Prof. Dr. H. Brenner **Osnabrück SS 2008**

Zahlentheorie

Vorlesung 11

Satz 11.1. *(von Euklid) Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen, die Menge aller Primzahlen sei endlich, sagen wir $\{p_1, p_2, \ldots, p_r\}$. Man betrachtet die Zahl

$$N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r \; + 1 \, .$$

Diese Zahl ist durch keine der Primzahlen p_i teilbar, da immer ein Rest 1 verbleibt. Damit sind die Primfaktoren von N nicht in der Ausgangsmenge enthalten - Widerspruch. □

Kann man weitere Aussagen darüber machen, wieviele Primzahlen es gibt? Wir werden zunächst die Frage betrachten, was man über die Reihe

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

sagen kann. Dies ist also die Summe aller Kehrwerte von Primzahlen,

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots .$$

Bekanntlich divergiert die harmonische Reihe, also die Summe über aller Kehrwerte von positiven ganzen Zahlen. Dagegen konvergiert die Summe über alle Kehrwerte von Quadraten, es gibt also im gewissen Sinn wenig Quadrate. Für jede unendliche Teilmenge $M \subseteq \mathbb{N}$ ist es eine interessante und meistens schwierige Frage, ob $\sum_{n \in M} \frac{1}{n}$ konvergiert oder divergiert. Für die Primzahlen werden wir das hier in Kürze beantworten. Die Beantwortung hängt eng mit der Riemannschen ζ-Funktion zusammen. Die hier benutzten Methoden gehören zur analytischen Zahlentheorie.

Georg Friedrich Bernhard Riemann (1826-1866)

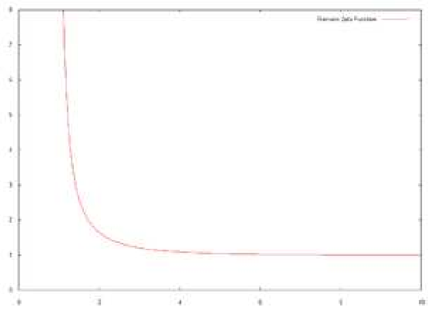
Definition 11.2. Die *Riemannsche ζ-Funktion* ist für $s \in \mathbb{C}$ mit Realteil 1 definiert durch

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

Satz 11.3. *(Geometrische Reihe) Für alle komplexen Zahlen z mit $|z| < 1$ konvergiert die Reihe $\sum_{k=0}^{\infty} z^k$ und es gilt*

$$\sum_{k=0}^{\infty} z^k = \frac{1}{1-z}\,.$$

Beweis. Dies wird in der Grundvorlesung Analysis bewiesen. □



Lemma 11.4. *Sei T eine endliche Menge von Primzahlen und sei s eine komplexe Zahl mit $\Re(s) > 0$. Es sei $M(T)$ die Menge aller natürlichen Zahlen, die sich als Produkt von Primzahlen aus T darstellen lassen. Dann ist*

$$\prod_{p \in T} \frac{1}{1-p^{-s}} = \sum_{n \in M(T)} \frac{1}{n^s}\,.$$

Beweis. Sei $T = \{p_1, \ldots, p_k\}$. Es ist $|p^{-s}| < 1$ nach Voraussetzung über den Realteil. Unter Verwendung der geometrischen Reihe ergibt sich

$$\begin{aligned}
\prod_{p \in T} \frac{1}{1-p^{-s}} &= \frac{1}{1-p_1^{-s}} \cdots \frac{1}{1-p_k^{-s}} \\
&= \left(\sum_{i=0}^{\infty} (p_1^{-s})^i\right) \cdots \left(\sum_{i=0}^{\infty} (p_k^{-s})^i\right) \\
&= \sum_{0 \le i_1, \ldots, i_k < \infty} (p_1^{-s})^{i_1} \cdots (p_k^{-s})^{i_k} \\
&= \sum_{n \in M(T)} n^{-s}\,.
\end{aligned}$$

□

Aus dieser Aussage ergibt sich sofort ein neuer Beweis dafür, dass es unendlich viele Primzahlen gibt. Wenn es nämlich nur endlich viele Primzahlen gäbe, so könnte man T als die endliche Menge aller Primzahlen ansetzen. Für $s = 1$ stünde dann links eine reelle Zahl, und rechts würde die Summe über alle natürlichen Kehrwerte stehen. Dies ist aber die harmonische Reihe, und diese divergiert!

Satz 11.5. *(Produktdarstellung der Riemannschen ζ-Funktion) Sei s eine komplexe Zahl mit $\Re(s) > 1$. Dann gilt für die Riemannsche ζ-Funktion die Produktdarstellung*

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

Beweis. Dies folgt aus Lemma 11.4, wenn man für T die ersten k Primzahlen überhaupt ansetzt und dann k gegen unendlich laufen lässt. Die Konvergenz der linken Seite, also die Wohldefiniertheit der ζ-Funktion, sichert dabei auch die Konvergenz der rechten Seite. □

Korollar 11.6. *Das unendliche Produkt*

$$\prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-1}}$$

divergiert.

Beweis. Dies folgt aus der endlichen Produktdarstellung (Satz 11.5) für $s = 1$. Man hat die Gleichheit

$$\prod_{p \in T_k} \frac{1}{1 - p^{-1}} = \sum_{n \in M(T_k)} \frac{1}{n} ,$$

wobei T_k die ersten k Primzahlen umfasse. Für $k \to \infty$ ergibt sich rechts die harmonische Reihe, die bekanntlich divergiert. Also divergiert auch das Produkt links. □

Wir können nun die oben formulierte Frage beantworten.

Satz 11.7. *(Euler) Die Reihe der Kehrwerte der Primzahlen, also*

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

divergiert.

Beweis. Das Produkt $\prod_{i=1}^{k} \frac{1}{1-p_i^{-1}}$ divergiert für $k \to \infty$ aufgrund von Korollar 11.6 und ist insbesondere unbeschränkt. Daher ist auch der natürliche Logarithmus davon unbeschränkt. Dieser ist

$$\ln\left(\prod_{i=1}^{k} \frac{1}{1 - p_i^{-1}} \right) = \sum_{i=1}^{k} \ln\left(\frac{1}{1 - p_i^{-1}} \right) = - \sum_{i=1}^{k} \ln(1 - p_i^{-1}) .$$

Die Potenreihenentwicklung des natürlichen Logarithmus ist

$$\ln(1 - x) = - \sum_{j=1}^{\infty} \frac{x^j}{j}$$

für $|x| < 1$. Angewendet auf die vorstehende Situation ergibt das

$$= \sum_{i=1}^{k} (\sum_{j=1}^{\infty} \frac{(p_i^{-1})^j}{j}) = \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i=1}^{k} \left(\sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j} \right) .$$

Für die hinteren Summanden hat man die Abschätzungen

$$\sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j} \leq \sum_{j=2}^{\infty} \left(\frac{1}{p_i} \right)^j = \left(\frac{1}{p_i} \right)^2 \left(\sum_{j=0}^{\infty} \left(\frac{1}{p_i} \right)^j \right) = \left(\frac{1}{p_i} \right)^2 \frac{1}{1 - p_i^{-1}} \leq \frac{2}{p_i^2} ,$$

wobei hinten wieder die geometrische Reihe benutzt wurde. Damit ist insgesamt

$$\sum_{i=1}^{k} \left(\sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j} \right) \leq \sum_{i=1}^{k} \frac{2}{p_i^2} \leq 2 \sum \frac{1}{n^2} .$$

Da die Summe der reziproken Quadrate konvergiert, ist diese Gesamtsumme beschränkt. Daher ist die Summe $\sum_{i=1}^{k} \frac{1}{p_i}$ unbeschränkt, was die Behauptung ist. □

Bemerkung 11.8. Ein Primzahlzwilling ist ein Paar bestehend aus p und $p+2$, wobei diese beiden Zahlen Primzahlen sind. Die ersten Beispiele sind

$$(3, 5),\ (5, 7),\ (11, 13),\ (17, 19),\ (29, 31), \ldots .$$

Es ist ein offenes Problem der Zahlentheorie, ob es unendlich viele Primzahlzwillinge gibt (was aber stark vermutet wird). Dagegen ist bekannt, dass die zugehörige Reihe, also

$$\sum_{p, p+2 \in \mathbb{P}} \frac{1}{p}$$

konvergiert. In diesem Sinne gibt es also, verglichen mit der Gesamtzahl der Primzahlen, wenige Primzahlzwillinge.

Die Funktion $\pi(x)$

Es gehört zu den schwierigsten Fragen der Zahlentheorie und der Mathematik überhaupt, die Verteilung der Primzahlen zu verstehen. Viele offene Fragen und Vermutungen beziehen sich auf Teilaspekte dieses Problems.

Einfachere Fragestellungen, die bereits die Schwierigkeit im Allgemeinen erahnen lassen, sind etwa: gibt es mehr Primzahlen unterhalb von n als zwischen n und n^2? Gibt es stets eine Primzahl zwischen n und $2n$? Gibt es stets eine Primzahl zwischen n^2 und $(n+1)^2$?

Es ist hilfreich, folgende Funktion einzuführen, die Primzahlfunktion genannt wird.

Definition 11.9. Die für $x \in \mathbb{R}$ definierte Funktion

$$x \longmapsto \pi(x) := \#\{p \leq x, p \text{ Primzahl}\}$$

heißt *Primzahlfunktion*.

Bemerkung 11.10. Die Primzahlfunktion zählt also, wieviele Primzahlen es unterhalb einer gewissen Schranke gibt. Sie nimmt offenbar nur natürliche Zahlen als Werte an und sie ist eine monton wachsende Treppenfunktion. Sie hat genau an den Primzahlen eine Sprungstelle. Die Frage nach der Verteilung von Primzahlen ist gleichbedeutend dazu, gute Approximationen bzw. Abschätzungen für sie durch andere, besser verstandene (analytische) Funktionen zu finden.

Jacques Salomon Hadamard (1865 Versailles - 1963 Paris)

Charles-Jean de La Vallée Poussin (1866 Löwen - 1962 Brüssel)

Ein Hauptresultat der analytischen Zahlentheorie ist der sogenannte Primzahlsatz von Hadamard und de la Vallée Pousin von 1896. Es besagt grob gesprochen, dass sich die Primzahlfunktion $\pi(x)$ in etwa so verhält wie $x/\ln(x)$, also dass der Quotient der beiden Funktionen gegen 1 konvergiert. Hier tritt der natürliche Logarithmus (zur Basis e) auf.

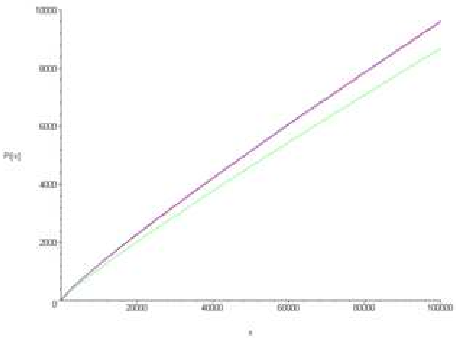
Satz 11.11. *Es gilt die asymptotische Abschätzung*

$$\pi(x) \sim \frac{x}{\ln(x)} \,.$$

Das heißt, dass

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = \lim_{x\to\infty} \frac{\pi(x)\ln(x)}{x} = 1 \,.$$

Beweis. Dies ist ein Satz der analytischen Zahlentheorie, den wir hier nicht beweisen. □



Wir erwähnen abschließend ohne Beweis noch den Satz von Dirichlet. Einzelne Spezialfälle werden in den Aufgaben besprochen.

Peter Gustav Lejeune Dirichlet (1805-1859)

Satz 11.12. *(von Dirichlet) Sei n eine natürliche Zahl und a eine zu n teilerfremde Zahl. Dann gibt es unendlich viele Primzahlen, die modulo n den Rest a haben.*

Beweis. Dies ist ein Satz der analytischen Zahlentheorie, den wir im Rahmen dieser Vorlesung nicht beweisen können. □

Abbildungsverzeichnis