PRIMZAHLEN SIND DER WAHNSINN

WOLFGANG WILLEMS

Unter dieser Überschrift titelte Agnieszka Lehmann 2006 ihre Rezension über den Film *Der Beweis - Liebe zwischen Genie und Wahnsinn*, in dem Gwyneth Paltrow die Tochter eines an Demenz leidenden Mathematikprofessors spielt, der ein Problem über Primzahlen zu lösen versucht. Ein Jahr später erschien der spanische Film *La habitation de Fermat*. In ihm behauptet ein Mathematiker, er habe die berühmte Vermutung von Goldbach, einem preußischen Mathematiker, der zu Beginn des 18ten Jahrhunderts lebte, bewiesen. Die Primzahlen haben also nicht nur Mathematiker in ihren Bann gezogen, sondern auch Filmkünstler und viele andere.

Was aber steckt hinter diesen Zahlen, die offenbar eine ungewöhnliche Faszination ausüben?

Primzahlen sind natürliche Zahlen, die nur durch 1 und sich selbst teilbar sind, wobei wir die 1 aus gewissen Gründen nicht als Primzahl zählen. Die kleinsten aufeinander folgenden Primzahlen sind also

$$2, 3, 5, 7, 11, 13, ...$$

Sie sind sozusagen die Bausteine, aus denen alle Zahlen aufgebaut sind, denn jede Zahl ist ein Produkt von Primzahlen, etwa

$$60 = 2 \times 2 \times 3 \times 5.$$

Schon der Grieche Euklid, der vor etwa 2300 Jahren in Alexandria lebte, wusste, dass es unendlich viele Primzahlen gibt. Wie man sie findet, hat uns Eratosthenes von Kyrene wenige Jahrzehnte nach dem Tod von Euklid verraten. Sein Verfahren wird heute als das *Sieb des Eratosthenes* bezeichnet und funktioniert sehr einfach. Will man alle Primzahlen bis zu einer gewissen Zahl n, etwa n=15 finden, so schreibt man alle Zahlen zwischen 2 und 15 auf.

$$2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15$$

Nun streicht man alle Vielfachen der 2, außer der 2 selbst.

$$2\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ 9\ 1\cancel{0}\ 11\ 1\cancel{2}\ 13\ 1\cancel{4}\ 15$$

Danach alle Vielfachen der ersten verbleibenden Zahl nach 2, also 3, außer der 3 selbst.

$$2\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}$$

Die nicht gestrichenen Zahlen sind nun bereits alle Primzahlen bis 15, da man nur die Vielfachen derjenigen Primzahlen streichen muss, deren Quadrat kleiner oder gleich n ist. Die Vielfachen der 5 muss man also nicht mehr streichen, da $5 \times 5 = 25$ größer als 15 ist.

Was aber macht sie so interessant?

Die Antwort ist einfach: *Wir verstehen sie nicht.* Ihr Auftreten scheint vollkommen wirr zu sein; mal erscheinen sie dicht hintereinander, etwa 3 und 5 oder 5 und 7; mal gibt es große Lücken, etwa zwischen den Primzahlen 887 und 907 eine Lücke von 19 Zahlen, die alle keine Primzahlen sind. Diese Lücken können sogar beliebig groß werden.

Bernhard Riemann

Die Verteilung der Primzahlen hat Bernhard Riemann (1826-1866) in der nach ihm benannten *Riemannschen Hypothese* beschrieben. Es ist eine Aussage über die Nullstellen der sog. Zetafunktion $\zeta(z)$, auf die wir hier nicht eingehen können. Es ist ein äußerst schwieriges Problem, da $\zeta(z)$ sehr kompliziert ist, und so gibt es bis heute auch keinen Beweis dafür. Es ist nur eine Vermutung. Was die Mathematiker nun extrem herausfordert, ist die Tatsache, dass viele Sätze in der Mathematik beginnen:

Wenn die Riemannsche Hypothese gilt, so gilt auch ...

Aber die Hypothese ist nur eine Vermutung, man weiß nicht, ob sie stimmt, auch wenn vieles für ihre Richtigkeit spricht. Man ist also sehr an einem Beweis interessiert, und das Clay Institut in Boston hat dafür ein Preisgeld von einer Million US-Dollar ausgesetzt.

Im Zusammenhang mit Primzahlen gibt es aber auch sehr viele einfache interessante Fragestellungen, die bis heute trotz großer Anstrengungen nicht beantwortet werden konnten, etwa:

1. *Gibt es unendlich viele Primzahlen p, für die auch $p + 2$ eine Primzahl ist?*

Beispiele dafür sind 3 und 5 oder 11 und 13. Sie heißen Primzahlzwillinge.

2. *Ist jede durch* 2 *teilbare Zahl, die größer oder gleich* 4 *ist, die Summe von zwei Primzahlen?*
Dies ist die zu Anfang erwähnte Vermutung von Goldbach. Etwa:
$4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5, 10 = 5 + 5$, $12 = 5 + 7, ...$

3. *Gibt es nur endlich viele Primzahlen der Form* $2^k + 1$, *also* k*-mal die* 2 *mit sich selbst multipliziert und* 1 *addiert?*
Wir kennen nur fünf:
$3 = 2^1 + 1$, $5 = 2^2 + 1$, $17 = 2^3 + 1$, $257 = 2^4 + 1$ und $65537 = 2^5 + 1$.
Diese Primzahlen heißen nach dem französischen Mathematiker Pierre de Fermat (1601-1665) Fermatsche Primzahlen.

Briefmarke PIERRE DE FERMAT

Er formulierte auch den *großen Fermatschen Satz*, der besagt, dass die Gleichung $x^n + y^n = z^n$ für $n > 2$ keine ganzzahligen Lösungen x, y, z hat.

Diese Aussage konnten die Mathematiker erst Mitte der 90ziger Jahre des letzten Jahrhunderts beweisen, also 350 Jahre nach der Entdeckung von Fermat.

4. *Wie viele Primzahlen der Form* $2^k - 1$ *gibt es?*

MARIN MERSENNE

Sie werden nach dem französischen Theologen und Mathematiker Marin Mersenne (1588-1648) auch Mersennesche Primzahlen genannt. Bekannt sind bis heute nur 47 von diesen. Die größte ist $2^{43112609} - 1$ und hat 12987189 Dezimalstellen. Sie ist z.Zt. die größte bekannte Primzahl und wurde 2008 entdeckt. Man kann sie in Bruchteilen einer Sekunde auf einem PC berechnen und ein Aufschreiben würde ein Buch mit mehr als 3000 Seiten füllen.

Was aber haben Primzahlen mit dem wirklichen Leben zu tun?

Godfrey Hardy (1877-1947), ein bedeutender Mathematiker, der sich speziell mit Zahlen beschäftigte, antwortete darauf : *Nichts, es ist Reine Mathematik, es ist einfach nur schön, es ist zu nichts nutze.* Er hatte zu seinen Lebzeiten sicher recht mit dieser Behauptung, aber seit seinem Tod sind mehr als 60 Jahre vergangen, und vieles hat sich im Computer-Zeitalter geändert.

Bei Überweisungen per Homebanking oder Surfen im Internet findet man oft auf dem Bildschirm den Hinweis *RSA verschlüsselt.* Dabei steht **RSA** für die drei Mathematiker Ronald **R**ivest, Adi **S**hamir und Leonard **A**dleman, die 1978 im amerikanischen Princeton, einer Hochburg der Mathematik, die nach ihnen benannte RSA-Verschlüsselung gefunden haben.


A. Shamir, R. Rivest, L. Adleman (von links)

Verschlüsseln bedeutet, dass man aus einem lesbaren Text einen Buchstabensalat, also einen nicht verständlichen Text macht. So können Nachrichten gegen unerlaubtes Lesen oder Verändern im Internet geschützt werden.

Das RSA-Verfahren lässt sich einfach beschreiben. Jeder Teilnehmer des Kommunikationsnetzes, so auch Bob, gibt unter seinem Namen eine Zahl n und eine weitere vorsichtig zu wählende Zahl e etwa in einem Buch, ähnlich dem Telefonbuch, öffentlich bekannt. Dabei ist n das Produkt aus zwei sehr großen Primzahlen, etwa p und q, die Bob allerdings streng geheim hält. Will Alice an Bob eine Nachricht senden, so schreibt sie diese als eine Folge von Zahlen x, die alle kleiner als n sind (Alice kennt n aus dem Eintrag von Bob im Telefonbuch.) Statt der Zahlen x, also der eigentlichen Nachricht, sendet sie Zahlen y, die sie als Reste der Division von x^e durch n erhält. (Man beachte, dass Alice aus dem Telefonbuch auch e kennt.) Bob kann dann aus den Zahlen y wegen der Kenntnis der beiden Primzahlen p und q die Zahlen x, also die eigentliche Nachricht, wiedergewinnen.

Wie aber findet man große Primzahlen, oder anders gefragt, wie kann man herausfinden, ob eine gegebene Zahl eine Primzahl ist?

Man denkt hier sofort an das Sieb des Eratosthenes. Leider führt es nicht zum Ziel, wenn die Primzahl sehr groß sein soll, da selbst Supercomputer für das viele Streichen zu lange brauchen. Selbst der 2004 von den drei Indern **A**grawal, **K**ayal und **S**axena gefundene **AKS**-Algorithmus, der nach seiner Entdeckung enormes Aufsehen erregte und in der *New York Times* in großer Aufmachung erschien, kommt zu keinem Ergebnis. Hier behelfen sich die Mathematiker mit Verfahren, mit denen man zwar nicht exakt feststellen kann, ob eine gegebene große Zahl eine Primzahl ist, aber mit einer hohen Wahrscheinlichkeit. Dann ist sie wahrscheinlich auch eine Primzahl und man kann sie im RSA-Verfahren benutzen.

Zurück zum Problem der Datenverschlüsselung.

Warum kann man nicht doch verschlüsselte Daten, die an Bob gesendet werden, entschlüsseln?

Man müsste dann bei alleiniger Kenntnis von n irgendwie die beiden Primfaktoren p und q von n finden, die aber nur Bob kennt. Ein solches Auffinden der Faktoren nennt man Faktorisieren. Dies kann man aber nicht, wenn p und q sehr groß sind, d.h. wenn sie mehr als etwa 150 Dezimalstellen haben. Oder anders gesagt: Bis heute gibt es kein allgemeines Verfahren, dass in einer angemessenen Zeit bei allen zur Verfügung stehenden Rechner-Resourcen die Primfaktorzerlegung einer Zahl stets berechnen kann. Von 1991 bis 2007 hatte die Firma RSA Laboratories Preisgelder zur Faktorisierung ausgesetzt. Für die Größte mit 617 Dezimalstellen bot sie 200000 US-Dollar. Aber selbst

26062623684139844921529879266674432197085925380486406416164
78519185999962854206936145028393191451461868351219816480591988
2053057222974116478065095809832377336510711545759,

eine Zahl mit nur 170 Dezimalstellen konnte bis heute nicht faktorisiert werden.

Die Sache mit den Primzahlen ist also eine endlose Geschichte. Primzahlen sind eben *Wahnsinnszahlen.*

Mathematik ist u.a. die Kunst, Wesentliches zu erkennen, dieses zu strukturieren und aus den Strukturen dann Aussagen abzuleiten.

Otto-von-Guericke Universität Magdbeurg, Fakultät für Mathematik, Universitätsplatz 2, 39106 Magdeburg
E-mail address: willems@ovgu.de