Philipps-Universität Marburg
Institut für Mathematik
SE: Klassische Probleme
Leitung: Benjamin Schwarz
Referentin: Ines David
WS 09/10

Ausarbeitung

UNENDLICHKEIT DER PRIMZAHLEN

Inhaltsverzeichnis

1 EINLEITUNG 1

2 BEWEIS VON EUKLID 1

3 BEWEIS VON GOLDBACH 2

4 BEWEIS VON EULER 4

5 PAUL ERDÖS 5

6 FÜRSTENBERG 7

7 SCHLUSSBEMERKUNG 8

8 LITERATURVERZEICHNIS 9

1 Einleitung

Die Primzahlen sind natürliche Zahlen wie 2,3,5,7,11,13,..., die nur von sich selbst und der 1 geteilt werden. Jede andere Zahl, die ungleich 1 und keine Primzahl ist, nennt man zerlegbar. Die Primzahlen spielen in dieser Zerlegung eine elementare Rolle. Nach dem Fundamentalsatz der Arithmetik lässt sich jede natürliche Zahl größer als 1 auf eine eindeutige Weise als Produkt aus Primzahlen schreiben. Aus dieser Tatsache, die ich an dieser Stelle nicht verifizieren möchte, ergibt sich die Frage:

Wie viele Primzahlen gibt es?

Die Antwort ist vielen bekannt: Es gibt unendlich viele. Jedoch ist dieses nicht mit dem Fundamentalsatz gezeigt. Man könnte annehmen, dass jede sehr große Zahl in Primfaktoren zerfällt. Jedoch nur auf Grundlage des Beweises der eindeutigen Zerlegung lässt sich diese Aussage weder bestätigen noch widerlegen. Im Folgenden werde ich vier Beweise mit Abwandlungen vorstellen. Manche der Beweise deuten auf interessante Entwicklungen hin, andere sind einfach nur trickreich und elementar. Jeder dieser Beweise ist in meinen Augen „schön“ und hat auf seine Weise etwas Besonderes. Einige von ihnen sind von bekannten Mathematikern andere von vergessenen. Natürlich gibt es noch viele weitere Beweise für die Existenz von unendlich vielen Primzahlen, auf die in der Literatur hingewiesen wird.

Bevor wir zu den Beweisen kommen, möchte ich einige allgemeine Bezeichnungen festhalten: $\mathbb{N} := \{1,2,3,4,...\}$ $\mathbb{P} := \{2,3,5,7,...\}$

2 Beweis von Euklid

Euklid von Alexandria lebte von 360 v. Chr. bis 280 v. Chr. Und bewies in seinem Buch „Elemente“ die Unendlichkeit der Primzahlen. Er ging dabei wie folgt vor:

Angenommen, es gibt nur endlich viele Primzahlen $\mathbb{P} = \{p_1, p_2, ..., p_r\}$.

Sei $P = p_1 * p_2 * ... * p_r$, das Produkt aller Primzahlen. Wir betrachten die Zahl

$$P+1 = (\prod_{1 \le i \le r} p_i) + 1.$$

Daraus ergeben sich zwei Fälle, (a) $P+1$ ist eine Primzahl oder (b) $P+1$ ist keine Primzahl. Im Fall (b) sei nun $p \in \mathbb{N}$ eine Primzahl mit $p | P+1$, daraus folgt, dass $p \notin \mathbb{P}$ denn sonst würde $p \mid P - p_1 * p_2 ... * p_r = 1$, was ein Widerspruch ist. Im Fall (a) haben wir auch eine weitere Primzahl gefunden, weil $P+1 \notin \mathbb{P}$ sein kann, da $p_i < P+1 \ \forall i \in \{1, 2, ..., r\}$. Dies zeigt, dass es unendlich viele Primzahlen gibt.

Dieser Beweis liefert leider kein zuverlässiges System Primzahlen zu erzeugen, aber es wirft die Frage auf: Gibt es unendlich viele Primzahlenprodukte *P*, wobei das zugehörige $P+1$ eine Primzahl ist? Das bis jetzt größte gefundene Produkt aus Primzahlen endet mit der Primzahl p_r=392113. Die so erzeugte Primzahl $P+1$ besteht dann 169966 Ziffern (D. Heuer, 09.2001).

Eine Abwandlung dieses Beweises schrieb Thomas Jean Stieltjes 1890. Er ging wie Euklid von der Annahme aus, dass $\mathbb{P}$ begrenzt ist. Er definierte auch ein Produkt aus allen Primzahlen $P = p_1 * p_2 * ... * p_r$. Er folgerte, dass man *P* auch schreiben kann als ein Produkt aus zwei Zahlen *m* und *n*, wobei $p_i \mid m$ oder $p_i \mid m \ \forall i \in \{1, 2, 3, ..., r\}$. Folglich ergibt sich auf Grund der eindeutigen Zerlegung in Primfaktoren, dass $p_i \nmid m+n$. Es gibt nun zwei Fälle, (a) $m+n \in \mathbb{P}$, was einen Widerspruch ergibt zu unserer Annahme, (b) $\exists p_j \notin \mathbb{P}$ eine Primzahl mit $p_j \mid m+n$. Fall (b) ist auch ein Widerspruch zu unserer Annahme und so muss es unendlich viele Primzahlen geben.

3 Beweis von Goldbach

Goldbach schrieb 1730 einen Brief an Leonhard Euler. Er hatte die Idee eine monoton steigende unendliche Folge (a_n) von natürlichen Zahlen zu finden, die paarweise teilerfremd ist. Aufgrund der eindeutigen Zerlegung in Primfaktoren würden ein Primfaktor p_1, welcher a_1 teilt, ein Primfaktor p_2 welcher a_2 teilt usw., alle verschieden sein. Daraus ergibt sich dann die Unendlichkeit der Primzahlen. Interessant an diesem Beweis ist die Tatsache, dass Goldbach über die Primzahlen an sich keine weiteren Annahmen oder Voraussetzungen benötigt.

Mit dieser Idee im Hinterkopf betrachtet er die *Fermat-Zahlen* mit der Form $F_n = 2^{2^n} + 1, \mathrm{n} \in \mathbb{N}$. Per Induktion über *n* lässt sich zeigen, dass

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

Für n=1 ist $F_0 = 3$ und $F_1 - 2 = 3$. Im Induktionsschluss $n \to n+1$ ergibt sich

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

$$= (2^{2^n})^2 - 1 = 2^{2^n} * 2^{2^n} - 1 = 2^{2^n + 2^n} - 1 = 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2 \,.$$

Sei m ein Teiler von F_k und F_n , $k < n$. So folgt aus der Rekursion $m \mid F_n - 2$ und daraus ergibt sich, dass m auch die Differenz von F_n und $F_n - 2$ teilt und damit die 2. Das bedeutet aber, dass nur m=1 oder m=2 sein kann. Der Fall m=2 ist aber nicht möglich, da alle Fermat-Zahlen ungerade sind. Somit ergibt sich die paarweise Teilerfremdheit für die Fermat-Zahlen und somit auch die Unendlichkeit der Primzahlen.

Wenn man die Fermat-Zahlen betrachtet, könnte man wie Fermat die Vermutung anstellen, dass diese alle Primzahlen seien. Für die ersten Fünf bis $F_4 = 65537$ stimmt diese Annahme auch. Bei der nächsten Zahl F_5 wurde es schon schwieriger, denn diese ist 10-stellig. Um die Primalität zu überprüfen brauchte man eine Tabelle mit allen Primzahlen bis 100000, welche es zu der Zeit nicht gab, oder man fand ein Kriterium für die Erkennung von Primzahlen. Dieses fand Fermat leider nicht, sondern erst Pepin im Jahre 1877. Interessant ist zu bemerken, dass schon Euler 100 Jahre vorher die Zerlegung von F_5 herausfand. Er stellte fest, dass jeder Faktor von F_n die Form $k * 2^{n+2} + 1$ haben muss. So entdeckte er die Zerlegung $F_5 = 641 * 6700417$. In den folgenden Jahrzehnten bis heute beschäftigten sich immer mehr Mathematiker mit diesem Phänomen. Bis heute ist F_4 die größte bekannte Fermat-Primzahl, die Zahlen bis F_{11} sind vollständig faktorisiert, für die Zahlen bis F_{24} ist bekannt, dass sie zerlegbar sind und die kleinste Zahl mit unbekannten Status ist F_{33}.

Der Ansatz von Goldbach wurde von einigen Mathematikern übernommen und so stellte beispielsweise Bellman im Jahre 1947 eine Methode vor, mit der man Folgen von paarweisen teilerfremden Zahlen erzeugen kann.

4 Beweis von Euler

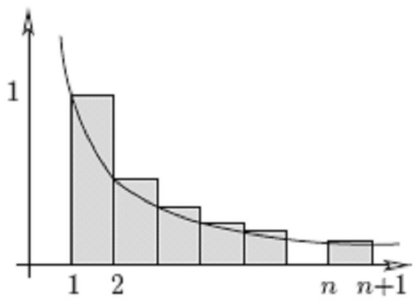
Leonhard Euler hat um 1748 zwei verschiedene Beweise für die Unendlichkeit der Primzahlen aufgestellt. In seinem ersten eher indirekten Beweis zeigt er, dass ein Ausdruck bestehend aus Primzahlen divergiert:

$$\sum_{p\in\mathbb{P}} \frac{1}{p^k} = \infty$$

In seinem zweiten Beweis greift er auf diese Erkenntnis zurück und verwendet einen ähnlichen Trick. Er geht davon aus, dass die Primzahlen eine aufsteigende Folge von Zahlen sind, wobei diese bei $p_1 < p_2 < p_3 ...$ beginnt.

Sei $\pi(x) = \#\{p \le x : p \in \mathbb{P}, \mathrm{x} \in \mathbb{R}\}$ die Anzahl der Primzahlen kleiner einer festen reellen Zahl x. Wir betrachten $\log(x)$ den natürlichen Logarithmus und definieren diesen als $\log(x) := \int_1^x \frac{1}{t}\,dt$. Als Nächstes vergleicht er die Fläche unter dem Graphen von $f(t) = \frac{1}{t}$

mit einer oberen Treppenfunktion. Für $n \le x \le n+1, n \in \mathbb{N}$, gilt



$$\log(x) \le 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + ... + \frac{1}{n} \le \sum{}' \, m$$

wobei die Reihe alle $m \in \mathbb{N}$, die nur Primteiler $p_i \le x$ besitzt, aufsummiert. Da m wie jede natürliche Zahl sich eindeutig als Produkt aus Vielfachen der Prim-

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

teiler darstellen lässt, ergibt sich

$$\sum{}' \frac{1}{m} = \prod_{p \le x,\, p \in \mathbb{P}} \Big(\sum_{k\ge 0} \frac{1}{p^k}\Big).$$

Die innere Summe $\sum_{k\ge 0} \frac{1}{p^k}$ ist eine geometrische Reihe und hat somit den Grenzwert

$\frac{1}{1-\frac{1}{p}}$. Daraus ergibt sich die Ungleichung

$$\log x \leq \prod_{p \leq x, p \in \mathbb{P}} (\sum_{k \geq 0} \frac{1}{p^k}) = \prod_{p \leq x, p \in \mathbb{P}} (\frac{1}{1-\frac{1}{p}}) = \prod_{p \leq x, p \in \mathbb{P}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}. \quad (1)$$

Für $p_k \geq k+1$ folgt deshalb

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}. \quad (2)$$

Wenn man nun (1) und (2) zusammenfügt, ergibt sich

$$\log(x) \leq \prod_{k \geq 0}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1 \quad .$$

Wir wissen, dass $\log(x)$ unbeschränkt ist und somit auch $\pi(x)$ unbeschränkt sein muss. Als weitere Erkenntnis aus diesem Beweis können wir $\log(x)$ als eine untere Grenze für die Anzahl der Primzahlen kleiner einer reellen Zahl festhalten.

5 Paul Erdös

Paul Erdös greift 1938 eine Idee von Euler auf, indem er die Reihe der inversen Primzahlen betrachtet. Er nimmt an, dass $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert. Des Weiteren definiert er die Primzahlen als eine aufsteigende Kette beginnend bei $p_1 < p_2 < \ldots$.Deshalb existiert ein $k \in \mathbb{N}$ mit $\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$.

Seien $p_1, \ldots, p_k$ *kleine* Primzahlen und $p_{k+1}, \ldots$ *große* Primzahlen. Für beliebige $N \in \mathbb{N}$

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

Sei nun N_G die Anzahl der n, $0 < n \leq N$, mit $p_{k+l} \mid n$, $l \in \mathbb{N}$, für mindestens ein l. Und sei N_K die Anzahl der m, $0 < m \leq N$, mit $p_j \mid m$, $j \in \{1, 2, \ldots, k\}$, und $p_{k+l} \nmid m \; \forall l \in \mathbb{N}$.

Sein Ziel war es N_G und N_K abzuschätzen um einen Widerspruch für $N_G + N_K = N$ zu erzeugen.

Bei der Betrachtung von N_G fällt auf, dass $\frac{N}{p_i}$ die Anzahl der $n \leq N$ wiedergibt, die von p_i für $i \geq k+1$ geteilt werden. Mit (1) und dieser Erkenntnis erhält man

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

Somit haben wir eine Abschätzung für N_G gefunden.

Jede Zahl, die nur kleine Primteiler hat, schreiben wir in der Form $m = a_m {b_m}^2$, $m \leq N$ wobei a_m der quadratfreie Teil ist. Daraus ergibt sich, dass a_m als Produkt verschiedener kleiner Primzahlen geschrieben werden kann. Insgesamt übersteigt die die Anzahl der quadratfreien Teile nicht 2^k, da es *k* kleine Primzahlen gibt. Für die Quadratteile kann man folgende Abschätzung betrachten $b_m \leq \sqrt{m} \leq \sqrt{N}$. Daraus ergibt sich

$$N_K \leq 2^k * \sqrt{N}$$

Nun haben wir für N_G und N_K eine Abschätzung. Da (2) für jedes beliebige *N* gilt, suchen wir ein *N*, welches $2^k * \sqrt{N} \leq \frac{N}{2}$ oder anders geschrieben $2^{k+1} \leq \sqrt{N}$.

Wir betrachten die Zahl $N = 2^{2k+2}$. Daraus ergibt sich für die Gleichung $N_G + N_K = N$

$$N = 2^k * \sqrt{2^{2k+2}} + \frac{2^{2k+2}}{2} < 2^k * \sqrt{2^{(k+1)^2}} + 2^{2k+1}$$

$$= 2^k * 2^{k+1} + 2^{2k+1} = 2^{2k+2} = N \ ,$$

was einen Widerspruch darlegt. Somit ist die Annahme falsch und es wurde gezeigt, dass $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert.

Eine Folgerung dieses Beweises ist die Tatsache, dass die Primzahlen dichter zusammen liegen als beispielsweise die Zahlen der Form $n^2 \in \mathbb{N}$, da die Reihe der inversen Quadrate konvergiert mit

$$\sum_{n=1}^{\infty} n^2 = \frac{\pi^2}{6} \ .$$

6 Fürstenberg

Als letzten Beweis möchte ich den von Hillel Fürstenberg vorstellen, den er 1955 als Student veröffentlichte. Sein Beweis weicht von anderen Beweisen stark ab, denn er gibt einen rein topologischen Beweis für ein zahlentheoretisches Problem. Bis kurz vor Ende des Beweises fragt man sich, was dieser mit der den Primzahlen und deren Unendlichkeit zu tun hat.

Er definiert auf $\mathbb{Z}$ folgende Topologie: Sei $a,b \in \mathbb{Z}$, $b > 0$ und

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

Jede Menge $N_{a,b}$ ist in beide Richtungen eine unendliche arithmetische Folge. Man kann sich diese als Punkte in einem zweidimensionalen Gitter vorstellen, welche nach $+\infty$ und $-\infty$ gehen. Zum Nachweis einer Topologie auf $\mathbb{Z}$ müssen folgende Axiome erfüllt sein:

(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

Eine Menge $M \subseteq \mathbb{Z}$ heißt offen, wenn M leer ist oder wenn es zu jedem $a \in M$ ein $b > 0$ existiert mit $N_{a,b} \subseteq M$. Daraus ergibt sich offensichtlich die Erfüllung des dritten sowie des ersten Axioms. Für das zweite Axiom betrachten wir zwei Mengen M_1 und M_2 beide offen und sei $a \in M_1 \cap M_2$ mit $N_{a,b_1} \subseteq M_1$ und $N_{a,b_2} \subseteq M_2$. Es folgt, dass $a \in N_{a,b_1 b_2} \subseteq M_1 \cap M_2$ ist. Damit sind die Axiome für eine Topologie auf $\mathbb{Z}$ erfüllt.

Nach der obigen Definition ist jede nicht leere offene Menge unendlich. (1)

Des Weiteren ist jede Menge $N_{a,b}$ abgeschlossen. (2)

Das ergibt sich aus

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

da $N_{a,b}$ ein Komplement einer offenen Menge ist.

An dieser Stelle kommen erst die Primzahlen ins Spiel. Wir wissen, dass jede Zahl $n \in \mathbb{N} \backslash \{-1,1\}$ mindestens einen Primteiler besitzt und so $n \in N_{0,p}$, $p \in \mathbb{P}$. Daraus folgt:

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

Wenn wir annehmen, dass $\mathbb{P}$ endlich ist, folgt daraus, das $\bigcup_{p \in \mathbb{P}} N_{0,p}$ nach (2) abgeschlossen ist. Das hat aber zur Folge, dass {-1,1} offen ist, was einen Widerspruch zu (1) darstellt.
Somit war die Annahme falsch und es wurde gezeigt, dass $\mathbb{P}$ unendlich ist.

7 Schlussbemerkung

Es gibt, wie bereits erwähnt, viele weitere Beweise, die auf teilweise sehr ähnlichen aber auch ganz anderen Ideen basieren. Viele Beweise haben weitere Fragen aufgeworfen. Neben der Frage wie viele Primzahlen es gibt, wurden unter anderem folgende Aspekte hinterfragt:
(1) Wie kann man Primzahlen erkennen?
(2) Wie sind die Primzahlen verteilt?
(3) Welche besondern Arten von Primzahlen gibt es?
Zu (1) wurden unterschiedliche Annahmen getroffen, beginnend beim Sieb des Eratosthenes über die Charakterisierung der Primzahlen von Wilson, bis hin zu Primzahlentest, welcher jedoch keine Faktorisierung angeben kann. Bei der Frage (2) kommt die uns bekannte $\pi(x)$ zum Tragen, welche in der Literatur unter dem Begriff Primzahlenfunktion gefunden werden kann. Als Weiteres wurden arithmetische Folgen untersucht, die aus Primzahlen bestehen, wie beispielsweise die Fermat-Zahlen. Zu den besonderen Arten von Primzahlen gehören zum Beispiel die Primzahlzwillinge, wobei p und p+2 Primzahlen sind, Primzahlmehrlinge oder auch die Mersennen-Primzahlen. Die bisher größte gefundene Primzahl ist $2^{13466917} - 1$ eine solche Mersenne-Primzahl.

8 Literaturverzeichnis

RIBENBOIM, P.:Meine Zahlen, meine Freunde. Springer Berlin Heidelberg (2009), S.65-81
RIBENBOIM, P.: Die Welt der Primzahlen. Springer Berlin Heidelberg (2006), S. 1-13
BEHRENDS, GRITZMANN, ZIEGLER: π & Co. Springer Berlin Heidelberg (2008), S.51-54

http://www.mathematik.de/ger/index.php
http://www.beweise.mathematic.de/