BACHELORARBEIT

Primzahlen in arithmetischen Progressionen und der Satz von Dirichlet

Verfasser
Gerald Eder

Wien, im Februar 2014

Studienkennzahl lt. Studienblatt:	A 033621
Studienrichtung lt. Studienblatt:	Mathematik
Betreuer:	Assoz. Prof. Dr. Dietrich Burde

Inhaltsverzeichnis

1 Einleitung

Die vorliegende Arbeit spannt den Bogen von Euklids Beweis über die Existenz von unendlich vielen Primzahlen (als Teilmenge der natürlichen Zahlen) bis hin zu Vermutungen über die Existenz von Primidealen in Zahlkörpern.
Zunächst wird der Beweis von Euklid noch einmal wiederholt und ein allgemeines Prinzip herausgeschält, das sich auf Primzahlen bestimmter Form anwenden lässt. Dabei werden auch die Grenzen des Prinzips dieses *„Euklidischen Beweises“* aufgezeigt und ein Kriterium von Murty und Thayn formuliert, warum dieses etwa auf Primzahlen der Form $4n + 3$ angewandt werden kann, aber bei der Folge $5n + 2$ versagt.
Lejeune Dirichlet gelang es bereits 1837 einen vollständigen Beweis für alle arithmetischen Progressionen mit teilerfremden Parametern zu geben. Der Zugang, den er gewählt hat, wird in Kapitel 3 mit der Einführung von Dirichlet-Charakteren, L-Reihen und weiterer Funktionen sowie für den Beweis nötiger Resultate vorbereitet. Der Beweis wird schließlich in Kapitel in einer moderneren Version von Shapiro aus dem Jahr 1950 geführt, der ein Resultat von Franz Mertens verwendet, das zu Dirichlets Lebzeiten noch nicht bekannt war. Dieses wird ebenfall in Kapitel 3 gezeigt.
Der bewiesene Satz von Dirichlet ist, wenn man so will, ein Spezialfall in zwei Richtungen. Zunächst behandelt er nur lineare Progressionen. Mit der Verallgemeinerung auf polynomiale Progressionen und der damit verbundenen Vermutung von Bunyakowsky beschäftigt sich der erste Teil des letzten Kapitels. Der zweite Teil von Kapitel 5 behandelt die Erweiterung des Primzahlbegriffs auf Primideale in Zahlkörpern sowie die Verbindung zum Dichtigkeitssatz von Tschebotareff. Dabei wird aber nur ein kurzer Überblick gegeben, da das Hauptaugenmerk auf den Satz von Dirichlet gerichtet ist und alles weitere den Rahmen dieser Arbeit sprengen würde.

2 Die Unendlichkeit der Primzahlen und Euklidische Beweise

Bereits Euklid konnte etwa 300 v. Chr. zeigen, dass es unendlich viele Primzahlen gibt. Genauer formulierte und bewies er in seinem berühmten Werk *Die Elemente* folgenden Satz:

Satz 2.1. Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen.

Beweis. Angenommen, es gibt nur endlich viele Primzahlen $p_1, p_2, ..., p_n$. Bildet man die Zahl $N := p_1 p_2 ... p_n + 1$, ist offensichtlich, dass $p_i \nmid N$, da $p_i \nmid 1 \; \forall i \in \{1, ..., n\}$. Also ist N entweder selbst prim oder aus Primzahlen zusammengesetzt, die nicht zu den p_i gehören. □

Auf ähnliche Weise lässt sich auch die Unendlichkeit von Primzahlen von bestimmter Gestalt bestimmen, wenn man die Zahl N anpasst; so gilt etwa

Satz 2.2. Es gibt unendlich viele Primzahlen der Form $4n + 3$.

Beweis. Angenommen es gibt nur endlich viele Primzahlen der Gestalt $4n + 3$. Man betrachtet die Zahl $N := 4(p_1 p_2 ... p_r) - 1$. Da sowohl das Produkt zweier Zahlen der Form $4k + 1$ als auch der Form $4k + 3$ die Gestalt $4k + 1$ hat, hat N die Form $4k + 3$. Die Primfaktoren können daher auch nicht alle die gleiche Form haben, es muss also mindestens einen Faktor $4m + 3$ geben, der N teilt und keiner von den p_i ist, da sonst auch $(4m + 3) \mid 1$ gelten würde. Dies ist aber nicht möglich. Daher existieren unendlich viele Primzahlen der Form $4n + 3$. □

Wir wollen nun untersuchen, für welche Zahlen man ähnliche Beweise geben kann. Dazu betrachten wir arithmetische Folgen mit teilerfremden Parametern:

Definition 2.3 (arithmetische Progression)**.** Eine *arithmetische Progression* ist eine Folge $a(n) = kn + l$ wobei $k, l \in \mathbb{N}$ fix gewählt sind mit $(k, l) = 1$ und n alle natürlichen Zahlen durchläuft.

Der Fall $(k, l) > 1$ wird ausgeschlossen, da dann höchstens eine Primzahl auftritt. Somit ist dieser Fall für diese Arbeit nicht von Bedeutung.

2.1 Euklidische Beweise - Eine Definition

Eine präzise Definition findet sich in **[MuTh]**:

Definition 2.4 („Euklidischer Beweis“)**.** Ein *„Euklidischer Beweis“* für eine arithmetische Progression $a_n = kn + l$ besteht darin ein Polynom $f \in \mathbb{Z}[x]$ zu finden, dessen Primteiler alle - bis auf endlich viele Ausnahmen - entweder von der Form $kn + 1$ oder $kn + l$ sind.

In den obigen Fällen sind diese Polynome $f_1(x) = x + 1$ bzw. $f_2(x) = 4x - 1$. Weitere Beispiele sind $f_3(x) = 4x^2 + 3$ für Primzahlen der Form $6n + 1$ oder $f_4(x) = x^4 - x^3 + 2x^2 + 1$ für die Progression $15n + 4$.
Die sich nun stellende Frage ist, ob es für alle arithmetischen Progressionen einen Euklidischen Beweis gibt oder anders ausgedrückt, ob sich der Satz von Dirichlet vollständig euklidisch beweisen lässt. **[MuTh]** liefern mit folgendem Theorem die Antwort und gleichzeitig ein Kriterium für welche Progressionen dies möglich ist.

2.2 Die Existenz von Euklidischen Beweisen

Satz 2.5. Für eine arithmetische Progression $\equiv l \mod k$ existiert ein Euklidischer Beweis (d.h. ein Polynom, das der obigen Definition entspricht) genau dann, wenn $l^2 \equiv 1 \mod k$.

Um dieses Kriterium anzuwenden, reicht es grundsätzlich zu zeigen, dass dies eine hinreichende Bedingung ist. Dafür sind einige Resultate von Nagell und Schur nötig. Für die in den Beweisen benötigten Resultate der Algebra, siehe beispielsweise **[JSch]**.

Lemma 2.6 (Schur)**.** Ein nicht konstantes Polynom $f \in \mathbb{Z}[x]$ besitzt unendlich viele Primteiler.

Beweis. Ist $f(0) = 0$, dann gilt $p \mid f(0)$ für jede Primzahl p und f hätte trivialerweise unendlich viele Primteiler. Sei deshalb $f(0) = c \neq 0$. Die Werte ± 1 können nur endlich viele Urbilder besitzen, daher existiert zumindest ein Primteiler, das heißt eine Primzahl p mit $p \mid f(n)$ für ein $n \in \mathbb{Z}$. Nehmen wir nun an, es gibt nur endlich viele solcher Primteiler, nämlich $p_1, p_2, ..., p_k$ und sei $Q = p_1 p_2 ... p_k$ das Produkt dieser Primzahlen. Dann existiert ein Polynom $g \in \mathbb{Z}[x]$ mit folgenden Eigenschaften:

1. $f(Qcx) = cg(x)$
2. $g(x) = 1 + c_1x + c_2x^2 + ...$
3. g besitzt aus demselben Grund wie f mindestens einen Primteiler p.
4. $Q \mid c_i \, \forall i$

Da p Primteiler von g ist, teilt p auch f, aber nicht Q, da p sonst auch 1 teilen würde. Das ist ein Widerspruch, also existieren unendlich viele Primteiler von f. □

Im folgenden bezeichnet ζ stets eine k-te Einheitswurzel und K sei die Galois-Erweiterung $\mathbb{Q}(\zeta)$ über $\mathbb{Q}$. Die zugehörige Galoisgruppe ist isomorph zur Gruppe $(\mathbb{Z}/k\mathbb{Z})^\times$.

Lemma 2.7 (Nagell)**.** Es seien $f, g \in \mathbb{Z}[x]$ nicht konstant und $P(f), P(g)$ die Mengen der Primteiler von f bzw. g. Dann enthält $P(f) \cap P(g)$ unendlich viele Elemente.

Beweis. Sei $f(\alpha) = g(\beta) = 0$. Nach einem Satz von Dedekind (siehe **[MuEs]**) ist p ein Primteiler von f, wenn p einen linearen Primidealfaktor in der Erweiterung $\mathbb{Q}(\alpha)$ besitzt. Eine analoge Aussage gilt auch für g. Wir betrachten den Zahlkörper $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ für ein $\theta \in \mathcal{O}_K$, dem Ring der ganzen Zahlen in K. Sei h das Minimalpolynom von θ, dann folgt aus dem Satz von Schur, dass es unendlich viele Primzahlen gibt, die einen linearen Primidealfaktor in $\mathbb{Q}(\alpha, \beta)$ und damit auch in $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\beta)$ besitzen. Damit existieren unendlich viele Primteiler für f und g. □

Lemma 2.8 (Schur)**.** Sei H eine Untergruppe der primen Restklassengruppe $(\mathbb{Z}/k\mathbb{Z})^\times$. Dann existiert ein irreduzibles Polynom $f \in \mathbb{Z}[x]$, dessen Primteiler bis auf endlich viele Ausnahmen in den Restklassen von H enthalten sind.

Beweis. Sei $\mathbb{Q}(\eta)$ der Fixkörper von H und $\eta = h(\zeta)$ für ein $h \in \mathbb{Z}[x]$. Seien weiters $m_1, ..., m_s$ Repräsentanten der Nebenklassen von H in $(\mathbb{Z}/k\mathbb{Z})^\times$.
Wir setzen $\eta_i = h(\zeta^{m_i}), 1 \leq i \leq s$, und nehmen an, die η_i wären nicht alle verschieden. Sei $\sigma_i \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ ein Automorphismus, der ζ auf ζ^i abbildet. Dann ist $\sigma_{m_i}(\eta) = \sigma_{m_j}(\eta)$ für $m_i \neq m_j$. Damit gilt auch $\sigma_{m_i m_j^{-1}}(\eta) = \eta$. Daraus folgt aber, dass m_i und m_j dieselbe Nebenklasse repräsentieren, was ein Widerspruch zur Annahme ist. Also sind die η_i die verschiedenen Konjugationen von η.
Wir definieren nun

$$f(x) = \prod_{i=1}^{s}(x - \eta_i). \tag{2.1}$$

Wegen der obigen Argumentation ist f irreduzibel in $\mathbb{Q}(x)$.
Sei nun p ein Primteiler von f mit $p \nmid k$ und $p \nmid D(f)$, wobei $D(f)$ die Diskriminante

von f ist. Da p ein Primteiler von f ist, existiert eine Zahl a, sodass

$$f(a) = \prod_{i=1}^{s}(a - \eta_i) \equiv 0(p). \tag{2.2}$$

Sei nun $\mathcal{P}$ ein Primideal, das (p) teilt. Dann gilt $\mathcal{P} \mid (a - \eta_i)$ für zumindest ein i. Wegen $a^p \equiv a(\text{mod } p)$ gilt auch $a^p \equiv a(\text{mod } \mathcal{P})$ und $h(x)^p \equiv h(x^p)(\text{mod } \mathcal{P})$. Damit erhalten wir

$$h(\zeta^{m_i}) \equiv \eta_i \equiv a \equiv a^p \equiv \eta_i^p \equiv h(\zeta^{m_i})^p \equiv h(\zeta^{pm_i})(\text{mod } \mathcal{P}). \tag{2.3}$$

Aus obiger Kongruenz folgt $\mathcal{P} \mid (h(\zeta^{m_i}) - h(\zeta^{pm_i}))$. Wegen $p \nmid k$ gilt $(k, pm_i) = 1$, also ist $h(\zeta^{pm_i})$ eines der η_i.
Ist nun $h(\zeta^{pm_i}) \neq h(\zeta^{m_i})$, so teilt $\mathcal{P}$ die Diskriminante, aber $p \mid D(f)$. Das ist ein Widerspruch zur Wahl von p.
Also gilt $h(\zeta^{pm_i}) = h(\zeta^{m_i})$ und damit fixiert σ_p die Erweiterung $\mathbb{Q}(\eta_i)$. Da aber $\mathbb{Q}(\eta_i)$ eine Galoiserweiterung ist und daher $\mathbb{Q}(\eta_i) = \mathbb{Q}(\eta)$, fixiert σ_p auch $\mathbb{Q}(\eta)$. Das heißt, p ist Teil einer Restklasse von H. □

Das folgende Lemma zeigt, dass auch die Umkehrung gilt.

Lemma 2.9 (Schur)**.** Sei f wie in Lemma 2.8, dann wird f von jeder Primzahl aus einer beliebigen Restklasse von H geteilt.

Beweis. Sei dazu p eine Primzahl aus einer beliebigen Restklasse von H, dann fixiert σ_p die Erweiterung $\mathbb{Q}(\eta)$ und es ist

$$\eta^p \equiv h(\zeta)^p \equiv h(\zeta^p) \equiv h(\zeta) \equiv \eta(\text{mod } p). \tag{2.4}$$

Damit gilt auch für jedes Primideal $\mathcal{P}$, das p teilt, dass $\eta^p \equiv \eta(\text{mod } \mathcal{P})$.
Da $\mathcal{O}_K$ ein Dedekindring ist, ist $\mathcal{P}$ ein maximales Ideal und der Faktorring $\mathcal{O}_K/\mathcal{P}$ damit ein Körper: Daher hat die Gleichung $x^p - x = 0$ höchstens p Lösungen. Das heißt, es existiert eine ganze Zahl a, sodass $\eta \equiv a(\text{mod } \mathcal{P})$. Damit wird $f(a)$ von $\mathcal{P}$ geteilt und damit auch von p, was zu zeigen war. □

Wählt man $H = \{1\}$ und betrachtet das k-te Kreisteilungspolynom ϕ_k, dann sind die einzigen Primzahlen, die die Diskriminante von ϕ_k teilen, jene, die k teilen. Da es nur endlich viele Primzahlen gibt, die k teilen, sind alle anderen (der unendlich vielen) Primteiler $\equiv 1(k)$.
Damit ist bereits für alle arithmetischen Progressionen $a(n) = kn + 1$, $n \in \mathbb{Z}$, gezeigt, dass darin unendlich viele Primzahlen $\equiv 1(k)$ enthalten sind. Nun betrachten wir den Fall von Primzahlen, die nicht kongruent 1 modulo k sind.

Satz 2.10. Ist $l^2 \equiv 1 \mod k$ für eine arithmetischen Progression $a_n = kn + l$, dann kann Euklidisch gezeigt werden, dass unendlich viele Primzahlen der Form $kn + l$ existieren.

Beweis. Dazu betrachten wir die Untergruppe $H = \{1, l\}$ der Gruppe $(\mathbb{Z}/k\mathbb{Z})^\times$ und wenden die bisher gezeigten Resultate an. Sei L der Fixkörper von H und $h(\zeta) = (u - \zeta)(u - \zeta^l)$ mit einem Parameter $u \in \mathbb{Z}$.
Wählt man u so, dass für alle Repräsentanten $m_i, 1 \leq i \leq s$ der Restklassen von H alle $h(\zeta^{m_i})$ verschieden sind, dann gilt $L = \mathbb{Q}(h(\zeta))$.
Wir setzen $\eta = h(\zeta)$ und wenden das Lemma von Nagell an. So erhalten wir ein Polynom, deren Primteiler bis auf endlich viele $\equiv 1(k)$ oder $\equiv l(k)$ sind, nämlich

$$f(x)^2 = \prod_{(a,k)=1} (x - (u - \zeta^a)(u - \zeta^{la})). \tag{2.5}$$

Wir stellen fest, dass $f(0)$ genau dem k-ten Kreisteilungspolynom $\phi(u)$ entspricht und wählen u als Vielfaches von k, sodass $f(0) = \phi_k(u) \equiv 1(k)$. Die Existenz eines solchen u folgt aus dem vorangegangenen Lemma und der Folgerung, dass nur endlich viele $\phi_k(x) \not\equiv 1(k)$ sind.
Nun wählen wir eine Primzahl $p \equiv l(k)$, sodass $p \nmid D(f)$ und mit dem Lemma von Schur können wir eine Zahl b finden mit $p \mid f(b)$, aber $p^2 \nmid f(b)$. Denn gälte $p^2 \mid f(b)$, dann wäre $f(b + p) = f(b) + pf'(b) \equiv pf'(b) (\mod p^2)$. Weil aber $p \nmid D(f)$, kann f keine doppelte Nullstelle modulo p haben und somit ist $f'(b) \not\equiv 0(p)$. Das heißt, aus $f(b) \equiv 0(p^2)$ folgt $f(b + p) \not\equiv 0(p^2)$.
Wir nehmen an, dass es nur endlich viele Primzahlen $p_i \equiv l(k)$ gibt, nämlich $p_1, ..., p_m$. Die Primfaktoren der Diskriminante $D(f)$ bezeichnen wir mit $q_1, ..., q_t$ und bilden die Zahl $Q := p_1 p_2 ... p_m q_1 q_2 ... q_t$. Mithilfe des Chinesischen Restsatzes lösen wir das System von Kongruenzen

$$\begin{aligned} c &\equiv b \mod p^2 \\ c &\equiv 0 \mod kQ \end{aligned} \tag{2.6}$$

Damit finden wir c so, dass $f(c) \equiv f(b) (\mod p^2)$ und $f(c) \equiv 0 (\mod kQ)$ und nach dem Lemma von Schur besitzt f nur jene Primzahlen als Teiler, die auch k teilen, die Diskriminante von f teilen oder $\equiv 1(k)$ oder $\equiv l(k)$ sind. Da aber $f(0) = \phi_k(u)$ und damit nur durch alle Primzahlen $\equiv 1(k)$ teilbar ist, ist $f(c)$ nur von Primzahlen $\equiv 1(k)$ und $\equiv l(k)$ teilbar. Wegen $p^2 \nmid f(c)$ ist $f(c) \equiv l(k)$. Da aber $f(0) \equiv f(c) \equiv 1(k)$ ist, ergibt sich ein Widerspruch. Also muss es unendlich viele Primzahlen der Form $kn + l$ geben. □

Der Beweis liefert mit (2.5) auch eine Formel um Polynome zu bestimmten Progressionen zu finden.

Die andere Richtung zeigt schließlich, dass jedes Polynom, das die für einen Euklidischen Beweis geforderten Eigenschaften erfüllt, einer Progression zugeordnet werden kann, für die $l^2 \equiv 1 \mod k$ gilt.
Damit kann der Satz von Dirichlet also nicht vollständig euklidisch bewiesen werden, denn sogar für einfach aussehende Beispiele wie $a_n = 5n + 2$ kann kein passendes Polynom gefunden werden. Für einen vollständigen Beweis, wie er in Kapitel 4 geführt wird, werden also andere Hilfsmittel benötigt. Diese beruhen allerdings auf einem völlig anderen Zugang als jener Euklids, wie das folgende Kapitel zeigt.

3 Die Methode von Dirichlet

Die Idee zum Beweis aus dem Jahr 1837 beruht darauf zu zeigen, dass die Summe $\sum_{p \equiv l(k)} \frac{\log p}{p}$ divergiert. Das ist ein ähnliches Argument, wie jenes von Euler, um die Unendlichkeit der Primzahlen zu zeigen. Dirichlets revolutionärer Ansatz besteht darin, die Primzahlen einer bestimmten arithmetischen Progression sozusagen einzufärben, um sie danach aus der oben genannten Summe zu isolieren und deren Divergenz zu zeigen.
Um diese „Einfärbung“ vorzunehmen, benutzte Dirichlet so genannte Charaktere, die in diesem Kapitel ausführlich behandelt werden.

3.1 Arithmetische Funktionen und Möbius-Inversion

Arithmetische Funktionen bilden eine wichtige Grundlage für den im nächsten Kapitel geführten Beweis und treten allgemein in der Zahlentheorie an vielen Stellen auf.
Wir wollen an dieser Stelle nur die wichtigsten Eigenschaften und Funktionen behandeln, die im weiteren Verlauf benötigt werden, eine ausführliche Behandlung findet man in **[Ap]** und **[Br]**.

Definition 3.1 (Arithmetische Funktion)**.** Eine Funktion $f : \mathbb{N} \to M, M \subseteq \mathbb{C}$ heißt *arithmetische* oder *zahlentheoretische Funktion*.

Wie man leicht durch Nachprüfen der Ringaxiome zeigen kann, gilt für die Menge $\mathcal{A}$ der arithmetischen Funktionen:

Satz 3.2. $(\mathcal{A}, +, *)$ ist ein kommutativer Ring mit Einselement, wobei das neutrale Element gegeben ist durch

$$I(n) = \begin{cases} 1 & \text{falls } n = 1, \\ 0 & \text{falls } n \geq 2. \end{cases}$$

Die Addition $+$ ist die übliche Addition von Funktionen und die Multiplikation ist gegeben durch die (Dirichlet-) Faltung

$$f * g(n) = \sum_{d|n} f(d) g(n/d).$$

Ein Element $f \in \mathcal{A}$ ist genau dann eine Einheit, wenn $f(1) \neq 0$.

Nun betrachten wir drei spezielle Elemente aus dem Ring der arithmetischen Funktionen, die im weiteren Verlauf noch eine Bedeutung haben.

Definition 3.3 (Euler'sche φ-Funktion)**.** Die *Euler'sche φ-Funktion* ist für ein $n \in \mathbb{N}$ gegeben durch

$$\varphi(n) = \sum_{\substack{(n,k)=1 \\ k \leq n}} 1. \tag{3.1}$$

Die φ-Funktion zählt also die zu n teilerfremden natürlichen Zahlen kleiner n und bestimmt damit gleichzeitig die Kardinalität des primen Restsystems $\mod n$.

Definition 3.4 (von Mangoldt-Funktion)**.** Für jede natürliche Zahl n ist die *von Mangoldt-Funktion* gegeben durch

$$\Lambda(n) = \begin{cases} \log p & \text{falls } n = p^m \text{ für eine Primzahl } p \text{ und } m \geq 1, \\ 0 & \text{sonst.} \end{cases} \tag{3.2}$$

Definition 3.5 (Möbius-Funktion)**.** Sei $n \in \mathbb{N}$ und besitze die Primfaktorzerlegung $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$. Dann ist die *Möbius-Funktion* μ gegeben durch

$$\mu = \begin{cases} 1 & \text{falls } n = 1, \\ 0 & \text{falls } n \text{ nicht quadratfrei,} \\ (-1)^r & \text{falls } a_i = 1 \forall i \in \{1, 2, .., k\} \end{cases} \tag{3.3}$$

Mit diesen Funktionen können weitere für den Beweis nützliche Resultate hergeleitet werden.
Im folgenden bezeichnet f stets eine auf der positiven x-Achse definierte reell- oder komplexwertige Funktion mit $f(x) = 0$ für $0 < x < 1$. Zunächst betrachten wir die Verknüpfung $\circ$, die definiert ist durch

$$\alpha \circ f = \sum_{n \leq x} \alpha(n) f(x/n), \tag{3.4}$$

wobei α eine beliebige arithmetische Funktion ist. Man kann diese Verknüpfung als *verallgemeinerte Faltung* bezeichnen, da die Einschränkung auf die natürliche Zahlen genau der Faltung $*$ entspricht, falls f für alle nicht-ganzzahligen Argumente verschwindet. Diese Verknüpfung ist aber im allgemeinen weder assoziativ noch kommutativ, jedoch besteht ein sehr nützlicher Zusammenhang zwischen $\circ$ und der Faltung $*$.

Lemma 3.6. Für zwei arithmetische Funktionen α, β gilt

$$\alpha \circ (\beta \circ f) = (\alpha * \beta) \circ f. \tag{3.5}$$

Beweis.

$$\begin{aligned} \alpha \circ (\beta \circ f)(x) &= \sum_{n \leq x} \alpha(n) \sum_{m \leq x/n} \beta(m) f\left(\frac{x}{mn}\right) = \sum_{mn \leq x} \alpha(n)\beta(m) f\left(\frac{x}{mn}\right) \\ &= \sum_{k \leq x} \left(\sum_{n|k} \alpha(n)\beta\left(\frac{k}{n}\right) \right) f\left(\frac{x}{k}\right) = \sum_{k \leq x} (\alpha * \beta)(k) f\left(\frac{x}{k}\right) \\ &= (\alpha * \beta) \circ f(x). \end{aligned} \tag{3.6}$$

□

Wir bemerken außerdem, dass das neutrale Element bezüglich $*$ auch ein linksneutrales Element bezüglich $\circ$ ist, denn

$$(I \circ f)(x) = \sum_{n \leq x} \left\lfloor \frac{1}{n} \right\rfloor f\left(\frac{x}{n}\right) = f(x). \tag{3.7}$$

Damit können wir nun die verallgemeinerte Inversionsformel beweisen.

Satz 3.7 (Allgemeine Inversionsformel)**.** Falls $\alpha \in \mathcal{A}$ ein inverses Element $\alpha^{-1} \in \mathcal{A}$ besitzt, so gilt

$$g(x) = \sum_{n \leq x} \alpha(n) f\left(\frac{x}{n}\right) \Leftrightarrow f(x) = \sum_{n \leq x} \alpha^{-1}(n) g\left(\frac{x}{n}\right) \tag{3.8}$$

Beweis. Sei $g = \alpha \circ f$, dann ist

$$\alpha^{-1} \circ g = \alpha^{-1} \circ (\alpha \circ f) = (\alpha^{-1} * \alpha) \circ f = I \circ f = f.$$

Die Umkehrung folgt analog mit $f = \alpha^{-1} \circ g$. □

Wählt man im obigen Fall $\alpha^{-1}(n) = \mu(n)\alpha(n)$, so erhält man die

Satz 3.8 (Allgemeine Möbius-Inversionsformel)**.** Für eine vollständig multiplikative Funktion $\alpha \in \mathcal{A}$ gilt

$$g(x) = \sum_{n \leq x} \alpha(n) f\left(\frac{x}{n}\right) \Leftrightarrow f(x) = \sum_{n \leq x} \mu(n)\alpha(n) g\left(\frac{x}{n}\right). \tag{3.9}$$

3.2 Charaktere

Definition 3.9 (Charakter)**.** Sei G eine Gruppe, dann heißt eine auf G definierte komplexwertige Funktion f *Charakter auf* G, falls f nicht identisch 0 ist und $f(ab) = f(a)f(b) \forall a, b, \in G$ gilt.

Charaktere besitzen eine Reihe von Eigenschaften, die im folgenden genannt werden. Die Nachprüfung erfolgt in einigen Fällen durch einfache Rechnung und wird daher hier nicht ausgeführt, findet sich aber beispielsweise in **[Ap]**.

Lemma 3.10 (Eigenschaften von Charakteren)**.** *G sei eine endliche Gruppe, dann gilt*

(i) Ist G eine endliche Gruppe mit neutralem Element e, dann gilt $f(e) = 1$ und $f(g)$ ist für alle $g \in G$ eine n-te Einheitswurzel.

(ii) Ist G abelsch und besitzt n Elemente, so gibt es genau n verschiedene Charaktere auf G.

(iii) Ist G abelsch, bilden die Charaktere mit der Operation $f_i f_j(g) := f_i(g) f_j(g) \forall g \in G$ eine multiplikative Gruppe $\widehat{G}$. Das neutrale Element dieser Gruppe ist der so genannte *Hauptcharakter* $f_1 := 1 \forall g \in G$ und $f^{-1} = {}^1/_f$.

(iv) Da stets $|f(g)| = 1$ gilt, entspricht der Kehrtwert der komplex-konjugierten, d.h. $f(g)^{-1} = {}^1/_{f(g)} = \overline{f}(g) = \overline{f(g)}$

Eine wichtige Eigenschaft von Charakteren ist die Orthogonalität. Diese spielt auch für Dirichlet-Charaktere eine wichtige Rolle und wird den Ausgangspunkt des Beweises für die Unendlichkeit der Primzahlen in arithmetischen Progressionen bilden. Deshalb wollen wir diese auch etwas ausführlicher behandeln.
Dabei werden dieselben Notationen verwendet, wie sie obigen Lemma eingeführt wurden.
Für die Gruppen $G \cong \widehat{G}$ gelten folgende Beziehungen:

Lemma 3.11. Sei G eine endliche abelsche Gruppe, $\widehat{G} \cong G$ die Charaktergruppe. Dann gilt für alle $g \in G$ und $f \in \widehat{G}$

$$\sum_{f \in \widehat{G}} f(g) = \begin{cases} n & g = e \\ 0 & \text{sonst.} \end{cases} \tag{3.10}$$

Beweis. Wir betrachten zuerst den einfachen Fall $g = e$. Dann gilt $f(e) = 1 \, \forall f \in \widehat{G}$ und die Summe über alle f ergibt klarerweise n.

Im Fall $g \neq e$ gibt es einen Charakter $\tilde{f}$ mit $\tilde{f}(g) \neq 1$ und für die Summe gilt aufgrund der Abgeschlossenheit von $\widehat{G}$ und der Multiplikativität der Charaktere

$$\sum_{f \in \widehat{G}} f(g) = \sum_{f \in \widehat{G}} f\tilde{f}(g) = \sum_{f \in \widehat{G}} f(g)\tilde{f}(g) = \tilde{f} \sum_{f \in \widehat{G}} f(g). \tag{3.11}$$

Aufgrund der Annahme $\tilde{f} \neq 1$ muss also $\sum_f = 0$ gelten. □

Lemma 3.12. Sei $\widehat{G}$ die Charaktergruppe einer endlichen abelschen Gruppe G. Dann gilt für alle $f \in \widehat{G}$

$$\sum_{g \in G} f(g) = \begin{cases} n & f = f_1 \\ 0 & \text{sonst.} \end{cases} \tag{3.12}$$

Beweis. Sei zunächst $f = f_1$. Wegen $f_1(g) = 1 \, \forall g \in G$ und $|G| = n$ ist die Behauptung offensichtlich erfüllt.
Sei also $f \neq f_1$. Da f nicht der Hauptcharakter ist, existiert ein $h \in G$ mit $f(h) \neq 1$ und mit g durchläuft auch das Produkt gh die ganze Gruppe. Also gilt

$$\sum_{g \in G} f(g) = \sum_{g \in G} f(gh) = \sum_{g \in G} f(g)f(h) = f(h) \sum_{g \in G} f(g). \tag{3.13}$$

Da $f(h) \neq 1$ gilt, kann die Gleichung nur erfüllt sein, falls die Summe 0 ist. □

Ersetzt man nun in (3.10) g durch $g^{-1}h$ und in (3.12) f durch $\overline{f'}f$, so erhält man den folgenden

Satz 3.13. Für $g, h \in G$ und $f, f' \in \widehat{G}$ gelten

$$\sum_{g \in G} \overline{f'}(g)f(g) = \begin{cases} n & \text{falls } f = f', \\ 0 & \text{sonst,} \end{cases} \tag{3.14}$$

$$\sum_{f \in \widehat{G}} \overline{f}(g)f(h) = \begin{cases} n & \text{falls } g = h, \\ 0 & \text{sonst.} \end{cases} \tag{3.15}$$

Wählen wir nun für G ein primes Restsystem, nämlich $(\mathbb{Z}/q\mathbb{Z})^\times$ für ein festes $q \in \mathbb{N}$, dann ist $|G| = \varphi(q)$. Die Charaktere auf G können damit auf ganz $\mathbb{Z}$ fortgesetzt werden und wir erhalten folgende Definition:

Definition 3.14 (Dirichlet-Charakter modulo q)**.** Für einen Charakter auf $G = (\mathbb{Z}/q\mathbb{Z})^\times$ gilt

$$\chi(n) = \begin{cases} f(n + q\mathbb{Z}) & \text{falls } (n, q) = 1, \\ 0 & \text{falls } (n, q) > 1. \end{cases} \tag{3.16}$$

und man bezeichnet $\chi(n)$ als *Dirichlet-Charakter modulo q*. Ein Dirichlet-Charakter ist weiterhin vollständig multiplikativ und q-periodisch.
Aufgrund der Isomorphie zu G existieren genau $\varphi(q)$ verschiedene Charaktere $\mod q$.

Betrachtet man nun die oben gezeigten Charakterrelationen für die eben definierten Dirichlet-Charaktere, erhält man die für den Beweis des Dirichlet'schen Satzes sehr wichtige Orthogonalitätseigenschaft.

Satz 3.15 (Orthogonalitätseigenschaft für Dirichlet-Charaktere modulo q)**.** Für $(q, a) = 1$ gilt

$$\sum_{\chi \in \widehat{G}} \overline{\chi}(a)\chi(n) = \begin{cases} \varphi(q) & \text{falls } n \equiv a \mod q, \\ 0 & \text{sonst.} \end{cases} \tag{3.17}$$

3.3 Reihen mit Charakteren

Wir kehren noch einmal zurück zum Ring $(\mathcal{A}, +, *)$ der arithmetischen Funktionen. Jeder solchen Funktion $a \in \mathcal{A}$ kann eine *formale Dirichletreihe* zugeordnet werden. Dazu führen wir eine Variable s ein, bilden die Summe

$$\sum_{n=1}^{\infty} a(n)n^{-s}$$

und finden beim Multiplizieren zweier solcher formaler Dirichletreihen

$$\sum_{n=1}^{\infty} a(n)n^{-s} \sum_{m=1}^{\infty} a(m)m^{-s} = \sum_{m,n=1}^{\infty} a(n)b(n)(nm)^{-s} = \sum_{k=1}^{\infty} a * b(k)k^{-s}. \tag{3.18}$$

Das heißt, die Multiplikation von Potenzreihen entspricht der Faltung von arithmetischen Funktionen. Damit bilden die *formalen Dirichlet-Reihen* einen zu $\mathcal{A}$ isomorphen Ring. Diese Tatsache ermöglicht es, einige nützliche Resultate zu zeigen. Wir beschränken uns in diesem Abschnitt auf jene, die zum Beweis des Satzes von Dirichlet benötigt werden. Dabei treten immer wieder spezielle Reihen auf, die so genannten

Definition 3.16 (L-Reihen)**.** Sei χ ein beliebiger Charakter $\mod k$ und $s \in \mathbb{C}$. Eine *L-Reihe* ist eine Summe

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{3.19}$$

Zunächst zeigen wir eine weitere hilfreiche Identität.

Lemma 3.17 (Abel'sche Identität)**.** Für eine beliebige arithmetische Funktion $a(n)$ sei

$$A(x) = \sum_{n \leq x} a(n),$$

wobei $A(x) = 0 \, \forall x < 1$. Sei f eine auf dem positiven Intervall $[y, x]$ stetig differenzierbare Funktion, dann gilt

$$\sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) \, dt. \tag{3.20}$$

Beweis. Seien $k = \lfloor x \rfloor, m = \lfloor y \rfloor$, sodass $A(x) = A(k)$ und $A(y) = A(m)$.

$$\begin{aligned}
\sum_{y < n \leq x} a(n) f(n) &= \sum_{n=m+1}^{k} a(n) f(n) = \sum_{n=m+1}^{k} \big(A(n) - A(n-1)\big) f(n) \\
&= \sum_{n=m+1}^{k} A(n) f(n) - \sum_{n=m}^{k-1} A(n) f(n+1) \\
&= \sum_{n=m+1}^{k-1} A(n) \big(f(n) - f(n+1)\big) + A(k) f(k) - A(m) f(m+1) \\
&= - \sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t) \, dt + A(k) f(k) - A(m) f(m+1) \\
&= - \sum_{n=m+1}^{k-1} \int_n^{n+1} A(t) f'(t) \, dt + A(k) f(k) - A(m) f(m+1) \\
&= - \int_{m+1}^{k} A(t) f'(t) \, dt + A(x) f(x) - \int_k^x A(t) f'(t) \, dt \\
&\quad - A(y) f(y) - \int_y^{m+1} A(t) f'(t) \, dt \\
&= A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) \, dt.
\end{aligned} \tag{3.21}$$

□

Da im weiteren Verlauf der Arbeit die $\mathcal{O}$-Notation oft verwendet wird, soll hier noch einmal die Definition wiederholt werden.

Definition 3.18 (Landau-Symbole)**.** Seien f, g auf einer Teilmenge der reellen Zahlen definierte Funktionen. Dann gilt

$$f(x) = \mathcal{O}(g(x)) :\Leftrightarrow \exists M > 0 : |f(x)| \leq M |g(x)|. \tag{3.22}$$

Satz 3.19. Sie $\chi \neq \chi_1$ ein Charakter $\mod k$ und $f \geq 0$ eine für $x \geq x_0$ stetig differenzierbare Funktion. Dann gilt für $y \leq x \leq x_0$, dass

$$\sum_{x<n\leq y} \chi(n)f(n) = \mathcal{O}(f(x)). \tag{3.23}$$

Gilt außerdem $\lim_{x\to\infty} f(x) = 0$, so konvergiert $\sum_{n=1}^{\infty} \chi(n)f(n)$ und für $x \geq x_0$ ist

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + \mathcal{O}(f(x)). \tag{3.24}$$

Beweis. Da χ nicht der Hauptcharakter ist, gilt wegen der Periodizität

$$A(mk) = \sum_{n=1}^{mk} \chi(n) = 0 \ \forall m \geq 2. \tag{3.25}$$

Daher gilt $|A(x)| < \varphi(k)$ für alle x. Die Summe $A(x)$ ist also beschränkt, das heißt $A(x) = \mathcal{O}(1)$.
Mithilfe der eben gezeigten Identität von Abel kann die Summe in (3.23) als Integral ausgedrückt werden.

$$\begin{aligned}\sum_{x<n\leq y} \chi(n)f(n) &= f(y)A(y) - f(x)A(x) - \int_x^y A(t)f'(t)\,dt \\ &= \mathcal{O}(f(y)) + \mathcal{O}(f(x)) + \mathcal{O}(\int_x^y -f'(t)\,dt) = \mathcal{O}(f(x)).\end{aligned} \tag{3.26}$$

Damit ist der erste Teil der Behauptung gezeigt. Gilt nun $f(x) \to 0$ für $x \to \infty$, dann folgt die Konvergenz der Reihe mit dem eben gezeigten, denn mit der rechten Seite verschindet auch die linke Seite, die gerade den Reihenrest darstellt. Somit folgt die Konvergenz mithilfe des Cauchy-Kriteriums.
Die letzte Behauptung erhält man mit

$$\sum_{n=1}^{\infty} \chi(n)f(n) = \sum_{n\leq x} \chi(n)f(n) + \lim_{y\to\infty} \sum_{x<n\leq y} \chi(n)f(n). \tag{3.27}$$

Wegen (3.23) ist der Limes gerade $\mathcal{O}(f(x))$ und der Beweis damit abgeschlossen. □

Wendet man (3.23) auf $f(x) = 1/x$ und $g(x) = \log x/x$ an, erhält man für $\chi \neq \chi_1$

$$\sum_{n\leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + \mathcal{O}\left(\frac{1}{x}\right) \tag{3.28}$$

$$\sum_{n\leq x} \frac{\chi(n)\log n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} + \mathcal{O}\left(\frac{\log x}{x}\right) \tag{3.29}$$

Die so erhaltenen Summen sind spezielle L-Reihen, nämlich $L(1,\chi)$ und $L'(1,\chi)$, die so genannte *Dirichlet-Ableitung*.

3.3.1 Exkurs: Die Riemann'sche Vermutung

Eine weitere spezielle Dirichlet-Reihe erhält man, wenn man anstelle von χ die konstante 1-Funktion wählt und die entstehende Reihe als Funktion in $s \in \mathbb{C}$ betrachtet.

Definition 3.20 (Riemann'sche Zeta-Funktion)**.**

$$L(s,1) = \zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{3.30}$$

Diese konvergiert für alle $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$. Wählt man etwa $s = 2$, so ist $\zeta(2) = \pi^2/6$, dessen Kehrwert beispielsweise die Wahrscheinlichkeit dafür ist, dass zwei zufällig ausgewählte ganze Zahlen teilerfremd sind.
Der zunächst nicht offensichtliche Zusammenhang zu Primzahlen wird klar, wenn die ζ-Funktion mithilfe sogenannter Euler-Produkte dargestellt wird. Für $\mathrm{Re}(s) > 1$ ist nämlich

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}. \tag{3.31}$$

Mithilfe der Funktionalgleichung

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s) \tag{3.32}$$

kann die ζ-Funktion auf die ganze komplexe Ebene fortgesetzt werden. Diese Fortsetzung ist die Basis für die Riemann'sche Vermutung, die folgende Aussage über die Gestalt der Nullstellen der ζ-Funktion macht.

Satz 3.21 (Riemann'sche Vermutung)**.** Der Realteil aller nicht-trivialen Nullstellen von $\zeta(s)$ ist $\frac{1}{2}$.

Als triviale Nullstellen bezeichnet man die negativen geraden Zahlen. Dass für diese tatsächlich $\zeta(-\mathbb{N}_g) = 0$ gilt, sieht man an der alternativen Darstellung

$$\zeta(s) = 2^s p i^{s-1} \sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s), \tag{3.33}$$

deren Faktor $\sin \pi s/2$ für negative gerade Zahlen verschwindet.

Obwohl die Vermutung nicht bewiesen ist, so gibt es doch Argumente, die für deren Gültigkeit sprechen. Einige davon sind in **[Bo]** aufgelistet.

Betrachtet man anstelle der konstanten 1-Funktion die viel allgemeineren L-Funktionen,

erhält man die dazu analoge verallgemeinerte Riemann'sche Vermutung. Dies ist allerdings nur ein erster Schritt, denn durch Ausweitung auf Zahlkörper und allgemeine Zeta-Funktionen kommt man zur erweiterten bzw. zur Großen Riemann'schen Vermutung, die allerdings an dieser Stelle nicht weiter behandelt werden (können).
Die Wichtigkeit der Riemann'schen Vermutung ergibt sich aus den weitreichenden Folgerungen, die daraus abgeleitet werden können. So etwa wäre damit auch die schwache Goldbach-Vermutung bewiesen, wie 1997 in **[DERZ]** gezeigt wurde. Außerdem könnte der Dichtigkeitssatz von Tschebotareff, das eine Verallgemeinerung des Satzes von Dirichlet für Zahlkörper darstellt, stärker formuliert werden. Es trifft eine Aussage darüber, welcher Anteil der Primzahlen in einer gegebenen Galoiserweiterung über $\mathbb{Q}$ vollständig zerfällt. Als Illustriation betrachten wir die (üblichen) ganzen Zahlen sowie die Gauß'schen ganzen Zahlen $\mathbb{Z}[i]$. Dort zerfällt die Primzahl $5 = (1+2i)(1-2i)$ vollständig, wogegen etwa 3 auch in $\mathbb{Z}[i]$ prim ist. Es stellt sich heraus, dass die Anzahl der zerlegbaren Primzahlen in diesem Fall gegen $1/2$ strebt, es zerfallen nämlich genau die Primzahlen der Form $4k+1$ vollständig und jene der Form $4k+3$ nicht. (siehe auch Kap. 5.2).

3.4 Ein Resultat von Mertens

Franz Mertens (1840-1927) wurde drei Jahre nach Veröffentlichung von Dirichlets Beweis geboren. Durch den Beweis einer von mehreren Identitäten, die als *Satz von Mertens* bekannt sind, konnte er deutlich zur Verkürzung des Beweises beitragen. So gelingt der Beweis von Shapiro, siehe **[Sh1]** bzw. **[Sh2]**, der sich einer Identität von Mertens bedient auf wenigen Seiten. Der ursprüngliche Beweis in **[Di]** basiert auf sehr komplexen analytischen Methoden, die im Laufe der Zeit mehrfach vereinfacht wurden.

Die Formel von Mertens besagt, dass $\sum_{p\leq x} \log p/p = \log x + \mathcal{O}(1)$.
Um dies zu beweisen, benötigen wir zwei Hilfssätze, die zuerst gezeigt werden.

Lemma 3.22 (Stirling)**.** Für $n \in \mathbb{N}$ gilt

$$\log n! = n\log n - n + \mathcal{O}(\log n). \tag{3.34}$$

Beweis. Der Beweis ergibt sich sofort durch Vergleich von Summe und Integral.

$$\log n! = \sum_{k=1}^{n} = \int_1^t \log t\, dt + \mathcal{O}(\log n). \tag{3.35}$$

Partielle Integration und Einsetzen der Grenzen beweist die Behauptung. □

Lemma 3.23. Für $n \in \mathbb{N}$ und p prim gilt

$$n! = \prod_{p \leq n} p^{e(p)} \Rightarrow e(p) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor. \tag{3.36}$$

Beweis. Von den n Faktoren in $n!$ sind genau $\lfloor \frac{n}{p} \rfloor$ durch p teilbar und genau $\lfloor \frac{n}{p^k} \rfloor$ durch p^k. Summiert man über alle k, so erhält man die Anzahl, wie oft der Faktor p in $n!$ auftritt. Da n fix und alle $p > 1$ sind, ist die Summe natürlich endlich und die Aussage gezeigt. □

Damit kann der Satz von Mertens bewiesen werden.

Satz 3.24. Für p prim und $x \in \mathbb{R}$ ist

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + \mathcal{O}(1). \tag{3.37}$$

Beweis. Logarithmieren von (3.36) führt zu

$$\log n! = \sum_{p \leq n} \log p^{e(p)} = \sum_{p \leq n} \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \log p. \tag{3.38}$$

Die so entstehende Doppelsumme kann durch

$$\sum_{p \leq n} \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \log p \leq n \sum_{p \leq n} \log p \sum_{k \geq 2} \frac{1}{p^k} = n \sum_{p \leq n} \frac{\log p}{p(p-1)} = \mathcal{O}(n) \tag{3.39}$$

abgeschätzt werden und man rechnet mithilfe eines Konvergenztests leicht nach, dass die letzte Summe auch für $n \to \infty$ endlich bleibt. Setzt man (3.34) und die eben erhaltene Abschätzung zusammen und fasst die $\mathcal{O}$-Terme zusammen, bekommt man

$$\sum_{p \leq n} \left\lfloor \frac{n}{p} \right\rfloor \log p = n \log n + \mathcal{O}(n). \tag{3.40}$$

Die geforderte Behauptung erhält man für natürliche Zahlen durch das Weglassen der Gaußklammer mit $\lfloor x \rfloor = x + \mathcal{O}(1)$, wenn man $\mathcal{O}(\sum_{p \leq n} \log p) = \mathcal{O}(n)$ zeigen kann. Durch die Gaußklammer erhält man schließlich auch Gültigkeit für reelle Zahlen, denn

$$\begin{aligned} \sum_{p \leq 2x} \log p - \sum_{p \leq x} \log p &= \sum_{p \leq \lfloor 2x \rfloor} \log p - \sum_{p \leq \lfloor x \rfloor} \log p \\ &= \sum_{p \leq 2\lfloor x \rfloor} \log p - \sum_{p \leq \lfloor x \rfloor} \log p + \mathcal{O}(\log x) = \mathcal{O}(x). \end{aligned} \tag{3.41}$$

Diese Abschätzung hält, da zwischen $2\lfloor x \rfloor$ und $\lfloor 2x \rfloor$ höchstens eine Primzahl sein kann. Dadurch kann als obere Schranke folgende Abschätzung gemacht werden:

$$\sum_{p \leq x} \log p = \sum_{i=1}^{\infty} \left(\sum_{p \leq x/2^{i-1}} \log p - \sum_{p \leq x/2^{i}} \log p \right) = \mathcal{O}\left(\sum_{i=1}^{\infty} \frac{x}{2^i} \right) = \mathcal{O}(x) \tag{3.42}$$

Damit ist die Behauptung gezeigt. □

4 Der Beweis des Satzes von Dirichlet

Mit all dem bisher gezeigten kann nun folgende Identität bewiesen werden, aus der die Aussage von Dirichlet direkt durch Grenzübergang für $x \to \infty$ folgt.

Satz 4.1 (Dirichlet). Seien $k, l \in \mathbb{N}, (k,l) = 1$ und $x > 1$. Dann gilt

$$\sum_{\substack{p \leq x \\ p \equiv l \mod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \mathcal{O}(1) \tag{4.1}$$

4.1 Die Beweisidee

Der Beweis selbst wird in mehreren Schritten geführt. Zunächst wird gezeigt, dass

$$\sum_{\substack{p \leq x \\ p \equiv l \mod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(l) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} + \mathcal{O}(1).$$

Um daraus die obige Aussage zu gewinnen, wird der Summand rechts abgeschätzt mit

$$\sum_{p \leq x} \frac{\chi(p) \log p}{p} \overset{L.2}{=} -L'(1,\chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} \qquad \text{sowie} \qquad L(1,\chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} \overset{L.3}{=} \mathcal{O}(1),$$

wobei stets $x > 1$ und $\chi \neq \chi_1$ gilt.
Damit bleibt zu zeigen, dass $L(1,\chi) \neq 0$, um in Lemma 3 durch $L(1,\chi)$ dividieren zu können, wodurch schließlich der Satz von Dirichlet bewiesen wird.

Um dies zu zeigen sei $N(k)$ die Anzahl aller Charaktere $\chi \neq \chi_1$, für die $L(1,\chi) = 0$ gilt. Dann ist $N(k)$ gerade, da Charaktere immer in konjugierten Paaren auftreten. In Lemma 4 wird (mithilfe von Lemma 5) gezeigt, dass

$$\sum_{\substack{p \leq x \\ p \equiv 1 \mod k}} \frac{\log p}{p} = \frac{1 - N(k)}{\varphi(k)} \log x + \mathcal{O}(1),$$

woraus sofort folgt, dass $N(k) = 0$ gelten muss, da sonst die rechte Seite der Gleichung negativ ist, aber die Summe links ausschließlich positive Summanden besitzt.

Dieser Strategie folgend werden nun alle fünf Lemmata der Reihe nach bewiesen.

4.2 Lemma 1

Lemma 4.2. Für $x > 1$ und p prim gilt

$$\sum_{\substack{p \leq x \\ p \equiv l \mod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(l) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} + \mathcal{O}(1). \tag{4.2}$$

Beweis. Der Ausgangspunkt ist die Orthogonalitätseigenschaft der Dirichlet-Charaktere in Satz 3.15.
Setzt man $m = p$, $n = l$, multipliziert beide Seiten mit $\frac{\log p}{p}$ und summiert über alle $p \leq x$, erhält man

$$\sum_{p \leq x} \sum_{r=1}^{\varphi(k)} \chi_r(p) \overline{\chi}_r(l) \frac{\log p}{p} = \varphi(k) \sum_{\substack{p \leq x \\ p \equiv l \mod k}} \frac{\log p}{p}, \tag{4.3}$$

da gerade alle Summanden $\not\equiv n \mod k$ auf der rechten Seite Null werden und damit wegfallen.
Spaltet man links den ersten Term der Summe ab (das ist der Term, der den Hauptcharakter χ_1 enthält), erhält man

$$\overline{\chi}_1(l) \sum_{p \leq x} \frac{\chi_1(p) \log p}{p} + \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(l) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} = \varphi(k) \sum_{\substack{p \leq x \\ p \equiv l \mod k}} \frac{\log p}{p}. \tag{4.4}$$

Nutzt man nun aus, dass $\overline{\chi}_1(l) = 1$ und $\chi_1(p) = 0$ falls $(p,k) \neq 1$ bzw. $\chi_1(p) = 1$ für $(p,k) = 1$, lässt sich die erste Summe darstellen als

$$\sum_{\substack{p \leq x \\ (p,k)=1}} \frac{\log p}{p} = \sum_{p \leq x} \frac{\log p}{p} - \sum_{\substack{p \leq x \\ p \mid k}} \frac{\log p}{p} = \sum_{p \leq x} \frac{\log p}{p} + \mathcal{O}(1) \overset{Mertens}{=} \log x + \mathcal{O}(1). \tag{4.5}$$

Setzt man diese Abschätzung in (4.4) ein, ergibt das schließlich

$$\varphi(k) \sum_{\substack{p \leq x \\ p \equiv l \mod k}} \frac{\log p}{p} = \log x + \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(l) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} + \mathcal{O}(1). \tag{4.6}$$

Dividiert man noch durch $\varphi(k)$, erhält man das gewünschte Resultat. □

4.3 Lemma 2

Lemma 4.3. Für $x > 1$ und $\chi \neq \chi_1$ gilt

$$\sum_{p \leq x} \frac{\chi(p)\log(p)}{p} = -L'(1,\chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} + \mathcal{O}(1). \tag{4.7}$$

Beweis. Wir betrachten zunächst die Summe $\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n}$ und stellen sie auf zwei Arten dar. Zuerst erlaubt uns die Definition der von Mangoldt-Funktion die Darstellung

$$\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{\substack{p \leq x \\ p^a \leq x}} \sum_{a=1}^{\infty} \frac{\chi(p^a)\log p}{p^a}. \tag{4.8}$$

Analog zu Lemma 1 kann man auch hier die linke Summe aufspalten und erhält

$$\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{p \leq x} \frac{\chi(p)\log p}{p} + \sum_{\substack{p \leq x \\ p^a \leq x}} \sum_{a=2}^{\infty} \frac{\chi(p^a)\log p}{p^a}. \tag{4.9}$$

Die letzte Summe kann mithilfe der geometrischen Reihe abgeschätzt werden, denn es gilt

$$\sum_{p} \log p \sum_{a=2}^{\infty} \frac{1}{p^a} = \sum_{p} \frac{\log p}{p(p-1)} < \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = \mathcal{O}(1). \tag{4.10}$$

Damit erhalten wir

$$\sum_{p \leq x} \frac{\chi_r(p)\log p}{p} = \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} + \mathcal{O}(1). \tag{4.11}$$

Andererseits gilt für die von Mangoldt-Funktion $\Lambda(n) = \sum_{d|n} \mu(d)\log({}^{n}/_{d})$. Damit bekommen wir

$$\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{n \leq x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) \log {}^{n}/_{d} \overset{n=cd}{=} \sum_{d \leq x} \frac{\mu(d)\chi(d)}{d} \sum_{c \leq {}^{x}/_{d}} \frac{\chi(c)\log c}{c}. \tag{4.12}$$

Für den letzten Umformungsschritt haben wir außerdem die Multiplikativität von χ benutzt. Für die Summe über c erhalten wir mit (3.29)

$$\sum_{c \leq {}^{x}/_{d}} \frac{\chi(c)\log c}{c} = -L'(1,\chi) + \mathcal{O}\left(\frac{\log {}^{x}/_{d}}{{}^{x}/_{d}}\right). \tag{4.13}$$

Einsetzen dieses Resultats in (4.12) liefert

$$\sum_{n\leq x}\frac{\chi(n)\Lambda(n)}{n} = -L'(1,\chi)\sum_{d\leq x}\frac{\mu(d)\chi(d)}{d} + \mathcal{O}\bigg(\sum_{d\leq x}\frac{1}{d}\frac{\log {}^{x}\!/_{d}}{{}^{x}\!/_{d}}\bigg) \tag{4.14}$$

und für den $\mathcal{O}$-Term erhalten wir nach Auflösen des Doppelbruchs und Aufspalten des Logarithmus

$$\begin{aligned}\frac{1}{x}\sum_{d\leq x}(\log x - \log d) &= \frac{1}{x}\bigg(\lfloor x\rfloor \log x - \sum_{d\leq x}\log d\bigg) = \frac{1}{x}\bigg(\lfloor x\rfloor \log x - \log\lfloor x\rfloor !\bigg)\\ &= \frac{1}{x}\bigg(\lfloor x\rfloor \log x - x\log x + \mathcal{O}(x)\bigg) = \mathcal{O}(1).\end{aligned} \tag{4.15}$$

Ersetzt man nun noch den Summanden mit der von Mangoldt-Funktion durch die Abschätzung (4.11), so ist die Behauptung gezeigt. □

4.4 Lemma 3

Lemma 4.4. Für $x > 1$ und $\chi \neq \chi_1$ gilt

$$L(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} = \mathcal{O}(1). \tag{4.16}$$

Beweis. Für den Beweis dieses Lemmas benutzen wir die Inversionsformel von Möbius. Wir wählen $\alpha(n) = \chi(n)$ und $f(x) = x$ in (3.9) und finden

$$x = \sum_{n\leq x}\mu(n)\chi(n)g({}^{x}\!/_{n}), \tag{4.17}$$

wobei $g(x) = \sum_{n\leq x}\chi(n){}^{x}\!/_{n} = x\sum_{n\leq x}{}^{\chi(n)}\!/_{n}$.
Mithilfe von (3.28) lässt sich $G(x)$ darstellen als $G(x) = xL(1,\chi) + \mathcal{O}(1)$.
Einsetzen in (4.17) und dividieren durch x vollendet den Beweis:

$$x = \sum_{n\leq x}\mu(n)\chi(n)\bigg(\frac{x}{n}L(1,\chi) + \mathcal{O}(1)\bigg) = xL(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} + \mathcal{O}(1). \tag{4.18}$$

□

4.5 Lemma 4

Lemma 4.5. Sei $\chi \neq \chi_1$ und $L(1,\chi) = 0$, dann gilt

$$L'(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} = \log x + \mathcal{O}(1). \tag{4.19}$$

Beweis. Wie in Lemma 3 verwenden wir noch einmal die Inversionsformel, wählen $a(n) = \chi(n)$ wie vorhin, aber $f(x) = x \log x$. Dies liefert

$$x \log x = \sum_{n \leq x} \mu(n)\chi(n) g(x/n), \tag{4.20}$$

wobei

$$g(x) = \sum_{n \leq x} \chi(n) \frac{x}{n} \log \frac{x}{n} = x \log x \sum_{n \leq x} \frac{\chi(n)}{n} - x \sum_{n \leq x} \frac{\chi(n) \log n}{n}. \tag{4.21}$$

Mit (3.29) ergibt sich unter Berücksichtigung von $L(1, \chi) = 0$

$$\begin{aligned} g(x) &= x \log x \left(L(1, \chi) + \mathcal{O}\left(\frac{1}{x}\right)\right) + x \left(L'(1, \chi) + \mathcal{O}\left(\frac{\log x}{x}\right)\right) \\ &= xL'(1, \chi) + \mathcal{O}(\log x). \end{aligned} \tag{4.22}$$

Wir setzen diesen Ausdruck in (4.20) ein und bekommen

$$\begin{aligned} x \log x &= \sum_{n \leq x} \mu(n)\chi(n) \left(\frac{x}{n} L'(1, \chi) + \mathcal{O}\left(\frac{\log x}{n}\right)\right) \\ &= xL'(1, \chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} + \mathcal{O}\Big(\sum_{n \leq x} (\log x - \log n)\Big). \end{aligned} \tag{4.23}$$

Aus dem Beweis von Lemma 2 ist bereits bekannt, dass der $\mathcal{O}$-Term rechts ein $\mathcal{O}(x)$ ist. Damit erhalten wir die Behauptung des Lemmas erneut durch abschließende Division durch x. □

4.6 Lemma 5

Lemma 4.6. Sei $x > 1$, dann gilt

$$\sum_{\substack{p \leq x \\ p \equiv 1 \mod k}} \frac{\log p}{p} = \frac{1 - N(k)}{\varphi(k)} \log x + \mathcal{O}(1). \tag{4.24}$$

Beweis. Wir beginnen mit dem in Lemma 1 bewiesen Resultat, wählen $l = 1$ und bekommen so

$$\sum_{\substack{p \leq x \\ p \equiv 1 \mod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(l) \sum_{p \leq x} \frac{\chi_r(p) \log p}{p} + \mathcal{O}(1). \tag{4.25}$$

Nach Lemma 2 gilt für die Summe rechts

$$\sum_{p\leq x} \frac{\chi(p)\log(p)}{p} = -L'(1,\chi) \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} + \mathcal{O}(1). \tag{4.26}$$

Lemma 3 besagt, dass die Summe im Fall $L(1,\chi) \neq 0$ ein $\mathcal{O}(1)$ ist und im Fall $L(1,\chi) = 0$ nach Lemma 4 gilt

$$-L'(1,\chi) \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = -\log x + \mathcal{O}(1). \tag{4.27}$$

Daraus folgt für die rechte Seite von (4.25) mit der Anzahl $N(k)$ der Charaktere für die $L(1,\chi)$verschwindet, dass

$$\sum_{\substack{p\leq x \\ p\equiv 1 \mod k}} \frac{\log p}{p} = \frac{1-N(k)}{\varphi(k)} \log x + \mathcal{O}(1). \tag{4.28}$$

Damit ist das Lemma bewiesen. □

Mit dem bereits ausgeführten Argument, dass Charaktere immer in konjungierten Paaren auftreten, folgt nun, dass $N(k) = 0$ gelten muss. Damit beweisen die eben gezeigten Lemmata, dass

$$\sum_{\substack{p\leq x \\ p\equiv l \mod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + \mathcal{O}(1). \tag{4.29}$$

Führt man nun den Grenzübergang $x \to \infty$ durch, besagt dieses Resultat, dass es unendliche viele Primzahlen der Form $kn + l$ gibt und der Satz von Dirichlet über Primzahlen in arithmetischen Progressionen ist gezeigt.

5 Verallgemeinerungen

5.1 Polynomiale Progressionen - die Bunyakowsky-Vermutung

Versucht man, den Satz von Dirichlet mit denselben Voraussetzungen, das heißt mit teilerfremden Koeffeizienten, auf Polynome höheren Grades zu verallgemeinern, kann man sehr einfach ein Polynom konstruieren, für den der Satz von Dirichlet nicht mehr gelten würde. So ist zum Beispiel

$$f(x) = x^2 + x + 2 = x(x+1) + 2 \tag{5.1}$$

offensichtlich irreduzibel über $\mathbb{Q}$ und $(1, 1, 2) = 1$, aber die zweite Darstellung zeigt, dass für ganzzahlige Werte von x die Funktionswerte immer gerade sind und damit 2 die einzige Primzahl in dieser Progression ist.
Im Jahr 1857 lieferte Viktor Bunyakovsky ein mögliches, aber noch unbewiesenes Kriterium:

Satz 5.1 (Bunyakovsky-Vermutung)**.** Sei $f(x) \in \mathbb{Z}[x]$ ein über $\mathbb{Q}$ irreduzibles Polynom mit positivem führenden Koeffizienten und es sei $d := ggT\{f(n)\}_{n\in\mathbb{Z}}$. Dann ist $f(n)/d$ prim für unendlich viele $n \in \mathbb{Z}$.

Alternativ kann die Vermutung auch so formuliert werden, dass eine polynomiale Progression unendlich viele Primzahlen enthält, wenn $ggT\{f(n)\}_{n\in\mathbb{N}} = 1$ gilt. Die Schwierigkeit in der Anwendung der Vermutung liegt allerdings darin, zumindest zwei teilerfremde Funktionswerte zu finden, da diese theoretisch erst für sehr große n auftreten können - falls überhaupt.
Eine Möglichkeit, den größten gemeinsamen Teiler der Funktionswerte zu bestimmen ist, das Polynom mithilfe des Binomialkoeffizienten darzustellen, das heißt

$$f(x) = a_1\binom{x}{1} + ... + a_m\binom{x}{m}. \tag{5.2}$$

Der größte gemeinsame Teiler der Funktionswerte entspricht dann jenem der Koeffizienten a_i.

Das Polynom aus dem Beispiel kann so dargestellt werden als $f(x) = 2\binom{x}{2} + 2$ und $(2,2) = 2 > 1$. Das Polynom erzeugt also nur eine Primzahl, nämlich 2.
Das Polynom $g(x) = x^2 + 1 = 2\binom{x}{2} + \binom{x}{1} + 1$ dagegen erfüllt alle Kriterien der Bunyakovsky-Vermutung und würde demnach unendlich viele Primzahlen erzeugen. In diesem Fall kann man auch leicht zwei teilerfremde Funktionswert finden, etwa $f(2) = 5$ und $f(4) = 17$, um die Voraussetzungen zu verifizieren. Dennoch kann daraus noch nicht auf unendlich viele prime Funktionswerte geschlossen werden, da die Vermutung nach wie vor unbewiesen ist.

5.2 Primideale in Zahlkörpern

Eine weitere Möglichkeit der Verallgemeinerung besteht darin, Primzahlen nicht als Teilmenge der natürlichen Zahlen zu studieren, sondern Primideale in Zahlkörpern. Dabei lässt sich das Konzept des Euklidischen Beweises verallgemeinern.

Definition 5.2 (Euklidischer Beweis)**.** Sei K/k eine abelsche Galoiserweiterung mit Galoisgruppe $G = Gal(K/k)$. Ein Ideal $\mathcal{P} \subset k$ heißt *Primteiler* eines Polynoms $f \in \mathcal{O}_k[x]$, falls $\mathcal{P}|f(a)$ für gewisse a im Ganzzahlring $\mathcal{O}_k$. Ein *Euklidischer Beweis* für ein $\sigma \in G$ bedeutet die Existenz eines Polynoms f sodass bis auf endlich viele Ausnahmen alle Primteiler von f entweder Frobeniuselement 1 oder σ haben.

Damit zeigen Murty und Thain **[MuTh]** ein Analogon zum eingangs behandelten Fall von Primzahlen in arithmetischen Progressionen, nämlich dass ein Euklidischer Beweis existiert, falls die Ordnungσ gleich 2 ist. Der Beweis erfolgt auf ganz ähnliche Weise, wird allerdings aufgrund seiner Länge hier nicht weiter ausgeführt.

Zum Abschluss geben wir noch ein Beispiel zur Anwendung des Dichtigkeitstheorems von Tschebotareff, das in Kapitel 3 bereits erwähnt wurde. Zunächst die exakte Formulierung, siehe auch **[Ch]**.

Satz 5.3 (Tschebotareff's Dichtigkeitssatz)**.** Sei L/K eine Galois-Erweiterung von Zahlkörpern mit Galoisgruppe $G = Gal(L/K)$ und einer Konjugationsklasse $C \subset G$. Dann hat die Menge der unverzweigten Primideale $\mathcal{P}$ von K mit Frobenius-Element C die natürliche Dichtigkeit $|C|/|G|$.

Um dies zu veranschaulichen betrachten wir die Symmetriegruppe $G = S_3$ mit den Konjugationsklassen $\{id\}$, $\{(1,2),(1,3),(2,3)\}$, $\{(1,2,3),(1,3,2)\}$. Gemäß dem Theorem gilt dann, dass $1/6$ der Primideale in 3 Faktoren zerfällt, die Hälfte in zwei Faktoren und ein Drittel gar nicht zerfällt, also auch in der Körpererweiterung prim bleibt.

Betrachten wir, um den Kreis zu schließen, den im Fall von Dirichlet behandelten Fall von linearen arithmetischen Progressionen $a_n = kn + l$, dann existieren genau $\varphi(k)$ Progressionen mit unendlich vielen Primzahlen, deren natürliche Dichtigkeit genau $1/\varphi(k)$ beträgt.

6 Literaturverzeichnis

Ap Apostol, Tom M.: Introduction to analytic number theory. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976

Bo Bombieri, Enrico: The Riemann hypothesis. The millennium prize problems, 107–124, Clay Math. Inst., Cambridge, MA, 2006

Br Brüdern, Jörg: Einführung in die analytische Zahlentheorie. Springer, Berlin, 1995

DERZ Deshouillers, J.-M.; Effinger, G.; te Riele, H.; Zinoviev, D.: A complete Vinogradov 3-primes theorem under the Riemann hypothesis. (English summary). Electron. Res. Announc. Amer. Math. Soc. 3 (1997), 99–104

Di Dirichlet, Lejeune: Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. Abhandlungen der Königlich Preußischen Akademie der Wissenschaften zu Berlin, 1837

JSch Jantzen, J.; Schwermer, J.: Algebra. Springer, Berlin, 2006

MuEs Murty, M.; Esmonde, J.: Problems in algebraic number theory. Second edition. Graduate Texts in Mathematics, 190. Springer-Verlag, New York, 2005

MuTh Murty, M. Ram; Thain, N.: Prime numbers in certain arithmetic progressions. Funct. Approx. Comment. Math. 35 (2006), 249–259

Po Pollack, P.: Hypothesis H and an impossibility theorem of Ram Murty. Rend. Semin. Mat. Univ. Politec. Torino 68 (2010), no. 2, 183–197

Ri Ribenboim, Paulo: Die Welt der Primzahlen, Geheimnisse und Rekorde. Springer, Berlin, 2006

Sh1 Shapiro, Harold N.: On primes in arithmetic progressions. I. Ann. of Math. (2) 52, (1950). 217–230

Sh2 Shapiro, Harold N.: On primes in arithmetic progressions. II. Ann. of Math. (2) 52, (1950). 231–243

Tsch Tschebotareff, N.: Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. (German) Math. Ann. 95 (1926), no. 1, 191–228