Schnappschüsse moderner Mathematik
aus Oberwolfach

№ 3/2014

Das ternäre Goldbach-Problem

Harald Helfgott

Leonhard Euler (1707–1783) war einer der besten Mathematiker des 18. Jahrhunderts und wohl auch aller Zeiten. Er korrespondierte oft mit seinem Freund, Christoph Goldbach (1690–1764), einem Universalgelehrten, der auch Mathematik betrieb und ebenso wie Euler in Russland lebte. In einem dieser Briefe im Juni 1782, machte Goldbach die folgende Vermutung zu Primzahlen:

> *Es scheinet wenigstens, dass eine jede Zahl, die größer ist als 2, ein aggregatum trium numerorum primorum sey.*

Goldbach behauptete also, dass sich jede Zahl, die größer ist als 2, als Summe dreier Primzahlen schreiben lässt.

In diesem Schnappschuss moderner Mathematik soll es darum gehen, in welchem Ausmaß Mathematiker Goldbachs Vermutung bewiesen haben. Wir wollen dabei insbesondere aktuellen Fortschritt betrachten.

1 Starke und schwache Goldbach-Vermutung

Seit Goldbach seine Vermutung aufgestellt hat, hat sich die Formulierung des Problems leicht geändert: Wir sagen heute "jede Zahl, die größer ist als 5" statt "jede Zahl, die größer ist als 2". Der Grund ist, dass Goldbach die Zahl 1 als Primzahl angesehen hat, was wir heute nicht mehr tun. Damit ließ sich für Goldbach die Zahl 3 als Summe dreier Primzahlen schreiben, für uns jedoch nicht. Goldbachs Vermutung wird meistens in zwei Teile geteilt:

- Die schwache (oder ternäre) Goldbach-Vermutung, die sagt, dass sich jede ungerade ganze Zahl, die größer ist als 5, schreiben lässt als die Summe dreier Primzahlen;
  zum Beispiel: $11 = 3 + 3 + 5$; $21 = 2 + 2 + 17$.
- Die starke (oder binäre) Goldbach-Vermutung, die sagt, dass sich jede gerade ganze Zahl, die größer ist als 2, schreiben lässt als die Summe zweier Primzahlen;
  zum Beispiel: $10 = 5 + 5$; $36 = 13 + 23$.

Wie die Namen andeuten, lässt sich die schwache Vermutung von der starken ableiten.[1] Und wie Euler selbst an Goldbach geschrieben hat, lässt sich von der starken Vermutung auch Goldbachs ursprüngliche Formulierung ableiten (und andersherum).

Die Geschichte dieses Problems lässt sich nachlesen in [1, Ch. XVIII]. Eine kurze Zusammenfassung: In der ersten Hälfte des 17. Jahrhunderts stellte René Descartes (1596–1650) eine ähnliche Behauptung zu der von Goldbach auf, allerdings in einem Manuskript, das erst posthum in 1901 veröffentlicht wurde. Während des 19. Jahrhunderts wurde die Vermutung für viele Zahlen von Hand nachgerechnet, aber es gab wenig Fortschritt in Richtung einer allgemeinen Lösung.

Die starke Vermutung ist immer noch weit entfernt davon, bewiesen zu werden. Die schwache Goldbach-Vermutung habe ich nach vielen Jahren Arbeit im Jahr 2013 bewiesen.

2 Beweis der schwachen Goldbach-Vermutung

Der Beweis baut auf grundlegende Erkenntnisse auf, die Hardy, Littlewood und Vinogradov zu Beginn des 20. Jahrhunderts formuliert haben. Vinogradov bewies 1937 [10], dass die Vermutung für alle ungeraden Zahlen, die größer

[1] Um eine ungerade Zahl $n \geq 5$ als Summe dreier Primzahlen zu schreiben, zieht man 3 ab und erhält eine gerade Zahl $n-3 \geq 2$. Wenn die starke Vermutung wahr ist, können wir $n-3$ als Summe zweier Primzahlen p_1 und p_2 schreiben; aber dann ist auch $n = (n-3)+3 = p_1+p_2+3$ die Summe der Primzahlen p_1, p_2 und 3.

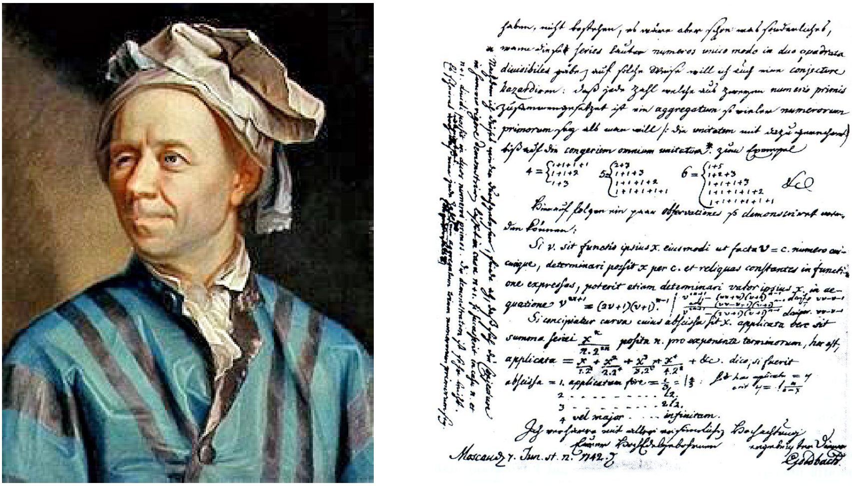

Abbildung 1: Euler und der Brief von Goldbach. Es scheint nicht-trivial zu sein, ein authentisches Bild von Goldbach zu finden.

sind als eine konstante Zahl C, wahr ist. (Hardy und Littlewood hatten schon früher dasselbe gezeigt, aber dazu angenommen, dass die verallgemeinerte Riemannsche Vermutung [2] wahr ist.) Seitdem wurde die Konstante C bestimmt und schrittweise verbessert, aber der beste (also kleinste) Wert von C, der bewiesen wurde, war

$$C = e^{3100} \approx 2 \cdot 10^{1346}$$

(Liu-Wang [8]), was immer noch viel zu groß ist. Wir können einfach nicht darauf hoffen, dass ein Computer die ersten 10^{1346} Fälle überprüfen kann – tatsächlich ist es ziemlich unwahrscheinlich, dass irgendeine Zivilisation auf der Erde oder im All, die jemals existieren wird, auch nur 10^{120} Fälle irgendeiner sinnvollen Behauptung einen nach dem anderen überprüfen könnte: Die Anzahl der Pikosekunden seit dem Anbeginn des Universums ist weniger als 10^{30} und die Anzahl der Protonen im beobachtbaren Universum wird derzeit auf etwa 10^{80} geschätzt. Das heißt, dass nicht einmal Parallelcomputer und galaktische Diktatur für so ein Unterfangen ausreichen würden.

Ich habe es geschafft, diese Konstante C auf 10^{27} zu verringern. Die starke Goldbach-Vermutung wurde von Computern schon bis $4 \cdot 10^{18}$ überprüft [9]; indem man diese Ergebnisse nutzt, kann man die schwache Goldbach-Vermutung

[2] Die verallgemeinerte Riemannsche Vermutung ist eine Standardvermutung, die seit sehr langer Zeit unbewiesen ist. Mehr zu ihr gibt es im englischen Schnappschuss 6/2014 *Dirichlet Series* von John E. M^cCarthy.

bis 10^{27} in wenigen Stunden auf einem modernen Computer überprüfen. (Tatsächlich hatten D. Platt und ich sie schon bis $8,8 \cdot 10^{30}$ auf Parallelcomputern überprüft [7].) Das heißt, dass die schwache Goldbach-Vermutung nun für alle ungeraden ganzen Zahlen bewiesen ist.

Es ist klar, warum ein einfaches Ausprobieren mit dem Computer eine Vermutung so wie die von Goldbach nur für Zahlen überprüfen kann, die kleiner als eine Konstante sind: eine solche Berechnung muss endlich sein. Aber warum sollte ein mathematischer Beweis nur für Zahlen gelten, die *größer* als eine Konstante C sind?

3 Methoden im Beweis

Tatsächlich ist das typisch für sogenannte *analytische* Beweise, das heißt, für Beweise, die Methoden wie Differential- und Integralrechnung, Fourier-Analysis und so weiter benutzen. Solch ein Beweis liefert üblicherweise mehr als die Information, dass eine ganze Zahl in einer bestimmten Weise geschrieben werden kann (hier: als Summe dreier Primzahlen), er liefert auch eine Schätzung für die Anzahl der verschiedenen Möglichkeiten. Die Schätzung nimmt dann die folgende Form an: die Anzahl der Möglichkeiten, eine ganze Zahl n in einer bestimmten Weise zu schreiben, wird beschrieben durch einen "Hauptterm" – eine Funktion $f(n)$ – und einen "Fehlerterm" – ein Term, der positiv oder negativ sein kann, aber dessen Betrag kleiner ist als eine Funktion $g(n)$. Wenn $f(n) > g(n)$ ist, beweist das, dass es mindestens eine Weise gibt, diese Zahl n als die Summe dreier Primzahlen zu schreiben.

Ein stark vereinfachtes Beispiel ist das folgende: Angenommen, wir könnten eine Schätzung mit $f(n) = n^2$ und $g(n) = 1000 \cdot n^{3/2}$ zeigen. Dann haben wir unsere Aussage bewiesen für den Fall, dass $f(n) > g(n)$ gilt, und diese Ungleichung ist wahr für alle $n > C$ mit $C = 10^6$.

Wie in diesem Beispiel ist es häufig der Fall, dass man zeigen kann, dass $f(n)$ größer **ist** als $g(n)$, aber eben nur, wenn n groß genug ist. Der Fall, dass n klein ist, muss dann von Hand (beziehungsweise mit einem Computer) überprüft werden. Das Ziel ist es deshalb, den Fehlerterm $g(n)$ so klein wie möglich zu machen; dadurch wird auch die Konstante C klein.[3]

Was sind die analytischen Methoden, die hier benutzt werden? Manche Leser mögen mit Fourier-Analysis vertraut sein, das heißt, dem Zerlegen einer zeitabhängigen Funktion in Sinuswellen mit verschiedenen Frequenzen. Wir machen das sogar jeden Tag, wenn wir ein analoges Radio anschalten, oder

[3] Wir können auch die Fragestellung etwas zu unseren Gunsten anpassen (zum Beispiel, indem wir manchen Primzahlen ein größeres Gewicht zukommen lassen), so dass der Hauptterm größer als der Fehlerterm wird; solch ein Anpassen hat auch noch andere Vorteile, insbesondere wenn die Gewichtung stetig ist.

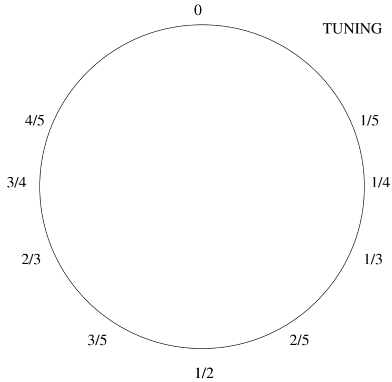

Abbildung 2: Der Drehregler am Radio eines Zahlentheoretikers.

wenn unser Gehirn einen bestimmten Ton heraushört, obwohl mehrere Töne zur gleichen Zeit gespielt werden.

Tatsächlich ist Fourier-Analysis allgemeiner als das: die betrachtete Funktion muss keine Funktion in einer stetigen Variablen, so wie Zeit, sein. Insbesondere, selbst wenn die Funktion nur auf den ganzen Zahlen definiert ist, können wir sie in Frequenzen zerlegen. Es ist hilfreich, diese Frequenzen auf einem Kreis anzuordnen und mit reellen Zahlen zwischen 0 und 1 zu beschreiben, ganz so, wie wir normalerweise Frequenzen auf einer Geraden anordnen und sie beschreiben als "88 Mhz" oder "A = 440 Hz". (Deshalb wird die Strategie, die wir hier beschreiben, auch *Kreismethode* genannt.)

In unserem Fall können wir eine Funktion f definieren, so dass $f(n) = 1$ ist, wenn n eine Primzahl ist und $f(n) = 0$, wenn n keine Primzahl ist. (In Wirklichkeit benutzen wir eine etwas kompliziertere Variante dieser Funktion: wir wollen zum Beispiel, dass $f(n)$ kontinuierlich kleiner wird, wenn n größer wird.) Warum sollte es nun hilfreich sein, solch eine Funktion in Funktionen der Form $n \mapsto \sin(2\pi\alpha n)$ oder $n \mapsto \cos(2\pi\alpha n)$ zu zerlegen?

Ein additives Problem, so wie das von Goldbach, kann mit Hilfe von *Faltungen* umformuliert werden. Die (additive) Faltung $g * h$ von zwei Funktionen g und h ist eine neue Funktion, die aus g und h konstruiert wird. Für eine Zahl n ist $(g * h)(n)$ definiert als die Summe aller $g(m_1)h(m_2)$, wobei wir alle Paare (m_1, m_2) von ganzen Zahlen betrachten, so dass $m_1 + m_2 = n$ ist. In Formeln heißt das

$$(g * h)(n) = \sum_{m_1+m_2=n} g(m_1)h(m_2).$$

Das heißt, wenn wir für die Funktion f, die wir eben definiert haben, zeigen könnten, dass $(f * f)(n) > 0$ gilt, dann wüssten wir dass n auf mindestens eine Weise als Summe zweier Primzahlen geschrieben werden kann. Zeigen wir hingegen $(f * f * f)(n) > 0$, dann wüssten wir, dass n auf mindestens eine Weise als Summe dreier Primzahlen geschrieben werden kann.[4]

Eine der elementaren Eigenschaften einer Zerlegung in Frequenzen ist es, dass das Verhalten einer Faltung unter solch einer Zerlegung sich einfach beschreiben lässt: Die *Fourier-Transformierte* von $g * h$ (das heißt, die Zerlegung in Frequenzen) ist das Produkt der Fourier-Transformierten von g und der Fourier-Transformierten von h. (Eine Fourier-Transformierte $\widehat{f}$ ist eine Funktion vom Raum der Frequenzen (in unserem Fall dem Kreis) in die komplexen Zahlen. Sie sagt aus, "wieviel" von $n \mapsto \sin(2\pi\alpha n)$ oder $n \mapsto \cos(2\pi\alpha n)$ in f enthalten ist; das heißt, es ist die Stärke dessen, was man hört, wenn man den Drehregler am Radio auf α stellt.)

Es stellt sich heraus, dass $\widehat{f}(\alpha)$ besonders groß ist, wenn α nahe zu einem Bruch mit kleinem Nenner ist (so wie die Brüche, die am Drehregler in Abbildung 2 zu sehen sind). (Das ist, wenn man so will, analog dazu, dass der Empfang beim Radio besser wird, wenn man den Drehregler näher an die Frequenz eines Radiosenders stellt.) Die Anteile des Kreises, die nahe zu solchen Brüchen sind, werden *Hauptbögen* genannt; der Rest heißt *Restbögen*. Seit dem Artikel von Vinogradov war der Kern der Idee immer, $\widehat{f}(\alpha)$ so genau wie möglich zu bestimmen, wenn α in einem Hauptbogen liegt, und dann zu zeigen, dass $\widehat{f}$ außerhalb kleine Werte annimmt. Das erlaubt es uns dann, ein Integral abzuschätzen, von dem wir wissen, dass es einen Wert nahe an $(f * f * f)(n)$ hat.

Leider ist das auch der Punkt, an dem dieser Ansatz zusammenbricht für die starke Goldbach-Vermutung. Hauptbögen werden "Haupt" genannt, nicht weil sie besonders groß sind (sind sie nicht), sondern weil sie den Hauptanteil des Integrals von $\widehat{f}(\alpha)^3$ auf dem Kreis ausmachen. Wenn man stattdessen $\widehat{f}(\alpha)^2$ integriert (so wie es der Fall ist, wenn man nun zwei statt drei Primzahlen aufaddiert), dann ist der Anteil der "Haupt"bögen nicht mehr der Hauptanteil – sondern das Integral von $|\widehat{f}(\alpha)|^2$ auf den Restbögen. Quadrieren verstärkt zwar die Spitzenausschläge, aber nicht so sehr wie es Kubieren tut. Um von hier aus weiterzukommen, müssten wir also $\widehat{f}(\alpha)$ relativ genau auf den Restbögen bestimmen; und das weiß im Moment noch niemand, wie wir das tun könnten.

4 Zusammenfassung

Dies ist der allgemeine Aufbau eines solchen Beweises. Was ist nun neu in meiner Arbeit? Ich habe den gesamten Beweis von Anfang an durchgearbeitet und in jedem Teilschritt Verbesserungen gefunden: die Abschätzungen für $\widehat{f}(\alpha)$ auf

[4] Warum gilt das?

den Hauptbögen, die oberen Schranken auf den Restbögen (der schwierigste Teil, meiner Meinung nach) und auch wie die beiden zusammenspielen. Einige der Methoden, die ich entwickelt oder verbessert habe, werden sich sicher auch in anderen Bereichen der Zahlentheorie oder vielleicht sogar der angewandten Mathematik als nützlich erweisen.

Manches von dem, was ich hier geschrieben habe, findet sich auch in einem englischen, etwas längeren und detaillierteren Text, den ich vor einigen Monaten geschrieben habe. Dieser Schnappschuss moderner Mathematik basiert teilweise auf dem genannten Text, der sich jedoch mehr auf die Neuheiten in meinem Beweis fokussiert. Die erste Version dieses längeren Textes erschien auf meinem Blog (http://valuevar.wordpress.com); spätere Versionen in Spanisch und Französisch wurden als [2] und [3] veröffentlicht. Derselbe Text diente auch als Grundlage eines noch detaillierteren Artikels, der im Zusammenhang mit meinem Vortrag auf der International Conference of Mathematicians in Korea im August 2014 in einem Tagungsband erscheinen wird. Und wer den gesamten Beweis lesen möchte, kann dies in meinen Artikeln [5], [4] und [6] tun, die ich versucht habe, so klar und lesbar wie möglich zu schreiben.

Bildquellen

Abb. 1, linke Seite: "Leonhard Euler, ein Porträt von Emanuel Handmann, 1753". Lizenziert unter Public domain via Wikimedia Commons, http://commons.wikimedia.org/wiki/File:Leonhard_Euler.jpg, [Online; abgerufen am 6.8.2014]

Abb. 1, rechte Seite: "Christian Goldbach: Correspondance mathémathique et physique de quelques célèbres géomètres du XVIIIème siècle (Vol. 1), St. Pétersbourg 1843, p. 125–129". Lizenziert unter Public domain via Wikimedia Commons, http://commons.wikimedia.org/wiki/File:Letter_Goldbach-Euler.jpg, [Online; abgerufen am 6.8.2014]

Literatur

[1] L. E. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality*, Chelsea Publishing Co., New York, 1966.

[2] H. A. Helfgott, *La conjetura débil de Goldbach*, La Gaceta de la Real Sociedad Matemática Española **16** (2013), Nr. 4.

[3] ———, *La conjecture de Goldbach ternaire*, Zur Veröffentlichung angenommen in *The Mathematical Gazette*.

[4] ———, *Major arcs for Goldbach's problem*, Preprint. Abrufbar unter http://arxiv.org/abs/1305.2897.

[5] ———, *Minor arcs for Goldbach's problem*, Preprint. Abrufbar unter http://arxiv.org/abs/1205.5252.

[6] ———, *The Ternary Goldbach Conjecture is true*, Preprint. Abrufbar unter http://arxiv.org/abs/1312.7748.

[7] H. A. Helfgott und D. Platt, *Numerical verification of ternary Goldbach*, Zur Veröffentlichung angenommen in *Experimental Mathematics*. Abrufbar unter http://arxiv.org/abs/1305.3062.

[8] M. Ch. Liu und T. Wang, *On the Vinogradov bound in the three primes Goldbach conjecture*, Acta Arithmetica **105** (2002), Nr. 2, 133–175.

[9] T. Oliveira e Silva, S. Herzog und S. Pardi, *Empirical verification of the even Goldbach conjecture, and computation of prime gaps, up to* $4 \cdot 10^{18}$, Zur Veröffentlichung angenommen in *Mathematics of Computation*, 2013.

[10] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Doklady Akademii Nauk SSSR **15** (1937), 291–294.

Harald Helfgott *forscht an der École Normale Supérieur in Paris, Frankreich.*

Übersetzt aus dem Englischen von
Anja Randecker

Mathematische Gebiete
Algebra und Zahlentheorie

Verbindungen zu anderen Gebieten
Informatik

DOI
10.14760/SNAP-2014-003-DE

Schnappschüsse moderner Mathematik aus Oberwolfach bieten spannende Einblicke in die aktuelle mathematische Forschung. Sie werden von Teilnehmerinnen und Teilnehmern des wissenschaftlichen Programms des Mathematischen Forschungsinstituts Oberwolfach (MFO) geschrieben. Die Schnappschüsse haben zum Ziel, Verständnis und Wertschätzung für moderne Mathematik und mathematische Forschung in der interessierten Öffentlichkeit weltweit zu fördern. Alle Schnappschüsse werden in Kooperation mit der IMAGINARY Onlineplattform veröffentlicht und können unter www.imaginary.org/snapshots sowie www.mfo.de/snapshots abgerufen werden.

ISSN 2626-1995