UNIVERSITY OF APPLIED SCIENCES

THM
TECHNISCHE HOCHSCHULE MITTELHESSEN

Martin Rehberg

Die Goldbach-Vermutung
Ausführungen zum Beweis des Satzes von Vinogradov nach Vaughan

Friedberger Hochschulschriften Band 35

Martin Rehberg

Die Goldbach-Vermutung
Ausführungen zum Beweis des Satzes von Vinogradov nach Vaughan

Friedberger Hochschulschriften Band 35

Friedberger Hochschulschriften Band 35

Herausgeber der Friedberger Hochschulschriften:
Die Dekaninnen und Dekane des Campus Friedberg
der Technischen Hochschule Mittelhessen

Einzelne Hochschulschriften auch online abrufbar:
www.thm.de/bibliothek/hochschulschriften

ISSN 1439-1112

PLATZHALTER

ab hier den Text der Arbeit ab dem Inhaltsverzeichnis einfügen

THM TECHNISCHE HOCHSCHULE MITTELHESSEN
CAMPUS FRIEDBERG
MND Mathematik, Naturwissenschaften und Datenverarbeitung

Die Goldbach-Vermutung

Ausführungen zum Beweis des Satzes von Vinogradov nach Vaughan

Bachelorarbeit

Studiengang Wirtschaftsmathematik

vorgelegt von

Martin Rehberg

Friedberg, im August 2013

Erstkorrektor der Arbeit: Prof. Dr. Kai Bruchlos
Zweitkorrektor der Arbeit: Prof. Dr. Ulrich Abel

Vorwort

Ziel der von mir vorgelegten Bachelorarbeit ist es, bestimmte Abschnitte des Beweises des Satzes von Vinogradov nach Vaughan auszuarbeiten. Dieser Satz steht, neben dem Satz von Brun und dem Satz von Hardy und Littlewood, zu Beginn einer Reihe von Lösungsversuchen der Goldbach-Vermutung. Diese Vermutung trifft Annahmen zur Darstellung der natürlichen Zahlen durch Primzahlen und lässt sich somit in die Zahlentheorie einordnen. Genauer wird vermutet, dass sich gerade Zahlen als Summe von zwei Primzahlen und ungerade Zahlen als Summe von drei Primzahlen darstellen lassen. Der Satz von Vinogradov gilt neben dem Satz von Schnirelmann und dem Satz von Chen als eines der wichtigsten Ergebnisse zur Goldbach-Vermutung. Eine grundlegende Einführung in diese Vermutung werde ich im ersten Kapitel geben. Dort möchte ich auch darstellen wie ich zu diesem Thema gekommen bin und wie sich meine weitere Arbeit aufbaut.
Abschließend möchte ich die Gelegenheit nutzen um mich bei allen zu bedanken, die mich unterstützt und so zum Entstehen meiner Bachelorarbeit beigetragen haben. Hervorheben möchte ich unter diesen Menschen zum einen Detlef Köpke. Auf seinen motivierenden Unterricht und Zuspruch führe ich es zurück, dass ich mich für eine mathematische Studienrichtung entschieden habe. Zum anderen gilt mein ganz besonderer Dank Hartmut Siebert. Obwohl sich Herr Siebert bereits im Ruhestand befindet, war er sofort bereit mich bei meiner Arbeit zu unterstützen. Ich empfinde dies keineswegs als eine Selbstverständlichkeit und bin froh über die offene Zusammenarbeit mit ihm, welche mir stets viel Freude bereitet hat.

Martin Rehberg
Friedberg, im August 2013

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Symbolverzeichnis

G_g	Menge der geraden Zahlen (S.4)
G_u	Menge der ungeraden Zahlen (S.4)
$r_{A,s}(N)$	Anzahl der Darstellungen von N als Summe von s Elementen der Menge $A \subset \mathbb{N}$ (S.10)
$r_{A,s}^{(N)}(m)$	Anzahl der Darstellungen von m als Summe von s Elementen der Menge $A \subset \mathbb{N}$, die N nicht überschreiten (S.11)
$\mathfrak{M}$	Menge der major arcs, auch Menge der Basisintervalle genannt (S.12 bzw. S.31)
$\mathfrak{m}$	Menge der minor arcs, auch Menge der Ergänzungsintervalle genannt (S.12 bzw. S.31)
$\mathfrak{S}(N)$	singuläre Reihe (S.12 bzw. S.49)
$J(N)$	singuläres Integral (S.12 bzw. S.56)
$r_{k,s}(N)$	Anzahl der Darstellungen von N als Summe von s natürlichen Zahlen, wobei jede Zahl in die k-te Potenz ($k \in \mathbb{N}$) erhoben ist (S.13)
$r(N)$	Zählfunktion für das ternäre Goldbachproblem (S.21)
$R(N)$	gewichtete Zählfunktion für das ternäre Goldbachproblem (S.22)
$F(\alpha)$	erzeugende Funktion von $R(N)$ (S.22)
$\mathfrak{M}(q,a)$	Basisintervall (S.25)
$\mathfrak{S}(Q,N)$	beschränkte singuläre Reihe (S.49)
$r_\delta(N)$	Anzahl der Darstellungen von N als Summe dreier Primzahlen p_1, p_2, p_3, wobei $p_i \leq N^{1-\delta}$ für mindestens ein $i = 1,2,3$ gelte (S.72)
$O(\cdot)$	Landau-Symbol „groß O“ (S.88)
$\ll$	Vinogradov-Symbol, Alternative zu $O(\cdot)$ (S.88)
$o(\cdot)$	Landau-Symbol „klein o“ (S.94)
$\prec$	Alternative zu $o(\cdot)$ (S.94)
$\sim$	asymptotisch gleich (S.95)
$\log m$	natürlicher Logarithmus von m (S.97)

p	Primzahl (S.97)
(m, n)	größter gemeinsamer Teiler von m und n (S.97)
$\mathcal{A}$	Menge der arithmetischen Funktionen (S.98)
$f * g$	Dirichlet-Produkt der Funktionen f und g (S.98)
$\varphi(n)$	Euler'sche φ-Funktion (S.100)
$\mu(n)$	Möbius'sche μ-Funktion (S.100)
$e(\alpha)$	abkürzende Schreibweise für $e^{2\pi i\alpha}$ (S.101)
$c_q(n)$	Ramanujan-Summe (S.101)
$\pi(x)$	π-Funktion, Anzahl der Primzahlen kleiner-gleich x (S.102)
$\vartheta(n)$	Chebychev'sche ϑ-Funktion (S.103)
$\psi(n)$	Chebychev'sche ψ-Funktion (S.103)
$\zeta(s)$	Riemann'sche ζ-Funktion (S.103)
$\Lambda(n)$	von Mangoldt'sche Λ-Funktion (S.104)
$[\alpha]$	ganzzahliger Anteil der rellen Zahl α (S.106); die Klammer wird auch Gauss-Klammer genannt (S.32)
$\{\alpha\}$	gebrochener Anteil der rellen Zahl α (S.106)
$\| \alpha \|$	Abstand der reellen Zahl α zur nächsten ganzen Zahl (S.106)

Kapitel 1

Einleitung

Wie bereits im Vorwort erwähnt, werde ich den ersten Abschnitt meiner Bachelorarbeit nutzen, um zur Goldbach-Vermutung einiges Grundlegendes auszuführen. Nachdem ich in dem Abschnitt „Themenfindung“ kurz erläutern werde wie ich zu diesem - für einen Student im Bereich Wirtschaftsmathematik wohl eher ungewöhnlichen - Thema gelangt bin, werde ich in dem darauf folgenden Abschnitt „Ziel und Aufbau der Arbeit“ mein weiteres Vorgehen in Bezug auf die verbliebenen Abschnitte des Kapitels 1, als auch der übrigen Kapitel darlegen.

1.1 Motivation und Ziel

1.1.1 Themenfindung

Dass ich mich für eine Bachelorarbeit mit Schwerpunkt Zahlentheorie entschieden habe, hat seinen Ursprung wohl dem glücklichen Ereignis zu verdanken, dass in meinem damaligen dritten Studiensemester die „Elementare Zahlentheorie“ das einzige Wahlpflichtmodul mit rein mathematischen Schwerpunkt war, welches ich wählen konnte. Seit diesem Zeitpunkt ließ mich die Begeisterung für diese Gebiet nicht los, sodass ich mich entschied, meinen Masterschwerpunkt im Bereich Zahlentheorie zu setzen und mich in meiner Bachelorarbeit einem Thema aus dieser zu widmen.
Nachdem ich in Herr Bruchlos den Betreuer für meine Bachelorarbeit gefunden hatte, begann ich mit der Suche nach einem Thema. Dabei durchforstete ich unterschiedliche mathematische Zeitschriften der Bibliothek in Friedberg. Ein Artikel der mich fesselte war „Das Goldbach'sche Problem“ [1] von Dieter Wolke. Eines der zentralen Ergebnisse, zu dem der Artikel kam, war der Satz von Vinogradov. Im Weiteren beschäftigte ich mich mit Literatur zur Goldbach-Vermutung und zu diesem speziellen Satz und schlug eine Ausarbeitung zum Beweis des Satzes von Vinogradov letztendlich als Thema für meine Bachelorarbeit vor. Nachdem Herr Bruchlos und auch der Zweitkorrektor Herr Abel meiner Themenwahl zugestimmt hatten, stand dem nichts mehr im Wege.

[1] *Wolke D.*: Das Goldbach'sche Problem, in: Mathematische Semesterberichte 41 (1994), S.55-67

1.1.2 Ziel und Aufbau der Arbeit

Nach der vorangegangenen Themenfindung soll in diesem Abschnitt dem/der LeserIn eine Orientierungshilfe zum weiteren Aufbau der Arbeit an die Hand gegeben werden. Das Ziel meiner Arbeit ist es, bestimmte Abschnitte des Beweises des Satzes von Vinogradov nach Vaughan auszuarbeiten. Als Fundament dafür wird im Abschnitt „Die Goldbach-Vermutung“ noch einmal ausführlich beschrieben, welche Fragestellung der Vermutung zugrunde liegt. Ausgehend von der ursprünglichen historischen Goldbach-Vermutung wird dargestellt, wie sich diese im Laufe der Zeit verändert hat. Zudem werden wichtige Resultate, zu denen auch der Satz von Vinogradov gehört, auf dem Weg zur Suche nach einer Lösung aufgeführt. Daran anschließend wird in „Berechnungen zur Goldbach-Vermutung“ gezeigt, wie sich das Wissen um den Bereich, in dem die Goldbach'sche Vermutung gilt, im Laufe der Zeit ständig verändert hat.
Um die Ausführungen zum Beweis des Satzes von Vinogradv nicht unnötig zu verlängern, werden im Anhang die notwendigen „Hilfsmittel zum Beweis des Satzes von Vinogradov“ bereitgestellt. Dabei setze ich als Grundwissen das Niveau eines/einer Bachelor-AbsolventenIn voraus. Um dem/der LeserIn aber nicht unnötig Arbeit zu bereiten, soll der Abschnitt auch genutzt werden, um bestimmte, bereits bekannte Ergebnisse in Erinnerung zu rufen. Ich empfehle nach Kapitel 1 zunächst einen Blick in den Anhang, bevor sich Kapitel 2 zugewandt wird. In diesem werde ich die dem Beweis zugrundeliegende *Kreismethode* skizzieren und zur besseren Orientierung eine Übersicht zum Aufbau des Beweises geben. Anschließend soll sich in Kapitel 3 den Ausführungen zum Beweis zugewandt werden. In diesem Kapitel ist auch eine kleine Eigenleistung von mir in Form von Korollar 3.2.6 und Korollar 3.4.4 zu finden. Die Vorgehensweise der Gliederung des Beweises in verschiedene Sätze und Propositionen orientiert sich hierbei, wie auch der Beweis selbst, hauptsächlich am Buch von Nathanson[2].

[2] *Nathanson, Melvyn B.*: Additive Number Theory - The Classical Bases, 2.Auflage, New York: Springer, 2010

1.2 Die Goldbach-Vermutung

Die Goldbach'sche Vermutung hat ihren Ursprung in dem Brief, den Christian Goldbach am 7. Juni 1742 an Leonhard Euler schrieb. Darin heißt es:

Es scheinet ... dass eine jede Zahl, die grösser [!] ist als 1, ein aggregatum trium numerorum primorum[3] *sey [!].* [4]

Dabei muss man berücksichtigen, dass zu Zeiten Goldbachs die Zahl Eins noch zur Menge der Primzahlen gerechnet wurde. In Eulers Antwort vom 30. Juni 1742 ist zu lesen:

Dass [!] ... ein jeder numerus par eine summa duorum priorum [5] *sey [!], halte ich für ein ganz gewisses theorema, ungeachtet ich dasselbe nicht demonstriren [!] kann.* [6]

Beide kamen danach nie wieder zu diesem Thema zurück.[7] Die besondere Bedeutung der Goldbach'schen Vermutung für die Zahlentheorie liegt in einer Art der Übertragung (wenn auch in abgeschwächter Form) des Hauptsatzes der elementaren Zahlentheorie vom multiplikativen ins additive. Dieser besagt, dass

Jede natürliche Zahl n in eindeutiger Weise, bis auf die Reihenfolge der Faktoren, das Produkt von Primzahlen ist.[8]

Die Goldbach'sche Vermutung stellt nun ein additives Pendant zu diesem dar, wenn auch die Eigenschaft der Eindeutigkeit fallen gelassen werden muss, wie die Beispiele $20 = 13 + 7 = 17 + 3$ bzw. $25 = 13 + 7 + 5 = 17 + 5 + 3$ leicht zeigen. Dennoch wäre die Übertragung der Eigenschaft der Primzahlen nicht nur in einem multiplikativen, sondern auch in einem additiven Sinne, Bausteine der natürlichen Zahlen zu sein, beeindruckend.
Seitdem man die Eins nicht mehr zur Menge der Primzahlen rechnet, werden zwei Goldbach-Vermutungen formuliert:

Jede gerade Zahl größer als Zwei ist als Summe zweier Primzahlen darstellbar. [9]
(binäre Goldbach-Vermutung)

Jede ungerade Zahl größer als Fünf ist als Summe dreier Primzahlen darstellbar. [10]
(ternäre Goldbach-Vermutung)

[3] *Es scheinet ... dass eine jede Zahl, die größer als 1 ist, die Summe dreier Primzahlen sei.*
[4] http://www.math.dartmouth.edu/euler/correspondence/letters/OO0765.pdf, 28.05.2013, 10Uhr
[5] *Das ... jede gerade Zahl die Summe zweier Primzahlen sei, halte ich für ein ganz gewisses Theorem, ungeachtet ich dasselbe nicht demonstrieren kann.*
[6] http://www.math.dartmouth.edu/euler/correspondence/letters/OO0766.pdf, 28.05.2013, 10Uhr
[7] Vgl. *Narkiewicz W.*, 2000, S.333
[8] Vgl. *Schmidt A.*, 2007, Satz 1.2.3, S.4
[9] *Bundschuh P.*, 2008, S.292
[10] *Bundschuh P.*, 2008, S.292

Dass bei der binären Goldbach-Vermutung die geraden Zahlen ab Vier und bei der ternären Goldbach-Vermutung die ungeraden Zahlen ab Sieben betrachtet werden, lässt sich folgendermaßen begründen:
Es sei $G_g = \{k \in \mathbb{Z} \mid k = 2n, n \in \mathbb{Z}\}$, $G_u = \{k \in \mathbb{Z} \mid k = 2n+1, n \in \mathbb{Z}\}$ die Zerlegung der ganzen Zahlen in die Menge der geraden Zahlen und die Menge der ungeraden Zahlen. Für die binäre Goldbach-Vermutung ist dann $1 + 1 = 2 \in G_g$ aber $1 \notin \mathbb{P}$, sodass erst bei $2 + 2 = 4 \in G_g$ begonnen werden kann. Für die ternäre Goldbach-Vermutung gilt dies auf ähnliche Weise. Hier ist $1 + 1 + 1 = 3 \in G_u$ und $1 + 2 + 2 = 5 \in G_u$, aber in beiden Fällen ist wieder $1 \notin \mathbb{P}$, sodass erst bei $2 + 2 + 3 = 7 \in G_u$ begonnen wird.
Als Beziehung zwischen der binären und der ternären Goldbach-Vermutung lässt sich feststellen, dass die ternäre Goldbach-Vermutung von der binären impliziert wird. Hierzu folgende Betrachtung:
Sei $n \geq 7$ und $n \in G_u$, dann lässt sich n darstellen als $n = 2k + 1$ mit $k \geq 3$. Zudem ist $n - 3 \geq 4$ und $n - 3 = 2k - 2 = 2(k - 1) \in G_g$, wobei der Faktor $(k - 1) \geq 2$ ist, da $k \geq 3$ gilt. Setzt man die Richtigkeit der binären Goldbach-Vermutung voraus, dann ist $n - 3$ mit $p_1, p_2 \in \mathbb{P}$ darstellbar als $n - 3 = p_1 + p_2 \iff n = p_1 + p_2 + 3$, also als Summe von drei Primzahlen.[11]
Auch beinhaltet die heutige Formulierung der Goldbach-Vermutung mehr, als die ursprüngliche, von Goldbach aufgestellte Vermutung. Für den Fall der binären Goldbach-Vermutung sei dies kurz aufgezeigt:
Es sei $(G_g, +)$ die Gruppe der geraden Zahlen mit der Addition als Verknüpfung, dass heißt es gilt *gerade + gerade = gerade*. Die Menge der ungeraden Zahlen G_u hingegen bildet keine solche Struktur, da bereits *ungerade + ungerade = gerade*, die Verküpfung bzgl. der Addition also nicht abgeschlossen ist. Es sei noch bemerkt, dass
gerade + ungerade = ungerade ist. Betrachtet man die Summer dreier Zahlen ergeben sich die vier Fälle[12]

(i) *gerade + gerade + gerade = gerade + gerade = gerade*

(ii) *gerade + gerade + ungerade = gerade + ungerade = ungerade*

(iii) *gerade + ungerade + ungerade = gerade + gerade = gerade*

(iv) *ungerade + ungerade + ungerade = ungerade + gerade = ungerade*

Eine gerade Zahl hat nach (i) und (iii) also einen geraden additiven Anteil. Da $2 \in \mathbb{P}$ die einzige gerade Primzahl ist, ist nach der ursprünglichen, von Goldbach selbst geäußerten Vermutung, eine gerade Zahl $2n = p_1 + p_2 + 2$ mit $p_1, p_2 \in \mathbb{P}$. Es ist jedoch nicht ersichtlich, wie daraus auf eine Darstellung der geraden Zahl $2n$ in der Form $2n = p_1' + p_2'$ mit $p_1', p_2' \in \mathbb{P}$ nach heutiger Formulierung der binären Goldbach-Vermutung geschlossen werden kann.[13]

[11] Vgl. *Bundschuh P.*, 2008, S.292
[12] Vgl. *Heuser H.*, Aufgabe 2, 2009, S.32,
[13] *Wolke D.*: Das Goldbach'sche Problem, in: Mathematische Semesterberichte 41 (1994), S.55

Für lange Zeit gab es keinen Fortschritt in Richtung einer Lösung der beiden Goldbach-Vermutungen, sodass nur Berechnungen als Hinweise auf eine eventuelle Richtigkeit dienten.[14] Auf einige dieser älteren, aber auch auf neuere, computergestütze Berechnungen wird der nächste Abschnitt zu sprechen kommen.
Noch im Jahr 1900 beurteilte Hilbert in seiner berühmten Rede „Mathematische Probleme“ auf dem Internationalen Mathematiker-Kongress in Paris die Aussichten, bei einer der Goldbach-Vermutungen in nächster Zeit voranzukommen, nicht besonders optimistisch.[15] Im Jahr 1919 gab es dann den ersten wesentlichen Fortschritt. Brun konnte zeigen, dass jede genügend große Zahl die Summe zweier 9-Fastprimzahlen ist. Dabei soll unter einer k-Fastprimzahl eine Zahl verstanden werden, die maximal das Produkt von k Primzahlen ist.[16] 1923 bewiesen Hardy und Littlewood mit der von ihnen entwickelten Kreismethode die Existenz eines n_0 derart, dass jede ungerade Zahl $n \geq n_0$ als Summe von drei Primzahlen geschrieben werden kann. Vorausgesetzt wurde hierbei allerdings eine Verallgemeinerung der unbewiesenen Riemann'schen Vermutung.[17] 1930 bewies Schnirelmann seinen berühmten Satz zur Existenz einer Konstanten r, sodass jede genügend große natürliche Zahl N als Summe von höchstens r Primzahlen dargestellt werden kann.[18] Vinogradov gelang es 1937 schließlich, das Resultat von Hardy und Littlewood von der unbewiesenen Annahme zu befreien. Sein bekannter Satz lautet demnach, dass *jede genügend große ungerade Zahl $n \geq n_0$ als Summe dreier Primzahlen dargestellt werden kann.*[19] Durch genaue Prüfung des Satzes von Vinogradov konnte Borodzkin 1956 zeigen, dass man $n_0 = 3^{3^{15}} \approx 10^{7.000.000}$ verwenden kann.[20] Das bis heute beste Resultat wurde 1973 von Chen veröffentlicht. Es besagt, dass jede genügend große gerade Zahl als Summe zweier Zahlen darstellbar ist, von denen die eine eine Primzahl und die andere eine 2-Fastprimzahl ist.[21] 1977 gelang Vaughan eine Vereinfachung des Beweises des Satzes von Vinogradov.[22] Es ist, wie dem Titelblatt zu entnehmen ist, auch Vaughans Beweis, der in dieser Arbeit vorgeführt wird. Chen und Wang konnten die untere Schranke von Borodzkin im Jahr 1989 auf $n_0 = 10^{43.000}$ und 1996 nochmals weiter auf $n_0 = 10^{7.194}$ senken. Dieser Wert ist allerdings immer noch zu groß, um die bis zu dieser Schranke fehlenden Zahlen durch Computerberechnungen abzudecken.[23] Ein jüngerer Beitrag zur Goldbach'schen Vermutung könnte von Tao aus dem Jahr 2012 stammen. Dieser will bewiesen haben, dass jede ungerade natürliche Zahl größer als Eins höchstens als Summe von fünf Primzahlen geschrieben werden kann.[24] Eine Bestätigung, beispielsweise seitens der Deutschen Mathematikervereinigung, steht noch aus.[25] Sein

[14] Vgl. *Narkiewicz W.*, 2000, S.333
[15] Vgl. *Bundschuh P.*, 2008, S.146 und 292
[16] Vgl. *Ribenboim P.*, 2011, S.222
[17] Vgl. *Bundschuh P.*, 2008, S.292
[18] Vgl. *Schwarz W.*, 1969, S.173
[19] Vgl. *Bundschuh P.*, 2008, S.292
[20] Vgl. *Ribenboim P.*, 2011, S.221
[21] Vgl. *Ribenboim P.*, 2011, S.222
[22] Vgl. *Nathanson M.B.*, 2010, S.230 und 337
[23] Vgl. *Ribenboim P.*, 2011, S.221
[24] Vgl. http://arxiv.org/abs/1201.6656, 16.03.2013, 14Uhr10 und http://www.spiegel.de/wissenschaft/mensch/primzahlraetsel-loesung-der-goldbachschen-vermutung-rueckt-naeher-a-833216.html, 12.06.2013, 11Uhr30
[25] Vgl. https://dmv.mathematik.de/aktuell/aktuell/archiv/1205.html, 12.03.2013, 22Uhr25

Beweis ist auf der Homepage der Cornell University öffentlich zugänglich.[26] Der wohl jüngste Beitrag zur Goldbach'schen Vermutung könnte noch aus diesem Jahr von Helfgott stammen und die ternäre Vermutung beweisen. Helfgott will die Lücke, die bisher noch zum Beweis der ternären Goldbach'schen Vermutung gefehlt hat geschlossen haben.[27]
Auf die Werte, die mittels Computereinsatz erzielt werden konnten, wird der kommende Abschnitt eingehen. Für eine historisch umfangreichere Darstellung der Entwicklung beider Goldbach'schen Vermutungen sei auf das Buch von Ribenboim im Literaturverzeichnis verwiesen. Eine Zusammenstellung der wichtigsten Originalarbeiten enthält das Buch von Wang (Wang, Yuan: The Goldbach Conjecture, 2.Auflage, Singapore: World Scientific, 2002).

[26] http://arxiv.org/pdf/1201.6656v4.pdf, 16.03.2013, 14Uhr10
[27] Vgl. http://www.spiegel.de/wissenschaft/mensch/beweis-fuer-schwache-goldbachsche-vermutung-a-901111.html, 24.07.2013, 17Uhr

1.3 Berechnungen zur Goldbach-Vermutung

In der Hoffnung, bessere Kenntnisse über die Goldbach'sche Vermutung zu erlangen, aber auch vielleicht einen Widerspruch zu finden, begann man in Ermangelung des mathematischen Fortschritts zu diesem Problem mit Berechnungen. Heute ist daraus auch eine Art Rekordjagt geworden. Dabei ist der Bereich, in dem man die Richtigkeit der Goldbach'schen Vermutung zeigen konnte, mittlerweile in beachtliche Dimensionen vorgedrungen.
Die folgende Übersicht zeigt das Wachstum der oberen Schranke n, bis zu welcher die Richtigkeit der binären Goldbach'schen Vermutung berechnet werden konnte[28]:

$1 \cdot 10^4$	Desboves (1885) [29]
$1 \cdot 10^5$	Pipping (1938) [30]
$1 \cdot 10^8$	Stein und Stein (1965) [31]
$2 \cdot 10^{10}$	Granville, van de Lune und te Riele (1989) [32]
$4 \cdot 10^{11}$	Sinisalo (1993) [33]
$1 \cdot 10^{14}$	Deshouillers, te Riele und Saouter (1998) [34]
$4 \cdot 10^{14}$	Richstein (1998) [35]
$2 \cdot 10^{16}$	Oliveira e Silva (März 2003) [36]
$6 \cdot 10^{16}$	Oliveira e Silva (Oktober 2003) [37]
$2 \cdot 10^{17}$	Oliveira e Silva (Februar 2005) [38]
$3 \cdot 10^{17}$	Oliveira e Silva (Dezember 2005) [39]
$12 \cdot 10^{17}$	Oliveira e Silva (2008) [40]
$1,6 \cdot 10^{18}$	Oliveira e Silva (2009) [41]
$4 \cdot 10^{18}$	Oliveira e Silva (2012) [42]

[28] Das man sich hierbei auf die binäre Goldbach'sche Vermutung beschränkte ist darin begründet, dass aus der Richtigkeit der binären Vermutung auf die Richtigkeit der ternären Vermutung geschlossen werden kann. Dies wurde bereits im Abschnitt „Die Goldbach-Vermutung“gezeigt.
[29] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[30] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[31] Vgl. *Ribenboim P.*, 2011, S.225
[32] Vgl. *Ribenboim P.*, 2011, S.225
[33] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[34] Vgl. *Ribenboim P.*, 2011, S.225
[35] Vgl. *Ribenboim P.*, 2011, S.225
[36] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[37] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[38] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[39] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[40] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50
[41] Vgl. *Ribenboim P.*, 2011, S.225
[42] Vgl. http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50

So lässt sich nun zumindest für die ternäre Goldbach'sche Vermutung festhalten, dass sie „nur noch“ im Bereich der ungeraden n mit $4 \cdot 10^{18} < n < 10^{7.194}$ auf ihre Richtigkeit überprüft werden braucht. Aufgrund dieser numerischen Resultate, als auch der Ergebnisse von Hardy und Littlewood, Vinogradov und Vaughan wird die ternäre Goldbach-Vermutung heute prinzipiell als gelöst betrachtet, während die binäre noch offen ist.[43] Ein interessantes Buch für jeden, der sich vor der selbstständigen Programmierung eines Algorithmus zu Berechnungen zur Goldbach-Vermutung scheut, gerne aber trotzdem einmal etwas dazu rechnen möchte, stammt von Norres (Norres, Mona: Mathematik Zahlentheorie, 1.Auflage, Sankt Augustin: Eigenverlag Mona Norres, 2011). In diesem wird ein Algorithmus auf Basis des gängigen Tabellenkalkulationsprogramms Excel vorgestellt. Ich möchte jedoch auch darauf hinweisen, dass ich dies im Gegensatz zur Autorin nicht als den Beweis der binären, als auch ternären Goldbach'schen Vermutung ansehe, wie die Autorin dies im Vorwort ihres Buches darstellt.

[43] *Bundschuh P.*, 2008, S.292

Kapitel 2

Beweisidee und -aufbau

Nachdem in dem vorangegangenen Kapitel die Goldbach-Vermutung vorgestellt worden ist, soll sich nun dem Satz von Vinogradov, manchmal auch Satz von Goldbach-Vinogradov genannt, zugewandt werden. Was sagt dieser Satz zur Goldbach-Vermutung aus?
Der Satz von Vinogradov besagt vereinfacht, dass jede genügend große ungerade Zahl N als Summe dreier Primzahlen dargestellt werden kann.[1] Diese sprachliche Aussage ergibt sich als Folgerung aus dem Satz von Vinogradov, wenn die technischen Details des Satzes zugunsten der sprachlichen Formulierung vernachlässigt werden. Für gerade N liefert der Satz von Vinogradov jedoch keine Aussage. Warum dem so ist, wird im Beweisaufbau (Abschnitt 2.2 Seite 15) deutlich. Im Zusammenhang mit dem Satz von Vinogradov soll zunächst ein kurzer Überblick zur Kreismethode geben werden, da diese dem Beweis zugrunde liegt. Um die wesentlichen Schritte beim Beweis nicht aus den Augen zu verlieren, ist vor den Ausführungen zum Beweis im nächsten Kapitel ein Abschnitt mit dem Beweisaufbau eingefügt.

2.1 Überblick zur Kreismethode

Wie bereits angekündigt, soll in diesem Abschnitt ein kurzer Überblick zur Kreismethode gegeben werden.[2] Ich möchte allerdings zu Beginn darauf hinweisen, dass ich nur die Grundzüge dieser Methode skizzieren werde. Für ein detailliertes Studium der Methode kann das Buch von Vaughan (*Vaughan, Robert Charles*: The Hardy-Littlewood Method, 2.Auflage, Cambridge: University Press, 1997) herangezogen werden, welches sich speziell mit dieser auseinandersetzt. Bedingt durch die Skizzierung der Methode bleiben aber leider auch wichtige Übergänge im Verborgenen. Dass dies aus mathematischer Sicht höchst unbefriedigend ist, ist mir durchaus bewusst. Meiner Meinung nach wäre es aber von größerem Nachteil, im Zusammenhang mit dem Satz von Vinogradov kein Wort zur Kreismethode verloren zu haben, weshalb ich mich bewusst für diese, wenn auch lückenhafte, Darstellung entschieden habe.

[1] Vgl. *Schwarz W.*, 1969, S.173

[2] Das meiste hierzu stammt aus dem Buch von Nathanson Abschnitt *5.1 The circle method* (*Nathanson, Melvyn B.*: Additive Number Theory - The Classical Bases, 2.Auflage, New York: Springer, 2010). Andere Quellen sind entsprechend gekennzeichnet.

2.1.1 Die Kreismethode nach Hardy, Littlewood und Ramanujan

Die Kreismethode wurde zwischen 1918 und 1920 von Hardy, Littlewood und Ramanujan als vielseitig einsetzbare Methode zur Behandlung additiver Fragestellungen entwickelt. Im Folgenden soll diese in ihrem Grundgedanken dargestellt werden. Im nächsten Abschnitt wird dann auf die Vereinfachung dieser Methode durch Vinogradov eingegangen. Die Ausgangssituation ist dabei folgende Fragestellung

Gegeben sei eine Teilmenge $A \subset \mathbb{N}$ und $s \in \mathbb{N}$. Gefragt wird nun nach der Anzahl der Darstellungen der natürlichen Zahl N als Summe von s Elementen aus A.

Zur Behandlung dieser Fragestellung wird der Ausdruck $r_{A,s}(N)$ eingeführt, unter welchem die Anzahl der Darstellungen von N als Summe von s Elementen von A verstanden werden soll. Zudem wird die erzeugende Funktion von A

$$f(z) := \sum_{a \in A} z^a \quad (z \in \mathbb{C}, |z| < 1)$$

eingeführt. Für diese formale Potenzreihe betrachtet man die s-te Potenz

$$f(z)^s = \left(\sum_{a \in A} z^a \right)^s .$$

Sortierung des Produkts unter Berücksichtigung der Bedeutung von $r_{A,s}(N)$ ergibt

$$f(z)^s = \left(\sum_{a \in A} z^a \right)^s = \sum_{N=0}^{\infty} r_{A,s}(N) z^N .$$

Um dann Koeffizienten $r_{A,s}(N)$ der Potenzreihe zu bestimmen kann die Cauchy'sche Integralformel verwendet werden. Mit dieser folgt dann

$$r_{A,s}(N) = \frac{1}{2\pi i} \int_{|z|=\rho} \frac{f(z)^s}{z^{N+1}} dz$$

für $\rho \in (0,1)$. Die Methode verdankt ihren Namen also der Wahl des Integrationsweges, dem Kreis mit Radius ρ. Obiger Integralausdruck für $r_{A,s}(N)$ wird dann auf ähnliche Weise wie der im nächsten Abschnitt gewonnene Integralausdruck ausgewertet. Genauer soll darauf aber nicht eingegangen werden.

2.1.2 Die Kreismethode nach Vinogradov

Ein alternativer Zugang zu $r_{A,s}(N)$ ergibt sich, wenn man eine andere erzeugende Funktion betrachtet. Vinogradov vereinfachte die Kreismethode für seinen Beweis zur Goldbach'schen Vermutung u.a. dadurch, dass er bemerkte, dass es möglich ist, bei der Betrachtung von $r_{A,s}(N)$ die Potenzreihe

$$f(z) = \sum_{a \in A} z^a \quad (z \in \mathbb{C}, |z| < 1)$$

durch das Polynom

$$p(z) := \sum_{\substack{a \in A \\ a \leq N}} z^a$$

zu ersetzen. Sei $r_{A,s}^{(N)}(m)$ die Anzahl der Darstellungen von m als Summe von s Elementen von A die N nicht überschreiten. Dann ergibt sich für die Betrachtung der s-ten Potenz des Polynoms $p(z)$

$$p(z)^s = \left(\sum_{\substack{a \in A \\ a \leq N}} z^a \right)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) z^m$$

Setzt man nun im Polynom $p(z)$ für z den Ausdruck $e(\alpha) = e^{2\pi i \alpha}$ ein, erhält man das trigonometrische Polynom

$$F(\alpha) := p(e(\alpha)) = \sum_{\substack{a \in A \\ a \leq N}} e(a\alpha).$$

Dessen s-te Potenz wiederum ist

$$F(\alpha)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) e(m\alpha).$$

Durch die Orthogonalitätsrelation für die Funktionen $e(n\alpha)$

$$\int_0^1 e(m\alpha) e(-n\alpha) = \begin{cases} 1 & \text{für } m = n \\ 0 & \text{für } m \neq n \end{cases}$$

gelangt man zu

$$r_{A,s}(N) = \int_0^1 F(\alpha)^s e(-N\alpha) d\alpha.$$

Der für $r_{A,s}(N)$ gewonnene Integralausdruck ist allerdings nur dann hilfreich, wenn es auch gelingt, das Integral auszuwerten. In vielen Fällen ist dies dadurch möglich, dass das Verhalten des Integranden in den rationalen Punkten des Integrationsbereichs näherungsweise bestimmt werden kann. Dies lässt sich sogar auf eine gewisse Umgebung um jeden rationalen

Punkt ausdehnen.[3] Es besteht also die Möglichkeit, das Integral näherungsweise auszuwerten.
Im weiteren Vorgehen wird das Einheitsintervall $[0,1]$ in zwei disjunkte Mengen aufgeteilt: die *major arcs* $\mathfrak{M}$ und die *minor arcs* $\mathfrak{m}$. Die major arcs $\mathfrak{M}$ sollen dabei aus allen reellen Zahlen bestehen, die gut durch rationale Zahlen approximiert werden können, also in einer gewissen Umgebung der rationalen Zahlen liegen. Für die minor arcs bleibt dann der Rest des Einheitsintervalls, also $\mathfrak{m} = [0,1]\backslash\mathfrak{M}$. Damit kann das Integral folgendermaßen aufgespalten werden:

$$\begin{aligned} r_{A,s}(N) &= \int_0^1 F(\alpha)^s e(-N\alpha)d\alpha \\ &= \int_{\mathfrak{M}} F(\alpha)^s e(-N\alpha)d\alpha + \int_{\mathfrak{m}} F(\alpha)^s e(-N\alpha)d\alpha. \end{aligned}$$

Die genaue Konstruktion der major arcs (und damit auch der minor arcs) ist dabei sowohl von dem zugrundeliegenden Problem, als auch von bestimmten Hilfsmitteln, bspw. solchen, die zur Auswertung des Integrals benötigt werden, abhängig.
Mit der Aufspaltung von $[0,1]$ in $\mathfrak{M}$ und $\mathfrak{m}$ ist es nun möglich, beide Integrale getrennt voneinander zu betrachten. Nachdem die major arcs $\mathfrak{M}$ so konstruiert wurden, dass auf diesem Bereich das Integral näherungsweise möglichst gut ausgewertet werden kann, soll diese Auswertung durchgeführt werden. $F(\alpha)^s$ wird dabei durch eine leichter zu integrierende Funktion ersetzt, welche bis auf einen Fehlerterm mit $F(\alpha)^s$ übereinstimmt. Bei dieser asymptotischen Auswertung mit Haupt- und Fehlerterm tritt der Hauptterm in jeder Anwendung der Kreismethode als Produkt einer Reihe und eines Integrals auf. Die Reihe soll *singuläre Reihe* $\mathfrak{S}(N)$ und das Integral *singuläres Integral* $J(N)$ genannt werden. Nach dieser Auswertung ist dann

$$\int_{\mathfrak{M}} F(\alpha)^s e(-N\alpha)d\alpha = \text{Hauptterm} + \text{1.Fehlerterm}.$$

Als letzter, wohl aber schwierigster Teil ist nun das Integral über die minor arcs abzuschätzen. Dabei muss gezeigt werden, dass für wachsendes N der Fehlerterm aus dem Beitrag der major arcs und minor arcs gegenüber dem Hauptterm aus dem Beitrag der major arcs zur asmyptotischen Formel für $r_{A,s}(N)$ geringer bleibt.[4] Wäre dies nicht der Fall, so wäre der gewonnene Ausdruck für $r_{A,s}(N)$ unbrauchbar. Ist es aber gelungen, dies zu zeigen, erhält man als zusammengesetztes Ergebnis

$$r_{A,s}(N) = \text{Hauptterm} + \text{1.Fehlerterm} + \text{2.Fehlerterm}.$$

Bevor abschließend noch ein Spezialfall für $r_{A,s}(N)$ betrachtet werden soll, noch eine kurze Bemerkung zur Namensgebung:

[3] Vgl. *Prachar K.*, 1957, S.179
[4] Vgl. *Miller S./Takloo-Bighash R.*, 2006, S.309 ff.

Während zu Beginn des Abschnittes tatsächlich noch ein Integral über den Kreisrand betrachtet wurde, spricht man auch beim Integral über $[0,1]$ und den Mengen $\mathfrak{M}$ und $\mathfrak{m}$ von der Kreismethode und Kreisbögen (arcs). Dieser Sprachgebrauch ist historisch bedingt und dient zur Abgrenzung der Kreismethode von anderen Methoden, die Probleme auf ähnliche Weise mit erzeugenden Funktionen angehen.
Von der Bezeichnung *major* arcs für den Bereich $\mathfrak{M}$ sollte man sich i.Ü. nicht dazu verleiten lassen anzunehmen, dass dieser Bereich groß sei. Tatsächlich bezieht sich die Namensgebung nicht auf die Größe des Bereichs, sondern auf dessen Beitrag zum asymptotischen Ausdruck für $r_{A,s}(N)$. In Wirklichkeit ist der Anteil der major arcs am Intervall $[0,1]$ kleiner als der Anteil der minor arcs, wobei letztere ihren Namen daher haben, dass der Beitrag des Integrals über diesen Bereich vernachlässigbar ist.[5]

Nun zum angesprochenen Spezialfall: Betrachtet man die Menge $A \subset \mathbb{N}$ aus der Fragestellung auf Seite 10, dann kann auch jedes Element von A in die k-te Potenz ($k \in \mathbb{N}$) erhoben sein. Für eine derartige Menge A ist das Symbol $r_{A,s}(N)$ ungeeignet, da diese Schreibweise es nicht ermöglicht die Potenz k anzugeben. Man führt deshalb ein neues Symbol ein. Ist die zugrunde liegende Menge $A = \mathbb{N}$, dann soll $r_{k,s}(N)$ die Anzahl der Darstellungen von N als Summe von s positiven k-ten Potenzen beschreiben.

Um beim Beweis des Satzes von Vinogradov das singuläre Integral $J(N)$ auswerten zu können, wird noch ein Spezialfall für $r_{k,s}(N)$ benötigt:

Satz 2.1.1.[6]
Sei $s \geq 1$ und $k = 1$. Dann gilt

$$r_{1,s}(N) = \binom{N-1}{s-1} = \frac{N^{s-1}}{(s-1)!} + O(N^{s-2}),$$

für alle natürlichen Zahlen N.

[5] Vgl. *Miller S./Takloo-Bighash R.*, 2006, S.312 ff.
[6] Vgl. *Nathanson M.B.*, Theorem 5.1, 2010, S.124

2.2 Beweisaufbau

Wie ich bereits zu Beginn dieses Kapitels beschrieben habe, handelt es sich bei dem Satz von Vinogradov um eine Aussage zur Darstellbarkeit einer ungeraden Zahl N als Summe dreier Primzahlen. Demnach lässt sich der Satz von Vinogradov der ternären Goldbach-Vermutung

Jede ungerade Zahl größer als Fünf ist als Summe dreier Primzahlen darstellbar. [7]

zuordnen. Sprachlich vereinfacht kann der Satz von Vinogradov wie folgt formuliert werden:

Jede genügend große ungerade Zahl N kann als Summe dreier Primzahlen dargestellt werden. [8]

In dieser Formulierung wurden die technischen Details jedoch vernachlässigt. Bei exakter mathematischer Formulierung lautet der Satz von Vinogradov:

Es existiert eine arithmetische Funktion $\mathfrak{S}(N)$ und positive Konstanten c_1, c_2 derart, dass

$$\frac{6}{\pi^2} \leq c_1 < \mathfrak{S}(N) < c_2 \leq \frac{2457}{\pi^6}$$

für alle genügend großen ungeraden natürlichen Zahlen N und

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right)$$

gilt.[9]

Dabei bezeichnet $r(N)$ die Zählfunktion für das ternäre Goldbachproblem, also die Anzahl der Darstellungen der ungeraden Zahl N als Summe dreier Primzahlen.
Dass der Satz von Vinogradov nur eine Aussage für ungerade Zahlen liefert[10], lässt sich an der Produktdarstellungen der singulären Reihe $\mathfrak{S}(N)$ erkennen. In Satz 3.2.5 und dem daran anschließenden Beweis wird

$$\mathfrak{S}(N) = \prod_{p\nmid N}\left(1 + \frac{1}{(p-1)^3}\right)\prod_{p|N}\left(1 - \frac{1}{(p-1)^2}\right)$$

[7] *Bundschuh P.*, 2008, S.292
[8] Vgl.*Schwarz W.*, 1969, S.173
[9] *Nathanson M.B,*, Theorem 8.1, 2010, S.212 und *Vinogradov, I.M.*, 2004, S.175
[10] Vgl.*Schwarz W.*, 1969, S.173

festgestellt. Wäre nun N gerade, dann folgt $2 \mid N$ womit das Produkt über die Teiler von N Null wird und der Ausdruck für $\mathfrak{S}(N)$ gegen Null divergiert[11] :

$$\begin{aligned} 2 \mid N &\Longrightarrow \left(1 - \frac{1}{(p-1)^2}\right) = \left(1 - \frac{1}{(2-1)^2}\right) = 0 \\ &\Longrightarrow \mathfrak{S}(N) = 0. \end{aligned}$$

In diesem Fall wäre auch $r(N) = 0$ und der Satz von Vinogradov würde keine Aussage liefern.
Das weitere Studium der Funktion $r(N)$ für ungerades N führt zur Abschätzung

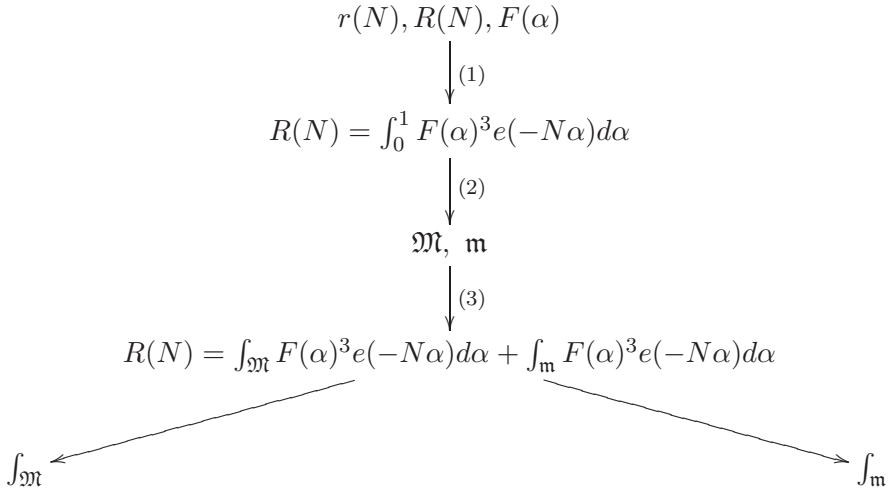
$$\frac{N^2}{(\log N)^3} \ll r(N) \ll \frac{N^2}{(\log N)^3}.$$

Es gibt also zwei Konstanten k_1 und k_2 mit $0 < k_1 < k_2$, sodass für genügend großes N

$$k_1 \cdot \frac{N^2}{(\log N)^3} \leq r(N) \leq k_2 \cdot \frac{N^2}{(\log N)^3}$$

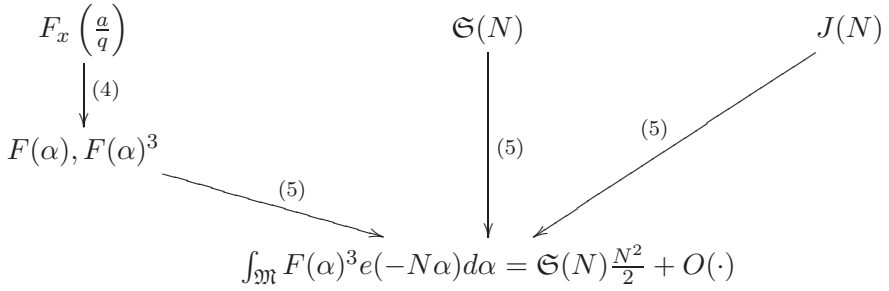
gilt. Um nun den Satz von Vinogradov zu gewinnen, wird im Beweis folgendermaßen vorgegangen:

Zunächst wird die Zählfunktion $r(N)$ eingeführt und zur besseren Handhabung mit einer Gewichtung versehen. Diese gewichtete Zählfunktion wird $R(N)$ genannt. Dem Vorgehen der Kreismethode folgend wird für $R(N)$ die erzeugende Funktion $F(\alpha)$ definiert. Für diese Funktionen wird in Schritt (1) mit der Orthogonalitätsrelation die Beziehung $R(N) = \int_0^1 F(\alpha)^3 e(-N\alpha)d\alpha$ hergeleitet. Ziel des weiteren Vorgehens ist nun die Aufspaltung des Integrationsbereichs. Zu diesem Zweck werden die Mengen $\mathfrak{M}$ und $\mathfrak{m}$ eingeführt (Schritt (2)). Dabei soll $\mathfrak{M}$ aus allen reellen Zahlen bestehen, die gut durch rationale approximiert werden können. Die beiden Mengen $\mathfrak{M}$ und $\mathfrak{m}$ sind eine disjunkte Zerlegung des Integrationsintervalls, womit in Schritt (3) die Zerlegung des Integrals $\int_0^1 F(\alpha)^3 e(-N\alpha)d\alpha$ in zwei getrennt voneinander auswertbare Integrale folgt.



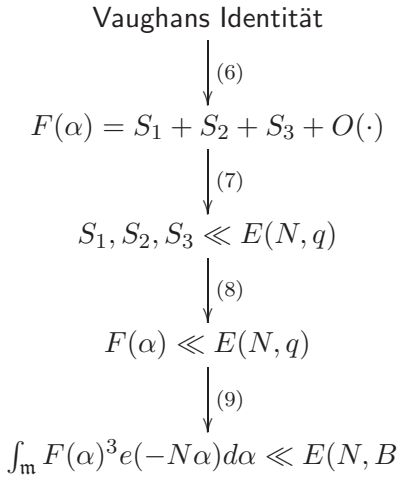
[11] Man beachte den Sprachgebrauch zu unendlichen Produkten Seite 107.

Zuerst soll dann das Integral über $\mathfrak{M}$ ausgewertet werden. Dabei empfiehlt es sich den Integrand $F(\alpha)^3$ durch eine leichter zu integrierende Funktion zu ersetzen, welche bis auf einen Fehlerterm mit $F(\alpha)^3$ übereinstimmt. Zu diesem Zweck wird die erzeugende Funktion $F(\cdot)$ zunächst an rationalen Stellen $\frac{a}{q}$ betrachtet. Die an diesen Stellen gefundene Näherung wird in Schritt (4) auf reelles α ausgedehnt und anschließend potenziert, um die Näherung für $F(\alpha)^3$ zu erhalten. Zwar könnte man mit diesem Ergebnis bereits mit der Auswertung des Integrals beginnen, würde diese aber an zwei Stellen für langwierige Betrachtungen zur dort auftretenden singulären Reihe $\mathfrak{S}(N)$ und singulären Integral $J(N)$ unterbrechen müssen. Um dies zu vermeiden werden diese voher definiert und ausgewertet. Die Ergebnisse zu $F(\alpha)^3,\ \mathfrak{S}(N)$ und $J(N)$ sollen dann nacheinander in Schritt (5) in die Auswertung des Integrals über $\mathfrak{M}$ einfließen. Ergebnis dieser Auswertung wird der Hauptterm $\mathfrak{S}(N)\frac{N^2}{2}$ und ein Fehlerterm $O(\cdot)$ sein.

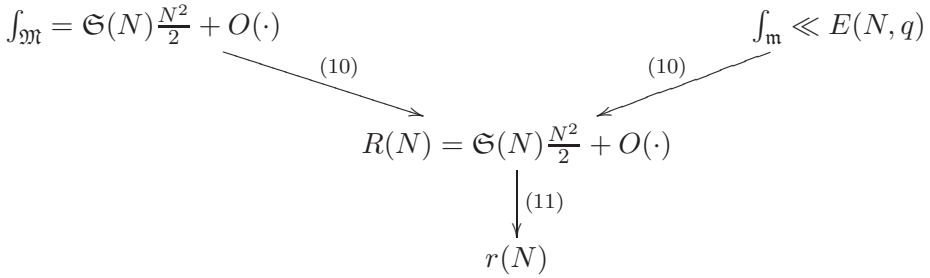


Auf die Auswertung des Integrals über $\mathfrak{M}$ folgt die Abschätzung des Integrals über $\mathfrak{m}$. Grundlage dieser Abschätzung ist *Vaughans Identität*. Diese ermöglicht in Schritt (6) die Zerlegung von $F(\alpha)$ in die drei Summen $S_1,\ S_2,\ S_3$ und einen Fehlerterm $O(\cdot)$. Daran anschließend können diese in Schritt (7) einzeln abgeschätzt werden.[12] Nach der Zusammenfassung der einzelnen Abschätzungen erhält man eine Abschätzung für $F(\alpha)$ (Schritt (8)), aus welcher sich wiederum eine Abschätzung des Integrals über $\mathfrak{m}$ herleiten lässt (Schritt (9)).

[12] Um die Abschätzung hervorzuheben wird das Vinogradov-Symbol verwendet. Jede der Summen ist dabei kleiner als ein Ausdruck der von N und q abhängig ist. Um diesen hier nicht vollständig ausschreiben zu müssen wird zur Abkürzung $E(N,q)$ geschrieben ($E(\cdot)$ für engl. estimate - Abschätzung). Es sei darauf hingewiesen das richtiger für jede Summe ein anderer Ausdruck $E_i(N,q)$ $(i=1,2,3)$ geschrieben werden müsste. Für eine übersichtlichere Darstellung habe ich darauf verzichtet.



Da nun beide Integrale in Haupt- und Fehlerterm ausgewertet bzw. abgeschätzt wurden, können die Ergebnisse in Schritt (10) zusammengetragen werden. Es ergibt sich ein Ausdruck für $R(N)$, welcher aus dem Hauptterm $\mathfrak{S}(N)\frac{N^2}{2}$ und einem Fehlerterm $O(\cdot)$ besteht. Durch geschickte Abschätzung von $R(N)$ kann in Schritt (11) $r(N)$ eingebracht werden.



Die Umformung dieser Abschätzung nach $r(N)$ liefert den zu Beginn des Abschnitts vorgestellten Ausdruck

$$r(n) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right)$$

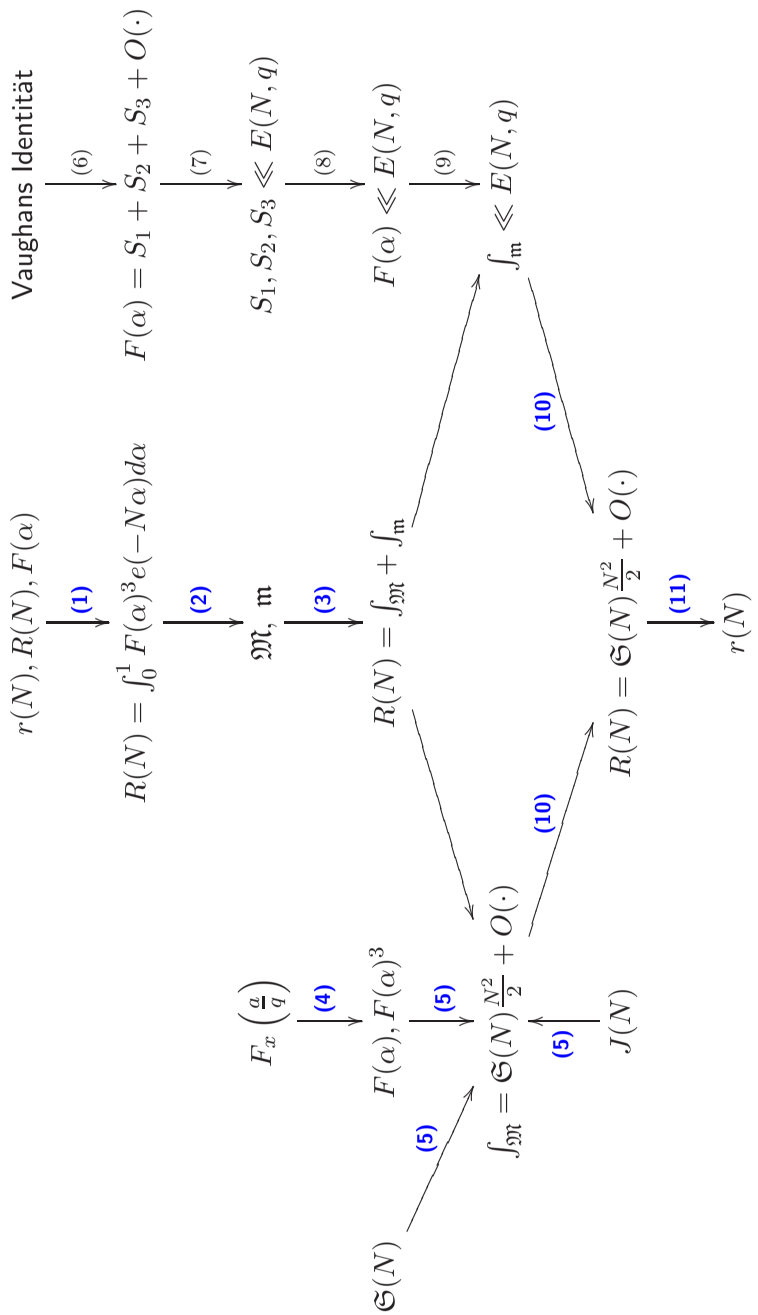
und damit den Satz von Vinogradov. Dieses Ergebnis vereinfachend in Worte fassend erhält man die Aussage

Jede genügend große ungerade Zahl N kann als Summe dreier Primzahlen dargestellt werden. [13]

[13] Vgl. *Schwarz W.*, 1969, S.173

Zum Abschluss dieses Abschnittes sollen die einzelnen Beweisabschnitte noch in einer zusammenfassenden Übersicht festgehalten werden. Farbig hervorgehoben ist, was ich nachfolgend in Kapitel 3 ausführen werde. Zusätzlich wird noch eine Tabelle bereitgestellt, welche den aufgeführten Schritten die entsprechenden Abschnitte und Aussagen zuordnet.[14]

[14] Die Aussage aus Nathonson Abschnitt 8.1 Theorem 8.3 findet sich im Anhang als Satz A.3.39, da es sich bei dieser um ein Hilfmittel handelt.


Vaughans Identität
$r(N), R(N), F(\alpha)$
$R(N) = \int_0^1 F(\alpha)^3 e(-N\alpha) d\alpha$
$\mathfrak{M},\ \mathfrak{m}$
$F_x\left(\frac{a}{q}\right)$
$F(\alpha), F(\alpha)^3$
$\mathfrak{S}(N)$
$\int_{\mathfrak{M}} = \mathfrak{S}(N)\frac{N^2}{2} + O(\cdot)$
$J(N)$
$R(N) = \mathfrak{S}(N)\frac{N^2}{2} + O(\cdot)$
$r(N)$
$F(\alpha) = S_1 + S_2 + S_3 + O(\cdot)$
$S_1, S_2, S_3 \ll E(N, q)$
$R(N) = \int_{\mathfrak{M}} + \int_{\mathfrak{m}}$
$F(\alpha) \ll E(N, q)$
$\int_{\mathfrak{m}} \ll E(N, q)$
(1)
(2)
(3)
(4)
(5)
(5)
(5)
(6)
(7)
(8)
(9)
(10)
(10)
(11)

Schritt	**Abschnitt**	**Aussage**	**Aussage Nathanson Abschnitt 8.1**
Schritt 1	Abschnitt 3.1	Definition 3.1.1 Definition 3.1.3 Definition 3.1.5 Proposition 3.1.6 Proposition 3.1.8	
Schritt 2	Abschnitt 3.1	Propsition 3.1.11 Definition 3.1.12 Proposition 3.1.14 Proposition 3.1.15 Proposition 3.1.17 Definition 3.1.18 Proposition 3.1.21	
Schritt 3	Abschnitt 3.1	Seite 35	
Schritt 4	Abschnitt 3.2.1	Proposition 3.2.1 Proposition 3.2.2 Proposition 3.2.3	Lemma 8.2 Lemma 8.2 Lemma 8.3
Schritt 5	Abschnitt 3.2.2 Abschnitt 3.2.3	Definition 3.2.4 Satz 3.2.5 Korollar 3.2.6 Definition 3.2.8 Proposition 3.2.9 Satz 3.2.10	 Theorem 8.2 Lemma 8.1 Lemma 8.1 Theorem 8.4
Schritt 6	Abschnitt 3.3.1	Proposition 3.3.1 Proposition 3.3.2	Lemma 8.4 Lemma 8.5
Schritt 7	Abschnitt 3.3.1	Proposition 3.3.3 Proposition 3.3.4 Proposition 3.3.5	Lemma 8.6 Lemma 8.7 Lemma 8.8
Schritt 8	Abschnitt 3.3.1	Satz 3.3.6	Theorem 8.5
Schritt 9	Abschnitt 3.3.2	Satz 3.3.7	Theorem 8.6
Schritt 10	Abschnitt 3.4	Satz 3.4.1	Theorem 8.7
Schritt 11	Abschnitt 3.4	Satz 3.4.2 Korollar 3.4.3 Korollar 3.4.4 Korollar 3.4.6	Theorem 8.1

Tabelle 2.1: Zuordnung Beweisschritte und Beweisabschnitte

Kapitel 3

Ausführungen zum Beweis

Da mit den vorangegangenen Kapiteln und dem Anhang nun alle notwendigen Mittel bereitgestellt sind, kann sich dem Beweis zugewandt werden. Dabei empfiehlt es sich parallel zur Beweisführung den Beweisaufbau heranzuziehen, um den Überblick nicht zu verlieren.

3.1 Zerlegung in Basis- und Ergänzungsintervalle

Zu Beginn dieses Abschnitts soll noch einmal an das ternäre Goldbachproblem erinnert werden:

Jede ungerade Zahl größer als Fünf ist als Summe dreier Primzahlen darstellbar. [1]

Entsprechend dem zu untersuchenden Problem wird eine Zählfunktion gewählt.

Definition 3.1.1 (Zählfunktion für das ternäre Goldbachproblem)**.**[2]
Sei N eine ungerade natürliche Zahl größer als Fünf. Dann heißt die Funktion

$$r(N) := \#\{(p_1, p_2, p_3) : p_1 + p_2 + p_3 = N\} = \sum_{p_1+p_2+p_3=N} 1$$

Zählfunktion für das ternäre Goldbachproblem.

Bemerkung 3.1.2.

(i) Unter N soll im Folgenden stets eine ungerade natürliche Zahl verstanden werden, unabhängig davon, ob dies beim Auftreten von N erwähnt wird oder nicht.

(ii) Es sei darauf hingewiesen, dass N im Verlauf des Beweises eine gewissen Mindestgröße abverlangt wird, welche über Fünf liegt. Die Bedingung $N > 5$ soll deshalb nicht weiter mitgeführt werden.

[1] *Bundschuh P.*, 2008, S.292
[2] Vgl.*Nathanson M.B.*, 2010, S.212

Für die Auswertung der Zählfunktion $r(N)$ wird es sich als günstig erweisen, zunächst nicht $r(N)$ selbst zu betrachten, sondern diese mit dem Logarithmus als Gewichtung zu versehen. Diese gewichtete Zählfunktion soll $R(N)$ genannt werden. Grund dieser Vorgehensweise ist, dass sich die gewichtete Zählfunktion technisch einfacher auswerten lässt. Ist dann $R(N)$ ausgewertet, kann das Ergebnis für $r(N)$ daraus abgeleitet werden.

Definition 3.1.3 (gewichtete Zählfunktion für das ternäre Goldbachproblem)**.**[3]
Sei N eine ungerade natürliche Zahl. Dann heißt die Funktion

$$R(N) := \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3$$

gewichtete Zählfunktion für das ternäre Goldbachproblem.

Bemerkung 3.1.4.[4]
Statt mit $\log p$ hätte man $r(N)$ auch mit der von Mangoldt'schen Λ-Funktion gewichten können.

Entsprechend dem Vorgehen bei der Kreismethode wird nun die erzeugende Funktion von $R(N)$ eingeführt.

Definition 3.1.5 (erzeugende Funktion von $R(N)$)**.**[5]
Mit $\alpha \in \mathbb{R}$ sei die erzeugende Funktion von $R(N)$ die Exponentialsumme

$$F(\alpha) := \sum_{p \leq N} (\log p) e(p\alpha).$$

Um nun $R(N)$ als Integral von $F(\alpha)$ darzustellen, wird noch die folgende Orthogonalitätsrelation benötigt.

Proposition 3.1.6.[6]
Sei $k \in \mathbb{Z}$ und $\omega \in \mathbb{R}$. Dann gilt mit der Integrationsvariablen α

$$\int_{-\omega}^{1-\omega} e(k\alpha) d\alpha = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{für } k \in \mathbb{Z}\backslash\{0\}. \end{cases}$$

Beweis.
Sei $\omega \in \mathbb{R}$ beliebig, aber fest gewählt. Dann gilt für $k = 0$

$$\int_{-\omega}^{1-\omega} e(k\alpha) d\alpha = \int_{-\omega}^{1-\omega} e(0 \cdot \alpha) d\alpha = \int_{-\omega}^{1-\omega} 1 d\alpha = [\alpha]_{-\omega}^{1-\omega} = 1 - \omega - (-\omega) = 1.$$

Unter Verwendung von Bemerkung A.1.15 soll der zweite Fall $k \in \mathbb{Z}\backslash\{0\}$ betrachtet werden.

[3] Vgl. *Nathanson M.B.*, 2010, S.214
[4] Vgl. *Davenport H.*, 2000, S.145
[5] Vgl. *Nathanson M.B.*, 2010, S.214
[6] Vgl. *Schwarz W.*, 1969, S.183

Für diesen ist

$$\begin{aligned}\int_{-\omega}^{1-\omega} e(k\alpha)d\alpha &= \int_{-\omega}^{1-\omega} e^{2\pi ik\alpha}d\alpha = \frac{1}{2\pi ik}[e^{2\pi ik\alpha}]_{-\omega}^{1-\omega} = \frac{1}{2\pi ik}\left(e^{2\pi ik(1-\omega)} - e^{-2\pi ik\omega}\right)\\ &= \frac{1}{2\pi ik}\left(e^{2\pi ik-2\pi ik\omega} - e^{-2\pi ik\omega}\right) = \frac{1}{2\pi ik}\left(\underbrace{e^{2\pi ik}}_{=1}e^{-2\pi ik\omega} - e^{-2\pi ik\omega}\right)\\ &= \frac{1}{2\pi ik}\left(e^{-2\pi ik\omega} - e^{-2\pi ik\omega}\right) = 0.\end{aligned}$$

□

Bemerkung 3.1.7.

Für $\omega = 0$ ergibt sich $\int_0^1 e(k\alpha)d\alpha = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{für } k \in \mathbb{Z}\backslash\{0\}. \end{cases}$

Unter Verwendung von Bemerkung 3.1.7 lässt sich nun $R(N)$ als Integral von $F(\alpha)$ darstellen.

Proposition 3.1.8.[7]
Es gilt

$$R(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 = \int_0^1 F(\alpha)^3 e(-N\alpha)d\alpha.$$

Beweis.
Der Schluss auf $R(N)$ ergibt sich durch Umformung des Integralausdrucks unter Berücksichtigung von Bemerkung 3.1.7. Als erstes soll $F(\alpha)^3$ ausgeschrieben werden. Es folgt

$$\begin{aligned}&\int_0^1 F(\alpha)^3 \cdot e(-N\alpha)d\alpha\\ &\qquad = \int_0^1 \sum_{p_1\leq N} \log p_1 e(p_1\alpha) \sum_{p_2\leq N} \log p_2 e(p_2\alpha) \sum_{p_3\leq N} \log p_3 e(p_3\alpha)\cdot e(-N\alpha)d\alpha.\end{aligned}$$

Im nächsten Schritt wird das Produkt der drei Summen über die Primzahlen betrachtet. Für dieses folgt mit Lemma A.1.5

$$\begin{aligned}&\int_0^1 \sum_{p_1\leq N} \log p_1 e(p_1\alpha) \sum_{p_2\leq N} \log p_2 e(p_2\alpha) \sum_{p_3\leq N} \log p_3 e(p_3\alpha)\cdot e(-N\alpha)d\alpha\\ &\qquad = \int_0^1 \sum_{p_1,p_2,p_3\leq N} \log p_1 \log p_2 \log p_3 \cdot e(p_1\alpha + p_2\alpha + p_3\alpha)\cdot e(-N\alpha)d\alpha.\end{aligned}$$

[7] Vgl. *Nathanson M.B.*, 2010, S.215

Als letztes sollen Satz A.1.10 mit der daran anschließenden Bemerkung A.1.11, sowie Bemerkung 3.1.7 angewandt werden. Mit diesen folgt

$$\begin{aligned}
&\int_0^1 \sum_{p_1,p_2,p_3\leq N} \log p_1 \log p_2 \log p_3 \cdot e(p_1\alpha + p_2\alpha + p_3\alpha)\cdot e(-N\alpha)d\alpha \\
&\qquad = \sum_{p_1,p_2,p_3\leq N} \int_0^1 \log p_1 \log p_2 \log p_3 \cdot e(p_1\alpha + p_2\alpha + p_3\alpha)\cdot e(-N\alpha)d\alpha \\
&\qquad = \sum_{p_1,p_2,p_3\leq N} \log p_1 \log p_2 \log p_3 \underbrace{\int_0^1 e(\alpha(p_1+p_2+p_3-N))d\alpha}_{=\begin{cases} 1 & \text{für } p_1+p_2+p_3=N \\ 0 & \text{sonst.}\end{cases}} \\
&\qquad = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 = R(N).
\end{aligned}$$

□

Bemerkung 3.1.9.
Für nachfolgende Betrachtungen genügt es also unter α eine reelle Zahl aus dem Intervall $[0,1]$ zu verstehen.

Nach dem vorangegangenen Kapitel mit dem Abschnitt zur Kreismethode ist bekannt, dass der Wert des Integralausdrucks für $R(N)$ vor allem durch die Werte auf bestimmten Teilmengen des Integrationsbereichs gegeben ist. Diese maßgeblichen Bereiche wurden major arcs genannt, während der Rest des Integrationsbereichs die minor arcs waren.[8] Im weiteren Vorgehen soll nun das Intervall $[0,1]$ in die beiden disjunkten Mengen der Basisintervalle $\mathfrak{M}$ und der Ergänzungsintervalle $\mathfrak{m}$ aufgespalten werden, welche sich für das ternäre Goldbachproblem als günstig erweisen.[9]

Zu diesem Zweck sei von nun an B eine beliebige, aber fest gewählte positive reelle Zahl und $Q := (\log N)^B$ gesetzt.

Bemerkung 3.1.10.
Es muss $Q > 1$ sein, denn für $Q = 1$ folgt

$$Q = 1 \implies (\log N)^B = 1 \implies \log N = 1 \implies N = e < 7.$$

[8] In Anlehnung an Schwarz (Schwarz, Wolfgang: *Einführung in Methoden und Ergebnisse der Primzahltheorie*, 1.Auflage, Mannheim: Bibliographisches Institut, 1969) Seite 184 soll im Folgenden statt der englischsprachigen Originalbezeichnung major arc der Begriff Basisintervall verwendet werden. Ebenso wird Menge der major arcs durch Menge der Basisintervalle ersetzt. Nachdem mir keine deutsche Übersetzung für die Menge der minor arcs bekannt ist, sollen diese als Menge der Ergänzungsintervalle bezeichnet werden.
[9] Es soll an dieser Stelle noch an Bemerkung A.3.3 erinnert werden.

Vor Definition der Basisintervalle soll noch eine notwendige Proposition eingeschoben werden:

Proposition 3.1.11.
Seien die natürliche Zahl q und die nichtnegative ganze Zahl a mit den Eigenschaften $0 \leq a \leq q$ und $(a, q) = 1$ gegeben. Ist $a = q$, dann folgt $a = q = 1$.
Für $a \neq 1$ bedeutet dies $\frac{a}{q} < 1$.

Beweis.
Es gilt

$$1 = (a, q) = (a, a) = a.$$

Diese Gleichung ist nur für die Zahl Eins erfüllt. □

Definition 3.1.12 (Basisintervall $\mathfrak{M}(q, a)$)**.**[10]
Seien die natürliche Zahl q und die nichtnegative ganze Zahl a mit den Eigenschaften $1 \leq q \leq Q$ und $0 \leq a \leq q$, sowie $(a, q) = 1$ gegeben. Dann heißen die Mengen

$$\mathfrak{M}(q, a) := \left\{ \alpha \in [0, 1] : \ \left| \alpha - \frac{a}{q} \right| \leq \frac{Q}{N} \right\}$$

für $q \geq 2$,

$$\mathfrak{M}(1, 0) := \left[0, \frac{Q}{N} \right]$$

für $a = 0, \ q = 1$ und

$$\mathfrak{M}(1, 1) := \left[1 - \frac{Q}{N}, 1 \right]$$

für $a = q = 1$ Basisintervalle.

Bemerkung 3.1.13.

(i) Entgegen dem Eindruck, den die Notation $\mathfrak{M}(q, a)$ vermitteln mag, hängt das Basisintervall $\mathfrak{M}(q, a)$ auch von B und N ab. Dass statt der Notation $\mathfrak{M}(N, B; q, a)$ die Notation $\mathfrak{M}(q, a)$ gewählt wurde, ist der bequemeren Schreibweise geschuldet.[11]

(ii) Es soll an dieser Stelle daran erinnert werden, dass für einen Bruch $\frac{a}{q}$ die Bedingung $(a, q) = 1$ bedeutet, dass dieser Bruch vollständig gekürzt ist.

(iii) Da jedes Basisintervall $\mathfrak{M}(q, a)$ den Punkt $\alpha = \frac{a}{q}$ enthält, ist jedes Basisintervall $\mathfrak{M}(q, a)$ nicht leer, also $\mathfrak{M}(q, a) \neq \emptyset$.

(iv) Sind die beiden vollständig gekürzten rationalen Zahlen $\frac{a}{q}$ und $\frac{\hat{a}}{\hat{q}}$ gleich, dann ist dies äquivalent zu $a = \hat{a}$ und $q = \hat{q}$. Für die beiden ungleichen vollständig gekürzten rationalen Zahlen $\frac{a}{q}$ und $\frac{a'}{q'}$ gilt analog: $\frac{a}{q} \neq \frac{a'}{q'} \Longleftrightarrow a \neq a'$ und $q \neq q'$.

[10] Vgl. *Nathanson M.B.*, 2010, S.126 und 214
[11] *Miller S./Takloo-Bighash R.*, Remark 13.3.12, 2006, S.319

Für weitere Betrachtungen des Basisintervalls $\mathfrak{M}(q,a)$ mit $q \geq 2$ soll dieses, wie auch $\mathfrak{M}(1,0)$ und $\mathfrak{M}(1,1)$, als abgeschlossenes Intervall dargestellt werden. Diese Darstellung wird sich als günstiger erweisen. Zu diesem Zweck wird noch folgende Proposition benötigt:

Proposition 3.1.14.
Seien die natürliche Zahl q und die nichtnegative ganze Zahl a mit den Eigenschaften $1 \leq q \leq Q$ und $0 \leq a \leq q$, sowie $(a,q) = 1$ gegeben. Es gilt

$$\lim_{N\to\infty} \frac{a}{q} - \frac{Q}{N} = \lim_{N\to\infty} \frac{a}{q} + \frac{Q}{N} = \frac{a}{q}.$$

Für große N bedeutet dies

(i) Für $q \geq 2$ ist

$$\left[\frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right] \subset [0,1].$$

(ii) Für $a = 0$ und $q = 1$ ist

$$\mathfrak{M}(1,0) = \left[0, \frac{Q}{N}\right] \subset [0,1].$$

(iii) Für $a = q = 1$ ist

$$\mathfrak{M}(1,1) = \left[1 - \frac{Q}{N}, 1\right] \subset [0,1].$$

Beweis.
Es soll zuerst der Grenzwert betrachtet werden. Mit Beispiel A.2.19 folgt

$$\frac{a}{q} = \frac{a}{q} \pm \lim_{N\to\infty} \frac{(\log N)^B}{N} = \frac{a}{q} \pm \lim_{N\to\infty} \frac{Q}{N} = \lim_{N\to\infty} \frac{a}{q} \pm \frac{Q}{N}.$$

Für $0 \leq a < q$ gilt $0 \leq \frac{a}{q} < 1$, womit für genügend großes N im ersten Fall

$$\left[\frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right] \subset [0,1]$$

folgt. Im zweiten und dritten Fall folgt ebenfalls mit Beispiel A.2.19 für genügend großes N

$$\mathfrak{M}(1,0) = \left[0, \frac{Q}{N}\right] \subset [0,1]$$

bzw.

$$\mathfrak{M}(1,1) = \left[1 - \frac{Q}{N}, 1\right] \subset [0,1].$$

□

Die Basisintervalle $\mathfrak{M}(1,0)$ und $\mathfrak{M}(1,1)$ sind für genügend großes N nach vorangegegener Proposition also eine Teilmenge des Integrationsintervalls $[0,1]$. Die angesprochene Darstellung des Basisintervalls $\mathfrak{M}(q,a)$ für $q \geq 2$ als abgeschlossenes Intervall aus dem Integrationsintervall stellt nun die folgende Proposition bereit.

Proposition 3.1.15.[12]
Für das Basisintervall mit $q \geq 2$ gilt

$$\mathfrak{M}(q,a) = \left[\frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right].$$

Beweis.
Sei für $q \geq 2$ das Basisintervall

$$\mathfrak{M}(q,a) = \left\{\alpha \in [0,1] : \quad \left|\alpha - \frac{a}{q}\right| \leq \frac{Q}{N}\right\}$$

gegeben. Mit Satz A.1.3 gilt

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{Q}{N} \Longleftrightarrow \frac{a}{q} - \frac{Q}{N} \leq \alpha \leq \frac{a}{q} + \frac{Q}{N}.$$

Es ist also

$$\mathfrak{M}(q,a) = \left\{\alpha \in [0,1] : \quad \left|\alpha - \frac{a}{q}\right| \leq \frac{Q}{N}\right\} = \left\{\alpha \in [0,1] : \ \frac{a}{q} - \frac{Q}{N} \leq \alpha \leq \frac{a}{q} + \frac{Q}{N}\right\}.$$

Mit der Definition eines abgeschlossenen Intervalls als $[a,b] := \{x \in \mathbb{R} : a \leq x \leq b\}$ und Proposition 3.1.14 (i) folgt für genügend großes N

$$\mathfrak{M}(q,a) = \left[\frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right].$$

□

Die Basisintervalle $\mathfrak{M}(q,a)$ mit $q \geq 2$ und $\mathfrak{M}(1,0)$, sowie $\mathfrak{M}(1,1)$ sind für genügend großes N also als abgeschlossene Intervalle aus dem Integrationsbereich darstellbar.

Bemerkung 3.1.16.
Für die Darstellung des Basisintervalls $\mathfrak{M}(q,a)$ mit $q \geq 2$ als abgeschlossenes Intervall ergibt sich folgendes Bild:

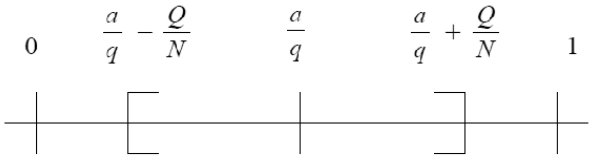


Abbildung 3.1: Skizze Basisintervall

Dessen Intervalllänge ist

$$|\mathfrak{M}(q,a)| = \frac{a}{q} + \frac{Q}{N} - \left(\frac{a}{q} - \frac{Q}{N}\right) = \frac{2Q}{N}.$$

[12] Zur Idee Vgl. *Nathanson M.B.*, 2010, S.126

Für die Intervalllänge der Basisintervalle $\mathfrak{M}(1,0)$ *und* $\mathfrak{M}(1,1)$ *gilt*

$$|\mathfrak{M}(1,0)| = |\mathfrak{M}(1,1)| = \frac{Q}{N}.$$

Unter Zuhilfenahme der Proposition 3.1.15 lässt sich zeigen, dass für genügend große N die Basisintervalle einander nicht überlappen, also paarweise disjunkt sind.

Proposition 3.1.17.[13]
Sei N genügend groß. Dann sind die Basisintervalle $\mathfrak{M}(q,a)$ *und* $\mathfrak{M}(\hat{q},\hat{a})$ *mit* $\frac{a}{q} \neq \frac{\hat{a}}{\hat{q}}$, $q \geq 2,\ \hat{q} \geq 2$ *disjunkt. Ebenso sind die Basisintervalle* $\mathfrak{M}(1,0)$ *und* $\mathfrak{M}(\tilde{q},\tilde{a})$ *mit* $\tilde{q} \geq 2$, *sowie* $\mathfrak{M}(1,1)$ *und* $\mathfrak{M}(\breve{q},\breve{a})$ *mit* $\breve{q} \geq 2$ *disjunkt.*

Beweis.
Als erstes sollen die Basisintervalle $\mathfrak{M}(q,a)$ und $\mathfrak{M}(\hat{q},\hat{a})$ mit $\frac{a}{q} \neq \frac{\hat{a}}{\hat{q}},\ q \geq 2,\ \hat{q} \geq 2$ betrachtet werden. Angenommen die Schnittmenge der beiden Basisintervalle $\mathfrak{M}(q,a)$ und $\mathfrak{M}(\hat{q},\hat{a})$ sei nicht leer, es gäbe also ein $\alpha \in \mathfrak{M}(q,a) \cap \mathfrak{M}(\hat{q},\hat{a})$. Nach Proposition 3.1.15 ist also

$$\alpha \in \left[\frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right] \cap \left[\frac{\hat{a}}{\hat{q}} - \frac{Q}{N}, \frac{\hat{a}}{\hat{q}} + \frac{Q}{N}\right].$$

Es sind im Folgenden zwei Fälle zu betrachten.

1.Fall: Sei $\frac{a}{q} > \frac{\hat{a}}{\hat{q}}$, dann ergibt sich folgende Anordnung der beiden Basisintervalle $\mathfrak{M}(q,a)$ und $\mathfrak{M}(\hat{q},\hat{a})$:

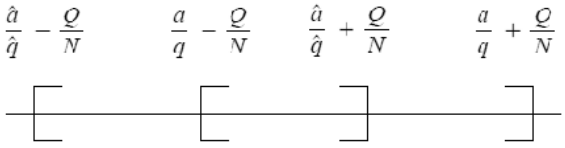


Abbildung 3.2: 1.Fall für überschneidende Basisintervalle

Es ist also

$$\alpha \in \left[\frac{a}{q} - \frac{Q}{N}, \frac{\hat{a}}{\hat{q}} + \frac{Q}{N}\right].$$

Für die Betrachtung der Intervalllänge ergibt sich somit

$$0 \leq \frac{\hat{a}}{\hat{q}} + \frac{Q}{N} - \left(\frac{a}{q} - \frac{Q}{N}\right) = \frac{\hat{a}}{\hat{q}} - \frac{a}{q} + \frac{2Q}{N} \implies \frac{a}{q} - \frac{\hat{a}}{\hat{q}} \leq \frac{2Q}{N}.$$

Aufgrund der zu Beginn des untersuchten Falles festgelegten Größenordnung $\frac{a}{q} > \frac{\hat{a}}{\hat{q}}$ folgt

$$\frac{a}{q} - \frac{\hat{a}}{\hat{q}} \leq \frac{2Q}{N} \implies \left|\frac{a}{q} - \frac{\hat{a}}{\hat{q}}\right| \leq \frac{2Q}{N}.$$

[13] Vgl. *Nathanson M.B.*, 2010, S.214

Nach Bemerkung 3.1.13 (iv) gilt für die beiden vollständig gekürzten Zahlen $\frac{a}{q} \neq \frac{\hat{a}}{\hat{q}} \iff a \neq \hat{a}$ und $q \neq \hat{q}$. Es muss also $|a\hat{q} - \hat{a}q| \geq 1$ gelten. Auch der Fall $\hat{a} = 0$ stellt hierbei kein Problem dar, da wegen der Ungleichheit $\hat{a} \neq a$ und $\hat{q} \geq 1$ der Term $a\hat{q} \geq 1$ bleibt. Mit $q \leq Q$ gelangt man zur Abschätzung

$$\left|\frac{a}{q} - \frac{\hat{a}}{\hat{q}}\right| = \left|\frac{a\hat{q} - \hat{a}q}{q\hat{q}}\right| = \frac{|a\hat{q} - \hat{a}q|}{q\hat{q}} \geq \frac{1}{q\hat{q}} \geq \frac{1}{Q^2}$$

Insgesamt ergibt sich die Abschätzung

$$\frac{1}{Q^2} \leq \frac{2Q}{N} \iff N \leq 2Q^3 = 2(\log N)^{3B}.$$

Für genügend großes N ist diese Ungleichung nach den Ausführungen zu Beispiel A.2.19 falsch. Widerspruch.

2.Fall: Sei $\frac{a}{q} < \frac{\hat{a}}{\hat{q}}$, dann ergibt sich folgende Anordnung der beiden Basisintervalle $\mathfrak{M}(q, a)$ und $\mathfrak{M}(\hat{q}, \hat{a})$:

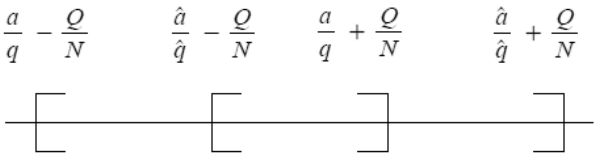


Abbildung 3.3: 2.Fall für überschneidende Basisintervalle

Es ist also

$$\alpha \in \left[\frac{\hat{a}}{\hat{q}} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right].$$

Für die Betrachtung der Intervalllänge ergibt sich somit

$$0 \leq \frac{a}{q} + \frac{Q}{N} - \left(\frac{\hat{a}}{\hat{q}} - \frac{Q}{N}\right) = \frac{a}{q} - \frac{\hat{a}}{\hat{q}} + \frac{2Q}{N} \implies \frac{\hat{a}}{\hat{q}} - \frac{a}{q} \leq \frac{2Q}{N}$$

Aufgrund der zu Beginn des untersuchten Falles festgelegten Größendordnung $\frac{a}{q} < \frac{\hat{a}}{\hat{q}}$ folgt

$$\frac{\hat{a}}{\hat{q}} - \frac{a}{q} \leq \frac{2Q}{N} \implies \left|\frac{\hat{a}}{\hat{q}} - \frac{a}{q}\right| = \left|\frac{a}{q} - \frac{\hat{a}}{\hat{q}}\right| \leq \frac{2Q}{N}.$$

An dieser Stelle kann auf die Argumentation des ersten Falles zurückgegriffen werden. Beide Fälle wurden somit zum Widerspruch geführt. Für genügend großes N ist also der Schnitt $\mathfrak{M}(q, a) \cap \mathfrak{M}(\hat{q}, \hat{a})$ leer.

Als nächstes sollen die Basisintervalle $\mathfrak{M}(\tilde{q},\tilde{a})$ mit $\tilde{q} \geq 2$ und $\mathfrak{M}(1,0)$ betrachtet werden. Angenommen die Schnittmenge der beiden Basisintervalle $\mathfrak{M}(\tilde{q},\tilde{a})$ und $\mathfrak{M}(1,0)$ sei nicht leer, es gäbe also ein $\alpha \in \mathfrak{M}(\tilde{q},\tilde{a}) \cap \mathfrak{M}(1,0)$. Nach Proposition 3.1.15 ist also

$$\alpha \in \left[0, \frac{Q}{N}\right] \cap \left[\frac{\tilde{a}}{\tilde{q}} - \frac{Q}{N}, \frac{\tilde{a}}{\tilde{q}} + \frac{Q}{N}\right].$$

Dann ergibt sich folgende Darstellung

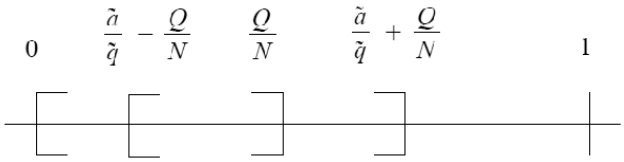


Abbildung 3.4: Unterer Rand

Es ist also

$$\alpha \in \left[\frac{\tilde{a}}{\tilde{q}} - \frac{Q}{N}, \frac{Q}{N}\right].$$

Dann ergibt die Betrachtung der Intervalllänge

$$0 \leq \frac{Q}{N} - \left(\frac{\tilde{a}}{\tilde{q}} - \frac{Q}{N}\right) = -\frac{\tilde{a}}{\tilde{q}} + \frac{2Q}{N} \implies \frac{\tilde{a}}{\tilde{q}} \leq \frac{2Q}{N}.$$

Für $\tilde{q} \geq 2$ kann $\tilde{a} = 0$ nicht auftreten, da sonst $(\tilde{q}, 0) = \tilde{q} \geq 2 \neq 1$ wäre. Es kann also von $\tilde{a} \geq 1$ ausgegangen werden. Mit $1 \leq \tilde{a}$ und $\frac{1}{Q} \leq \frac{\tilde{a}}{\tilde{q}}$ kann weiter abgeschätzt werden und es folgt

$$\frac{1}{Q} \leq \frac{\tilde{a}}{\tilde{q}} \leq \frac{2Q}{N} \implies \frac{1}{Q} \leq \frac{2Q}{N} \implies N \leq 2Q^2 = 2\left(\log N\right)^{2B},$$

was für genügend großes N nach Beispiel A.2.19 falsch ist. Widerspruch. Für genügend großes N ist also der Schnitt $\mathfrak{M}(1,0) \cap \mathfrak{M}(\tilde{q},\tilde{a})$ leer.

Als letztes sollen die Basisintervalle $\mathfrak{M}(\breve{q},\breve{a})$ mit $\breve{q} \geq 2$ und $\mathfrak{M}(1,1)$ betrachtet werden. Angenommen die Schnittmenge der beiden Basisintervalle $\mathfrak{M}(\breve{q},\breve{a})$ und $\mathfrak{M}(1,1)$ sei nicht leer, es gäbe also ein $\alpha \in \mathfrak{M}(\breve{q},\breve{a}) \cap \mathfrak{M}(1,1)$. Nach Proposition 3.1.15 ist also

$$\alpha \in \left[\frac{\breve{a}}{\breve{q}} - \frac{Q}{N}, \frac{\breve{a}}{\breve{q}} + \frac{Q}{N}\right] \cap \left[1 - \frac{Q}{N}, 1\right].$$

Dann ergibt sich folgende Darstellung

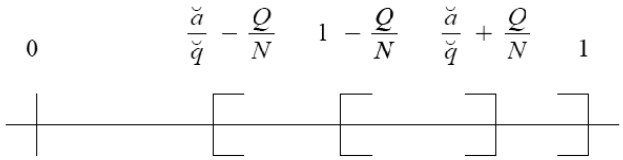


Abbildung 3.5: Oberer Rand

Es ist also

$$\alpha \in \left[1 - \frac{Q}{N}, \frac{\breve{a}}{\breve{q}} + \frac{Q}{N}\right].$$

Die Betrachtung der Intervalllänge ergibt dann

$$0 \leq \frac{\breve{a}}{\breve{q}} + \frac{Q}{N} - \left(1 - \frac{Q}{N}\right) = \frac{\breve{a}}{\breve{q}} - 1 + \frac{2Q}{N} \implies 1 - \frac{\breve{a}}{\breve{q}} = \frac{\breve{q} - \breve{a}}{\breve{q}} \leq \frac{2Q}{N}$$
$$\implies \breve{q} - \breve{a} \leq \frac{2Q\breve{q}}{N} \leq \frac{2Q^2}{N}.$$

Mit $\breve{q} \geq 2$ kann der Fall $\breve{a} = \breve{q} = 1$ nicht eintreten. Es kann also von $\breve{a} < \breve{q}$ ausgegangen werden, woraus folgt, dass die Differenz $\breve{q} - \breve{a} \geq 1$ ist. Damit folgt

$$\breve{q} - \breve{a} \leq \frac{2Q^2}{N} \implies N \leq \frac{2Q^2}{\breve{q} - \breve{a}} \leq 2Q^2,$$

was für genügend große N nach Beispiel A.2.19 falsch ist. Widerspruch. Für genügend großes N ist also der Schnitt $\mathfrak{M}(\breve{q}, \breve{a}) \cap \mathfrak{M}(1,1)$ leer. □

Es soll nun die *Menge der Basisintervalle* $\mathfrak{M}$ als Vereinigung der Basisintervalle definiert werden. Die *Menge der Ergänzungsintervalle* $\mathfrak{m}$ ist dadurch dann automatisch als Rest des Intervalls $[0,1]$ festgelegt.

Definition 3.1.18 (Menge der Basisintervalle $\mathfrak{M}$, Menge der Ergänzungsintervalle $\mathfrak{m}$)**.**[14]
Seien die natürliche Zahl q und die nichtnegative ganze Zahl a mit den Eigenschaften $1 \leq q \leq Q$ und $0 \leq a \leq q$, sowie $(a,q) = 1$ gegeben. Die Vereinigung der Basisintervalle heißt die Menge der Basisintervalle und wird mit

$$\mathfrak{M} := \bigcup_{q=1}^{[Q]} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a) \subseteq [0,1]$$

bezeichnet.

$$\mathfrak{m} := [0,1] \backslash \mathfrak{M}$$

wird die Menge der Ergänzungsintervalle genannt.

[14] Vgl. *Nathanson M.B.*, 2010, S.214 und
Vgl. *Miller S./Takloo-Bighash R.*, 2006, S.319

Bemerkung 3.1.19.
Die Klammer [...] wurde bereits im Anhang Seite 106 eingeführt. Diese ordnet jeder reellen Zahl x die größte ganze Zahl $\leq x$ zu und wird Gauss-Klammer genannt.[15]

Dem besseren Verständnis soll nachfolgendes Beispiel dienen.

Beispiel 3.1.20.
Die Menge der major arcs

$$\mathfrak{M} = \bigcup_{q=1}^{[Q]} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a)$$

soll für verschiedene Ausprägungen des Wertes $[Q]$ betrachtet werden.

(i) Sei $[Q] = 2$. Dann ist

$$\mathfrak{M} = \bigcup_{q=1}^{2} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a) = \left(\bigcup_{\substack{a=0 \\ (a,1)=1}}^{1} \mathfrak{M}(1,a) \right) \cup \left(\bigcup_{\substack{a=0 \\ (a,2)=1}}^{2} \mathfrak{M}(2,a) \right).$$

Nach Bestimmung der größten gemeinsamen Teiler $(0,1) = 1$ und $(1,1) = 1$ folgt für die erste Vereinigung

$$\bigcup_{\substack{a=0 \\ (a,1)=1}}^{1} \mathfrak{M}(1,a) = \mathfrak{M}(1,0) \cup \mathfrak{M}(1,1) = \left[0, \frac{Q}{N}\right] \cup \left[1 - \frac{Q}{N}, 1\right].$$

Nach Bestimmung der größten gemeinsamen Teiler $(0,2) = 2 \neq 1, (1,2) = 1$ und $(2,2) = 2 \neq 1$ folgt für die zweite Vereinigung

$$\bigcup_{\substack{a=0 \\ (a,2)=1}}^{2} \mathfrak{M}(2,a) = \mathfrak{M}(2,1) = \left[\frac{1}{2} - \frac{Q}{N}, \frac{1}{2} + \frac{Q}{N}\right].$$

Insgesamt ergibt sich

$$\begin{aligned} \mathfrak{M} &= \bigcup_{q=1}^{2} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a) \\ &= \left[0, \frac{Q}{N}\right] \cup \left[\frac{1}{2} - \frac{Q}{N}, \frac{1}{2} + \frac{Q}{N}\right] \cup \left[1 - \frac{Q}{N}, 1\right], \end{aligned}$$

also die Basisintervalle an den Punkten 0, $\frac{1}{2}$ und 1.

[15] Vgl. *Scheid H.*, 1994, S.29

(ii) Sei $[Q] = 3$. *Es soll direkt*

$$\mathfrak{M} = \bigcup_{q=1}^{3} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a) = \mathfrak{M}(1,0) \cup \mathfrak{M}(1,1) \cup \mathfrak{M}(2,1) \cup \left(\bigcup_{\substack{a=0 \\ (a,3)=1}}^{3} \mathfrak{M}(3,a) \right).$$

betrachtet werden. Nach Bestimmung der größten gemeinsamen Teiler $(0,3) = 3 \neq 1$, $(1,3) = 1, (2,3) = 1$ *und* $(3,3) = 3 \neq 1$ *folgt*

$$\begin{aligned}
\mathfrak{M} &= \mathfrak{M}(1,0) \cup \mathfrak{M}(1,1) \cup \mathfrak{M}(2,1) \cup \left(\bigcup_{\substack{a=0 \\ (a,3)=1}}^{3} \mathfrak{M}(3,a) \right) \\
&= \mathfrak{M}(1,0) \cup \mathfrak{M}(1,1) \cup \mathfrak{M}(2,1) \cup \mathfrak{M}(3,1) \cup \mathfrak{M}(3,2) \\
&= \left[0, \frac{Q}{N}\right] \cup \left[\frac{1}{3} - \frac{Q}{N}, \frac{1}{3} + \frac{Q}{N}\right] \cup \left[\frac{1}{2} - \frac{Q}{N}, \frac{1}{2} + \frac{Q}{N}\right] \\
&\quad \cup \left[\frac{2}{3} - \frac{Q}{N}, \frac{2}{3} + \frac{Q}{N}\right] \cup \left[1 - \frac{Q}{N}, 1\right].
\end{aligned}$$

Es ergeben sich also die Basisintervalle an den Punkten $0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}$ *und* 1.

Bei dieser Zerlegung nimmt die Menge der Basisintervalle den größeren Anteil des Intervalls $[0,1]$ ein, so wie es bereits im vorangegangenem Abschnitt zur Kreismethode erwähnt wurde.

Proposition 3.1.21.[16]
Für die Mächtigkeit der Menge der Basisintervalle gilt

$$|\mathfrak{M}| < \frac{2Q^3}{N}.$$

Für $N \to \infty$ *bedeutet dies* $|\mathfrak{M}| \to 0$.

Beweis.
Nach Bemerkung 3.1.16 ist die Intervalllänge eines Basisintervalls

$$|\mathfrak{M}(q,a)| = \frac{2Q}{N}$$

für $q \geq 2$, wobei für die Randintervalle

$$|\mathfrak{M}(1,0)| = |\mathfrak{M}(1,1)| = \frac{Q}{N}$$

[16] Zur Idee Vgl. *Miller S./Takloo-Bighash R.*, Exercise 13.3.13, 2006, S.320

gilt. Da sich die Mächtigkeit jeder durch Vereinigung entstandenen Menge als Summe der Mächtigkeiten der Teilmengen ergibt, folgt mit Proposition 3.1.17

$$\begin{aligned}
|\mathfrak{M}| &= \left| \bigcup_{q=1}^{[Q]} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a) \right| = \sum_{q=1}^{[Q]} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} |\mathfrak{M}(q,a)| \\
&= \sum_{\substack{a=0 \\ (a,1)=1}}^{1} |\mathfrak{M}(1,a)| + \sum_{\substack{a=0 \\ (a,2)=1}}^{2} |\mathfrak{M}(2,a)| + ... + \sum_{\substack{a=0 \\ (a,[Q])=1}}^{[Q]} |\mathfrak{M}([Q],a)| \\
&= |\mathfrak{M}(1,0)| + |\mathfrak{M}(1,1)| + \sum_{\substack{a=0 \\ (a,2)=1}}^{2} |\mathfrak{M}(2,a)| + ... + \sum_{\substack{a=0 \\ (a,[Q])=1}}^{[Q]} |\mathfrak{M}([Q],a)| \\
&= \frac{Q}{N} + \frac{Q}{N} + \sum_{\substack{a=0 \\ (a,2)=1}}^{2} |\mathfrak{M}(2,a)| + ... + \sum_{\substack{a=0 \\ (a,[Q])=1}}^{[Q]} |\mathfrak{M}([Q],a)| \\
&= \frac{2Q}{N} + \sum_{\substack{a=0 \\ (a,2)=1}}^{2} |\mathfrak{M}(2,a)| + ... + \sum_{\substack{a=0 \\ (a,[Q])=1}}^{[Q]} |\mathfrak{M}([Q],a)|.
\end{aligned}$$

Da in jeder Summe maximal $[Q] \leq Q$ Summanden auftreten, kann weiter

$$\frac{2Q}{N} + \sum_{\substack{a=0 \\ (a,2)=1}}^{2} |\mathfrak{M}(2,a)| + ... + \sum_{\substack{a=0 \\ (a,[Q])=1}}^{[Q]} |\mathfrak{M}([Q],a)| < \underbrace{\frac{2Q^2}{N} + \frac{2Q^2}{N} + ... + \frac{2Q^2}{N}}_{Q-mal} = \frac{2Q^3}{N}$$

abgeschätzt werden. In der entstandenen Abschätzung für die Mächtigkeit der Menge der Basisintervalle

$$|\mathfrak{M}| < \frac{2Q^3}{N}$$

geht der Ausdruck $\frac{2Q^3}{N} = \frac{2(\log N)^{3B}}{N}$ nach Beispiel A.2.19 mit wachsendem N gegen Null. Es muss also auch $|\mathfrak{M}|$ mit wachsendem N gegen Null gehen. □

Bemerkung 3.1.22.
Mit wachsendem N liegt der Hauptteil des Intervalls $[0,1]$ *in der Menge der Ergänzungsintervalle* $\mathfrak{m}$.

Mit dieser Zerlegung des Integrationsintervalls $[0,1]$ in die, für genügend großes N disjunkte, Menge der Basisintervalle $\mathfrak{M}$ und die Menge der Ergänzungsintervalle $\mathfrak{m}$, kann zur Betrachtung von $R(N)$ zurückgekehrt werden.
Als abkürzende Schreibweise für die Summe der Integrale über jedes einzelne Basisintervall, also

$$\sum_{q=1}^{[Q]} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} F(\alpha)^3 e(-N\alpha) d\alpha = \sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} F(\alpha)^3 e(-N\alpha) d\alpha,$$

soll

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha) d\alpha$$

verwendet werden. Nach Proposition 3.1.14 und Proposition 3.1.15 ist jedes Basisintervall ein abgeschlossenes Intervall aus dem Integrationsintervall $[0,1]$. Da sich diese nach Proposition 3.1.17 nicht überlappen, bereitet die Summierung der Integrale keine Probleme.[17]
Ist $\mathfrak{m}_1$ ein offenes Intervall zwischen zwei Basisintervallen, dann ist

$$\int_{\mathfrak{m}_1} F(\alpha)^3 e(-N\alpha) d\alpha$$

ein Lebesgue-Integral[18]. Da $\mathfrak{m}$ als Vereinigung disjunkter offener Mengen wieder offen ist[19], ist

$$\int_{\mathfrak{m}} F(\alpha)^3 e(-N\alpha) d\alpha$$

ein Lebesgue-Integral[20]. Es folgt[21]

$$\begin{aligned} \int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha) d\alpha + \int_{\mathfrak{m}} F(\alpha)^3 e(-N\alpha) d\alpha &= \int_0^1 F(\alpha)^3 e(-N\alpha) d\alpha \\ &= \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 \\ &= R(N). \end{aligned}$$

Die Spaltung des Integralausdrucks für $R(N)$ ermöglicht es nun, einen asymptotischen Ausdruck für $R(N)$ zu gewinnen. Der Hauptteil dieses Ausdrucks wird sich dabei aus dem Integral über die Menge der Basisintervalle $\mathfrak{M}$ ergeben, während das Integral über die Menge der Ergänzungsintervalle $\mathfrak{m}$ zum Fehlerterm beiträgt. Mit dem Integral über die Menge der Basisintervalle wird sich der nächste Abschnitt befassen.

[17] Mit Bemerkung A.1.11 handelt es sich um die Summe von Riemann-Integralen (deren Integrationsintervalle einander nicht überschneiden).
[18] *Elstrodt, J.*, 2007, S.129
[19] Proposition 3.1.17 in Verbindung mit *Heuser H.*, Satz 34.8, 2009, S.218
[20] *Elstrodt, J.*, Gleichung (3.4), 2007, S.129 in Verbindung mit *Heuser H.*, Satz 124.4, 2008, S.91
[21] Vgl.*Nathanson M.B.*, 2010, S.215

3.2 Das Integral über die Basisintervalle

In diesem Abschnitt soll der Hauptterm von $R(N)$ aus der Auswertung des Integrals über die Menge der Basisintervalle $\mathfrak{M}$ gewonnen werden. Hierzu wird $F(\alpha)$ zunächst an rationalen Stellen betrachtet. Im Anschluss daran sollen dann die singuläre Reihe und das singuläre Integral ausgewertet werden, bevor sich zum Abschluss dieses Abschnitts dem Integral über die Menge der Basisintervalle zugewandt wird.

3.2.1 Die erzeugende Funktion an rationalen Stellen

In diesem Abschnitt wird $F(\alpha)$ zunächst an den rationalen Stellen $\alpha = \frac{a}{q}$ betrachtet. Als Hilfsmittel zu dieser Betrachtung wird zunächst allerdings noch folgende Proposition benötigt.

Proposition 3.2.1.[22]
Seien r und q natürliche Zahlen für die $p \equiv r \ mod \ q$ gelte. Dann ist $p \mid q$ äuivalent zu $(r, q) > 1$.

Beweis.
Sei $p \equiv r \ mod \ q$ für die natürlichen Zahlen r und q vorausgesetzt. Im ersten Schritt soll von $p \mid q$ auf $(r, q) > 1$ geschlossen werden. Mit der Definition der Kongruenz gilt

$$p \equiv r \ mod \ q \Longleftrightarrow \exists \lambda \in \mathbb{Z} : \ p - r = \lambda q \Longleftrightarrow r = p - \lambda q.$$

Zudem ist nach der Definition der Teilbarkeit

$$p \mid q \Longleftrightarrow q = mp.$$

Die Zahl m ist aufgrund der Bedingung $1 \leq q \leq Q$ eine natürliche Zahl. Dann folgt für den größten gemeinsamen Teiler

$$(r, q) = (p - \lambda q, q) = (p - \lambda mp, mp) = (p(1 - \lambda m), mp) = p > 1,$$

da die kleinste Primzahl 2 ist. Auch Bedenken wegen ungünstiger Fälle können mit Bemerkung A.3.3 ausgeräumt werden, denn für $\lambda = m = 1$ folgt

$$(p(1 - 1), p) = (0, p) = p.$$

Im zweiten Schritt ist von $(r, q) > 1$ auf $p \mid q$ zu schließen. Ist der größte gemeinsame Teiler der Zahlen r und q größer als Eins, dann sind beide Zahlen nicht teilerfremd und es folgt

$$(r, q) > 1 \implies \exists m \in \mathbb{N}, \ m = (r, q) > 1 : \ m \mid r \text{ und } m \mid q.$$

Nach der Definition der Teilbarkeit ist

$$m \mid q \Longleftrightarrow q = \hat{m}m$$

[22] Vgl. *Nathanson M.B.*, 2010, S.216

mit $\hat{m} \in \mathbb{N}$. Mit Satz A.3.4 folgt

$$m \mid p \Longrightarrow m = p,$$

da p eine Primzahl ist. Durch einsetzen gelangt man nun zu

$$q = \hat{m}m = \hat{m}p \Longleftrightarrow p \mid q.$$

Damit ist der Beweis abgeschlossen. □

Nun zur Betrachtung an den rationalen Stellen.

Proposition 3.2.2.[23]
Sei

$$F_x(\alpha) := \sum_{p \leq x} (\log p) e(p\alpha)$$

und seien B und C positive reelle Zahlen. Ist $1 \leq q \leq Q = (\log N)^B$ und $(q, a) = 1$, dann ist

$$F_x\left(\frac{a}{q}\right) = \frac{\mu(q)}{\varphi(q)} x + O\left(\frac{QN}{(\log N)^C}\right)$$

für $1 \leq x \leq N$, wobei die implizite Konstante nur von B und C abhängig ist.

Beweis.
Sei die rationale Zahl $\alpha = \frac{a}{q}$ mit $q \in \mathbb{N}, a \in \mathbb{N}_0$ und den Eigenschaften $1 \leq q \leq Q = (\log N)^B$ für $B > 0$, sowie $(q, a) = 1$ gegeben. Dann ist

$$F_x\left(\frac{a}{q}\right) = \sum_{p \leq x} \log p \cdot e\left(\frac{pa}{q}\right)$$

aufgrund der Periodizität von $e(\cdot)$ und der Teilerfremdheit von a und q von den Resten abhängig, die nach Division von p durch q bleiben. Sortieren der p nach Restklassen $mod\ q$, also nach $p \equiv r\ mod\ q$ für $r = 1, ..., q$ ergibt

$$\begin{aligned}\sum_{p \leq x} \log p \cdot e\left(\frac{pa}{q}\right) &= \sum_{r=1}^{q} \sum_{\substack{p \leq x \\ p \equiv r\ mod\ q}} \log p \cdot e\left(\frac{pa}{q}\right) \\ &= \sum_{\substack{r=1 \\ (r,q)=1}}^{q} \sum_{\substack{p \leq x \\ p \equiv r\ mod\ q}} \log p \cdot e\left(\frac{pa}{q}\right) + \sum_{\substack{r=1 \\ (r,q)>1}}^{q} \sum_{\substack{p \leq x \\ p \equiv r\ mod\ q}} \log p \cdot e\left(\frac{pa}{q}\right).\end{aligned}$$

[23] *Nathanson M.B.*, Lemma 8.2, 2010, S.216

Letztere der beiden Summen soll nun abgeschätzt werden. Mit Proposition 3.2.1 folgt für diese

$$\sum_{\substack{r=1\\(r,q)>1}}^{q} \sum_{p\leq x \atop p\equiv r \mod q} \log p \cdot e\left(\frac{pa}{q}\right) = \sum_{\substack{p\leq x\\ p|q}} \log p \cdot e\left(\frac{pa}{q}\right).$$

Die Anwendung der Hilfsmittel Satz A.1.4 und Satz A.1.14 (iii), sowie die Tatsache, dass $\log p$ für jede Primzahl positiv ist, also $\log p > 0$ für jede Primzahl gilt, führt zu

$$\begin{aligned}\left|\sum_{\substack{p\leq x\\ p|q}} \log p \cdot e\left(\frac{pa}{q}\right)\right| &\leq \sum_{\substack{p\leq x\\ p|q}} \left|\log p \cdot e\left(\frac{pa}{q}\right)\right| = \sum_{\substack{p\leq x\\ p|q}} \log p \cdot \left|e\left(\frac{pa}{q}\right)\right| \\ &= \sum_{\substack{p\leq x\\ p|q}} \log p.\end{aligned}$$

Da die letzte Summe aufgrund der Bedingung $p \leq x \leq N$ nicht alle Primzahlen beinhalten muss, die q teilen, kann im Weiteren

$$\sum_{\substack{p\leq x\\ p|q}} \log p \leq \sum_{p|q} \log p$$

abgschätzt werden. Mittels Logarithmusregel folgt dann für die Summe über die Teiler von q, dass

$$\sum_{p|q} \log p = \log p_1 + ... + \log p_n = \log p_1 ... p_n$$

ist. Da nicht ausgeschlossen werden kann, dass in der Primfaktorzerlegung von q eine oder gar mehrere Primzahlen mehrfach vorkommen, q also Primzahlen in höherer Potenz als Eins beinhalten kann, folgt die Abschätzung

$$\log p_1 ... p_n \leq \log q.$$

Dieser Ausdruck lässt sich wegen der Eigenschaft $q \leq Q$ mit

$$\log q \leq \log Q$$

abschätzen. Insgesamt kann also festgehalten werden, dass

$$\sum_{\substack{r=1\\(r,q)>1}}^{q} \sum_{p\leq x \atop p\equiv r \mod q} \log p \cdot e\left(\frac{pa}{q}\right) = O\left(\log Q\right)$$

gilt. Mit dieser Abschätzung soll zur Betrachtung von $F_x\left(\frac{a}{q}\right)$ zurückgekehrt werden. Es ist dann

$$\sum_{\substack{r=1\\(r,q)=1}}^{q} \sum_{\substack{p\leq x\\ p\equiv r \ mod \ q}} \log p \cdot e\left(\frac{pa}{q}\right) + \sum_{\substack{r=1\\(r,q)>1}}^{q} \sum_{\substack{p\leq x\\ p\equiv r \ mod \ q}} \log p \cdot e\left(\frac{pa}{q}\right)$$
$$= \sum_{\substack{r=1\\(r,q)=1}}^{q} \sum_{\substack{p\leq x\\ p\equiv r \ mod \ q}} \log p \cdot e\left(\frac{pa}{q}\right) + O\left(\log Q\right).$$

Für die weitere Betrachtung soll wieder die Periodizität von $e(\cdot)$ genutzt werden. Da $p \equiv r \ mod \ q$ äquivalent zur Existenz einer ganzen Zahl λ ist, mit welcher $p - r = \lambda q \Longleftrightarrow p = \lambda q + r$ gilt, folgt durch Einsetzen

$$e\left(\frac{pa}{q}\right) = e^{2\pi i \frac{pa}{q}} = e^{2\pi i \frac{(\lambda q + r)a}{q}} = e^{2\pi i \lambda a + 2\pi i \frac{ra}{q}} = \underbrace{e^{2\pi i \lambda a}}_{=1} e^{2\pi i \frac{ra}{q}} = e\left(\frac{ra}{q}\right).$$

Damit ist

$$\sum_{\substack{r=1\\(r,q)=1}}^{q} \sum_{\substack{p\leq x\\ p\equiv r \ mod \ q}} \log p \cdot e\left(\frac{pa}{q}\right) + O\left(\log Q\right) = \sum_{\substack{r=1\\(r,q)=1}}^{q} \sum_{\substack{p\leq x\\ p\equiv r \ mod \ q}} \log p \cdot e\left(\frac{ra}{q}\right) + O\left(\log Q\right)$$
$$= \sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right) \sum_{\substack{p\leq x\\ p\equiv r \ mod \ q}} \log p + O\left(\log Q\right).$$

Mit der Definition der weiterentwickelten ϑ-Funktion von Seite 105 und dem Satz von Siegel-Walfisz, Satz A.3.39, folgt weiter

$$\sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right) \sum_{\substack{p\leq x\\ p\equiv r \ mod \ q}} \log p + O\left(\log Q\right) = \sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right) \vartheta(x;q,a) + O\left(\log Q\right)$$
$$= \sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right) \left(\frac{x}{\varphi(q)} + O\left(\frac{x}{(\log x)^C}\right)\right) + O\left(\log Q\right),$$

wobei die implizite Konstante nun von der reellen Zahl $C > 0$ abhängig ist. Als nächstes kann mit der Definition der Ramanujan-Summe, Definition A.3.21, eine übersichtlichere

Darstellung erreicht werden:

$$\begin{aligned}\sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right)\left(\frac{x}{\varphi(q)}+O\left(\frac{x}{(\log x)^C}\right)\right)+O\left(\log Q\right)&\\ = c_q(a)\left(\frac{x}{\varphi(q)}+O\left(\frac{x}{(\log x)^C}\right)\right)+O\left(\log Q\right)&\\ = \frac{c_q(a)}{\varphi(q)}x+c_q(a)O\left(\frac{x}{(\log x)^C}\right)+O\left(\log Q\right).&\end{aligned}$$

In letzterer Darstellung soll nun zunächst der zweite Term zusammengefasst werden. Daran anschließend folgt eine Zusammenfassung mit dem dritten Term. Mit den Hilfsmitteln Satz A.1.4 und Satz A.1.14 (iii) folgt

$$\begin{aligned}\left|c_q(a)O\left(\frac{x}{(\log x)^C}\right)\right| &= \left|\sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right)O\left(\frac{x}{(\log x)^C}\right)\right|\\ &\leq \left|\sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right)\cdot K_C\cdot\frac{x}{(\log x)^C}\right|\\ &\leq \sum_{\substack{r=1\\(r,q)=1}}^{q}\left|e\left(\frac{ra}{q}\right)\cdot K_C\cdot\frac{x}{(\log x)^C}\right|\\ &= \sum_{\substack{r=1\\(r,q)=1}}^{q}\left|e\left(\frac{ra}{q}\right)\right|\cdot K_C\cdot\frac{x}{(\log x)^C}\\ &= \sum_{\substack{r=1\\(r,q)=1}}^{q} 1\cdot K_C\cdot\frac{x}{(\log x)^C}\\ &\leq K_C\cdot\frac{qx}{(\log x)^C}.\end{aligned}$$

Mit Beispiel A.2.19, sowie $x \leq N$ und $q \leq Q = (\log N)^B$ $(B > 0)$ folgt weiter

$$K_C\cdot\frac{qx}{(\log x)^C} \leq K_C\cdot\frac{QN}{(\log N)^C}.$$

Es kann zusammenfassend

$$c_q(a)O\left(\frac{x}{(\log x)^C}\right) = O\left(\frac{QN}{(\log N)^C}\right)$$

festgehalten werden. Dabei ist die implizite Konstante von den reellen Zahlen $B > 0$ und $C > 0$ abhängig. Damit folgt

$$\begin{aligned}\frac{c_q(a)}{\varphi(q)}x + c_q(a)O\left(\frac{x}{(\log x)^C}\right) + O\left(\log Q\right) &= \frac{c_q(a)}{\varphi(q)}x + O\left(\frac{QN}{(\log N)^C}\right) + O\left(\log Q\right) \\ &= \frac{c_q(a)}{\varphi(q)}x + O\left(\max\left\{\frac{QN}{(\log N)^C}, \log Q\right\}\right).\end{aligned}$$

Für die Zusammenfassung der beiden $O(\cdot)$-Terme ist nun noch das Maximum zu ermitteln. Es folgt für entsprechendes N

$$(\log N)^B > \log(\log N)^B \Longrightarrow (\log N)^B \cdot \frac{N}{(\log N)^C} = \frac{QN}{(\log N)^C} > \log(\log N)^B = \log Q.$$

Daraus folgt die Zusammenfassung

$$O\left(\max\left\{\frac{QN}{(\log N)^C}, \log Q\right\}\right) = O\left(\frac{QN}{(\log N)^C}\right),$$

wobei die implizite Konstante von den reellen Zahlen $B > 0$ und $C > 0$ abhängig ist. Insgesamt ist damit

$$\frac{c_q(a)}{\varphi(q)}x + O\left(\max\left\{\frac{QN}{(\log N)^C}, \log Q\right\}\right) = \frac{c_q(a)}{\varphi(q)}x + O\left(\frac{QN}{(\log N)^C}\right).$$

Als letztes wird nun noch Korollar A.3.24 benötigt. Wegen der Teilerfremdheit $(q, a) = 1$ ergibt sich mit diesem $c_q(a) = \mu(q)$ und es ist dann

$$F_x\left(\frac{a}{q}\right) = \frac{\mu(q)}{\varphi(q)}x + O\left(\frac{QN}{(\log N)^C}\right),$$

wobei die implizite Konstante noch von den reellen Zahlen $B > 0$ und $C > 0$ abhängig ist. □

In nächsten Schritt wird die gewonnene Asymptotik ausgedehnt, indem $F(\alpha)$ für $\alpha = \frac{a}{q} + \beta$ betrachtet wird. Dabei soll unter β eine reelle Zahl verstanden werden. Anschließend wird das Ergebnis dann für die Funktion $F(\alpha)^3$ hergeleitet, denn diese ist es, welche im Integral über die Menge der Basisintervalle $\mathfrak{M}$ auftritt.

Proposition 3.2.3.[24]
Sei

$$u(\beta) := \sum_{m=1}^{N} e(m\beta)$$

und seien B und C positive reellen Zahlen, wobei $C > 2B$ gelte. Für $\alpha \in \mathfrak{M}(q,a)$, $\alpha = \frac{a}{q}+\beta$ ist dann

$$F(\alpha) = \frac{\mu(q)}{\varphi(q)} u(\beta) + O\left(\frac{Q^2 N}{(\log N)^C}\right)$$

und

$$F(\alpha)^3 = \frac{\mu(q)}{\varphi(q)^3} u(\beta)^3 + O\left(\frac{Q^2 N^3}{(\log N)^C}\right),$$

wobei die impliziten Konstanten nur von B und C abhängen.

Beweis.
Sei $\frac{a}{q}$ eine rationale Zahl mit $q \in \mathbb{N}, a \in \mathbb{N}_0$ und den Eigenschaften $1 \leq q \leq Q = (\log N)^B$ für $B > 0$, sowie $(q,a) = 1$. Weiter sei $\alpha = \frac{a}{q} + \beta$ eine reelle Zahl aus dem Basisintervall $\mathfrak{M}(q,a)$ mit passend gewähltem β, also einem solchen β, für das aufgrund der Definition 3.1.12 des Basisintervalls $\mathfrak{M}(q,a) := \left\{\alpha \in [0,1] : \left|\alpha - \frac{a}{q}\right| \leq \frac{Q}{N}\right\}$ die Abschätzung

$$\left|\alpha - \frac{a}{q}\right| = \left|\frac{a}{q} + \beta - \frac{a}{q}\right| = |\beta| \leq \frac{Q}{N}$$

gelte. Auf diese Abschätzung von β soll im weiteren Verlauf des Beweises noch Bezug genommen werden. Als nützliche Hilfsfunktion soll noch

$$\lambda(m) := \begin{cases} \log p & \text{für } m = p \in \mathbb{P} \\ 0 & \text{sonst} \end{cases}$$

bereitgestellt werden. Um nun eine Näherung für die erzeugende Funktion $F(\cdot)$ aus Definition 3.1.5 herzuleiten, wird $F(\cdot)$ mit $\alpha = \frac{a}{q} + \beta$ betrachtet. Sei

$$u(\beta) := \sum_{m=1}^{N} e(m\beta),$$

[24] *Nathanson M.B.*, Lemma 8.1, 2010, S.215 und
Nathanson M.B., Lemma 8.3, 2010, S.217

dann ist mit $\lambda(m)$ die Differenz

$$\begin{aligned}\left|F(\alpha)-\frac{\mu(q)}{\varphi(q)}u(\beta)\right| &= \left|\sum_{p\leq N}\log p\cdot e(p\alpha)-\frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{N}e(m\beta)\right| \\ &= \left|\sum_{m=1}^{N}\lambda(m)e(m\alpha)-\frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{N}e(m\beta)\right| \\ &= \left|\sum_{m=1}^{N}\lambda(m)e\left(m\left(\frac{a}{q}+\beta\right)\right)-\frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{N}e(m\beta)\right| \\ &= \left|\sum_{m=1}^{N}\lambda(m)e\left(\frac{ma}{q}+m\beta\right)-\frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{N}e(m\beta)\right|.\end{aligned}$$

Mittels der Umformung

$$e\left(\frac{ma}{q}+m\beta\right)=e^{2\pi i\left(\frac{ma}{q}+m\beta\right)}=e^{2\pi i\frac{ma}{q}}\cdot e^{2\pi im\beta}=e\left(\frac{ma}{q}\right)\cdot e\left(m\beta\right)$$

folgt für die Differenz

$$\begin{aligned}&\left|\sum_{m=1}^{N}\lambda(m)e\left(\frac{ma}{q}+m\beta\right)-\frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{N}e(m\beta)\right| \\ &\qquad= \left|\sum_{m=1}^{N}\lambda(m)e\left(\frac{ma}{q}\right)e\left(m\beta\right)-\sum_{m=1}^{N}\frac{\mu(q)}{\varphi(q)}e(m\beta)\right| \\ &\qquad= \left|\sum_{m=1}^{N}\left(\lambda(m)e\left(\frac{ma}{q}\right)-\frac{\mu(q)}{\varphi(q)}\right)e(m\beta)\right|.\end{aligned}$$

Zur Anwendung der partiellen Summation, Satz A.3.43, sollen für $1\leq x\leq N$ die Definitionen

$$A(x):=\sum_{1\leq m\leq x}\left(\lambda(m)e\left(\frac{ma}{q}\right)-\frac{\mu(q)}{\varphi(q)}\right)$$

und

$$f(m):=e(m\beta)$$

getroffen werden. Da die Funktion $f(m)$ nach Satz A.1.14 (ii) auf ganz $\mathbb{C}$ holomorph, die Ableitung

$$f'(m)=2\pi i\beta e^{2\pi im\beta}=2\pi i\beta e(m\beta)$$

also stetig ist, folgt mit partieller Summation

$$\left|\sum_{m=1}^{N}\left(\lambda(m)e\left(\frac{ma}{q}\right)-\frac{\mu(q)}{\varphi(q)}\right)e(m\beta)\right| = \left|A(N)e(N\beta)-\int_1^N A(x)\left(e(x\beta)\right)'dx\right|$$
$$= \left|A(N)e(N\beta)-2\pi i\beta\int_1^N A(x)e(x\beta)dx\right|.$$

Um den letzten Ausdruck abschätzen zu können, soll zunächst für $1 \leq x \leq N$ die Summenfunktion $A(x)$ abgeschätzt werden. Für diese ist

$$\begin{aligned}
&\left|A(x)-\left(\sum_{1\leq m\leq x}\lambda(m)e\left(\frac{ma}{q}\right)-\frac{\mu(q)}{\varphi(q)}x\right)\right| \\
&= \left|\sum_{1\leq m\leq x}\left(\lambda(m)e\left(\frac{ma}{q}\right)-\frac{\mu(q)}{\varphi(q)}\right)-\left(\sum_{1\leq m\leq x}\lambda(m)e\left(\frac{ma}{q}\right)-\frac{\mu(q)}{\varphi(q)}x\right)\right| \\
&= \left|\sum_{1\leq m\leq x}\lambda(m)e\left(\frac{ma}{q}\right)-\sum_{1\leq m\leq x}\frac{\mu(q)}{\varphi(q)}-\sum_{1\leq m\leq x}\lambda(m)e\left(\frac{ma}{q}\right)+\frac{\mu(q)}{\varphi(q)}x\right| \\
&= \left|-\sum_{1\leq m\leq x}\frac{\mu(q)}{\varphi(q)}+\frac{\mu(q)}{\varphi(q)}x\right| = \left|\sum_{m=1}^{[x]}\frac{\mu(q)}{\varphi(q)}-\frac{\mu(q)}{\varphi(q)}x\right| \\
&= \left|\frac{\mu(q)}{\varphi(q)}\sum_{m=1}^{[x]}1-\frac{\mu(q)}{\varphi(q)}x\right| = \left|\frac{\mu(q)}{\varphi(q)}[x]-\frac{\mu(q)}{\varphi(q)}x\right| \\
&= \left|([x]-x)\frac{\mu(q)}{\varphi(q)}\right| = \left|(x-[x])\frac{\mu(q)}{\varphi(q)}\right|.
\end{aligned}$$

Mit der auf Seite 106 erklärten Aufspaltung einer reellen Zahl $x = [x] + \{x\},\ \{x\} \in [0,1)$ und Berücksichtigung des Wertebereichs der μ-Funktion, welcher aus den Elementen der Menge $\{-1,0,1\}$ besteht, folgt als weitere Abschätzung

$$\left|(x-[x])\frac{\mu(q)}{\varphi(q)}\right| = \left|\{x\}\cdot\frac{\mu(q)}{\varphi(q)}\right| < \left|\frac{\mu(q)}{\varphi(q)}\right| \leq \left|\frac{1}{\varphi(q)}\right| = \frac{1}{\varphi(q)}.$$

Unter Berücksichtigung des Wachstumsverhaltens der φ-Funktion kann letzter Ausdruck mit

$$\frac{1}{\varphi(q)} \leq 1$$

abgeschätzt werden. Es ist also

$$A(x) = \sum_{1\leq m\leq x}\lambda(m)e\left(\frac{ma}{q}\right)-\frac{\mu(q)}{\varphi(q)}x+O\left(1\right).$$

Im nächsten Schritt wird auf die Definition von $F_x(\cdot)$ aus Proposition 3.2.2 zurückgegriffen. Nach dieser ist

$$F_x\left(\frac{a}{q}\right) = \sum_{p \leq x} \log p \cdot e\left(\frac{pa}{q}\right)$$

womit

$$\sum_{1 \leq m \leq x} \lambda(m) e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)} x + O(1) = F_x\left(\frac{a}{q}\right) - \frac{\mu(q)}{\varphi(q)} x + O(1)$$

folgt. Nachdem das Resultat von Proposition 3.2.2

$$F_x\left(\frac{a}{q}\right) = \frac{\mu(q)}{\varphi(q)} x + O\left(\frac{QN}{(\log N)^C}\right)$$

auch als

$$F_x\left(\frac{a}{q}\right) - \frac{\mu(q)}{\varphi(q)} x = O\left(\frac{QN}{(\log N)^C}\right)$$

geschrieben werden kann, wobei die implizite Konstante in beiden Darstellungen von den positiven reellen Zahlen B und C abhängig ist, folgt

$$F_x\left(\frac{a}{q}\right) - \frac{\mu(q)}{\varphi(q)} x + O(1) = O\left(\frac{QN}{(\log N)^C}\right) + O(1).$$

Es gilt

$$\begin{aligned} O\left(\frac{QN}{(\log N)^C}\right) + O(1) &= O\left(\max\left\{\frac{QN}{(\log N)^C}, 1\right\}\right) \\ &= O\left(\max\left\{\frac{N}{(\log N)^{C-B}}, 1\right\}\right) = O\left(\frac{QN}{(\log N)^C}\right), \end{aligned}$$

womit die Abschätzung

$$A(x) = O\left(\frac{QN}{(\log N)^C}\right)$$

festgehalten werden kann. Die implizite Konstante ist dabei natürlich weiterhin von den reellen Zahlen $B > 0$ und $C > 0$ abhängig. Mit der gewonnenen Abschätzung für $A(x)$ kann nun die Abschätzung von

$$\left| A(N) e(N\beta) - 2\pi i \beta \int_1^N A(x) e(x\beta) dx \right|$$

fortgesetzt werden. Mit der Integralabschätzung Satz A.1.17 und Satz A.1.14 (iii) folgt

$$\begin{aligned}
\left|A(N)e(N\beta) - 2\pi i\beta\int_1^N A(x)e(x\beta)dx\right| &\leq |A(N)e(N\beta)| + \left|-2\pi i\beta\int_1^N A(x)e(x\beta)dx\right| \\
&= |A(N)\,|\cdot|\,e(N\beta)| + 2\pi\,|\beta| \cdot \left|\int_1^N A(x)e(x\beta)dx\right| \\
&\leq \Big|A(N)\Big| + 2\pi\,|\beta| \int_1^N |A(x)e(x\beta)|\,dx \\
&= \Big|A(N)\Big| + 2\pi\,|\beta| \int_1^N |A(x)| \cdot |e(x\beta)|\,dx \\
&= \Big|A(N)\Big| + 2\pi\,|\beta| \int_1^N |A(x)|\,dx \\
&= \Big|A(N)\Big| + 2\pi\,|\beta| \left(|A(x)|\,[x]_1^N\right) \\
&= |A(N)\,| + 2\pi\,|\beta|\,(N-1)\,|A(x)| \\
&\leq |A(N)\,| + 2\pi\,|\beta| \cdot N \cdot \max\{|A(x)| : 1 \leq x \leq N\}.
\end{aligned}$$

Es gilt also die Abschätzung

$$A(N)e(N\beta) - 2\pi i\beta\int_1^N A(x)e(x\beta)dx \ll |A(N)| + |\beta| \cdot N \cdot \max\{|A(x)| : 1 \leq x \leq N\}.$$

Nun kommen die gewonnenen Abschätzungen

$$|\beta| \leq \frac{Q}{N} \quad \text{und} \quad A(x) = O\left(\frac{QN}{(\log N)^C}\right)$$

zum Einsatz. Mit diesen Abschätzungen folgt

$$\begin{aligned}
|A(N)| + |\beta| \cdot N \cdot \max\{|A(x)| : 1 \leq x \leq N\} &\leq O\left(\frac{QN}{(\log N)^C}\right) + \frac{Q}{N} \cdot N \cdot O\left(\frac{QN}{(\log N)^C}\right) \\
&= O\left(\frac{QN}{(\log N)^C}\right) + Q \cdot O\left(\frac{QN}{(\log N)^C}\right) \\
&= O\left(\frac{QN}{(\log N)^C}\right) + O\left(\frac{Q^2N}{(\log N)^C}\right) \\
&= O\left(\max\left\{\frac{QN}{(\log N)^C}, \frac{Q^2N}{(\log N)^C}\right\}\right) \\
&= O\left(\frac{Q^2N}{(\log N)^C}\right).
\end{aligned}$$

Zusammenfassend kann damit

$$F(\alpha) - \frac{\mu(q)}{\varphi(q)}u(\beta) = O\left(\frac{Q^2N}{(\log N)^C}\right)$$

bzw.

$$F(\alpha) = \frac{\mu(q)}{\varphi(q)} u(\beta) + O\left(\frac{Q^2 N}{(\log N)^C}\right)$$

festgehalten werden, wobei die implizite Konstante von den positiven reellen Zahlen B und C abhängig ist. Für den Hauptterm gilt unter Berücksichtigung der Werte der μ- und φ-Funktion die Abschätzung

$$\left|\frac{\mu(q)}{\varphi(q)} u(\beta)\right| = \left|\frac{\mu(q)}{\varphi(q)}\right| \cdot |u(\beta)| \leq |u(\beta)| = \left|\sum_{m=1}^{N} e(m\beta)\right|,$$

welche mit Satz A.1.4 und Satz A.1.14 (iii) weiter durch

$$\left|\sum_{m=1}^{N} e(m\beta)\right| \leq \sum_{m=1}^{N} |e(m\beta)| = \sum_{m=1}^{N} 1 = N$$

abgeschätzt werden kann. Im Fehlerterm soll deshalb $C > 2B$ gesetzt werden, denn dann gilt

$$\frac{Q^2 N}{(\log N)^C} = \frac{(\log N)^{2B} N}{(\log N)^C} = \frac{N}{(\log N)^{C-2B}} < N.$$

Für den Beweis des zweiten Teils der Proposition ist nun die Funktion $F(\alpha)^3$ zu betrachten. Es folgt für diese

$$\begin{aligned}
F(\alpha)^3 &= \left(\frac{\mu(q)}{\varphi(q)} u(\beta) + O\left(\frac{Q^2 N}{(\log N)^C}\right)\right)^3 \\
&= \sum_{k=0}^{3} \binom{3}{k} \left(\frac{\mu(q)}{\varphi(q)} u(\beta)\right)^{3-k} \left(O\left(\frac{Q^2 N}{(\log N)^C}\right)\right)^k \\
&= \binom{3}{0} \left(\frac{\mu(q)}{\varphi(q)} u(\beta)\right)^3 \left(O\left(\frac{Q^2 N}{(\log N)^C}\right)\right)^0 + \binom{3}{1} \left(\frac{\mu(q)}{\varphi(q)} u(\beta)\right)^2 \left(O\left(\frac{Q^2 N}{(\log N)^C}\right)\right)^1 \\
&\quad + \binom{3}{2} \left(\frac{\mu(q)}{\varphi(q)} u(\beta)\right)^1 \left(O\left(\frac{Q^2 N}{(\log N)^C}\right)\right)^2 + \binom{3}{3} \left(\frac{\mu(q)}{\varphi(q)} u(\beta)\right)^0 \left(O\left(\frac{Q^2 N}{(\log N)^C}\right)\right)^3 \\
&= \frac{\mu(q)^3}{\varphi(q)^3} u(\beta)^3 + 3 \cdot \frac{\mu(q)^2}{\varphi(q)^2} u(\beta)^2 \cdot O\left(\frac{Q^2 N}{(\log N)^C}\right) \\
&\quad + 3 \cdot \frac{\mu(q)}{\varphi(q)} u(\beta) \cdot O\left(\left(\frac{Q^2 N}{(\log N)^C}\right)^2\right) + O\left(\left(\frac{Q^2 N}{(\log N)^C}\right)^3\right).
\end{aligned}$$

Berücksichtigt man, dass die μ-Funktion nur die Werte der Menge $\{-1, 0, 1\}$ annimmt, folgt $\mu(q)^3 = \mu(q)$ und für den ersten Term ist

$$\frac{\mu(q)^3}{\varphi(q)^3} u(\beta)^3 = \frac{\mu(q)}{\varphi(q)^3} u(\beta)^3.$$

Für die nachfolgende Abschätzung soll zum einen $|u(\beta)| \leq N$ verwendet werden, was bereits zuvor gezeigt wurde. Zum anderen soll zur Abschätzung der Terme $\frac{\mu(q)^2}{\varphi(q)^2}$ und $\frac{\mu(q)}{\varphi(q)}$ verwendet werden, dass die μ-Funktion maximal den Wert Eins und die φ-Funktion minimal den Wert Eins annimmt. Es folgt damit

$$\begin{aligned}
&\frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + 3\cdot\frac{\mu(q)^2}{\varphi(q)^2}u(\beta)^2\cdot O\left(\frac{Q^2N}{(\log N)^C}\right) + 3\cdot\frac{\mu(q)}{\varphi(q)}u(\beta)\cdot O\left(\left(\frac{Q^2N}{(\log N)^C}\right)^2\right)\\
&\qquad + O\left(\left(\frac{Q^2N}{(\log N)^C}\right)^3\right)\\
&\leq \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + 3N^2O\left(\frac{Q^2N}{(\log N)^C}\right) + 3NO\left(\left(\frac{Q^2N}{(\log N)^C}\right)^2\right)\\
&\qquad + O\left(\left(\frac{Q^2N}{(\log N)^C}\right)^3\right)\\
&= \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(3\frac{Q^2N^3}{(\log N)^C}\right) + O\left(3\frac{Q^4N^3}{(\log N)^{2C}}\right) + O\left(\frac{Q^6N^3}{(\log N)^{3C}}\right)\\
&= \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\frac{Q^2N^3}{(\log N)^C}\right) + O\left(\frac{Q^4N^3}{(\log N)^{2C}}\right) + O\left(\frac{Q^6N^3}{(\log N)^{3C}}\right)\\
&= \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\max\left\{\frac{Q^2N^3}{(\log N)^C}, \frac{Q^4N^3}{(\log N)^{2C}}, \frac{Q^6N^3}{(\log N)^{3C}}\right\}\right)\\
&= \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\max\left\{\frac{N^3}{(\log N)^{C-2B}}, \frac{N^3}{(\log N)^{2C-4B}}, \frac{N^3}{(\log N)^{3C-6B}}\right\}\right)\\
&= \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\max\left\{\frac{N^3}{(\log N)^{C-2B}}, \frac{N^3}{(\log N)^{2(C-2B)}}, \frac{N^3}{(\log N)^{3(C-2B)}}\right\}\right).
\end{aligned}$$

Da das Minimum der Exponenten im Nenner

$$\min\{C-2B, 2(C-2B), 3(C-2B)\} = C-2B$$

ist, folgt

$$\max\left\{\frac{N^3}{(\log N)^{C-2B}}, \frac{N^3}{(\log N)^{2(C-2B)}}, \frac{N^3}{(\log N)^{3(C-2B)}}\right\} = \frac{N^3}{(\log N)^{C-2B}} = \frac{Q^2N^3}{(\log N)^C}.$$

Damit ist

$$\begin{aligned}
&\frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\max\left\{\frac{Q^2N^3}{(\log N)^C}, \frac{Q^4N^3}{(\log N)^{2C}}, \frac{Q^6N^3}{(\log N)^{3C}}\right\}\right)\\
&\qquad = \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\frac{Q^2N^3}{(\log N)^C}\right).
\end{aligned}$$

Zusammenfassend kann also festgehalten werden, dass

$$F(\alpha)^3 = \frac{\mu(q)}{\varphi(q)^3}u(\beta)^3 + O\left(\frac{Q^2N^3}{(\log N)^C}\right)$$

gilt, wobei die implizite Konstante von den positiven reellen Zahlen B und C abhängig ist, für welche $C > 2B$ gesetzt ist. □

3.2.2 Die singuläre Reihe und das singuläre Integral

In diesem Abschnitt wird sich der singulären Reihe und dem singulären Integral zugewandt. Theoretisch sind zwar alle notwendigen Vorbetrachtungen abgeschlossen um das Integral über die Menge der Basisintervalle $\mathfrak{M}$ auswerten zu können, dabei wird man allerdings auch auf die *singuläre Reihe* $\mathfrak{S}(N)$ und das *singuläre Integral* $J(N)$ stoßen. Um die Auswertung des Integrals über die Menge der Basisintervalle $\mathfrak{M}$ nicht unnötig mit Betrachtungen zu diesen zu verlängern, sollen diese zuvor ausgewertet werden.

Definition 3.2.4 (singuläre Reihe für das ternäre Goldbachproblem)**.**[25]
Die arithmetische Funktion

$$\mathfrak{S}(N) := \sum_{q=1}^{\infty} \frac{\mu(q)c_q(N)}{\varphi(q)^3}$$

heißt singuläre Reihe für das ternäre Goldbachproblem, wobei $c_q(N)$ die Ramanujan-Summe

$$c_q(N) = \sum_{\substack{a=1 \\ (q,a)=1}}^{q} e\left(\frac{aN}{q}\right)$$

bezeichnet.

Für die singuläre Reihe gilt

Satz 3.2.5.[26]
Es gilt:

(i) Die singuläre Reihe $\mathfrak{S}(N)$ konvergiert absolut und gleichmäßig auf $\mathbb{N}$.

(ii) Für die beschränkte singuläre Reihe

$$\mathfrak{S}(N,Q) := \sum_{q \leq Q} \frac{\mu(q)c_q(N)}{\varphi(q)^3}$$

gilt für jedes $\varepsilon > 0$

$$\mathfrak{S}(N,Q) = \mathfrak{S}(N) + O\left(Q^{-(1-\varepsilon)}\right),$$

wobei die implizite Konstante nur von ε abhängig ist.

(iii) Die singuläre Reihe $\mathfrak{S}(N)$ hat das Euler-Produkt

$$\mathfrak{S}(N) = \prod_{p} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{p^2 - 3p + 3}\right).$$

[25] Vgl. *Nathanson M.B.*, 2010, S.212
[26] Vgl. *Nathanson M.B.*, Theorem 8.2, 2010, S.212 und *Vinogradov, I.M.*, 2004, S.175

(iv) Für die singuläre Reihe $\mathfrak{S}(N)$ existieren positive Konstanten c_1 und c_2, sodass

$$\frac{6}{\pi^2} \leq c_1 < \mathfrak{S}(N) < c_2$$

für alle ungeraden N gilt.

Beweis.
Der Beweis der Proposition ist in vier Teile gegliedert. Im ersten Teil soll gezeigt werden, dass $\mathfrak{S}(N)$ absolut und gleichmäßig konvergiert. Daran anschließend soll im zweiten Teil die Abschätzung zwischen $\mathfrak{S}(N)$ und $\mathfrak{S}(N,Q)$ hergeleitet werden. Der dritte Teil befasst sich mit der Darstellung von $\mathfrak{S}(N)$ als Produkt bevor im vierten Teil die Existenz der positiven Konstanten c_1 und c_2 gezeigt wird.

1. Teil: Um die absolute und gleichmäßige Konvergenz von $\mathfrak{S}(N)$ zu zeigen muss zunächst eine geeignete Abschätzung für die Ramanujan-Summe $c_q(N)$ hergeleitet werden. Nach Satz A.3.25 kann diese auch als

$$c_q(N) = \frac{\mu\left(\frac{q}{(q,N)}\right)}{\varphi\left(\frac{q}{(q,N)}\right)} \cdot \varphi(q)$$

dargestellt werden. Unter Berücksichtigung der Werte der μ- und φ-Funktion folgt für $q \in \mathbb{N}$ die Abschätzung

$$|c_q(N)| = \left|\frac{\mu\left(\frac{q}{(q,N)}\right)}{\varphi\left(\frac{q}{(q,N)}\right)} \cdot \varphi(q)\right| = \left|\frac{\mu\left(\frac{q}{(q,N)}\right)}{\varphi\left(\frac{q}{(q,N)}\right)}\right| \cdot |\varphi(q)| \leq |\varphi(q)| = \varphi(q).$$

Als weiteres Hilfsmittel wird noch die Abschätzung aus Satz A.3.14

$$q^{1-\varepsilon} < \varphi(q) \Longleftrightarrow \frac{1}{\varphi(q)} < \frac{1}{q^{1-\varepsilon}}$$

für $\varepsilon > 0$ und genügend großes q benötigt. Mit den bereitgestellten Abschätzungen und unter Berücksichtigung der Werte der μ- und φ-Funktion folgt

$$\begin{aligned}\left|\frac{\mu(q)c_q(N)}{\varphi(q)^3}\right| = \frac{|\mu(q)| \cdot |c_q(N)|}{\varphi(q)^3} &\leq \frac{|\mu(q)| \cdot \varphi(q)}{\varphi(q)^3} \leq \frac{1}{\varphi(q)^2} \\ &< \frac{1}{(q^{1-\varepsilon})^2} = \frac{1}{q^{2-2\varepsilon}} = \frac{1}{q^{-\varepsilon}q^{2-\varepsilon}} = q^{-\varepsilon}\frac{1}{q^{2-\varepsilon}}.\end{aligned}$$

Mit genügend großem q und $\varepsilon > 0$ folgt weiter

$$q^{-\varepsilon}\frac{1}{q^{2-\varepsilon}} \ll \frac{1}{q^{2-\varepsilon}}.$$

Nach Satz A.1.8 konvergiert

$$\sum_{q=1}^{\infty} \frac{1}{q^{2-\varepsilon}}$$

für $0 < \varepsilon < 1$. Da

$$\left|\frac{\mu(q)c_q(N)}{\varphi(q)^3}\right| \leq K_\varepsilon \cdot \frac{1}{q^{2-\varepsilon}} \quad (K_\varepsilon > 0)$$

für genügend großes q gilt, folgt mit dem Majorantenkriterium Satz A.1.6, dass $\mathfrak{S}(N)$ für $N \in \mathbb{N}$ absolut konvergiert.
Mit dem Weierstraß'schen Majorantenkriterium Satz A.1.7 folgt die gleichmäßige Konvergenz auf $\mathbb{N}$.

2.Teil: In diesem Teil soll die Beziehung $\mathfrak{S}(N,Q) = \mathfrak{S}(N) + O\left(Q^{-(1-\varepsilon)}\right)$ hergeleitet werden. Zu diesem Zweck betrachtet man die Differenz

$$|\mathfrak{S}(N,Q) - \mathfrak{S}(N)| = |\mathfrak{S}(N) - \mathfrak{S}(N,Q)| = \left|\sum_{q=1}^{\infty} \frac{\mu(q)c_q(N)}{\varphi(q)^3} - \sum_{q\leq Q} \frac{\mu(q)c_q(N)}{\varphi(q)^3}\right|$$
$$= \left|\sum_{q>Q} \frac{\mu(q)c_q(N)}{\varphi(q)^3}\right|.$$

Mit der folgenden Abschätzung aus dem ersten Teil

$$\left|\frac{\mu(q)c_q(N)}{\varphi(q)^3}\right| \leq \frac{1}{\varphi(q)^2} < q^{-\varepsilon}\frac{1}{q^{2-\varepsilon}} \ll \frac{1}{q^{2-\varepsilon}}$$

und Satz A.1.9 folgt

$$\left|\sum_{q>Q} \frac{\mu(q)c_q(N)}{\varphi(q)^3}\right| \leq \sum_{q>Q} \left|\frac{\mu(q)c_q(N)}{\varphi(q)^3}\right| \leq \sum_{q>Q} \frac{1}{\varphi(q)^2} \ll \sum_{q>Q} \frac{1}{q^{2-\varepsilon}},$$

wobei die implizite Konstante von $\varepsilon > 0$ abhängig ist. Mit Satz A.2.20 folgt die weitere Abschätzung

$$\sum_{q>Q} \frac{1}{q^{2-\varepsilon}} \ll Q^{1-(2-\varepsilon)} = Q^{-1+\varepsilon} = Q^{-(1-\varepsilon)}.$$

Als Ergebnis kann also die Abschätzung

$$\mathfrak{S}(N,Q) - \mathfrak{S}(N) = O\left(Q^{-(1-\varepsilon)}\right)$$

bzw.

$$\mathfrak{S}(N,Q) = \mathfrak{S}(N) + O\left(Q^{-(1-\varepsilon)}\right)$$

festgehalten werden, wobei die implizite Konstante nur von $\varepsilon > 0$ abhängig ist.

3.Teil: Die Herleitung der Darstellung von $\mathfrak{S}(N)$ als Euler-Produkt soll in diesem Teil erfolgen. Um die notwendigen Umformungen möglichst geschlossen durchführen zu können, soll zuerst die Ramanujan-Summe $c_q(N)$ bzgl. ihres Verhaltens auf Primteiler von N untersucht werden. Sei $q = p$ und p ein Teiler von N dann folgt

$$p \mid N \Longrightarrow (p, N) = p.$$

Für die Darstellung der Ramanujan-Summe nach Satz A.3.23 bedeutet dies

$$c_p(N) = \sum_{d|(p,N)} \mu\left(\frac{p}{d}\right) d = \sum_{d|p} \mu\left(\frac{p}{d}\right) d.$$

Als Teiler von p kann d nur die Werte 1 und p annehmen und es folgt weiter mit der Definition der μ-Funktion, Definition A.3.15

$$\sum_{d|p} \mu\left(\frac{p}{d}\right) d = \mu\left(\frac{p}{p}\right) \cdot p + \mu\left(\frac{p}{1}\right) = \mu(1) \cdot p + \mu(p) = p - 1.$$

Es kann also $c_p(N) = p - 1$ für $p \mid N$ festgehalten werden. Ist p jedoch kein Teiler von N, dann folgt

$$p \nmid N \Longrightarrow (p, N) = 1.$$

Mit Korollar A.3.24 und der Definition der μ-Funktion, Definition A.3.15 ist dann

$$c_p(N) = \mu(p) = (-1)^1 = -1.$$

Für die Ramanujan-Summe gilt also

$$c_p(N) = \begin{cases} p - 1 & \text{für } p \mid N \\ -1 & \text{für } p \nmid N. \end{cases} \qquad (*)$$

Um $\mathfrak{S}(N)$ mit Satz A.3.46 als Euler-Produkt darzustellen sind noch die Voraussetzungen des Satzes zu prüfen. Der Ausdruck

$$\frac{\mu(q)c_q(N)}{\varphi(q)^3}$$

wird sich dann multiplikativ verhalten, wenn es jede der beteiligten Funktionen und die Ramanujan-Summe tun. Für die μ-Funktion soll Satz A.3.16, für die φ-Funktion Satz A.3.13 und für die Ramanujan-Summe Satz A.3.22 verwendet werden. Ist $(m, n) = 1$, dann gilt also

$$\frac{\mu(mn)c_{mn}(N)}{\varphi(mn)^3} = \frac{\mu(m)\mu(n)c_m(N)c_n(N)}{\varphi(m)^3\varphi(n)^3} = \frac{\mu(m)c_m(N)}{\varphi(m)^3} \cdot \frac{\mu(n)c_n(N)}{\varphi(n)^3}.$$

Die noch vorausgesetzte Konvergenz wurde bereits im ersten Teil des Beweises gezeigt. Mit Satz A.3.46 folgt nun

$$\begin{aligned}\mathfrak{S}(N) &= \sum_{q=1}^{\infty} \frac{\mu(q)c_q(N)}{\varphi(q)^3} = \prod_p \left(1 + \sum_{j=1}^{\infty} \frac{\mu(p^j)c_{p^j}(N)}{\varphi(p^j)^3}\right) \\ &= \prod_p \left(1 + \frac{\mu(p)c_p(N)}{\varphi(p)^3} + \frac{\mu(p^2)c_{p^2}(N)}{\varphi(p^2)^3} + ...\right).\end{aligned}$$

Für die μ-Funktion ergibt sich mit Definition A.3.15 und der sich daran anschließenden Bemerkung - $\mu(p^j) = 0$ für $j \geq 2$ und $\mu(p) = -1$ - , dass

$$\begin{aligned}\prod_p \left(1 + \frac{\mu(p)c_p(N)}{\varphi(p)^3} + \frac{\mu(p^2)c_{p^2}(N)}{\varphi(p^2)^3} + ...\right) &= \prod_p \left(1 + \frac{\mu(p)c_p(N)}{\varphi(p)^3}\right) \\ &= \prod_p \left(1 - \frac{c_p(N)}{\varphi(p)^3}\right)\end{aligned}$$

gilt. Nachdem für eine Primzahl nicht gleichzeitig $p \mid N$ und $p \nmid N$ gelten kann, kann das Produkt aufgespalten werden. Mit $(*)$ gilt nun:

$$\begin{aligned}\prod_p \left(1 - \frac{c_p(N)}{\varphi(p)^3}\right) &= \prod_{p\nmid N} \left(1 - \frac{c_p(N)}{\varphi(p)^3}\right) \prod_{p|N} \left(1 - \frac{c_p(N)}{\varphi(p)^3}\right) \\ &= \prod_{p\nmid N} \left(1 + \frac{1}{\varphi(p)^3}\right) \prod_{p|N} \left(1 - \frac{p-1}{\varphi(p)^3}\right).\end{aligned}$$

Nun soll Korollar A.3.12 für die φ-Funktion verwendet werden, mit welchem

$$\begin{aligned}\prod_{p\nmid N} \left(1 + \frac{1}{\varphi(p)^3}\right) \prod_{p|N} \left(1 - \frac{p-1}{\varphi(p)^3}\right) &= \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{p-1}{(p-1)^3}\right) \\ &= \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right)\end{aligned}$$

folgt. Vor dem letzten Umformungsschritt soll noch eine Termumformung eingeschoben werden. Es ist

$$\begin{aligned}\frac{1 - \frac{1}{(p-1)^2}}{1 + \frac{1}{(p-1)^3}} &= \frac{1 - \frac{1}{(p-1)^2}}{1 + \frac{1}{(p-1)^3}} \cdot \frac{(p-1)^3}{(p-1)^3} = \frac{(p-1)^3 - (p-1)}{(p-1)^3 + 1} = \frac{p^3 - 3p^2 + 3p - 1 - p + 1}{p^3 - 3p^2 + 3p - 1 + 1} \\ &= \frac{p^3 - 3p^2 + 2p}{p^3 - 3p^2 + 3p} = \frac{p^2 - 3p + 2 + 1 - 1}{p^2 - 3p + 3} = 1 - \frac{1}{p^2 - 3p + 3},\end{aligned}$$

womit dann die Umformung

$$\begin{aligned}
&\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)\\
&\qquad=\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(\left(1-\frac{1}{(p-1)^2}\right)\cdot\frac{\left(1+\frac{1}{(p-1)^3}\right)}{\left(1+\frac{1}{(p-1)^3}\right)}\right)\\
&\qquad=\prod_{p\nmid N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(\frac{1-\frac{1}{(p-1)^2}}{1+\frac{1}{(p-1)^3}}\right)\\
&\qquad=\prod_{p}\left(1+\frac{1}{(p-1)^3}\right)\prod_{p|N}\left(1-\frac{1}{p^2-3p+3}\right)
\end{aligned}$$

gilt.

4.Teil: Im letzten Teil des Beweises soll nun die Existenz der positiven Konstanten c_1 und c_2 hergeleitet werden, mit welchen die Abschätzung $c_1 < \mathfrak{S}(N) < c_2$ gilt. Es soll mit der Abschätzung nach unten begonnen werden. Mit der Produktdarstellung von $\mathfrak{S}(N)$ folgt

$$\mathfrak{S}(N)=\prod_{p\nmid N}\underbrace{\left(1+\frac{1}{(p-1)^3}\right)}_{>1}\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)>\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right).$$

Da für die Faktoren

$$0<1-\frac{1}{(p-1)^2}<1\quad(p\in\mathbb{P}\backslash\{2\})$$

gilt, wird das Produkt umso kleiner, je mehr Faktoren in dieses eingehen. Hieraus folgt

$$\begin{aligned}
\prod_{p|N}\left(1-\frac{1}{(p-1)^2}\right)&>\prod_{p\geq 3}\left(1-\frac{1}{(p-1)^2}\right)\\
&=\left(1-\frac{1}{(3-1)^2}\right)\left(1-\frac{1}{(5-1)^2}\right)\left(1-\frac{1}{(7-1)^2}\right)...\\
&>\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)...\\
&=\prod_{p}\left(1-\frac{1}{p^2}\right).
\end{aligned}$$

Mit Satz A.3.31 und Bemerkung A.3.33 ist das letzte Produkt

$$\prod_{p}\left(1-\frac{1}{p^2}\right)=\frac{1}{\zeta(2)}=\frac{1}{\frac{\pi^2}{6}}=\frac{6}{\pi^2}.$$

Es gilt also die Abschätzung

$$\frac{6}{\pi^2}<\mathfrak{S}(N).$$

Nachdem damit gezeigt wurde, dass $\mathfrak{S}(N)$ nach unten beschränkt ist, kann auf die Existenz einer positiven Konstanten c_1 geschlossen werden für welche

$$\frac{6}{\pi^2} \leq c_1 < \mathfrak{S}(N)$$

gilt. Da im ersten Teil des Beweises $\mathfrak{S}(N)$ nach oben durch eine konvergente Reihe abgeschätzt werden konnte, existiert auch eine positive Konstante c_2 mit welcher $\mathfrak{S}(N) < c_2$ gilt. Insgesamt gilt also

$$\frac{6}{\pi^2} \leq c_1 < \mathfrak{S}(N) < c_2.$$

□

Korollar 3.2.6.
Für die singuläre Reihe $\mathfrak{S}(N)$ existieren positive Konstanten c_1 und c_2, sodass

$$\frac{6}{\pi^2} \leq c_1 < \mathfrak{S}(N) < c_2 \leq \frac{2457}{\pi^6}$$

für alle ungeraden N gilt.

Beweis.
Die Abschätzung nach unten kann Satz 3.2.5 (iv) entnommen werden. Für die Abschätzung nach oben soll die Produktdarstellung

$$\mathfrak{S}(N) = \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{p^2 - 3p + 3}\right)$$

abgeschätzt werden. Es folgt

$$\begin{aligned}
\mathfrak{S}(N) &= \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \underbrace{\left(1 - \frac{1}{p^2 - 3p + 3}\right)}_{<1} \\
&\leq \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \\
&= \left(1 + \frac{1}{(2-1)^3}\right) \prod_{p \geq 3} \left(1 + \frac{1}{(p-1)^3}\right) \\
&= 2 \cdot \prod_{p \geq 3} \left(1 + \frac{1}{(p-1)^3}\right) \\
&= 2 \cdot \left(1 + \frac{1}{(3-1)^3}\right) \left(1 + \frac{1}{(5-1)^3}\right) \left(1 + \frac{1}{(7-1)^3}\right) ... \\
&< 2 \cdot \left(1 + \frac{1}{2^3}\right) \left(1 + \frac{1}{3^3}\right) \left(1 + \frac{1}{5^3}\right) ... \\
&= 2 \cdot \prod_p \left(1 + \frac{1}{p^3}\right).
\end{aligned}$$

Mit Satz A.3.32 und Bemerkung A.3.33 folgt weiter

$$2 \cdot \prod_p \left(1 + \frac{1}{p^3}\right) = 2 \cdot \frac{\zeta(3)}{\zeta(6)} = 2 \cdot \frac{\zeta(3)}{\frac{\pi^6}{945}} = \frac{1890 \cdot \zeta(3)}{\pi^6}$$
$$< \frac{1890 \cdot 1,3}{\pi^6} = \frac{2457}{\pi^6}.$$

Es gilt also

$$\frac{6}{\pi^2} \leq c_1 < \mathfrak{S}(N) < c_2 \leq \frac{2457}{\pi^6}$$

für die positiven Konstanten c_1 und c_2. □

Bemerkung 3.2.7.

(i) Die hier aufgeführten Abschätzungen der singulären Reihe $\mathfrak{S}(N)$ sind noch ungenau, denn tatsächlich ist $\mathfrak{S}(N) \approx 1$ für große ungerade N.[27] *Mit mehr Aufwand lässt sich also eine bessere obere bzw. untere Schranke finden.*

(ii) Als Beziehung zwischen $\mathfrak{S}(N)$ und $\mathfrak{S}(N,Q)$ soll festgehalten werden, dass

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \frac{\mu(q)c_q(N)}{\varphi(q)^3} = \lim_{Q\to\infty} \sum_{q\leq Q} \frac{\mu(q)c_q(N)}{\varphi(q)^3} = \lim_{Q\to\infty} \mathfrak{S}(N,Q)$$

gilt.

Es soll sich nun dem singulären Integral zugewandt werden.

Definition 3.2.8 (singuläres Integral für das ternäre Goldbachproblem)**.**[28]
Das Integral

$$J(N) := \int_{-\frac{1}{2}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta) d\beta$$

heißt singuläres Integral für das ternäre Goldbachproblem.

Für das singuläre Integral gilt

Proposition 3.2.9.[29]
Sei $J(N)$ das singuläre Integral für das ternäre Goldbachproblem. Es gilt

$$J(N) = \frac{N^2}{2} + O(N).$$

[27] *Davenport H.*, 2000, S.146
[28] *Nathanson M.B.*, Lemma 8.1, 2010, S.215
[29] *Nathanson M.B.*, Lemma 8.1, 2010, S.215

Beweis.
Zur Auswertung des singulären Integrals $J(N)$ sei für reelles β die Summe $u(\beta)$ wie in Proposition 3.2.3 definiert, also

$$u(\beta) = \sum_{m=1}^{N} e(m\beta) = \sum_{m \leq N} e(m\beta).$$

Es folgt für das singuläre Integral mit Lemma A.1.5, sowie Satz A.1.10 und Bemerkung A.1.11

$$\begin{aligned}
J(N) &= \int_{-\frac{1}{2}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta) d\beta \\
&= \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{m_1 \leq N} e(m_1\beta) \sum_{m_2 \leq N} e(m_2\beta) \sum_{m_3 \leq N} e(m_3\beta) \cdot e(-N\beta) d\beta \\
&= \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{m_1, m_2, m_3 \leq N} e(m_1\beta + m_2\beta + m_3\beta) \cdot e(-N\beta) d\beta \\
&= \int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{m_1, m_2, m_3 \leq N} e\left(\beta(m_1 + m_2 + m_3 - N)\right) d\beta \\
&= \sum_{m_1, m_2, m_3 \leq N} \int_{-\frac{1}{2}}^{\frac{1}{2}} e\left(\beta(m_1 + m_2 + m_3 - N)\right) d\beta.
\end{aligned}$$

Mit der Orthogonalitätsrelation Proposition 3.1.6 für $\omega = \frac{1}{2}$ folgt weiter

$$\sum_{m_1, m_2, m_3 \leq N} \underbrace{\int_{-\frac{1}{2}}^{\frac{1}{2}} e(\beta(m_1 + m_2 + m_3 - N)) d\beta}_{= \begin{cases} 1 & \text{für } m_1 + m_2 + m_3 = N \\ 0 & \text{sonst.} \end{cases}} = \sum_{m_1 + m_2 + m_3 = N} 1.$$

Nachdem jedes m_i $(i = 1, 2, 3)$ alle natürlichen Zahlen bis N durchläuft handelt es sich bei letztem Ausdruck um die Anzahl der Darstellungen von N als Summe von drei natürlichen Zahlen. Mit Satz 2.1.1 folgt nun

$$\sum_{m_1 + m_2 + m_3 = N} 1 = r_{1,3}(N) = \binom{N-1}{2} = \frac{N^2}{2} + O(N).$$

□

Nachdem damit die Betrachtung der singulären Reihe $\mathfrak{S}(N)$ und des singulären Integrals $J(N)$ abgeschlossen ist, soll im nächten Abschnitt das Integral über die Menge der Basisintervalle $\mathfrak{M}$ ausgewertet werden.

3.2.3 Auswertung des Integrals

Das zentrale Ergebnis dieses Abschnitts, die Auswertung des Integrals über die Menge der Basisintervalle $\mathfrak{M}$, kann nun hergeleitet werden. Zu diesem Zweck sei an die vereinbarte abkürzende Schreibweise

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha$$

von Seite 35 erinnert. Im selben Sinn soll auch

$$\int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha)d\alpha$$

als abkürzende Schreibweise verstanden werden.

Satz 3.2.10.[30]
Für die beiden positiven reellen Zahlen B und C mit $C > 2B$, sowie $\varepsilon > 0$ ist das Integral über die Menge der Basisintervalle

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^{(1-\varepsilon)B}}\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right),$$

wobei die impliziten Konstanten nur von B, C und ε abhängig sind.

Beweis.
Der Beweis zur Auswertung des Integrals über die Menge der Basisintervalle $\mathfrak{M}$ lässt sich in zwei Schritte gliedern. Im ersten Schritt soll mit der durch Proposition 3.2.3 gegebenen Näherung zu $F(\alpha)^3$ eine Abschätzung zwischen den Integralen

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha$$

und

$$\int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha)d\alpha$$

hergeleitet werden. Der zweite Schritt befasst sich mit der Betrachtung des letzteren Integrals. Es soll nun mit dem ersten Schritt begonnen werden.
Sei $\alpha = \frac{a}{q} + \beta$ eine reelle Zahl aus dem Basisintervall $\mathfrak{M}(q,a)$ mit den üblichen Eigenschaften $q \in \mathbb{N},\ a \in \mathbb{N}_0,\ 1 \leq q \leq Q = (\log N)^B$ für reelles $B > 0$, $(q,a) = 1$ und passend gewähltem $\beta \in \mathbb{R}$, also einem solchen β für das die Abschätzung $|\beta| \leq \frac{Q}{N}$ gelte. Die Betrachtung der Differenz der beiden oben genannten Integrale und die Auflösung der abkürzenden Schreibweise führt zu

[30] *Nathanson M.B.*, Theorem 8.4, 2010, S.218

$$\begin{aligned}\left|\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha - \int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)d\alpha\right| \\ = \left|\int_{\mathfrak{M}} \left(F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha-\frac{a}{q}\right)^3\right) e(-N\alpha)d\alpha\right| \\ = \left|\sum_{q\leq Q}\sum_{\substack{a=0\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \left(F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha-\frac{a}{q}\right)^3\right) e(-N\alpha)d\alpha\right|.\end{aligned}$$

Da $\alpha = \frac{a}{q} + \beta \Longleftrightarrow \beta = \alpha - \frac{a}{q}$ ist, folgt mit Proposition 3.2.3

$$F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha-\frac{a}{q}\right)^3 = F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\beta\right)^3 \ll \frac{Q^2N^3}{(\log N)^C}$$

mit einer von den positiven reellen Zahlen B und C abhängigen impliziten Konstanten, womit sich die Abschätzung

$$\begin{aligned}\sum_{q\leq Q}\sum_{\substack{a=0\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \left(F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha-\frac{a}{q}\right)^3\right) e(-N\alpha)d\alpha \\ \ll \sum_{q\leq Q}\sum_{\substack{a=0\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \frac{Q^2N^3}{(\log N)^C} d\alpha\end{aligned}$$

ergibt. Zu dieser sei noch bemerkt, dass mit Satz A.1.14 (iii) $|e(-N\alpha)| = 1$ gilt. Zur Abschätzung des Integrals soll Satz A.1.12 verwendet werden. Für ein Basisintervall mit $q \geq 2$ folgt mit Bemerkung 3.1.16

$$\left|\int_{\mathfrak{M}(q,a)} \frac{Q^2N^3}{(\log N)^C} d\alpha\right| = \left|\int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} \frac{Q^2N^3}{(\log N)^C} d\alpha\right| \leq 2\cdot\frac{Q}{N}\cdot\frac{Q^2N^3}{(\log N)^C} = 2\cdot\frac{Q^3N^2}{(\log N)^C},$$

während für die Randintervalle $\mathfrak{M}(1,0)$ und $\mathfrak{M}(1,1)$ unter Berücksichtigung von Definition 3.1.12 und Bemerkung 3.1.16

$$\left|\int_{\mathfrak{M}(1,0)} \frac{Q^2N^3}{(\log N)^C} d\alpha\right| = \left|\int_{0}^{\frac{Q}{N}} \frac{Q^2N^3}{(\log N)^C} d\alpha\right| \leq \frac{Q}{N}\cdot\frac{Q^2N^3}{(\log N)^C} = \frac{Q^3N^2}{(\log N)^C}$$

bzw.

$$\left|\int_{\mathfrak{M}(1,1)} \frac{Q^2N^3}{(\log N)^C} d\alpha\right| = \left|\int_{1-\frac{Q}{N}}^{1} \frac{Q^2N^3}{(\log N)^C} d\alpha\right| \leq \frac{Q}{N}\cdot\frac{Q^2N^3}{(\log N)^C} = \frac{Q^3N^2}{(\log N)^C}$$

folgt. Da

$$\frac{Q^3N^2}{(\log N)^C} < 2\cdot\frac{Q^3N^2}{(\log N)^C}$$

ist, kann für jedes Integral über ein Basisintervall die Abschätzung

$$\int_{\mathfrak{M}(q,a)} \frac{Q^2N^3}{(\log N)^C} d\alpha \ll \frac{Q^3N^2}{(\log N)^C}$$

festgehalten werden. Mit dieser folgt dann

$$\sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \frac{Q^2N^3}{(\log N)^C} d\alpha \ll \sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \frac{Q^3N^2}{(\log N)^C} = \frac{Q^3N^2}{(\log N)^C} \cdot \sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} 1.$$

Als nächstes soll die Summe abgeschätzt werden, wobei $[Q] \leq Q$ zu berücksichtigen ist. Nach Abschätzung durch

$$\sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} 1 = \sum_{q=1}^{[Q]} \sum_{\substack{a=0\\(a,q)=1}}^{q} 1 = \sum_{\substack{a=0\\(a,1)=1}}^{1} 1 + ... + \sum_{\substack{a=0\\(a,[Q])=1}}^{[Q]} 1 \leq \underbrace{Q + ... + Q}_{Q-mal} = Q^2$$

folgt mit $Q = (\log N)^B$ für $B > 0$

$$\frac{Q^3N^2}{(\log N)^C} \cdot \sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} 1 \leq \frac{Q^5N^2}{(\log N)^C} = \frac{(\log N)^{5B}N^2}{(\log N)^C} = \frac{N^2}{(\log N)^{C-5B}}.$$

Insgesamt soll die Abschätzung

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha) d\alpha - \int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha) d\alpha = O\left(\frac{N^2}{(\log N)^{C-5B}}\right)$$

bzw.

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha) d\alpha = \int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha) d\alpha + O\left(\frac{N^2}{(\log N)^{C-5B}}\right)$$

festgehalten werden, wobei die implizite Konstante von den positiven reellen Zahlen B und C abhängig ist. Der erste Schritt des Beweises ist damit abgeschlossen.

Im zweiten Schritt soll nun wie angekündigt das Integral

$$\int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha) d\alpha$$

genauer betrachtet werden. Für dieses folgt nach Auflösung der abkürzenden Schreibweise

$$\begin{aligned}\int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha) d\alpha &= \sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha) d\alpha \\ &= \sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3} \int_{\mathfrak{M}(q,a)} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha) d\alpha.\end{aligned}$$

Betrachtet man den Integranden, dann stellt man fest, dass dieser 1-periodisch ist. Es ist also

$$\begin{aligned} u\left(\alpha-\frac{a}{q}+1\right)^3 e(-N\alpha+1) &= \left(\sum_{m=1}^{N} e^{2\pi i\left(\alpha-\frac{a}{q}+1\right)}\right)^3 e^{2\pi i(-N\alpha+1)} \\ &= \left(\sum_{m=1}^{N} e^{2\pi i\left(\alpha-\frac{a}{q}\right)} \underbrace{e^{2\pi i}}_{=1}\right)^3 e^{2\pi i(-N\alpha)} \underbrace{e^{2\pi i}}_{=1} \\ &= u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha). \end{aligned}$$

Für den Wert des Integrals macht es also keinen Unterschied, ob über $\left[0,\frac{Q}{N}\right]\cup\left[1-\frac{Q}{N},1\right]$ oder über $\left[1-\frac{Q}{N},1+\frac{Q}{N}\right]$ integriert wird, bildlich

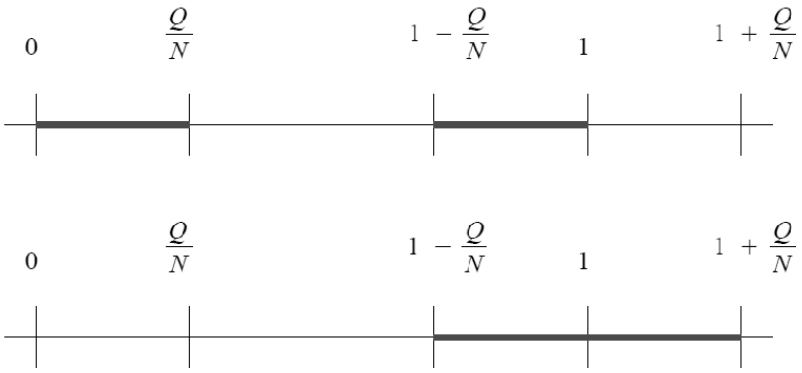


Abbildung 3.6: Intervallvergleich

Berücksichtigt man dies, dann kann

$$\begin{aligned} &\sum_{q\le Q}\sum_{\substack{a=0\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3}\int_{\mathfrak{M}(q,a)} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)d\alpha \\ &\qquad = \sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3}\int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)d\alpha \\ &\qquad = \sum_{q\le Q}\frac{\mu(q)}{\varphi(q)^3}\sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha-\frac{a}{q}\right)^3 e(-N\alpha)d\alpha \end{aligned}$$

geschrieben werden. Da $\alpha = \frac{a}{q} + \beta$ ist, folgt

$$\begin{aligned} e(-N\alpha) = e^{2\pi i(-N\alpha)} &= e^{2\pi i\left(-N\left(\frac{a}{q}+\beta\right)\right)} = e^{2\pi i\left(-\frac{Na}{q}\right)} e^{2\pi i(-N\beta)} \\ &= e\left(-\frac{Na}{q}\right) e\left(-N\beta\right) \end{aligned}$$

und weiter

$$\begin{aligned} &\sum_{q\leq Q} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha) d\alpha \\ &\qquad = \sum_{q\leq Q} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha - \frac{a}{q}\right)^3 e\left(-\frac{Na}{q}\right) e\left(-N\beta\right) d\alpha \\ &\qquad = \sum_{q\leq Q} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(-\frac{Na}{q}\right) \int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha - \frac{a}{q}\right)^3 e\left(-N\beta\right) d\alpha \\ &\qquad = \sum_{q\leq Q} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(-\frac{Na}{q}\right) \int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha - \frac{a}{q}\right)^3 e\left(-N\left(\alpha - \frac{a}{q}\right)\right) d\alpha. \end{aligned}$$

Auf das Integral soll nun die Substitutionsregel Satz A.1.18 angewandt werden. Da die Voraussetzungen

$$f : \left[\frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right] \to \mathbb{C},\ \alpha \to u\left(\alpha - \frac{a}{q}\right)^3 e\left(-N\left(\alpha - \frac{a}{q}\right)\right)$$

ist stückweise stetig,

$$g : \left[-\frac{Q}{N}, \frac{Q}{N}\right] \to \left[\frac{a}{q} - \frac{Q}{N}, \frac{a}{q} + \frac{Q}{N}\right],\ \beta \to \frac{a}{q} + \beta$$

ist reell, monoton, stetig und stückweise stetig differenzierbar gelten, folgt

$$\begin{aligned} &\int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha - \frac{a}{q}\right)^3 e\left(-N\left(\alpha - \frac{a}{q}\right)\right) d\alpha \\ &\qquad = \int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\frac{a}{q} + \beta - \frac{a}{q}\right)^3 e\left(-N\left(\frac{a}{q} + \beta - \frac{a}{q}\right)\right) \cdot 1\ d\beta \\ &\qquad = \int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\beta\right)^3 e\left(-N\beta\right) d\beta. \end{aligned}$$

Damit folgt

$$\sum_{q\leq Q}\frac{\mu(q)}{\varphi(q)^3}\sum_{\substack{a=1\\(a,q)=1}}^{q} e\left(-\frac{Na}{q}\right)\int_{\frac{a}{q}-\frac{Q}{N}}^{\frac{a}{q}+\frac{Q}{N}} u\left(\alpha-\frac{a}{q}\right)^3 e\left(-N\left(\alpha-\frac{a}{q}\right)\right)d\alpha$$

$$=\sum_{q\leq Q}\frac{\mu(q)}{\varphi(q)^3}\sum_{\substack{a=1\\(a,q)=1}}^{q} e\left(-\frac{Na}{q}\right)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\beta\right)^3 e\left(-N\beta\right)d\beta.$$

Mit der Definition der Ramanujan-Summe, Definition A.3.21, kann das letzte Ergebnis umgeformt werden zu

$$\sum_{q\leq Q}\frac{\mu(q)}{\varphi(q)^3}\sum_{\substack{a=1\\(a,q)=1}}^{q} e\left(-\frac{Na}{q}\right)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\beta\right)^3 e\left(-N\beta\right)d\beta$$

$$=\sum_{q\leq Q}\frac{\mu(q)}{\varphi(q)^3}\cdot c_q(-N)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\beta\right)^3 e\left(-N\beta\right)d\beta.$$

Nachdem mit Satz A.3.2 und Satz A.3.25 für die Ramanujan-Summe

$$c_q(-N)=\frac{\mu\left(\frac{q}{(q,-N)}\right)}{\varphi\left(\frac{q}{(q,-N)}\right)}\cdot\varphi(q)=\frac{\mu\left(\frac{q}{(|q|,|-N|)}\right)}{\varphi\left(\frac{q}{(|q|,|-N|)}\right)}\cdot\varphi(q)=\frac{\mu\left(\frac{q}{(q,N)}\right)}{\varphi\left(\frac{q}{(q,N)}\right)}\cdot\varphi(q)=c_q(N)$$

gilt, lässt sich die beschränkte singuläre Reihe $\mathfrak{S}(N,Q)$ aus Satz 3.2.5 einsetzen

$$\sum_{q\leq Q}\frac{\mu(q)}{\varphi(q)^3}\cdot c_q(-N)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\beta\right)^3 e\left(-N\beta\right)d\beta$$

$$=\sum_{q\leq Q}\frac{\mu(q)}{\varphi(q)^3}\cdot c_q(N)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\beta\right)^3 e\left(-N\beta\right)d\beta$$

$$=\mathfrak{S}(N,Q)\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u\left(\beta\right)^3 e\left(-N\beta\right)d\beta.$$

Es ist nun noch das Integral auszuwerten. Für die obere Grenze $\frac{Q}{N}=\frac{(\log N)^B}{N}$ kann aufgrund des langsameren Wachstums des Logarithmus nach Beispiel A.2.19 ein genügend großes N gefunden werden, ab dem bei festem $B>0$ die Ungleichung $\frac{Q}{N}<\frac{1}{2}$ gilt. Dann gilt auch $-\frac{1}{2}<-\frac{Q}{N}$ und es ergibt sich folgende Darstellung

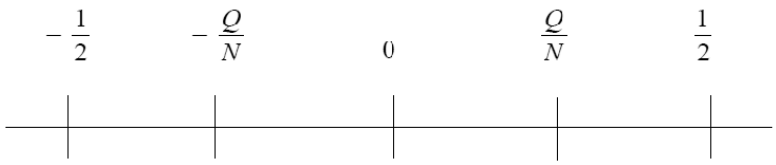


Abbildung 3.7: Intervall um Null

Abkürzend wird die Zerlegung

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} = \int_{-\frac{1}{2}}^{-\frac{Q}{N}} + \int_{-\frac{Q}{N}}^{\frac{Q}{N}} + \int_{\frac{Q}{N}}^{\frac{1}{2}} \implies \int_{-\frac{Q}{N}}^{\frac{Q}{N}} = \int_{-\frac{1}{2}}^{\frac{1}{2}} - \int_{-\frac{1}{2}}^{-\frac{Q}{N}} - \int_{\frac{Q}{N}}^{\frac{1}{2}}$$

durchgeführt. Nacheinander sollen nun die Integrale auf der rechten Seite ausgewertet bzw. abgeschätzt werden. Das erste Integral

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta)\, d\beta$$

ist offensichtlich das singuläre Integral $J(N)$, welches in Proposition 3.2.9 bereits ausgewertet wurde. Es gilt nach dieser

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta)\, d\beta = J(N) = \frac{N^2}{2} + O(N).$$

Für das zweite Integral folgt mit Satz A.1.17 und Satz A.1.14 (iii)

$$\begin{aligned}
\left| -\int_{-\frac{1}{2}}^{-\frac{Q}{N}} u(\beta)^3 e(-N\beta)\, d\beta \right| &= \left| \int_{-\frac{1}{2}}^{-\frac{Q}{N}} u(\beta)^3 e(-N\beta)\, d\beta \right| \\
&\leq \int_{-\frac{1}{2}}^{-\frac{Q}{N}} \left| u(\beta)^3 e(-N\beta) \right| d\beta \\
&= \int_{-\frac{1}{2}}^{-\frac{Q}{N}} \left| u(\beta)^3 \right| \cdot |e(-N\beta)|\, d\beta \\
&= \int_{-\frac{1}{2}}^{-\frac{Q}{N}} |u(\beta)|^3\, d\beta.
\end{aligned}$$

Um zur weiteren Abschätzung Satz A.3.40 verwenden zu können, sei daran erinnert, dass $\| \beta \|$ den Abstand der reellen Zahl β zur nächsten ganzen Zahl bezeichnet, wie auf Seite 106

eingeführt. Für β aus dem Integrationsintervall, also einem β mit $|\beta| \leq \frac{1}{2} \Longleftrightarrow -\frac{1}{2} \leq \beta \leq \frac{1}{2}$, gilt $\parallel \beta \parallel = |\beta|$. Mit Satz A.3.40 folgt die Abschätzung

$$u(\beta) = \sum_{m=1}^{N} e(m\beta) \ll \min\left(N - 0, \parallel \beta \parallel^{-1}\right) = \min\left(N, |\beta|^{-1}\right) = |\beta|^{-1} = \frac{1}{|\beta|},$$

mit welcher dann

$$\int_{-\frac{1}{2}}^{-\frac{Q}{N}} |u(\beta)|^3 \, d\beta \ll \int_{-\frac{1}{2}}^{-\frac{Q}{N}} \frac{1}{|\beta|^3} d\beta$$

folgt. Weiter ist dann

$$\begin{aligned}
\int_{-\frac{1}{2}}^{-\frac{Q}{N}} \frac{1}{|\beta|^3} d\beta &= \int_{-\frac{1}{2}}^{-\frac{Q}{N}} -\frac{1}{\beta^3} d\beta = -\left[-\frac{1}{2\beta^2}\right]_{-\frac{1}{2}}^{-\frac{Q}{N}} \\
&= -\left(-\frac{1}{2\left(-\frac{Q}{N}\right)^2} - \left(-\frac{1}{2\left(-\frac{1}{2}\right)^2}\right)\right) = -\left(-\frac{1}{2 \cdot \frac{Q^2}{N^2}} + 2\right) \\
&= \frac{1}{2} \cdot \frac{N^2}{Q^2} - 2 < \frac{1}{2} \cdot \frac{N^2}{Q^2},
\end{aligned}$$

womit insgesamt für das Integral die Abschätzung

$$\int_{-\frac{1}{2}}^{-\frac{Q}{N}} u(\beta)^3 \, e(-N\beta) \, d\beta \ll \frac{N^2}{Q^2}$$

festgehalten werden kann. Unter Anwendung derselben Hilfsmittel wie beim zweiten Integral folgt für das dritte Integral die Abschätzung

$$\begin{aligned}
\left| -\int_{\frac{Q}{N}}^{\frac{1}{2}} u(\beta)^3 \, e(-N\beta) \, d\beta \right| &= \left| \int_{\frac{Q}{N}}^{\frac{1}{2}} u(\beta)^3 \, e(-N\beta) \, d\beta \right| \\
&\leq \int_{\frac{Q}{N}}^{\frac{1}{2}} \left| u(\beta)^3 \, e(-N\beta) \right| d\beta \\
&= \int_{\frac{Q}{N}}^{\frac{1}{2}} \left| u(\beta)^3 \right| \cdot |e(-N\beta)| \, d\beta = \int_{\frac{Q}{N}}^{\frac{1}{2}} |u(\beta)|^3 \, d\beta \\
&\ll \int_{\frac{Q}{N}}^{\frac{1}{2}} \frac{1}{|\beta|^3} d\beta = \int_{\frac{Q}{N}}^{\frac{1}{2}} \frac{1}{\beta^3} d\beta = \left[-\frac{1}{2\beta^2}\right]_{\frac{Q}{N}}^{\frac{1}{2}} \\
&= -\frac{1}{2\left(\frac{1}{2}\right)^2} - \left(-\frac{1}{2\left(\frac{Q}{N}\right)^2}\right) = -2 + \frac{1}{2} \cdot \frac{N^2}{Q^2} \\
&< \frac{1}{2} \cdot \frac{N^2}{Q^2}.
\end{aligned}$$

Für das dritte Integral gilt also die Abschätzung

$$\int_{\frac{Q}{N}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta)\, d\beta \ll \frac{N^2}{Q^2}.$$

Die Abschätzungen der drei Integrale sollen nun zusammengefasst werden. Es folgt

$$\begin{aligned}
&\int_{-\frac{Q}{N}}^{\frac{Q}{N}} u(\beta)^3 e(-N\beta)\, d\beta \\
&\quad = \int_{-\frac{1}{2}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta)\, d\beta - \int_{-\frac{1}{2}}^{-\frac{Q}{N}} u(\beta)^3 e(-N\beta)\, d\beta - \int_{\frac{Q}{N}}^{\frac{1}{2}} u(\beta)^3 e(-N\beta)\, d\beta \\
&\quad = \frac{N^2}{2} + O(N) + O\left(\frac{N^2}{Q^2}\right) + O\left(\frac{N^2}{Q^2}\right) \\
&\quad = \frac{N^2}{2} + O\left(\max\left\{N, \frac{N^2}{Q^2}\right\}\right).
\end{aligned}$$

Da nach Beispiel A.2.19 für genügend großes N bei festem $B > 0$

$$\frac{N^2}{Q^2} > N \Longleftrightarrow N > Q^2 = (\log N)^{2B}$$

gilt, folgt

$$\frac{N^2}{2} + O\left(\max\left\{N, \frac{N^2}{Q^2}\right\}\right) = \frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right).$$

Damit zum Produkt der beschränkten singulären Reihe $\mathfrak{S}(N,Q)$ und dem Integral über $\left[-\frac{Q}{N}, \frac{Q}{N}\right]$ zurückkehrend, erhält man

$$\mathfrak{S}(N,Q) \int_{-\frac{Q}{N}}^{\frac{Q}{N}} u(\beta)^3 e(-N\beta)\, d\beta = \mathfrak{S}(N,Q)\left(\frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right)\right).$$

Mit der Abschätzung

$$\mathfrak{S}(N,Q) = \mathfrak{S}(N) + O\left(\frac{1}{Q^{1-\varepsilon}}\right)$$

aus Satz 3.2.5 folgt weiter

$$\begin{aligned}
\mathfrak{S}(N,Q)\left(\frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right)\right) &= \left(\mathfrak{S}(N) + O\left(\frac{1}{Q^{1-\varepsilon}}\right)\right)\left(\frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right)\right) \\
&= \mathfrak{S}(N)\frac{N^2}{2} + \mathfrak{S}(N) O\left(\frac{N^2}{Q^2}\right) + \frac{N^2}{2} O\left(\frac{1}{Q^{1-\varepsilon}}\right) + O\left(\frac{1}{Q^{1-\varepsilon}}\right) O\left(\frac{N^2}{Q^2}\right).
\end{aligned}$$

Da die singuläre Reihe $\mathfrak{S}(N)$ nach Korollar 3.2.6 durch $\frac{2457}{\pi^6}$ beschränkt ist, also die Abschätzung

$$\mathfrak{S}(N) = O\left(\frac{2457}{\pi^6}\right) = O(1)$$

gilt, folgt

$$\mathfrak{S}(N)O\left(\frac{N^2}{Q^2}\right) = O(1)O\left(\frac{N^2}{Q^2}\right) = O\left(\frac{N^2}{Q^2}\right).$$

Zudem kann

$$\frac{N^2}{2}O\left(\frac{1}{Q^{1-\varepsilon}}\right) = O\left(\frac{1}{2}\cdot\frac{N^2}{Q^{1-\varepsilon}}\right) = O\left(\frac{N^2}{Q^{1-\varepsilon}}\right)$$

und

$$O\left(\frac{1}{Q^{1-\varepsilon}}\right)O\left(\frac{N^2}{Q^2}\right) = O\left(\frac{N^2}{Q^{2(1-\varepsilon)}}\right)$$

zusammengefasst werden, womit

$$\begin{aligned}
&\mathfrak{S}(N)\frac{N^2}{2} + \mathfrak{S}(N)O\left(\frac{N^2}{Q^2}\right) + \frac{N^2}{2}O\left(\frac{1}{Q^{1-\varepsilon}}\right) + O\left(\frac{1}{Q^{1-\varepsilon}}\right)O\left(\frac{N^2}{Q^2}\right)\\
&\quad= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{Q^2}\right) + O\left(\frac{N^2}{Q^{1-\varepsilon}}\right) + O\left(\frac{N^2}{Q^{2(1-\varepsilon)}}\right)\\
&\quad= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\max\left\{\frac{N^2}{Q^2}, \frac{N^2}{Q^{1-\varepsilon}}, \frac{N^2}{Q^{2(1-\varepsilon)}}\right\}\right)
\end{aligned}$$

folgt. Mit

$$\min\{2, 1-\varepsilon, 2(1-\varepsilon)\} = 1-\varepsilon$$

für $\varepsilon > 0$ bleibt

$$\mathfrak{S}(N)\frac{N^2}{2} + O\left(\max\left\{\frac{N^2}{Q^2}, \frac{N^2}{Q^{1-\varepsilon}}, \frac{N^2}{Q^{2(1-\varepsilon)}}\right\}\right) = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{Q^{1-\varepsilon}}\right).$$

Die implizite Konstante ist nun von $\varepsilon > 0$ abhängig, da Satz 3.2.5 verwendet wurde. Zusammenfassend ist also

$$\begin{aligned}
\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha &= \int_{\mathfrak{M}} \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha)d\alpha + O\left(\frac{N^2}{(\log N)^{C-5B}}\right)\\
&= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{Q^{1-\varepsilon}}\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right)\\
&= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^{(1-\varepsilon)B}}\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right),
\end{aligned}$$

wobei die impliziten Konstanten von den positiven reellen Zahlen B und C, sowie $\varepsilon > 0$ abhängig sind. □

Damit ist die Betrachtung des Integrals über die Menge der Basisintervalle $\mathfrak{M}$ abgeschlossen und es kann sich im nächsten Abschnitt dem Integral über die Menge der Ergänzungsintervalle $\mathfrak{m}$ zugewandt werden.

3.3 Das Integral über die Ergänzungsintervalle

Zur Abschätzung dieses Integrals sind wieder einige Vorbetrachtungen notwendig. Diese sollen im ersten Abschnitt dieses Unterkapitels bereitgestellt werden, bevor sich im zweiten Abschnitt der Abschätzung des Integrals zugewandt wird.

3.3.1 Exponentialsummen mit Primzahlen

Als erstes Hilfsmittel wird zunächst wird Vaughans Identität benötigt.

Proposition 3.3.1 (Vauhans Identität)**.**[31]
Für $u \geq 1$ sei

$$M_u(k) := \sum_{\substack{d|k \\ d \leq u}} \mu(d).$$

Sei zudem $\Phi(k,l)$ eine arithmetische Funktion von zwei Variablen, dann gilt

$$\sum_{u<l\leq N} \Phi(1,l) + \sum_{u<k\leq N} \sum_{u<l\leq \frac{N}{k}} M_u(k)\Phi(k,l) = \sum_{d\leq u} \sum_{u<l\leq \frac{N}{d}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Phi(dm,l).$$

Unter Verwendung von Vaughans Identität mit $u = N^{\frac{2}{5}}$ und $\Phi(k,l) = \Lambda(l)e(\alpha kl)$ kann $F(\alpha)$ aufgespalten werden.

Proposition 3.3.2.[32]
Für jedes reelle α ist

$$F(\alpha) = S_1 - S_2 - S_3 + O\left(N^{\frac{1}{2}}\right),$$

wobei

$$S_1 = \sum_{d\leq N^{\frac{2}{5}}} \sum_{l\leq \frac{N}{d}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm),$$

$$S_2 = \sum_{d\leq N^{\frac{2}{5}}} \sum_{l\leq N^{\frac{2}{5}}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm)$$

und

$$S_3 = \sum_{k>N^{\frac{2}{5}}} \sum_{N^{\frac{2}{5}}<l\leq \frac{N}{k}} M_{N^{\frac{2}{5}}}(k)\Lambda(l)e(\alpha kl)$$

gilt.

Sie Summen S_1, S_2 und S_3 können nun getrennt voneinander abgeschätzt werden.

[31] *Nathanson M.B.*, Lemma 8.4, 2010, S.220
[32] *Nathanson M.B.*, Lemma 8.5, 2010, S.221

Proposition 3.3.3.[33]

Sei $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, *wobei* $1 \leq q \leq N$ *und* $(a,q) = 1$ *gelte. Dann ist*

$$|S_1| \ll \left(\frac{N}{q} + N^{\frac{2}{5}} + q\right)(\log N)^2 .$$

Proposition 3.3.4.[34]

Sei $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, *wobei* $1 \leq q \leq N$ *und* $(a,q) = 1$ *gelte. Dann ist*

$$|S_2| \ll \left(\frac{N}{q} + N^{\frac{4}{5}} + q\right)(\log N)^2 .$$

Proposition 3.3.5.[35]

Sei $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, *wobei* $1 \leq q \leq N$ *und* $(a,q) = 1$ *gelte. Dann ist*

$$|S_3| \ll \left(\frac{N}{q^{\frac{1}{2}}} + N^{\frac{4}{5}} + N^{\frac{1}{2}} q^{\frac{1}{2}}\right)(\log N)^4 .$$

Damit ist fast alles bereitgestellt um die Abschätzung des Integrals durchzuführen. Fasst man die Abschätzungen über S_1, S_2 und S_3 zusammen, erhält man die Abschätzung von Vinogradov.

Satz 3.3.6 (Vinogradov)**.**[36]

Sei $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, *wobei a und q ganze Zahlen seien, für die* $1 \leq q \leq N$ *und* $(a,q) = 1$ *gelte. Dann ist*

$$F(\alpha) \ll \left(\frac{N}{q^{\frac{1}{2}}} + N^{\frac{4}{5}} + N^{\frac{1}{2}} q^{\frac{1}{2}}\right)(\log N)^4 .$$

Mit der Abschätzung von Vinogradov soll im nächsten Abschnitt zum Integral über die Menge der Ergänzungsintervalle $\mathfrak{m}$ zurückgekehrt werden.

[33] *Nathanson M.B.*, Lemma 8.6, 2010, S.222
[34] *Nathanson M.B.*, Lemma 8.7, 2010, S.224
[35] *Nathanson M.B.*, Lemma 8.8, 2010, S.224
[36] *Nathanson M.B.*, Theorem 8.5, 2010, S.220

3.3.2 Abschätzung des Integrals

Nachdem alle notwendigen Hilfsmittel zusammengetragen sind, soll das Integral über die Menge der Ergänzungsintervalle abgeschätzt werden.

Satz 3.3.7.[37]
Für jedes $B > 0$ gilt

$$\int_{\mathfrak{m}} F(\alpha)^3 e(-N\alpha)d\alpha \ll \frac{N^2}{(\log N)^{\frac{B}{2}-5}},$$

wobei die implizite Konstante nur von B abhängig ist.

3.4 Beweisschluss zur asymptotischen Formel

Aus der Auswertung des Integrals über die Menge der Basisintervalle $\mathfrak{M}$ und der Abschätzung des Integrals über die Menge der Ergänzungsintervalle $\mathfrak{m}$ kann nun Vinogradovs Formel für $R(N)$ zusammengesetzt werden.

Satz 3.4.1 (Vinogradov)**.**[38]
Sei $\mathfrak{S}(N)$ die singuläre Reihe für das ternäre Goldbachproblem. Für jede genügend große ungerade natürliche Zahl N und für jedes $A > 0$ gilt

$$R(N) = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right),$$

wobei die implizite Konstante nur von A abhängig ist.

Beweis.
Die Ergebnisse zur Integralaufspaltung von Seite 35, Satz 3.2.10 und Satz 3.3.7 sollen nun zusammengetragen werden. Es folgt mit diesen

$$\begin{aligned} R(N) &= \int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha + \int_{\mathfrak{m}} F(\alpha)^3 e(-N\alpha)d\alpha \\ &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^{(1-\varepsilon)B}}\right) + O\left(\frac{N^2}{(\log N)^{C-5B}}\right) + O\left(\frac{N^2}{(\log N)^{\frac{B}{2}-5}}\right) \\ &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\max\left\{\frac{N^2}{(\log N)^{(1-\varepsilon)B}}, \frac{N^2}{(\log N)^{C-5B}}, \frac{N^2}{(\log N)^{\frac{B}{2}-5}}\right\}\right). \end{aligned}$$

Für reelles $A > 0$ sei $B := 2A + 10,\ C := A + 5B$ und speziell $\varepsilon := \frac{1}{2}$, dann ist

$$\begin{aligned} \min\left\{(1-\varepsilon)B, C-5B, \frac{B}{2}-5\right\} &= \min\left\{\frac{1}{2}(2A+10), A+5B-5B, \frac{1}{2}(2A+10)-5\right\} \\ &= \min\{A+5, A, A\} = A. \end{aligned}$$

[37] *Nathanson M.B.*, Theorem 8.6, 2010, S.227
[38] *Nathanson M.B.*, Theorem 8.7, 2010, S.228

Damit folgt für den $O(\cdot)$-Term

$$O\left(\max\left\{\frac{N^2}{(\log N)^{(1-\varepsilon)B}}, \frac{N^2}{(\log N)^{C-5B}}, \frac{N^2}{(\log N)^{\frac{B}{2}-5}}\right\}\right) = O\left(\frac{N^2}{(\log N)^A}\right),$$

womit weiter

$$\begin{aligned}\mathfrak{S}(N)\frac{N^2}{2} + O\left(\max\left\{\frac{N^2}{(\log N)^{(1-\varepsilon)B}}, \frac{N^2}{(\log N)^{C-5B}}, \frac{N^2}{(\log N)^{\frac{B}{2}-5}}\right\}\right)\\ = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right)\end{aligned}$$

folgt. Die implizite Konstante ist dabei nur noch von der positiven reellen Zahl A abhängig. □

Aus der asymptotischen Formel für $R(N)$, der gewichteten Zählfunktion der Anzahl der Darstellungen von N als Summe dreier Primzahlen, kann nun Vinogradovs asymptotische Formel für $r(N)$ abgeleitet werden.

Satz 3.4.2 (Vinogradov).[39]
Es existiert eine arithmetische Funktion $\mathfrak{S}(N)$ und positive Konstanten c_1, c_2 derart, dass

$$\frac{6}{\pi^2} \leq c_1 < \mathfrak{S}(N) < c_2 \leq \frac{2457}{\pi^6}$$

für alle genügend großen ungeraden natürlichen Zahlen N und

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\left(1 + O\left(\frac{\log\log N}{\log N}\right)\right)$$

gilt.

Beweis.
Der Beweis des Satzes lässt sich in drei Teile zerlegen: Im ersten und zweiten Teil wird eine obere bzw. untere Schranke für die gewichtete Zählfunktion $R(N)$ hergeleitet, wobei bei diesen Abschätzungen die Zählfunktion $r(N)$ eingebracht werden kann. Im dritten Teil des Beweises werden die gewonnenen Abschätzungen zusammengefasst und durch Umformung lässt sich anschließend der asymptotische Ausdruck für $r(N)$ herleiten.
Die obere Schranke für $R(N)$ ergibt sich wie folgt: Nach Definition 3.1.3 ist

$$R(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3.$$

Da für jeden Faktor die Abschätzung $\log p_i \leq \log N$ $(i = 1, 2, 3)$ gilt, folgt

$$R(N) \leq \sum_{p_1+p_2+p_3=N} (\log N)^3 = (\log N)^3 \sum_{p_1+p_2+p_3=N} 1.$$

[39] *Nathanson M.B.*, Theorem 8.1, 2010, S.212 und
Vinogradov, I.M., 2004, S.175

Ein Blick auf Definition 3.1.1 lässt die Zählfunktion $r(N)$ erkennen, also

$$(\log N)^3 \sum_{p_1+p_2+p_3=N} 1 = (\log N)^3 \, r(N),$$

womit insgesamt die Abschätzung

$$R(N) \leq (\log N)^3 \, r(N)$$

festgehalten werden kann. Zur Herleitung der unteren Schranke sind zunächst einige Vorbetrachtungen notwendig.
Für $0 < \delta < \frac{1}{2}$ sei $r_\delta(N)$ die Anzahl der Darstellungen von N als Summe dreier Primzahlen, also $N = p_1 + p_2 + p_3$, wobei $p_i \leq N^{1-\delta}$ für mindestens ein $i = 1, 2, 3$ gelte. Kurz

$$r_\delta(N) := \sum_{\substack{p_1+p_2+p_3=N \\ p_i \leq N^{1-\delta} \text{ für mindestens ein } i}} 1 = \sum_{\substack{p_1+p_2+p_3=N \\ p_1 \leq N^{1-\delta} \,\vee\, p_2 \leq N^{1-\delta} \,\vee\, p_3 \leq N^{1-\delta}}} 1.$$

Dann lässt sich $r_\delta(N)$ folgendermaßen abschätzen:

$$r_\delta(N) = \sum_{\substack{p_1+p_2+p_3=N \\ p_1 \leq N^{1-\delta} \,\vee\, p_2 \leq N^{1-\delta} \,\vee\, p_3 \leq N^{1-\delta}}} 1 \leq 3 \cdot \sum_{\substack{p_1+p_2+p_3=N \\ p_1 \leq N^{1-\delta}}} 1 \ll \sum_{\substack{p_1+p_2+p_3=N \\ p_1 \leq N^{1-\delta}}} 1.$$

Dies lässt sich umschreiben zu

$$\sum_{\substack{p_1+p_2+p_3=N \\ p_1 \leq N^{1-\delta}}} 1 = \sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_1+p_2+p_3=N} 1 \right).$$

Da für die innere Summe p_1 fest gewählt ist, folgt

$$\sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_1+p_2+p_3=N} 1 \right) = \sum_{p_1 \leq N^{1-\delta}} \left(\sum_{\substack{p_2,p_3: \\ p_2+p_3=N-p_1}} 1 \right).$$

Durch Abschwächung der Summationsbedingung der inneren Summe
($p_2 + p_3 = N - p_1 \Rightarrow p_2 < N$) vergrößert sich diese:

$$\sum_{p_1 \leq N^{1-\delta}} \left(\sum_{\substack{p_2,p_3: \\ p_2+p_3=N-p_1}} 1 \right) \leq \sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_2<N} 1 \right).$$

Umsortierung und die Definition der π-Funktion, Definition A.3.26, führen zu

$$\sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_2<N} 1 \right) = \left(\sum_{p_1 \leq N^{1-\delta}} 1 \right) \cdot \left(\sum_{p_2<N} 1 \right) = \pi\left(N^{1-\delta}\right) \pi\left(N\right).$$

Zur weiteren Abschätzung soll die Ungleichung von Chebyshev, Satz A.3.28, verwendet werden. Nach dieser gilt für eine Konstante $c > 0$

$$\pi(x)\log x \leq cx \implies \pi(x) \leq c \cdot \frac{x}{\log x} \implies \pi(x) \ll \frac{x}{\log x},$$

womit weiter

$$\pi\left(N^{1-\delta}\right)\pi\left(N\right) \ll \frac{N^{1-\delta}}{\log\left(N^{1-\delta}\right)} \cdot \frac{N}{\log N} = \frac{N^{2-\delta}}{(1-\delta)\log N \log N} = \frac{N^{2-\delta}}{(1-\delta)\left(\log N\right)^2}$$

abgeschätzt werden kann. Für $0 < \delta < \frac{1}{2}$ folgt $\frac{1}{2} < 1 - \delta < 1$, also $1 < \frac{1}{1-\delta} < 2$. Damit ergibt sich die Abschätzung

$$\frac{N^{2-\delta}}{(1-\delta)\left(\log N\right)^2} < 2 \cdot \frac{N^{2-\delta}}{\left(\log N\right)^2} \ll \frac{N^{2-\delta}}{\left(\log N\right)^2}.$$

Aus der Vorbetrachtung kann also insgesamt die Abschätzung

$$r_\delta(N) \ll \frac{N^{2-\delta}}{\left(\log N\right)^2}$$

festgehalten werden. Mit dieser soll nun die untere Schranke für $R(N)$ hergeleitet werden. Zunächst folgt Aufgrund der Summationsbedingung

$$R(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 \geq \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} \log p_1 \log p_2 \log p_3.$$

Da für jeden Faktor die Abschätzung $\log p_i > \log\left(N^{1-\delta}\right)\ (i = 1,2,3)$ gilt, folgt weiter

$$\begin{aligned}
\sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} \log p_1 \log p_2 \log p_3 &> \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} \left(\log\left(N^{1-\delta}\right)\right)^3 \\
&= \left(\log\left(N^{1-\delta}\right)\right)^3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} 1 \\
&= \left((1-\delta)\log N\right)^3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} 1 \\
&= (1-\delta)^3\left(\log N\right)^3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} 1.
\end{aligned}$$

Die Betrachtung der Differenz[40]

$$\begin{aligned} r(N) - r_\delta(N) &= \sum_{p_1+p_2+p_3=N} 1 - \sum_{\substack{p_1+p_2+p_3=N \\ p_1\leq N^{1-\delta} \ \vee \ p_2\leq N^{1-\delta} \ \vee \ p_3\leq N^{1-\delta}}} 1 \\ &= \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} 1 \end{aligned}$$

führt zu

$$(1-\delta)^3 (\log N)^3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} 1 = (1-\delta)^3 (\log N)^3 (r(N) - r_\delta(N)) .$$

An dieser Stelle soll die gewonnene Abschätzung

$$r_\delta(N) \ll \frac{N^{2-\delta}}{(\log N)^2}$$

verwendet werden. Mit dieser folgt

$$(1-\delta)^3 (\log N)^3 (r(N) - r_\delta(N)) \gg (1-\delta)^3 (\log N)^3 \left(r(N) - \frac{N^{2-\delta}}{(\log N)^2} \right) .$$

Die damit hergeleitete untere Abschätzung

$$(1-\delta)^3 (\log N)^3 \left(r(N) - \frac{N^{2-\delta}}{(\log N)^2} \right) \ll R(N)$$

ist nun noch in zwei Schritten für deren weitere Verwendung umzuformen. Im ersten Schritt soll Lemma A.2.7 (iii) entsprechend für das Vinogradov-Symbol verwendet werden, womit

$$\begin{aligned} (\log N)^3 \left(r(N) - \frac{N^{2-\delta}}{(\log N)^2} \right) &= (\log N)^3 r(N) - (\log N) N^{2-\delta} \\ &\ll \frac{1}{(1-\delta)^3} R(N) \end{aligned}$$

folgt. Im zweiten Schritt wird Lemma A.2.7 (v) entsprechend für das Vinogradov-Symbol angewandt, wobei die Definitionen

$$f_1 := (\log N)^3 r(N) - (\log N) N^{2-\delta} \ll \frac{1}{(1-\delta)^3} R(N) =: g_1$$

und

$$f_2 := (\log N) N^{2-\delta} \ll (\log N) N^{2-\delta} =: g_2$$

[40] Da mindestens eine der Aussagen der Summationsbedingung $A : p_1 \leq N^{1-\delta}, B : p_2 \leq N^{1-\delta}$, $C : p_3 \leq N^{1-\delta}$ richtig ist, ist dies gleichbedeutend mit $A \vee B \vee C$. Dessen Gegenteil ist $\overline{A \vee B \vee C} = \overline{A} \wedge \overline{B} \wedge \overline{C}$. Als Bedingung an die drei Primzahlen: $p_1, p_2, p_3 > N^{1-\delta}$.

getroffen seien. Dann folgt

$$(\log N)^3 r(N) - (\log N) N^{2-\delta} + (\log N) N^{2-\delta} = (\log N)^3 r(N) \ll \frac{1}{(1-\delta)^3} R(N) + (\log N) N^{2-\delta}.$$

Die umgeformte Abschätzung

$$(\log N)^3 r(N) \ll \frac{1}{(1-\delta)^3} R(N) + (\log N) N^{2-\delta}$$

soll bei der Zusammenführung mit der oberen Abschätzung noch von δ befreit werden. Nachfolgend wird dies vorbereitet:
Für $0 < \delta < \frac{1}{2}$ wurde bereits $\frac{1}{2} < 1 - \delta < 1$ bzw. $1 < \frac{1}{1-\delta} < 2$ festegestellt. Damit folgt

$$1 < \frac{1}{(1-\delta)^3} < 8$$

und weiter

$$\begin{aligned}
0 &< \frac{1}{(1-\delta)^3} - 1 = \frac{1}{(1-\delta)^3} - \frac{(1-\delta)^3}{(1-\delta)^3} = \frac{1-(1-\delta)^3}{(1-\delta)^3} \\
&< 8\left(1-(1-\delta)^3\right) = 8 - 8(1-\delta)^3 = 8 - 8\sum_{k=0}^{3} \binom{3}{k} 1^{3-k} (-\delta)^3 \\
&= 8 - 8\sum_{k=0}^{3} \binom{3}{k} (-\delta)^3 = 8 - 8\left(\binom{3}{0}(-\delta)^0 + \binom{3}{1}(-\delta)^1 + \binom{3}{2}(-\delta)^2 + \binom{3}{3}(-\delta)^3\right) \\
&= 8 - 8\left(1 - 3\delta + 3\delta^2 - \delta^3\right) = 24\delta - 24\delta^2 + 8\delta^3.
\end{aligned}$$

Dieser Ausdruck lässt sich für $0 < \delta < \frac{1}{2}$ durch 24δ abschätzen, denn

$$\delta < 3 \implies \delta^3 < 3\delta^2 \implies 8\delta^3 < 24\delta^2 \implies 24\delta - 24\delta^2 + 8\delta^3 < 24\delta$$

Also gilt

$$0 < \frac{1}{(1-\delta)^3} - 1 < 24\delta.$$

Ebenfalls wird bei der Zusammenfassung der oberen und umgeformten unteren Abschätzung noch eine Abschätzung für $R(N)$ benötigt. Nach Satz 3.4.1 gilt

$$R(N) = \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right),$$

wobei die implizite Konstante von $A > 0$ abhängig ist. Da für die singuläre Reihe $\mathfrak{S}(N)$ nach Korollar 3.2.6 die Abschätzung $\frac{6}{\pi^2} < \mathfrak{S}(N) < \frac{2457}{\pi^6}$, also $\mathfrak{S}(N) = O(1)$ gilt, folgt

$$\begin{aligned} R(N) &= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right) = O(1)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right) \\ &= O\left(\frac{N^2}{2}\right) + O\left(\frac{N^2}{(\log N)^A}\right) = O\left(N^2\right) + O\left(\frac{N^2}{(\log N)^A}\right) \\ &= O\left(\max\left\{N^2, \frac{N^2}{(\log N)^A}\right\}\right) = O\left(N^2\right), \end{aligned}$$

also $R(N) \ll N^2$. Mit den zuvor gewonnenen Ergebnissen kann sich der Zusammenführung der oberen und umgeformten unteren Abschätzung zugewandt werden. Es folgt

$$\begin{aligned} R(N) \leq (\log N)^3 r(N) \implies 0 &\leq (\log N)^3 r(N) - R(N) \\ &\ll \frac{1}{(1-\delta)^3} R(N) + (\log N) N^{2-\delta} - R(N) \\ &= \left(\frac{1}{(1-\delta)^3} - 1\right) R(N) + (\log N) N^{2-\delta} \\ &\leq 24\delta R(N) + (\log N) N^{2-\delta} \\ &\ll \delta R(N) + (\log N) N^{2-\delta} \\ &\ll \delta N^2 + (\log N) N^{2-\delta} \\ &= \delta N^2 + \frac{(\log N) N^2}{N^\delta} \\ &= N^2 \left(\delta + \frac{\log N}{N^\delta}\right). \end{aligned}$$

Diese Ungleichungen gelten für alle $\delta \in \left(0, \frac{1}{2}\right)$ und die implizite Konstante ist dabei nicht von δ abhängig. Sei nun für genügend großes N

$$\delta := \frac{2\log(\log N)}{\log N},$$

dann folgt mit den Logarithmusregeln $\log_c b = \frac{\log_a b}{\log_a c}$ und $a^{\log_a b} = b$

$$\begin{aligned} \delta + \frac{\log N}{N^\delta} &= \frac{2\log(\log N)}{\log N} + \frac{\log N}{N^{\frac{2\log(\log N)}{\log N}}} = \frac{2\log(\log N)}{\log N} + \frac{\log N}{N^{2\log_N(\log N)}} \\ &= \frac{2\log(\log N)}{\log N} + \frac{\log N}{(\log N)^2} = \frac{2\log(\log N)}{\log N} + \frac{1}{\log N} \\ &\leq 2 \cdot \frac{\log(\log N)}{\log N} + \frac{\log(\log N)}{\log N} = 3 \cdot \frac{\log(\log N)}{\log N} \\ &\ll \frac{\log(\log N)}{\log N}. \end{aligned}$$

Es ist also

$$0 \leq (\log N)^3 r(N) - R(N) \ll N^2 \left(\delta + \frac{\log N}{N^\delta}\right) \ll N^2 \cdot \frac{\log(\log N)}{\log N},$$

bzw.

$$(\log N)^3 r(N) = R(N) + O\left(\frac{N^2 \log(\log N)}{\log N}\right).$$

Sei im weiteren $A \geq 1$. Mit Satz 3.4.1 folgt

$$\begin{aligned}
(\log N)^3 r(N) &= R(N) + O\left(\frac{N^2 \log(\log N)}{\log N}\right) \\
&= \mathfrak{S}(N)\frac{N^2}{2} + O\left(\frac{N^2}{(\log N)^A}\right) + O\left(\frac{N^2 \log(\log N)}{\log N}\right) \\
&= \mathfrak{S}(N)\frac{N^2}{2} + \mathfrak{S}(N)\frac{N^2}{2} \cdot O\left(\frac{N^2}{(\log N)^A} \cdot \frac{2}{\mathfrak{S}(N)N^2}\right) \\
&\qquad + \mathfrak{S}(N)\frac{N^2}{2} \cdot O\left(\frac{N^2 \log(\log N)}{\log N} \cdot \frac{2}{\mathfrak{S}(N)N^2}\right) \\
&= \mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\frac{N^2}{(\log N)^A} \cdot \frac{2}{\mathfrak{S}(N)N^2}\right) + O\left(\frac{N^2 \log(\log N)}{\log N} \cdot \frac{2}{\mathfrak{S}(N)N^2}\right)\right) \\
&= \mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\frac{1}{(\log N)^A\, \mathfrak{S}(N}\right) + O\left(\frac{\log(\log N)}{(\log N)\, \mathfrak{S}(N}\right)\right).
\end{aligned}$$

Da für die singuläre Reihe $\mathfrak{S}(N)$ nach Korollar 3.2.6 die Abschätzung $\frac{6}{\pi^2} < \mathfrak{S}(N) < \frac{2457}{\pi^6}$, also $\frac{1}{\mathfrak{S}(N)} = O(1)$ gilt, folgt

$$\begin{aligned}
&\mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\frac{1}{(\log N)^A\, \mathfrak{S}(N}\right) + O\left(\frac{\log(\log N)}{(\log N)\, \mathfrak{S}(N)}\right)\right) \\
&\qquad = \mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\frac{1}{(\log N)^A}\right) + O\left(\frac{\log(\log N)}{(\log N)}\right)\right) \\
&\qquad = \mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\max\left\{\frac{1}{(\log N)^A}, \frac{\log(\log N)}{(\log N)}\right\}\right)\right).
\end{aligned}$$

Für genügend großes N gilt die Ungleichung $1 < \log(\log N)$. Zudem ist $\min\{A, 1\} = 1$ für $A \geq 1$. Es folgt

$$O\left(\max\left\{\frac{1}{(\log N)^A}, \frac{\log(\log N)}{(\log N)}\right\}\right) = O\left(\frac{\log(\log N)}{(\log N)}\right),$$

also

$$(\log N)^3 r(N) = \mathfrak{S}(N)\frac{N^2}{2}\left(1 + O\left(\frac{\log(\log N)}{(\log N)}\right)\right).$$

Die Division durch $(\log N)^3$ liefert den asymptotischen Ausdruck für $r(N)$:

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2\,(\log N)^3}\left(1 + O\left(\frac{\log(\log N)}{(\log N)}\right)\right).$$

□

Weitere Untersuchungen von $r(N)$ führen zu folgenden Folgerungen

Korollar 3.4.3.[41]
Sei N eine genügend große ungerade natürliche Zahl. Es gilt

$$\frac{N^2}{(\log N)^3} \ll r(N).$$

Beweis.
Zur Herleitung dieser Abschätzung soll die umformulierte Darstellung von Satz 3.4.2

$$r(n) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\,(1 + f(N))$$
$$|f(N)| \leq K \cdot \frac{\log\log N}{\log N}\ (K > 0)$$

verwendet werden. Mit Satz A.1.3 folgt

$$|f(N)| \leq K \cdot \frac{\log\log N}{\log N} \Longleftrightarrow -K \cdot \frac{\log\log N}{\log N} \leq f(N) \leq K \cdot \frac{\log\log N}{\log N}.$$

Für genügend großes N folgt weiter

$$1 + f(N) \geq 1 - K \cdot \frac{\log\log N}{\log N} \geq \frac{1}{2},$$

womit sich die Abschätzung

$$\begin{aligned} r(n) &= \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\,(1 + f(N)) \\ &\geq \mathfrak{S}(N)\frac{N^2}{2(\log N)^3} \cdot \frac{1}{2} = \mathfrak{S}(N)\frac{N^2}{4(\log N)^3} \end{aligned}$$

ergibt. Mit der Abschätzung der singulären Reihe $\mathfrak{S}(N) > \frac{6}{\pi^2}$ aus Satz 3.2.5 folgt nun

$$\mathfrak{S}(N)\frac{N^2}{4(\log N)^3} > \frac{6}{\pi^2} \cdot \frac{N^2}{4(\log N)^3} = \frac{3}{2\pi^2} \cdot \frac{N^2}{(\log N)^3}.$$

Es kann also

$$\frac{3}{2\pi^2} \cdot \frac{N^2}{(\log N)^3} \leq r(N) \implies \frac{N^2}{(\log N)^3} \leq \frac{2\pi^2}{3} \cdot r(N) \ll r(N)$$

[41] Vgl. *Davenport H.*, 2000, S.146

festgehalten werden. Abschließend gilt also

$$\frac{N^2}{(\log N)^3} \ll r(N).$$

□

Korollar 3.4.4.
Sei N eine genügend große ungerade natürliche Zahl. Es gilt

$$\frac{N^2}{(\log N)^3} \ll r(N) \ll \frac{N^2}{(\log N)^3}.$$

Beweis.
Die Abschätzung nach unten kann Korollar 3.4.3 entnommen werden. Ausgangspunkt der Abschätzung nach oben ist auch hier die umformulierte Darstellung von Satz 3.4.2

$$r(n) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\,(1 + f(N))$$
$$|f(N)| \leq K \cdot \frac{\log\log N}{\log N}\ (K > 0).$$

Mit Satz A.1.3 folgt

$$|f(N)| \leq K \cdot \frac{\log\log N}{\log N} \iff -K \cdot \frac{\log\log N}{\log N} \leq f(N) \leq K \cdot \frac{\log\log N}{\log N}.$$

Für genügend großes N folgt weiter

$$1 + f(N) \leq 1 + K \cdot \frac{\log\log N}{\log N} \leq \frac{3}{2},$$

womit sich die Abschätzung

$$r(n) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\,(1 + f(N)) \leq \mathfrak{S}(N)\frac{N^2}{2(\log N)^3} \cdot \frac{3}{2} = \mathfrak{S}(N)\frac{3N^2}{4(\log N)^3}$$

ergibt. Mit der Abschätzung der singulären Reihe $\mathfrak{S}(N) < \frac{2457}{\pi^6}$ aus Korollar 3.2.6 folgt nun

$$\mathfrak{S}(N)\frac{3N^2}{4(\log N)^3} < \frac{2457}{\pi^6} \cdot \frac{3N^2}{4(\log N)^3} = \frac{7371}{4\pi^6} \cdot \frac{N^2}{(\log N)^3}.$$

Es gilt also

$$r(N) \leq \frac{7371}{4\pi^6} \cdot \frac{N^2}{(\log N)^3} \ll \frac{N^2}{(\log N)^3},$$

womit

$$r(N) \ll \frac{N^2}{(\log N)^3}$$

festgehalten werden kann. □

Bemerkung 3.4.5.
Es existieren zwei Konstanten k_1 und k_2 mit $0 < k_1 < k_2$, sodass für genügend großes N

$$k_1 \cdot \frac{N^2}{(\log N)^3} \leq r(N) \leq k_2 \cdot \frac{N^2}{(\log N)^3}$$

gilt.

Technische Details vernachlässigend kann als vereinfachtes Ergebnis festgehalten werden

Korollar 3.4.6.
Jede genügend große ungerade natürliche Zahl ist als Summe dreier Primzahlen darstellbar.

Anhang A

Hilfsmittel zum Beweis des Satzes von Vinogradov

Dieser Abschnitt beinhaltet die Hilfsmittel, die zum Beweis des Satzes von Vinogradov benötigt werden. Dabei sollen im ersten Teil weitestgehend solche aus der reellen und komplexen Analysis bereitgestellt werden. Im zweiten Teil wird dann eine geeignete Notation zur Beschreibung des Wachstums von Funktionen bereitgestellt, während im dritten Teil einiges aus der Zahlentheorie dargestellt wird. Auf eine Trennung zwischen beispielsweiser elementarer und analytischer Zahlentheorie wurde hierbei bewusst verzichtet. Eine solche wäre der Übersichtlichkeit nachteilig gewesen.

A.1 Hilfsmittel der reellen und komplexen Analysis

Die in diesem Abschnitt dargestellten Sätze und Begriffe sind breit gefächert und lassen sich nicht immer eindeutig der reellen bzw. komplexen Analysis zuordnen. So finden sich hier auch Erläuterungen zu Begriffen der Diskreten Mathematik bzw. Kombinatorik und der Funktionalanalysis. Für einzelne Begriffe jedoch separate Abschnitte einzuführen wäre der Übersichtlichkeit der Hilfsmittel sicher nicht dienlich gewesen, sodass ich darauf verzichtet habe. Zu Beginn stehen die Hilfsmittel und Begriffe der reellen Analysis. So wird mit Ungleichungen begonnen, dann auf die Konvergenz von Reihen im Allgemeinen und einer speziellen Reihe zu sprechen gekommen. Daran anschließend sollen Ergebnisse vorgestellt werden, die Integrale beinhalten. Die komplexe Analysis wird dann mit der komplexen Exponentialfunktion, einem Grenzwertsatz und einer Ungleichung für Integrale von komplexwertigen Funktionen begonnen. Daran anschließend wird auf das Integral über den Kreisrand und die Cauchy'sche Integralformel zu sprechen gekommen. Zum Abschluss des Abschnittes werden noch der Begriff der Orthogonalitätsrelation und der erzeugenden Funktion vorgestellt.

Die nachfolgenden Ungleichungen sprechen jeweils für sich, sodass es keiner weiteren Ausführung zu diesen bedarf. Die Variablen stehen dabei in den ersten drei Ungleichungen durchweg für reelle Zahlen.

Satz A.1.1.[1]
Ist $p_1 < p_2$ *und* $q > 0$, *so gilt* $\frac{p_1}{q} < \frac{p_2}{q}$.
Ist $0 < q_1 < q_2$ *und* $p > 0$, *so gilt* $\frac{p}{q_2} < \frac{p}{q_1}$, *insbesondere ist* $\frac{1}{q_2} < \frac{1}{q_1}$.

Satz A.1.2.[2]
Gleichsinnige Ungleichungen dürfen miteinander multipliziert werden, wenn alle Glieder positiv sind. Ist also $0 < a < b$ *und* $0 < c < d$, *so ist* $ac < bd$.

Satz A.1.3.[3]
Sei $\varepsilon > 0$. *Dann gilt sowohl* $|x| \leq \varepsilon \iff -\varepsilon \leq x \leq \varepsilon$,
als auch $|x - x_0| \leq \varepsilon \iff x_0 - \varepsilon \leq x \leq x_0 + \varepsilon$.

Satz A.1.4.[4]
Für den Betrag in $\mathbb{C}$ *gilt die Dreiecksungleichung* $|z_1 + z_2| \leq |z_1| + |z_2|$.

Zur Zusammenfassung des Produkts von Summen soll folgendes Lemma bereitgestellt werden:

Lemma A.1.5.[5]

Es gilt $\left(\sum_{l=1}^{n} a_l\right) \cdot \left(\sum_{k=1}^{n} b_k\right) = \sum_{l,k=1}^{n} a_l b_k$.

Um Untersuchungen des Konvergenzverhaltens durchzuführen werden das Majorantenkriterium und das Weierstraß'sche Majorantenkriterium benötigt.

Satz A.1.6 (Majorantenkriterium)**.**[6]
Ist $\sum c_n$ *eine konvergente Reihe mit nichtnegativen Gliedern und gilt fast immer* $|a_n| \leq c_n$, *so muss auch* $\sum a_n$ *konvergieren - und zwar sogar absolut.*

Satz A.1.7 (Weierstraß'sches Majorantenkriterium)**.**[7]
Sei eine Folge reellwertiger Funktionen $f_1, f_2, ...$ *gegeben, die alle auf derselben Menge* X *definiert sind, so nennt man* (f_n) *eine Funktionenfolge auf* X. *Ist für alle* $k \in \mathbb{N}$ *und alle* $x \in X$ *stets* $|f_k(x)| \leq c_k$ *und ist die Zahlenreihe* $\sum c_k$ *konvergent, so muss die Funktionenreihe* $\sum f_k$ *gleichmäßig auf* X *konvergieren.*

Es ist noch zu beachten, dass dieses Kriterium nur angewandt werden kann, wenn die Reihe $\sum f_k(x)$ für jedes $x \in X$ absolut konvergiert.[8] Beide Sätze behalten ihre Gültigkeit, auch

[1] *Heuser H.*, Satz 5.8, 2009, S.46
[2] Vgl.*Heuser H.*, Satz 5.6, 2009, S.46
[3] Vgl.*Heuser H.*, Satz 10.3 und anschl. Bemerkung, 2009, S.84
[4] Vgl.*Fischer W./Lieb I.*, Satz 1.1, 1994, S.4
[5] Vgl.*Heuser H.*, 2009, S.93
[6] Vgl.*Heuser H.*, Satz 33.4, 2009, S.46 und 555
[7] Vgl.*Heuser H.*, Satz 105.3, 2009, S.538 und 555
[8] Vgl.*Heuser H.*, 2009, S.555

wenn man die auftretenden reellen Größen durch komplexe ersetzt.[9] Im Speziellen wird noch benötigt:

Satz A.1.8.[10]
Die Reihe $\sum \frac{1}{n^\alpha}$ ist für $\alpha \leq 1$ divergent und für $\alpha > 1$ konvergent.

Satz A.1.9.[11]
Eine absolut konvergente Reihe $\sum_{k=0}^{\infty} a_k$ ist erst recht konvergent, und es gilt für sie die verallgemeinerte Dreiecksungleichung

$$\left| \sum_{k=0}^{\infty} a_k \right| \leq \sum_{k=0}^{\infty} |a_k|.$$

Der letzte Satz behält seine Gültigkeit, auch wenn man die auftretenden reellen Größen durch komplexe Größen ersetzt.[12] Nun soll sich den notwendigen Hilfsmitteln zugewandt werden, welche Integrale beinhalten.

Satz A.1.10.[13]
Sei $R[a,b]$ die Menge aller auf dem reellen Intervall $[a,b]$ Riemann-integrierbaren Funktionen. Seien die Funktionen $f, g \in R[a,b]$ und c eine Konstante, dann sind auch die Summe $f+g$ und jedes Vielfache cf Elemente von $R[a,b]$ und es gilt

$$\int_a^b (f+g)dx = \int_a^b f dx + \int_a^b g dx \text{ und } \int_a^b cf dx = c\int_a^b f dx.$$

Bemerkung A.1.11.[14]
Sei die Funktion $f : [a,b] \to \mathbb{C}$ gegeben. Ist f stetig, dann gilt $f \in R[a,b]$.

Satz A.1.12 (Fundamentalungleichung für R-Integrale)**.**[15]
Es bezeichne $\langle a,b\rangle := [min(a,b), max(a,b)]$, falls $a \neq b$. Dann gilt
$\left| \int_a^b f dx \right| \leq |b-a| \cdot \|f\|_\infty$ *, wobei $\|f\|_\infty$ die Supremumsnorm von f auf $\langle a,b\rangle$ ist.*

Satz A.1.13 (Substitutionsregel)**.**[16]
Es seien die folgenden Voraussetzungen erfüllt:
(a) f ist stetig auf $\langle a,b\rangle$ und g stetig differenzierbar auf $\langle \alpha,\beta\rangle$.
(b) Es ist $g(\langle \alpha,\beta\rangle) \subset \langle a,b\rangle$ und $g(\alpha) = a,\ g(\beta) = b$.
Dann gilt die Substitutionsformel $\int_a^b f(x)dx = \int_\alpha^\beta f(g(t))g'(t)dt.$

[9] Vgl. *Heuser H.*, 2009, S.16
[10] Vgl. *Heuser H.*, Satz 33.3, 2009, S.204
[11] Vgl. *Heuser H.*, Satz 31.4, 2009, S.193
[12] Vgl. *Heuser H.*, 2009, S.192
[13] Vgl. *Heuser H.*, Satz 79.4, 2009, S.453ff.
[14] Vgl. *Heuser H.*, 2008, S.393
[15] Vgl. *Heuser H.*, Satz 81.3, 2009, S.353 und S.462
[16] *Heuser H.*, Satz 81.6, 2009, S.464

Einige Eigenschaften betreffend die komplexe Exponentialfunktion sind in folgendem Satz festgehalten:

Satz A.1.14.

(i) Die komplexe Exponentialfunktion e^z ist für alle $z \in \mathbb{C}$ stets von Null verschieden.[17]

(ii) Die komplexe Exponentialfunktion e^z ist eine auf ganz $\mathbb{C}$ holomorphe Funktion.[18] *Insbesondere bedeutet dies, dass diese auf $\mathbb{C}$ stetig differenzierbar, ja sogar beliebig oft differenzierbar ist.*[19]

(iii) Es ist $\left|e^{iy}\right| = 1$ für alle $y \in \mathbb{R}$.[20]

(iv) Es ist $e^{2\pi i} = 1$.[21]

Bemerkung A.1.15.
Für die ganze Zahl k ist nach Satz A.1.14 (iv) $\left(e^{2\pi i}\right)^k = e^{k(2\pi i)} = (1)^k = 1.$

Hilfreich für Grenzwertbetrachtungen ist

Satz A.1.16.[22]
Seien die Funktionen $f : \mathbb{C} \to \mathbb{C},\ g : \mathbb{C} \to \mathbb{C}$ sowie $L, M \in \mathbb{C}$ gegeben. Gilt $f(z) \to L$ und $g(z) \to M$ für $z \to z_0$, dann gilt für $z \to z_0$ auch

(i) $f(z) + g(z) \to L + M$

(ii) $f(z)g(z) \to LM$

(iii) $\frac{f(z)}{g(z)} \to \frac{L}{M}$, *vorausgesetzt das* $M \neq 0$ *ist.*

Eine nützliche Ungleichung bezüglich der Integration komplexwertiger Funktionen auf reellen Intervallen ist folgende:

Satz A.1.17.[23]
Es sei $f : [a, b] \to \mathbb{C}$ stückweise stetig. Dann ist $\left|\int_a^b f(t)dt\right| \leq \int_a^b |f(t)|\, dt.$

Eine Übertragung der reellen Substitutionsregel für komplexwertige Funktionen stellt nachfolgender Satz bereit.

[17] Vgl. *Fischer W./Lieb I.*, 1994, S.31
[18] Vgl. *Fischer W./Lieb I.*, 1994, S.31
[19] Vgl. *Heuser H.*, 2008, S.347
[20] Vgl. *Heuser H.*, 2009, S.397
[21] Vgl. *Heuser H.*, Gleichung (68.6), 2009, S.395
[22] Vgl. *Gamelin T.G.*, Theorem, 2001, S.37
[23] *Fischer W./Lieb I.*, Hilfssatz, 1994, S.37

Satz A.1.18.[24]
Sei g eine reelle, monotone, stetige und stückweise stetig differenzierbare Funktion, die das Intervall $[a, b]$ auf das Intervall $[c, d]$ abbildet und sei $f : [c, d] \to \mathbb{C}$ stückweise stetig, so gilt

$$\int_a^b f(g(t))g'(t)dt = \int_c^d f(s)ds.$$

Nun noch eine kurze Erinnerung zur Integration im Komplexen: Sei $r \in \mathbb{R}, r > 0$ fest gewählt und sei $z_0 \in \mathbb{C}$. Dann bezeichnet

$$\overline{D_r(z_0)} := \{z \in \mathbb{C} : \ \mid z - z_0 \mid \leq r\}$$

die abgeschlossene Kreisscheibe mit Radius r um z_0,

$$D_r(z_0) := \{z \in \mathbb{C} : \ \mid z - z_0 \mid < r\}$$

die offene Kreisscheibe mit Radius r um z_0 und

$$\partial D_r(z_0) := \{z \in \mathbb{C} : \ \mid z - z_0 \mid = r\}$$

den Kreisrand.[25] Die Abbildung

$$\kappa : \ [0, 2\pi] \to \mathbb{C}, \ t \to z_0 + re^{it}$$

ist dann ein einfach geschlossener glatter Weg, dessen Spur $Sp(\kappa) = \kappa([0, 2\pi])$ den Kreisrand $\partial D_r(z_0)$ beschreibt. Bezeichnet man diesen Weg mit $\kappa(r, z_0)$, dann ist

$$\int_{\partial D_r(z_0)} f(z)dz = \int_{\kappa(r,z_0)} f(z)dz$$

das Integral über den Kreisrand, welches auch häufig als

$$\int_{\partial D_r(z_0)} f(z)dz = \int_{|z-z_0|=r} f(z)dz$$

dargestellt wird.[26] Ist nun $G \subset \mathbb{C}$ ein Gebiet und $B \subset G$ eine offene Teilmenge, dann liegt B *relativ kompakt* in G, geschrieben $B \subset\subset G$, wenn $\overline{B}$ kompakt und in G enthalten ist.[27] Dies erlaubt die Darstellung der Cauchy'schen Integralformel:

Satz A.1.19 (Cauchy'sche Intergralformel)**.**[28]
Sei $G \subset \mathbb{C}$ ein Gebiet, $f : G \to \mathbb{C}$ holomorph, $z_0 \in G$ und $r > 0$, so dass $D_r(z_0) \subset\subset G$ ist. Dann gilt für alle $z \in D_r(z_0)$:

$$f(z) = \frac{1}{2\pi i} \int_{D_r(z_0)} \frac{f(\zeta)}{\zeta - z} d\zeta.$$

[24] *Fischer W./Lieb I.*, Substitutionsregel, 1994, S.37
[25] Vgl.*Fischer W./Lieb I.*, 1994, S.5ff
[26] Vgl.*Fischer W./Lieb I.*, 1994, S.38ff
[27] *Fritzsche K.*, Definition, 2009, S.81
[28] Vgl.*Fritzsche K.*, Satz 2.2.11, 2009, S.84

Nun zum Begriff der Orthogonalitätsrelation. Dieser lässt sich der Funktionalanalysis bzw. der Theorie der Fourierreihen, welche hier nicht tiefgehend behandelt werden soll, zuordnen. Nur soviel sei zur Klärung des Begriffs gesagt:
Definiert man für zwei Funktionen deren Skalarprodukt auf einem reellen Intervall $[a, b]$ durch

$$(f, g) := \int_a^b f(x)g(x)dx,$$

so sollen in Anlehnung an den Begriff aus der Linearen Algebra diese beiden Funktionen *orthogonal* zueinander genannt werden, wenn $(f, g) = 0$ ist.[29] Eine Gleichung der Art

$$(f, g) = \int_a^b f(x)g(x)dx = 0$$

enthällt offensichtlich eine Orthogonalitätsaussage, weshalb man diese auch Orthogonalitätsrelation nennt.[30] Betrachtet man nun statt den nur von x abhängigen Funktionen $f(x)$ und $g(x)$ die Funktionen $f_m(x)$ und $g_n(x)$, die in einer hier nicht näher bestimmten Weise noch von $m, n \in \mathbb{N}_0$ abhängig seien, dann wird die Orthogonalitätsrelation in Abhängigkeit von m, n formuliert als[31]:

$$\int_a^b f_m(x)g_n(x)dx = \begin{cases} \lambda > 0 & \text{für } m = n \\ 0 & \text{für } m \neq n. \end{cases}$$

Weitere wichtige Begriffe sind die formale Potenzreihe und die erzeugende Funktion. Diese Begriffe lassen sich der Kombinatorik oder allgemeiner der diskreten Mathematik, welche diese als Teilgebiet beinhaltet, zuordnen. Während man sich in der Analysis primär mit dem Konvergenzverhalten von Potenzreihen beschäftigt, ist für die Kombinatorik auch das rein formale Rechnen mit solchen von Bedeutung. Dabei ist zwar die Konvergenz einer Potenzreihe für viele Aufgaben der Kombinatorik von Interesse, oft aber keine notwendige Voraussetzung für das Aufstellen einer solchen.[32]
Ist nun bei kombinatorischen Fragestellungen eine Folge $a_0, a_1, ...$ von Zählkoeffizienten gesucht, so werden diese als Koeffizienten der formalen Potenzreihe
$A(z) = \sum_{n\geq 0} a_n z^n$ $(z \in \mathbb{C})$ aufgefasst. Durch diese Darstellung mittels formaler Potenzreihe ist es möglich, mit den Koeffizienten als „Ganzes“ zu rechnen. Dabei meint „formal“, dass die Potenzen z^n nur als Aufhänger für das Rechnen verwendet werden, man Konvergenzfragen aber wie bereits erwähnt ersteinmal völlig außer acht lässt. Grundsätzlich werden zwei Typen formaler Potenzreihen unterschieden:

[29] Vgl. *Heuser H.*, 2008, S.123ff
[30] Vgl. *Heuser H.*, 2006, S.26ff
[31] Vgl. *Heuser H.*, 2008, S.123ff und
Vgl. *Zygmund A.*, 1959, S.5
[32] Vgl. *Tittmann P.*, 2000, S.46

Für die Folge (a_n) unterscheidet man zwischen der *erzeugenden Funktion*[33]

$$A(z) := \sum_{n\geq 0} a_n z^n \ (z \in \mathbb{C}),$$

und der *erzeugenden Funktion vom Exponentialtyp*[34]

$$\hat{A}(z) := \sum_{n\geq 0} \frac{a_n}{n!} z^n \ (z \in \mathbb{C}).$$

Im Abschnitt zur Kreismethode wird man allerdings noch sehen, dass erzeugende Funktionen auch in anderer Gestalt auftreten können.

[33] Vgl. *Aigner M.*, 2009, S.57
[34] Vgl. *Aigner M.*, 2009, S.65

A.2 Landau'sche Ordnungssymbole

In diesem Abschnitt soll die notwendige Notation zur Beschreibung von Größenordnungen zwischen Funktionen bereitgestellt werden. Zu diesem Zweck werden die Bachmann-Landau-Symbole $O(\cdot)$ und $o(\cdot)$ eingeführt. Diese eignen sich zur übersichtlichen Beschreibung von Eigenschaften von Funktionen besonders dadurch, dass sie es erlauben auf die Angabe von numerischen Größen zu verzichten.[35] Darüber hinaus wird auch das Vinogradov-Symbol $\ll$ als Alternative zu $O(\cdot)$, das Symbol $\prec$ als Alternative zu $o(\cdot)$ und das Symbol $\sim$ bereitgestellt. Letzteres Symbol lässt sich aus einem besonderen Fall für $o(\cdot)$ motivieren. Auf die jeweiligen Vorzüge eines Symbols wird dann an geeigneter Stelle eingegangen.

Soll zum Ausdruck gebracht werden, dass eine Funktionen betragsmäßig höchstens so schnell wächst wie eine andere Funktion, kann das $O(\cdot)$- oder $\ll$-Symbol verwendet werden.

Definition A.2.1 ($O(\cdot)$-und $\ll$-Symbol)**.**[36]
Sei $\mathbb{D}$ eine offene Teilmenge der reellen Zahlen und seien die Funktionen $f : \mathbb{D} \to \mathbb{C}$ und $g : \mathbb{D} \to \mathbb{R}^+$ gegeben und für alle genügend großen reellen x definiert. Die Funktion $f(x)$ soll dann mit

$$O(g(x))$$

bezeichnet werden, wenn eine Konstante $c > 0$ und ein x_0 derart existieren, sodass für alle $x \geq x_0$ die Ungleichung

$$|f(x)| \leq c \cdot g(x)$$

gilt. Symbolisch:

$$f(x) = O(g(x)) \text{ oder } f(x) \ll g(x).$$

Bemerkung A.2.2.

(i) Eingeführt wurde die Notation mit $O(\cdot)$ erstmals von Bachmann in seinem Buch zur analytischen Zahlentheorie. Durch Landau wurde diese dann populär.[37] Zudem ergänzte Landau das Symbol $o(\cdot)$, auf welches später noch eingegangen wird. Das von Vinogradov eingeführte Symbol $\ll$ kann als Alternative zur $O(\cdot)$-Notation verwendet werden.[38]

(ii) Ist $f(x)$ eine Funktion der genannten Art, dann schreibt man $f(x) = O(g(x))$ bzw. $f(x) \ll g(x)$, was nicht mehr und nicht weniger aussagen soll, als dass $f(x)$ betragsmäßig durch $g(x)$ abgeschätzt werden kann.

(iii) Gilt $f(x) = O(g(x))$ bzw. $f(x) \ll g(x)$, so sagt man $f(x)$ ist ein „groß O" von $g(x)$ bzw. $f(x)$ ist „kleiner kleiner" $g(x)$.[39]

[35] Vgl. *Menzer, H.*, 2010, S.207
[36] Vgl. *Nathanson M.B.*, 2010, S.xiii, *Hardy G./ Wright E.*, 1990, S.7 ff. und *Prachar K.*, 1957, S.15 und S.191
[37] Vgl. *Steger A.*, 2007, S.11
[38] Vgl. *Vaughan, R.C.*, 1997, S.xiii
[39] Vgl. *Menzer, H.*, Bemerkung 4.5.1, 2010, S.208

(iv) Der Vorteil der eingeführten Symbolik liegt darin, dass diese bei Untersuchungen wesentliche Eigenschaften einer Funktion zum Ausdruck bringt. Es ist allerdings darauf zu achten, dass Gleichungen in denen der Ausdruck $O(\cdot)$ auftritt eigentlich keine Gleichungen sind und von links nach rechts gelesen werden.

(v) Die Konstante $c > 0$ wird auch implizite Konstante genannt.[40] Diese Konstante ist zwar von x unabhängig, kann aber durchaus noch von anderen Parametern abhängen. Ist dem so, dann müssen diese Parameter angegeben werden.

(vi) Gilt $|f(x)| \leq cg(x)$, dann gilt mit der positiven Konstanten $c' > c$ auch $|f(x)| \leq c'g(x)$. Die implizite Konstante ist also nicht eindeutig.

(vii) Der exakte Wert der impliziten Konstanten ist nicht von Bedeutung. Von Bedeutung ist lediglich, dass eine solche Konstante existiert. In manchen Fällen wäre es auch ein langwieriger Prozess den exakten Wert bestimmen zu wollen, bspw. wenn diese noch von einem oder gar mehreren Parametern abhängt, die nicht näher bestimmt werden können. Die Stärke der eingeführten Notation liegt also auch darin, dass sie es erlaubt die Existenz einer impliziten Konstanten aufzuschreiben, ohne deren Wert angeben zu müssen.

(viii) Es wurde zwar $O(g(x))$ bzw. $f(x) = O(g(x))$ für eine bekannte Funktion $f(x)$ definiert, nicht aber das Zeichen $O(g(x))$ alleine. Es empfiehlt sich jedoch die Bezeichnung handlicher zu machen. An dieser Stelle soll deshalb vereinbart werden, dass $O(g(x))$ eine unbestimmte Funktion bezeichnet, für welche die Abschätzung der Definition A.2.1 gilt.[41] Wann immer also das Zeichen $O(g(x))$ auftritt ist zu beachten, dass $O(g(x))$ eine abkürzende Bezeichnung für eine unbekannte Funktion ist, welche betragsmäßig durch $g(x)$ abgeschätzt werden kann.

(ix) Sei $f(x) := f_1(x) - f_2(x)$. Dann soll $f_1(x) = f_2(x) + O(g(x))$ dasselbe wie $f_1(x) - f_2(x) = f(x) = O(g(x))$ bedeuten.[42]

(x) Statt $f(x) \ll g(x)$ kann auch $g(x) \gg f(x)$ geschrieben werden.

[40] Vgl. *Nathanson M.B.*, 2010, S.xiii
[41] Vgl. *Hardy G./ Wright E.*, 1990, S.7 ff.
[42] Vgl. *Miller S./Takloo-Bighash R.*, 2006, S.34

Beispiel A.2.3.

(i) Seien auf $\mathbb{R}$ *die Funktionen* $f(x) = \sin(x)$ *und* $g(x) \equiv 1$ *gegeben. Dann gilt für alle reellen Zahlen*

$$|\sin(x)| \leq 1.$$

Es ist also $\sin(x) = O(1)$ *bzw.* $\sin(x) \ll 1$*, wobei* $O(1)$ *stets so zu verstehen ist, dass die abgschätzte Funktion beschränkt bleibt.*

(ii) Seien auf $\mathbb{R}^+$ *die Funktionen* $f_1(x) = \sin(x),\ f_2(x) = \cos(x)$ *und* $g(x) = x$ *gegeben. Dann gilt für alle* $x \geq 1$

$$|\sin(x) - \cos(x)| \leq x.$$

Also kann $\sin(x) = \cos(x) + O(x),\ \sin(x) - \cos(x) = O(x)$ *oder* $\sin(x) - \cos(x) \ll x$ *geschrieben werden.*

(iii) Es ist $O(1) + O(1) = O(1)$*, denn die Summe zweier beschränkter Funktionen ist wieder beschränkt.*
Es ist $O(x) + O(e^x) = O(e^x)$*, denn die Summe einer linear und einer exponentiell abschätzbaren Funktion ist wieder exponentiell abschätzbar.*

(iv) Dass es von Bedeutung ist, bei der Formulierung von Aussagen mit $O(\cdot)$*-Termen darauf zu achten, dass diese von links nach rechts zu lesen sind, verdeutlicht nachfolgende Betrachtung:*
So ist $O(x) = O(x^2)$ *richtig und besagt nur, dass eine durch* x *abschätzbare Funktion auch durch* x^2 *abgeschätzt werden kann. Falsch hingegen wäre* $O(x^2) = O(x)$ *zu schreiben, denn eine durch* x^2 *abschätzbare Funktion kann zwar, muss aber nicht durch* x *abschätzbar sein.*

Nachdem die eingeführten Symbole $O(\cdot)$ und $\ll$ beide dasselbe Verhalten der Funktion $f(x)$ beschreiben, stellt sich die berechtigte Frage, warum dafür zwei Notationen verwendet werden sollen. Die Einführung der beiden Symbole lässt sich damit begründen, dass jedes der beiden Symbole Darstellungsvorteile bietet, die das andere Symbol nicht oder nur eingeschränkt leisten kann. Das Symbol $O(\cdot)$ soll aufgrund des Gleichheitszeichen bevorzugt dann verwendet werden, wenn es gilt Ergebnisse in einem Satz, Lemma o.ä. festzuhalten. Das Symbol $\ll$ hingegen erlaubt es, Abschätzungen optisch klarer zu formulieren, denn für diesen Zweck ist die Schreibweise $f(x) \ll g(x)$ geeigneter als $f(x) = O(g(x))$. Besonders bei Ketten von Abschätzungen wie $f(x) \ll g(x) \ll h(x)$ wäre eine Notation mit $O(\cdot)$ unübersichtlicher. Ein Blick auf das folgende Beispiel macht die Vorzüge der $O(\cdot)$-Notation gegenüber $\ll$ zum Festhalten von Ergebnissen deutlicher.

Beispiel A.2.4.
Seien die Funktionen $f_1 : \mathbb{R} \to \mathbb{C}, f_2 : \mathbb{R} \to \mathbb{C}$ und $g : \mathbb{R} \to \mathbb{R}^+$, sowie eine Konstante $c > 0$ gegeben und es gelte für alle $x \geq x_0$

$$|f_1(x) - f_2(x)| \leq cg(x).$$

Es kann dann

$$f_1(x) = f_2(x) + O(g(x)) \qquad (*)$$

geschrieben werden. Nachdem allerdings auch

$$|f_1(x) - f_2(x)| = |f_2(x) - f_1(x)| \leq cg(x)$$

gilt, kann ebenso gut

$$f_2(x) = f_1(x) + O(g(x)) \qquad (**)$$

geschrieben werden. Die Darstellung $(*)$ ermöglicht es die Funktion $f_1(x)$ durch die Funktion $f_2(x)$ zu beschreiben, wobei der Term $O(g(x))$ als Fehler- bzw. Restterm interpretiert werden kann. Ebenso ermöglicht Darstellung $(**)$ eine Interpretation der Funktion $f_2(x)$ durch $f_1(x)$ und den Term $O(g(x))$. Die Darstellungen $(*)$ und $(**)$ kann das $\ll$-Symbol allerdings nicht leisten. Lediglich

$$f_1(x) - f_2(x) = O(g(x)) \text{ bzw. } f_2(x) - f_1(x) = O(g(x))$$

kann als

$$f_1(x) - f_2(x) \ll g(x) \text{ bzw. } f_2(x) - f_1(x) \ll g(x)$$

geschrieben werden. Dafür bietet das $\ll$-Symbol wie bereits erwähnt deutliche Vorteile bei der Darstellung von Ungleichungsketten.

Es ist also situationsabhängig, welchem der beiden Symbole der Vorzug gegeben wird. Dass es für den Umgang mit $O(\cdot)$-Ausdrücken bereits in einfachen Fällen genügt, sich die Bedeutung des Ausdrucks zu verdeutlichen, konnte in Beispiel A.2.3 (iii) festgestellt werden. Dennoch sollen einige Grundregeln für den Umgang mit derartigen Ausdrücken bereitgestellt werden. Zuerst soll jedoch noch darauf eingegangen werden, dass die Notation mit $O(\cdot)$ auch in dem Sinne Vorteile bringt, dass „überflüssige Details“ in den $O(\cdot)$-Term verschoben werden können, sodass der Blick auf das Wesentliche bestehen bleibt.

Beispiel A.2.5.[43]
Stößt man in Rechnungen auf den Ausdruck $\sqrt{n+a}$ $(n \in \mathbb{N})$ *mit einer Konstanten* a, *so kann man wegen* $\sqrt{n+a} = \sqrt{n} + O(1)$ *die Rechnung mit dem bequemeren Ausdruck* $\sqrt{n} + O(1)$ *fortsetzen, da* $\sqrt{n+a} - \sqrt{n} \leq |a|$ *gilt.*
Die Ungleichung $\sqrt{n+a} - \sqrt{n} \leq |a|$ *ergibt sich dabei aus der Multiplikation von* $\sqrt{n+a} - \sqrt{n}$ *mit* $\frac{\sqrt{n+a}+\sqrt{n}}{\sqrt{n+a}+\sqrt{n}}$ *und Berücksichtigung der Fälle* $a \geq 0$, $a < 0$.
Das daraus erhaltene Resultat $\sqrt{n+a} - \sqrt{n} = O(1)$ *lässt sich nach Bemerkung A.2.2* (ix) *auch als* $\sqrt{n+a} = \sqrt{n} + O(1)$ *schreiben.*

Bemerkung A.2.6.
Mit dem Symbol $\ll$ *wäre auch die Notation* $\sqrt{n+a} - \sqrt{n} \ll 1$ *möglich gewesen, nicht aber* $\sqrt{n+a} = \sqrt{n} + O(1)$.

Nun zu den bereits angesprochenen Grundregeln für den Umgang mit $O(\cdot)$- und $\ll$-Ausdrücken.

Lemma A.2.7.

(i) Konstanten in $O(\cdot)$*-Termen*
Sei $k > 0$. *Die Abschätzung* $f(x) = O(k \cdot g(x))$ *ist äquivalent zu* $f(x) = O(g(x))$. *Insbesondere ist also für* $g(x) \equiv 1$ *die Abschätzung* $f(x) = O(k)$ *äquivalent zu* $f(x) = O(1)$.

(ii) Transitivität
Ist $f(x) = O(g(x))$ *und* $g(x) = O(h(x))$, *dann ist auch* $f(x) = O(h(x))$.

(iii) Produkte in $O(\cdot)$*-Terme verschieben*[44]
Sei $f(x) = O(g(x))$ *und* $h(x) > 0$. *Dann ist* $h(x) \cdot f(x) = O(h(x) \cdot g(x))$.

(iv) Produkte von $O(\cdot)$*-Termen*[45]
Sei $f_1(x) = O(g_1(x))$ *und* $f_2(x) = O(g_2(x))$. *Dann ist* $f_1(x) \cdot f_2(x) = O(g_1(x) \cdot g_2(x))$.

(v) Summe von $O(\cdot)$*-Termen*[46]
Sei $f_1(x) = O(g_1(x))$ *und* $f_2(x) = O(g_2(x))$. *Dann ist*
$f_1(x) + f_2(x) = O(g_1(x) + g_2(x)) = O\left(\max\{g_1(x), g_2(x)\}\right)$.

Beweis.

(i) Seien die Funktionen $f : \mathbb{R} \to \mathbb{C}$ und $g : \mathbb{R} \to \mathbb{R}^+$ gegeben. Zunächst soll von $f(x) = O(k \cdot g(x))$ auf $f(x) = O(g(x))$ geschlossen werden.
Vorausgesetzt sei die Existenz der Konstanten $c > 0$ und $k > 0$, sowie eines x_0, sodass für alle $x \geq x_0$ die Ungleichung $|f(x)| \leq c \cdot k \cdot g(x)$ gelte. Es kann also $f(x) = O(k \cdot g(x))$ geschrieben werden. Sei die positive Konstante $\hat{c}$ definiert als $\hat{c} := c \cdot k$. Es folgt für alle $x \geq x_0$, dass $|f(x)| \leq c \cdot k \cdot g(x) = \hat{c} \cdot g(x)$ gilt. Also kann $f(x) = O(g(x))$ geschrieben werden.

[43] Vgl. *Aigner M.*, 2009, S.93
[44] Vgl. *Schwarz W.*, 1969, S.201
[45] Vgl. *Schwarz W.*, 1969, S.201
[46] Vgl. *Schwarz W.*, 1969, S.201

Es ist nun von $f(x) = O(g(x))$ auf $f(x) = O(k \cdot g(x))$ zu schließen.
Sei vorausgesetzt, dass eine Konstante $\hat{c} > 0$ und ein x_0 derart existieren, dass für alle $x \geq x_0$ die Ungleichung $|f(x)| \leq \hat{c} \cdot g(x)$ gilt. Demnach kann $f(x) = O(g(x))$ geschrieben werden. Mit $\breve{k} := \frac{\hat{c}}{k}$ folgt für alle $x \geq x_0$, dass
$|f(x)| \leq \hat{c} \cdot g(x) = \frac{\hat{c}}{k} \cdot k \cdot g(x) = \breve{k} \cdot k \cdot g(x)$ und es kann $f(x) = O(k \cdot g(x))$ geschrieben werden.

(ii) Seien die Funktionen $f : \mathbb{R} \to \mathbb{C}$, $g : \mathbb{R} \to \mathbb{R}^+$ und $h : \mathbb{R} \to \mathbb{R}^+$ gegeben. Zudem gebe es positive Konstanten c und k, sowie ein x_0 derart, dass für alle $x \geq x_0$ die Ungleichungen $|f(x)| \leq c \cdot g(x)$ und $|g(x)| \leq k \cdot h(x)$ gelten. Es kann also $f(x) = O(g(x))$ und $g(x) = O(h(x))$ geschrieben werden. Da die Funktion g nur positive Werte annimmt, ist $|g(x)| = g(x) \leq k \cdot h(x)$. Mit $\hat{c} := \max\{1, c \cdot k\}$ folgt für alle $x \geq x_0$ dass $|f(x)| \leq c \cdot g(x) \leq \hat{c} \cdot h(x)$ ist, womit $f(x) = O(h(x))$ geschrieben werden kann.

(iii) Seien die Funktionen $f : \mathbb{R} \to \mathbb{C}$, $g : \mathbb{R} \to \mathbb{R}^+$ und $h : \mathbb{R} \to \mathbb{R}^+$ gegeben. Vorausgesetzt sei die Existenz der Konstanten $c > 0$ und eines x_0, sodass für alle $x \geq x_0$ die Ungleichung $|f(x)| \leq c \cdot g(x)$ gelte. Es kann also $f(x) = O(g(x))$ geschrieben werden. Durch Multiplikation mit der Funktion $h(x) > 0$ folgt für alle $x \geq x_0$, dass $h(x) \cdot |f(x)| = |h(x) \cdot f(x)| \leq c \cdot h(x) \cdot g(x)$ gilt, womit $h(x) \cdot f(x) = O(h(x) \cdot g(x))$ geschrieben werden kann.

(iv) Seien die Funktionen $f_i : \mathbb{R} \to \mathbb{C}$ und $g_i : \mathbb{R} \to \mathbb{R}^+$ für $i = 1, 2$ gegeben. Zudem gebe es die positiven Konstanten c_1 und c_2, sowie ein x_0 derart, dass für alle $x \geq x_0$ die Ungleichungen $|f_1(x)| \leq c_1 \cdot g_1(x)$ und $|f_2(x)| \leq c_2 \cdot g_2(x)$ gelten. Dann kann $f_1(x) = O(g_1(x))$ und $f_2(x) = O(g_2(x))$ geschrieben werden. Sei $k := \max\{1, c_1 \cdot c_2\}$. Durch Multiplikation der Funktionen $f_1(x)$ und $f_2(x)$ folgt für alle $x \geq x_0$, dass $|f_1(x)| \cdot |f_2(x)| = |f_1(x) \cdot f_2(x)| \leq k \cdot g_1(x) \cdot g_2(x)$ gilt, womit
$f_1(x) \cdot f_2(x) = O(g_1(x) \cdot g_2(x))$ geschrieben werden kann.

(v) Seien die Funktionen $f_i : \mathbb{R} \to \mathbb{C}$ und $g_i : \mathbb{R} \to \mathbb{R}^+$ für $i = 1, 2$ gegeben. Zudem gebe es die positiven Konstanten c_1 und c_2, sowie ein x_0 derart, dass für alle $x \geq x_0$ die Ungleichungen $|f_1(x)| \leq c_1 \cdot g_1(x)$ und $|f_2(x)| \leq c_2 \cdot g_2(x)$ gelten. Dann kann $f_1(x) = O(g_1(x))$ und $f_2(x) = O(g_2(x))$ geschrieben werden. Es sollen nun die impliziten Konstanten c_1 und c_2 durch die Konstante k mit $k \geq c_1, k \geq c_2$ ersetzt werden. Mit der Dreiecksungleichung Satz A.1.4 folgt für alle $x \geq x_0$, dass
$|f_1(x) + f_2(x)| \leq |f_1(x)| + |f_2(x)| \leq c_1 \cdot g_1(x) + c_2 \cdot g_2(x) \leq k \cdot g_1(x) + k \cdot g_2(x) = k(g_1(x) + g_2(x))$ gilt und es kann $f_1(x) + f_2(x) = O(g_1(x) + g_2(x))$ geschrieben werden.
Im zweiten Schritt sei $g(x) := \max\{g_1(x), g_2(x)\}$. Dann folgt mit $\breve{k} := 2k$, dass $k(g_1(x) + g_2(x)) \leq k(g(x) + g(x)) = 2k \cdot g(x) = \breve{k} \cdot g(x)$, womit
$f_1(x) + f_2(x) = O(g_1(x) + g_2(x)) = O\left(\max\{g_1(x), g_2(x)\}\right)$ geschrieben werden kann.

□

Bemerkung A.2.8.
Da die Bedingung zur Verwendung des $O(\cdot)$-Symbols identisch zu der des $\ll$-Symbols ist, lassen sich die Grundregeln aus Lemma A.2.7 entsprechend übertragen.

Soviel zu den Symbolen $O(\cdot)$ und $\ll$. Als nächstes sollen die verbliebenen Symbole $o(\cdot)$, $\prec$ und $\sim$ eingeführt werden. Da von diesen allerdings kaum Gebrauch gemacht wird, wird die Darstellung etwas knapper gehalten.

Soll zum Ausdruck gebracht werden, dass eine Funktion betragsmäßig langsamer wächst als eine andere Funktion, kann die $o(\cdot)$-Notation verwendet werden.

Definition A.2.9 ($o(\cdot)$- und $\prec$-Symbol).[47]
Seien die Funktionen $f : \mathbb{R} \to \mathbb{C}$ und $g : \mathbb{R} \to \mathbb{R}^+$ gegeben. Die Funktion $f(x)$ soll dann mit

$$o(g(x))$$

bezeichnet werden, wenn der Grenzwert des Quotienten $\frac{|f(x)|}{g(x)}$ für $x \to \infty$ existiert und Null ist, also

$$\lim_{x\to\infty} \frac{|f(x)|}{g(x)} = 0$$

gilt. Symbolisch:

$$f(x) = o(g(x)) \text{ oder } f(x) \prec g(x).$$

Bemerkung A.2.10.

(i) Gilt $f(x) = o(g(x))$, so sagt man $f(x)$ ist ein „klein o“ von $g(x)$.

(ii) Ist $f(x)$ eine Funktion der genannten Art, dann schreibt man $f(x) = o(g(x))$ bzw. $f(x) \prec g(x)$, was nicht mehr und nicht weniger aussagen soll, als dass das beschriebene Grenzwertverhalten gilt.

(iii) Sei $f(x) := f_1(x) - f_2(x)$. Dann soll $f_1(x) = f_2(x) + o(g(x))$ dasselbe wie $f_1(x) - f_2(x) = f(x) = o(g(x))$ bedeuten.[48]

(iv) Wie schon bei $O(\cdot)$ ist auch bei $o(\cdot)$ darauf zu achten, dass Gleichungen mit $o(\cdot)$ von links nach rechts zu lesen sind.

Beispiel A.2.11.
Sei $f(x) = x$ und $g(x) = x^2$, dann ist $\lim_{x\to\infty} \frac{x}{x^2} = 0$. Also ist $x = o(x^2)$.

Ebenso wie das Zeichen $\ll$ kann das $\prec$-Symbol vorteilhaft bei Ketten von Abschätzungen zum Einsatz kommen. Als einzige Eigenschaft soll deshalb die Transitivität aufgeführt werden.

[47] Vgl. *Hardy G./ Wright E.*, 1990, S.7 ff. und *Prachar K.*, 1957, S.15 und S.191
[48] Vgl. *Miller S./Takloo-Bighash R.*, 2006, S.34

Lemma A.2.12.
Gilt $f(x) \prec g(x)$ und $g(x) \prec h(x)$, dann auch $f(x) \prec h(x)$.

Beweis.
Nach der Voraussetzung gilt $\frac{|f(x)|}{g(x)} \to 0$ $(x \to \infty)$ und $\frac{|g(x)|}{h(x)} \to 0$ $(x \to \infty)$. Da $g(x) > 0$ ist, gilt $|g(x)| = g(x)$. Mit Satz A.1.16 (ii) folgt dann $\frac{|f(x)|}{g(x)} \cdot \frac{g(x)}{h(x)} = \frac{|f(x)|}{h(x)} \to 0$ $(x \to \infty)$, also ist $f(x) \prec h(x)$. □

Bemerkung A.2.13.
Da die dem Symbol $o(\cdot)$ zugrunde liegende Definition identisch zu der von $\prec$ ist, gilt die Transitivität auch für $o(\cdot)$. Ist also $f(x) = o(g(x))$ und $g(x) = o(h(x))$, dann ist $f(x) = o(h(x))$.

Beispiel A.2.14.
Aus $x \prec x^2$ und $x^2 \prec x^3$ folgt $x \prec x^3$.

Soll zum Ausdruck gebracht werden, dass zwei Funktionen in etwa gleich schnell wachsen, kann das Symbol $\sim$ verwendet werden. Die Einführung dieses Symbols lässt sich dabei aus der Gleichung $f(x) = g(x) + o(g(x))$ motivieren. Für diese gilt offenbar

$$\lim_{x\to\infty} \frac{|f(x) - g(x)|}{g(x)} = 0.$$

Mit $g(x) > 0$ folgt

$$\frac{|f(x) - g(x)|}{g(x)} = \left|\frac{f(x) - g(x)}{g(x)}\right| = \left|\frac{f(x)}{g(x)} - 1\right| \implies \lim_{x\to\infty} \left|\frac{f(x)}{g(x)} - 1\right| = 0.$$

Es muss also

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

gelten. Dieses Verhalten soll als Grundlage für nachfolgende Definition verwendet werden.

Definition A.2.15 ($\sim$-Symbol)**.**
Seien die Funktionen $f : \mathbb{R} \to \mathbb{C}$ und $g : \mathbb{R} \to \mathbb{R}^+$ gegeben. Dann soll $f(x) \sim g(x)$ geschrieben werden, wenn der Grenzwert des Quotienten $\frac{f(x)}{g(x)}$ für $x \to \infty$ existiert und Eins ist, also

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

gilt.

Bemerkung A.2.16.[49]
Gilt $f(x) \sim g(x)$, dann sagt man $f(x)$ und $g(x)$ sind asymptotisch gleich.

[49] Vgl. *Aigner M.*, 2009, S.91

Beispiel A.2.17.
Es ist $x+1 \sim x$, *denn* $\lim\limits_{x\to\infty} \dfrac{x+1}{x} = 1$.

Als einziges der hier vorgestellten Symbole ist die asymptotische Gleichheit eine Äquivalenzrelation.

Lemma A.2.18.
Für die asymptotische Gleichheit gilt

(i) Reflexivität: Es gilt $f(x) \sim f(x)$.

(ii) Symmetrie : Gilt $f(x) \sim g(x)$, *dann auch* $g(x) \sim f(x)$.

(iii) Transitivität: Gilt $f(x) \sim g(x)$ *und* $g(x) \sim h(x)$, *dann auch* $f(x) \sim h(x)$.

Beweis.

(i) Es gilt $\dfrac{f(x)}{f(x)} = 1 \to 1 \ (x \to \infty)$.

(ii) Gelte $\dfrac{f(x)}{g(x)} \to 1 \ (x \to \infty)$ und $1 \to 1 \ (x \to \infty)$. Mit Satz A.1.16 (iii) folgt dann $\dfrac{1}{\frac{f(x)}{g(x)}} = \dfrac{g(x)}{f(x)} \to 1 \ (x \to \infty)$.

(iii) Gelte $\dfrac{f(x)}{g(x)} \to 1 \ (x \to \infty)$ und $\dfrac{g(x)}{h(x)} \to 1 \ (x \to \infty)$. Dann folgt mit Satz A.1.16 (ii) auch $\dfrac{f(x)}{g(x)} \cdot \dfrac{g(x)}{h(x)} = \dfrac{f(x)}{h(x)} \to 1 \ (x \to \infty)$.

□

Abschließend soll ein Beispiel betrachtet werden, welches sich beim Beweis des Satzes von Vinogradov noch als nützlich erweisen wird.

Beispiel A.2.19.[50]
Es ist $\lim\limits_{x\to\infty} \dfrac{(\ln x)^\beta}{x^\alpha} = 0$ *für jedes* $\alpha, \beta > 0$.

Jede noch so große Potenz von $\ln x$ für $x \to \infty$ wächst also wesentlich langsamer gegen ∞, als jede noch so kleine (positive) Potenz von x. Unter Verwendung der eingeführten Symbole lässt sich festhalten:

$$(\ln x)^\beta = o\left(x^\alpha\right) \text{ bzw. } (\ln x)^\beta \prec x^\alpha \text{ für jedes } \alpha, \beta > 0.$$

Ebenfalls ist nun die Notation bereitgestellt um folgendes Hilfsmittel anzuführen:

[50] Vgl. *Heuser H.*, Beispiel 5, 2009, S.289

Satz A.2.20.[51]
Sei $x \geq 1$ und $k > 1$. Es gilt die Abschätzung

$$\sum_{n>x} \frac{1}{n^k} = O\left(x^{1-k}\right).$$

A.3 Hilfsmittel der Zahlentheorie

Dieser Abschnitt beinhaltet die notwendigen Hilfsmittel aus der Zahlentheorie. Dabei wird mit einigen grundlegenden Eigenschaften zur Teilbarkeit und dem größten gemeinsamen Teiler begonnen. Anschließend wird die Menge der arithmetischen Funktionen betrachtet, die mit den Verknüpfungen Addition und Dirichlet-Multiplikation einen kommutativen Ring mit Einselement bildet. Nachdem damit die arithmetischen Funktionen eingeführt sind, sollen einige spezielle Vertreter dieser Funktionen und ausgewählte Resultate zu diesen dargestellt werden. Den Abschluss diese Abschnittes bilden dann eine Abschätzung unter der Voraussetzung der Teilerfremdheit, der Approximationssatz von Dirichlet und Konvergenzbetrachtungen von unendlichen Produkten, sowie das Euler-Produkt.
Es sollen noch zwei Notationen vereinbart werden: Unter $\log m$ ist stets der natürliche Logarithmus zu verstehen. Damit wird der in der Zahlentheorie üblichen Notation gefolgt.[52] Zum anderen soll der Buchstabe p immer für ein Element aus der Menge der Primzahlen $\mathbb{P}$ reserviert bleiben. Dies erspart es, dies immer wieder explizit in Definitionen, Sätzen oder Lemmata zu erwähnen.

Dass es genügt, sich bei Teilbarkeitsbetrachtungen auf die natürlichen Zahlen zu beschränken, zeigt der folgende Satz:

Satz A.3.1.[53]
Es seien $m, n \in \mathbb{Z}$. Gilt $m \mid n$, so auch $-m \mid n$ und $m \mid -n$.

Auch der größte gemeinsame Teiler (m, n) der ganzen Zahlen m und n ist stets in den natürlichen Zahlen zu finden.

Satz A.3.2.[54]
Seien $m, n \in \mathbb{Z}$. Es gilt $(m, n) = (|m|, |n|)$.

Bemerkung A.3.3.[55]
Es sei an dieser Stelle daran erinnert, dass man für ein ganzzahliges $a \neq 0$ den größten gemeinsamen Teiler $(0, a) := |a|$ definiert.

Bezüglich der Kongruenz zweier Zahlen wird noch folgender Satz benötigt

[51] *Miller S./Takloo-Bighash R.*, Exercise 2.2.13, 2006, S.35
[52] Vgl. *Reiss K./Schmieder G.*, 2007, S.402
[53] Vgl. *Bundschuh P.*, Satz, 2008, S.4
[54] Vgl. *Reiss K./Schmieder G.*, Satz 5.1.1, 2007, S.127
[55] Vgl. *Schmidt A.*, 2007, S.2

Satz A.3.4.[56]
Vorausgesetzt es sei $a \equiv b \ (mod\ m)$ *mit* $a, b, d, m \in \mathbb{Z},\ m > 0,\ d > 0$. *Gilt* $d \mid m$ *und* $d \mid a$, *dann gilt auch* $d \mid b$.

Nun soll sich den arithmetischen Funktionen zugewandt werden.

Definition A.3.5 (Arithmetische Funktion)**.**[57]
Eine Funktion $f : \mathbb{N} \to \mathbb{C}$ *heißt arithmetische Funktion. Die Menge* $\mathcal{A}$ *sei die Menge der arithmetischen Funktionen.*

Eine arithmetische Funktion wird abhängig vom vorliegenden Fachbuch auch *zahlentheoretische Funktion* genannt. Unabhägig vom Namen sind dies Funktionen, die eine zahlentheoretische Relevanz haben.[58] Da diese Eigenschaft jedoch nicht ordentlich in einer Definition zu fassen und zudem vom Betrachter abhängig ist, fällt die Definition allgemeiner aus.
Auf $\mathcal{A}$ sollen zwei Verknüpfungen definiert werden. Sind zwei arithmetische Funktionen f, g gegeben und sollen addiert werden, so ist unter der Summe $(f + g)$ zu verstehen, dass $(f + g)(n) := f(n) + g(n)$ ist. Diese Verknüpfung ist kommutativ und assoziativ. Zudem besitzt jede arithmetische Funktion f ein Inverses $-f$, gegeben durch $(-f)(n) = -f(n)$, und für alle arithmetischen Funktionen gibt es ein neutrales Element, die Nullfunktion.[59]
Die zweite Verknüpfung auf $\mathcal{A}$ ist das Dirichlet-Produkt.

Definition A.3.6 (Dirichlet-Produkt)**.**[60]
Seien $f, g \in \mathcal{A}$, *dann ist ihr Dirichlet-Produkt die arithmetische Funktion* $h = (f * g)$ *definiert durch*

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

Für das Dirichlet-Produkt gelten die Kommutativität und die Assoziativität.

Satz A.3.7.[61]
Seien $f, g, k \in \mathcal{A}$, *dann gilt*

$$f * g = g * f \ \textit{(Kommutativgesetz)}$$
$$(f * g) * k = f * (g * k) \ \textit{(Assoziativgesetz).}$$

Definiert man die arithmetische Funktion $\delta(n)$ durch

$$\delta(n) := \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{für } n \geq 2 \end{cases}$$

[56] Vgl. *Apostol T.M.*, Theorem 5.5, 1976, S.109
[57] Vgl. *Nathanson M.B.*, 2010, S.301
[58] Vgl. *Reiss K./Schmieder G.*, 2007, S.399
[59] Vgl. *Nathanson M.B.*, 2010, S.301
[60] Vgl. *Apostol T.M.*, 1976, S.29
[61] Vgl. *Apostol T.M.*, 1976, S.29

so gilt für jedes $f \in \mathcal{A}$

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

Mit der Funktion δ gibt es also ein neutrales Element bezüglich der Dirichlet-Multiplikation.[62] Da die definierten Verknüpfungen Addition und Dirichlet-Multiplikation auch dem Distributivgesetz genügen,[63] kann als Ergebnis festgehalten werden:

Satz A.3.8.[64]
Die Menge der arithmetischen Funktionen $\mathcal{A}$ bildet zusammen mit der Addition und dem Dirichlet-Produkt den kommutativen Ring $(\mathcal{A}, +, *)$ mit Einselement $\delta(n)$.

Eine bedeutende Eigenschaft, die eine arithmetische Funktion besitzen kann, soll an dieser Stelle noch erwähnt werden:

Definition A.3.9 (Multiplikativität arithmetischer Funktionen)**.**[65]
Sei $f \in \mathcal{A}$ und nicht identisch Null. Dann heißt f multiplikativ, wenn $f(mn) = f(m)f(n)$ für alle $m, n \in \mathbb{N}$ mit $(m, n) = 1$ gilt.

Die Eigenschaft $(m, n) = 1$ bezeichnet man als *Teilerfremdheit*.[66] In Verbindung mit dem Hauptsatz der elementaren Zahlentheorie[67] wird die Bedeutung dieser Eigenschaft deutlich: Durch diese sind multiplikative arithmetische Funktionen über die eindeutige Primfaktorzerlegung vollständig mittels ihre Werte auf Primzahlpotenzen festgelegt.[68]

Ist also $n \in \mathbb{N}$ vollständig als Produkt von Primzahlen zerlegt, d.h. $n = p_1^{\alpha_1}...p_k^{\alpha_k} = \prod_{j=1}^{k} p_j^{\alpha_j}$,

dann ist für eine multiplikative arithmetische Funktion $f(n) = \prod_{j=1}^{k} f(p_j^{\alpha_j})$.[69]

Nachdem nun die arithmetischen Funktionen eingeführt sind, sollen einige bekannte Vertreter dieser Klasse von Funktionen dargestellt werden.[70] Die bekannteste dieser Funktionen ist wohl die Euler'sche φ-Funktion. Für $n \geq 1$ ist $\varphi(n)$ die Anzahl der natürlichen Zahlen $a \leq n$, die zu n teilerfremd sind, also $\varphi(n) = \#\{a \in \mathbb{N} \mid 1 \leq a \leq n \text{ und } (a, n) = 1\}$.[71] Als Zählfunktion kann die φ-Funktion definiert werden durch

[62] Vgl. *Nathanson M.B.*, 2010, S.302
[63] Vgl. *Bundschuh P.*, 2008, S.42
[64] Vgl. *Nathanson M.B.*, 2010, S.302
[65] Vgl. *Apostol T.M.*, 1976, S.33
[66] Vgl. *Reiss K./Schmieder G.*, Definition 5.1.2, 2007, S.130
[67] siehe Seite 3
[68] Vgl. *Schulze-Pillot R.*, 2008, S.51
[69] Vgl. *Bundschuh P.*,Proposition, 2008, S.36
[70] Die hierbei verwendeten griechischen Buchstaben sollen in der gesamten Arbeit stets für diese Funktionen reserviert bleiben.
[71] Vgl. *Nathanson M.B.*, 2010, S.314

Definition A.3.10 (Euler'sche φ-Funktion).[72]
Sei $n \geq 1$. Dann heißt die Funktion

$$\varphi(n) := \sum_{\substack{a \leq n \\ (a,n)=1}} 1$$

Euler'sche φ-Funktion.

Eine Formel für die φ-Funktion in Abhängigkeit von der Primfaktorzerlegung einer natürlichen Zahl stellt der anschließende Satz bereit:

Satz A.3.11.[73]
Sei $n \geq 1$ und $n = \prod_{j=1}^{k} p_j^{\alpha_j}$. Dann ist

$$\varphi(n) = \prod_{j=1}^{k} \left(p_j^{\alpha_j} - p_j^{\alpha_j - 1} \right) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j} \right) = n \prod_{\substack{p \mid n \\ p \in \mathbb{P}}} \left(1 - \frac{1}{p} \right).$$

Insbesondere ergibt sich sofort

Korollar A.3.12.[74]
Es ist $\varphi(p) = p - 1$ und $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Die φ-Funktion ist außerdem eine multiplikative arithmetische Funktion.

Satz A.3.13.[75]
Für $(m, n) = 1$ gilt $\varphi(mn) = \varphi(m)\varphi(n)$.

Auch kann man $\varphi(n)$ in einem gewissen Sinne abschätzen:

Satz A.3.14.[76]
Sei $\varepsilon > 0$. Dann ist $n^{1-\varepsilon} < \varphi(n) < n$ für alle genügend großen n.

Als nächste arithmetische Funktion soll die Möbius'sche μ-Funktion eingeführt werden.

Definition A.3.15 (Möbius'sche μ-Funktion).[77]
Die Möbius'sche μ-Funktion sei definiert durch $\mu(1) := 1$ und für $n > 1, n = p_1^{\alpha_1} ... p_k^{\alpha_k}$ sei

$$\mu(n) := \begin{cases} (-1)^k & \text{für } \alpha_1 = ... = \alpha_k = 1 \\ 0 & \text{sonst.} \end{cases}$$

[72] Vgl. *Schwarz W.*, 1969, S.203
[73] Vgl. *Holz M.*, 2010, S.100
[74] Vgl. *Holz M.*, 2010, S.99
[75] Vgl. *Apostol T.M.*, Theorem 2.5, 1976, S.28
[76] Vgl. *Nathanson M.B,*, Theorem A.16, 2010, S.315
[77] Vgl. *Apostol T.M.*, Definition, 1976, S.24

Es ist also $\mu(n) = 0$, genau dann wenn n durch ein Quadrat einer Primzahl teilbar ist.[78] Die μ-Funktion gehört ebenfalls zu den multiplikativen arithmetischen Funktionen.

Satz A.3.16.[79]
Für $(m, n) = 1$ *gilt* $\mu(mn) = \mu(m)\mu(n)$.

Betrachtet man die summierte μ-Funktion, so gilt

Satz A.3.17.[80]
Für $n \geq 1$ *ist* $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{für } n \geq 1. \end{cases}$

Eine Beziehung zwischen der Euler'schen φ-Funktionen und der Möbius'schen μ-Funktion formuliert der folgende Satz:

Satz A.3.18.[81]
Für $n \geq 1$ *gilt* $\varphi(n) = \sum_{d|n} \mu(d) \cdot \left(\frac{n}{d}\right)$.

Eine besondere Summe, die in Verbindung zur φ- und μ-Funktion steht, ist die Ramanujan-Summe. Es soll vor der Definition dieser noch eine Notation vereinbart werden:

Definition A.3.19.[82]
Sei α *eine reelle Zahl. Als abkürzende Notation definiert man* $e(\alpha) := e^{2\pi i\alpha}$.

Lemma A.3.20.
Die Funktion $e(\alpha)$ *ist 1-periodisch, d.h. es gilt* $e(\alpha + 1) = e(\alpha)$.

Beweis
Unter Verwendung von Satz A.1.14 (iv) gilt
$e(\alpha + 1) = e^{2\pi i(\alpha+1)} = e^{2\pi i\alpha+2\pi i} = e^{2\pi i\alpha} \underbrace{e^{2\pi i}}_{=1} = e^{2\pi i\alpha} = e(\alpha).$ □

Definition A.3.21 (Ramanujan-Summe)**.**[83]
Es seien $q, n \in \mathbb{Z}$ *mit* $q \geq 1$. *Die Exponentialsumme*

$$c_q(n) := \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{an}{q}\right)$$

heißt Ramanujan-Summe.

[78] Vgl. *Schwarz W.*, 1969, S.203
[79] Vgl. *Nathanson M.B.*, 2010, S.309
[80] Vgl. *Apostol T.M.*, Theorem 2.1, 1976, S.25
[81] Vgl. *Apostol T.M.*, Theorem 2.3, 1976, S.26
[82] *Nathanson M.B.*, 2010, S.123
[83] Vgl. *Nathanson M.B.*, 2010, S.320ff.

Da $n \in \mathbb{Z} \supset \mathbb{N}$ ist die Ramanujan-Summe keine arithmetische Funktion im Sinne der getroffenen Definition A.3.5. Sie genügt aber einer multiplikativen Eigenschaft, ähnlich der Multiplikativität bei arithmetischen Funktionen.

Satz A.3.22.[84]
Die Ramanujan-Summe $c_q(n)$ ist eine multiplikative Funktion von q, d.h. für $(q, q') = 1$ gilt $c_{qq'}(n) = c_q(n)c_{q'}(n)$.

Die Grundlage der Verbindung zu $\mu(n)$ bildet die folgende Darstellung:

Satz A.3.23.[85]
Die Ramanujan-Summe $c_q(n)$ kann dargestellt werden in der Form $c_q(n) = \sum_{d|(q,n)} \mu\left(\frac{q}{d}\right) d$.

Aus dieser ergibt sich

Korollar A.3.24.[86]
Für $(q, n) = 1$ ist $c_q(n) = \mu(q)$.

Es gilt sogar eine Beziehung zwischen $\varphi(n)$, $\mu(n)$ und der Ramanujan-Summe:

Satz A.3.25.[87]
Die Ramanujan-Summe $c_q(n)$ kann dargestellt werden in der Form $c_q(n) = \frac{\mu\left(\frac{q}{(q,n)}\right)}{\varphi\left(\frac{q}{(q,n)}\right)} \cdot \varphi(q)$.

Es sollen nun Funktionen betrachtet werden, die sich auf die Verteilung der Primzahlen, also auf die Anzahl der Primzahlen unter einer gewissen Zahl x beziehen. Dies ist die Frage nach dem Wachstum der π-Funktion $\pi(x) = \#\{p : p \leq x\}$.[88] Als Zählfunktion kann diese wie folgt definiert werden:

Definition A.3.26 (π-Funktion)**.**[89]
Sei $x \in \mathbb{R}, x > 0$. Dann heißt die Funktion

$$\pi(x) := \sum_{p \leq x} 1$$

π-Funktion.

In diesem Zusammenhang stößt man unweigerlich auf die Chebyshev'sche ϑ- und ψ-Funktion.

[84] Vgl. *Nathanson M.B.*, Theorem A.23, 2010, S.321
[85] Vgl. *Nathanson M.B.*, Theorem A.24, 2010, S.321
[86] Vgl. *Nathanson M.B.*, Theorem A.24, 2010, S.321
[87] Vgl. *Nathanson M.B.*, Theorem A.25, 2010, S.322
[88] *Brüdern J.*, 1995, S.2
[89] Vgl. *Nathanson M.B.*, 2010, S.153

Definition A.3.27 (Chebyshev'sche ϑ- und ψ-Funktion)**.**[90]
Sei $x \in \mathbb{R}, x > 0$. Dann heißt die Funktion

$$\vartheta(x) := \sum_{p \leq x} \log p$$

Chebyshev'sche ϑ-Funktion und die Funktion

$$\psi(x) := \sum_{p^k \leq x} \log p$$

Chebyshev'sche ψ-Funktion.

Für diese drei Funktionen gilt die Ungleichung von Chebyshev:

Satz A.3.28 (Chebyshev)**.**[91]
Es existieren positive Konstanten c_1 und c_2, so dass $c_1 x \leq \vartheta(x) \leq \psi(x) \leq \pi(x) \log x \leq c_2 x$ für alle $x \geq 2$ gilt.

Ebenfalls wird man im Zusammenhang mit der π-Funktion auf die bekannte Riemann'sche Zetafunktion treffen.

Definition A.3.29 ((reelle) Riemann'sche ζ-Funktion)**.**[92]
Sei $s \in \mathbb{R},\ s > 1$. Dann heißt die Funktion

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

(reelle) Riemann'sche ζ-Funktion.

Bemerkung A.3.30.
Allgemein definiert man die Riemann'sche ζ-Funktion für komplexe Zahlen. Traditionell schreibt man für diese $s = \sigma + it$ mit reellen σ und t. Hier wird allerdings nur die ζ-Funktion für reelle $s > 1$ benötigt.

Für diese Funktion sollen noch folgende Produktformelen bereitgestellt werden:

Satz A.3.31.[93]
Für $s > 1$ ist $\prod_p \left(1 - \frac{1}{p^s}\right) = \frac{1}{\zeta(s)}$.

Satz A.3.32.[94]
Für $s > 1$ ist $\prod_p \left(1 + \frac{1}{p^s}\right) = \frac{\zeta(s)}{\zeta(2s)}$.

[90] Vgl. *Nathanson M.B.*, 2010, S.153
[91] Vgl. *Nathanson M.B.*, Theorem 6.3, 2010, S.155
[92] Vgl. *Scheid H.*, 1994, S.292
[93] Vgl. *Reiss K./Schmieder G.*, 2007, S.413
[94] Vgl. *Scheid H.*, Aufgabe A.24, 1994, S.323

Bemerkung A.3.33.[95]
Es ist $\zeta(2) = \frac{\pi^2}{6},\ \zeta(6) = \frac{\pi^6}{945}$ *und* $\zeta(3) \approx 1,20205... < 1,3.$

Eine arithmetische Funktion, die eine bedeutende Rolle in der Verteilung der Primzahlen hat[96], ist die von Mangoldt'sche Λ-Funktion.

Definition A.3.34 (von Mangoldt'sche Λ-Funktion)**.**[97]
Sei $n \geq 1$*. Dann heißt die Funktion*

$$\Lambda(n) := \begin{cases} \log\ p & \text{für } n = p^m \text{ ist eine Primzahlpotenz} \\ 0 & \text{sonst.} \end{cases}$$

von Mangoldt'sche Λ*-Funktion.*

Der nächste Satz zeigt, dass sich die Λ-Funktion auf natürliche Weise aus dem Hauptsatz der elementaren Zahlentheorie ergibt[98]:

Satz A.3.35.[99]
Für die natürliche Zahl $n \geq 1$ *ist* $\log n = \sum_{d|n} \Lambda(d).$

Eine Beziehung zur Chebyshev'sche ψ-Funktion formuliert der folgende Satz:

Satz A.3.36.[100]
Es ist $\psi(x) = \sum_{1 \leq m \leq x} \Lambda(m).$

Als Antwort auf die gestellte Frage nach dem Wachstum der π-Funktion soll noch der von Gauss vermutete und von Hadamard/de la Vallée-Poussin bewiesene Primzahlsatz angegeben werden.[101]

Satz A.3.37 (Primzahlsatz)**.**[102]
Für $x \to \infty$ *ist* $\pi(x) \sim \frac{x}{\log x}$*, also* $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$

Nachdem die Frage nach der Verteilung der Primzahlen aufgetreten ist, liegt es nahe auch nach der Verteilung der Primzahlen in Restklassen zu fragen. Angesichts dieser neuen Fragestellung entwickelt sich die π-Funktion weiter zu

[95] Vgl. *Reiss K./Schmieder G.*, 2007, S.412ff. und Vgl. *Schmidt A.*, 2007, S.144
[96] Vgl. *Apostol T.M.*, 1976, S.32
[97] Vgl. *Apostol T.M.*, Definition, 1976, S.32
[98] Vgl. *Apostol T.M.*, 1976, S.32
[99] Vgl. *Apostol T.M.*, Theorem 2.10, 1976, S.32
[100] Vgl. *Nathanson M.B.*, 2010, S.155
[101] Vgl. *Reiss K./Schmieder G.*, 2007, S.402
[102] Vgl. *Bundschuh P.*, Primzahlsatz, 2008, S.302

$\pi(x;q,a) = \#\{p \leq x : p \equiv a \text{ mod } q\}$.[103] Hierbei werden q und a als teilerfremd vorausgesetzt. Die weiterentwickelten Zählfunktionen erhalten dann folgende Gestalt[104]:

$$\pi(x;q,a) := \sum_{\substack{p \leq x \\ p \equiv a \ mod \ q}} 1$$

$$\vartheta(x;q,a) := \sum_{\substack{p \leq x \\ p \equiv a \ mod \ q}} \log p$$

$$\psi(x;q,a) := \sum_{\substack{n \leq x \\ n \equiv a \ mod \ q}} \Lambda(n)$$

Die Antwort auf diese Frage gibt der Dirichlet'sche Primzahlsatz:

Satz A.3.38 (Dirichlet'scher Primzahlsatz)**.**[105]
Zu gegebenen teilerfremden Zahlen a, q gibt es unendlich viele Primzahlen $p \equiv a$ mod q. Die Reihe $\sum_{p \equiv a \ mod \ q} \frac{1}{p}$ ist divergent.

Sind also a, q teilerfremd, dann enthält die Restklasse a mod q unendlich viele Primzahlen. Mit Hilfe des Primzahlsatzes lässt sich sogar zeigen, dass

$$\pi(x;q,a) \sim \frac{1}{\varphi(q)} \cdot \frac{x}{\log x}$$

gilt. Die Primzahlen verteilen sich also gleichmäßig auf die $\varphi(q)$ Restklassen mod q.[106]

In diesem Zusammenhang soll noch der Satz von Siegel-Walfisz festgehalten werden:

Satz A.3.39 (Siegel-Walfisz)**.**[107]
Sei $q \geq 1$ und $(q,a) = 1$, dann gilt für ein $C > 0$

$$\vartheta(x;q,a) = \sum_{\substack{p \leq x \\ p \equiv a \ mod \ q}} \log p = \frac{x}{\varphi(q)} + O\left(\frac{x}{(\log x)^C}\right)$$

und zwar für alle $x \geq 2$, wobei die implizite Konstante nur von C abhängig ist.

Es sei noch auf den Schwachpunkt des Satzes hingewiesen, dass die Konstante C nicht expliziet berechnet werden kann.[108] Für den hier dargestellten Beweis des Satzes von Vinogradov wird dies allerdings keine Rolle spielen.

[103] *Brüdern J.*, 1995, S.110
[104] *Schwarz W.*, 1969, S.135
[105] *Brüdern J.*, Dirichletscher Primzahlsatz, 1995, S.36
[106] Vgl.*Scheid H.*, 1994, S.354
[107] Vgl.*Nathanson M.B.*, Theorem 8.3, 2010, S.216
[108] *Brüdern J.*, 1995, S.114

Die beiden aufgeworfenen Fragen nach der Verteilung der Primzahlen sind für sich interessante Themen, die hier aber nicht weiter vertieft werden sollen. Alles was aus diesen für den Beweis des Satzes von Vinogradov benötigt wird, wurde dargestellt, sodass für eine vertiefende Betrachtung auf die Bücher von Apostol, Bundschuh, Brüdern, Davenport, Prachar, Scheid und Schwarz im Literaturverzeichnis verwiesen wird.

Im weiteren sollen zuerst noch zwei Abschätzungen und der Approximationssatz von Dirichlet betrachtet werden, bevor mit der Partiellen Summation, dem unendlichen Produkt und dem Euler-Produkt alle notwendigen Hilfsmittel dieses Abschnitts bereitgestellt sind. Die erste Abschätzung betrifft $e(\alpha)$. Vor Betrachtung dieser sind allerdings noch einige Notationen zu verabreden. Der ganzzahlige Anteil einer reellen Zahl α soll $[\alpha]$ sein, während der gebrochene Anteil durch $\{\alpha\}$ dargestellt wird. Dann gilt offensichtlich $[\alpha] \in \mathbb{Z}$, $\{\alpha\} \in [0,1)$ und $\alpha = [\alpha] + \{\alpha\}$. Sei unter $\| \alpha \|$ der Abstand der reellen Zahl α zur nächsten ganzen Zahl, also $\| \alpha \| = \min\{| \alpha - n | : n \in \mathbb{Z}\} = \min(\{\alpha\}, 1 - \{\alpha\}) \in [0, \frac{1}{2}]$ zu verstehen[109], dann gilt

Satz A.3.40.[110]
Für jedes $\alpha \in \mathbb{R}$ und $N_1, N_2 \in \mathbb{Z}$ mit $N_1 < N_2$ gilt

$$\sum_{n=N_1+1}^{N_2} e(\alpha n) \ll \min\big(N_2 - N_1, \| \alpha \|^{-1}\big).$$

Der bereits erwähnte Dirichlet'sche Approximationssatz ist eine qualitative Aussage über die Approximation reeller Zahlen durch rationale Zahlen mit kleinem Nenner.[111]

Satz A.3.41 (Approximationssatz von Dirichlet)**.**[112]
Seien $\alpha, Q \in \mathbb{R}$ und $Q \geq 1$. Dann existieren $a, q \in \mathbb{Z}$, so dass $1 \leq q \leq Q$, $(a,q) = 1$ und $\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}$.

Die Bedingung $(a,q) = 1$ ist hier so zu verstehen, dass der Bruch der beiden Zahlen vollständig gekürzt ist. Nun zu einer Abschätzung, die eine derartige Approximationsaussage voraussetzt.

Satz A.3.42.[113]
Sei $\alpha \in \mathbb{R}$. Ist $\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}$, wobei $q \geq 1$ und $(a,q) = 1$ ist, dann gilt für $U \geq 1, U \in \mathbb{R}$ und $n \in \mathbb{N}$, dass $\sum_{1 \leq k \leq U} \min\left(\frac{n}{k}, \frac{1}{\| \alpha k \|}\right) \ll \left(\frac{n}{q} + U + q\right) \log 2qU.$

Eine bestimmte Umformung der Summe von Produkten beschreibt der nächste Satz:

[109] Vgl. *Nathanson M.B.*, 2010, S.103
[110] Vgl. *Nathanson M.B.*, Lemma 4.7, 2010, S.104
[111] *Brüdern J.*, Lemma 6.4.3, 1995, S.212
[112] Vgl. *Nathanson M.B.*, Theorem 4.1, 2010, S.98
[113] Vgl. *Nathanson M.B.*, Lemma 4.10, 2010, S.108

Satz A.3.43 (Partielle Summation).[114]
Seien $u(n)$ und $f(n)$ arithmetische Funktionen und sei die Summenformel definiert durch

$$U(t) := \sum_{n \leq t} u(n).$$

Seien $a, b \in \mathbb{N}_0$ mit $a < b$. Dann ist

$$\sum_{n=a+1}^{b} u(n)f(n) = U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).$$

Seien $x, y \in \mathbb{R}$ mit $0 \leq y < x$. Ist $f(x)$ eine Funktion mit stetiger Ableitung auf $[y, x]$, dann ist

$$\sum_{y < n \leq x} u(n)f(n) = U(x)f(x) - U(y)f(y) - \int_y^x U(t)f'(t)dt.$$

Hat insbesondere $f(t)$ eine stetige Ableitung auf $[1, x]$, dann ist

$$\sum_{n \leq x} u(n)f(n) = U(x)f(x) - \int_1^x U(t)f'(t)dt.$$

Den Schluss des Abschnitts bildet nun eine kurze Einführung in die unendlichen Produkte, welche als Grundlage für das Euler-Produkt benötigt wird.
Sei $\alpha_1, \alpha_2, ..., \alpha_n, ...$ eine Folge komplexer Zahlen. Dann ist unter dem n-ten Partialprodukt in dieser Folge die Zahl $p_n = \alpha_1\alpha_2...\alpha_n = \prod_{k=1}^{n} \alpha_k$ zu verstehen. Wenn für $n \to \infty$ die Folge der n-ten Partialprokukte gegen einen Grenzwert $\alpha \neq 0$ konvergiert, dann sagt man das unendliche Produkt $\prod_{k=1}^{\infty} \alpha_k$ konvergiert und schreibt
$\prod_{k=1}^{\infty} \alpha_k = \lim_{n\to\infty} p_n = \lim_{n\to\infty} \prod_{k=1}^{n} \alpha_k = \alpha$.
Man sagt das unendliche Produkt divergiert, wenn der Grenzwert der Folge der Partialprodukte nicht existiert oder wenn dieser zwar existiert, aber den Wert Null hat. Im letzten Fall sagt man auch das unendliche Produkt divergiert gegen Null.
Sei nun $\alpha_k = 1 + a_k$. Ist das unendliche Produkt $\prod_{k=1}^{\infty} (1 + a_k)$ konvergent, so ist sicher $a_k \neq -1$ für alle k.[115] Es gilt außerdem:

Satz A.3.44.[116]
Sei $a_k \geq 0$ für alle $k \geq 1$. Das unendliche Produkt $\prod_{k=1}^{\infty} (1 + a_k)$ konvergiert genau dann, wenn die unendliche Reihe $\sum_{k=1}^{\infty} a_k$ konvergiert.

Man sagt das unendliche Produkt $\prod_{k=1}^{\infty} (1 + a_k)$ konvergiert absolut, wenn das unendliche Produkt $\prod_{k=1}^{\infty} (1 + \mid a_k \mid)$ konvergiert. Es gilt, dass Konvergenz aus absoluter Konvergenz folgt.

[114] Vgl. *Nathanson M.B.*, Theorem A.4, 2010, S.304
[115] Vgl. *Nathanson M.B.*, 2010, S.323
[116] Vgl. *Nathanson M.B.*, Theorem A.26, 2010, S.323

Satz A.3.45.[117]
Konvergiert das unendliche Produkt $\prod_{k=1}^{\infty}(1+a_k)$ *absolut, so ist es auch konvergent.*

Ein *Euler-Produkt* ist nun ein Produkt über alle Primzahlen, also ein spezielles unendliches Produkt. Zur Abkürzung schreibt man $\prod_p$, wie es oft bei Summen $\sum_p$ üblich ist.

Satz A.3.46.[118]
Sei $f(n)$ *eine multiplikative Funktion, die nicht überall Null ist. Konvergiert die Reihe* $\sum_{n=1}^{\infty} f(n)$ *absolut, dann ist*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(1 + f(p) + f(p^2) + ...\right) = \prod_p \left(1 + \sum_{k=1}^{\infty} f(p^k)\right).$$

[117] Vgl. *Nathanson M.B.*, Theorem A.27, 2010, S.324
[118] Vgl. *Nathanson M.B.*, Theorem A.28, 2010, S.325

Literaturverzeichnis

Wissenschaftliche Quellen

Aigner, Martin: *Diskrete Mathematik*, 6.Auflage, Wiesbaden: Vieweg + Teubner, 2009

Apostol, Tom M.: *Introduction to Analytic Number Theory*, 1.Auflage, New York: Springer, 1976

Brüdern, Jörg: *Einführung in die analytische Zahlentheorie*, 1.Auflage, Berlin: Springer, 1995

Bundschuh, Peter: *Einführung in die Zahlentheorie*, 6.Auflage, Berlin: Springer, 2008

Davenport, Harold: *Multiplicative Number Theory*, 3.Auflage, New York: Springer, 2000

Elstrodt, Jürgen: *Maß- und Integrationstheorie*, 5.Auflage, New York: Springer, 2007

Fischer, Wolfgang/Lieb, Ingo: *Funktionentheorie*, 24.Auflage, Wiesbaden: Vieweg, 1994

Fritzsche, Klaus: *Grundkurs Funktionentheorie*, 1.Auflage, Heidelberg: Spektrum, 2009

Gamelin, Theodore W.: *Complex Analysis*, 1.Auflage, New York: Springer, 2001

Hardy, Godfrey Harold /Wright, Edward Maitland: *An introduction to the Theory of Numbers*, 5.Auflage, Oxford: University Press, 1990

Heuser, Harro: *Lehrbuch der Analysis - Teil 1*, 17.Auflage, Wiesbaden: Vieweg + Teubner, 2009

Heuser, Harro: *Lehrbuch der Analysis - Teil 2*, 14.Auflage, Wiesbaden: Vieweg + Teubner, 2008

Heuser, Harro: *Funktionalanalysis*, 4.Auflage, Wiesbaden: Vieweg + Teubner, 2006

Holz, Michael: *Repetitorium Algebra*, 3.Auflage, Barsinghausen: Binomi-Verlag, 2010

Menzer, Hartmut: *Zahlentheorie*, 1.Auflage, München: Oldenbourg Wissenschaftsverlag, 2010

Miller, Steven /Takloo-Bighash, Ramin : *An Invitation to Modern Number Theory*, 1.Auflage, Princeton: University Press, 2006

Narkiewicz, Wladyslaw: *The Development of Prime Number Theory - From Euclid to Hardy and Littlewood*, 1.Auflage, Berlin: Springer, 2000

Nathanson, Melvyn B.: *Additive Number Theory - The Classical Bases*, 2.Auflage, New York: Springer, 2010

Prachar, Karl: *Primzahlverteilung*, 1.Auflage, Berlin: Springer, 1957

Reiss, Kristina/Schmieder Gerald: *Basiswissen Zahlentheorie - Eine Einführung in Zahlen und Zahlenbereiche*, 2.Auflage, Berlin: Springer, 2007

Ribenboim, Paulo: *Die Welt der Primzahlen - Geheimnisse und Rekorde*, 2.Auflage, Berlin: Springer, 2011

Scheid, Harald: *Zahlentheorie*, 2.Auflage, Mannheim: Bibliographisches Institut, 1994

Schwarz, Wolfgang: *Einführung in Methoden und Ergebnisse der Primzahltheorie*, 1.Auflage, Mannheim: Bibliographisches Institut, 1969

Schmidt, Alexander: *Einführung in die algebraische Zahlentheorie*, 1.Auflage, Berlin: Springer, 2007

Schulze-Pillot, Rainer: *Einführung in und Algebra und Zahlentheorie*, 2.Auflage, Berlin: Springer, 2008

Steger, Angelika: *Diskrete Strukturen*, 2.Auflage, Berlin: Springer, 2007

Tittmann, Peter: *Einführung in die Kombinatorik*, 1.Auflage, Berlin: Spektrum Akademischer Verlag, 2000

Vaughan, Robert Charles: *The Hardy-Littlewood Method*, 2.Auflage, Cambridge: University Press, 1997

Vinogradov, Iwan Matwejewitsch: *The Method of Trigonometric Sums in the Theory of Numbers*, 1.Auflage, New York: Dover Publications, 2004

Wolke, Dieter: *Das Goldbach'sche Problem*, *Mathematische Semesterberichte 41*, Berlin: Springer-Verlag 1994, 55-67

Zygmund, Antoni: *Trigonometric Series*, 2.Auflage, Cambridge: University Press, 1959

Internetquellen

http://arxiv.org/abs/1201.6656, 16.03.2013, 14Uhr10

http://arxiv.org/pdf/1201.6656v4.pdf, 16.03.2013, 14Uhr10

https://dmv.mathematik.de/aktuell/aktuell/archiv/1205.html, 12.03.2013, 22Uhr25

http://mathworld.wolfram.com/GoldbachConjecture.html, 13.03.2013, 19Uhr50

http://www.math.dartmouth.edu/euler/correspondence/letters/OO0765.pdf, 28.05.2013, 10Uhr

http://www.math.dartmouth.edu/euler/correspondence/letters/OO0766.pdf, 28.05.2013, 10Uhr

http://www.spiegel.de/wissenschaft/mensch/primzahlraetsel-loesung-der-goldbachschen-vermutung-rueckt-naeher-a-833216.html, 12.06.2013, 11Uhr30

http://www.spiegel.de/wissenschaft/mensch/beweis-fuer-schwache-goldbachsche-vermutung-a-901111.html, 24.07.2013, 17Uhr

Technische Hochschule Mittelhessen

Campus Friedberg
Wilhelm-Leuschner-Str. 13
61169 Friedberg

www.thm.de