Primtests
und der
Satz von Ankeny

Jürgen Lerner

Diplomarbeit

bei
Prof. Dr. W. Baur
Fachbereich für Mathematik und Statistik
Universität Konstanz

Konstanz, im Juni 2002

Einleitung

Eine einfache Methode, zu einer gegebenen, natürlichen Zahl n algorithmisch zu entscheiden, ob n prim ist, oder zusammengesetzt, ist für die Zahlen $a = 2, 3, \ldots, \lfloor\sqrt{n}\rfloor$ eine Division mit Rest von n durch a durchzuführen und zu prüfen, ob der Rest gleich null ist. Bei "großen" [1] Zahlen ist diese Vorgehensweise aber, selbst von Computern, nicht mehr in angemessener Zeit durchführbar.
Eine bessere Vorgehensweise ist, algorithmisch schnell zu testende Eigenschaften von Primzahlen zu prüfen. Eine erste solche Eigenschaft folgt aus dem kleinen Satz von FERMAT (3.2.1), welcher besagt, daß falls n eine ungerade Primzahl ist, so gilt für jedes a mit $1 < a < n$ die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$. Finden wir zu einem Kandidaten n also ein a, welches diese Bedingung verletzt, [2] so haben wir einen Beweis für die Zusammengesetztheit von n. Umgekehrt erhalten wir so aber leider keinen Beweis für die Primheit von n; es gibt sogar zusammengesetzte Zahlen n für die jedes $a \in (\mathbb{Z}/(n))^*$ die obige Kongruenz erfüllt, siehe (3.3.3).
Ein besseres Kriterium ist das EULER Kriterium (3.2.3) welches besagt, daß für eine ungerade Primzahl n und für alle a mit $1 < a < n$ gilt, $a^{(n-1)/2} \equiv 1 \pmod{n}$ genau dann, wenn a ein quadratischer Rest (siehe 3.2.2) modulo n ist und $a^{(n-1)/2} \equiv -1 \pmod{n}$, sonst. [3]
Wenn auch die Umkehrung des EULER Kriteriums wiederum falsch ist so gilt doch, daß falls n zusammengesetzt ist, so wird dieses Kriterium nur von Zahlen a aus einer echten Untergruppe von $(\mathbb{Z}/(n))^*$ - also höchstens $(n-1)/2$ vielen - erfüllt (3.3.15).
Auch wenn so die Zusammengesetztheit einer Zahl n wahrscheinlich recht schnell bewiesen wird, so kann man doch erst dann sicher sein, eine Primzahl gefunden zu haben nachdem man $\frac{n-1}{2} + 1$ (positive) Tests durchgeführt hat, was gegenüber dem ersten Ansatz sogar noch eine Verschlechterung darstellt.
Wie bereits erwähnt bilden, im Falle einer zusammengesetzten Zahl n, die Zahlen zu denen n sich bezüglich des EULER Kriteriums wie eine Primzahl verhält, eine echte Untergruppe von $(\mathbb{Z}/(n))^*$. Interessant ist nun also eine obere Schranke für die Zahlen $x \in \mathbb{R}$ mit der Eigenschaft, dass alle $a \leq x$ zu einer (gemeinsamen) echten Untergruppe von $(\mathbb{Z}/(n))^*$ gehören, oder - was äquivalent dazu ist - so daß die $a \leq x$ noch nicht die ganze Gruppe $(\mathbb{Z}/(n))^*$ erzeugen.
Diese Diplomarbeit behandelt das Theorem von ANKENY, welches besagt dass, un-

[1] Was in diesem Zusammenhang eine große Zahl ist hängt von der zur Verfügung stehenden Rechengeschwindigkeit ab - und natürlich davon, wie lange man warten will. Im Moment könnte man Zahlen mit etwa 1000 Binärstellen ganz sicher als "groß" bezeichnen

[2] die Bedingung ist schnell überprüfbar, siehe Anhang A

[3] auch die Eigenschaft, ein quadratischer Rest zu sein ist schnell überprüfbar, siehe Anhang A

ter Voraussetzung der **erweiterten Riemannschen Hypothese (ERH)** (siehe (1.1.1)), für jedes $n \in \mathbb{N}$ die multiplikative Gruppe $(\mathbb{Z}/(n))^*$ von Primzahlen der Größe $\mathcal{O}\left((\log n)^2\right)$ erzeugt wird, woraus insbesondere folgt, dass sich im obigen Fall eine Zahl, welche die Zusammengesetztheit von n beweist, schnell finden lässt.

Der Rest dieser Arbeit gliedert sich folgendermaßen:
Im Kapitel 1 wird der Satz von ANKENY formuliert, sowie eine Beweisskizze gegeben, die insbesondere auch den Zusammenhang zwischen diesem Satz und den Nullstellen der L-Funktionen herausstellt. Der Beweis des Satzes folgt in Kaptitel 2 unter überwiegender Verwendung von analytischen Methoden. Es werden einige bekannte Resultate der analytischen Zahlentheorie verwendet, ohne daß diese dort bewiesen werden. Kapitel 3 bringt Anwendungen aus der algorithmischen Zahlentheorie. Neben dem bereits in der Einleitung besprochenen Primtest, wird gezeigt werden daß sich unter Voraussetzung der erweiterten Riemannschen Hypothese ein quadratischer Nichtrest modulo einer ungeraden Primzahl schnell finden lässt. Außerdem wird ein weiterer Primtest, basierend auf einem anderen Kriterium, behandelt, sowie eine obere Schranke für die kleinste Primzahl p gegeben, die für teilerfremde $n \in \mathbb{N}$, $a \in \mathbb{Z}$ die Kongruenz $p \equiv a \pmod{n}$ erfüllt.
Im Anhang A werden die grundlegenden zahlentheoretischen Algorithmen besprochen, die im Kapitel 3 verwendet wurden, wobei auch insbesondere die behaupteten Laufzeiten gezeigt werden.

Inhaltsverzeichnis

Standardbezeichnungen

Immer bezeichnet $\mathbb{N} = \{1, 2, 3, \dots\}$ die Menge der natürlichen Zahlen, die wir bei 1 beginnen lassen, $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Mit dem Symbol p werden ausschließlich positive Primzahlen benannt. Genauso werden hier nur positive ganze Zahlen *prim* genannt. $\mathrm{ggT}(m, n)$ bezeichnet den größten gemeinsamen Teiler, $\mathrm{kgV}(m, n)$ das kleinste positive, gemeinsame Vielfache von $m, n \in \mathbb{Z}$. Beide Bezeichnungen lassen sich auf endliche Mengen ganzer Zahlen übertragen.
Ist $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen, so bezeichnet $\sum_{p\leq x} a_p$ die Summe über alle Folgenglieder, die mit positiven Primzahlen $\leq x$ indiziert sind, auch ohne dass die Zahlen p noch einmal explizit *prim* genannt werden.
Eine komplexe Zahl wird oft als $s = \sigma + it$ geschrieben. $\sigma \in \mathbb{R}$ ist der Realteil von s ($\sigma = \operatorname{Re} s$), $t \in \mathbb{R}$ ist der Imaginärteil von s ($t = \operatorname{Im} s$).

Ein **Charakter** χ einer endlichen, abelschen Gruppe G, ist ein Gruppenhomomorphismus $\chi : G \to \mathbb{C}^*$. Ein Charakter χ von $(\mathbb{Z}/(m))^*$ lässt sich zu einer Abbildung $\chi : \mathbb{Z} \to \mathbb{C}^*$, [4] mittels

$$\chi(a) := \begin{cases} \chi(a \bmod m), & \text{falls } \mathrm{ggT}(a, m) = 1, \\ 0 \qquad\qquad\quad , & \text{falls } \mathrm{ggT}(a, m) \neq 1 \end{cases}$$

fortsetzen. So eine Abbildung χ wird DIRICHLET-Charakter (modulo m) genannt. Der durch den konstanten Charakter $\chi \equiv 1$ induzierte DIRICHLET-Charakter wird **Hauptcharakter** (modulo m) genannt und mit χ_1 bezeichnet.
Ist χ ein DIRICHLET-Charakter, so wird durch

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

eine analytische Funktion, auf $\operatorname{Re} s > 1$ definiert. Funktionen diesen Typs heißen (DIRICHLETSCHE) L-Funktionen. L-Funktionen lassen sich, im Fall $\chi \neq \chi_1$, zu holomorphen Funktionen auf $\mathbb{C}$, im Fall $\chi = \chi_1$, zu holomorphen Funktionen auf $\mathbb{C} \setminus \{0\}$ fortsetzen (siehe Abschnitt 2.2).

Für einen DIRICHLET-Charakter χ modulo m hat die Abbildung χ eingeschränkt auf $\{n : \mathrm{ggT}(n, m) = 1\}$ immer noch die Periode m. Es kann aber noch kürzere Perioden geben. Ist m' die kürzeste, so gilt $m'|m$. Gilt $m' = m$ so wird χ **primitiv** genannt. Der Hauptcharakter wird nicht zu den primitiven gezählt.

[4] Die doppelte Belegung des Symbols χ sollte keine Verwechslungen mit sich bringen.

Umgekehrt gilt, daß falls χ' ein Charakter modulo m' ist und m ein Vielfaches von m' so lässt sich durch

$$\chi(n) := \begin{cases} \chi'(n) \text{ für } \mathrm{ggT}(n,m) = 1, \\ 0 \text{ für } \mathrm{ggT}(n,m) \neq 1 \end{cases}$$

ein Charakter modulo m konstruieren. Man sagt χ werde von χ' induziert. Es lässt sich zeigen, daß es zu jedem Charakter χ modulo m ein $m'|m$ und einen Charakter modulo m' gibt, der χ induziert.

Die MANGOLD-Funktion $\Lambda : \mathbb{N} \longrightarrow \mathbb{C}$ ist definiert durch

$$\Lambda(n) := \begin{cases} \log p & \text{falls } n = p^k, \\ 0 & \text{sonst.} \end{cases}$$

Kapitel 1

Der Satz von Ankeny

Wie bereits in der Einleitung besprochen, geht es in ANKENYS Satz um eine (möglichst kleine) obere Schranke für die Zahlen $x \in \mathbb{R}$ mit der Eigenschaft, daß alle $a \in (\mathbb{Z}/(n))^*$ mit $1 < a < x$ in einer gegebenen echten Untergruppe U von $(\mathbb{Z}/(n))^*$ liegen.
Zu einer solchen Gruppe U gibt es einen nichttrivialen (d.h. ungleich dem Hauptcharakter) DIRICHLET-Charakter χ der auf U identisch 1 ist. Die Idee besteht darin, zu einem solchen χ und x die Summe

$$\sum_{p \leq x} \chi(p)(\log p)(x-p)$$

nach oben und unten abzuschätzen.
Die Voraussetzungen an χ und der Primzahlsatz lassen vermuten, dass es positive Konstanten $C, c \in \mathbb{R}$ gibt so, dass, für große x, die Abschätzungen $c \cdot x^2 \leq \sum_{p \leq x} \chi(p)(\log p)(x-p) \leq C \cdot x^2$ gelten.
Für die obere Abschätzung wird diese Summe durch ein Integral über die logarithmische Ableitung von $\mathrm{L}(s, \chi)$ ausgedrückt. Zur Abschätzung dieses Integrals ist es entscheidend wie groß die Realteile von Polstellen von $\frac{\mathrm{L}'}{\mathrm{L}}(s, \chi)$ höchstens sein können.

1.1 Die erweiterte Riemannsche Hypothese

Bekannt ist, dass für einen DIRICHLET-Charakter χ die zugehörige L-Funktion $\mathrm{L}(s, \chi)$ Nullstellen an einigen der nicht-positiven ganzen Zahlen hat und nullstellenfrei in $\mathrm{Re}\, s \geq 1$ ist[1]. Weiterhin ist bekannt, dass $\mathrm{L}(s, \chi)$ unendlich viele Nullstellen in der Menge $\{s \in \mathbb{C} \; ; \; 0 < \mathrm{Re}\, s < 1\}$, die im folgenden der **kritische Streifen** genannt wird, hat.
Aus den Funktionalgleichungen von $\mathrm{L}(s, \chi)$ (2.5 und 2.6) folgt, dass die Nullstellen von $\mathrm{L}(s, \chi)$, im kritischen Streifen, punktsymmetrisch zu $s = 1/2$ auftreten. Insbesondere hat die Funktion $\mathrm{L}(s, \chi)$ eine Nullstelle mit Realteil $1/2 - \delta$, $(0 \leq \delta < 1/2)$, falls sie eine Nullstelle mit Realteil $1/2 + \delta$ hat.
Abschätzungen von komplexen Integralen über $\frac{\mathrm{L}'}{\mathrm{L}}(s, \chi)$ werden umso besser, je kleiner eine obere Schranke für die Realteile von Nullstellen ist. Die erweiterte Riemannsche

[1] im Fall $\chi = \chi_1$ hat $\mathrm{L}(s, \chi)$ einen Pol an $s = 1$

Hypothese besagt nun, dass sich die Nullstellen bezüglich dieses Kriteriums so gut verhalten, wie nur möglich.

Hypothese 1.1.1 ***Erweiterte Riemannsche Hypothese (ERH)***
Sei χ ein Dirichlet-*Charakter. Dann haben alle Nullstellen von $\mathrm{L}(s,\chi)$ im kritischen Streifen den Realteil $1/2$.*

1.2 Formulierung des Satzes

Definition 1.2.1 *Für eine natürliche Zahl n setzen wir*

$$G(n) := \min\{x \in \mathbb{R}\,;\ (\mathbb{Z}/(n))^*\ \textit{wird von Primzahlen } p \le x,\ p \not| n\ \textit{erzeugt}\}.$$

Wie bereits erwähnt, ist eine äquivalente Formulierung die, daß $G(n)$ das Supremum der reellen Zahlen x ist, für die es eine echte Untergruppe von $(\mathbb{Z}/(n))^*$ gibt, die alle $p \in (\mathbb{Z}/(n))^*$, $p \le x$ enthält.
Aus der eindeutigen Primfaktorzerlegung folgt, daß man in der Formulierung auch "Primzahl" durch "natürliche Zahl größer 1" hätte ersetzen können.
Leicht lässt sich zeigen, daß $G(n)$ eine natürliche Zahl ist.

Wir formulieren nun den Hauptsatz dieser Arbeit:

Satz 1.2.2 ***Der Satz von Ankeny***
Unter Voraussetzung der ERH *gilt $G(n) = \mathcal{O}\left((\log n)^2\right)$.*

Der Beweis von (1.2.2) wird in Kapitel 2 folgen.
Für die Anwendungen in Kapitel 3 notieren wir das folgende Korollar, welches äquivalent zum Satz von Ankeny ist.

Korollar 1.2.3 *(ERH) Es gibt eine Konstante C so, dass für alle $n \in \mathbb{N}$ und jede echte Untergruppe $U \in (\mathbb{Z}/n)^*$ gilt:*
Es gibt eine positive ganze Zahl $a < C \cdot (\log n)^2$ mit $a \in (\mathbb{Z}/n)^* \setminus U$.

□

Korollar (1.2.3) genügt, um zu zeigen, dass für die algorithmischen Probleme in Kapitel 3 polynomiale Algorithmen existieren. Um einen Algorithmus anzugeben benötigt man oft die Konstante C explizit.
Hierfür zitieren wir [BS96, Theorem 8.8.17] dessen Beweis in [Bac90] gefunden werden kann.

Satz 1.2.4 *(ERH) Sei U eine echte Untergruppe von $(\mathbb{Z}/n)^*$. Dann gibt es ein $m > 0$ mit $m \notin U$ und $m \le 2(\log n)^2$. Ferner gibt es ein $m' \in (\mathbb{Z}/n)^* \setminus U$ mit $m' \le 3(\log n)^2$.*

□

1.3 Heuristik zum Satz von Ankeny

Die Idee besteht darin, die Summe

$$\sum_{p\leq x}\Lambda(p)\,\chi(p)\,(x-p)\,, \tag{1.1}$$

unter bestimmten Voraussetzungen an x und χ, geeignet nach oben und unten abzuschätzen.
Nehmen wir an, $x\in\mathbb{R}$ sei so (klein), dass die Primzahlen kleiner gleich x die multiplikative Gruppe $(\mathbb{Z}/(n))^*$ noch nicht erzeugen. Dann erzeugen sie eine echte Untergruppe U von $(\mathbb{Z}/(n))^*$ und wir finden einen nichttrivialen DIRICHLET-Charakter χ modulo n, der auf U identisch 1 ist. Unter Vernachlässigung der Primteiler von n (deren Beitrag, wie sich noch zeigen wird, gering ist) ist χ identisch 1 auf allen Primzahlen kleiner gleich x. Damit erhält man eine untere Abschätzung für (1.1):

$$\sum_{p\leq x}\Lambda(p)\,\chi(p)\,(x-p)\approx\sum_{p\leq x}(\log p)\,(x-p)\approx\frac{x^2}{2}.$$

Die letzte Abschätzung folgte aus dem Primzahlsatz.
Als Abschätzung nach oben wollen wir einen Term, der für festes n von kleinerer Größenordnung in x ist. Wir werden sehen, dass wir eine Abschätzung der Form $\mathcal{O}\left(x^{2-\delta}\log n\right)$ für die Summe (1.1) erhalten, wobei δ, je nach Aufwand den wir treiben, zwischen 0 (exklusiv) und 1/2 (inklusiv) liegt. Dann folgt aus unterer und oberer Abschätzung: $x^2=\mathcal{O}\left(x^{2-\delta}\log n\right)$, also $x^\delta=\mathcal{O}(\log n)$, also $x=\mathcal{O}\left((\log n)^{1/\delta}\right)$, was polynomial in der Stellenzahl von n ist. Das beste Resultat, das wir erhalten werden ist $\delta=1/2$, also $x=\mathcal{O}\left((\log n)^2\right)$
Die Abschätzung nach oben ist wesentlich komplizierter und wir werden hierfür starken Gebrauch von der erweiterten Riemannschen Hypothese machen.
Die Vorgehensweise lässt sich folgendermaßen skizzieren: Um die Summe (1.1) als komplexes Integral auszudrücken bemerken wir, dass für die logarithmische Ableitung von $\mathrm{L}(s,\chi)$ gilt:

$$-\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)=\sum_{n=1}^{\infty}\frac{\Lambda(n)\,\chi(n)}{n^s}.$$

Die PERRONSCHE Formel [2] besagt, dass für ein $c\in\mathbb{R}$, welches größer ist als die absolute Konvergenzabszisse der Reihe, und für $y>0$ gilt:

$$\sum_{n\leq y}\Lambda(n)\,\chi(n)=-\frac{1}{2\pi i}\int\limits_{c-i\infty}^{c+i\infty}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,\frac{x^s}{s}\,ds.$$

Bilden wir über diese Gleichung das Integral von 0 bis x nach y, so erhalten wir:

$$\sum_{n\leq x}\Lambda(n)\,\chi(n)\,(x-n)=-\frac{1}{2\pi i}\int\limits_{c-i\infty}^{c+i\infty}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,\frac{x^{s+1}}{s(s+1)}\,ds. \tag{1.2}$$

[2] wir werden eine ähnliche Formel in Lemma (2.5.2) beweisen

Obwohl wir über alle natürlichen Zahlen, und nicht nur über Primzahlen, summieren, haben wir damit schon beinahe die gewünschte Summe erhalten. Die MANGOLD Funktion $\Lambda(n)$ ist 0 wenn n keine Primzahlpotenz ist. Motiviert durch ähnliche Fälle wollen wir einmal annehmen, dass die Primpotenzen p^k mit $k \geq 2$ einen Beitrag von geringerer Größenordnung liefern, und begnügen uns damit, das Integral abzuschätzen.
Hierzu bemerken wir, zunächst ohne Beweis (siehe Satz (2.4.7)), dass sich die Funktion $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ - wenn wir einen konstanten Abstand von den Nullstellen von L einhalten - im Wesentlichen durch $\mathcal{O}(\log(m|t|))$ abschätzen können, wobei m der Modulus von χ und t der Imaginärteil von s ist. Im Bereich $\operatorname{Re} s \geq 1+\varepsilon > 1$ lässt sich $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ durch eine Konstante abschätzen.
Der reelle Parameter c darf in $\mathbb{R}_{>1}$ frei gewählt werden; der maßgebliche Anteil des Integrals in Gleichung (1.2) ist dann allerdings $x^{c+1} > x^2$, und dies ist bereits zu groß. Wir müssen also die Integrationslinie weiter nach links verschieben, um den Exponenten unter 2 zu drücken. Hierfür wenden wir den CAUCHYSCHEN Integralsatz, bzw. den Residuensatz an.
Nach der erweiterten Riemannschen Hypothese hat $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ - da χ nicht der Hauptcharakter ist - keine Polstellen in $\operatorname{Re} s > 1/2$. Wenden wir den CAUCHYSCHEN Integralsatz auf ein Rechteck mit den Ecken $\frac{1}{2}+\delta' \pm iT$, $c \pm iT$ für $T > 0$, $c > 1$, $\delta' > 0$ an, und lassen dann T gegen ∞ gehen, so können wir die Summe in (1.2) durch das Integral über die Gerade $\operatorname{Re} s = \frac{1}{2}+\delta'$ ausdrücken.
Nun erhalten wir für die Summe - mit Hilfe von Satz (2.4.7) - die Größenordnung $\mathcal{O}\left(x^{3/2+\delta'}\log n\right)$, für jedes $\delta' > 0$, was genügt, $G(n) = \mathcal{O}\left((\log n)^{2+\varepsilon}\right)$, für jedes $\varepsilon > 0$ zu beweisen, was bereits polynomial in der Stellenzahl von n ist.
Um schließlich auf den behaupteten Exponenten von 2 zu kommen müssen wir die Integrationslinie in den Bereich $0 < \operatorname{Re} s < 1/2$ verschieben. Dann schließen wir aber Polstellen von $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ ein und müssen den Residuensatz anwenden, sowie etwas kompliziertere Terme abschätzen (siehe 2.6.1).
Wir bemerken schon hier, dass es mit dieser Methode egal sein wird wo genau wir die Integrationslinie ziehen - solange wir nur zwischen 0 und 1/2 bleiben. Zwar liefert das Integral einen umso kleineren Wert, je weiter wir nach links gehen; es wird sich aber die Summe über die Residuen an den Nullstellen von L als der dominante Term herausstellen, und dieser ist bereits von der Größenordnung $\mathcal{O}\left(x^{3/2}\log n\right)$. Im Beweis werden wir, um uns weitere Parameter zu ersparen, über die Gerade $\operatorname{Re} s = 1/4$ integrieren.

Kapitel 2

Beweis des Satzes von Ankeny

2.1 Gliederung des Beweises

Wir verteilen die Beweisschritte, die wir in Abschnitt (1.3) angedeutet haben, folgendermaßen auf die Abschnitte dieses Kapitels:

Um das Integral in Gleichung (1.2) geeignet abschätzen zu können benötigen wir erstens, dass die Nullstellen von $\mathrm{L}(s, \chi)$ im kritischen Streifen nicht zu dicht liegen, und zweitens, dass die logarithmische Ableitung von L im kritischen Streifen (und in hinreichender Entfernung der Nullstellen) nicht zu stark wächst. Wir werden dies in Abschnitt (2.4) zeigen.

Dazu benötigen wir aber einige bekannte Sätze aus der Funktionentheorie, nämlich die Funktionalgleichung von L, die in (2.2) notiert wird, sowie die Produktentwicklung einer Funktion, die L sehr ähnlich ist und die wir in Abschnitt (2.3) aus der Funktionalgleichung ableiten werden.

Obwohl wir die Resultate aus Abschnitt (2.4) nicht nur für primitive, sondern für allgemeine Dirichlet-Charaktere brauchen, werden wir zunächst nur mit primitiven arbeiten. Beide Resultate lassen sich dann aber leicht, im benötigten Umfang, auf allgemeine Charaktere verallgemeinern.

In Abschnitt (2.5) beweisen wir, dass die Gleichung (1.2) gilt. In Abschnitt (2.6) führen wir die Verschiebung der Integrationslinie mittels des Residuensatzes durch und zeigen, dass dann das Integral, sowie die Summe über die Residuen, wie behauptet beschränkt sind, woraus die obere Abschätzung folgt.

In Abschnitt (2.7) folgt dann schließlich der eigentliche Beweis von Ankenys Theorem (1.2.2) aus der oberen Abschätzung der Primzahlsumme.

2.2 Funktionalgleichung der L-Funktionen

Wir notieren in diesem Abschnitt einige bekannte Sätze aus der Funktionentheorie, die wir nicht beweisen werden. Diese Sätze können zum Beispiel in [Brü95] gefunden werden.

In den Funktionalgleichungen spielt die sogenannte Gammafunktion eine ent-

scheidende Rolle, siehe [Brü95, 2.1]. Sie wird zunächst in $\operatorname{Re} s > 0$ durch

$$\Gamma(s) := \int_0^\infty e^{-u} u^{s-1}\, du \tag{2.1}$$

definiert. Dort ist sie holomorph in s. Mittels der Funktionalgleichung $s\Gamma(s) = \Gamma(s+1)$ lässt sie sich meromorph auf ganz $\mathbb{C}$ fortsetzen. Γ hat an den Stellen $-n$ für $n \in \mathbb{N}_0$ Pole erster Ordnung, sonst ist sie holomorph und hat keine Nullstellen.
Für später benötigen wir noch eine Abschätzung für Γ, sowie für die logarithmische Ableitung von Γ die als STIRLINGSCHE Formel bekannt ist.

Satz 2.2.1 *Sei $\delta > 0$. Für $s \in \mathbb{C}$, $|\arg(s)| \le \pi - \delta$ gelten:*

$$\log \Gamma(s) = \left(s - \frac{1}{2}\right) \log s - s + \frac{1}{2} \log 2\pi + \mathcal{O}\left(|s|^{-1}\right) \tag{2.2}$$

und

$$\frac{\Gamma'}{\Gamma}(s) = \log s + \mathcal{O}\left(|s|^{-1}\right). \tag{2.3}$$

Wie bereits erwähnt werden die folgenden Sätze zunächst nur für primitive Charaktere notiert. Dies ist aber keine wesentliche Einschränkung, da falls ein DIRICHLET-Charakter χ mod m von einem (primitiven) Charakter χ' mod m' induziert wird, so folgt aus den Eulerprodukten für L

$$\mathrm{L}(s,\chi) = \prod_{p \nmid m} \left(1 - \frac{\chi'(p)}{p^{-s}}\right)^{-1} = \mathrm{L}(s,\chi') \prod_{p \mid m} \left(1 - \frac{\chi'(p)}{p^{-s}}\right), \tag{2.4}$$

d.h. jede L-Funktion ist gleich einer L-Funktion über einen primitiven Charakter, mal ein endliches Produkt.

Wir geben als nächstes die Funktionalgleichung für die DIRICHLETSCHEN L-Funktionen an; diese kann in [Brü95, 2.4] gefunden werden.
Wir benötigen die Definition der GAUSSSCHEN Summe:

Definition 2.2.2 *Sei χ ein* DIRICHLET*-Charakter modulo m. Setze die* GAUSSSCHE *Summe $\tau(\chi)$ durch*

$$\tau(\chi) := \sum_{n=1}^{m} \chi(n) \exp(2\pi i n/m)$$

Die Funktionalgleichung für L nimmt eine etwas andere Gestalt an, je nachdem ob $\chi(-1) = 1$, oder $\chi(-1) = -1$.

Satz 2.2.3 ***Funktionalgleichung von*** L
Sei χ ein primitiver Charakter modulo $m \ge 2$ mit $\chi(-1) = 1$. Dann ist $\mathrm{L}(s,\chi)$ eine ganze Funktion in s, und es gilt:

$$\Gamma\left(\frac{1-s}{2}\right) \mathrm{L}(1-s,\overline{\chi}) = \frac{\sqrt{m}}{\tau(\chi)} \left(\frac{\pi}{m}\right)^{-s+\frac{1}{2}} \Gamma\left(\frac{s}{2}\right) \mathrm{L}(s,\chi). \tag{2.5}$$

Es gilt $\mathrm{L}(s,\chi) = 0$ für $s = 0, -2, -4, \ldots$, alle anderen Nullstellen liegen im kritischen Streifen.

Sei χ ein primitiver Charakter modulo $m \geq 2$ mit $\chi(-1) = -1$. Dann ist $\mathrm{L}(s,\chi)$ eine ganze Funktion in s, und es gilt:

$$\Gamma\left(\frac{2-s}{2}\right)\mathrm{L}(1-s,\overline{\chi}) = \frac{i\sqrt{m}}{\tau(\chi)}\left(\frac{\pi}{m}\right)^{-s+\frac{1}{2}}\Gamma\left(\frac{s+1}{2}\right)\mathrm{L}(s,\chi). \tag{2.6}$$

Es gilt $\mathrm{L}(s,\chi) = 0$ für $s = -1,-3,-5,\ldots$, alle anderen Nullstellen liegen im kritischen Streifen.

□

Die beiden Funktionalgleichungen (2.5) und (2.6) können auf eine einfachere Form gebracht werden. Hierfür definieren wir eine ganze Funktion, deren Nullstellen genau die Nullstellen von $\mathrm{L}(s,\chi)$ im kritischen Streifen sind.

Definition 2.2.4 *Sei χ ein* DIRICHLET-*Charakter modulo $m \geq 2$. Ferner sei $\kappa = 1$ falls $\chi(-1) = -1$ und $\kappa = 0$ falls $\chi(-1) = 1$. Wir definieren:*

$$\xi(s,\chi) := \left(\frac{\pi}{m}\right)^{-\frac{s}{2}}\Gamma\left(\frac{1}{2}(s+\kappa)\right)\mathrm{L}(s,\chi). \tag{2.7}$$

Die Pole von $\Gamma\left(\frac{1}{2}(s+\kappa)\right)$ fallen dabei genau mit den Nullstellen von $\mathrm{L}(s,\chi)$, die auf der negativen reellen Achse liegen, zusammen und werden so zu einer hebbaren Singularität.
Für primitive Charaktere χ folgt aus Satz (2.2.3) eine Funktionalgleichung für ξ:

Korollar 2.2.5 *Sei χ ein primitiver Charakter modulo m. Dann gilt*

$$\xi(1-s,\overline{\chi}) = \frac{\mathrm{i}^{\kappa}\sqrt{m}}{\tau(\chi)}\xi(s,\chi). \tag{2.8}$$

ξ ist ganz und außerhalb des kritischen Streifens nullstellenfrei.

2.3 Hadamard-Produkt

Wir werden als nächstes die Funktion ξ als ein Produkt über die Nullstellen darstellen. Diese Darstellung folgt aus dem Produksatz von HADAMARD. Der Beweis folgt im Wesentlichen [Brü95, 2.5], nur wurde hier die JENSENSCHE Formel durch eine einfachere Aussage ersetzt, die für den Beweis ausreicht.

Definition 2.3.1 *Wir bezeichnen mit $\mathcal{N}(\chi)$ die Folge [1] der Nullstellen ρ von $\xi(s,\chi)$, mit $0 < \mathrm{Re}\,\rho < 1$, wobei jede Nullstelle gemäß ihrer Vielfachheit aufgelistet sei.*

$\mathcal{N}(\chi)$ ist, wie bereits bemerkt, identisch mit der Folge der Nullstellen von $\mathrm{L}(s,\chi)$ im kritischen Streifen.

[1] die genaue Reihenfolge ist egal

Satz 2.3.2 ***Das Hadamard-Produkt von*** ξ.
Sei χ *ein primitiver Charakter modulo* $m \geq 2$. *Dann hat* $\xi(s,\chi)$ *unendlich viele Nullstellen im kritischen Streifen und für geeignete komplexe Zahlen* $A = A(\chi)$ *und* $B = B(\chi)$ *gilt*

$$\xi(s,\chi) = \mathrm{e}^{(A+Bs)} \prod_{\rho \in \mathcal{N}(\chi)} \left(1 - \frac{s}{\rho}\right) \mathrm{e}^{s/\rho}. \tag{2.9}$$

Für den Beweis von (2.3.2) zeigen wir zuächst einige Aussagen über ganze Funktionen, deren Wachstumsverhalten gewissen Schranken unterliegt.

Lemma 2.3.3 *Seien* $C, \lambda > 0$ *reelle Konstanten. Ferner sei* f *eine ganze Funktion die die Abschätzung* $\mathrm{Re}\, f(s) \leq C(1 + |s|^{\lambda})$ *für alle* s *auf einer Folge von Kreislinien* $|s| = R_\nu$ *mit* $\lim_{\nu\to\infty} R_\nu = \infty$ *erfüllt.*
Dann ist f *ein Polynom vom Grad kleiner, gleich* $\lfloor \lambda \rfloor$.

Die Voraussetzungen sind z.B. dann erfüllt wenn $f(s) = \mathcal{O}\left(|s|^{\lambda}\right)$ gilt. Wir werden in der Anwendung von Lemma (2.3.3) aber tatsächlich nur die schwächeren Voraussetzungen haben.
Beweis: Der Beweis beruht auf den aus der reellen Analysis bekannten Orthogonalitätsrelationen

$$\int_0^{2\pi} \cos(k\alpha)\sin(n\alpha)\, d\alpha = 0, \tag{2.10}$$

und

$$\int_0^{2\pi} \cos(k\alpha)\cos(n\alpha)\, d\alpha = \int_0^{2\pi} \sin(k\alpha)\sin(n\alpha)\, d\alpha = \begin{cases} \pi & \text{für } k = n, \\ 0 & \text{für } k \neq n, \end{cases} \tag{2.11}$$

für $k, n \in \mathbb{N}$.
Betrachtet man die Funktion $f(s) - f(0)$ anstelle von f so sieht man, dass ohne Einschränkung $f(0) = 0$ angenommen werden kann. Damit hat f eine in ganz $\mathbb{C}$ konvergente Potenzreihenentwicklung der Form

$$f(s) = \sum_{n=1}^{\infty} (a_n + ib_n) s^n$$

mit reellen a_n, b_n. Schreibt man $s = r\mathrm{e}^{i\theta}$ so erhält man

$$\mathrm{Re}\, f(s) = \sum_{n=1}^{\infty} (a_n \cos(n\theta) - b_n \sin(n\theta)) r^n.$$

Die Reihe konvergiert gleichmäßig auf $|s| = r$. Daher folgt, für $k \geq 1$, aus (2.10) und (2.11) durch Vertauschung von Summation und Integration

$$\int_0^{2\pi} \cos(k\theta)\mathrm{Re}\, f(s)\, d\theta = a_k r^k \pi,$$

wobei $r = |s|$. Diese Formel gilt wegen $a_0 = 0$ und dem CAUCHYCHEN Integralsatz auch noch für $k = 0$. Damit folgt für $k \geq 0$, $\nu \in \mathbb{N}$ und $s = R_\nu \cdot \mathrm{e}^{i\theta}$

$$|a_k| \leq \frac{1}{\pi R_\nu^k} \int_0^{2\pi} |\mathrm{Re}\, f(s)|\, d\theta = \frac{1}{\pi R_\nu^k} \int_0^{2\pi} |\mathrm{Re}\, f(s)| + \mathrm{Re}\, f(s)\, d\theta$$

$$= \frac{2}{\pi R_\nu^k} \int_0^{2\pi} \max(\mathrm{Re}\, f(s), 0)\, d\theta = \mathcal{O}\left(R_\nu^{\lambda-k}\right).$$

Ist nun $k > \lambda$ so folgt mit $\nu \to \infty$ (also $R_\nu \to \infty$), dass $a_k = 0$ gilt.
Für die b_k wird das Integral $\int_0^{2\pi} \sin(k\theta)\mathrm{Re}\, f(s)\, d\theta$ gebildet, ansonsten wird genau gleich argumentiert. □

Lemma (2.3.3) kann nun auf ganze, nullstellenfreie Funktionen, deren Logarithmus einer Abschätzung durch ein Polynom genügt, angewandt werden. Wir benötigen den Begriff der Wachstumsordnung einer ganzen Funktion.

Definition 2.3.4 *Eine ganze Funktion f, die einer Abschätzung $f(s) = \mathcal{O}\left(\exp\left(|s|^\alpha\right)\right)$, $\alpha > 0$ genügt, heißt eine Funktion **endlicher Ordnung**. Für solche Funktionen f heißt die reelle Zahl*

$$\inf\left\{\alpha > 0\ ;\ f(s) = \mathcal{O}\left(\exp\left(|s|^\alpha\right)\right)\right\}$$

*die **Ordnung** von f.*

Die Bedingung $\alpha > 0$ benötigt man dafür, dass die Menge nach unten beschränkt ist. Tatsächlich würde für eine konstante (und damit ganze) Funktion f die Abschätzung $f(s) = \mathcal{O}\left(\exp\left(|s|^\alpha\right)\right)$ für jedes $\alpha \in \mathbb{R}$ gelten. Interessant ist diese Definition aber nur für nicht-konstante Funktionen und für diese gilt die Abschätzung $f(s) = \mathcal{O}\left(\exp\left(|s|^0\right)\right)$ nicht mehr, d.h. die Ordnung ist größer, gleich 0 (auch wenn man in obiger Definition die Bedingung $\alpha > 0$ fallen lassen würde).
Das nächste Lemma zeigt, dass ganze, nullstellenfreie Funktionen endlicher Ordnung sehr genau charakterisiert werden können.

Lemma 2.3.5 *Ist f eine ganze, nullstellenfreie Funktion endlicher Ordnung so gilt $f = \mathrm{e}^P$ mit einem Polynom P. Die Ordnung von f ist der Grad von P.*

Beweis: Wir zeigen zuerst, dass $\log f$ eine ganze Funktion ist.
Da f nullstellenfrei und ganz ist, ist die (zunächst nur meromorphe) Funktion f'/f ganz. Das heißt f'/f lässt sich durch ein global konvergente Potenzreihe

$$\frac{f'}{f}(s) = \sum_{n=0}^{\infty} a_n s^n$$

mit gewissen $a_n \in \mathbb{C}$ darstellen. Wir definieren eine ganze Funktion g indem wir diese Potenzreihe koeffizientenweise integrieren und einen Absolutkoeffizienten addieren so, dass $\exp(g(0)) = f(0)$:

$$g(s) := \log(f(0)) + \sum_{n=0}^{\infty} \frac{a_n}{n+1} s^{n+1}.$$

Da $g' = f'/f$ gilt, ist $g = \log f + c$ für eine Konstante c. Der Wert von g an 0 liefert, dass diese Konstante gleich 0 ist.
Sei α die Ordnung von f, $\varepsilon > 0$. Es gilt $\operatorname{Re} g(s) \leq C(|s|^{\alpha+\varepsilon})$, nach Lemma (2.3.3) ist g also ein Polynom vom Grad kleiner, gleich $\lfloor \alpha \rfloor$. Wir haben nur noch zu zeigen, dass $\deg g = \lfloor \alpha \rfloor = \alpha$ ist. Dies ist aber klar, da sonst $f = \exp(g)$ eine kleinere Ordnung als α hätte. □

Bemerkung 2.3.6 *Nach Lemma (2.3.3) genügt es, die Abschätzung* $f(s) = \mathcal{O}(\exp(|s|^{\alpha}))$ *auf einer Folge von Kreislinien* $|s| = R_\nu$ *mit* $\lim_{\nu\to\infty} R_\nu = \infty$ *zu haben.*

Wir werden als nächstes allgemeine Funktionen endlicher Ordnung behandeln. Dafür zeigen wir zunächst, dass deren Nullstellen nicht zu dicht liegen können.

Lemma 2.3.7 *Seien* $0 < r < R$ *reelle Zahlen. Ferner sei* f *holomorph in* $|s| \leq R$ *und habe mindestens* n *Nullstellen (gemäß ihrer Vielfachheit gezählt) in* $|s| \leq r$.
Dann ist mit $M := \max\{|f(s)| \,;\, |s| = R\}$

$$|f(0)| \left(\frac{R}{r}\right)^n \leq M.$$

Dieses Lemma ist eine Verschärfung des Maximumprinzips. Gilt zusätzlich $f(0) \neq 0$ so kann es dazu benutzt werden die Anzahl der Nullstellen in $|s| \leq r$ abzuschätzen.
Beweis: Seien $a_1, \ldots, a_n$ alle Nullstellen von f in $|s| \leq r$ (entsprechend ihrer Vielfachheit gezählt). Setze

$$\phi(s) := f(s) \cdot \prod_{\nu=1}^{n} \frac{R^2 - \overline{a}_\nu s}{R(s - a_\nu)}.$$

Die Singularitäten von ϕ (die genau an den a_ν auftreten) sind alle hebbar, da sie mit den Nullstellen von f zusammenfallen. Daher ist ϕ holomorph in $|s| \leq R$. Weiterhin gilt $R^2 - \overline{a}_\nu s \neq 0$ für alle $\nu = 1, \ldots, n$ und alle s mit $|s| \leq R$, da $|\overline{a}_\nu| \leq r < R$, also $|\overline{a}_\nu s| < R^2$.
Somit erhält man für $|s| \leq R$

$$f(s) = \phi(s) \prod_{\nu=1}^{n} \frac{R(s - a_\nu)}{R^2 - \overline{a}_\nu s}. \tag{2.12}$$

Speziell für $|s| = R$ und $\nu = 1, \ldots, n$ gilt

$$\begin{aligned} |R(s - a_\nu)|^2 = R^2(s\overline{s} - s\overline{a}_\nu - a_\nu\overline{s} + a_\nu\overline{a}_\nu) &= R^2 \left(R - \overline{a}_\nu \frac{s}{R}\right)\left(R - a_\nu \frac{\overline{s}}{R}\right) \\ &= |R^2 - \overline{a}_\nu s|^2, \end{aligned}$$

so, dass $\left|\frac{R(s-a_\nu)}{R^2-\overline{a}_\nu s}\right| = 1$ für $|s| = R$, $\nu = 1, \ldots, n$ folgt. Daher gilt $|\phi(s)| = |f(s)| \leq M$ für $|s| = R$, und nach dem Maximumprinzip $|\phi(0)| \leq M$. Aus Gleichung (2.12) erhält man damit

$$|f(0)| = |\phi(0)| \prod_{\nu=1}^{n} \frac{R|a_\nu|}{R^2} \leq M \left(\frac{r}{R}\right)^n$$

und daraus $|f(0)| \cdot \left(\frac{R}{r}\right)^n \leq M$, wie behauptet. □

Wir werden für den Rest des Abschnitts voraussetzen, dass die betrachteten Funktionen nicht identisch verschwinden, um den trivialen Sonderfall der Nullfunktion auszuschließen. D.h. die betrachteten Funktionen haben höchstens abzählbar viele Nullstellen.

Satz 2.3.8 *Sei f eine ganze Funktion der Ordnung α. Die Folge der Nullstellen von f sei $s_1, s_2, \dots$, wobei jede Nullstelle entsprechend ihrer Vielfachheit aufgelistet sei. Dann gilt für jedes $\varepsilon > 0$*

$$\sum_{j:|s_j|\leq R} 1 = \mathcal{O}(R^{\alpha+\varepsilon}).$$

Ist $\beta > \alpha$, so konvergiert die Reihe

$$\sum_{s_j\neq 0} |s_j|^{-\beta}.$$

Beweis: Sei $\varepsilon > 0$. Wir können f als $f(s) = s^k g(s)$ mit einer ganzen Funktion g mit $g(0) \neq 0$ schreiben. Daher gelte ohne Einschränkung $f(0) \neq 0$. Wir schreiben $\mathrm{num}(R)$ als die Anzahl der Nullstellen von f in $|s| \leq R$. Aus Lemma (2.3.7) folgt für $R > 0$, e die Eulerzahl

$$\left(\frac{\mathrm{e}R}{R}\right)^{\mathrm{num}(R)} \leq \frac{M_{\mathrm{e}R}}{|f(0)|},$$

wobei $M_{\mathrm{e}R}$ das Maximum von f auf $|s| = \mathrm{e}R$ bezeichne. Da f von Ordnung α ist gibt es ein $C > 0$ so, dass $M_{\mathrm{e}R} \leq C \exp\left((\mathrm{e}R)^{\alpha+\varepsilon/2}\right) \leq C \exp\left(R^{\alpha+\varepsilon}\right)$, für große R. Damit folgt

$$\sum_{j:|s_j|\leq R} 1 = \mathrm{num}(R) \leq \log \frac{M_{\mathrm{e}R}}{|f(0)|} = \mathcal{O}(R^{\alpha+\varepsilon}).$$

Die Konvergenz der Reihe folgt aus der Abschätzung für die Anzahl der Nullstellen mittels partieller Summation, die wir ohne Beweis im folgenden Lemma notieren werden[2].

Lemma 2.3.9 *Seien $y \in \mathbb{R}_{\geq 0}$, $g : [y, \infty) \to \mathbb{C}$ stetig differenzierbar. Seien $a_n \in \mathbb{C}$ gegeben und $A(x) := \sum_{n\leq x} a_n$. Dann gilt für $x > y$*

$$\sum_{y<n\leq x} a_n g(n) = A(x)g(x) - A(y)g(y) - \int_y^x A(\xi)g'(\xi)\,d\xi. \tag{2.13}$$

□

Hier setze $a_n := \mathrm{num}(n+1) - \mathrm{num}(n)$ und $g : [1, \infty) \to \mathbb{C}; t \mapsto t^{-\beta}$.

[2] siehe z.B. [Brü95, Lemma 1.1.3]

Sei α' so gewählt, dass $\alpha < \alpha' < \beta$. Dann zeigt das bereits Bewiesene, dass es eine Konstante $C' > 0$ gibt so, dass $\mathrm{num}(R) \leq C' R^{\alpha'}$. Es folgt für $N \in \mathbb{N}$

$$\begin{aligned}\sum_{2\leq|s_j|\leq N} |s_j|^{-\beta} &\leq \sum_{n>1}^{N} \sum_{j:n\leq|s_j|\leq n+1} n^{-\beta} = \sum_{n>1}^{N} a_n g(n) \\ &\overset{(2.3.9)}{=} \mathrm{num}(N)\cdot N^{-\beta} - \mathrm{num}(1) + \int_1^N \beta \frac{\mathrm{num}(\xi)}{\xi^{\beta+1}}\, d\xi \\ &\leq C' N^{\alpha'-\beta} - \mathrm{num}(1) + C'\beta \int_1^N \xi^{\alpha'-\beta-1}\, d\xi.\end{aligned}$$

Wegen $\beta > \alpha'$ ist $\alpha' - \beta - 1 < -1$, d.h. das Integral $\int_1^\infty \xi^{\alpha'-\beta-1}\, d\xi$ existiert; außerdem gilt $N^{\alpha'-\beta} \to 0$ für $N \to \infty$, was die Konvergenz der Reihe zeigt. □

Wir können nun zeigen, dass sich ganze Funktionen endlicher Ordnung als ein Produkt über die Nullstellen schreiben lassen. Allerdings werden wir dies nur für Funktionen der Ordnung 1 formulieren.

Satz 2.3.10 ***(Hadamard)***
Sei f eine ganze Funktion der Ordnung 1. Sei $k := 0$, falls 0 keine Nullstelle von f ist, sonst sei k die Ordnung der Nullstelle von f bei 0. Seien $s_j, j \in J \subset \mathbb{N}$ die Nullstellen von f in $s \neq 0$ entsprechend ihrer Vielfachheit aufgelistet. Dann gilt

$$f(s) = s^k \mathrm{e}^{A+Bs} \prod_{j\in J} \left(1 - \frac{s}{s_j}\right) \mathrm{e}^{s/s_j},$$

für geeignete komplexe Zahlen A und B.

Der Satz gilt auch für ganze Funktionen endlicher Ordnung $\alpha > 1$ mit einem Polynom vom Grad $\lfloor \alpha \rfloor$ in s anstatt $A + Bs$ und etwas komplizierteren Exponenten über e. Wir werden ihn aber nur in dieser Form benötigen und auch nur in dieser beweisen.
Beweis: Ist J endlich,so folgt die Aussage des Satzes aus Lemma (2.3.5) nach Abspalten von endlich vielen Faktoren der Form $(1 - s/s_j)\,\mathrm{e}^{s/s_j}$. Daher gelte ohne Einschränkung $J = \mathbb{N}$.
Abspalten von s^k zeigt weiterhin, dass wir ohne Einschränkung $f(0) \neq 0$ annehmen können. Nach Satz (2.3.8) konvergiert also die Reihe $\sum |s_j|^{-2}$. Wir setzen

$$P(s) := \prod_{j=1}^{\infty} \left(1 - \frac{s}{s_j}\right) \mathrm{e}^{s/s_j},$$

und zeigen als nächstes, dass P auf jeder kompakten Teilmenge von $\mathbb{C}$ gleichmäßig und absolut konvergiert, also eine ganze Funktion darstellt, welche unabhängig von der Abzählung der Nullstellen wohldefiniert ist.

Für alle j gilt

$$\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j} = \left(1-\frac{s}{s_j}\right)\left(1+\frac{s}{s_j}+\frac{1}{2}\left(\frac{s}{s_j}\right)^2+\sum_{\nu=3}^{\infty}\frac{1}{\nu!}\left(\frac{s}{s_j}\right)^{\nu}\right)$$
$$= 1-\frac{1}{2}\left(\frac{s}{s_j}\right)^2-\sum_{\nu=3}^{\infty}\frac{\nu-1}{\nu!}\left(\frac{s}{s_j}\right)^{\nu}.$$

Das heißt

$$P(s) := \prod_{j=1}^{\infty}\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}$$

ist absolut konvergent, genau dann wenn

$$\sum_{j=1}^{\infty}\left|\frac{1}{2}\left(\frac{s}{s_j}\right)^2+\sum_{\nu=3}^{\infty}\frac{\nu-1}{\nu!}\left(\frac{s}{s_j}\right)^{\nu}\right| = \sum_{j=1}^{\infty}\frac{1}{|s_j|^2}\cdot\left|\frac{1}{2}s^2+s^2\sum_{\nu=3}^{\infty}\frac{\nu-1}{\nu!}\left(\frac{s}{s_j}\right)^{\nu-2}\right| \tag{2.14}$$

konvergiert.
Nun ist $|\frac{1}{2}s^2 - s^2\sum_{\nu=3}^{\infty}\frac{\nu-1}{\nu!}\left(\frac{s}{s_j}\right)^{\nu-2}| < \infty$ für alle $j\in\mathbb{N}$ und s aus einer kompakten Menge. Da $|s_j|\to\infty$ für $j\to\infty$ gilt, [3] sind diese Terme sogar gleichmäßig für alle $j\in\mathbb{N}$ und s aus einer kompakten Menge beschränkt. Aus der Konvergenz von $\sum|s_j|^{-2}$ folgt damit die Konvergenz von (2.14).

P hat genau die Nullstellen von f (mit den gleichen Vielfachheiten), also ist f/P eine ganze nullstellenfreie Funktion. Hat f/P nun auch noch die Ordnung kleiner, gleich 1, so folgt die Behauptung dieses Satzes aus Lemma (2.3.5). Nach Bemerkung (2.3.6) genügt es sogar die Abschätzung $f(s)/P(s) = \mathcal{O}\left(\exp(|s|^{1+\varepsilon})\right)$ (für jedes $\varepsilon>0$) auf einer Folge von Kreislinien $|s|=R_\nu$ mit $\lim_{\nu\to\infty}R_\nu=\infty$ zu haben.
Wir zeigen zuerst, dass eine Folge $(R_\nu)_{\nu\in\mathbb{N}}$ mit $\lim_{\nu\to\infty}R_\nu=\infty$ und $|R-|s_j||>|s_j|^{-2}$ für alle j und alle $R\in(R_\nu)_{\nu\in\mathbb{N}}$ existiert.
Die Summe der Längen der (reellen) Intervalle $I_j := \left[|s_j|-|s_j|^{-2}, |s_j|+|s_j|^{-2}\right]$ ist beschränkt durch $2\sum_{j=1}^{\infty}|s_j|^{-2}<\infty$. Es gilt also $\bigcup_{j=1}^{\infty}I_j \not\supset [a,\infty)$, für alle $a\in\mathbb{R}$. Daher gibt es beliebig große R mit der gewünschten Eigenschaft.
Wir bemerken, dass auch jedes Endstück von $(R_\nu)_{\nu\in\mathbb{N}}$ diese Eigenschaften hat. D.h. wir können (und werden) wiederholt endliche Anfangsstücke der Folge weglassen.
Sei nun $\varepsilon>0$ und $R\in(R_\nu)_{\nu\in\mathbb{N}}$. Wir zeigen $f(s)/P(s)=\mathcal{O}\left(\exp\left(R^{1+\varepsilon}\right)\right)$ auf $|s|=R$.
Dafür teilen wir P in die drei Podukte über die Nullstellen s_j mit $|s_j|<(1/2)R$, $(1/2)R\le|s_j|\le 2R$ und $2R<|s_j|$ auf.
Für den Rest des Beweises gelte $|s|=R$.
Für die j mit $|s_j|<(1/2)R$ gilt:

$$\left|\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}\right| \ge \left(\left|\frac{s}{s_j}\right|-1\right)\mathrm{e}^{-|s|/|s_j|} > \mathrm{e}^{-R/|s_j|}.$$

[3] dies gilt selbst dann wenn die s_j nicht der Größe nach geordnet werden

Dies zeigt für genügend große R

$$\left|\prod_{j:|s_j|<(1/2)R}\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}\right| > \exp\left(-R\sum_{j:|s_j|<(1/2)R}|s_j|^{-1}\right)$$
$$> \exp\left(-R^{1+\varepsilon}\sum_{j:|s_j|<(1/2)R}|s_j|^{-1-\varepsilon}\right).$$

Aus Satz (2.3.8) folgt damit, dass (evtl. wiederum für größere R) die Abschätzung

$$\left|\prod_{j:|s_j|<(1/2)R}\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}\right| > \exp\left(-R^{1+\varepsilon}\sum_{j=1}^{\infty}|s_j|^{-1-\varepsilon}\right) > \exp\left(-R^{1+2\varepsilon}\right) \quad (2.15)$$

gilt.

Für die j mit $|s_j| > 2R$ zeigen wir zuerst, dass es ein $c > 0$ gibt so, dass für alle $\lambda \in \mathbb{C}$ mit $|\lambda| < 1/2$ die Ungleichung

$$|(1-\lambda)\mathrm{e}^{\lambda}| \geq \mathrm{e}^{-c|\lambda|^2} \quad (2.16)$$

gilt. Für (zum Beispiel) $c := 1$ folgt aus

$$(1-\lambda)\,\mathrm{e}^{\lambda} = 1 - \frac{1}{2}\lambda^2 - \sum_{\nu=3}^{\infty}\frac{\nu-1}{\nu!}\lambda^{\nu}.$$

und

$$\mathrm{e}^{-c|\lambda|^2} = 1 - c|\lambda|^2 + c^2|\lambda|^4\sum_{\nu=2}^{\infty}\frac{1}{\nu!}(-c)^{\nu-2}|\lambda|^{2\nu-4},$$

dass es ein $\delta > 0$ gibt so, dass (2.16) für alle $\lambda \in \mathbb{C}$ mit $|\lambda| < \delta$ gilt. Weiterhin gibt es ein $c \geq 1$ so, dass für alle $\delta \leq |\lambda| < 1/2$ die Ungleichung gilt, da die rechte Seite mit $c \to \infty$ (unabhängig von λ im Bereich $\delta \leq |\lambda| < 1/2$) gegen 0 konvergiert. Die Vergrößerung von c macht (2.16) für $|\lambda| < \delta$ nicht ungültig, da auch hier die rechte Seite für größere c kleiner wird.
Aus (2.16) erhält man mit $\lambda = s/s_j$ (es gilt hier $|s/s_j| < 1/2$)

$$\left|\prod_{j:|s_j|>2R}\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}\right| > \exp\left(-c\sum_{j:|s_j|>2R}(R/|s_j|)^2\right).$$

Ohne Einschränkung gelte $\varepsilon < 1$, also $\left(\frac{R}{|s_j|}\right)^{1+\varepsilon} > \left(\frac{R}{|s_j|}\right)^2$, wegen $0 < R/|s_j| < 1$. Somit erhält man, für große R, aus der oberen Abschätzung

$$\left|\prod_{j:|s_j|>2R}\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}\right| > \exp\left(-cR^{1+\varepsilon}\sum_{j=1}^{\infty}|s_j|^{-1-\varepsilon}\right) > \exp\left(-R^{1+2\varepsilon}\right). \quad (2.17)$$

Für die j mit $(1/2)R \leq |s_j| \leq 2R$ benutzt man die spezielle Wahl von R und erhält damit

$$\left|\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}\right| \geq \mathrm{e}^{-2}\left|1-\frac{s}{s_j}\right| \geq \mathrm{e}^{-2}\frac{|s-s_j|}{2R} \geq CR^{-3}, \tag{2.18}$$

für eine positive Konstante $C \in \mathbb{R}$.
Nach Satz (2.3.8) gibt es höchstens $\mathcal{O}(R^{1+\varepsilon})$ viele j mit $(1/2)R \leq |s_j| \leq 2R$ und man erhält aus den Abschätzungen (2.15), (2.17) und (2.18)

$$|P(s)| > \left(C \cdot R^{-3}\right)^{R^{1+\varepsilon}} \exp\left(-2R^{1+2\varepsilon}\right) > \exp\left(-R^{1+3\varepsilon}\right)$$

für genügend große R. Da f die Ordnung 1 hat folgt

$$f(s)/P(s) = \mathcal{O}\left(\exp(R^{1+4\varepsilon})\right)$$

für $|s| = R$, $R \in (R_\nu)_{\nu\in\mathbb{N}}$. Damit ist nach Bemerkung (2.3.6) $f(s)/P(s) = \exp(A+Bs)$ für geeignete $A, B \in \mathbb{C}$. □

In Satz (2.3.8) wurde gezeigt, dass für ganze Funktionen der Ordnung 1 die Summe über die Nullstellen

$$\sum_{s_j\neq 0} |s_j|^{-1-\varepsilon}$$

für jedes $\varepsilon > 0$ konvergiert. Für $\varepsilon = 0$ kann die Reihe sowohl konvergent, als auch divergent sein. Konvergiert sie, so hat dies eine schärfere Schranke für das Wachstum der Funktion zur Folge:

Satz 2.3.11 *Seien f eine ganze Funktion der Ordnung 1, $(s_j)_{j\in J\subset\mathbb{N}}$ wie in (2.3.10) die Nullstellen. Dann gilt: Falls $\sum |s_j|^{-1}$ konvergiert so gibt es ein $c > 0$ so, dass f die Abschätzung $f(s) = \mathcal{O}(\exp(c|s|))$ erfüllt.*

Beweis: Für alle j gilt $\left|\left(1-\frac{s}{s_j}\right)\mathrm{e}^{\lambda}\right| \leq \mathrm{e}^{2s/s_j}$. Damit folgt aus Satz (2.3.10) und der Konvergenz der Reihe

$$|f(s)| = \left|s^k \mathrm{e}^{A+Bs}\prod_{j\in J}\left(1-\frac{s}{s_j}\right)\mathrm{e}^{s/s_j}\right| \leq \left|\mathrm{e}^{B's}\right| \exp\left(2|s|\sum_{j\in J}\frac{1}{|s_j|}\right) \leq \exp\left(c|s|\right),$$

wobei $B', c > 0$ geeignet. □

Wir kommen nun zum Beweis der Produktentwicklung von ξ (Satz 2.3.2).
Beweis: Es gilt $\xi(0,\chi) \neq 0$, daher ist das k in Satz (2.3.10) gleich 0.
Um zu zeigen, dass ξ unendlich viele Nullstellen hat müssen wir nach (2.3.11) zeigen, dass ξ nicht die Abschätzung $\xi(s,\chi) = \mathcal{O}(\exp(|s|^1))$ erfüllt; um die behauptete Darstellung zu zeigen benötigen wir nach (2.3.10) dass ξ von Ordnung 1 ist.

Für die Abschätzung nach oben genügt es, nach der Funktionalgleichung (2.8), $\xi(s,\chi) = \mathcal{O}(\exp(|s|^{1+\varepsilon}))$ (für jedes $\varepsilon > 0$) nur für die s mit $\operatorname{Re} s \geq 1/2$ zu beweisen. Nach Definition (2.7) gilt

$$\xi(s,\chi) = \left(\frac{\pi}{m}\right)^{-\frac{s}{2}} \Gamma\left(\frac{1}{2}(s+\kappa)\right) \mathrm{L}(s,\chi).$$

Der Γ-Term wächst nach der STIRLINGSCHEN Formel (2.2), asymptotisch wie $\exp(|s|(\log|s|))$, was in $\mathcal{O}(\exp(|s|^{1+\varepsilon}))$, aber nicht in $\mathcal{O}(\exp(|s|^1))$ ist. Dieser Term wird sich als der Dominante herausstellen, woraus dann beide Behauptungen folgen. Der Term $\left(\frac{\pi}{m}\right)^{-\frac{s}{2}}$ ist in $\mathcal{O}(\exp(|s|))$, Wir müssen somit nur noch $\mathrm{L}(s,\chi)$ in $\operatorname{Re} s \geq 1/2$ abschätzen. Wir setzen

$$\mathrm{X}(x) := \sum_{n \leq x} \chi(n).$$

Nach den Charakterrelationen ist $\mathrm{X}(m) = 0$ und damit wegen der Periodizität von χ auch $\mathrm{X}(qm) = 0$, für alle $q \in \mathbb{N}$. Da auch noch $|\chi(n)| \leq 1$ gilt, folgt $\mathrm{X}(x) \leq m$, für alle $x \in \mathbb{R}$. Damit erhält man mittels partieller Summation (2.3.9) in $\operatorname{Re} s > 0$ und für $N \in \mathbb{N}$

$$\begin{aligned}\left|\sum_{1\leq n\leq N} \chi(n) n^{-s}\right| &= \left|\mathrm{X}(N)N^{-s} - 1 + s\int_1^N \mathrm{X}(x)x^{-s-1}\,dx\right| \\ &\leq m\left(N^{-s} + s\int_1^N x^{-\operatorname{Re} s-1}\,dx\right)\end{aligned}$$

woraus $\mathrm{L}(s,\chi) = \mathcal{O}(|s|)$[4] folgt. □

2.4 Logarithmische Ableitung von L

Wir gewinnen nun aus den Abschnitten (2.2) und (2.3) eine Abschätzung der Nullstellendichte, sowie eine Abschätzung der logarithmischen Ableitung von L. Hier kommt es nun aber darauf an, dass alle auftretenden Konstanten unabhängig von χ (insbesondere unabhängig vom Modulus von χ) sind.

2.4.1 Nullstellendichte

Für die Abschätzungen in den folgenden Abschnitten benötigen wir eine Aussage darüber, dass die Nullstellen von L im kritischen Streifen nicht zu dicht liegen. [5] Hierfür ziehen wir zunächst einige Folgerungen aus dem HADAMARD-Produkt (2.3.2) und der Funktionalgleichung von ξ (2.8).

[4] die implizite Konstante ist hier abhängig von χ

[5] hier können wir aber nicht einfach Satz (2.3.8) anwenden, da wir einerseits eine bessere Abschätzung als $\#\{\rho \in \mathcal{N}(\chi)\,;\ |\rho| \leq R\} = \mathcal{O}(R^{1+\varepsilon})$ benötigen, andererseits die implizite Konstante unabhängig von χ sein muss

Logarithmisches Differenzieren von (2.3.2) liefert:

$$\frac{\xi'}{\xi}(s,\chi) = B(\chi) + \sum_{\rho\in\mathcal{N}(\chi)} \left(\frac{1}{s-\rho} + \frac{1}{\rho}\right). \tag{2.19}$$

Da wir Abschätzungen benötigen, die unabhängig vom Modulus von χ, also von m, sind, würden wir gerne die, von χ abhängige, Konstante $B(\chi)$ berechnen. Dies gelingt aber nicht, da die Nullstellen von $\xi(s,\chi)$ nicht symmetrisch zur reellen Achse liegen. Wir erhalten aber eine Identität für den Realteil von $B(\chi)$ mit einer Reihe über $\mathcal{N}(\chi)$, die für die späteren Abschätzungen ausreichen wird.
Wir zeigen zunächst die folgende

Behauptung 2.4.1

1. *Für alle ρ aus dem kritischen Streifen gilt: $\rho\in\mathcal{N}(\chi) \iff \overline{\rho}\in\mathcal{N}(\overline{\chi})$.*
2. *Für alle ρ aus dem kritischen Streifen gilt: $\rho\in\mathcal{N}(\chi) \iff 1-\overline{\rho}\in\mathcal{N}(\chi)$.*

Beweis:
1: Es gilt folgende Kette von Äquivalenzen:

$$\rho\in\mathcal{N}(\chi) \Leftrightarrow \sum_{n=1}^{\infty}\frac{\chi(n)}{n^{\rho}} = 0 \Leftrightarrow \overline{\sum_{n=1}^{\infty}\frac{\chi(n)}{n^{\rho}}} = 0 \Leftrightarrow \sum_{n=1}^{\infty}\frac{\overline{\chi}(n)}{n^{\overline{\rho}}} = 0 \Leftrightarrow \overline{\rho}\in\mathcal{N}(\overline{\chi}).$$

2: Wir benutzen die Funktionalgleichung von ξ in (2.8) und erhalten:

$$\rho\in\mathcal{N}(\chi) \Leftrightarrow \xi(\rho,\chi) = 0 \Leftrightarrow \xi(1-\rho,\overline{\chi}) = 0 \Leftrightarrow 1-\rho\in\mathcal{N}(\overline{\chi}) \Leftrightarrow 1-\overline{\rho}\in\mathcal{N}(\chi).$$

Die letzte Äquivalenz folgte aus (1). □
Logarithmisches Differenzieren der Funktionalgleichung (2.8) liefert $\frac{\xi'}{\xi}(s,\chi) = \frac{\xi'}{\xi}(1-s,\overline{\chi})$. Setzt man hier $s=0$ ein so erhält man mit (2.19)

$$\begin{aligned} B(\chi) = \frac{\xi'}{\xi}(0,\chi) = -\frac{\xi'}{\xi}(1,\overline{\chi}) &= -B(\overline{\chi}) + \sum_{\overline{\rho}\in\mathcal{N}(\overline{\chi})}\left(\frac{1}{1-\overline{\rho}} + \frac{1}{\overline{\rho}}\right) \\ &= -B(\overline{\chi}) + \sum_{\rho\in\mathcal{N}(\chi)}\left(\frac{1}{1-\overline{\rho}} + \frac{1}{\overline{\rho}}\right). \end{aligned}$$

Die letzte Gleichheit gilt nach Behauptung (2.4.1,1).
Mit $B(\overline{\chi}) = \overline{B(\chi)}$ und Übergang zum Realteil folgt

$$2\mathrm{Re}\, B(\chi) = -\sum_{\rho\in\mathcal{N}(\chi)} \mathrm{Re}\left(\frac{1}{1-\overline{\rho}} + \frac{1}{\overline{\rho}}\right).$$

Nach Behauptung (2.4.1,2) kann $\frac{1}{1-\overline{\rho}}$ durch $\frac{1}{\rho}$ ersetzt werden [6]. Insgesamt folgt:

$$2\mathrm{Re}\, B(\chi) = -\sum_{\rho\in\mathcal{N}(\chi)} \mathrm{Re}\left(\frac{1}{\rho} + \frac{1}{\overline{\rho}}\right) = -2\sum_{\rho\in\mathcal{N}(\chi)} \mathrm{Re}\left(\frac{1}{\rho}\right), \text{ also}$$

[6] Umordnen ist hier zulässig, da alle Summanden nicht-negativ sind

$$\operatorname{Re} B(\chi) = -\sum_{\rho \in \mathcal{N}(\chi)} \operatorname{Re}\left(\frac{1}{\rho}\right). \tag{2.20}$$

Wir erhalten noch aus der Definition von ξ in (2.7) und der logarithmischen Ableitung von ξ (2.19) eine Formel für die logarithmische Ableitung von L:

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = -\frac{1}{2}\log\frac{m}{\pi} - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa}{2}\right) + B(\chi) + \sum_{\rho \in \mathcal{N}(\chi)}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right). \tag{2.21}$$

Wir notieren noch das folgende Lemma

Lemma 2.4.2 *Für einen* Dirichlet-*Charakter χ und $\operatorname{Re} s \geq 3/2$ ist $\mathrm{L}(s,\chi) = \mathcal{O}(1)$. Die implizite Konstante ist unabhängig vom Modulus von χ.*

Beweis: Es gilt:

$$\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leq \sum_{n=1}^{\infty} \frac{\log n}{n^{3/2}} = \mathcal{O}(1).$$

□

Die nächsten drei Lemmata dienen dazu, eine obere Schranke für die Anzahl der Nullstellen von L in einem Rechteck mit den Ecken $0 \pm iT$, $1 \pm iT$ zu finden. Lemma (2.4.3) und Lemma (2.4.4) sind aus [Mur01].

Lemma 2.4.3 *Sei $s = \sigma + it$, χ ein primitiver Charakter modulo m.*
Für $1 \leq \sigma \leq 2$ gilt:

$$\sum_{\rho \in \mathcal{N}(\chi)} \operatorname{Re}\left(\frac{1}{s-\rho}\right) = \operatorname{Re}\left(\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right) + \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right),$$

wobei die Konstante in $\mathcal{O}$ unabhängig von m und s ist.

Beweis: Aus der logarithmischen Ableitung von L (2.21) folgt zusammen mit Gleichung (2.20)

$$-\operatorname{Re}\left(\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right) = \frac{1}{2}\log\frac{m}{\pi} + \frac{1}{2}\operatorname{Re}\left(\frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa}{2}\right)\right) - \sum_{\rho \in \mathcal{N}(\chi)} \operatorname{Re}\left(\frac{1}{s-\rho}\right).$$

Nach der Stirlingschen Formel (2.3) gilt

$$\frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa}{2}\right) = \log\left(\frac{s+\kappa}{2}\right) + \mathcal{O}\left(\left|\frac{s+\kappa}{2}\right|^{-1}\right).$$

Hier ist $\left|\frac{s+\kappa}{2}\right|^{-1}$ wegen $\operatorname{Re} s \geq 1$ und $\kappa \geq 0$ beschränkt. Da der Realteil von s beschränkt ist, ist $\log\left(\frac{s+\kappa}{2}\right)$ in $\mathcal{O}\left(\log\left(|t|+2\right)\right)$, d.h. der Γ-Term ist von dieser Größenordnung. Mit $\frac{1}{2}\log\frac{m}{\pi} = \mathcal{O}\left(\log m\right)$ ergibt sich die Behauptung. □

Lemma 2.4.4 *Sei χ ein primitiver Charakter modulo m. Schreibe $\rho = \beta + i\gamma$ für die Nullstellen von $\mathrm{L}(s,\chi)$. Dann gilt für alle $t \in \mathbb{R}$:*

$$\sum_{\rho \in \mathcal{N}(\chi)} \frac{1}{1+(t-\gamma)^2} = \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right). \tag{2.22}$$

Beweis: Setzt man $s = 2 + it$ in Lemma (2.4.3) ein, so erhält man, da $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ für solche s beschränkt ist (2.4.2)

$$\sum_{\rho \in \mathcal{N}(\chi)} \mathrm{Re}\left(\frac{1}{s-\rho}\right) = \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right). \tag{2.23}$$

Nun ist für jedes $\rho \in \mathcal{N}(\chi)$:

$$\mathrm{Re}\left(\frac{1}{s-\rho}\right) = \frac{2-\beta}{(2-\beta)^2+(t-\gamma)^2} \geq \frac{1}{4+(t-\gamma)^2} \geq \frac{1}{4\cdot\left(1+(t-\gamma)^2\right)},$$

woraus mit Abschätzung (2.23) die Behauptung folgt. □

Wir geben als nächstes eine Abschätzung für die Dichte der Nullstellen von $\mathrm{L}(s,\chi)$ an. Hierfür definieren wir:

Definition 2.4.5 *Für einen Charakter χ und $T \in \mathbb{R}_{>0}$ setze:*

$$\mathrm{N}(T,\chi) := \#\{\rho \in \mathcal{N}(\chi) \ ; \ \mathrm{Im}\ (\rho) \leq T\}.$$

Lemma 2.4.6 *Es gelten*

$$\mathrm{N}(T+1,\chi) - \mathrm{N}(T,\chi) = \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right), \tag{2.24}$$

und

$$\mathrm{N}(T,\chi) = \mathcal{O}\left(T\cdot\log\left(m\left(|t|+2\right)\right)\right). \tag{2.25}$$

Beweis: Die zweite Aussage folgt durch Summation aus der ersten.
Zum Beweis der ersten Aussage sei χ zunächst ein primitiver Charakter.
Es gilt für $\rho = \beta + i\gamma$

$$(T \leq \gamma \leq T+1) \Longleftrightarrow (0 \leq \gamma - T \leq 1).$$

Also leistet ein $\rho \in \mathcal{N}(\chi)$ welches die linke Seite der obigen Äquivalenz erfüllt, in der Summe aus (2.22) einen Beitrag größer, gleich 1/2. Nach Lemma (2.4.4) liegt deren Anzahl also in $\mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right)$.
Die Aussage für allgemeine Charaktere folgt aus der für primitive und Gleichung (2.4)[7], da $\prod_{p|m}\left(1-\frac{\chi'(p)}{p^{-s}}\right)$ keine Nullstellen in $\mathrm{Re}\, s \neq 0$ hat. □

[7] χ' sei der primitive Charakter, der χ induziert

2.4.2 Abschätzung von $\frac{\mathrm{L}'}{\mathrm{L}}$

Satz 2.4.7 *Sei χ ein* DIRICHLET*-Charakter modulo m, $\varepsilon > 0$, $s = \sigma + it \in \mathbb{C}$. Dann gilt:*

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = \begin{cases} \mathcal{O}(1), & \text{falls} \quad \sigma \geq 3/2 \\ \sum\limits_{\substack{\rho \in \mathcal{N}(\chi) \\ |t - \operatorname{Im}\rho| \leq 1}} \frac{1}{s-\rho} + \mathcal{O}(\log(m(|t|+2))), & \text{falls} \quad \varepsilon \leq \sigma \leq 2. \end{cases} \tag{2.26}$$

Die impliziten Konstanten sind dabei unabhängig von m und s. Dagegen ändert sich die zweite Konstante mit ε. [8]

Beweis:
1.Fall ($\sigma \geq 3/2$): Dies ist Lemma (2.4.2).
2.Fall ($\varepsilon \leq \sigma \leq 2$): Sei zunächst χ ein primitiver Charakter.
Wir erinnern, dass $\kappa = 1$ falls $\chi(-1) = -1$ und $\kappa = 0$ sonst (also falls $\chi(-1) = 1$).
Es gilt Gleichung (2.21), die wir hier noch einmal wiederholen:

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = -\frac{1}{2}\log\frac{m}{\pi} - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa}{2}\right) + B(\chi) + \sum_{\rho \in \mathcal{N}(\chi)}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right).$$

Nach der STIRLINGSCHEN Formel (2.3) gilt:

$$\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+\kappa}{2}\right) = \frac{1}{s+\kappa} + \mathcal{O}\left(\log\left(\frac{|s|+\kappa}{2}\right)\right).$$

Da $\sigma \geq \varepsilon$ und $\kappa \geq 0$, ist $\left|\frac{1}{s+\kappa}\right| = \mathcal{O}(1)$. Weiterhin ist $|s| = \mathcal{O}(|t|+2)$ so, dass insgesamt folgt:

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = B(\chi) + \sum_{\rho \in \mathcal{N}(\chi)}\left(\frac{1}{s-\rho} + \frac{1}{\rho}\right) + \mathcal{O}(\log(m(|t|+2))). \tag{2.27}$$

Setzt man in (2.27) $s = 2 + it$ ein und zieht die entstandene Gleichung von der für allgemeines s ab, so erhält man, da $\frac{\mathrm{L}'}{\mathrm{L}}(2+it,\chi) = \mathcal{O}(1)$:

$$\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi) = \sum_{\rho \in \mathcal{N}(\chi)}\left(\frac{1}{s-\rho} + \frac{1}{\rho} - \frac{1}{2+it-\rho}\right) + \mathcal{O}(\log(m(|t|+2))). \tag{2.28}$$

Wir zeigen als nächstes, dass die Differenz

$$\sum_{\rho \in \mathcal{N}(\chi)}\left(\frac{1}{s-\rho} + \frac{1}{\rho} - \frac{1}{2+it-\rho}\right) - \sum_{\substack{\rho \in \mathcal{N}(\chi) \\ |t - \operatorname{Im}\rho| \leq 1}} \frac{1}{s-\rho},$$

welche die Gleichung (2.28) noch von der behaupteten Abschätzung trennt, ebenfalls in $\mathcal{O}(\log(m(|t|+2)))$ liegt.

[8] In der Anwendung dieses Satzes wird $\varepsilon = 1/4$ fest gewählt sein

Der Beitrag der $\frac{1}{2+it-\rho}$ mit $|\mathbf{Im}\,\rho - t| \leq 1$: Es gilt wegen $\mathrm{Re}\,(2+it-\rho) = 2-\mathrm{Re}\,\rho \geq 1$, die Abschätzung $\left|\frac{1}{2+it-\rho}\right| \leq 1$, und nach Lemma (2.4.6) gibt es nur $\mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right)$ viele ρ, die $|\mathrm{Im}\,\rho - t| \leq 1$ erfüllen.
Der Beitrag der $\frac{1}{s-\rho} - \frac{1}{2+it-\rho}$ mit $|\mathbf{Im}\,\rho - t| > 1$:
Hier gilt:

$$\left|\frac{1}{s-\rho} - \frac{1}{2+it-\rho}\right| = \left|\frac{2-\sigma}{(s-\rho)\,(2+it-\rho)}\right| = \mathcal{O}\left((t-\mathrm{Im}\,\rho)^{-2}\right).$$

Mit Lemma (2.4.6) folgt für $n \in \mathbb{Z}$, $n \neq 0$, $n \neq -1$:

$$\sum_{\substack{\rho\in\mathcal{N}(\chi)\\ t+n\leq \mathrm{Im}\,\rho\leq t+n+1}} \frac{1}{s-\rho} - \frac{1}{2+it-\rho} = \mathcal{O}\left(n^{-2}\cdot\log\left(m\left(|t+n|+2\right)\right)\right).$$

Summation über alle $n \in \mathbb{Z}$, $n \neq 0$, $n \neq -1$ ergibt schließlich:

$$\sum_{\substack{\rho\in\mathcal{N}(\chi)\\ |\mathrm{Im}\,\rho - t|>1}} \frac{1}{s-\rho} - \frac{1}{2+it-\rho} = \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right).$$

Für einen allgemeinen Charakter $\chi \bmod m$ sei χ' ein primitiver Charakter $\bmod m'$ (es folgt $m'|m$), der χ induziert. Wir erhalten aus dem bereits bewiesenen

$$\frac{\mathrm{L}'}{\mathrm{L}}\left(s,\chi'\right) = \sum_{\substack{\rho\in\mathcal{N}(\chi)\\ |t-\mathrm{Im}\,\rho|\leq 1}} \frac{1}{s-\rho} + \mathcal{O}\left(\log\left(m'\left(|t|+2\right)\right)\right) \tag{2.29}$$

und aus (2.4) folgt

$$\frac{\mathrm{L}'}{\mathrm{L}}\left(s,\chi\right) = \frac{\mathrm{L}'}{\mathrm{L}}\left(s,\chi'\right) + \sum_{\substack{p|m\\ p\nmid m'}} \frac{\chi'(p)\log p}{p^s - \chi'(p)} \tag{2.30}$$

Nun ist, für $\sigma \geq \varepsilon > 0$, $|p^s| \geq 2^\varepsilon \geq 1+\varepsilon' > 1$ [9] (und $|\chi'(p)| = 1$). Also ist der Betrag des Nenners jedes Summanden größer, gleich ε'. Damit folgt aus (2.29) und (2.30)

$$\begin{aligned}
\frac{\mathrm{L}'}{\mathrm{L}}\left(s,\chi\right) &= \sum_{\substack{\rho\in\mathcal{N}(\chi)\\ |t-\mathrm{Im}\,\rho|\leq 1}} \frac{1}{s-\rho} + \mathcal{O}\left(\log\left(m'\left(|t|+2\right)\right)\right) + \mathcal{O}(1)\sum_{\substack{p|m\\ p\nmid m'}} \frac{1}{\varepsilon'}\log p \\
&= \sum_{\substack{\rho\in\mathcal{N}(\chi)\\ |t-\mathrm{Im}\,\rho|\leq 1}} \frac{1}{s-\rho} + \mathcal{O}\left(\log\left(m'\left(|t|+2\right)\right)\right) + \mathcal{O}(1)\frac{1}{\varepsilon'}\log\left(m/m'\right) \\
&= \sum_{\substack{\rho\in\mathcal{N}(\chi)\\ |t-\mathrm{Im}\,\rho|\leq 1}} \frac{1}{s-\rho} + \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right).
\end{aligned}$$

□

[9] wobei $\varepsilon' > 0$ unabhängig von χ und s ist

Setzen wir nun voraus, dass alle $\rho \in \mathcal{N}$ auf der Geraden $\operatorname{Re} s = 1/2$ liegen (ERH), so können wir aus den Resultaten dieses Abschnittes eine Abschätzung für $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ auf $\operatorname{Re} s = 1/4$ gewinnen.
Das folgende Korollar ist in [BS96], ohne Beweis, notiert.

Korollar 2.4.8 *Sei χ ein* Dirichlet-*Charakter modulo $m \geq 2$. Unter Voraussetzung der ERH gilt für alle $t \in \mathbb{R}$*

$$\frac{\mathrm{L}'}{\mathrm{L}}(1/4 + it, \chi) = \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right),$$

wobei die implizite Konstante unabhängig von t und χ ist.

Beweis: Nach Satz (2.4.7) gilt

$$\frac{\mathrm{L}'}{\mathrm{L}}(1/4 + it, \chi) = \sum_{\substack{\rho \in \mathcal{N}(\chi) \\ |t - \operatorname{Im}\rho| \leq 1}} \frac{1}{1/4 + it - \rho} + \mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right).$$

Da nach der ERH jedes ρ den Realteil $1/2$ hat, ist jeder Summand durch 4 beschränkt. Nach Lemma (2.4.6) gibt es $\mathcal{O}\left(\log\left(m\left(|t|+2\right)\right)\right)$ viele. □

2.5 Die Perronsche Formel

Wir arbeiten nun daran, die Primzahlsumme (1.1) durch ein Integral über eine analytische Funktion auszudrücken. Hierfür benötigen wir zwei Lemmata, deren Aussage und Beweis sehr ähnlich zur Perronschen Formel sind, (siehe z.B. [Brü95]). Der Beweis ist hier aber wesentlich einfacher, da in unserer Version der Nenner des Integranden quadratisch mit $|s|$ gegen ∞ geht.

Lemma 2.5.1 *Seien $y, T, c > 0$. Dann gilt:*

$$\frac{1}{2\pi i}\int_{c-iT}^{c+iT} \frac{y^{s+1}}{s\left(s+1\right)}\,ds = \begin{cases} R_1\left(y,T\right), & y \leq 1 \\ y - 1 + R_2\left(y,T\right), & y > 1 \end{cases} \tag{2.31}$$

wobei

$$\left|R_1\left(y,T\right)\right| \leq c_1 \cdot \frac{y^{c+1}}{T},$$

mit einer Konstanten $c_1 \in \mathbb{R}$, die unabhängig von y und T ist, und

$$\lim_{T\to\infty} \left|R_2\left(y,T\right)\right| = 0.$$

Beweis: Betrachte den Kreis K_R mit Radius $R = \sqrt{c^2 + T^2}$ um 0.
Ohne Einschränkung gelte $R > 1$ so, dass beide Polstellen von $\frac{y^{s+1}}{s(s+s)}$ (also 0 und 1) in K_R liegen.

1.Fall ($y \leq 1$): Sei γ der Kreisabschnitt von K_R, der in der Halbebene $\operatorname{Re} s \geq c$ von $c - iT$ bis $c + iT$ verläuft. $\frac{y^{s+1}}{s(s+s)}$ ist holomorph in dem von γ und der Strecke $[c - iT, c + iT]$ umschlossenen Gebiet. Man erhält:

$$R_1(y,T) := \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{y^{s+1}}{s(s+1)}\, ds = \frac{1}{2\pi i} \int_{\gamma} \frac{y^{s+1}}{s(s+1)}\, ds.$$

Wegen $y \leq 1$ ist der Betrag von y^{s+1} dann am größten, wenn der Realteil von s am kleinsten ist. Daher lässt sich der Betrag des Zählers nach oben durch y^{c+1} abschätzen. Weiter können wir den des Nenner nach unten durch R^2 abschätzen und erhalten

$$|R_1(y,T)| \leq \frac{1}{2\pi} \int_{\gamma} \frac{y^{c+1}}{R^2}\, ds \leq \frac{1}{2\pi} \pi R \cdot \frac{y^{c+1}}{R^2} \leq \frac{1}{2} \frac{y^{c+1}}{T},$$

wie behauptet.
2.Fall ($y > 1$): Sei γ' der Kreisabschnitt von K_R, der in der Halbebene $\operatorname{Re} s \leq c$ von $c - iT$ bis $c + iT$ verläuft. Der Integrand hat an der Stelle $s = 0$ das Residuum y und an der Stelle $s = -1$ das Residuum -1. Man erhält:

$$\frac{1}{2\pi i} \cdot \left(\int_{c-iT}^{c+iT} \frac{y^{s+1}}{s(s+1)}\, ds - \int_{\gamma'} \frac{y^{s+1}}{s(s+1)}\, ds \right) = y - 1.$$

Hieraus folgt:

$$R_2(y,T) := \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{y^{s+1}}{s(s+1)}\, ds - (y-1) = \frac{1}{2\pi i} \int_{\gamma'} \frac{y^{s+1}}{s(s+1)}\, ds.$$

Nun kann der Betrag des Zählers nach oben durch y^{c+1}, der des Nenners nach unten durch $R(R-1)$ abgeschätzt werden:

$$|R_2(y,T)| \leq \frac{1}{2\pi i} \int_{\gamma'} \frac{y^{c+1}}{R(R-1)}\, ds \leq \frac{1}{2\pi} 2\pi R \frac{y^{c+1}}{R(R-1)} = \frac{y^{c+1}}{R-1},$$

also $\lim_{T\to\infty} |R_2(y,T)| = 0$, was noch zu zeigen war. □

Lemma 2.5.2 *Seien $x, T, c > 0$. Ferner sei $(a_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen, deren Dirichlet-Reihe $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ für $s = c$ absolut konvergiere. Dann gilt:*

$$\sum_{n\leq x} a_n (x-n) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \left(\sum_{n=1}^{\infty} \frac{a_n}{n^s} \right) \frac{x^{s+1}}{s(s+1)}\, ds + R(T), \tag{2.32}$$

wobei $\lim_{T\to\infty} |R(T)| = 0$.

Beweis: Aus der absoluten Konvergenz von $\sum_{n=1}^{\infty} \frac{a_n}{n^c}$ folgt gleichmäßige Konvergenz auf der Strecke $[c-iT, c+iT]$. Daher erhält man durch Vertauschen von Summation und Integration

$$I := \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \left(\sum_{n=1}^{\infty} \frac{a_n}{n^s} \right) \frac{x^{s+1}}{s\,(s+1)}\, ds = \sum_{n=1}^{\infty} a_n n \cdot \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{\left(\frac{x}{n}\right)^{s+1}}{s\,(s+1)}\, ds\,.$$

Setze, für $n \in \mathbb{N}$, $y_n := \frac{x}{n}$ Anwendung von Lemma (2.5.1) liefert [10]:

$$I = \sum_{n \le x} a_n \underbrace{(y_n - 1)\, n}_{=(x-n)} + \sum_{n<x} R_2\,(y_n, T)\, a_n \cdot n \; + \sum_{n \ge x} R_1\,(y_n, T)\, a_n \cdot n\,.$$

Da für $n = x$ der Term $y_n - 1 = 0$ ist, war es zulässig die erste Summe, statt über $n < x$, über $n \le x$ laufen zu lassen.
Es muss nun noch gezeigt werden, dass die zweite und dritte Summe für $T \to \infty$ gegen 0 gehen. Bei der zweiten Summe ist dies richtig, da es für jeden der endlich vielen Summanden gilt.
Die dritte Summe erfüllt die Abschätzung[11]:

$$\left| \sum_{n \ge x} R_1\,(y_n, T)\, a_n \cdot n \right| \le \frac{c_1}{T} \sum_{n \ge x} \left(\frac{x}{n}\right)^{c+1} |a_n| \cdot n \; = \frac{c_1 \cdot x^{c+1}}{T} \cdot \sum_{n \ge x} \frac{|a_n|}{n^c} \; = \frac{c'}{T},$$

für eine von T unabhängige Konstante c'. □

2.6 Die obere Abschätzung

Wir werden nun die obere Abschätzung

$$\sum_{p \le x} \Lambda\,(p)\, \chi\,(p)\, (x-p) \; = \mathcal{O}\left(x^{3/2} \log m\right)$$

unter Voraussetzung der erweiterten Riemannschen Hypothese (ERH) beweisen. Das folgende Lemma ist von Bach und Shallit [BS96].

Lemma 2.6.1 *Sei χ ein* Dirichlet-*Charakter modulo $m \ge 2$, $\delta_\chi := 1$ falls χ der Hauptcharakter ist, $\delta_\chi := 0$ sonst.*
(ERH) Dann gilt:

$$\sum_{p \le x} \Lambda\,(p)\, \chi\,(p)\, (x-p) \; = \delta_\chi \frac{x^2}{2} + \mathcal{O}\left(x^{3/2} \log m\right)$$

wobei die implizite Konstante unabhängig von x und m ist.

[10] die Bezeichnungen R_1 und R_2 seien so gewählt wie in Lemma (2.5.1)
[11] c_1 sei so gewählt wie in Lemma (2.5.1)

Beweis: Wir wenden Lemma (2.5.2) auf

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)\,\chi(n)}{n^s} = -\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$$

an, und erhalten für $T \geq 0$: [12]

$$\sum_{n\leq x} \Lambda(n)\,\chi(n)\,(x-n) = -\frac{1}{2\pi i}\int_{2-iT}^{2+iT} \frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,\frac{x^{s+1}}{s(s+1)}\,ds + R(T), \tag{2.33}$$

wobei $R(T) \to 0$ für $T \to \infty$.
Obwohl $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ auf $\operatorname{Re} s = 2$ beschränkt ist können wir das Integral noch nicht genügend scharf abschätzen.
Um auf den behaupteten Exponenten von 3/2 zu kommen müssen wir die Integrationslinie links von $\operatorname{Re} s = 1/2$ ziehen. Hier gilt Formel (2.33) aber nicht, da die absolute Konvergenzabszisse bei 1 liegt. Um die Summe durch ein Integral entlang $\operatorname{Re} s = 1/4$ ausdrücken zu können, wenden wir deshalb den Residuensatz auf das Rechteck mit den Ecken $\frac{1}{4} \pm iT$, $2 \pm iT$ an.
Die wagerechten Strecken sollten dabei ausreichend weit von den Nullstellen von $\mathrm{L}(s,\chi)$ entfernt sein. Dies ist möglich, da die Nullstellen-Dichte nach Lemma (2.4.6) nicht zu stark zunimmt. Wir notieren das folgende Lemma, dessen Beweis wir später nachreichen werden:

Lemma 2.6.2 *Es gibt eine Folge $(T_k)_{k\in\mathbb{N}}$ positiver reeller Zahlen mit $\lim_{k\to\infty} T_k = \infty$, und für alle $k \in \mathbb{N}$*

$$\forall \rho \in \mathcal{N}(\chi) \;\; \textit{gilt} \;\; |T_k - |\operatorname{Im}\rho|| \geq \frac{1}{T_k}.$$

Im Rechteck befinden sich die Nullstellen $\rho \in \mathcal{N}(\chi)$ von $\mathrm{L}(s,\chi)$, sowie im Fall $\chi = \chi_1$ eine Polstelle von $\mathrm{L}(s,\chi)$ bei $s = 1$. Wir berechnen die Residuen von $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ an diesen Stellen mittels der folgenden

Bemerkung 2.6.3 *Ist f eine meromorphe Funktion, definiert auf einer Teilmenge $U \subset \mathbb{C}$, so ist f'/f eine meromorphe Funktion auf U, deren Polstellenmenge gleich der Vereinigung der Nullstellenmenge mit der Polstellenmenge von f ist. Ferner gilt für die Residuen von f'/f an einem s_0 aus der Polstellenmenge von f'/f:*

$$\operatorname{Res}\left(f'/f, s_0\right) = \begin{cases} -k, & \textit{falls } f \textit{ an } s_0 \textit{ einen Pol der Ordnung } k \textit{ hat,} \\ k, & \textit{falls } s_0 \textit{ Nullstelle } k\textit{-ter Ordnung von } f \textit{ ist.} \end{cases}$$

Falls $\chi = \chi_1$ so hat $\mathrm{L}(s,\chi)$ an $s = 1$ einen Pol der Ordnung 1, d.h. $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ hat an $s = 1$ einen Pol mit Residuum -1.
An $s = \rho \in \mathcal{N}(\chi)$ hat $\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)$ einen Pol mit Residuum k, falls k die Nullstellenordnung von $\mathrm{L}(s,\chi)$ an ρ ist. In diesem Fall kommt ρ aber auch k-mal in $\mathcal{N}(\chi)$ vor und wir berechnen k-mal ein Residuum von 1.

[12] die absolute Konvergenzabszisse der Reihe $\sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}$ ist gleich 1

Damit gilt für $T \in (T_k)$:

$$\begin{aligned}\sum_{n\leq x}\Lambda(n)\chi(n)(x-n) &= -\frac{1}{2\pi i}\int_{2-iT}^{2+iT}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\cdot\frac{x^{s+1}}{s(s+1)}\,ds + R(T)\\ &= -\frac{1}{2\pi i}\left(\int_{2-iT}^{\frac{1}{4}-iT}+\int_{\frac{1}{4}-iT}^{\frac{1}{4}+iT}+\int_{\frac{1}{4}+iT}^{2+iT}\right)\frac{x^{s+1}}{s(s+1)}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,ds\\ &\quad +\delta_\chi\frac{x^2}{2}-\sum_{\substack{\rho\in\mathcal{N}(\chi)\\ |\operatorname{Im}\rho|\leq T}}\frac{x^{\rho+1}}{\rho(\rho+1)}+R(T).\end{aligned}$$

Wir zeigen als nächstes, dass die beiden äußeren Integrale für $T\to\infty$ gegen 0 gehen. Man hat:

$$I_\pm := \left|\int_{\frac{1}{4}\pm iT}^{2\pm iT}\frac{x^{s+1}}{s(s+1)}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,ds\right| \leq 2\frac{x^3}{T^2}\max_{s\in[\frac{1}{4}\pm iT,2\pm iT]}\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right|.$$

Da $T\in(T_k)$ (siehe Lemma 2.6.2) gilt nach Satz (2.4.7) und Lemma (2.4.6):

$$\max_{s\in[\frac{1}{4}\pm iT,2\pm iT]}\left|\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\right| \leq \sum_{\substack{\rho\in\mathcal{N}(\chi)\\ |T-\operatorname{Im}\rho|\leq 1}} T + \mathcal{O}(\log(m(|T|+2))) = \mathcal{O}(T\log(mT)).$$

Dies ist hinreichend klein, denn da der Nenner quadratisch mit $T\to\infty$ gegen ∞ geht, folgt nun dass $I_\pm$ für $T\in(T_k), T\to\infty$ gegen 0 gehen.
Mit $T\in(T_k), T\to\infty$ erhält man:

$$\sum_{n\leq x}\Lambda(n)\chi(n)(x-n) = \delta_\chi\frac{x^2}{2}-\sum_{\rho\in\mathcal{N}(\chi)}\frac{x^{\rho+1}}{\rho(\rho+1)}-\frac{1}{2\pi i}\int_{\frac{1}{4}-\infty}^{\frac{1}{4}+\infty}\frac{x^{s+1}}{s(s+1)}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,ds.$$

Als nächstes zeigen wir, dass die rechte Seite dieser Gleichung in $\delta_\chi\frac{x^2}{2}+\mathcal{O}\left(x^{3/2}\log m\right)$ ist.
Die Summe der Residuen liefert mit Lemma (2.4.6):

$$\begin{aligned}\left|\sum_{\rho\in\mathcal{N}(\chi)}\frac{x^{\rho+1}}{\rho(\rho+1)}\right| &\leq x^{3/2}\sum_{\rho\in\mathcal{N}(\chi)}\left|\frac{1}{\rho(\rho+1)}\right| \leq x^{3/2}\left(\sum_{k=0}^{\infty}\frac{N(k+1,\chi)-N(k,\chi)}{k^2+(1/2)^2}\right)\\ &\leq x^{3/2}\left(\sum_{k=0}^{\infty}\frac{c_2\cdot\log(m(k+2))}{k^2+1/4}\right)=\mathcal{O}\left(x^{3/2}\log m\right).\end{aligned}$$

Das Integral liefert mit Korollar (2.4.8):

$$\left|\int_{\frac{1}{4}-\infty}^{\frac{1}{4}+\infty}\frac{x^{s+1}}{s(s+1)}\frac{\mathrm{L}'}{\mathrm{L}}(s,\chi)\,ds\right| \leq 2x^{5/4}\int_0^\infty\frac{c_3\cdot\log(m(t+2))}{t^2+\left(\frac{1}{4}\right)^2}\,dt=\mathcal{O}\left(x^{5/4}\log m\right).$$

Insgesamt haben wir bisher

$$\sum_{n\leq x}\Lambda(n)\chi(n)(x-n) = \delta_\chi\frac{x^2}{2}+\mathcal{O}\left(x^{3/2}\log m\right).$$

Dies ist schon beinahe das gewünschte Ergebnis. Es sind nur noch die Primpotenzen p^k mit $k\geq 2$ zuviel. Wir zeigen schließlich noch, dass deren Beitrag vernachlässigbar ist. [13]

$$\begin{aligned}\sum_{\substack{p^k\leq x\\ k\geq 2}}\Lambda\left(p^k\right)\left|\chi\left(p^k\right)\right|\left(x-p^k\right) &\leq x\sum_{\substack{p^k\leq x\\ k\geq 2}}\log(p)\\ &\leq x\sum_{2\leq k\leq\log_2 x}\vartheta\left(x^{1/k}\right)\\ &\leq x\left(\vartheta\left(x^{1/2}\right)+(\log_2 x)\cdot\vartheta\left(x^{1/3}\right)\right)=\mathcal{O}\left(x^{3/2}\right).\end{aligned}$$

□

Wir reichen jetzt noch den fehlenden Beweis für Lemma (2.6.2) nach.
Beweis: Unterteilt man für $n\in\mathbb{N}$ die beiden Streifen $n\leq|\mathrm{Im}\,s|<n+1$ in $2n$ Teile der Form $n+j\frac{1}{2n}\leq|\mathrm{Im}\,s|<n+(j+1)\frac{1}{2n}$ für $j=0,\ldots,2n-1$, so gibt es, nach Lemma (2.4.6), unendlich viele solcher Teilstreifen, die keine Nullstelle enthalten.
Wählt man die T_k so, dass iT_k jeweils in der Mitte eines solchen Streifens liegt, so erhält man eine Folge mit den gewünschten Eigenschaften. □

2.7 Beweis des Satzes von Ankeny

Wir kommen nun zum Beweis von (1.2.2):
Beweis: Sei $x<G(n)$. Dann erzeugen die Primzahlen kleiner gleich x eine echte Untergruppe U von $(\mathbb{Z}/(n))^*$ und es gibt einen Dirichlet-Charakter $\chi\neq\chi_1$ modulo n mit $\chi_{|U}\equiv 1$. [14] Insbesondere ist für $p\leq x$:

$$\chi(p)=\begin{cases}0, & \text{falls } p|n,\\ 1, & \text{falls } p\nmid n.\end{cases}\tag{2.34}$$

Wir werden zeigen, dass notwendigerweise $x=\mathcal{O}\left((\log n)^2\right)$ gilt, woraus die Behauptung folgt.
Wie bereits in der Beweisskizze (Abschnitt 1.3) erwähnt, besteht die Idee darin, die Summe $\sum_{p\leq x}\Lambda(p)\chi(p)(x-p)$ geeignet nach oben und unten abzuschätzen.
Für die Abschätzung nach oben benutzen wir Lemma (2.6.1), und erhalten, da χ nicht der Hauptcharakter ist:

$$\sum_{p\leq x}\Lambda(p)\chi(p)(x-p)=\mathcal{O}\left(x^{3/2}\log n\right).\tag{2.35}$$

[13] In den folgenden Gleichungen ist $\vartheta(y):=\sum_{p\leq y}\log p=\mathcal{O}(y)$; die Abschätzung gilt nach dem Primzahlsatz.
[14] Nehme einen nichttrivialen Charakter auf $(\mathbb{Z}/(n))^*/U$

Wir zeigen als nächstes, dass es, unter den Voraussetzungen an χ und x (2.34), ein x_0 und ein $c > 0$ gibt so, dass

$$\sum_{p \leq x} \Lambda(p)\, \chi(p)\, (x-p) \geq c\left(x^2 - x \log n\right) \tag{2.36}$$

für alle $x \geq x_0$gilt.
Zum Beweis bemerken wir, dass nach (2.34) gilt:

$$\sum_{p \leq x} \Lambda(p)\, \chi(p)\, (x-p) = \sum_{p \leq x} (\log p)\, (x-p) - \sum_{\substack{p \leq x \\ p \mid n}} (\log p)\, (x-p).$$

Hier lässt sich der erste Term durch ein Integral über die Tschebyscheffsche ϑ-Funktion ausdrücken:

$$\sum_{p \leq x} (\log p)\, (x-p) = \int_0^x \vartheta(t)\, dt = \frac{x^2}{2} + \mathrm{o}\left(x^2\right).$$

Für den zweiten Term zeigt eine grobe Abschätzung:

$$\sum_{\substack{p \leq x \\ p \mid n}} (\log p)\, (x-p) \leq x \cdot \sum_{p \mid n} (\log p) = x \cdot \log \prod_{p \mid n} p \leq x \log n,$$

was den Beweis von (2.36) beendet.
Aus (2.35) und (2.36) folgt, dass es ein x_1 und ein $c' > 0$ gibt so, dass $x^2 - x \log n \leq c' x^{3/2} \log n$ für alle $x \geq x_1$ gilt. Hieraus folgt $\sqrt{x} = \mathcal{O}(\log n)$, also

$$x = \mathcal{O}\left((\log n)^2\right).$$

□

Kapitel 3

Anwendungen des Satzes von Ankeny

3.1 Einleitung

Ankenys Theorem hat bedeutende Anwendungen in der algorithmischen Zahlentheorie, da es besagt, dass man - falls die ERH korrekt ist - Elemente von $(\mathbb{Z}/(n))^*$, die außerhalb einer echen Untergruppe liegen, deterministisch in polynomialer Zeit finden kann.
Die Bezeichnung *polynomial* heißt in diesem Zusammenhang "polynomial in der Stellenzahl von n":

Definition 3.1.1 *Ein Algorithmus, der als Eingabe eine natürliche Zahl n erhält, hat **polynomiale** Laufzeit, falls es ein $k \in \mathbb{N}$ gibt so, dass die Anzahl der ausgeführten Bitoperationen in $\mathcal{O}\left((\log n)^k\right)$ liegt.*

Der restliche Teil dieses Kapitels gliedert sich folgendermaßen:
In Abschnitt (3.2) werden wir zeigen, dass sich ein quadratischer Nichtrest (siehe 3.2.2) modulo einer ungeraden Primzahl in polynomialer Zeit finden lässt. Diese Resultate werden auch im Abschnitt (3.3.1) eine bedeutende Rolle spielen, wo gezeigt werden wird, dass sich der probabilistische Primzahltest von Solovay und Strassen - unter Voraussetzung der ERH - deterministisch machen lässt. Ein weiterer Primtest folgt in (3.3.2).
Im Abschnitt (3.4) folgen schließlich noch zwei Aussagen über die kleinste Primzahl p, die für ein mit $n \in \mathbb{N}$ teilerfremdes $a \in \mathbb{Z}$, die Kongruenz $p \equiv a \pmod{n}$ erfüllt[1], sowie über die kleinste Primzahl die in eine Nebenklasse einer Untergruppe von $(\mathbb{Z}/(n))^*$ fällt.
Die Inhalte dieses Kapitels sind aus Bach und Shallit [BS96].

3.2 Der kleinste quadratische Nichtrest

Wir notieren zuerst einen Satz, der grundlegend für dieses Kapitel ist.

[1] eine solche Primzahl existiert nach dem Dirichletschen Primzahlsatz

Satz 3.2.1 ***Der kleine Satz von Fermat.***
Ist p prim und $a \in (\mathbb{Z}/(p))^*$, so gilt $a^{p-1} \equiv 1 \pmod{p}$.

Beweis: Wir zeigen zuerst durch Induktion über a, dass $a^p \equiv a \pmod{p}$, für alle $a \in (\mathbb{Z}/(p))^*$.
Die Behauptung ist richtig für $a = 1$. Sei sie richtig für $a \geq 1$.
Wir bemerken, dass Potenzieren mit p ein Ring-Homomorphismus in $(\mathbb{Z}/(p))$ ist, da der Binomialkoeffizient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, aufgrund der eindeutigen Primfaktorzerlegung, für $1 \leq k \leq p-1$ ein Vielfaches von p, also kongruent 0 mod p ist.
Damit erhalten wir aus der Induktionsannahme $(a+1)^p \equiv a^p + 1^p \equiv a + 1 \pmod{p}$, also die Aussage für $a + 1$.
Multiplikation mit $a^{-1} \in (\mathbb{Z}/(p))^*$ liefert die Behauptung des Satzes. □

Definition 3.2.2 *Seien $n \in \mathbb{N}$, $a \in \mathbb{Z}$ teilerfremd. Dann wird a ein quadratischer Rest modulo n genannt, genau dann, wenn $x^2 \equiv a \pmod{n}$ eine Lösung x hat. Andernfalls wird a ein quadratischer Nichtrest modulo n genannt.*

Wir zeigen als nächstes ein äquivalentes Kriterium für quadratische Reste modulo einer ungeraden Primzahl p, sowie, dass wir in diesem Fall einen quadratischen Nichtrest in polynomialer Zeit finden können - vorausgesetzt die ERH ist richtig.
Das folgende Kriterium wird auch in Abschnitt (3.3.1) eine bedeutende Rolle spielen.

Satz 3.2.3 ***(Eulerkriterium)*** *Sei p eine ungerade Primzahl, $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a,p) = 1$.*
Dann ist a ein quadratischer Rest modulo p falls $a^{(p-1)/2} \equiv 1 \pmod{p}$,
und a ist ein quadratischer Nichtrest modulo p falls $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Für den Beweis von (3.2.3) benötigen wir einige Vorarbeit:

Lemma 3.2.4 *Seien $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $d := \mathrm{ggT}(a,n)$. Dann gilt für jedes $b \in \mathbb{Z}$:*

$$ax \equiv b \pmod{n} \text{ hat eine Lösung } x \text{ genau dann, wenn } d \mid b.$$

Beweis:
"$\Longrightarrow$" Sei x_0 eine Lösung von $ax \equiv b \pmod{n}$. Dann gibt es ein $k \in \mathbb{Z}$ so, dass $ax_0 - kn = b$ und, da $d|a$ und $d|n$, folgt $d|b$.
"$\Longleftarrow$" Gelte $d|b$. Da $d = \mathrm{ggT}(a,n)$ gibt es ganze Zahlen x_1, y_1 so, dass $ax_1 + ny_1 = d$.
Mit $c := b/d$ folgt $ax_1c + ny_1c = b$.
Damit ist $x_0 := x_1c$ also eine Lösung von $ax \equiv b \pmod{n}$. □

Lemma 3.2.5 *Seien $n \in \mathbb{N}$, $(\mathbb{Z}/(n))^*$ zyklisch, $a \in \mathbb{Z}$, $\mathrm{ggT}(a,n) = 1$, $d := \mathrm{ggT}(m, \varphi(n))$. Dann gilt:*

$$\exists x \in \mathbb{Z} : a \equiv x^m \pmod{n} \Longleftrightarrow a^{\varphi(n)/d} \equiv 1 \pmod{n}.$$

Beweis: Sei $g \in \mathbb{Z}$ ein Erzeugendes für $(\mathbb{Z}/(n))^*$ und $b \in \mathbb{N}$ so, dass $a \equiv g^b \pmod{n}$.
"$\Longrightarrow$" Sei $x \in \mathbb{Z}$ mit $a \equiv x^m \pmod{n}$ und $y \in \mathbb{N}$ mit $x \equiv g^y \pmod{n}$. Es folgt $g^{my} \equiv g^b \pmod{n}$ und daraus, da $\operatorname{ord}_n(g) = \varphi(n)$,[2] $my \equiv b \pmod{\varphi(n)}$. Die Existenz einer Lösung für diese Kongruenz impliziert nach Lemma (3.2.4) $d|b$. Daher

$$a^{\varphi(n)/d} \equiv g^{b\varphi(n)/d} \equiv \left(g^{\varphi(n)}\right)^{b/d} \equiv 1 \pmod{n}$$

wie behauptet.
"$\Longleftarrow$" Gelte $a^{\varphi(n)/d} \equiv 1 \pmod{n}$, also $g^{b\varphi(n)/d} \equiv 1 \pmod{n}$. Hieraus folgt $\varphi(n) = \operatorname{ord}(g) \,|b\varphi(n)/d$ also $d|b$. Nach Lemma (3.2.4) hat $my \equiv b \pmod{\varphi(n)}$ also eine Lösung, d.h. $\exists y, e \in \mathbb{Z}$ mit $ym + e\varphi(n) = b$. Damit ist

$$(g^y)^m \equiv g^b \equiv a \pmod{n},$$

also a eine m-te Potenz. □

Wir kommen nun zum Beweis des EULER-Kriteriums, Satz (3.2.3):
Beweis: Ist p prim, so ist $\mathbb{Z}/(p)$ ein Körper. Daher ist $(\mathbb{Z}/(p))^*$ zyklisch, und wir können Lemma (3.2.5) anwenden.
Weiterhin gilt $a^{(p-1)/2} \equiv \sqrt{1} \equiv \pm 1 \pmod{p}$, nach dem kleinen Satz von Fermat (3.2.1), und der Tatsache dass es modulo einer ungeraden Primzahl genau zwei Quadratwurzeln der 1 gibt.
In der Notation von (3.2.5) ist hier $\varphi(p) = p - 1$ und $d = \operatorname{ggT}(2, \varphi(p)) = 2$. Also:

$$a \text{ ist quadratischer Rest modulo } p \Longleftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p},$$

und

$$a \text{ ist quadratischer Nichtrest modulo } p \Longleftrightarrow a^{(p-1)/2} \equiv -1 \pmod{p},$$

was insbesondere die Aussage des EULER-Kriteriums beinhaltet. □
Aus dem EULER-Kriterium folgt mit dem nächsten Lemma, dass die quadratischen Reste modulo einer ungeraden Primzahl p eine echte Untergruppe von $(\mathbb{Z}/(p))^*$ bilden, so dass wir mit ANKENYS Theorem und der ERH einen quadratischen Nichtrest in polynomialer Zeit finden können, indem wir die Zahlen $2, 3, \ldots$, bis zu einer Grenze, die polynomial in $\log p$ ist, testen.

Lemma 3.2.6 *Sei p eine ungerade Primzahl. Dann hat $X^{(p-1)/2} = 1$ genau $(p-1)/2$ Lösungen in $\mathbb{Z}/(p)$.*

Beweis: Es ist $X^{p-1} - 1 = \left(X^{(p-1)/2} - 1\right) \cdot \left(X^{(p-1)/2} + 1\right) \in \mathbb{F}_p[X]$. Nach dem KLEINEN SATZ VON FERMAT (3.2.1) hat $X^{p-1} - 1$ alle Elemente von $(\mathbb{Z}/(p))^*$, d.h. genau $p-1$ verschiedene Nullstellen. Da $X^{(p-1)/2} + 1$ nicht mehr als $(p-1)/2$ Nullstellen haben kann, folgt die Behauptung. □

Korollar 3.2.7 *Es gibt einen quadratischen Nichtrest, modulo einer ungeraden Primzahl.*

□

Wir erhalten den folgenden Algorithmus, der bei Eingabe einer ungeraden Primzahl p einen quadratischen Nichtrest modulo p ausgibt.

[2] wir schreiben $\operatorname{ord}_n(a)$ für die multiplikative Ordnung der Restklasse von $a \in \mathbb{Z}$ in $(\mathbb{Z}/n)^*$

```
  ******************************************
QUADRATISCHER NICHTREST(p)
Für  a ← 1 bis p − 1
    Falls a^{(p−1)/2} ≡ −1 (mod p)
        gib  a  zurück; halt
******************************************
```

Satz 3.2.8 *Sei $p > 2$ prim. Dann liefert* QUADRATISCHER NICHTREST(p) *einen quadratischen Nichtrest modulo p.*
Unter Voraussetzung der ERH liegt die Laufzeit in $\mathcal{O}\left((\log p)^5\right)$.

Beweis: Nach Lemma (3.2.6) gibt es ein a, $1 \leq a \leq p-1$ mit $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, also $a^{(p-1)/2} \equiv -1 \pmod{p}$, d.h. der Algorithmus gibt eine Zahl a aus. Nach dem EULER-Kriterium (3.2.3) ist der Algorithmus korrekt, d.h. a ist ein quadratischer Nichtrest modulo p.
Setzen wir nun noch die ERH voraus, so liefert Korollar (1.2.3), da die quadratischen Reste nach (3.2.3) und (3.2.6) eine echte Untergruppe von $(\mathbb{Z}/(p))^*$ bilden, dass die äußerste Schleife $\mathcal{O}\left((\log p)^2\right)$ oft ausgeführt wird. Aus Satz (A.1.1) folgt damit die behauptete Laufzeit. □

3.3 Primtests

Wir geben in diesem Abschnitt zwei deterministische Algorithmen, die bei Eingabe einer ungeraden natürlichen Zahl n , entscheiden ob n prim ist, oder zusammengesetzt. Die Laufzeit beider Algorithmen ist polynomial, die Algorithmen sind korrekt, falls die ERH gilt, ansonsten hat man noch keinen Beweis für ihre Korrektheit.

3.3.1 Der Solovay-Strassen Test

Der folgende Test wurde von SOLOVAY und STRASSEN entwickelt und verwendet das EULER-Kriterium (3.2.3).
Wir benötigen zuerst zwei grundlegende Definitionen:

Definition 3.3.1 *Für eine ungerade Primzahl p und $a \in \mathbb{Z}$ definieren wir das Legendre-Symbol $\left(\frac{a}{p}\right)$ durch*

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & a \text{ ist ein quadratischer Rest modulo } p \\ -1, & a \text{ ist ein quadratischer Nichtrest modulo } p \\ 0, & p|a \end{cases}.$$

Das LEGENDRE-Symbol lässt sich auf ungerade natürliche Zahlen verallgemeinern.

Definition 3.3.2 *Sei $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} \in \mathbb{N}$ ungerade, und $a \in \mathbb{Z}$. Wir definieren das Jacobi-Symbol $\left(\frac{a}{n}\right)$ durch*

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{e_k}$$

Die Verwendung des gleichen Symbols für JACOBI- und LEGENDRE-Symbol bringt keine Missverständnisse mit sich, da für eine ungerade Primzahl beide Definitionen zusammenfallen.
Aus dem EULER-Kriterium folgt, dass wenn wir für eine ungerade natürliche Zahl n ein $a \in (\mathbb{Z}/(n))^*$ finden, so dass $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ so haben wir einen Beweis für die Zusammengesetztheit von n. Unklar ist aber erstens ob es für jede ungerade zusammengesetzte Zahl n ein entsprechendes a gibt, und zweitens, falls ja, wie lange wir suchen müssen.
Wir werden als nächstes zeigen, dass für eine ungerade zusammengesetzte Zahl n, mindestens die Hälfte der Elemente von $(\mathbb{Z}/(n))^*$ die Zusammengesetztheit von n - mittels des EULER-Kriteriums - beweisen. Mit ANKENYS Theorem (und unter Voraussetzung der ERH) folgt sogar, dass wir eine solche Zahl, deterministisch in polynomialer Zeit finden können.

Da für zusammengesetzte, natürliche Zahlen n, die für alle $a \in (\mathbb{Z}/(n))^*$, die Kongruenz $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ erfüllen, insbesondere $a^{n-1} \equiv 1 \pmod{n}$ gilt, handelt es sich bei solche Zahlen um sogenannte CARMICHAEL-Zahlen:

Definition 3.3.3 *Eine zusammengesetzte Zahl n heißt* CARMICHAEL*-Zahl, falls für alle $a \in (\mathbb{Z}/(n))^*$, die Kongruenz $a^{n-1} \equiv 1 \pmod{n}$ gilt.*

Wir werden als nächstes CARMICHAEL-Zahlen näher untersuchen. Dazu ist die folgende Funktion nützlich:

Definition 3.3.4 *Setze für eine natürliche Zahl n*

$$\lambda(n) := \exp\left((\mathbb{Z}/(n))^*\right),$$

wobei für eine endliche, abelsche Gruppe G der Exponent von G, $\exp(G)$ erklärt ist als

$$\exp(G) := \min\{e \in \mathbb{N} \,;\, \forall a \in G\ (a^e = 1)\}.$$

Wir erhalten eine erste Charakterisierung von CARMICHAEL-Zahlen:

Lemma 3.3.5 *Sei $n \in \mathbb{N}$ zusammengesetzt. Es gilt:*

$$n \text{ ist CARMICHAEL} \iff \lambda(n) \,|\, n-1.$$

Beweis:
"$\Longrightarrow$" Sei $a \in (\mathbb{Z}/(n))^*$. Da n CARMICHAEL, gilt $a^{n-1} \equiv 1 \pmod{n}$. Division mit Rest zeigt, dass es $b, r \in \mathbb{N}, r < \lambda(n)$ gibt, so dass $n-1 = b\lambda(n) + r$. Damit folgt $a^r \equiv a^{r+b\lambda(n)} \equiv a^{n-1} \equiv 1 \pmod{n}$. Und da dies für alle $a \in (\mathbb{Z}/(n))^*$ gilt, aber $r < \lambda(n)$ ist, muss, nach Definition von λ, $r = 0$ sein, also $\lambda(n) \,|\, n-1$.
"$\Longleftarrow$" Wir müssen nur zeigen, dass für alle $a \in (\mathbb{Z}/(n))^*$, $a^{n-1} \equiv 1 \pmod{n}$. Das ist, da $n-1$ ein Vielfaches des Exponenten von $(\mathbb{Z}/(n))^*$ ist, klar. □

Wie das nächste Lemma zeigt, können wir $\lambda(n)$ explizit berechnen (wofür wir allerdings die Faktorisierung von n benötigen).

Lemma 3.3.6

1. *Falls p eine ungerade Primzahl ist, $e \in \mathbb{N}, e \geq 1$, so ist $\lambda(p^e) = p^{e-1}(p-1)$.*
2. *Falls $n = \prod_{i=1}^{k} p_i^{e_i}$, die p_i prim und paarweise verschieden, so ist $\lambda(n) = \mathrm{kgV}\{\lambda(p_i^{e_i}) \ ; \ i = 1, \ldots, k\}$.*

Zur Vollständigkeit halten wir fest (ohne Beweis):

Bemerkung 3.3.7

1. $\lambda(1) = 1$.
2. $\lambda(2) = 1$, $\lambda(4) = 2$ *und für* $e \geq 3$ *ist* $\lambda(2^e) = 2^{e-2}$

Für den Beweis der beiden Aussagen aus Lemma (3.3.6) benötigen wir einen Satz über die multiplikative Struktur der Gruppe $(\mathbb{Z}/n)^*$ für den Fall, dass n die Potenz einer ungeraden Primzahl ist.
Schreibe im folgenden Satz U_n für $(\mathbb{Z}/(n))^*$.

Satz 3.3.8 *Seien p, e ganze Zahlen, mit $p \geq 3$ prim und $e \geq 1$. Dann ist U_{p^e} zyklisch.*

Beweis: Ist $e = 1$, so ist U_{p^e} als Einheitengruppe eines Körpers zyklisch. Sei also $e \geq 2$. Es genügt zu zeigen, dass U_{p^e} ein Element der Ordnung $p-1$ und eines der Ordnung p^{e-1} enthält. Denn dann ist, falls $\mathrm{ord}_{p^e}(a) = p-1$ und $\mathrm{ord}_{p^e}(b) = p^{e-1}$, die Ordnung der Restklasse von ab in U_{p^e} gleich $p^{e-1}(p-1)$ (siehe Behauptung 3.3.9), also ist U_{p^e} zyklisch.
Zeige dass U_{p^e} ein Element der Ordnung $p-1$ enthält: Sei $a \in \mathbb{Z}$ so, dass $\mathrm{ord}_p(a) = p-1$. Dann hat $b := a^{p^{e-1}}$ die Ordnung $p-1$ in U_{p^e}, denn $b^{p-1} \equiv 1 \pmod{p^e}$ und sei $j \geq 1$ mit $b^j \equiv 1 \pmod{p^e}$, so gilt auch $b^j \equiv 1 \pmod{p}$,[3] d.h. $a^{j \cdot p^{e-1}} \equiv 1 \pmod{p}$, also $p-1 | j$.
Zeige dass die Restklasse von $(1+p)$ in U_{p^e} die Ordnung p^{e-1} hat: Für alle $f \geq 0$ gilt

$$(1+p)^{p^f} = 1 + p^{f+1} + \sum_{i=2}^{p^f} \binom{p^f}{i} p^i.$$

Wir zeigen, dass jeder Summand der Form $\binom{p^f}{i} p^i$ für $2 \leq i \leq p^f$ von p^{f+2} geteilt wird. Dann folgt

$$(1+p)^{p^f} \equiv 1 \pmod{p^{f+1}} \text{ und } (1+p)^{p^f} \not\equiv 1 \pmod{p^{f+2}},$$

also

$$(1+p)^{p^{e-1}} \equiv 1 \pmod{p^e} \text{ und } (1+p)^{p^{e-2}} \not\equiv 1 \pmod{p^e},$$

[3] die Projektion $U_{p^e} \to U_p$ ist ein Gruppenhomomorphismus

d.h. $\mathrm{ord}_{p^e}(1+p) = p^{e-1}$.
Sei also $2 \leq i \leq p^f$. Wir schreiben für eine Primzahl q und $n \in \mathbb{N}$ die Vielfachheit mit der q n teilt als $\nu_q(n) := \max\left\{j \geq 0\ ;\ p^j | n\right\}$. Es gilt $\nu_q(m \cdot n) = \nu_q(n) + \nu_q(m)$; ν_q läßt sich mittels $\nu_q(n/m) := \nu_q(n) - \nu_q(m)$ auf rationale Zahlen fortsetzen. Damit ist

$$\nu_p\left(\binom{p^f}{i}\right) = \nu_p\left(p^f\right) + \nu_p\left(\frac{p^f-1}{1}\right) + \ldots + \nu_p\left(\frac{p^f-(i-1)}{i-1}\right) + \nu_p\left(\frac{1}{i}\right).$$

Nun sind alle Summanden bis auf den ersten und letzten gleich 0, da für $1 \leq j \leq p^f - 1$ gilt $\nu_p\left(p^f - j\right) = \nu_p\left(j\right)$, also $\nu_p\left(\frac{p^f-j}{j}\right) = 0$. Insgesamt ergibt sich

$$\nu_p\left(\binom{p^f}{i}\right) = f - \nu_p(i).$$

Zu zeigen ist nur noch $\nu_p\left(\binom{p^f}{i} p^i\right) \geq f+2$, also (nach obiger Gleichung äquivalent) $i \geq \nu_p(i) + 2$. Diese Ungleichung gilt für $\nu_p(i) = 0$; sonst ist $i \geq 3^{\nu_p(i)} \geq \nu_p(i) + 2$. □

Wir beweisen nun Lemma (3.3.6).
Beweis:
Zu (1): Aus Satz (3.3.8) folgt, dass für $p \geq 3$ $(\mathbb{Z}/p^e)^*$ zyklisch ist also ein Element der Ordnung $|(\mathbb{Z}/p^e)^*| = \varphi\left(p^e\right) = p^{e-1}\left(p-1\right)$ hat. Da dies bereits die Gruppenordnung ist, folgt die Behauptung.
Zu (2): Setze $t := \mathrm{kgV}\left\{\lambda\left(p_i^{e_i}\right)\ ;\ i = 1, \ldots, k\right\}$. Dann ist für alle $x \in \mathbb{Z}$ und alle $i = 1, \ldots, k$, $x^t \equiv 1 \pmod{p_i^{e_i}}$. Nach dem chinesischen Restsatz ist also auch $x^t \equiv 1 \pmod{n}$.
Wir zeigen schließlich noch, dass es ein Element der Ordnung t in $(\mathbb{Z}/(n))^*$ gibt, woraus dann die Behauptung folgt.
Sei a_i von Ordnung $\lambda\left(p_i^{e_i}\right)$ in $\left(\mathbb{Z}/\left(p_i^{e_i}\right)\right)^*$. Nach dem chinesischen Restsatz gibt es $x_0 \in \mathbb{Z}$ so, dass für alle $i = 1, \ldots, k$ gilt: $x_0 \equiv a_i \pmod{p_i^{e_i}}$. Wir zeigen, dass x_0 die Ordnung t hat.
Dies folgt durch Induktion über k (die Anzahl verschiedener Primteiler von n) mittels folgender Behauptung:

Behauptung 3.3.9 *Seien $m, m' \in \mathbb{N}$ mit $\mathrm{ggT}\left(m, m'\right) = 1$, $x \in \mathbb{Z}$, $a := \mathrm{ord}_m\left(x\right)$, $b := \mathrm{ord}_{m'}\left(x\right)$. Dann ist $\mathrm{ord}_{mm'}\left(x\right) = \mathrm{kgV}\left(a, b\right)$.*

Beweis: Setze $d := \mathrm{kgV}\left(a, b\right)$, und $f := \mathrm{ord}_{mm'}\left(x\right)$. Da d ein Vielfaches der Ordnung von x in $\left(\mathbb{Z}/\left(m\right)\right)^*$ und in $\left(\mathbb{Z}/\left(m'\right)\right)^*$ ist gilt:

$$\exists k, k' \in \mathbb{Z} \text{ so, dass } x^d = 1 + km \text{ und } x^d = 1 + k'm'. \tag{3.1}$$

Hieraus folgt $km = k'm'$ und wegen der Teilerfremdheit von m und m' erhält man $m | k'$. Das heißt es gibt ein $k'' \in \mathbb{Z}$ mit $k' = mk''$ was zusammen mit (3.1) $x^d = 1 + k''mm'$, also $x^d \equiv 1 \pmod{mm'}$ ergibt. Das impliziert nun $f | d$.
Umgekehrt haben wir $x^f \equiv 1 \pmod{m}$ und $x^f \equiv 1 \pmod{m'}$, also $a | f$ und $b | f$. Da somit f ein Vielfaches von a und b ist gilt auch $d | f$. □□

Aus den beiden vorangehenden Lemmata können wir weitere Eigenschaften von CARMICHAEL-Zahlen ableiten:

Lemma 3.3.10 *Ist $n \in \mathbb{N}$ eine* CARMICHAEL*-Zahl so ist n*

1. *ungerade,*
2. *quadratfrei und*
3. *teilbar durch mindestens 3 paarweise verschiedene Primzahlen.*

Beweis:
Zu (1): Da $n > 2$ ist[4], gilt $-1 \not\equiv 1 \pmod{n}$, also auch für jede ungerade Zahl $s \in \mathbb{N}$ $(-1)^s \not\equiv 1 \pmod{n}$, d.h. $\lambda(n)$ muss gerade sein. Da für n als CARMICHAEL-Zahl nach Lemma (3.3.5) $\lambda(n) \mid n-1$ gilt, folgt, dass auch $n-1$ gerade, d.h. n ungerade ist.
Zu (2): Angenommen es gebe eine Primzahl p mit $p^2 | n$. Da nach (1) p ungerade ist folgt aus Lemma (3.3.6) $p | \lambda(n)$, was wiederum $p | n-1$ impliziert. Nach Annahme gilt auch noch $p | n$, woraus $p | 1$ folgt, was ein Widerspruch ist.
Zu (3): Hat n keine drei verschiedenen Primteiler so folgt, da n zusammengesetzt ist, $n = pq$ für Primzahlen p und q. Nach (1) sind p und q ungerade, und wir erhalten mit Lemma (3.3.6) $p-1 | \lambda(n)$, also folgt aus der für CARMICHAEL-Zahlen gültigen Aussage (3.3.5) $\lambda(n) \mid n-1$

$$pq - 1 = n - 1 \equiv 0 \pmod{p-1}. \tag{3.2}$$

Da $p \equiv 1 \pmod{p-1}$ erhält man aus (3.2) $q \equiv 1 \pmod{p-1}$. Daher gilt $q \geq p$. Wir können nun alle Folgerungen auch mit q und p vertauscht durchführen, und erhalten $p \geq q$, also $p = q$, d.h. $n = p^2$ im Widerspruch zu (2). □

Wir benötigen noch einige grundlegende Eigenschaften des LEGENDRE-Symbols und des JACOBI-Symbols:

Lemma 3.3.11 *Das* LEGENDRE*-Symbol ist multiplikativ im ersten Argument, d.h. Für p prim, $p > 2$ und $a, b \in \mathbb{Z}$ gilt*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Gilt zusätzlich $a \equiv b \pmod{p}$, so hat man

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Beweis: Die erste Aussage ist richtig falls a oder b von p geteilt wird. Gelte also im folgenden $\mathrm{ggT}(a,p) = \mathrm{ggT}(b,p) = 1$. Dann erhält man mit dem Eulerkriterium (3.2.3):

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} \cdot b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

[4] n ist als CARMICHAEL-Zahl zusammengesetzt

Da das LEGENDRE-Symbol nur die Werte $0, \pm 1$ annimmt, bedeutet Kongruenz modulo p Gleichheit, woraus die erste Aussage folgt.
Die zweite ist klar nach der Definition eines quadratischen Restes (3.2.2) und der Definition des LEGENDRE-Symbols. □
Das JACOBI-Symbol erfüllt, unter anderem, die folgenden Eigenschaften:

Lemma 3.3.12 *Seien $m, n \in \mathbb{N}$ ungerade, $a, b \in \mathbb{Z}$. Dann gelten für das* JACOBI-*Symbol*

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \tag{3.3}$$

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right). \tag{3.4}$$

Gilt $a \equiv b \pmod{n}$, so hat man

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right). \tag{3.5}$$

Beweis: Die erste Aussage folgt aus der entsprechenden für das LEGENDRE-Symbol, die zweite aus der Definition des JACOBI-Symbols.
Weiter bemerkt man, dass falls $a \equiv b \pmod{n}$, so sind a und b auch kongruent modulo jedem Primteiler von n. Die dritte Aussage folgt damit aus der entsprechenden für das LEGENDRE-Symbol. □

Definition 3.3.13 *Sei n eine ungerade, zusammengesetzte natürliche Zahl, $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$. Dann wird n eine* EULER*-Pseudoprimzahl zur Basis a genannt falls $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$.*

Der Name kommt daher, dass sich n, für dieses a, in Bezug auf das EULER-Kriterium, wie eine Primzahl verhält.
Wir definieren die Gruppe der Zahlen, zu deren Basis n, falls zusammengesetzt, eine EULER-Pseudoprimzahl ist.

Definition 3.3.14 *Sei n eine ungerade natürliche Zahl. Wir setzen:*

$$E(n) := \left\{ a \in (\mathbb{Z}/(n))^* \ ; \ a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n} \right\}$$

Da beide Seiten der Kongruenz multiplikativ in a sind, handelt es sich in der Tat um eine Gruppe.
Ist n eine ungerade Primzahl, so ist $E(n)$ gleich der gesamten multiplikativen Gruppe $(\mathbb{Z}/(n))^*$. Grundlegend für den SOLOVAY-STRASSEN Test ist das folgende Lemma, welches besagt, dass für eine zusammengesetzte, ungerade Zahl n, $E(n)$ eine echte Untergruppe ist, also höchstens die Hälfte aller $a \in (\mathbb{Z}/(n))^*$ auf n fälschlicherweise wie auf eine Primzahl reagieren.

Lemma 3.3.15 *Sei $n \in \mathbb{N}_{\geq 3}$ ungerade. Dann gilt:*

$$n \text{ ist prim} \iff E(n) = (\mathbb{Z}/(n))^*.$$

Beweis:
"$\Longrightarrow$" Ist n eine ungerade Primzahl, so folgt für $a \in (\mathbb{Z}/(n))^*$ aus dem Eulerkriterium (3.2.3) $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, daher $E(n) = (\mathbb{Z}/(n))^*$.
"$\Longleftarrow$" Angenommen $E(n) = (\mathbb{Z}/(n))^*$ aber n sei zusammengesetzt. Dann ist $a^{n-1} \equiv \left(\frac{a}{n}\right)^2 \equiv 1 \pmod{n}$, für alle $a \in (\mathbb{Z}/(n))^*$. Also ist n eine CARMICHAEL-Zahl und nach Lemma (3.3.10) ungerade und quadratfrei. D.h. es gibt eine ungerade Primzahl p so, dass $n = p \cdot r$, $r > 1$, $\mathrm{ggT}(p, r) = 1$, $r \neq 2$.
Sei g ein quadratischer Nichtrest modulo p. [5] Nach dem chinesischen Restsatz gibt es ein $a \in (\mathbb{Z}/(n))^*$ mit $a \equiv g \pmod{p}$ und $a \equiv 1 \pmod{r}$. Damit erhalten wir mit Hilfe von Lemma (3.3.12):

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p\,r}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{r}\right) = \left(\frac{g}{p}\right) \cdot \left(\frac{1}{r}\right) = -1 \cdot 1 = -1$$

Also ist $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \equiv -1 \pmod{n}$ und da $r|n$ folgt $a^{(n-1)/2} \equiv -1 \pmod{r}$; wir haben aber auch $a \equiv 1 \pmod{r}$. Widerspruch[6]. □

Mittels dieses Lemmas erhalten wir einen probabilistischen Primtest für ungerade $n \in \mathbb{N}_{\geq 3}$, der als zusätzliche Eingabe ein (zufälliges) $a \in \{2, 3, \ldots, n-1\}$ erhält:

```
  ********************************************
SOLOVAY-STRASSEN(n, a)
(1) Falls  ggT(a, n) ≠ 1
     gib 'zusammengesetzt' zurück; halt
Sonst
    (2) Falls  a^((n-1)/2) ≢ (a/n)  (mod n)
        gib 'zusammengesetzt' zurück; halt
    Sonst
        gib 'prim' zurück
**********************************************
```

Satz 3.3.16 *Ist n eine ungerade Primzahl so gibt* SOLOVAY-STRASSEN(n, a) `'prim'` *zurück. Ist n ungerade und zusammengesetzt so gibt* SOLOVAY-STRASSEN(n, a) *für mindestens die Hälfte der $a \in \{2, 3, \ldots, n-1\}$* `'zusammengesetzt'` *zurück. Der Algorithmus benötigt $\mathcal{O}\left((\log n)^3\right)$ Bit-Operationen.*

Beweis: Ist n eine ungerade Primzahl, so wird in Schritt (1) nie ein ggT ungleich 1 berechnet und der Algorithmus wird zu Schritt (2) gehen. Dort wird nach dem EULER-Kriterium `'prim'` zurückgegeben.
Ist n ungerade, zusammengesetzt und $a \notin (\mathbb{Z}/(n))^*$ so gibt Schritt (1) `'zusammengesetzt'` zurück. Andernfalls ist $a \in (\mathbb{Z}/(n))^*$ und nach Lemma (3.3.15) ist $E(n)$ eine echte Untergruppe von $(\mathbb{Z}/(n))^*$. Daher

$$|E(n)| \leq |(\mathbb{Z}/(n))^*|/2 = \varphi(n)/2 \leq (n-1)/2.$$

[5] siehe Korollar (3.2.7)
[6] Wegen $r \neq 2$ ist $-1 \not\equiv 1 \pmod{r}$

D.h. a liegt mit Wahrscheinlichkeit $\geq 1/2$ außerhalb von $E(n)$, erfüllt also mit Wahrscheinlichkeit $\geq 1/2$ nicht die Kongruenz $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ so, dass mit dieser Wahrscheinlichkeit `'zusammengesetzt'` ausgegeben wird.
Zur behaupteten Laufzeit, bemerken wir, dass das JACOBI-Symbol in $\mathcal{O}\left((\log n)^2\right)$ Schritten (siehe Satz A.2.2), und die Potenz modulo n in $\mathcal{O}\left((\log n)^3\right)$ Schritten (siehe Satz A.1.1) berechnet werden können. □

Indem wir ANKENYS Theorem anwenden erhalten wir hieraus einen deterministischen Primzahltest für ungerade $n \in \mathbb{N}_{\geq 3}$:

```
**********************************************
```
DETERMINISTISCHER SOLOVAY-STRASSEN(n)
```
für a ← 2 bis  min (n − 1, 2 (log n)^2)
    Falls SOLOVAY-STRASSEN(n, a) 'zusammengesetzt' zurückgibt,
        gib 'zusammengesetzt' zurück; halt
gib 'prim' zurück
**********************************************
```

Satz 3.3.17 *(ERH) Für eine ungerade Zahl $n \in \mathbb{N}_{\geq 3}$ gibt* DETERMINISTISCHER SOLOVAY-STRASSEN(n) `'prim'` *zurück, genau dann, wenn n prim ist.*
Die Laufzeit ist in $\mathcal{O}\left((\log n)^5\right)$.

Beweis: Ist n eine ungerade Primzahl so gibt SOLOVAY-STRASSEN(n, a) für kein $a \in \{2, 3, \ldots, n-1\}$ `'zusammengesetzt'` zurück, d.h. DETERMINISTISCHER SOLOVAY-STRASSEN(n) gibt schließlich `'prim'` zurück.
Ist n zusammengesetzt, so ist nach Lemma (3.3.15) $E(n)$ eine echte Untergruppe von $(\mathbb{Z}/n)^*$, also gibt es nach Korollar (1.2.4) eine positive ganze Zahl $a \leq 2(\log n)^2$ mit $a \notin E(n)$. Für dieses a gibt SOLOVAY-STRASSEN(n, a) `'zusammengesetzt'` zurück, was demnach auch die Ausgabe von DETERMINISTISCHER SOLOVAY-STRASSEN(n) ist.
Die behauptete Laufzeit folgt aus der Anzahl der Wiederholungen der äußeren Schleife sowie Satz (3.3.16). □

3.3.2 Der Miller-Rabin Test

Ein anderer Primtest stammt von MILLER und RABIN und verwendet das Konzept der *starken Pseudoprimzahlen.*

Definition 3.3.18 *Sei n ungerade, zusammengesetzt, $n - 1 = 2^s d$, $s > 0$, $2 \not| d$, $a \in (\mathbb{Z}/(n))^*$. Dann wird n starke Pseudoprimzahl zur Basis a genannt, falls*

$$a^d \equiv 1 \pmod{n}, \text{ oder}$$
$$a^{2^r d} \equiv -1 \pmod{n} \text{ für ein } r,\ 0 \leq r < s.$$

Ähnlich wie bei Euler-Pseudoprimheit definieren wir die Menge[7] der Zahlen $a \in (\mathbb{Z}/(n))^*$ die n, bezüglich des obigen Kriteriums, wie eine Primzahl aussehen lassen.

$$S(n) := \left\{ a \in (\mathbb{Z}/(n))^* \ ; \ a^d \equiv 1 \bmod n \vee \exists r \left(0 \leq r < s \wedge a^{2^r d} \equiv -1 \bmod n \right) \right\}. \tag{3.6}$$

Das nächste Lemma besagt, dass im Falle einer zusammengesetzten Zahl n die Chancen gut stehen, bald einen Beweis für die Zusammengesetztheit zu finden.

Lemma 3.3.19 *Sei $n \geq 3$ ungerade. Dann gilt:*

1. *n ist prim $\Longleftrightarrow S(n) = (\mathbb{Z}/(n))^*$.*
2. *Falls n zusammengesetzt ist so gilt: $|S(n)| \leq (n-1)/4$.*

Beweis:
Sei n prim. Für $a \in (\mathbb{Z}/(n))^*$ gilt $a^{n-1} \equiv 1 \pmod{n}$. Wir bemerken dass $\mathbb{Z}/(n)$ ein Körper ist, es also genau zwei Quadratwurzeln der 1 (nämlich 1 und -1) gibt. Betrachte also die Folge $a_t := a^{(n-1)/2^t}$ für $0 < t \leq s$. Nach obiger Bemerkung gibt es entweder ein t so, dass $a_t \equiv -1 \pmod{n}$ oder auch $a_s = a^d \equiv 1 \pmod{n}$. In beiden Fällen ist $a \in S(n)$.
Umgekehrt, sei n zusammengesetzt. Wir werden zeigen, dass $|S(n)| \leq (n-1)/4$, woraus auch die noch fehlende Implikation der ersten Behauptung folgt.
Sei $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ die Primfaktorzerlegung von n. Ferner sei k die größte ganze Zahl für die es ein $b \in (\mathbb{Z}/(n))^*$ mit $b^{2^k} \equiv -1 \pmod{n}$ gibt.

Behauptung 3.3.20 *k ist wohldefiniert.*

Beweis: $(-1)^{2^0} \equiv -1 \pmod{n}$, d.h. die Menge, über die das Maximum genommen wird, ist nicht leer.
Wir zeigen noch, dass $k \leq \nu_2(\lambda(n)) - 1$.
$\forall b \in (\mathbb{Z}/(n))^*$ gilt $b^{\lambda(n)} \equiv 1 \pmod{n}$. $\lambda(n)$ lässt sich schreiben als $\lambda(n) = 2^{\nu_2(\lambda(n))}c$, wobei c ungerade ist. Falls es nun ein $e \geq \nu_2(\lambda(n))$ und ein $b \in (\mathbb{Z}/(n))^*$ gibt, mit $b^{2^e} \equiv -1 \pmod{n}$, so ist auch $b^{\lambda(n)\cdot 2^{(e-\nu_2(\lambda(n)))}} = b^{2^e c} \equiv -1 \pmod{n}$[8], was aber wegen $b^{\lambda(n)} \equiv 1 \pmod{n}$ nicht sein kann. □

Behauptung 3.3.21 *Es ist $n \equiv 1 \pmod{2^{k+1}}$.*

Beweis: Es genügt zu zeigen, dass $p_i \equiv 1 \pmod{2^{k+1}}$, für alle $i, 1 \leq i \leq r$.
Hierzu sei also p ein Primteiler von n. Die Definition von k impliziert, dass es ein $b \in (\mathbb{Z}/(n))^*$ gibt, mit $b^{2^k} \equiv -1 \pmod{n}$. Sei $t := \mathrm{ord}_p(b)$. Wegen $b^{2^{k+1}} \equiv 1 \pmod{n}$ und $p|n$ folgt $b^{2^{k+1}} \equiv 1 \pmod{p}$, also $t|2^{k+1}$. Wir zeigen als nächstes, dass $t \nmid 2^k$:
Falls $t|2^k$ so ist $b^{2^k} \equiv 1 \pmod{p}$, also $b^{2^k} = ap + 1$ für ein $a \in \mathbb{Z}$. Wegen $b^{2^k} \equiv -1 \pmod{n}$ gibt es ein $a' \in \mathbb{Z}$ so, dass $b^{2^k} = a'n - 1 = a'pn' - 1$, wobei $n' := n/p$. Zusammen ergibt sich $ap + 1 = a'pn' - 1$ und daraus $p|2$, was nicht sein kann, da n nur ungerade Primteiler hat.

[7] hier erhalten wir tatsächlich keine Gruppe
[8] c ist ungerade

Wir haben $t|2^{k+1}$, also $2^{k+1} = qt$ für ein $q \in \mathbb{Z}$. Aus $t \not| 2^k$ folgt $2 \not| q$ und damit $2^{k+1}|t$. Wegen $b^{p-1} \equiv 1 \pmod{p}$ folgt $t|p-1$, also $2^{k+1}|p-1$, was äquivalent ist zu $p \equiv 1 \pmod{2^{k+1}}$. □
Setze $m := 2^k d$, dann folgt aus Behauptung (3.3.21) $2m|n-1$.
Wir betrachten die folgende Kette von Untergruppen von $(\mathbb{Z}/(n))^*$:

$$\begin{array}{lll} (\mathbb{Z}/(n))^* & & \\ \cup & & \\ J & := & \left\{a \in (\mathbb{Z}/(n))^* \ ; \ a^{n-1} \equiv 1 \pmod{n}\right\} \\ \cup & & \\ K & := & \{a \in (\mathbb{Z}/(n))^* \ ; \ \forall i \, (a^m \equiv \pm 1 \pmod{p_i^{e_i}})\} \\ \cup & & \\ L & := & \{a \in (\mathbb{Z}/(n))^* \ ; \ a^m \equiv \pm 1 \pmod{n}\} \\ \cup & & \\ M & := & \{a \in (\mathbb{Z}/(n))^* \ ; \ a^m \equiv 1 \pmod{n}\} \end{array}$$

Wir bemerken, dass $K \subset J$ aus $2m|n-1$ und dem chinesischen Restsatz folgt, die anderen Relationen sind trivial.

Behauptung 3.3.22 *Es gilt $S(n) \subset L$.*

Beweis: Ist $a^d \equiv 1 \pmod{n}$ so ist natürlich auch $a^m \equiv 1 \pmod{n}$.
Ist dagegen $a^{2^t d} \equiv -1 \pmod{n}$ so folgt aus der Definition von k, dass $t \leq k$, also auch $a^m \equiv -1 \pmod{n}$. □
Wir werden zeigen, dass falls $n \neq 9$, so ist L eine Untergruppe vom Index ≥ 4 in $(\mathbb{Z}/(n))^*$, was $|S(n)| \leq (n-1)/4$ zeigt.

Bemerkung 3.3.23 *Ist dagegen $n = 9$ so berechnen wir $S(n)$ explizit und erhalten $S(n) = \{-1, 1\}$. Also gilt auch hier $|S(n)| \leq (n-1)/4$.*

Behauptung 3.3.24 *Ist $n \neq 9$ so ist L eine Untergruppe vom Index ≥ 4 in $(\mathbb{Z}/(n))^*$.*

Beweis: Wir zeigen zuerst, dass jedes Element a von

$$G := \left\{a' \in (\mathbb{Z}/(n))^* \ ; \ \forall i \left(a' \equiv \pm 1 \pmod{p_i^{e_i}}\right)\right\}$$

eine 2^k-te Potenz modulo n ist. Dies sieht man folgendermaßen:
Für jedes i ist, nach Definition von k sowohl 1 als auch -1 eine 2^k-te Potenz modulo $p_i^{e_i}$. [9] Es gibt also für jedes i ein $q_i \in (\mathbb{Z}/(p_i^{e_i}))^*$ mit $q_i^{2^k} \equiv a \pmod{p_i^{e_i}}$. Nach dem chinesischen Restsatz gibt es ein q mit $q^{2^k} \equiv a \pmod{n}$. Da $m = 2^k d$, mit d ungerade, ist folgt:

$$\text{jedes Element von } G \text{ ist eine } m\text{-te Potenz modulo } n. \tag{3.7}$$

Wir zeigen, dass M den Index 2^r in $K = \{a \in (\mathbb{Z}/(n))^* \ ; \ a^m \in G\}$ hat.

[9] Für 1 ist das klar. Ferner impliziert die Definition von k die Existenz eines Elementes b mit $b^{2^k} \equiv -1 \pmod{n}$, also auch $\pmod{p_i^{e_i}}$, was eine 2^k-te Wurzel von -1 liefert.

Hierzu betrachtet man den Gruppenhomorphismus ϕ von K in das direkte Produkt von r Kopien der (multiplikativen) Gruppe, die aus ± 1 besteht, definiert durch:

$$\begin{array}{rcl} \phi : K & \longrightarrow & \langle \pm 1 \rangle^r , \\ a & \longmapsto & \langle a^m \pmod{p_i^{e_i}} \rangle_i . \end{array}$$

ϕ ist surjektiv, da nach dem chinesischen Restsatz ein r-Tupel des direkten Produkts einem Element aus G entspricht, und dieses nach (3.7) eine m-te Potenz ist, was die Existenz eines Urbildes in K liefert.
$M = \ker(\phi)$, woraus folgt dass K/M die Ordnung 2^r, also M den Index 2^r in K hat. Genauso zeigt man, dass M den Index 2 in L hat.
Hieraus folgt nun

$$[K : L] = \frac{[K : M]}{[L : M]} = 2^{r-1}.$$

Aus dem Diagramm sieht man

$$[(\mathbb{Z}/(n))^* : L] \geq [(\mathbb{Z}/(n))^* : J] \cdot [K : L] = 2^{r-1} \cdot [(\mathbb{Z}/(n))^* : J] .$$

Falls $r \geq 3$ so haben wir $[(\mathbb{Z}/(n))^* : L] \geq 4$, wie behauptet.
Falls $r \leq 2$ so kann n nach Lemma (3.3.10) keine CARMICHAEL-Zahl sein. Also ist $[(\mathbb{Z}/(n))^* : J] \geq 2$. D.h. ist $r = 2$, so haben wir wiederum $[(\mathbb{Z}/(n))^* : L] \geq 4$.
Sei schließlich noch $r = 1$. Dann ist $n = p^e$, $e \geq 2$ und $|J| = p-1$. D.h. $[(\mathbb{Z}/(n))^* : J] = p^{e-1}$, was ≥ 4 ist, falls nicht $p = 3$ und $e = 2$ also $n = 9$, was aber ausgeschlossen war. □□

Wir erhalten den folgenden probabilistischen Primtest für eine ungerade Zahl n, der als zusätzliche Eingabe ein (zufälliges) $a \in \{1, 2, \ldots, n-1\}$ erhält:

```
**********************************************
```
MILLER-RABIN(n, a)
```
(1) schreibe n − 1 = 2^s · d, d ungerade
(2) berechne  (mod n)  a_0 = a^d, a_1 = a_0^2, ... , a_k = a_{k-1}^2,
bis k = s, oder a_k ≡ 1 (mod n)
(3) Falls (k = s) und a_k ≠ 1), gib 'zusammengesetzt' zurück; halt
(4)   sonst, falls (k = 0), gib 'prim' zurück; halt
(5)     sonst, falls (a_{k-1} ≠ −1), gib 'zusammengesetzt' zurück; halt
(6)       sonst gib 'prim' zurück
**********************************************
```

Satz 3.3.25 *Ist n eine ungerade Primzahl, so gibt* MILLER-RABIN(n, a) *für alle a 'prim' zurück. Ist n eine ungerade, zusammengesetzte Zahl, so gibt* MILLER-RABIN(n, a) *für mindestens $3/4$ der a, $1 \leq a \leq n-1$ 'zusammengesetzt' zurück. Der Algorithmus benötigt $\mathcal{O}\left((\log n)^3\right)$ Bitoperationen.*

Beweis: Ist n eine ungerade Primzahl, so gibt Schritt `(3)` niemals 'zusammengesetzt' zurück. Sonst sei k der kleinsten index so, dass $a_k \equiv 1 \pmod{n}$. Dann falls $k = 0$, so gibt der Algorithmus in Zeile `(4)` 'prim' zurück. Sonst gilt $a_{k-1} \equiv -1 \pmod{n}$ und in Zeile `(5)` wird 'prim' zurückgegeben.

Sein nun n eine ungerade, zusammengesetzte Zahl.
Ist $a \notin (\mathbb{Z}/(n))^*$ so gilt $a^{2^s d} \not\equiv 1 \pmod{n}$ und deshalb wird in Zeile `(3)` 'zusammengesetzt' zurückgegeben.
Sei also $a \in (\mathbb{Z}/(n))^*$. Lemma (3.3.19) besagt, dass mindestens 3/4 aller $a \in (\mathbb{Z}/(n))^*$ nicht in $S(n)$[10] liegen. Für diese gibt der Algorithmus 'zusammengesetzt' zurück.
Zur behaupteten Laufzeit bemerkt man, dass der zeitaufwendigste Teil die Berechnung von $a^d, a^{2d}, \ldots, a^{2^k d} \pmod{n}$ ist. Satz (A.1.1) zeigt, dass $a^d \pmod{n}$ in $\mathcal{O}\left((\log n)^3\right)$ berechnet werden kann. Von dort ausgehend können die $a^{2^k d} \pmod{n}$ durch Quadrieren wiederum in $\mathcal{O}\left((\log n)^3\right)$ berechnet werden. □
Mittels Korollar (1.2.4) und unter der Voraussetzung der ERH kann dieser Primtest wiederum deterministisch gemacht werden:

```
**********************************************
```
DETERMINISTISCHER MILLER-RABIN(n)
```
für a ← 1 bis  min(n − 1, 2(log n)^2)
    Falls MILLER-RABIN(n, a) 'zusammengesetzt' zurückgibt,
        gib 'zusammengesetzt' zurück; halt
gib 'prim' zurück
**********************************************
```

Satz 3.3.26 *(ERH) Für eine ungerade Zahl $n \in \mathbb{N}_{\geq 3}$ gibt* DETERMINISTISCHER MILLER-RABIN(n) `'prim'` *zurück, genau dann, wenn n prim ist.*
Die Laufzeit ist in $\mathcal{O}\left((\log n)^5\right)$.

Der Beweis ist sehr ähnlich zum Beweis von Satz (3.3.17). Nur muß man darauf achten, dass die Menge $S(n)$ hier keine Gruppe bildet (vgl. $E(n)$ beim SOLOVAY-STRASSEN Test).
Beweis: Ist n eine ungerade Primzahl so gibt MILLER-RABIN(n, a) für kein $a \in \{1, 2, \ldots, n-1\}$ `'zusammengesetzt'` zurück, d.h. DETERMINISTISCHER MILLER-RABIN(n) gibt schließlich `'prim'` zurück.
Sei n zusammengesetzt. Wir zeigen, dass es ein $a \leq 2(\log n)^2$ mit $a \notin S(n)$ gibt. Dann ist die Ausgabe von MILLER-RABIN(n, a) für dieses a `'zusammengesetzt'`.
Nach Behauptung (3.3.22) genügt zu zeigen, dass es ein $a \leq 2(\log n)^2$ mit $a \notin L$ [11] gibt. Dies ist richtig nach Korollar (1.2.4), da L nach Behauptung (3.3.24) eine echte Untergruppe von $(\mathbb{Z}/(n))^*$ ist.
Die behauptete Laufzeit folgt aus der Anzahl der Wiederholungen der äußeren Schleife sowie Satz (3.3.25). □

3.4 Zum Dirichletschen Primzahlsatz

Der DIRICHLETSCHE Primzahlsatz besagt, dass zu jedem $n \in \mathbb{N}$ und jedem $a \in (\mathbb{Z}/(n))^*$ die Anzahl der Primzahlen $p \leq x$ mit $p \equiv a \pmod{n}$ asymptotisch gleich $x/(\varphi(n) \log x)$ ist. Unklar ist aber, wie groß, die kleinste Primzahl sein kann, die diese Kongruenz erfüllt.
Wir werden eine Aussage darüber, unter Verwendung der ERH zeigen.

[10] siehe Definition (3.6)
[11] L sei so definiert wie im Beweis von Lemma (3.3.19)

Satz 3.4.1 *Seien $n \in \mathbb{N}$ und $a \in (\mathbb{Z}/(n))^*$. Dann ist, unter Voraussetzung der ERH, die kleinste Primzahl kongruent zu $a \bmod n$ in $\mathcal{O}\left(\varphi(n)^2(\log n)^2\right)$.*

Obwohl wir hier die ERH voraussetzen, liefert dieser Satz keinen effizienten Algorithmus zur Auffindung einer solchen Primzahl. Die natürliche Vorgehensweise wäre die, die Zahlen $a, a+n, \ldots$ auf Primheit zu testen. Satz (3.4.1) impliziert, dass $a+kn$ für ein k in $\mathcal{O}\left(\frac{\varphi(n)^2}{n}(\log n)^2\right)$ prim ist. Aber $\varphi(n)$ wächst, für bestimmte Zahlen, in etwa wie n, so dass wir selbst mit einem polynomialen Primtest nicht auf polynomiale Laufzeit kommen.
Wir kommen zum Beweis von (3.4.1) aus Lemma (2.6.1).
Beweis: Lemma (2.6.1) besagt, dass unter der Voraussetzung der ERH für einen DIRICHLET-Charakter $\chi \bmod n$

$$1_\chi \frac{x^2}{2} - \sum_{p \le x} \Lambda(p)\chi(p)(x-p) = \mathcal{O}\left(x^{3/2}\log n\right). \tag{3.8}$$

Nehmen wir nun an, x sei so gewählt, dass alle Primzahlen kleiner, gleich x von $a \bmod n$ verschieden sind. Bilden wir die Summe über alle Charaktere modulo n, so erhalten wir aus Gleichung (3.8) und den Charakterrelationen

$$\frac{x^2}{2} = \sum_\chi \overline{\chi}(a)\left(1_\chi \frac{x^2}{2} - \sum_{p \le x}\Lambda(p)\chi(p)(x-p)\right) = \mathcal{O}\left(\varphi(n)x^{3/2}\log n\right).$$

Teilt man durch $x^{3/2}$ und quadriert dann die Abschätzung so folgt $x = \mathcal{O}\left(\varphi(n)^2(\log n)^2\right)$, was die Behauptung des Satzes impliziert. □

Satz (3.4.1) ist ein Spezialfall des folgenden Satzes, welcher die Aussage auf mehrelementige Untergruppen von $(\mathbb{Z}/(n))^*$ verallgemeinert.

Satz 3.4.2 *Seien G eine Untergruppe von $(\mathbb{Z}/(n))^*$ vom Index d und N eine Nebenklasse von G. Dann ist, unter Voraussetzung der ERH, die kleinste Primzahl, deren Restklasse in N liegt, in $\mathcal{O}\left(d^2(\log n)^2\right)$.*

Beweis: Wie der von Satz (3.4.1), nur wird die Summe über die (d-vielen) Charaktere von $(\mathbb{Z}/(n))^*/G$ gebildet. □

Literaturverzeichnis

[Bac90] E. Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, July 1990.

[Brü95] Brüdern. *Einführung in die analytische Zahlentheorie*. Springer, 1995.

[BS96] E. Bach and J. Shallit. *Algorithmic Number Theory*, volume 1. The MIT Press, Cambridge, Massachusetts, 1996.

[Mur01] M.Ram Murty. *Problems in Analytic Number Theory*. Springer, 2001.

Anhang A

Algorithmen der Zahlentheorie

Wir geben hier einige grundlegende Algorithmen aus der Zahlentheorie, die insbesondere dafür benötigt werden, die Laufzeiten aus Kapitel 3 zu beweisen.

A.1 Potenzen modulo n

In einigen der Algorithmen in Kapitle 3 benötigte man die Berechnung von $a^e \bmod n$. Multipliziert man wiederholt mit a und nimmt das Ergebniss modulo n so erhält man einen Algorithmus, dessen Laufzeit in $\mathcal{O}\left(e(\log n)^2\right)$ liegt. Dies ist aber, da e oft die selbe Größenordnung wie n hat nicht effizient.
Eine Verbesserung erhält man auf einfache Weise, falls $e = 2^k$. Dann kann nämlich das Ergebnis durch k-maliges Quadrieren erhalten werden. Die Laufzeit ist dann in $\mathcal{O}\left(k(\log n)^2\right) = \mathcal{O}\left((\log e)(\log n)^2\right)$.
Für allgemeines e ist die Laufzeit höchstens doppelt so hoch, d.h. in der selben Kompexitätsklasse.
Wir erhalten den folgenden Algorithmus, der für $a, e, n \in \mathbb{N}$, $a^e \bmod n$ berechnet

```
  *******************************************
Power(a, e, n)
falls e = 0 gib '1' zurück; halt
sonst, falls e mod 2 = 0
    t ← Power(a, e/2, n)
    gib t^2 mod n zurück; halt
sonst
    t ← Power(a, e − 1, n)
    gib at mod n zurück
*******************************************
```

Satz A.1.1 *Seien a, e, n ganze Zahlen, mit $n \geq 2$, $e \geq 0$, und $0 \leq a < n$. Ferner bezeichne für $e > 0$, $s(e)$ die Stellenzahl und $s_1(e)$ die Anzahl der Einsen in der Binärdarstellung von e. Dann berechnet der Algorithmus* **Power** *$a^e \bmod n$. Ist $e = 0$ so werden keine Quadrierung und eine Multiplikation mit a, sonst $s(e) - 1$ Quadrierungen und $s_1(e)$ Multiplikationen mit a ausgeführt. Die Laufzeit liegt in $\mathcal{O}\left(\log(e+1)(\log n)^2\right)$.*

Beweis: Wir beweisen zuerst per Induktion über e, dass der Algorithmus korrekt ist und mit der behaupteten Anzahl von Quadrierungen und Multiplikationen auskommt. Die Aussage ist richtig für $e = 0$ und $e = 1$. Sei $e > 1$ und die Aussage gelte für alle $f < e$.
Zur Vereinfachung der Notation wird der Term "mod$n$" im Beweis weggelassen.
Ist $e = 2k + 1$ ungerade, dann berechnet der Algorithmus zuerst a^{2k} (unter Verwendung von $s(2k) - 1$ Quadrierungen[1] und $s_1(2k)$ Multiplikationen mit a), und multipliziert das Ergebnis dann mit a. Insgesamt werden also $s(2k) - 1 = s(2k + 1) - 1$ Quadrierungen und $s_1(2k) + 1 = s_1(2k + 1)$ Multiplikationen mit a ausgeführt.
Ist $e = 2k$ gerade, dann berechnet der Algorithmus zuerst a^k (unter Verwendung von $s(k) - 1$ Quadrierungen und $s_1(k)$ Multiplikationen mit a), und quadriert dieses Ergebnis. Insgesamt werden also $s(k) = s(2k) - 1$ Quadrierungen und $s_1(k) = s_1(2k)$ Multiplikationen mit a ausgeführt.
Die behauptete Laufzeit folgt aus $s(e) = \mathcal{O}(\log(e + 1))$, $s_1(e) = \mathcal{O}(\log(e + 1))$ und der Tatsache, dass eine Multiplikation modulo n mit $\mathcal{O}\left((\log n)^2\right)$ Bitoperationen ausgeführt werden kann. □
Wir bemerken, dass die Laufzeit, unter Verwendung eines schnelleren Multiplikationsalgorithmus' noch verbessert werden kann.

A.2 Jacobi-Symbol

Die Berechnung des JACOBI-Symbols benutzt das Lemma (3.3.12) sowie weitere Eigenschaften, die wir hier nur notieren werden.

Bemerkung A.2.1 *Sei n eine ungerade natürliche Zahl. Das* JACOBI*-Symbol hat die folgenden Eigenschaften.*

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2},$$

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8},$$

und, falls a eine ungerade natürliche Zahl ist, $\mathrm{ggT}(a, n) = 1$*, dann*

$$\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}.$$

Die letzte Aussage ist bekannt als das quadratische Reziprozitätsgesetz.

Zur Berechnung von $\left(\frac{a}{n}\right)$, $0 < a < n$ schreibt man

$$\begin{aligned} a &= 2^e \cdot n' \\ n &= qn' + a' \quad , \end{aligned}$$

[1] $2k > 0$

wobei n' ungerade und $0 \leq a' < n'$. Wir erhalten mit Lemma (3.3.12) und Bemerkung (A.2.1)

$$\left(\frac{a}{n}\right) = (-1)^{e\cdot\frac{n^2-1}{8}} \left(\frac{n'}{n}\right) = (-1)^{e\cdot\frac{n^2-1}{8}+\frac{n-1}{2}\cdot\frac{n'-1}{2}} \left(\frac{n}{n'}\right) = (-1)^s \left(\frac{a'}{n'}\right), \qquad (A.1)$$

wobei $s := e \cdot \frac{n^2-1}{8} + \frac{n-1}{2} \cdot \frac{n'-1}{2}$.
Es ist nicht nötig, s explizit zu berechnen, da der Wert $(-1)^s$ nur von e mod 2, n' mod 4 und n mod 8 abhängt. Wir erhalten den folgenden Algorithmus zur Berechnung des JACOBI-Symbols.

```
  ********************************************
Jacobi(a, n)
t ← 1
solange(a ≠ 0) führe aus
    solange(a mod 2 = 0) führe aus
        a ← a/2
        falls(n mod 8 = 3), oder (n mod 8 = 5 ) dann  t ← −t
    tausche a und n aus
    falls(a mod 4 = 3), und (n mod 4 = 3 ) dann  t ← −t
    a ← a mod n
falls(n = 1) dann gib t zurück
    sonst gib 0 zurück
**********************************************
```

Satz A.2.2 *Sei n eine ungerade natürliche Zahl und $a \in \mathbb{Z}$ mit $0 < a < n$. Dann berechnet der Algorithmus **Jacobi**(a, n) das* JACOBI*-Symbol $\left(\frac{a}{n}\right)$ in $\mathcal{O}((\log a)(\log n))$ Bit-operationen.*

Beweis: Die Korrektheit folgt aus der Gleichung (A.1) sowie aus den Eigenschaften des JACOBI-Symbols in Lemma (3.3.12) und Bemerkung (A.2.1).
Zur behaupteten Laufzeit definieren wir die (endlichen) Folgen (a_j) und (n_j) durch: $a_0 := a$, $n_0 := n$ und a_j, n_j für $j = 1, \ldots, k$ seien so gewählt, dass die Gleichungen

$$\begin{aligned} a_0 &= 2^{e_1} n_1 \\ n_0 &= q_1 n_1 + a_1 \\ a_1 &= 2^{e_2} n_2 \\ n_1 &= q_2 n_2 + a_2 \\ &\vdots \\ a_{k-1} &= 2^{e_k} n_k \\ n_{k-1} &= q_k n_k + a_k, \end{aligned}$$

gelten, wobei die n_j ungerade und $a_k = 0$ sind. Es gilt $n = n_0 > a_0 \geq n_1 > a_1 \geq n_2 > \cdots > a_{k-1} \geq n_k > a_k = 0$.
Wir zeigen als nächstes, dass $k = \mathcal{O}(\log n)$ gilt. Denn ist für ein j q_j ungerade, so muss a_j gerade sein, also $e_{j+1} \geq 1$ und daher $n_{j+1} \leq a_j/2 < n_j/2$. Ist dagegen q_j

gerade, so gilt $q_j \geq 2$, also $n_j \leq n_{j-1}/2$. So gilt für jedes j, $n_{j+1} < n_{i-1}/2$, woraus $n_{2j} < n \cdot 2^{-j}$ folgt; daher $k = \mathcal{O}(\lg n)$.
Wir erhalten, als Kosten des Algorithmus [2]

$$\sum_{1 \leq j \leq k} (e_j + 1)(\lg a_{j-1}) + (\lg q_j)(\lg n_j).$$

Da $q_1 q_2 \cdots q_k \leq n$ gilt, hat man

$$\sum_{1 \leq j \leq k} (\lg q_j)(\lg n_j) \leq (\lg n_1)(k + \log q_1 q_2 \cdots q_k) = \mathcal{O}((\lg a)(\lg n)).$$

Genauso sieht man, dass $2^{e_1 + \cdots + e_k} \leq a$, also

$$\sum_{1 \leq j \leq k} (e_j + 1)(\lg a_{j-1}) \leq (\lg a)(k + \sum_{1 \leq j \leq k} e_j) = \mathcal{O}((\lg a)(\lg n)),$$

womit die Behauptung gezeigt ist. □

[2] $\lg n := \log_2 n = \mathcal{O}(\log n)$

Urhebervermerk

Ich versichere, dass ich die vorliegende Arbeit selbständig angefertigt habe und nur die angegebenen Hilfsmittel und Quellen verwendet wurden.

Konstanz, im Juni 2002

Jürgen Lerner