RSA & Co. in der Schule

Moderne Kryptologie, alte Mathematik, raffinierte Protokolle

Neue Folge – Teil 4: Gibt es genügend Primzahlen für RSA?

von Helmut Witten und Ralph-Hardo Schulz

Falltüreigenschaften

Für die moderne, asymmetrische Kryptografie benötigt man sogenannte *Einwegfunktionen mit Falltür* (kurz: Falltürfunktionen; engl. *trapdoor one-way functions* bzw. *trapdoor functions*). Das sind Funktionen, die leicht berechnet werden können, deren Umkehrfunktion aber praktisch unmöglich zu bestimmen ist – es sei denn, man verfügt über gewisse zusätzliche Informationen, die nicht öffentlich zugänglich sind. Man kann dies durch einen Briefkasten veranschaulichen: Es ist einfach, einen Brief einzuwerfen, aber schwierig, ihn wieder herauszufischen – es sei denn, man hat den Schlüssel zum Briefkasten. Ein weiteres Beispiel ist ein Vorhängeschloss, das man leicht durch Zudrücken schließen kann, zum (unkomplizierten) Öffnen benötigt man aber ebenfalls einen Schlüssel (vgl. auch Kardel, 1984; siehe Bild 1).

Im Fall des asymmetrischen Kryptosystems RSA wird die Falltüreigenschaft mithilfe zweier sehr großer Primzahlen p und q konstruiert; diese müssen auf jeden Fall geheim gehalten werden – sonst ist das Kryptosystem „geknackt". Die Ver- und Entschlüsselung erfolgt mit modularem Potenzieren bezüglich des Moduls $n = p \cdot q$; dafür muss der Modul n veröffentlicht werden. Die Falltüreigenschaft erhält man bei RSA dadurch, dass das Multiplizieren sehr großer Zahlen einfach durchgeführt werden kann, die Umkehrung (das Faktorisieren) aber einen vielfach höheren Rechenaufwand erfordert. Wie mithilfe von zwei Primzahlen ein komplettes RSA-Kryptosystem konstruiert werden kann, haben wir bereits in Witten/Schulz 2006a und 2006b erklärt. Da es in dieser Folge nur um die Primzahlen für RSA gehen soll, wollen wir das an dieser Stelle nicht wiederholen. Eine gute Einführung in das RSA-Verfahren findet man z.B. unter http://www.matheprisma.de/Module/RSA/index.htm. (*Anmerkung:* Viele weitere Internetquellen und Unterrichtsmaterialien zum Thema *Kryptologie* im Allgemeinen und *RSA* im Besonderen sind im CryptoPortal für Lehrerinnen und Lehrer unter https://www.cryptoportal.org/ zusammengestellt; vgl. auch Esslinger/Koy, 2009, und Esslinger u.a., [10]2010).

http://en.wikipedia.org/wiki/File:Early_padlock.jpg

Bild 1: Vorhängeschloss am Petersdom in Rom – ein frühes Beispiel für die Falltüreigenschaft!

Ein aktuelles und beeindruckendes Beispiel für die Falltüreigenschaft ist die Zahl RSA-768 aus der inzwischen beendeten RSA-Challenge (siehe http://www.rsa.com/rsalabs/node.asp?id=2093 und http://www.heise.de/security/meldung/RSA-768-geknackt-899073.html). Zur Erinnerung: Dieser Wettbewerb wurde am 18. März 1991 gestartet; die Firma RSA-Security veröffentlichte eine Liste mit sogenannten Semiprimzahlen, d.h. zusammengesetzten Zahlen mit genau zwei Primfaktoren; eine vollständige Aufstellung dieser Zahlen mit dem aktuellen Status findet man z.B. unter http://en.wikipedia.org/wiki/RSA_Factoring_Challenge. Die kleinste dieser Zahlen, RSA-100 (eine Semiprimzahl mit 100 Dezimalstellen), wurde bereits am 1. April 1991 von dem bekannten Zahlentheoretiker Arjen K. Lenstra in die beiden Primfaktoren zerlegt, aber die meisten der größeren Zahlen aus dieser Liste sind immer noch nicht faktorisiert. (*Anmerkung:* Während die Bitlängen von RSA-Schlüsseln in der Regel Zweierpotenzen sind, wurden bei der RSA-Challenge auch Zahlen anderer Größenordnungen zur Verfügung gestellt.)

Dreizehn Wissenschaftler von der Universität Bonn und weiteren international bedeutenden Forschungseinrichtungen in Japan, Frankreich, USA, der Schweiz und den Niederlanden haben die Zahl RSA-768 (s.u.) am 12. Dezember 2009 in ihre beiden Primfaktoren zerlegt. Der Zusatz 768 bedeutet in diesem Fall, dass die Zahl eine Länge von 768 Bit bzw. 232 Dezimalstel-

Bild 2:
Carl Friedrich Gauß im Alter von 50 Jahren – Lithographie von Siegfried Detlev Bendixen (1828).

Quelle: LOG-IN-Archiv / Astronomische Nachrichten, 7. Band, 1829, Frontispiz

len besitzt. Das Team benötigte 2½ Jahre für die Zerlegung. Die Forscher nutzten ein Computernetzwerk; auf einem herkömmlichen PC hätte das Knacken dieses Schlüssels nach ihren Angaben rund 2000 Jahre gedauert (Kleinjung u.a., 2010).

Es folgt ein kleines PYTHON-Programm mit der Zahl RSA-768 und den beiden Primfaktoren p und q aus der zitierten Arbeit. Wenn man dieses Programm von dem PYTHON-Interpreter ausführen lässt, erhält man auch auf einem älteren PC im Bruchteil einer Sekunde die Ausgabe „True“, d.h. die Zerlegung ist tatsächlich korrekt. Nebenbei erlebt man auch, dass Zahlen mit 116 Dezimalstellen sehr schnell multipliziert werden können – ganz im Gegensatz zum Aufwand, der für die Faktorisierung dieses Produktes erforderlich war!

```
RSA768=123018668453011775513049495838496272077285356
959533479219732245215172640050726365751874520219978 6
469389956474942774063845925192557326303453731548268 5
079170261221429134616704292143116022212404792747377 9
408066535141959745985690214 3413

p=334780716989568987860441698482126908177047949837 13
768568912431388982883793878002287614711652531743087 7
37814467999489

q=367460436667995904282446337996279526322791581643 43
087642676032283815739666511279233373417143396810270 0
92798736308917

print p*q==RSA768
```

Der Rechenaufwand für die Zerlegung war zwar sehr hoch, dennoch gilt die RSA-Verschlüsselung mit 768 Bit langen Schlüsseln künftig als unsicher. Wenn man bedenkt, dass sowohl die Verarbeitungsgeschwindigkeit der Rechner als auch die Leistungsfähigkeit der Faktorisierungsalgorithmen ständig zunehmen, ist es vernünftig, immer einen gehörigen „Sicherheitsabstand“ bei den verwendeten Moduln einzuhalten, sie also eher zu groß als zu klein zu wählen.

Weil die Zahl RSA-512 vor rund einem Jahrzehnt zerlegt wurde, gehen die Forscher in der zitierten Arbeit davon aus, dass die Rechenleistung zum Bewältigen der noch nicht zerlegten Zahl RSA-1024 in rund zehn Jahren zur Verfügung stehen dürfte. Ihre Empfehlung lautet daher, alle RSA-Schlüssel mit 1024 Bit bis spätestens 2014 aus dem Verkehr zu ziehen. (*Anmerkung:* In der Praxis werden z.B. bei virtuellen privaten Netzen, den VPN, teilweise schon jetzt 4096-Bit-Schlüssel verwendet.)

Wenn man also ab 2014 möglichst 2048-Bit-Schlüssel verwenden soll, damit kein Brute-Force-Angriff infrage kommt, benötigt man Primzahlen mit einer Länge von 1024 Bit bzw. 308 oder 309 Dezimalstellen, da die beiden Primzahlen, aus denen der Modul n zusammengesetzt wird, aus Sicherheitsgründen etwa die gleiche Länge haben, aber auch nicht zu dicht beieinander liegen sollen.

Man weiß zwar schon seit dem Altertum, dass es unendlich viele Primzahlen gibt, die sind aber immer dünner gesät, je größer sie werden. Es stellt sich damit die Frage:

> Wie viele Primzahlen mit 1024 Bit gibt es ungefähr?

Die Antwort auf diese Frage erhält man in guter Näherung durch den *Gauß'schen Primzahlsatz*, den der 15-jährige Gauß im Jahr 1792 entdeckte. In diesem Beitrag geben wir einen Überblick über Forschungen und Ergebnisse zur Verteilung der Primzahlen, soweit sie für das RSA-Kryptosystem interessant sind.

Der Gauß'sche Primzahlsatz

Carl Friedrich Gauß (siehe Bild 2) wurde 1777 in Braunschweig geboren. Seine außergewöhnliche Begabung wurde schon früh erkannt, er galt als mathematisches Wunderkind (siehe auch S. 94 in diesem Heft). Im Alter von 14 Jahren bekam er eine Logarithmentafel geschenkt, in der ihn besonders die Tabelle der Primzahlen faszinierte.

Vor ihm hatten schon andere bedeutende Mathematiker versucht, Formeln zur Erzeugung möglichst vieler Primzahlen zu finden. Einer der erfolgreichsten war dabei der Mönch Marin Mersenne (1588–1648) mit den nach ihm benannten Zahlen. Auf Leonhard Euler (1707–1783) geht die Erkenntnis zurück, dass die Summe der Kehrwerte der Primzahlen gegen unendlich strebt (Aigner/Ziegler, 2008, S. 53 f.; Kramer, 2008, S. 218). Damit hatte er einen weiteren Beweis gefunden, dass es unendlich viele Primzahlen gibt – sonst müsste die Summe mit endlich vielen Summanden ja endlich sein. Darüber hinaus hatte Euler bewiesen, dass die Reihe mit den Kehrwerten aller Quadratzahlen erstaunlicherweise gegen $\pi^2/6$ konvergiert (Barthe, 2008, S. 85 f.). So konnte er zeigen, dass die Primzahlen „dichter“ in der Menge der natürlichen Zahlen liegen als die Quadratzahlen.

Euler war aber nicht zufrieden mit seinem Ergebnis; er schrieb im Jahr 1751: „Es gibt einige Geheimnisse, die der menschliche Geist niemals durchdringen wird. Wir brauchen nur einen Blick auf die Tabelle der Primzahlen zu werfen, und wir sollten erkennen, dass es dort weder Ordnung noch Regeln gibt“ (zitiert nach: du Sautoy, ^{2}2004, S. 63).

Gauß suchte und fand 1793 einen anderen Ansatz, indem er fragte, wie viele Primzahlen sich zwischen der Zahl 1 und einer beliebigen reellen Zahl x befinden (hierzu und zum Folgenden siehe z.B. Kramer, 2008, S. 218 ff.). Dazu führte er die sogenannte Primzahlfunktion $\pi(x)$ ein:

$\pi(x)$ ist die Anzahl aller Primzahlen kleiner oder gleich x.

Beispielsweise ist $\pi(10) = 4$ (die Primzahlen sind in diesem Fall 2, 3, 5, 7) und $\pi(11) = 5$ (siehe Bild 3). Eine Verwechslungsgefahr mit der Kreiszahl π besteht nicht, weil bei der Primzahlfunktion stets ein Argument angegeben werden muss.

Wenn der Definitionsbereich dieser Funktion immer weiter vergrößert wird, tritt der Treppencharakter in der grafischen Darstellung mehr und mehr in den Hintergrund (siehe Bild 4). Mithilfe der Logarithmentafel konnte Gauß – wenigstens näherungsweise – „Ordnung und Regeln“ erkennen, und zwar

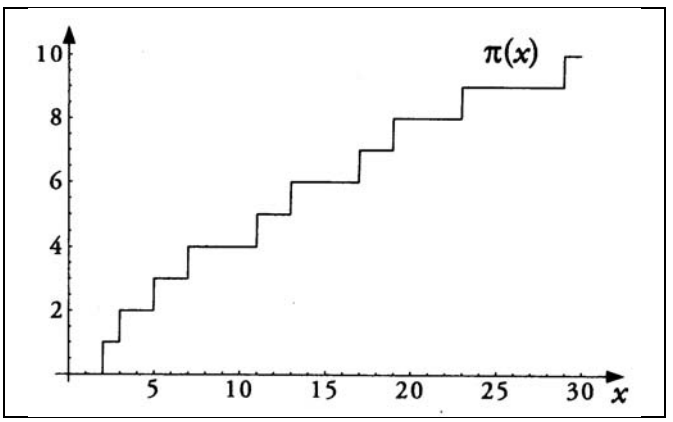
$\pi(x) \sim x/\ln x$

Das bedeutet, dass die Primzahlfunktion und die Funktion $x/\ln x$ für große Werte von x asymptotisch gleich sind; der Quotient beider Funktionen strebt für $x \to \infty$ gegen 1.

Dieser Zusammenhang wird heutzutage als Primzahlsatz (*Prime Number Theorem*) bezeichnet und wird allgemein als eines der erstaunlichsten Ergebnisse der Zahlentheorie angesehen, weil er zwei mathematische Gegenstände zusammenführt, die scheinbar nichts miteinander zu tun haben: Die Primzahlen, die immer natürliche Zahlen sein müssen, mit den Logarithmen, die für die reellen Zahlen u.a. eingeführt wurden, um die Multiplikation zweier reeller Zahlen auf die Addition ihrer Logarithmen zurückzuführen.

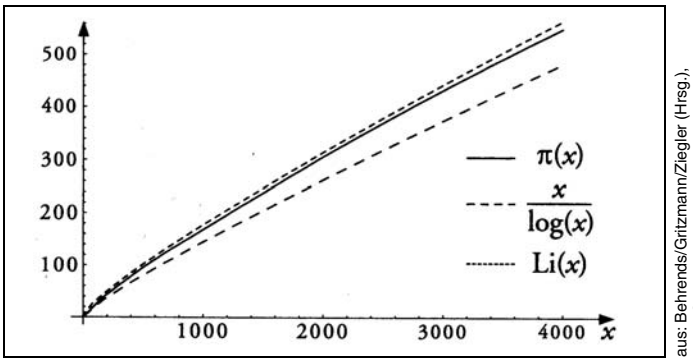
Wie konnte Gauß diese Beziehung zwischen der Verteilung der Primzahlen und dem Logarithmus finden? Er untersuchte den mittleren Abstand zwischen zwei Primzahlen und fand, dass er in der Nähe einer Zahl n ungefähr $\ln n$ beträgt. Das bedeutet, dass der mittlere Abstand zwischen zwei Primzahlen für sehr große n immer langsamer wächst. Eine andere Sichtweise interpretiert dieses Ergebnis stochastisch: Eine zufällig herausgegriffene Zahl in der Nähe von n ist mit der Wahrscheinlichkeit $1/\ln n$ eine Primzahl.

Mithilfe dieses Satzes können wir die Frage beantworten, wie viele Primzahlen mit 1024 Bit es ungefähr gibt. Der mittlere Abstand zwischen zwei Primzahlen



aus: Behrends/Gritzmann/Ziegler (Hrsg.), 2008, S. 219

Bild 3: Primzahlfunktion $\pi(x)$.



aus: Behrends/Gritzmann/Ziegler (Hrsg.), 2008, S. 219

Bild 4: Primzahlfunktion $\pi(x)$ im Intervall 1 bis 4000.

Anmerkung: In dieser Abbildung wird der natürliche Logarithmus mit $\log(x)$ bezeichnet.

in diesem Bereich der natürlichen Zahlen ist nach Gauß ca. $\ln 2^{1024} = 1024 \cdot \ln 2 \approx 709{,}8$. Mit anderen Worten: Hier ist im Mittel jede 710. Zahl eine Primzahl. Das erscheint zunächst nicht sehr viel, aber wir müssen dies ja in Beziehung zu der Größenordnung der betrachteten Zahlen setzen. Es gibt 2^{1023} Zahlen mit 1024 Bit (man denkt sich die erste Ziffer fest auf 1 gestellt, für jede der 1023 restlichen Ziffern gibt es die beiden Möglichkeiten 0 oder 1). Im Dezimalsystem ausgedrückt sind das ungefähr $8{,}99 \cdot 10^{307}$ Zahlen, geteilt durch 709,8 ergibt, dass ca. $1{,}266 \cdot 10^{305}$ Primzahlen mit 1024 Bit existieren.

Wie verlässlich ist dieser Zahlenwert? Gauß selbst war ein passionierter Rechner. In einem Brief aus dem Jahr 1849 schrieb er, dass es 216745 Primzahlen unterhalb von 3000000 gibt (der Wert ist allerdings nur fast richtig, in Wirklichkeit sind es 216826 Primzahlen unterhalb dieser Schranke; vgl.. Stein, 2009, S.15). Auf diese Weise konnte Gauß die Abweichung von $\pi(x)$ und $x/\ln x$ aber nur für (relativ) kleine x-Werte bestimmen.

Einen wichtigen Durchbruch erzielte im Jahr 1850 Pafnuti Lwowitsch Tschebyscheff, indem er zeigte, dass die Abweichung zwischen beiden Funktionswerten unabhängig von der Größe von x höchstens 11 Prozent betragen kann (Ribenboim, 2006, S.168). Diese Abschätzung wurde 1892 von James Joseph Sylvester auf 5 Prozent verbessert (Ribenboim, 2006, S.180). Die aktuell beste Abschätzung wurde im Jahr 1962 von John Barkley Rosser und Lowell Schoenfeld gefunden (gültig für $x \geq 11$; vgl. Ribenboim, 2006, S.180):

$$x/\ln x \leq \pi(x) \leq x/\ln x\ (1+3/(2\ln x)).$$

In unserem Fall erhält man damit die folgende exakte Abschätzung nach unten:

$$\pi(2^{1024}) - \pi(2^{1023}) \geq$$
$$2^{1024}/\ln 2^{1024} - 2^{1023}/\ln 2^{1023}\ (1+3/(2\ln 2^{1023})) \geq$$
$$2^{1023}/\ln 2\ (2/1024 - 1/1023\ (1 + 3/(2\cdot 1023 \ln 2)) \geq$$
$$1{,}262449 \cdot 10^{305}$$

Mit dem PYTHON-Interpreter berechnet man dieses Ergebnis mit

Fortsetzung übernächste Seite, oben

Bernhard Riemann und die Riemann'sche Vermutung

Bernhard Riemann wurde am 17. September 1826 in der Nähe von Dannenberg (Elbe) geboren; sein Vater war lutherischer Pfarrer. Riemann besuchte von 1840 bis 1842 ein Gymnasium in Hannover; nach dem Tod seiner Großmutter musste er an das Johanneum in Lüneburg wechseln. Dort erkannte der Direktor Schmalfuß seine mathematische Begabung. Da Riemann sehr schüchtern war und von seinen neuen Schulkameraden gehänselt wurde, durfte er in der Lehrerbibliothek arbeiten, wo ihm z.B. das Zahlentheoriebuch *Théorie des Nombres* von Legendre zur Verfügung stand. Schmalfuß erinnerte sich später in einem Brief an einen Freund: „Schon damals war er ein Mathematiker, neben dessen Fähigkeiten man sich als Lehrer armselig vorkam" (zitiert nach: du Sautoy, [2]2004, S. 82).

LOG-IN-Archiv

Bernhard Riemann, Fotografie aus dem Jahr 1863.

Riemann studierte in Göttingen und in Berlin. Gauß, der zu dieser Zeit schon alt war, erkannte seine herausragende mathematische Begabung und förderte ebenso wie Dirichlet seine Laufbahn. 1851 beendete Riemann seine Dissertation über ein Thema aus der Funktionentheorie und habilitierte sich 1854 in Göttingen mit einer Arbeit über Differentialgeometrie. 1857 erhielt er eine außerordentliche Professur, 1859 wurde er nach dem Tode Dirichlets dessen und damit auch Gauß' Nachfolger. Er starb leider sehr früh am 20. Juli 1866 im Alter von nur 39 Jahren an Tuberkulose in Selasca bei Verbania am Lago Maggiore, wo er auch begraben ist.

Trotz seines kurzen Lebens hat Riemann ein umfangreiches mathematisches Werk hinterlassen, u.a. eine Fundierung des Integralbegriffs (das Riemann'sche Integral) und Wegweisendes zur Funktionentheorie (Riemann'sche Flächen, Riemann'scher Abbildungssatz). Mit seinen Arbeiten zur Differentialgeometrie (Riemann'sche Geometrie) leistete er wichtige Vorarbeiten zu Einsteins allgemeiner Relativitätstheorie.

Zur Zahlentheorie hat Riemann nur eine einzige Arbeit veröffentlicht, nämlich den schon erwähnten kurzen Artikel über die Anzahl der Primzahlen unter einer gegebenen Größe, den er anlässlich seiner Aufnahme in die königlich-preußische Akademie der Wissenschaften eingereicht hatte. Die Riemann'sche Vermutung ist darin nur kurz erwähnt, gefolgt von der Bemerkung: „Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich habe indess die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien."

Es geht dabei um die Frage, ob die sogenannten nichttrivialen Nullstellen der Riemann'schen Zeta-Funktion, die durch

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

mit einer komplexen Variablen s mit Realteil größer 1 definiert ist (und durch eine geeignete Formel auf ganz $\mathbf{C}$ fortgesetzt werden kann), allesamt den gleichen Realteil ½ besitzen und damit alle auf der „kritischen Geraden" liegen, die parallel zur imaginären Achse durch $x = ½$ verläuft. Die „trivialen" Nullstellen sind dabei die negativen ganzen geraden Zahlen –2, –4, –6, …, die aber keineswegs einfach zu berechnen sind. Der Zusammenhang mit den Primzahlen ergibt sich aus der schon von Euler gefundenen Beziehung (gültig für s mit Realteil größer 1),

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prim}} \frac{1}{1 - \frac{1}{p^s}} = \frac{1}{(1 - \frac{1}{2^s})\,(1 - \frac{1}{3^s})\,(1 - \frac{1}{5^s})\,\ldots}$$

wobei Π_p ein unendliches Produkt über alle Primzahlen p darstellt. Der Ausdruck folgt aus dem Satz über die Eindeutigkeit der Primfaktorzerlegung und der Summationsformel für die geometrische Reihe (vgl. Kramer, 2008, S. 218).

Riemann selbst hat in seiner Arbeit eine explizite Formel für $\pi(x)$ angegeben, die eng mit den Nullstellen der Zeta-Funktion zusammenhängt. Bei der Untersuchung von Riemanns Nachlass durch den Mathematiker Carl Ludwig Siegel in den Dreißigerjahren des vorigen Jahrhunderts stellte sich heraus, dass Riemann umfängliche Berechnungen zur Bestimmung der ersten Nullstellen angestellt hatte.

Da die Riemann'sche Vermutung durch ein einziges Gegenbeispiel widerlegt werden könnte, wurden in der zweiten Hälfte des 20. Jahrhunderts Computer zur Nullstellenbestimmung eingesetzt, zuerst von Alan Turing im Jahr 1953. Turing berechnete auf diese Weise 1104 Nullstellen. Inzwischen sind die ersten 10^{13} Nullstellen berechnet worden, ohne dass sich der gesuchte Widerspruch gezeigt hat. Obwohl es sich bei allen Rechnungen um numerische Verfahren handelt, zeigen diese durch die verwendeten Algorithmen exakt und nicht nur annähernd, dass sich die untersuchten Nullstellen auf der kritischen Geraden befinden.

Der schwedische Mathematiker Helge von Koch, Informatiklehrerinnen und -lehrern bekannt durch die Kochkurve, zeigte im Jahr 1901, dass die Riemann'sche Vermutung äquivalent ist zu der Abschätzung

$$\pi(x) = \mathrm{Li}\,(x) + \mathcal{O}\,(\sqrt{x} \cdot \ln x)$$

und lieferte damit die bestmögliche Fehlerabschätzung für die stärkere Form des Gauß'schen Primzahlsatzes. (*Anmerkung:* Das Symbol $\mathcal{O}$ (Groß-Oh) ist eines der Landau-Symbole und steht für die Ordnung einer Funktion. Hier besagt es, dass der Fehler bei der Näherung von $\pi(x)$ durch das logarithmische Integral $\mathrm{Li}\,(x)$ höchstens von der Ordnung Wurzel x mal $\ln x$ ist, also nicht wesentlich schneller als diese Zahl wächst (vgl. http://de.wikipedia.org/wiki/Landau-Symbole).)

```
>>> from math import log
>>> (2**1023/log(2))*(2.0/1024 -
(1.0/1023)*(1.0 + 3.0/(2*1023*log(2))))
1.262449260590472e+305
```

Die Abweichung zu dem oben berechneten Wert liegt also im Promillebereich. (*Anmerkung:* Die Funktion log aus dem Modul math berechnet den natürlichen Logarithmus.)

Wenn man bedenkt, dass die Zahl aller Elementarteilchen unseres Universums auf weniger als 10^{80} geschätzt wird, ist es schon von der Physik her unmöglich, eine Liste dieser Zahlen zu speichern, abgesehen da-

1 Million Dollar für den Beweis der Riemann'schen Vermutung

„An einem heißen, schwülen Augustmorgen des Jahres 1900 hielt David Hilbert, damals Professor für Mathematik an der Universität von Göttingen, einen Vortrag an der Sorbonne in Paris." So beginnt das sehr lesenswerte Buch *Die Musik der Primzahlen – Auf den Spuren des größten Rätsels der Mathematik* von Marcus du Sautoy (^{2}2004). Hilbert legte in diesem Vortrag eine Liste von 23 ungelösten Problemen vor, die die mathematische Forschung des 20. Jahrhunderts nachhaltig beeinflussen sollten.

Viele dieser Probleme, wie der fehlende Beweis des großen Satzes von Fermat (Singh, 2000), sind inzwischen gelöst, oder es wurde deren Unlösbarkeit bewiesen. Für die spätere Entwicklung der Informatik war Hilberts zweites Problem bedeutsam: „Sind die arithmetischen Axiome widerspruchsfrei?" Nach einem der Unvollständigkeitssätze von Kurt Gödel kann diese Frage allein aus den Axiomen nicht beantwortet werden. Alan Turing kam bei dem Halteproblem von Automaten zu einem ähnlichen Ergebnis. In der praktischen Informatik lautet die Frage: Kann man ein Programm entwickeln, das als Eingabe den Quelltext eines zweiten Programms sowie dessen Eingabewerte erhält und das dann entscheiden kann, ob das zweite Programm terminiert, d.h. nicht endlos weiterläuft? Um dieses Problem zu lösen, entwickelte er das Konzept der später so genannten Turing-Maschine, das sich für die theoretische Fundierung der Informatik in den folgenden Jahrzehnten als sehr fruchtbar erweisen sollte. Alan Turing bewies 1936, dass es keine Turing-Maschine gibt, die das Halteproblem für alle Eingaben löst.

Das berühmteste, immer noch nicht gelöste Problem ist das achte auf Hilberts Liste: „Besitzen alle nichttrivialen Nullstellen der Riemann'schen Zeta-Funktion den Realteil ½?" Dies ist die kürzeste Formulierung der Riemann'schen Vermutung.

Zum hundertsten Jahrestag von Hilberts Vortrag stellte eine Gruppe von anerkannten Experten eine Liste von sieben ungelösten Milleniums-Problemen zusammen. Für jedes dieser Probleme lobte der amerikanische Multimillionär Landon T. Clay einen Preis von 1 Million Dollar aus und gründete das *Clay Mathematics Institute of Cambridge* (CMI), Massachusetts (http://www.claymath.org/), um die Preisvergabe zu organisieren und zu überwachen (Basieux, ^{2}2005).

Zu diesen sieben Milleniums-Problemen gehört die Riemann'sche Vermutung: http://www.claymath.org/millennium/Riemann_Hypothesis/. Unter dieser Adresse findet sich u.a. eine genauere Beschreibung des Problems durch Enrico Bombieri, der in dem oben erwähnten Buch von Marcus du Sautoy eine prominente Rolle spielt. Auch die Informatik hat es mit dem P=NP-Problem in die Liste des Clay-Instituts geschafft (http://www.claymath.org/millennium/P_vs_NP/), die Problemformulierung stammt in diesem Fall von dem Turing-Preisträger Stephen A. Cook, der in der theoretischen Informatik durch die Entwicklung des Konzepts der NP-Vollständigkeit berühmt wurde.

In einem Interview in der Zeitschrift *Spektrum der Wissenschaft* wurde Gerd Faltings, der Anfang der Achtzigerjahre des vorigen Jahrhunderts mit 28 Jahren durch seinen Beweis der Mordell'schen Vermutung bekannt wurde und heute Direktor am Max-Planck-Institut für Mathematik in Bonn ist, zu dem Preisgeld von 1 Million Dollar für die sieben Milleniums-Probleme befragt: „Wenn ich etwa die Riemann'sche Vermutung lösen könnte, dann wäre mir das Preisgeld aber egal. Eine Million Dollar haben viele, aber so etwas lösen, das können nur ganz wenige."

Eines der sieben Milleniums-Probleme, die Poincaré-Vermutung, wurde inzwischen von dem 1966 geborenen russischen Mathematiker Grigori Perelman gelöst. Er lehnte im Jahr 2006 die Annahme der Fields-Medaille für diese Leistung ab. Am 18. März 2010 wurde ihm das 1-Million-Dollar-Preisgeld der Clay-Stiftung zuerkannt, aber auch dieses lehnte er nach einer Meldung der russischen Nachrichtenagentur Interfax vom 1. Juli 2010 ab. Es sei bei der Ehrung für die Lösung der Poincaré-Vermutung ungerecht zugegangen. „Der Hauptgrund ist, kurz gesagt, meine Unzufriedenheit mit der Organisation der mathematischen Gesellschaft", wird er von Interfax zitiert. „Mir gefallen deren Entscheidungen nicht, ich halte sie für ungerecht", erklärte er weiter. So sei der Beitrag des US-Amerikaners Richard Hamilton zur Klärung der Poincaré-Vermutung „um kein bisschen geringer als meiner".

Foto: picture alliance/dpa/epa-Bildfunk

Grigori Perelman bewies die Poincaré-Vermutung und lehnte die Fields-Medaille und das 1-Million-Dollar-Preisgeld der Clay-Stiftung ab.

Seit einigen Jahren hat Perelman sich völlig aus der Öffentlichkeit zurückgezogen, lukrative Stellenangebote aus den USA konnten den arbeitslosen Mathematiker nicht locken; den zahlreichen Interview-Wünschen kam er bislang nicht nach. Nach der Einschätzung von Gerd Faltings ist Perelman ein seriöser Fachmann, dem offenbar der Medienrummel zuwider ist. Ein einfühlsames Feature zu Perelman wurde am 11. Mai 2008 vom Deutschlandfunk ausgestrahlt, das Sende-Manuskript findet sich unter http://www.dradio.de/dlf/sendungen/wib/779407/

von, dass die zur Erzeugung dieser Liste benötigte Rechenzeit alle menschlichen Maße übersteigen würde. Ganz sicher reichen diese Primzahlen für alle denkbaren Verschlüsselungen im Universum!

Später konnte Gauß die Näherung mithilfe des Integrallogarithmus $\mathrm{Li}(x)$ verbessern.

$$\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$$

(*Anmerkung:* $\mathrm{Li}(x)$ wird in der Integralform angegeben, weil das Integral nicht elementar berechnet werden kann.)

Auch hierfür gilt $\pi(x) \sim \mathrm{Li}(x)$. Im Bild 4, Seite 99, sind $\pi(x)$, $x/\ln x$ und $\mathrm{Li}(x)$ im Intervall 1 bis 4000 eingezeichnet. In diesem Maßstab kann man nicht mehr erkennen, dass es sich bei $\pi(x)$ um eine Treppenfunktion handelt.

Gauß selbst konnte diese asymptotischen Beziehungen nicht beweisen, das gelang erst 1896 unabhängig voneinander Jacques Hadamard (1865–1963) und Charles-Jean de La Vallée Poussin (1866–1962). Wichtige Vorarbeiten für diese Beweise stammen aus der berühmten Arbeit *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, die Bernhard Riemann im Jahr 1859 veröffentlichte. Mit dieser Arbeit begründete Rie-

Zum Weiterlesen

Die Geschichte vom Primzahlsatz und der Riemann'schen Vermutung wird ausführlich in dem unterhaltsamen populärwissenschaftlichen Buch von Marcus du Sautoy (^{2}2004) geschildert. Sehr lesenswert ist auch die Antrittsvorlesung von Don Zagier vom 5. Mai 1975 an der Universität Bonn zu dem Thema „Die ersten 50 Millionen Primzahlen", die in der englischen Übersetzung online verfügbar ist (Zagier, 1975). Das Thema wird in dem Buch „Die Welt der Primzahlen" von Paulo Ribenboim in der bei diesem Autor gewohnten Qualität humorvoll und ausführlich abgehandelt (Ribenboim, 2006).

Ein aktueller Hochschultext zur Zahlentheorie, der als Leitfaden die Verteilung der Primzahlen zugrunde

http://www.cryptool.de/

Mit CrypTool wird das Schützen von Daten verständlich.

legt und in dem die hier angeschnittenen Fragen weiter in die Tiefe gehend behandelt werden, ist das Buch von Benjamin Fine und Gerhard Rosenberger (Fine/Rosenberger, 2007).

Eine etwas knappere Einführung auf Grundstudiums-Niveau stammt von dem Projektleiter des Open Source CAS-Projekts *SAGE* (siehe http://www.sagemath.org/), William Stein: „Elementary Number Theory: Primes, Congruences, and Secrets", in dem auch die Grundlagen der modernen asymmetrischen Kryptografie erklärt werden (Stein, 2009). Beispielrechnungen werden in diesem Buch natürlich mit SAGE durchgeführt, das auch in der Lage ist, Funktionsgraphen zur Verteilung der Primzahlen zu erzeugen. SAGE steht für: Software für Algebra- und Geometrie-Experimente bzw. ***S**oftware for **A**lgebra and **G**eometry **E**xperimentation*. Nach einer Ankündigung auf der Homepage von William Stein ist der Text des Buches mittlerweile als kostenfreie PDF-Datei dank einer großzügigen Zusage des Springer-Verlags erschienen (siehe http://modular.math.washington.edu/ent.pdf).

Als Beilage zu dem bekannten und vielfach ausgezeichneten Programm CrypTool (vgl. Esslinger/Koy, 2009, und http://www.cryptool.org/) gibt es ein CrypTool-Skript mit dem Untertitel „Kryptographie, Mathematik und mehr" von Bernhard Esslinger (dem Chefentwickler von CrypTool) und dem Entwickler-Team. In der aktuellen 10. Auflage hat es 276 Seiten mit einem umfänglichen Kapitel zu Primzahlen (Kap. 3), eine Einführung in die elementare Zahlentheorie mit Beispielen (Kap. 4) und den aktuellen Primzahlrekorden (4.11.4). Das Skript enthält weiterhin Code-Beispiele zur Kryptografie und zur Zahlentheorie, geschrieben in SAGE; außerdem gibt es in einem Anhang eine kurze Einführung zur Benutzung von SAGE.

Ebenfalls in CrypTool enthalten ist ein E-Learning Programm zur Zahlentheorie und zur asymmetrischen Verschlüsselung von Martin Ramberger (Universität Konstanz), das auch als Stand-alone-Programm funktioniert (Bezug: http://www.uni-koblenz.de/~rambo/).

Einen Überblick über die „größten Rätsel der Mathematik" und damit auch über die Riemann'sche Vermutung bietet das *Spektrum Dossier* 6/09, in dem aktualisierte Artikel zum Jahr der Mathematik aus dem *Spektrum der Wissenschaft* zusammengestellt wurden. Dort ist das im Kasten S. 101 erwähnte Interview mit Gerd Faltings abgedruckt.

Sehr empfehlenswert ist das Buch „π & Co. – Kaleidoskop der Mathematik", herausgegeben anlässlich des Jahres der Mathematik von Erhard Behrends, Peter Gritzmann und Günter M. Ziegler (Behrends/ Gritzmann/Ziegler, 2008). In diesem Buch finden sich u. a. auch Artikel zur Riemann'schen Vermutung, zum P=NP-Problem und zu Primzahltests.

mann die analytische Zahlentheorie, in der Methoden der Funktionentheorie zur Erforschung zahlentheoretischer Fragen verwendet werden. Außerdem enthält dieses Papier die berühmte *Riemann'sche Vermutung*, bis zum heutigen Tag eines der wichtigsten offenen Probleme der Mathematik. Für den Beweis dieser Vermutung wurde inzwischen ein Preisgeld von 1 Million Dollar ausgelobt (siehe die Kästen „Bernhard Riemann und die Riemann'sche Vermutung", S. 100, und „1 Million Dollar für den Beweis der Riemann'schen Vermutung", S. 101).

Für den Gauß'schen Primzahlsatz sind neben den erwähnten „klassischen" Beweisen von Hadamard und de La Vallée Poussin inzwischen weitere, vereinfachte Varianten des Beweises gefunden worden (vgl. Kramer, 2008, S. 219). Der bislang kürzeste Beweis stammt von D. J. Newman und D. Zagier und findet sich u. a. im Beweisarchiv von Wikibooks:

http://de.wikibooks.org/wiki/Beweisarchiv:_Zahlentheorie:_Analytische_Zahlentheorie:_Primzahlsatz

Ausblick

In der nächsten Folge dieser Beitragsreihe werden wir uns, wie angekündigt, mit der Frage beschäftigen, wie man Primzahlen mit einer Länge von 1024 Bit (oder mit 308 bzw. 309 Dezimalstellen) erhalten kann. Mithilfe des Primzahlsatzes kann man sich leicht davon überzeugen, dass klassische Methoden zum Auffinden von Primzahlen (wie das Sieb des Eratosthenes) mit Zahlen dieser Größenordnung völlig überfordert sind.

In einer weiteren Folge werden wir uns mit der Frage der Sicherheit der RSA-Verschlüsselung beschäftigen, die eng mit dem Faktorisierungsproblem zusammenhängt: Welcher Aufwand ist erforderlich, um eine Semiprimzahl in ihre beiden Faktoren zu zerlegen? Hier zeigen sich interessante Anwendungen eines wichtigen Teilgebietes der theoretischen Informatik, nämlich der Komplexitätstheorie mit der Abschätzung der Effizienz von Algorithmen.

(wird fortgesetzt)

Helmut Witten
Brandenburgische Straße 23
10707 Berlin

E-Mail: helmut@witten-berlin.de

Prof. Dr. Ralph-Hardo Schulz
Freie Universität Berlin
Fachbereich Mathematik und Informatik
Institut für Mathematik
Arnimallee 3
14195 Berlin

E-Mail: rhschulz@zedat.fu-berlin.de

Wir danken Bernhard Esslinger und Hermann Puhlmann sowie – last but not least – Astrid Witten für Verbesserungsvorschläge zu den ersten Entwürfen dieses Beitrags.

Im **LOG-IN-Service** (siehe Seite 143) können alle hier aufgeführten und noch weitere Internetquellen zum Thema dieses Beitrags als interaktive PDF-Datei ebenso wie eine Liste mit den Errata zur letzten Folge dieser Beitragsserie (Witten/Schulz, 2008) heruntergeladen werden.

Literatur und Internetquellen

Aigner, M.; Ziegler, G. M.: Sechs Beweise für die Unendlichkeit der Primzahlen. In: Behrends/Gritzmann/Ziegler (Hrsg.), 2008, S. 51–54.

Barthe, D.: Leonhard Eulers unendliche Summen. In: Behrends/Gritzmann/Ziegler (Hrsg.), 2008, S. 83–87.

Basieux, P.: Die Top Seven der mathematischen Vermutungen. Reinbek bei Hamburg: rororo science, ^{2}2005.

Behrends, E.; Gritzmann; P., Ziegler, G. M. (Hrsg.): π & Co. – Kaleidoskop der Mathematik. Berlin, Heidelberg: Springer, 2008.

du Sautoy, M.: Die Musik der Primzahlen – Auf den Spuren des größten Rätsels der Mathematik. München: C. H. Beck, ^{2}2004.

Esslinger, B.; Koy, H.: Kryptologie im Unterricht mit CrypTool. In: LOG IN, 29. Jg. (2009), H. 157/158, S. 75–78.

Esslinger, B. u. a.: Das CrypTool-Skript – Kryptographie, Mathematik und mehr. ^{10}2010.
http://www.cryptool.com/download/CrypToolScript-de.pdf

Fine, B.; Rosenberger, G.: Number Theory – An Introduction via the Distribution of Primes. Boston Birkhäuser, 2007.

Kardel, F.: Die Falltürfunktion als mathematische Grundlage für eine Codierung und Decodierung auf dem Kleincomputer. In: LOG IN, 4. Jg. (1984); Teil 1: H. 1, S. 56–62; Teil 2: H. 2, S. 61–62; Teil 3: H. 3, S. 62–64.

Kleinjung, Th. u. a.: Factorization of a 768-bit RSA modulus – version 1.4, February 18, 2010.
http://eprint.iacr.org/2010/006.pdf

Kramer, J.: Die Riemannsche Vermutung. In: Behrends/Gritzmann/Ziegler (Hrsg.), 2008, S. 216–221.

Ribenboim, P.: Die Welt der Primzahlen – Geheimnisse und Rekorde. Berlin, Heidelberg, New York: Springer, 2006.

Riemann, B.: Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse. In: Monatsberichte der Berliner Akademie, November 1859
http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript/zeta.pdf
http://www.claymath.org/millennium/Riemann_Hypothesis/1859_manuscript/riemann1859.pdf

Singh, S.: Fermats letzter Satz – Die abenteuerliche Geschichte eines mathematischen Rätsels. München: dtv, 2000.

Stein, W.: Elementary Number Theory – Primes, Congruences, and Secrets. New York: Springer, 2009.
http://modular.math.washington.edu/ent/ent.pdf

Witten, H.; Schulz, R.-H.: RSA & Co. in der Schule – Neue Folge Teil 1. RSA für Einsteiger. In: LOG IN, 26. Jg. (2006a), H. 140, S. 45–54.

Witten, H.; Schulz, R.-H.: RSA & Co. in der Schule – Neue Folge Teil 2: RSA für große Zahlen. In: LOG IN, 26. Jg. (2006b), H. 143, S. 50–58.

Witten, H.; Schulz, R.-H.: RSA & Co. in der Schule – Neue Folge Teil 3: RSA und die elementare Zahlentheorie. In: LOG IN, 28. Jg. (2008), H. 152, S. 60–70.

Zagier, D: The First 50 Million Prime Numbers. Überarbeitete Fassung der Antrittsvorlesung an der Universität Bonn, 5.5.1975.
http://modular.math.washington.edu/edu/2007/simuw07/misc/zagier-the_first_50_million_prime_numbers.pdf

Alle Internetquellen wurden zuletzt am 31. August 2010 geprüft.