) = f(e)g(e) = 1 \neq 0$, mistõttu on kahe karakteri korrutis samuti karakter.

Olgu $f \in G^*$. Ühikelemendiks on peakarakter f_1, sest iga $a \in G$ korral

$$(ff_1)(a) = f(a)f_1(a) = f(a) \cdot 1 = f(a).$$

Elemendi f pöördelemendiks sobib funktsioon $\frac{1}{f}$, mis on defineeritud iga $a \in G$ korral kui $\left(\frac{1}{f}\right)(a) = \frac{1}{f(a)}$.

Et $f(a)$ on ühejuur, siis $f(a) \neq 0$ ning järelikult leidub $\frac{1}{f(a)}$. Seega sobib $\frac{1}{f(a)}$ pöördelemendiks, sest $a \in G$ korral $f(a) \cdot \left(\frac{1}{f}\right)(a) = f(a) \cdot \frac{1}{f(a)} = \frac{f(a)}{f(a)} = 1$.

On lihtne näha, et $\frac{1}{f}$ on tõepoolest karakter, sest mistahes $a \in G$ korral kehtib $\left(\frac{1}{f}\right)(a) = \frac{1}{f(a)} \neq 0$ ja $a, b \in G$ korral

$$\left(\frac{1}{f}\right)(a) \cdot \left(\frac{1}{f}\right)(b) = \frac{1}{f(a)} \cdot \frac{1}{f(b)} = \frac{1}{f(ab)} = \left(\frac{1}{f}\right)(ab).$$

□

Definitsioon 3.8. *Olgu D suvaline hulk ning antud funktsioon $f : D \to \mathbb{C}$. Märgime tähisega $\overline{f}$ sellist funktsiooni, et $\overline{f}(a) = \overline{f(a)}$ iga $a \in D$ korral.*

Lause 3.9. *Olgu f lõpliku Abeli rühma G karakter, siis funktsioon $\overline{f}$ on samuti rühma G karakter ning on karakteri f pöördelement rühmas G^*.*

Tõestus. Iga karakteri f korral kehtib $|f(a)| = 1$. Et $|f(a)| = f(a)\overline{f(a)}$, siis järelikult $\frac{1}{f(a)} = \overline{f(a)}$. Seega $\frac{1}{f} = \overline{f}$ ning teoreemi 3.7 kohaselt on $\overline{f}$ karakteri f pöördelement. Nii et $\overline{f}$ on samuti rühma G karakter. □

Olgu G mingi n. järku lõplik Abeli rühm, $G = \{a_1, a_2, \dots, a_n\}$ ja olgu $f_1, f_2, \dots, f_n$ G karakterid, kus f_1 on peakarakter.

Definitsioon 3.10. *Defineerime, et $A = A(G)$ on $n \times n$ maatriks $[a_{ij}]$, mille i-nda rea ja j-nda veeru element on $a_{ij} = f_i(a_j)$.*

Tõestame, et sellisel maatriksil A leidub pöördmaatriks ning hiljem kasutame seda karakterite ortogonaalsusseose tuletamiseks.

Teoreem 3.11. *Maatriksi A i-nda rea elementide summa S avaldub järgmiselt:*

$$S = \sum_{r=1}^{n} f_i(a_r) = \begin{cases} n, & \textit{kui } f_i \textit{ on peakarakter } (i = 1), \\ 0, & \textit{ülejäänud juhtudel.} \end{cases}$$

Tõestus. Kui $f_i = f_1$, on iga liidetav 1 ja $S = n$. Kui aga $f_i \neq f_1$, leidub G element b nii, et $f_i(b) \neq 1$. Et $a_r \in G$ ja G on lõplik Abeli rühm, siis ka $ba_r \in G$. Lemma 1.12 tõttu võime kirjutada

$$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b) \sum_{r=1}^{n} f_i(a_r) = f_i(b)S,$$

mistõttu $S(1 - f_i(b)) = 0$. Et $f_i(b) \neq 1$, siis järelikult $S = 0$. □

Kasutame seda teoreemi, et tõestada järgmist.

Teoreem 3.12. *Tähistagu A^* sellist $n \times n$ maatriksit, mis on saadud maatriksi A transponeerimisel ja elementhaaval kaaskompleksarvu võtmisel, st*

$$A^* = [b_{ij}] = [\overline{a_{ji}}].$$

Siis maatriks A on pööratav ja selle pöördmaatriks on $\frac{1}{n}A^*$.

Tõestus. Olgu $B = AA^*$. Maatriksi B i-ndas rea ja j-ndas veeru element b_{ij} on kujul

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\overline{f_j(a_r)} = \sum_{r=1}^{n} f_i(a_r)\overline{f}_j(a_r) = \sum_{r=1}^{n} (f_i\overline{f}_j)(a_r) = \sum_{r=1}^{n} f_k(a_r),$$

kus $f_k = f_i\overline{f}_j = \dfrac{f_i}{f_j}$ lause 3.9 tõttu. Võrdus $\dfrac{f_i}{f_j} = f_1$ kehtib pöördelemendi ühesuse tõttu siis ja ainult siis, kui $i = j$. Juhul $i \neq j$ saame peakarakterist erineva karakteri. Seega teoreemi 3.11 kohaselt saame, et

$$b_{ij} = \begin{cases} n, & \text{kui } i = j, \\ 0, & \text{kui } i \neq j. \end{cases}$$

Teisisõnu, $B = nI$, kus I on $n \times n$ järku ühikmaatriks. Sellest järeldub, et $\det(A) \neq 0$, mistõttu leidub maatriksil A teoreemi 1.13 põhjal pöördmaatriks A^{-1}

ning korrutades võrduse mõlemaid pooli elemendiga $\frac{1}{n}A^{-1}$ saame, et

$$A^{-1} = \left(\frac{1}{n}A^{-1}\right)(nI) = \frac{1}{n}A^{-1}B = \frac{1}{n}A^{-1}AA^* = \frac{1}{n}A^*.$$

□

Teoreem 3.13 (Karakterite ortogonaalsusseos)**.** *Kehtib*

$$\sum_{r=1}^{n} \overline{f}_r(a_i)f_r(a_j) = \begin{cases} n, & kui\ a_i = a_j, \\ 0, & kui\ a_i \neq a_j. \end{cases} \tag{3.1}$$

Tõestus. Maatriksi A pöördmaatriksi olemasolust järeldub, et $A^*A = nI$, sest $A^*A = nA^{-1}A = nI$. Aga maatriksi A^*A i-nda rea ja j-nda veeru element on võrdne võrduse (3.1) vasakul olev summaga. □

4 Dirichlet' karakterid

Selles peatükis tutvustame lugejale Dirichlet' karaktereid. Nende teooria on tunduvalt laiem, kuid siin kaetud materjal on valitud Dirichlet' teoreemi tõestuse ühe olulise sammu tõestamise eesmärgiga. See samm näitab, et reaalarvuliste väärtustega mitte-peakarakterite χ korral $L(1,\chi) \neq 0$.

Eelnevalt vaatasime mistahes lõpliku Abeli rühma G karaktereid. Selles peatükis vaatleme rühma $U(\mathbb{Z}_k)$, kus positiivne täisarv k on fikseeritud. Meenutame, et $U(\mathbb{Z}_k)$ on lõplik $\varphi(k)$. järku rühm.

Definitsioon 4.1. *Defineerime igale $U(\mathbb{Z}_k)$ karakterile f vastava aritmeetilise funktsiooni $\chi = \chi_f$ järgmiselt:*

$$\chi(n) = \begin{cases} f(\overline{n}), & kui\ (n,k) = 1, \\ 0, & kui\ (n,k) > 1. \end{cases}$$

Funktsiooni χ on nimetatakse Dirichlet' karakteriteks mooduli k järgi.

Dirichlet' peakarakteriks nimetatakse Dirichlet' karakterit χ_1, mis vastab rühma $U(\mathbb{Z}_k)$ peakarakterile f_1 ning seetõttu on defineeritud järgnevalt:

$$\chi_1(n) = \begin{cases} 1, & kui\ (n,k) = 1, \\ 0, & kui\ (n,k) > 1 \end{cases} \tag{4.1}$$

Kui $(n,k) = 1$, kehtib $\chi(n)^{\varphi(k)} = 1$ ehk $\chi(n)$ on $\varphi(k)$. astme ühejuur.

Lause 4.2. *Kui χ on Dirichlet' karakter mooduli k järgi, on seda ka $\overline{\chi}$.*

Tõestus. Kui $(n,k) > 1$, siis $\chi(n) = 0$ ning järelikult $\overline{\chi}(n) = \overline{\chi(n)} = 0$. Kui aga $(n,k) = 1$, siis $\overline{\chi}(n) = \overline{f}(\overline{n})$ ja et lause 3.9 kohaselt on $\overline{f}$ rühma $U(\mathbb{Z}_k)$ karakter saamegi, et $\overline{\chi}$ on Dirichlet' karakter. $\square$

Teoreem 4.3 (Dirichlet' karakterite omadused)**.** *Mooduli k järgi on kokku $\varphi(k)$ erinevat Dirichlet' karakterit. Kõik karakterid on multiplikatiivsed ning perioodilised perioodiga k, teisisõnu:*

$$\chi(mn) = \chi(m)\chi(n) \text{ iga } m,\ n \text{ korral ja}$$
$$\chi(n+k) = \chi(n) \text{ iga } n \text{ korral}$$

Teistpidi, kui χ on multiplikatiivne, perioodiline perioodiga k ning $(n,k) > 1$ korral $\chi(n) = 0$, on χ üks Dirichlet' karakteritest mooduli k järgi.

Tõestus. Teoreemi 3.6 kohaselt on rühmas $U(\mathbb{Z}_k)$ kokku $\varphi(k)$ karakterit f ning seega mooduli k järgi on kokku $\varphi(k)$ Dirichlet' karakterit χ_f.

Karakteri χ_f multiplikatiivsus järeldub sellest, et $\chi(1) = f(\overline{1}) = 1 \neq 0$ ning karakteri f multiplikatiivsusest juhul, kui $(m,k) = 1$ ja $(n,k) = 1$. Kui kas $(m,k) > 1$ või $(n,k) > 1$, siis ka $(mn,k) > 1$, seega Dirichlet' karakteri definitsiooni kohaselt $\chi(mn) = 0 = \chi(m)\chi(n)$.

Näitame, et χ on perioodiline. Arvuteooriast teame, et $(n+k,k) = (n,k)$. Seega kui $(n+k,k) = 1$, siis ka $(n,k) = 1$ ning kui $(n+k,k) > 1$, siis ka $(n,k) > 1$.

Vaatleme juhtu $(n+k,k) = 1$. Sel juhul $\chi_f(n+k) = f(\overline{n+k}) = f(\overline{n}) = \chi_f(n)$. Kui nüüd $(n+k,k) > 1$, siis $\chi_f(n+k) = 0 = \chi_f(n)$, sest ka $(n,k) > 1$. Järelikult mõlemas olukorras $\chi(n+k) = \chi(n)$ ja χ on perioodiline.

Vastupidise väite tõestamiseks näitame, et funktsioon $f : U(\mathbb{Z}_k) \to \mathbb{C}$, mis on defineeritud võrdusega

$$f(\overline{n}) = \chi(n), \text{ kui } (n,k) = 1,$$

on rühma $U(\mathbb{Z}_k)$ karakter. Sel juhul saamegi, et χ on Dirichlet' karakter mooduli k järgi.

Funktsiooni f definitsiooni korrektsus tuleneb χ perioodilisusest. Näitame, et f on multiplikatiivne. Kuna χ on multiplikatiivne, leidub mingi $c \in U(\mathbb{Z}_k)$, mille korral $\chi(c) \neq 0$. Järelikult $f(\overline{c}) = \chi(c) \neq 0$ ning f ei ole konstantselt 0.

Nüüd, et χ on multiplikatiivne, saame, et $f(\overline{mn}) = \chi(mn) = \chi(m)\chi(n) = f(\overline{m})f(\overline{n})$, kui $(n, k) = 1$ ja $(m, k) = 1$. Seega sellest, et f ei ole konstantselt 0 ja näidatust saame, et f on ka multiplikatiivne.

Nüüd eeldustest, et $\chi(n) = 0$, kui $(n, k) > 1$ ja sellest, et f on $U(\mathbb{Z}_k)$ karakter järeldub, et χ on tõepoolest Dirichlet' karakter mooduli k järgi. □

Toome paar näidet Dirichlet' karakteritest, kus funktsioonid esitame tabelkujul.

Näide 4.4. *Esmalt vaatame juhtu $k = 5$. Paneme tähele, et teoreemi 4.3 põhjal on mistahes multiplikatiivne ja perioodiline aritmeetiline funktsioon χ perioodiga 5, mille korral $\chi(n) = 0$, kui $(n, k) > 1$, alati Dirichlet' karakter mooduli 5 järgi, ja selliseid karaktereid on kokku $\varphi(5) = 4$ tükki. Seega on küllalt, kui konstrueerime 4 erinevat selliste omadustega funktsiooni.*

Perioodilisuse tõttu piisab, kui defineerime funktsioonid lõigul $[1, 5]$. Eelduse kohaselt $\chi(5) = 0$ ning seega jätame $n = 5$ veeru tabelist välja. Kui $1 \leq n < 5$, siis $\overline{n} \in U(\mathbb{Z}_5)$. Rühma $U(\mathbb{Z}_5)$ moodustaja on 2 ning seega $U(\mathbb{Z}_5) = \{\overline{2}, \overline{2^2}, \overline{2^3}, \overline{2^4}\}$.

Teoreemi 3.2 kohaselt on χ väärtused ühejuured. Et $\operatorname{ord}(2) = 4$, on järelikult $n = 2$ korral võimalikud väärtused ± 1 ja $\pm i$. Tabelisse saame kohe kirja panna, et peakarakter χ_1 on mistahes n korral 1 ja mistahes karakteri χ korral $\chi(1) = 1$. Seejärel täidame veeru $n = 2$. Kasutame χ multiplikatiivsust, et täita ka ülejäänud veerud. Näiteks veeru $n = 4$ saame täita järgmiselt: teame, et $\chi(2)\chi(2) = \chi(4)$, seega võttes veeru $n = 2$ elemendid ruutu, saame vastavad veeru $n = 4$ elemendid. Sedasi saamegi järgmise tabeli.

n	1	2	3	4
$\chi_1(n)$	1	1	1	1
$\chi_2(n)$	1	-1	-1	1
$\chi_3(n)$	1	i	$-i$	-1
$\chi_4(n)$	1	$-i$	i	-1

Märgime siinkohal veel ära, et konkreetses näites $\chi(2)\chi(3) = \chi(6) = \chi(1)$*, mis tähendab, et* $n = 3$ *korral saame veeru täidetud, kui kirjutame sinna veerus* $n = 2$ *asuvate arvude pöördväärtused. Tabeli kontrollimiseks saame kasutada teoreemi 3.11, mille kohaselt ühe rea elementide summa (v.a.* χ_1 *korral) peab olema* 0*.*

Näide 4.5. *Võtame* $k = 15$ *ja toimime sarnaselt eelmise näitega. Tabeli koostamiseks vaatame arve* $1 \leq n < 15$*, mille korral* $\overline{n} \in U(\mathbb{Z}_{15})$*. Määrame nende elementide järgud.*

$\overline{n}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
$\mathrm{ord}(\overline{n})$	1	4	2	4	4	2	4	2

Järkude määramise tulemusena näeme, et moodustajat ei ole. Küll aga valides 2 *ja* 11*, saame neid kombineerides kõik rühma* $U(\mathbb{Z}_{15})$ *elemendid kätte. Täpsemalt saame, et* $U(\mathbb{Z}_{15}) = \{\overline{2}, \overline{2^2}, \overline{2^3}, \overline{2^4}, \overline{2 \cdot 11}, \overline{2^2 \cdot 11}, \overline{2^3 \cdot 11}, \overline{2^4 \cdot 11}\}$*. Kasutame seda teadmist ning* χ *multiplikatiivsust ja perioodilisust ning koostame tabeli. Esmalt kanname sisse veerud* $n = 2$ *ja* $n = 11$ *jaoks. Et* $\overline{2}$ *järk on* 4*, on sellel neli võimalikku väärtust:* ± 1 *ja* $\pm i$*. Kirjutame need erinevad väärtused järjest üksteise alla. Teame, et* $\overline{11}$ *järk on* 2*, seega sellel on kokku kaks võimalikku väärtust:* 1 *ja* -1*. Kirjutame veergu* $n = 11$ *neli arvu* 1 *üksteise alla ja siis veel neli korda* -1*. Seejärel hakkame nende kahe veeru abil teisi veergusid täitma. Esmalt otsime arve, mis on teineteise pöördelemendid. Mooduli* 15 *korral on nendeks paarideks* 2 *ja* 8 *ning* 7 *ja* 13*. Seega veeru* $n = 8$ *saame, võttes veeru* $n = 2$ *elementidest pöördväärtused. Siis arvutame veeru* $\chi(7)$ *kasutades teadmist, et* $\chi(2)\chi(11) = \chi(7)$ *ja saame kohe täidetud ka* *veeru* $n = 13$, *võttes veeru* $n = 7$ *elementidest pöördväärtused. Kasutades eelnevalt leitud esitusi mooduli* 15 *järgi, mis on kujutatud tabeli esimesel real, saame täita ka ülejäänud tabeli. Näiteks* $\chi(2)^2 \cdot \chi(11) = \chi(2^2 \cdot 11) = \chi(14 + 2 \cdot 15) = \chi(14)$ *ehk veeru* $n = 2$ *vastava elemendi ruutu võtmisel ja vastava veeru* $n = 11$ *elemendiga korrutamisel, saame veeru* $n = 14$ *vastava elemendi.*

	2^4	2^1	2^2	$11 \cdot 2$	2^3	11	$11 \cdot 2^3$	$11 \cdot 2^2$
n	1	2	4	7	8	11	13	14
$\chi_1(n)$	1	1	1	1	1	1	1	1
$\chi_2(n)$	1	-1	1	-1	-1	1	-1	1
$\chi_3(n)$	1	i	-1	i	$-i$	1	$-i$	-1
$\chi_4(n)$	1	$-i$	-1	$-i$	i	1	i	-1
$\chi_5(n)$	1	1	1	-1	1	-1	-1	-1
$\chi_6(n)$	1	-1	1	1	-1	-1	1	-1
$\chi_7(n)$	1	i	-1	$-i$	$-i$	-1	i	1
$\chi_8(n)$	1	$-i$	-1	i	i	-1	$-i$	1

Paneme tähele, et kui mingi veeru täitmisel ilmub kuhugi ritta mitte-reaalarvuline ühejuur on meile kasulik lause 4.2. Selle kohaselt saame täita ühe järgnevatest ridadest nii, et võtame selle rea, milles oli vähemalt üks mitte-reaalarvuline ühejuur, kõikidest elementidest kaaskompleksid. Juhul, kui oleme mõned veerud juba ette täielikult ära täitnud, saame kaaskomplekside rea tabelisse sellegipoolest lisada ning ei pea eelnevalt täidetud veerge muutma, sest selline karakter peab alati leiduma.

Teoreem 4.6 (Dirichlet' karakterite ortogonaalsusseos)**.** *Tähistagu* $\chi_1, \ldots, \chi_{\varphi(k)}$ *Dirichlet' karaktereid mooduli* k *järgi. Olgu* m *ja* n *kaks täisarvu ja kehtigu* $(n, k) = 1$. *Siis saame*

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\overline{\chi}_r(n) = \begin{cases} \varphi(k), & \text{kui } m \equiv n \pmod{k}, \\ 0, & \text{kui } m \not\equiv n \pmod{k}. \end{cases}$$

Tõestus. Olgu $(m,k)=1$. Teoreemis 3.13 tõestasime, et

$$\sum_{r=1}^{n} \overline{f}_r(a_i) f_r(a_j) = \begin{cases} n, \text{ kui } a_i = a_j, \\ 0, \text{ kui } a_i \neq a_j, \end{cases} \tag{4.2}$$

kus n tähistab rühma järku ja karakterite arvu. Et $(n,k)=1$ ja $(m,k)=1$, valime selles võrduses $a_i = \overline{n}$, $a_j = \overline{m}$. Paneme tähele, et $\overline{m} = \overline{n}$ siis ja ainult siis, kui mooduli k järgi kehtib $m \equiv n$. Seega saame võrduse kohandada meie juhule vastavaks järgmiselt

$$\sum_{r=1}^{n} \overline{\chi}_r(n)\chi_r(m) = \begin{cases} \varphi(k), \text{ kui } m \equiv n \pmod{k}, \\ 0, \text{ kui } m \not\equiv n \pmod{k}. \end{cases} \tag{4.3}$$

Kui $(m,k)>1$, siis Dirichlet' karakterite definitsiooni kohaselt $\chi_r(m)=0$. Seega iga liige summas kaob ning kehtib $m \not\equiv n \pmod{k}$, sest $(n,k)=1$ ja $(m,k)>1$. □

Teoreem 4.7. *Olgu χ mitte-peakarakter mooduli k järgi ja olgu f mittenegatiivne funktsioon, millel on iga $x \geq x_0$ korral pidev negatiivne tuletis $f'(x)$. Kui $y \geq x \geq x_0 > 0$, saame*

$$\sum_{x<n\leq y} \chi(n) f(n) = O(f(x)). \tag{4.4}$$

Kui veel lisaks $f(x) \to 0$, kui $x \to \infty$, siis lõpmatu rida $\sum\limits_{n=1}^{\infty} \chi(n)f(n)$ koondub ja iga $x \geq x_0$ korral

$$\sum_{n\leq x} \chi(n) f(n) = \sum_{n=1}^{\infty} \chi(n) f(n) + O(f(x)). \tag{4.5}$$

Tõestus. Olgu $A(x) = \sum\limits_{n\leq x} \chi(n)$. Vaatleme summat $A(k) = \sum\limits_{n=1}^{k} \chi(n)$. Definitsiooni 4.1 kohaselt kui $(n,k)>1$, on liidetav $\chi(n)=0$. Kui $(n,k)=1$, siis kuna χ ei ole peakarakter, saame teoreemist 3.11, et mistahes mitte-peakarakteri χ_i korral

$\sum_{\substack{n=1 \\ (n,k)=1}}^{k} \chi_i(n) = \sum_{\overline{n} \in U(\mathbb{Z}_k)} \chi_i(n) = 0$. Järelikult $A(k) = \sum_{n=1}^{k} \chi(n) = 0$.

Et karakter χ on perioodiline, siis ka $A(mk) = 0, m = 2, 3, \ldots$ sest alates liikmest k on summas $A(mk)$ liikmed kujul $\chi(k+1) = \chi(1), \chi(k+2) = \chi(2), \ldots$. Summa $A(x) = \sum_{n \leq x} \chi(n)$ saame jaotada järgmiselt osasummadeks

$$\sum_{n \leq x} \chi(n) = \sum_{n=1}^{k} \chi(n) + \sum_{n=k+1}^{2k} \chi(n) + \ldots + \sum_{n=mk+1}^{x} \chi(n).$$

Teame, et $\sum_{n=1}^{k} \chi(n) = 0$ ning perioodilisuse tõttu on ka järgmised osasummad võrdsed nulliga. Vaatleme viimast osasummat. Kui $[x]$ on mingi k-kordne, saame, et ka viimane osasumma on 0. Kui ei ole, siis on meil seal kuni k elementi, millest kõige rohkem $\varphi(k)$ tükki on sellised arvud n, mille korral $(n,k) = 1$ ning et $\chi(n)$ on ühejuur, siis $|\chi(n)| = 1$. Ülejäänute korral $\chi(n) = 0$. Seega eemaldades nulliga võrduvad osasummad võime hinnata $|A(x)| \leq \sum_{n=mk+1}^{x} |\chi(n)| \leq \varphi(k)$. Teisisõnu, definitsiooni 1.19 kohaselt $A(x) = O(1)$.

Et χ on aritmeetiline funktsioon ning funktsioonil f leidub intervallis $[x,y]$ pidev tuletis, saame kasutada Abeli samasuse teoreemi 2.15, et esitada summa 4.4 integraalina, ja lause 1.20 omaduste (5) ja (1) põhjal

$$\sum_{x < n \leq y} \chi(n) f(n) = f(y)A(y) - f(x)A(x) - \int_x^y A(t) f'(t) dt$$

Kuna $A(x) = O(1)$, leidub $K > 0$, et $|A(x)| \leq K$. See tähendab, et $-K \leq A(x) \leq K$. Kuna $f'(t)$ on negatiivne, siis $Kf'(t) \leq A(t)f'(t) \leq -Kf'(t)$. Teame Abeli samasusest 2.15, et $A(t)f'(t)$ on lõigul $[x,y]$ integreeruv. Seega integraali monotoonsusomaduse 1.15 põhjal

$$K(f(y) - f(x)) = \int_x^y K f'(t) dt \leq \int_x^y A(t) f'(t) dt \leq -\int_x^y K f'(t) dt = K(f(x) - f(y)).$$

Viimasest tuleneb, et $\int_x^y A(t)f'(t)dt = O(f(x) - f(y))$ ning kehtib

$$\begin{aligned}\sum_{x<n\leq y} \chi(n)f(n) &= f(y)A(y) - f(x)A(x) - \int_x^y A(t)f'(t)dt \\ &= O(f(y)) + O(f(x)) + O(f(x) - f(y)).\end{aligned}$$

Teoreemi eelduse kohaselt on mittenegatiivsel funktsioonil f negatiivne tuletis, mis tähendab, et f on kahanev funktsioon. Kuna $y \geq x$, siis $0 \leq f(y) \leq f(x)$ ning $f(y) = O(f(x))$. Lisaks kehtib

$$f(y) \leq f(x) \Rightarrow 0 \leq f(x) - f(y) \leq f(x) \Rightarrow f(x) - f(y) = O(f(x)).$$

Järelikult kasutades lause 1.20 omadusi (2) ja (3) ning eelnevaid teadmisi saame, et $O(f(y)) + O(f(x)) + O(f(x) - f(y)) = 3O(f(x)) = O(f(x))$. Sellega oleme tõestanud võrduse (4.4).

Kui nüüd $f(x) \to 0$, kui $x \to \infty$, siis võrdus (4.4) näitab, et rida $\sum_{n=1}^{\infty} \chi(n)f(n)$ koondub Cauchy koondumistunnuse (1.17) tõttu, sest lause 1.20 omaduse (3) kohaselt kui $f(x) \to 0$, siis $O(f(x)) \to 0$.

Et tõestada võrdust (4.5), märgime lihtsalt, et

$$\sum_{n=1}^{\infty} \chi(n)f(n) = \sum_{n\leq x} \chi(n)f(n) + \lim_{y\to\infty} \sum_{x<n\leq y} \chi(n)f(n).$$

Võrduse (4.4) tõttu on piirväärtus $O(f(x))$. Et lause 1.20 omaduse (3) tõttu $O(f(x)) = -O(f(x))$, võime eelmise võrduse kirjutada, kui

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x)).$$

□

Teoreem 4.8. *Kui χ on mitte-peakarakter mooduli k järgi, siis read* $\sum_{n=1}^{\infty} \frac{\chi(n)}{n}$, $\sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}}$ *ja* $\sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n}$ *koonduvad ning kehtivad hinnangud:*

$$\text{juhul } x \geq 1: \quad \sum_{n \leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{x}\right), \tag{4.6}$$

$$\sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right), \tag{4.7}$$

$$\sum_{n \leq x} \frac{\chi(n) \ln n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n} + O(1) + O\left(\frac{\ln x}{x}\right), \tag{4.8}$$

$$\text{juhul } x \geq 3: \quad \sum_{n \leq x} \frac{\chi(n) \ln n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n) \ln n}{n} + O\left(\frac{\ln x}{x}\right). \tag{4.9}$$

Tõestus. Tõestame võrduse (4.6). Olgu χ mitte-peakarakter mooduli k järgi ning olgu $f(x) = \frac{1}{x}$. Teame, et funktsioon on mittenegatiivne, sest $x \geq 1$ ning $f'(x) = -\frac{1}{x^2}$, mis iga $x \geq 1$ korral on tõepoolest negatiivne. Seega on teoreemi 4.7 eeldused $x_0 = 1$ korral täidetud. Et $f(x) \to 0$, kui $x \to \infty$, siis saame kasutades teoreemi 4.7 võrdust (4.5), et iga $x \geq 1$ korral

$$\sum_{n \leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{x}\right).$$

Järmisena tõestame võrduse (4.7). Valime $f(x) = \frac{1}{\sqrt{x}}$. Taas kehtib see, et kui $x \geq 1$, on tegemist mittenegatiivse funktsiooniga, millel on negatiivne pidev tuletis $f'(x) = -\frac{1}{2x\sqrt{x}}$ iga $x \geq 1$ korral. Ka sel korral $f(x) \to 0$, kui $x \to \infty$ ning seega, kasutades võrdust (4.5) eeldusel $x_0 = 1$, saame:

$$\sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right).$$

Viimaks tõestame võrdused (4.8) ja (4.9). Kui valida $f(x) = \frac{\ln x}{x}$, siis $x \geq 3$ korral on funktsioon mittenegatiivne ning tuletis $f'(x) = \frac{1-\ln x}{x^2} = -\frac{\ln x - 1}{x^2}$ negatiivne.

Lisaks on teada, et kehtib $f(x) \to 0$, kui $x \to \infty$, sest kasutades piirväärtuse $\lim_{x\to\infty} \frac{\ln x}{x}$ korral L'Hospital'i reeglit, saame $\lim_{x\to\infty} \frac{1}{x} = 0$. Seega saame eeldusel, et $x_0 = 3$ kasutada teoreemi 4.7 võrdust (4.5) ning kirjutada, et $x \geq 3$ korral kehtib

$$\sum_{n\leq x} \frac{\chi(n)\ln n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n} + O\left(\frac{\ln x}{x}\right).$$

Juhul $x \geq 1$ märgime esmalt, et kuna $\sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n}$ on koonduv rida, kehtib $\sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n} = O(1)$. Seega $x \in [1,3)$ korral, kuna summa $\sum_{1\leq n\leq 2} \frac{\chi(n)\ln n}{n}$ on ülimalt kaheliikmeline, siis

$$\begin{aligned}
\sum_{1\leq n\leq x} \frac{\chi(n)\ln n}{n} &= \sum_{1\leq n\leq x} \frac{\chi(n)\ln n}{n} + \sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n} + 0 - \sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n} \\
&= O(1) + \sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n} + O\left(\frac{\ln x}{x}\right) + O(1) \\
&= \sum_{n=1}^{\infty} \frac{\chi(n)\ln n}{n} + O\left(\frac{\ln x}{x}\right) + O(1). \qquad (4.10)
\end{aligned}$$

Et $0 = O(1)$, siis saab seda võrdusele (4.8) liites ka $x \geq 3$ korral samasuguse kuju, ehk oleme tõestanud võrduse (4.9). □

Teoreem 4.9. *Olgu χ reaalarvuliste väärtustega karakter mooduli k järgi ja*

$$A(n) = \sum_{d|n} \chi(d).$$

Siis $A(n) \geq 0$ iga n korral ja $A(n) \geq 1$, kui n on täisruut.

Tõestus. Algarvu astmete jaoks kehtib

$$A(p^a) = \sum_{t=0}^{a} \chi(p^t) = 1 + \sum_{t=1}^{a} \chi(p)^t.$$

Viimane võrdus järeldub Dirichlet' karakterite multiplikatiivsusest teoreemist 4.3.

Teame, et $\chi(p)$ on kas 0 või ühejuur, seega $\chi(p)$ saab olla kas 0, 1 või -1, sest -1 ja 1 on ainsad reaalarvulised ühejuured. Järelikult on meil kolm võimalust:

1. kui $\chi(p) = 0$, siis $A(p^a) = 1 + \sum_{t=1}^{a} 0^t = 1$,
2. kui $\chi(p) = 1$, siis $A(p^a) = 1 + \sum_{t=1}^{a} 1^t = a + 1$,
3. kui $\chi(p) = -1$, siis $A(p^a) = 1 + \sum_{t=1}^{a} (-1)^t = \begin{cases} 0, & \text{kui a on paaritu,} \\ 1, & \text{kui a on paaris.} \end{cases}$

Kui a on paaris, siis igal juhul kehtib $A(p^a) \geq 1$.

Märgime siinkohal, et A on nõrgalt multiplikatiivne, sest $A(n) = \sum_{d|n} \chi(d) = \sum_{d|n} \chi(d) u\left(\frac{n}{d}\right) = \chi * u$ ning teoreemist 2.9 teame, et kuna χ on multiplikatiivne ja u on nõrgalt multiplikatiivne, on järelikult A nõrgalt multiplikatiivne. Kui $n = 1$, siis $A(n) = A(1) = \chi(1) = 1$. Kui $n > 1$, saame selle kirja panna kujule $n = p_1^{a_1} \dots p_r^{a_r}$ ja sel juhul $A(n) = A(p_1^{a_1}) \dots A(p_r^{a_r})$, sest A on nõrgalt multiplikatiivne. Iga tegur $A(p_i^{a_i}) \geq 0$, seega ka $A(n) \geq 0$. Lisaks kui n on täisruut, siis iga astendaja a_i on paaris, seega iga tegur $A(p_i^{a_i}) \geq 1$, seega ka $A(n) \geq 1$. Sellega on teoreem tõestatud. □

Tähistame edaspidi

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

Tõestame nüüd oluline Dirichlet' teoreemi tõestuseks vajamineva vahetulemuse. Meie eesmärk on näidata, et reaalarvuliste väärtustega

mitte-peakarakterite χ korral kehtib $L(1, \chi) \neq 0$.

Teoreem 4.10. *Olgu χ reaalarvuliste väärtustega Dirichlet' karakter mooduli k järgi, $\chi \neq \chi_1$. Tähistame*

$$A(n) = \sum_{d|n} \chi(d) \text{ ja } B(x) = \sum_{n \leq x} \frac{A(n)}{\sqrt{n}}.$$

Siis:

$$B(x) \to \infty, \ \textit{kui } x \to \infty, \tag{4.11}$$

$$B(x) = 2\sqrt{x}L(1,\chi) + O(1), \ \textit{iga } x \geq 1 \textit{ korral.} \tag{4.12}$$

Ning seega $L(1,\chi) \neq 0$.

Tõestus. Tõestame väite 4.11. Kasutades teoreemi 4.9, saame, et

$$B(x) = \sum_{n\leq x} \frac{A(n)}{\sqrt{n}} = \sum_{\substack{n\leq x\\ n=m^2}} \frac{A(n)}{\sqrt{n}} + \sum_{\substack{n\leq x\\ n\neq m^2}} \frac{A(n)}{\sqrt{n}} \geq \sum_{\substack{n\leq x\\ n=m^2}} \frac{A(n)}{\sqrt{n}} \geq \sum_{\substack{n\leq x\\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m\leq\sqrt{x}} \frac{1}{m}.$$

Summa $\sum_{m\leq\sqrt{x}} \frac{1}{m}$ läheneb lõpmatusele, kui $x \to \infty$, sest harmooniline rida $\sum \frac{1}{m}$ hajub. Seega on 4.11 tõestatud.

Väite 4.12 tõestamiseks kirjutame

$$B(x) = \sum_{n\leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q,d\\ qd\leq x}} \frac{\chi(d)}{\sqrt{qd}},$$

sest kuna $d|n$, siis leidub selline q, et $qd = n$. Et $n \leq x$, siis $qd \leq x$.

Nüüd kasutame teoreemis 2.14 olevat võrdust (2.5), mis ütleb, et kui funktsioonid f ja g on aritmeetilised ning $a, b \in \mathbb{R}^+$ on sellised, et $ab = x$, siis

$$\sum_{\substack{q,d\\ qd\leq x}} f(d)g(q) = \sum_{n\leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n\leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b), \tag{4.13}$$

kus $F(x) = \sum_{n\leq x} f(n)$ ja $G(x) = \sum_{n\leq x} g(n)$.

Valime $a = b = \sqrt{x}$ ning olgu $f(n) = \frac{\chi(n)}{\sqrt{n}}$ ja $g(n) = \frac{1}{\sqrt{n}}$, kusjuures sellised funktsioonid f ja g on aritmeetilised funktsioonid. Järelikult kehtib

$$B(x) = \sum_{\substack{q,d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}} = \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}). \quad (4.14)$$

Teoreemi 2.13 võrdus (2.3) annab meile, et

$$G(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = \frac{x^{1-\frac{1}{2}}}{1-\frac{1}{2}} + \zeta\left(\frac{1}{2}\right) + O\left(x^{-\frac{1}{2}}\right) = 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right), \quad (4.15)$$

kus $A = \zeta\left(\frac{1}{2}\right)$.

Teoreemi 4.8 kohaselt rida $\sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}}$ koondub ning võrdusest (4.7)

$$F(x) = \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = B + O\left(\frac{1}{\sqrt{x}}\right), \quad (4.16)$$

kus $B = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}}$.

Et A on konstant ning B on teoreemi 4.8 põhjal koonduva rea summa, siis $A = O(1)$ ja $B = O(1)$. Vaatleme korrutist $F(\sqrt{x})G(\sqrt{x})$. Kasutame lauseid 1.20, 1.22 ja fakti, et $\frac{1}{\sqrt[4]{x}} \to 0$ ning saame

$$\begin{aligned}
F(\sqrt{x})G(\sqrt{x}) &= 2Bx^{\frac{1}{4}} + BA + B \cdot O\left(\frac{1}{\sqrt[4]{x}}\right) + 2\sqrt[4]{x} \cdot O\left(\frac{1}{\sqrt[4]{x}}\right) \\
&\quad + A \cdot O\left(\frac{1}{\sqrt[4]{x}}\right) + O\left(\frac{1}{\sqrt[4]{x}}\right) \cdot O\left(\frac{1}{\sqrt[4]{x}}\right) \\
&= 2Bx^{\frac{1}{4}} + O(1) + O\left(\frac{1}{\sqrt[4]{x}}\right) + O(1) + O\left(\frac{1}{\sqrt[4]{x}}\right) + o(1) \cdot o(1) \\
&= 2Bx^{\frac{1}{4}} + O(1) + o(1) + O(1) + o(1) + O(1) \cdot O(1) \\
&= 2Bx^{\frac{1}{4}} + O(1) + O(1) + O(1) + O(1) + O(1) \\
&= 2Bx^{\frac{1}{4}} + 5 \cdot O(1) = 2Bx^{\frac{1}{4}} + O(1), \quad (4.17)
\end{aligned}$$

Kasutades võrdust (4.17), teoreemi 4.8 võrduseid (4.6) ja (4.7), lauset 1.20, selles teoreemis antud võrdust (4.15) ning valemit (4.18), mille allpool tõestame, annab võrdus (4.14)

$$\begin{aligned}
B(x) = &\sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}}\left(2\sqrt{\frac{x}{n}} + A + O\left(\sqrt{\frac{n}{x}}\right)\right) + \sum_{n\le\sqrt{x}} \frac{1}{\sqrt{n}}\left(B + O\left(\sqrt{\frac{n}{x}}\right)\right)\\
&- 2Bx^{\frac{1}{4}} + O(1)\\
&= 2\sqrt{x}\sum_{n\le\sqrt{x}} \frac{\chi(n)}{n} + A\sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + \sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}}\cdot O\left(\sqrt{\frac{n}{x}}\right) + B\sum_{n\le\sqrt{x}} \frac{1}{\sqrt{n}}\\
&+ \sum_{n\le\sqrt{x}} \frac{1}{\sqrt{n}}\cdot O\left(\sqrt{\frac{n}{x}}\right) - 2Bx^{\frac{1}{4}} + O(1)\\
&\overset{(4.18)}{=} 2\sqrt{x}\left(\sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{\sqrt{x}}\right)\right) + A\left(\sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt[4]{x}}\right)\right)\\
&+ O(1) + B\cdot G(\sqrt{x}) + O\left(\frac{1}{\sqrt{x}}\sum_{n\le\sqrt{x}} 1\right) - 2Bx^{\frac{1}{4}} + O(1)\\
&= 2\sqrt{x}L(1,\chi) + 2\sqrt{x}\cdot O\left(\frac{1}{\sqrt{x}}\right) + AB + A\cdot O\left(\frac{1}{\sqrt[4]{x}}\right) + O(1)\\
&+ B\left(2x^{\frac{1}{4}} + A + O\left(\frac{1}{\sqrt[4]{x}}\right)\right) + O\left(\frac{1}{\sqrt{x}}\cdot\sqrt{x}\right) - 2Bx^{\frac{1}{4}} + O(1)\\
&= 2\sqrt{x}L(1,\chi) + 2\cdot O(1) + O(1) + O(1)\cdot o(1) + O(1) + 2Bx^{\frac{1}{4}}\\
&+ AB + B\cdot O\left(\frac{1}{\sqrt[4]{x}}\right) + O(1) - 2Bx^{\frac{1}{4}} + O(1)\\
&= 2\sqrt{x}L(1,\chi) + 2\cdot O(1) + O(1)\cdot O(1) + 2\cdot O(1) + O(1)\cdot o(1) + 2\cdot O(1)\\
&= 2\sqrt{x}L(1,\chi) + 6\cdot O(1) + 2\cdot O(1)\cdot O(1)\\
&= 2\sqrt{x}L(1,\chi) + O(1).
\end{aligned}$$

Märgime, et kuna $\chi(n)$ on ühejuur, siis $\chi(n) = O(1)$. Seega lause 1.20 omaduste (1), (5) ja (6) tõttu

$$\sum_{n\le\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \cdot O\left(\sqrt{\frac{n}{x}}\right) = \sum_{n\le\sqrt{x}} \frac{O(1)}{\sqrt{n}} \cdot O\left(\sqrt{\frac{n}{x}}\right) = \sum_{n\le\sqrt{x}} O\left(\frac{1}{\sqrt{x}}\right)$$
$$= O\left(\sum_{n\le\sqrt{x}} \frac{1}{\sqrt{x}}\right) = O\left(\sqrt{x} \cdot \frac{1}{\sqrt{x}}\right) = O(1). \qquad (4.18)$$

See tõestab võrduse (4.12). Võrdustest (4.11) ja (4.12) järeldub, et $L(1,\chi) \neq 0$, sest vastasel juhul kehtiks $B(x) = O(1)$, mis läheb vastuollu väitega (4.11).

$\square$

Kasutatud allikad

[1] Tom M. Apostol. *Introduction to Analytic Number Theory*. Springer, 1976.

[2] Mati Kilp. *Algebra I*. Eesti Matemaatika Selts, 2005.

[3] Valdis Laan ja Lauri Tart. *Arvuteooria*. 2024. URL: https://kodu.ut.ee/~ltart/Arvuteooria_k2024/kon_2024.pdf (vaadatud 01.06.2024).

[4] Toivo Leiger. *Ühe muutuja matemaatiline analüüs*. 2020. URL: https://courses.ms.ut.ee/LTMS.00.022/2023_spring/uploads/Main/YMMA_loengud_21k.pdf (vaadatud 01.06.2024).

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Leene Lotta Lüdimois,

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose Dirichlet' karakterid, mille juhendaja on Lauri Tart, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Leene Lotta Lüdimois
10. juuni 2024