Neues aus Wissenschaft und Lehre

Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2008/2009

HEINRICH HEINE UNIVERSITÄT DÜSSELDORF

d|u|p düsseldorf university press

Jahrbuch der Heinrich-Heine-Universität Düsseldorf

2008/2009

d|u|p

Jahrbuch der Heinrich-Heine-Universität Düsseldorf 2008/2009

Herausgegeben vom Rektor
der Heinrich-Heine-Universität Düsseldorf
Univ.-Prof. Dr. Dr. H. Michael Piper

Konzeption und Redaktion:
Univ.-Prof. em. Dr. Hans Süssmuth

d|u|p

Einbandgestaltung: Monika Uttendorfer
Titelbild: Leben auf dem Campus
Redaktionsassistenz: Georg Stüttgen
Beratung: Friedrich-K. Unterweg
Satz: Friedhelm Sowa, LaTeX
Herstellung: WAZ-Druck GmbH & Co. KG, Duisburg
Gesetzt aus der Adobe Times
ISBN 978-3-940671-33-2

Inhalt

Juristische Fakultät

Partnerschaften der Heinrich-Heine-Universität Düsseldorf

Gesellschaft von Freunden und Förderern der Heinrich-Heine-Universität Düsseldorf e.V.

Forschergruppen an der Heinrich-Heine-Universität Düsseldorf

Beteiligungen an Forschergruppen

Sofja Kovalevskaja-Preisträger

Graduiertenausbildung an der Heinrich-Heine-Universität Düsseldorf

Nachwuchsforschergruppen an der Heinrich-Heine-Universität Düsseldorf

Interdisziplinäre Forscherverbünde an der Heinrich-Heine-Universität Düsseldorf

Kooperation der Heinrich-Heine-Universität Düsseldorf und des Forschungszentrums Jülich

Ausgründungen aus der Heinrich-Heine-Universität Düsseldorf

Zentrale Einrichtungen der Heinrich-Heine-Universität Düsseldorf

Zentrale Universitätsverwaltung

Universitäts- und Landesbibliothek

Zentrum für Informations- und Medientechnologie

Sammlungen in der Universitäts- und Landesbibliothek Düsseldorf

Ausstellungen

Geschichte der Heinrich-Heine-Universität Düsseldorf

Forum Kunst

Chronik der Heinrich-Heine-Universität Düsseldorf

FRITZ GRUNEWALD

Primzahlen und Kryptographie

Mathematik wird seit Jahrtausenden betrieben. Oft stehen Probleme, die aus Anwendungsbereichen kommen, im Mittelpunkt der Forschung. Die erzielten Resultate sind für unsere Zivilisation unverzichtbar. Hier sind insbesondere die Teilgebiete Numerik, Optimierung und Stochastik zu nennen. Schon die Bezeichnungen dieser Gebiete machen die Orientierung auf die Anwendungen, zum Beispiel in der Technik, in der Physik oder auch in der Medizin, deutlich. An der Heinrich-Heine-Universität gibt es in den Bereichen der angewandten Mathematik sehr starke Arbeitsgruppen. Diese sind mit anderen Fächern der Mathematisch-Naturwissenschaftlichen und der Medizinischen Fakultät eng vernetzt. Über die Erfolge in der Anwendung dieser mathematischen Bereiche gäbe es in der Tat viel zu berichten. Dieser Artikel handelt jedoch von Anwendungen der Zahlentheorie, einem Gebiet der reinen Mathematik.

In der Zahlentheorie spielen Aspekte der Anwendbarkeit bei den wichtigen Entwicklungen zunächst kaum eine Rolle. Es handelt sich hier um ein Gebiet, das sich immer an traditionellen Grundlagenproblemen orientiert hat. Ein solches ist das Primzahl-Verteilungsproblem. Dieses wurde von dem 15-jährigen Carl Friedrich Gauß (1777–1855) am Ende des 18. Jahrhunderts formuliert. Im Kapitel „Die Vermutungen von Gauß und Riemann“ findet sich eine präzise Beschreibung der Vermutung von Carl Friedrich Gauß. Die damit verbundenen Fragestellungen sind bis heute ungelöst. Aber schon die Lösungsversuche haben zu zentralen, auch für Anwendungen wichtigen Entwicklungen geführt. Zum Beispiel ist die Theorie der komplexen Zahlen von Bernhard Riemann weitergetrieben worden, um Methoden zum Studium der Zeta-Funktionen zu entwickeln. Diese Funktionen sind von großer innermathematischer Relevanz insbesondere in der Zahlentheorie. Die Untersuchungsmethoden aber werden heute in den Standardvorlesungen für Ingenieure unterrichtet. Wie man sieht, generieren schwierige Probleme der reinen Mathematik Methoden, die große Ausstrahlungskraft haben.

Die Primzahlvermutung von Gauß ist logisch äquivalent zu einer Vermutung über die Lage der Nullstellen der Riemannschen Zeta-Funktion, siehe Kapitel „Die Vermutungen von Gauß und Riemann“. Diese wurde von Riemann, einem Studenten von Gauß, in der denkwürdigen Arbeit „Über die Anzahl der Primzahlen unter einer gegebenen Größe“ aus dem Jahr 1859 aufgestellt. Sie gilt heute als einer der wichtigsten unbewiesenen Sachverhalte der Mathematik. Als im Jahr 2000 sieben Probleme ausgewählt wurden, von denen die Mathematiker erwarten, dass sie im dritten Jahrtausend eine besondere Rolle spielen werden, war die Vermutung von Riemann eines davon.[1] Für die Lösung eines jeden dieser Probleme ist ein Preisgeld von einer Million US$ ausgesetzt.

[1] Vgl. http://www.claymath.org/millennium/(11.11.2009).

Die Zahlentheorie hat in den letzten 30 Jahren eine große Rolle bei der Entwicklung von Verschlüsselungssystemen gespielt. Das wichtigste von diesen so genannten Kryptosystemen findet sich im Kapitel „Das RSA-Kryptosystem“. Insbesondere sind Methoden, mit denen man Primzahlen finden kann, wichtig geworden. Die dafür grundlegenden Techniken werden regelmäßig in den Vorlesungen an der Heinrich-Heine-Universität unterrichtet. Diese Veranstaltungen werden im Moment von mir und von Frau Univ.-Prof. Dr. Elena Klimenko gehalten. Um die Lehre an der Heinrich-Heine-Universität in diesem Bereich zu unterstützen, hat der Deutsche Akademische Austausch Dienst (DAAD) eine zweijährige Gastprofessur für Frau Klimenko eingerichtet.

Außerdem wird in Düsseldorf aktiv über Zeta-Funktionen geforscht. Manchmal spielen hier auch Verallgemeinerungen der von Riemann studierten Funktionen eine wichtige Rolle. Ich habe auf dem letzten internationalen Kongress der Mathematiker, der alle vier Jahre stattfindet, über die insbesondere an der Heinrich-Heine-Universität erzielten Fortschritte berichtet.[2]

Ich danke Daniel Appel, Rüdiger Braun, Elena Klimenko und Wilhelm Singhof für ihre Hilfe bei meiner Arbeit an diesem Manuskript.

Die natürlichen Zahlen und die Primzahlen

Die natürlichen Zahlen $1, 2, 3, \ldots$ bilden den Zahlbereich, den wir als ersten in unserem Leben kennenlernen. Die Mathematik hat für ihn

$$\mathbb{N} = \{\, 1, 2, 3, \ldots \}$$

als Bezeichnung gewählt. Natürliche Zahlen messen Anzahlen. Man erhält alle, indem man ausgehend von der 1 neue Zahlen durch Addieren der 1 generiert, das heißt $\mathbb{N} = \{\, 1, 1+1, 1+1+1, \ldots \}$.

Natürliche Zahlen kann man nicht nur addieren, sondern auch multiplizieren. Wir sind aus der Schule mit diesen Operationen vertraut. Die Multiplikation natürlicher Zahlen führt zu einer wichtigen Relation zwischen Zahlen. Wir sagen: Die natürliche Zahl m *teilt* die Zahl n, falls es eine weitere Zahl k gibt, die die Eigenschaft

$$n = k \cdot m \tag{1}$$

hat. Zum Beispiel teilt 3 die Zahl 15, aber nicht die 19. Wir nennen die Zahlen k, m auch *Teiler* von n. Gilt die Gleichung (1) zwischen den Zahlen n, m, k und sind k, m beide nicht gleich 1, so ist n zerlegbar. Die Primzahlen sind die natürlichen Zahlen, die nicht zerlegbar sind. Präziser definieren wir:

Definition 1. *Eine natürliche Zahl ist eine Primzahl, falls sie nicht gleich* 1 *ist und falls sie außer* 1 *und sich selber keine weiteren Teiler besitzt.*

In Tabelle 1 sind die Primzahlen unter den Zahlen bis 108 fett gedruckt.

Ein erster, sehr erfolgreicher Versuch, die natürlichen Zahlen und die Primzahlen in mathematisch präziser Weise zu beschreiben, wurde von Euklid (circa 365–300 vor Christus) unternommen. Er schreibt mit seinem vielbändigen Werk *Die Elemente* das erfolgreichste

[2] Vgl. Grunewald und DuSautoy (2006).

1	**2**	**3**	4	**5**	6	**7**	8	9	10	**11**	12
13	14	15	16	**17**	18	**19**	20	21	22	**23**	24
25	26	27	28	**29**	30	**31**	32	33	34	35	36
37	38	39	40	**41**	42	**43**	44	45	46	**47**	48
49	50	51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70	**71**	72
73	74	75	76	77	78	**79**	80	81	82	**83**	84
85	86	87	88	**89**	90	91	92	93	94	95	96
97	98	99	100	**101**	102	**103**	104	105	106	**107**	108

Tab. 1: Die Primzahlen bis 108

n	Zerlegung	n	Zerlegung
2	2	11	11
3	3	12	$2 \cdot 2 \cdot 3$
4	$2 \cdot 2$	13	13
5	5	14	$2 \cdot 7$
6	$2 \cdot 3$	15	$3 \cdot 5$
7	7	16	$2 \cdot 2 \cdot 2 \cdot 2$
8	$2 \cdot 2 \cdot 2$	17	17
9	$3 \cdot 3$	18	$2 \cdot 3 \cdot 3$
10	$2 \cdot 5$	19	19

Tab. 2: Zerlegungen

Mathematikbuch aller Zeiten. Noch heute haben große Teile davon wissenschaftliche Bedeutung. Die Kapitel VII bis IX enthalten die Arithmetik, das heißt die Theorie der Zahlen. Hier beschreibt Euklid einen axiomatischen Aufbau der natürlichen Zahlen. Ausgehend von allgemein einleuchtenden Eigenschaften der Zahlen führt Euklid mit genau eingegrenzten Schlussweisen Beweise. Als einen der ersten Sätze über natürliche Zahlen zeigt er in Buch VII der *Elemente*:

Satz 1. *Jede natürliche Zahl, die größer als* 1 *ist, ist entweder eine Primzahl oder wird von einer solchen geteilt.*

In einer von Gauß formulierten etwas moderneren Version zeigt man heutzutage in der Vorlesung:

Satz 2 (Fundamentalsatz der Arithmetik)**.** *Jede natürliche Zahl, die größer ist als* 1*, lässt sich (bis auf die Reihenfolge der Faktoren) eindeutig als Produkt von Primzahlen darstellen.*

In Tabelle 2 finden sich für einige kleine Zahlen die zugehörigen Produktdarstellungen. Diese multiplikative Schreibweise der Zahlen nennt man auch *Primfaktorzerlegung*. Die Primzahlen bilden somit die Bausteine, aus denen sich alle natürlichen Zahlen multiplikativ zusammensetzen.

Nach dem Beweis des Vorgängers (Satz 1) des Fundamentalsatzes der Arithmetik stellt Euklid sich die Frage, ob es wohl endlich viele oder unendlich viele Primzahlen gibt. Nach

den Daten in Tabelle 1 kann man vermuten, dass Letzteres der Fall sein wird. In der Tat beweist Euklid in Buch VIII der *Elemente*:

Satz 3. *Es gibt unendlich viele Primzahlen.*

Der Beweis von Satz 1 ist nicht sehr schwer. Interessanter ist der darauf aufbauende Beweis von Satz 3. Es handelt sich hier um den historisch ersten Fall eines Beweises durch Widerspruch. Das von Euklid beschriebene Argument verläuft folgendermaßen: Gibt es nur endlich viele Primzahlen, so können wir diese in einer Liste aufzählen. Seien also $p_1 = 2$, $p_2 = 3$, $\ldots$, p_r alle Primzahlen. Wir setzen dann

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_r + 1. \tag{2}$$

Wir erhalten also die natürliche Zahl N, indem wir alle Primzahlen multiplizieren und zu dem Resultat die 1 addieren. Da N sicher größer als 2 ist, hat N also nach Satz 1 einen Primteiler, das heißt N wird von einer der Primzahlen $p_1, p_2, \ldots, p_r$ geteilt. Kann dies wirklich sein? Nehmen wir an, dass p_1 ein Teiler von N ist, dann würde p_1 auch ein Teiler von $N - p_1 \cdot p_2 \cdot \ldots \cdot p_r$ sein. Diese Zahl ist jedoch gleich 1 und wir können folgern, dass p_1 die Zahl 1 teilt. Dies ist nicht möglich. Genauso kann man schließen, dass auch jede andere in der Primfaktorzerlegung vorkommende Primzahl die linke Seite und auch den ersten Summanden der rechten Seite der Gleichung (2) und damit auch die Zahl 1 teilt. Wir haben also die Annahme, dass es nur endlich viele Primzahlen gibt, zum Widerspruch geführt, und Satz 3 ist bewiesen.

Probleme

In diesem Kapitel bespreche ich Probleme der Zahlentheorie, die seit langem studiert wurden und die durch das im Kapitel „Das RSA-Kryptosystem“ beschriebene Verschlüsselungsverfahren eine zusätzliche Bedeutung erhielten.

Das erste Problem ist durch die letzten Jahrhunderte meistens in etwas unpräziser Form studiert worden. Es lautet

Problem 1. *Wie sind die Primzahlen verteilt?*

Man fragt grob gesprochen, ob die Primzahlen relativ selten oder doch häufiger in der Reihe der natürlichen Zahlen auftauchen. Diese Frage wurde von Gauß in seiner Primzahlvermutung in faszinierender Weise konkretisiert. Diese ist im Kapitel „Die Vermutungen von Gauß und Riemann“ diskutiert.

Die Verschlüsselungsmethode aus dem Kapitel „Das RSA-Kryptosystem“ benutzt Primzahlen. Somit haben wir auch ein Interesse an der folgenden Frage.

Problem 2. *Wie findet man (große) Primzahlen?*

Man könnte daran denken, hier einfach große Zahlen aufzuschreiben und zu überprüfen, ob sie einen echten Teiler besitzen. Diese Methode funktioniert aber nur theoretisch, da sie sehr langsam ist. Wir werden also auf die folgende Frage geführt.

Problem 3. *Wie erkenne ich (schnell), ob eine Zahl eine Primzahl ist oder nicht?*

Eine Methode, oder wie man sagt ein Algorithmus, der entscheidet, ob eine Zahl n eine Primzahl ist oder nicht, nennt man einen Primzahltest. Die Güte eines solchen Tests wird durch die Anzahl der Rechenschritte gemessen, die er braucht, um diese Frage für ein n

zu entscheiden. Die naive Methode (Ausprobieren aller möglichen Teiler) braucht ungefähr n Rechenschritte und ist damit sehr schlecht. Im Jahr 2002 wurde der so genannte AKS-Algorithmus[3] von drei indischen Mathematikern entdeckt. Das war eine große wissenschaftliche Sensation. Er braucht nur $100\log(n)^{11}$ Schritte für die Entscheidung, ob n eine Primzahl ist oder nicht. Hier ist $\log(n)$ der natürliche Logarithmus von n (siehe Wikipedia). Er ist von der gleichen Größenordnung wie die Anzahl der Stellen von n, also sehr viel kleiner als n. Für eine 100-stellige Zahl benötigt der AKS-Algorithmus nur etwa 10^{20} Rechenschritte, der naive Algorithmus hingegen braucht 10^{100} Schritte. Das ist eine massive Ersparnis. Mit modernen Primzahltests kann man schon viele Primzahlen mit ungefähr 80 Stellen finden. Für größere Zahlen ist es nur in Ausnahmefällen gelungen, ihre Primalität nachzuweisen.

Hier möchte ich auch noch über die jahrhundertelange, und nach Satz 3 niemals endende, Jagd auf die größte Primzahl berichten. Die zeitliche Entwicklung des Weltrekords ist aus Tabelle 3 ersichtlich.

1500:	$2^{17}-1=131071$
1770:	$2^{31}-1=2147483647$
1952:	$2^{607}-1=531137992816767098689588206552468627329593117727031923199444138200403559860852242739162502265229285668889329486246501015346579337652707239409519978766587351943831270835393219031728127$
1957	$2^{3217}-1$ hat 969 Stellen
1990:	$2^{756839}-1$ hat 227832 Stellen
2004:	$2^{24036583}-1$ hat 7235733 Stellen
bestehender Weltrekord:	$2^{43112609}-1$ hat 12978189 Stellen

Tab. 3: Weltrekorde: Die größten Primzahlen

Die Einträge in Tabelle 3 zeigen, dass wir keine Methode haben, um wirklich große Primzahlen zu finden. Mit dem Einsatz von Computern (etwa ab 1940) hat sich unser Wissen verbessert. Wie oben erwähnt, ist es mit heutigen Algorithmen möglich, eine große Menge von 80-stelligen Primzahlen zu finden. Bei Zahlen von spezieller Form, wie das bei den Zahlen in Tabelle 3 der Fall ist, können wir in noch höhere Bereiche vordringen.

Das letzte Problem, das ich hier nennen will, ist besonders für die zentrale Sicherheitsfrage des im Kapitel „Das RSA-Kryptosystem“ diskutierten Verschlüsselugsverfahrens wichtig. Wir wissen schon aus dem Kapitel „Die natürlichen Zahlen und die Primzahlen“, dass sich jede natürliche Zahl, die größer ist als 1, als Produkt von Primzahlen darstellen lässt (Primfaktorzerlegung). Aber es bleibt die Frage:

Problem 4. *Wie berechne ich (schnell) die Primfaktorzerlegung einer natürlichen Zahl?*

Hat man die Primfaktorzerlegung einer natürlichen Zahl vorliegen, so sieht man, ob diese eine Primzahl ist oder nicht. Eine schnelle Lösung für Problem 4 zieht also eine Antwort auf die Frage in Problem 3 nach sich. Zurzeit wissen wir aber nicht, ob es einen schnellen Algorithmus gibt, der Problem 4 löst. Es gibt viele Zahlen von Interesse, von

[3] Vgl. http://de.wikipedia.org/wiki/AKS-Primzahltest(11.11.2009).

denen wir wissen, dass sie keine Primzahlen sind, für die wir aber keinen Primteiler finden können. Im Kapitel „Rechnen modulo n“ findet sich ein (schneller) Algorithmus, der, ohne einen Teiler konkret zu finden, doch die Zerlegbarkeit von natürlichen Zahlen zeigen kann.

In diesem Zusammenhang ist die Geschichte der Zahl RSA704 interessant. Diese Zahl ist von der Firma RSA[4] (siehe auch Kapitel „Das RSA-Kryptosystem“) generiert worden. Sie ist

$$RSA704 = 74037563479561712828046796097429573142593188889231289084936$$
$$232638972765034028266276891996419625117843995894330502127 58$$
$$537011896809828673317327310893090055250511687706329907239 63$$
$$807867100860969625379346505637963 59$$

.

Diese Zahl hat 212 Dezimalstellen und ist das Produkt von zwei ungefähr 100-stelligen Primzahlen. Die Firma RSA hat vor einigen Jahren ein Preisgeld von 30.000 US$ für die Faktorisierung von RSA704 ausgelobt. Die Aufgabe konnte bisher nicht gelöst werden.

Was veranlasste die Firma RSA zu der Auslobung von so viel Geld? Wie im Kapitel „Das RSA-Kryptosystem“ erläutert, verkauft RSA Verschlüsselungssysteme, deren Sicherheit darauf beruht, dass man Zahlen wie RSA704 nicht in vertretbarer Zeit faktorisieren kann. In einigen wenigen Fällen ist es gelungen, RSA-Zahlen mit riesigem Aufwand zu faktorisieren[5]. Aber es handelte sich jeweils um Zahlen, die viel kleiner als RSA704 waren. Seit kurzem hat RSA die Auslobung eingestellt, wohl im Vertrauen darauf, dass es keinen schnellen Algorithmus gibt, der Problem 4 löst. Aus mathematischer Sicht muss man aber sagen, dass wir nichts darüber wissen.

Die Vermutungen von Gauß und Riemann

Wir wissen aus dem Kapitel „Die natürlichen Zahlen und die Primzahlen“, dass es unendlich viele Primzahlen gibt. Die Kette der Primzahlen wird also nie abbrechen. Aber wie sind sie verteilt? Kommen die Primzahlen in regelmäßigen Abständen oder sind sie dünn und unregelmäßig verteilt? Das Interesse an solchen Fragen begann um 1700. Eine präzise Formulierung des Problems wurde zum ersten Mal von Carl Friedrich Gauß gegeben. Er hatte sich, angeregt durch ein Mathematikbuch, das er als Geschenk erhalten hatte, schon als Schüler mit den Primzahlen beschäftigt. Im Alter von ungefähr 15 Jahren formuliert er die bis heute unbewiesene Primzahlvermutung.

Um diese zu verstehen, definieren wir die Funktion π, die Primzahlen zählt; in der Bezeichnungsweise von Gauß setzen wir

$$\pi(x) = \text{Anzahl der Primzahlen, die kleiner oder gleich } x \text{ sind.} \tag{3}$$

Aus Tabelle 1 finden wir leicht die Werte:

$$\pi(10) = 4, \qquad \pi(20) = 8, \qquad \pi(100) = 25.$$

[4] Vgl. http://www.rsa.com (11.11.2009).
[5] Vgl. http://www.heise.de/newsticker/meldung/RSA-576-geknackt-89907.html (11.11.2009).

Abb. 1: Carl Friedrich Gauß (1777–1855)

Gauß hatte gerade in der Schule gelernt, dass man Funktionen versteht, indem man ihre Werte in ein Schaubild einträgt. Macht man das bis $x = 50$, so sieht man Abbildung 2.

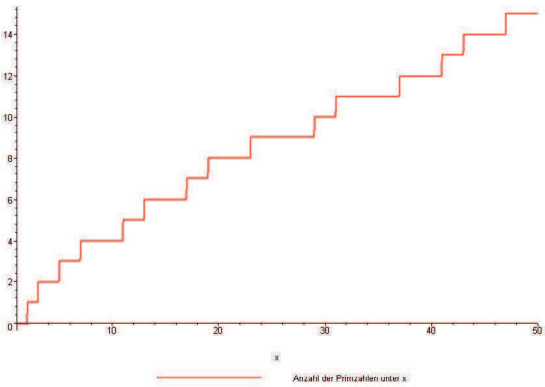

Abb. 2: Der Graph von π bis $x = 50$

Die Funktion π ist eine monoton steigende Treppenfunktion, deren Wert um 1 nach oben springt, wenn man mit x eine Primzahl passiert. Durch diese Sprungstellen ist der Verlauf des Graphen von π unstetig. Zeichnet man den Graphen von π bis $x = 50000$, so sieht man Abbildung 3.

Gauß realisiert das wissenschaftliche Wunder, dem er hier gegenübersteht. Die Sprungstellen verschwimmen zu einem stetig oder sogar differenzierbar (glatt) aussehenden Graphen. Er fragt sich dann, ob er den Graphen einer bekannten Funktion in Abbildung 3 sieht.

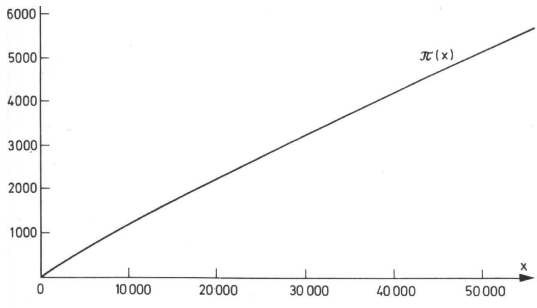

Abb. 3: Der Graph von π bis $x = 50000$

Um diese Frage auf der Basis größerer Datenmengen beurteilen zu können, bestimmt er in jeder freien Minute die Primzahlen in immer größeren Intervallen. Dabei entscheidet er schon als Schüler die Primalität von Zahlen mit großem Geschick. Er erkennt, dass Abbildung 3 die Funktion

$$G(x) = \frac{x}{\log(x)}$$

als gute Approximation für die Primzahlfunktion $\pi(x)$ nahelegt. Die Übereinstimmung ist sehr gut. Gauß sieht die untere Kurve ($G(x)$) als Annäherung für die mittlere Kurve ($\pi(x)$) wie in Abbildung 4 gezeichnet.

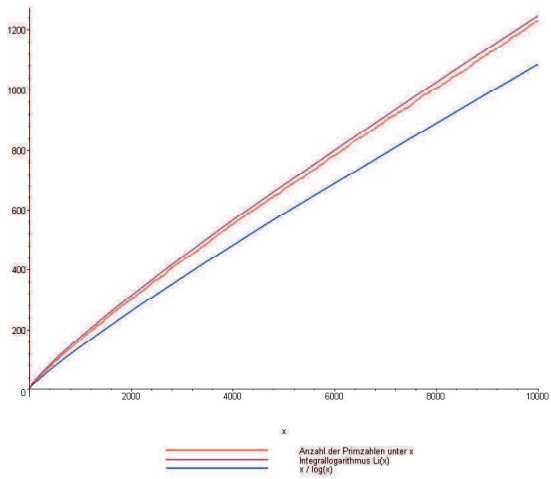

Abb. 4: Approximationen an $\pi(x)$

Er gibt sich aber mit diesem Resultat noch nicht zufrieden. Durch das Studium von ihm vorliegenden Logarithmentafeln erkennt er, dass der Integrallogarithmus $\mathrm{Li}(x)$ noch eine weit bessere Approximation an $\pi(x)$ liefert als $G(x)$. Der Integrallogarithmus ist durch

die Formel

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$

definiert. Das heißt, der Wert $\mathrm{Li}(x)$ ist gleich dem Flächeninhalt zwischen der x-Achse und dem Graphen von $1/\log(x)$ gemessen über das Intervall zwischen 2 und x. Diese, an die Definition des Logarithmus als Flächeninhalt zwischen der x-Achse und dem Graphen von $1/x$ gemessen über das Intervall zwischen 1 und x erinnernde Definition ist in Abbildung 5 dargestellt.

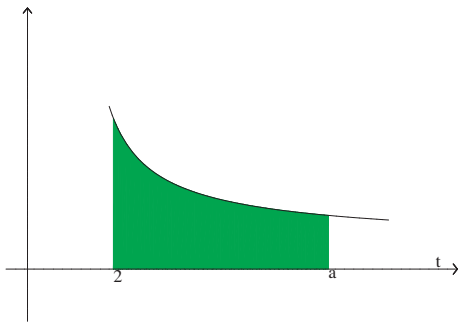

Abb. 5: Der Integrallogarithmus

Der Graph von $\mathrm{Li}(x)$ ist der obere Graph in Abbildung 4. Er zeigt eine verblüffende Übereinstimmung mit dem Graphen von $\pi(x)$.

Der Schüler Carl Friedrich Gauß formuliert nun seine Vermutung, für die er lebenslang Berechnungen von Anzahlen von Primzahlen ausführt. Die Primzahlverteilungsvermutung von Gauß lautet:

$$\pi(x) = \mathrm{Li}(x) + \text{Fehler höchstens von der Größe } \sqrt{x} \cdot \log(x). \tag{4}$$

Es handelt sich hier um eine Approximation erster Güte der Sprungfunktion $\pi(x)$ durch die glatte Funktion $\mathrm{Li}(x)$. Um diese Übereinstimmung nochmals zu demonstrieren, habe ich die Funktionswerte in Tabelle 4 zusammengestellt.

x	$\pi(x)$	$x/\log(x)$	$\mathrm{Li}(x)$
10	4	4	4
100	25	22	29
1000	168	145	176
10000	1229	1086	1245
100000	9592	8668	9629
1000000	78498	72382	78626
10000000	664579	620421	664917
100000000	5761455	5428681	5762208
10^{12}	37607912018	36191206825	37607950279

Tab. 4: Approximation von $\pi(x)$ (gerundet)

Die Funktion $\pi(x)$ ist für große x sehr schwer zu berechnen. Man muss ja von jeder natürlichen Zahl zwischen 1 und x entscheiden, ob sie eine Primzahl ist oder nicht. Die Funktion $\mathrm{Li}(x)$ ist hingegen ganz leicht zu berechnen. Man benutzt dazu einfache numerische Integrationsprogramme. Dies macht die Übereinstimmung in Tabelle 4 umso erstaunlicher.

Die Primzahlvermutung ist bis heute unbewiesen. Aber im Jahr 1896 wurde von Jacques Salomon Hadamard und Charles-Jean-Gustave-Nicolas de la Vallée-Poussin eine schwache Form dieser Vermutung gezeigt. Ihr Resultat lautet

$$\pi(x) \sim \frac{x}{\log(x)}. \tag{5}$$

Dabei bedeutet die Formelschreibweise $f(x) \sim g(x)$ für Funktionen f, g, dass der Quotient $f(x)/g(x)$ für $x \to \infty$ gegen 1 konvergiert. Man beachte, dass (5) von der Vermutung (4) impliziert wird, aber doch wesentlich schwächer als diese ist.

Wir kommen jetzt zu dem Beitrag von Bernhard Riemann (1826–1866) zum Problem der Primzahlverteilung. Riemann war ein Student von Gauß in Göttingen. Mit zwei bahnbrechenden Arbeiten wurde er bei Gauß promoviert und habilitierte sich auch. Zu seiner Aufnahme in die Berliner Akademie der Wissenschaften reicht er die Arbeit „Über die Anzahl der Primzahlen unter einer gegebenen Größe“ ein. Diese Arbeit ist etwas skizzenhaft geschrieben, aber sie ist ein sehr wichtiger Beitrag zur Zahlentheorie und zur Analysis. Die erste Seite dieser bedeutenden Abhandlung ist in Abbildung 8 zu sehen.

Abb. 6: Bernhard Riemann (1826–1866)

In seiner Arbeit studiert Riemann die analytischen Eigenschaften der (Riemannschen) Zeta-Funktion $\zeta(s)$. Diese ist definiert durch die Reihe:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots \tag{6}$$

Um diese Definition zu verstehen, muss man etwas über die komplexen Zahlen sagen. Diese bilden eine Zahlbereichserweiterung der reellen Zahlen, die nötig wurde, weil gewisse Gleichungen ($x^2 = -1$) keine reellen Lösungen haben. Die Theorie der komplexen Zahlen und auch der zugehörigen Funktionen wurde erstmals von Gauß auf ein sicheres Fundament gestellt. Riemann hat sie mit dem Ziel des Studiums der Funktion $\zeta(s)$ wesentlich weiterentwickelt. Die komplexen Zahlen werden mit

$$\mathbb{C} = \{\, a + bi \,|\, a,\ b \text{ sind reelle Zahlen und } i^2 = -1 \,\}$$

bezeichnet, wir stellen sie uns wie in Abbildung 7 als Punkte der Ebene vor.

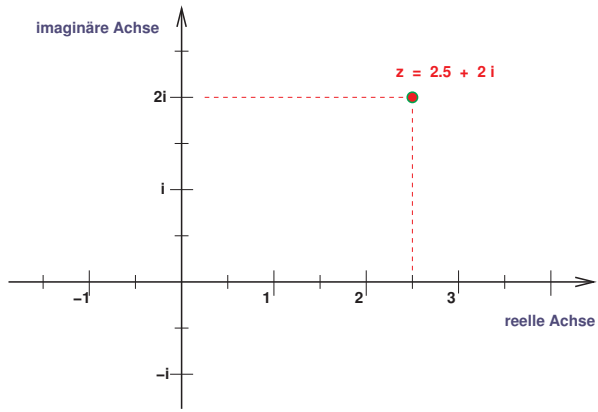

Abb. 7: Die komplexe Ebene

Die reellen Komponenten a, b einer komplexen Zahl $a + bi$ heißen Realteil (a) und Imaginärteil (b) der Zahl.

Um die Definition (6) der Zeta-Funktion zu verstehen, muss man als Erstes erklären, wie man eine positive reelle Zahl ($1/2,\ 1/3, \ldots$) mit einer komplexen Zahl s potenziert. Das wird durch Fortsetzung der bekannten reellen Definition möglich. Die unendliche Summe in (6) konvergiert für alle komplexen Zahlen s mit einem Realteil, der größer als 1 ist. Diese so in der entsprechenden Halbebene der komplexen Zahlen definierte Funktion hat sehr gute analytische Eigenschaften, sie ist zum Beispiel überall ableitbar. Riemann erhält in seiner Arbeit auch noch einen anderen Ausdruck für $\zeta(s)$, er zeigt

$$\zeta(s) = \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \ldots, \tag{7}$$

wobei das Produkt über alle Primzahlen zu erstrecken ist. Hier zeigt sich ein erster enger analytischer Zusammenhang zwischen den natürlichen Zahlen und den Primzahlen. Man kann Gleichung (7) dazu benutzen, um noch einmal zu zeigen, dass es unendlich viele Primzahlen gibt. Außerdem impliziert diese Gleichheit, dass die Zeta-Funktion für keine komplexe Zahl s, die einen Realteil echt größer als 1 hat, den Wert 0 annimmt.

Ein wichtiger nächster Schritt ist die Fortsetzbarkeit der Zeta-Funktion. Diese ist von Riemann bewiesen worden. Sie besagt, dass die Zeta-Funktion eine eindeutig bestimmte

Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.

Bernhard Riemann

[Monatsberichte der Berliner Akademie, November 1859.]

Meinen Dank für die Auszeichnung, welche mir die Akademie durch die Aufnahme unter ihre Correspondenten hat zu Theil werden lassen, glaube ich am besten dadurch zu erkennen zu geben, dass ich von der hierdurch erhaltenen Erlaubniss baldigst Gebrauch mache durch Mittheilung einer Untersuchung über die Häufigkeit der Primzahlen; ein Gegenstand, welcher durch die Interesse, welches *Gauss* und *Dirichlet* demselben längere Zeit geschenkt haben, einer solchen Mittheilung vielleicht nicht ganz unwerth erscheint.

Bei dieser Untersuchung diente mir als Ausgangspunkt die von *Euler* gemachte Bemerkung, dass das Product

$$\Pi \frac{1}{1-\frac{1}{p^s}} = \Sigma \frac{1}{n^s},$$

wenn für p alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der reelle Theil von s grösser als 1 ist; es lässt sich indess leicht ein immer gültig bleibender Ausdruck der Function finden. Durch Anwendung der Gleichung

$$\int_0^\infty e^{-nx} x^{s-1}\, dx = \frac{\Pi(s-1)}{n^s}$$

erhält man zunächst

$$\Pi(s-1)\zeta(s) = \int_0^\infty \frac{x^{s-1}\, dx}{e^x - 1}.$$

Abb. 8: Manuskript von Riemann

differenzierbare Fortsetzung auf die komplexen Zahlen $\mathbb{C}$ ohne die 1 besitzt. Wir können ab jetzt über die Werte der Zeta-Funktion in der ganzen komplexen Ebene (außer 1) reden.

Der Beweis des Primzahlsatzes (5) benutzt entscheidend, dass die Riemannsche Zeta-Funktion für kein komplexes s mit Realteil 1 den Wert 0 annimmt.

Bernhard Riemann stellt sich nun die Frage, wo die Nullstellen seiner Zeta-Funktion liegen. Er findet heraus, dass sich bei den negativen geraden ganzen Zahlen Nullstellen befinden. Diese nennt man heute die trivialen Nullstellen. Riemann zeigt auch, dass sonst nirgends außerhalb des Streifens zwischen den Geraden Realteil gleich 0 und Realteil gleich 1 (dieser heißt der kritische Streifen) Nullstellen liegen. Im kritischen Streifen gibt es unendlich viele Nullstellen. Einige davon sind in Abbildung 9 als fette Punkte zu sehen.

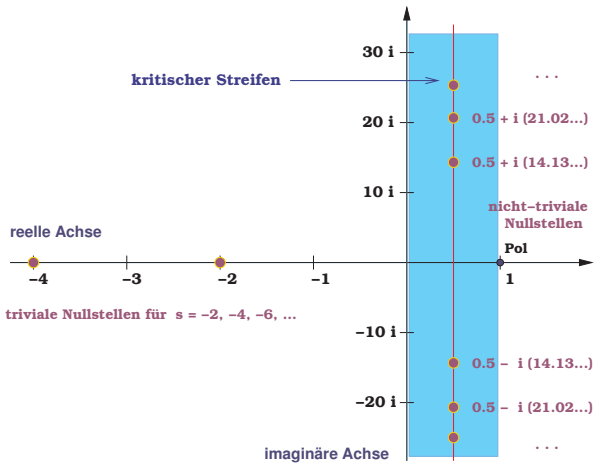

Abb. 9: Der kritische Streifen

Die Vermutung von von Riemann besagt:

Alle Nullstellen im kritischen Streifen der Riemannschen Zeta-Funktion haben Realteil gleich $1/2$.

Diese Vermutung ist bis heute nicht bewiesen. Sie gilt als eines der wichtigsten Probleme der Mathematik. Ein Grund dafür ist der folgende, von Riemann bewiesene

Satz 4. *Die Riemannsche Vermutung ist logisch äquivalent zur Vermutung von Carl Friedrich Gauß über die Primzahlverteilung (4).*

Rechnen modulo n

In diesem Kapitel möchte ich das Rechnen in Zahlbereichen erläutern, die aus den natürlichen Zahlen in einfacher Weise abgeleitet werden. Das Rechnen in diesen neuen Bereichen wird für das im nächsten Kapitel geschilderte Verschlüsselungsverfahren wichtig werden.

Als Erstes erweitern wir die natürlichen Zahlen durch Hinzunahme der 0 und der negativen Zahlen zur Menge der ganzen Zahlen. Die mathematische Bezeichnung ist

$$\mathbb{Z} = \{\ldots, -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\}.$$

Ganze Zahlen kann man wieder addieren und multiplizieren. Im Unterschied zu natürlichen Zahlen kann man beliebige ganze Zahlen voneinander abziehen und erhält wieder eine ganze Zahl.

Sei n eine feste natürliche Zahl. Wir sagen, dass zwei ganze Zahlen a, b *kongruent* modulo n sind, falls ihre Differenz $a - b$ durch die Zahl n teilbar ist. Wir schreiben dafür

$$a \equiv b \bmod n.$$

Zum Beispiel ist 17 kongruent zu 20, 26 und -4528 modulo 3, hingegen ist 17 nicht kongruent zu -18 modulo 3.

Die Theorie der Kongruenzen wurde von Gauß in seinem im Jahr 1801 veröffentlichten Werk *Disquisitiones Arithmeticae* entwickelt. Der Begriff der Kongruenz liefert interessante Einteilungen der ganzen Zahlen. Jede natürliche Zahl a ist kongruent modulo n zu einer eindeutig bestimmten Zahl in der Menge

$$\{0, 1, \ldots, (n-1)\}. \tag{8}$$

Diese Menge beinhaltet die Zahlen, die sich als Reste bei Division durch n ergeben können. Man kann dann diese Reste addieren oder auch multiplizieren und danach wieder zum zugehörigen Rest übergehen. Damit ist das Rechnen im Zahlbereich (8) definiert. Man sagt dann, dass man modulo n rechnet.

Zu beachten ist, dass jede Zahl a kongruent zu ihrem Rest bei Division durch n ist. Zum Beispiel ergibt sich bei Division von 17 durch 3 der Rest 2, und in der Tat gilt $17 \equiv 2 \mod 3$.

Als Beispiel für das Rechnen modulo 15 bestimme ich jetzt den Rest der Zahl 2^{15} bei Division durch 15. Eine Möglichkeit, das zu tun, ist, $2^{15} = 32768$ durch 15 mit Rest zu dividieren (wie man es in der Schule gelernt hat). Nach einer längeren Rechnung erhalten wir das Resultat $2^{15} \equiv 8 \mod 15$. Es gibt aber folgende, sehr viel einfachere Weise, dieses einzusehen. Wir rechnen einfach

$$2^{15} = 2^4 \cdot 2^4 \cdot 2^4 \cdot 2^3 \equiv 8 \mod 15 \tag{9}$$

wobei wir $2^4 = 16 \equiv 1 \mod 15$ benutzen.

Wie in diesem Beispiel angedeutet, gibt es im Allgemeinen ein sehr schnelles Verfahren, um $a^e \mod n$ für ganze Zahlen a auszuwerten. Über die Werte von $a^e \mod n$ gibt es noch ein bemerkenswertes generelles Resultat.

Satz 5 (Kleiner Satz von Fermat)**.** *Sei n eine Primzahl und a eine ganze Zahl. Dann gilt $a^n \equiv a \mod n$.*

Mit diesem Ergebnis kann man manchmal schnell herausfinden, dass eine gegebene Zahl keine Primzahl ist. Zum Beispiel ergibt unsere Rechnung (9) zusammen mit Satz 5, dass 15 keine Primzahl ist. Das erscheint uns als offensichtliche Bemerkung, aber man beachte, dass wir zu diesem Resultat gelangt sind, ohne die Primfaktorzerlegung von 15 zu berechnen. Wie schon im Kapitel „Probleme“ erwähnt, ist die Berechnung der Primfaktorzerlegung einer Zahl schwieriger, als zu entscheiden, ob sie eine Primzahl ist oder nicht. Mit dem eben demonstrierten Test lässt sich nicht entscheiden, ob eine gegebene Zahl eine Primzahl ist oder nicht. Es gibt tatsächlich Zahlen, die diesen Test bestehen, aber dennoch keine Primzahlen sind. Solche Zahlen nennt man Carmichael-Zahlen.

Das RSA-Kryptosystem

In diesem Kapitel schildere ich eine moderne Verschlüsselungsmethode, das RSA-Kryptosystem. Diese Methode wird heutzutage in der Praxis vielfach verwendet, von Banken, bei der Kommunikation von Privatpersonen und auch für militärische Zwecke. Bei meiner Darstellung werde ich insbesondere die Bezüge zu den im Kapitel „Probleme“ erläuterten zahlentheoretischen Problemen erklären.

Die Ausgangslage ist einfach: Person $\mathcal{A}$ will an $\mathcal{B}$ die Nachricht M schicken. Wir symbolisieren dies durch:

$$\mathcal{A} \xrightarrow{M} \mathcal{B}.$$

Bei dem Sendeprozess können die verwendeten Signale abgefangen werden. Um das Bekanntwerden der Nachricht M zu verhindern, verabreden $\mathcal{A}$ und $\mathcal{B}$, die Nachricht M zu der Nachricht $V(M)$ zu verschlüsseln. Aus $V(M)$ soll M nur schwer erkennbar sein. Aber der Empfänger $\mathcal{B}$ muss die Möglichkeit haben, M aus $V(M)$ zu berechnen.

Klassische Verschlüsselungsmethoden beruhen darauf, dass $\mathcal{A}$ und $\mathcal{B}$ sowohl das Verfahren zur Verschlüsselung als auch das zur Entschlüsselung kennen. Beide Verfahren sind dann natürlich geheim zu halten. Die Enigma (griechisch für Rätsel) ist wohl die bekannteste Chiffriermaschine. Während des Zweiten Weltkrieges wurden mit ihr die meisten Funksprüche der deutschen Wehrmacht und Marine verschlüsselt und auch entschlüsselt. Dieser Code wurde schließlich immer wieder von britischen Mathematikern geknackt.

Bei dem RSA-Verfahren ist die Verschlüsselungsmethode öffentlich und kann von jedermann verwendet werden, die Entschlüsselungsmethode kennt aber nur $\mathcal{B}$. Das hat auch den Vorteil, dass viele $\mathcal{A}$ ohne weitere Probleme mit $\mathcal{B}$ kommunizieren können. Das RSA-Verfahren wurde 1977 von Ronald L. Rivest, Adi Shamir und Leonard Adleman am Massachusetts Institute of Technology entwickelt. Der Name RSA setzt sich aus den Anfangsbuchstaben ihrer Familiennamen zusammen. Es ist das erste in der Praxis wichtige so genannte asymmetrische Verschlüsselungsverfahren. Das RSA-Verfahren wurde 1983 zum Patent angemeldet. Am 21. September 2000 lief dieses Patent aus.

Um die Vorgehensweise von RSA zu schildern, nehmen wir an, dass M eine nicht zu große natürliche Zahl ist. Es gibt viele sehr schnelle Methoden, um geschriebene Texte in solche Zahlen zu verwandeln – natürlich so, dass der umgekehrte Prozess genauso schnell möglich ist. Im Folgenden ist die Vorgehensweise bei Verwendung von RSA beschrieben.

Erzeugung des öffentlichen und privaten Schlüssels

Der öffentliche Schlüssel ist ein Zahlenpaar (e, N) und der private Schlüssel ein Zahlenpaar (d, N), wobei N bei beiden Schlüsseln gleich ist. Wir verabreden noch, dass die Zahl M, die die Nachricht enthält, kleiner als N ist. Beide Schlüssel werden vom Empfänger $\mathcal{B}$ in der folgenden Weise erzeugt:

Im ersten Schritt wählt $\mathcal{B}$ zwei verschiedene Primzahlen $p \neq q$ und berechnet dann die Produkte

$$N = p \cdot q, \qquad E = (p-1) \cdot (q-1).$$

Um die obige Zusatzvoraussetzung (M ist kleiner als N) zu garantieren, können die Primzahlen p, q natürlich nicht zu klein gewählt werden. Als nächstes wählt $\mathcal{B}$ eine natürliche Zahl e, die zwischen 1 und E liegt (und nicht gleich 1 ist) und die teilerfremd zu e ist. Danach findet $\mathcal{B}$ eine natürliche Zahl d, die ebenfalls zwischen 1 und E liegt und die

$$e \cdot d \equiv 1 \mod E$$

erfüllt. Ein solches d gibt es immer, und es gibt sehr effiziente Verfahren, um d aus E und e zu berechnen. Die schnellste bekannte Methode beruht wieder auf Argumenten von

Euklid. Man verwendet den aus der Schule bekannten Euklidischen Algorithmus.[6] Nach der Berechnung von d ist die Erzeugung der Schlüssel abgeschlossen. Der öffentliche Schlüssel ist das Zahlenpaar (e, N) und der private Schlüssel das Zahlenpaar (d, N), Die Zahlen p, q und E werden nicht mehr benötigt und sollten nach der Schlüsselerstellung auf sichere Weise gelöscht werden. Der öffentliche Schlüssel (e, N) wird von $\mathcal{B}$ jetzt in der Tat veröffentlicht. Solche Informationen finden sich heutzutage im Internet, zum Beispiel auf den Webseiten von Banken.

Verschlüsseln von Nachrichten

Nach unseren Verabredungen möchte $\mathcal{A}$ die Zahl M an $\mathcal{B}$ senden. Er, das heißt $\mathcal{A}$, verschafft sich den öffentlichen Schlüssel (e, N) und überprüft, ob N und M teilerfremd sind. Falls dies nicht der Fall ist, kauft $\mathcal{A}$ einen neuen Schlüssel. Für die Überprüfung der Teilerfremdheit ist wieder der Euklidische Algorithmus das schnellstmögliche Verfahren. Danach berechnet $\mathcal{A}$

$$V(M) \equiv M^e \mod N.$$

Dies ist leicht möglich (wie wir in Rechnung (9) gesehen haben) und erzeugt aus der geheimen Zahl M die völlig neue Zahl $V(M)$. Diese neue Zahl schickt $\mathcal{A}$ an $\mathcal{B}$.

Entschlüsseln von Nachrichten

Der Empfänger $\mathcal{B}$ erhält jetzt die Zahl $V(M)$. Wie kann er daraus die Nachricht M zurückerhalten? Er benutzt den nur ihm bekannten privaten Schlüssel (d, N), um

$$K \equiv V(M)^d \mod N \tag{10}$$

zu berechnen. Natürlich soll die so gewonnene Zahl K wieder zwischen 1 und N liegen. Wir verwenden nun folgenden, in Analogie zu Satz 5 stehenden Sachverhalt.

Satz 6. *Seien p, q Primzahlen und $N = p \cdot q$, $E = (p-1)((q-1)$. Seien e, d natürliche Zahlen, die $ed \equiv 1 \mod E$ erfüllen. Sei weiter M eine zu N teilerfremde Zahl, die zwischen 1 und N liegt. Wähle die ganze Zahl $V(M)$ so, dass sie $V(M) \equiv M^e \mod N$ erfüllt, und die natürliche Zahl K zwischen 1 und N so, dass sie $K \equiv V(M)^d \mod N$ erfüllt. Dann gilt $K = M$.*

Somit hat $\mathcal{B}$ die Nachricht M aus $V(M)$ durch die Rechnung (10) zurückgewonnen.

Bevor ich die Probleme des eben beschriebenen RSA-Verfahrens bespreche, möchte ich ein einfaches Beispiel angeben, anhand dessen man das Vorgehen bei der RSA-Verschlüsselung leicht verfolgen kann.

Ein Beispiel

Die Nachricht:	$M = 72$
Wahl der Primzahlen:	$p = 11$ und $q = 29$
Die Zahlen N, E:	$N = 319$, $E = 280$
Der öffentliche Schlüssel:	$(33, 319)$
Der private Schlüssel:	$(17, 319)$

[6] Vgl. http://de.wikipedia.org/wiki/Euklidischer_Algorithmus (11.11.2009).

Als Erstes muss jetzt $\mathcal{A}$ die Zahl $72^{33} \mod 319$ berechnet werden. Dazu braucht man die große Zahl 72^{33} nicht zu kennen. Man rechnet einfach konsequent modulo 319:

$$72^2 \equiv 80, \quad 72^4 \equiv (72^2)^2 \equiv 80^2 \equiv 20, \quad 72^8 \equiv 81, \qquad \mod 319,$$

$$72^{16} \equiv 181, \quad 72^{32} \equiv 223, \quad 72^{33} \equiv 106 \mod 319.$$

Die verschlüsselte Nachricht ist also $V(M) = 106$. Nach Erhalt muss $\mathcal{B}$ die Zahl $106^{17} \mod 319$ berechnen. In der Tat erhält er $106^{17} \equiv 72 \mod 319$.

Probleme

Nun zu zwei wichtigen Problemen, die mit dem RSA-Kryptosystem verknüpft sind.

Problem 5. *Woher hat $\mathcal{B}$ die Primzahlen?*

Wie im Kapitel „Probleme“ weiter oben geschildert, gibt es heutzutage schnelle Algorithmen zur Primzahlerkennung. Da aber, aus Sicherheitsgründen, für die Verschlüsselung 50- bis 60-stellige Zahlen verwendet werden müssen, ist es doch nicht einfach, genügend viele davon zu generieren. Diesem Bedarf folgend gibt es Firmen, wie zum Beispiel RSA[7], die Primzahlen der entsprechenden Größe verkaufen.

Die wichtigste Frage ist natürlich:

Problem 6. *Wie sicher ist das RSA-Verfahren?*

Hier muss man sagen: Wir wissen es nicht. Verfolgt man die Schritte des RSA-Verfahrens, wie ich es oben geschildert habe, so liegt das zentrale Sicherheitsproblem in der Zahl N, die Teil des öffentlichen Schlüssels ist. Diese Zahl ist Produkt der von $\mathcal{B}$ gewählten Primzahlen p, q, das heißt $N = p \cdot q$. Wäre es möglich, die Primfaktorzerlegung von N in vertretbarer Zeit zu berechnen, wäre der Code geknackt. Das führt uns zurück zu Problem 4. Wir kennen im Moment keine Lösung dieses Problems, wir wissen noch nicht einmal, ob es eine Lösung dafür gibt.

Literatur

GRUNEWALD, F. und M. DUSAUTOY (2006). „Zeta-Functions for groups and rings“, *Proceedings of the ICM (Madrid)*. Zürich, Bd. II., 131–149.

[7] Vgl. http://www.rsa.com (11.11.2009).

ISBN 978-3-940671-33-2