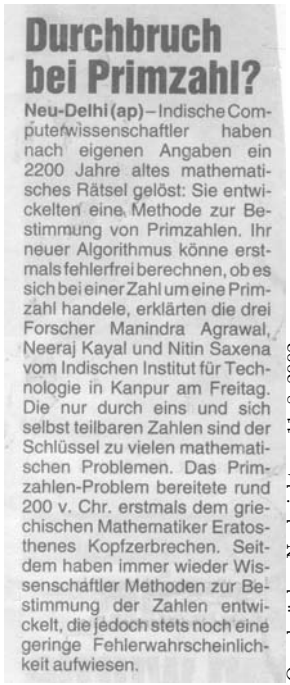

Durchbruch bei Primzahl?

Neu-Delhi (ap) – Indische Computerwissenschaftler haben nach eigenen Angaben ein 2200 Jahre altes mathematisches Rätsel gelöst: Sie entwickelten eine Methode zur Bestimmung von Primzahlen. Ihr neuer Algorithmus könne erstmals fehlerfrei berechnen, ob es sich bei einer Zahl um eine Primzahl handele, erklärten die drei Forscher Manindra Agrawal, Neeraj Kayal und Nitin Saxena vom Indischen Institut für Technologie in Kanpur am Freitag. Die nur durch eins und sich selbst teilbaren Zahlen sind der Schlüssel zu vielen mathematischen Problemen. Das Primzahlen-Problem bereitete rund 200 v. Chr. erstmals dem griechischen Mathematiker Eratosthenes Kopfzerbrechen. Seitdem haben immer wieder Wissenschaftler Methoden zur Bestimmung der Zahlen entwickelt, die jedoch stets noch eine geringe Fehlerwahrscheinlichkeit aufwiesen.

Osnabrücker Nachrichten, 11. 8. 2002

Ein Durchbruch für „Jedermann“

von Folkmar Bornemann

„New Method Said to Solve Key Problem in Math“ titelte die New York Times am 8. August 2002 und meinte den Nachweis von PRIMES $\in \mathcal{P}$*, ein bislang großes offenes Problem der algorithmischen Zahlentheorie und theoretischen Informatik. Manindra Agrawal, Neeraj Kayal und Nitin Saxena vom Indian Institute of Technology war es durch einen überraschend eleganten und brilliant einfachen Algorithmus gelungen, die binnen weniger Tage von der Korrektheit überzeugte Fachwelt ins Schwärmen zu versetzen: „This algorithm is beautiful“ (Carl Pomerance), „It's the best result I've heard in over 10 years“ (Shafi Goldwasser).*

Vier Tage vor der Schlagzeile in der *New York Times*, an einem Sonntag, hatten die drei einen neunseitigen Preprint mit dem Titel „PRIMES is in P“ an 15 Fachleute verschickt. Noch am Abend gratulierten Jaikumar Radhakrishnan und Vikraman Arvind. Montag früh befand einer der Altmeister des Fachs, Carl Pomerance, das Resultat für korrekt, organisierte in seiner Begeisterung für den Nachmittag ein spontanes Seminar und informierte Sara Robinson von der *New York Times*. Dienstag wurde der Preprint im Internet frei zugänglich [1]. Donnerstag beendete eine weitere Koryphäe, Hendrik Lenstra Jr., eine kurze Nörgelei im E-Mail-Verteiler `NMBRTHRY` mit dem Diktum:

> The remarks [...] are unfounded and/or inconsequential. The proofs [...] do NOT have too many additional problems to mention. The only true mistake is [...], but that is quite easy to fix. Other mistakes [...] are too minor to mention. The paper is in substance completely correct.

Und bereits am Freitag stellte Dan Bernstein einen auf eine Seite verkürzten, geglätteten Beweis des Hauptresultats ins Netz [2].

Diese für die Mathematik ungewöhnlich kurze Prüfungsphase spiegelt neben der Kürze und Eleganz des Arguments auch seine technische Einfachheit wider, „suited for undergraduates“. Zwei der Autoren, Kayal und Saxena, haben selbst erst dieses Frühjahr ihren Bachelor-Abschluss in Computer Science erworben. Handelt es sich also ausnahmsweise um einen für „Jedermann“ verstehbaren Durchbruch?

Hans-Magnus Enzensberger positionierte in seiner Rede auf dem Berliner ICM 1998 die Mathematik sowohl im „Jenseits der Kultur“ als auch in einem goldenen Zeitalter durch Erfolge einer Qualität, die er beim Theater oder Sport vermisste. Allerdings stellen etliche jener Erfolge selbst viele Mathematiker vor die Frage nach dem Jenseits und Diesseits *innerhalb* der Mathematik. Konnte ein Nichtspezialist – Hand auf's Herz: wieviele von uns sind nicht ein solcher „Jedermann“? – den Beweis der Fermat'schen Vermutung durch Andrew Wiles zwar weder wirklich begreifen noch gar in voller Gänze würdigen, so halfen ihm populärwissenschaftliche Bemühungen wie das Buch von Simon Singh wenigstens anhand eines fernen Echos die Zusammenhänge zu ahnen. Bei den diesjährigen Empfängern der Fields-Medaille dürfte sich wohl kein Autor finden, der „Jedermann“ behilflich wäre, ihre Erfolge und deren Bedeutung nachzuvollziehen.

So bastelt jeder an seiner Zinne des Turms zu Babel namens Mathematik und hält die hier erzielten Erfolge für die wesentlichen. Selten genug stellt sich wie jetzt Anfang August ein Erfolg, ja gar ein Durchbruch ein, der vom Fundament des Turms aus für „Jedermann“ in sich verstehbar wäre.

Angesichts dessen sprach Paul Leyland aus, was viele dachten: „Everyone is now wondering what else has been similarly overlooked.“

Kann dies erklären, was Agrawal in großes Erstaunen versetzte („I never imagined that our result will be of much interest to traditional mathematicians“); nämlich warum auf die eigens eingerichtete Webseite innerhalb der ersten zehn Tage über zwei Millionen Zugriffe erfolgten und dreihunderttausendfach der Preprint heruntergeladen wurde?

- 10.1515/dmvm-2002-0079

> “When a long outstanding problem is finally solved, every mathematician would like to share in the pleasure of discovery by following for himself what has been done. But too often he is stymied by the abstruseness of so much of contemporary mathematics. The recent negative solution to [...] is a happy counterexample. In this article, a complete account of this solution is given; the only knowledge a reader needs to follow the argument is a little number theory: specifically basic information about divisibility of positive integers and linear congruences.”
>
> Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly 80 (1973), pp. 233–269, erster Absatz der Einleitung.

Als Numeriker kein algorithmischer Zahlentheoretiker, außerhalb meiner Zinne solch ein „Jedermann“, wollte ich die Probe auf's Exempel machen.

Das Problem

Erfreulicherweise motivieren die Drei ihre Arbeit nicht mit der Bedeutung von Primzahlen für Kryptographie und E-Commerce, sondern sie übernehmen zu Beginn vom geschichtsbewussten Don Knuth ein Zitat des großen Carl Friedrich Gauß aus dem Artikel 329 der *Disquisitiones Arithmeticae* (1801), hier wiedergegeben in der Maser'schen Übersetzung von 1889:

> Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten als auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. [...] ausserdem dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen.

In der Schule lernt man das Sieb des Eratosthenes kennen; nur leider benötigt damit der Nachweis, dass n prim ist, eine Rechenzeit im wesentlichen proportional zu n selbst. Die Eingabelänge[1] der Zahl ist hingegen proportional zur Anzahl der Dualstellen, also in etwa $\log_2 n$, so dass wir hier einen Algorithmus mit *exponentieller* Laufzeit $O(2^{\log_2 n})$ vor uns haben. Um nochmals Gauß aus dem Artikel 329 seiner *Disquisitiones* zu zitieren:

> Trotzdem muss man gestehen, dass alle bisher angegebenen Methoden entweder auf sehr specielle Fälle beschränkt oder so mühsam und weitläufig sind, dass sie [...] auf grössere Zahlen aber meistenteils kaum angewendet werden können.

Kann die Primalität sehr großer Zahlen *prinzipiell* effizient entschieden werden? Diese Frage wird im Rahmen der modernen Komplexitätstheorie mathematisch durch die Forderung einer *polynomialen* Laufzeit konkretisiert: Gibt es einen deterministischen[2] Algorithmus, der mit einem festen Exponenten κ für jede natürliche Zahl n in $O(\log^\kappa n)$ Rechenschritten entscheidet, ob diese prim ist oder nicht; kurz die bislang große offene Frage: gilt $\text{PRIMES} \in \mathcal{P}$?

Stand der Dinge vor August 2002

Spätestens seit Gauß ist die Entscheidung über die Primalität einer Zahl im Falle der Zusammengesetztheit nicht länger mit einer (partiellen) Faktorisierung verbunden. Im Artikel 334 der *Disquisitiones* heißt es:

> Die letztere [Bemerkung] aber verdient insofern den Vorzug, als sie meistens eine einfachere Rechnung gestattet, indessen giebt sie nicht immer [...] die Factoren der zusammengesetzten Zahlen selbst, jedoch unterscheidet auch sie die zusammengesetzten Zahlen von den Primzahlen.

Ausgangspunkt vieler solcher Verfahren ist der kleine Satz von Fermat. Er besagt, dass für eine *Primzahl* n und eine zu n teilerfremde Zahl a stets gilt

$$a^n \equiv a \mod n.$$

Leider ist die Umkehrung falsch, Primzahlen lassen sich auf diese Weise nicht charakterisieren. Andererseits „using the Fermat congruence is so simple, that it seems a shame to give up on it just because there are a few counter examples“ (Carl Pomerance). So nimmt es nicht Wunder, dass Verfeinerungen dieses Kriteriums Grundlage wichtiger Algorithmen sind:

Der elementare *probabilistische* Algorithmus von Miller und Rabin aus dem Jahre 1976 bemüht einen Zufallszahlengenerator und stellt nach k Durchläufen entweder fest, dass die Zahl *mit Sicherheit* zusammengesetzt ist, oder dass die Zahl *höchstwahrscheinlich* prim ist, wobei die Wahrscheinlichkeit eines Irrtums bei unter 4^{-k} liegt. Die Zeitkomplexität liegt bei $O(k \log^2 n)$, wobei das Groß-O eine relativ

1 Den Unterschied zwischen der *Größe* einer Zahl und ihrer *Länge* macht man sich am besten an solch plakativen Giganten klar wie der Anzahl der Atome im Universum, ca. 10^{79}, oder der Gesamtanzahl aller je von Mensch und Computer durchgeführten Rechenoperationen, ca. 10^{24}: 80 bzw. 25 Dezimalziffern sind vergleichsweise schnell hingeschrieben.

2 D. h. ein Algorithmus, der ohne Zufallszahlen auskommt, im Gegensatz zu *probabilistischen*, die solche benötigen.

kleine Konstante enthält. Der Algorithmus ist in der Praxis also sehr schnell und findet seine Verwendung in Kryptographie und E-Commerce zur Produktion von „industrial-grade primes“ (Henri Cohen). In der Sprache der Komplexitätstheorie heißt dies knapp PRIMES $\in$ co-$\mathcal{RP}$.

Beim *deterministischen* Algorithmus von Adleman, Pomerance und Rumely aus dem Jahre 1983 wird sehr viel mehr Theorie betrieben und der kleine Fermat'sche Satz so auf ganze Zahlen eines Kreisteilungskörpers verallgemeinert, dass Primzahlen vollständig charakterisiert werden können. Die Laufzeit liegt bei superpolynomialem $(\log n)^{O(\log\log\log n)}$, die beste für einen deterministischen Algorithmus vor dem August 2002. Der dreifache Logarithmus im Exponenten wächst allerdings so langsam, dass sich praktische Varianten im Rekordfieber von Primalitätsbeweisen für Zahlen mit mehreren tausend Dezimalstellen exzellent geschlagen haben.[3]

Eine andere Klasse moderner Algorithmen benutzt elliptische Kurven beziehungsweise abelsche Varietäten höheren Geschlechts. So konnten Adleman und Huang 1992 in einem sehr schwierigen und technischen Büchlein zeigen, dass es einen *probabilistischen* Algorithmus polynomialer Laufzeit gibt, der nach k Durchläufen entweder eine definitive Antwort liefert (Irrtum ausgeschlossen) oder gar keine, letzteres aber mit einer Wahrscheinlichkeit kleiner 2^{-k}. In der Sprache der Komplexitätstheorie heißt dies knapp PRIMES $\in \mathcal{ZPP}$.

Vor diesem Hintergrund, angesichts des erreichten Schwierigkeitsgrades und des Ausbleibens weiterer Erfolge in über zehn Jahren, war nicht zu erwarten, dass die Ausgangsfrage kurz, elegant und für „Jedermann“ verständlich beantwortet werden könnte.

Auftritt Manindra Agrawal

Der Informatiker und Komplexitätstheoretiker Manindra Agrawal erwarb 1991 seinen Doktortitel am Department of Computer Science & Engineering des Indian Institute of Technology in Kanpur (IITK). Nach einem Aufenthalt als Humboldt-Stipendiat an der Universität Ulm 1995/96 („I really enjoyed the stay in Ulm. It helped me in my research and career in many ways.“) kehrte er als Professor nach Kanpur zurück. Er hatte im vergangenen Jahr auf sich aufmerksam gemacht, als er eine abgeschwächte Form

Manindra Agrawal

der Isomorphie-Vermutung der Komplexitätstheorie bewies.[4]

Um 1999 arbeitete er mit seinem Doktorvater Somenath Biswas an der Frage, mit probabilistischen Algorithmen die Gleichheit von Polynomen zu entscheiden. Als unschuldige Anwendung findet sich in der Publikation „Primality and Identity Testing via Chinese Remaindering“ [3] ein neuer probabilistischer Primalitätstest.

Ausgangspunkt war dabei eine Verallgemeinerung des kleinen Fermat'schen Satzes auf *Polynome*, die eine leichte Übungsaufgabe für eine einführende Zahlentheorie- oder Algebra-Vorlesung sein könnte: Sind die natürlichen Zahlen a und n teilerfremd, so ist n *dann und nur dann* prim, wenn im Ring der Polynome $\mathbb{Z}[x]$ gilt

$$(x-a)^n \equiv (x^n - a) \mod n.$$

Eine sehr elegante Charakterisierung von Primzahlen, aber keine zunächst brauchbare. Allein die Berechnung von $(x-a)^n$ verlangt mehr Rechenzeit als das Sieb des Eratosthenes. Aber gerade für Polynome dieser Größe hatten Agrawal und Biswas einen probabilistischen Gleichheitstest beschränkter Irrtumswahrscheinlichkeit entwickelt, der auf die vollständige Aufstellung der Polynome verzichtete. Leider befand sich der resultierende Test polynomialer Laufzeit weit außer Konkurrenz zu dem von Miller und Rabin. Eine neue Idee war geboren und taugte zunächst nur für eine Fußnote in der Geschichte der Primalitätstests.

Zwei Jahre später begann Agrawal, mit seinen Studenten am IITK das Potential der neuen Primzahl-

3 Der Held einer anderen Geschichte, Preda Mihăilescu, hat in seiner Dissertation an der ETH Zürich wesentliche Verfeinerungen dieses Algorithmus entwickelt und war lange Zeit mit seinen Implementierungen an der Rekordjagd beteiligt. Jetzt soll er die Catalan'sche Vermutung bewiesen haben, vgl. den Beitrag von Gerhard Frey auf S. 8

4 Die Isomorphie-Vermutung von Berman und Hartmanis impliziert $\mathcal{P} \neq \mathcal{NP}$. Ein Beweis würde also das erste der sieben Milleniumsprobleme des Clay-Instituts lösen und eine Million Dollar einbringen.

charakterisierung, an das er fest glaubte, genauer zu untersuchen.

Zwei Bachelor-Arbeiten

Das Zulassungsverfahren zum Studium am Indian Institute of Technology ist äußerst streng und selektiv. Für das Studium an einem der sieben Standorte des IIT und zwei weiteren Institutionen gibt es ein zweistufiges gemeinsames Zulassungsverfahren („Joint Entrance Examination (JEE)“). So bewarben sich für die Zulassung in diesem Jahr 150 000 Inder, nach einer ersten dreistündigen Klausur in Mathematik, Physik und Chemie wurden 15 000 zur zweiten Prüfung eingeladen, bestehend aus je einer zweistündigen Klausur in den drei Fächern. Schließlich wurden 2900 Studienplätze vergeben, davon 45 für Informatik am sehr renommierten IIT in Kanpur. Kein Wunder, dass in Indien gutes Geld mit der Vorbereitung der Kandidaten auf die gefürchtete JEE verdient wird und Absolventen des IIT in aller Welt mit Kusshand eingestellt werden.

Mit solch hochmotivierten Studenten arbeitete Agrawal nun weiter am Primalitätstest. Mit Rajat Bhattacharjee und Prashant Pandey kam die Idee auf, statt der viel zu großen Polynompotenzen $(x-a)^n$ nur deren Reste nach Division durch x^r-1 zu betrachten. Bleibt r logarithmisch in n, so lassen sich diese sehr viel kleineren Reste mit geschickten Algorithmen direkt in polynomialer Laufzeit berechnen.

Ist n eine Primzahl, so ist sicherlich[5]

$$(x-a)^n \equiv x^n - a \mod (x^r-1, n) \qquad (T_{r,a})$$

für jedes r und zu n teilerfremde a. Welche a und r erlauben den umgekehrten Schluss, dass n prim ist?

Die beiden Studenten fixierten in ihrer gemeinsamen Bachelor-Arbeit [4] $a=1$ und untersuchten die nötigen r. Durch Auswertung von Experimenten mit $r \le 100$ und $n \le 10^{10}$ gelangten sie zu folgender Vermutung. Falls r kein Teiler von n ist und

$$(x-1)^n \equiv x^n - 1 \mod (x^r-1, n) \qquad (T_{r,1})$$

gilt, ist entweder n prim oder es gilt $n^2 \equiv 1 \mod r$. Letzteres ist für eine der ersten $\log_2 n$ Primzahlen r nicht der Fall, so dass man einen Nachweis der Primalität von n in polynomialer Laufzeit $O(\log^{3+\varepsilon} n)$ erhalten würde.

Nun traten die bislang fehlenden Helden unserer Geschichte auf, die Studenten Neeraj Kayal und Nitin Saxena. Beide waren Mitglieder der indischen

Neeraj Kayal

Nitin Saxena

Mannschaft bei der internationalen Mathematik-Olympiade 1997. Informatik statt Mathematik studierten sie wegen der besseren Berufsaussichten, fanden aber in der Komplexitätstheorie einen Weg, sich weiterhin mit Mathematik auf hohem Niveau zu befassen.

Sie untersuchten in ihrer gemeinsamen Bachelor-Arbeit die Beziehung des Tests $(T_{r,1})$ zu bekannten Primalitätstest-Primitiven, die wie $(T_{r,1})$ im negativen Fall zwar den Nachweis liefern, dass eine Zahl zusammengesetzt ist, im positiven Fall hingegen keinen definitiven Schluss zulassen. Die Ernte fiel reich aus. Sie konnten zeigen, dass die Gültigkeit der Riemann'schen Vermutung erlauben würde, zum Primalitätsbeweis den Test $(T_{r,1})$ auf $r = 2, \ldots, 4\log_2^2 n$ zu beschränken. Auf diese Weise erhielte man einen deterministischen Algorithmus der Zeitkomplexität $O(\log^{6+\epsilon} n)$. Desweiteren konnten sie zeigen, dass die von Bhattacharjee und Pandey formulierte Vermutung aus einer seit langem geäußerten Vermutung von Carl Pomerance folgt.

Und sie führten im Zusammenhang einer von ihnen untersuchten Gruppe „introspektiver“ Zahlen eine Beweisidee ein, die sich später als wesentlich erweisen sollte.

Die im April 2002 abgegebene Arbeit [5] der beiden trägt den Titel „Towards a deterministic polynomial-time primality test“. Eine Vision, das Ziel ist schon fest im Auge.

Veränderung des Blickwinkels

Sie fuhren in diesem Sommer zunächst nicht zur Familie nach Hause, sondern begannen sofort mit dem Doktorstudium. Saxena hatte eigentlich ins Ausland gehen wollen, aber – Ironie des Schicksals – kein Stipendium für die Universität seiner Wahl erhalten.

Nur eine kleine Veränderung des Blickwinkels ist noch nötig. Beide Bachelor-Arbeiten haben den Test $(T_{r,a})$ für festes $a=1$ und variierendes r studiert. Was kommt heraus, wenn man stattdessen r fixiert

5 Ich folge der Notation von Agrawal et al. und bezeichne mit $p(x) \equiv q(x) \mod (x^r-1, n)$ die Gleichheit der Reste der Polynome $p(x)$ und $q(x)$ nach Division durch x^r-1 und Division der Koeffizienten durch n.

und a variieren lässt? Am Morgen des 10. Juli gelang der Durchbruch: bei geeigneter Wahl der Parameter erhält man nichts weniger als eine Charakterisierung von *Primzahlpotenzen*.

Das durch Dan Bernstein geglättete Ergebnis lautet nun wie folgt.

Satz von Agrawal-Kayal-Saxena. *Für $n \in \mathbb{N}$ seien q, r prim und $s \le n$ so gewählt, dass $q \mid r-1$, $n^{(r-1)/q} \not\equiv 0, 1 \mod r$ und*

$$\binom{q+s-1}{s} \ge n^{2\lfloor\sqrt{r}\rfloor}.$$

Gilt dann für alle $1 \le a < s$, dass (i) a teilerfremd zu n ist und (ii) im Ring der Polynome $\mathbb{Z}[x]$ $(x-a)^n \equiv x^n - a \mod (x^r-1, n)$, so ist n eine Primzahlpotenz.

Der einfache, kurze und ideenreiche Beweis des Satzes bereitet soviel Vergnügen, dass ich es mir nicht verkneifen konnte, ihn im Anhang zu skizzieren.

Der Satz führt unmittelbar zum mittlerweile so genannten **AKS-Algorithmus**:[6]

1. Entscheide, ob n echte Potenz einer natürlichen Zahl ist. Wenn ja, gehe zu Schritt 5.
2. Wähle (q, r, s) gemäß den Voraussetzungen des Satzes.
3. Für $a = 1, \ldots, s-1$ tue jeweils folgendes:
   (i) Ist a Teiler von n, gehe zu Schritt 5.
   (ii) Ist $(x-a)^n \not\equiv x^n - a \mod (x^r-1, n)$, gehe zu Schritt 5.
4. n ist prim. Fertig.
5. n ist zusammengesetzt. Fertig.

Schritt 1 lässt sich mit Varianten der Newton-Iteration in polynomialer Laufzeit erledigen. Die Laufzeit des dominierenden Schrittes 3 ist bei Verwendung schneller FFT-basierter Arithmetik gegeben durch $\tilde{O}(s\, r \log^2 n)$, wobei die Tilde über dem Groß-O weitere logarithmische Faktoren in s, r und $\log_2 n$ unterdrückt.

Wir müssen also für unser Ziel s und r höchstens polynomial in $\log n$ wachsen lassen. Dies ist Aufgabe des Schritts 2. Schauen wir uns zunächst an, was prinzipiell möglich ist. Wählt man $s = \theta q$ mit einem festen Faktor θ, so liefert die Stirling'sche Formel die Asymptotik

$$\log \binom{q+s-1}{s} \sim c_\theta^{-1} q.$$

Die Bedingungen des Satzes erfordert demnach asymptotisch

$$q \gtrsim 2c_\theta \lfloor\sqrt{r}\rfloor \log n.$$

Für große n kann das im wesentlichen nur funktionieren, wenn es wenigstens unendlich viele Primzahlen r gibt, so dass $r-1$ einen Primfaktor $q \ge r^{1/2+\delta}$ besitzt. Dabei handelt es sich um ein gut studiertes Problem der analytischen Zahlentheorie.

Sophie Germain und die Fermat'sche Vermutung

Das bestmögliche Preis-Leistungsverhältnis q/r erhält man für die nach Sophie Germain benannten ungeraden Primzahlen q, für welche auch $r = 2q+1$ prim ist. Sie hatte 1823 für diese Primzahlen gezeigt, dass der sogenannte erste Fall der Fermat'schen Vermutung gilt: $x^q + y^q = z^q$ besitzt keine ganzzahlige Lösung mit $q \nmid xyz$. Deshalb begann man sich brennend dafür zu interessieren, ob es denn wenigstens unendlich viele dieser freundlichen Primzahlen gibt. Unglücklicherweise weiß man es bis auf den heutigen Tag nicht. Heuristische Überlegungen führten Hardy und Littlewood 1922 jedoch zu folgender sehr präzisen Vermutung über die tatsächliche Dichte von Germain-Primzahlen

$$\#\{q \le x : q \text{ und } 2q+1 \text{ sind prim}\} \sim \frac{2C_2\, x}{\ln^2 x},$$

wobei $C_2 = 0.6601618158\ldots$ die Primzahlzwillings-Konstante ist.

Wäre diese Vermutung richtig, so könnte man Primzahlen q und $r = 2q+1$ der Größe $O(\log^2 n)$ finden, welche den Voraussetzungen des Satzes der Drei entsprechen. Der AKS-Algorithmus hätte dann die polynomiale Laufzeit $\tilde{O}(\log^6 n)$. Da die Vermutung bis $x = 10^{10}$ eindrucksvoll bestätigt worden ist, wird sich der AKS-Algorithmus in jedem Fall für bis zu 100 000-stellige Zahlen n wie einer der Komplexität $\tilde{O}(\log^6 n)$ verhalten.

Fast zehn Jahre vor dem endgültigen Beweis der Fermat'schen Vermutung durch Andrew Wiles bewiesen Adleman, Fouvry und Heath-Brown 1985, was mit Hilfe der Germain-Primzahlen nicht gelungen war, nämlich dass der erste Fall für unendlich viele Primzahlen richtig ist [6]. Dabei hatten Adleman und Heath-Brown in Verallgemeinerung der Germain-Primzahlen genau jene Paare (q, r) studiert, die auch für den AKS-Algorithmus eine große Rolle spielen.

6 Unter `http://www.ma.tum.de/m3/ftp/Bornemann/PARI/aks.txt` findet sich eine lauffähige Implementierung für das frei verfügbare Zahlentheorie-Programmpaket PARI-GP (`http://www.parigp-home.de`).

Eine Fields-Medaille

Präzise verlangten sie, dass die Abschätzung

$$\#\left\{r \le x : q, r \text{ prim}; q \mid r-1; q \ge x^{1/2+\delta}\right\} \ge c_\delta \frac{x}{\ln x}$$

einen zulässigen Exponenten $\delta > 1/6$ besitzt. Die Jagd nach dem größten δ hatte 1969 mit Morris Goldfeld [7] begonnen, der $\delta \approx 1/12$ erhalten hatte. Étienne Fouvry [8] beendete sie vorläufig 1985 mit $\delta = 0,1687 > 1/6$. Alle diese Arbeiten benutzen sehr tiefe Methoden aus der analytischen Zahlentheorie, welche das *große Sieb* des Enrico Bombieri weiterentwickeln. Dieses Sieb hatte er 1965 im Alter von 25 Jahren publiziert, 1974 erhielt er die Fields-Medaille. Es dürfte also „Jedermann“ schwer fallen, den Beweis dieser Abschätzung im Detail verstehen zu wollen. Manindra Agrawals Antwort auf meine Frage, ob sich einer der drei dieser Mühe unterzogen hätte, lautet:

> We tried! But Sieve theory was too dense for us – we have no background in analytical number theory. So after a while we just gave up.

Sie brauchten es auch nicht, „the result was stated there in precisely the form we needed“, und sie konnten sich seiner Korrektheit im Vertrauen auf Begutachtungen und eines gewissen zeitlichen Abstandes gewiss sein. Umso mehr als das Ergebnis von Fouvry im Zusammenhang mit der heiß umkämpften Fermat'schen Vermutung stand und in den *Inventiones* erschienen war.

Oder doch nicht? Fouvry vergaß bei der Zitation eines Lemmas von Bombieri, Friedlander und Iwaniec eine Bedingung mit anzugeben und mit zu berücksichtigen. Diese zusätzliche Bedingung *verkleinert* den ermittelten Wert von δ – auf $\delta = 0,1683 > 1/6$. Er hätte auch unterhalb der kritischen Schwelle sein können. Fouvry hat diese Korrektur später Roger Baker mitgeteilt und sie ist in einem Überblicksartikel [9] von diesem und Glyn Harman 1996 publiziert worden.

Agrawal, Kayal und Saxena waren übrigens auf Fouvrys Artikel über eine Internetsuche mit *Google* in der Literaturliste einer Arbeit von Pomerance und Shparlinski gestoßen. Auf Nachfrage nach dem besten bekannten Wert für δ hatte ersterer sie dann auf die Arbeit von Baker und Harman verwiesen.

Unabhängig vom bestmöglichen Wert reicht $\delta > 0$ aus, um ein für den AKS-Algorithmus zulässiges Tripel (q, r, s) der benötigten polynomialen Größe zu garantieren,

$$r = O(\log^{1/\delta} n), \qquad q, s = O(\log^{1+1/2\delta} n).$$

Der AKS-Algorithmus hat damit insgesamt eine garantierte Laufzeit von $\tilde{O}(\log^{3+3/2\delta} n)$. Damit ist die Aussage PRIMES $\in \mathcal{P}$ bewiesen, der Durchbruch gelungen. Gratulation! Fouvrys korrigierter Wert für δ liefert $\tilde{O}(\log^{11.913} n)$, oder einfacher zu merken und dann auch ohne Tilde: $O(\log^{12} n)$.[7]

Der Direktor des IIT in Kanpur, Sanjay Dhande, war so begeistert von der Schlagzeile in der New York Times, dass er sich sicher zeigte, Agrawal würde für die höchsten Auszeichnungen in der Mathematik nominiert. In vier Jahren wird er 40 Jahre alt sein.

Wie praktisch!?

In den Newsgroups und den Zeitungen wird schnell die Frage nach der praktischen Verwertbarkeit gestellt, sind doch große Primzahlen heute wichtiger Bestandteil von Kryptographie und E-Commerce. Halten wir zunächst einmal fest, dass ein wichtiges *theoretisches* Problem gelöst wurde, an dem sich mehrere Jahrzehnte die Fachwelt vergeblich versucht hat. Agrawal selbst betont stets, dass ihn das Problem als intellektuelle Herausforderung interessiert hat und der AKS-Algorithmus gegenwärtig sehr viel langsamer ist als jene Algorithmen, mit welchen die Rekorde der Stellenanzahl von Primzahlbeweisen auf derzeitig 5020 Dezimalstellen[8] hochgetrieben wurden. Man darf schließlich nicht vergessen, dass es sich bei der Definition von Komplexitätsklassen wie $\mathcal{P}$ um das rein theoretische Konzept einer asymptotischen Aussage für $n \to \infty$ handelt. Der Laufzeitvorteil eines polynomialen gegenüber eines superpolynomialen Algorithmus kann daher im Einzelfall sehr wohl erst für so große n in Erscheinung treten, für die keiner der beiden Algorithmen auf gängiger Hardware noch zu unseren Lebzeiten eine Antwort liefern würde. Es kommt in der Praxis auch auf die Konstanten im Groß-O der Komplexitätsabschätzung an.

„Industrial-grade primes“ unterer Qualitätsstufe mit 512 Dualstellen werden auf einem handelsüblichen 2GHz-PC mit Hilfe des Miller-Rabin-Test in Bruchteilen einer Sekunde erzeugt. Bei Bedarf kann in wenigen Sekunden mit dem auf elliptischen Kurven basierenden ECPP-Verfahren nach Atkin-Morain ihre

7 Hendrik Lenstra soll den Exponenten mittlerweile auf 8 gesenkt haben, siehe SIAM News vom September 2002, S. 8.
8 Bitte nicht mit der Rekordjagd nach der *größten* bekannten Primzahl verwechseln, zur Zeit $2^{13\,466\,917} - 1$, eine Mersenne'sche Primzahl mit 4 053 946 Dezimalstellen. Diese Zahlen sind voller Struktur und lassen hochspezialisierte Algorithmen ans Werk.
9 Z. B. mit dem unter `http://www.znz.freesurf.fr/pages/primo.html` frei verfügbaren Programm PRIMO von Marcel Martin, das derzeitig den Rekord hält.

Primalität tatsächlich *bewiesen* werden.[9] Die Laufzeitkomplexität dieses *probabilistischen* Algorithmus ist zwar eine „cloudy issue“ (Carl Pomerance), aber heuristische Überlegungen legen nahe, dass der Erwartungswert gerade auch bei $\tilde{O}(\log^6 n)$ liegt.

Hingegen ist wegen der hohen Kosten der polynomialen Kongruenzen im dritten Schritt des AKS-Algorithmus die Konstante im vermuteten $\tilde{O}(\log^6 n)$-Laufzeitverhalten so groß, dass er an einer 512-Bit-Primzahl zur Zeit ein geschätztes Vierteljahr arbeiten müsste. Dabei ist diese Konstante dank Dan Bernstein, Hendrik Lenstra und José Voloch bereits gegenüber der ursprünglichen Formulierung des Algorithmus um wenigstens den Faktor 10^5 verbessert worden – Stand vom 29. August.[10]

Es fehlt also noch etwa ein Faktor 10^6 zur Konkurrenzfähigkeit. Auch das ECPP-Verfahren startete mit einer völlig inpraktikablen, aber grundlegend neuen Idee von Goldwasser und Kilian. Und die jetzt von Agrawal, Kayal und Saxena vorgelegte Methode ist so unvorhergesehen neu und brilliant, dass wir getrost abwarten können, wozu sie im weiteren Reifungsprozess noch alles fähig sein wird.

Die Medien und stille Post

Bis auf einen exzellent recherchierten, fachlich korrekten, gut lesbaren und ausführlichen Bericht [10] in der indischen Wochenzeitschrift *Frontline* vom 17. August ist die Darstellung in den allgemeinen Medien ein Trauerspiel. Meine Nachfrage nach seinem Eindruck überging Agrawal mit einem höflichen „Leave aside the general public coverage“.

Die anfänglich zitierte New York Times feiert das Ergebnis zwar als Triumph, verunklart aber diesen durch die gewählten Vereinfachungen bis zur Lächerlichkeit: polynomiale Laufzeit wird zu „quickly“, deterministisch zu „definitively“. Der Artikel liest sich dann wie folgt: Drei Inder erzielten Durchbruch, da der Computer nun „quickly and definitively“ sagen könne, ob eine Zahl prim sei. Allerdings habe der neue Algorithmus keine unmittelbaren Anwendungen, da bereits existierende Verfahren schneller seien und sich praktisch nicht irrten. Toller Durchbruch, wird sich der Leser sagen.

The Associated Press (ap) machte aus dem Artikel der New York Times eine Agenturmeldung, dabei wird „definitively“ zu „accurately“, der Aspekt der Laufzeit gerät vollends in den Hintergrund. Zu welch Kuriositäten diese Agenturmeldung nach der Übersetzung von „accurately“ durch „fehlerfrei“ führte, kann anhand des eingangs abgebildeten Artikel aus den Osnabrücker Nachrichten bewundert werden. Schlimm trieb es am Ende dieser stillen Post die Tagesschau auf ihrer Webseite. Am 12. August fand sich unter der Überschrift „Endlich: Primzahlen können exakt berechnet werden!“ solch Schwachsinn wie „Der Jubel an Deutschlands Schulen ist grenzenlos: Endlich kann man Primzahlen angstfrei berechnen!“ Auf Proteste von Teilnehmern des Diskussionsforums `de.sci.mathematik` wurde der Bericht von der Webseite entfernt.

Und die großen deutschsprachigen Tageszeitungen? Die *Süddeutsche Zeitung* berichtete gar nicht, die *Neue Züricher Zeitung* erst am 30. August. Der Artikel suggeriert fälschlicherweise, dass bislang für die in der Kryptographie verwendeten Primzahlen kein absolut sicheres Zertifikat ihrer Primalität „innert vernünftiger Zeit“ berechenbar wäre und genau dies jetzt den drei Indern gelungen sei. Das Ergebnis sei aber doch nicht so großartig wie von den Nachrichtenagenturen und Medien gefeiert, da die größten heute bekannten Primzahlen damit nicht behandelt werden könnten.

Die *Frankfurter Allgemeine Zeitung* brachte im Feuilleton am 9. August unter der Überschrift „Polynomiale Götter: Findige Inder und ihre Primzahlen“ einen kryptischen Text, der zunächst die Beziehung indischer Mathematik zur indischen Götterwelt herstellt und dann vier solcher Gottheiten ein kurzes Gespräch über das neue Ergebnis führen lässt:

> „Wozu ist das denn bitte gut?“ ereiferte sich Agni polternd, und Lakschmi erwiderte voreilig: „Zum Klauen! Man braucht Primzahlen ja zur Verschlüsselung von Daten bei deren elektronischer Übertragung, es gibt da diverse sogenannte kryptographische Algorithmen wie RSA oder den Data Encryption Standard DES; Schlüssel sind Zahlen mit Primfaktorzerlegung, und wenn das jetzt so einfach in einer Zeit geht, die eine ganzrationale Funktion der Eingabedaten ist . . .“ „Aber das gab's doch vorher schon, zum Beispiel den Miller-Rabin-Test, wenn man den oft genug wiederholt, kann man ein Primtestergebnis mit fast beliebig großer Richtigkeitswahrscheinlichkeit auch für die dicksten Zahlen finden“, widersprach Rudra. „Und die verschlüsselnde Primfaktorzerlegung hat mit dem Test, ob eine Zahl überhaupt prim ist, außerdem nix zu tun, das ist ein ganz anderes Problem, für Sicherheitsleute ist das wertlos, was die Typen da gemacht haben.“ Uschas, die Gastgeberin, fand schließlich, als es dämmerte, das versöhnend-erlösende Wort: „Freuen wir uns einfach über ein elegantes Ergebnis, das auch der Westen bewundert, und das Weiteratmen unserer großen mathematischen Tradition!“

Welchem Leser soll bitte daraus der Grund für die Bewunderung klar werden?

10 Vgl. `http://fatphil.asdf.org/maths/AKS`

- 10.1515/dmvm-2002-0079

Zukunftspläne

Die Drei planen, ihre Arbeit bei den *Annals of Mathematics* einzureichen und befinden sich hierzu im Kontakt mit Peter Sarnak. Sie wollen den Artikel neu aufschreiben, „in a more ‘mathematical’ way as opposed to ‘computer science’ way as that would be more suitable in Annals“.

Und zur Gefühlslage und Zukunft der beiden Doktoranden Kayal und Saxena sagt Agrawal:

> They are happy, but at the same time quite cool about it. I would say they are very level-headed boys. As for their PhD, yes I am sure that this work will qualify for their PhD. But I have advised them to stay back for a couple of years since this is the best time they have for learning. They still need to pick up so many things. But they are free to make the decision – they already have an offer from TIFR [Tata Institute of Fundamental Research].

Anhang

Wie versprochen folgt jetzt eine Beweisskizze für den Satz von Agrawal-Kayal-Saxena. Ich folge dabei der geglätteten Präsentation durch Dan Bernstein in [2].

Beweisskizze. Man nimmt einen Primteiler p von n, für den bereits $p^{(r-1)/q} \not\equiv 0, 1 \mod r$ ist, und zeigt, dass falls (i) und (ii) für alle $1 \leq a < s$ gilt, die Zahl n eine Potenz von p ist.

Hierzu betrachtet man – wie Agrawal an jenem Morgen des 10. Juli, als der Satz gefunden wurde – Produkte der Form $t = n^i p^j$ mit $0 \leq i, j \leq \lfloor \sqrt{r} \rfloor$. Nach dem Schubfachprinzip gibt es zwei verschiedene Paare (i_1, j_1) und (i_2, j_2) solcher Exponenten, für die $t_1 = n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} = t_2 \mod r$ gilt. Ziel ist nun der Nachweis, dass tatsächlich $t_1 = t_2$ gelten muss, was $n = p^\ell$ für ein gewisses ℓ nach sich zieht.

Aus (ii) folgt mit Hilfe des kleinen Fermat'schen Satzes für alle $1 \leq a \leq p$ und $\mu = 1, 2$

$$(x - a)^{t_\mu} \equiv x^{t_\mu} - a \mod (x^r - 1, p). \qquad (*)$$

Solche Exponenten t_μ hatten Kayal und Saxena in ihrer Bachelor-Arbeit „introspektive“ Zahlen genannt und für diese gezeigt, dass sich die Kongruenz $t_1 \equiv t_2 \mod r$ zu einer Kongruenz $t_1 \equiv t_2 \mod \#G$ mit $\#G \gg r$ liften läßt. Durch geeignete Wahl der Parameter wird $\#G$ so groß, dass $t_1 = t_2$ folgt. Das Lifting ist Agrawal zufolge „the nicest part of the paper.“

Wie liftet man? Wegen $t_1 \equiv t_2 \mod r$ teilt $x^r - 1$ die Differenz $x^{t_1} - x^{t_2}$, so dass aus (*) schließlich folgt

$$(x - a)^{t_1} \equiv (x - a)^{t_2} \mod (x^r - 1, p).$$

Also ist $g^{t_1} = g^{t_2}$ für alle $g \in G$; dabei bezeichnet G die aus den Linearfaktoren $(\zeta_r - a)$ erzeugte multiplikative Untergruppe des durch Adjunktion der $r$ten Einheitswurzel ζ_r erzeugten Kreisteilungskörpers über $\mathbb{Z}/p\mathbb{Z}$. Nimmt man nun ein primitives Element g, d. h. eines der Ordnung $\#G$, so folgt $\#G \mid (t_1 - t_2)$.

Wegen (i) und da $p^{(r-1)/q} \not\equiv 0, 1 \mod n$ gilt, besitzt andererseits die Gruppe G – nach etwas Kombinatorik und elementarer Theorie von Kreisteilungspolynomen – wenigstens $\binom{q+s-1}{s}$ Elemente. Also ist nach Voraussetzung an den Binomialkoeffizienten

$$|t_1 - t_2| < n^{\lfloor \sqrt{r} \rfloor} p^{\lfloor \sqrt{r} \rfloor} \leq n^{2\lfloor \sqrt{r} \rfloor} \leq \binom{q + s - 1}{s} \leq \#G$$

und daher wie gewünscht $t_1 = t_2$.

Danksagung

Mein herzlicher Dank gilt Manindra Agrawal für die Bereitwilligkeit, mit der er trotz tausender Gratulationen per E-Mail meine Fragen nach Hintergrundinformationen sehr persönlich und ausführlich beantwortete.

Literatur

[1] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, *PRIMES is in P*, IIT Kanpur, Preprint vom 6. 8. 2002, `www.cse.iitk.ac.in/news/primality.html`.

[2] Daniel Bernstein, *An Exposition of the Agrawal-Kayal-Saxena Primality-Proving Theorem*, 2. Fassung vom 20. 8. 2002, `cr.yp.to/papers.html#aks`.

[3] Manindra Agrawal, Somenath Biswas, *Primality and identity testing via chinese remaindering*, in *Proceedings of the Anual IEEE Symposium on Foundations of Computer Science*, pp. 202–209, 1999.

[4] Rajat Bhattacharjee, Prashant Pandey, *Primality Testing*, Bachelor of Technology Project Report, IIT Kanpur 2001, `www.cse.iitk.ac.in/research/btp-reports.html`.

[5] Neeraj Kayal, Nitin Saxena, *Towards a Deterministic Polynomial-Time Primality Test*, Bachelor of Technology Project Report, IIT Kanpur, April 2002, `www.cse.iitk.ac.in/research/btp-reports.html`.

[6] D. Roger Heath-Brown, *The First Case of Fermat's Last Theorem*, Math. Intelligencer 7(4), pp. 40–47&55, 1985.

[7] Morris Goldfeld, *On the number of primes p for which $p + a$ has a large prime factor*, Mathematika 16, pp. 23–27, 1969.

[8] Étienne Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, Invent. Math. 79, 383–407, 1985.

[9] Roger C. Baker, Glyn Harman, *The Brun-Titchmarsh Theorem on Average*, in *Proceedings of a conference in honor of Heini Halberstam, Vol. 1*, pp. 39–103, 1996.

[10] R. Ramachandran, *A prime solution*, Frontline, India's National Magazine, Vol. 19, Heft 17 vom 17. 8. 2002, `www.flonnet/com/fl1917/19171290.htm`.

[11] Sara Robinson, *New Method Said to Solve Key Problem in Math*, New York Times vom 8. 8. 2002.

[12] gsz., *Methode zur Zertifizierung von Primzahlen*, Neue Züricher Zeitung vom 30.8.2002.

[13] Dietmar Dath, *Polynomiale Götter: Findige Inder und ihre Primzahlen*, FAZ vom 9. 8. 2002.

Adresse des Autors
Prof. Dr. Folkmar Bornemann
Zentrum Mathematik
Technische Universität München
85747 Garching bei München
`bornemann@ma.tum.de`