

## Computeralgebra in Lehre, Ausbildung und Weiterbildung IV: 13.-16.04.2004, Kloster Schöntal

Wir möchten an dieser Stelle bereits auf unsere Tagung *Computeralgebra in Lehre, Ausbildung und Weiterbildung IV* hinweisen, die 2004, wieder in der Woche nach Ostern, im Kloster Schöntal stattfinden wird. Rechts sehen Sie ein Foto von einem Vortrag bei der Schöntal-Tagung im vergangenen Jahr. Weitere Informationen, auch zu den vorangegangenen Tagungen, finden Sie auf der Internetseite <http://www.fachgruppe-computeralgebra.de/CLAW>.



---

## Themen und Anwendungen der Computeralgebra

---

Der folgende Artikel ist unter gleichem Titel in den *Mitteilungen der Deutschen Mathematiker-Vereinigung*, Heft 4-2002, 14–21 erschienen. Wir bedanken uns für die Erlaubnis, ihn hier in einer gekürzten und aktualisierten Fassung abdrucken zu dürfen.

### Ein Durchbruch für „Jedermann“

Folkmar Bornemann

#### Zusammenfassung

„New Method Said to Solve Key Problem in Math“ titelte die *New York Times* am 8. August 2002 und meinte den Nachweis von  $\text{PRIMES} \in \mathcal{P}$ , 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 „ $\text{PRIMES}$  is in  $\mathcal{P}$ “ verschickt. Montag früh befand Carl Pomerance das Resultat für korrekt, organisierte in seiner Begeisterung für den Nachmittag ein spontanes Seminar und informierte die *New York Times*. Dienstag wurde der Preprint im Internet frei zugänglich [1]. Donnerstag beendete 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.

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?

Als Numeriker kein algorithmischer Zahlentheoretiker, außerhalb meiner Sinne solch ein „Jedermann“, wollte ich die Probe aufs Exempel machen.

## Das Problem

Erfreulicherweise motivieren die Drei ihre Arbeit nicht mit der Bedeutung von Primzahlen für die Kryptographie, 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 Maserischen Übersetzung von 1889:

Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren 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 Hilfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommen.

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, wobei die Eingabelänge der Zahl proportional zur Anzahl der Dualstellen, also in etwa  $\log_2 n$  ist. Gibt es also einen deterministischen Algorithmus, der mit einem festen Exponenten  $\kappa$  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

$$a^n \equiv a \pmod{n}.$$

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

Beim *deterministischen* Algorithmus von Adleman, Pomerance und Rumely aus dem Jahre 1983 wird sehr viel mehr Theorie betrieben und der kleine Fermatsche 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.

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  $\text{PRIMES} \in \mathcal{ZPP}$ .

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.



Manindra Agrawal

## Auftritt Manindra Agrawal

Der Informatiker und Komplexitätstheoretiker Manindra Agrawal erwarb 1991 seinen Dokortitel 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 vor zwei Jahren auf sich aufmerksam gemacht, als er eine abgeschwächte Form der Isomorphie-Vermutung der Komplexitätstheorie bewies.<sup>2</sup>

Um 1999 arbeitete er mit seinem Doktorvater Somnath 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“ ein neuer probabilistischer Primalitätstest.

Ausgangspunkt war dabei eine Verallgemeinerung des kleinen Fermatschen 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

$$(x - a)^n \equiv (x^n - a) \pmod{n}.$$

Eine sehr elegante Charakterisierung von Primzahlen, aber zunächst keine 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 Primzahlcharakterisierung, 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 im letzten 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 Kussband 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<sup>3</sup>

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

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  $a = 1$  und untersuchten die nötigen  $r$ . Durch Auswertung von Experimenten mit  $r \leq 100$  und  $n \leq 10^{10}$  gelangten sie zu folgender Vermutung. Falls  $r$  und  $n$  teilerfremd sind und

$$(x - 1)^n \equiv x^n - 1 \pmod{(x^r - 1, n)} \quad (T_{r,1})$$

<sup>2</sup>Die Isomorphie-Vermutung von Berman und Hartmanis impliziert  $\mathcal{P} \neq \mathcal{NP}$ .

<sup>3</sup>Ich folge der Notation von Agrawal et al. und bezeichne mit  $p(x) \equiv q(x) \pmod{(x^r - 1, n)}$  die Gleichheit der Reste der Polynome  $p(x)$  und  $q(x)$  nach Division durch  $x^r - 1$  und Division der Koeffizienten durch  $n$ .

gilt, ist entweder  $n$  prim oder es gilt  $n^2 \equiv 1 \pmod{r}$ . 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.



Neeraj Kayal



Nitin Saxena

Nun traten die bislang fehlenden Helden unserer Geschichte auf, die Studenten Neeraj Kayal und Nitin Saxena. Beide waren Mitglieder der indischen 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 Primalitystest-Primitiven und 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 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 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  $s \leq n$  so gewählt, dass  $q \mid r - 1$ ,

$n^{(r-1)/q} \not\equiv 0, 1 \pmod{r}$  und

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

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

Der einfache, kurze und ideenreiche Beweis des Satzes bereitet soviel Vergnügen, dass er jedem Leser zur Lektüre ans Herz gelegt sei.

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

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  $a = 1, \dots, s - 1$  tue jeweils folgendes:
  - (i) Ist  $a$  Teiler von  $n$ , gehe zu Schritt 5.
  - (ii) Ist  $(x - a)^n \not\equiv x^n - a \pmod{(x^r - 1, n)}$ , 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  $\tilde{O}(sr \log^2 n)$ , 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 Schrittes 2. Schauen wir uns zunächst an, was prinzipiell möglich ist. Wählt man  $s = \theta q$  mit einem festen Faktor  $\theta$ , so liefert die Stirlingsche Formel die Asymptotik

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

Die Bedingungen des Satzes erfordern 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  $q \geq r^{1/2+\delta}$  besitzt. Dabei handelt es sich um ein gut studiertes Problem der analytischen Zahlentheorie.

## Sophie Germain und die Fermatsche 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 Fermatschen 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

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

wobei  $C_2 = 0,6601618158\dots$  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 Fermatschen 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 [3]. 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.

## Eine Fields-Medaille

Präzise verlangten sie, dass die Abschätzung

$$\#\{r \leq x \mid q, r \text{ prim}; q \mid r - 1; q \geq x^{1/2+\delta}\} \geq c_\delta \frac{x}{\ln x}$$

einen zulässigen Exponenten  $\delta > 1/6$  besitzt. Die Jagd nach dem größten  $\delta$  hatte 1969 mit Morris Goldfeld [4] begonnen, der  $\delta \approx 1/12$  erhalten hatte. Étienne Fouvry [5] 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 Fermatschen 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  $\delta$  – 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 [6] 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  $\delta$  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,

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

Der AKS-Algorithmus hat damit insgesamt eine garantierte Laufzeit von  $\tilde{O}(\log^{3+3/2\delta} n)$ . Damit ist die Aussage  $\text{PRIMES} \in \mathcal{P}$  bewiesen, der Durchbruch gelungen.<sup>4</sup> Gratulation! Fouvrys korrigierter Wert für  $\delta$  liefert  $\tilde{O}(\log^{11,913} n)$ , oder einfacher zu merken und dann auch ohne Tilde:  $O(\log^{12} n)$ .

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

<sup>4</sup>Am 22. Januar 2003 stellte Dan Bernstein eine Version seines Papiers [2] ins Netz, die eine leichte Variation des Satzes von Agrawal-Kayal-Saxena enthält und es erlaubt, ganz ohne tiefliegende analytische Zahlentheorie auszukommen. Nach Anwendung eines Satzes von Tschebyscheff (das Produkt der Primzahlen  $\leq 2k$  ist mindestens  $2^k$ ) ergibt sich nämlich, dass der Algorithmus mit  $r, s = O(\log^5 n)$  funktioniert. Somit ist heute der Nachweis von  $\text{PRIMES} \in \mathcal{P}$  vollständig elementar und bis ins letzte für „Jedermann“ nachvollziehbar. Diese Variation wurde Bernstein bereits am 14. August 2002 von ihrem Erfinder Hendrik Lenstra mitgeteilt. Vielleicht hat Paulo Ribenboim ja recht, wenn er mir schreibt: „Our specialists should reflect about their convoluted reasoning.“

die höchsten Auszeichnungen in der Mathematik nominiert.<sup>5</sup> 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 der Kryptographie. 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 derzeit 5020 Dezimalstellen<sup>6</sup> 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  $n \rightarrow \infty$  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-Tests in Bruchteilen einer Sekunde erzeugt. Bei Bedarf kann in wenigen Sekunden mit dem auf elliptischen Kurven basierenden ECPP-Verfahren nach Atkin-Morain ihre Primalität tatsächlich *bewiesen* werden.<sup>7</sup> 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 etwa ein paar Tage arbeiten müsste.<sup>8</sup> Dabei ist diese Konstante dank Dan Bernstein, Hendrik Lenstra, Felipe Voloch, Bjorn Poonen und Jeff Vaaler bereits gegenüber der ursprünglichen Formulierung des Algorithmus um wenigstens den Faktor  $2 \cdot 10^6$  verbessert worden – Stand vom 25. Januar 2003, vgl. [2].

Es fehlt also noch etwa ein Faktor  $10^5$  zur Konkurrenzfähigkeit. Auch das ECPP-Verfahren startete mit ei-

ner 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.

## 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].

## 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](http://www.cse.iitk.ac.in/news/\\primality.html).
- [2] Daniel Bernstein, *Proving Primality after Agrawal-Kayal-Saxena*, Fassung vom 25. 1. 2003, [cr.yp.to/papers.html#aks](http://cr.yp.to/papers.html#aks).
- [3] D. Roger Heath-Brown, *The First Case of Fermat’s Last Theorem*, *Math. Intelligencer* 7(4), pp. 40–47&55, 1985.

<sup>5</sup>Am 30. Oktober 2002 wurde ihm bereits der *Clay Research Award* verliehen. Bisherige Preisträger waren Andrew Wiles, die Stochastiker Smirnov und Schramm und die Träger der Fields-Medaille Connes, Lafforgue und Witten.

<sup>6</sup>Bitte nicht mit der Rekordjagd nach der *größten* bekannten Primzahl verwechseln, zur Zeit  $2^{13\,466\,917} - 1$ , eine Mersennesche Primzahl mit 4 053 946 Dezimalstellen. Diese Zahlen sind voller Struktur und lassen hochspezialisierte Algorithmen ans Werk.

<sup>7</sup>Z. B. mit dem unter <http://www.znz.freesurf.fr/pages/primos.html> frei verfügbaren Programm PRIMO von Marcel Martin, das derzeit den Rekord hält.

<sup>8</sup>Ein entsprechendes Experiment dürfte in den nächsten Monaten sicherlich erfolgen.

- [4] Morris Goldfeld, *On the number of primes  $p$  for which  $p + a$  has a large prime factor*, *Mathematika* 16, pp. 23–27, 1969.
- [5] Étienne Fouvry, *Théorème de Brun-Titchmarsh; application au théorème de Fermat*, *Invent. Math.* 79, 383–407, 1985.
- [6] 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.

Stark gekürzte und aktualisierte Fassung des Beitrags gleichen Titels in den *Mitteilungen der Deutschen Mathematiker-Vereinigung*, Heft 4-2002, 14–21.

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

## Polynomielle Gleichungen mit Massenwirkungskinetik

Karin Gatermann

Bei der Modellierung von chemischen Reaktionssystemen treten spezielle dünnbesetzte polynomielle Gleichungssysteme auf, die wir mit Methoden der Computeralgebra, algebraischen Geometrie und der diskreten Mathematik untersuchen. Ziel ist es, die Struktur der Gleichungen und ihre Konsequenzen so genau wie möglich zu verstehen.

Das zeitliche (bzw. raumzeitliche) Verhalten der Konzentrationen  $x_i$  von Chemikalien während einer Reaktion wird durch eine gewöhnliche Differentialgleichung (bzw. partielle Differentialgleichung) beschrieben. Das Standardmodell ist die sogenannte *Massenwirkungskinetik*, wodurch eine polynomielle Differentialgleichung

$$\dot{x} = Y_s I_a I_K \Psi(x), \quad \Psi_j(x) = x^{y_j}, j = 1, \dots, n$$

entsteht. Dabei sind die Matrizen  $Y_s$  und  $I_a$  durch die Struktur der Reaktionen (Stöchiometrie) gegeben, während die Matrix  $I_K$  die Reaktionsgeschwindigkeiten  $k_{ij}$  als Parameter enthält, von denen oft nur die Größenordnung bekannt ist. Die Exponenten der auftretenden Monome sind im Wesentlichen Spalten der Matrix  $Y_s$ . Zusätzliche Bedingungen wie z. B. die Massenerhaltung werden durch lineare Gleichungen  $v_i^t x - c_i = 0$  berücksichtigt. Die Hauptfrage, zu deren Antwort die Computeralgebra einen Beitrag leistet, ist die Frage nach positiven stationären Lösungen und deren Abhängigkeit von den Parametern. Diese Frage fällt folglich in das Gebiet der reellen algebraischen Geometrie.

Für Anwender ist die Analyse der Gleichungsstruktur von großer Bedeutung, da diese Struktur die Struktur der Lösungen impliziert. Insbesondere interessiert die Abhängigkeit von den Parametern. So können bei der Modellierung von chemischen Prozessen schon sehr früh Modelle verworfen werden (Modelldiskriminierung). Das ist der erste Schritt zum Verständnis des dynamischen Verhaltens. Insbesondere ist das Auftreten

mehrerer reeller positiver Lösungen die Grundlage für die Existenz von Reaktions-Diffusions-Wellen. Außerdem ist es die Voraussetzung für die Anwendung der singulären Störungstheorie.

Über die stationären Lösungen der Differentialgleichungen, ihre Stabilität und Hopf-Verzweigung gibt es eine reichhaltige nicht-algebraische Literatur [1,3,4,5]. Sehr bekannt sind zum Beispiel das deficiency-zero-Theorem und das deficiency-one-Theorem von Feinberg [4,5]. Wie wir in [6] gezeigt haben, beruht das deficiency-one-Theorem darauf, dass eine homogene torische Varietät einen eindeutigen Schnitt mit einem Kegel hat (siehe Abbildung 1).

Um dies zu verstehen, ist die torische Geometrie, sind also die torischen Ideale und ihre zugehörigen Varietäten entscheidend.

Im Gegensatz zur recht abstrakten Theorie betrachten wir Varietäten, die der Theoretiker als konkrete Einbettungen bezeichnet. Gegeben Polynome mit auftretenden Monomen  $x^{y_1}, \dots, x^{y_n}$  und Matrix der Exponenten, so bezeichnet man

$$I_{\hat{Y}} = \{f \in \mathbb{C}[z] \mid f(x_0 x^{y_1}, \dots, x_0 x^{y_n}) = 0, \forall x, x_0\}$$

als homogenes torisches Ideal. Die Monome parametrisieren die zugehörige torische Varietät. In Singular und anderen CA-Systemen gibt es Implementationen effizienter Spezialalgorithmen für die Berechnung von Gröbnerbasen solcher torischen Ideale. Eine einfache und fundamentale Idee der algebraischen Geometrie ist, die Lösung des ursprünglichen Gleichungssystems auf die Lösung eines linearen, eines binomiellen und eines monomiellen Gleichungssystems zurückzuführen.

Ein wichtiges Ergebnis der torischen Geometrie betrifft die Anzahl der komplexen Lösungen von dünnbesetzten Gleichungssystemen. Diese sogenannte BKK-Anzahl kann man entweder durch eine gemischte Unterteilung der Newton-Polytope ausrechnen [2] oder