Die Musik der Primzahlen, I

Der Primzahlsatz und die Riemannsche Vermutung

Prof. Dr. Stefan Wewers

Institut für Algebra und Zahlentheorie
Universität Ulm

26. Februar 2021

Rückblick: das Faktorisierungsproblem

Rückblick: das Faktorisierungsproblem

Für die RSA-Verschlüsselung muss Bob eine RSA-Zahl wählen,

$$N = p \cdot q,$$

mit großen Primzahlen p, q.

Rückblick: das Faktorisierungsproblem

Für die RSA-Verschlüsselung muss Bob eine RSA-Zahl wählen,

$$N = p \cdot q,$$

mit großen Primzahlen p, q.

Die Zahl N ist Teil des *öffentlichen Schlüssels*, die Primzahlen p, q werden benutzt, um den *geheimen Schlüssel* zu generieren.

Rückblick: das Faktorisierungsproblem

Für die RSA-Verschlüsselung muss Bob eine RSA-Zahl wählen,

$$N = p \cdot q,$$

mit großen Primzahlen p, q.

Die Zahl N ist Teil des *öffentlichen Schlüssels*, die Primzahlen p, q werden benutzt, um den *geheimen Schlüssel* zu generieren.

Die Sicherheit des RSA-Systems besteht darin, dass es praktisch unmöglich ist, die Zahl N zu faktorisieren.

Rückblick: das Faktorisierungsproblem

Für die RSA-Verschlüsselung muss Bob eine RSA-Zahl wählen,

$$N = p \cdot q,$$

mit großen Primzahlen p, q.

Die Zahl N ist Teil des *öffentlichen Schlüssels*, die Primzahlen p, q werden benutzt, um den *geheimen Schlüssel* zu generieren.

Die Sicherheit des RSA-Systems besteht darin, dass es praktisch unmöglich ist, die Zahl N zu faktorisieren.

Bob muss also in der Lage sein, *zufällige* Primzahlen einer bestimmten Größenordnung zu wählen, die ein Angreifer nicht "erraten" kann.

Der Primzahlsatz

Wieviele Primzahlen gibt es?

Der Primzahlsatz

Wieviele Primzahlen gibt es?

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, 27, 29, \ldots$$

Der Primzahlsatz

Wieviele Primzahlen gibt es?

$$\begin{aligned} p &= 2, 3, 5, 7, 11, 13, 17, 19, 23, 27, 29, \ldots \\ &\quad \ldots, 101, 103, 107, 109, 113, 127, \ldots \end{aligned}$$

Der Primzahlsatz

Wieviele Primzahlen gibt es?

$$\begin{aligned} p &= 2, 3, 5, 7, 11, 13, 17, 19, 23, 27, 29, \ldots \\ &\quad \ldots, 101, 103, 107, 109, 113, 127, \ldots \end{aligned}$$

Theorem (Euklid, ca. 200 v.Chr.)

Es gibt unendlich viele Primzahlen.

Der Primzahlsatz

Wieviele Primzahlen gibt es?

$$\begin{aligned} p &= 2, 3, 5, 7, 11, 13, 17, 19, 23, 27, 29, \ldots \\ &\quad \ldots, 101, 103, 107, 109, 113, 127, \ldots \end{aligned}$$

Theorem (Euklid, ca. 200 v.Chr.)

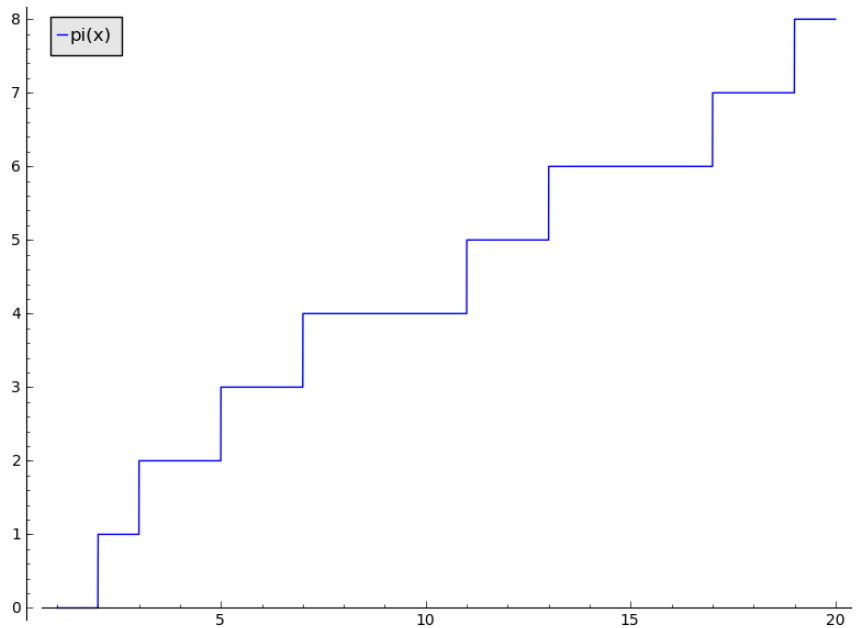
Es gibt unendlich viele Primzahlen.

Leider gibt Euklids Beweis keine befriedigende Antwort auf die Frage, wie *häufig* Primzahlen vorkommen.

Der Primzahlsatz

Sei

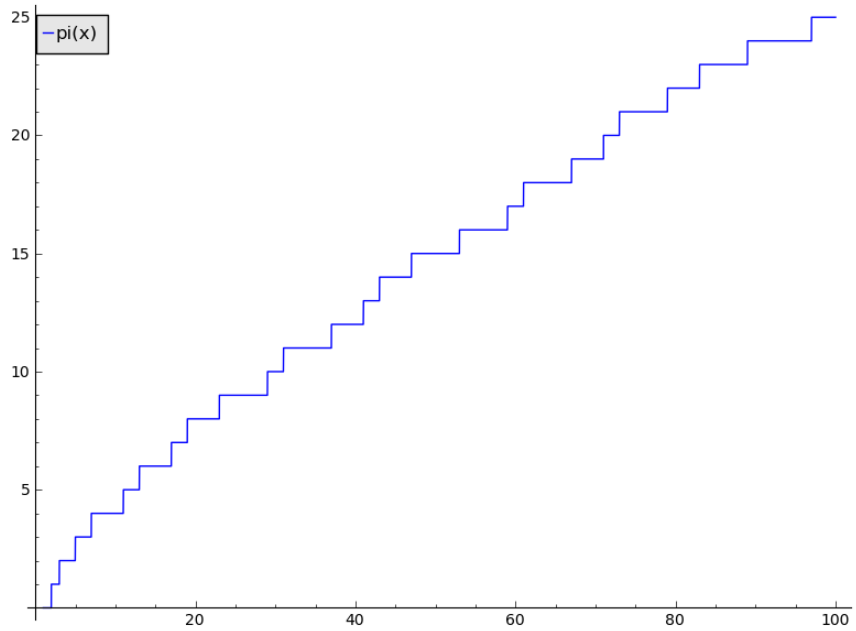
$$\pi(x) := \text{Anzahl der Primzahlen } p \leq x.$$



Der Primzahlsatz

Sei

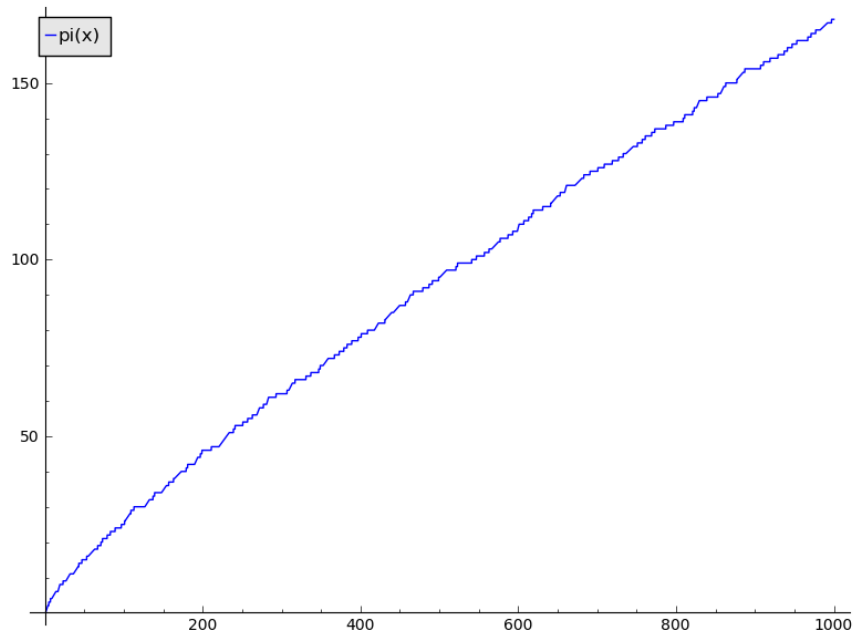
$$\pi(x) := \text{Anzahl der Primzahlen } p \leq x.$$



Der Primzahlsatz

Sei

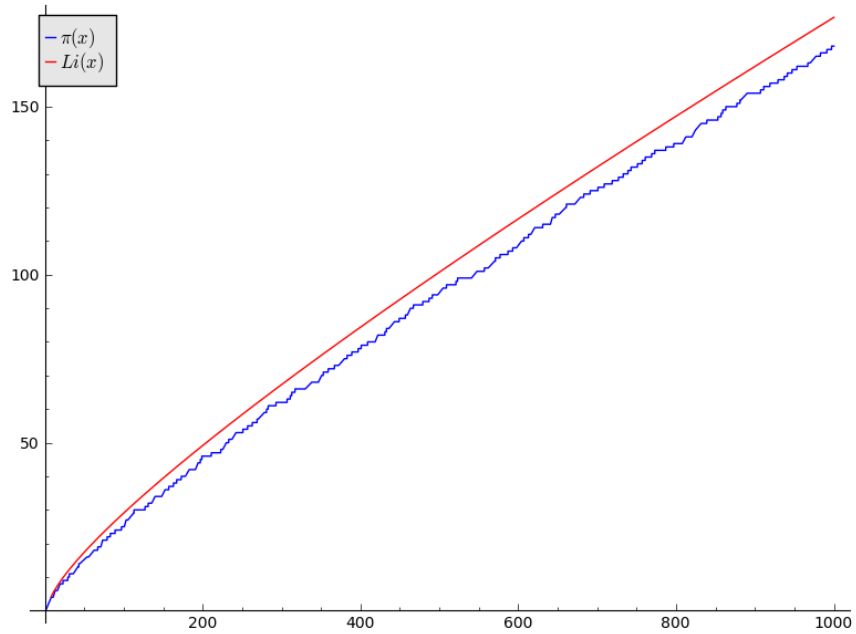
$$\pi(x) := \text{Anzahl der Primzahlen } p \leq x.$$



Der Primzahlsatz

Sei

$$\pi(x) := \text{Anzahl der Primzahlen } p \leq x.$$



Satz (Hadamard, de La Vallée Poussin, 1896)

$$\pi(x) \sim Li(x) \quad \textit{für } x \to \infty,$$

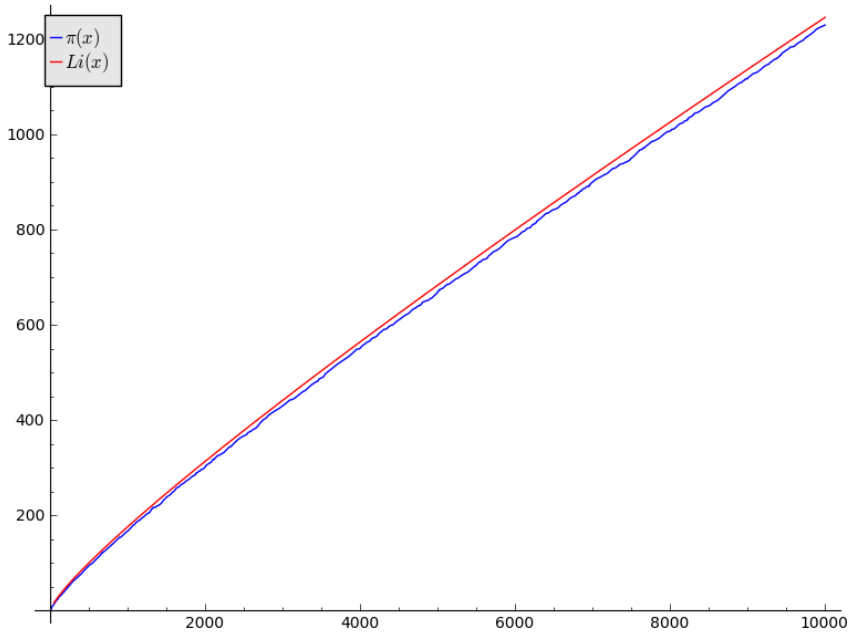
wobei

$$Li(x) := \int_2^x \frac{\mathrm{d}t}{\log(x)}.$$

Der Primzahlsatz

Sei

$$\pi(x) := \text{Anzahl der Primzahlen } p \leq x.$$



Satz (Hadamard, de La Vallée Poussin, 1896)

$$\pi(x) \sim Li(x) \quad \textit{für } x \to \infty,$$

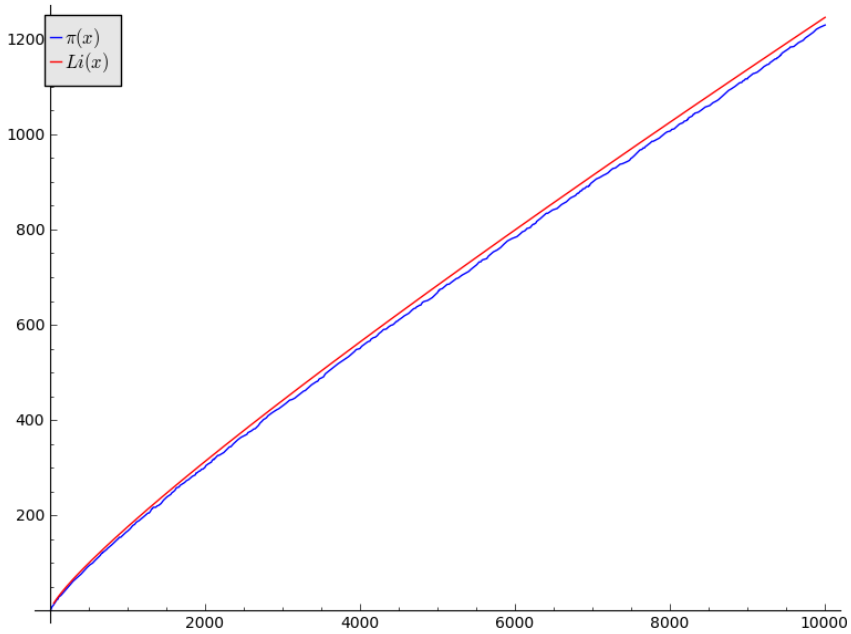
wobei

$$Li(x) := \int_2^x \frac{\mathrm{d}t}{\log(x)}.$$

Der Primzahlsatz

Sei

$$\pi(x) := \text{Anzahl der Primzahlen } p \leq x.$$



Heuristische Interpretation

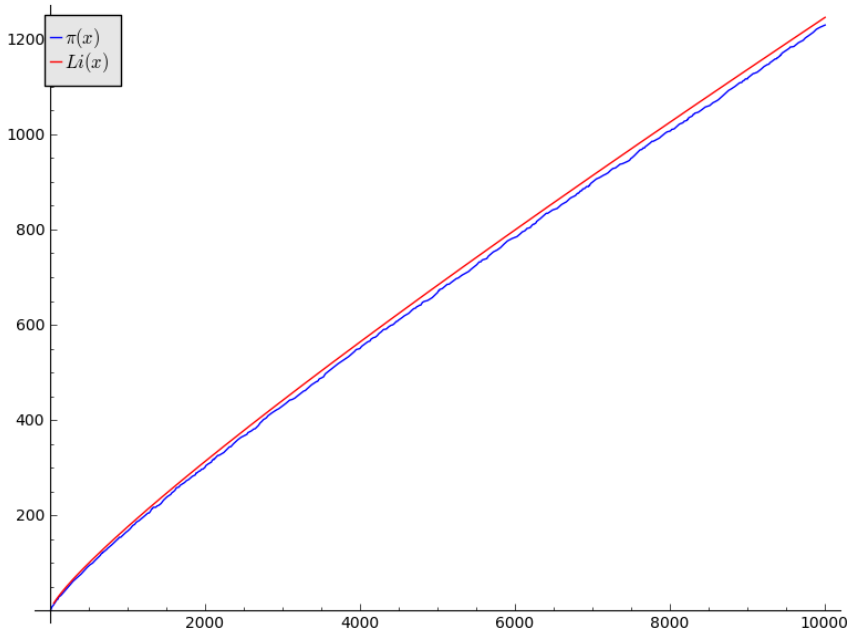
Die 'Wahrscheinlichkeit', dass eine zufällig gewählte Zahl n eine Primzahl ist, ist

$$P(n \in \mathbb{P}) \sim \frac{1}{log(n)}.$$

Der Primzahlsatz

Sei

$$\pi(x) := \text{Anzahl der Primzahlen } p \leq x.$$



Die Riemannsche Vermutung

würde zeigen:

$$\pi(x) = Li(x) + \mathcal{O}\left(\sqrt{x}\log(x)\right).$$

Die Riemannsche Vermutung

Die Riemannsche Vermutung wurde 1859 von B. Riemann in seiner berühmten Arbeit *Über die Anzahl der Primzahlen unter einer gegebenen Größe* (Monatsbericht der Berliner Akademie, November 1859) formuliert:

Die Riemannsche Vermutung

Die Riemannsche Vermutung wurde 1859 von B. Riemann in seiner berühmten Arbeit *Über die Anzahl der Primzahlen unter einer gegebenen Größe* (Monatsbericht der Berliner Akademie, November 1859) formuliert:

> *Man findet nun in der That etwa so viel reelle Wurzeln innerhalb dieser Grenzen, und es ist sehr wahrscheinlich, daß alle Wurzeln reell sind. Hievon wäre allerdings ein strenger Beweis zu wünschen; ich habe indeß die Aufsuchung desselben, nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien.*

Die Riemannsche Vermutung

Die Riemannsche Vermutung ist bis heute nicht bewiesen und gilt als das größte offene Problem der Mathematik.

D. Hilbert (1862-1943) antwortete auf die Frage '*Wenn Sie in 500 Jahren wieder aufwachen würden, was würden Sie dann tun?*':

Die Riemannsche Vermutung

Die Riemannsche Vermutung ist bis heute nicht bewiesen und gilt als das größte offene Problem der Mathematik.

D. Hilbert (1862-1943) antwortete auf die Frage '*Wenn Sie in 500 Jahren wieder aufwachen würden, was würden Sie dann tun?*':

> *Ich würde fragen, ob jemand die Riemannsche Vermutung gelöst hätte.*

Die Riemannsche Vermutung

Die Riemannsche Vermutung ist bis heute nicht bewiesen und gilt als das größte offene Problem der Mathematik.

D. Hilbert (1862-1943) antwortete auf die Frage '*Wenn Sie in 500 Jahren wieder aufwachen würden, was würden Sie dann tun?*':

> *Ich würde fragen, ob jemand die Riemannsche Vermutung gelöst hätte.*

Seit 2000 ist die R.V. eines der 7 mathematischen *Jahrtausendprobleme*, auf die vom *Clay Mathematics Institute* ein Preis von 1.000.000 $ ausgeschrieben ist.

Frage:

Gibt es mehr Quadratzahlen als Primzahlen?

Frage:

Gibt es mehr Quadratzahlen als Primzahlen?

Wir werden zeigen, dass es viel mehr Primzahlen als Quadratzahlen gibt, denn

Frage:

Gibt es mehr Quadratzahlen als Primzahlen?

Wir werden zeigen, dass es viel mehr Primzahlen als Quadratzahlen gibt, denn

$$\sum_{n\geq 1} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots$$

Frage:

Gibt es mehr Quadratzahlen als Primzahlen?

Wir werden zeigen, dass es viel mehr Primzahlen als Quadratzahlen gibt, denn

$$\sum_{n\geq 1} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \ldots = \frac{\pi^2}{6}$$

(Euler),

Frage:

Gibt es mehr Quadratzahlen als Primzahlen?

Wir werden zeigen, dass es viel mehr Primzahlen als Quadratzahlen gibt, denn

$$\sum_{n\geq 1} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \ldots = \frac{\pi^2}{6}$$

(Euler), aber

$$\sum_{p} \frac{1}{p} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots = \infty.$$

Die Riemannsche ζ-Funktion

Bereits 1744 betrachtete Euler die durch eine unendliche Reihe definierte Funktion

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \ldots .$$

Die Riemannsche ζ-Funktion

Bereits 1744 betrachtete Euler die durch eine unendliche Reihe definierte Funktion

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \ldots .$$

Dies ist nur für $s > 1$ definiert, und hat in $s = 1$ einen Pol:

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \ldots \quad \rightarrow \quad \infty$$

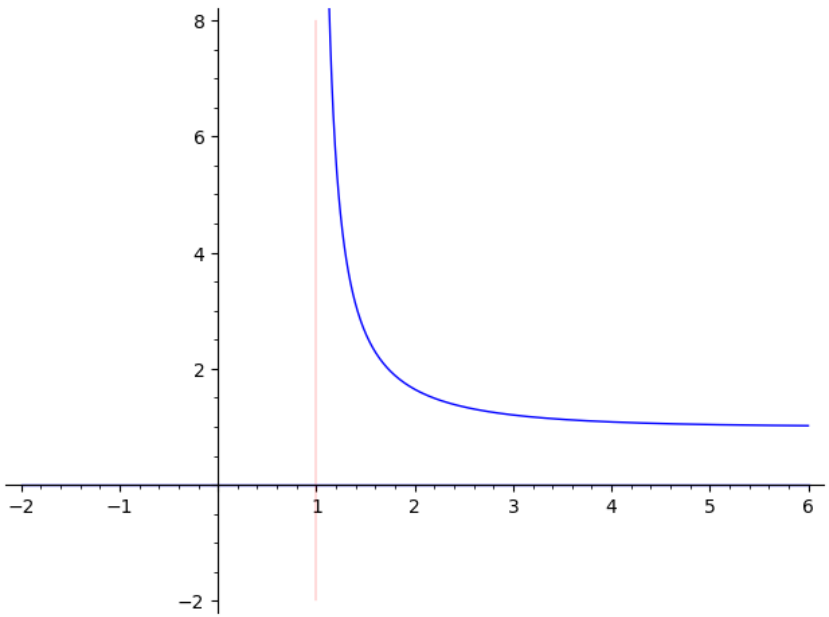
Die Riemannsche ζ-Funktion

Bereits 1744 betrachtete Euler die durch eine unendliche Reihe definierte Funktion

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \ldots .$$

Dies ist nur für $s > 1$ definiert, und hat in $s = 1$ einen Pol:

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \ldots \quad \to \quad \infty$$



Das Euler-Produkt

Das Euler-Produkt

Der Zusammenhang mit den Primzahlen ergibt sich aus der Produktformel

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

Das Euler-Produkt

Der Zusammenhang mit den Primzahlen ergibt sich aus der Produktformel

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

Diese Formel kodiert in 'analytischer Form' den Fundamentalsatz der Arithmetik:

Jede natürliche Zahl n kann auf eindeutige Weise als ein Produkt von Primzahlen geschrieben werden:

$$n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}.$$

Neuer Beweis für Euklids Satz

Eulers Trick: betrachte

$$\log(\zeta(s))$$

Neuer Beweis für Euklids Satz

Eulers Trick: betrachte

$$\log(\zeta(s)) = -\sum_{p} \log(1 - p^{-s})$$

Neuer Beweis für Euklids Satz

Eulers Trick: betrachte

$$\log(\zeta(s)) = -\sum_p \log(1 - p^{-s}) \sim \sum_p \frac{1}{p^s}.$$

Neuer Beweis für Euklids Satz

Eulers Trick: betrachte

$$\log(\zeta(s)) = -\sum_p \log(1 - p^{-s}) \sim \sum_p \frac{1}{p^s}.$$

Da $\log(\zeta(s)) \to \infty$ für $s \to 1$, folgt die Divergenz der Reihe

$$\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots \to \infty.$$

Neuer Beweis für Euklids Satz

Eulers Trick: betrachte

$$\log(\zeta(s)) = -\sum_p \log(1 - p^{-s}) \sim \sum_p \frac{1}{p^s}.$$

Da $\log(\zeta(s)) \to \infty$ für $s \to 1$, folgt die Divergenz der Reihe

$$\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \ldots \to \infty.$$

Dies zeigt insbesondere, dass es unendlich viele Primzahlen gibt!

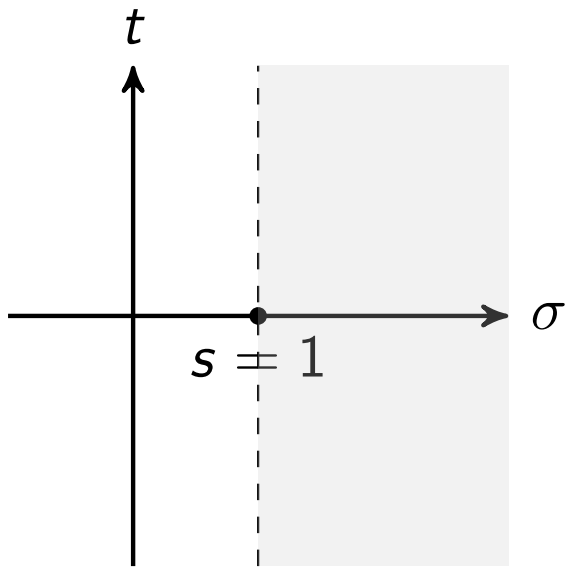
Die Riemannsche ζ-Funktion auf $\mathbb{C}$

Die Riemannsche ζ-Funktion auf $\mathbb{C}$

Riemann betrachtet die Funktion $\zeta(s)$ als Funktion eines *komplexen Parameters* $s = \sigma + i \cdot t$.

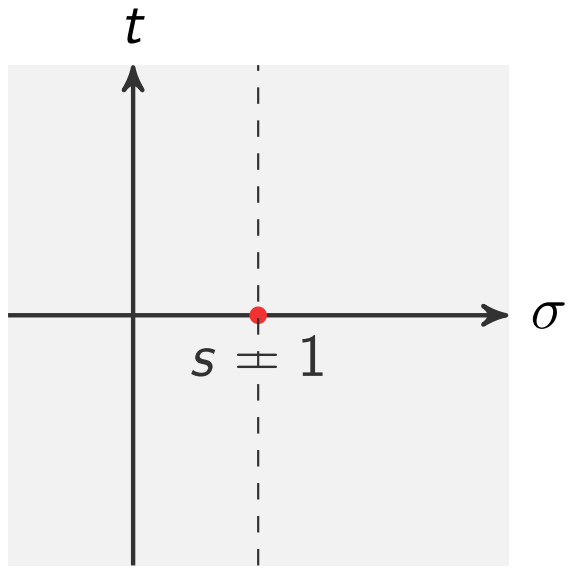
Die Riemannsche ζ-Funktion auf $\mathbb{C}$

Riemann betrachtet die Funktion $\zeta(s)$ als Funktion eines *komplexen Parameters* $s = \sigma + i \cdot t$. Die Reihe $\zeta(s) = 1 + 1/2^s + 1/3^s + \ldots$ ist dann für $\sigma > 1$ definiert:



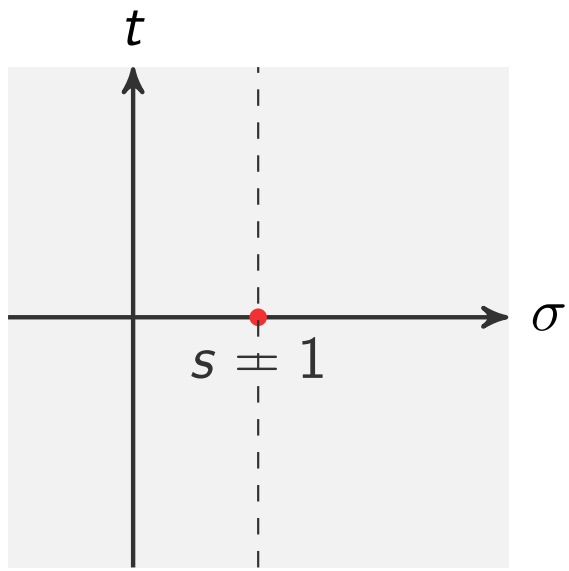
Die Riemannsche ζ-Funktion

Dann definiert Riemann eine *analytische Fortsetzung* von $\zeta(s)$ für alle komplexen Zahlen $s \neq 1$. Nur in $s = 1$ hat die Funktion eine *Polstelle*:



Die Riemannsche ζ-Funktion

Dann definiert Riemann eine *analytische Fortsetzung* von $\zeta(s)$ für alle komplexen Zahlen $s \neq 1$. Nur in $s = 1$ hat die Funktion eine *Polstelle*:



Es gilt z.B.

$$\zeta(-1) = 1 + 2 + 3 + \ldots = -\frac{1}{12}.$$

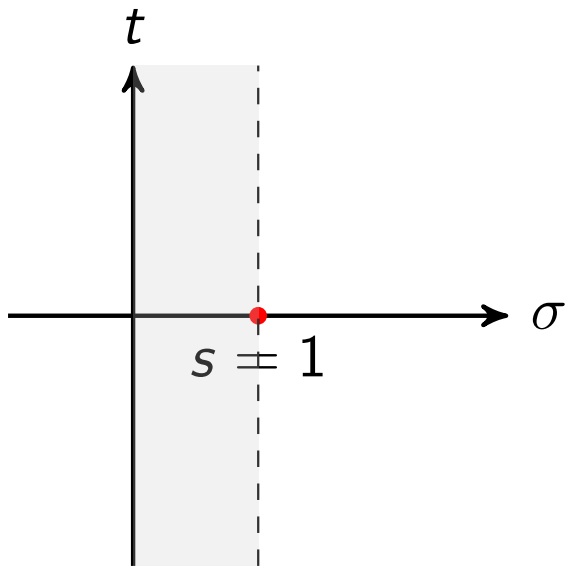
Beweis des Primzahlsatzes

Beweis des Primzahlsatzes

Aufbauend auf den Arbeiten von Riemann wurde der *Primzahlsatz* 1869 von Hadamard und de La Vallée Poussin bewiesen.

Beweis des Primzahlsatzes

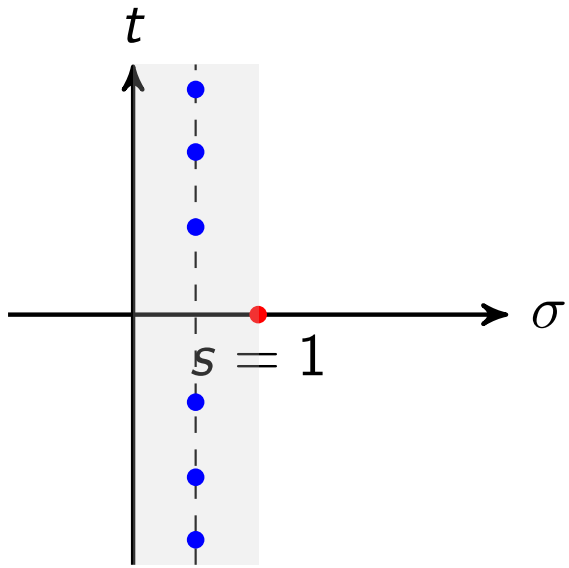
Aufbauend auf den Arbeiten von Riemann wurde der *Primzahlsatz* 1869 von Hadamard und de La Vallée Poussin bewiesen. Das zentrale Argument: die ζ-Funktion hat *keine* Nullstellen auf der Geraden $\sigma = 1$:



Die Riemannsche Vermutung

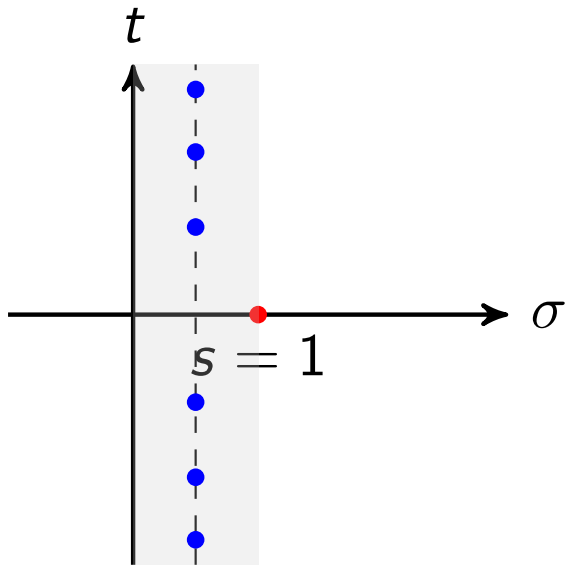
Die Riemannsche Vermutung

Die Riemannsche Vermutung: Alle (nichttrivialen) Nullstellen von $\zeta(s)$ liegen auf der Geraden $\sigma = 1/2$:



Die Riemannsche Vermutung

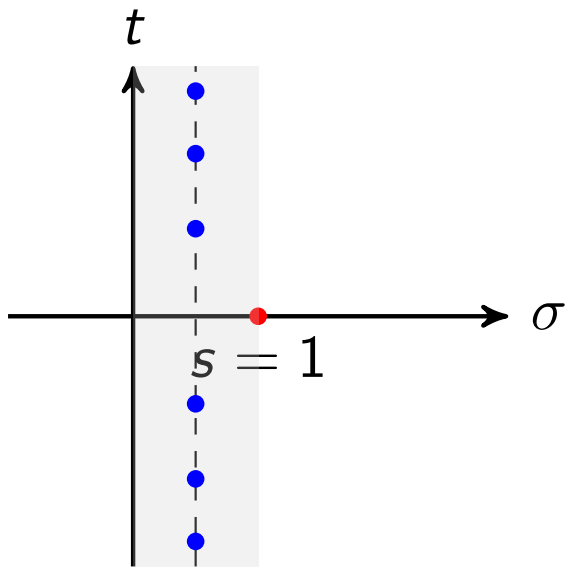
Die Riemannsche Vermutung: Alle (nichttrivialen) Nullstellen von $\zeta(s)$ liegen auf der Geraden $\sigma = 1/2$:



Es ist bekannt, dass es ∞ viele Nullstellen gibt, und dass die Vermutung für die ersten 10 Billionen von ihnen zutrifft.

Die Riemannsche Vermutung

Die Riemannsche Vermutung: Alle (nichttrivialen) Nullstellen von $\zeta(s)$ liegen auf der Geraden $\sigma = 1/2$:



Die die ersten Nullstellen sind $\rho = 1/2 + i \cdot \theta$, mit

$$\theta = \pm 14.134.., \quad \pm 21.022.., \quad \pm 25.010.., \ldots$$

Die Riemannsche Vermutung

Der Beweis des Primzahlsatzes zeigt: die Riemannsche Vermutung ist äquivalent zur (bestmöglichen) Abschätzung des Fehlerterms:

$$|\pi(x) - \mathrm{Li}(x)| = \mathcal{O}(\sqrt{x}\log(x)).$$

Die Riemannsche Vermutung

Der Beweis des Primzahlsatzes zeigt: die Riemannsche Vermutung ist äquivalent zur (bestmöglichen) Abschätzung des Fehlerterms:

$$|\pi(x) - \mathrm{Li}(x)| = \mathcal{O}(\sqrt{x}\log(x)).$$

Zitat von M.V. Berry (einem Physiker!):

> *..there is a sense in which we can give a one-line non-technical statement of the Riemann hypothesis: 'The primes have music in them!'*

Dies werden wir in der nächsten Vorlesung unter Beweis stellen..

Die Riemannsche Vermutung

Der Beweis des Primzahlsatzes zeigt: die Riemannsche Vermutung ist äquivalent zur (bestmöglichen) Abschätzung des Fehlerterms:

$$|\pi(x) - \mathrm{Li}(x)| = \mathcal{O}(\sqrt{x}\log(x)).$$

Zitat von M.V. Berry (einem Physiker!):

> *..there is a sense in which we can give a one-line non-technical statement of the Riemann hypothesis: 'The primes have music in them!'*

Dies werden wir in der nächsten Vorlesung unter Beweis stellen..

Vielen Dank für Ihre Aufmerksamkeit!