Zur Ästhetik mathematischer Beweisführung

Jens-Peter M. Zemke
zemke@tu-harburg.de

Institut für Numerische Simulation
Technische Universität Hamburg-Harburg

23.10.2006

TUHH
Technische Universität Hamburg-Harburg

Übersicht

Die Unendlichkeit der Menge der Primzahlen

- Beweis nach Euklid
- Beweis nach Christian Goldbach
- Beweis nach Leonhard Euler
- Beweis nach Harry Fürstenberg

Übersicht

Die Unendlichkeit der Menge der Primzahlen

- Beweis nach Euklid
- Beweis nach Christian Goldbach
- Beweis nach Leonhard Euler
- Beweis nach Harry Fürstenberg

Das Bertrandsche Postulat

- Beweis nach Paul Erdős

Übersicht

Übersicht

Vorwissen

Definition (natürliche Zahlen)

Die Menge $\mathbb{N} = \{1, 2, 3, ...\}$ der natürlichen Zahlen ist definiert durch die folgenden 5 Peano-Axiome:

$$1 \in \mathbb{N} \tag{1}$$

$$\forall\, n \in \mathbb{N}\ \exists!\ n' \in \mathbb{N} \tag{2}$$

$$\forall\, n \in \mathbb{N} : 1 \neq n' \tag{3}$$

$$\forall\, n, m \in \mathbb{N} : n' = m' \Rightarrow n = m \tag{4}$$

$$\forall\, M \subset \mathbb{N} : (1 \in M \wedge \forall\, n \in M \Rightarrow n' \in M) \Rightarrow M = \mathbb{N} \tag{5}$$

Vorwissen

Definition (natürliche Zahlen)

Die Menge $\mathbb{N} = \{1, 2, 3, ...\}$ der natürlichen Zahlen ist definiert durch die folgenden 5 Peano-Axiome:

$$1 \in \mathbb{N} \tag{1}$$

$$\forall\, n \in \mathbb{N}\ \exists!\ n' \in \mathbb{N} \tag{2}$$

$$\forall\, n \in \mathbb{N} : 1 \neq n' \tag{3}$$

$$\forall\, n, m \in \mathbb{N} : n' = m' \Rightarrow n = m \tag{4}$$

$$\forall\, M \subset \mathbb{N} : (1 \in M \wedge \forall\, n \in M \Rightarrow n' \in M) \Rightarrow M = \mathbb{N} \tag{5}$$

Bemerkung

Das Axiom (5) *ist das sogenannte Induktionsaxiom.*

Vorwissen

Definition (Addition natürlicher Zahlen)

Die Addition $(+)$ natürlicher Zahlen $m, n \in \mathbb{N}$ ist definiert durch

$$n + 1 := n', \qquad n + m' := (n + m)'. \tag{6}$$

Vorwissen

Definition (Addition natürlicher Zahlen)

Die Addition $(+)$ natürlicher Zahlen $m, n \in \mathbb{N}$ ist definiert durch

$$n + 1 := n', \qquad n + m' := (n + m)'. \tag{6}$$

Definition (Multiplikation natürlicher Zahlen)

Die Multiplikation $(\cdot)$ natürlicher Zahlen $m, n \in \mathbb{N}$ ist definiert durch

$$n \cdot 1 := n, \qquad n \cdot m' := (n \cdot m) + n. \tag{7}$$

Vorwissen

Definition (Addition natürlicher Zahlen)

Die Addition $(+)$ natürlicher Zahlen $m, n \in \mathbb{N}$ ist definiert durch

$$n + 1 := n', \qquad n + m' := (n + m)'. \tag{6}$$

Definition (Multiplikation natürlicher Zahlen)

Die Multiplikation $(\cdot)$ natürlicher Zahlen $m, n \in \mathbb{N}$ ist definiert durch

$$n \cdot 1 := n, \qquad n \cdot m' := (n \cdot m) + n. \tag{7}$$

Übungsaufgabe

Man beweise, dass die so definierten Operationen Addition und Multiplikation kommutativ, assoziativ und distributiv sind und mit den bereits "bekannten" Operationen übereinstimmen.

Vorwissen

Definition (Teilbarkeit)

Eine Zahl $n \in \mathbb{N}$ heisst teilbar durch $m \in \mathbb{N}$, in Zeichen $m|n$, wenn es ein $x \in \mathbb{N}$ gibt mit $mx = n$.

Vorwissen

Definition (Teilbarkeit)

Eine Zahl $n \in \mathbb{N}$ heisst teilbar durch $m \in \mathbb{N}$, in Zeichen $m|n$, wenn es ein $x \in \mathbb{N}$ gibt mit $mx = n$.

Definition (Primzahl)

Eine Primzahl $p \in \mathbb{N}$ ist eine Zahl, deren Menge der Teiler die Mächtigkeit zwei hat, in Zeichen

$$\mathbb{P} := \{p \in \mathbb{N} : \#\{x : x|p\} = 2\}, \tag{8}$$

wobei $\mathbb{P}$ im Folgenden die Menge der Primzahlen bezeichne.

Vorwissen

Definition (Teilbarkeit)

Eine Zahl $n \in \mathbb{N}$ heisst teilbar durch $m \in \mathbb{N}$, in Zeichen $m|n$, wenn es ein $x \in \mathbb{N}$ gibt mit $mx = n$.

Definition (Primzahl)

Eine Primzahl $p \in \mathbb{N}$ ist eine Zahl, deren Menge der Teiler die Mächtigkeit zwei hat, in Zeichen

$$\mathbb{P} := \{p \in \mathbb{N} : \#\{x : x|p\} = 2\}, \tag{8}$$

wobei $\mathbb{P}$ im Folgenden die Menge der Primzahlen bezeichne.

Bemerkung

Damit ist Eins keine Primzahl.

Vorwissen

Definition (Primteiler)

Ein Primteiler p einer Zahl n ist ein Teiler von n, der eine Primzahl ist.

Vorwissen

Definition (Primteiler)

Ein Primteiler p einer Zahl n ist ein Teiler von n, der eine Primzahl ist.

Theorem

Jede natürliche Zahl ungleich Eins hat Primteiler.

Vorwissen

Definition (Primteiler)

Ein Primteiler p einer Zahl n ist ein Teiler von n, der eine Primzahl ist.

Theorem

Jede natürliche Zahl ungleich Eins hat Primteiler.

Beweis.

Übungsaufgabe. □

Vorwissen

Definition (Primteiler)

Ein Primteiler p einer Zahl n ist ein Teiler von n, der eine Primzahl ist.

Theorem

Jede natürliche Zahl ungleich Eins hat Primteiler.

Beweis.

Übungsaufgabe. □

Theorem

Eins hat keine Primteiler.

Vorwissen

Definition (Primteiler)

Ein Primteiler p einer Zahl n ist ein Teiler von n, der eine Primzahl ist.

Theorem

Jede natürliche Zahl ungleich Eins hat Primteiler.

Beweis.

Übungsaufgabe. □

Theorem

Eins hat keine Primteiler.

Beweis.

Die Mächtigkeit der Menge der Teiler ist gleich Eins. □

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Angenommen, es gäbe endlich viele Primzahlen $p_1, \ldots, p_n$.

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Angenommen, es gäbe endlich viele Primzahlen $p_1, \ldots, p_n$. Dann hat die Zahl

$$c = \prod_{i=1}^{n} p_i + 1 \tag{9}$$

keine der Zahlen p_i als Teiler.

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Angenommen, es gäbe endlich viele Primzahlen $p_1, \ldots, p_n$. Dann hat die Zahl

$$c = \prod_{i=1}^{n} p_i + 1 \tag{9}$$

keine der Zahlen p_i als Teiler. Sei p ein Primteiler von c.

□

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Angenommen, es gäbe endlich viele Primzahlen $p_1, \ldots, p_n$. Dann hat die Zahl

$$c = \prod_{i=1}^{n} p_i + 1 \tag{9}$$

keine der Zahlen p_i als Teiler. Sei p ein Primteiler von c. Dann unterscheidet sich p von allen bisher bekannten p_i.

□

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Angenommen, es gäbe endlich viele Primzahlen $p_1, \ldots, p_n$. Dann hat die Zahl

$$c = \prod_{i=1}^{n} p_i + 1 \tag{9}$$

keine der Zahlen p_i als Teiler. Sei p ein Primteiler von c. Dann unterscheidet sich p von allen bisher bekannten p_i, da sonst $p|c$ und $p|\prod p_i$.

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Angenommen, es gäbe endlich viele Primzahlen $p_1, \ldots, p_n$. Dann hat die Zahl

$$c = \prod_{i=1}^{n} p_i + 1 \tag{9}$$

keine der Zahlen p_i als Teiler. Sei p ein Primteiler von c. Dann unterscheidet sich p von allen bisher bekannten p_i, da sonst $p|c$ und $p|\prod p_i$ und damit $p|1$, was laut Annahme nicht sein kann. □

Übersicht

Vorwissen

Definition (relativ prim)

Zwei Zahlen r und p heissen relativ prim (teilerfremd), wenn

$$(x|r) \wedge (x|p) \Rightarrow x = 1. \tag{10}$$

Vorwissen

Definition (relativ prim)

Zwei Zahlen r und p heissen relativ prim (teilerfremd), wenn

$$(x|r) \wedge (x|p) \Rightarrow x = 1. \tag{10}$$

Definition (Fermat-Zahlen)

Die n-te Fermat-Zahl F_n ist definiert durch $F_n := 2^{2^n} + 1$.

Vorwissen

Definition (relativ prim)

Zwei Zahlen r und p heissen relativ prim (teilerfremd), wenn

$$(x|r) \wedge (x|p) \Rightarrow x = 1. \tag{10}$$

Definition (Fermat-Zahlen)

Die n-te Fermat-Zahl F_n ist definiert durch $F_n := 2^{2^n} + 1$.

Lemma

Es gilt die Rekursion

$$\prod_{k=0}^{n-1} F_k = F_n - 2. \tag{11}$$

Vorwissen

Beweis durch Induktion und dritte binomische Formel.

Induktionsanfang $n = 1$:

Vorwissen

Beweis durch Induktion und dritte binomische Formel.

Induktionsanfang $n = 1$:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3, \qquad F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5, \tag{12}$$

$$F_0 = F_1 - 2. \tag{13}$$

Vorwissen

Beweis durch Induktion und dritte binomische Formel.

Induktionsanfang $n = 1$:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3, \qquad F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5, \tag{12}$$

$$F_0 = F_1 - 2. \tag{13}$$

Induktionsannahme: (11) sei korrekt für n.

Vorwissen

Beweis durch Induktion und dritte binomische Formel.

Induktionsanfang $n = 1$:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3, \qquad F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5, \tag{12}$$

$$F_0 = F_1 - 2. \tag{13}$$

Induktionsannahme: (11) sei korrekt für n.
Induktionsschritt $n \to n + 1$:

Vorwissen

Beweis durch Induktion und dritte binomische Formel.

Induktionsanfang $n = 1$:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3, \qquad F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5, \tag{12}$$

$$F_0 = F_1 - 2. \tag{13}$$

Induktionsannahme: (11) sei korrekt für n.
Induktionsschritt $n \to n + 1$:

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k \right) F_n = (F_n - 2)F_n \tag{14}$$

$$= (2^{2^n} + 1 - 2)(2^{2^n} + 1) = (2^{2^n} - 1)(2^{2^n} + 1) \tag{15}$$

$$= (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2. \tag{16}$$

Goldbach: Beweis durch Umformulierung

Der Beweis von Christian Goldbach (in einem Brief an Leonhard Euler 1730) erfolgt durch das Auffinden unendlich vieler jeweils relativ primer Zahlen.

Goldbach: Beweis durch Umformulierung

Der Beweis von Christian Goldbach (in einem Brief an Leonhard Euler 1730) erfolgt durch das Auffinden unendlich vieler jeweils relativ primer Zahlen.

Theorem

Je zwei Fermat-Zahlen sind relativ prim.

Goldbach: Beweis durch Umformulierung

Der Beweis von Christian Goldbach (in einem Brief an Leonhard Euler 1730) erfolgt durch das Auffinden unendlich vieler jeweils relativ primer Zahlen.

Theorem

Je zwei Fermat-Zahlen sind relativ prim.

Beweis durch Widerspruch.

Sei x ein Teiler von F_k und F_n, oBdA sei $k < n$.

Goldbach: Beweis durch Umformulierung

Der Beweis von Christian Goldbach (in einem Brief an Leonhard Euler 1730) erfolgt durch das Auffinden unendlich vieler jeweils relativ primer Zahlen.

Theorem

Je zwei Fermat-Zahlen sind relativ prim.

Beweis durch Widerspruch.

Sei x ein Teiler von F_k und F_n, oBdA sei $k < n$. Dann ist x auch ein Teiler von $\prod_{k=0}^{n-1} F_k$ und damit auch von 2.

□

Goldbach: Beweis durch Umformulierung

Der Beweis von Christian Goldbach (in einem Brief an Leonhard Euler 1730) erfolgt durch das Auffinden unendlich vieler jeweils relativ primer Zahlen.

Theorem

Je zwei Fermat-Zahlen sind relativ prim.

Beweis durch Widerspruch.

Sei x ein Teiler von F_k und F_n, oBdA sei $k < n$. Dann ist x auch ein Teiler von $\prod_{k=0}^{n-1} F_k$ und damit auch von 2. Da aber alle Fermat-Zahlen ungerade sind, folgt daraus sofort $x = 1$.

□

Goldbach: Beweis durch Umformulierung

Der Beweis von Christian Goldbach (in einem Brief an Leonhard Euler 1730) erfolgt durch das Auffinden unendlich vieler jeweils relativ primer Zahlen.

Theorem

Je zwei Fermat-Zahlen sind relativ prim.

Beweis durch Widerspruch.

Sei x ein Teiler von F_k und F_n, oBdA sei $k < n$. Dann ist x auch ein Teiler von $\prod_{k=0}^{n-1} F_k$ und damit auch von 2. Da aber alle Fermat-Zahlen ungerade sind, folgt daraus sofort $x = 1$, also sind F_k und F_n relativ prim.

□

Goldbach: Beweis durch Umformulierung

Der Beweis von Christian Goldbach (in einem Brief an Leonhard Euler 1730) erfolgt durch das Auffinden unendlich vieler jeweils relativ primer Zahlen.

Theorem

Je zwei Fermat-Zahlen sind relativ prim.

Beweis durch Widerspruch.

Sei x ein Teiler von F_k und F_n, oBdA sei $k < n$. Dann ist x auch ein Teiler von $\prod_{k=0}^{n-1} F_k$ und damit auch von 2. Da aber alle Fermat-Zahlen ungerade sind, folgt daraus sofort $x = 1$, also sind F_k und F_n relativ prim. Da F_k und F_n beliebig waren, ist der Satz bewiesen. □

Übersicht

Vorwissen

Theorem (Eindeutigkeit und Existenz der Primfaktorzerlegung)

Für alle $n \in \mathbb{N}$ existiert eine eindeutige Primfaktorzerlegung

$$n = \prod_{i=1}^{\ell} p_i^{k_i}, \quad p_1 < p_2 < \cdots < p_\ell \leqslant n, \tag{17}$$

wobei $p_i \in \mathbb{P}$ paarweise verschiedene endlich viele ($\ell \in \mathbb{N}_0$ Stück) Primzahlen sind, und $k_i \in \mathbb{N}$ deren Vielfachheit angibt. ($\prod_{i=1}^{0} a_i := 1$)

Vorwissen

Theorem (Eindeutigkeit und Existenz der Primfaktorzerlegung)

Für alle $n \in \mathbb{N}$ existiert eine eindeutige Primfaktorzerlegung

$$n = \prod_{i=1}^{\ell} p_i^{k_i}, \quad p_1 < p_2 < \cdots < p_\ell \leqslant n, \tag{17}$$

wobei $p_i \in \mathbb{P}$ paarweise verschiedene endlich viele ($\ell \in \mathbb{N}_0$ Stück) Primzahlen sind, und $k_i \in \mathbb{N}$ deren Vielfachheit angibt. ($\prod_{i=1}^{0} a_i := 1$)

Beweis.

Da jede Zahl Primteiler hat, und Primzahlen grösser gleich 2 sind, folgt, dass die rekursive Konstruktion der Primfaktorzerlegung durch sukzessives Teilen durch einen Primteiler terminiert. Das beweist die Existenz.

□

Vorwissen

Theorem (Eindeutigkeit und Existenz der Primfaktorzerlegung)

Für alle $n \in \mathbb{N}$ existiert eine eindeutige Primfaktorzerlegung

$$n = \prod_{i=1}^{\ell} p_i^{k_i}, \quad p_1 < p_2 < \cdots < p_\ell \leqslant n, \tag{17}$$

wobei $p_i \in \mathbb{P}$ paarweise verschiedene endlich viele ($\ell \in \mathbb{N}_0$ Stück) Primzahlen sind, und $k_i \in \mathbb{N}$ deren Vielfachheit angibt. ($\prod_{i=1}^{0} a_i := 1$)

Beweis.

Da jede Zahl Primteiler hat, und Primzahlen grösser gleich 2 sind, folgt, dass die rekursive Konstruktion der Primfaktorzerlegung durch sukzessives Teilen durch einen Primteiler terminiert. Das beweist die Existenz.

Die Eindeutigkeit folgt aus der Teilbarkeitsrelation, denn seien zwei Primfaktorzerlegungen $n = \prod_{i=1}^{\ell} p_i^{k_i} = \prod_{j=1}^{m} q_j^{k_j}$ gegeben, dann sind auch alle enthaltenen Primzahlpotenzen Teiler beider Zerlegungen. □

Vorwissen

Definition (natürlicher Logarithmus)

Der natürliche Logarithmus $\ln$ sei definiert über die Integration

$$\ln(x) := \int_1^x \frac{dt}{t}. \tag{18}$$

Vorwissen

Definition (natürlicher Logarithmus)

Der natürliche Logarithmus $\ln$ sei definiert über die Integration

$$\ln(x) := \int_1^x \frac{dt}{t}. \tag{18}$$

Bemerkung

Aus der Definition ist ersichtlich, dass $\ln(x)$ *unbeschränkt wächst, in Zeichen* $\lim_{x\to\infty} \ln(x) = \infty$.

Vorwissen

Definition (natürlicher Logarithmus)

Der natürliche Logarithmus $\ln$ sei definiert über die Integration

$$\ln(x) := \int_1^x \frac{dt}{t}. \tag{18}$$

Bemerkung

Aus der Definition ist ersichtlich, dass $\ln(x)$ *unbeschränkt wächst, in Zeichen* $\lim_{x\to\infty} \ln(x) = \infty$.

Definition (Primzahlzählfunktion)

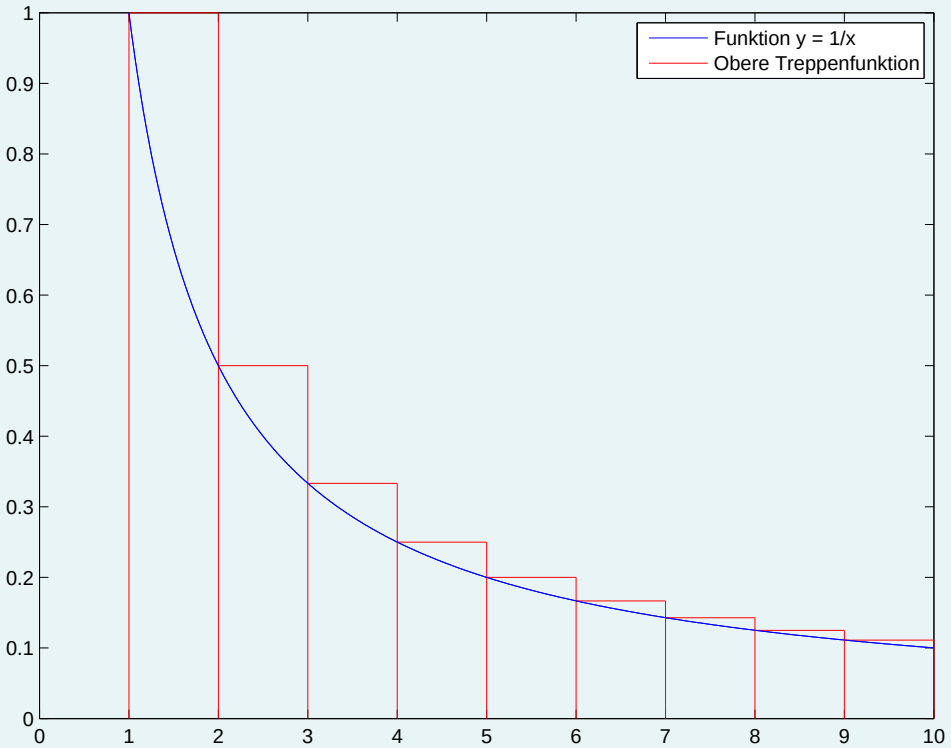
Wir definieren für alle $x \in \mathbb{R}$ die Primzahlzählfunktion π durch

$$\pi(x) := \#\{p \leqslant x \,:\, p \in \mathbb{P}\}. \tag{19}$$

Vorwissen

Bemerkung (zur Integration)

Obere Treppenfunktionen geben leicht berechenbare obere Schranken:



Vorwissen

Lemma

Die geometrische Reihe

$$G(q) := \sum_{k=0}^{\infty} q^k \tag{20}$$

konvergiert, wenn $|q| < 1$. *Der Grenzwert ist durch* $(1-q)^{-1}$ *gegeben.*

Vorwissen

Lemma

Die geometrische Reihe

$$G(q) := \sum_{k=0}^{\infty} q^k \tag{20}$$

konvergiert, wenn $|q| < 1$. *Der Grenzwert ist durch* $(1-q)^{-1}$ *gegeben.*

Beweis.

Die Reihe ist der Limes der endlichen Summe

$$G_n(q) := \sum_{k=0}^{n} q^k = 1 + q + q^2 + q^3 + \cdots + q^n. \tag{21}$$

Vorwissen

Lemma

Die geometrische Reihe

$$G(q) := \sum_{k=0}^{\infty} q^k \tag{20}$$

konvergiert, wenn $|q| < 1$. *Der Grenzwert ist durch* $(1-q)^{-1}$ *gegeben.*

Beweis.

Die Reihe ist der Limes der endlichen Summe

$$G_n(q) := \sum_{k=0}^{n} q^k = 1 + q + q^2 + q^3 + \cdots + q^n. \tag{21}$$

Nun gilt $(1-q)G_n(q) = G_n(q) - qG_n(q) = 1 - q^{n+1}$.

Vorwissen

Lemma

Die geometrische Reihe

$$G(q) := \sum_{k=0}^{\infty} q^k \tag{20}$$

konvergiert, wenn $|q| < 1$. *Der Grenzwert ist durch* $(1-q)^{-1}$ *gegeben.*

Beweis.

Die Reihe ist der Limes der endlichen Summe

$$G_n(q) := \sum_{k=0}^{n} q^k = 1 + q + q^2 + q^3 + \cdots + q^n. \tag{21}$$

Nun gilt $(1-q)G_n(q) = G_n(q) - qG_n(q) = 1 - q^{n+1}$, und da $|q| < 1$ folgt mit $\lim_{n\to\infty} q^{n+1} = 0$ das Lemma. □

Euler: Beweis mit Mitteln der Analysis

Theorem

Für alle $x \in \mathbb{R}_+$ *gilt* $\ln(x) \leqslant \pi(x) + 1$.

Euler: Beweis mit Mitteln der Analysis

Theorem

Für alle $x \in \mathbb{R}_+$ *gilt* $\ln(x) \leqslant \pi(x) + 1$.

Beweis.

Aus der Definition des Logarithmus folgt mit einer oberen Treppenfunktion

$$\ln(x) \leqslant 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \leqslant \sum{}' \frac{1}{m}, \quad n \leqslant x < n+1, \tag{22}$$

wobei die Summierung über alle $m \in \mathbb{N}$ *erfolgt, so dass nur Primfaktoren* $p \leqslant x$ *enthalten sind. Jedes solche* m *kann auf eindeutige Weise geschrieben werden als* $m = \prod_{p \leqslant x} p^{k_p}$*, damit gilt dann*

$$\ln(x) \leqslant \sum{}' \frac{1}{m} = \prod_{p \in \mathbb{P}, p \leqslant x} \left(\sum_{k \geqslant 0} \frac{1}{p^k} \right). \tag{23}$$

Euler: Beweis mit Mitteln der Analysis

Beweis.

Die innere Summe ist eine geometrische Reihe mit Faktor $1/p < 1$, woraus

$$\ln(x) \leqslant \prod{}' \frac{1}{1-\frac{1}{p}} = \prod{}' \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \tag{24}$$

folgt. Da trivialerweise $p_k \geqslant k+1$ gilt (wenn Primzahlen aufeinander folgen würden, wäre $p_k = k+1$, da Eins keine Primzahl ist), folgt weiter

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leqslant 1 + \frac{1}{k} = \frac{k+1}{k}. \tag{25}$$

Daraus folgt

$$\ln(x) \leqslant \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1. \tag{26}$$

□

Euler: Beweis mit Mitteln der Analysis

Theorem

Es gibt unendlich viele Primzahlen.

Euler: Beweis mit Mitteln der Analysis

Theorem

Es gibt unendlich viele Primzahlen.

Beweis.

Da der Logarithmus nicht beschränkt ist, folgt, dass auch $\pi(x)$ über alle Grenzen wächst, damit existieren unendlich viele Primzahlen. □

Übersicht

Vorwissen

Definition (Teilmenge)

Eine Teilmenge T einer Menge M ist eine Menge mit der Eigenschaft, dass jedes $x \in T$ auch Element von M ist.

Vorwissen

Definition (Teilmenge)

Eine Teilmenge T einer Menge M ist eine Menge mit der Eigenschaft, dass jedes $x \in T$ auch Element von M ist.

Definition (Potenzmenge)

Die Potenzmenge $\mathcal{P}M$ einer Menge M ist die Menge aller Teilmengen von M.

Vorwissen

Definition (Teilmenge)

Eine Teilmenge T einer Menge M ist eine Menge mit der Eigenschaft, dass jedes $x \in T$ auch Element von M ist.

Definition (Potenzmenge)

Die Potenzmenge $\mathcal{P}M$ einer Menge M ist die Menge aller Teilmengen von M.

Definition (Topologie)

Sei M eine Menge. Eine Topologie auf M ist ein System von Teilmengen $\mathcal{O} \subset \mathcal{P}M$ aus M, welches die folgenden Axiome erfüllt:

- $\emptyset \in \mathcal{O}, M \in \mathcal{O}$.
- $O_i \in \mathcal{O}, i \in I \Rightarrow \bigcup_{i \in I} O_i \in \mathcal{O}$.
- $O_1, O_2 \in \mathcal{O} \Rightarrow O_1 \cap O_2 \in \mathcal{O}$.

Vorwissen

Definition (offene Mengen)

Sei $\mathcal{O} = \{O\}$ eine Topologie auf M. Die Mengen O werden als offene Mengen bezeichnet.

Vorwissen

Definition (offene Mengen)

Sei $\mathcal{O} = \{O\}$ eine Topologie auf M. Die Mengen O werden als offene Mengen bezeichnet.

Definition (abgeschlossene Mengen)

Sei $\mathcal{O} = \{O\}$ eine Topologie auf M. Eine Menge A wird als abgeschlossen bezeichnet, wenn das Komplement $M \setminus A$ offen ist, also $M \setminus A \in \mathcal{O}$ gilt.

Vorwissen

Definition (offene Mengen)

Sei $\mathcal{O} = \{O\}$ eine Topologie auf M. Die Mengen O werden als offene Mengen bezeichnet.

Definition (abgeschlossene Mengen)

Sei $\mathcal{O} = \{O\}$ eine Topologie auf M. Eine Menge A wird als abgeschlossen bezeichnet, wenn das Komplement $M \setminus A$ offen ist, also $M \setminus A \in \mathcal{O}$ gilt.

Der kommende Beweis basiert auf der Konstruktion gewisser offener und abgeschlossener Teilmengen der Menge der ganzen Zahlen

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}. \tag{27}$$

Fürstenberg: Beweis mit Mitteln der Topologie

Theorem

Es gibt unendlich viele Primzahlen.

Fürstenberg: Beweis mit Mitteln der Topologie

Theorem

Es gibt unendlich viele Primzahlen.

Beweis.

Wir definieren erst einmal für alle $a, b \in \mathbb{Z}$, $b \neq 0$ *die Mengen*

$$N_{a,b} := \{a + nb : n \in \mathbb{Z}\} \tag{28}$$

Dann definieren wir uns geeignete offene Mengen. Die leere Menge sei in $\mathcal{O}$, *und alle Mengen* $O \subset \mathbb{Z}$ *mit*

$$\forall\, a \in O\ \exists\, b > 0 : N_{a,b} \subset O \tag{29}$$

seien enthalten in $\mathcal{O}$. *Dann definiert* $\mathcal{O}$ *eine Topologie auf* $\mathbb{Z}$.

Fürstenberg: Beweis mit Mitteln der Topologie

Beweis.

Dass $\mathcal{O}$ eine Topologie auf $\mathbb{Z}$ definiert, sieht man wie folgt.

Per definitionem ist die leere Menge ein Element von $\mathcal{O}$, und da alle Mengen $N_{a,b}$ Teilmengen von $\mathbb{Z}$ sind, ist auch $\mathbb{Z} \in \mathcal{O}$.

Die Vereinigung von offenen Menge ist entweder die leere Menge, also offen, oder enthält mit

$$a \in \bigcup_{i \in I} O_i \Rightarrow \exists\, k \in I \,:\, a \in O_k \tag{30}$$

eine Menge $N_{a,b}$, $a \in N_{a,b} \subset O_k$.

Der Durchschnitt zweier offener Mengen O_1 und O_2 ist entweder leer oder enthält mit $a \in O_1 \cap O_2$ mit $N_{a,b_1} \subset O_1$ und $N_{a,b_2} \subset O_2$ auch

$$a \in N_{a,b_1 b_2} \subset O_1 \cap O_2. \tag{31}$$

Fürstenberg: Beweis mit Mitteln der Topologie

Beweis.

Aus den Definitionen sieht man unmittelbar:
1) Jede nicht-leere offene Menge ist unendlich.
2) Jede Menge $N_{a,b}$ ist abgeschlossen.

1) ist trivial, 2) folgt aus $N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$.
Jede Zahl $n \neq -1, 1$ hat einen (vorzeichenbehafteten) Primteiler p, also gilt

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}. \tag{32}$$

Wenn $\mathbb{P}$ endlich wäre, wäre die rechte Seite der Gleichung eine endliche Vereinigung von abgeschlossenen Mengen und demnach abgeschlossen. Damit müsste das Komplement in $\mathbb{Z}$, also die Menge $\{-1, 1\}$, aber offen sein, im Gegensatz zur Beobachtung 1). □

Übersicht

Bertrands Postulat

Es gibt also unendlich viele Primzahlen. Bereits im Jahre 1845 postulierte Joseph Bertrand, dass zwischen n und $2n$ immer (mindestens) eine Primzahl liegen müsse, also

Bertrands Postulat

Es gibt also unendlich viele Primzahlen. Bereits im Jahre 1845 postulierte Joseph Bertrand, dass zwischen n und $2n$ immer (mindestens) eine Primzahl liegen müsse, also

Theorem (Bertrandsches Postulat)

Für alle $n \in \mathbb{N}$ gibt es eine Primzahl $p \in \mathbb{P}$ mit $n < p \leqslant 2n$.

Bertrands Postulat

Es gibt also unendlich viele Primzahlen. Bereits im Jahre 1845 postulierte Joseph Bertrand, dass zwischen n und $2n$ immer (mindestens) eine Primzahl liegen müsse, also

Theorem (Bertrandsches Postulat)

Für alle $n \in \mathbb{N}$ gibt es eine Primzahl $p \in \mathbb{P}$ mit $n < p \leqslant 2n$.

> *"Chebyschev said it, and I'll say it again: there's always a prime between n and $2n$."*

Bertrands Postulat

Es gibt also unendlich viele Primzahlen. Bereits im Jahre 1845 postulierte Joseph Bertrand, dass zwischen n und $2n$ immer (mindestens) eine Primzahl liegen müsse, also

Theorem (Bertrandsches Postulat)

Für alle $n \in \mathbb{N}$ gibt es eine Primzahl $p \in \mathbb{P}$ mit $n < p \leqslant 2n$.

> *"Chebyschev said it, and I'll say it again: there's always a prime between n and $2n$."*

Chebyschev bewies das Bertrandsche Postulat im Jahre 1850, allerdings auf ziemlich komplizierte Art und Weise. Der folgende, deutlich einfachere Beweis stammt von Paul Erdős aus dem Jahre 1932, als Erdős 19 Jahre alt war.

Vorwissen

Definition (n-Fakultät)

Die Fakultät der Zahl $n \in \mathbb{N}$ is rekursiv definiert als

$$1! := 1, \qquad (n')! = (n+1)! := (n!) \cdot n' = n! \cdot (n+1). \tag{33}$$

Vorwissen

Definition (n-Fakultät)

Die Fakultät der Zahl $n \in \mathbb{N}$ is rekursiv definiert als

$$1! := 1, \qquad (n')! = (n+1)! := (n!) \cdot n' = n! \cdot (n+1). \tag{33}$$

Definition (Binomialkoeffizienten)

Die Binomialkoeffizienten sind ganze Zahlen definiert durch

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}. \tag{34}$$

Vorwissen

Definition (n-Fakultät)

Die Fakultät der Zahl $n \in \mathbb{N}$ is rekursiv definiert als

$$1! := 1, \qquad (n')! = (n+1)! := (n!) \cdot n' = n! \cdot (n+1). \tag{33}$$

Definition (Binomialkoeffizienten)

Die Binomialkoeffizienten sind ganze Zahlen definiert durch

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}. \tag{34}$$

Definition (Gauß-Klammer)

Die (untere) Gauß-Klammer $\lfloor x \rfloor \in \mathbb{Z}$ von $x \in \mathbb{R}$ ist definiert durch $\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \leqslant x\}$.

Vorwissen

Theorem (Satz von Legendre)

Die Zahl $n!$ enthält den Primfaktor p genau

$$\sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{35}$$

Mal.

Vorwissen

Theorem (Satz von Legendre)

Die Zahl $n!$ enthält den Primfaktor p genau

$$\sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{35}$$

Mal.

Beweis.

Genau $\left\lfloor \frac{n}{p} \right\rfloor$ der Faktoren von $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ sind durch p teilbar, nämlich $p, 2p, \ldots$.

Vorwissen

Theorem (Satz von Legendre)

Die Zahl $n!$ enthält den Primfaktor p genau

$$\sum_{k \geqslant 1} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{35}$$

Mal.

Beweis.

Genau $\left\lfloor \frac{n}{p} \right\rfloor$ der Faktoren von $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ sind durch p teilbar, nämlich $p, 2p, \ldots$.

Genauso verfährt man nun für die höheren Potenzen p^k von p und deren Vielfache. Die Summe ist also im Übrigen sogar endlich. □

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Erdős Beweis basiert auf einer cleveren Abschätzung geschickt gewählter Binomialkoeffizienten. Er setzt sich aus fünf Unterabschnitten, hier präsentiert in der Form fünfer Lemmata, zusammen.

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Erdős Beweis basiert auf einer cleveren Abschätzung geschickt gewählter Binomialkoeffizienten. Er setzt sich aus fünf Unterabschnitten, hier präsentiert in der Form fünfer Lemmata, zusammen.

Lemma (Landau-Trick)

Bertrands Postulat gilt für $n \leqslant 4000$.

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Erdős Beweis basiert auf einer cleveren Abschätzung geschickt gewählter Binomialkoeffizienten. Er setzt sich aus fünf Unterabschnitten, hier präsentiert in der Form fünfer Lemmata, zusammen.

Lemma (Landau-Trick)

Bertrands Postulat gilt für $n \leqslant 4000$.

Beweis.

Man rechnet mehr oder minder schnell nach, dass $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001$ Primzahlen sind. Damit ist der Beweis dann reduziert auf simples (stupides) Nachprüfen. □

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

Für alle $x \in \mathbb{R}$, $x \geqslant 2$ gilt

$$\prod_{p \leqslant x} p \leqslant 4^{x-1}. \tag{36}$$

Dabei ist das Produkt, wie alle folgenden, nur über die Primzahlen p.

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

Für alle $x \in \mathbb{R}$, $x \geqslant 2$ gilt

$$\prod_{p \leqslant x} p \leqslant 4^{x-1}. \tag{36}$$

Dabei ist das Produkt, wie alle folgenden, nur über die Primzahlen p.

Beweis.

Für die größte Primzahl $q \leqslant x$ gilt

$$\prod_{p \leqslant x} p = \prod_{p \leqslant q} p, \quad \text{und} \quad 4^{q-1} \leqslant 4^{x-1}. \tag{37}$$

Also reicht es, den Beweis über die Primzahlen $q = x$ zu führen. Für $q = 2$ stimmt die Behauptung. Also bleiben die ungeraden Primzahlen $q = 2m + 1$.

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Beweis.

Der Beweis arbeitet mit Induktion. Wir zerlegen zuerst das Produkt,

$$\prod_{p \leqslant 2m+1} p = \prod_{p \leqslant m+1} p \prod_{m+1 < p \leqslant 2m+1} p. \tag{38}$$

Laut Induktionsannahme gilt

$$\prod_{p \leqslant m+1} p \leqslant 4^m. \tag{39}$$

Aus der Beobachtung, dass

$$\binom{2m+1}{m} = \binom{2m+1}{m+1} = \frac{(2m+1)!}{m!(m+1)!} \tag{40}$$

eine ganze Zahl ist, wobei die Primzahlen $m+1 < p \leqslant 2m+1$ *alle den Zähler,*

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Beweis.

aber nicht den Nenner teilen, folgt

$$\prod_{m+1<p\leqslant 2m+1} p \leqslant \binom{2m+1}{m}, \tag{41}$$

und mit

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}, \quad \binom{2m+1}{m} = \binom{2m+1}{m+1} \tag{42}$$

folgt weiter

$$\prod_{p\leqslant q} p = \prod_{p\leqslant 2m+1} p \leqslant 4^m \binom{2m+1}{m} \leqslant 4^m 2^{2m} = 4^{2m} = 4^{q-1}. \tag{43}$$

□

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

In der Primfaktorzerlegung des Binomialkoeffizienten $\binom{2n}{n}$, $n \geqslant 3$ sind Primzahlen $\sqrt{2n} < p \leqslant 2n$ höchstens einmal, Primzahlen $\frac{2}{3}n < p \leqslant n$ sogar keinmal enthalten. Die größte enthaltene Potenz von p ist kleiner gleich $2n$.

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

In der Primfaktorzerlegung des Binomialkoeffizienten $\binom{2n}{n}$, $n \geqslant 3$ sind Primzahlen $\sqrt{2n} < p \leqslant 2n$ höchstens einmal, Primzahlen $\frac{2}{3}n < p \leqslant n$ sogar keinmal enthalten. Die größte enthaltene Potenz von p ist kleiner gleich $2n$.

Beweis.

Nach dem Satz von Legendre enthält

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} \in \mathbb{N} \tag{44}$$

den Primfaktor p genau

$$\sum_{k \geqslant 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \tag{45}$$

Mal.

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Beweis.

Jeder Summand ist gleich Eins oder Null, weil

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) = 2 \tag{46}$$

gilt und der Ausdruck auf der linken Seite eine natürliche Zahl ist.

Wenn $p^k > 2n$ *ist, ist der Summand gleich Null. Damit folgt*

$$\sum_{k \geqslant 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right) \leqslant \max\{r \,:\, p^r \leqslant 2n\}. \tag{47}$$

Also ist die größte Potenz von p*, die* $\binom{2n}{n}$ *teilt, nicht größer als* $2n$*.*

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Beweis.

Wir hatten schon bewiesen: “Die größte Potenz von p, die $\binom{2n}{n}$ teilt, ist nicht größer als $2n$.”

Insbesondere sind demnach Primzahlen p, die größer sind als $\sqrt{2n}$, höchstens einmal enthalten.

Primzahlen p mit $\frac{2}{3}n < p \leqslant n$, $n \geqslant 3$ teilen $\binom{2n}{n}$ gar nicht. Für $3p > 2n$ und $n \geqslant 3$, damit $p \geqslant 3$ sind p und $2p$ die einzigen Vielfachen von p, die als Faktoren im Zähler von

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} \tag{48}$$

auftauchen, während zwei p-Faktoren im Nenner stehen. □

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

Es gilt

$$\frac{4^n}{2n} \leqslant \binom{2n}{n}. \tag{49}$$

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

Es gilt

$$\frac{4^n}{2n} \leqslant \binom{2n}{n}. \tag{49}$$

Beweis.

Für $n \geqslant 2$ folgt dies aus der Beobachtung, dass der mittlere Binomialkoeffizient die größte Zahl aus den $2n$ Zahlen

$$\binom{2n}{0} + \binom{2n}{2n}, \qquad \binom{2n}{j}, \quad j = 1, \ldots, 2n-1 \tag{50}$$

ist, und die Summe aller Binomialkoeffizienten . . .

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Beweis.

. . . und die Summe aller Binomialkoeffizienten

$$\sum_{j=0}^{2n} \binom{2n}{j} = 2^{2n} = 4^n \tag{51}$$

ist. Da der größte Wert größer oder gleich dem Mittelwert ist, folgt die Behauptung.

Für $n = 1$ folgt die Behauptung durch simples Nachrechnen:

$$\frac{4^1}{2 \cdot 1} = \frac{4}{2} = 2 \leqslant 2 = \frac{2}{1} = \frac{2!}{1!1!} = \binom{2 \cdot 1}{1}. \tag{52}$$

□

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

Es gilt

$$4^n \leqslant (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\leqslant \frac{2}{3}n} p \cdot \prod_{n<p\leqslant 2n} p, \qquad n \geqslant 3. \tag{53}$$

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Lemma

Es gilt

$$4^n \leqslant (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n} p \cdot \prod_{n<p\leqslant 2n} p, \qquad n \geqslant 3. \tag{53}$$

Beweis.

Zusammengefasst gilt nach bisherigen Lemmata

$$\frac{4^n}{2n} \leqslant \binom{2n}{n} \leqslant \prod_{p\leqslant\sqrt{2n}} 2n \cdot \prod_{\sqrt{2n}<p\leqslant\frac{2}{3}n} p \cdot \prod_{n<p\leqslant 2n} p, \qquad n \geqslant 3, \tag{54}$$

und damit, weil es nicht mehr als $\sqrt{2n}$ Primzahlen $p \leqslant \sqrt{2n}$ gibt, folgt die Behauptung. □

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Theorem (Bertrandsches Postulat)

Für alle $n \in \mathbb{N}$ gibt es eine Primzahl $p \in \mathbb{P}$ mit $n < p \leqslant 2n$.

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Theorem (Bertrandsches Postulat)

Für alle $n \in \mathbb{N}$ gibt es eine Primzahl $p \in \mathbb{P}$ mit $n < p \leqslant 2n$.

Beweis durch Widerspruch.

Wenn das Postulat inkorrekt, also

$$\prod_{n<p\leqslant 2n} p = \prod_{\emptyset} p = 1 \tag{55}$$

wäre, dann gälte sicherlich

$$4^n \leqslant (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n}<p\leqslant \frac{2}{3}n} p \leqslant (2n)^{1+\sqrt{2n}} 4^{\frac{2}{3}n}, \tag{56}$$

also auch

$$4^{\frac{1}{3}n} \leqslant (2n)^{1+\sqrt{2n}}. \tag{57}$$

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Beweis durch Widerspruch.

Das kann für $n > 4000$ *nicht stimmen, denn mittels Induktion folgt*

$$\alpha + 1 < 2^{\alpha}, \qquad \alpha \geqslant 2 \tag{58}$$

und so für $n \geqslant 32$, *damit* $\sqrt[6]{2n} \geqslant 2$,

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\left\lfloor \sqrt[6]{2n} \right\rfloor + 1\right)^6 < 2^{6\lfloor \sqrt[6]{2n} \rfloor} \leqslant 2^{6\sqrt[6]{2n}}, \tag{59}$$

und damit für $n \geqslant 41$, *so dass* $18 < 2\sqrt{2n}$ *gilt,*

$$4^n = 2^{2n} \leqslant (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}. \tag{60}$$

Erdős: Beweis mit Hilfe der Binomialkoeffizienten

Beweis durch Widerspruch.

Dieses liefert die Bedingung

$$(2n)^{1/3} < 20 \tag{61}$$

und damit

$$n < 4000. \tag{62}$$

Damit ist alles bewiesen, für $n \leqslant 4000$ mittels des Landau-Tricks, für $n > 4000$ durch Widerspruch. □

Übersicht

Der Fundamentalsatz der Algebra

Der in diesem Abschnitt behandelte Fundamentalsatz der Algebra wird in der folgenden Form behandelt:

Theorem (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle $z \in \mathbb{C}$.

Der Fundamentalsatz der Algebra

Der in diesem Abschnitt behandelte Fundamentalsatz der Algebra wird in der folgenden Form behandelt:

Theorem (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle $z \in \mathbb{C}$.

Manchmal ist es leichter, nur Polynome mit Koeffizienten aus den reellen Zahlen zu betrachten. Dieses stellt keine wesentliche Einschränkung dar:

Der Fundamentalsatz der Algebra

Der in diesem Abschnitt behandelte Fundamentalsatz der Algebra wird in der folgenden Form behandelt:

Theorem (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle $z \in \mathbb{C}$.

Manchmal ist es leichter, nur Polynome mit Koeffizienten aus den reellen Zahlen zu betrachten. Dieses stellt keine wesentliche Einschränkung dar:

Lemma

Ist c eine Nullstelle des reellen Polynomes $P(z) = \overline{p(\overline{z})}p(z)$, dann ist c oder $\overline{c}$ eine Nullstelle des komplexen Polynomes $p(z)$.

Vorwissen

Es folgen einige Resultate ohne Beweis.

Lemma (Dreiecksungleichung; Definitheit)

Der Absolutbetrag in $\mathbb{C}$ hat folgende Eigenschaften:

Dreiecksungleichung: *Für $z, w \in \mathbb{C}$ gilt* $||z| - |w|| \leqslant |z \pm w| \leqslant |z| + |w|$.

Definitheit: *Aus $|z| = 0$ folgt $z = 0$.*

Vorwissen

Es folgen einige Resultate ohne Beweis.

Lemma (Dreiecksungleichung; Definitheit)

Der Absolutbetrag in $\mathbb{C}$ hat folgende Eigenschaften:

Dreiecksungleichung: *Für $z, w \in \mathbb{C}$ gilt $||z| - |w|| \leqslant |z \pm w| \leqslant |z| + |w|$.*

Definitheit: *Aus $|z| = 0$ folgt $z = 0$.*

Definition (Polynom)

Ein Polynom vom Grad n mit Koeffizienten $a_i \in \mathbb{K}$, $i = 0, 1, \ldots, n$ in einem Körper $\mathbb{K}$ ist eine Funktion p der Gestalt

$$p(z) = \sum_{k=0}^{n} a_k z^k = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0, \quad a_n \neq 0. \tag{63}$$

Vorwissen

Definition (Stetigkeit)

Eine Funktion $f : D \to \mathbb{C}$ heißt stetig in z, wenn

$$\forall\, \epsilon > 0\, \exists\, \delta > 0 \,:\, |f(w) - f(z)| < \epsilon\, \forall\, |w - z| < \delta. \tag{64}$$

Eine Funktion heißt stetig, wenn sie in jedem Punkt des Definitionsbereiches stetig ist.

Vorwissen

Definition (Stetigkeit)

Eine Funktion $f : D \to \mathbb{C}$ heißt stetig in z, wenn

$$\forall\, \epsilon > 0\ \exists\, \delta > 0\ :\ |f(w) - f(z)| < \epsilon\ \forall\ |w - z| < \delta. \tag{64}$$

Eine Funktion heißt stetig, wenn sie in jedem Punkt des Definitionsbereiches stetig ist.

Theorem (Satz vom Minimum und Maximum: Weierstraß)

Jede stetige Funktion $f : K \to \mathbb{R}$ auf einem Kompaktum K nimmt ein Maximum und ein Minimum an, d.h., es gibt ein $\xi_1 \in K$ und ein $\xi_2 \in K$, so dass für alle $x \in K$

$$f(\xi_1) \leqslant f(x) \leqslant f(\xi_2) \tag{65}$$

gilt.

Vorwissen

Lemma (Polarkoordinaten)

Jede komplexe Zahl $c \neq 0$ läßt sich in eindeutiger Weise in sogenannten Polarkoordinaten (r, φ) darstellen gemäß

$$c = r(\cos(\varphi) + i\sin(\varphi)) = re^{i\varphi}, \quad \textit{wobei} \quad r = |c| \in \mathbb{R}_+, \varphi \in (-\pi, \pi]. \tag{66}$$

Vorwissen

Lemma (Polarkoordinaten)

Jede komplexe Zahl $c \neq 0$ läßt sich in eindeutiger Weise in sogenannten Polarkoordinaten (r, φ) darstellen gemäß

$$c = r(\cos(\varphi) + i\sin(\varphi)) = re^{i\varphi}, \quad \textit{wobei} \quad r = |c| \in \mathbb{R}_+, \varphi \in (-\pi, \pi]. \tag{66}$$

Beweis.

Dieses sieht man wie folgt. Es ist laut Lemma nur noch φ zu bestimmen. Sei

$$\frac{c}{|c|} = \xi + i\eta, \quad \xi, \eta \in \mathbb{R}. \tag{67}$$

Dann gilt $|\xi + i\eta|^2 = \xi^2 + \eta^2 = 1$. Setze nun $\alpha = \arccos(\xi)$. Dann gilt $\xi = \cos(\alpha)$ und zumindestens $\eta = \pm\sin(\alpha)$. Wir setzen $\varphi = \alpha$, wenn $\eta = \sin(\alpha)$ und $\varphi = -\alpha$ sonst. Es gilt $\cos(-\alpha) = \cos(\alpha)$ und $\sin(-\alpha) = -\sin(\alpha)$. □

Vorwissen

Lemma (Existenz von k-ten Wurzeln)

Die Gleichung $z^k = c$ mit beliebigem festen $c \in \mathbb{C}$ hat eine Lösung.

Vorwissen

Lemma (Existenz von k-ten Wurzeln)

Die Gleichung $z^k = c$ mit beliebigem festen $c \in \mathbb{C}$ hat eine Lösung.

Beweis.

Jede komplexe Zahl $c \neq 0$ läßt sich in Polarkoordinaten als $c = |c|e^{i\varphi}$ darstellen. Die Zahl

$$\sqrt[k]{c} := \sqrt[k]{|c|}e^{i\varphi/k} \tag{68}$$

leistet das Gewünschte. Wenn $c = 0$ ist 0 eine Lösung. □

Argand: Beweis durch Minimierung

Im Folgenden sei $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ mit $n > 1$.

Lemma (Existenz des Minimums)

Die Funktion $|p|$ nimmt auf $\mathbb{C}$ ein Minimum an.

Argand: Beweis durch Minimierung

Im Folgenden sei $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ mit $n > 1$.

Lemma (Existenz des Minimums)

Die Funktion $|p|$ nimmt auf $\mathbb{C}$ ein Minimum an.

Beweis.

Sei r definiert als $r := 1 + |a_{n-1}| + \cdots + |a_0|$. Dann gilt für $|z| \geqslant r \geqslant 1$

$$|p(z)| \geqslant |z|^n - \left(|a_{n-1}||z|^{n-1} + \cdots + |a_1||z| + |a_0|\right) \tag{69}$$

$$\geqslant |z|^n - \left(|a_{n-1}| + \cdots + |a_1| + |a_0|\right)|z|^{n-1} \tag{70}$$

$$\geqslant |z|^n - (r-1)|z|^{n-1} \geqslant |z|^n - (|z|-1)|z|^{n-1} = |z|^{n-1} \geqslant r^{n-1} \geqslant r. \tag{71}$$

Die Funktion $|p|$ nimmt auf der berandeten Kreisscheibe $\overline{K_r(0)}$ nach dem Satz von Weierstraß ein Minimum an. Da $|p(0)| = |a_0| < r$, ist dieses Minimum das globale Minimum auf ganz $\mathbb{C}$. □

Argand: Beweis durch Minimierung

Lemma (Negative Charakterisierung des Minimums)

Sei $|p(z_0)| \neq 0$. *Dann ist* z_0 *kein Minimum, d.h., es gibt ein* z_1 *mit*

$$|p(z_1)| < |p(z_0)|. \tag{72}$$

Argand: Beweis durch Minimierung

Lemma (Negative Charakterisierung des Minimums)

Sei $|p(z_0)| \neq 0$. Dann ist z_0 kein Minimum, d.h., es gibt ein z_1 mit

$$|p(z_1)| < |p(z_0)|. \tag{72}$$

Beweis.

Sei

$$s(w) := \frac{p(z_0 + w)}{p(z_0)} = 1 + bw^k + \cdots . \tag{73}$$

Sei β eine k-te Wurzel von $-b^{-1}$. Dann gilt

$$q(x) := s(\beta x) =: 1 - x^k + Q(x) =: 1 - x^k + x^{k+1}R(x). \tag{74}$$

Sei $C > 0$ eine obere Schranke für $|R|$ auf $\overline{K_1(0)}$. Dann gilt

$$|Q(x)| \leqslant C|x|^{k+1}, \quad |x| \leqslant 1, \tag{75}$$

Argand: Beweis durch Minimierung

Beweis.

und daher

$$|Q(x)| \leqslant |x|^k, \quad 0 < |x| < \min(1, C^{-1}). \tag{76}$$

Für reelle x_0 mit $0 < x_0 < \min(1, C^{-1})$ folgt nun

$$|q(x_0)| \leqslant 1 - x_0^k + |Q(x_0)| < 1 - x_0^k + x_0^k = 1. \tag{77}$$

Das bedeutet wiederum $|s(\beta x_0)| < 1$ und damit

$$|p(z_0 + \beta x_0)| < |p(z_0)|. \tag{78}$$

Setzen von $z_1 = z_0 + \beta x_0$ vollendet den Beweis. □

Argand: Beweis durch Minimierung

Theorem (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle $z \in \mathbb{C}$.

Argand: Beweis durch Minimierung

Theorem (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle $z \in \mathbb{C}$.

Beweis.

Nach dem ersten Lemma nimmt $|p(z)|$ ein Minimum an, nach dem zweiten Lemma geben Punkte $z_0 \in \mathbb{C}$ mit $|p(z_0)| \neq 0$ kein Minimum. Damit ist das Minimum gleich 0. Nach dem ersten Lemma existiert daher ein Punkt $z_1 \in \mathbb{C}$ mit $|p(z_1)| = 0$, also aufgrund der Definitheit des Absolutbetrages auch mit $p(z_1) = 0$. □

Übersicht

Vorwissen

Dieser Beweis liegt eigentlich eher jenseits der Möglichkeiten eines Studienanfängers. Wir geben daher nur eine Skizze, bestehend aus vier Vorraussetzungen in Form (meist hier nicht bewiesener) Lemmata und dem Hauptbeweis.

Vorwissen

Dieser Beweis liegt eigentlich eher jenseits der Möglichkeiten eines Studienanfängers. Wir geben daher nur eine Skizze, bestehend aus vier Vorraussetzungen in Form (meist hier nicht bewiesener) Lemmata und dem Hauptbeweis.

Lemma (Folgerung aus dem Zwischenwertsatz)

Jedes reelle Polynom ungeraden Grades besitzt eine Nullstelle in $\mathbb{R}$.

Vorwissen

Dieser Beweis liegt eigentlich eher jenseits der Möglichkeiten eines Studienanfängers. Wir geben daher nur eine Skizze, bestehend aus vier Vorraussetzungen in Form (meist hier nicht bewiesener) Lemmata und dem Hauptbeweis.

Lemma (Folgerung aus dem Zwischenwertsatz)

Jedes reelle Polynom ungeraden Grades besitzt eine Nullstelle in $\mathbb{R}$.

Lemma (Existenz des Zerfällungskörpers)

Zu jedem nichtkonstanten reellen Polynom gibt es einen Oberkörper $\mathbb{K}$ des Körpers $\mathbb{R}$, so dass p in Linearfaktoren zerfällt.

Vorwissen

Lemma (Hauptsatz über symmetrische Funktionen)

Es sei $\mathbb{K}$ ein Oberkörper von $\mathbb{R}$, es seien $\zeta_1, \ldots, \zeta_n$ Elemente aus $\mathbb{K}$, und es seien

$$\eta_k := \sum_{1 \leqslant \nu_1 < \cdots < \nu_k \leqslant n} \zeta_{\nu_1} \cdot \ldots \cdot \zeta_{\nu_k} \tag{79}$$

die "elementarsymmetrischen Funktionen" in $\zeta_1, \ldots, \zeta_n$. Dann gilt

$$\prod_{\nu=1}^{n} (x - \zeta_\nu) = x^n - \eta_1 x^{n-1} + \eta_2 x^{n-2} - \cdots + (-1)^n \eta_n. \tag{80}$$

Jedes in den ζ_i symmetrische Polynom (invariant unter Vertauschungen der ζ_i) ist ein reelles Polynom in den η_i.

Vorwissen

Lemma (Wurzeln von Parabeln)

Jedes quadratische komplexe Polynom zerfällt in $\mathbb{C}[z]$ in Linearfaktoren.

Vorwissen

Lemma (Wurzeln von Parabeln)

Jedes quadratische komplexe Polynom zerfällt in $\mathbb{C}[z]$ in Linearfaktoren.

Beweis.

OBdA nehmen wir an, dass

$$p(z) = z^2 - 2bz - c = (z-b)^2 - (b^2 + c), \quad b, c \in \mathbb{C}. \tag{81}$$

Dann sind unter Verwendung der beiden Zweige der Wurzel die Zahlen

$$z_\pm = b \pm \sqrt{b^2 + c} \in \mathbb{C} \tag{82}$$

Nullstellen, d.h., $p(z) = (z - z_+)(z - z_-)$. □

Laplace: Laplacescher Kunstgriff

Theorem (Fundamentalsatz der Algebra; reelle Version)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{R}$ hat eine Nullstelle $z \in \mathbb{C}$.

Laplace: Laplacescher Kunstgriff

Theorem (Fundamentalsatz der Algebra; reelle Version)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{R}$ hat eine Nullstelle $z \in \mathbb{C}$.

Beweis.

Sei $p = x^n - b_1 x^{n-1} + b_2 x^{n-2} - \cdots + (-1)^n b_n$ vom Grad n. Setze $n = 2^k q$, wobei $q \in \mathbb{N}$ ungerade ist. Der Beweis basiert auf Induktion nach k.

Der Fall $k = 0$ folgt nach dem ersten Lemma. Sei also $k \geqslant 1$. Nach dem zweiten Lemma gibt es einen Oberkörper $\mathbb{K}$ von $\mathbb{R}$ und Elemente $\zeta_i \in \mathbb{K}$, so dass

$$p(z) = \prod_{i=1}^{n} (z - \zeta_i) \tag{83}$$

gilt.

Laplace: Laplacescher Kunstgriff

Beweis.

Definiere für jede reelle Zahl t

$$L_t(x) := \prod_{1 \leqslant \mu < \nu \leqslant n} (x - \zeta_\mu - \zeta_\nu - t\zeta_\mu\zeta_\nu) \in \mathbb{K}[x]. \tag{84}$$

Entwickelt man nach Potenzen von x*, so sind alle Koeffizienten reelle symmetrische Polynome in* $\zeta_1, \ldots, \zeta_n$*, denn* L_t *ist per definitionem unter Permutationen der* ζ_i *invariant.*

Damit sind die Koeffizienten nach dem dritten Lemma reelle Polynome in den elementarsymmetrischen Funktionen der ζ_i*, d.h., den* b_i*. Daher ist* $L_t \in \mathbb{R}[x]$ *für alle* $t \in \mathbb{R}$*.*

Da p *den Grad* $n = 2^k q$ *hatte, hat* L_t *den Grad* $\frac{1}{2}n(n-1) = 2^{k-1}q(2^k q - 1)$*.*

Laplace: Laplacescher Kunstgriff

Beweis.

Da L_t den Grad $2^{k-1}q(2^kq-1)$ hat und mit q wegen $k \geqslant 1$ auch $q(2^kq-1)$ ungerade ist, hat L_t nach Induktionsannahme für alle $t \in \mathbb{R}$ eine Nullstelle in $\mathbb{C}$.

Also gibt es auf Grund der Produktform von L_t für alle $t \in \mathbb{R}$ Indices $\mu < \nu$, so dass

$$\zeta_\mu + \zeta_\nu + t\zeta_\mu\zeta_\nu \in \mathbb{C}. \tag{85}$$

Da es nur $\frac{1}{2}n(n-1)$ Indexpaare mit $1 \leqslant \mu < \nu \leqslant n$ aber unendlich viele $t \in \mathbb{R}$ gibt, lassen sich $r, s \in \mathbb{R}$ mit $r \neq s$ und κ, λ mit $1 \leqslant \kappa < \lambda \leqslant n$ finden mit

$$\zeta_\kappa + \zeta_\lambda + r\zeta_\kappa\zeta_\lambda \in \mathbb{C}, \tag{86}$$

$$\zeta_\kappa + \zeta_\lambda + s\zeta_\kappa\zeta_\lambda \in \mathbb{C}. \tag{87}$$

Laplace: Laplacescher Kunstgriff

Beweis.

Aus $r \neq s$ folgt

$$u := \zeta_\kappa \zeta_\lambda \in \mathbb{C}, \quad v := \zeta_\kappa + \zeta_\lambda \in \mathbb{C}. \tag{88}$$

Damit sind ζ_κ und ζ_λ die Nullstellen von

$$z^2 - vz + u \in \mathbb{C}[z], \tag{89}$$

und nach dem vierten Lemma folgt demnach $\zeta_\kappa, \zeta_\lambda \in \mathbb{C}$. □


Königsberger
Analysis 1. Zweite Auflage.
Springer, Berlin, 1992.


Martin Aigner, Günter M. Ziegler
Das BUCH der Beweise.
Springer, Berlin, 2002.


Ebbinghaus et al.
Zahlen. Dritte Auflage.
Springer, Berlin, 1992.