
Martin Aigner · Günter M. Ziegler
Das BUCH der Beweise
Springer

Das BUCH der Beweise

Martin Aigner
Günter M. Ziegler

Das BUCH der Beweise

5. Auflage

Mit Zeichnungen von Karl H. Hofmann

Springer

Martin Aigner
Institut für Mathematik
Freie Universität Berlin
Berlin, Deutschland

Günter M. Ziegler
Institut für Mathematik
Freie Universität Berlin
Berlin, Deutschland

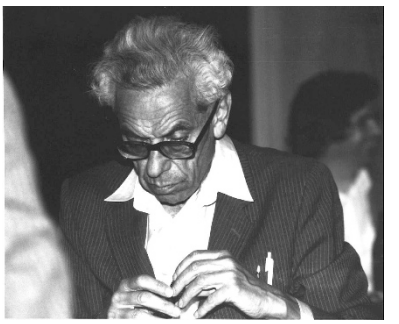
ISBN 978-3-662-57766-0 ISBN 978-3-662-57767-7 (eBook)
https://doi.org/10.1007/978-3-662-57767-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Paul Erdős erzählte gerne von dem BUCH, in dem Gott die *perfekten* Beweise für mathematische Sätze aufbewahrt, dem berühmten Zitat von G. H. Hardy entsprechend, dass es für hässliche Mathematik keinen dauerhaften Platz gibt. Erdős hat auch gesagt, dass man nicht an Gott zu glauben braucht, aber dass man als Mathematiker an das BUCH glauben sollte. Vor ein paar Jahren haben wir ihm vorgeschlagen, gemeinsam eine erste (und sehr bescheidene) Annäherung an das BUCH aufzuschreiben. Er hat die Idee enthusiastisch aufgenommen und sich, ganz typisch für ihn, sofort an die Arbeit gemacht und Seiten über Seiten mit Notizen und Vorschlägen produziert. Unser Buch sollte ursprünglich im März 1998 erscheinen, als Geschenk zu Erdős' 85stem Geburtstag. Durch seinen Tod im Sommer 1996 konnte er kein Koautor werden. Stattdessen ist dieses Buch seinem Andenken gewidmet.



Paul Erdős

Wir haben keine Definition oder Charakterisierung dafür, was einen Beweis zum BUCH-Beweis macht; anbieten können wir hier nur die Beispiele, die *wir* ausgewählt haben, in der Hoffnung, dass die Leser unseren Enthusiasmus teilen werden über brillante Ideen, schlaues Vorgehen, wunderschöne Einsichten und überraschende Wendungen. Wir hoffen auch, dass unsere Leser dies trotz aller Defizite in unserer Darstellung genießen können. Die Auswahl der Beweise hat Paul Erdős selbst stark beeinflusst. Er hat eine große Zahl der Themen vorgeschlagen, und viele der Beweise gehen direkt auf ihn zurück oder sie entstanden durch sein besonderes Talent dafür, die richtige Frage zu stellen oder die richtige Vermutung zu formulieren. So spiegelt dieses Buch in großem Umfang das wider, was nach Paul Erdős Beweise aus dem BUCH ausmacht.

„DAS BUCH“

Beschränkt wurde unsere Auswahl von Themen dadurch, dass wir für die Lektüre nicht mehr Mathematik voraussetzen wollten, als man im Grundstudium lernt. Ein bisschen Lineare Algebra, ein bisschen Analysis und Zahlentheorie, und ein gerüttelt Maß elementarer Konzepte und Ideen aus der Diskreten Mathematik sollten ausreichen, um alles in diesem Buch zu verstehen und zu genießen.

Wir sind den vielen Menschen unendlich dankbar, die uns bei diesem Projekt geholfen und unterstützt haben — unter ihnen den Studenten aus einem Seminar, in dem eine erste Version des Buches besprochen wurde, wie auch Benno Artmann, Stephan Brandt, Stefan Felsner, Eli Goodman, Hans Mielke und besonders Tom Trotter. Viele Leser der englischen Ausgabe dieses Buches haben uns geschrieben und mit ihren Anmerkungen und Hinweisen die zweite englische wie auch diese deutsche Ausgabe gefördert, unter ihnen Christian Elsholtz, Jürgen Elstrodt, Daniel Grieser,

Roger Heath-Brown, Lee L. Keener, Christian Lebœuf, Hanfried Lenz, Nicolas Puech, John Scholes, Bernulf Weißbach, Dirk Werner und *viele* andere. Mit der Technik und Gestaltung dieses Buches haben uns unter anderem Margrit Barrett, Christian Bressler, Christoph Eyrich, Ewgenij Gawrilow, Michael Joswig und Jörg Rambau immens geholfen. Elke Pose danken wir für den Einsatz und den Enthusiasmus, mit dem sie viele viele kleine verrauschte Diktierkassetten in perfektes LaTeX verwandelt hat. Herzlichen Dank schulden wir Ruth Allewelt und Karl-Friedrich Koch vom Springer-Verlag Heidelberg. Ganz besonderer Dank (er weiß wofür) geht an Torsten Heldmann. Karl Heinrich Hofmann danken wir für die wunderbaren Zeichnungen, mit denen wir diesen Band illustrieren dürfen, und dem großen Paul Erdős für seine Inspiration.

Berlin, September 2001 *Martin Aigner · Günter M. Ziegler*

Vorwort zur fünften Auflage

Die Idee zu diesem Projekt wurde während mehrerer Gespräche mit dem unvergleichlichen Paul Erdős im Mathematischen Forschungsinstitut Oberwolfach geboren. Vor fast zwanzig Jahren haben wir das Buch auf dem Internationalen Mathematiker-Kongress 1998 in Berlin präsentiert, zuerst nur auf Englisch: Damals konnten wir uns unmöglich vorstellen, welch wunderbare und andauernde Resonanz unser Buch über DAS BUCH haben würde, mit all den herzlichen Briefen, interessanten Kommentaren und Vorschlägen, neuen Auflagen, und bis heute dreizehn Übersetzungen. Es ist keine Übertreibung zu sagen, dass die Arbeit am Buch ein Teil unseres Lebens geworden ist.

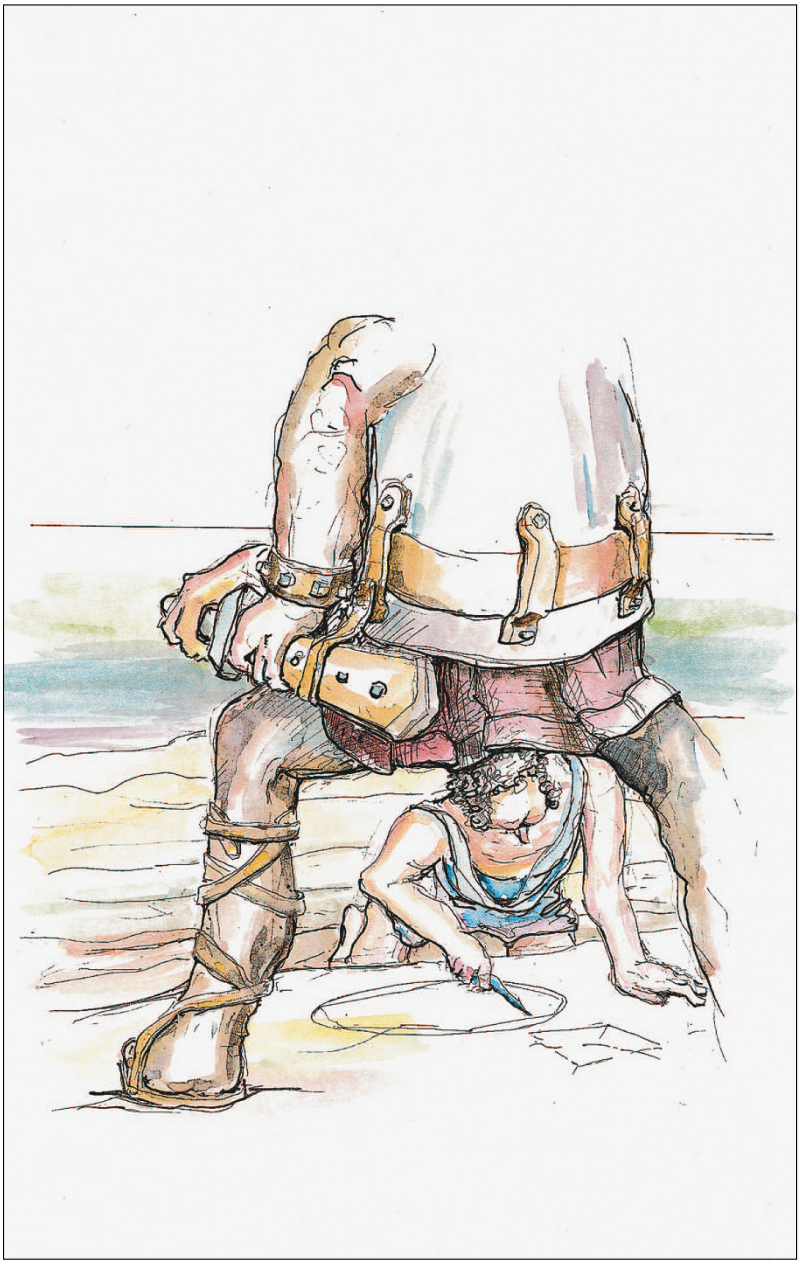
Diese fünfte deutsche Auflage enthält neben verschiedenen Ergänzungen, von denen viele von unseren Lesern vorgeschlagen wurden, auch ein ganz neues Kapitel über van der Waerdens Permanenten-Vermutung.

Wir danken allen, die uns über all diese Jahre geholfen und ermutigt haben. Die zweite deutsche Auflage hat von besonders wertvollen Hinweisen von David Bevan, Anders Björner, Dietrich Braess, John Cosgrave, Hubert Kalf, Günter Pickert, Alistair Sinclair und Herb Wilf profitiert. Für die dritte Auflage danken wir besonders Oliver Deiser, Michael Harbeck, Stefan Hougardy, Hendrik W. Lenstra, Günter Rote, Carsten Schultz und Moritz W. Schmitt für ihre Beiträge. Für die vierte Auflage sind wir Ian Agol, France Dacar, Christopher Deninger, Michael D. Hirschhorn, Franz Lemmermeyer, Raimund Seidel, Tord Sjödin und John M. Sullivan dankbar für Ideen und Vorschläge, sowie Christoph Eyrich, Marie-Sophie Litz, Miriam Schlöter und Jan Schneider für technische Hilfe. Die fünfte Auflage hat besonders von Hinweisen von David Benko, France Dacar, Jan Peter Schäfermeyer und Yuliya Semikina profitiert. Danke wie immer an Elke Pose und Torsten Heldmann für die Unterstützung im Hintergrund. Ganz besonderer Dank gebührt Ruth Allewelt vom Springer-Verlag in Heidelberg sowie Karl Heinrich Hofmann, der immer wieder neue wunderbare Zeichnungen beigesteuert hat.

Berlin, März 2018 *Martin Aigner · Günter M. Ziegler*

Inhalt

Zahlentheorie



„Irrationalität und π“

Sechs Beweise für die Unendlichkeit der Primzahlen

Kapitel 1

Es liegt nahe, dass wir mit dem wahrscheinlich ältesten Beweis aus dem BUCH beginnen: Euklids Beweis, dass es unendlich viele Primzahlen gibt.

■ **Euklids Beweis.** Für eine beliebige endliche Menge $\{p_1, \ldots, p_r\}$ von Primzahlen sei $n := p_1 p_2 \cdots p_r + 1$ und p ein Primteiler von n. Wir sehen, dass p von allen p_i verschieden ist, da sonst p sowohl die Zahl n als auch das Produkt $p_1 p_2 \cdots p_r$ teilen würde, somit auch die 1, was nicht sein kann. Eine endliche Menge $\{p_1, \ldots, p_r\}$ kann also niemals die Menge *aller* Primzahlen sein. □

Bevor wir fortfahren, wollen wir einige (sehr übliche) Bezeichnungen einführen: so schreiben wir $\mathbb{N} = \{1, 2, 3, \ldots\}$ für die Menge der natürlichen Zahlen, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ ist die Menge der ganzen Zahlen, und $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ bezeichnet die Menge der Primzahlen.

Im Folgenden werden wir einige weitere Beweise kennenlernen (aus einer viel längeren Liste), die uns und hoffentlich auch den Lesern besonders gefallen. Wenn diese Beweise auch verschiedene Ansätze benutzen, so ist doch allen eine Idee gemeinsam: die natürlichen Zahlen wachsen ins Unendliche, und jede natürliche Zahl $n \geq 2$ hat einen Primteiler. Diese beiden Tatsachen erzwingen, dass die Menge $\mathbb{P}$ unendlich ist. Der nächste Beweis ist von Christian Goldbach (aus einem Brief an Leonhard Euler 1730), der dritte Beweis ist offenbar Folklore, der vierte von Euler selbst, der fünfte wurde von Harry Fürstenberg vorgeschlagen, und der letzte stammt von Paul Erdős.

Der zweite und dritte Beweis benutzt jeweils eine spezielle Zahlenfolge.

■ **Zweiter Beweis.** Betrachten wir zunächst die folgenden *Fermat-Zahlen* $F_n = 2^{2^n} + 1$ für $n = 0, 1, 2, \ldots$. Wir werden zeigen, dass je zwei Fermat-Zahlen relativ prim sind, also muss es unendlich viele Primzahlen geben. Zum Beweis verifizieren wir die Rekursion

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

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 auch 2 teilt, das heißt, es ist $m = 1$ oder 2. Der Fall $m = 2$ ist aber ausgeschlossen, da alle Fermat-Zahlen ungerade sind.

Zum Beweis der Rekursion verwenden wir Induktion nach n. Für $n = 1$

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

Die ersten Fermat-Zahlen

M. Aigner und G. M. Ziegler, *Das BUCH der Beweise*,
https://doi.org/10.1007/978-3-662-57767-7_1

Der 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

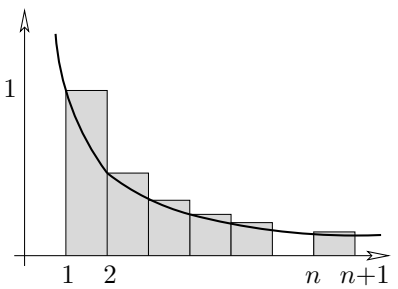
$$a \sim b :\iff ba^{-1} \in U.$$

Es folgt aus den Gruppenaxiomen, dass $\sim$ 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 $|G|$. □

Für den Spezialfall, in dem $U = \{a, a^2, \ldots, a^m\}$ 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. Insbesondere gilt $a^{|G|} = 1$.



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

haben wir $F_0 = 3$ und $F_1 - 2 = 3$. Mit Induktion erhalten wir nun

$$\prod_{k=0}^{n} F_k \;=\; \Big(\prod_{k=0}^{n-1} F_k\Big) F_n \;=\; (F_n - 2)F_n \;=$$
$$= (2^{2^n} - 1)(2^{2^n} + 1) \;=\; 2^{2^{n+1}} - 1 \;=\; F_{n+1} - 2. \qquad \square$$

■ **Dritter Beweis.** Angenommen $\mathbb{P}$ ist endlich und p die größte Primzahl. Dann betrachten wir dieses Mal die so genannte *Mersenne-Zahl* $2^p - 1$ und zeigen, dass jeder Primteiler q von $2^p - 1$ größer als p ist, was den gewünschten Widerspruch ergibt. Sei q ein Primteiler von $2^p - 1$, dann gilt $2^p \equiv 1 \pmod q$. Da p 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 (siehe den Kasten am Rand) wissen, dass die Ordnung jedes Elementes die Gruppengröße teilt, folgt $p \mid q - 1$ und daher $p < q$. □

Als Nächstes kommt ein Beweis, der elementare Analysis benützt.

■ **Vierter Beweis.** Sei $\pi(x) := \#\{p \le x : p \in \mathbb{P}\}$ die Anzahl der Primzahlen, die kleiner oder gleich der reellen Zahl x sind. Wir nummerieren die Primzahlen $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ in aufsteigender Größe. Es sei $\log x$ der natürliche Logarithmus, definiert als $\log x = \int_1^x \frac{1}{t} dt$.

Nun vergleichen wir die Fläche unter dem Graphen der Funktion $f(t) = \frac{1}{t}$ mit einer oberen Treppenfunktion. (Siehe den Anhang auf Seite 13, wo diese Methode erläutert wird.) Für $n \le x < n + 1$ haben wir daher

$$\log x \;\le\; 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}$$
$$\le\; {\sum}' \frac{1}{m}, \quad \text{wobei dies die Summe über alle } m \in \mathbb{N} \text{ bezeichnen soll, die nur Primfaktoren } p \le x \text{ enthalten.}$$

Da jede solche Zahl m auf *eindeutige* Weise als ein Produkt der Form $\prod_{p \le x} p^{k_p}$ geschrieben werden kann, sehen wir, dass die letzte Summe gleich

$$\prod_{\substack{p \in \mathbb{P} \\ p \le x}} \Big(\sum_{k \ge 0} \frac{1}{p^k}\Big)$$

ist. Die innere Summe ist eine geometrische Reihe mit Faktor $\frac{1}{p}$, woraus

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

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

$$\frac{p_k}{p_k - 1} \;=\; 1 + \frac{1}{p_k - 1} \;\le\; 1 + \frac{1}{k} \;=\; \frac{k+1}{k},$$

erhalten wir

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

Nun wissen wir, dass die Funktion $\log x$ nicht beschränkt ist, und schließen daraus, dass $\pi(x)$ ebenfalls unbeschränkt ist: also gibt es unendlich viele Primzahlen. □

■ **Fünfter Beweis.** Nach Analysis kommt jetzt Topologie! Betrachten wir die folgende merkwürdige Topologie auf der Menge $\mathbb{Z}$ der ganzen Zahlen. 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 unendliche arithmetische Folge. Wir nennen nun eine 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. 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 Durchschitt 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:

(A) Jede nicht-leere offene Menge ist unendlich.

(B) Jede Menge $N_{a,b}$ ist auch abgeschlossen.

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

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

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

Bis jetzt haben wir noch nicht von den Primzahlen gesprochen — aber nun kommen sie ins Spiel. Da jede Zahl $n \neq 1, -1$ einen Primteiler p hat und daher in der Menge $N_{0,p}$ enthalten ist, 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 (B) eine endliche Vereinigung von abgeschlossenen Mengen und daher abgeschlossen. Folglich wäre $\{1, -1\}$ eine offene Menge, im Widerspruch zu (A). □

„Flache Steine,
ins Unendliche geworfen“

■ **Sechster Beweis.** Unser letzter Beweis führt uns einen großen Schritt weiter und weist nicht nur nach, dass es unendlich viele Primzahlen gibt, sondern auch, dass die Reihe $\sum_{p\in\mathbb{P}} \frac{1}{p}$ divergiert. Der erste Beweis dieses

wichtigen Resultats wurde von Euler gegeben (und ist ebenfalls sehr interessant), aber der folgende Beweis von Erdős ist von makelloser Schönheit.

Es sei $p_1, p_2, p_3, \dots$ 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 eine natürliche Zahl k geben mit $\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}$. Wir wollen die Primzahlen $p_1, \dots, p_k$ *kleine* Primzahlen nennen, und die anderen $p_{k+1}, p_{k+2}, \dots$ *große* Primzahlen. Für jede beliebige natürliche Zahl N gilt somit

$$\sum_{i\geq k+1} \frac{N}{p_i} \;<\; \frac{N}{2}. \tag{1}$$

Sei N_b die Anzahl der positiven ganzen Zahlen $n \leq N$, die durch mindestens eine große Primzahl teilbar sind, und N_s die Anzahl der positiven Zahlen $n \leq N$, die nur kleine Primteiler besitzen. Wir werden zeigen, dass für ein geeignetes N

$$N_b + N_s \;<\; N$$

gilt, und dies wird den gewünschten Widerspruch ergeben, da nach Definition $N_b + N_s$ natürlich gleich N sein muss.

Um N_b abzuschätzen, bemerken wir, dass $\lfloor \frac{N}{p_i} \rfloor$ die positiven ganzen Zahlen $n \leq N$ zählt, die Vielfache von p_i sind. Mit (1) erhalten wir daraus

$$N_b \;\leq\; \sum_{i\geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \;<\; \frac{N}{2}. \tag{2}$$

Nun betrachten wir N_s. Wir schreiben jede Zahl $n \leq N$, die nur kleine Primteiler hat, in der Form $n = a_n b_n^2$, wobei a_n den quadratfreien Teil bezeichnet. Jedes a_n ist dann ein Produkt von *verschiedenen* kleinen Primzahlen, und wir schließen, dass es genau 2^k verschiedene quadratfreie Teile gibt. Weiter sehen wir wegen $b_n \leq \sqrt{n} \leq \sqrt{N}$, dass es höchstens $\sqrt{N}$ verschiedene Quadratteile gibt, und es folgt

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

Da (2) für *jedes* N gilt, müssen wir nur eine Zahl N finden, die $2^k\sqrt{N} \leq \frac{N}{2}$ erfüllt, oder was dasselbe ist, $2^{k+1} \leq \sqrt{N}$ — und solch eine Zahl ist zum Beispiel $N = 2^{2k+2}$. □

Anhang: Unendlich viele weitere Beweise

Die Liste der Beweise für die Unendlichkeit der Primzahlen enthält noch weitere alte und neue Brillanten, aber einer aus jüngster Zeit ist ganz anders und verdient, eigens herausgehoben zu werden.

Wir versuchen Folgen $S = (s_1, s_2, s_3, \dots)$ zu finden mit der Eigenschaft, dass die Menge $\mathbb{P}_S$ der Primzahlen, die mindestens ein Folgenglied teilen, unendlich ist. Jede solche Folge liefert dann einen neuen Beweis für die Unendlichkeit der Primzahlen. Die Fermat-Zahlen F_n aus dem zweiten

Beweis bilden so eine Folge, während die Potenzen von 2 nicht funktionieren. Viele weitere Beispiele gehen auf einen Satz von Issai Schur zurück, der im Jahr 1912 zeigte, dass für jedes nicht-konstante Polynom $p(x)$ mit ganzzahligen Koeffizienten die Menge $\{p(n) \neq 0 : n \in \mathbb{N}\}$ solch eine Folge bildet. Nehmen wir $p(x) = x$, so liefert Schurs Resultat genau den Satz von Euklid. Als ein weiteres Beispiel ergibt $p(x) = x^2 + 1$, dass die Zahlen der Form „Quadrat plus 1“ unendlich viele verschiedene Primteiler enthalten.


Issai Schur

Das folgende Resultat von Christian Elsholtz ist ein wahres Juwel: es verallgemeinert den Satz von Schur, der Beweis ist einfach nur raffiniertes Abzählen und er ist in einem gewissen Sinne bestmöglich.

Es sei $S = (s_1, s_2, s_3, \dots)$ eine Folge von ganzen Zahlen. Wir sagen

- S ist *fast injektiv*, wenn jeder Wert höchstens c Mal vorkommt für eine Konstante c, und
- S hat *subexponentielles Wachstum*, falls $|s_n| \leq 2^{2^{f(n)}}$ für alle n gilt, wobei $f : \mathbb{N} \to \mathbb{R}_+$ eine Funktion ist mit $\frac{f(n)}{\log_2 n} \to 0$.

(Anstelle der Basis 2 könnten wir jede andere Basis größer als 1 nehmen. Zum Beispiel führt $|s_n| \leq e^{e^{f(n)}}$ auf dieselbe Klasse von Folgen.)

Satz. *Ist $S = (s_1, s_2, s_3, \dots)$ eine fast injektive Folge mit subexponentiellem Wachstum, dann ist die Menge $\mathbb{P}_S$ der Primzahlen, die mindestens eines der Folgenglieder von S teilen, unendlich.*

■ **Beweis.** Wir können annehmen, dass $f(n)$ monoton wächst; anderenfalls ersetzen wir $f(n)$ durch die Funktion $F(n) = \max_{i \leq n} f(i)$; es ist leicht nachzuprüfen, dass mit diesem $F(n)$ die Folge nach wie vor die subexponentielle Wachstumsbedingung erfüllt.

Wir führen nun einen Widerspruchsbeweis: Nehmen wir an, dass $\mathbb{P}_S = \{p_1, \dots, p_k\}$ endlich ist. Wir schreiben jedes s_n als

$$s_n = \varepsilon_n p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \text{ mit } \varepsilon_n \in \{1, 0, -1\}, \ \alpha_i \geq 0,$$

wobei die $\alpha_i = \alpha_i(n)$ von n abhängen. (Für $s_n = 0$ setzen wir $\alpha_i = 0$ für alle i.) Dann gilt

$$2^{\alpha_1 + \cdots + \alpha_k} \ \leq \ |s_n| \ \leq \ 2^{2^{f(n)}} \quad \text{für } s_n \neq 0,$$

und wenn wir den binären Logarithmus nehmen

$$0 \ \leq \ \alpha_i \ \leq \ \alpha_1 + \cdots + \alpha_k \ \leq \ 2^{f(n)} \quad \text{für } 1 \leq i \leq k.$$

Also gibt es nicht mehr als $2^{f(n)} + 1$ mögliche Werte für jedes $\alpha_i = \alpha_i(n)$. Da $f(n)$ monoton ist, ergibt sich daraus eine erste Abschätzung

$$\#\{\text{verschiedene } |s_n| \neq 0 \text{ für } n \leq N\} \ \leq \ (2^{f(N)} + 1)^k \ \leq \ 2^{(f(N)+1)k}.$$

Andererseits ist S fast injektiv, also sind höchstens c der Folgenglieder gleich 0 und jeder positive Absolutwert kann höchstens $2c$ Mal auftreten. Das liefert uns die untere Abschätzung

$$\#\{\text{verschiedene } |s_n| \neq 0 \text{ für } n \leq N\} \ \geq \ \frac{N - c}{2c}.$$

Insgesamt ergibt dies

$$\frac{N-c}{2c} \;\leq\; 2^{k(f(N)+1)},$$

oder nach Logarithmieren

$$\log_2(N-c) - \log_2(2c) \;\leq\; k\,(f(N)+1) \quad \text{für alle } N.$$

Das ist aber für großes N sicher falsch, da k und c Konstanten sind und $\frac{\log_2(N-c)}{\log_2 N}$ für $N \to \infty$ gegen 1 konvergiert, während $\frac{f(N)}{\log_2 N}$ gegen 0 strebt. □

Kann man die Bedingungen abschwächen? Jedenfalls ist keine der beiden überflüssig.

Dass wir die „fast injektive“ Bedingung brauchen, sieht man an Folgen S wie $(2,2,2,\dots)$ oder $(1,2,2,4,4,4,4,8,\dots)$, welche die Wachstumsbedingung erfüllen, wohingegen $\mathbb{P}_S = \{2\}$ endlich ist.

Zur Wachstumsbedingung wollen wir nur bemerken, dass sie jedenfalls nicht zu einer Bedingung der Form $\frac{f(n)}{\log_2 n} \leq \varepsilon$ für ein festes $\varepsilon > 0$ abgeschwächt werden kann. Um das zu sehen, untersucht man für ein großes k und für fest gewählte Primzahlen $p_1, \dots, p_k$ die ansteigende Folge S aller Zahlen der Form $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Diese Folge wächst ungefähr wie $2^{2^{f(n)}}$ mit $\frac{f(n)}{\log_2 n} \approx \frac{1}{k}$, während $\mathbb{P}_S$ nach Konstruktion endlich ist.

Literatur

[1] B. ARTMANN: *Euclid — The Creation of Mathematics,* Springer-Verlag, New York 1999.

[2] C. ELSHOLTZ: *Prime divisors of thin sequences,* Amer. Math. Monthly **119** (2012), 331-333.

[3] P. ERDŐS: *Über die Reihe* $\sum \frac{1}{p}$, Mathematica, Zutphen B **7** (1938), 1-2.

[4] L. EULER: *Introductio in Analysin Infinitorum,* Tomus Primus, Lausanne 1748; Opera Omnia, Ser. 1, Vol. 8.

[5] H. FÜRSTENBERG: *On the infinitude of primes,* Amer. Math. Monthly **62** (1955), 353.

[6] I. SCHUR: *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen,* Sitzungsberichte der Berliner Math. Gesellschaft **11** (1912), 40-50.

Das Bertrandsche Postulat

Kapitel 2

Wir haben gesehen, dass die Primzahlen $2, 3, 5, 7, \ldots$ eine unendliche Folge bilden. Daraus kann man auch folgern, dass es beliebig große Lücken zwischen den Primzahlen geben muss. Schreibt man nämlich $N := 2 \cdot 3 \cdot 5 \cdots p$ für das Produkt aller Primzahlen, die kleiner sind als $k+2$, dann kann keine der k Zahlen

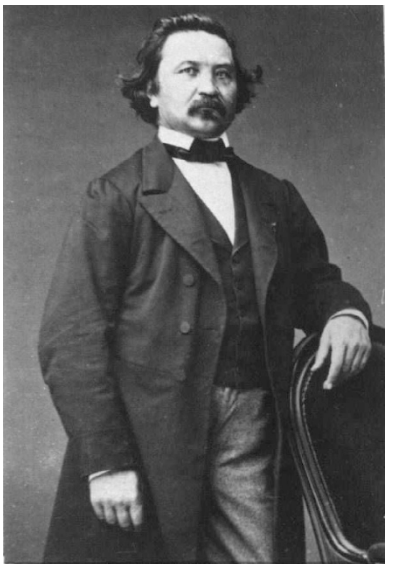
$$N+2, N+3, N+4, \ldots, N+k, N+(k+1)$$

prim sein, denn für $2 \le i \le k+1$ hat i einen Primfaktor, der kleiner ist als $k+2$, und dieser Faktor teilt auch N, und damit auch $N+i$. Mit diesem Rezept finden wir zum Beispiel für $k = 10$, dass keine der zehn Zahlen

$$2312, 2313, 2314, \ldots, 2321$$

prim ist.

Aber es gibt trotzdem obere Schranken für die Größe der Lücken in der Folge der Primzahlen. Das „Bertrandsche Postulat“ besagt nämlich, dass „die Lücke bis zur nächsten Primzahl nie größer sein kann als die Zahl, an der wir die Suche beginnen“. Diese berühmte Behauptung wurde 1845 von Joseph Bertrand aufgestellt und immerhin bis $n = 3\,000\,000$ verifiziert. Vollständig bewiesen, für alle n, hat sie Pafnuty Tschebyschew im Jahr 1850. Einen viel einfacheren Beweis hat das indische Genie Ramanujan gefunden. Unser Beweis aus dem BUCH ist von Paul Erdős: aus seinem ersten Aufsatz, der 1932 erschien, als Erdős 19 war.



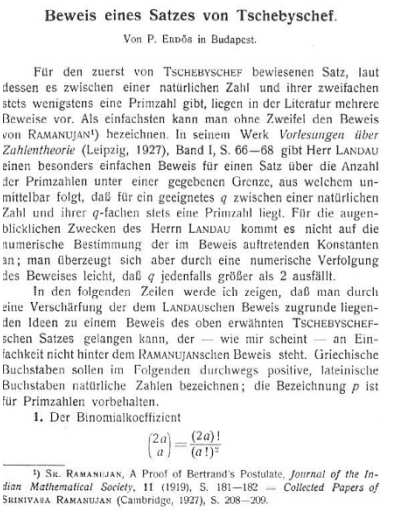
Joseph Bertrand

Das Bertrandsche Postulat
Für jedes $n \ge 1$ gibt es eine Primzahl p mit $n < p \le 2n$.

■ **Beweis.** Wir werden die Größe des Binomialkoeffizienten $\binom{2n}{n}$ so genau abschätzen, dass wir zeigen können, dass der Binomialkoeffizient „zu klein ausfallen“ würde, wenn er keine Primfaktoren im Bereich $n < p \le 2n$ hätte. Die Oper hat insgesamt fünf Akte.

(1) Wir beweisen das Bertrandsche Postulat zunächst für $n \le 511$. Dafür muss man nicht 511 Fälle abarbeiten: Es reicht (das ist der „Landau-Trick“) zu überprüfen, dass

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 521$$



Beweis eines Satzes von Tschebyschef.

Von P. Erdős in Budapest.

Für den zuerst von Tschebyschef bewiesenen Satz, laut dessen es zwischen einer natürlichen Zahl und ihrer zweifachen stets wenigstens eine Primzahl gibt, liegen in der Literatur mehrere Beweise vor. Als einfachsten kann man ohne Zweifel den Beweis von Ramanujan[1]) bezeichnen. In seinem Werk *Vorlesungen über Zahlentheorie* (Leipzig, 1927), Band I, S. 66—68 gibt Herr Landau einen besonders einfachen Beweis für einen Satz über die Anzahl der Primzahlen unter einer gegebenen Grenze, aus welchem unmittelbar folgt, daß für ein geeignetes q zwischen einer natürlichen Zahl und ihrer q-fachen stets eine Primzahl liegt. Für die augenblicklichen Zwecken des Herrn Landau kommt es nicht auf die numerische Bestimmung der im Beweis auftretenden Konstanten an; man überzeugt sich aber durch eine numerische Verfolgung des Beweises leicht, daß q jedenfalls größer als 2 ausfällt.

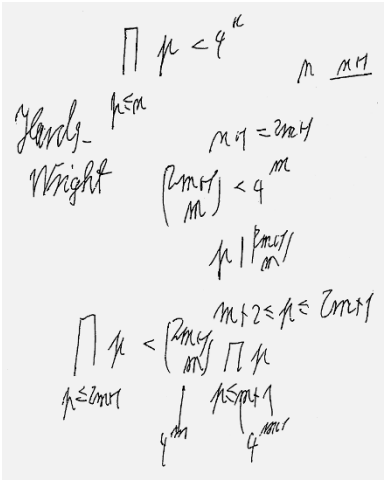
In den folgenden Zeilen werde ich zeigen, daß man durch eine Verschärfung der dem Landauschen Beweis zugrunde liegenden Ideen zu einem Beweis des oben erwähnten Tschebyschefschen Satzes gelangen kann, der — wie mir scheint — an Einfachkeit nicht hinter dem Ramanujanschen Beweis steht. Griechische Buchstaben sollen im Folgenden durchwegs positive, lateinische Buchstaben natürliche Zahlen bezeichnen; die Bezeichnung p ist für Primzahlen vorbehalten.

1. Der Binomialkoeffizient

$$\binom{2a}{a} = \frac{(2a)!}{(a!)^2}$$

[1]) Sr. Ramanujan, A Proof of Bertrand's Postulate, *Journal of the Indian Mathematical Society*, 11 (1919), S. 181—182 — *Collected Papers of* Srinivasa Ramanujan (Cambridge, 1927), S. 208—209.

M. Aigner und G. M. Ziegler, *Das BUCH der Beweise*,
https://doi.org/10.1007/978-3-662-57767-7_2



eine Folge von Primzahlen ist, in der jede Primzahl kleiner ist als zweimal die vorhergehende. Also enthält jedes Interval $\{y : n < y \le 2n\}$, mit $n \le 511$, eine dieser elf Primzahlen.

(2) Als Nächstes zeigen wir

$$\prod_{p\le x} p \;\le\; 4^{x-1} \qquad \text{für alle reellen } x \ge 2, \tag{1}$$

wobei unsere Notation — hier und im Folgenden — implizieren soll, dass das Produkt über alle *Primzahlen* $p \le x$ genommen wird. Unser Beweis dafür verwendet Induktion über die Anzahl dieser Primzahlen. Er stammt nicht aus Erdős' erstem Aufsatz, aber er ist auch von Erdős (der Rand zeigt Notizen dazu in seiner Handschrift), und er ist ein wahrer BUCH-Beweis. Zunächst gilt für die größte Primzahl $q \le x$

$$\prod_{p\le x} p \;=\; \prod_{p\le q} p \qquad \text{und} \qquad 4^{q-1} \;\le\; 4^{x-1}.$$

Damit reicht es, (1) für den Fall zu zeigen, dass $x = q$ eine Primzahl ist. Für $q = 2$ erhalten wir „$2 \le 4$“, also kümmern wir uns jetzt um die ungeraden Primzahlen $q = 2m+1$. (Dabei dürfen wir mit einem Induktionsschluss annehmen, dass die Aussage schon für alle ganzen Zahlen in $\{2, 3, \ldots, 2m\}$ bewiesen ist.) Für $q = 2m+1$ zerlegen wir das Produkt und rechnen

$$\prod_{p\le 2m+1} p \;=\; \prod_{p\le m+1} p \cdot \prod_{m+1<p\le 2m+1} p \;\le\; 4^m \binom{2m+1}{m} \;\le\; 4^m 2^{2m} \;=\; 4^{2m}.$$

Alle Komponenten dieses „Einzeilers“ sind leicht einzusehen. So gilt

$$\prod_{p\le m+1} p \;\le\; 4^m$$

nach Induktionsvoraussetzung. Die Ungleichung

$$\prod_{m+1<p\le 2m+1} p \;\le\; \binom{2m+1}{m}$$

folgt aus der Beobachtung, dass $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ eine ganze Zahl ist, wobei die Primzahlen, die auf der linken Seite auftauchen, alle den Zähler $(2m+1)!$ teilen, aber nicht den Nenner $m!(m+1)!$. Und schließlich gilt

$$\binom{2m+1}{m} \;\le\; 2^{2m}$$

weil

$$\binom{2m+1}{m} \text{ und } \binom{2m+1}{m+1}$$

zwei (gleiche!) Summanden sind, die in der Summe

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} \;=\; 2^{2m+1}$$

enthalten sind.

(3) Nach dem Satz von Legendre (siehe den Kasten) enthält $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ den Primfaktor p genau

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right)$$

Mal. Dabei ist jeder Summand höchstens 1, weil er

$$\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor \;<\; \frac{2n}{p^k} - 2\left(\frac{n}{p^k} - 1\right) \;=\; 2$$

erfüllt und eine ganze Zahl ist. Die Summanden verschwinden sogar, wenn $p^k > 2n$ ist.
Damit enthält $\binom{2n}{n}$ den Faktor p

$$\sum_{k\geq 1}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\left\lfloor\frac{n}{p^k}\right\rfloor\right) \;\leq\; \max\{r : p^r \leq 2n\}$$

Mal. Also ist die größte Potenz von p, die $\binom{2n}{n}$ teilt, nicht größer als $2n$. Insbesondere sind Primzahlen p, die größer als $\sqrt{2n}$ sind, höchstens einmal in $\binom{2n}{n}$ enthalten.
Und schließlich — und laut Erdős ist dies der Knackpunkt seines Beweises — teilen Primzahlen p im Bereich $\frac{2}{3}n < p \leq n$ den Binomialkoeffizienten $\binom{2n}{n}$ überhaupt nicht! Für $3p > 2n$ (und $n \geq 3$, und damit $p \geq 3$) sind nämlich p und $2p$ die einzigen Vielfachen von p, die als Faktoren im Zähler von $\frac{(2n)!}{n!n!}$ auftauchen, während wir zwei p-Faktoren im Nenner haben.

(4) Jetzt können wir $\binom{2n}{n}$ abschätzen, wobei wir eine Anregung von Raimund Seidel aufnehmen, die die ursprüngliche Rechnung von Erdős noch verbessert. Für $n \geq 3$ erhalten wir mit einer Abschätzung von Seite 15 für die untere Schranke

$$\frac{4^n}{2n} \;\leq\; \binom{2n}{n} \;\leq\; \prod_{p\leq\sqrt{2n}} 2n \;\cdot\; \prod_{\sqrt{2n}<p\leq\frac{2}{3}n} p \;\cdot\; \prod_{n<p\leq 2n} p.$$

Es gibt nicht mehr als $\sqrt{2n}$ Primzahlen im ersten Faktor. Verwenden wir (1) für den zweiten Faktor und bezeichnen mit $P(n)$ die Anzahl der Primzahlen zwischen n und $2n$, so erhalten wir

$$\frac{4^n}{2n} \;<\; \left((2n)^{\sqrt{2n}}\right)\cdot\left(4^{\frac{2}{3}n}\right)\cdot(2n)^{P(n)},$$

somit

$$4^{\frac{n}{3}} \;<\; (2n)^{\sqrt{2n}+1+P(n)}. \tag{2}$$

(5) Nehmen wir den Logarithmus zur Basis 2, so wird aus der letzten Ungleichung

$$P(n) \;>\; \frac{2n}{3\log_2(2n)} - (\sqrt{2n}+1). \tag{3}$$

Der Satz von Legendre

Die Zahl $n!$ enthält den Primfaktor p genau

$$\sum_{k\geq 1}\left\lfloor\frac{n}{p^k}\right\rfloor$$

Mal.

■ **Beweis.** Genau $\lfloor\frac{n}{p}\rfloor$ der Faktoren von $n! = 1\cdot 2\cdot 3\cdots n$ sind durch p teilbar, was uns $\lfloor\frac{n}{p}\rfloor$ p-Faktoren liefert. Weiter sind $\lfloor\frac{n}{p^2}\rfloor$ der Faktoren von $n!$ sogar durch p^2 teilbar, was die nächsten $\lfloor\frac{n}{p^2}\rfloor$ Primfaktoren p von $n!$ liefert, usw. □

Beispiele wie
$\binom{26}{13} = 2^3\cdot 5^2\cdot 7\cdot 17\cdot 19\cdot 23$
$\binom{28}{14} = 2^3\cdot 3^3\cdot 5^2\cdot 17\cdot 19\cdot 23$
$\binom{30}{15} = 2^4\cdot 3^2\cdot 5\cdot 17\cdot 19\cdot 23\cdot 29$
zeigen, dass „sehr kleine“ Primfaktoren $p < \sqrt{2n}$ in höherer Potenz in $\binom{2n}{n}$ auftauchen können, „kleine“ Primzahlen mit $\sqrt{2n} < p \leq \frac{2}{3}n$ tauchen höchstens einmal auf, während Faktoren in dem Intervall $\frac{2}{3}n < p \leq n$ überhaupt nicht auftauchen.

Es bleibt zu zeigen, dass die rechte Seite in (3) positiv ist für genügend große n. Wir beweisen, dass dies ab $n = 2^9 = 512$ der Fall ist (es stimmt sogar schon ab $n = 468$). Schreiben wir $2n - 1 = (\sqrt{2n} - 1)(\sqrt{2n} + 1)$ und kürzen $(\sqrt{2n} + 1)$ heraus, so genügt der Nachweis von

$$\sqrt{2n} - 1 \;>\; 3\log_2(2n) \quad \text{für } n \geq 2^9. \tag{4}$$

Für $n = 2^9$ besagt (4) genau $31 > 30$, und ein Vergleich der Ableitungen $(\sqrt{x} - 1)' = \frac{1}{2}\frac{1}{\sqrt{x}}$ und $(3\log_2 x)' = \frac{3}{\log 2}\frac{1}{x}$ zeigt, dass $\sqrt{x} - 1$ schneller wächst als $3\log_2 x$ wenn $x > (\frac{6}{\log 2})^2 \approx 75$ ist, und daher sicherlich ab $x \geq 2^{10} = 1024$. □

Aus solchen Abschätzungen kann man noch mehr herausholen: Ein Vergleich der Ableitungen für (4) ergibt die schärfere Ungleichung

$$\sqrt{2n} - 1 \;\geq\; \frac{21}{4}\log_2(2n) \quad \text{für } n \geq 2^{11},$$

was mit einer kurzen Rechnung und (3) zu

$$P(n) \;\geq\; \frac{2}{7}\frac{n}{\log_2(2n)}$$

führt.

Das ist keine schlechte Abschätzung: die „wahre“ Anzahl der Primzahlen in diesem Bereich ist ungefähr $n/\log n$. Dies folgt aus dem „Primzahlsatz“, der besagt, dass der Grenzwert

$$\lim_{n\to\infty} \frac{\#\{p \leq n : p \text{ Primzahl}\}}{n/\log n}$$

existiert, und gleich 1 ist. Dieses berühmte Resultat wurde zuerst von Hadamard und de la Vallée-Poussin 1896 bewiesen; Selberg und Erdős haben 1948 einen elementaren Beweis (ohne komplexe Analysis, aber immer noch lang und kompliziert) gefunden. Über den Primzahlsatz selbst ist das letzte Wort wohl noch nicht gesprochen: So würde etwa ein Beweis der Riemannschen Vermutung (siehe Seite 71), eines der wichtigsten ungelösten Probleme der Mathematik, auch eine substantielle Verbesserung der Abschätzungen im Primzahlsatz liefern. Aber auch das Bertrandsche Postulat könnte man noch ordentlich verbessern. Die folgende Frage von Opperman (1882) ist nämlich immer noch nicht beantwortet [4, S. 248]:

> *Gibt es für jedes $n \geq 2$ mindestens eine Primzahl zwischen $(n-1)n$ und n^2, und mindestens eine zwischen n^2 und $n(n+1)$? Gibt es also zwischen zwei aufeinander folgenden Quadratzahlen immer mindestens zwei Primzahlen?*

Immerhin ist die letzte Aussage für den Fall bewiesen, dass man statt Quadratzahlen hinreichend große Kubikzahlen betrachtet [3].

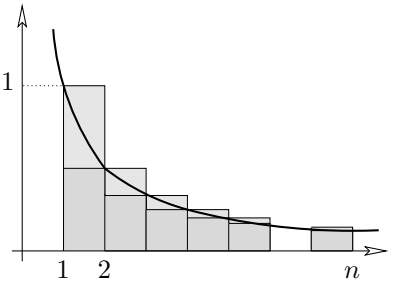
Anhang: Einige Abschätzungen

Abschätzung durch Integrale

Es gibt eine sehr einfache aber effektive Methode, Summen durch Integrale abzuschätzen, die uns schon auf Seite 4 begegnet ist. Um beispielsweise die *harmonischen Zahlen*

$$H_n \;=\; \sum_{k=1}^{n} \frac{1}{k}$$

abzuschätzen, machen wir die nebenstehende Skizze und leiten aus ihr



$$H_n - 1 \;=\; \sum_{k=2}^{n} \frac{1}{k} \;<\; \int_1^n \frac{1}{t}\,dt \;=\; \log n$$

ab, indem wir die Fläche unter dem Graphen von $f(t) = \frac{1}{t}$ $(1 \le t \le n)$ mit der Fläche der dunkler schraffierten Rechtecke vergleichen, und

$$H_n - \frac{1}{n} \;=\; \sum_{k=1}^{n-1} \frac{1}{k} \;>\; \int_1^n \frac{1}{t}\,dt \;=\; \log n,$$

indem wir mit der Fläche der größeren Rechtecke (also auch der heller schraffierten Teile) vergleichen. Zusammen genommen ergibt dies

$$\log n + \frac{1}{n} \;<\; H_n \;<\; \log n \;+\; 1.$$

Insbesondere gilt also $\lim\limits_{n\to\infty} H_n \to \infty$, und die Wachstumsgeschwindigkeit von H_n ist durch $\lim\limits_{n\to\infty} \frac{H_n}{\log n} = 1$ gegeben. Aber man kennt viel bessere Abschätzungen (siehe [2]), wie

$$H_n \;=\; \log n + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} + O\left(\frac{1}{n^6}\right),$$

Hier bezeichnet $O\left(\frac{1}{n^6}\right)$ eine Funktion $f(n)$, die $f(n) \le c\frac{1}{n^6}$ erfüllt, für eine Konstante $c > 0$.

wobei $\gamma \approx 0.5772$ die „Eulersche Konstante“ bezeichnet.

Fakultäten abschätzen — die Stirlingsche Formel

Dieselbe Methode, auf

$$\log(n!) \;=\; \log 2 + \log 3 + \cdots + \log n \;=\; \sum_{k=2}^{n} \log k$$

angewendet, liefert

$$\log((n-1)!) \;<\; \int_1^n \log t\,dt \;<\; \log(n!),$$

wobei sich das Integral leicht ausrechnen lässt:

$$\int_1^n \log t\,dt \;=\; \Big[t\log t - t\Big]_1^n \;=\; n\log n - n + 1.$$

Damit bekommen wir eine untere Abschätzung

$$n! \;>\; e^{n\log n - n + 1} \;=\; e\Big(\frac{n}{e}\Big)^n$$

und gleichzeitig eine obere Abschätzung

$$n! \;=\; n\,(n-1)! \;<\; ne^{n\log n - n + 1} \;=\; en\Big(\frac{n}{e}\Big)^n.$$

Diese beiden Abschätzungen reichen für viele Zwecke aus; wieder kann man aber „wenn nötig“ mit genauerer Analyse mehr herausholen, insbesondere die *Stirlingsche Formel*

$$n! \;\sim\; \sqrt{2\pi n}\,\Big(\frac{n}{e}\Big)^n.$$

Hier bedeutet $f(n) \sim g(n)$, dass $\lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = 1$ gilt.

Aber es gibt noch sehr viel präzisere Versionen dieses Resultats, etwa

$$n! \;=\; \sqrt{2\pi n}\,\Big(\frac{n}{e}\Big)^n \left(1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{51840n^3} + O\left(\frac{1}{n^4}\right)\right).$$

Binomialkoeffizienten abschätzen

Schon aus der Definition der Binomialkoeffizienten $\binom{n}{k}$ als die Anzahl der k-Teilmengen einer n-Menge wissen wir, dass die Folge $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ der Binomialkoeffizienten

- sich aufsummiert zu $\sum\limits_{k=0}^{n} \binom{n}{k} = 2^n$
- symmetrisch ist: $\binom{n}{k} = \binom{n}{n-k}$.

Aus der Funktionalgleichung $\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$ leitet man leicht ab, dass für jedes n die Binomialkoeffizienten $\binom{n}{k}$ eine Folge bilden, die symmetrisch und *unimodal* ist: sie steigt bis zur Mitte an, so dass die mittleren Binomialkoeffizienten die größten in der Folge sind:

$$1 = \tbinom{n}{0} < \tbinom{n}{1} < \cdots < \tbinom{n}{\lfloor n/2\rfloor} = \tbinom{n}{\lceil n/2\rceil} > \cdots > \tbinom{n}{n-1} > \tbinom{n}{n} = 1.$$

Hier bezeichnen $\lfloor x\rfloor$ bzw. $\lceil x\rceil$ die Zahl x, abgerundet bzw. aufgerundet bis zur nächsten ganzen Zahl.

Mit Hilfe der oben angegebenen Formeln für die Asymptotik der Fakultäten kann man sehr genaue Abschätzungen für die Größe der Binomialkoeffizienten ableiten. In diesem Buch brauchen wir aber nur sehr schwache und einfache Abschätzungen, wie die folgenden:

$$\binom{n}{k} \;\le\; 2^n \qquad \text{für alle } k \le n,$$

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5  10  10   5   1
    1   6  15  20  15   6   1
  1   7  21  35  35  21   7   1
```

Das Pascalsche Dreieck

und

$$\binom{n}{\lfloor n/2 \rfloor} \;\geq\; \frac{2^n}{n} \qquad \text{für } n \geq 2,$$

mit Gleichheit nur für $n = 2$. Insbesondere haben wir

$$\binom{2n}{n} \;\geq\; \frac{4^n}{2n} \qquad \text{für } n \geq 1.$$

Der mittlere Binomialkoeffizient $\binom{n}{\lfloor n/2 \rfloor}$ ist nämlich der größte Eintrag in der Folge der n Zahlen $\binom{n}{0} + \binom{n}{n}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$, deren Summe 2^n und deren Mittelwert damit $\frac{2^n}{n}$ ist.
Schließlich halten wir als obere Schranke für die Binomialkoeffizienten

$$\binom{n}{k} \;=\; \frac{n(n-1)\cdots(n-k+1)}{k!} \;\leq\; \frac{n^k}{k!} \;\leq\; \frac{n^k}{2^{k-1}}$$

fest, was eine halbwegs vernünftige Abschätzung für die „kleinen“ Binomialkoeffizienten am Anfang der Folge ist, für die n im Vergleich zu k groß ist.

Literatur

[1] P. ERDŐS: *Beweis eines Satzes von Tschebyschef,* Acta Sci. Math. (Szeged) **5** (1930-32), 194-198.

[2] R. L. GRAHAM, D. E. KNUTH & O. PATASHNIK: *Concrete Mathematics. A Foundation for Computer Science,* Addison-Wesley, Reading MA 1989.

[3] F. ISCHEBECK: *Primzahlfragen und ihre Geschichte,* Mathematische Semesterberichte **40** (1993), 121-132.

[4] P. RIBENBOIM: *The New Book of Prime Number Records,* Springer-Verlag, New York 1989.

Binomialkoeffizienten sind (fast) nie Potenzen

Kapitel 3

Im Nachklang zu Bertrands Postulat wollen wir jetzt ein sehr schönes Resultat über Binomialkoeffizienten besprechen. Im Jahr 1892 verschärfte Sylvester das Bertrandsche Postulat auf die folgende Weise:

> *Ist $n \geq 2k$, so hat mindestens eine der Zahlen $n, n-1, \ldots, n-k+1$ einen Primteiler p, der größer als k ist.*

Man beachte, dass dies für $n = 2k$ genau das Bertrandsche Postulat ergibt. Erdős gab 1934 einen kurzen und elementaren Beweis des Satzes von Sylvester, der auch aus dem BUCH stammt und auf ähnlichen Überlegungen wie im letzten Kapitel beruht.

Die folgende Aussage ist offensichtlich äquivalent zum Satz von Sylvester:

> *Der Binomialkoeffizient*
>
> $$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \qquad (n \geq 2k)$$
>
> *hat immer einen Primteiler $p > k$.*

Mit dieser Beobachtung wenden wir uns einem weiteren Juwel von Erdős zu:

> *Wann ist $\binom{n}{k}$ eine Potenz m^ℓ?*

Der Fall $k = \ell = 2$ führt zu einem klassischen Thema: Multiplikation von $\binom{n}{2} = m^2$ mit 8 und Umordnung der Terme ergibt

$$(2n-1)^2 - 2(2m)^2 = 1,$$

also einen Spezialfall der *Pellschen Gleichung* $x^2 - 2y^2 = 1$. In der Zahlentheorie lernt man, dass diese Gleichung unendlich viele positive Lösungen (x_k, y_k) hat, die durch $x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k$ für $k \geq 1$ gegeben sind. Die kleinsten Beispiele sind $(x_1, y_1) = (3, 2)$, $(x_2, y_2) = (17, 12)$ und $(x_3, y_3) = (99, 70)$; sie ergeben $\binom{2}{2} = 1^2$, $\binom{9}{2} = 6^2$ und $\binom{50}{2} = 35^2$.

Für $k = 2$ und $\ell > 2$ gibt es keine weiteren Lösungen, und für $k = 3$ ist bekannt, dass $\binom{n}{3} = m^\ell$ die eindeutige Lösung $n = 50$, $m = 140$, $\ell = 2$ besitzt (siehe Győry [3]). Aber nun sind die Potenzen schon zu Ende. Für $k \geq 4$ und jedes $\ell \geq 2$ gibt es keine Lösungen, und dies ist genau der Inhalt des Satzes von Erdős.

M. Aigner und G. M. Ziegler, *Das BUCH der Beweise*,
https://doi.org/10.1007/978-3-662-57767-7_3

Satz. *Die Gleichung*

$$\binom{n}{k} \;=\; m^\ell$$

hat keine ganzzahligen Lösungen für $\ell \geq 2$ *und* $4 \leq k \leq n-4$.

■ **Beweis.** Wir nehmen an, der Satz sei falsch, und $\binom{n}{k} = m^\ell$ sei eine ganzzahlige Lösung. Dabei dürfen wir wegen $\binom{n}{k} = \binom{n}{n-k}$ voraussetzen, dass $n \geq 2k$ gilt. Die Annahme führen wir nun in den folgenden vier Schritten zum Widerspruch.

(1) Nach dem Satz von Sylvester gibt es einen Primteiler p von $\binom{n}{k}$, der größer als k ist. Damit teilt p^ℓ das Produkt $n(n-1)\cdots(n-k+1)$. Weiterhin kann jedes solche $p > k$ nur einen der Faktoren $n-i$ teilen, und wir schließen $p^\ell \mid n-i$, und daraus

$$n \;\geq\; p^\ell \;>\; k^\ell \;\geq\; k^2.$$

(2) Wir betrachten einen beliebigen Faktor $n-j$ des Zählers und schreiben ihn in der Form $n-j = a_j m_j^\ell$, wobei a_j nicht durch eine echte ℓ-te Potenz teilbar ist. Nach **(1)** sehen wir, dass a_j nur Primteiler besitzt, die kleiner oder gleich k sind. Als Nächstes wollen wir $a_i \neq a_j$ für $i \neq j$ zeigen. Es sei im Gegenteil $a_i = a_j$ für $i < j$. Dann haben wir $m_i \geq m_j + 1$ und

$$\begin{aligned} k \;&>\; (n-i)-(n-j) \;=\; a_j(m_i^\ell - m_j^\ell) \;\geq\; a_j((m_j+1)^\ell - m_j^\ell) \\ &>\; a_j \ell m_j^{\ell-1} \;\geq\; \ell(a_j m_j^\ell)^{1/2} \;\geq\; \ell(n-k+1)^{1/2} \\ &\geq\; \ell(\tfrac{n}{2}+1)^{1/2} \;>\; n^{1/2}, \end{aligned}$$

aber dies widerspricht der obigen Ungleichung $n > k^2$.

(3) Als Nächstes beweisen wir, dass die a_is genau die Zahlen $1, 2, \ldots, k$ in einer gewissen Reihenfolge sind. Nach Erdős ist dies das Kernstück des Beweises. Da wir schon wissen, dass die a_is alle verschieden sind, genügt es zu zeigen, dass

$$a_0 a_1 \cdots a_{k-1} \;\mid\; k!$$

gilt. Substituieren wir $n - j = a_j m_j^\ell$ in die Gleichung $\binom{n}{k} = m^\ell$, so erhalten wir

$$a_0 a_1 \cdots a_{k-1} (m_0 m_1 \cdots m_{k-1})^\ell \;=\; k! m^\ell.$$

Nach Kürzen der gemeinsamen Faktoren in $m_0 m_1 \cdots m_{k-1}$ und m ergibt dies

$$a_0 a_1 \cdots a_{k-1} u^\ell \;=\; k! v^\ell$$

mit $\mathrm{ggT}(u, v) = 1$. Es bleibt zu zeigen, dass $v = 1$ ist. Im Fall $v > 1$ enthält v einen Primteiler p. Da $\mathrm{ggT}(u, v) = 1$ ist, muss p ein Primteiler von $a_0 a_1 \cdots a_{k-1}$ sein und daher kleiner oder gleich k sein. Nach dem

Satz von Legendre (siehe Seite 11) wissen wir, dass $k!$ die Primzahl p zur Potenz $\sum_{i\geq 1}\lfloor\frac{k}{p^i}\rfloor$ enthält. Nun schätzen wir den Exponenten von p in dem Produkt $n(n-1)\cdots(n-k+1)$ ab. Sei i eine positive ganze Zahl und seien $b_1 < b_2 < \cdots < b_s$ die Vielfachen von p^i unter den k Zahlen $n, n-1, \ldots, n-k+1$. Dann haben wir $b_s = b_1 + (s-1)p^i$, und daher

$$(s-1)p^i \;=\; b_s - b_1 \;\leq\; n-(n-k+1) \;=\; k-1,$$

was

$$s \;\leq\; \left\lfloor\frac{k-1}{p^i}\right\rfloor + 1 \;\leq\; \left\lfloor\frac{k}{p^i}\right\rfloor + 1$$

impliziert.

Wir sehen also, dass für jedes i die Anzahl der Vielfachen von p^i unter den Zahlen $n, \ldots, n-k+1$, und daher auch unter den a_js, durch $\lfloor\frac{k}{p^i}\rfloor + 1$ beschränkt ist. Dies liefert uns, dass der Exponent von p in $a_0a_1\cdots a_{k-1}$ höchstens

$$\sum_{i=1}^{\ell-1}\Big(\Big\lfloor\frac{k}{p^i}\Big\rfloor + 1\Big)$$

sein kann, aufgrund derselben Überlegung, die wir für den Beweis des Satzes von Legendre in Kapitel 2 benutzt haben. Der einzige Unterschied ist, dass dieses Mal die Summe bei $i = \ell - 1$ endet, da die a_js keine ℓ-ten Potenzen enthalten.

Insgesamt sehen wir also, dass der Exponent von p in v^ℓ höchstens

$$\sum_{i=1}^{\ell-1}\Big(\Big\lfloor\frac{k}{p^i}\Big\rfloor + 1\Big) - \sum_{i\geq 1}\Big\lfloor\frac{k}{p^i}\Big\rfloor \;\leq\; \ell - 1$$

sein kann, und wir haben unseren gewünschten Widerspruch erhalten, da v^ℓ eine ℓ-te Potenz ist.

Dies genügt bereits, um den Fall $\ell = 2$ zu erledigen. In der Tat muss wegen $k \geq 4$ eine der Zahlen a_i gleich 4 sein, aber wir wissen schon, dass die a_is keine Quadrate enthalten. Also können wir für den Rest des Beweises $\ell \geq 3$ annehmen.

Unsere Analyse bis hierher stimmt mit der Gleichung $\binom{50}{3} = 140^2$ überein:

$$\begin{aligned} 50 &= 2\cdot 5^2\\ 49 &= 1\cdot 7^2\\ 48 &= 3\cdot 4^2 \end{aligned}$$

und $5\cdot 7\cdot 4 = 140$.

(4) Wegen $k \geq 4$ haben wir $a_{i_1} = 1$, $a_{i_2} = 2$, $a_{i_3} = 4$ für gewisse i_1, i_2, i_3, das heißt,

$$n - i_1 = m_1^\ell,\;\; n - i_2 = 2m_2^\ell,\;\; n - i_3 = 4m_3^\ell.$$

Wir behaupten, dass $(n-i_2)^2 \neq (n-i_1)(n-i_3)$ gilt. Anderenfalls setzen wir $b = n - i_2$ und $n - i_1 = b - x$, $n - i_3 = b + y$ mit $0 < |x|, |y| < k$. Damit haben wir

$$b^2 = (b-x)(b+y) \quad \text{oder} \quad (y-x)b = xy,$$

wobei $x = y$ ersichtlich unmöglich ist. Nach Teil **(1)** folgt daraus

$$|xy| \;=\; b|y-x| \;\geq\; b \;>\; n-k \;>\; (k-1)^2 \;\geq\; |xy|,$$

ein offensichtlicher Widerspruch.

Wir haben also $m_2^2 \neq m_1 m_3$, wobei wir $m_2^2 > m_1 m_3$ annehmen können (der andere Fall ist analog), und wenden uns nun der letzten Kette von Ungleichungen zu. Es gilt

$$\begin{aligned} 2(k-1)n &> n^2 - (n-k+1)^2 > (n-i_2)^2 - (n-i_1)(n-i_3) \\ &= 4[m_2^{2\ell} - (m_1 m_3)^\ell] \geq 4[(m_1 m_3 + 1)^\ell - (m_1 m_3)^\ell] \\ &\geq 4\ell m_1^{\ell-1} m_3^{\ell-1}. \end{aligned}$$

Wegen $\ell \geq 3$ und $n > k^\ell \geq k^3 > 6k$ ergibt dies

$$\begin{aligned} 2(k-1)nm_1m_3 &> 4\ell m_1^\ell m_3^\ell = \ell(n-i_1)(n-i_3) \\ &> \ell(n-k+1)^2 > 3(n-\frac{n}{6})^2 > 2n^2. \end{aligned}$$

Mit $m_i \leq n^{1/\ell} \leq n^{1/3}$ erhalten wir schließlich

$$kn^{2/3} \geq km_1m_3 > (k-1)m_1m_3 > n,$$

oder $k^3 > n$. Mit diesem Widerspruch ist der Beweis vollständig. □

Literatur

[1] P. ERDŐS: *A theorem of Sylvester and Schur,* J. London Math. Soc. **9** (1934), 282-288.

[2] P. ERDŐS: *On a diophantine equation,* J. London Math. Soc. **26** (1951), 176-178.

[3] K. GYŐRY: *On the diophantine equation* $\binom{n}{k} = x^l$, Acta Arithmetica **80** (1997), 289-295.

[4] J. J. SYLVESTER: *On arithmetical series,* Messenger of Math. **21** (1892), 1-19, 87-120; Collected Mathematical Papers Vol. 4, 1912, 687-731.

Der Zwei-Quadrate-Satz von Fermat

Kapitel 4

> *Welche Zahlen können als Summe von zwei Quadraten dargestellt werden?*

Diese Frage ist so alt wie die Zahlentheorie, und ihre Lösung ist ein Klassiker in diesem Gebiet. Die größte Hürde auf dem Weg zur Lösung ist der Nachweis, dass jede Primzahl der Form $4m+1$ eine Summe von zwei Quadraten ist. G. H. Hardy schreibt, dass dieser *Zwei-Quadrate-Satz* von Fermat „ganz zu Recht als einer der besten Sätze der Arithmetik angesehen wird". Trotzdem ist einer unserer BUCH-Beweise ziemlich neu.

Wir beginnen mit ein paar „Aufwärmübungen". Zunächst müssen wir zwischen der Primzahl $p=2$, den Primzahlen der Form $p=4m+1$, und den Primzahlen der Form $p=4m+3$ unterscheiden. Jede Primzahl fällt in genau eine dieser Kategorien. Ganz leicht können wir jetzt festhalten (mit Hilfe der Methode von Euklid), dass es unendlich viele Primzahlen der Form $4m+3$ gibt. Wenn es nämlich nur endlich viele gäbe, dann könnten wir die größte Primzahl p_k von dieser Form betrachten. Setzt man dann

$$N_k \;:=\; 2^2 \cdot 3 \cdot 5 \cdots p_k - 1$$

(wobei $p_1=2$, $p_2=3$, $p_3=5$, ... die Folge der Primzahlen bezeichnet), dann sieht man, dass N_k kongruent zu $3 \pmod 4$ ist, also einen Primfaktor der Form $4m+3$ haben muss, und dieser Primfaktor ist größer als p_k, Widerspruch.

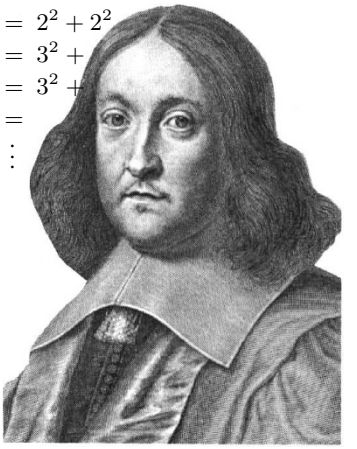
Unser erstes Lemma charakterisiert die Primzahlen, für die -1 im Körper $\mathbb{Z}_p$ ein Quadrat ist (siehe dazu den Kasten über Primkörper auf der nächsten Seite). Es wird uns auch einen einfachen Beweis für die Tatsache liefern, dass es unendlich viele Primzahlen der Form $4m+1$ gibt.

Lemma 1. *Für jede Primzahl p der Form $p=4m+1$ hat die Gleichung $s^2 \equiv -1 \pmod p$ zwei Lösungen $s \in \{1,2,\ldots,p-1\}$, für $p=2$ gibt es genau eine solche Lösung, während es für Primzahlen von der Form $p=4m+3$ keine Lösung gibt.*

■ **Beweis.** Für $p=2$ ist $s=1$. Für ungerades p konstruieren wir eine Äquivalenzrelation auf der Menge $\{1,2,\ldots,p-1\}$, die dadurch erzeugt wird, dass wir jedes Element mit seinem additiven und seinem multiplikativen Inversen in $\mathbb{Z}_p$ in Relation setzen, die wir mit $-x$ bzw. $\overline{x}$ bezeichnen. Damit enthalten die „allgemeinen" Äquivalenzklassen vier Elemente

$$\{x, -x, \overline{x}, -\overline{x}\},$$

$1 = 1^2 + 0^2$
$2 = 1^2 + 1^2$
$3 =$
$4 = 2^2 + 0^2$
$5 = 2^2 + 1^2$
$6 =$
$7 =$
$8 = 2^2 + 2^2$
$9 = 3^2 +$
$10 = 3^2 +$
$11 =$
$\vdots$



Pierre de Fermat

M. Aigner und G. M. Ziegler, *Das BUCH der Beweise*,
https://doi.org/10.1007/978-3-662-57767-7_4

weil eine solche vierelementige Menge die Inversen für alle ihre Elemente enthält. Es gibt jedoch auch kleinere Äquivalenzklassen, die auftreten, wenn einige dieser vier Elemente nicht voneinander verschieden sind:

- $x \equiv -x$ ist für ungerades p unmöglich.
- $x \equiv \overline{x}$ ist äquivalent zu $x^2 \equiv 1$. Dies hat zwei Lösungen, nämlich $x = 1$ und $x = p - 1$, und entspricht der Äquivalenzklasse $\{1, p-1\}$ der Größe 2.
- $x \equiv -\overline{x}$ ist äquivalent zu $x^2 \equiv -1$. Diese Gleichung hat entweder keine Lösung, oder zwei verschiedene Lösungen $x_0, p - x_0$: in diesem Fall ist die Äquivalenzklasse $\{x_0, p - x_0\}$.

Für $p = 11$ ist die Zerlegung $\{1, 10\}, \{2, 9, 6, 5\}, \{3, 8, 4, 7\}$; für $p = 13$ ist sie $\{1, 12\}, \{2, 11, 7, 6\}, \{3, 10, 9, 4\}, \{5, 8\}$: das Paar $\{5, 8\}$ entspricht den zwei Lösungen von $s^2 \equiv -1 \bmod 13$.

Die Menge $\{1, 2, \ldots, p-1\}$ hat $p - 1$ Elemente, und wir haben sie in Quadrupel (Äquivalenzklassen der Größe 4) aufgeteilt, plus ein oder zwei Paare (Äquivalenzklassen der Größe 2). Für $p - 1 = 4m + 2$ folgt daraus, dass es nur ein Paar $\{1, p-1\}$ gibt, der Rest besteht aus Quadrupeln, und damit hat $s^2 \equiv -1 \pmod p$ keine Lösung. Für $p - 1 = 4m$ muss es aber ein zweites Paar geben, und dieses enthält die beiden Lösungen von $s^2 \equiv -1$, nach denen gefragt war. □

Lemma 1 besagt, dass jeder ungerade Primteiler von $M^2 + 1$ von der Form $4m+1$ sein muss. Das impliziert, dass es unendlich viele Primzahlen dieser Form gibt: andernfalls betrachte man $(2 \cdot 3 \cdot 5 \cdots q_k)^2 + 1$, wobei q_k die größte solche Primzahl ist, und führe dies wie vorhin zum Widerspruch.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Addition und Multiplikation in $\mathbb{Z}_5$

Primkörper

Für jede Primzahl p bildet die Menge $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ mit Addition und Multiplikation „modulo p“ einen endlichen Körper. Diese Körper haben viele interessante Aspekte; wir werden nur die folgenden drei einfachen Eigenschaften brauchen:

- Für $x \in \mathbb{Z}_p$, $x \neq 0$, ist das Inverse bezüglich Addition (für das wir üblicherweise $-x$ schreiben) durch $p - x \in \{1, 2, \ldots, p-1\}$ gegeben. Wenn $p > 2$ ist, dann sind x und $-x$ verschiedene Elemente von $\mathbb{Z}_p$.
- Jedes $x \in \mathbb{Z}_p \backslash \{0\}$ hat ein eindeutiges multiplikatives Inverses $\overline{x} \in \mathbb{Z}_p \backslash \{0\}$, mit $x\overline{x} \equiv 1 \pmod p$.
  Aus der Definition der Primzahlen folgt nämlich, dass die Abbildung $\mathbb{Z}_p \to \mathbb{Z}_p$, $z \mapsto xz$ für $x \neq 0$ injektiv ist. Auf der endlichen Menge $\mathbb{Z}_p \backslash \{0\}$ muss sie damit aber auch surjektiv sein, und deswegen gibt es für jedes x ein eindeutiges $\overline{x} \neq 0$ mit $x\overline{x} \equiv 1 \pmod p$.
- Die Quadrate $0^2, 1^2, 2^2, \ldots, h^2$ definieren verschiedene Elemente von $\mathbb{Z}_p$, für $h = \lfloor \frac{p}{2} \rfloor$.
  Dies folgt daraus, dass $x^2 \equiv y^2$ bzw. $(x+y)(x-y) \equiv 0$ impliziert, dass entweder $x \equiv y$ oder $x \equiv -y$ gilt. Die $1 + \lfloor \frac{p}{2} \rfloor$ Elemente $0^2, 1^2, \ldots, h^2$ nennt man die *Quadrate* in $\mathbb{Z}_p$.

An dieser Stelle bemerken wir „ganz nebenbei“, dass es für *alle* Primzahlen eine Lösung der Gleichung $x^2 + y^2 \equiv -1 \pmod p$ gibt. Es gibt nämlich $\lfloor \frac{p}{2} \rfloor + 1$ verschiedene Quadrate x^2 in $\mathbb{Z}_p$, und es gibt $\lfloor \frac{p}{2} \rfloor + 1$ verschiedene Zahlen der Form $-(1 + y^2)$. Diese zwei Mengen von Zahlen sind aber zu groß um disjunkt zu sein, weil $\mathbb{Z}_p$ insgesamt nur p Elemente hat, und deswegen muss es x und y geben mit $x^2 \equiv -(1 + y^2) \pmod p$.

Lemma 2. *Keine Zahl $n = 4m + 3$ ist eine Summe von zwei Quadraten.*

■ **Beweis.** Das Quadrat einer geraden Zahl ist $(2k)^2 = 4k^2 \equiv 0 \pmod 4$, während Quadrate von ungeraden Zahlen $(2k + 1)^2 = 4(k^2 + k) + 1 \equiv 1 \pmod 4$ ergeben. Damit ist jede Summe von zwei Quadraten zu $0, 1$ oder $2 \pmod 4$ kongruent. □

Dies reicht uns als Beleg dafür, dass die Primzahlen $p = 4m+3$ „schlecht“ sind. Also kümmern wir uns jetzt erst mal um die „guten“ Eigenschaften der Primzahlen von der Form $p = 4m + 1$. Das folgende Resultat ist der wichtigste Schritt auf dem Weg zur Lösung unseres Problems.

Proposition. *Jede Primzahl der Form $p = 4m + 1$ ist eine Summe von zwei Quadraten, sie kann also als $p = x^2 + y^2$ dargestellt werden, mit natürlichen Zahlen x und y.*

Wir werden hier zwei Beweise dieses Resultats präsentieren — beide sind elegant und überraschend. Der erste Beweis glänzt durch eine bemerkenswerte Anwendung des Schubfachprinzips (das schon „ganz nebenbei“ vor Lemma 2 aufgetreten ist; Kapitel 28 bietet mehr davon), und durch einen bestechenden Übergang zu Argumenten „modulo p“ und zurück. Wir verdanken ihn dem norwegischen Zahlentheoretiker Axel Thue.

■ **Beweis.** Wir betrachten die Paare (x', y') von ganzen Zahlen mit $0 \le x', y' \le \sqrt{p}$, das heißt $x', y' \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$. Es gibt genau $(\lfloor\sqrt{p}\rfloor + 1)^2$ solche Paare. Mit der Abschätzung $\lfloor x \rfloor + 1 > x$ für $x = \sqrt{p}$ sehen wir, dass es mehr als p solche Paare von ganzen Zahlen gibt. Also können für ein festes $s \in \mathbb{Z}$ die Werte $x' - sy'$, die man aus den Paaren (x', y') erzeugt, nicht alle modulo p verschieden sein. Also gibt es für jedes s zwei verschiedene Paare

$$(x', y'),\ (x'', y'') \ \in\ \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}^2$$

mit

$$x' - sy' \ \equiv\ x'' - sy'' \pmod p.$$

Nun nehmen wir Differenzen: Wir haben $x' - x'' \equiv s(y' - y'') \pmod p$. Wenn wir also

$$x \coloneqq |x' - x''|, \quad y \coloneqq |y' - y''|$$

definieren, dann erhalten wir

$$(x, y) \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}^2 \quad \text{mit} \quad x \equiv \pm sy \pmod p.$$

Weiterhin wissen wir, dass x und y nicht beide Null sein können, weil die Paare (x', y') und (x'', y'') ja verschieden sind.

Für $p = 13$, $\lfloor\sqrt{p}\rfloor = 3$ betrachten wir $x', y' \in \{0, 1, 2, 3\}$. Für $s = 5$ nimmt die Summe $x' - sy' \pmod{13}$ die folgenden Werte an:

x' \ y'	0	1	2	3
0	0	8	3	11
1	1	9	4	12
2	2	10	5	0
3	3	11	6	1

Sei nun s eine Lösung von $s^2 \equiv -1 \pmod p$, die nach Lemma 1 existieren muss. Dann gilt $x^2 \equiv s^2 y^2 \equiv -y^2 \pmod p$, und wir erhalten

$$(x, y) \in \mathbb{Z}^2 \quad \text{mit} \quad 0 < x^2 + y^2 < 2p \quad \text{und} \quad x^2 + y^2 \equiv 0 \pmod p.$$

Die Primzahl p ist aber die einzige Zahl zwischen 0 und $2p$, die durch p teilbar ist. Also gilt $x^2 + y^2 = p$: fertig! □

Unser zweiter Beweis für die Proposition — ganz sicher auch ein Beweis aus dem BUCH — wurde von Roger Heath-Brown 1971 entdeckt und erschien 1984. (Eine Kurzversion „in einem Satz“ wurde von Don Zagier angegeben.) Er ist so elementar, dass wir dafür nicht einmal das Lemma 1 brauchen.

Das Argument von Heath-Brown basiert auf drei Involutionen: einer ziemlich offensichtlichen, einer überraschenden, und einer ganz trivialen zum Schluss. Die zweite Involution entspricht einer versteckten Struktur auf der Menge der ganzzahligen Lösungen der Gleichung $4xy + z^2 = p$.

■ **Beweis.** Wir untersuchen die Menge

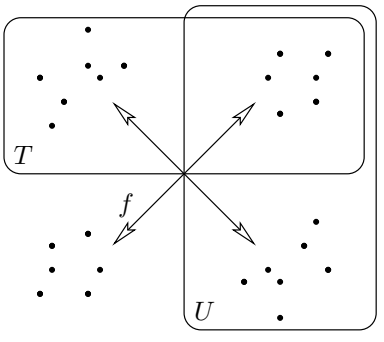
$$S \;:=\; \{(x, y, z) \in \mathbb{Z}^3 : 4xy + z^2 = p, \quad x > 0, \quad y > 0\}.$$

Diese Menge ist endlich: aus $x \geq 1$ und $y \geq 1$ folgt nämlich $y \leq \frac{p}{4}$ und $x \leq \frac{p}{4}$. Damit gibt es aber nur endlich viele mögliche Werte für x und y, und für gegebenes x und y gibt es höchstens zwei Werte für z.

1. Die erste lineare Involution ist

$$f : S \longrightarrow S, \quad (x, y, z) \longmapsto (y, x, -z),$$

also „vertausche x und y und negiere z“. Dies bildet ganz offensichtlich S auf sich selbst ab, und es ist eine *Involution*: Zweimal angewendet, ergibt es die Identität. Dieses f hat offenbar keine Fixpunkte, weil aus $z = 0$ sofort $p = 4xy$ folgen würde, was nicht sein kann. Schließlich bildet f die Lösungen in



$$T \;:=\; \{(x, y, z) \in S : z > 0\}$$

auf die Lösungen in $S \backslash T$ ab, die $z < 0$ erfüllen. Also vertauscht f die Vorzeichen von $x - y$ und von z, und bildet somit auch die Lösungen in

$$U \;:=\; \{(x, y, z) \in S : (x - y) + z > 0\}$$

auf die Lösungen in $S \backslash U$ ab. Dafür müssen wir nur überprüfen, dass es keine Lösungen gibt mit $(x - y) + z = 0$. Aber die gibt es nicht, weil daraus sofort $p = 4xy + z^2 = 4xy + (x - y)^2 = (x + y)^2$ folgen würde.

Was liefert uns nun die Analyse von f? Die hauptsächliche Beobachtung ist, dass f die Mengen T und U mit ihren Komplementen $S \backslash T$ bzw. $S \backslash U$ in Bijektion setzt; deshalb haben T und U beide die halbe Kardinalität von S *— also haben T und U dieselbe Kardinalität.*