Dirichlets Primzahlsatz

Benjamin Sambale

10. Februar 2023

Bemerkung 1. Bekanntlich existieren unendlich viele ungerade Primzahlen p, d. h. $p \equiv 1 \pmod 2$. Dirichlet [4] bewies 1837, dass für teilerfremde natürliche Zahlen a, d unendlich viele Primzahlen $p \equiv a \pmod d$ existieren. Sein Beweis benutzt tiefliegende Eigenschaften der Riemannschen ζ-Funktion und man glaubte lange, dass es keinen „elementaren" Beweis (d. h. ohne Funktionentheorie) geben kann. Ein solcher Beweis wurde erst 1949 von Selberg [13] gefunden (siehe auch [2, 15, 17]). Da Selbergs Beweis deutlich länger und technischer ist, verfolgen wir einen analytischen Ansatz, der mit elementaren Eigenschaften des komplexen Logarithmus auskommt (inspiriert von Chapman [1]). Es werden lediglich Kenntnisse der Analysis 1 im Umfang von Forsters Buch [7] benötigt.

Definition 2. Für $s \in \mathbb{R}$ mit $s > 1$ definieren wir die *Riemannsche ζ-Funktion*

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

Bemerkung 3. Wegen

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \le 1 + \frac{1}{2^s} + \frac{1}{2^s} + 4\frac{1}{4^s} + \ldots = \sum_{n=0}^{\infty} 2^{n(1-s)} = \frac{1}{1-2^{1-s}} < \infty$$

konvergiert $\zeta(s)$ für $s > 1$. Für $s = 1$ erhält man hingehen die harmonische Reihe $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$.

Lemma 4. *Für $s > 1$ gilt $\frac{1}{s-1} < \zeta(s) < \frac{s}{s-1}$. Insbesondere ist*

$$\lim_{s \to 1} (s-1)\zeta(s) = 1. \tag{1}$$

Beweis. Für $n \in \mathbb{N}$ gilt $\frac{1}{n+1} < \int_n^{n+1} x^{-n} \mathrm{d}x < \frac{1}{n}$ (Stichwort: Treppenfunktion). Summieren über n ergibt

$$\zeta(s) - 1 = \sum_{n=2}^{\infty} \frac{1}{n^s} < \int_1^{\infty} x^{-s} \mathrm{d}x < \zeta(s).$$

Wir berechnen

$$\int_1^{\infty} x^{-s} \mathrm{d}x = \lim_{n \to \infty} \int_1^{n} x^{-s} \mathrm{d}x = -\lim_{n \to \infty} \frac{x^{-s+1}}{s-1}\Big|_1^n = \frac{1}{s-1}$$

(vgl. [7, Beispiel (20.1)]). Daraus folgt leicht die Behauptung. □

Satz 5. *Sei A eine endliche abelsche Gruppe und $\hat{A} := \mathrm{Hom}(A, \mathbb{C}^\times)$. Dann gilt:*

(i) Durch punktweise Multiplikation ist $\hat{A}$ eine abelsche Gruppe der Ordnung $|A|$, die unter komplexer Konjugation abgeschlossen ist.

(ii) Für $B \le A$ ist die Einschränkungsabbildung $\hat{A} \to \hat{B}$ ein Epimorphismus. Insbesondere besitzt jedes $\lambda \in \hat{B}$ genau $|A : B|$ Fortsetzungen nach A.

(iii) Für $\lambda, \mu \in \hat{A}$ gilt die erste Orthogonalitätsrelation

$$\sum_{a \in A} \lambda(a)\overline{\mu(a)} = \begin{cases} |A| & \text{falls } \lambda = \mu, \\ 0 & \text{falls } \lambda \neq \mu. \end{cases}$$

(iv) Für $a, b \in A$ gilt die zweite Orthogonalitätsrelation

$$\sum_{\lambda \in \hat{A}} \lambda(a)\overline{\lambda(b)} = \begin{cases} |A| & \text{falls } a = b, \\ 0 & \text{falls } a \neq b. \end{cases}$$

Beweis.

(i) Für $\lambda, \mu \in \hat{A}$ ist $\lambda\mu \in \hat{A}$ mit $(\lambda\mu)(a) := \lambda(a)\mu(a)$ für $a \in A$. Offenbar wird $\hat{A}$ auf diese Weise zu einer abelschen Gruppe. Nach dem Hauptsatz über endliche abelsche Gruppen existieren $a_1, \ldots, a_n \in A$ mit $A = \langle a_1 \rangle \oplus \ldots \oplus \langle a_n \rangle$. Sei $d_i := |\langle a_i \rangle|$ für $i = 1, \ldots, n$. Für $\lambda \in \hat{A}$ gilt $\lambda(a_i)^{d_i} = \lambda(a_i^{d_i}) = \lambda(1) = 1$, d. h. $\lambda(a_i)$ ist eine d_i-te Einheitswurzel. Insbesondere gibt es höchstens d_i Möglichkeiten für $\lambda(a_i)$. Da λ durch die Bilder von $a_1, \ldots, a_n$ eindeutig bestimmt ist, folgt $|\hat{A}| \le d_1 \ldots d_n = |A|$. Jedes Element in A lässt sich eindeutig in der Form $a_1^{k_1} \ldots a_n^{k_n}$ mit $0 \le k_i \le d_i - 1$ für $i = 1, \ldots, n$ schreiben. Sei $\zeta_i \in \mathbb{C}$ eine d_i-te Einheitswurzel. Dann definiert

$$\lambda(a_1^{k_1} \ldots a_n^{k_n}) := \zeta_1^{k_1} \ldots \zeta_n^{k_n}$$

einen Homomorphismus $A \to \mathbb{C}^\times$. Unterschiedliche Wahlen der ζ_i definieren verschiedenen λ. Dies zeigt $|\hat{A}| \ge |A|$. Für $\lambda \in \hat{A}$ ist auch $\overline{\lambda} \in \hat{A}$ mit $\overline{\lambda}(a) := \overline{\lambda(a)}$ für $a \in A$.

(ii) Die Einschränkung $\Gamma\colon \hat{A} \to \hat{B}$, $\lambda \mapsto \lambda_{|B}$ ist offenbar ein Homomorphismus. Für $\lambda \in \mathrm{Ker}(\Gamma)$ gilt $B \le \mathrm{Ker}(\lambda)$. Nach dem Homomorphiesatz lässt sich λ als Element von $\widehat{A/B}$ auffassen. Umgekehrt definiert jedes $\hat{\lambda} \in \widehat{A/B}$ durch $a \mapsto \hat{\lambda}(aB)$ ein Element aus $\mathrm{Ker}(\Gamma)$. Aus (i) folgt $|\mathrm{Ker}(\Gamma)| = |\widehat{A/B}| = |A/B|$. Nach dem Homomorphiesatz ist

$$|\Gamma(A)| = |\hat{A} : \mathrm{Ker}(\Gamma)| = \frac{|A|}{|A/B|} = |B| = |\hat{B}|,$$

d. h. Γ surjektiv. Die zweite Aussage folgt, da das Urbild von λ eine Nebenklasse nach $\mathrm{Ker}(\Gamma)$ ist.

(iii) Im Fall $\lambda = \mu$ ist $\lambda(a)\overline{\mu(a)} = |\lambda(a)|^2 = 1$, da $\lambda(a)$ eine Einheitswurzel ist. Wir können daher $\lambda \neq \mu$ annehmen. Dann existiert ein $b \in A$ mit $\lambda(b)\overline{\mu(b)} \neq 1$. Aus

$$\lambda(b)\overline{\mu(b)} \sum_{a \in A} \lambda(a)\overline{\mu(a)} = \sum_{a \in A} \lambda(ab)\overline{\mu(ab)} = \sum_{a \in A} \lambda(a)\overline{\mu(a)}$$

folgt die Behauptung.

(iv) Da die Werte von $\lambda \in \hat{A}$ Einheitswurzeln sind, gilt $\overline{\lambda(a)} = \lambda(a^{-1})$. Wir können daher $b = 1$ annehmen. Für $a = 1$ ist die Behauptung trivial. Sei also $a \neq 1$ und $B := \langle a \rangle$. Nach (ii) gilt

$$\sum_{\lambda \in \hat{A}} \lambda(a) = |A/B| \sum_{\mu \in \hat{B}} \mu(a).$$

Sei $k := |B|$ und $\zeta \in \mathbb{C}^\times$ eine primitive k-te Einheitswurzel. Der Beweis von (i) zeigt

$$\sum_{\mu \in \hat{B}} \mu(a) = 1 + \zeta + \ldots + \zeta^{k-1} = \frac{1 - \zeta^k}{1 - \zeta} = 0. \qquad \square$$

Definition 6. Im Folgenden sei stets $d \geq 2$ eine natürliche Zahl. Eine Funktion $\chi\colon \mathbb{Z} \to \mathbb{C}$ heißt *Dirichlet-Charakter* modulo d, falls für alle $a, b \in \mathbb{Z}$ gilt

- $\chi(a) = 0 \iff \mathrm{ggT}(a, d) > 1$,
- $\chi(ab) = \chi(a)\chi(b)$,
- $\chi(a + d) = \chi(a)$.

Die Menge der Dirichlet-Charaktere modulo d sei Ψ_d. Die zu χ gehörige *L-Reihe* ist durch

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

für $s \in \mathbb{R}$ mit $s > 1$ definiert.

Bemerkung 7.

(i) Sei $A := (\mathbb{Z}/d\mathbb{Z})^\times$. Durch Einschränkung erhält man einen Monomorphismus $\Gamma\colon \Psi_d \to \hat{A} = \mathrm{Hom}(A, \mathbb{C}^\times)$. Da sich jeder Homomorphismus $\lambda \in \hat{A}$ durch $\lambda(n) := 0$ für $\mathrm{ggT}(n, d) > 1$ zu einem Dirichlet-Charakter fortsetzen lässt, ist Γ ein Isomorphismus. Insbesondere ist $|\Psi_d| = |\hat{A}| = |A| = \varphi(d)$ nach Satz 5.

(ii) Mit $\chi \in \Psi_d$ ist auch $\overline{\chi} \in \Psi_d$ nach Satz 5. Im Fall $\chi = \overline{\chi}$ nennen wir χ *reell*. Ggf. gilt $\chi(\mathbb{Z}) \subseteq \{0, \pm 1\}$. Der *triviale* Dirichlet-Charakter χ_0 mit den Werten 0 und 1 ist reell.

(iii) Für $\chi \in \Psi_d$ und $s > 1$ gilt

$$\sum_{n=1}^{\infty} \frac{|\chi(n)|}{n^s} \leq \zeta(s).$$

Daher ist $L(s, \chi)$ absolut konvergent.

Lemma 8 (Euler-Produkt)**.** *Für jeden Dirichlet-Charakter χ und $s > 1$ gilt*

$$L(s, \chi) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi(p)p^{-s}}. \tag{2}$$

Beweis. Sei $\mathbb{P}_N := \{p \in \mathbb{P} : p \leq N\} = \{p_1, \dots, p_t\}$. Sei Z_N die Menge der natürlichen Zahlen, deren Primfaktoren in $\mathbb{P}_N$ liegen. Nach dem Cauchy-Produkt für absolut konvergente Reihen (siehe [7, Satz 8.3]) gilt

$$\prod_{p \in \mathbb{P}_N} \frac{1}{1-\chi(p)p^{-s}} = \prod_{i=1}^{t} \sum_{k=0}^{\infty} \frac{\chi(p_i^k)}{p_i^{ks}} = \sum_{k=0}^{\infty} \sum_{k_1+\ldots+k_t=k} \frac{\chi(p_1^{k_1} \cdots p_t^{k_t})}{(p_1^{k_1} \cdots p_t^{k_t})^s} = \sum_{n \in Z_N} \frac{\chi(n)}{n^s},$$

wobei die Reihenfolge der Zahlen in Z_N auf Grund der absoluten Konvergenz keine Rolle spielt (siehe [7, Satz 7.8]). Die Behauptung folgt mit $N \to \infty$. □

Beispiel 9. Offensichtlich gilt auch $\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1-p^{-s}}$ für $s > 1$. Für den trivialen Dirichlet-Charakter $\chi_0 \in \Psi_d$ ergibt sich

$$L(s, \chi_0) = \prod_{\substack{p \in \mathbb{P} \\ p \nmid d}} \frac{1}{1-p^{-s}} = \zeta(s) \prod_{\substack{p \in \mathbb{P} \\ p \mid d}} \frac{p^s - 1}{p^s}$$

und

$$\lim_{s \to 1} L(s, \chi_0)(s-1) = \lim_{s \to 1} \zeta(s)(s-1) \lim_{s \to 1} \prod_{p \mid d} \frac{p^s - 1}{p^s} \overset{(1)}{=} \frac{\varphi(d)}{d}. \tag{3}$$

Insbesondere ist $\lim_{s \to 1} L(s, \chi_0) = \infty$. Wir werden sehen, dass sich nicht-triviale Dirichlet-Charaktere anders verhalten.

Satz 10. *Für $s > 1$ gilt*

$$\prod_{\chi \in \Psi_d} L(s, \chi) \geq 1. \tag{4}$$

Beweis. Nach (2) gilt

$$P := \prod_{\chi \in \Psi_d} L(s, \chi) = \prod_{\substack{p \in \mathbb{P} \\ p \nmid d}} \prod_{\chi \in \Psi_d} \frac{1}{1-\chi(p)p^{-s}}$$

(beachte $|\Psi_d| = \varphi(d) < \infty$). Sei e die Ordnung von $p + d\mathbb{Z} \in (\mathbb{Z}/d\mathbb{Z})^\times$ und $f := \varphi(d)/e$. Nach Satz 5(ii) (angewendet auf $\langle p + d\mathbb{Z} \rangle \leq (\mathbb{Z}/d\mathbb{Z})^\times$) durchlaufen die Zahlen $\{\chi(p) : \chi \in \Psi_d\}$ alle e-ten Einheitswurzeln und jede Einheitswurzel tritt genau f-mal auf. Für eine primitive e-te Einheitswurzel $\omega \in \mathbb{C}$ gilt $X^e - 1 = \prod_{k=1}^{e}(X - \omega^k)$. Dies zeigt

$$\prod_{\chi \in \Psi_d} \frac{1}{1-\chi(p)p^{-s}} = \Big(\prod_{k=1}^{e} \frac{p^s}{p^s - \omega^k} \Big)^f = \frac{p^{sef}}{(p^{se}-1)^f} > 1.$$

Somit ist $P \geq 1$. □

Lemma 11 (Abelsche Summation)**.** *Seien $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{C}$ und $A_k := \sum_{i=1}^{k} a_i$. Dann gilt*

$$\sum_{k=1}^{n} a_k b_k = A_n b_n + \sum_{k=1}^{n-1} A_k (b_k - b_{k+1}). \tag{5}$$

Beweis. Induktion nach n: Für $n = 1$ ist $\sum_{k=1}^{n} a_k b_k = A_1 b_1$. Sei nun $n \geq 1$. Dann gilt

$$\begin{aligned}\sum_{k=1}^{n} a_k b_k &= A_{n-1}b_{n-1} + \sum_{k=1}^{n-2} A_k(b_k - b_{k+1}) + a_n b_n = \sum_{k=1}^{n-1} A_k(b_k - b_{k+1}) + A_{n-1}b_n + a_n b_n \\ &= A_n b_n + \sum_{k=1}^{n-1} A_k(b_k - b_{k+1}).\end{aligned}$$

□

Folgerung 12. *Seien $a_1, a_2, \ldots \in \mathbb{C}$, sodass die Partialsummen $A_n := \sum_{k=1}^{n} a_k$ beschränkt sind. Sei $b_1, b_2, \ldots \in \mathbb{R}$ eine monoton fallende Nullfolge. Dann konvergiert $\sum_{n=1}^{\infty} a_n b_n$.*

Beweis. Sei $|A_n| \leq C$ für alle $n \in \mathbb{N}$. Für $n \leq m$ gilt

$$\Big|\sum_{k=n}^{m} a_k b_k\Big| \overset{(5)}{\leq} |A_m - A_{n-1}|b_m + \sum_{k=n}^{m-1} |A_k - A_{n-1}| \underbrace{(b_k - b_{k+1})}_{\geq 0} \leq 2Cb_n.$$

Wegen $\lim_{n\to\infty} b_n = 0$ bilden die Partialsummen $\sum_{k=1}^{n} a_k b_k$ eine Cauchyfolge. □

Definition 13. Stetigkeit und Differenzierbarkeit von komplexen Funktionen $f\colon \mathbb{C} \to \mathbb{C}$ definiert man wie im Reellen:

- Wir sagen f *konvergiert* im Punkt $z \in \mathbb{C}$ gegen $a \in \mathbb{C}$, falls

$$\forall \epsilon > 0\, \exists \delta > 0\, \forall w \in \mathbb{C} \setminus \{z\} : |z - w| < \delta \Longrightarrow |f(z) - a| < \epsilon.$$

  Ggf. schreiben wir $\lim_{w\to z} f(w) = a$.

- Man nennt f *stetig* im Punkt $z \in \mathbb{C}$, falls $\lim_{w\to z} f(w) = f(z)$ gilt. Ist f in jedem Punkt des Definitionsbereichs stetig, so heißt f *stetig*.

- Man nennt f *differenzierbar* im Punkt $z \in \mathbb{C}$, falls

$$f'(z) := \lim_{w\to z} \frac{f(z) - f(w)}{z - w}$$

  existiert. Ggf. nennt man $f'(z)$ die *Ableitung* von f in z. Ist f in jedem Punkt des Definitionsbereichs differenzierbar, so heißt f *differenzierbar*.

Bemerkung 14. Ist f differenzierbar in z, so ist f auch stetig in z. Die üblichen Ableitungsregeln gelten für komplexe Funktionen genau wie im Reellen (die Beweise in [7, Satz 15.2] übertragen sich). Insbesondere ist $(fg)' = f'g + fg'$ (Produktregel) und $(f \circ g)' = (f' \circ g)g'$ (Kettenregel) für differenzierbare Funktionen $f, g\colon \mathbb{C} \to \mathbb{C}$.

Beispiel 15. Bekanntlich ist die *Exponentialfunktion*

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \qquad z \mapsto \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

differenzierbar mit $\exp' = \exp$. Für $z \in \mathbb{C}$ gilt $\exp(z) = e^z$, wobei $e := \exp(1) \approx 2{,}718$ die *eulersche Zahl* ist. Die Einschränkung $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ ist surjektiv und streng monoton steigend. Sie besitzt mit dem *natürlichen Logarithmus* $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ eine differenzierbare Umkehrfunktion (siehe [7, Satz 15.3]).

Bemerkung 16. Aus dem Cauchy-Produkt absolut konvergenter Reihen folgt

$$\exp(z+w) = \exp(z)\exp(w)$$

für $z, w \in \mathbb{C}$ (siehe [7, Satz 8.4]). Induktiv erhält man $\exp(z_1 + \ldots + z_n) = \exp(z_1)\ldots\exp(z_n)$ für $z_1, \ldots, z_n \in \mathbb{C}$. Aus der Stetigkeit von exp folgt

$$\exp\Big(\sum_{k=1}^{\infty} z_k\Big) = \prod_{k=1}^{\infty} \exp(z_k) \tag{6}$$

für jede konvergente Reihe $\sum_{k=1}^{\infty} z_k$.

Satz 17. *Sei $\chi \in \Psi_d \setminus \{\chi_0\}$. Dann ist $L(s,\chi)$ auf $[1,\infty)$ stetig mit $L(1,\chi) \neq 0$.*

Beweis (Monsky [10]). Für $n \in \mathbb{N}$ und $s \geq 1$ sei $a_n := \chi(n)$ und $b_n := \frac{1}{n^s}$. Nach der ersten Orthogonalitätsrelation (Satz 5) gilt

$$A_d := \sum_{n=1}^{d} a_n = \sum_{n=1}^{d} \chi(n)\chi_0(n) = 0$$

und es folgt

$$|A_k| \leq \sum_{n=d\lfloor k/d \rfloor+1}^{k} |\chi(n)| \leq d$$

für alle $k \in \mathbb{N}$. Der Beweis von Folgerung 12 zeigt

$$\Big|L(s,\chi) - \sum_{n=1}^{N-1} \frac{\chi(n)}{n^s}\Big| \leq \Big|\sum_{n=N}^{\infty} a_n b_n\Big| \leq \frac{2d}{N^s} \leq \frac{2d}{N}.$$

Daher konvergieren die Partialsummen von $L(s,\chi)$ gleichmäßig gegen $L(s,\chi)$ für $s \geq 1$. Insbesondere ist $L(s,\chi)$ stetig auf $[0,\infty)$ nach [7, Satz 21.1].

Nehmen wir nun $L(1,\chi) = 0$ an.

Fall 1: $\overline{\chi} \neq \chi$.
Für $f\colon \mathbb{R}_{\geq 1} \to \mathbb{R}$, $x \mapsto x^{-1} - x^{-s}$ gilt

$$f'(x) \leq 0 \iff sx^{-s-1} - x^{-2} \leq 0 \iff x \geq s^{\frac{1}{s-1}} =: t,$$

wobei $t = 1$ für $s = 1$. Daher ist f für $x \geq t$ monoton fallend.[1] Insbesondere ist $b_n := f(n) = \frac{1}{n} - \frac{1}{n^s}$ eine monoton fallende Nullfolge für $n \geq t$. Nach dem Mittelwertsatz, angewendet auf $g\colon \mathbb{R} \to \mathbb{R}$, $s \mapsto n^{-s}$, existiert $1 \leq \xi_n \leq s$ mit

$$b_n = g(1) - g(s) = g'(\xi_n)(1-s) = \frac{\ln(n)}{n^{\xi_n}}(s-1)$$

(siehe [7, Corollar 16.1, Beispiel (15.18)]). Mit b_n ist auch $\frac{\ln(n)}{n^{\xi_n}}$ eine monoton fallende Nullfolge für $n \geq t$. Nach Folgerung 12 konvergiert

$$\gamma(s) := \sum_{n=1}^{\infty} a_n \frac{\ln(n)}{n^{\xi_n}}$$

[1] es gilt $t = (1 + (s-1))^{\frac{1}{s-1}} \leq e$ nach [7, Beispiel (15.13)]

für alle $s \geq 1$ (die endlichen vielen Summanden $n \leq t$ haben keinen Einfluss auf die Konvergenz). Der Beweis von Folgerung 12 zeigt (wie für $L(s,\chi)$), dass die Partialsummen gleichmäßig konvergieren und $\gamma(s)$ somit stetig auf $[0,\infty)$ ist. Insgesamt ist

$$L(s,\chi) = L(s,\chi) - L(1,\chi) = -\sum_{n=1}^{\infty} a_n b_n = (1-s)\gamma(s) \tag{7}$$

für $s \geq 1$.

Nach Voraussetzung gilt $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$. Das Produkt $P(s) := \prod_{\psi\in\Psi_d} L(s,\psi)$ aus (4) lässt sich aufspalten in $P(s) = L(s,\chi_0)L(s,\chi)L(s,\overline{\chi})Q(s)$. Die Stetigkeit von $L(s,\psi)$ für alle $\psi \neq \chi_0$ zeigt $\lim_{s\to 1} Q(s) < \infty$. Nach (7) und (3) ist andererseits

$$\lim_{s\to 1} L(s,\chi_0)L(s,\chi)L(s,\overline{\chi}) = \lim_{s\to 1} L(s,\chi_0)(1-s) \lim_{s\to 1}(1-s)\gamma(s)\overline{\gamma(s)} = 0.$$

Also ist auch $\lim_{s\to 1} P(s) = 0$ im Widerspruch zu (4).

Fall 2: $\overline{\chi} = \chi$.
Für $0 \leq x < 1$ und $n \in \mathbb{N}$ ist $\frac{x^n}{1-x^n} \leq \frac{x^n}{1-x}$. Daher konvergiert

$$f(x) := \sum_{n=1}^{\infty} \chi(n) \frac{x^n}{1-x^n}$$

absolut für $0 \leq x < 1$. Es gilt

$$-f(x) = \frac{1}{1-x} L(1,\chi) - f(x) = \sum_{n=1}^{\infty} a_n \underbrace{\left(\frac{1}{n(1-x)} - \frac{x^n}{1-x^n}\right)}_{=:b_n}$$

mit

$$\begin{aligned}(1-x)(b_n - b_{n+1}) &= \frac{1}{n} - \frac{1}{n+1} - \frac{x^n}{1+x+\ldots+x^{n-1}} + \frac{x^{n+1}}{1+x+\ldots+x^n} \\ &= \frac{1}{n(n+1)} - \frac{x^n}{(1+x+\ldots+x^{n-1})(1+x+\ldots+x^n)}.\end{aligned}$$

Aus der Ungleichung zwischen arithmetischen und geometrischen Mittel folgt

$$\frac{1-x^n}{1-x} = 1+x+\ldots+x^{n-1} \geq n x^{\frac{1}{n}\binom{n}{2}} = n x^{\frac{n-1}{2}} \geq n x^{n/2} \geq n x^n.$$

Damit erhält man $b_n \geq 0$ und

$$(1-x)(b_n - b_{n+1}) \geq \frac{1}{n(n+1)} - \frac{x^n}{n(n+1)x^n} = 0,$$

d. h. $1 = b_1 \geq b_2 \geq \ldots \geq 0$. Abelsche Summation ergibt

$$\Big|\sum_{k=1}^{n} a_k b_k\Big| \leq d b_n + d\sum_{k=1}^{n-1}(b_k - b_{k+1}) = d b_1 = d.$$

Insbesondere ist $f(x)$ beschränkt auf $[0,1)$. Wegen $\frac{x^n}{1-x^n} = \sum_{k=1}^{\infty} x^{kn}$ gilt

$$\begin{aligned}\Big|\sum_{n=1}^{N} \chi(n)\frac{x^n}{1-x^n} - \sum_{n=1}^{N}\Big(\sum_{k\mid n}\chi(k)\Big)x^n\Big| &= \Big|\sum_{n=1}^{N}\chi(n)\sum_{k=\lfloor N/n\rfloor+1}^{\infty} x^{kn}\Big| \leq \sum_{n=1}^{N}\frac{x^{n\lfloor N/n\rfloor+n}}{1-x^n} \\ &\leq \frac{1}{1-x}\sum_{n=1}^{N} x^N = \frac{Nx^N}{1-x} \xrightarrow{N\to\infty} 0.\end{aligned}$$

Dies zeigt

$$f(x)=\sum_{n=1}^{\infty}\underbrace{\Big(\sum_{k\mid n}\chi(k)\Big)}_{=:c_n}x^n.$$

Da χ reell ist, gilt $\chi(k)\in\{0,\pm1\}$ für alle $k\in\mathbb{N}$. Für jede Primzahl p folgt $c_{p^r}=1+\chi(p)+\ldots+\chi(p)^r\ge 0$. Mit der Primfaktorzerlegung $n=p_1^{r_1}\ldots p_t^{r_t}$ ergibt sich

$$c_n=c_{p_1^{r_1}}\ldots c_{p_t^{r_t}}\ge 0.$$

Wegen $d\ge 2$ besitzt d einen Primteiler p. Dann gilt $c_{p^r}=1$ und $f(x)\ge\sum_{r=1}^{\infty}x^{p^r}$. Folglich ist $\lim_{x\to 1}f(x)=\infty$ im Widerspruch zu Beschränktheit von $f(x)$. □

Beispiel 18. Nach [7, Satz 22.11, Beispiel (19.25), Beispiel (23.3)] gilt

$$\begin{aligned}
L(2,\chi_0)&=1+\frac{1}{9}+\frac{1}{25}+\ldots=\zeta(2)-\frac{1}{4}\zeta(2)=\frac{\pi^2}{8} && (\chi_0\in\Psi_2),\\
L(1,\chi)&=1-\frac{1}{3}+\frac{1}{5}\mp\ldots=\frac{\pi}{4} && (\chi\in\Psi_4\setminus\{\chi_0\}),\\
L(3,\chi)&=1-\frac{1}{27}+\frac{1}{125}\mp\ldots=\frac{\pi^3}{32} && (\chi\in\Psi_4\setminus\{\chi_0\}).
\end{aligned}$$

Aus der Partialbruchzerlegung des Cotangens [7, Satz 21.7(a)] mit $x=\frac{1}{3}$ bzw. $x=\frac{1}{6}$ folgt außerdem

$$\begin{aligned}
L(1,\chi)&=1+\sum_{n=1}^{\infty}\Big(\frac{1}{3n+1}-\frac{1}{3n-1}\Big)=\frac{1}{3}\pi\cot(\pi/3)=\frac{\pi}{3\sqrt{3}} && (\chi\in\Psi_3\setminus\{\chi_0\}),\\
L(1,\chi)&=1+\sum_{n=1}^{\infty}\Big(\frac{1}{6n+1}-\frac{1}{6n-1}\Big)=\frac{1}{6}\pi\cot(\pi/6)=\frac{\pi}{2\sqrt{3}} && (\chi\in\Psi_6\setminus\{\chi_0\}).
\end{aligned}$$

Definition 19. Eine nichtleere Teilmenge $Z\subseteq\mathbb{C}$ heißt *konvex*, falls für alle $x,y\in Z$ die Verbindungsstrecke $\{\lambda x+(1-\lambda)y:0\le\lambda\le 1\}$ zwischen x und y in Z liegt.

Lemma 20. *Sei $Z\subseteq\mathbb{C}$ konvex und $f\colon Z\to\mathbb{C}$ differenzierbar mit $f'(z)=0$ für alle $z\in Z$. Dann ist f konstant.*

Beweis. Seien $x,y\in Z$. Die reelle Funktion

$$g\colon[0,1]\to\mathbb{R},\qquad \lambda\mapsto f\big(\lambda x+(1-\lambda)y\big)+\overline{f\big(\lambda x+(1-\lambda)y\big)}=2\mathrm{Re}\big(f(\lambda x+(1-\lambda)y)\big)$$

ist wohldefiniert (da Z konvex ist) und erfüllt

$$g'(\lambda)=(x-y)f'\big(\lambda x+(1-\lambda)y\big)+\overline{(x-y)f'\big(\lambda x+(1-\lambda)y\big)}=0$$

für alle $0\le\lambda\le 1$ nach der Kettenregel. Aus dem Mittelwertsatz folgt, dass g konstant ist (siehe [7, Corollar 16.3]). Insbesondere ist $\mathrm{Re}(f(x))=\frac{1}{2}g(1)=\frac{1}{2}g(0)=\mathrm{Re}(f(y))$. Analog zeigt man $\mathrm{Im}(f(x))=\mathrm{Im}(f(y))$. Also ist f auf Z konstant. □

Bemerkung 21. Nach [7, Satz 14.9] lässt sich jedes $z \in \mathbb{C}^\times$ in eindeutig *Polarkoordinaten*

$$z = re^{\mathrm{i}\varphi} = r(\cos\varphi + \mathrm{i}\sin\varphi)$$

mit $r = |z| > 0$ und $-\pi < \varphi \le \pi$ schreiben. Daher ist die Einschränkung

$$\exp\colon \{z \in \mathbb{C} : -\pi < \mathrm{Im}(z) \le \pi\} \to \mathbb{C}^\times$$

bijektiv.

Definition 22. Der *Hauptzweig* des komplexen *Logarithmus* ist durch

$$\log\colon \mathbb{C}^\times \to \mathbb{C}, \qquad re^{\mathrm{i}\varphi} \mapsto \ln(r) + \mathrm{i}\varphi \qquad (r > 0,\ -\pi < \varphi \le \pi)$$

definiert.

Bemerkung 23. Für $z = re^{\mathrm{i}\varphi} \in \mathbb{C}$ gilt

$$\exp(\log(z)) = \exp(\ln(r) + \mathrm{i}\varphi) = re^{\mathrm{i}\varphi} = z. \tag{8}$$

Andererseits ist $\log(\exp(2\pi\mathrm{i})) = \log(1) = \ln(1) = 0 \ne 2\pi\mathrm{i}$.

Lemma 24.

(i) *Der komplexe Logarithmus ist auf* $D := \mathbb{C} \setminus \mathbb{R}_{\le 0}$ *differenzierbar mit* $\log'(z) = \frac{1}{z}$ *für* $z \in D$.

(ii) *Für* $z \in \mathbb{C}^\times$ *mit* $|z| < 1$ *gilt* $\log(1 - z) = -\sum_{n=1}^\infty \frac{z^n}{n}$.

Beweis.

(i) Nach [7, Beispiel (15.13)] ist $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ differenzierbar mit $\ln'(x) = 1/x$ für $x > 0$. Sei $z = re^{\mathrm{i}\varphi} \in D$ mit $r > 0$ und $-\pi < \varphi < \pi$. Sei $z_k := r_k e^{\mathrm{i}\varphi_k} \in D$ eine Folge mit $\lim_{k\to\infty} z_k = z$ und $-\pi < \varphi_k < \pi$ für $k \in \mathbb{N}$. Dann existiert ein $\epsilon > 0$ mit $|\varphi - \varphi_k| < 2\pi - \epsilon$ für alle $k \in \mathbb{N}$. Wegen

$$|r - r_k| = ||z| - |z_k|| \le |z - z_k| \xrightarrow{k\to\infty} 0$$

gilt $\lim_{k\to\infty} r_k = r$. Aus

$$\cos(\varphi - \varphi_k) + \mathrm{i}\sin(\varphi - \varphi_k) = e^{\mathrm{i}(\varphi - \varphi_k)} = \frac{r_k}{r}\frac{z}{z_k} \xrightarrow{k\to\infty} 1$$

und $|\varphi - \varphi_k| < 2\pi - \epsilon$ folgt $\lim_{k\to\infty} \varphi_k = \varphi$ (die Stetigkeit von arccos gilt nach [7, Satz 12.1, Satz 14.8]). Dies zeigt

$$\lim_{k\to\infty} \log(z_k) = \lim_{k\to\infty} (\ln(r_k) + \mathrm{i}\varphi_k) = \ln(r) + \mathrm{i}\varphi = z,$$

d. h. log ist stetig auf D. Nehmen wir nun $z_k \ne z$ für $k \in \mathbb{N}$ an. Als Umkehrfunktion der eingeschränkten Exponentialfunktion ist log injektiv. Insbesondere gilt $\log(z_k) \ne \log(z)$. Dies zeigt

$$\lim_{k\to\infty} \frac{\log(z) - \log(z_k)}{z - z_k} \overset{(8)}{=} \frac{1}{\lim\limits_{k\to\infty} \frac{\exp(\log(z)) - \exp(\log(z_k))}{\log(z) - \log(z_k)}} = \frac{1}{\exp'(\log(z))} = \frac{1}{\exp(\log(z))} = \frac{1}{z}$$

für alle $z \in D$.

(ii) Nach (i) ist die Funktion $f(z) := \log(1-z)$ auf der konvexen Menge $Z := \{z \in \mathbb{C} : |z| < 1\}$ differenzierbar mit $f'(z) = -\log'(1-z) = -\frac{1}{1-z}$ für $z \in Z$. Wegen

$$\sum_{n=1}^{\infty} \frac{|z|^n}{n} \le \sum_{n=1}^{\infty} |z|^n = \frac{|z|}{1-|z|} < \infty$$

konvergiert die Reihe $g(z) := -\sum_{n=1}^{\infty} \frac{z^n}{n}$ absolut für $z \in Z$. Nach [7, Satz 21.6] gilt

$$g'(z) = -\sum_{n=1}^{\infty} z^{n-1} = -\frac{1}{1-z} = f'(z).$$

Nach Lemma 20 existiert eine Konstante C mit $f(z) = g(z) + C$ und $C = f(0) - g(0) = 0$. $\square$

Bemerkung 25. Aus Lemma 24 folgt

$$\log\Big(\frac{1}{1-z}\Big) = \log\Big(\frac{1-z}{1-z}\Big) - \log(1-z) = \log(1) - \log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n} \tag{9}$$

für $|z| < 1$.

Satz 26 (Dirichlets Primzahlsatz)**.** *Für alle teilerfremden Zahlen $a, d \in \mathbb{N}$ gilt*

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

Insbesondere existieren unendlich viele Primzahlen $p \equiv a \pmod d$.

Beweis. O. B. d. A. sei $d \ge 2$. Nach Satz 17 existiert ein $t > 1$ mit $L(s, \chi) \ne 0$ für alle $\chi \in \Psi_d$ und $1 < s < t$ (beachte $L(s, \chi_0) \ge 1$ für alle $s > 1$). Im Folgenden sei stets $1 < s < t$. Für $\chi \in \Psi_d$ gilt

$$\sum_{p \in \mathbb{P}} \sum_{k=2}^{\infty} \frac{|\chi(p^k)|}{kp^{ks}} \le \sum_{p \in \mathbb{P}} \sum_{k=2}^{\infty} (p^{-s})^k = \sum_{p \in \mathbb{P}} \frac{p^{-2s}}{1-p^{-s}} = \sum_{p \in \mathbb{P}} \frac{1}{p^s(p^s-1)} \le \sum_{n=2}^{\infty} \Big(\frac{1}{n-1} - \frac{1}{n}\Big) = 1.$$

Nach der zweiten Orthogonalitätsrelation (Satz 5) ist

$$\sum_{\psi \in \Psi_d} \overline{\chi(a)}\chi(p) = \begin{cases} |\Psi_d| = \varphi(d) & \text{falls } p \equiv a \pmod d, \\ 0 & \text{sonst.} \end{cases}$$

Dies zeigt

$$f(s) := \sum_{\chi \in \Psi_d} \overline{\chi(a)} \sum_{p \in \mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} = \sum_{p \in \mathbb{P}} \sum_{\chi \in \Psi_d} \overline{\chi(a)} \Big(\frac{\chi(p)}{p^s} + \sum_{k=2}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\Big) \le \varphi(d) \sum_{p \equiv a \pmod d} \frac{1}{p^s} + C$$

für eine Konstante C (da Ψ_d nach Satz 5 unter komplexer Konjugation abgeschlossen ist, ist $f(s) \in \mathbb{R}$). Es genügt daher $\lim_{s \to 1} f(s) = \infty$ zu zeigen. Wegen $|\chi(p)p^{-s}| < 1$ gilt

$$\exp\Big(\sum_{p \in \mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}\Big) \overset{(6)+(9)}{=} \prod_{p \in \mathbb{P}} \exp\Big(\log\Big(\frac{1}{1-\chi(p)p^{-s}}\Big)\Big) \overset{(8)}{=} \prod_{p \in \mathbb{P}} \frac{1}{1-\chi(p)p^{-s}} \overset{(2)}{=} L(s, \chi).$$

Für $\chi \ne \chi_0$ ist also $\lim_{s \to 1} \sum_{p \in \mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}$ beschränkt. Wegen $\mathrm{ggT}(a, d) = 1$ ist andererseits $\chi_0(a) = 1$ und $\lim_{s \to 1} \sum_{p \in \mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi_0(p^k)}{kp^{ks}} = \infty$ nach Beispiel 9. Dies zeigt $\lim_{s \to 1} f(s) = \infty$. $\square$

Bemerkung 27.

(i) Seien $a, d \in \mathbb{N}$ teilerfremd und $\mathbb{P}_n := \{p \in \mathbb{P} : p \leq n\}$. Man kann zeigen, dass sich die Primzahlen „gleichmäßig“ auf die primen Restklassen verteilen, d. h.

$$\lim_{n\to\infty} \frac{|\{p \in \mathbb{P}_n : p \equiv a \pmod d\}|}{|\mathbb{P}_n|} = \frac{1}{\varphi(d)}.$$

(ii) In der Funktionentheorie setzt man die Riemannsche ζ-Funktion zu einer holomorphen Funktion auf $\mathbb{C} \setminus \{1\}$ fort. Sie besitzt dann die sogenannten trivialen Nullstellen $-2k$ für $k \in \mathbb{N}$. Der *Gaußsche Primzahlsatz*

$$\lim_{n\to\infty} \frac{|\mathbb{P}_n| \ln(n)}{n} = 1$$

ist äquivalent zu $\zeta(s) \neq 0$ für $\mathrm{Re}(s) = 1$ und lässt sich daher mit Funktionentheorie beweisen (siehe [3, 11, 16]). Auch hier gibt es „elementare“ Beweise von Erdős [6], Selberg [14] und anderen (siehe [8, 9, 12]).

(iii) Die *Riemannsche Vermutung* besagt, dass alle nicht-trivialen Nullstellen von ζ den Realteil $\frac{1}{2}$ haben. Dies ist eines der größten ungelösten Probleme der Mathematik. Man weiß, dass es unendlich viele solche Nullstellen gibt. Die Nullstelle mit dem kleinsten positiven Imaginärteil ist $\approx \frac{1}{2} + 14{,}347\,\mathrm{i}$. Ein Beweis der Riemannschen Vermutung würde die folgende Verbesserung des Gaußschen Primzahlsatz implizieren:

$$\Big| n - \sum_{p\in\mathbb{P}_n} \log(p) \Big| < \frac{\sqrt{n}\ln(n/\ln(n))^2}{8\pi} \qquad (n \geq e^{78})$$

(siehe [5, Proposition 2.5]).

Literatur

[1] R. Chapman, *Dirichlet's theorem a real variable approach*, `https://empslocal.ex.ac.uk/people/staff/rjchapma/etc/dirichlet.pdf`, 2008.

[2] H. Daboussi, *On the prime number theorem for arithmetic progressions*, J. Number Theory **31** (1989), 243–254.

[3] J.-M. De Koninck and F. Luca, *Analytic number theory*, Graduate Studies in Mathematics, Vol. 134, American Mathematical Society, Providence, RI, 2012.

[4] P. G. L. Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abhandlungen der Königlich Preussischen Akademie der Wissenschaften (1837), 45–81.

[5] P. Dusart, *Estimates of the kth prime under the Riemann hypothesis*, Ramanujan J. **47** (2018), 141–154.

[6] P. Erdös, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 374–384.

[7] O. Forster, *Analysis. 1*, Grundkurs Mathematik, Springer Spektrum, Wiesbaden, 2016 (12. Auflage).

[8] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Sixth edition, Oxford University Press, Oxford, 2008.

[9] A. Hildebrand, *The prime number theorem via the large sieve*, Mathematika **33** (1986), 23–30.

[10] P. Monsky, *Simplifying the proof of Dirichlet's theorem*, Amer. Math. Monthly **100** (1993), 861–862.

[11] D. J. Newman, *Simple analytic proof of the prime number theorem*, Amer. Math. Monthly **87** (1980), 693–696.

[12] F. K. Richter, *A new elementary proof of the Prime Number Theorem*, Bull. Lond. Math. Soc. **53** (2021), 1365–1375.

[13] A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Ann. of Math. (2) **50** (1949), 297–304.

[14] A. Selberg, *An elementary proof of the prime-number theorem*, Ann. of Math. (2) **50** (1949), 305–313.

[15] A. Selberg, *An elementary proof of the prime-number theorem for arithmetic progressions*, Canad. J. Math. **2** (1950), 66–78.

[16] D. Zagier, *Newman's short proof of the prime number theorem*, Amer. Math. Monthly **104** (1997), 705–708.

[17] H. Zassenhaus, *Über die Existenz von Primzahlen in arithmetischen Progressionen*, Comment. Math. Helv. **22** (1949), 232–259.