

Analytische Zahlentheorie

Vorlesung Wintersemester 2004/05
Peter Müller

12. Oktober 2004

Inhaltsverzeichnis

1	Einführung	1
2	Arithmetische Funktionen	3
3	Dirichlet-Reihen	5
4	Erste Eigenschaften der Riemannsches Zetafunktion	11
5	Der Primzahlsatz	14
6	Charaktere abelscher Gruppen	20
7	Der Dirichletsche Primzahlsatz	22
8	Die Gammafunktion	26
9	Mehr zur Riemannsches Zetafunktion	29
10	Das große Sieb der Zahlentheorie	35
11	Zwei Anwendungen des großen Siebs	41

1 Einführung

Die analytische Zahlentheorie befasst sich in erster Linie mit der Verteilung von Primzahlen und anderen arithmetischen Dichtefragen. Die bis heute stärksten Methoden kommen aus der Funktionentheorie. In diesem Zusammenhang ist die *Riemannsche Vermutung* (siehe Abschnitt 9) von großer

Bedeutung; diese Vermutung ist wohl die wichtigste offene Frage in der Mathematik¹.

Die Menge der Primzahlen bezeichnen wir mit \mathbb{P} . Meist bezeichnet p eine Primzahl. Die Primfaktorzerlegung von n schreiben wir als $n = \prod p_i^{e_i}$.

Das vielleicht früheste Resultat der analytischen Zahlentheorie ist

Satz 1.1 (Euklid). *Es gibt unendlich viele Primzahlen.*

Beweis. Seien $p_1, p_2, \dots, p_r \in \mathbb{P}$ verschieden. Dann ist $1 + p_1 p_2 \dots p_r > 1$ durch kein p_i , $i = 1, 2, \dots, r$, teilbar, liefert also einen neuen Primteiler p_{r+1} . Setze das Verfahren unbeschränkt fort. \square

Für reelles x sei $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Obiger Beweis liefert eine sehr schwache untere Abschätzung von $\pi(x)$. Eine bessere Abschätzung (und erneuten Beweis für Euklids Satz) liefert das folgende elegante Argument von Erdős.

Satz 1.2. *Es gilt $\pi(n) \geq \frac{\log n}{\log 4}$ für alle $n \in \mathbb{N}$.*

Beweis. Schreibe jedes $m \in \{1, 2, \dots, n\}$ eindeutig in der Form $m = a^2 b$ mit $a, b \in \mathbb{N}$ und b quadratfrei. Für a gibt es $\leq \sqrt{n}$ Möglichkeiten, und für b gibt es höchstens $2^{\pi(n)}$ Möglichkeiten. Es folgt $n \leq \sqrt{n} 2^{\pi(n)}$, und daraus folgt die Behauptung. \square

Unsere ersten Ziele in der Vorlesung sind der Beweis des Primzahlsatzes (Abschnitt 5)

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n / \log n} = 1$$

und des Dirichletschen Primzahlsatzes (siehe Abschnitt 7), nämlich dass in jeder arithmetischen Folge $a\mathbb{N} + b$ mit teilerfremden $a, b \in \mathbb{N}$ unendlich viele Primzahlen liegen.

Aufgaben. Die folgenden Aufgaben behandeln weitere einfache Zugänge zu Primzahlabeschätzungen.

1. (Polya) Zeige, dass die Zahlen $2^{2^m} + 1$, $m = 0, 1, 2, \dots$, paarweise teilerfremd sind. Welche untere Schranke für $\pi(n)$ folgt daraus?

¹Siehe http://www.claymath.org/Millennium_Prize_Problems/ für weitere Informationen, und wie man 1 Million \$ verdienen kann...

2. Der folgende Beweis von Euler für die Unendlichkeit der Primzahlenmenge ist wesentlich konzeptioneller, und kann als Startpunkt und Motivation für die folgenden zwei Abschnitte gesehen werden. Fülle die Details in folgendem Argument aus:

$$\begin{aligned} \prod_{p \leq n} \frac{1}{1 - \frac{1}{p}} &= \prod_{p \leq n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots\right) \\ &\geq 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n} \\ &> \log n \end{aligned}$$

3. Diese Aufgabe enthält einfache, aber wichtige Abschätzungen der Fakultätsfunktion. Zeige

$$e\left(\frac{n}{e}\right)^n < n! < en\left(\frac{n}{e}\right)^n$$

für alle $n \in \mathbb{N}$. Tipp: Zeige mittels Riemann-Summen $\log(n-1)! < \int_1^n \log t \, dt < \log n!$, und verwende $n! = n(n-1)!$.

4. Für $x \in \mathbb{R}$ sei $[x]$ die größte ganze Zahl $\leq x$. Sei p^e die höchste Potenz von $p \in \mathbb{P}$, die $n!$ teilt. Zeige $e = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$. Dies benutzte Tchebychev, um elementare Abschätzungen zur Primzahlverteilung zu erzielen. Zeige zum Beispiel

$$\sum_{p \leq n} \frac{\log p}{p-1} \geq \log n - 1.$$

5. Sei $2 \leq p \in \mathbb{N}$. Zeige, dass der Binomialkoeffizient $\binom{p}{k}$ für alle $1 \leq k \leq p-1$ durch p teilbar ist genau dann, wenn p eine Primzahl ist. (Hinweis: Sei p nicht prim, und q ein Primteiler von p . Sei q^k die höchste Potenz, die p teilt. Zeige, dass q^k kein Teiler von $\binom{p}{q}$ ist.)

2 Arithmetische Funktionen

Sei \mathcal{A} die Menge der Funktionen $\mathbb{N} \rightarrow \mathbb{C}$. Die Funktion $f \in \mathcal{A}$ heißt *multiplikativ*, wenn $f(mn) = f(m)f(n)$ für alle teilerfremde m, n gilt, und es ein $n \in \mathbb{N}$ gibt mit $f(n) \neq 0$. Gilt $f(mn) = f(m)f(n)$ sogar für alle $m, n \in \mathbb{N}$, so heißt f *vollständig multiplikativ*.

Ist d ein Teiler von n , so schreiben wir $d|n$.

Neben der gewöhnlichen Addition auf \mathcal{A} definieren wir ein Produkt \star , die *Faltung* durch

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

Lemma 2.1. Sind $f, g \in \mathcal{A}$ multiplikativ, dann auch $f \star g$.

Beweis. Übung. □

Satz 2.2. $(\mathcal{A}, +, \star)$ ist ein kommutativer Ring mit Einselement η , mit $\eta(1) = 1$ und $\eta(n) = 0$ für $n > 1$. Ferner gilt: $f \in \mathcal{A}$ ist eine Einheit genau dann, wenn $f(1) \neq 0$.

Beweis. Der einfache Nachweis der Ringaxiome sei als Übung überlassen.

Sei f eine Einheit, es gibt also $g \in \mathcal{A}$ mit $f \star g = \eta$. Es folgt $1 = \eta(1) = f(1)g(1)$, also $f(1) \neq 0$.

Sei nun $f \in \mathcal{A}$ mit $f(1) \neq 0$. Setze $g(1) = 1/f(1)$, und für $n > 1$ definiere $g(n)$ rekursiv durch

$$0 = \eta(n) = (f \star g)(n) = f(1)g(n) + \sum_{1 < d|n} f(d)g\left(\frac{n}{d}\right).$$

□

Satz 2.3. Sei $f \in \mathcal{A}$ multiplikativ. Dann gilt $f(1) = 1$, und f^{-1} ist ebenfalls multiplikativ.

Beweis. Sei $n \in \mathbb{N}$ mit $f(n) \neq 0$. Aus $f(n) = f(n \cdot 1) = f(n)f(1)$ folgt $f(1) = 1$. Nach Satz 2.2 hat f eine Inverse $g \in \mathcal{A}$, also $f \star g = \eta$. Für $n = \prod p_i^{e_i}$ definiere $h(n) = \prod g(p_i^{e_i})$. Nach Definition ist h multiplikativ, und es gilt $h = g$ auf Primpotenzen. Auf Primpotenzen gilt $f \star h = \eta$, ferner ist $f \star h$ nach Lemma 2.1 multiplikativ, somit gilt $f \star h = \eta$ auf \mathbb{N} , also $g = h$, und die Behauptung folgt. □

Definition. Sei $\epsilon \in \mathcal{A}$ definiert durch $\epsilon(n) = 1$ für alle $n \in \mathbb{N}$. Dann heißt $\mu := \epsilon^{-1}$ die Möbiusfunktion.

Satz 2.4. Sei μ die Möbiusfunktion. Dann gilt

$$\mu(n) = \begin{cases} 1 & \text{falls } n = 1, \\ 0 & \text{falls } n > 1 \text{ nicht quadratfrei,} \\ (-1)^r & \text{falls } n = p_1 p_2 \dots p_r \text{ mit } p_i \in \mathbb{P} \text{ verschieden.} \end{cases}$$

Beweis. μ ist multiplikativ nach Satz 2.3, daher gilt $\mu(1) = 1$, und wir müssen nur den Fall $n = p^e$ betrachten.

Es gilt $0 = (\epsilon \star \mu)(p) = \mu(1) + \mu(p)$, also $\mu(p) = -1$. Sei nun $e \geq 2$. Aus $0 = (\epsilon \star \mu)(p^e) = \sum_{d|p^e} \mu(d) = \sum_{i=0}^e \mu(p^i) = \sum_{i=2}^e \mu(p^i)$ folgt induktiv $\mu(p^e) = 0$. □

Als Folge des bisherigen notieren wir die klassische Möbiussche Umkehrformel.

Korollar 2.5. Sei

$$F(n) = \sum_{d|n} f(d)$$

für alle $n \in \mathbb{N}$. Dann gilt

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

Beweis. Aus $F = \epsilon \star f$ folgt $\mu \star F = \mu \star (\epsilon \star f) = (\mu \star \epsilon) \star f = \eta \star f = f$. \square

Sind $f, g \in \mathcal{A}$, so ordnen wir diesen Funktionen formale *Dirichlet-Reihen*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

zu. Formales Ausmultiplizieren von $F(s)G(s)$ liefert

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f \star g)(n)}{n^s}.$$

Somit steht die Faltung zu Dirichlet-Reihen im analogen Verhältnis wie das wohlvertraute Cauchy-Produkt $\sum_{i=0}^n f(i)g(n-i)$ zu den Potenzreihen. Dieser Zusammenhang ist der Grund für die Bedeutung der Dirichlet-Reihen in der Zahlentheorie.

Aufgaben. 1. Vervollständige die Beweise von Lemma 2.1 und Satz 2.2.

2. Gilt Lemma 2.1 auch dann, wenn multiplikativ durch vollständig multiplikativ ersetzt wird?
3. Sei $id(n) = n$ für alle $n \in \mathbb{N}$. Welche Interpretation haben $\epsilon \star \epsilon$ und $\epsilon \star id$? Gib einen direkten Beweis für die Multiplikativität dieser Funktionen.

3 Dirichlet-Reihen

Die Produkte im folgenden Satz heißen Euler-Produkte.

Satz 3.1. Sei $f \in \mathcal{A}$ multiplikativ, und $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ absolut konvergent für $s \in \mathbb{C}$. Dann gilt

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{sk}}.$$

Ist f sogar vollständig multiplikativ, so gilt

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{f(p)}{p^s}}.$$

Beweis. Sei $F = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$. Sei $\epsilon > 0$, und $N \in \mathbb{N}$ mit $\sum_{n > N} \left| \frac{f(n)}{n^s} \right| < \epsilon$. Setze $P = \{p \in \mathbb{P} \mid p \leq N\}$, und sei M die Menge der natürlichen Zahlen die nur Primfaktoren aus P enthalten. Es gilt

$$\prod_{p \in P} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{sk}} = \sum_{n \in M} \frac{f(n)}{n^s}.$$

Aus $\{1, 2, \dots, N\} \subseteq M$ folgt daher

$$\left| F - \prod_{p \in P} \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{sk}} \right| \leq \sum_{n > N} \frac{f(n)}{n^s} < \epsilon.$$

Ist f vollständig multiplikativ, so gilt

$$\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{sk}} = \sum_{k=0}^{\infty} \left(\frac{f(p)}{p^s} \right)^k = \frac{1}{1 - \frac{f(p)}{p^s}}.$$

□

Beispiele. 1. Sei $f = \epsilon \equiv 1$ und $s > 1$. Wir erhalten die *Riemannsche Zetafunktion*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}.$$

Hier sieht man schön, wie die harmlos aussehende linke Seite mit den Primzahlen verbunden wird.

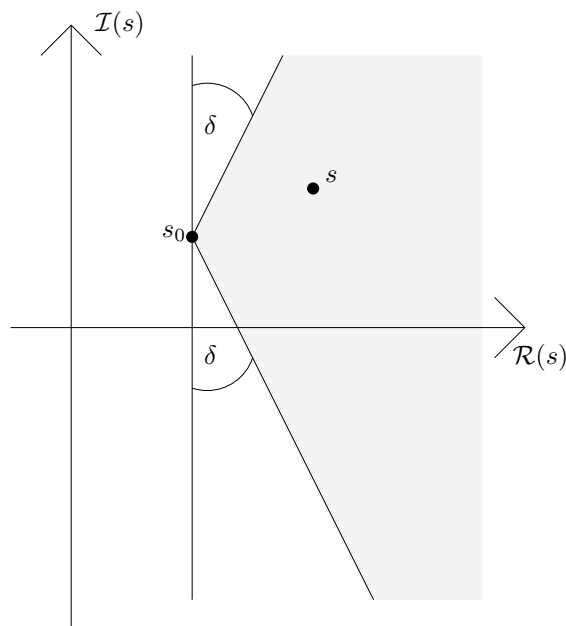
2. Wieder sei $s > 1$. Setze $F(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$. Aus $\epsilon \star \mu = \eta$ folgt $\zeta(s)F(s) = 1$, also

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s} \right).$$

Bemerkung. Vertauschung von Summation und Grenzübergang läßt sich vielfach nur mit großem Aufwand rechtfertigen. Die Argumente sind meist sehr trickreich und kompliziert, und keineswegs langweilige Routine, wie man das von der Analysis oft kennt. Diese Vertauschungen sind oft äquivalent zu tiefen zahlentheoretischen Aussagen, und sind deshalb ein Hauptthema der analytischen Zahlentheorie. Man kann zum Beispiel elementar ohne großen Aufwand zeigen, dass der Primzahlsatz folgt, sobald man die Konvergenz der Reihe $\sum_{n=1}^{\infty} \frac{\mu(n)}{n}$ kennt. Auch sehen wir in Kürze ohne großen Aufwand, dass $\lim_{s \rightarrow 1} \frac{1}{\zeta(s)} = 0$ gilt. Aber daraus folgt nicht ohne weiteres die Konvergenz der Reihe.

Für $s \in \mathbb{C}$ bezeichnen $\mathcal{R}(s)$ und $\mathcal{I}(s)$ den Realteil bzw. Imaginärteil von s .

Satz 3.2. Sei $a \in \mathcal{A}$, $s_0 \in \mathbb{C}$, und $\sum_{n=1}^{\infty} \frac{a(n)}{n^{s_0}}$ konvergiere (nicht notwendig absolut). Dann ist für alle $\delta > 0$ die Reihe $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ gleichmäßig konvergent in $G_\delta := \{s \in \mathbb{C} \mid |\arg(s - s_0)| \leq \frac{\pi}{2} - \delta\}$. Insbesondere ist $F(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ holomorph in $\mathcal{R}(s) > \mathcal{R}(s_0)$.



Beweis. Setzt man $a_n = a'_n n^{s_0}$, so sieht man, dass man $s_0 = 0$ annehmen darf. Der Beweis benutzt die wichtige Technik der *partiellen Summation*. Dieses diskrete Analogon der partiellen Integration wird uns noch oft begegnen.

Seien $M, N \in \mathbb{N}$ mit $M \leq N$. Für $z \in \mathbb{R}$ setze

$$A(z) = \sum_{M \leq n \leq z} a(n).$$

Dann gilt

$$\begin{aligned} \sum_{M \leq n \leq N} \frac{a(n)}{n^s} &= \sum_{M \leq n \leq N} (A(n) - A(n-1)) \frac{1}{n^s} \\ &= \sum_{n=M}^N \frac{A(n)}{n^s} - \sum_{n=M-1}^{N-1} \frac{A(n)}{(n+1)^s} \\ &= \sum_{n=M}^{N-1} A(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + \frac{A(N)}{N^s} - \underbrace{\frac{A(M-1)}{M^s}}_{=0}. \end{aligned}$$

Schreibe² $s = \sigma + it$ mit $\sigma, t \in \mathbb{R}$.

Es gilt

$$\begin{aligned} \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| &= \left| s \int_n^{n+1} z^{-s-1} dz \right| \\ &\leq |s| \int_n^{n+1} z^{-\sigma-1} dz \\ &= \frac{|s|}{\sigma} \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right). \end{aligned}$$

Sei nun $\epsilon > 0$ beliebig. Wähle $M(\epsilon)$, so dass $|A(z)| < \epsilon$ für alle $M(\epsilon) < M \leq z$ gilt.

Aus den bisherigen Abschätzungen folgt

$$\begin{aligned} \left| \sum_{M \leq n \leq N} \frac{a(n)}{n^s} \right| &\leq \sum_{n=M}^{N-1} \epsilon \frac{|s|}{\sigma} \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right) + \frac{\epsilon}{N^\sigma} \\ &= \epsilon \frac{|s|}{\sigma} \left(\frac{1}{M^\sigma} - \frac{1}{N^\sigma} \right) + \frac{\epsilon}{N^\sigma}. \end{aligned}$$

²Die etwas merkwürdige Mischung aus lateinischen und griechischen Buchstaben für die Komponenten einer komplexen Zahl ist traditionell in der analytischen Zahlentheorie, wir folgen auch hier dieser Notation.

Wegen $\frac{\sigma}{|s|} = \sin \delta$ und $0 \leq \frac{1}{M^\sigma} - \frac{1}{N^\sigma}, \frac{1}{N^\sigma} \leq 1$ gilt weiter

$$\begin{aligned} \left| \sum_{M \leq n \leq N} \frac{a(n)}{n^s} \right| &\leq \frac{\epsilon}{\sin \delta} \left(\frac{1}{M^\sigma} - \frac{1}{N^\sigma} \right) + \frac{\epsilon}{N^\sigma} \\ &\leq \frac{\epsilon}{\sin \delta} + \epsilon \\ &= \epsilon \left(1 + \frac{1}{\sin \delta} \right). \end{aligned}$$

Hieraus folgt die Behauptung. \square

Korollar 3.3. In Satz 3.2 gilt $\lim_{\substack{s \rightarrow s_0 \\ s \in G_\delta}} F(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^{s_0}}$.

Beweis. Wegen gleichmäßiger Konvergenz in G_δ vertauschen Summation und Grenzwertbildung. \square

Bemerkung. Nach Satz 3.2 existiert genau ein $\alpha \in \mathbb{R} \cup \{\pm\infty\}$, so dass die Reihe $\sum \frac{a(n)}{n^s}$ für $\mathcal{R}(s) > \alpha$ konvergiert, und für $\mathcal{R}(s) < \alpha$ divergiert. Man nennt α deshalb die *Konvergenzabszisse*. Vorsicht: Für $\mathcal{R}(s) > \alpha$ muss im allgemeinen keine absolute Konvergenz vorliegen. Obwohl die Konvergenzabszisse dem Konvergenzradius von Potenzreihen entspricht, ist hier die Situation also komplizierter.

Wenn der Summationsbereich für eine Dirichlet-Reihe von 1 bis ∞ ist, dann schreiben wir ab jetzt häufig \sum ohne Angabe der Summationsgrenzen.

Die folgende Aussage ist eine Art Identitätssatz für Dirichlet-Reihen.

Satz 3.4. Seien $F(s) = \sum \frac{a_n}{n^s}$ und $G(s) = \sum \frac{b_n}{n^s}$ für $\mathcal{R}(s) > \alpha$ konvergent. Es gelte $F(\sigma) = G(\sigma)$ für alle hinreichend großen σ . Dann gilt $a_n = b_n$ für alle $n \in \mathbb{N}$.

Beweis. Wir dürfen $b_n = 0$ annehmen (betrachte $\sum \frac{a_n - b_n}{n^s}$). Sei also $F(\sigma) = 0$ für alle hinreichend großen σ . Sei m minimal mit $a_m \neq 0$. Wir erhalten $0 = F(\sigma)m^\sigma = a_m + \sum_{n>m} a_n \left(\frac{m}{n}\right)^\sigma$. Von dieser letzten Summe zeigen wir, dass sie für $\sigma \rightarrow \infty$ gegen 0 konvergiert. Sei $\beta > \alpha$. Wegen der Konvergenz von $\sum \frac{a_n}{n^\beta}$ gibt es $C \in \mathbb{R}$ mit $|a_n| \leq n^\beta$ für alle $n \in \mathbb{N}$. Für $\sigma > \beta + 1$ liefert ein Vergleich mit Riemann-Summen

$$\begin{aligned} \left| \sum_{n>m} a_n \left(\frac{m}{n}\right)^\sigma \right| &\leq C \cdot m^\sigma \sum_{n=m+1}^{\infty} \frac{1}{n^{\sigma-\beta}} \\ &\leq C \cdot m^\sigma \int_m^{\infty} z^{\beta-\sigma} dz \\ &= C \cdot \frac{m^{\beta+1}}{\sigma - \beta - 1}, \end{aligned}$$

und der letzte Teil konvergiert offensichtlich für $\sigma \rightarrow \infty$ gegen 0. \square

Ist $s_0 \in \mathbb{C}$ und $h(s)$ meromorph in \mathbb{C} , so ist der Konvergenzkreis um s_0 gerade so groß, dass er die erste Singularität von h trifft. Eine analoge Aussage gilt für Dirichlet-Reihen nicht. Ein in vielen Fällen wichtiger Ersatz ist aber die folgende Aussage von Landau.

Satz 3.5. Sei $\sum \frac{a_n}{n^s}$ eine Dirichlet-Reihe mit Konvergenzabszisse α . Ferner sei $0 \leq a_n \in \mathbb{R}$ für alle $n \in \mathbb{N}$. Dann lässt sich die für $\Re(s) > \alpha$ holomorphe Funktion $f(s) = \sum \frac{a_n}{n^s}$ nicht holomorph nach α fortsetzen.

Beweis. Ohne Einschränkung können wir $\alpha = 0$ annehmen. Wir nehmen an, dass sich $f(s)$ auf einen Kreis um 0 holomorph fortsetzen lässt. Dann ist $f(s)$ holomorph in einem offenen Kreis um 1 mit einem Radius $1 + 2\epsilon > 1$. Die Taylorreihe mit Entwicklungspunkt 1 ist

$$f(s) = \sum_{k=0}^{\infty} \frac{f^{(k)}(1)}{k!} (s-1)^k.$$

Diese Reihe konvergiert also auch für $s = -\epsilon$. Die Reihe $\sum \frac{a_n}{n^s}$ konvergiert für $s > 0$ gleichmäßig, daher konvergieren auch alle Ableitungen $(-1)^k \sum \frac{a_n (\log n)^k}{n^s}$ gleichmäßig. Wegen $a_n \geq 0$ konvergiert die folgende Doppelsumme absolut, was die Vertauschung der Summation rechtfertigt. Die folgende erste Zeile konvergiert, daraus erhalten wir wegen

$$\begin{aligned} \sum_{k=0}^{\infty} \frac{f^{(k)}(1)}{k!} (-\epsilon - 1)^k &= \sum_{k=0}^{\infty} \frac{(\epsilon + 1)^k}{k!} \sum_{n=1}^{\infty} \frac{a_n (\log n)^k}{n} \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n} \sum_{k=0}^{\infty} \frac{(\epsilon + 1)^k (\log n)^k}{k!} \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n} e^{(\epsilon+1) \log n} \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n^{-\epsilon}} \end{aligned}$$

die Konvergenz der Dirichlet-Reihe $\sum \frac{a_n}{n^s}$ für $s = -\epsilon < 0$, im Widerspruch dazu, dass die Konvergenzabszisse 0 ist. \square

Aufgaben. 1. Sei $\lambda(n)$ die Anzahl der Primteiler von n , mit Vielfachheit gezählt. Zeige $\frac{\zeta(2s)}{\zeta(s)} = \sum \frac{\lambda(n)}{n^s}$.

4 Erste Eigenschaften der Riemannschen Zetafunktion

Wir erinnern daran, dass die Riemannsche Zetafunktion durch

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

definiert ist. Die folgende Aussage zeigt, dass $\zeta(s)$ eine in $\mathcal{R}(s) > 1$ holomorphe Funktion ist.

Lemma 4.1. *Die Reihe $\sum_{n=1}^{\infty} \frac{1}{n^s}$ konvergiert absolut und lokal gleichmäßig für $\sigma = \mathcal{R}(s) > 1$.*

Beweis. Die Behauptung folgt sofort aus einem Vergleich mit Riemann-Summen:

$$\sum_{n=M+1}^{\infty} \left| \frac{1}{n^s} \right| = \sum_{n=M+1}^{\infty} \frac{1}{n^\sigma} \leq \int_M^{\infty} \frac{dz}{z^\sigma} = \frac{1}{\sigma-1} \cdot \frac{1}{M^{\sigma-1}}$$

□

Wir notieren eine einfache, aber wichtige Folgerung.

Lemma 4.2. *Für $\mathcal{R}(s) > 1$ gilt $\zeta(s) \neq 0$.*

Beweis. Sei $\sigma = \mathcal{R}(s) > 1$ und $\zeta(s) \neq 0$. Aus

$$\left| \frac{1}{\zeta(s)} \right| = \left| \sum \frac{\mu(n)}{n^s} \right| \leq \sum \frac{1}{n^\sigma} = \zeta(\sigma)$$

folgt

$$|\zeta(s)| \geq \frac{1}{\zeta(\sigma)}.$$

Beide Seiten der Ungleichung hängen stetig von s ab, daher gilt diese Ungleichung ohne die Einschränkung $\zeta(s) \neq 0$. Die Behauptung folgt. □

Satz 4.3. $\zeta(s) - \frac{1}{s-1}$ hat eine holomorphe Fortsetzung nach $\mathcal{R}(s) > 0$.

Beweis. Durch partielle Summation erhalten wir für $\Re(s) > 1$ eine Integraldarstellung von $\zeta(s)$:

$$\begin{aligned}
\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\
&= \sum_{n=1}^{\infty} \frac{n - (n-1)}{n^s} \\
&= \sum_{n=1}^{\infty} n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \\
&= \sum_{n=1}^{\infty} n \int_n^{n+1} \frac{s}{z^{s+1}} dz \\
&= s \sum_{n=1}^{\infty} \int_n^{n+1} \frac{[z]}{z^{s+1}} dz \\
&= s \int_1^{\infty} \frac{[z]}{z^{s+1}} dz
\end{aligned}$$

Vergleich mit der asymptotisch sehr ähnlichen Funktion $s \int_1^{\infty} \frac{z}{z^{s+1}} dz = \frac{s}{s-1}$ liefert $\zeta(s) - \frac{s}{s-1} = s \int_1^{\infty} \frac{[z]-z}{z^{s+1}} dz$. Aber $|z - [z]| \leq 1$, also $\int_1^{\infty} \left| \frac{[z]-z}{z^{s+1}} \right| dz \leq \int_1^{\infty} \frac{dz}{z^{\sigma+1}} = \frac{1}{\sigma}$. Daher konvergiert $\int_1^{\infty} \frac{z-[z]}{z^{s+1}} dz$ gleichmäßig in jedem Kompaktum in $\Re(s) > 0$, ist also holomorph. Die Behauptung folgt. \square

Oben sahen wir recht einfach $\zeta(s) \neq 0$ für $\Re(s) > 1$. Diese Aussage dehnen wir nun aus auf $\Re(s) = 1$. Der Beweis beruht auf einem genialen Trick von Hadamard, versehen mit Vereinfachungen durch Mertens und de la Vallée Poussin. Der ursprüngliche Beweis von de la Vallée Poussin umfasste etwa 25 Seiten!

Im Beweis verwenden wir eine einfache Aussage über die *von Mangoldt Funktion* $\Lambda(n)$.

Lemma 4.4. Für $n \in \mathbb{N}$ definiere $\Lambda(n)$ durch $\Lambda(n) = \log p$, wenn n eine Potenz von $p \in \mathbb{P}$ ist, und $\Lambda(n) = 0$ sonst. Dann gilt für $\Re(s) > 1$

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

Beweis. Aus der Definition folgt sofort $\log n = \sum_{d|n} \Lambda(d)$, also $\log = \epsilon \star \Lambda$. Aus $-\zeta'(s) = \sum_{n=1}^{\infty} \frac{\log n}{n^s}$ folgt $-\zeta'(s) = \zeta(s) \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$. (Beachte, dass die angegebenen Reihen in $\Re(s) > 1$ absolut und in jedem Kompaktum gleichmäßig konvergieren.) \square

Satz 4.5. $\zeta(s) \neq 0$ für $\mathcal{R}(s) \geq 1$.

Beweis. Für $\mathcal{R}(s) > 1$ kennen wir die Aussage schon, es sei also $\mathcal{R}(s) = 1$.

Setze $F(s) = -\frac{\zeta'(s)}{\zeta(s)}$. Wir wissen, dass $F(s)$ meromorph für $\mathcal{R}(s) > 0$ ist. Sei r die Ordnung von $\zeta(s)$ in s_0 , d.h. $\zeta(s) = (s-s_0)^r h(s)$, mit $h(s_0) \neq 0$ und h holomorph in einer Umgebung von s_0 . Aus $(s-s_0)\frac{\zeta'(s)}{\zeta(s)} = \frac{rh(s)+(s-s_0)h'(s)}{h(s)}$ folgt

$$\lim_{\epsilon \rightarrow 0} \epsilon F(s_0 + \epsilon) = -r.$$

Sei $s = 1 + i\alpha$ eine Nullstelle von $\zeta(s)$ der Ordnung $\mu \geq 0$. Sei $\nu \geq 0$ die Ordnung von $\zeta(s)$ in $1 + 2i\alpha$. Dies liefert

$$\begin{aligned} \lim_{\epsilon \searrow 0} \epsilon F(1 + \epsilon) &= 1 \\ \lim_{\epsilon \searrow 0} \epsilon F(1 + \epsilon \pm i\alpha) &= -\mu \\ \lim_{\epsilon \searrow 0} \epsilon F(1 + \epsilon \pm 2i\alpha) &= -\nu. \end{aligned}$$

Wegen

$$\begin{aligned} \sum_{r=-2}^2 \binom{4}{2+r} F(1 + \epsilon + ir\alpha) &= \sum_{r=-2}^2 \binom{4}{2+r} \sum_{n \in \mathbb{N}} \frac{\Lambda(n)}{n^{1+\epsilon+ir\alpha}} \\ &= \sum_{n \in \mathbb{N}} \frac{\Lambda(n)}{n^{1+\epsilon}} (n^{\frac{i\alpha}{2}} + n^{-\frac{i\alpha}{2}})^4 \\ &\geq 0 \end{aligned}$$

folgt $-\nu - 4\mu + 6 - 4\mu - \nu \geq 0$, also $8\mu \leq 6 - 2\nu \leq 6$, und das ist nur für $\mu = 0$ möglich. \square

Im nächsten Abschnitt benötigen wir die folgende Aussage.

Satz 4.6. Sei $\Phi(s) = \sum_{p \in \mathbb{P}} \frac{\log p}{p^s}$. Dann ist $\Phi(s) - \frac{1}{s-1}$ holomorph in $\mathcal{R}(s) \geq 1$.

Beweis. Sei wieder $F(s) = -\frac{\zeta'(s)}{\zeta(s)}$. Aus dem bisherigen wissen wir, dass $F(s) - \frac{1}{s-1}$ holomorph in $\mathcal{R}(s) \geq 1$ ist. Die Behauptung folgt also, wenn wir zeigen, dass sich $F(s) - \Phi(s)$ nach $\mathcal{R}(s) \geq 1$ holomorph fortsetzen läßt. Offenbar gilt für $\mathcal{R}(s) > 1$

$$F(s) - \Phi(s) = \sum_{\substack{p \in \mathbb{P} \\ 2 \leq r \in \mathbb{N}}} \frac{\log p}{(p^r)^s}.$$

Die folgende Rechnung zeigt sogar holomorphe Fortsetzbarkeit von $F(s) - \Phi(s)$ nach $\mathcal{R}(s) > \frac{1}{2}$. Dabei ist $C = 2/(2 - \sqrt{2})$, und wir verwenden $\frac{1}{p^{2\sigma} - p^\sigma} \leq \frac{C}{p^{2\sigma}}$ für $p \in \mathbb{P}$ und $\sigma > 1/2$.

$$\begin{aligned}
 \left| \sum_{\substack{p \in \mathbb{P} \\ 2 \leq r \in \mathbb{N}}} \frac{\log p}{(p^r)^s} \right| &\leq \sum_{\substack{p \in \mathbb{P} \\ 2 \leq r \in \mathbb{N}}} \frac{\log p}{(p^r)^\sigma} \\
 &= \sum_{p \in \mathbb{P}} \frac{\log p}{p^{2\sigma} - p^\sigma} \\
 &\leq C \sum_{p \in \mathbb{P}} \frac{\log p}{p^{2\sigma}} \\
 &\leq C \sum_{n \in \mathbb{N}} \frac{\log n}{n^{2\sigma}} \\
 &= -\zeta'(2\sigma)
 \end{aligned}$$

□

Aufgaben. 1. Für $n \in \mathbb{N}$ ist die Eulersche φ -Funktion $\varphi(n)$ definiert als die Anzahl der zu n teilerfremden Zahlen aus $\{1, 2, \dots, n\}$. Zeige $\sum_{d|n} \varphi(d) = n$.

Hinweis: Zeige, dass es in der zyklischen Gruppe der Ordnung n für alle $d | n$ genau $\varphi(d)$ Elemente der Ordnung d gibt.

2. Zeige, dass φ multiplikativ ist, und gib eine Formel für $\varphi(p^m)$, $p \in \mathbb{P}$, $m \in \mathbb{N}$ an.

3. Sei G eine endliche zyklische Gruppe der Ordnung n . Für $g \in G$ sei $|g|$ die Ordnung von g . Sei $a(n)$ die durchschnittliche Ordnung der Elemente von G , d.h. $a(n) = \frac{1}{n} \sum_{g \in G} |g|$. Zeige³ $\varphi(n) \leq a(n) \leq \frac{\zeta(2)\zeta(3)}{\zeta(6)} \varphi(n)$.

Hinweis: $a(n)/\varphi(n)$ multiplikativ ist. Berechne $a(p^m)/\varphi(p^m)$.

5 Der Primzahlsatz

Definition 5.1. Für Funktionen f, g schreiben wir $f \sim g$, wenn $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$ gilt.

³Dieses Resultat erscheint in einer gemeinsamen Arbeit von von zur Gathen, Knopfmacher, Luca, Lucht und Shparlinski.

Der Primzahlsatz $\pi(n) \sim \frac{n}{\log n}$ wurde bereits um 1800 von verschiedenen Mathematikern (Gauß, Legendre, ...) vermutet. Erst 1896 konnten Hadamard [Had96] und de la Vallée Poussin [dlVP96] diese Vermutung beweisen. Eine bahnbrechende Vorarbeit ist Riemanns kurze Arbeit [Rie] von 1858. In der Folge wurde der analytische Beweis vereinfacht (Landau, Wiener, ...). 1980 fand D. J. Newman [New80] einen besonders einfachen Beweis. Dieser wurde später von Korevaar [Kor82] und Zagier [Zag97] noch etwas vereinfacht. Wir werden weitgehend Zagiers Darstellung folgen.

Lange Zeit suchte man elementare Beweise des Primzahlsatzes, d.h. solche, die keine Funktionentheorie verwenden. Bereits 1852 bewies Tchebychev durch Betrachtung der Primfaktorzerlegung von $n!$ (siehe Aufgabe 4 in Abschnitt 1) und raffinierten elementaren Argumenten die Existenz von $0 < c_1 < c_2$ (mit expliziten Beispielen), so dass $c_1 \frac{n}{\log n} < \pi(n) < c_2 \frac{n}{\log n}$ gilt. Ferner zeigte er: Falls der Grenzwert $\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\log n}$ existiert, dann ist er 1.

Erst knapp 100 Jahre später gelangen 1949 Erdős und Selberg elementare Beweise. Trotz späterer Vereinfachungen sind die sogenannten elementaren Beweise auch heute noch sehr technisch und undurchsichtig.

Die wesentliche Neuerung durch Newman ist der einfache Beweis des folgenden Satzes von Ingham 1935.

Satz 5.2. *Sei $f(t)$ ($t \geq 0$) eine beschränkte und lokal integrierbare Funktion. Ferner sei die Laplace-Transformierte $g(z) = \int_0^\infty f(t)e^{-zt} dt$ ($\Re(z) > 0$) holomorph nach $\Re(z) \geq 0$ fortsetzbar. Dann existiert $\int_0^\infty f(t)dt$, und es gilt $\int_0^\infty f(t)dt = g(0)$.*

Beweis. Für $T > 0$ ist $g_T(z) := \int_0^T f(t)e^{-zt} dt$ offensichtlich holomorph in \mathbb{C} . Wir wollen $\lim_{T \rightarrow \infty} g_T(0) = g(0)$ zeigen.

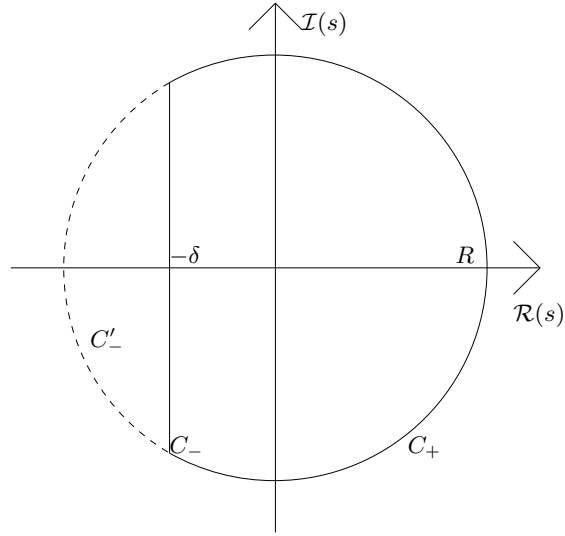
Sei $R > 0$ beliebig, und $\delta > 0$ (in Abhängigkeit von R) so gewählt, dass $g(z)$ auf $G := \{z \in \mathbb{C} \mid |z| \leq R, \Re(z) \geq -\delta\}$ holomorph ist. Sei C der Rand von G . Die Cauchysche Integralformel liefert⁴

$$g(0) - g_T(0) = \frac{1}{2\pi i} \int_C (g(z) - g_T(z)) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z}. \quad (1)$$

Wir schätzen den Integranden auf verschiedenen Teilen von C ab. Sei $C_+ = \{z \in C \mid \Re(z) > 0\}$. Wähle B mit $|f(t)| < B$ für alle $t \geq 0$. Auf C_+ gilt

$$|g(z) - g_T(z)| = \left| \int_T^\infty f(t)e^{-zt} dt \right| \leq B \int_T^\infty |e^{-zt}| dt = B \cdot \frac{e^{-\Re(z)T}}{\Re(z)}$$

⁴Der Faktor e^{zT} im Integrand ist durch die folgenden Rechnungen nahegelegt. Der Trick in Newmans Beweis ist das Hinzufügen des Faktors $1 + \frac{z^2}{R^2}$, welcher dort Nullstellen hat, wo der Integrand ohne diesen Faktor groß werden würde, siehe Aufgabe 3 unten.



und

$$|e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z}| = e^{\mathcal{R}(z)T} \cdot \frac{2\mathcal{R}(z)}{R^2}.$$

Daher ist der Integrand in Gleichung (1) auf C_+ betragsmäßig durch $\frac{2B}{R^2}$ beschränkt. Somit gilt

$$\left| \frac{1}{2\pi i} \int_{C_+} (g(z) - g_T(z)) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} \right| \leq \frac{1}{2\pi} \cdot \frac{2B}{R^2} \cdot R\pi = \frac{B}{R}.$$

Nun wenden wir uns dem anderen Teil $C_- = \{z \in C \mid \mathcal{R}(z) < 0\}$ zu. Zunächst betrachten wir $\int_{C_-} (g_T(z)) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z}$. Wegen der Holomorphie von $g_T(z)$ in \mathbb{C} können wir C_- durch den Halbkreis $C'_- = \{z \in \mathbb{C} \mid |z| = R, \mathcal{R}(z) < 0\}$ ersetzen. Wie oben folgt für $z \in C'_-$

$$|g_T(z)| = \left| \int_0^T f(t) e^{-zt} dt \right| \leq B \int_{-\infty}^T |e^{-zt}| dt = B \cdot \frac{e^{-\mathcal{R}(z)T}}{|\mathcal{R}(z)|}$$

und

$$|e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z}| = e^{\mathcal{R}(z)T} \cdot \frac{2|\mathcal{R}(z)|}{R^2},$$

also

$$\left| \frac{1}{2\pi i} \int_{C_-} (g_T(z)) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} \right| \leq \frac{B}{R}.$$

Nun betrachte $\frac{1}{2\pi i} \int_{C_-} (g(z)) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z}$. Beachte, dass $g(z) \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z}$ unabhängig von T ist, und $\lim_{T \rightarrow \infty} e^{zT} = 0$ gilt. Es folgt

$$\limsup_{T \rightarrow \infty} |g(0) - g_T(0)| \leq \frac{2B}{R}.$$

Aber R war beliebig gewählt, die Behauptung folgt. \square

Ersetzt man im Satz $f(t)$ durch $h(e^t)$, und macht die Variablentransformation $e^t = x$, so erhält man folgendes

Korollar 5.3. Sei $h(x)$ ($x \geq 1$) eine beschränkte und lokal integrierbare Funktion. Ferner sei $g(z) = \int_1^\infty h(x) \frac{dx}{x^{z+1}}$ ($\Re(z) > 0$) holomorph nach $\Re(z) \geq 0$ fortsetzbar. Dann existiert $\int_1^\infty h(x) \frac{dx}{x}$, und es gilt $\int_1^\infty h(x) \frac{dx}{x} = g(0)$.

Die Primzahlzählfunktion $\pi(n)$ lässt sich nicht direkt mit Dirichlet-Reihen in Verbindung bringen. Als Brücke dient uns die für $x \in \mathbb{R}$ definierte Funktion

$$\theta(x) = \sum_{p \leq x} \log p.$$

Wir beginnen mit einer elementaren Aussage von Tchebychev.

Lemma 5.4. Für $x \geq 1$ ist $\frac{\theta(x)}{x}$ beschränkt.

Beweis. Jede Primzahl p mit $n < p \leq 2n$ teilt $\binom{2n}{n} = \frac{2n \cdot (2n-1) \cdots (n+1)}{1 \cdot 2 \cdots n}$, hieraus folgt

$$e^{\theta(2n) - \theta(n)} = \prod_{n < p \leq 2n} p \leq \binom{2n}{n} \leq \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n},$$

also

$$\theta(2n) - \theta(n) \leq \frac{2n}{\log 2}.$$

Für $N \in \mathbb{N}$ wähle $m \in \mathbb{N}_0$ mit $2^{m-1} < N \leq 2^m$. Die Behauptung folgt nun aus

$$\begin{aligned} \theta(N) &\leq \theta(2^m) \\ &= \theta(2^m) - \theta(2^0) \\ &= (\theta(2^m) - \theta(2^{m-1})) + \cdots + (\theta(2) - \theta(1)) \\ &\leq \frac{1}{\log 2} (2^m + 2^{m-1} + \cdots + 2^1) \\ &= \frac{2}{\log 2} (2^m - 1) \\ &\leq \frac{4}{\log 2} 2^{m-1} \\ &< \frac{4}{\log 2} N. \end{aligned}$$

\square

Der Schlüssel zum Primzahlsatz ist die folgende Anwendung von obigem Konvergenzsatz.

Lemma 5.5. *Das Integral $\int_1^\infty \frac{\theta(x)-x}{x^2} dx$ konvergiert.*

Beweis. Für $\mathcal{R}(s) > 1$ gilt

$$\begin{aligned}\Phi(s) &= \sum_{p \in \mathbb{P}} \frac{\log p}{p^s} \\ &= \sum_{n=2}^{\infty} \frac{\theta(n) - \theta(n-1)}{n^s} \\ &= \sum_{n=1}^{\infty} \theta(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \\ &= \sum_{n=1}^{\infty} \theta(n) \int_n^{n+1} \frac{s}{x^{s+1}} dx \\ &= s \int_1^\infty \frac{\theta(x)}{x^{s+1}} dx.\end{aligned}$$

Die Funktion $h(x) = \frac{\theta(x)}{x} - 1$ erfüllt die Voraussetzungen von Korollar 5.3. Wir berechnen

$$\begin{aligned}g(z) &= \int_1^\infty h(x) \frac{dx}{x^{z+1}} \\ &= \int_1^\infty \frac{\theta(x) - x}{x^{z+2}} dx \\ &= \frac{\Phi(z+1)}{z+1} - \frac{1}{z}.\end{aligned}$$

Nach Satz 4.6 ist $\frac{\Phi(z+1)}{z+1} - \frac{1}{z}$ holomorph in $\mathcal{R}(z) \geq 0$, Korollar 5.3 liefert daher die Existenz von $\int_1^\infty \frac{\theta(x)-x}{x^2} dx$. \square

Der restliche Weg zum Primzahlsatz besteht aus Routineargumenten.

Satz 5.6. *Es gilt $\theta(x) \sim x$.*

Beweis. Man nehme an, es gibt $\lambda > 1$ mit $\theta(u) \geq \lambda u$ für beliebig große u . Aus der Monotonie von $\theta(u)$ folgt für diese u

$$\int_u^{\lambda u} \frac{\theta(x) - x}{x^2} dx \geq \int_u^{\lambda u} \frac{\lambda u - x}{x^2} dx = \int_1^\lambda \frac{\lambda - y}{y^2} dy > 0,$$

unabhängig von u . Dies widerspricht Lemma 5.5. Sei nun $\lambda < 1$ mit $\theta(u) \leq \lambda u$ für beliebig große u . Eine ähnliche Rechnung liefert den Widerspruch

$$\int_{\lambda u}^u \frac{\theta(x) - x}{x^2} dx \leq \int_{\lambda u}^u \frac{\lambda - y}{y^2} dy < 0.$$

□

Nun erhalten wir das Ziel dieses Abschnitts.

Satz 5.7. *Es gilt $\pi(x) \sim \frac{x}{\log x}$.*

Beweis. Aus

$$\theta(x) = \sum_{p \leq x} \log p \leq \sum_{p \leq x} \log x = \pi(x) \cdot \log x$$

folgt zusammen mit Satz 5.6

$$\limsup_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = \limsup_{x \rightarrow \infty} \frac{\theta(x)}{x} = 1.$$

Es bleibt $\liminf_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1$ zu zeigen. Wir nehmen an, dass das nicht gilt.

Dann gibt es $\epsilon > 0$ und eine unendliche Teilmenge $M \subseteq \mathbb{N}$ mit $\frac{\pi(x)}{x/\log x} \geq 1 + \epsilon$ für $x \in M$. Wähle $\delta > 0$ mit $1 + \rho := (1 - \delta)(1 + \epsilon) > 1$. Wegen $\pi(x^{1-\delta}) \leq x^{1-\delta}$ gilt für $x \in M$:

$$\begin{aligned} \theta(x) &\geq \sum_{x^{1-\delta} < p \leq x} \log p \\ &\geq \log x^{1-\delta} (\pi(x) - \pi(x^{1-\delta})) \\ &\geq (1 - \delta) \log x \left((1 + \epsilon) \frac{x}{\log x} - x^{1-\delta} \right) = (1 + \rho)x - (1 - \delta) \log x \cdot x^{1-\delta}. \end{aligned}$$

Wegen $\lim_{x \rightarrow \infty} \frac{(1-\delta) \log x \cdot x^{1-\delta}}{x} = 0$ folgt daraus $\limsup_{x \rightarrow \infty} \frac{\theta(x)}{x} \geq 1 + \rho$, im Widerspruch zu Satz 5.6. □

Aufgaben. 1. Zeige $\frac{n}{\log n} \sim \int_2^n \frac{dt}{\log t}$.

2. Sei p_n die n -te Primzahl. Zeige $p_n \sim n \log n$.

3. Man überzeuge sich davon, dass Newmans Beweis nicht funktioniert, wenn man die einfachere Formel $g(0) - g_T(0) = \frac{1}{2\pi i} \int_C (g(z) - g_T(z)) e^{zT} \frac{dz}{z}$ benutzt.

6 Charaktere abelscher Gruppen

Charaktere werden im nächsten Abschnitt das Hilfsmittel sein, Elemente aus arithmetischen Progressionen herauszufiltern. Mit dieser Technik werden wir den Primzahlsatz von Dirichlet beweisen, der besagt, dass in jeder arithmetischen Folge $a + nb$, $n \in \mathbb{N}$ mit teilerfremden $a, b \in \mathbb{N}$ unendlich viele Primzahlen liegen.

Sei G eine endliche abelsche Gruppe. Wir erinnern an den Satz (siehe zum Beispiel ???), dass G das direkte Produkt zyklischer Gruppen ist. Das heißt es gibt Elemente $g_1, g_2, \dots, g_r \in G$ und $u_1, u_2, \dots, u_r \in \mathbb{N}$, so dass jedes Element $g \in G$ eine eindeutige Darstellung $g = g_1^{e_1} g_2^{e_2} \dots g_r^{e_r}$ mit $1 \leq e_i \leq u_i$ hat.

Mit \mathbb{C}^* bezeichnen wir die multiplikative Gruppe $\mathbb{C} \setminus \{0\}$.

Definition. Ein Charakter χ von G ist ein Gruppenhomomorphismus $G \rightarrow \mathbb{C}^*$. Die Menge aller Charaktere von G bezeichnen wir mit \hat{G} .

Bemerkung. (a) Die Werte von χ sind Einheitswurzeln, denn sei $g \in G$, dann gibt es $m \in \mathbb{N}$ mit $g^m = 1$, also $1 = \chi(1) = \chi(g^m) = \chi(g)^m$.

(b) Die Menge \hat{G} ist eine Gruppe, mit der Multiplikation $(\chi_1 \chi_2)(g) = \chi_1(g) \chi_2(g)$.

Satz 6.1. Es gilt $|\hat{G}| = |G|$.

Beweis. Seien g_i, u_i wie oben, und $\chi \in \hat{G}$. Der Charakter χ ist durch seine Werte auf den g_i festgelegt. Wegen $1 = \chi(1) = \chi(g_i^{u_i}) = \chi(g_i)^{u_i}$ ist $\chi(g_i)$ eine u_i te Einheitswurzel, nimmt also einen von u_i möglichen Werten an. Es folgt $|\hat{G}| \leq u_1 u_2 \dots u_r = |G|$.

Umgekehrt sei ζ_i für $i = 1, 2, \dots, r$ eine u_i te Einheitswurzel. Offenbar gibt es $u_1 u_2 \dots u_r = |G|$ Möglichkeiten für die Wahl eines solchen Tupels $\zeta_1, \zeta_2, \dots, \zeta_r$. Man definiert eine Abbildung $\chi : G \rightarrow \mathbb{C}^*$ durch $\chi(g_1^{e_1} g_2^{e_2} \dots g_r^{e_r}) = \zeta_1^{e_1} \zeta_2^{e_2} \dots \zeta_r^{e_r}$. Eine einfache Rechnung zeigt $\chi \in \hat{G}$. \square

Lemma 6.2. (a) Sei $1 \neq \chi \in \hat{G}$. Dann gilt $\sum_{g \in G} \chi(g) = 0$.

(b) Sei $1 \neq g \in G$. Dann gilt $\sum_{\chi \in \hat{G}} \chi(g) = 0$.

Beweis. (a) Sei $1 \neq \chi \in \hat{G}$. Dann gibt es $h \in G$ mit $\chi(h) \neq 1$. Mit g durchläuft auch hg die Elemente der Gruppe G . Daher gilt

$$S = \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \sum_{g \in G} \chi(h) \chi(g) = \chi(h) \sum_{g \in G} \chi(g) = \chi(h) S,$$

also $(\chi(h) - 1)S = 0$, und schließlich $S = 0$.

(b) Sei nun $1 \neq g \in G$. Mittels obiger expliziter Beschreibung der Elemente in \hat{G} zeigt man leicht, dass es ein $\psi \in \hat{G}$ gibt mit $\psi(g) \neq 1$. Mit χ durchläuft auch $\psi\chi$ die Menge \hat{G} . Wie oben folgt

$$S = \sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} (\psi\chi)(g) = \psi(g) \sum_{\chi \in \hat{G}} \chi(g) = \psi(g)S,$$

also $S = 0$, da $\psi(g) - 1 \neq 0$. □

Bemerkung. Wegen $1 = \chi(gg^{-1}) = \chi(g)\chi(g)^{-1}$ gilt $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$, wobei $\bar{\chi}$ den komplex konjugierten Charakter bezeichnet, also $\bar{\chi}(g) = \overline{\chi(g)}$ für alle g .

Als Folge obigen Lemmas bekommen wir

Korollar 6.3. (a) Seien $\chi, \psi \in \hat{G}$. Dann gilt

$$\sum_{g \in G} \chi(g)\bar{\psi}(g) = \begin{cases} |G|, & \chi = \psi \\ 0, & \chi \neq \psi \end{cases}$$

(b) Seien $g, h \in G$. Dann gilt

$$\sum_{\chi \in \hat{G}} \chi(g)\bar{\chi}(h) = \begin{cases} |G|, & g = h \\ 0, & g \neq h \end{cases}$$

Beweis. Es gilt $\chi\bar{\chi} = 1$ genau dann wenn $\chi = \psi$, Behauptung (a) folgt dann sofort aus obigem Lemma. Genauso folgt (b), denn $\chi(g)\bar{\chi}(h) = \chi(g)\chi(h^{-1}) = \chi(gh^{-1})$. □

Für $a, b \in \mathbb{Z}$ mit a, b nicht beide 0 bezeichnen wir mit $(a, b) \in \mathbb{N}$ den größten gemeinsamen Teiler von a und b .

Definition. Sei $N \in \mathbb{N}$, und $G = (\mathbb{Z}/N\mathbb{Z})^* = \{n + N\mathbb{Z} \mid (n, N) = 1\}$ die Einheitengruppe des Restklassenrings $\mathbb{Z}/N\mathbb{Z}$. Sei $\chi' \in \hat{G}$. Wir setzen χ' zu einer Funktion auf $\mathbb{Z}/N\mathbb{Z}$ fort, indem wir $\chi'(n + N\mathbb{Z}) = 0$ setzen für $(n, N) \neq 1$. Dies definiert eine Funktion $\chi : \mathbb{Z} \rightarrow \mathbb{C}$ durch $\chi(n) = \chi'(n + N\mathbb{Z})$. Ein solches χ heißt *Dirichlet-Charakter modulo N* .

Bemerkung. Man zeigt sofort, dass eine Abbildung $\chi : \mathbb{Z} \rightarrow \mathbb{C}$ genau dann ein Dirichlet-Charakter modulo N ist, wenn folgende Bedingungen erfüllt sind:

- (i) $\chi(n) = 0$ genau dann wenn $(n, N) \neq 1$.
- (ii) χ ist vollständig multiplikativ.
- (iii) Aus $N \mid a - b$ folgt $\chi(a) = \chi(b)$.

Beispiele. (a) Der Hauptcharakter χ_0 entsteht aus $\chi' = 1$ von oben, also $\chi(n) = 1$ oder 0 , je nachdem ob $(n, N) = 1$ oder $\neq 1$.

- (b) Sei $p \in \mathbb{P}$. Das Legendresymbol $\chi(n) = \left(\frac{n}{p}\right)$ definiert einen Dirichlet-Charakter modulo p .

7 Der Dirichletsche Primzahlsatz

Das analytische Hilfsmittel zum Beweis des Dirichletschen Primzahlsatzes sind die zu Dirichlet-Charakteren gehörigen Dirichlet-Reihen.

Definition. Sei χ ein Dirichlet-Charakter modulo N . Dann ist

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

die zugehörige Dirichlet-Reihe.

Satz 7.1. Die Reihe $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ stellt eine in $\Re(s) > 1$ holomorphe Funktion dar, ferner gilt dort $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$.

Beweis. Sei $s_0 = \Re(s)$. Aus $|\chi(n)| \leq 1$ folgt $\sum_{n=1}^{\infty} \left| \frac{\chi(n)}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^{s_0}} = \zeta(s_0)$, und das ergibt den ersten Teil der Behauptung. Die Produktentwicklung folgt aus der vollständigen Multiplikativität von χ und Satz ???. \square

Lemma 7.2. Sei χ_0 der Hauptcharakter modulo N . Dann hat $L(s, \chi_0)$ eine holomorphe Fortsetzung nach $\{s \mid \Re(s) > 0, s \neq 1\}$. In $s = 1$ hat $L(s, \chi_0)$ einen Pol 1. Ordnung.

Beweis. Für $\Re(s) > 1$ gilt

$$\begin{aligned} L(s, \chi_0) &= \prod_{p \nmid N} \frac{1}{1 - \frac{1}{p^s}} \\ &= \prod_p \frac{1}{1 - \frac{1}{p^s}} \prod_{p \mid N} \left(1 - \frac{1}{p^s}\right) \\ &= \zeta(s) \prod_{p \mid N} \left(1 - \frac{1}{p^s}\right). \end{aligned}$$

Die Behauptung folgt nun aus den bekannten Eigenschaften von $\zeta(s)$. \square

Lemma 7.3. Sei χ ein Dirichlet-Charakter, der kein Hauptcharakter ist. Dann hat $L(s, \chi)$ eine holomorphe Fortsetzung nach $\Re(s) > 0$.

Beweis. Sei χ ein Dirichlet-Charakter modulo N . Dann ist χ periodisch mit der Periode N , und wegen Lemma ??? gilt $\sum_{n=1}^N \chi(n) = 0$. Daher sind die Partialsummen $A(x) = \sum_{n \leq x} \chi(n)$ beschränkt, also $|A(x)| \leq C$ für ein $C > 0$ und alle x . (Man kann $C = N$ wählen.) Für $\Re(s) > 1$ liefert partielle Summation

$$\begin{aligned} L(s, \chi) &= \sum_{n=1}^{\infty} \frac{A(n) - A(n-1)}{n^s} \\ &= \sum_{n=1}^{\infty} A(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \\ &= \sum_{n=1}^{\infty} A(n) \int_n^{n+1} s \frac{dt}{t^{s+1}} \\ &= s \int_1^{\infty} \frac{A(t)}{t^{s+1}} dt. \end{aligned}$$

Das Integral konvergiert gleichmäßig auf Kompakta in $\Re(s) > 0$, die Behauptung folgt. \square

Beim Beweis des Primzahlsatzes war die Aussage wesentlich, dass die Zetafunktion keine Nullstellen in $\Re(s) \geq 1$ hat. Eine ähnliche Situation tritt beim Beweis des Dirichletschen Primzahlsatzes auf. Hier benötigen wir die Aussage $L(1, \chi) \neq 0$. Diese Aussage ist weniger trivial als man vielleicht auf den ersten Blick vermuten würde. Der Beweis behandelt nicht eine einzelne Dirichlet-Reihe, sondern verwendet den Trick, dass man ein Produkt von Dirichlet-Reihen zu verschiedenen Charakteren betrachtet, über das man leichter etwas beweisen kann. Als Vorbereitung dient das folgende

Lemma 7.4. Sei $N \in \mathbb{N}$ und $F(s)$ das Produkt der Dirichlet-Reihen $L(s, \chi)$, wo χ die Dirichlet-Charaktere modulo N durchläuft. Dann gilt $F(s) \geq 1$ für alle $s \geq 1$.

Beweis. Für $s \geq 1$ gilt

$$F(s) = \prod_{\chi} \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

Die Behauptung folgt aus einer Umsortierung absolut konvergenter Reihen

$$\begin{aligned}\log F(s) &= \sum_{\chi} \sum_p \sum_{v=1}^{\infty} \frac{1}{v} \left(\frac{\chi(p)}{p^s}\right)^v \\ &= \sum_p \sum_{v=1}^{\infty} \frac{1}{vp^{vs}} \sum_{\chi} \chi(p^v) \\ &\geq 0,\end{aligned}$$

da für $n \in \mathbb{N}$ stets $\sum_{\chi} \chi(n) \geq 0$ gilt. (Die Summe verschwindet außer für $n \equiv 1 \pmod{N}$, in diesem Fall ist sie $\varphi(N)$.) \square

Satz 7.5. *Sei χ ein Dirichlet-Charakter, der kein Hauptcharakter ist. Dann gilt $L(1, \chi) \neq 0$.*

Beweis. Sei $L(1, \chi) = 0$, wo χ ein Dirichlet-Charakter modulo N ist. Sei $F(s)$ wie im vorigen Lemma. Da $F(1) \neq 0$ und $L(s, \chi_0)$ einen Pol 1. Ordnung in $s = 1$ hat, ist χ der einzige Dirichlet-Charakter modulo N , so dass die zugehörige Dirichlet-Reihe in 1 verschwindet. Insbesondere ist χ reellwertig, denn aus $L(1, \chi) = 0$ folgt $L(1, \bar{\chi}) = 0$, also $\chi = \bar{\chi}$.

Setze $G(s) = \zeta(s)L(s, \chi)$. Offenbar ist $G(s)$ holomorph in $\Re(s) > 0$. Es gilt

$$G(s) = \zeta(s)L(s, \chi) = \sum \frac{a(n)}{n^s}$$

mit $a(n) = \sum_{d|n} \chi(d)$. Da χ multiplikativ ist, gilt das gleiche auch für $a(n)$. Da $\chi(d)$ reell ist, und $\chi(d)$ entweder 0 ist oder eine Einheitswurzel, gilt stets $\chi(d) \in \{-1, 0, 1\}$. Es ist

$$a(p^r) = \sum_{k=0}^r \chi(p^k) = \sum_{k=0}^r \chi(p)^k.$$

Daher gilt stets $a(p^r) \geq 1$, außer wenn $\chi(p) = -1$ und r ungerade ist. In diesem Fall ist $a(p^r) = 0$. Aus der Multiplikativität von $a(n)$ folgt nun $a(n) \geq 0$ und $a(n^2) \geq 1$ für alle $n \in \mathbb{N}$.

Wir können also den Satz ??? von Landau anwenden. Die Dirichlet-Reihe von $G(s)$ konvergiert zum Beispiel für $s = \frac{1}{2}$. Aber

$$\sum_n \frac{a(n)}{\sqrt{n}} \geq \sum_n \frac{a(n^2)}{n} \geq \sum_n \frac{1}{n} = \infty,$$

ein Widerspruch. \square

Nun können wir das Ziel dieses Abschnitts beweisen.

Satz 7.6. *Seien $a, N \in \mathbb{N}$ mit $(a, N) = 1$. Dann gibt es unendlich viele Primzahlen p mit $p \equiv a \pmod{N}$. Es gilt sogar*

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv a \pmod{N}}} \frac{1}{p} = \infty.$$

Beweis. In den folgenden Summen durchläuft χ die Menge der Dirichlet-Charaktere modulo N . Für $s > 1$ gilt

$$\begin{aligned} \sum_{\substack{p \in \mathbb{P}, r \in \mathbb{N} \\ p^r \equiv a \pmod{N}}} \frac{1}{rp^{rs}} &= \sum_{p \in \mathbb{P}, r \in \mathbb{N}} \frac{1}{rp^{rs}} \frac{1}{\varphi(N)} \sum_{\chi} \chi(p^r) \bar{\chi}(a) \\ &= \frac{1}{\varphi(N)} \sum_{\chi} \bar{\chi}(a) \sum_{p \in \mathbb{P}, r \in \mathbb{N}} \frac{\chi(p)^r}{rp^{rs}} \\ &= \frac{1}{\varphi(N)} \sum_{\chi} \bar{\chi}(a) \sum_{p \in \mathbb{P}} \log \frac{1}{1 - \frac{\chi(p)}{p^s}} \\ &= \frac{1}{\varphi(N)} \sum_{\chi} \bar{\chi}(a) \log L(s, \chi) \\ &= \frac{1}{\varphi(N)} (\log L(s, \chi_0) + \sum_{\chi \neq \chi_0} \bar{\chi}(a) \log L(s, \chi)). \end{aligned}$$

Es gilt $\lim_{s \searrow 1} \log L(s, \chi_0) = \infty$. Sei $\chi \neq \chi_0$. Da $L(1, \chi) \neq 0$, hat $\lim_{s \searrow 1} \log L(s, \chi)$ einen endlichen Grenzwert. Daher gilt $\lim_{s \searrow 1} \sum_{\substack{p \in \mathbb{P}, r \in \mathbb{N} \\ p^r \equiv a \pmod{N}}} \frac{1}{rp^{rs}} = \infty$, also

$\sum_{\substack{p \in \mathbb{P}, r \in \mathbb{N} \\ p^r \equiv a \pmod{N}}} \frac{1}{rp^r} = \infty$. Aber die Teilreihe mit $r \geq 2$ konvergiert wegen

$$\begin{aligned} \sum_{\substack{p \in \mathbb{P}, r \geq 2 \\ p^r \equiv a \pmod{N}}} \frac{1}{rp^r} &\leq \sum_{p \in \mathbb{P}} \sum_{r \geq 2} \frac{1}{rp^r} \\ &\leq \sum_{p \in \mathbb{P}} \sum_{r \geq 2} \frac{1}{2p^r} \\ &= \frac{1}{2} \sum_{p \in \mathbb{P}} \frac{1}{p(p-1)} \\ &\leq \frac{1}{2} \sum_{n \geq 2} \frac{1}{n(n-1)} \\ &= \frac{1}{2} \sum_{n \geq 2} \left(\frac{1}{n-1} - \frac{1}{n} \right) \\ &= \frac{1}{2}. \end{aligned}$$

Daher divergiert die zu $r = 1$ gehörige Teilfolge, die Behauptung folgt. \square

8 Die Gammafunktion

Die Gammafunktion Γ ist nach der Logarithmus- und Exponentialfunktion die wohl nächst einfache und -wichtige transzendente Funktion der Funktionentheorie. Da sie im Zusammenhang mit der Riemannschen Zetafunktion eine wichtige Rolle spielt, wollen wir nicht auf die Literatur verweisen, sondern Wielandts eleganten und schnellen Zugang zu den wesentlichen Eigenschaften darstellen.

Historisch entwickelte sich die Gammafunktion aus dem Versuch, die Fakultätsfunktion $n!$ zu einer reellen oder komplexen Funktion mit guten Eigenschaften fortzusetzen.

Der folgende Satz enthält die Definition der Gammafunktion Γ .

Satz 8.1. *Das Gammaintegral $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$ konvergiert in $\Re(z) > 0$ absolut, und stellt dort eine holomorphe Funktion dar.*

Beweis. Für $t \geq 1$ gibt es eine Konstante $C > 1$ mit $|t^{z-1} e^{-t}| \leq C \cdot e^{-t/2}$, und für $t \leq 1$ gilt $|t^{z-1} e^{-t}| \leq t^{\Re(z)-1}$. Daraus folgt schnell, dass die Folge holomorpher Funktionen $\int_{1/n}^n t^{z-1} e^{-t} dt$ lokal gleichmäßig gegen $\Gamma(z)$ konvergiert. Daher ist auch $\Gamma(z)$ holomorph. \square

Satz 8.2. Γ lässt sich holomorph nach $\mathbb{C} \setminus S$, $S := \{0, -1, -2, \dots\}$, fortsetzen, und genügt der Funktionalgleichung $\Gamma(z+1) = z\Gamma(z)$. Ferner gilt: $\Gamma(n+1) = n!$ für alle $n \in \mathbb{N}_0$, und $\Gamma(z)$ hat einen Pol erster Ordnung in $-n \in S$ mit Residuum $\frac{(-1)^n}{n!}$.

Beweis. $\Gamma(1) = \int_0^\infty e^{-t} dt = 1$. Integration von $\frac{d}{dt}(-t^z e^{-t}) = t^z e^{-t} + z t^{z-1} e^{-t}$ von 0 bis ∞ liefert $\Gamma(z+1) = z\Gamma(z)$. Hieraus folgt durch mehrfache Anwendung für $n \in \mathbb{N}_0$

$$\Gamma(z) = \frac{\Gamma(z+n+1)}{z(z+1)\dots(z+n)}.$$

Dies zeigt die holomorphe Fortsetzbarkeit nach $\mathbb{C} \setminus S$. Ferner hat Γ in S Pole der Ordnung ≤ 1 . Wir berechnen das Residuum in $-n \in S$:

$$\lim_{z \rightarrow -n} (z+n)\Gamma(z) = \frac{\Gamma(1)}{(-n)(-n+1)\dots(-1)} = \frac{(-1)^n}{n!}.$$

□

Bemerkung. Sei $0 < a < b$. Aus $|\Gamma(z)| \leq \Gamma(\mathcal{R}(z))$ für $\mathcal{R}(z) > 0$ folgt, dass $\Gamma(z)$ im Parallelstreifen $\{z \in \mathbb{C} \mid a \leq \mathcal{R}(z) < b\}$ beschränkt ist.

Die Funktionalgleichung, zusammen mit einer Beschränktheit in einem Parallelstreifen, liefert eine Art Umkehrung.

Satz 8.3 (Wielandt 1939). Sei $\mathbb{C}_+ = \{z \in \mathbb{C} \mid \mathcal{R}(z) > 0\}$, und $f : \mathbb{C}_+ \rightarrow \mathbb{C}$ holomorph mit

(a) f ist beschränkt auf $\{z \in \mathbb{C} \mid 1 \leq \mathcal{R}(z) < 2\}$.

(b) $f(z+1) = zf(z)$ für alle $z \in \mathbb{C}_+$.

Dann gilt $f(z) = f(1)\Gamma(z)$ für alle $z \in \mathbb{C}_+$.

Beweis. Wie für $\Gamma(z)$ zeigt man: $f(z)$ ist nach $\mathbb{C} \setminus S$ holomorph fortsetzbar, und $f(z+1) = zf(z)$ für alle $z \in \mathbb{C} \setminus S$. Ferner hat f in $-n \in S$ einen Pol der Ordnung ≤ 1 mit Residuum $\frac{(-1)^n}{n!}f(1)$. Daher hat $h(z) = f(z) - f(1)\Gamma(z)$ nur hebbare Singularitäten, also ist $h(z)$ eine ganze Funktion. Offensichtlich ist $h(z)$ in $\{z \in \mathbb{C} \mid 1 \leq \mathcal{R}(z) < 2\}$ beschränkt. Setze $H(z) = h(z)h(1-z)$. Wegen $H(z+1) = h(z+1)h(-z) = zh(z)h(-z) = -h(z)(-zh(-z)) = -h(z)h(-z+1) = -H(z)$ ist die ganze Funktion $H(z)$ auf \mathbb{C} beschränkt. Nach Liouville ist $H(z)$ eine Konstante. Wir berechnen $H(1) = h(0)h(1) = h(0)(f(1) - f(1)\Gamma(1)) = 0$, also $h(z)h(1-z) = 0$ für alle $z \in \mathbb{C}$. Aber die Nullstellen ganzer Funktionen $\neq 0$ liegen diskret in \mathbb{C} , daher ist $h(z) = 0$ für alle $z \in \mathbb{C}$, und die Behauptung folgt. □

Lemma 8.4. Die Reihe $\sum_{n=1}^{\infty} ((1 + \frac{z}{n})e^{-\frac{z}{n}} - 1)$ konvergiert absolut und kompakt auf \mathbb{C} .

Beweis. Die Funktion $\frac{(1+w)e^{-w}-1}{w^2}$ ist holomorph auf \mathbb{C} , also insbesondere stetig. Für alle $r > 0$ gibt es daher eine Konstante C , so dass $|\frac{(1+w)e^{-w}-1}{w^2}| \leq C$ gilt für alle $|w| \leq r$. Für $|z| \leq r$ und $n \in \mathbb{N}$ gilt daher $|(1 + \frac{z}{n})e^{-\frac{z}{n}} - 1| \leq C \frac{|z|^2}{n^2} \leq C \frac{r^2}{n^2}$. Aber $\sum_{n=1}^{\infty} C \frac{r^2}{n^2}$ konvergiert, und die Behauptung folgt. \square

Hieraus folgt aus einfachen Aussagen über die Holomorphie von Produkten (siehe etwa ???)

Korollar 8.5. $H(z) = \prod_{n=1}^{\infty} (1 + \frac{z}{n})e^{-\frac{z}{n}}$ ist eine ganze Funktion, mit $H(z) = 0$ genau dann wenn $-z \in \mathbb{N}$.

Lemma 8.6. Der Grenzwert $\gamma = \lim_{n \rightarrow \infty} (1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \log n)$ existiert, und heisst Eulersche Konstante.

Beweis. Übung. \square

Lemma 8.7. Setze $G_n(z) = ze^{-z \log n} \prod_{\nu=1}^n (1 + \frac{z}{\nu})$. Dann gilt $\lim_{n \rightarrow \infty} G_n(z) = ze^{\gamma z} H(z)$.

Beweis. Folgt aus $G_n(z) = ze^{z(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \log n)} \prod_{\nu=1}^n (1 + \frac{z}{\nu})e^{-\frac{z}{\nu}}$. \square

Korollar 8.8. $G(z) = \lim_{n \rightarrow \infty} G_n(z)$ ist ganz, und hat Nullstellen erster Ordnung in $z \in S = \{0, -1, -2, \dots\}$, und sonst keine weiteren Nullstellen.

Aus dem folgenden Satz folgt insbesondere, dass $\Gamma(z)$ keine Nullstellen in \mathbb{C} hat; eine Eigenschaft, die nicht direkt aus der Integraldefinition zu folgen scheint.

Satz 8.9 (Gauß). Für alle $z \in \mathbb{C}$ gilt $\frac{1}{\Gamma(z)} = G(z) = \lim_{n \rightarrow \infty} \frac{n^{-z}}{n!} z(z+1) \dots (z+n)$.

Beweis. Es ist nur $\frac{1}{G(z)} = \Gamma(z)$ zu zeigen. $G(z)$ hat keine Nullstellen für $\Re(z) > 0$, daher ist $\frac{1}{G(z)}$ holomorph für $\Re(z) > 0$. Für $\Re(z) > 0$ und $\nu \in \mathbb{N}_0$ gilt $|n^{-z}| = n^{-\Re(z)}$ und $|z + \nu| \geq \Re(z) + \nu$, also $|G_n(z)| \geq G_n(\Re(z))$. Für $n \rightarrow \infty$ folgt $|\frac{1}{G(z)}| \leq |\frac{1}{G(\Re(z))}|$. Insbesondere ist $\frac{1}{G(z)}$ beschränkt im Streifen $\{z \in \mathbb{C} | 1 \leq \Re(z) < 2\}$. Weiter zeigt eine einfache Rechnung $zG_n(z+1) = \frac{z+n+1}{n} G_n(z)$. Für $n \rightarrow \infty$ folgt daraus $\frac{1}{G(z+1)} = z \frac{1}{G(z)}$. Wielandts Satz ??? liefert $\frac{1}{G(z)} = \frac{1}{G(1)} \Gamma(z)$. Ferner ist $G_n(1) = \frac{1}{n} \prod_{\nu=1}^n \frac{1+\nu}{\nu} = \frac{n+1}{n}$, also $G(1) = 1$, und die Behauptung folgt. \square

Eine weitere wichtige Identität ist

Satz 8.10 (Euler). Für alle $z \in \mathbb{C} \setminus \mathbb{Z}$ gilt

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}.$$

Beweis. Die meromorphe Funktion $f(z) = \Gamma(z)\Gamma(1-z)$ hat Pole erster Ordnung in $n \in \mathbb{Z}$, mit Residuum $(-1)^n$. Dasselbe gilt für die Funktion $\frac{\pi}{\sin \pi z}$. Daher ist $h(z) = f(z) - \frac{\pi}{\sin \pi z}$ holomorph nach \mathbb{C} fortsetzbar. Der Parallelstreifen $B = \{z \in \mathbb{C} \mid 1 \leq \Re(z) \leq 2\}$ wird durch $z \mapsto 3-z$ bijektiv auf sich abgebildet. Daher sind $\Gamma(z)$ und $\Gamma(3-z)$ beschränkt auf B . Sei $Q = \{z \in B \mid -1 \leq \Im(z) \leq 1\}$. Wegen $\Gamma(1-z) = \frac{\Gamma(3-z)}{(2-z)(1-z)}$ ist dann $\Gamma(1-z)$ auf $B \setminus Q$ beschränkt. Man zeigt leicht, dass auch $\frac{\pi}{\sin \pi z}$ auf $B \setminus Q$ beschränkt ist, also ist $h(z)$ auf $B \setminus Q$ beschränkt. Die ganze Funktion h ist auch auf dem Kompaktum Q beschränkt, daher ist $h(z)$ auf B und schließlich wegen $h(z+1) = -h(z)$ in ganz \mathbb{C} beschränkt. Nach Liouville ist $h(z)$ eine Konstante. Aus $h(\frac{1}{2}) = -h(-\frac{1}{2})$ folgt $h(z) = 0$ für alle $z \in \mathbb{C}$, was zu zeigen war. \square

Als Folge erhalten wir die klassische Produktdarstellung der Sinusfunktion.

Korollar 8.11. In \mathbb{C} gilt

$$\frac{\pi}{\sin \pi z} = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right).$$

In diesen Zusammenhang gehört auch die Verdoppelungsformel von Legendre.

Satz 8.12 (Legendre). In \mathbb{C} gilt

$$\Gamma\left(\frac{z}{2}\right)\Gamma\left(\frac{z+1}{2}\right) = \frac{\sqrt{\pi}}{2^{z-1}}\Gamma(z).$$

Beweis. Die ganze Funktion $f(z) = 2^{z-1}\Gamma\left(\frac{z}{2}\right)\Gamma\left(\frac{z+1}{2}\right)$ erfüllt die Voraussetzungen aus Wielandts Satz 8.3. Es folgt $f(z) = f(1)\Gamma(z)$. Es gilt $f(1) = \Gamma\left(\frac{1}{2}\right)\Gamma(1) = \Gamma\left(\frac{1}{2}\right)$. Aus Satz 8.10 folgt $\Gamma\left(\frac{1}{2}\right)^2 = \Gamma\left(\frac{1}{2}\right)\Gamma\left(1 - \frac{1}{2}\right) = \pi$, und die Behauptung folgt, da $\Gamma\left(\frac{1}{2}\right) > 0$, also $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$. \square

9 Mehr zur Riemannschen Zetafunktion

In diesem Abschnitt beweisen wir unter anderem die Funktionalgleichung der Zetafunktion. Hierfür ist eine Vielzahl von Beweisen bekannt, siehe etwa

Titchmarsh ????. Wir folgen einem der Beweise aus Riemanns kurzer Arbeit ????. Die Methode ist vielleicht nicht die schnellste. Allerdings liefert sie eine Integraldarstellung der Zetafunktion, die sowohl vom theoretischen als auch vom praktischen Standpunkt aus sehr wichtig ist. Diese Integraldarstellung basiert auf Eigenschaften einer Thetafunktion $\theta(z)$, die im wesentlichen eine Modulform ist ??? (mehr dazu). Wir entwickeln die benötigten Eigenschaften ad hoc.

Lemma 9.1. *Sei $\varepsilon > 0$. Dann konvergiert die Reihe $\theta(z) = \sum_{n=-\infty}^{\infty} e^{-\pi zn^2}$ gleichmäßig und absolut in $\mathcal{R}(z) \geq \varepsilon$. Insbesondere ist $\theta(z)$ eine in $\mathcal{R}(z) > 0$ holomorphe Funktion, die Thetafunktion.*

Beweis. Für $n \geq 1$ und $\mathcal{R}(z) \geq \varepsilon$ gilt $|e^{-\pi zn^2}| \leq e^{-\pi n\varepsilon}$, die Behauptung folgt dann aus $\sum_{n=m}^{\infty} e^{-\pi n\varepsilon} = \frac{e^{-\pi m\varepsilon}}{1-e^{-\pi\varepsilon}}$. \square

Für große $x > 0$ konvergiert die Thetareihe sehr schnell. Ist hingegen x nahe bei 0, dann sind erst mal viele Summanden nahe bei 1, bevor gute Konvergenz einsetzt. Die folgende Transformationsformel erlaubt es, den Fall kleiner x auf den Fall großer x zurückzuführen. Der Beweis benutzt die klassische Technik des Residuensatzes zur Berechnung von Reihen. Andere Beweise benutzen z.B. die Poissonsche Summenformel, siehe etwa Brüdern???

Satz 9.2. *Für $x > 0$ gilt $\theta(x) = \frac{1}{\sqrt{x}}\theta(\frac{1}{x})$.*

Beweis (Landsberg 1893). Sei $x > 0$ fixiert. Wir wählen $N \in \mathbb{N}$, und betrachten den positiv orientierten Rand ∂R des Rechtecks mit den Eckpunkten $\pm(N + \frac{1}{2}) \pm i$. Die obere und untere Kante seien L_+ und L_- , die linke und rechte Kante seien M_+ und M_- . Die Funktion $f(t) = \frac{e^{-\pi xt^2}}{e^{2\pi it} - 1}$ ist holomorph in $\mathbb{C} \setminus \mathbb{Z}$, und hat Pole in $n \in \mathbb{Z}$ mit Residuum $\frac{1}{2\pi i} e^{-\pi xn^2}$. Der Residuensatz liefert

$$\sum_{n=-N}^N e^{-\pi xn^2} = \int_{\partial R} f(t) dt.$$

Sei $t \in M_+$, also $t = N + \frac{1}{2} + i\tau$ mit $-1 \leq \tau \leq 1$. Es gilt $|e^{2\pi it} - 1| = 1 + e^{-2\pi\tau} \geq 1$ und $|e^{-\pi xt^2}| = e^{-\pi x((N+\frac{1}{2})^2 - \tau^2)} < e^{-\pi x N^2}$. Hieraus folgt $\lim_{N \rightarrow \infty} \int_{M_+} f(t) dt = 0$, und analog folgt die entsprechende Aussage für M_- . Einfache Abschätzungen zeigen die Existenz der Grenzwerte $\lim_{N \rightarrow \infty} \int_{L_{\pm}} f(t) dt$. Es folgt

$$\theta(x) = \lim_{N \rightarrow \infty} \int_{L_+} f(t) dt + \lim_{N \rightarrow \infty} \int_{L_-} f(t) dt.$$

Sei $t \in L_+$. Dann gilt $|e^{2\pi it}| < 1$, also $\frac{1}{e^{2\pi it}-1} = -\sum_{n=0}^{\infty} e^{2\pi int}$. Daher gilt

$$\begin{aligned} \int_{L_+} f(t) dt &= \int_{L_+} \frac{e^{-\pi x t^2}}{e^{2\pi it}-1} dt \\ &= -\int_{L_+} \sum_{n=0}^{\infty} e^{-\pi x t^2 + 2\pi int} dt \\ &= -\sum_{n=0}^{\infty} \int_{L_+} e^{-\pi x t^2 + 2\pi int} dt \\ &= -\sum_{n=0}^{\infty} e^{-\frac{\pi n^2}{x}} \int_{L_+} e^{-\pi x (t - \frac{ni}{x})^2} dt, \end{aligned}$$

wobei Summation und Integration wegen gleichmäßiger Konvergenz vertauscht werden dürfen. Das Integral \int_{L_+} für $N \rightarrow \infty$ bezeichnen wir mit $\int_{-\infty+i}^{\infty+i}$. In obiger Gleichung darf Summation und der Grenzübergang $N \rightarrow \infty$ vertauscht werden. Es folgt

$$\begin{aligned} \lim_{N \rightarrow \infty} \int_{L_+} f(t) dt &= \sum_{n=0}^{\infty} e^{-\frac{\pi n^2}{x}} \int_{-\infty+i}^{\infty+i} e^{-\pi x (t - \frac{ni}{x})^2} dt \\ &= \sum_{n=0}^{\infty} e^{-\frac{\pi n^2}{x}} \int_{-\infty+i(1-\frac{ni}{x})}^{\infty+i(1-\frac{ni}{x})} e^{-\pi x w^2} dw, \end{aligned}$$

wobei wir im letzten Schritt die Substitution $w = t - \frac{ni}{x}$ gemacht haben. Der Cauchysche Integralsatz und eine einfache Abschätzung zeigen, dass wir den Integrationsweg im letzten Integral um $-i(1 - \frac{n}{x})$ verschieben dürfen. Es gilt also

$$\lim_{N \rightarrow \infty} \int_{L_+} f(t) dt = \sum_{n=0}^{\infty} e^{-\frac{\pi n^2}{x}} \int_{-\infty}^{\infty} e^{-\pi x w^2} dt.$$

Mittels der Substitution $u = \pi x w^2$ berechnen wir das Integral, und beachten, dass nach Satz 8.10 $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ gilt:

$$\int_{-\infty}^{\infty} e^{-\pi x w^2} dt = 2 \int_0^{\infty} e^{-\pi x w^2} dt = 2 \int_0^{\infty} \frac{e^{-u} u^{-\frac{1}{2}}}{2\sqrt{\pi x}} du = \frac{1}{\sqrt{\pi x}} \Gamma(\frac{1}{2}) = \frac{1}{\sqrt{x}}.$$

Hieraus folgt

$$\lim_{N \rightarrow \infty} \int_{L_+} f(t) dt = \frac{1}{\sqrt{x}} \sum_{n=0}^{\infty} e^{-\frac{\pi n^2}{x}}.$$

Ähnlich verfahren wir mit L_- , und erhalten

$$\lim_{N \rightarrow \infty} \int_{L_-} f(t) dt = \frac{1}{\sqrt{x}} \sum_{n=-1}^{-\infty} e^{-\frac{\pi n^2}{x}},$$

und die Behauptung folgt wegen

$$\theta(x) = \lim_{N \rightarrow \infty} \int_{L_+} f(t) dt + \lim_{N \rightarrow \infty} \int_{L_-} f(t) dt = \frac{1}{\sqrt{x}} \sum_{n=-\infty}^{\infty} e^{-\frac{\pi n^2}{x}} = \frac{1}{\sqrt{x}} \theta\left(\frac{1}{x}\right).$$

□

Wir wissen bereits, dass die Zetafunktion $\zeta(s)$ im Streifen $0 < \mathcal{R}(s) < 1$ holomorph ist. Die folgende Aussage ist die Funktionalgleichung der Zetafunktion, und wird uns unter anderem die holomorphe Fortsetzbarkeit von $\zeta(s)$ nach $\mathbb{C} \setminus \{1\}$ liefern.

Lemma 9.3. Für $0 < \mathcal{R}(s) < 1$ setze $\xi(s) = s(s-1)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$. Dann hat $\xi(s)$ eine holomorphe Fortsetzung nach \mathbb{C} , und es gilt $\xi(s) = \xi(1-s)$.

Beweis. In $\Gamma(\frac{s}{2}) = \int_0^\infty e^{-t} t^{\frac{s}{2}-1} dt$ setze $t = \pi n^2 x$. Dies ergibt

$$\Gamma\left(\frac{s}{2}\right) = \pi^{\frac{s}{2}} n^s \int_0^\infty e^{-\pi x n^2} x^{\frac{s}{2}-1} dx.$$

Für $s > 1$ folgt daraus

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \int_0^\infty \left(\sum_{n=1}^\infty e^{-\pi x n^2} \right) x^{\frac{s}{2}-1} dx = \int_0^\infty \omega(x) x^{\frac{s}{2}-1} dx$$

mit $\omega(x) = \sum_{n=1}^\infty e^{-\pi x n^2} = \frac{\theta(x)-1}{2}$. Aus Satz 9.2 folgt $\omega\left(\frac{1}{x}\right) = -\frac{1}{2} + \frac{1}{2}\sqrt{x} + \sqrt{x}\omega(x)$. Dies verwenden wir in der folgenden Rechnung:

$$\begin{aligned} \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) &= \int_0^1 \omega(x) x^{\frac{s}{2}-1} dx + \int_1^\infty \omega(x) x^{\frac{s}{2}-1} dx \\ &= \int_1^\infty \omega\left(\frac{1}{y}\right) y^{1-\frac{s}{2}} \frac{dy}{y^2} + \int_1^\infty \omega(x) x^{\frac{s}{2}-1} dx \\ &= \int_1^\infty \left(-\frac{1}{2} + \frac{1}{2}y^{\frac{1}{2}} + y^{\frac{1}{2}}\omega(y)\right) y^{-\frac{s}{2}-1} dy + \int_1^\infty \omega(x) x^{\frac{s}{2}-1} dx \\ &= -\frac{1}{s} - \frac{1}{1-s} + \int_1^\infty \omega(x) (x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1}) dx. \end{aligned}$$

Es gilt also

$$\xi(s) = 1 + s(s-1) \int_1^\infty \omega(x) (x^{-\frac{s}{2}-\frac{1}{2}} + x^{\frac{s}{2}-1}) dx.$$

Wegen $\omega(x) \leq \sum_{n=1}^\infty e^{-\pi xn} = \frac{e^{-\pi x}}{1-e^{-\pi x}} \leq \frac{e^{-\pi x}}{1-e^{-\pi}}$ für $x \geq 1$ konvergiert das Integral gleichmäßig auf allen kompakten Teilmengen von \mathbb{C} , und stellt daher eine ganze Funktion dar. Insbesondere hat $\xi(s)$ eine holomorphe Fortsetzung nach \mathbb{C} , und es gilt $\xi(s) = \xi(1-s)$, da die Darstellung von $\xi(s)$ invariant unter der Ersetzung von s mit $1-s$ ist. \square

Als unmittelbare Folgerung notieren wir

Satz 9.4. $\zeta(s)$ lässt sich holomorph nach $\mathbb{C} \setminus \{1\}$ fortsetzen, hat eine einfache "triviale Nullstellen" in $-2, -4, -6, \dots$. Die restlichen Nullstellen liegen im Parallelstreifen $0 < \mathcal{R}(s) < 1$, und liegen darin symmetrisch zur Achse $\mathcal{R}(s) = \frac{1}{2}$.

Beweis. Wir benutzen, dass $\Gamma(\frac{s}{2})$ keine Nullstellen hat, aber Pole erster Ordnung in $0, -2, -4, \dots$ besitzt. Da $\zeta(s)$ nach ??? keine Nullstellen für $\mathcal{R}(s) \geq 1$ besitzt, gilt das gleiche auch für $\xi(s)$, wobei wir noch verwenden, dass $\zeta(s)$ einen Pol in 1 besitzt. Wegen $\xi(s) = \xi(1-s)$ hat daher $\xi(s)$ keine Nullstellen in $\mathcal{R}(s) \leq 0$. Für $\mathcal{R}(s) \leq 0$ hat $\zeta(s)$ genau dort eine Nullstelle, wo $s\Gamma(\frac{s}{2})$ einen Pol hat, mit Polordnung gleich der Nullstellenordnung von $\zeta(s)$, also in $-2, -4, -6, \dots$. Die Aussage über die restlichen Nullstellen folgt nun aus $\xi(s) = \xi(1-s)$ und der folgenden Überlegung: $\xi(x)$ ist reellwertig für $x > 1$, daher hat die Potenzreihenentwicklung von $\xi(s)$ um $x = 2$ reelle Koeffizienten, und somit gilt $\xi(\bar{s}) = \overline{\xi(s)}$. \square

Häufig verwendet man die Funktionalgleichung, um Aussagen über die Zetafunktion für $\mathcal{R}(s) \leq \frac{1}{2}$ zurückzuführen auf Aussagen für $\mathcal{R}(s) \geq \frac{1}{2}$. Für diese Zwecke ist die folgende Form der Funktionalgleichung sehr nützlich, die man aus $\xi(s) = \xi(1-s)$ gewinnt unter Verwendung der Formeln von Euler 8.10 und Legendre 8.12:

Satz 9.5. Es gilt $\zeta(1-s) = 2(2\pi)^{-s} \cos \frac{\pi s}{2} \Gamma(s) \zeta(s)$.

Im folgenden wollen wir noch einige einfache Aussagen über die nicht trivialen Nullstellen von $\zeta(s)$ beweisen. Hierzu braucht man obere Abschätzungen von $\zeta(\sigma + it)$ bei festem σ für große t . Üblicherweise gewinnt man sie mittels obiger Funktionalgleichung und der Sterlingformel für die Gammafunktion. Da wir die Stirlingformel hier nicht bewiesen haben, und auch deren Anwendung etwas technisch ist, gehen wir hier anders vor.

Lemma 9.6. Sei $m \in \mathbb{N}$. Dann gibt es ein Polynom $P_m(z)$ vom Grad $\leq m-1$, und eine Funktion $f_m : \mathbb{R} \rightarrow \mathbb{R}$ mit folgenden Eigenschaften: (a) $f_m(x)$ ist periodisch mit Periode 1, (b) $\int_0^1 f_m(x) dx = 0$, (c) $f_1(x) = \frac{1}{2} + [x] - x$, (d) für $m \geq 2$ ist $f_m(x)$ stetig, und

$$\zeta(s) = \frac{1}{s-1} + P_m(s) + s(s+1)\dots(s+m-1) \int_1^\infty \frac{f_m(x)}{x^{s+m}} dx$$

für alle $s \in \mathbb{C}$ mit $\Re(s) > 1 - m$.

Beweis. Setze $f_1(x) = \frac{1}{2} + [x] - x$. Aus $\int_1^\infty \frac{dx}{x^{s+1}} = \frac{1}{s}$ und dem Beweis von ??? folgt die Behauptung für $m = 1$ mit $P_1(X) = \frac{1}{2}$. Der allgemeine Fall folgt durch vollständige Induktion. Die Behauptung gelte für m . Sei $f_{m+1}(x)$ eine Stammfunktion von $f_m(x)$. Wegen (a) und (b) für $f_m(x)$ folgt die Bedingung (a) für $f_{m+1}(x)$. Durch Addition einer geeigneten Konstanten bleibt (a) erhalten, und (b) lässt sich erfüllen. Nach Konstruktion ist (d) erfüllt. Die behauptete Identität folgt dann mittels partieller Integration, da

$$\begin{aligned} \int_1^\infty \frac{f_m(x)}{x^{s+m}} dx &= \left[\frac{f_{m+1}(x)}{x^{s+m}} \right]_1^\infty + (s+m) \int_1^\infty \frac{f_{m+1}(x)}{x^{s+m+1}} dx \\ &= -f_{m+1}(1) + (s+m) \int_1^\infty \frac{f_{m+1}(x)}{x^{s+m+1}} dx. \end{aligned}$$

Dabei beachte man, dass das Integral im angegebenen Bereich konvergiert, da der Zähler wegen Stetigkeit und Periodizität beschränkt ist. \square

Eine direkte Folgerung ist

Korollar 9.7. Sei $n \in \mathbb{N}_0$, und $\delta > 0$. Dann gibt es $r, C > 0$, so dass

$$|\zeta(s)| \leq C|s|^{n+1}$$

gilt für alle s mit $\Re(s) \geq -n + \delta$ und $|s| > r$.

Beweis. Wir verwenden den Satz mit $m = n + 1$. Sei $|f_m(x)| \leq K$ für alle x . Die Behauptung folgt dann aus

$$\left| \int_1^\infty \frac{f_m(x)}{x^{s+m}} dx \right| \leq \int_1^\infty \frac{K}{x^{1+\delta}} dx = \frac{K}{\delta}.$$

\square

Aufgaben. 1. Zeige, dass $\zeta(x)$ für $0 < x < 1$ keine Nullstellen hat. (Hinweis: Zeige und benutze $(1 - 2^{1-x})\zeta(x) = 1 - \frac{1}{2^x} + \frac{1}{3^x} - \dots$ für $x > 0$.)

10 Das große Sieb der Zahlentheorie

Als Motivation betrachten wir das Sieb des Erathostenes zur Anzahlbestimmung der Primzahlen bis zu einer Größe N . Dabei setzen wir voraus, dass die Primzahlen bereits bis \sqrt{N} bekannt sind. Sei A die Menge der Primzahlen a mit $\sqrt{N} < a \leq N$. Für $p \leq \sqrt{N}$ ist kein $a \in A$ durch p teilbar, also enthält A höchstens $p-1$ modulo p verschiedene Elemente. Mit Siebmethoden versucht man nun diese Information zu benutzen um die Mächtigkeit von A nach oben abzuschätzen. Eine sehr starke Methode ist das große Sieb.

Definition. Sei $A \subseteq \mathbb{Z}$ und $p \in \mathbb{P}$. Die Anzahl der modulo p verschiedenen Restklassen der Elemente in A bezeichnen wir mit $p(A)$.

In obigem Beispiel gilt also $p(A) \leq p-1$ für alle $p \leq \sqrt{N}$.

Satz 10.1. Sei $\emptyset \neq A \subset \mathbb{Z}$ eine endliche Menge und $Q \geq 1$. Für $p \in \mathbb{P}$ sei $v(p) \leq p$ mit $p(A) \leq v(p)$.

Setze

$$L(Q) = \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \prod_{p|q} \frac{p - v(p)}{v(p)}.$$

Ferner sei $N = \max(A) - \min(A) + 1$. Dann gilt

$$|A| \leq \frac{\pi N + Q^2}{L}.$$

Bemerkung. Im Satz gilt $v(p) \neq 0$, denn da A nicht leer ist, kommt mindestens eine Restklasse modulo p vor, also $p(A) \geq 1$.

Mit erheblichem höherem Aufwand lässt sich die obige Abschätzung verbessern, der Zähler $\pi N + Q^2$ kann durch $N - 1 + Q^2$ ersetzt werden, siehe z.B. ???.

Der Beweis des Satzes verwendet die endliche Fourierreihe $S(t) = \sum_{a \in A} e^{2\pi i t a}$. Für die Zwischenschritte betrachten wir allerdings allgemeinere Summen $\sum_{a \in A} c_a e^{2\pi i t a}$. Wir beginnen mit einigen Vorbereitungen.

Lemma 10.2 (Gallagher). Sei $f : [0, 1] \rightarrow \mathbb{C}$ stetig differenzierbar. Dann gilt

$$\left| f\left(\frac{1}{2}\right) \right| \leq \int_0^1 (|f(t)| + \frac{1}{2}|f'(t)|) dt.$$

Beweis. Mittels partieller Integration verifiziert man

$$f(x) = \int_0^1 f(t) dt + \int_0^x t \cdot f'(t) dt + \int_x^1 (t-1) f'(t) dt,$$

und daraus folgt die Behauptung für $x = \frac{1}{2}$, da der Faktor vor $f'(t)$ stets zwischen 0 und $\frac{1}{2}$ liegt. \square

Durch Variablentransformation erhalten wir daraus

Korollar 10.3. *Sei $x \in \mathbb{R}$, $\delta > 0$, und $f : [x - \frac{\delta}{2}, x + \frac{\delta}{2}] \rightarrow \mathbb{C}$ stetig differenzierbar. Dann gilt*

$$|f(x)| \leq \int_{x-\frac{\delta}{2}}^{x+\frac{\delta}{2}} \left(\frac{1}{\delta} |f(t)| + \frac{1}{2} |f'(t)| \right) dt.$$

Aus Gründen der Vollständigkeit beweisen wir noch schnell die wohlbekannte Ungleichung von Cauchy-Schwarz.

Lemma 10.4. (a) *Seien $f, g : [0, 1] \rightarrow \mathbb{C}$ stetig. Dann gilt*

$$\left(\int_0^1 |f(t)g(t)| dt \right)^2 \leq \int_0^1 |f(t)|^2 dt \int_0^1 |g(t)|^2 dt.$$

(b) *Seien $a_i, b_i \in \mathbb{C}$ mit $i = 1, 2, \dots, n$. Dann gilt*

$$\left(\sum_i |a_i b_i| \right)^2 \leq \sum_i |a_i|^2 \sum_i |b_i|^2.$$

Beweis. Wir dürfen $f(t) \geq 0$, $g(t) \geq 0$ für alle $t \in [0, 1]$ annehmen. Für alle $z \in \mathbb{R}$ ist $\int_0^1 (f(t) - zg(t))^2 dt \geq 0$, also

$$\int_0^1 f(t)^2 dt + z^2 \int_0^1 g(t)^2 dt \geq 2z \int_0^1 f(t)g(t) dt.$$

Ist $g(t) = 0$ für alle t , dann ist nichts zu zeigen. Sei also g nicht identisch 0. Setze $z = \int_0^1 f(t)g(t) dt / \int_0^1 g(t)^2 dt$, die Behauptung (a) folgt. Analog zeigt man (b), indem man Integration durch Summation ersetzt. \square

Im folgenden betrachten wir Fourierpolynome

$$S(t) = \sum_{n=M+1}^{M+N} c_n e^{2\pi i t n}$$

mit $M \in \mathbb{Z}$, $N \in \mathbb{N}$, $c_n \in \mathbb{C}$. Offenbar hat $S(t)$ die Periode 1. Wegen

$$\int_0^1 e^{2\pi i t(n-m)} dt = \begin{cases} 1 & \text{falls } n = m \\ 0 & \text{sonst} \end{cases}$$

für $n, m \in \mathbb{Z}$ gilt die im folgenden wichtige Beziehung

$$\sum_{n=M+1}^{M+N} |c_n|^2 = \int_0^1 |S(t)|^2 dt.$$

Definition. Für $\alpha \in \mathbb{R}$ sei $\|\alpha\|$ der Abstand von α zur nächsten ganzen Zahl.

Satz 10.5. Sei $\delta > 0$, und $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{R}$ gegeben mit $\|\alpha_u - \alpha_v\| \geq \delta$ für alle $1 \leq u < v \leq r$. Dann gilt

$$\sum_{j=1}^r |S(\alpha_j)|^2 \leq (\pi N + \frac{1}{\delta}) \sum_{n=M+1}^{M+N} |c_n|^2.$$

Beweis. Sei $M_0 \in \mathbb{Z}$ beliebig, und setze

$$T(t) = \sum_{n=M_0+1}^{M_0+N} c_{n-(M-M_0)} e^{2\pi i t n} = e^{2\pi i (M-M_0) t} S(t).$$

Wegen $|S(t)| = |T(t)|$ sehen wir, dass wir zum Beweis M beliebig wählen dürfen.

Zunächst sehen wir, dass man $\delta \leq \frac{1}{2}$ annehmen darf. Denn falls $\delta > \frac{1}{2}$, dann gilt $r = 1$ wegen $\|\alpha\| \leq \frac{1}{2}$ für alle $\alpha \in \mathbb{R}$. Aber für $r = 1$ folgt die Behauptung aus der Cauchy-Schwarzschen Ungleichung:

$$|S(\alpha_1)|^2 \leq \sum_{n=M+1}^{M+N} |c_n|^2 \sum_{n=M+1}^{M+N} |e^{2\pi i \alpha_1 n}| = N \sum_{n=M+1}^{M+N} |c_n|^2.$$

Korollar 10.3 mit $f(t) = S(t)^2$ liefert

$$|S(\alpha_j)|^2 \leq \frac{1}{\delta} \int_{\alpha_j - \frac{\delta}{2}}^{\alpha_j + \frac{\delta}{2}} |S(t)|^2 dt + \int_{\alpha_j - \frac{\delta}{2}}^{\alpha_j + \frac{\delta}{2}} |S(t)S'(t)| dt.$$

Sei $\Pi : \mathbb{R} \rightarrow [0, 1)$ die Reduktion modulo \mathbb{Z} , also $\Pi(\alpha) = \alpha - [\alpha]$. Ist $I \subset \mathbb{R}$ ein offenes Intervall der Länge ≤ 1 , dann ist die Einschränkung von Π auf I injektiv. Ferner gilt: Hat die reelle Funktion $f(t)$ die Periode 1, dann ist $\int_I f(t) dt = \int_{\Pi(I)} f(t) dt$. Nach Voraussetzung sind die Mengen $\Pi((\alpha_j - \frac{\delta}{2}, \alpha_j + \frac{\delta}{2})) \subseteq [0, 1)$ paarweise disjunkt. Daher gilt

$$\sum_{j=1}^r |S(\alpha_j)|^2 \leq \frac{1}{\delta} \int_0^1 |S(t)|^2 dt + \int_0^1 |S(t)S'(t)| dt = \frac{1}{\delta} \sum_{n=M+1}^{M+N} |c_n|^2 + \int_0^1 |S(t)S'(t)| dt$$

□

Die Cauchy-Schwarzsche Ungleichung liefert

$$\left(\int_0^1 |S(t)S'(t)| dt \right)^2 \leq \int_0^1 |S(t)|^2 dt \int_0^1 |S'(t)|^2 dt = \sum_{n=M+1}^{M+N} |c_n|^2 \int_0^1 |S'(t)|^2 dt.$$

Wegen $S'(t) = \sum_{n=M+1}^{M+N} 2\pi i n c_n e^{2\pi i n t}$ gilt

$$\int_0^1 |S'(t)|^2 dt = 4\pi^2 \sum_{n=M+1}^{M+N} n^2 |c_n|^2.$$

Wie Anfangs bemerkt, dürfen wir M beliebig wählen. Wir setzen $M = \lfloor -\frac{N}{2} \rfloor$, dann gilt $n^2 \leq \frac{1}{4}N^2$, also

$$\int_0^1 |S'(t)|^2 dt \leq \pi^2 N^2 \sum_{n=M+1}^{M+N} |c_n|^2,$$

und hieraus folgt die Behauptung.

Bemerkung. Mit größerem analytischen Aufwand kann man den Faktor $\pi N + \frac{1}{\delta}$ zu $N - 1 + \frac{1}{\delta}$ verkleinern, siehe???,???

Im folgenden bezeichnen wir den größten gemeinsamen Teiler der ganzen Zahlen a und b mit (a, b) . Wir notieren ein wichtiges

Korollar 10.6. Sei $Q \geq 1$ und $S(t) = \sum_{n=M+1}^{M+N} c_n e^{2\pi i n t}$ wie oben. Dann gilt

$$\sum_{\substack{1 \leq j \leq q \leq Q \\ (j, q) = 1}} |S(\frac{j}{q})|^2 \leq (\pi N + Q^2) \sum_{n=M+1}^{M+N} |c_n|^2.$$

Beweis. Sei $\{\alpha_1, \alpha_2, \dots, \alpha_r\}$ die Menge der gekürzten Brüche $\frac{j}{q}$ mit $1 \leq j \leq q \leq Q$. Seien $\frac{j}{q} \neq \frac{j'}{q'}$ zwei solche Brüche. Wegen

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

folgt die Behauptung mit $\delta = \frac{1}{Q^2}$. □

Wir beginnen nun mit der Betrachtung modulo Primzahlen. Sei $\emptyset \neq A \subset \mathbb{Z}$ eine endliche Teilmenge, und für $n \in A$ sei $c_n \in \mathbb{C}$. Setze $S(t) = \sum_{n \in A} c_n e^{2\pi i n t}$. Sei $p(A) \leq v(p) \leq p$ beliebig. Definiere die multiplikative Funktion g durch

$$g(q) = \begin{cases} \prod_{p|q} \frac{p-v(p)}{v(p)} & \text{falls } q \text{ quadratfrei} \\ 0 & \text{sonst.} \end{cases}$$

Satz 10.7. *Mit den Bezeichnungen von oben gilt für alle $q \in \mathbb{Q}$*

$$\sum_{\substack{j=1 \\ (j,q)=1}}^q |S(\frac{j}{q})|^2 \geq g(q) |\sum_n c_n|^2.$$

Beweis. Wegen $\sum_n c_n = S(0)$ ist

$$g(q) |S(0)|^2 \leq \sum_{\substack{j=1 \\ (j,q)=1}}^q |S(\frac{j}{q})|^2 \quad (2)$$

zu zeigen. Für $\beta \in \mathbb{R}$ setze $\tilde{c}_n = c_n e^{2\pi i \beta n}$ und $\tilde{S}(t) = \sum_n \tilde{c}_n e^{2\pi i t n} = S(t + \beta)$. Ungleichung (2) für \tilde{S} statt S schreibt sich dann als

$$g(q) |S(\beta)|^2 \leq \sum_{\substack{j=1 \\ (j,q)=1}}^q |S(\frac{j}{q} + \beta)|^2. \quad (3)$$

Gilt also (2) für festes q und alle S , dann gilt auch (3) für alle S und alle $\beta \in \mathbb{R}$.

Seien $q, q' \in \mathbb{N}$ mit $(q, q') = 1$, und (2) gelte für q und q' . Wir zeigen, dass (2) dann auch für qq' gilt.

Sei $1 \leq j \leq q$, $(j, q) = 1$, $1 \leq j' \leq q'$, $(j', q') = 1$. Man rechnet sofort nach, dass die Zahlen $jq' + j'q$ für verschiedene Paare (j, j') inkongruent modulo qq' sind. Ferner gilt $(jq' + j'q, qq') = 1$. Wegen $\varphi(q)\varphi(q') = \varphi(qq')$ durchlaufen die Zahlen $jq' + j'q$ modulo qq' genau die zu qq' teilerfremden c mit $1 \leq c \leq qq'$. Zusammen mit (3) mit $\beta = \frac{j}{q}$ und wegen $S(t) = S(t + 1)$ folgt

$$\begin{aligned} \sum_{\substack{c=1 \\ (c,qq')=1}}^{qq'} |S(\frac{c}{qq'})|^2 &= \sum_{\substack{j=1 \\ (j,q)=1}}^q \sum_{\substack{j'=1 \\ (j',q')=1}}^{q'} |S(\frac{j}{q} + \frac{j'}{q'})|^2 \\ &\geq g(q') \sum_{\substack{j=1 \\ (j,q)=1}}^q |S(\frac{j}{q})|^2 \\ &\geq g(q')g(q) |S(0)|^2 \\ &= g(qq') |S(0)|^2. \end{aligned}$$

Daher müssen wir (2) nur noch für Primpotenzen nachweisen. Wegen $g(q) = 0$ für nicht quadratfreie q sei also $q = p$ eine Primzahl. Sei $\zeta = e^{\frac{2\pi i}{p}}$. Wegen

$$\sum_{j=0}^{p-1} \zeta^{ju} = \begin{cases} p & p \text{ teilt } u \\ 0 & \text{sonst} \end{cases}$$

und $S(\frac{j}{p}) = \sum_n c_n \zeta^{jn}$ gilt

$$\begin{aligned}
\sum_{j=0}^{p-1} |S(\frac{j}{p})|^2 &= \sum_{j=0}^{p-1} \left(\sum_m c_m \zeta^{jm} \right) \left(\sum_n \bar{c}_m \zeta^{-jn} \right) \\
&= \sum_{m,n} c_m \bar{c}_n \sum_{j=0}^{p-1} \zeta^{j(m-n)} \\
&= p \sum_{\substack{m,n \\ p|m-n}} c_m \bar{c}_n \\
&= p \sum_{k=0}^{p-1} \sum_{\substack{m,n \\ p|m-k \\ p|n-k}} c_m \bar{c}_n \\
&= p \sum_{k=0}^{p-1} \sum_{\substack{m \\ p|m-k}} c_m \sum_{\substack{n \\ p|n-k}} \bar{c}_m \\
&= p \sum_{k=0}^{p-1} |C_k|^2 \text{ mit}
\end{aligned}$$

$$C_k = \sum_{\substack{n \\ p|n-k}} c_n.$$

Höchstens $v(p)$ der Terme C_k sind von 0 verschieden, denn ist $C_k \neq 0$, dann gibt es ein $n \in A$ mit $p|n-k$. Die Cauchy-Schwarzsche Ungleichung, summiert über die höchstens $v(p)$ Indizes k mit $C_k \neq 0$, liefert

$$\begin{aligned}
\sum_k |C_k|^2 \cdot v(p) &= \sum_k |C_k|^2 \cdot \sum_k 1^2 \\
&\geq \left(\sum_k |C_k| \cdot 1 \right)^2 \\
&\geq \left| \sum_k C_k \right|^2 \\
&= \left| \sum_n c_n \right|^2,
\end{aligned}$$

also

$$\begin{aligned} \sum_{j=1}^{p-1} |S(\frac{j}{p})|^2 &= \sum_{j=0}^{p-1} |S(\frac{j}{p})|^2 - |\sum_n c_n|^2 \\ &\geq \frac{p}{v(p)} |\sum_n c_n|^2 - |\sum_n c_n|^2 \\ &= \frac{p - v(p)}{v(p)} |\sum_n c_n|^2, \end{aligned}$$

was zu zeigen war. \square

Damit folgt nun sofort der Beweis von Satz 10.1. Sei $A \subset \mathbb{Z}$ gegeben mit $N = \max A - \min A + 1$. Dann gilt $A \subseteq [M + 1, M + N]$ mit $M = \min(A) + 1$. Setze $S(t) = \sum_{n \in A} e^{2\pi i t n}$. Satz 10.7 liefert für $q \leq Q$

$$g(q)|A|^2 \leq \sum_{\substack{j=1 \\ (j,q)=1}}^q |S(\frac{j}{q})|^2.$$

Dies summieren wir über alle $q \leq Q$. Korollar 10.6 liefert dann

$$L(Q) \cdot |A|^2 \leq \sum_{\substack{1 \leq j \leq q \leq Q \\ (j,q)=1}} |S(\frac{j}{q})|^2 \leq (\pi N + Q^2) \cdot |A|,$$

und daraus folgt die Behauptung.

Aufgaben. 1. Sei $c > 0$, so dass für alle stetig differenzierbaren Funktionen $f : [0, 1] \rightarrow \mathbb{C}$ die Ungleichung $|f(\frac{1}{2})| \leq \int_0^1 (|f(t)| + c|f'(t)|) dt$ gilt. Zeige $c \geq \frac{1}{2}$.

11 Zwei Anwendungen des großen Siebs

Das große Sieb ist vor allem dazu geeignet, arithmetische Aussagen über kleine Intervalle ganzer Zahlen zu machen. Hierzu wollen wir zwei Beispiele betrachten. Zuerst betrachten wir die Anzahl der Primzahlen in kurzen Intervallen, und danach beweisen wir eine obere Schranke für die Anzahl von Primzahlzwillingen.

Das Hauptproblem ist dabei, gute untere Abschätzungen für $L(Q)$ zu finden. Sei A eine Menge von Primzahlen $a > Q$. Dann gilt natürlich $p(A) \leq$

$v(p) = p - 1$ für $p \leq Q$, da kein $a \in A$ durch $p \leq Q$ teilbar ist. In diesem Fall ist also

$$L(Q) \geq \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \prod_{p|q} \frac{1}{p-1}.$$

In einer weiteren Anwendung sei A eine Menge, so dass für $a \in A$ sowohl a als auch $a+2$ Primzahlen sind, und $a > Q$ gilt. Offenbar gilt dann $2(A) \leq 1$ und $p(A) \leq p - 2$ für $3 \leq p \leq Q$.

Lemma 11.1. *Für $Q \geq 1$ gilt*

$$L(Q) \geq \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \prod_{p|q} \frac{1}{p-1} \geq \log Q.$$

Beweis. Für quadratfreie q gilt $q = \prod_{p|q} p$. Es folgt

$$\begin{aligned} \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \prod_{p|q} \frac{1}{p-1} &= \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \frac{1}{q} \prod_{p|q} \frac{1}{1 - \frac{1}{p}} \\ &= \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \frac{1}{q} \prod_{p|q} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) \\ &= \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \frac{1}{q} \sum_{u \in M(q)} \frac{1}{u}, \end{aligned}$$

wo $M(q)$ die Menge der natürlichen Zahlen bezeichnet, deren Primfaktoren schon in q vorkommen. Sei $n \leq Q$, und $\prod p_i^{\alpha_i}$ die Primfaktorzerlegung von n . Setze $q = \prod p_i$, und $u = \prod p_i^{\alpha_i - 1} \in M(q)$. Wegen $n = qu$ und $q \leq Q$ quadratfrei kommt $\frac{1}{n}$ in obiger Summe vor. Daher gilt

$$\sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \frac{1}{q} \sum_{u \in M(q)} \frac{1}{u} \geq \sum_{n \leq Q} \frac{1}{n} \geq \log Q,$$

und die Behauptung folgt. □

Hieraus erhalten wir nun

Satz 11.2. *Sei $M \in \mathbb{N}$, $2 \leq N \in \mathbb{N}$. Dann gibt es im Intervall $[M+1, M+N]$ nicht mehr als $(2\pi + 3) \frac{N}{\log N}$ Primzahlen.*

Beweis. Setze $Q = \sqrt{N}$. Sei A die Menge der Primzahlen in $[M+1, M+N]$. Wir betrachten zuerst den Fall $M \geq Q$. Dann ist A disjunkt zur Menge der Primzahlen $\leq Q$, es gilt also $p(A) \leq p-1$ für alle $p \leq Q$. Obiges Lemma, zusammen mit Satz 10.1, liefert daher

$$|A| \leq \frac{\pi N + Q^2}{L(Q)} \leq \frac{\pi N + Q^2}{\log Q} = (2\pi + 2) \frac{N}{\log N} \leq (2\pi + 3) \frac{N}{\log N}.$$

Sei nun $M < Q = \sqrt{N}$. Die Überlegung von gerade gezeigt

$$\pi(M+N) - \pi(Q) \leq (2\pi + 2) \frac{N}{\log N}.$$

Wegen $M < Q$ und $\pi(Q) \leq Q$ gilt weiter

$$|A| \leq \pi(M+N) = \pi(M+N) - \pi(Q) + \pi(Q) \leq (2\pi + 2) \frac{N}{\log N} + Q.$$

Man verifiziert schnell $\sqrt{N} \geq \log N$ für $N > 1$, also $Q = \sqrt{N} \leq \frac{N}{\log N}$, und die Behauptung folgt. \square

Unsere zweite Anwendung betrifft die Primzahlzwillinge $(a, a+2)$ mit $a, a+2 \in \mathbb{P}$. Für $Q \geq 1$ sei $v(p) = p-2$ für $3 \leq p \leq Q$, und $v(2) = 1$. Mit dem Kroneckerdelta können wir das kompakt als $v(p) = p-2 + \delta_{2,p}$ schreiben. Wir beweisen ein Analogon zu obigem Lemma.

Lemma 11.3. *Für $Q \geq 1$ gilt*

$$L(Q) = \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \prod_{p|q} \frac{2 - \delta_{2,p}}{p - 2 + \delta_{2,p}} \geq \frac{(\log Q)^2}{4}.$$

Beweis. Sei $\lambda'(n)$ die Anzahl der ungeraden Primfaktoren (mit Vielfachheit) von n ist. Natürlich gilt $2^{\lambda'(p)} = 2 - \delta_{2,p}$. Ferner ist die Funktion $2^{\lambda'(n)}$

vollständig multiplikativ. Analog wie oben erhalten wir

$$\begin{aligned}
L(Q) &= \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \prod_{p|q} \frac{2^{\lambda'(p)}}{p - 2^{\lambda'(p)}} \\
&= \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \frac{2^{\lambda'(q)}}{q} \prod_{p|q} \frac{1}{1 - \frac{2^{\lambda'(p)}}{p}} \\
&= \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \frac{2^{\lambda'(q)}}{q} \prod_{p|q} \sum_{k=1}^{\infty} \frac{2^{\lambda'(p^k)}}{p^k} \\
&= \sum_{\substack{q \leq Q \\ q \text{ quadratfrei}}} \sum_{u \in M(q)} \frac{2^{\lambda'(qu)}}{qu}.
\end{aligned}$$

Schreibt man wieder jedes $n \leq Q$ in der Form $n = qu$ wie oben, so sehen wir

$$L(Q) \geq \sum_{n \leq Q} \frac{2^{\lambda'(n)}}{n}.$$

Sei $n = 2^\alpha \prod p_i^{\alpha_i}$ die Primfaktorzerlegung von n mit p_i ungerade. Sei $\tau'(n)$ die Anzahl der ungeraden Teiler von n . Für $\alpha \in \mathbb{N}$ gilt $1 + \alpha \leq 2^\alpha$, also

$$\tau'(n) = \prod (1 + \alpha_i) \leq \prod 2^{\alpha_i} = 2^{\lambda'(n)}.$$

Daher gilt

$$L(Q) \geq \sum_{n \leq Q} \frac{\tau'(n)}{n}.$$

In der folgenden Rechnung verwenden wir die Trivialität, dass $\tau'(n)$ gleich

der Anzahl aller Paare $a, b \in \mathbb{N}$ mit $(2a - 1)b = n$ ist. Wir erhalten

$$\begin{aligned}
L(Q) &\geq \sum_{n \leq Q} \frac{\tau'(n)}{n} \\
&= \sum_{n \leq Q} \sum_{\substack{a,b \\ (2a-1)b=n}} \frac{1}{(2a-1)b} \\
&= \sum_{\substack{a,b \\ (2a-1)b \leq Q}} \frac{1}{(2a-1)b} \\
&= \sum_{a \leq \frac{Q+1}{2}} \frac{1}{2a-1} \sum_{b \leq \frac{Q}{2a-1}} \\
&\geq \sum_{a \leq \frac{Q+1}{2}} \frac{1}{2a-1} \log \frac{Q}{2a-1} \\
&\geq \int_1^{\frac{Q+1}{2}} \frac{\log Q - \log(2t-1)}{2t-1} dt \\
&= \left[\frac{\log(2t-1) \cdot (2 \log Q - \log(2t-1))}{4} \right]_1^{\frac{Q+1}{2}} \\
&= \frac{(\log Q)^2}{4}
\end{aligned}$$

□

Wir kommen nun zur Anwendung auf Primzahlzwillinge.

Satz 11.4. Für $2 \leq N \in \mathbb{N}$ sei $\pi_2(N)$ die Anzahl der $n \in \mathbb{N}$ mit $n \leq N$, so dass n und $n + 2$ Primzahlen sind. Dann gilt $\pi_2(N) \leq 68 \frac{N}{(\log N)^2}$.

Beweis. Sei A die Menge der $\sqrt{N} \leq n \in \mathbb{N}$, so dass n und $n + 2$ Primzahlen sind. Wir verwenden Satz 10.1 mit $Q = \sqrt{N}$ und $v(p) = p - 2 + \delta_{2,p}$. Zusammen mit dem Lemma erhalten wir

$$\pi_2(N) - \pi_2(\sqrt{N}) \leq 16(1 + \pi) \frac{N}{(\log N)^2}.$$

Natürlich gilt $\pi_2(\sqrt{N}) \leq \sqrt{N}$. Sei $\gamma = \frac{4}{e}$. Man rechnet nach, dass $\gamma N^{\frac{1}{4}} \geq \log N$ gilt für alle reellen $N \geq 1$. Hieraus folgt $\sqrt{N} \leq \gamma^2 \frac{N}{(\log N)^2}$. Die Behauptung folgt nun aus $16(1 + \pi) + \frac{4}{e} = 67.737 \dots < 68$. □

Es ist nicht schwer zu sehen, dass $\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty$, siehe Aufgabe ???. Mit einer Siebmethode, die verschieden vom großen Sieb ist, konnte 19?? bereits Brun eine obere Abschätzung für $\pi_2(N)$ beweisen. Als Folge erhielt er, dass die Summe über die Kehrwerte der Primzahlzwillinge konvergiert. Dies folgt sofort aus folgendem

Korollar 11.5. *Sei A die Menge der $n \in \mathbb{N}$ mit $n, n + 2 \in \mathbb{P}$. Dann gilt*

$$\sum_{n \in A} \frac{1}{n} < \infty.$$

Beweis. Sei $3 \leq N \in \mathbb{N}$. Wegen

$$\begin{aligned} \sum_{\substack{n \in A \\ n \leq N}} \frac{1}{n} &= \sum_{n \leq N} \frac{\pi_2(n) - \pi_2(n-1)}{n} \\ &= \sum_{3 \leq n \leq N} \pi_2(n) \left(\frac{1}{n} - \frac{1}{n+1} \right) + \frac{\pi_2(N)}{N+1} \\ &\leq 68 \sum_{3 \leq n \leq N} \frac{n}{(\log n)^2} \frac{1}{n(n+1)} + 68 \frac{N}{(N+1)(\log N)^2} \\ &< 68 \sum_{3 \leq n \leq N} \frac{1}{n(\log n)^2} + 68 \frac{1}{(\log N)^2} \end{aligned}$$

ist nur die Konvergenz der Reihe $\sum_{n \geq 3} \frac{1}{n(\log n)^2}$ zu zeigen. Aber es gilt

$$\sum_{n=3}^N \frac{1}{n(\log n)^2} \leq \int_2^N \frac{dt}{t(\log t)^2} = \frac{1}{\log 2} - \frac{1}{\log N},$$

und daraus folgt die Behauptung. □

Index

$L(Q)$, 35
 $[x]$, 3
 $\Gamma(z)$, 26
 $\Lambda(n)$, 12
 \mathbb{P} , 2
 \mathcal{A} , 3
 $\mathcal{I}(s)$, 7
 $\mathcal{R}(s)$, 7
 χ , 20
 γ , 28
 $\mu(n)$, 4
 $\pi(x)$, 2
 $\pi_2(x)$, 45
 \star , 3
 $\theta(x)$, 17
 $\theta(z)$, 30
 $\varphi(n)$, 14
 $|$, 3
 ξ , 32
 $\zeta(s)$, 6
 $f \sim g$, 14
 $p(A)$, 35

Literatur

- [dlVP96] C.-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Ann. Soc. Sci. Bruxelles (1896), **20**, 183–256, 281–397.
- [Had96] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. Soc. Math. France (1896), **24**, 199–220.
- [Kor82] J. Korevaar, *On Newman's quick way to the prime number theorem*, Math. Intelligencer (1982), **4**(3), 108–115.
- [New80] D. J. Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly (1980), **87**(9), 693–696.
- [Rie] B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Größe*, Monatsber. Preuss. Akad. Wiss., November 1859, 671–680 ().
- [Zag97] D. Zagier, *Newman's short proof of the prime number theorem*, Amer. Math. Monthly (1997), **104**(8), 705–708.