

Das BUCH der Beweise
Unendlich viele Primzahlen

Heike Birsul

Dezember 2021

Inhaltsverzeichnis

1 Einführung	3
1.1 Wiederholung von Definitionen	3
2 Euklids Beweis	3
2.1 Euklid von Alexandria (Quelle: [Wal17], Bd. 2 S.84)	3
2.2 Vorüberlegung	4
2.3 Der Beweis von Euklid [AZH15], S.3	4
3 Goldbachs Beweis	4
3.1 Christian Goldbach Quelle: [Wal17], Bd.2 S. 308	4
3.2 Fermat-Zahlen	4
3.3 Beweis von Goldbach Vgl. [AZH15], S.3-4	5
4 Eulers Beweis	6
4.1 Leonhard Euler vgl. [Wal17], Bd.2 S.87-88	6
4.2 Beweis von Leonhard Euler vgl. [AZH15], S. 4	7
5 Erdös' Beweis	10
5.1 Paul Erdös (Vgl. [Wal17], Bd.2 S.65-66)	10
5.2 Beweis von Paul Erdös vgl. [AZH15], S.5-6	10

1 Einführung

Im folgenden werden vier der sechs Beweise aus dem BUCH der Beweise, Kapitel 1, von Martin Aigner und Günter M. Ziegler ([AZH15]) zur Behauptung, dass es unendlich viele Primzahlen gibt, vorgestellt.

1.1 Wiederholung von Definitionen

Definition (Teiler). Seien $a, b \in \mathbb{N}$. Man sagt a teilt b , wenn es eine Zahl $k \in \mathbb{N}$ gibt, für die gilt: $b = k \cdot a$.
 a ist dann *Teiler* von b .

Definition (Primzahl). Eine natürliche Zahl $p \in \mathbb{N}$ heißt *Primzahl*, wenn sie nur die 1 und sich selbst als Teiler hat. Sei \mathbb{P} die Menge aller Primzahlen.

Satz (Fundamentalsatz der elementaren Zahlentheorie). Seien $p_1, \dots, p_r \in \mathbb{P}$ paarweise verschieden $r \in \mathbb{N}$ und $a_1, \dots, a_r \in \mathbb{N}$. Jede natürliche Zahl n besitzt eine eindeutige Darstellung der Form (heißt Primfaktorzerlegung):

$$n = p_1^{a_1} \cdot \dots \cdot p_r^{a_r}$$

Beweis. Vgl. [KP13], S. 25

□

2 Euklids Beweis

2.1 Euklid von Alexandria (Quelle: [Wal17], Bd. 2 S.84)



Abbildung 1: Darstellung Euklids im Oxford University Museum.

Euklid von Alexandria lebte um 300 V. Chr. Es ist fast nichts über sein Leben bekannt. Die meisten Vermutungen über sein Leben sind Rückschlüsse, die man über Anekdoten und seine Schriften schloss. Vermutlich wurde er in Athen geboren und lehrte im Museion in Alexandria.

2.2 Vorüberlegung

Hilfssatz. *Eine natürliche Zahl a und $a + 1$ sind teilerfremd. (Sie haben nur den gemeinsamen Teiler 1.)*

Beweis. Angenommen $b \in \mathbb{N}, b \neq 1$ und b teilt a und $a + 1$.
 Dann existieren $k, l \in \mathbb{N}$ mit $a = kb$ (1) und $a + 1 = lb$ (2)
 Zieht man (1) von (2) ab, so folgt:

$$1 = lb - kb$$

Mit dem Distributivgesetz und weil $k, l \in \mathbb{N}$ folgt direkt: $b = 1$. □

2.3 Der Beweis von Euklid [AZH15], S.3

Satz. *Es gibt unendlich viele Primzahlen.*

Beweis. Sei $\{p_1, p_2, \dots, p_r\}$, $r \in \mathbb{N}$ eine beliebige *endliche* Menge von Primzahlen. Sei $n = p_1 \cdot p_2 \cdot \dots \cdot p_r + 1$ und sei p ein Primteiler von n .
 Mit dem Hilfssatz folgt: $p_1 \cdot p_2 \cdot \dots \cdot p_r$ und n sind teilerfremd.
 Also gilt $p \notin \{p_1, p_2, \dots, p_r\}$
 \Rightarrow Eine endliche Menge kann nicht alle Primzahlen enthalten. □

3 Goldbachs Beweis

3.1 Christian Goldbach Quelle: [Wal17], Bd.2 S. 308

Der Beweis aus einem Brief von Goldbach an Leonard Euler (1730). (Vgl. [AZH15], S.3) Geboren wurde Goldbach im Jahr 1690 in Königsberg (Kalininograd), er starb 1764 in Moskau.

1725 wurde er Professor für Geschichte und Mathematik in St. Petersburg. Er lieferte wichtige Beiträge zur Zahlentheorie. (Viele in Korrespondenz mit Euler.) Unter anderem stellte er die Goldbach-Probleme auf, welche zum Teil heute noch nicht bewiesen, bzw. widerlegt wurden.

3.2 Fermat-Zahlen

Definition (Fermat-Zahlen vgl. [AZH15], S.3). Sei $n \in \mathbb{N} \cup \{0\}$. Dann heißen:

$$F_n = 2^{2^n} + 1$$

Fermat-Zahlen .

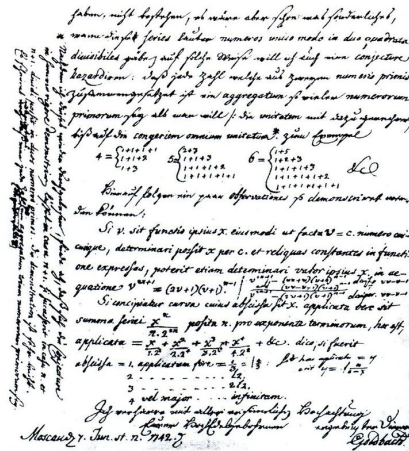


Abbildung 2: Brief von Goldbach an Euler aus dem Jahr 1742.

Beispiel. Die ersten fünf Fermat-Zahlen:

$$\begin{aligned}
 F_0 &= 3 \\
 F_1 &= 5 \\
 F_2 &= 17 \\
 F_3 &= 257 \\
 F_4 &= 65537 \\
 F_5 &= 641 \cdot 6700417
 \end{aligned}$$

3.3 Beweis von Goldbach vgl. [AZH15], S.3-4

Der Beweis nutzt die folgenden Eigenschaften:

- Es gibt unendlich viele Fermat-Zahlen. (Klar, per Definition)
- Je zwei Fermatzahlen sind relativ prim (teilerfremd) (noch zu zeigen)
- Wenn beides stimmt, gibt es unendlich viele Teiler, also auch unendlich viele Primzahlen.

Um zu zeigen, dass je zwei Fermatzahlen teilerfremd sind, zeigen wir die folgende Rekursion:

Hilfssatz. Für $n \in \mathbb{N}$ und $n \geq 1$ gilt:

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

Stimmt diese, so folgt, dass falls m gemeinsamer Teiler von $\prod_{k=0}^{n-1} F_k$ und F_n ist, so ist $m = 1$ oder $m = 2$. Da alle Fermat-Zahlen per Definition ungerade sind, folgt somit, dass $m = 2$ kein Teiler sein kann. Also gilt, dass nur $m = 1$ gemeinsamer Teiler von $\prod_{k=0}^{n-1} F_k$ und F_n ist.

Beweis. Beweis via Induktion über n :
(Induktionsanfang:) Für $n = 1$ gilt:

$$\prod_{k=0}^0 F_k = F_0 = 3$$

$$F_1 - 2 = 5 - 2 = 3$$

Damit stimmt die Behauptung für den Induktionsanfang.
(Induktionsbehauptung) Für $n \in \mathbb{N}$ gilt:

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

(Induktionsschritt): Zeige, dass, wenn die Induktionsbehauptung gilt, sie auch für $n + 1$ gilt:

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

$$\stackrel{Def. F_n}{=} (2^{2^n} - 1) (2^{2^n} + 1)$$

$$\stackrel{Bin. F.}{=} 2^{2^{n+1}} - 1$$

$$\stackrel{Def. F_n}{=} F_{n+1} - 2$$

□

Da es unendlich viele Fermat-Zahlen gibt und je zwei Fermat-Zahlen relativ prim sind, gibt es also unendlich viele Primzahlen. □

4 Eulers Beweis

4.1 Leonhard Euler vgl. [Wal17], Bd.2 S.87-88

Leonhard Euler war einer der einflussreichsten Mathematiker des 18. Jahrhunderts. Geboren wurde er 1707 in Basel und er starb 1783 in St. Petersburg. Große Teile seines Lebens verbrachte Euler in St. Petersburg und Berlin. Besonders viel trug er zur Analysis bei und auch der folgende Beweis bedient sich dieser.



Abbildung 3: Gemälde von Jakob Emanuel Handmann, 1756

4.2 Beweis von Leonhard Euler vgl. [AZH15], S. 4

Zur Übersicht, lässt sich der Ablauf des Beweises wie folgt beschreiben:

- Für den Beweis wird eine Funktion $\pi(x)$ definiert, die die Primzahlen kleiner x zählt.
- Wir schätzen $\pi(x)$ mithilfe der Logarithmus-Funktion ab, nämlich: $\log x \leq \pi(x) + 1$
- Da $\log x$ unbeschränkt ist, folgt dass $\pi(x)$ unbeschränkt ist.

Zunächst machen wir die folgenden Vorüberlegungen:

- $\log x = \int_1^x \frac{1}{t} dt$, denn $\int_1^x \frac{1}{t} dt = \log x - \log 1 = \log x$
 $\underbrace{\log 1}_{=0}$
- Wir können $\log x$ mit der oberen Treppenfunktion von $\frac{1}{t}$ abschätzen (Vgl. 4)

Die graue Fläche lässt sich wie folgt berechnen (Jede Stufe ist 1 breit)

$$\begin{aligned} &\text{Graue Fläche} \\ &= 1 \cdot \frac{1}{1} + 1 \cdot \frac{1}{2} + \dots + 1 \cdot \frac{1}{n-1} + 1 \cdot \frac{1}{n} = \sum_{l=1}^n \frac{1}{l} \end{aligned}$$

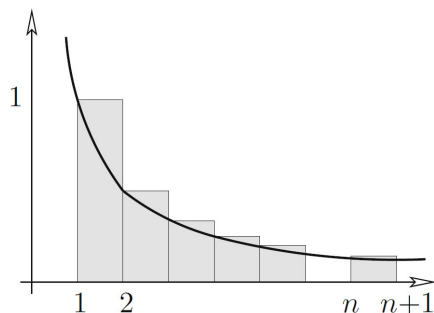
Also folgt: $\log x \leq \sum_{l=1}^n \frac{1}{l}$.

Definition.

$$\sum' \frac{1}{m}$$

sei die Summe aller $m \in \mathbb{N}$, die nur Primfaktoren $p \leq x$ enthalten.

Abbildung 4: Obere Treppenfunktion von $\frac{1}{t}$ für $n \leq x \leq n+1$:



Eine obere Treppenfunktion für
 $f(t) = \frac{1}{t}$

Da es unendlich viele solcher m gibt, gilt:

$$\log x \leq \sum_{l=1}^n \frac{1}{l} \leq \sum' \frac{1}{m}$$

Wegen des Fundamentalsatzes der elementaren Zahlentheorie, kann man m wie folgt schreiben:

$$m = \prod_{p \leq x} p^{k_p}$$

Also:

$$\sum' \frac{1}{m} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

Es stellt sich die Frage, warum die letzte Gleichheit gilt.

Betrachte beispielsweise die folgenden Potenzreihen und ihr Produkt (Das wäre zum Beispiel $\sum' \frac{1}{m}$ für $x = 3$):

$$\begin{aligned} \sum_{k=0} \frac{1}{2^k} &= \frac{1}{1} + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots \\ \sum_{k=0} \frac{1}{3^k} &= \frac{1}{1} + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \dots \\ \sum_{k=0} \frac{1}{2^k} \cdot \sum_{k=0} \frac{1}{3^k} &= \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots \right) \cdot \left(\frac{1}{1} + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \dots \right) \end{aligned}$$

Multipliziert man die Klammern aus, so kann man sich vorstellen, dass jeder Summand der ersten Reihe ($p = 2$) mit jedem Summanden der zweiten Reihe

($p = 3$) einmal kombiniert wird und auf diese Weise alle gesuchten m aufsummiert werden.

Die innere Summe von

$$\sum' \frac{1}{m} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

ist eine geometrische Reihe. Also:

$$\log x \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1} \quad (1)$$

Nun wird wie angekündigt $\pi(x)$ als die Anzahl aller Primzahlen kleiner als x definiert:

$$\pi(x) := \#\{p \leq x : p \in \mathbb{P}\} \quad (2)$$

Und die Menge \mathbb{P} der Primzahlen in aufsteigender Reihenfolge durchnummeriert.

$$\mathbb{P} = \{p_1, p_2, p_3, \dots\} \quad (3)$$

Durch letzteres gilt offensichtlich: $p_k \geq k + 1$

Beispiel. Für die ersten drei p_k gilt:

$$p_1 = 2 \text{ und } k + 1 = 1 + 1 = 2$$

$$p_2 = 3 \text{ und } k + 1 = 2 + 1 = 3$$

$$p_3 = 5 \text{ und } k + 1 = 3 + 1 = 4 < 5$$

Mit (2) und (3) gilt:

$$\log x \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k-1}$$

Aus $p_k \geq k + 1$ für alle $k \in \mathbb{N}$ folgt:

$$\frac{p_k}{p_k-1} = \frac{p_k-1+1}{p_k-1} = \frac{p_k-1}{p_k-1} + \frac{1}{p_k-1} = 1 + \frac{1}{p_k-1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

Woraus wiederum folgt:

$$\log x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$$

Zusammenfassend:

- $\pi(x)$ zählt die Anzahl der Primzahlen kleiner x .
- Wir haben gezeigt $\log x \leq \pi(x) + 1$.

- Es ist bekannt, dass $\log x$ unbeschränkt ist.
- $\Rightarrow \pi(x)$ ist ebenso unbeschränkt.
- \Rightarrow Es gibt unendlich viele Primzahlen.

□

5 Erdős' Beweis

5.1 Paul Erdős (Vgl. [Wal17], Bd.2 S.65-66)

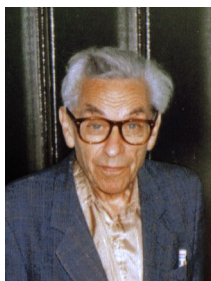


Abbildung 5: CC-BY Kmhmh (wikipedia-user)

Paul Erdős wurde 1913 in Budapest geboren und ist 1996 in Warschau gestorben. Er reiste während seines Lebens viel und blieb selten länger als ein paar Monate an einer Institution, um zu lehren. Er arbeitete auf diese Weise mit rund 450 Mathematikern und Mathematikerinnen zusammen und verfasste über 1500 Arbeiten. Auch die Idee des Buches kam mit von ihm. (Vgl. [AZH15], S. V)

5.2 Beweis von Paul Erdős vgl. [AZH15], S.5-6

- Es wird gezeigt: $\sum_{p \in \mathbb{P}} \frac{1}{p}$ divergiert.
- \Rightarrow Es gibt unendlich viele Primzahlen.
- Zur Erinnerung: Eine Reihe divergiert, wenn sie keinen Grenzwert besitzt.

Sei $(p_n)_{n \in \mathbb{N}}$ die Folge der Primzahlen in aufsteigender Ordnung. Angenommen, die Reihe $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert, dann folgt, dass es eine natürliche Zahl k gibt, für die gilt:

$$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2} \quad (4)$$

Außerdem könnte dann gefolgert werden, dass die Menge der Primzahlen endlich ist.

Bemerkung. Die Reihe ähnelt der harmonischen Reihe, ausgenommen von den $\frac{1}{n}$, $n \in \mathbb{N}$, die keine reziproken Primzahlen sind. Die harmonische Reihe divergiert im Unendlichen). (vgl. [For16], S. 71)

Definition (Kleine Primzahlen). Für obiges k gilt, dass p_1, \dots, p_k *kleine Primzahlen* sind.

Definition (Große Primzahlen). Für obiges k gilt, dass p_{k+1}, \dots *große Primzahlen* sind.

Für jede beliebige natürliche Zahl N gilt, wegen (4):

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2} \quad (5)$$

Sei N_b die Anzahl der positiven ganzen Zahlen $n \leq N$, die durch mind eine große Primzahl teilbar ist.

Sei N_s die Anzahl der pos. ganzen Zahlen $n \leq N$, die durch nur kleine Primzahlen teilbar ist.

Es ist klar, dass $N_b + N_s = N$ gilt, denn wir zählen auf diese Weise alle Zahlen kleiner oder gleich N .

Es wird gezeigt werden: Mit dieser Definition großer und kleiner Primzahlen, die von der Konvergenz der Reihe der reziproken Primzahlen abhängt, gilt: $N_b + N_s < N$

Es ist sinnvoll mit dem Abschätzen von N_b zu beginnen:

$\lfloor \frac{N}{p_i} \rfloor$ zählt die positiven ganzen Zahlen, die Vielfache von p_i sind.

Beispiel. $N = 13$ und $p_i = 3 \Rightarrow \lfloor \frac{N}{p_i} \rfloor = 4$
 $\Rightarrow 4$ *Vielfache, nämlich 3, 6, 9, 12*

Mit (5) folgt also:

$$N_b = \sum_{i \geq k+1} \lfloor \frac{N}{p_i} \rfloor < \frac{N}{2} \quad (6)$$

Als nächstes wird N_s abgeschätzt:

Schreibe jede natürliche Zahl $n \leq N$, die nur kleine Primzahlen besitzt, in der Form: $n = a_n b_n^2$, wobei a_n der quadratfreie Teil ist.

a_n ist Produkt *verschiedener* kleiner Primzahlen (Fundamentalsatz).

Laut Annahme, gibt es nur k kleine Primzahlen.

Daraus folgt, dass es genau 2^k *verschiedene* quadratfreie Teile gibt.

Bemerkung. Wenn wir n verschiedene, kleine Primzahlen haben, können wir die Anzahl der Zahlen, die $k \leq n$ verschiedene, kleine Primzahlen als Teiler haben, mittels $\binom{n}{k}$ ermitteln.

Suchen wir nun also die Zahlen, die 1 bis n verschiedene, kleine Primzahlen als Teiler haben, so gilt:

$$\sum_{k=0}^n \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$$

(Vgl. [For16], S.11)

Für die b_n (also die nicht quadratfreien Teile) gilt, dass mit $n = a_n b_n^2$:

$$b_n \leq \sqrt{n} \leq \sqrt{N}$$

Also $N_s \leq 2^k \sqrt{N}$

(6) gilt für alle N , finde nun ein N , für das $N_s \leq 2^k \sqrt{N}$ gilt:

$$\begin{aligned} 2^k \sqrt{N} &\leq \frac{N}{2} \\ 2^{k+1} &\leq \sqrt{N} \\ 2^{2k+2} &\leq N \end{aligned}$$

Die Ungleichung $N_s + N_b < N$ gilt also für $N = 2^{2k+2}$.

Zusammenfassend:

- Annahme: $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert.

⇒ (5)

- Per Konstruktion von N_s und N_b muss gelten $N_b + N_s = N$, wenn N eine beliebige natürliche Zahl ist.
- Wir haben gezeigt, wenn $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert, dann gibt es ein N , für das gilt $N_s + N_b < N$
- Widerspruch zur Konstruktion von N_s und N_b ! D.h. $\sum_{p \in \mathbb{P}} \frac{1}{p}$ muss divergieren.

⇒ Es gibt unendlich viele Primzahlen.

□

Literatur

- [KP13] Jürg Kramer und Anna-Maria von Pippich. *Von den natürlichen Zahlen zu den Quaternionen: Basiswissen Zahlbereiche und Algebra*. Springer Spektrum, 2013.
- [AZH15] Martin Aigner, Günter M. Ziegler und Karl H. Hofmann. *Das Buch der Beweise*. Springer, 2015.
- [For16] Otto Forster. *Analysis 1 Differential- und Integralrechnung einer Veränderlichen*. 12. Aufl. Springer Spektrum, 2016.
- [Wal17] Guido Walz (Hrsg.) *Lexikon der Mathematik*. Springer Spektrum, 2017.