

## Zahlentheorie

### Vorlesung 11

#### Die Unendlichkeit der Primzahlen

SATZ 11.1. *Es gibt unendlich viele Primzahlen.*

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

$$N = p_1 \cdot p_2 \cdot p_3 \cdots p_r + 1.$$

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

Eine Liste aller Primzahlen  $\leq 100000$  findet sich hier.

Kann man weitere Aussagen darüber machen, wie viele 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,

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

Bekanntlich divergiert die harmonische Reihe, also die Summe über aller Kehrwerte von positiven ganzen Zahlen. Dagegen konvergiert die Summe über alle Kehrwerte von Quadraten (und zwar gegen  $\frac{\pi^2}{6}$ ), 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  $\zeta$ -Funktion zusammen. Die hier benutzten Methoden gehören zur analytischen Zahlentheorie.



Georg Friedrich Bernhard Riemann (1826-1866)

DEFINITION 11.2. Die *Riemannsche  $\zeta$ -Funktion* ist für  $s \in \mathbb{C}$  mit Realteil  $\operatorname{Re}(s) > 1$  durch

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

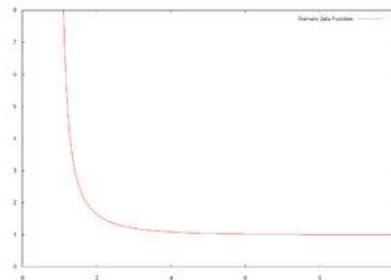
definiert.

Wir erinnern an die Konvergenz der geometrischen Reihe.

SATZ 11.3. Für alle komplexen Zahlen  $z$  mit  $|z| < 1$  konvergiert die Reihe  $\sum_{k=0}^{\infty} z^k$  absolut 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  $\operatorname{Re}(s) > 0$ . 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  $T = \{p_1, \dots, p_k\}$ . Es ist  $|p^{-s}| < 1$  nach Voraussetzung über den Realteil. Unter Verwendung der geometrischen Reihe ergibt sich

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

□

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. Es wäre dann  $M(T) = \mathbb{N}$ . 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.** *Sei  $s$  eine komplexe Zahl mit  $\Re(s) > 1$ . Dann gilt für die Riemannsche  $\zeta$ -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 Menge der ersten  $k$  Primzahlen überhaupt ansetzt und dann  $k$  gegen unendlich laufen lässt. Die Konvergenz der linken Seite, also die Wohldefiniertheit der  $\zeta$ -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 Lemma 11.4 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  $k \rightarrow \infty$  ergibt sich rechts die harmonische Reihe, die bekanntlich divergiert. Also divergiert auch das Produkt links.  $\square$

Wir können nun die oben formulierte Frage beantworten.

**SATZ 11.7.** *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  $k \rightarrow \infty$  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 Potenzreihenentwicklung 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

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

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

$$\sum_{i=1}^k \left( \sum_{j=2}^{\infty} \frac{(p_i^{-1})^j}{j} \right) \leq \sum_{i=1}^k \frac{2}{p_i^2} \leq 2 \sum_{n \in \mathbb{N}_+} \frac{1}{n^2}.$$

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.  $\square$

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

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

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.

BEMERKUNG 11.9. Die Frage, ob es unendlich viele Primzahlzwillinge gibt, besitzt verschiedene schwächere Varianten. Man kann sich zum Beispiel fragen, ob es unendlich oft vorkommt, dass es in einem Zehnerintervall zwei Primzahlen gibt, oder dass es in einem Hunderterintervall zwei Primzahlen gibt, und so weiter. Die ersten Primzahlen vermitteln dabei ein Bild, dass Primzahlen ziemlich häufig sind. Sie werden aber zunehmend seltener, so dass es für hohe Hunderterintervalle, sagen wir für die Zahlen von

$$1000000000000000 \text{ bis } 1000000000000100$$

ziemlich unwahrscheinlich ist, eine Primzahl zu enthalten, geschweige denn zwei Primzahlen. Bis vor kurzem war es nicht bekannt, ob es überhaupt eine Zahl  $m$  mit der Eigenschaft gibt, dass es unendlich viele Intervalle der Länge  $m$  gibt, die zwei Primzahlen enthalten ( $m = 2$  wäre die positive Lösung des Primzahlzwillingsproblems). Im Jahr 2013 bewies Zhang Yitang, dass man

$$m = 70000000$$

nehmen kann, dass es also unendlich viele Intervalle der Form

$$[k, k + 70000000]$$

gibt, in denen zwei Primzahlen liegen. Dieses Resultat ist ein Durchbruch in der Primzahlzwillingsforschung, da es erstmals zeigt, dass sich Primzahlen unendlich oft „ziemlich nahe“ kommen. Zwischenzeitlich wurde die Schranke von 70000000 auf 252 gesenkt, siehe <http://arxiv.org/pdf/1402.4849v2.pdf>.

### 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, die folgende Funktion einzuführen, die *Primzahlfunktion* genannt wird.

DEFINITION 11.10. Die für  $x \in \mathbb{R}$  definierte Funktion

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

heißt *Primzahlfunktion*.



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



Jacques Salomon Hadamard (1865  
Versailles - 1963 Paris)

BEMERKUNG 11.11. Die Primzahlfunktion zählt also, wie viele Primzahlen es unterhalb einer gewissen Schranke gibt. Sie nimmt offenbar nur natürliche Zahlen als Werte an und sie ist eine monoton 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.

Ein Hauptresultat der analytischen Zahlentheorie ist der sogenannte Primzahlsatz von Hadamard und de la Vallée Poussin 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.

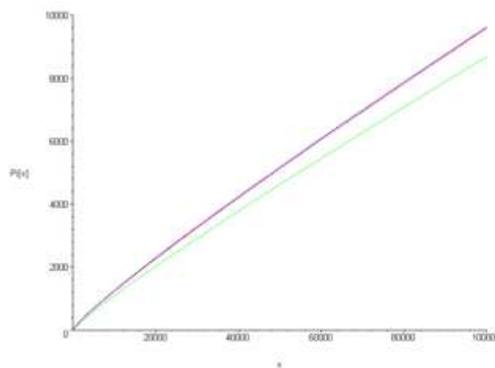
SATZ 11.12. *Es gilt die asymptotische Abschätzung*

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

Das heißt

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

*Beweis.* Dies ist ein Satz der analytischen Zahlentheorie, den wir hier nicht beweisen.  $\square$



Den Primzahlsatz kann man auch so verstehen, dass die Wahrscheinlichkeit, dass eine Zahl in der Größenordnung  $x$  eine Primzahl ist, gleich  $\frac{1}{\ln x}$  ist. In der Tat ist sogar das Integral dazu, also der sogenannte *Integrallogarithmus*  $\text{Li}(x) = \int_2^x \frac{1}{\ln t} dt$  eine bessere Approximation für  $\pi(x)$  als  $x/\ln x$ . Für  $x = 1000000$  ist  $\pi(x) = 78498$ ,  $\text{Li}(x) = 78628$  und  $\frac{x}{\ln x} = 72382$  (die beiden letzten Werte gerundet).



Peter Gustav Lejeune Dirichlet (1805-1859)

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

SATZ 11.13. *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.  $\square$



Generationenübergreifend forschen. Hier Paul Erdős und Terence Tao.

Der folgende Satz wurde 2004 von Ben Green und Terence Tao bewiesen.

SATZ 11.14. *Zu jedem  $k$  gibt es arithmetische Progressionen der Länge  $k$ , die nur aus Primzahlen bestehen.*

*Beweis.* Dies können wir hier nicht beweisen.  $\square$

Eine arithmetische Progression innerhalb der Primzahlen der Länge 7 ist

$$7, 157, 307, 457, 607, 757, 907.$$

Die derzeit längste bekannte arithmetische Progression besitzt 26 Glieder, nämlich

$$43142746595714191 + 23681770 \cdot 223092870 \cdot n, \text{ für } n = 0, \dots, 25.$$

## Abbildungsverzeichnis

Quelle = Georg Friedrich Bernhard Riemann.jpeg , Autor = Benutzer Ævar Arnfjörð Bjarmason auf Commons, Lizenz = PD	2
Quelle = Zeta.png , Autor = Benutzer Anarkman auf Commons, Lizenz = CC-by-sa 3.0	2
Quelle = De La Vallée Poussin.jpg , Autor = Benutzer Sonuwe auf Commons, Lizenz = PD	6
Quelle = Hadamard2.jpg , Autor = Benutzer Gian- auf en.wikipedia.org, Lizenz = PD	6
Quelle = PrimeNumberTheorem.png , Autor = FredStober, Lizenz = PD	7
Quelle = Peter Gustav Lejeune Dirichlet.jpg , Autor = Benutzer Magnus Manske auf Commons, Lizenz = PD	7
Quelle = Paul_Erdos_with_Terence_Tao.jpg , Autor = Benutzer PaulTheOctopus auf Commons, Lizenz = CC-by-sa 2.0	8