Behauptung: Es gibt unendlich viele Primzahlen.

1 Der Beweis von Euklid

Annahme: Es gibt endlich viele Primzahlen $\{p_1, \ldots, p_r\}$.

Wir bilden die Zahl $n = p_1 \cdot \ldots \cdot p_r + 1$.
Nun gibt es zwei Möglichkeiten. Entweder n ist eine Primzahl. Das wäre ein Widerspruch und es folgt die Unendlichkeit der Primzahlen. Oder die Zahl n ist keine Primzahl. Dann besitzt sie aber einen Primteiler p, der sowohl $p_1 \cdot \ldots \cdot p_r$ als auch 1 teilt. Da 1 keinen Primteiler besitzt, folgt ein Widerspruch und die Behauptung. $\square$

2 Ein Beweis mit Hilfe der *Fermat-Zahlen*

Folgender Beweis wurde von Christian Goldbach entdeckt, welcher diesen in einem Brief an Leonhard Euler im Jahr 1730 verfasst hat.

Wir betrachten zunächst die *Fermat-Zahlen* $F_n = 2^{(2^n)} + 1$, für $n = 0, 1, 2 \ldots$.
Zum Beispiel: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$. Im Folgenden werden wir zeigen, dass je zwei *Fermat-Zahlen* relativ prim, also teilerfremd sind. Da es unendlich viele Fermat-Zahlen gibt, folgt daraus, dass es auch unendlich viele Primzahlen gibt. Dazu beweisen wir die Rekursion

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

mit Induktion über n:

IA: Für $n = 1$ haben wir $F_0 = F_1 - 2 = 3$.

IV:

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

IS: Mit $n \mapsto n + 1$ haben wir zu zeigen:

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

IB:

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) \cdot F_n \overset{\text{IV}}{=} (F_n - 2) \cdot F_n = \left(2^{(2^n)} - 1\right) \cdot \left(2^{(2^n)} + 1\right)$$
$$= 2^{(2^n+1)} - 1 = 2^{(2^n+1)} + 1 - 2 = F_{n+1} - 2 \qquad \square$$

Ist m nun ein gemeinsamer Teiler von F_k und F_n (mit $k < n$).
Dann folgt aus der Rekursion, dass m die Zahl $\prod F_k$ teilt und damit auch $F_n - 2$. Da m aber F_n teilt, muss m auch 2 teilen. Das heißt, dass m entweder 1 oder 2 ist. Da alle *Fermat-Zahlen* ungerade sind, ist der gemeinsame Teiler zweier *Fermat-Zahlen* also 1, damit sind sie teilerfremd und die Unendlichkeit der Primzahlen ist bewiesen. $\square$

3 Ein Beweis mit Hilfe der *Mersenne-Zahlen*

Wer diesen Beweis entdeckt hat, ist unbekannt.

Annahme: Es gibt endlich viele Primzahlen $\{p_1, \ldots, p_r\}$ und p_r sei die Größte.

Wir betrachten die *Mersenne-Zahl* $2^{p_r} - 1$ und werden zeigen, dass jeder Primteiler q von dieser Zahl größer ist als p_r, was den gewünschten Widerspruch ergibt. Sei also q ein Primteiler von $2^{p_r} - 1$. Wenn wir also die Zahl $2^{p_r} - 1$ durch q teilen erhalten wir keinen Rest. Teilen wir allerdings die Zahl 2^{p_r} durch q so erhalten wir den Rest 1. Es gilt also $2^{p_r} \equiv 1(\mod q)$.
Betrachten wir in dem Zusammenhang die multiplikative Gruppe $\mathbb{Z}_q \backslash \{0\}$ des Körpers $\mathbb{Z}_q$, so stellen wir fest, dass die Ordnung des Elements $2 \in \mathbb{Z}_q \backslash \{0\}$ die Ordnung p_r besitzt. Weiterhin gilt $|\mathbb{Z}_q \backslash \{0\}| = q - 1$, die Anzahl der Elemente ist also $q - 1$.
Mit dem Satz von Lagrange[1] wissen wir, dass die Ordnung jedes Elements der Gruppe die Gruppengrößte teilt. Es gilt also $p_r | q - 1$ und damit $p_r < q$. Dies ist ein Widerspruch und es folgt die Behauptung. $\square$

[1] Der Beweis befindet sich im Anhang.

4 Ein Beweis aus der Topologie

Der Beweis der nun geführt wird, wurde 1955 von Hillel Fürstenberg als Student veröffentlicht. Er zeichnet sich dadurch aus, dass er mit Mittel aus der Topologie ein zahlentheoretisches Problem löst, wodurch dieser Beweis schlussendlich im *BUCH der Beweise* aufgeführt ist.

Eine Topologie besteht aus Teilmengen (offene Mengen) einer Grundmenge. Wir definieren uns nun folgende Topologie auf $\mathbb{Z}$:

$$S(a,b) = \{an + b | n \in \mathbb{Z}\} = a\mathbb{Z} + b, \text{ mit } a, b \in \mathbb{N}$$

Jede Menge $S(a,b)$ ist in beide Richtungen eine unendliche arithmetische Folge. Zum Nachweis einer Topologie auf $\mathbb{Z}$ mussen folgende Axiome erfüllt sein:

(a) Die leere Menge und $\mathbb{Z}$ sind offen.

(b) Der Durchschnitt endlich vieler offener Mengen ist wieder offen.

(c) 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 $b \in M$ ein $a > 0$ existiert mit $S(a,b) \subseteq M$. Daraus ergeben sich die Axiome der Topologie folgendermaßen:

zu (a) Per Definiton ist die leere Menge offen und da alle Mengen $S(a,b)$ Teilmengen von $\mathbb{Z}$ sind, ist $\mathbb{Z}$ ebenso offen.

zu (b) Wir betrachten zwei Mengen M_1 und M_2, beide offen und sei $b \in M_1$ und $b \in M_2$ mit $S(a_1,b) \subseteq M_1$ und $S(a_2,b) \subseteq M_2$. Es folgt, dass für alle $b \in M_1 \cap M_2$ gilt: $S(a_1a_2,b) \subseteq M_1 \cap M_2$. Die Menge $M_1 \cap M_2$ ist also offen.

zu (c) Sei M_i offen, also existiert für alle $b_i \in M_i$ ein $a_i > 0$, so dass $S(a_i,b_i) \subseteq M_i$. Daraus folgt, dass

$$\forall b_i \in \bigcup_i M_i \; \exists a_i > 0 \text{ mit } S(a_i,b_i) \subseteq \bigcup_i M_i$$

gilt. Damit ist $\bigcup_i M_i$ wieder offen.

Alle Axiome für eine Topologie sind damit erfüllt. Es folgen nun zwei Eigenschaften dieser Topologie:

(1) Jede nicht-leere offene Menge ist unendlich, das Komplement einer nicht-leeren endlichen Menge kann keine abgeschlossene Menge sein.

(2) Jede Menge $S(a,b)$ ist auch abgeschlossen.

Die erste Eigenschaft folgt direkt aus der Definition. Zur zweiten Eigenschaft bemerken wir, dass wir $S(a,b)$ als das Komplement einer offenen Menge darstellen können und daher abgeschlossen ist:

$$S(a,b) = \mathbb{Z} \backslash \bigcup_{j=1}^{a-1} S(a, b+j)$$

Primzahlen haben bis jetzt noch keine Rolle gespielt. Nun kommen sie allerdings ins Spiel. Die Zahlen -1 und $+1$ sind die einzigen ganzen Zahlen, welche keine Vielfachen von Primzahlen sind, also

$$\mathbb{Z} \backslash \{-1, +1\} = \bigcup_{p \in \mathbb{P}} S(p, 0).$$

Die linke Seite der Gleichung ist nach (1) keine abgeschlossene Menge. Wegen (2) sind die Mengen $S(p,0)$ abgeschlossen. Nehmen wir an $\mathbb{P}$ sei endlich, dann wäre die (dann endliche) Vereinigung der abgeschlossenen Mengen auf der rechten Seite eine abgeschlossene Menge. Daraus ergibt sich ein Widerspruch und es folgt die Behauptung. $\square$

5 Anhang

Der Satz von Lagrange[2]:
Sei G eine endliche Gruppe.

(1) Ist H eine Untergruppe von G, so gilt $|H| \mid |G|$.

(2) Insbesondere teilt die Ordnung eines Elementes x von G die Gruppenordnung. Also für $x \in G$ gilt $|x| \mid |G|$.

Beweis: Wir betrachten für jedes $a \in G$ die Nebenklasse Ha. $h \mapsto ha$ ist eine Bijektion zwischen der Untergruppe H und der Nebenklasse Ha, da aus $h_1 a = h_2 a$ folgt, dass $h_1 = h_2$ ist. Darum sind alle Nebenklassen gleich groß und mit $a \in Ha$ folgt, dass G in endlich viele disjunkte

[2] http://de.wikipedia.org/wiki/Satz_von_Lagrange

Nebenklassen zerlegt werden kann, wobei jede dieser Nebenklassen $|H|$ Elemente besitzt. Daher muss $|G|$ ein Vielfaches von $|H|$ sein.
Die zweite Aussage des Satzes ist eine einfache Folgerung der ersten, da die von x erzeugte Untergruppe gerade die Ordnung $|x|$ besitzt. $\square$