1
Wie viele Primzahlen gibt es?

Die Frage, wie viele Primzahlen es gibt, wird durch den fundamentalen Satz beantwortet:

Es gibt unendlich viele Primzahlen.

Ich werde mehrere Beweise für diesen Satz vorstellen, darunter vier Varianten unterschiedlicher Ansätze. Die Beweise stammen von berühmten Mathematikern, aber auch von solchen, die in Vergessenheit geraten sind. Manche der Beweise deuten auf interessante Entwicklungen hin, andere sind einfach nur raffiniert oder merkwürdig. Natürlich gibt es noch mehr Beweise für die Existenz unendlich vieler Primzahlen – wenn auch nicht unendlich viele.

I Beweis von Euklid

Angenommen, $p_1 = 2 < p_2 = 3 < \cdots < p_r$ würde die Gesamtheit aller Primzahlen darstellen. Es sei $P = p_1 p_2 \cdots p_r + 1$ und p eine Primzahl, die P teilt. Dann kann p keine der Zahlen $p_1, p_2, \ldots, p_r$ sein, denn andernfalls müsste p auch die Differenz $P - p_1 p_2 \cdots p_r = 1$ teilen, was aber unmöglich ist. Daher ist p eine zusätzliche Primzahl, so dass $p_1, p_2, \ldots, p_r$ nicht schon alle Primzahlen gewesen sein können. □

Ich bezeichne die aufsteigend unendliche Folge der Primzahlen nun stets durch

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \ldots,\ p_n,\ \ldots .$$

P. Ribenboim, *Die Welt der Primzahlen*, 2. Aufl., Springer-Lehrbuch,
DOI 10.1007/978-3-642-18079-8_1, © Springer-Verlag Berlin Heidelberg 2011

Eine elegante Variante des euklidischen Beweises wurde 1878 von Kummer angegeben.

Beweis von Kummer. Angenommen, es gäbe nur endlich viele Primzahlen $p_1 < p_2 < \cdots < p_r$. Es sei $N = p_1 p_2 \cdots p_r$, wobei $N > 2$. Die Zahl $N - 1$, die wie alle natürlichen Zahlen ein Produkt von Primzahlen ist, muss mit N einen gemeinsamen Teiler p_i haben, der dann wiederum die Differenz $N - (N - 1) = 1$ teilen müsste, was nicht sein kann. □

Dieser Beweis eines bedeutenden Mathematikers gleicht einer Perle: Er ist rund, glanzvoll und schön in seiner Einfachheit.

Ein ähnlicher Beweis wie der von Kummer wurde 1890 von Stieltjes vorgestellt, einem weiteren großen Mathematiker.

Wenn Ihnen Kummers Beweis gefallen hat, vergleichen Sie ihn doch mit dem folgenden, der noch einfacher und schöner ist. Auf ihn wurde ich von W. Narkiewicz aufmerksam gemacht. Der Beweis wurde 1915 von H. Brocard im *Intermédiaire des Mathématiciens* 22, Seite 253, veröffentlicht und dort Hermite zugeschrieben. Hierbei handelt es sich um eine weitere Variante des euklidischen Beweises:

Es genügt zu zeigen, dass es für jede natürliche Zahl n eine Primzahl p gibt, die größer als n ist. Zu diesem Zweck betrachte man einen beliebigen Primteiler p der Zahl $n! + 1!$ (Wenn Sie das zweite !, das eigentlich den Beweis abschließt, nicht mögen, dann beziehen Sie es einfach auf die 1.)

Euklids Beweis ist zwar recht einfach, doch gibt er keinerlei Auskunft über die Beschaffenheit der neuen Primzahl, die in jedem Schritt erzeugt wird. Man weiß nur, dass sie in ihrer Größe höchstens gleich $P = p_1 p_2 \cdots p_n + 1$ ist. Es kann also sein, dass die Zahl P für manche Indizes n selbst eine Primzahl, für andere n aber zerlegbar ist.

Für jedes prime p bezeichne $p\#$ das Produkt aller Primzahlen q mit $q \leq p$. Der Ausdruck $p\#$ wird auch die *Primfakultät* von p genannt.[1]

Folgende Fragen sind bislang ungeklärt:

Gibt es unendlich viele Primzahlen p, für die $p\# + 1$ prim ist?
Gibt es unendlich viele Primzahlen p, für die $p\# + 1$ zerlegbar ist?

[1] Anm. d. Übers.: Nach einem Vorschlag von Dubner (1987) wird im Englischen das Produkt $p\#$ als *primorial of p* bezeichnet, in Anlehnung an das englische Wort *factorial* für die Fakultät einer Zahl.

Rekord

Die größten bekannten Primzahlen der Form $p\# + 1$ sind:

Primzahl	Stellen	Jahr	Entdecker
$392113\# + 1$	169966	2001	D. Heuer u. a.
$366439\# + 1$	158936	2001	D. Heuer u. a.
$145823\# + 1$	63142	2000	A.E. Anderson, D.E. Robinson u. a.

Die Zahlen $p\# + 1$ wurden für alle $p < 120000$ von Caldwell & Gallot (2002) auf ihre Primalität hin untersucht. Dabei stellte sich heraus, dass sie im betrachteten Intervall nur für $p = 2$, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, 24029 und 42209 prim sind. Frühere Arbeiten stammen von Borning (1972), Templer (1980), Buhler, Crandall & Penk (1982), Caldwell & Dubner (1993), und Caldwell (1995).

Caldwell & Gallot führten eine ähnliche Untersuchung für Zahlen der Form $p\# - 1$ durch. Im oben erwähnten Artikel wird berichtet, dass diese Zahlen im Bereich von $p < 120000$ nur für $p = 3$, 5, 11, 13, 41, 89, 317, 337, 991, 1873, 2053, 2377, 4093, 4297, 4583, 6569, 13033 und 15877 Primzahlen sind.

Inzwischen weiß man, dass für die Formen $p\# + 1$ und $p\# - 1$ außer den genannten Primzahlen keine weiteren mit $p < 637000$ beziehungsweise $p < 650000$ existieren.

Der Beweis von Euklid wirft noch weitere Fragen auf. Eine davon ist diese: Man betrachte die Folge $q_1 = 2$, $q_2 = 3$, $q_3 = 7$, $q_4 = 43$, $q_5 = 139$, $q_6 = 50\,207$, $q_7 = 340\,999$, $q_8 = 2\,365\,347\,734\,339, \ldots$, wo q_{n+1} der größte Primfaktor von $q_1 q_2 \cdots q_n + 1$ ist (so dass $q_{n+1} \neq q_1, q_2, \ldots, q_n$). Hierzu stellte Mullin (1963) folgende Fragen: Enthält die Folge $(q_n)_{n\geq 1}$ alle Primzahlen? Falls nicht, sind nur endlich viele ausgeschlossen? Ist die Folge monoton?

Was die erste Frage angeht, so ist leicht einzusehen, dass die 5 in Mullins Folge nicht vorkommen kann. Darüber hinaus fanden Cox & van der Poorten (1968) Kongruenzkriterien, mit deren Hilfe man entscheiden kann, ob eine Primzahl nicht zur Folge gehört. Auf diese Weise konnten sie zeigen, dass 2, 3, 7 und 43 die einzigen Primzahlen bis einschließlich 47 sind, die Mullins Folge angehören. Der ausführliche Beweis ist im Buch von Narkiewicz (2000) enthalten.

Bezüglich der zweiten Frage herrscht die Meinung vor, dass es unendlich viele Primzahlen gibt, die nicht Element von Mullins Folge sind, was die zweite Frage negativ beantworten würde. Schließlich konnte Naur 1984 durch Erweiterung vorausgegangener Berechnungen zeigen, dass $q_{10} < q_9$; die Folge ist also nicht monoton.

Im Jahre 1991 betrachtete Shanks die ähnlich erzeugte Folge $l_1 = 2$, $l_2 = 3$, $l_3 = 7$, $l_4 = 43$, $l_5 = 13$, $l_6 = 53$, $l_7 = 5$, $l_8 = 6\,221\,671$, ..., wobei diesmal l_{n+1} der kleinste Primfaktor von $l_1 l_2 \cdots l_n + 1$ ist. Shanks vermutete, dass $(l_n)_{n\geq 1}$ sämtliche Primzahlen enthält. Die Gültigkeit dieser Aussage ist bisher weder bewiesen noch widerlegt. Wagstaff bestimmte 1993 alle Folgenglieder l_n mit $n \leq 43$, indem er Berechnungen von Guy & Nowakowski aus dem Jahre 1975 fortführte.

Die Berechnung von Gliedern dieser beiden Folgen erfordert es in der Regel, Zahlen von beträchtlicher Größe in ihre Primteiler zu zerlegen. Dies wird mit zunehmender Stellenanzahl immer schwieriger.

So konnten erst im März 2010 vier weitere Folgenglieder l_n bestimmt werden, nachdem l_{44} als ein 68-stelliger Primteiler der 180-stelligen Zahl $l_1 l_2 \cdots l_{43} + 1$ gefunden war. Zur Bestimmung des nächsten Terms l_{48} ist nun eine 256-stellige Zahl zu faktorisieren.

Auf das Problem der Faktorisierung von Zahlen werde ich in Kapitel 2, Abschnitt XI, D eingehen.

Im Jahre 1985 betrachtete Odoni die ähnlich erzeugte Folge

$$w_1 = 2,\ w_2 = 3,\ w_3 = 7,\ \ldots,\ w_{n+1} = w_1 w_2 \cdots w_n + 1$$

und zeigte, dass es unendlich viele Primzahlen gibt, die kein Glied der Folge teilen. Andererseits gibt es natürlich unendlich viele Primzahlen, die irgendein w_i teilen.

II Ein Beweis von Goldbach!

Der Grundgedanke im Beweis von Goldbach ist zugleich einfach und ergiebig. Es genügt, eine unendliche Folge natürlicher Zahlen $1 < a_1 < a_2 < a_3 < \cdots$ zu finden, die paarweise teilerfremd sind (das heißt, sie haben keine gemeinsamen Teiler). Falls also p_1 eine Primzahl ist, die a_1 teilt, die Primzahl p_2 die Zahl a_2 teilt, und so weiter, dann sind alle $p_1, p_2, \ldots$ verschieden.

Der Sinn dieses Ansatzes besteht darin, dass der größte gemeinsame Teiler durch fortgesetzte euklidische Divisionen ermittelt werden kann, ohne dass die Primfaktoren der Zahlen bekannt sein müssten.

Für einen guten Einfall scheint niemand die Urheberschaft beanspruchen zu können, insbesondere dann, wenn es sich um einen einfachen Gedanken handelt. In diesem Fall dachte ich ursprünglich, dass er von Pólya & Szegö stammt (siehe deren Buch von 1924). E. Specker wies mich aber darauf hin, dass Pólya eine Übungsaufgabe von Hurwitz (1891) verwendet hatte. Schließlich machte W. Narkiewicz mich darauf aufmerksam, dass es Goldbach war, der den nachfolgenden Beweis in einem Brief an Euler (20./31. Juli 1730) aufschrieb. Dieser Beweis, der auf den Fermat-Zahlen beruht, ist vielleicht der einzige, den Goldbach schriftlich festgehalten hat.

Die Fermat-Zahlen $F_n = 2^{2^n} + 1$ *(für* $n \geq 0$*) sind paarweise teilerfremd.*

Beweis. Durch Induktion über m kann man leicht zeigen, dass $F_m - 2 = F_0 F_1 \cdots F_{m-1}$; daher ist F_n Teiler von $F_m - 2$, wenn $n < m$. Falls nun eine Primzahl p sowohl F_n als auch F_m teilen sollte, müsste sie auch $F_m - 2$ und F_m und somit die 2 teilen, daher bleibt nur $p = 2$. Aber F_n ist ungerade und deshalb nicht durch 2 teilbar, was zeigt, dass die beiden Fermat-Zahlen teilerfremd sind. □

Im Einzelnen lauten die ersten Fermat-Zahlen $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. Es sind allesamt Primzahlen. F_5 ist bereits 10-stellig, und jede weitere Fermat-Zahl ist ungefähr so groß wie das Quadrat der vorherigen, so dass die Zahlen der Folge sehr rasch anwachsen. Die Frage, ob für gegebenes n die Zahl F_n eine Primzahl ist oder wie man gegebenenfalls einen Primteiler von ihr finden kann, stellt ein wichtiges Problem dar, das ich in Kapitel 2 noch einmal aufgreifen werde.

Es wäre wünschenswert, weitere unendliche Folgen paarweise teilerfremder Zahlen zu finden, ohne dabei die Existenz unendlich vieler Primzahlen vorauszusetzen. In einer 1964 erschienenen Arbeit ging Edwards dieser Frage nach und gab verschiedene solcher rekursiv definierter Folgen an. Wenn beispielsweise S_0 und a teilerfremde ganze Zahlen sind, wobei $S_0 > a \geq 1$, dann sind die Glieder der durch die rekursive Relation

$$S_n - a = S_{n-1}(S_{n-1} - a) \quad (\text{für } n \geq 1)$$

definierten Folge S_n paarweise teilerfremd. Im einfachsten Falle, wenn also $S_0 = 3$ und $a = 2$, ergibt sich die Folge der Fermat-Zahlen: $S_n = F_n = 2^{2^n} + 1$.

Entsprechend erhält man, wenn S_0 ungerade ist und

$$S_n = S_{n-1}^2 - 2 \quad (\text{für } n \geq 1),$$

gesetzt wird, wiederum eine Folge S_n paarweise teilerfremder Zahlen.

Diese Folge, die ähnlich schnell wächst wie die obige, wurde von Lucas näher untersucht. Ich werde darauf in Kapitel 2 zurückkommen.

Ebenfalls ohne die Unendlichkeit der Anzahl von Primzahlen vorauszusetzen, fand Bellman im Jahre 1947 eine Methode, unendliche Folgen paarweise teilerfremder Zahlen zu erzeugen. Man beginnt mit einem nichtkonstanten Polynom $f(X)$ mit ganzzahligen Koeffizienten, wobei $f(0) \neq 0$. Zudem gelte, dass immer wenn n, $f(0)$ teilerfremd sind, dies auch für $f(n)$, $f(0)$ der Fall ist. Nun sei $f_1(X) = f(X)$ und $f_{m+1}(X) = f\big(f_m(X)\big)$ für $m \geq 1$.

Wenn es vorkommt, dass $f_m(0) = f(0)$ für alle $m \geq 1$, und außerdem n und $f(0)$ teilerfremd sind, dann sind auch die Zahlen n, $f_1(n)$, $f_2(n), \ldots, f_m(n), \ldots$ paarweise teilerfremd. So erfüllt beispielweise $f(X) = (X-1)^2 + 1$ die Voraussetzungen, und es ergibt sich $f_n(-1) = 2^{2^n} + 1$, womit wir wieder bei den Fermat-Zahlen sind!

Die folgende Beweisvariante, die auf den Ansatz von Hurwitz zurückgeht, wurde mir freundlicherweise von P. Schorn mitgeteilt.

Beweis von Schorn. Zunächst stellt man fest: Wenn n eine natürliche Zahl ist und $1 \leq i < j \leq n$, dann gilt

$$\mathrm{ggT}\big((n!)i + 1, (n!)j + 1\big) = 1.$$

Denn wenn man $j = i + d$ setzt, dann ist $1 \leq d < n$ und daher

$$\mathrm{ggT}\big((n!)i + 1), (n!)j + 1\big) = \mathrm{ggT}\big((n!)i + 1, n!d\big) = 1,$$

weil jede Primzahl p, die $(n!)d$ teilt, höchstens gleich n ist.

Falls nun die Anzahl der Primzahlen m wäre und man $n = m + 1$ wählt, folgt aus obiger Bemerkung, dass die $m+1$ Zahlen $(m+1)!i+1$ $(1 \leq i \leq m+1)$ paarweise teilerfremd sind, so dass es mindestens $m + 1$ verschiedene Primzahlen geben muss, ein Widerspruch zur Annahme. □

III Beweis von Euler

Dies ist ein eher indirekter Beweis, den man in einem gewissem Sinne als unnatürlich bezeichnen kann. Andererseits führt er jedoch zu höchst bedeutsamen Folgerungen, auf die ich noch hinweisen werde.

Euler zeigte, dass es unendlich viele Primzahlen geben muss, weil ein bestimmter, aus allen Primzahlen gebildeter Ausdruck unendlich groß wird.

Es sei p eine beliebige Primzahl. Dann ist $1/p < 1$, und die geometrische Reihe summiert sich zu

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-(1/p)} .$$

Für eine weitere Primzahl q ergibt sich analog

$$\sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1-(1/q)} .$$

Indem man diese Gleichungen miteinander multipliziert, erhält man:

$$1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \cdots = \frac{1}{1-(1/p)} \times \frac{1}{1-(1/q)} .$$

Die linke Seite ist genau die Summe der Inversen aller natürlichen Zahlen der Form $p^h q^k$ ($h \geq 0$, $k \geq 0$), wobei jede genau einmal gezählt wird, denn jede natürliche Zahl besitzt eine eindeutige Darstellung als Produkt von Primfaktoren. Diese einfache Idee ist die Basis des nun folgenden Beweises.

Beweis von Euler. Angenommen, $p_1, p_2, \ldots, p_n$ seien sämtliche Primzahlen. Für jedes $i = 1, \ldots, n$ ist

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1-(1/p_i)} .$$

Wenn man diese n Gleichungen miteinander multipliziert, erhält man

$$\prod_{i=1}^{n} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \prod_{i=1}^{n} \frac{1}{1-(1/p_i)} .$$

Die linke Seite ist gleich der Summe der Inversen aller natürlichen Zahlen, jeweils einmal gezählt, was sich aus der Eindeutigkeit der Primfaktorenzerlegung ergibt.

Die Reihenfolge der Summation ist beliebig, weil die Summanden der Reihe positiv sind. Daher ist die linke Seite gleich $\sum_{n=1}^{\infty}(1/n)$, und diese Reihe ist divergent. Doch die rechte Seite hat offensichtlich einen endlichen Wert, und dies ist ein Widerspruch. □

In Kapitel 4 werde ich auf die Entwicklungen eingehen, die sich hieraus ergeben.

IV Beweis von Thue

Der Beweis von Thue (1897) benutzt lediglich den Fundamentalsatz der eindeutigen Darstellung einer natürlichen Zahl als ein Produkt von Primfaktoren.

Beweis von Thue. Es seien $n, k \geq 1$ natürliche Zahlen, die der Ungleichung $(1+n)^k < 2^n$ genügen, und $p_1 = 2$, $p_2 = 3$, $\ldots$, p_r alle Primzahlen bis 2^n. Nehmen wir an, dass $r \leq k$.

Aufgrund des Fundamentalsatzes über die Primfaktorenzerlegung lässt sich jede Zahl m, $1 \leq m \leq 2^n$, in eindeutiger Weise schreiben als

$$m = 2^{e_1} \cdot 3^{e_2} \cdots p_r^{e_r},$$

wobei $0 \leq e_1 \leq n$, $0 \leq e_2 \leq n, \ldots, 0 \leq e_r \leq n$.

Das Abzählen aller möglichen Kombinationen ergibt

$$2^n \leq (n+1)n^{r-1} < (n+1)^r \leq (n+1)^k < 2^n,$$

was nicht sein kann. Also muss $r \geq k+1$ sein.

Wähle nun $n = 2k^2$. Aus $1 + 2k^2 < 2^{2k}$ für jedes $k \geq 1$ gewinnt man

$$(1+2k^2)^k < 2^{2k^2} = 4^{k^2}.$$

Daher gibt es bis 4^{k^2} mindestens $k+1$ Primzahlen. Da aber k beliebig gewählt werden kann, zeigt dies, dass es unendlich viele Primzahlen gibt. □

Tatsächlich zeigt der Beweis auch, dass $k+1$ eine untere Schranke für die Anzahl der Primzahlen kleiner als 4^{k^2} ist, was sogar ein quantitatives Resultat darstellt – wenngleich ein ziemlich schlechtes.

Im Kapitel 4 werde ich Fragen dieser Art noch einmal aufgreifen.

V Drei vergessene Beweise

Die nächsten Beweise stammen von Perott, Auric und Métrod. Wer erinnert sich schon an diese Namen? Wenn es nicht Dicksons *History of the Theory of Numbers* gäbe, wären sie wohl völlig in Vergessenheit geraten. Wie ich zeigen werde, sind diese Beweise gleichermaßen unterhaltsam wie geistreich, obwohl sie zu keinen neuen Erkenntnissen führen.

A Beweis von Perott

Der Beweis von Perott stammt aus dem Jahre 1881.

Man muss hierzu wissen, dass die Reihe $\sum_{n=1}^{\infty}(1/n^2)$ konvergiert, mit einer Summe kleiner als 2. (Dass diese Summe genau $\pi^2/6$ beträgt, ist ein berühmtes Resultat von Euler, auf das ich in Kapitel 4 noch einmal zurückkommen werde.) Tatsächlich ist

$$\sum_{n=1}^{\infty}\frac{1}{n^2} < 1+\sum_{n=1}^{\infty}\frac{1}{n(n+1)} = 1+\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right) = 1+1 = 2.$$

Nehmen wir nun an, es gäbe nur r Primzahlen $p_1 < p_2 < \cdots < p_r$. Es sei N eine beliebige ganze Zahl mit $p_1p_2\cdots p_r < N$. Die Anzahl derjenigen $m \le N$, die nicht durch ein Quadrat teilbar sind, ist 2^r (was genau der Anzahl der möglichen Mengen verschiedener Primzahlen entspricht), weil jede Zahl in eindeutiger Weise das Produkt von Primzahlen ist. Da nur höchstens N/p_i^2 Zahlen $m \le N$ durch p_i^2 teilbar sind, ist die Anzahl derjenigen $m \le N$, die sich durch irgendein Quadrat teilen lassen, höchstens gleich $\sum_{i=1}^{r}(N/p_i^2)$. Daher ist

$$N \le 2^r + \sum_{i=1}^{r}\frac{N}{p_i^2} < 2^r + N\left(\sum_{n=1}^{\infty}\frac{1}{n^2}-1\right) = 2^r + N(1-\delta),$$

für ein $\delta > 0$.

Wenn man N so wählt, dass $N\delta \ge 2^r$ wird, führt dies zu einem Widerspruch. □

B Beweis von Auric

Der Beweis von Auric, der 1915 veröffentlicht wurde, ist sehr einfach.

Angenommen, es gäbe nur r Primzahlen $p_1 < p_2 < \cdots < p_r$. Es sei $t \ge 1$ eine beliebige ganze Zahl und $N = p_r^t$. Aufgrund der eindeutigen Primfaktorenzerlegung lässt sich jede Zahl m, $1 \le m \le N$, als $m = p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r}$ schreiben, wobei die Folge $(f_1, f_2, \ldots, f_r)$, $f_i \ge 0$, eindeutig festgelegt ist. Aus $p_1^{f_i} \le p_i^{f_i} \le m \le N = p_r^t$ ergibt sich für $i = 1, 2, \ldots, r$, dass $f_i \le tE$, wobei $E = (\log p_r)/(\log p_1)$. Daher ist die Anzahl N (von ganzen Zahlen m, $1 \le m \le N$) höchstens gleich der Anzahl von Folgen $(f_1, f_2, \ldots, f_r)$, und somit ist $p_r^t = N < (tE+1)^r < t^r(E+1)^r$. Für genügend großes t wird diese Ungleichung unwahr, was zeigt, dass die Anzahl der Primzahlen ins Unendliche wachsen muss. □

C Beweis von Métrod

Der Beweis von Métrod aus dem Jahre 1917 ist ebenfalls sehr einfach.

Angenommen, es gäbe nur r Primzahlen $p_1 < p_2 < \cdots < p_r$. Es sei $N = p_1 p_2 \cdots p_r$, und $Q_i = N/p_i$ für $i = 1, 2, \ldots, r$. Für kein i teilt p_i die Zahl Q_i, wohingegen p_i Teiler von Q_j ist, sofern $j \neq i$. Man setze nun $S = \sum_{i=1}^{r} Q_i$ und bezeichne mit q einen beliebigen Primteiler von S. Dann ist q verschieden von allen p_i, denn p_i teilt Q_j für alle $i \neq j$, doch p_i ist kein Teiler von Q_i. Daher muss q eine weitere Primzahl sein! □

VI Beweis von Washington

Der Beweis von Washington (1980) führt über kommutative Algebra. Die Zutaten sind elementare Fakten der Theorie der Hauptidealringe, Faktorringe, Dedekindscher Ringe und algebraischer Zahlen, und können in jedem einschlägigen Fachbuch nachgelesen werden, wie etwa dem von Samuel (1967): Es sind keinerlei Geheimnisse damit verbunden. Zunächst werde ich die benötigten Tatsachen angeben:

1. In jedem Zahlkörper endlichen Grades ist der Ring der algebraischen Zahlen ein Dedekindscher Ring: Jedes vom Nullideal verschiedene Ideal ist in eindeutiger Weise ein Produkt von Primidealen.

2. In jedem Zahlkörper endlichen Grades gibt es nur endlich viele Primideale, die eine beliebige gegebene Primzahl p teilen.

3. Ein Dedekindscher Ring mit nur endlich vielen Primidealen ist ein Hauptidealring, und somit ist jedes von Null verschiedene Element das bis auf Einheiten eindeutige Produkt von Primelementen.

Beweis von Washington. Man betrachte den Körper aller Zahlen der Form $a + b\sqrt{-5}$, wobei a, b rationale Zahlen sind. Der Ring der algebraischen Zahlen dieses Körpers setzt sich aus den Zahlen obiger Form zusammen, in denen a, b gewöhnliche ganze Zahlen sind. Man kann leicht zeigen, dass 2, 3, $1+\sqrt{-5}$, $1-\sqrt{5}$ Primzahlen dieses Rings sind, da sie sich nicht in das Produkt algebraischer Zahlen zerlegen lassen, es sei denn, einer der Faktoren ist eine „Einheit“ 1 oder -1. Man beachte zudem, dass

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2 \times 3,$$

so dass die Zerlegung der 6 in Primfaktoren nicht eindeutig ist. Daher ist dieser Ring kein Faktorring und somit auch kein Hauptidealring. Es muss also nach obiger Tatsache 3 unendlich viele Primideale geben, und aufgrund von Tatsache 2 ist die Existenz unendlich vieler Primzahlen nachgewiesen. □

VII Beweis von Furstenberg

Dieser originelle Beweis basiert auf topologischen Überlegungen und wurde 1955 veröffentlicht. Da er so kurz ist, kann ich ihn nicht besser darstellen als im Wortlaut. Hier wird er in deutscher Übersetzung wiedergegeben:

> In dieser Mitteilung möchten wir einen elementaren „topologischen“ Beweis der Unendlichkeit der Primzahlen vorschlagen. Wir führen eine Topologie im Raum der ganzen Zahlen S ein, indem wir die arithmetischen Folgen ($-\infty$ bis $+\infty$) als Basis verwenden. Es ist nicht schwer zu verifizieren, dass dies wirklich einen topologischen Raum darstellt. Tatsächlich kann man zeigen, dass S unter dieser Topologie normal und daher metrisierbar ist. Jede arithmetische Folge ist abgeschlossen und auch offen, da ihr Komplement die Vereinigung anderer arithmetischer Folgen derselben Differenz ist. Daraus resultiert, dass die Vereinigung jeder endlichen Anzahl arithmetischer Folgen abgeschlossen ist. Betrachte nun die Menge $A = \bigcup A_p$, wobei A_p sich aus allen Vielfachen von p zusammensetzt und p die Menge der Primzahlen ≥ 2 durchläuft. Die einzigen Zahlen, die nicht zu A gehören, sind -1 und 1, und da die Menge $\{-1, 1\}$ offensichtlich nicht offen ist, kann A nicht abgeschlossen sein. Daher ist A keine endliche Vereinigung abgeschlossener Mengen, was beweist, dass es unendlich viele Primzahlen gibt. □

Golomb hat Furstenbergs Gedanken weiterentwickelt und veröffentlichte 1959 einen interessanten kleinen Artikel darüber.