Sechs Beweise für die Unendlichkeit der Primzahlen

Seminar aus Reiner Mathematik

Carina Melcher

0910445

Graz, Jannuar 2014

Vorwort

Diese Seminararbeit wurde im Rahmen der Lehrveranstaltung „621.224 Seminar aus (Reiner Mathematik)“ im Wintersemester 2013/2014 erstellt und behandelt das Kapitel „Sechs Beweise für die Unendlichkeit der Primzahlen“ aus dem Werk „Proofs from THE BOOK“ von Martin Aigner und Günter Ziegler.

Bevor ich auf die einzelnen Beweise eingehe, werde ich in der Einleitung kurz näher auf die Primzahlen an sich eingehen. Danach folgt in meinen Ausführungen jeweils vor jedem der sechs Beweise eine kurze Information zu den einzelnen Mathematikern.

Beginnen werde ich mit dem ältesten Beweis, welcher von Euklid stammt, der darauffolgende ist von Christian Goldbach, der Dritte ist Folklore, der vierte Beweis ist von Euler, der Fünfte von Harry Fürstenberg und der letzte Beweis wurde von Paul Erdős vorgeschlagen.

Inhaltsverzeichnis

1 Einleitung

Bereits in Euklids Buch „Elemente“ gibt es eine Definition der Primzahl. Das erste der drei arithmetischen Bücher beginnt mit 22 Definitionen, wobei es hier drei Definitionen gibt, welche für uns interessant sind.

Definition 1. *Einheit ist das, wonach jedes Ding eins genannt wird.*

Definition 2. *Zahl ist die aus Einheiten zusammengesetzte Menge.*

Definition 3. *Primzahl ist eine Zahl, die sich durch die Einheit messen lässt.*

Unter einer Einheit versteht Euklid nicht nur einen bloßen Begriff, sondern die Eigenschaft konkreter Dinge. Das bedeutet, es ist ein Maßstab für andere, gleichartige „konkrete Dinge“ wie zum Beispiel ein Apfel, ein Stock oder auch ein Gedanke.

Zahlen erhält man dann folglich, wenn man in diesem Maßstab misst, wobei man der historischen Treue wegen beachten muss, dass stets mehrere Einheiten vorkommen müssen. Somit ist 1 für Euklid keine Zahl sondern eine Einheit.

Folglich ist für Euklid eine Primzahl eine Zahl, welche größer 1 ist, die sich also durch keine andere Zahl messen lässt. Dies ist ein Unterschied zur heutigen Zeit, denn hier wird die Zahl selbst nicht als Teiler ihrer selbst angesehen.

Abgesehen von diesen kleinen Unterschieden definieren wir die Primzahlen heute wie folgt:

Definition 4. *Eine natürliche Zahl $p > 1$ heißt Primzahl, wenn sie nur triviale Teiler besitzt. Die Menge aller Primzahlen wird $\mathbb{P}$ bezeichnet.*

Bemerkung. *Jede natürliche Zahl besitzt die Teiler 1 und n. Diese werden triviale Teiler genannt.*

Bemerkung. *Somit sind die ersten Primzahlen $2, 3, 5, 7, 11, 13, 17$. Wobei 2 die einzige gerade Primzahl ist, da jede gerade Zahl per Definition durch 2 teilbar ist.*

Eine einfache Methode um Primzahlen bis zu einer nicht zu großen Zahl N herauszufinden ist das Sieb des Eratosthenes. Hierbei schreibt man die Zahlen von 2 bis N in eine Reihe. 2 bleibt als Primzahl stehen, alle anderen geraden Zahlen werden gestrichen. Die erste nicht gestrichene Zahl ist die Primzahl 3. Alle Vielfachen von 3 werden wieder gestrichen.[Trost, 1953][Kowol, 1995]

Die größte Primzahl, die man bisher entdeckt hat ist die Zahl $2^{57885161} - 1$, welche 17,4 Millionen Stellen besitzt. Entdeckt wurde diese 2013 von Curtis Coopers , einem Mathematiker von der University of Central Missouri in Warrensburg.[Dambeck, 2013]

Ein wichtiger und bekannter Satz, welcher mit den Primzahlen in einem Atemzug genannt werden muss, ist der Fundamentalsatz der Zahlentheorie. Dieser sagt aus, dass die Primzahlen die Bausteine für den multiplikativen Aufbau der natürlichen Zahlen sind.

Satz 1 (Fundamentalsatz der Zahlentheorie)**.** *Jede natürliche Zahl n lässt sich bis auf die Reihenfolge eindeutig als Produkt von Primzahlen darstellen.*

Abschließend möchte ich noch einige allgemeine Bezeichnungen festhalten, welche sich in meinen Ausführungen immer wieder finden werden:

$\mathbb{N} := \{1, 2, 3, 4, ...\}$

$\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\}$

$\mathbb{P} := \{2, 3, 5, 7, ...\}$

2 Sechs Beweise für die Unendlichkeit der Primzahlen

Auch wenn all diese nachfolgenden Beweise verschiedene Ansätze benutzen, so haben doch alle eine Idee gemeinsam - und zwar, dass die natürlichen Zahlen ins Unendliche wachsen und dass jede natürliche Zahl $n \geq 2$ einen Primteiler hat. Diese beiden Tatsachen erzwingen, dass die Menge $\mathbb{P}$ unendlich ist.

Stellen wir uns nun die Frage, wieviele Primzahlen es gibt. Die Antwort ist vielen bekannt - es gibt unendlich viele. Einen ersten Beweis dazu stellte Euklid auf.

2.1 Euklids Beweis

Euklid von Alexandria war ein griechischer Mathematiker, welcher warscheinlich im 3. Jahrhundert vor Christus in Alexandria lebte. Das wohl bekannteste Werk Euklids, die „Elemente“, spielen seit rund 2300 Jahren eine wichtige Rolle, nicht nur in der Mathematik, sondern auch in der Philosophie und der allgemeinen Kulturgeschichte. Das Buch die Elemente, griechisch Stoicheia, ist inhaltlich keine eigene Leistung von Euklid, es ist vielmehr ein Zusammenfassen der mathematischen Ergebnisse aus älteren Zeiten - größtenteils aus den Schriften von Hippokrates von Chios, Theaitetos und Eudoxos. Sein Verdienst ist es jedoch, dass er diesen Wissensstand basierend auf Axiome, Postulate und Definitionen aufbereitet hat.

Über das Leben des Euklids ist wenig bekannt. Die Forschungen über ihn wurden dadurch erschwert, dass Euklid ein sehr häufiger Name in der Antike war und dass es unzählige Referenzen auf Personen namens Euklid in der Literatur gibt. Es gibt sogar die Vermutung, dass Euklid nie wirklich existierte, sondern dass dieser Name nur ein Pseudonym für eine Gruppe von Mathematikern war, die die Kenntnisse des damaligen Standes der Mathematik zusammengetragen haben. Allerdings ist diese Theorie ziemlich unwahrscheinlich.

Der Name Euklid findet sich weiters in vielen mathematischen Strukturen wieder, wie zum Beispiel der euklidische Abstand, die euklidische Geometrie, die euklidische Norm und viele mehr.[Bulmer-Thomas, 2008][Schreiber, 1987][van der Waerden]

Kommen wir nun zu Euklids Beweis über die Unendlichkeit von Primzahlen, wofür er einen Widerspruchsbeweis verwendet. Bevor wir den Beweis durchführen, definieren wir uns noch einen Primteiler.

Definition 5. *Ist $n \in \mathbb{N}$, $p \in \mathbb{P}$ und gilt $p \mid n$, dann ist p ein Primteiler von n.*

Nun aber zu Euklids Beweis.

Beweis. Wir nehmen an es gibt endlich viele Primzahlen $\mathbb{P} = \{p_1, p_2, ..., p_r\}$.

Sei $n = p_1 * p_2 * p_3 * ... * p_r + 1$ und $p \in \mathbb{P}$ mit $p \mid n$ (p Primteiler von n).

Da $p \mid (p_1 p_2 ... p_r) + 1$ und $p \mid (p_1 p_2 ... p_r)$ folgt daraus, dass $p \mid (p_1 p_2 ... p_r) + 1 - (p_1 p_2 ... p_r)$ woraus $p \mid 1$ folgt. $\lightning$

Dies ist jedoch nicht möglich, da 1 durch keine Primzahl teilbar ist. Also ist die Menge $\{p_1, p_2, ..., p_r\}$ niemals die Menge aller Primzahlen. $\square$

Bemerkung. *Dieser Beweis des Euklids zeigt eine Variante auf, wie man aus vorgegebenen Primzahlen mindestens eine weitere Primzahl berechnet. Dazu berechnet man das Produkt dieser Primzahlen und addiert 1 zu diesem Produkt:* $n = 1 + p_1 * p_2 * ... * p_r = 1 + \prod_{i=1}^{r} p_i$

Anschließend werden die Primfaktoren der neuegewonnenen Zahl n berechnet. Alle Primfaktoren sind dann Primzahlen, die in der ursprünglichen Primzahlmenge nicht vorhanden waren.

Nehmen wir als Beispiel die Zahlen $3, 5, 7$. Nach der obigen Formel berechnet man sich n: $n = 1 + 3 * 5 * 7 = 2 * 53$. Man hat somit also zwei neue Primzahlen 2 und 53 gefunden.

2.2 Beweis von Goldbach

Christian Goldbach ist ein deutscher Mathematiker, welcher 1690 in Preußen geboren wurde. Zu seinen Lebzeiten genoss Goldbach in der wissenschaftlichen Welt hohes Ansehen, später war sein Name so gut wie vergessen. Er wirkte von 1725 bis 1742 an der Petersburger Akademie der Wissenschaften, an welcher auch Daniel und Nikolaus II Bernoulli und Leonhard Euler forschten.

Er ist bis heute wegen der weder bewiesenen noch wiederlegten Goldbachschen Vermutung bekannt, welche er in einem Brief an Euler 1742 formulierte. Die Goldbachsche Vermutung gehört bis heute zu den ältesten und bedeutendsten ungelösten Problemen der Zahlentheorie.[Juškevič und Kopelevič, 1994][O'Connor und Robertson, 2006]

Der nachfolgende Beweis zur Unendlichkeit der Primzahlen ist ebenfalls aus einem Brief an Leonhard Euler aus dem Jahre 1730 und benutzt die spezielle Zahlenfolge.

Für den Beweis betrachten wir zunächst die Fermat-Zahlen.

Definition 6. *Eine Fermat-Zahl ist eine Zahl der Form* $F_n = 2^{2^n} + 1$ *für* $n = 0, 1, 2, ...$

Bemerkung. *Die ersten Fermat Zahlen lauten* $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, ...$

Bemerkung. *Alle Fermat Zahlen sind ungerade.*

Definition 7. *Zwei Zahlen* m *und* n *heißen relativ prim (teilerfremd),*

wenn $ggT(m, n) = 1$.

Kommen wir nun zu Goldbachs Beweis.

Beweis. Wir zeigen nun, dass je zwei Fermat-Zahlen relativ prim sind, also muss es auch unendlich viele Primzahlen geben.

Für den Beweis verifizieren wir die Rekursion

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

woraus die Behauptung unmittelbar folgen wird.

Ist nämlich m ein gemeinsamer Teiler von F_k und F_n mit $k < n$, so folgt aus der Rekursion, dass m $F_n - 2$ teilt und damit auch die Differenz von F_n und $F_n - 2$. Damit teilt m auch 2. Das bedeutet, dass $m = 1$ oder $m = 2$ ist. Der Fall $m = 2$

ist aber ausgeschlossen, da alle Fermat Zahlen ungerade sind. Somit ergibt sich die paarweise Teilerfremdheit der Fermatzahlen und damit auch die Unendlichkeit der Primzahlen.

Für den Beweis verwenden wir eine Induktion nach n.

Induktionsbeginn: Sei $n = 1$: Dann ist $F_0 = 3$ und $F_1 - 2 = 3$ ✓

Induktionsvoraussetzung: Es gilt $\prod_{k=0}^{n-1} F_k = F_n - 2$ und zu zeigen ist, dass $\prod_{k=0}^{n} F_k = F_{n+1} - 2$ ist.

Induktionsschluss: $n \to n + 1$

$\prod_{k=0}^{n} F_k = (\prod_{k=0}^{n-1} F_k)F_n = (F_n - 2)F_n = ((2^{2^n} + 1) - 2)(2^{2^n} + 1) = (2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^{n+1}} - 1) = F_{n+1} - 2$

□

2.3 Dritter Beweis

Der nachfolgende Beweis ist Folklore und keinem Mathematiker zuzuschreiben. Beginnen wir vorerst mit Definitionen um diesen Beweis später führen zu können.

Definition 8. *Eine Mersenne-Zahl ist eine Zahl der Form* $2^n - 1$, *wobei* $n \geq 1$ *ist.*

Definition 9. *Eine Menge* G *mit einer Funktion* $* : G \times G \to G, (g, h) \mapsto g * h$ *heißt Gruppe, wenn folgende Bedingungen erfüllt sind:*

1. $G \neq \emptyset$
2. $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$ *(Assoziativität)*
3. $\exists e \in G$, *sodass*
   - **a)** $\forall g \in G \quad g * e = g = e * g$ *(neutrales Element)*
   - **b)** $\forall g \in G \quad \exists g' \in G$ *mit* $g * g' = e = g' * g$ *(jedes* g *in* G *hat Inverses)*

Definition 10. *Eine Gruppe* G *heißt zyklisch, wenn* $\exists a \in G$: $G = \langle a \rangle$.

Dabei ist $\langle a \rangle = \langle \{a\} \rangle$ *die von* a *erzeugte Untergruppe von* G, *definiert als* $\langle a \rangle = \bigcap_{H \leq G, a \in H}$. *Wir wissen, dass*

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{..., a^{-2}, a^{-1}, e, a, a^2, ...\} \text{ gilt.}$$

Für additiv geschriebene Gruppen $(G, +)$ *ist*

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\} = \{..., -2a, -a, e, a, 2a, ...\}$$

Satz 2 (Satz von Lagrange)**.** *Ist G eine endliche (multiplikative) Gruppe und U eine Untergruppe, dann ist $|U|$ ein Teiler von $|G|$.*

Beweis. Betrachte die binäre Relation

$$a \backsim b :\Longleftrightarrow ba^{-1} \in U.$$

Es folgt aus den Gruppenaxiomen, dass $\backsim$ eine Äquivalenzrelation ist. Die Äquivalenzklasse eines Elementes a ist genau die Nebenklasse

$$Ua = \{xa : x \in U\}.$$

Da nun ersichtlich $|Ua| = |U|$ gilt, zerfällt G in Äquivalenzklassen, die alle die Größe $|U|$ haben. Also ist $|U|$ ein Teiler von $|G|$. □

Bemerkung. *Für den Spezialfall, in dem $U = \{a, a^2, ..., a^m = 1\}$ eine zyklische Untergruppe von G ist, besagt dies, dass m (die kleinste positive Zahl mit $a^m = 1$, genannt die Ordnung von a die Gruppengröße $|G|$ teilt.*

Kommen wir nun zum Beweis für die Unendlichkeit der Primzahlen.

Beweis. Angenommen $\mathbb{P}$ ist endlich und p die größte Primzahl. Wir betrachten diesmal die Mersenne-Zahl $2^p - 1$ und zeigen, dass jeder Primteiler q von $2^p - 1$ größer als p ist, was dann den gewünschten Widerspruch ergibt.

Sei q ein Primteiler von $2^p - 1$. Wenn wir jetzt also die Zahl $2^p - 1$ durch q teilen, erhalten wir keinen Rest. Teilen wir allerdings 2^p durch q so erhalten wir Rest 1. Es gilt also $2^p \equiv 1 \pmod{q}$.

Da p eine Primzahl ist, folgt daraus, dass die 2 in der multiplikativen Gruppe $\mathbb{Z}_q \backslash \{0\}$ des Körpers $\mathbb{Z}_q$ die Ordnung p hat. Diese Gruppe enthält $q - 1$ Elemente.

Da wir nach dem Satz von Lagrange wissen, dass die Ordnung jedes Elementes die Gruppengröße teilt, folgt $p \mid q - 1$ und daher $p < q$.

□

2.4 Eulers Beweis

Der Schweizer Mathematiker Leonhard Euler wurde 1707 in Basel geboren und gilt wegen seiner Forschungen im Bereich der Analysis und Zahlentheorie zu einem der größten Mathematiker.

Bereits mit 13 Jahren begann er in Basel zu studieren, wo sein Lehrmeister Johann Bernoulli war, welcher schon sehr früh sein Potential entdeckte. Später berief ihn Daniel Bernoulli an die Universität in St. Petersburg. Dort traf er auf Christian Goldbach, mit welchem er im ständigen Briefwechsel stand. 1741 wurde er von Friedrich dem Großen an die Königlich-Preußische Akademie der Wissenschaften nach Berlin berufen, wo er weiter sehr eng mit Christian Goldbach arbeitete. Daufhin wirkte er noch an der Akademie in St. Petersburg.

Euler war einer der weitaus produktivsten Mathematiker der Menschheitsgeschichte und weiters auch einer der größten Gelehrten aller Zeiten. Auf ihn geht ein Großteil der mathematischen Symbolik zurück, wie zum Beispiel das *Summenzeichen*, Pi, $f(x)$ für f als Funktion, die eulersche Zahl und die imaginäre Zahl.

Über Eulers Charakter äußern sich alle Zeitgenossen und Biografien gleich. Er war ein Sonnenkind mit offenen und heiterem Gemüt, unkompliziert, humorvoll und gesellig. Obwohl er in seiner zweiten Lebenshälfte zu dem wohlhabenden bis reichen Teil der Gesellschaft gehörte, war er immer ein sehr bescheidener Mensch. Eine große Rolle in seinem Leben spielte die Religion, die oftmals ein wichtiger Schlüssel zum Verständnis vieler Fakten in seinem Leben war.

Leonhard Euler hat 1748 zwei verschiedene Beweise für die Unendlichkeit der Primzahlen aufgestellt. In seinem ersten eher indirekten Beweis zeigt er, dass der Ausdruck $\sum_{p\in\mathbb{P}} \frac{1}{p^k} = \infty$ bestehend aus Primzahlen divergiert. [Fellmann, 1995][O'Connor und Robertson, 1998]

In seinem zweiten Beweis greift er auf diese Erkenntnis zurück und geht davon aus, dass die Primzahlen eine aufsteigende Folgen von Zahlen sind, wobei diese bei $p_1 < p_2 < ...$ beginnt.

Beweis. Sei $p(x) := \#\{p \leq x : p \in \mathbb{P}\}$ die Anzahl der Primzahlen, die kleiner oder gleich der reellen Zahl x sind.

Wir nummerieren $\mathbb{P} = \{p_1, p_2, p_3, ...\}$ in aufsteigender Reihenfolge. Weiters definieren wir uns den natürlichen Logarithmus als $\log x = \int_1^x \frac{1}{t} dt$.

Wir vergleichen nun die Fläche unter dem Graphen der Funktion $f(t) = \frac{1}{t}$ mit einer oberen Treppenfunktion.

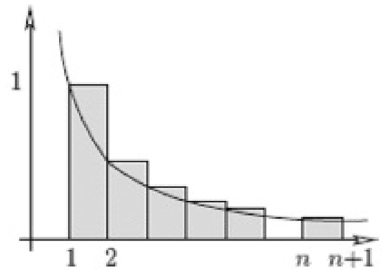

Abbildung 2.1: Eine obere Treppenfunktion für $f(t) = \frac{1}{t}$

Für $n \leq x < n+1$, für $n \in \mathbb{N}$ erhalten wir

$$\log x \leq 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n-1} + \frac{1}{n} \leq \sum{}' \frac{1}{m}$$

Wobei $\sum' \frac{1}{m}$ die Summe über allen $m \in \mathbb{N}$ bezeichnen soll, welche nur Primfaktoren $p \leq x$ enthalten. Es lässt sich jede solche Zahl m auf eindeutige Weise als Produkt der Form $\prod_{p \leq x} p^{k_p}$ (also als Produkt aus Vielfachen der Primteiler) schreiben. Daraus ergibt sich, dass

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

ist. Die innere Summe ist eine geometrische Reihe mit Faktor $\frac{1}{p}$ und hat deshalb den Grenzwert $\frac{1}{1-\frac{1}{p}}$.

Daraus folgt, dass

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

ist. Da offensichtlich $p_k \geq k+1$ ist und daher

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

erhalten wir

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

Nun wissen wir, dass die Funktion $\log x$ nicht beschränkt ist und schließen daraus, dass $p(x)$ ebenfalls unbeschränkt ist. Also gibt es unendlich viele Primzahlen. $\square$

2.5 Beweis von Harry Fürstenberg

Hillel Fürstenberg, bei seinen Freunden besser unter Harry Fürstenberg bekannt, war das Kind einer jüdischen Familie, welche in Deutschland lebte. Kurz bevor er 1935 geboren wurde, kam Hitler an die Macht, wodurch sich auch die Lebensumstände für Juden zum Schlechten veränderte. Kurz vor dem Ausbruch des zweiten Weltkrieges emmigrierte deshalb die Familie Fürstenberg nach Amerika. Seine universitäre Ausbildung brachte ihn in verschiedene Städte der USA, bevor er dann eine Professorenstelle in Jerusalem annahm.

Sein Beschäftigungsfeld ist die Warscheinlichkeitstheorie, Ergodentheorie, topologische Dynamik und die Zahlentheorie.[O'Connor und Robertson, 2010b]

Seinen Beweis über die Unendlichkeit der Primzahlen veröffentlichte er als Student im Jahre 1955. Dieser Beweis weicht von den anderen stark ab, da er einen rein topologischen Beweis für ein zahlentheoretischen Problem gefunden hat.

Bemerkung. *Zum Nachweis einer Topologie auf $\mathbb{Z}$ müssen folgende Axiome gelten:*

1. *Die leere Menge und $\mathbb{Z}$ sind offen.*
2. *Der Durchschnitt endlich vieler offener Mengen ist wieder offen.*
3. *Die Vereinigung unendlich vieler offener Mengen ist wieder offen.*

Er definiert dafür auf $\mathbb{Z}$ die nachfolgende Topologie.

Beweis. Für $a, b \in \mathbb{Z}, b > 0$ setzen wir

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

Jede Menge $N_{a,b}$ ist eine in beiden Richtungen unendlich arithmetische Folge.

Wir nennen nun die Menge $O \subseteq \mathbb{Z}$ offen, wenn entweder O leer ist oder wenn zu jedem $a \in O$ ein $b > 0$ existiert mit $N_{a,b} \subseteq O$. Offensichtlich ist dann jede Vereinigung von offenen Mengen wieder offen. Daraus ergibt sich offensichtlich die Erfüllung des ersten und dritten Axioms.

Nun noch zur Erfüllung des zweiten Axioms. Falls O_1 und O_2 offen sind und $a \in O_1 \cap O_2$ mit $N_{a,b_1} \subseteq O_1$ und $N_{a,b_2} \subseteq O_2$, so ist $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Daraus folgt, dass jeder Durchschnitt von endlich vielen offenen Mengen wiederum offen ist.

Diese Familie von offenen Mengen erfüllt also die Axiome einer Topologie auf $\mathbb{Z}$.

Wir notieren zwei Tatsachen:

1. Jede nichtleere offene Menge ist unendlich.
2. Jede Menge $N_{a,b}$ ist auch abgeschlossen.

Das erste Resultat folgt direkt aus der Definition. Zu (2) bemerken wir

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b},$$

sodass also $N_{a,b}$ das Komplement einer offenen Menge ist und daher abgeschlossen.

Nun kommen die Primzahlen ins Spiel. Da jede Zahl $n \notin \{1, -1\}$ einen Primteiler p hat und daher in der Menge $N_{0,p}$ enthalten ist (für p Primteiler in n, schließen wir

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

Wäre nun $\mathbb{P}$ endlich, so wäre $\bigcup_{p \in \mathbb{P}} N_{0,p}$ nach (2) eine endliche Vereinigung von abgeschlossenen Mengen und daher abgeschlossen. Folglich wäre $\{1, -1\}$ eine offene Menge, im Widerspruch zu Tatsache (1).

Somit ist die Annahme falsch und es folgt, dass $\mathbb{P}$ unendlich ist. $\square$

2.6 Beweis von Erdős

Paul Erdős, welcher 1913 in Budapest geboren wurde, war einer der bedeutendsten Mathematiker des 20. Jahrhunderts. Erdős hauptsächliches Arbeitsgebiet waren die Zahlentheorie und Kombinatorik. Von ihm stammt die Idee von dem BUCH, denn er ist der Meinung, dass es perfekte Beweise zu mathematischen Sätzen gibt. Er begann auch an der Ausarbeitung des Buches mit Notizen und Vorschlägen, verstarb allerdings vor der Veröffentlichung. Einer seiner bekanntesten Aussprüche war „man brauche als Mathematiker zwar nicht an Gott zu glauben, jedoch sollte man an das Buch glauben“.

Eines seiner Merkmale von Paul Erdős war sein merkwürdiger Akzent im Englischen, welchen er durch seinen Vater erlernte. Dieser war nämlich während des 1. Weltkrieges ein Kriegsgefangener in Sibirien und brachte sich in dieser Zeit selbst aus Büchern Englisch bei.

Erdős benötigte für sein Studium mit Doktorabschluss nur vier Jahre und reiste danach als Stipendiat weit umher, da der Antisemitismus immer mehr aufkam. Auch er lehrte an der Universität in Jerusalem, an welcher er offiziell für 30 Jahre unterrichtete. Er arbeitete mit 509 Mathematikern zusammen und so entstand auch die Erdős-Zahl. Jene Mathematiker, die direkt mit Paul Erdős zusammenarbeiteten haben die Erdős-Zahl 1, solche, die zwar nicht mit Erdős zusammenarbeiteten, aber mit jemanden mit Erdős-Zahl 1, haben die Erdős-Zahl 2, usw. [O'Connor und Robertson, 2010a][Baker et al., 1990]

Nun aber zu seinem Beweis. Er greift hierbei eine Idee von Euler auf, indem er die Reihe der inversen Primzahlen betrachtet. Er zeigt damit nicht nur, dass es unendlich viele Primzahlen gibt, sondern auch, dass die Reihe $\sum_{p\in\mathbb{P}} \frac{1}{p}$ divergiert.

Um diesen Beweis zu führen, definieren wir uns eine quadratfreie Zahl.

Definition 11. *Eine natürliche Zahl heißt quadratfrei, wenn es außer der Eins keine Quadratzahl gibt, die diese Zahl teilt. Anders formuliert tritt in der eindeutigen Primfaktorzerlegung $n = p_1, ..., p_k$ einer quadratfreien Zahl keine Primzahl mehr als einmal auf.*

Der erste Beweis dieses wichtigen Resultates wurde von Euler gegeben, aber der darauffolgende von Paul Erdős ist makellos.

Beweis. Es sei $p_1, p_2, p_3, ...$ die Folge der Primzahlen in aufsteigender Ordnung.

Nehmen wir an, dass die Reihe $\sum_{p\in\mathbb{P}} \frac{1}{p}$ konvergiert. Dann muss es nämlich eine natürliche Zahl k geben mit $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$.

Wir nennen nun die Primzahlen $p_1, ..., p_k$ kleine Primzahlen und die anderen $p_{k+1}, p_{k+2}, ...$ große Primzahlen. Für jede beliebige natürliche Zahl N gilt somit

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

Sei N_b die Anzahl der positiven ganzen Zahlen $n \leq N$, die durch mindestens eine große Primzahl teilbar sind. Sei N_s die Anzahl der positiven Zahlen $n \leq N$, die nur kleine Primteiler besitzen.

Wir werden nun zeigen, dass für ein geeignetes N

$$N_b + N_s < N$$

gilt. Dies wird den gewünschten Widerspruch ergeben, da nach Definition $N_b + N_s = N$ sein muss.

Um N_b abzuschätzen, halten wir fest, dass $\lfloor \frac{N}{p_i} \rfloor$ die positiven ganze Zahlen $n \leq N$ zählt, die Vielfache von p_i sind.

Mit (1) erhalten wir daraus

$$N_b \leq \textstyle\sum_{i\geq k+1} \lfloor \frac{N}{p_i} \rfloor < \frac{N}{2}. \ (2)$$

Somit haben wir eine Abschätzung für N_b gefunden.

Wir betrachten nun N_s. Wir schreiben jede Zahl $n \leq N$, die nur kleine Primteiler in der Form $n = a_n b_n^2$ besitzt, wobei a_n den quadratfreien Teil bezeichnet. Daraus ergibt sich, dass a_n als Produkt verschiedener kleiner Primzahlen geschrieben werden kann. Insgesamt gibt es genau 2^k verschiedene quadratfreie Teile, da es k kleine Primzahlen gibt.

Wir sehen weiter, dass wegen $b_n \leq \sqrt{n} \leq \sqrt{N}$, es höchstens $\sqrt{N}$ verschiedene Quadratteile gibt.

Es folgt daraus, dass

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

Da (2) für jedes N gilt, müssen wir nur eine Zahl N finden, die $2^k \sqrt{N} \leq \frac{N}{2} \iff 2^{k+1} \leq \sqrt{N}$ erfüllt. Solch eine Zahl ist zum Beispiel $N = 2^{2k+2}$.

$\square$

Literaturverzeichnis

Baker, A. et al. (1990): A tribute to Paul Erdős. Cambridge University Press 2.6

Bulmer-Thomas, I. (2008): Euclid. encyclopedia.com. URL http://www.encyclopedia.com/topic/Euclid.aspx 2.1

Dambeck, H. (2013): 17,4 Millionen Stellen: Computer entdeckt Rekord Mersenne Primzahl. Spiegel online. URL http://www.spiegel.de/wissenschaft/mensch/17-4-millionen-stellen-computer-entdeckt-rekord-mersenne-primzahl-a-882646.html 1

Fellmann, E. A. (1995): Leonhard Euler. Rowohlt Taschenbuch Verlag 2.4

Juškevič, A. P. und Kopelevič, J. K. (1994): Christian Goldbach. Birkenhäuser Verlag 2.2

Kowol, G. (1995): Primz. Philosophisch-Anthroposophischer Verlag am Goetheanum 1

O'Connor, J. J. und Robertson, E. F. (1998): Leonhard Euler. URL http://www-history.mcs.st-andrews.ac.uk/Biographies/Euler.html 2.4

O'Connor, J. J. und Robertson, E. F. (2006): Christian Goldbach. URL http://www-history.mcs.st-andrews.ac.uk/Biographies/Goldbach.html 2.2

O'Connor, J. J. und Robertson, E. F. (2010a): Erdős. URL http://www-history.mcs.st-and.ac.uk/Biographies/Erdos.html 2.6

O'Connor, J. J. und Robertson, E. F. (2010b): Hillel Furstenberg. URL http://www-history.mcs.st-and.ac.uk/Biographies/Furstenberg.html 2.5

Schreiber, P. (1987): Euklid. BSB B. G. Teubner Verlag 2.1

Trost, D. E. (1953): Primzahlen. Verlag Birkhäuser 1

van der Waerden, B. L. (): Euclid. britannica.com. URL http://www.britannica.com/EBchecked/topic/194880/Euclid 2.1