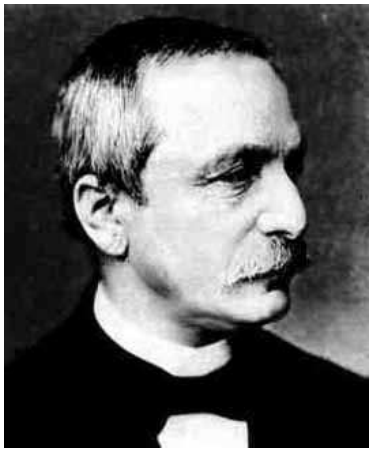
Kapitel 2
Rechnen mit ganzen Zahlen

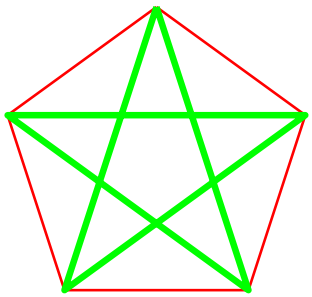
In einen Vortrag bei der Berliner Naturforscher-Versammlung sagte LEOPOLD KRONECKER 1886: „Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.“ In seinem gesamten Werk versuchte er immer wieder, alles auf arithmetische Eigenschaften ganzer Zahlen zurückzuführen.



LEOPOLD KRONECKER (1823–1891) ist heute zwar Vielen nur im Zusammenhang mit dem KRONECKER-δ bekannt, er war aber einer der bedeutendsten deutschen Mathematiker seiner Zeit. Seine Arbeiten befaßten sich mit Algebra, Zahlentheorie und Analysis, wobei er insbesondere die Verbindungen zwischen der Analysis und den beiden anderen Gebieten erforschte. Bekannt ist auch seine Ablehnung jeglicher mathematischer Methoden, die, wie die Mengenlehre oder Teile der Analysis, unendliche Konstruktionen verwenden. Er war deshalb mit vielen anderen bedeutenden Mathematikern seiner Zeit verfeindet, z.B. mit CANTOR und mit WEIERSTRASS.

Auch in der frühen griechischen Mathematik spielten die natürlichen Zahlen eine herausragende Rolle. Zwar ging es dort vor allem um Geometrie, und eine Strecke läßt sich beispielsweise beliebig oft halbieren, was bei natürlichen Zahlen bekanntlich nicht der Fall ist. Schon PYTHAGORAS ($\sim$570–$\sim$510) und seine Schüler versuchten aber stets, zu zwei Strecken ein gemeinsames „Maß“ zu finden, d.h. eine dritte Strecke, von der beide Ausgangsstrecken ganzzahlige Vielfache sind. Einige Gelehrte spekulieren sogar, daß PLATON (428/427–348/347) in seiner (nicht überlieferten) ungeschriebenen Lehre die gesamte Welt der Ideen auf (natürliche) Zahlen zurückführen wollte.

Das Wahrzeichen der Pythagoräer war das Pentagramm, d.h. die Figur aus allen Diagonalen eines regelmäßigen Fünfecks (Pentagons). Um 450 vor Christus erkannte der Pythagoräer HIPPASSOS VON METAPONT, daß es für die Diagonale und die Seite eines Pentagons kein solchen gemeinsames Maß geben konnte, daß es also auch das gibt, was wir heute als irrationale Zahlen bezeichnen. Hier stehen die beiden Streckenlängen im Verhältnis des *goldenen Schnitts,* in Zahlen ausgedrückt $\frac{1}{2}(1+\sqrt{5})$.



Die Mitglieder von PLATONs Akademie interessierten sich nicht für die Lösung von Gleichungen. Praktische Anwendungen der Arithmetik waren für sie etwas Minderwertiges, das nur für Handwerker, Händler und andere Leute, die ihr Geld durch Arbeit verdienen mußten, taugte, und denen war es egal, ob der Weinmenge, den sie verkauften, ein ganzzahliges Vielfaches einer Maßeinheit war oder nicht.

Erst DIOPHANTOS von Alexandrien beschäftigte sich in seinem Buch *Arithmetika* systematisch mit ganzzahligen Lösungen von Gleichungen mit ganzzahligen Koeffizienten; man bezeichnet diese deshalb heute nach ihm als *diophantische Gleichungen.*

Über das Leben von DIOPHANTOS ist praktisch nichts bekannt. Anhand der Daten anderer Autoren, die ihn zitierten *bzw.* die von ihm zitiert wurden, läßt sich *mit Sicherheit* nur sagen, daß sein Werk später als 150 vor Christus und früher als 350 nach Christus entstanden sein muß. Es ist nur teilweise überliefert. Bemerkenswert ist auch, daß er als erster ein eigenes Symbol für eine unbekannte Zahl benutzte. Dieses Symbol war allerdings kein Buchstabe, sondern eine Neuschöpfung.

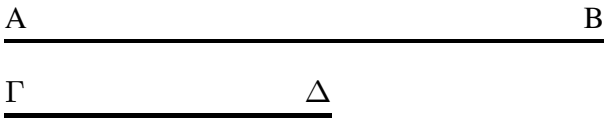
In diesem Kapitel wollen wir zumindest lineare diophantische Gleichungen betrachten sowie einige andere Probleme im Umgang mit ganzen Zahlen. Ausgangspunkt für die meisten Anwendungen ist der aus der Linearen Algebra bekannte EUKLIDische Algorithmus, den wir deshalb kurz wiederholen wollen.

§1: Der Euklidische Algorithmus

Bei EUKLID, in Proposition 2 des siebten Buchs seiner *Elemente,* wird er (in der Übersetzung von CLEMENS THAER in Oswalds Klassikern der exakten Wissenschaft) so beschrieben:

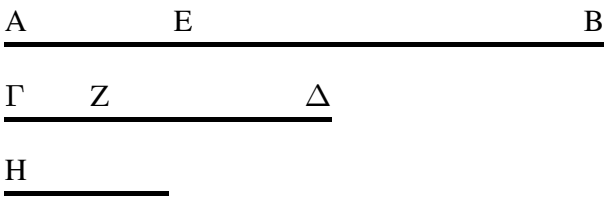
Zu zwei gegebenen Zahlen, die nicht prim gegeneinander sind, ihr größtes gemeinsames Maß zu finden.

Die zwei gegebenen Zahlen, die nicht prim, gegeneinander sind, seien AB, ΓΔ. Man soll das größte gemeinsame Maß von AB, ΓΔ finden.



Wenn ΓΔ hier AB mißt – sich selbst mißt es auch – dann ist ΓΔ gemeinsames Maß von ΓΔ, AB. Und es ist klar, daß es auch das größte ist, denn keine Zahl größer ΓΔ kann ΓΔ messen.

Wenn ΓΔ aber AB nicht mißt, und man nimmt bei AB, ΓΔ abwechselnd immer das kleinere vom größeren weg, dann muß (schließlich) eine Zahl übrig bleiben, die die vorangehende mißt. Die Einheit kann nämlich nicht übrig bleiben; sonst müßten AB, ΓΔ gegeneinander prim sein, gegen die Voraussetzung. Also muß eine Zahl übrig bleiben, die die vorangehende mißt. ΓΔ lasse, indem es BE mißt, EA, kleiner als sich selbst übrig; und EA lasse, indem es ΔZ mißt, ZΓ, kleiner als sich selbst übrig; und ΓZ messe AE.



Da Γ*Z* AE mißt und AE ΔZ, muß ΓZ auch ΔZ messen; es mißt aber auch sich selbst, muß also auch das Ganze ΓΔ messen. ΓΔ mißt aber BE; also mißt ΓZ auch BE; es mißt aber auch EA, muß also auch das Ganze BA messen. Und es mißt auch ΓΔ; ΓZ mißt also AB und ΓΔ; also ist ΓZ gemeinsames Maß von AB, ΓΔ. Ich behaupte, daß es auch das größte ist. Wäre nämlich ΓZ nicht das größte gemeinsame Maß von AB, ΓΔ, so müßte irgendeine Zahl größer ΓZ die Zahlen AB und ΓΔ messen. Dies geschehe; die Zahl sei H. Da H dann ΓΔ mäße und ΓΔ BE mißt, mäße H auch BE; es soll aber auch das Ganze BA messen, müßte also auch den Rest AE messen. AE mißt aber ΔZ; also müßte H auch ΔZ messen; es soll aber auch das Ganze ΔΓ messen, müßte also auch den Rest ΓZ messen, als größere Zahl die kleinere; dies ist unmöglich. Also kann keine Zahl größer ΓZ die Zahlen AB und ΓΔ messen; ΓZ ist also das größte gemeinsame Maß von AB, ΓΔ; dies hatte man beweisen sollen.

Aus heutiger Sicht erscheint die Voraussetzung, daß die betrachteten Größen nicht teilerfremd sein dürfen, seltsam. Sie erklärt sich daraus, daß in der griechischen Philosophie und Mathematik die Einheit eine Sonderrolle einnahm und nicht als Zahl angesehen wurde: Die Zahlen begannen erst mit der Zwei. Dementsprechend führt EUKLID in Proposition 1 des siebten Buchs fast wörtlich dieselbe Konstruktion durch für den Fall von teilerfremden Größen. Schon wenig später wurde die Eins auch in Griechenland als Zahl anerkannt, und für uns heute ist die Unterscheidung ohnehin bedeutungslos. Wir können die Bedingung, daß der ggT ungleich eins sein soll, also einfach ignorieren.

Das dem EUKLIDischen Algorithmus zugrunde liegende Prinzip der *Wechselwegnahme* oder wechselseitigen Subtraktion war in der griechischen Mathematik spätestens gegen Ende des fünften vorchristlichen Jahrhunderts bekannt unter dem Namen Antanairesis (ἀνταναιρεσις) oder auch Anthyphairesis (ἀνθυφαιρεσις); damit bewies bereits HIPPASSOS, daß das Längenverhältnis zwischen der Diagonale und der Seite eines regelmäßigen Fünfecks keine rationale Zahl ist. Auch der Algorithmus selbst geht mit ziemlicher Sicherheit, wie so vieles in den Elementen, *nicht* erst auf EUKLID zurück: Seine *Elemente* waren das wohl mindestens vierte Buchprojekt dieses Namens, und alles spricht dafür, daß er vieles von seinen Vorgängern übernommen hat. Seine Elemente waren dann aber mit Abstand die erfolgreichsten, so daß die anderen in Vergessenheit gerieten und verloren gingen; EUKLID wurde schließlich als *der* Stoichist bekannt nach dem griechischen Titel στοιχεῖα der Elemente.

Es ist nicht ganz sicher, ob EUKLID (Εὐκλειδης) wirklich gelebt hat; es ist möglich, wenn auch sehr unwahrscheinlich, daß EUKLID nur ein Pseudonym für eine Autorengruppe ist. (Das nebenstehende Bild aus dem 18. Jahrhundert ist reine Phantasie.) EUKLID ist vor allem bekannt als Autor der *Elemente,* in denen er die Geometrie seiner Zeit systematisch darstellte und (in gewisser Weise) auf wenige Definitionen sowie die berühmten fünf Postulate zurückführte. Sie entstanden um 300 v. Chr.. EUKLID arbeitete wohl am Museion in Alexandrien. Außer den Elementen schrieb er ein Buch über Optik und weitere, teilweise verschollene Bücher.

Wenn wir nicht mit Zirkel und Lineal arbeiten, sondern rechnen, können wir die mehrfache „Wegnahme“ einer Strecke von einer anderen einfacher beschreiben durch eine Division mit Rest: Sind a und b die (als natürliche Zahlen vorausgesetzten) Längen der beiden Strecken und ist $a : b = q$ Rest r, so kann man q mal die Strecke b von a wegnehmen; was übrig bleibt ist eine Strecke der Länge $r < b$.

EUKLIDs Konstruktion wird dann zu folgendem Algorithmus für zwei natürliche Zahlen a, b:

Schritt 0: Setze $r_0 = a$ und $r_1 = b$.

Schritt i, $i \geq 1$**:** Falls r_i verschwindet, endet der Algorithmus mit $\mathrm{ggT}(a, b) = r_{i-1}$; andernfalls sei r_{i+1} der Rest bei der Division von r_{i-1} durch r_i.

EUKLID behauptet, daß dieser Algorithmus stets endet und daß das Ergebnis der größte gemeinsame Teiler der Ausgangszahlen a, b ist, d.h. die größte natürliche Zahl, die sowohl a als auch b teilt.

Da der Divisionsrest r_{i+1} stets echt kleiner ist als sein Vorgänger r_i und eine Folge immer kleiner werdender nichtnegativer ganzer Zahlen notwendigerweise nach endlich vielen Schritten die Null erreicht, muß der Algorithmus in der Tat stets enden. Daß er mit dem richtigen Ergebnis endet, ist ebenfalls leicht zu sehen, denn im i-ten Schritt ist

$$r_{i-1} = q_i r_i + r_{i+1} \quad \text{oder} \quad r_{i+1} = r_{i-1} - q_i r_i \,,$$

so daß jeder gemeinsame Teiler von r_i und r_{i+1} auch ein Teiler von r_{i-1} ist und umgekehrt jeder gemeinsame Teiler von r_{i-1} und r_i auch r_{i+1} teilt. Somit haben r_i und r_{i-1} dieselben gemeinsamen Teiler wie r_i und r_{i+1}, insbesondere haben sie denselben größten gemeinsamen Teiler. Durch Induktion folgt, daß in jedem Schritt $\mathrm{ggT}(r_i, r_{i-1}) = \mathrm{ggT}(a, b)$ ist. Im letzten Schritt ist $r_i = 0$; da jede natürliche Zahl Teiler der Null ist, ist dann $r_{i-1} = \mathrm{ggT}(r_i, r_{i-1}) = \mathrm{ggT}(a, b)$, wie behauptet.

Mehr als zwei Tausend Jahre nach der Entdeckung von Anthyphairesis und EUKLIDischem Algorithmus, 1624 in Bourg-en-Bresse, modifizierte BACHET DE MÉZIRIAC in der zweiten Auflage seines Buchs *Problèmes*

plaisants et délectables qui se fonts par les nombres den Algorithmus so, daß er zu zwei teilerfremden natürlichen Zahlen a, b zwei weitere natürliche Zahlen x, y konstruiert, für die $ax - by = 1$ ist. Bei ihm heißt das in seiner Proposition XVIII: *Deux nombres premiers entre eux estant donnéz, treuuer le moindre multiple de chascun d'iceux, surpassant de l'unité un multiple de l'autre.* (Für zwei gegebene teilerfremde Zahlen das kleinste Vielfache von jeder der beiden zu finden, das um eins größer ist als ein Vielfaches der anderen.) Er sucht also nicht nur irgendwelche natürlichen Zahlen x, y, sondern verlangt auch noch, daß x minimal ist. (1993 brachte der Verlag Blanchard eine vereinfachte fünfte Auflage heraus, in der so „komplizierte" Dinge wie der Beweis dieser Proposition leider fehlen.)

CLAUDE GASPAR BACHET SIEUR DE MÉZIRIAC (1581-1638) verbrachte den größten Teil seines Lebens in seinem Geburtsort Bourg-en-Bresse. Er studierte bei den Jesuiten in Lyon und Milano und trat 1601 in den Orden ein, trat aber bereits 1602 wegen Krankheit wieder aus und kehrte nach Bourg zurück. Die erste Auflage seines Buchs erschien 1612. Am bekanntesten ist BACHET für seine lateinische Übersetzung der *Arithmetika* von DIOPHANTOS. In einem Exemplar davon schrieb FERMAT seine Vermutung an den Rand. Auch Gedichte von BACHET sind erhalten. 1635 wurde er Mitglied der französischen Akademie der Wissenschaften.

Seine Methode läßt sich leicht verallgemeinern auf den Fall, daß a, b nicht teilerfremd sind: Man muß einfach beide durch ihren ggT teilen und das Ergebnis wieder mit diesem multiplizieren.

Das Verfahren beruht darauf, daß wir bei der Division mit Rest den Divisionsrest als Dividend minus Quotient mal Divisor darstellen; im EUKLIDischen Algorithmus ist also jedes r_i eine ganzzahlige Linearkombination von r_{i-1} und r_{i-2}; indem wir diese Linearkombinationen ineinander einsetzen, erhalten wir den ggT als letzten von null verschiedenen Divisionsrest als ganzzahlige Linearkombination der beiden Ausgangszahlen. Obwohl dies bei EUKLID nicht zu finden ist, redet man heute vom *erweiterten* EUKLID*ischen Algorithmus* oder von der *Identität von* BÉZOUT, benannt nach einem Mathematiker, der das Verfahren

142 Jahre nach BACHET beschrieb und auf Polynome in einer Variablen verallgemeinerte.

ETIENNE BÉZOUT (1730-1783) wurde in Nemours in der Île-de-France geboren, wo seine Vorfahren Magistrate waren. Er ging stattdessen an die Akademie der Wissenschaften und schrieb mehrere Lehrbücher für die Militärausbildung. Im 1766 erschienenen dritten Band (von vier) seines *Cours de Mathématiques à l'usage des Gardes du Pavillon et de la Marine* ist die Identität von BÉZOUT dargestellt. Seine Bücher waren so erfolgreich, daß sie ins Englische übersetzt und als Lehrbücher z.B. in Harvard benutzt wurden. Heute ist er vor allem auch bekannt durch seinen Beweis, daß sich zwei Kurven der Grade n und m ohne gemeinsame Komponenten in höchstens nm Punkten schneiden können.

Formal sieht der erweiterte EUKLIDische Algorithmus folgendermaßen aus:

Schritt 0: Setze $r_0 = a$, $r_1 = b$, $\alpha_0 = \beta_1 = 1$ und $\alpha_1 = \beta_0 = 0$. Für $i = 1$ ist dann

$$r_{i-1} = \alpha_{i-1}a + \beta_{i-1}b \quad \text{und} \quad r_i = \alpha_i a + \beta_i b\,.$$

Im i-ten Schritt werden neue Zahlen berechnet derart, daß diese Gleichungen auch für $i + 1$ gelten:

Schritt i, $i \geq 1$**:** Falls r_i verschwindet, endet der Algorithmus mit

$$\text{ggT}(a, b) = r_{i-1} = \alpha_{i-1}a + \beta_{i-1}b\,.$$

Andernfalls dividiere man r_{i-1} durch r_i; der Divisionsrest sei r_{i+1}. Dann ist

$$\begin{aligned} r_{i+1} = r_{i-1} - q_i r_i &= (\alpha_{i-1}a + \beta_{i-1}b) - q_i(\alpha_i a + \beta_i b) \\ &= (\alpha_{i-1} - q_i\alpha_i)a + (\beta_{i-1} - q_i\beta_i)b\,; \end{aligned}$$

die gewünschten Gleichungen gelten also für

$$\alpha_{i+1} = \alpha_{i-1} - q_i\alpha_i \quad \text{und} \quad \beta_{i+1} = \beta_{i-1} - q_i\beta_i\,.$$

Genau wie oben folgt, daß der Algorithmus für alle natürlichen Zahlen a und b endet und daß am Ende der richtige ggT berechnet wird; außerdem sind die α_i und β_i so definiert, daß in jedem Schritt $r_i = \alpha_i a + \beta_i b$ ist,

insbesondere wird also im letzten Schritt der ggT als Linearkombination der Ausgangszahlen dargestellt.

Dieser Algorithmus liefert sofort ein Verfahren, mit dem wir diophantische Gleichungen der Form $ax + by = c$ mit $a, b, c \in \mathbb{Z}$ für zwei Unbekannte $x, y \in \mathbb{Z}$ lösen können:

Der größte gemeinsame Teiler $d = \text{ggT}(a, b)$ von a und b teilt offensichtlich jeden Ausdruck der Form $ax + by$ mit $x, y \in \mathbb{Z}$; falls d kein Teiler von c ist, kann es also keine ganzzahlige Lösung geben.

Ist aber $c = rd$ ein Vielfaches von d und ist $d = \alpha a + \beta b$ die lineare Darstellung des ggT nach dem erweiterten EUKLIDischen Algorithmus, so haben wir mit $x = r\alpha$ und $y = r\beta$ offensichtlich eine Lösung gefunden.

Ist (x', y') eine weitere Lösung, so ist

$$a(x - x') + b(y - y') = c - c = 0 \quad \text{oder} \quad a(x - x') = b(y' - y)\,.$$

$v = a(x - x') = b(y' - y)$ ist also ein gemeinsames Vielfaches von a und b und damit auch ein Vielfaches des kleinsten gemeinsamen Vielfachen von a und b. Dieses kleinste gemeinsame Vielfache ist ab/d, es muß also eine ganze Zahl m geben mit

$$x - x' = m \cdot \frac{b}{d} \quad \text{und} \quad y' - y = m \cdot \frac{a}{d}\,.$$

Die allgemeine Lösung der obigen Gleichung ist somit

$$x = r\alpha - m \cdot \frac{b}{d} \;\text{ und }\; y = r\beta + m \cdot \frac{a}{d} \quad \text{mit} \quad m \in \mathbb{Z}\,.$$

Als Beispiel betrachten wir eines der Probleme aus dem Buch von BACHET:

Il y a 41 personnes en un banquet tant hommes que femmes et enfants qui en tout dépensent 40 sous, mais chaque homme paye 4 sous, chaque femme 3 sous, chaque enfant 4 deniers. Je demande combien il y a d'hommes, combien de femmes, combien d'enfants.

(Bei einem Bankett sind 41 Personen, Männer, Frauen und Kinder, die zusammen vierzig Sous ausgeben, aber jeder Mann zahlt vier Sous, jede

Frau drei Sous und jedes Kind 4 Deniers. Ich frage, wie viele Männer, wie viele Frauen und wie viele Kinder es sind.)

Sobald man weiß, daß zwölf Deniers ein Sou sind (und zwanzig Sous ein Pfund), kann man dies in ein lineares Gleichungssystem übersetzen: Ist x die Zahl der Männer, y die der Frauen und z die der Kinder, so muß gelten $x + y + z = 41$ und $4x + 3y + \frac{1}{3}z = 40$.

Im Gegensatz zum Fall der in Schule und Linearer Algebra betrachteten linearen Gleichungssystemen kommen hier natürlich nur nichtnegative ganze Zahlen als Lösungen in Frage.

Zur Lösung kann man zunächst die erste Gleichung nach z auflösen und in die zweite Gleichung einsetzen; dies führt auf die Gleichung

$$\frac{11}{3}x + \frac{8}{3}y = \frac{79}{3} \quad \text{oder} \quad 11x + 8y = 79\,.$$

Da elf und acht teilerfremd sind, teilt ihr ggT die rechte Seite; das Problem hat also ganzzahlige Lösungen. Um diese zu finden, müssen wir zunächst den ggT von 11 und 8 als Linearkombination dieser Zahlen darstellen.

Elf durch acht ist eins Rest drei, also ist $3 = 1 \cdot 11 - 1 \cdot 8$.

Im nächsten Schritt dividieren wir acht durch drei mit dem Ergebnis zwei Rest zwei, also ist $2 = 1 \cdot 8 - 2 \cdot 3 = 1 \cdot 8 - 2 \cdot (1 \cdot 11 - 1 \cdot 8) = -2 \cdot 11 + 3 \cdot 8$.

Im letzten Schritt wird daher drei durch zwei dividiert und wir sehen erstens, daß der ggT gleich eins ist (was hier keine Überraschung ist), und zweitens, daß gilt $1 = 3 - 2 = (1 \cdot 11 - 1 \cdot 8) - (-2 \cdot 11 + 3 \cdot 8) = 3 \cdot 11 - 4 \cdot 8$.

Damit haben wir auch eine Darstellung von 79 als Linearkombination von elf und acht:

$$79 = 79 \cdot (3 \cdot 11 - 4 \cdot 8) = 237 \cdot 11 - 316 \cdot 8\,.$$

Dies ist allerdings nicht die gesuchte Lösung: BACHET dachte sicherlich nicht an 237 Männer, -316 Frauen und 119 Kinder.

Nun ist aber die obige Gleichung $1 = 3 \cdot 11 - 4 \cdot 8$ nicht die einzige Möglichkeit zur Darstellung der Eins als Linearkombination von acht

und elf: Da $8 \cdot 11 - 11 \cdot 8$ verschwindet, können wir ein beliebiges Vielfaches dieser Gleichung dazu addieren und bekommen die allgemeinere Lösung

$$(3 + 8k) \cdot 11 - (4 + 11k) \cdot 8 = 1 \, .$$

Entsprechend können wir auch ein beliebiges Vielfaches dieser Gleichung zur Darstellung von 79 addieren:

$$79 = (237 + 8k) \cdot 11 - (316 + 11k) \cdot 8 \, .$$

Wir müssen k so wählen, daß sowohl die Anzahl $237 + 8k$ der Männer als auch die Anzahl $-(316 + 11k)$ der Frauen positiv oder zumindest nicht negativ wird, d.h. $-\frac{237}{8} \leq k \leq -\frac{316}{11}$. Da k ganzzahlig sein muß, kommt nur $k = -29$ in Frage; es waren also fünf Männer, drei Frauen und dazu noch $41 - 5 - 3 = 33$ Kinder. Ihre Gesamtausgaben belaufen sich in der Tat auf $5 \cdot 4 + 3 \cdot 3 + 33 \cdot \frac{1}{3} = 40$ Sous.

Im Beweis, daß der EUKLIDische Algorithmus stets nach endlich vielen Schritten abbricht, hatten wir argumentiert, daß der Divisionsrest stets kleiner ist als der Divisor, so daß er irgendwann einmal null werden muß; dann endet der Algorithmus.

Damit haben wir auch eine obere Schranke für den Rechenaufwand zur Berechnung von $\mathrm{ggT}(a, b)$: Wir müssen höchstens b Divisionen durchführen.

Das erscheint zwar auf den ersten Blick als ein recht gutes Ergebnis; wenn man aber bedenkt, daß der EUKLIDische Algorithmus heute in der Kryptographie auf rund tausendstellige Zahlen angewendet wird, verliert diese Schranke schnell ihre Nützlichkeit: Da unser Universum ein geschätztes Alter von zehn Milliarden Jahren, also ungefähr $3 \cdot 10^{18}$ Sekunden hat, ist klar, daß auch der schnellste heutige Computer, selbst wenn er zu Beginn des Universum zu rechnen begonnen hätte, bis heute nur einen verschwindend kleinen Bruchteil von 10^{1000} Divisionen ausgeführt hätte. Wäre 10^{1000} eine realistische Aufwandsabschätzung, könnten wir an eine Anwendung des EUKLIDischen Algorithmus auf tausendstellige Zahlen nicht einmal denken. Zum Glück fand GABRIEL LAMÉ 1844 eine viel schärfere Schranke, für deren Beweis ich auf

Lehrbücher der Zahlentheorie oder auf das Skriptum meiner Zahlentheorievorlesung verweisen möchte:

Satz von Lamé: Die kleinsten natürlichen Zahlen a, b, für die beim EUKLIDischen Algorithmus $n \geq 2$ Divisionen benötigt werden, sind $a = F_{n+2}$ und $b = F_{n+1}$. Dabei sind die sogenannten FIBONACCI-Zahlen F_n rekursiv definiert durch

$$F_0 = F_1 = 1 \quad \text{und} \quad F_{n+1} = F_n + F_{n-1} \quad \text{für } n \geq 1 \,.$$

(Für $n = 1$ gilt der Satz nur, wenn wir zusätzlich voraussetzen, daß $a \neq b$ ist; für $n \geq 2$ ist dies automatisch erfüllt.)

GABRIEL LAMÉ (1795–1870) studierte von 1813 bis 1817 Mathematik an der Ecole Polytechnique, danach bis 1820 Ingenieurwissenschaften an der Ecole des Mines. Auf Einladung Alexanders I. kam er 1820 nach Rußland, wo er in St. Petersburg als Professor und Ingenieur unter anderem Vorlesungen über Analysis, Physik, Chemie und Ingenieurwissenschaften hielt. 1832 erhielt er einen Lehrstuhl für Physik an der Ecole Polytechnique in Paris, 1852 einen für mathematische Physik und Wahrscheinlichkeitstheorie an der Sorbonne. 1836/37 war er wesentlich am Bau der Eisenbahnlinien Paris-Versailles und Paris–St. Germain beteiligt.

Man kann auch eine geschlossene Formel für die F_n finden; setzt man diese ein, erhält man für $b = F_{n+1}$ mit dem Satz von LAMÉ die Abschätzung

$$\begin{aligned} n &\approx \log_\phi \sqrt{5}\, b - 1 = \log_\phi b + \log_\phi \sqrt{5} - 1 = \frac{\ln b}{\ln \phi} + \frac{\ln \sqrt{5}}{\ln \phi} - 1 \\ &\approx 2{,}078 \ln b + 0{,}672 \,. \end{aligned}$$

Für beliebige Zahlen $a > b$ können nicht mehr Divisionen notwendig sein als für die auf b folgenden nächstgrößeren FIBONACCI-Zahlen, also gibt obige Formel für jedes b eine obere Grenze. Die Anzahl der Divisionen wächst daher nicht (wie oben bei der naiven Abschätzung) wie b, sondern höchstens wie $\log b$. Für tausendstellige Zahlen a, b müssen wir daher nicht mit 10^{1000} Divisionen rechnen, sondern mit weniger als fünf Tausend, was auch mit weniger leistungsfähigen Computern problemlos und schnell möglich ist.

Tatsächlich gibt natürlich auch die hier berechnete Schranke nur selten den tatsächlichen Aufwand wieder; fast immer werden wir mit erheblich weniger auskommen. Im übrigen ist auch alles andere als klar, ob wir den ggT auf andere Weise nicht möglicherweise schneller berechnen können. Da wir aber für Zahlen der Größenordnung, die in heutigen Anwendungen interessieren, selbst mit der Schranke für den schlimmsten Fall ganz gut leben können, sei hier auf diese Fragen nicht weiter eingegangen. Interessenten finden mehr dazu z.B. in den Abschnitten 4.5.2+3 des Buchs
DONALD E. KNUTH: The Art of Computer Programming, *vol. 2:* Seminumerical Algorithms, *Addison-Wesley,* ^{3}1997
Eine deutsche Übersetzung des relevanten Kapitels erschien 2001 bei Springer unter dem Titel *Arithmetik.*

§2: Die multiplikative Struktur der ganzen Zahlen

Eine Primzahl ist bekanntlich eine natürliche Zahl p, die genau zwei Teiler hat, nämlich die Eins und sich selbst; insbesondere ist also $p \neq 1$. Der erweiterte EUKLIDische Algorithmus zeigt eine wichtige Folgerung aus dieser Definition:

Lemma: Wenn eine Primzahl das Produkt $\prod_{i=1}^{n} a_i$ von n natürlichen Zahlen a_i teilt, teilt sie mindestens einen der Faktoren.

Beweis: Für $n = 1$ gibt es nichts zu beweisen.

Für $n = 2$ setzen wir kurz $a_1 = a$ und $a_2 = b$. Falls p ein Teiler von a ist, stimmt die Behauptung. Andernfalls muß der ggT von a und p gleich eins sein, denn er ist ein Teiler von p und ungleich p. Es gibt daher eine Darstellung

$$1 = \alpha a + \beta p \quad \text{mit} \quad \alpha, \beta \in \mathbb{Z}\,.$$

Dann ist $b = \alpha ab + \beta pb$ durch p teilbar, denn sowohl ab also auch pb sind Vielfache von p, was die Behauptung beweist.

Für $n > 2$ beweisen wir die Behauptung induktiv: Angenommen, sie gilt für $n - 1$ und p teilt $\prod_{i=1}^{n} a_i$. Falls p ein Teiler von a_n ist, stimmt die Behauptung; andernfalls muß p wegen des bereits bewiesenen Falls

$n = 2$ ein Teiler von $\prod_{i=1}^{n-1} a_i$ sein und teilt nach Induktionsannahme einen der Faktoren.

■

Eine wichtige Folgerung aus diesem Lemma ist der sogenannte *Hauptsatz der elementaren Zahlentheorie:*

Satz: Jede natürliche Zahl läßt sich bis auf Reihenfolge eindeutig als ein Produkt von Primzahlpotenzen schreiben.

Beweis: Wir zeigen zunächst, daß sich jede natürliche Zahl überhaupt als Produkt von Primzahlpotenzen schreiben läßt. Falls dies nicht der Fall wäre, gäbe es ein minimales Gegenbeispiel M. Dies kann nicht die Eins sein, denn die ist ja das leere Produkt, und es kann auch keine Primzahl sein, denn die ist ja das Produkt mit sich selbst als einzigem Faktor. Somit hat M einen echten Teiler N, d.h. $1 < N < M$.

Da M das minimale Gegenbeispiel war, lassen sich N und $\frac{M}{N}$ als Produkte von Primzahlpotenzen schreiben, also auch $M = N \cdot \frac{M}{N}$.

Bleibt noch zu zeigen, daß die Produktdarstellung bis auf die Reihenfolge der Faktoren eindeutig ist. Auch hier gäbe es andernfalls wieder ein minimales Gegenbeispiel M, das somit mindestens zwei verschiedene Darstellungen

$$M = \prod_{i=1}^{r} p_i^{e_i} = \prod_{j=1}^{s} q_j^{f_j}$$

hätte. Da die Eins durch kein Produkt dargestellt werden kann, in dem wirklich eine Primzahl vorkommt, ist $M > 1$, und somit steht in jedem der beiden Produkte mindestens eine Primzahl.

Da p_1 Teiler von M ist, teilt es auch das rechtsstehende Produkt, also nach dem gerade bewiesenen Lemma mindestens einen der Faktoren, d.h. mindestens ein q_j. Da q_j eine Primzahl ist, muß dann $p_1 = q_j$ sein. Da M als minimales Gegenbeispiel vorausgesetzt war, unterscheiden sich die beiden Produkte, aus denen dieser gemeinsame Faktor gestrichen wurde, höchstens durch die Reihenfolge der Faktoren, und damit gilt dasselbe für die beiden Darstellungen von M.

■

Als erste Anwendung dieses Satzes wollen wir zeigen

Satz: Die reelle Zahl x erfülle die Gleichung

$$x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0 \quad \text{mit} \quad a_i \in \mathbb{Z}\,.$$

Dann ist x entweder ganzzahlig oder irrational.

Beweis: Jede rationale Zahl x kann als Quotient $x = p/q$ zweier zueinander teilerfremder ganzer Zahlen p und q geschrieben werden. Multiplizieren wir die Gleichung

$$\left(\frac{p}{q}\right)^d + a_{d-1}\left(\frac{p}{q}\right)^{d-1} + \cdots + a_1\left(\frac{p}{q}\right) + a_0 = 0$$

mit q^d, erhalten wir die nennerlose Gleichung

$$p^d + a_{d-1}p^{d-1}q + \cdots + a_1 pq^{d-1} + a_0 q^d = 0\,.$$

Auflösen nach p^d führt auf

$$\begin{aligned} p^d &= -a_{d-1}p^{d-1}q - \cdots - a_1 pq^{d-1} - a_0 q^d \\ &= q\cdot(-a_{n-1}p^{n-1} - \cdots - a_1 pq^{n-2} - a_0 q^{n-1})\,, \end{aligned}$$

d.h. q muß ein Teiler von p^d sein, was wegen der Eindeutigkeit der Primfaktorzerlegung von p^d sowie der vorausgesetzten Teilerfremdheit von p und q nur für $q = \pm 1$ der Fall sein kann. Somit ist x eine ganze Zahl, wie behauptet. ∎

Insbesondere ist also eine n-te Wurzel einer natürlichen Zahl entweder ganzzahlig oder irrational.

Als Übungsaufgabe kann man mit der Beweismethode des obigen Satzes zusammen mit unserem früheren Ergebnis, wonach ganzzahlige Nullstellen ganzzahliger Polynome den konstanten Koeffizienten teilen müssen, leicht ein Verfahren zur Bestimmung rationaler Lösungen durch Probieren herleiten: Ist eine rationale Lösung der Gleichung

$$a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 = 0 \quad \text{mit} \quad a_i \in \mathbb{Z}\,,$$

so ist bei einer Darstellung von x als gekürztem Bruch der Nenner ein Teiler von a_d und der Zähler teilt a_0.

§3: Die Verteilung der Primzahlen

Nachdem wir wissen, daß jede natürliche Zahl als Produkt von Primzahlpotenzen darstellbar ist, stellt sich als nächstes die Frage, wie viele Primzahlen es gibt. Die Antwort finden wir schon in EUKLIDs Elementen; der dort gegebene Beweis dürfte immer noch der einfachste sein: Es gibt unendlich viele Primzahlen, denn gäbe es nur endlich viele Primzahlen $p_1, \ldots, p_n$, so könnten wir deren Produkt P bilden und die Primzerlegung von $P+1$ betrachten. Da P durch alle p_i teilbar ist, kann $P+1$ durch kein p_i teilbar sein. Andererseits ist natürlich auch $P+1$ als Produkt von Primzahlpotenzen darstellbar; also muß es außer $p_1, \ldots, p_n$ noch weitere Primzahlen geben, im Widerspruch zur Annahme.

Um nicht ganz auf dem Stand von vor rund zweieinhalb Jahrtausenden stehen zu bleiben, wollen wir uns noch einen zweiten, auf EULER zurückgehenden Beweis ansehen.

Dazu betrachten wir für eine reelle Zahl $s > 1$ die unendliche Reihe

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

Als erstes müssen wir uns überlegen, daß diese Reihe konvergiert. Da alle Summanden positiv sind, müssen wir dafür nur zeigen, daß es eine gemeinsame obere Schranke für alle Teilsummen gibt. Da die Funktion $x \mapsto 1/x^s$ für $x > 0$ monoton fallend ist, haben wir für $n-1 \le x \le n$ die Abschätzung $1/n^s \le 1/x^s$, d.h.

$$\sum_{n=1}^{N} \frac{1}{n^s} = 1 + \sum_{n=2}^{N} \frac{1}{n^s} \le 1 + \int_1^N \frac{dx}{x^s}$$

$$< 1 + \int_1^{\infty} \frac{dx}{x^s} = 1 + \frac{1}{s-1} = \frac{s}{s-1} \, .$$

Somit ist $\zeta(s)$ für alle $s > 1$ wohldefiniert.

Einen Zusammenhang mit Primzahlen liefert der folgende

Satz: *a)* Für $s > 1$ ist $\zeta(s) = \prod_{p \text{ prim}} \frac{1}{1 - \frac{1}{p^s}}$.

b) Für alle $N \in \mathbb{N}$ und alle reellen $s > 0$ ist $\sum_{n=1}^{N} \frac{1}{n^s} \leq \prod_{\substack{p \leq N \\ p \text{ prim}}} \frac{1}{1 - \frac{1}{p^s}}$.

Beweis: Wir beginnen mit *b).* Für $N = 1$ steht hier die triviale Formel $1 \leq 1$; sei also $N \geq 2$, und seien $p_1, \ldots, p_r$ die sämtlichen Primzahlen kleiner oder gleich N. Nach der Summenformel für die geometrische Reihe ist

$$\frac{1}{1 - \frac{1}{p_k^s}} = \sum_{\ell=0}^{\infty} \frac{1}{p_k^{\ell s}} ,$$

und das Produkt der rechtsstehenden Reihen über $k = 1$ bis r ist wegen der Eindeutigkeit der Primzerlegung die Summe über alle jene $1/n^s$, für die n keinen Primteiler größer N hat. Darunter sind insbesondere alle $n \leq N$, womit *b)* bewiesen wäre.

Die Differenz zwischen $\zeta(s)$ und dem Produkt auf der rechten Seite von *b)* ist gleich der Summe über alle $1/n^s$, für die n mindestens einen Primteiler größer N haben. Diese Summe ist natürlich höchstens gleich der Summe aller $1/n^s$ mit $n > N$, und die geht wegen der Konvergenz von $\zeta(s)$ gegen null für $N \to \infty$. Damit ist auch *a)* bewiesen. ∎

Auch daraus folgt, daß es unendlich viele Primzahlen gibt: Gäbe es nämlich nur endlich viele, so stünde auf der rechten Seite von *b)* für jedes hinreichend große N das Produkt über die *sämtlichen* Primzahlen. Da es nur endlich viele Faktoren hat, wäre es auch für $s = 1$ endlich, und damit müßte

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

kleiner oder gleich dieser Zahl sein, im Widerspruch zur Divergenz der harmonischen Reihe.

Verglichen mit dem Beweis aus EUKLIDs Elementen ist EULERs Methode erheblich komplizierter. Um trotzdem ihre Existenzberechtigung

zu haben, sollte sie uns daher auch mehr Informationen liefern. In welchem Maße sie dies tatsächlich leistet, geht wahrscheinlich sogar noch deutlich über alles hinaus, was EULER seinerzeit träumen konnte.

Zunächst einmal können wir Teil *b)* für $s = 1$ zu einer quantitativen Abschätzung bezüglich der Anzahl $\pi(N)$ der Primzahlen kleiner oder gleich N umformulieren: Wie oben im Konvergenzbeweis für $\zeta(s)$ können wir aus der Monotonie der Funktion $x \mapsto 1/x$ folgern, daß für alle $N \in \mathbb{N}$ gilt

$$\log(N+1) = \int_1^{N+1} \frac{dx}{x} < \sum_{n=1}^{N} \frac{1}{n} < 1 + \int_1^{N} \frac{dx}{x} = 1 + \log N \, .$$

Zur Abschätzung der linken Seite beachten wir einfach, daß der Faktoren $1/(1-1/p)$ für $p = 2$ gleich zwei ist, ansonsten aber kleiner. Somit ist

$$\log(N+1) < \sum_{n=1}^{N} \frac{1}{n} \leq \prod_{\substack{p \leq N \\ p \text{ prim}}} \frac{1}{1-\frac{1}{p}} \leq 2^{\pi(N)}$$

und damit

$$\pi(N) \geq \frac{\log\log(N+1)}{\log 2} \, .$$

Wie wir bald sehen werden, ist das allerdings eine sehr schwache Abschätzung.

EULERs Methode erlaubt uns auch, die Dichte der Primzahlen zu vergleichen mit der Dichte beispielsweise der Quadratzahlen: Wie wir oben gesehen haben, konvergiert $\zeta(s)$ für alle $s > 1$, insbesondere also konvergiert die Summe $\zeta(2)$ der inversen Quadratzahlen. EULER konnte mit seiner Methode zeigen, daß die Summe der inversen Primzahlen *divergiert,* so daß die Primzahlen zumindest in diesem Sinne dichter liegen als die Quadratzahlen und alle anderen Potenzen mit (reellem) Exponenten $s > 1$.

Zum Beweis fehlt uns nur noch eine Analysis I Übungsaufgabe: Wir wollen uns überlegen, daß für alle $0 \leq x \leq \frac{1}{2}$ gilt $(1-x) \geq 4^{-x}$. An den Intervallenden stimmen beide Funktionen überein, und $1-x$ ist eine lineare Funktion. Es reicht daher, wenn wir zeigen, daß 4^{-x} eine

konvexe Funktion ist, daß also ihre zweite Ableitung überall im Intervall positiv ist. Das ist aber klar, denn die ist einfach $\log(4)^2 \cdot 4^{-x}$. Für jede Primzahl p ist daher

$$1 - \frac{1}{p} \geq 4^{-1/p} \quad \text{und} \quad \frac{1}{1 - \frac{1}{p}} \leq 4^{1/p} \, .$$

Zusammen mit der vorigen Abschätzung folgt

$$\log(N+1) < \prod_{\substack{p \leq N \\ p \text{ prim}}} \frac{1}{1 - \frac{1}{p}} \leq \prod_{\substack{p \leq N \\ p \text{ prim}}} 4^{1/p} = 4^{\sum \frac{1}{p}} \, ,$$

wobei die Summe im Exponenten über alle Primzahlen $p \leq N$ geht. Da $\log(N+1)$ für $N \to \infty$ gegen unendlich geht, muß somit auch die Summe der inversen Primzahlen divergieren.

Mit diesen Bemerkungen fängt allerdings die Nützlichkeit der Funktion $\zeta(s)$ für das Verständnis der Funktion $\pi(N)$ gerade erst an: Ein Jahrhundert nach EULER erkannte RIEMANN, daß die Funktion $\zeta(s)$ ihre wahre Nützlichkeit für das Studium von $\pi(N)$ erst zeigt, wenn man sie auch für komplexe Argumente s betrachtet. Jeder, der sich ein bißchen mit Funktionen einer komplexer Veränderlichen auskennt, kann leicht zeigen, daß $\zeta(s)$ auch für komplexe Zahlen mit Realteil größer ein konvergiert: Der Imaginärteil des Exponenten führt schließlich nur zu einem Faktor vom Betrag eins.

GEORG FRIEDRICH BERNHARD RIEMANN (1826-1866) war Sohn eines lutherischen Pastors und schrieb sich 1946 auf Anraten seines Vaters an der Universität Göttingen für das Studium der Theologie ein. Schon bald wechselte an die Philosophische Fakultät, um dort unter anderem bei GAUSS Mathematikvorlesungen zu hören. Nach Promotion 1851 und Habilitation 1854 erhielt er dort 1857 einen Lehrstuhl. Trotz seines frühen Todes initiierte er grundlegende auch noch heute fundamentale Entwicklungen in der Geometrie, der Zahlentheorie und über abelsche Funktionen. Wie sein Nachlaß zeigte, stützte er seine 1859 aufgestellte Vermutung über die Nullstellen der ζ-Funktion auf umfangreiche Rechnungen.

RIEMANNs wesentliche Erkenntnis war, daß sich $\zeta(s)$ fortsetzen läßt zu einer analytischen Funktion auf der gesamten Menge der komplexen Zahlen mit Ausnahme der Eins (wo die ζ-Funktion wegen der Divergenz der harmonischen Reihe keinen endlichen Wert haben kann).

Für Leser, die nicht mit dem Konzept der analytischen Fortsetzung vertraut sind, möchte ich ausdrücklich darauf hinweisen, daß dies selbstverständlich nicht bedeutet, daß die definierende Summe der ζ-Funktion für reelle Zahlen kleiner eins oder komplexe Zahlen mit Realteil kleiner oder gleich eins konvergiert: Analytische Fortsetzung besteht darin, daß eine differenzierbare Funktion (die im Komplexen automatisch beliebig oft differenzierbar ist und um jeden Punkt in eine TAYLOR-Reihe entwickelt werden kann) via TAYLOR-Reihen über ihren eigentlichen Definitionsbereich hinweg ausgedehnt wird. Man kann beispielsweise zeigen, das $\zeta(-1) = -\frac{1}{12}$ ist. Setzt man $s = -1$ in die für $s > 1$ gültige Reihe ein, erhält man die Summe aller natürlicher Zahlen, die selbstverständlich nicht gleich $-\frac{1}{12}$ ist, sondern divergiert. Entsprechend hat $\zeta(s)$ Nullstellen bei allen geraden negativen Zahlen, obwohl auch hier die entsprechenden Reihen divergieren. Diese Nullstellen bezeichnet man als die sogenannten *trivialen* Nullstellen der ζ-Funktion, da sie sich sofort aus einer bei der Konstruktion der analytischen Fortsetzung zu beweisenden Funktionalgleichung ablesen lassen. Für die Primzahlverteilung spielen vor allem die übrigen, die sogenannten nichttrivialen Nullstellen, eine große Rolle.

Wie wir gerade gesehen haben, liegen die Primzahlen zumindest in einem gewissen Sinne dichter als die Quadratzahlen. Zur Einstimmung auf das Problem der Primzahlverteilung wollen wir uns kurz mit der (deutlich einfacheren) Verteilung der Quadratzahlen beschäftigen.

Die Folge der Abstände zwischen zwei aufeinanderfolgenden Quadratzahlen ist einfach die Folge der ungeraden Zahlen, denn

$$(n+1)^2 - n^2 = 2n + 1 \,.$$

Zwei aufeinanderfolgende Quadratzahlen $Q < Q'$ haben daher die Differenz $Q' - Q = 2\sqrt{Q} + 1$.

Bei den Primzahlen ist die Situation leider sehr viel unübersichtlicher: EULER meinte sogar, die Verteilung der Primzahlen sei ein Geheimnis,

das der menschliche Verstand nie erfassen werde. Der kleinstmögliche Abstand zwischen zwei verschiedenen Primzahlen ist offensichtlich eins, der Abstand zwischen zwei und drei. Er kommt nur an dieser einen Stelle vor, denn außer der Zwei sind schließlich alle Primzahlen ungerade.

Der Abstand zwei ist schon deutlich häufiger: Zwei ist beispielsweise der Abstand zwischen drei und fünf, aber auch der zwischen den Primzahlen $10^{100} + 35737$ und $10^{100} + 35739$. Das größte derzeit bekannte Beispiel bilden die im September 2016 im Rahmen von PrimeGrid (www.primegrid.com) gefundenen beiden Zahlen

$$2\,996\,863\,034\,895 \cdot 2^{1290000} \pm 1 \,.$$

Seit langer Zeit wird vermutet, daß es unendlich viele solcher *Primzahlzwillinge* gibt; experimentelle Untersuchungen deuten sogar darauf hin, daß ihre Dichte für Zahlen der Größenordnung n bei ungefähr $1 : (\log n)^2$ liegen sollte, aber bislang konnte noch niemand auch nur beweisen, daß es unendlich viele gibt.

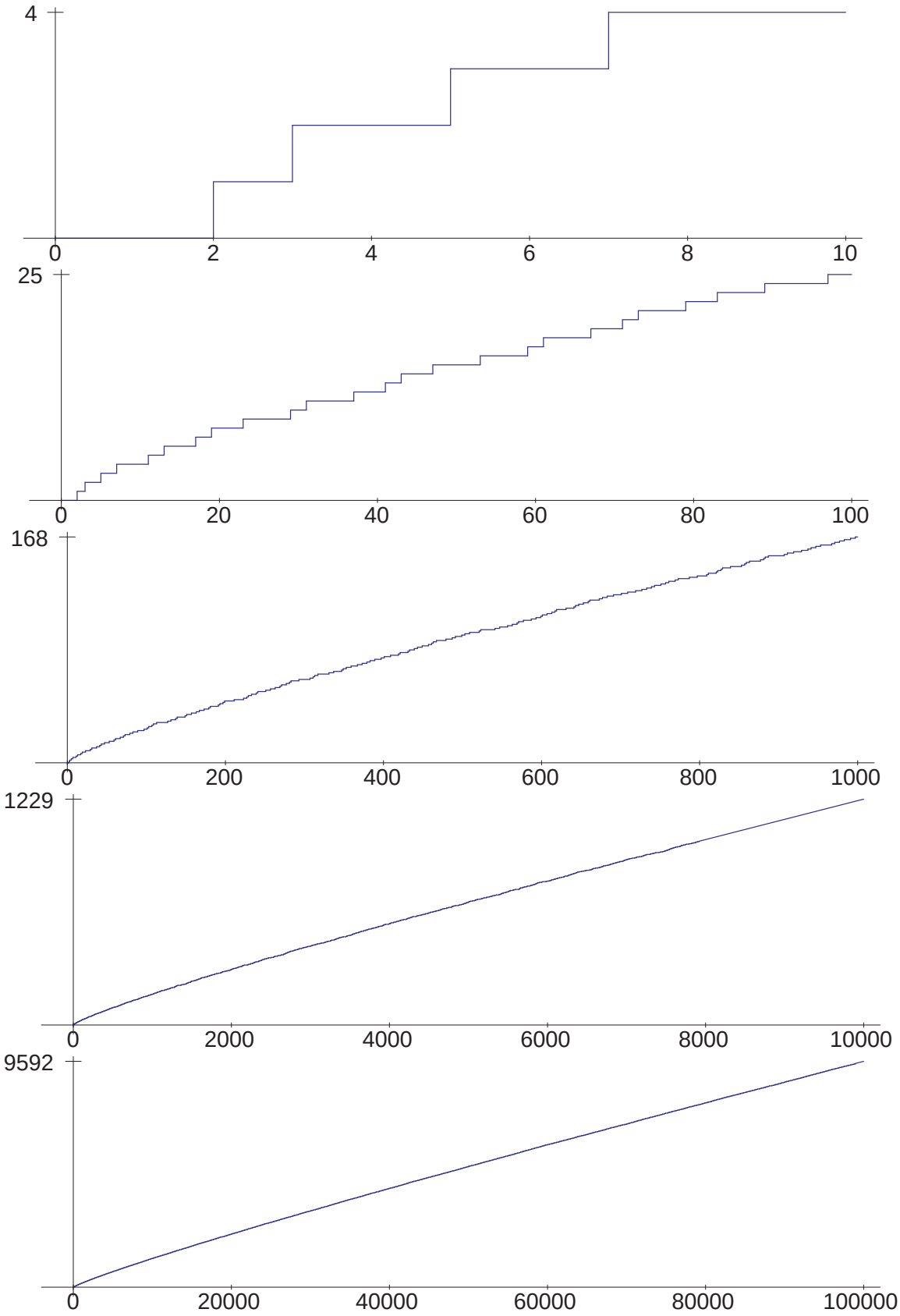
Eine obere Grenze für den Abstand zwischen zwei aufeinanderfolgenden Primzahlen gibt es genauso wenig wie bei den Quadratzahlen: Ist $n \geq 2$ und $2 \leq i \leq n$, so ist die Zahl $n! + i$ durch i teilbar und somit keine Primzahl. Der Abstand zwischen der größten Primzahl kleiner oder gleich $n! + 1$ und ihrem Nachfolger ist somit mindestens n.

Um einen ersten Eindruck von der Verteilung der Primzahlen zu bekommen, betrachten wir den Graphen der Funktion

$$\pi\colon \begin{cases} \mathbb{R}_{>0} \to \mathbb{N}_0 \\ \quad x \mapsto \text{Anzahl der Primzahlen} \leq x \end{cases} .$$

Die Abbildungen auf der vorigen Seite zeigen ihn für die Intervalle von null bis 10^i für $i = 1, \ldots, 5$. Wie man sieht, werden die Graphen immer glatter, und bei den beiden letzten Bilder könnte man glauben, es handle sich um den Graphen einer differenzierbaren Funktion; daher auch die Schreibweise $\pi(x)$ statt – wie bisher – $\pi(N)$.

Auf den ersten Blick sieht diese Funktion fast linear aus.; sieht man sich allerdings die Zahlenwerte genauer an, so sieht man schnell, daß


4
0
2
4
6
8
10
25
0
20
40
60
80
100
168
0
200
400
600
800
1000
1229
0
2000
4000
6000
8000
10000
9592
0
20000
40000
60000
80000
100000

$\pi(x)$ etwas langsamer wächst als eine lineare Funktion; die Funktion $x/\log x$ ist eine deutlich bessere Approximation. In der Tat können wir auch mit unseren sehr elementaren Mitteln eine entsprechende Aussage beweisen:

Satz: Es gibt Konstanten $c_1, c_2 > 0$, so daß gilt:

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x} \, .$$

Beweis: Wir betrachten die neue Funktion

$$\vartheta(x) = \sum_{p \le x} \log p \, ,$$

wobei ein Summationsindex p hier wie stets in diesem Beweis bedeuten soll, daß wir über alle *Primzahlen* mit der jeweils angegebenen Eigenschaft summieren.

Dann ist einerseits

$$\pi(x) = \sum_{p \le x} \frac{\log p}{\log p} \ge \sum_{p \le x} \frac{\log p}{\log x} = \frac{\vartheta(x)}{\log x} \, ,$$

andererseits ist

$$\begin{aligned} \vartheta(x) = \sum_{p \le x} \log p &\ge \sum_{\sqrt{x} < p \le x} \log p > \log\left(\sqrt{x}\right) \left(\pi(x) - \pi\left(\sqrt{x}\right) \right) \\ &= \frac{1}{2} \log(x) \left(\pi(x) - \pi\left(\sqrt{x}\right) \right) \end{aligned}$$

und damit auch $\pi(x) < \dfrac{2\vartheta(x)}{\log x} + \pi\left(\sqrt{x}\right) < \dfrac{2\vartheta(x)}{\log x} + \sqrt{x}$. Wenn wir also zeigen können

1. Es gibt Konstanten $c_1, c_3 > 0$, so daß $c_1 x < \vartheta(x) < c_3 x$
2. $\displaystyle\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$,

dann folgt die Behauptung des Satzes.

Zum Beweis der ersten Aussage betrachten wir die Primzerlegung

$$n! = \prod_{p \le n} p^{e_p}$$

von $n!$. Unter den natürlichen Zahlen bis n sind $\left[\frac{n}{p}\right]$ durch p teilbar, $\left[\frac{n}{p^2}\right]$ durch p^2, *usw.;* daher ist

$$e_p = \sum_{k\geq 1} \left[\frac{n}{p^k}\right] \quad \text{und} \quad \log n! = \sum_{p\leq n} e_p \log p = \sum_{p\leq n} \sum_{k\geq 1} \left[\frac{n}{p^k}\right] \log p\,.$$

Die Summanden mit $k > 1$ liefern dabei nur einen kleinen Beitrag:

$$\sum_{p\leq n} \sum_{k\geq 2} \left[\frac{n}{p^k}\right] \log p \leq \sum_{p\leq n} \left(\log p \cdot \sum_{k\geq 2} \frac{n}{p^k} \right) = n \sum_{p\leq n} \frac{\log p}{p(p-1)}$$

nach der Summenformel für die geometrische Reihe:

$$\sum_{k\geq 2} \frac{1}{p^k} = \frac{1}{p^2} \cdot \frac{1}{1-\frac{1}{p}} = \frac{1}{p^2-p} = \frac{1}{p(p-1)}\,.$$

Zur weiteren Abschätzung ersetzen wir die Summe über alle Primzahlen kleiner oder gleich n durch die Summe über alle Zahlen bis n und beachten, daß für reellen $x \geq 2$ gilt $\log x < \sqrt{x}$, also

$$\frac{\log x}{x(x-1)} < \frac{\sqrt{x}}{x^2} = \frac{1}{x^{3/2}} \quad \text{und damit folgt}$$

$$\sum_{p\leq n} \frac{\log p}{p(p-1)} \leq \sum_{i=2}^{n} \frac{\log i}{i(i-1)} \leq \sum_{i=2}^{n} \frac{1}{i^{3/2}}\,.$$

Da $\sum_{i=1}^{\infty} \frac{1}{i^s}$ für alle $s > 1$ konvergiert, konvergiert die rechts stehende Summe für $n \to \infty$ gegen einen endlichen Wert (ungefähr 1,612375), ist also $O(1)$, und damit ist $\sum_{k\geq 2} \frac{1}{p^k} = O(n)$. Setzen wir dies in die Formel für $\log n!$ ein, erhalten wir nach allen bislang bewiesenen Abschätzungen, daß

$$\log n! = \sum_{p\leq n} \left[\frac{n}{p}\right] \log p + O(n)\,.$$

Dies können wir vergleichen mit der STIRLINGschen Formel

$$\log n! = n \log n - n + O(\log n)\,,$$

deren Beweis für Leser, die ihn noch nicht kennen, im Anhang zu diesem Paragraphen skizziert ist. Kombinieren wir dies mit der gerade bewiesenen Formel, ist also

$$\sum_{p\le n} \left[\frac{n}{p}\right] \log p = n \log n + O(n)\,. \qquad (*)$$

Damit ist

$$\begin{aligned}\textstyle\sum_{p\le 2n} \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) \log p &= 2n\log 2n - 2n\log n + O(2n)\\ &= 2n\log 2 + O(n) = O(n)\,.\end{aligned}$$

Hier ist $\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]$ stets entweder null oder eins; speziell für die Primzahlen p mit $n < p < 2n$ ist $\left[\frac{n}{p}\right] = 0$ und $\left[\frac{2n}{p}\right] = 1$. Somit ist

$$\vartheta(2n) - \vartheta(n) = \sum_{n<p<2n} \log p \le \sum_{p\le 2n} \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) \log p = O(n)\,.$$

Die Formel $\vartheta(2n) - \vartheta(n) = O(n)$ bleibt gültig, wenn wir n durch eine reelle Zahl x ersetzen; somit ist

$$\vartheta(x) = \sum_{i=0}^{\infty} \left(\vartheta\Big(\frac{x}{2^i}\Big) - \vartheta\Big(\frac{x}{2^{i+1}}\Big)\right) = O\left(\sum_{i=0}^{\infty} \frac{x}{2^i}\right) = O(x)\,,$$

womit die obere Schranke für $\vartheta(x)$ bewiesen wäre.

Bevor wir uns der unteren Schranke zuwenden, beweisen wir zunächst die zweite Aussage. Natürlich ist $\frac{n}{p} = \left[\frac{n}{p}\right] + O(1)$, also ist nach $(*)$

$$\begin{aligned}\sum_{p\le n} \frac{n}{p} \log p &= \sum_{p\le n} \left[\frac{n}{p}\right] \log p + O\left(\sum_{p\le n} \log p\right)\\ &= n\log n + O(n) + O\big(\vartheta(n)\big) = n\log n + O(n)\,,\end{aligned}$$

denn wie wir gerade gesehen haben ist $\vartheta(n) = O(n)$. Kürzen wir die obige Formel durch n, erhalten wir die gewünschte Aussage

$$\sum_{p\le n} \frac{\log p}{p} = \log n + O(1)\,,$$

die natürlich auch dann gilt, wenn wir n durch eine reelle Zahl x ersetzen: Der Term $O(1)$ schluckt alle dabei auftretenden zusätzlichen Fehler.

Für $0 < \alpha < 1$ ist daher

$$\sum_{\alpha x < p \le x} \frac{\log p}{p} = \log x - \log \alpha x + O(1) = \log \frac{1}{\alpha} + O(1)\,,$$

wobei der Fehlerterm $O(1)$ nicht von α abhängt.

Da $\log \frac{1}{\alpha}$ für $\alpha \to 0$ gegen ∞ geht, ist für hinreichend kleine Werte von α und $x > c/\alpha$ für irgendein $c > 2$ beispielsweise

$$\sum_{\alpha x < p \le x} \frac{\log p}{p} > 10\,,$$

und für solche Werte von α und c ist dann

$$10 < \sum_{\alpha x < p \le x} \frac{\log p}{p} < \frac{1}{\alpha x} \sum_{\alpha x < p \le x} \log p \le \frac{\vartheta(x)}{\alpha x}\,.$$

Somit ist $10\alpha x < \vartheta(x)$, womit auch die untere Schranke aus der ersten Behauptung bewiesen wäre und damit der gesamte Satz. ∎

Der bewiesene Satz ist nur ein schwacher Abglanz dessen, was über die Funktion $\pi(x)$ bekannt ist. Zum Abschluß des Kapitels seien kurz einige der wichtigsten bekannten und vermuteten Eigenschaften von $\pi(x)$ zusammengestellt. Diese knappe Übersicht folgt im wesentlichen dem Artikel *Primzahlsatz* aus

> DAVID WELLS: Prime Numbers – The Most Mysterious Figures in Math, *Wiley,* 2005,

einer Zusammenstellung im Lexikonformat von interessanten Tatsachen und auch bloßen Kuriosa aus dem Umkreis der Primzahlen.

GAUSS kam 1792, im Alter von 15 Jahren also, durch seine Experimente zur Vermutung, daß $\pi(x)$ ungefähr gleich dem sogenannten *Integrallogarithmus* von x sein sollte:

$$\pi(x) \approx \mathrm{Li}(x) \underset{\text{def}}{=} \int_2^x \frac{d\xi}{\log \xi}\,.$$

Auch LEGENDRE versuchte, $\pi(x)$ anhand experimenteller Daten anzunähern. Er stellte dazu eine Liste aller Primzahlen bis 400 000 zusammen, das sind immerhin 33 860 Stück, und suchte eine glatte Kurve, die den Graphen von π möglichst gut annähert. In seinem 1798 erschienenen Buch *Essai sur la théorie des nombres* gab er sein Ergebnis an als

$$\pi(x) \approx \frac{x}{\log x - 1{,}08366} .$$

Über ein halbes Jahrhundert später gab es den ersten Beweis einer Aussage: PAFNUTIJ L'VOVIČ ČEBYŠĒV (1821–1894), in der Numerik meist bekannt in der Schreibweise TSCHEBYTSCHEFF, zeigte 1851: *Falls* der Grenzwert

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x}$$

existiert, muß er den Wert eins haben.

1852 bewies er dann ein deutlich schärferes Resultat: Für *hinreichend große* Werte von x ist

$$c_1 \cdot \frac{x}{\log x} < \pi(x) < c_2 \cdot \frac{x}{\log x} \quad \text{mit} \quad c_1 \approx 0{,}92 \ \text{ und } \ c_2 \approx 1{,}105 .$$

1896 schließlich zeigten der französische Mathematiker JACQUES SALOMON HADAMARD (1865–1963) und sein belgischer Kollege CHARLES JEAN GUSTAVE NICOLAS BARON DE LA VALLÉE POUSSIN (1866–1962) unabhängig voneinander die Aussage, die heute als **Primzahlsatz** bekannt ist:

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

Dies bedeutet nun freilich nicht, daß damit die Formeln von GAUSS und von LEGENDRE überflüssig wären: Die Tatsache, daß der Quotient zweier Funktionen asymptotisch gleich eins ist, erlaubt schließlich immer noch beträchtliche Unterschiede zwischen den beiden Funktionen: Nur der *relative* Fehler muß gegen null gehen.

Offensichtlich ist für jedes $a \in \mathbb{R}$

$$\lim_{x\to\infty} \frac{x/\log x}{x/(\log x - a)} = \lim_{x\to\infty} \frac{\log x - a}{\log x} = 1 - \lim_{x\to\infty} \frac{a}{\log x} = 1 ,$$

und es ist auch nicht schwer zu zeigen, daß $\lim\limits_{x\to\infty} \dfrac{x/\log x}{\mathrm{Li}(x)} = 1$ ist. Nach dem Primzahlsatz ist daher auch für jedes $a \in \mathbb{R}$

$$\pi(x) \sim \frac{x}{\log x - a} \quad \text{und} \quad \pi(x) \sim \mathrm{Li}(x)\,.$$

Wie DE LA VALLÉE POUSSIN zeigte, liefert der Wert $a = 1$ unter allen reellen Zahlen a die beste Approximation an $\pi(x)$, aber $\mathrm{Li}(x)$ liefert eine noch bessere Approximation. Für kleine Werte von x sieht man das auch in der folgenden Tabelle, in der alle reellen Zahlen zur nächsten ganzen Zahl gerundet sind. Wie kaum anders zu erwarten, liefert LEGENDREs Formel für 10^4 und 10^5 die besten Werte:

n	$\pi(n)$	$\frac{n}{\log n}$	$\frac{n}{\log n-1}$	$\frac{n}{\log n-1{,}08366}$	$\mathrm{Li}(n)$
10^3	168	145	169	172	178
10^4	1 229	1 086	1 218	1 231	1 246
10^5	9 592	8 686	9 512	9 588	9 630
10^6	78 489	72 382	78 030	78 534	78 628
10^7	664 579	620 420	661 459	665 138	664 918
10^8	5 761 455	5 428 681	5 740 304	5 769 341	5 762 209
10^9	50 847 478	48 254 942	50 701 542	50 917 519	50 849 235

Wenn wir genaue Aussagen über $\pi(x)$ machen wollen, sollten wir also etwas über die Differenz $\mathrm{Li}(x) - \pi(x)$ wissen. Hier kommen wir in das Reich der offenen Fragen, und nach derzeitigem Verständnis hängt alles ab von der oben erwähnten RIEMANNschen Zetafunktion. Nach einer berühmten Vermutung von RIEMANN haben alle nichttrivialen Nullstellen von $\zeta(s)$ den Realteil ein halb. Falls dies stimmt, ist

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x}\log x)\,.$$

Die RIEMANNsche Vermutung ist eines der wichtigsten ungelösten Probleme der heutigen Mathematik; sie war 1900 eines der HILBERTschen Probleme und ist auch eines der sieben *Millennium problems,* für deren Lösung das CLAY Mathematics Institute in Cambridge, Mass. 2000 einen Preis von jeweils einer Million Dollar ausgesetzt hat; für Einzelheiten siehe `http://www.claymath.org/millennium/` .

Anhang: Die Eulersche Summenformel und die Stirlingsche Formel

Die EULERsche Summenformel erlaubt es, eine endliche Summe auf ein Integral zurückzuführen und dadurch in vielen Fällen erst rechnerisch handhabbar zu machen. Wir betrachten eine reellwertige differenzierbare Funktion f, deren Definitionsbereich das Intervall $[1,\, n]$ enthält.

Für eine reelle Zahl x bezeichnen wir weiterhin mit $[x]$ die größte ganze Zahl kleiner oder gleich x; außerdem führen wir noch die Bezeichnung $\{x\} \underset{\text{def}}{=} x - [x]$ ein für den gebrochenen Anteil von x. Für eine ganze Zahl k ist somit $\{x\} = x - k$ für alle x aus dem Intervall $[k,\, k+1)$.

Partielle Integration führt auf die Gleichung

$$\int_k^{k+1} \big(\{x\} - \tfrac{1}{2}\big) f'(x)\, dx = \big(x - k - \tfrac{1}{2}\big) f(x) \Big|_k^{k+1} - \int_k^{k+1} f(x)\, dx$$

$$= \frac{f(k+1) + f(k)}{2} - \int_k^{k+1} f(x)\, dx\,.$$

Addition aller solcher Gleichungen von $k = 1$ bis $k = n - 1$ liefert

$$\int_1^n \big(\{x\} - \tfrac{1}{2}\big) f'(x)\, dx = \frac{f(1)}{2} + \sum_{k=2}^{n-1} f(k) + \frac{f(n)}{2} - \int_1^n f(x)\, dx\,,$$

womit man die Summe der $f(k)$ berechnen kann:

Satz (EULERsche Summenformel): Für eine differenzierbare Funktion $f\colon D \to \mathbb{R}$, deren Definitionsbereich das Intervall $[1,\, n]$ umfaßt, ist

$$\sum_{k=1}^{n} f(k) = \int_1^n f(x)\, dx + \frac{f(1) + f(n)}{2} + \int_1^n \big(\{x\} - \tfrac{1}{2}\big) f'(x)\, dx\,.$$

■

Für die Abschätzung von $n!$ interessiert uns speziell der Fall, daß $f(x) = \log x$ der natürliche Logarithmus ist; hier wird die EULERsche

Summenformel zu

$$\log n! = \int_1^n \log x\,dx + \frac{\log n}{2} + \int_1^n \frac{\{x\}-\frac{1}{2}}{x}\,dx$$

$$= x(\log x - 1)\Big|_1^n + \frac{\log n}{2} + \int_1^n \frac{\{x\}-\frac{1}{2}}{x}\,dx$$

$$= n(\log n - 1) + 1 + \frac{\log n}{2} + \int_1^n \frac{\{x\}-\frac{1}{2}}{x}\,dx\,.$$

In dieser Formel stört noch das rechte Integral; dieses können wir wie folgt abschätzen: Für eine natürliche Zahl k ist

$$\int_k^{k+1} \frac{\{x\}-\frac{1}{2}}{x}\,dx = \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{x}{k+\frac{1}{2}+x}\,dx$$

$$= \int_0^{\frac{1}{2}} \left(\frac{x}{k+\frac{1}{2}+x} - \frac{x}{k+\frac{1}{2}-x}\right) dx = \int_0^{\frac{1}{2}} \frac{-2x^2}{\left(k+\frac{1}{2}\right)^2 - x^2}\,dx\,.$$

Im Intervall von 0 bis $\frac{1}{2}$ ist der Integrand monoton fallend, d.h.

$$0 \geq \frac{-2x^2}{\left(k+\frac{1}{2}\right)^2 - x^2} \geq \frac{-\frac{1}{2}}{\left(k+\frac{1}{2}\right)^2 - \frac{1}{4}} = \frac{-2}{(2k+1)^2 - 1} \geq -\frac{1}{2k^2}\,,$$

und damit ist

$$0 \geq \int_k^{k+1} \frac{\{x\}-\frac{1}{2}}{x}\,dx = \int_0^{\frac{1}{2}} \frac{-2x^2}{\left(k+\frac{1}{2}\right)^2 - x^2}\,dx \geq -\frac{1}{4k^2}\,,$$

denn wir können das Integral abschätzen durch das Produkt aus der Länge des Integrationsintervalls und dem Minimum des Integranden. Summation von $k = 1$ bis $n-1$ schließlich gibt die Abschätzung

$$0 \geq \int_1^n \frac{\{x\}-\frac{1}{2}}{x}\,dx \geq -\sum_{k=1}^{n-1} \frac{1}{4k^2} > -\frac{1}{4}\sum_{k=1}^{\infty} \frac{1}{k^2}$$

für das störende Integral aus der obigen Formel. Da die Summe rechts konvergiert, konvergiert auch das Integral für $n \to \infty$ gegen einen Grenzwert I. Somit ist

$$\log n! = n(\log n - 1) + \frac{\log n}{2} + I + 1 + o(1)\,,$$

also folgt insbesondere die Abschätzung

$$\log n! = n \log n + O(n)\,,$$

die wir im Beweis des Satzes über $\pi(x)$ verwendet haben.

§4: Das Sieb des Eratosthenes

Das klassische Verfahren zur Bestimmung aller Primzahlen unterhalb einer bestimmten Schranke geht zurück auf ERATOSTHENES im vorchristlichen Jahrhundert. Es funktioniert folgendermaßen:

Um alle Primzahlen kleiner oder gleich einer Zahl N zu finden, schreibe man zunächst die Zahlen von eins bis N in eine Reihe.

Eins ist nach Definition keine Primzahl – für klassische griechische Mathematiker wie EUKLID war die Eins schließlich nicht einmal eine Zahl. Also streichen wir die Eins durch. Die Zwei ist prim, aber ihre echten Vielfachen sind natürlich keine Primzahlen, werden also durchgestrichen. Dazu müssen wir nicht von jeder Zahl nachprüfen, ob sie durch zwei teilbar ist, sondern wir streichen einfach nach der Zwei jede zweite Zahl aus der Liste durch.

Die erste nichtdurchgestrichene Zahl der Liste ist dann die Drei. Sie muß eine Primzahl sein, denn hätte sie einen von eins verschiedenen kleineren Teiler, könnte das nur die Zwei sein, und alle Vielfachen von zwei (außer der Zwei selbst) sind bereits durchgestrichen.

Auch die echten Vielfachen der Drei sind keine Primzahlen, werden also durchgestrichen. Auch dazu streichen wir wieder einfach jede dritte Zahl aus der Liste durch, unabhängig davon, ob sie bereits durchgestrichen ist oder nicht. (Alle durch sechs teilbaren Zahlen sind offensichtlich schon durchgestrichen.)

Genauso geht es weiter mit der Fünf *usw.;* nach jedem Durchgang durch die Liste muß offenbar die erste noch nicht durchgestrichene Zahl eine

Primzahl sein, denn alle Vielfache von kleineren Primzahlen sind bereits durchgestrichen, und wenn eine Zahl überhaupt einen echten Teiler hat, dann ist sie natürlich auch durch eine echt kleinere Primzahl teilbar.

ERATOSTHENES (Ερατοσθένες) wurde 276 v.Chr. in Cyrene im heutigen Libyen geboren, wo er zunächst von Schülern des Stoikers ZENO ausgebildet wurde. Danach studierte er noch einige Jahre in Athen, bis ihn 245 der Pharao PTOLEMAIOS III als Tutor seines Sohns nach Alexandrien holte. 240 wurde er dort Bibliothekar der berühmten Bibliothek im Museion.
Heute ist er außer durch sein Sieb vor allem durch seine Bestimmung des Erdumfangs bekannt. Er berechnete aber auch die Abstände der Erde von Sonne und Mond und entwickelte einen Kalender, der Schaltjahre enthielt. 194 starb er in Alexandrien, nach einigen Überlieferungen, indem er sich, nachdem er blind geworden war, zu Tode hungerte.

Wie lange müssen wir dieses Verfahren durchführen? Wenn eine Zahl x Produkt zweier echt kleinerer Faktoren u, v ist, können u und v nicht beide größer sein als $\sqrt{x}$: Sonst wäre schließlich $x = uv$ größer als x. Also ist einer der beiden Teiler u, v kleiner oder gleich $\sqrt{x}$, so daß x mindestens einen Teiler hat, dessen Quadrat kleiner oder gleich x ist. Damit ist eine zusammengesetzte Zahl x durch mindestens eine Primzahl p teilbar mit $p^2 \leq x$. Für das Sieb des ERATOSTHENES, angewandt auf die Zahlen von eins bis N heißt das, daß wir aufhören können, sobald die erste nichtdurchgestrichene Zahl p ein Quadrat $p^2 > N$ hat; dann können wir sicher sein, daß jede zusammengesetzte Zahl $x \leq N$ bereits einen kleineren Primteiler als p hat und somit bereits durchgestrichen ist. Die noch nicht durchgestrichenen Zahlen in der Liste sind also Primzahlen.

Damit lassen sich leicht von Hand alle Primzahlen bis hundert finden, mit etwas Fleiß auch die bis Tausend, aber sicher nicht die hundertstelligen.

Trotzdem kann uns ERATOSTHENES helfen, zumindest zu zeigen, daß gewissen Zahlen nicht prim sind: Wenn wir Primzahlen in einem Intervall $[a,\ b]$ suchen, d.h. also Primzahlen p mit

$$a \leq p \leq b\,,$$

so können wir ERATOSTHENES auf dieses Intervall fast genauso anwenden wie gerade eben auf das Intervall $[1,\ N]$:

Wir gehen aus von einer Liste $p_1, \ldots, p_r$ der ersten Primzahlen; dabei wählen wir r so, daß die Chancen auf nicht durch p_r teilbare Zahlen im Intervall $[a,\ b]$ noch einigermaßen realistisch sind, d.h. wir gehen bis zu einer Primzahl p_r, die ungefähr in der Größenordnung der Intervallänge $b - a$ liegt.

Nun können wir mit jeder der Primzahlen p_i sieben wie im klassischen Fall; wir müssen nur wissen, wo wir anfangen sollen.

Dazu berechnen wir für jedes p_i den Divisionsrest $r_i = a \bmod p_i$. Dann ist $a - r_i$ durch p_i teilbar, liegt allerdings nicht im Intervall $[a,\ b]$. Die erste Zahl, die wir streichen müssen, ist also $a - r_i + p_i$, und von da an streichen wir einfach, ohne noch einmal dividieren zu müssen, wie gehabt jede p_i-te Zahl durch.

Was nach r Durchgängen noch übrig bleibt, sind genau die Zahlen aus $[a,\ b]$, die durch keine der Primzahlen p_i teilbar sind. Sie können zwar noch größere Primteiler haben, aber wichtig ist, daß wir mit minimalem Aufwand für den Großteil aller Zahlen aus $[a,\ b]$ gesehen haben, daß sie keine Primzahlen sind. Für den Rest brauchen wir andere Verfahren, aber die sind allesamt erheblich aufwendiger als ERATOSTHENES, so daß sich diese erste Reduktion auf jeden Fall lohnt.

§5: Kongruenzenrechnung

Zwei ganze Zahlen lassen sich im allgemeinen nicht durcheinander dividieren. Trotzdem – oder gerade deshalb – spielen Teilbarkeitsfragen in der Zahlentheorie eine große Rolle. Das technische Werkzeug zu ihrer Behandlung ist die Kongruenzenrechnung.

Definition: Wir sagen, zwei ganze Zahlen $x, y \in \mathbb{Z}$ seien kongruent modulo m für eine natürliche Zahl m, in Zeichen $x \equiv y \bmod m$, wenn $x - y$ durch m teilbar ist.

Die Kongruenz modulo m definiert offensichtlich eine Äquivalenzrelation auf $\mathbb{Z}$: Jede ganze Zahl ist kongruent zu sich selbst, denn $x - x = 0$

ist durch jede natürliche Zahl teilbar. Wenn $x - y$ durch m teilbar ist, so auch $y - x = -(x - y)$, und ist schließlich $x \equiv y \bmod m$ und $y \equiv z \bmod m$, so sind $x - y$ und $y - z$ durch m teilbar, also auch ihre Summe $x - z$, und damit ist auch $x \equiv z \bmod m$.

Zwei Zahlen $x, y \in \mathbb{Z}$ liegen genau dann in derselben Äquivalenzklasse, wenn sie bei der Division durch m denselben Divisionsrest haben; es gibt somit m Äquivalenzklassen, die den m möglichen Divisionsresten $0, 1, \ldots, m-1$ entsprechen.

Lemma: Ist $x \equiv x' \bmod m$ und $y \equiv y' \bmod m$, so ist auch

$$x \pm y \equiv x' \pm y' \bmod m \quad \text{und} \quad x'y' \equiv xy \bmod m\,.$$

Beweis: Sind $x - x'$ und $y - y'$ durch m teilbar, so auch

$$(x \pm y) - (x' \pm y') = (x - x') \pm (y - y') \qquad \text{und}$$
$$xy - x'y' = x(y - y') + y'(x - x')$$

■

Im folgenden wollen wir das Symbol „mod“ nicht nur in Kongruenzen wie $x \equiv y \bmod m$ benutzen, sondern auch – wie in einigen Programmiersprachen üblich – als Rechenoperation:

Definition: Für eine ganze Zahl x und eine natürliche Zahl m bezeichnet $x \bmod m$ jene ganze Zahl $0 \le r < m$ mit $x \equiv r \bmod m$.

$x \bmod m$ ist also einfach der Divisionsrest bei der Division von x durch m.

Beim Rechnen modulo einer Zahl m ersetzt man alle Rechenergebnisse durch ihren Wert modulo m; sie liegen also stets zwischen null und $m - 1$. Anwendungen findet dies beispielsweise in der Computeralgebra: Da man auch für Polynome in einer Veränderlichen über einem Körper eine Division mit Rest hat, kann man auch hier größte gemeinsame Teiler mit dem EUKLIDischen Algorithmus berechnen. Wenn die führenden Koeffizienten nicht eins sind, bekommt man dabei selbst bei Polynomen mit ganzzahligen Koeffizienten oft sehr schnell gigantische Nenner. Wenn man allerdings weiß, daß der ggT ein Polynom mit ganzzahligen Koeffizienten ist und auch eine Schranke M für den Betrag

der Koeffizienten kennt, genügt es, wenn man den ggT modulo einer Zahl $m \geq 2M + 1$ berechnen kann. Tatsächlich genügt es sogar, wenn man ihn modulo hinreichend vieler kleinerer Zahlen kennt, denn der folgende Satz zeigt uns, wie man diese Ergebnisse kombinieren kann zu einer Kongruenz modulo einer größeren Zahl.

Der Legende nach zählten chinesische Generäle ihre Truppen, indem sie diese mehrfach antreten ließen in Reihen verschiedener Breiten $m_1, \ldots, m_r$ und jedesmal nur die Anzahl a_r der Soldaten in der letzten Reihe zählten. Aus den r Relationen

$$x \equiv a_1 \bmod m_1, \quad \ldots, \quad x \equiv a_r \bmod m_r$$

bestimmten sie dann die Gesamtzahl x der Soldaten.

Ob es im alten China wirklich Generäle gab, die soviel Mathematik konnten, sei dahingestellt. Beispiele zu diesem Satz finden sich jedenfalls bereits 1247 in den chinesischen *Mathematischen Abhandlungen in neun Bänden* von CH'IN CHIU-SHAO (1202–1261), allerdings geht es dort nicht um Soldaten, sondern um Reis.

CH'IN CHIU-SHAO oder QIN JIUSHAO wurde 1202 in der Provinz Sichuan geboren. Auf eine wilde Jugend mit vielen Affairen folgte ein wildes und alles andere als gesetzestreues Berufsleben in Armee, öffentlicher Verwaltung und illegalem Salzhandel. Als Jugendlicher studierte er an der Akademie von Hang-chou Astronomie, später brachte ihm ein unbekannter Lehrer Mathematik bei. Insbesondere studierte er die in vorchristlicher Zeit entstandenen *Neun Bücher der Rechenkunst,* nach deren Vorbild er 1247 seine deutlich anspruchsvolleren *Mathematischen Abhandlungen in neun Bänden* publizierte, die ihn als einen der bedeutendsten Mathematiker nicht nur Chinas der damaligen Zeit ausweisen. Zum chinesischen Restesatz schreibt er, daß er ihn von den Kalendermachern gelernt habe, diese ihn jedoch nur rein mechanisch anwendeten ohne ihn zu verstehen. CH'IN CHIU-SHAO starb 1261 in Meixian, wohin er nach einer seiner vielen Entlassungen aus einer Haft wegen krimineller Machenschaften geschickt worden war.

Wir wollen uns zunächst überlegen, unter welchen Bedingungen ein solches Verfahren überhaupt funktionieren kann. Offensichtlich können die obigen r Relationen eine natürliche Zahl nicht eindeutig festlegen, denn ist x eine Lösung und M irgendein gemeinsames Vielfaches der sämtlichen m_i, so ist auch $x+M$ eine Lösung – M ist schließlich modulo aller m_i kongruent zur Null.

Außerdem gibt es Relationen obiger Form, die unlösbar sind, beispielsweise das System

$$x \equiv 2 \bmod 4 \quad \text{und} \quad x \equiv 3 \bmod 6\,,$$

dessen erste Gleichung nur gerade Lösungen hat, während die zweite nur ungerade hat. Das Problem hier besteht darin, daß zwei ein gemeinsamer Teiler von vier und sechs ist, so daß jede der beiden Kongruenzen auch etwas über $x \bmod 2$ aussagt: Nach der ersten ist x gerade, nach der zweiten aber ungerade.

Dieses Problem können wir dadurch umgehen, daß wir nur Moduln m_i zulassen, die paarweise teilerfremd sind. Dies hat auch den Vorteil, daß jedes gemeinsame Vielfache der m_i Vielfaches des Produkts aller m_i sein muß, so daß wir x modulo einer vergleichsweise großen Zahl kennen.

Chinesischer Restesatz: Das System von Kongruenzen

$$x \equiv a_1 \bmod m_1, \quad \ldots, \quad x \equiv a_r \bmod m_r$$

hat für paarweise teilerfremde Moduln m_i genau eine Lösung x mit $0 \le x < m_1 \cdots m_r$. Jede andere Lösung $y \in \mathbb{Z}$ läßt sich in der Form $x + km_1 \cdots m_r$ schreiben mit $k \in \mathbb{Z}$.

Beweis: Wir beginnen mit dem Fall zweier Kongruenzen

$$x \equiv a \bmod m \quad \text{und} \quad y \equiv b \bmod n$$

mit zueinander teilerfremden Zahlen m und n. Ihr ggT eins läßt sich nach dem erweiterten EUKLIDischen Algorithmus als $1 = \alpha m + \beta n$ schreiben. Somit ist

$$1 - \alpha m = \beta n \equiv \begin{cases} 1 & \bmod m \\ 0 & \bmod n \end{cases} \quad \text{und} \quad 1 - \beta n = \alpha m \equiv \begin{cases} 0 & \bmod m \\ 1 & \bmod n \end{cases},$$

also löst

$$x = \beta n a + \alpha m b \equiv \begin{cases} a & \bmod m \\ b & \bmod n \end{cases}$$

das Problem. Für jede weitere Lösung y ist $x - y \equiv 0$ sowohl modulo n als auch modulo m, also ist $x - y$ durch nm teilbar und hat somit die

Form $y = x + kmn$ mit einem $k \in \mathbb{Z}$. Umgekehrt löst natürlich auch jedes solche y die Kongruenz; die allgemeine Lösung ist daher

$$x = \beta na + \alpha mb + kmn$$

mit einem beliebigen $k \in \mathbb{Z}$.

Der allgemeine Satz folgt nun leicht durch vollständige Induktion nach r: Für $r = 1$ ist die Aussage trivial; sei also $r \geq 2$. Nach Induktionsannahme gibt es ein $y \in \mathbb{Z}$ mit $0 \leq y < m_1 \cdots m_{r-1}$, so daß

$$y \equiv a_1 \bmod m_1, \quad \ldots, \quad y \equiv a_{r-1} \bmod m_{r-1}\,,$$

und die sämtlichen Lösungen sind genau die Zahlen $y + km_1 \cdots m_{r-1}$ mit $k \in \mathbb{Z}$. Sei $m = m_1 \cdots m_{r-1}$; nach dem bereits bewiesenen Fall von nur zwei Kongruenzen gibt es ein $x \in \mathbb{Z}$ mit $0 \leq x < mm_r$. so daß

$$x \equiv y \bmod m \quad \text{und} \quad x \equiv a_r \bmod m_r\,,$$

und x ist modulo $mm_r = m_1 \cdots m_r$ eindeutig. Damit ist der Satz vollständig bewiesen.

■

Als Beispiel betrachten wir die beiden Kongruenzen

$$x \equiv 1 \bmod 17 \quad \text{und} \quad x \equiv 5 \bmod 19\,.$$

Zunächst wenden wir den erweiterten EUKLIDischen Algorithmus an auf die beiden Moduln 17 und 19:

$$19 : 17 = 1 \text{ Rest } 2 \Longrightarrow 2 = 19 - 17$$

$$17 : 2 = 8 \text{ Rest } 1 \Longrightarrow 1 = 17 - 8 \cdot 2 = 9 \cdot 17 - 8 \cdot 19$$

Also ist $9 \cdot 17 = 153 \equiv 0 \bmod 17$ und $\equiv 1 \bmod 19$; außerdem ist $-8 \cdot 19 = -152$ durch 19 teilbar und $\equiv 1 \bmod 17$. Die Zahl

$$x = -152 \cdot 1 + 153 \cdot 5 = 613$$

löst somit das Problem. Da 613 größer ist als $17 \cdot 19 = 323$, ist allerdings nicht 613 die kleinste positive Lösung, sondern $613 - 323 = 290$.

Zur Lösung des Systems

$$x \equiv 5 \bmod 10, \quad x \equiv 9 \bmod 11, \quad x \equiv 6 \bmod 13$$

lösen wir zunächst nur das System

$$x \equiv 5 \bmod 10 \quad \text{und} \quad x \equiv 9 \bmod 11 \,.$$

Da $1 = 11 - 10$, ist $11 \equiv 0 \bmod 11$ und $11 \equiv 1 \bmod 10$; entsprechend ist $-10 \equiv 0 \bmod 10$ und $-10 \equiv 1 \bmod 11$. Also ist

$$x = 5 \cdot 11 - 9 \cdot 10 = -35$$

eine Lösung; die allgemeine Lösung ist $-35 + 110k$ mit $k \in \mathbb{Z}$. Die kleinste positive Lösung ist $-35 + 110 = 75$.

Unser Ausgangssystem ist somit äquivalent zu den beiden Kongruenzen

$$x \equiv 75 \bmod 110 \quad \text{und} \quad x \equiv 6 \bmod 13 \,.$$

Um es zu lösen, müssen wir zunächst die Eins als Linearkombination von 110 und 13 darstellen. Hier bietet sich keine offensichtliche Lösung an, also verwenden wir den erweiterten EUKLIDischen Algorithmus:

$$110 : 13 = 8 \text{ Rest } 6 \Longrightarrow 6 = 110 - 8 \cdot 13$$

$$13 : 6 = 2 \text{ Rest } 1 \Longrightarrow 1 = 13 - 2 \cdot (110 - 8 \cdot 12) = 17 \cdot 13 - 2 \cdot 110$$

Also ist $17 \cdot 13 = 221 \equiv 1 \bmod 110$ und $\equiv 0 \bmod 13$; genauso ist $-2 \cdot 110 = 220 \equiv 1 \bmod 13$ und $\equiv 9 \bmod 110$. Eine ganzzahlige Lösung unseres Problems ist somit

$$75 \cdot 221 - 6 \cdot 220 = 15\,255 \,.$$

Die allgemeine Lösung ist

$$15\,255 + k \cdot 110 \cdot 13 = 15\,255 + 1\,430k \quad \text{mit} \quad k \in \mathbb{Z} \,.$$

Da $15\,255 : 1\,430 = 10$ Rest 955 ist, erhalten wir 955 als kleinste Lösung.

Alternativ läßt sich die Lösung eines Systems aus r Kongruenzen auch in einer geschlossenen Form darstellen, allerdings um den Preis einer n-maligen statt $(n-1)$-maligen Anwendung des EUKLIDischen Algorithmus und größeren Zahlen schon von Beginn an: Um das System

$$x \equiv a_i \bmod m_i \quad \text{für} \quad i = 1, \ldots, r$$

zu lösen, berechnen wir zunächst für jedes i das Produkt

$$\widehat{m}_i = \prod_{j \neq i} m_j$$

der sämtlichen übrigen m_j und bestimmen dazu ganze Zahlen α_i, β_i, für die gilt $\alpha_i m_i + \beta_i \widehat{m}_i = 1$. Dann ist

$$x = \sum_{j=1}^{n} \beta_j \widehat{m}_j a_j \equiv \beta_i \widehat{m}_i a_i = (1 - \alpha_i m_i) a_i \equiv a_i \bmod m_i \, .$$

Natürlich wird x hier – wie auch bei der obigen Formel – oft größer sein als das Produkt der m_i; um die kleinste Lösung zu finden, müssen wir also noch modulo diesem Produkt reduzieren.

Im obigen Beispiel wäre

$$\begin{array}{llll} m_1 = 10 & \widehat{m}_1 = 11 \cdot 13 = 143 & 1 = 43 \cdot 10 - 3 \cdot 143 \\ m_2 = 11 & \widehat{m}_2 = 10 \cdot 13 = 130 & 1 = -59 \cdot 11 + 5 \cdot 130 \\ m_3 = 13 & \widehat{m}_3 = 10 \cdot 11 = 110 & 1 = 17 \cdot 13 - 2 \cdot 110 \, , \end{array}$$

also

$$x = -3 \cdot 143 \cdot 5 + 5 \cdot 130 \cdot 9 - 2 \cdot 110 \cdot 6 = -2145 + 5850 - 1320 = 2385 \, .$$

Modulo $10 \cdot 11 \cdot 13$ erhalten wir natürlich auch hier wieder 955.

§6: Der kleine Satz von Fermat

Die meisten Mathematiker kennen FERMAT vor allem wegen seiner 1994 von ANDREW WILES bewiesenen Vermutung über Summen n-ter Potenzen; im englischen Sprachraum wurde sie auch schon lange vor diesem Beweis als FERMAT's *big theorem* bezeichnet. In Analogie zu diesem „großen" Satz von FERMAT gibt es auch einen kleinen; diesen hat er wirklich bewiesen.

Kleiner Satz von Fermat: Für jedes $a \in \mathbb{Z}$ und jede Primzahl p ist

$$a^p \equiv a \bmod p \, ;$$

ist a nicht durch p teilbar, gilt auch $a^{p-1} \equiv 1 \bmod p$.

Beweis: Wir betrachten zunächst nur nichtnegative Werte von a und beweisen die erste Aussage dafür durch vollständige Induktion:

Für $a = 0$ ist $0^p = 0$, also erst recht kongruent Null modulo p; genauso ist für $a = 1$ auch $a^p = 1$.

Für $a > 1$ schreiben wir

$$a^p = \big((a-1)+1\big)^p = \sum_{i=0}^{p} \binom{p}{i} (a-1)^i \quad \text{mit} \quad \binom{p}{i} = \frac{p!}{i!\,(p-i)!}\,.$$

Falls $1 \le i \le p-1$, ist der Nenner von $\binom{p}{i}$ nicht durch p teilbar, wohl aber der Zähler. Somit ist auch $\binom{p}{i}$ durch p teilbar, also kongruent Null modulo p. Damit ist

$$a^p \equiv \binom{p}{0}(a-1)^0 + \binom{p}{p}(a-1)^p = 1 + (a-1) = a \bmod p$$

nach Induktionsannahme.

Dies beweist die erste Aussage für $a \ge 0$. Für $a < 0$ ist im Falle $p = 2$ sowohl $-a \equiv a \bmod 2$ als auch $a^p = (-a)^p$; für ungerades p ist $(-a)^p = -(a^p)$, so daß die Behauptung in beiden Fällen folgt.

Zum Beweis der zweiten Behauptung beachten wir, daß

$$a^p - a = a\,(a^{p-1} - 1)\,,$$

wie wir gerade bewiesen haben, durch p teilbar ist. Falls a nicht durch p teilbar ist, muß also $a^{p-1} - 1$ durch p teilbar sein, und genau das ist die Behauptung.

■

Der französische Mathematiker PIERRE DE FERMAT (1601–1665) wurde in Beaumont-de-Lomagne im Departement Tarn et Garonne geboren. Bekannt ist er heutzutage vor allem für seine 1994 von ANDREW WILES bewiesene Vermutung, wonach die Gleichung $x^n + y^n = z^n$ für $n \ge 3$ keine ganzzahlige Lösung mit $xyz \neq 0$ hat. Dieser „große“ Satzes von FERMAT, von dem FERMAT lediglich in einer Randnotiz behauptete, daß er ihn beweisen könne, erklärt den Namen der obigen Aussage. Obwohl FERMAT sich sein Leben lang sehr mit Mathematik beschäftigte und wesentliche Beiträge zur Zahlentheorie, Wahrscheinlichkeitstheorie und Analysis lieferte, war er hauptberuflich Jurist.

Wenn wir entscheiden wollen, ob eine gegebene Zahl p prim ist, kann die folgende Umkehrung des kleinen Satzes von FERMAT nützlich sein:

Lemma: Sind a, p zwei zueinander teilerfremde natürliche Zahlen, und ist $a^{p-1} \not\equiv 1 \bmod p$, so ist p keine Primzahl. ∎

Beispiel: Ist $F_{20} = 2^{2^{20}} + 1$ eine Primzahl? Falls ja, ist nach dem kleinen Satz von FERMAT insbesondere $3^{F_{20}-1} \equiv 1 \bmod F_{20}$. Nachrechnen zeigt, daß $3^{(F_{20}-1)/2} \not\equiv \pm 1 \bmod F_{20}$, die Zahl ist also nicht prim. (Das „Nachrechnen“ ist bei dieser 315653-stelligen Zahl natürlich keine Übungsaufgabe für Taschenrechner: 1988 brauchte eine Cray X-MP dazu 82 Stunden, eine Cray-2 immerhin noch zehn; siehe *Math. Comp.* **50** (1988), 261–263. Die anscheinend etwas weltabgewandt lebenden Autoren meinten, das sei die teuerste bislang produzierte 1-Bit-Information.)

Die Umkehrung gilt leider nicht: Es gibt unendlich viele Nichtprimzahlen n, die sogenannten CARMICHAEL-Zahlen, für die $a^{n-1} \equiv 1 \bmod n$ ist für jedes zu n teilerfremde a. Trotzdem wird es für große Zahlen zunehmend unwahrscheinlich, daß eine Zahl p für auch nur ein a den obigen Test besteht, ohne Primzahl zu sein. In der Arbeit

SU HEE KIM, CARL POMERANCE: The probability that a Random Probable Prime is Composite, *Math. Comp.* **53** (1989), 721–741,

sind u.a. die folgenden Schranken ε zu finden für die Wahrscheinlichkeit, daß für eine Nichtprimzahl p und ein zufällig gewähltes a die Kongruenz $a^{p-1} \equiv 1 \bmod p$ gilt:

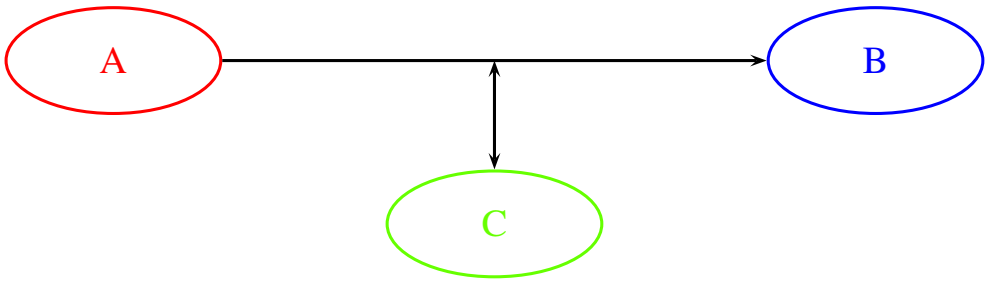
$p \approx 10^{60}$	10^{70}	10^{80}	10^{90}	10^{100}
$\varepsilon \le 7{,}16 \cdot 10^{-2}$	$2{,}87 \cdot 10^{-3}$	$8{,}46 \cdot 10^{-5}$	$1{,}70 \cdot 10^{-6}$	$2{,}77 \cdot 10^{-8}$
$p \approx 10^{120}$	10^{140}	10^{160}	10^{180}	10^{200}
$\varepsilon \le 5{,}28 \cdot 10^{-12}$	$1{,}08 \cdot 10^{-15}$	$1{,}81 \cdot 10^{-19}$	$2{,}76 \cdot 10^{-23}$	$3{,}85 \cdot 10^{-27}$
$p \approx 10^{300}$	10^{400}	10^{500}	10^{600}	10^{700}
$\varepsilon \le 5{,}8 \cdot 10^{-29}$	$5{,}7 \cdot 10^{-42}$	$2{,}3 \cdot 10^{-55}$	$1{,}7 \cdot 10^{-68}$	$1{,}8 \cdot 10^{-82}$
$p \approx 10^{800}$	10^{900}	10^{1000}	10^{2000}	10^{3000}
$\varepsilon \le 5{,}4 \cdot 10^{-96}$	$1{,}0 \cdot 10^{-109}$	$1{,}2 \cdot 10^{-123}$	$8{,}6 \cdot 10^{-262}$	$3{,}8 \cdot 10^{-397}$

Die Arbeit beruht im wesentlichen auf der von POMERANCE betreuten Masterarbeit des ersten Autors und enthält natürlich auch eine Formel für ε; diese ist aber zu grausam zum Abdrucken.

Natürlich kennt die Zahlentheorie auch effiziente Tests, mit denen sich *beweisen* läßt, daß eine gegebene Zahl p prim ist. Diese sind allerdings deutlich aufwendiger als der FERMAT-Test, so daß man sie erst anwendet, wenn die Zahl bereits den FERMAT-Test bestanden hat.

§7: Anwendungen in der Kryptographie

Das Grundproblem der Kryptographie ist das folgende:



A möchte eine Nachricht m an B übermitteln, jedoch besteht die Gefahr, daß alles, was er an B schickt, auf dem Weg dorthin von C gelesen und vielleicht auch verändert wird; außerdem könnte C eventuell versuchen, sich gegenüber B als A auszugeben oder umgekehrt.

Die Kryptographie versucht, dies zu verhindern, indem A anstelle von m eine verschlüsselte Nachricht c schickt, aus der zwar B, nicht aber C die Nachricht m und gegebenenfalls weitere Informationen rekonstruieren kann. Bei sogenannten *Blockchiffren* teilt man die Nachricht auf in Blöcke aus einer endlichen Menge M, im einfachsten Fall die Menge der Buchstaben des Alphabets, und verschlüsselt durch eine bijektive Abbildung von M nach M.

Eine bekannte (und sehr schlechte) Form der Verschlüsselung geht auf CAESAR zurück. Der römische Schriftsteller SUETON schreibt in Kapitel 56 des ersten Buchs DIVUS IULIUS *(der göttliche Julius)* seines Werks DE VITA CAESARUM:

> extant et ad ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est d pro a et perinde reliquas commutet.

> Erhalten sind auch seine Briefe an CICERO, ebenso an seine engeren Freunde über private Angelegenheiten, in denen er, was etwa geheim zu überbringen war, in verschlüsselter Form schrieb, nämlich in einer solchen Anordnung der Buchstaben, daß kein einziges Wort herauskam. Falls hier jemand nachforschen und der Sache nachgehen will, möge er den vierten Buchstaben des Alphabets, d.h. D für A und so fort setzen.

(aus SUETON: Kaiserbiographien*, Akademie Verlag Berlin,* 1993)

CAESAR verschob das Alphabet also einfach zyklisch nach dem Schema

$$A \to D, \quad B \to E, \ldots, W \to Z, \quad X \to A, \quad Y \to B, \quad Z \to C\,.$$

Gerade für jemand, der seine Verbündete so oft wechselte wie CAESAR hat ein solches Verfahren den großen Nachteil, daß jeder, der es einmal benutzt hat, auch künftig alle damit verschlüsselten Nachrichten lesen kann.

Wie AUGUSTE KERCKHOFFS 1883 in seiner grundlegenden Arbeit *La cryptographie militaire* feststellte, muß man bei jedem in größerem Umfang eingesetzten Verfahren davon ausgehen, daß es sich nicht über einen längeren Zeitraum hinweg geheimhalten läßt. Anstelle einer einfachen Verschlüsselungsfunktion f, die jeder Nachricht m einen Chiffretext $c = f(m)$ zuordnet, soll man eine Funktion benutzen, die außer von m auch noch von einem zweiten Parameter s abhängt, dem *Schlüssel.* Somit ist also $c = f(m, s)$. Die Sicherheit des Verfahrens darf laut KERCKHOFFS nur von der Geheimhaltung des (häufig zu wechselnden) Schlüssels s abhängen, nicht von der der Funktion f.

Viele heutige Kryptoverfahren sind oder beruhen auf Blockchiffren. Dazu wird die zu übermittelnde Nachricht aufgespalten in eine Folge von Blöcken einer vorgegebenen Länge. Oft sind das 128 Bit, also 16 Byte; bei den hier betrachteten Verfahren werden die Blöcke allerdings deutlich länger sein.

Bezeichnet $\mathcal{B}$ die Menge aller möglicher Blöcke und $\mathcal{S}$ die Menge aller möglicher Schlüssel, so ist eine Verschlüsselungsfunktion also von der

Form

$$f\colon \begin{cases} \mathcal{B} \times \mathcal{S} \to \mathcal{B} \\ (m, s) \mapsto f(m, s) \end{cases},$$

und die Entschlüsselungsfunktion

$$g\colon \begin{cases} \mathcal{B} \times \mathcal{S} \to \mathcal{B} \\ (m, s) \mapsto g(m, s) \end{cases}$$

ist so definert, daß $g\big(f(m, s), s\big) = m$ ist für alle $m \in \mathcal{B}$.

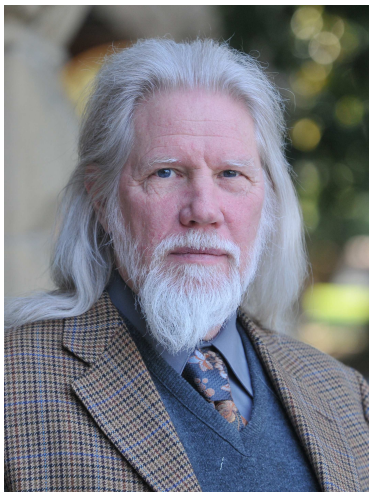
JEAN-GUILLAUME-HUBERT-VICTOR-FRANÇOIS-ALEXANDRE-AUGUSTE KERCKHOFFS VON NIEUWENHOF (1835–1903) wurde in der heute niederländischen Ortschaft Nuth geboren. Er studierte an der Universität Liège, wo er mit dem Doktor der Literaturwissenschaften abschloß. Nachdem er mehrere Stellen als Lehrer in den Niederlanden und in Frankreich bekleidet hatte, wurde er schließlich Professor für Deutsch an der Ecole des Hautes Etudes Commerciales in Paris. Außer für seine Arbeit zur Militärkryptographie ist er vor allem auch noch für linguistische Studien bekannt, insbesondere auch zur heute weithin vergessenen Kunstsprache Volapük.

Wenn ein Schlüssel häufig gewechselt wird, müssen sich die beteiligen Partner jeweils miteinander verständigen, was entweder ein Treffen oder vertrauenswürdige Boten voraussetzt – beides ist mit großem Aufwand verbunden.

1976 publizierten MARTIN HELLMAN, damals Assistenzprofessor an der Stanford University, und sein Forschungsassistent WHITFIELD DIFFIE eine Arbeit mit dem Titel *New directions in cryptography* (IEEE Trans. Inform. Theory **22**, 644–654; inzwischen auch im Netz zu finden), in der sie vorschlugen, den Vorgang der *Ver*schlüsselung und den der *Ent*schlüsselung völlig voneinander zu trennen: Es sei schließlich nicht notwendig, daß der Sender einer verschlüsselten Nachricht auch in der Lage sei, diese zu *ent*schlüsseln.

Der Vorteil eines solchen Verfahrens wäre, daß jeder potentielle Empfänger nur einen einzigen Schlüssel bräuchte und dennoch sicher sein

könnte, daß nur er selbst seine Post entschlüsseln kann. Der Schlüssel müßte nicht einmal geheimgehalten werden, da es ja nicht schadet, wenn jedermann Nachrichten *ver*schlüsseln kann. In einem Netzwerk mit n Teilnehmern bräuchte man also nur n Schlüssel, um jedem Teilnehmer zu erlauben, mit jeden anderen zu kommunizieren, und diese Schlüssel könnten sogar in einem öffentlichen Verzeichnis stehen. Bei einem symmetrischen Kryptosystem wäre der gleiche Zweck nur erreichbar mit $\frac{1}{2}n(n-1)$ Schlüsseln, die zudem noch durch ein sicheres Verfahren wie etwa ein persönliches Treffen oder durch vertrauenswürdige Boten ausgetauscht werden müßten.



BAILEY WHITFIELD DIFFIE wurde 1944 geboren. Erst im Alter von zehn Jahren lernte er lesen; im gleichen Jahr hielt eine Lehrerin an seiner New Yorker Grundschule einen Vortrag über Chiffren. Er ließ sich von seinem Vater alle verfügbare Literatur darüber besorgen, entschied sich dann 1961 aber doch für ein Mathematikstudium am MIT. Um einer Einberufung zu entgehen, arbeitete er nach seinem Bachelor bei Mitre; später, nachdem sein Interesse an der Kryptographie wieder erwacht war, kam er zu Martin Hellman nach Stanford, der ihn als Forschungsassistent einstellte. 1991–2009 arbeitete er als *chief security officer* bei Sun Microsystems; heute ist er *consulting professor* in Stanford.
`http://cisac.stanford.edu/people/whitfield_diffie/`

MARTIN HELLMAN wurde 1945 in New York geboren. Er studierte Elektrotechnik zunächst bis zum Bachelor an der dortigen Universität; für das Studium zum Master und zur Promotion ging er nach Stanford. Nach kurzen Zwischenaufenthalten am Watson Research Center der IBM und am MIT wurde er 1971 Professor an der Stanford University. Nach seiner Emeritierung 1996 gab er noch lange Kurse, mit denen er Schüler für mathematische Probleme interessieren wollte. 2015 erhielt er den Turing Award.
`http://www-ee.stanford.edu/~hellman/`

DIFFIE und HELLMAN machten nur sehr vage Andeutungen, wie ein System mit öffentlichen Schritten aussehen könnte. Es ist zunächst einmal klar, daß ein solches System keine beweisbare absolute Sicherheit

bieten kann, denn die Verschlüsselungsfunktion ist eine bijektive Abbildung zwischen endlichen Mengen, und jeder, der die Funktion kennt, kann zumindest im Prinzip auch ihre Umkehrfunktion berechnen.

Nun läßt sich aber nicht jede theoretisch mögliche Berechnung auch praktisch durchführen; es reicht, wenn wir sicher sein können, daß derzeit niemand die Umkehrfunktion wirklich berechnen kann. Nur darauf beruht die Sicherheit eines Kryptosystems mit öffentlichen Schlüsseln, und leider sind wir uns nie ganz sicher, sondern können nur mit unseren Erfahrungen argumentieren, die umso verläßlicher sind, je länger sich Wissenschaftler im öffentlichen Bereich mit dem Problem beschäftigt haben. Ideal sind also alte, klassische Probleme der Mathematik, an denen schon Generationen von Mathematikern gearbeitet haben.

DIFFIE und HELLMAN bezeichnen eine Funktion, deren Umkehrfunktion nicht mit vertretbarem Aufwand berechnet werden kann, als *Einwegfunktion* und schlagen als Verschlüsselungsfunktion eine solche Einwegfunktion vor. Damit hat man aber noch kein praktikables Kryptosystem, denn bei einer echten Einwegfunktion ist es auch für den legitimen Empfänger nicht möglich, seinen Posteingang zu entschlüsseln. DIFFIE und HELLMAN schlagen deshalb eine Einwegfunktion mit *Falltür* vor, wobei der legitime Empfänger zusätzlich zu seinem öffentlichen Schlüssel noch über einen geheimen Schlüssel verfügt, mit dem er (und nur er) diese Falltür öffnen kann.

Natürlich hängt alles davon ab, ob es solche Einwegfunktionen mit Falltür wirklich gibt. DIFFIE und HELLMAN gaben keine an, und unter den Experten gab es durchaus einige Skepsis bezüglich der Möglichkeit, solche Funktionen zu finden.

Tatsächlich existierten aber bereits damals Systeme, die auf solchen Funktionen beruhten, auch wenn sie nicht in der offenen Literatur dokumentiert waren: Die britische *Communications-Electronics Security Group* (CESG) hatte bereits Ende der sechziger Jahre damit begonnen, nach entsprechenden Verfahren zu suchen, um die Probleme des Militärs mit dem Schlüsselmanagement zu lösen, aufbauend auf (impraktikablen) Ansätzen von AT&T zur Sprachverschlüsselung während des zweiten Weltkriegs. Die Briten sprachen nicht von Kryp-

tographie mit öffentlichen Schlüsseln, sondern von *nichtgeheimer Verschlüsselung,* aber das Prinzip war das gleiche.

Erste Ideen dazu sind in einer auf Januar 1970 datierten Arbeit von JAMES H. ELLIS zu finden, ein praktikables System in einer auf den 20. November 1973 datierten Arbeit von CLIFF C. COCKS. Wie im Milieu üblich, gelangte nichts über diese Arbeiten an die Öffentlichkeit; erst 1997 veröffentlichten die *Goverment Communications Headquarters* (GCHQ), zu denen CESG gehört, einige Arbeiten aus der damaligen Zeit; eine Zeitlang waren sie auch auf dem Server `http://www.cesg.gov.uk/` zu finden, wo sie allerdings inzwischen anscheinend wieder verschwunden sind.

In der offenen Literatur erschien ein Jahr nach der Arbeit von DIFFIE und HELLMAN das erste Kryptosystem mit öffentlichen Schlüsseln: RON RIVEST, ADI SHAMIR und LEN ADLEMAN, damals alle drei am Massachussetts Institute of Technology, fanden nach rund vierzig erfolglosen Ansätzen 1977 schließlich jenes System, das heute nach ihren Anfangsbuchstaben mit RSA bezeichnet wird:

Das System wurde 1983 von der eigens dafür gegründeten Firma RSA Computer Security Inc. patentiert und mit großem kommerziellem Erfolg vermarktet. Das Patent lief zwar im September 2000 aus, die Firma ist aber weiterhin erfolgreich im Kryptobereich tätig.

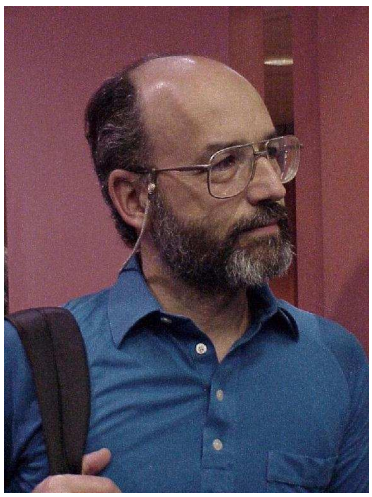
RSA ist übrigens identisch mit dem von laut GCHQ von COCKS vorgeschlagenen System. Die Beschreibung durch RIVEST, SHAMIR und ADLEMAN erschien 1978 unter dem Titel *A method for obtaining digital signatures and public-key cryptosystems* in Comm. ACM **21**, 120–126.

Ausgangspunkt ist die folgende Kombination aus kleinem Satz von FERMAT mit dem erweiterten EUKLIDischen Algorithmus:

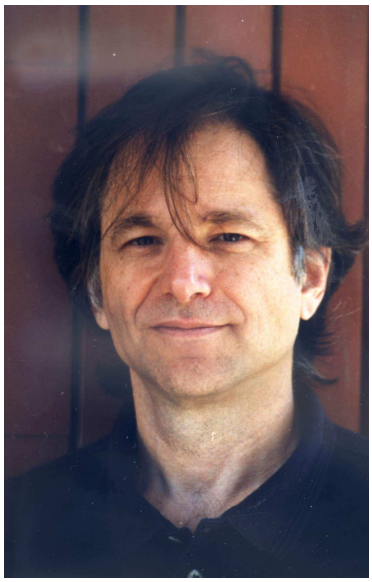
Lemma: Ist p eine Primzahl und $e \in \mathbb{N}$ teilerfremd zu $p-1$, so ist die Abbildung

$$\begin{cases} \{0,\ldots,p-1\} \to \{0,\ldots,p-1\} \\ x \mapsto x^e \bmod p \end{cases}$$

RONALD LINN RIVEST wurde 1947 in Schenectady im US-Bundesstaat New York geboren. Er studierte zunächst Mathematik an der Yale University, wo er 1969 seinen Bachelor bekam; danach studierte er in Stanford Informatik. Nach seiner Promotion 1974 wurde er Assistenzprofessor am Massachussetts Institute of Technology, wo er heute einen Lehrstuhl hat. Er arbeitet immer noch auf dem Gebiet der Kryptographie und entwickelte eine ganze Reihe weiterer Verfahren, auch symmetrische Verschlüsselungsalgorithmen und Hashverfahren. Er ist Koautor eines Lehrbuchs über Algorithmen. Im laufenden Herbstsemester hält er u.a. eine Vorlesung über COVID-19. Seine home page ist `//http://theory.lcs.mit.edu/~rivest/` .



ADI SHAMIR wurde 1952 in Tel Aviv geboren. Er studierte zunächst Mathematik an der dortigen Universität; nach seinem Bachelor wechselte er ans Weizmann Institut, wo er 1975 seinen Master und 1977 die Promotion in Informatik erhielt. Nach einem Jahr als Postdoc an der Universität Warwick und drei Jahren am MIT kehrte er ans Weizmann Institut zurück, wo er bis heute Professor ist. Außer für RSA ist er bekannt sowohl für die Entwicklung weiterer Kryptoverfahren als auch für erfolgreiche Angriffe gegen Kryptoverfahren. Er schlug auch einen optischen Spezialrechner zur Faktorisierung großer Zahlen vor. `http://www.wisdom.weizmann.ac.il/profile/scientists/shamir-profile.html`



LEONARD ADLEMAN wurde 1945 in San Francisco geboren. Er studierte in Berkeley, wo er 1968 einen BS in Mathematik und 1976 einen PhD in Informatik erhielt. Thema seiner Dissertation waren zahlentheoretische Algorithmen und ihre Komplexität. Von 1976 bis 1980 war er an der mathematischen Fakultät des MIT; seit 1980 arbeitet er an der University of Southern California in Los Angeles. Seine Arbeiten beschäftigen sich mit Zahlentheorie, Kryptographie und Molekularbiologie. Er führte nicht nur 1994 die erste Berechnung mit einem „DNS-Computer“ durch, sondern arbeitete auch auf dem Gebiet der Aidsforschung. Heute hat er einen Lehrstuhl für Informatik und Molekularbiologie. `https://adelman.usc.edu`

bijektiv, und ihre Umkehrabbildung ist von der Form

$$\begin{cases} \{0,\dots,p-1\} \to \{0,\dots,p-1\} \\ x \mapsto x^d \bmod p \end{cases}$$

mit einem $d \in \mathbb{N}$.

Beweis: Nach dem erweiterten EUKLIDischen Algorithmus gibt es natürliche Zahlen d und k derart, daß

$$ed - k(p-1) = \mathrm{ggT}(e, p-1) = 1$$

ist und damit $ed = 1 + k(p-1)$. Für jedes zu p teilerfremde $x \in \mathbb{Z}$ ist dann

$$\left(x^e\right)^d = x^{ed} = x^{1+k(p-1)} = x \cdot \left(x^{p-1}\right)^k \equiv x \bmod p$$

nach dem kleinen Satz von FERMAT. Ist x nicht teilerfremd zu p, also ein Vielfaches von p, ist auch x^{ed} eines, so daß $x^{ed} \equiv x \equiv 0 \bmod p$ ist. Damit ist $x^{ed} \equiv x \bmod p$ für alle $x \in \mathbb{Z}$. ∎

Hier ist $\mathcal{B}$ die Menge aller ganzer Zahlen zwischen Null und $p-1$, und $\mathcal{S}$ besteht aus allen Paaren (p, e) aus einer Primzahl p und einer zu $p-1$ teilerfremden natürlichen Zahl $e > 1$. Die Verschlüsselungsfunktion ist

$$f\colon \begin{cases} \mathcal{B} \times \mathcal{S} \to \mathcal{B} \\ \big(m, (p,e)\big) \mapsto m^e \bmod p \end{cases},$$

und die Entschlüsselungsfunktion

$$g\colon \begin{cases} \mathcal{B} \times \mathcal{S} \to \mathcal{B} \\ \big(m, (p,d)\big) \mapsto m^d \bmod p \end{cases}$$

verwendet einen anderen Schlüssel als f. Nach dem gerade bewiesenen Lemma gilt für alle $m \in \mathcal{B}$ und $(p, e) \in \mathcal{S}$ die Gleichung

$$g\Big(f\big(m,(p,e)\big),(p,d)\Big) = m\,,$$

wenn d wie oben aus p und e berechnet wird.

Damit haben wir aber leider noch kein Kryptosystem Problem: Jeder, der außer p und e auch den erweiterten EUKLIDischen Algorithmus kennt, kann d berechnen.

Wenn wir die Primzahl p aber ersetzen durch das Produkt $N = pq$ zweier verschiedener Primzahlen p, q und verlangen, daß e teilerfremd sowohl zu $p-1$ als auch zu $q-1$ ist, ändert sich die Situation ganz entscheidend: Natürlich ist weiterhin

$$x^{1+\ell(p-1)} \equiv x \bmod p \quad \text{und} \quad x^{1+m(q-1)} \equiv x \bmod q$$

für alle $\ell, m \in \mathbb{N}_0$. Wenn wir für $\ell = k(q-1)$ ein Vielfaches von $q-1$ wählen und für $m = k(p-1)$ das entsprechende Vielfache von $p-1$, folgt, daß $x^{1+k(p-1)(q-1)} \equiv x$ ist sowohl modulo p als auch modulo q, also auch modulo $N = pq$ für alle $k \in \mathbb{N}_0$.

Da e teilerfremd zu $(p-1)(q-1)$ vorausgesetzt war, liefert uns EUKLID natürliche Zahlen d, k, so daß

$$ed - k(p-1)(q-1) = 1 \quad \text{und} \quad ed = 1 + k(p-1)(q-1)$$

ist. Somit ist für alle $x \in \{0, 1, \ldots N-1\}$

$$\left(x^e\right)^d = x^{ed} = x^{1+k(p-1)(q-1)} \equiv x \bmod N\,.$$

Für die Menge $\mathcal{B}$ aller ganzer Zahlen von Null bis $N-1$ und die Menge $\mathcal{S}$ aller Paare (N, e), wobei $N = pq$ das Produkt zweier verschiedener Primzahen ist und die natürliche Zahl e teilerfremd zu $p-1$ und zu $q-1$ sein muß, erfüllen

$$f\colon \begin{cases} \mathcal{B} \times \mathcal{S} \to \mathcal{B} \\ \big(m, (N, e)\big) \mapsto m^e \bmod N \end{cases}$$

und

$$g\colon \begin{cases} \mathcal{B} \times \mathcal{S} \to \mathcal{B} \\ \big(m, (N, d)\big) \mapsto m^d \bmod N \end{cases},$$

somit die Gleichung

$$g\Big(f\big(m, (N, e)\big), (N, d)\Big) = m$$

für alle $m \in \mathcal{B}$ und alle $(N, e) \in \mathcal{S}$, sofern d zu (N, e) wie oben berechnet wurde. Insbesondere sind beide Funktionen für festgehaltene Schlüssel bijektive Abbildung von $\mathcal{B}$ nach $\mathcal{B}$.

Zum Verschlüsseln muß man nur N und e kennen, zum Entschlüsseln N und d. Um d aus N und e zu berechnen, muß man aber noch $(p-1)(q-1)$ kennen, und das ist äquivalent zur Kenntnis von p und q:

$$(p-1)(q-1) = pq - (p+q) + 1 = N - (p+q) + 1 \; ;$$

wer N und $(p-1)(q-1)$ kennt, kennt also sowohl pq als auch $p+q$, und kann damit p und q berechnen.

Wegen der Eindeutigkeit der Primzerlegung sind p und q natürlich schon durch N eindeutig bestimmt, und für kleine N lassen sie sich auch leicht finden. Für Zahlen mit mehreren hundert Dezimalstellen wird das Problem allerdings ungleich schwieriger; der derzeitige Rekord in der offenen Literatur für Zahlen, die ein gut gewähltes Produkt zweier ungefähr gleich großer Primzahlen sind, ist die Faktorisierung einer 250-stelligen Zahl (829 Bit) im Februar 2020 durch drei Teams bestehend aus FABRICE BOUDOT, der an der Universität von Limoges, aber auch für das französische Verteidigungsministerium arbeitet, PIERRICK GAUDRY, AURORE GUILLEVIC, EMMANUEL THOME und PAUL ZIMMERMANN aus Nancy und NADIA HENINGER von der University of California in San Diego. Sie geben den Rechenaufwand mit 2700 CPU-Jahren an, bezogen auf einen mit 2,1 GHz getakteten Prozessor.

Selbstverständlich gibt es Geheimdienste mit erheblich besserer Rechnerausstattung als der an Universitäten und Forschungseinrichtungen; insbesondere dürften diese auch Spezialhardware haben, während die hier zitierten Forscher mit (vielen) Standard-PCs arbeiteten. Auf der algorithmischen Seite allerdings ist es unwahrscheinlich, daß Geheimdienste wesentlich mehr wissen als die Experten an Universitäten und Forschungsinstituten; daher kann man hoffen, daß Geheimdienste gut gewählte Produkte zweier Primzahlen mit wesentlich mehr als 1000 Bit nicht faktorisieren können.

Um vor Überraschungen geschützt zu sein, sollte man allerdings darauf noch einen erheblichen Sicherheitszuschlag geben. In der Europäischen Union ist die *Senior Officials Group Information Security* (SOGIS) für entsprechende Empfehlungen zuständig; ihr aktuellstes Dokument stammt vom Januar 2020 und unterscheidet zwischen *legacy* und *recommended mechanisms. Legacy* bedeutet *überliefert, hergebracht*

oder in diesem Zusammenhang auch *Altlast,* d.h. übergangsweise noch toleriert; bis zum 31. Dezember 2025 werden RSA-Moduld mit mindestens 1900 Bit noch toleriert. Empfohlen sind aber heute schon welche mit mindestens drei Tausend Bit.

Ansonsten sollten die Primzahlen ungefähr gleiche Größenordnung haben, denn wenn eine davon sehr klein ist, kann man sie natürlich schnell finden. Sie dürfen allerdings auch nicht zu nahe beieinander liegen, denn sonst führt ein Verfahren von FERMAT zur Faktorisierung: Dieser berechnet die Zahlen $N + x^2$ für $x = 1, 2, 3, \ldots$ so lange, bis eine Quadratzahl $N + x^2 = y^2$ gefunden ist. Dann liefert die dritte binomische Formel die Faktorisierung

$$N = y^2 - x^2 = (y + x)(y - x) = p \cdot q \,.$$

Da $p - q = 2x$ ist, sind hier $\frac{1}{2}\,|p - q|$ Schritte notwendig.

Es gibt allerdings eine Modifikation, mit der es schneller geht: Für große Zahlen N ist es besser, nicht die Zahlen $N + x^2$ für $x \in \mathbb{N}_0$ darauf zu testen, ob $N + x^2 = y^2$ ein Quadrat ist, denn offensichtlich ist $y \geq \sqrt{N}$, und der Abstand zwischen zwei Quadraten dieser Größenordnung ist recht groß: $(y + 1)^2 = y^2 + 2y + 1 > 2\sqrt{N}$. Dagegen sind die Abstände zwischen den Zahlen $N + x^2$ zumindest am Anfang sehr klein. Es ist daher effizienter, wenn man nacheinander die Zahlen y^2 mit $y \geq \sqrt{N}$ darauf testet, ob $y^2 - N$ das Quadrat einer ganzen Zahl x ist. Da x zumindest am Anfang relativ klein ist, geht dieser Test auch schneller als bei der klassischen Vorgehensweise.

Wenn wir davon ausgehen, daß N kein Quadrat ist (was bei RSA selbstverständlich gilt), ist $y = [\sqrt{N}] + 1$ die kleinste ganze Zahl nach $\sqrt{N}$. Der modifizierte Algorithmus verläuft somit wie folgt:

1. Schritt: Setze $y = [\sqrt{N}] + 1$ und $D = y^2 - N$.

2. Schritt: Teste, ob $D = x^2$ Quadrat einer natürlichen Zahl x ist; falls ja, endet der Algorithmus und $N = y^2 - x^2 = (y - x)(y + x)$.

3. Schritt: Ersetze D durch $D + 2y + 1$ und y durch $y + 1$ und gehe zurück zu Schritt 2.

Man beachte, daß nach dem dritten Schritt wieder $D = y^2 - N$ ist, da $(y+1)^2 = y^2 + 2y + 1$ ist. Die Addition von $2y + 1$ zu D geht allerdings, gerade für große Zahlen, deutlich schneller, als die Berechnung des Quadrats $(y + 1)^2$.

Betrachten wir als Beispiel die Zahl $N = 159\,212\,357$. Ihre Quadratwurzel ist ungefähr 12 617,938, also beginnen wir mit $y = 12\,618$ und setzen $D = y^2 - N = 1\,567$. Das ist keine Quadratzahl; daher erhöhen wir D auf $D + 2y + 1 = 26\,804$ und y auf $y + 1 = 12\,619$. Auch die Quadratwurzel des neuen D ist nicht ganzzahlig, also wird im nächsten Durchgang

$$D = 28\,804 + 2 \cdot 12\,619 + 1 = 52\,043 \quad \text{und} \quad y = 12\,619 + 1 = 12\,620\,.$$

Wieder ist D kein Quadrat. Im nächsten Durchgang wird

$$D = 52\,043 + 2 \cdot 12\,620 + 1 = 77\,284 = 278^2$$

und $y = 12\,620 + 1 = 12\,621$. Mit $x = 278$ ist daher

$$N = (y - x)(y + x) = 12343 \cdot 12899\,.$$

Damit hatten wir im vierten Anlauf Erfolg; nach FERMATs klassischer Vorgehensweise wäre dies erst beim 278. Versuch der Fall gewesen.

Für interessierte Leser sei (auch wenn dies nicht wirklich zum Stoff der Vorlesung gehört) gezeigt, wie man den Aufwand nach der modifizierten Methode abschätzen kann:

Angenommen, $N = pq$ mit $p < \sqrt{N} < q$. Dann ist

$$N = pq = \frac{(p+q)^2 - (p-q)^2}{4} = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2\,,$$

der Algorithmus endet also mit $y = \frac{1}{2}(p + q)$, und die Anzahl der getesteten y-Werte ist $\frac{1}{2}(p + q) - [\sqrt{N}]$. Um zu sehen, wie viele das sind, brauchen wir eine Abschätzung für $p + q$:

Lemma: $N = pq$ sei das Produkt zweier verschiedener Zahlen p und q, und $\Delta = p - q > 0$. Dann ist

$$0 < p + q - 2\sqrt{N} < \frac{\Delta^2}{4\sqrt{N}}\,.$$

Beweis: Nach den drei binomischen Formeln ist

$$\Delta^2 = (p-q)^2 = p^2 - 2pq + q^2 = (p+q)^2 - 4pq = (p+q)^2 - 4N$$
$$= (p+q-2\sqrt{N})(p+q+2\sqrt{N})\,.$$

Da Δ^2 und $p+q+2\sqrt{N}$ positiv sind, muß auch $p+q-2\sqrt{N}$ positiv sein, d.h. $p+q > 2\sqrt{N}$. (Dies ist, für unseren speziellen Fall, der allgemeine Satz, wonach das geometrische Mittel $\sqrt{xy}$ zweier positiver reeller Zahlen größer oder gleich dem arithmetischen ist mit Gleichheit nur im Fall $x = y$.) Die obige Gleichung für Δ^2 zeigt daher, daß

$$0 < p+q-2\sqrt{N} < \frac{\Delta^2}{p+q+2\sqrt{N}} < \frac{\Delta^2}{4\sqrt{N}}$$

ist. ∎

Wir interessieren uns für die Zahl $\frac{1}{2}(p+q) - [\sqrt{N}]$; diese ist ungefähr gleich

$$\frac{1}{2}(p+q) - \sqrt{N} < \frac{\Delta^2}{8\sqrt{N}}\,.$$

Ist also $\Delta \leq c\sqrt[4]{N}$, so brauchen wir höchstens $c^2/8$ Versuche. Bei den Zahlen, um die es bei RSA-Moduln geht, nimmt jeder einzelne Versuch nur wenig Zeit in Anspruch; auch für ein c in der Größenordnung von mehreren Tausend ist die Faktorisierung daher leicht durchführbar. Damit ist klar, daß die Differenz der beiden Primfaktoren eines RSA-Moduls deutlich größer als die vierte Wurzel von N sein muß. Für ein N mit 2000 Bit heißt dies, daß sich die beiden Faktoren schon deutlich vor dem 1500. Bit in mindestens einem Bit unterscheiden müssen.

Empfohlen wird, daß die beiden Primfaktoren p, q zufällig und unabhängig voneinander erzeugt werden und aus einem Bereich stammen, in dem

$$\varepsilon_1 < |\log_2 p - \log_2 q| < \varepsilon_2$$

gilt. Als *Anhaltspunkte* werden dabei die Werte $\varepsilon_1 = 0{,}1$ und $\varepsilon_2 = 30$ vorgeschlagen; ist p die kleinere der beiden Primzahlen, soll also

$$10^{-3}p \approx 2^{-10}p < q < 2^{30}p \approx 10^9 p$$

gelten.

Für den Exponenten e wurde lange Zeit der kleinstmögliche Wert drei verwendet; das ist nicht nur problematisch, wenn die zu verschlüsselnde Nachricht x so klein ist, daß $c = x^3 < N$ ist, so daß sich x einfach als $\sqrt[3]{c}$ berechnen läßt. Probleme gibt es auch, wenn die gleiche Nachricht als Rundbrief an mehrere Adressaten verschickt wird: Falls ein Angreifer die Nachrichten an drei Adressaten mit RSA-Moduln N_1, N_2 und N_3 abfängt, kennt er x^3 mod N_i für $i = 1, 2, 3$ und kann nach dem chinesischen Restesatz x^3 mod $N_1N_2N_3$ berechnen. Da x kleiner ist als jedes N_i, ist $x^3 < N_1N_2N_3$, und er kann x als dritte Wurzel in $\mathbb{Z}$ berechnen.

Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt daher, daß e nicht zu klein sein darf, sondern die Ungleichungen $2^{16} + 1 \leq e < 2^{256}$ erfüllen sollte. (Bei zu großen werden von e besteht die Gefahr, daß d klein wird, was zu gefährlichen Angriffsmöglichkeiten führen kann.)

Auch bei Beachtung aller dieser Vorschriften und Empfehlungen ist das Verfahren so wie beschrieben immer noch unbrauchbar: Nehmen wir an, wir verschicken einfach eine (streng geheime) Antwort *Ja* oder *Nein.* Ein Gegner muß dann nur die beiden Nachrichten *Ja* und *Nein* verschlüsseln und sehen, welche zum abgefangenen Chiffretext führt. Um dieses Problem zu umgehen, „opfert“ man einen Teil der möglichen Bits und setzt die höchsten mindestens 128 Bit der Nachricht auf Zufallswerte. Dann kann jeder Block auf 2^{128} verschiedene Weisen verschlüsselt werden, und derzeit geht man davon aus, daß 2^{128} Versuche jenseits der Möglichkeiten eines jeden Gegners liegen. Die Nachricht selbst wird natürlich einfach in irgendeiner Weise binär kodiert, meist im ASCII-Code, und die gesamte Bitfolge einschließlich der Zufallsbits wird dann als natürliche Zahl interpretiert.

Man kann übrigens oft kleinere öffentliche Exponenten d zu gebenen öffentlichen Schlüsseln (N, e) bekommen, wenn man den erweiterten EUKLIDischen Algorithmus nicht auf e und $(p-1)(q-1)$ anwendet, sondern auf e und ein kleineres gemeinsames Vielfaches von $p-1$ und $q-1$. Man überzeugt sich leicht davon, daß alle obigen Beweise für beliebige gemeinsame Vielfache von $p-1$ und $q-1$ funktionieren.

Für die praktische Anwendung des RSA-Verfahrens müssen wir uns noch überlegen, wie man die Potenzen x^e mod N *bzw.* x^d mod N effizient berechnen kann. Nehmen wir der Einfachheit halber an, wir rechnen mit einem Modul N von 2 048 Bit, was heute ja gerade noch toleriert wird.

Damit haben auch die zu übermittelnde Nachrichtenblöcke eine Länge von mindestens 2 048 Bit, also 256 Byte, und die e-te Potenz der entsprechenden Zahlen hat die e-fache Länge. Für die Verschlüsselung können wir einen kleinen Exponenten e wählen, für die Entschlüsselung allerdings wird der Exponent d mit an Sicherheit grenzender Wahrscheinlichkeit in der Größenordnung von N liegen, so daß m^d eine Bitlänge von etwa $(2\,048)^2$ Bit hat, also ein halbes Megabyte.

Dafür hat ein heutiger Computer natürlich mehr als genug Speicherplatz, aber er muß die Zahlen auch berechnen, und zumindest wenn man das in der dümmstmöglichen Weise durchführt, indem man sukzessive die Potenzen $m, m^2, m^3, \ldots$ berechnet, überfordern auch deutlich kleinere Exponenten selbst die besten heutigen Supercomputer um Größenordnungen.

Tatsächlich gibt es aber keinen Grund, die natürliche Zahl m^d wirklich zu berechnen: Wir brauchen schließlich nur m^d mod N. Außerdem käme hoffentlich auch kein Leser auf die dumme Idee, die Zahl 3^{32} durch 31-fache Multiplikation mit Drei zu berechnen: Da $32 = 2^5$ ist, läßt sich das Ergebnis viel schneller als

$$3^{32} = \left(\left(\left(\left(3^2\right)^2\right)^2\right)^2\right)^2$$

durch nur fünfmaliges Quadrieren berechnen.

Entsprechend können wir für jede gerade Zahl $n = 2m$ die Potenz x^n als Quadrat von x^m berechnen. Für einen ungeraden Exponenten e ist $e-1$ gerade, wenn wir also m^e als Produkt von m und m^{e-1} darstellen, können wir zumindest im nächsten Schritt wieder die Formel für gerade Exponenten verwenden. Da uns das Ergebnis nur modulo N interessiert, können wir zudem nach jeder Multiplikation und jeder Quadrierung

das Ergebnis modulo N reduzieren; auf diese Weise entsteht nie ein Zwischenergebnis, das größer ist als N^2.

Dies führt auf folgenden rekursiven Algorithmus zur Berechnung von $m^e \bmod N$:

Falls $e = 2f$ gerade ist, berechne man zunächst $m^f \bmod N$ nach diesem Algorithmus und quadriere das Ergebnis modulo N; andernfalls gibt es im Falle $e = 1$ nichts zu tun, und für $e > 1$ berechne man zunächst $m^{e-1} \bmod N$ und multipliziere das Ergebnis modulo N mit m.

Falls e eine Zahl mit r Bit ist, erfordert dieser Algorithmus $r - 1$ Quadrierungen und höchstens r, im Mittel rund $r/2$ Multiplikationen mit m. Für einen Exponenten mit 2 048 Bit brauchen wir also im Mittel rund 3 072 Multiplikationen, auf keinen Fall aber mehr als 4 096, und damit wird ein heutiger Computer problemlos fertig.

Bleibt noch die Frage: Wie multiplizieren wir zwei Zahlen mit einer Länge von mehreren Tausend Bit?

Für Taschenrechner wie auch für die 32- oder 64-Bit-Register eines Computers sind sie natürlich viel zu groß. Trotzdem ist die vielleicht erstaunliche Antwort auf obige Frage, daß wir genau so vorgehen können, wie wir es in der Schule gelernt haben: Zwar gibt es Multiplikationsalgorithmen, die asymptotisch schneller sind als die Schulmethode, aber tatsächlich schneller werden sie erst, wenn die Zahlen eine Bitlänge haben, die eher bei Millionen liegt als bei bloßen Tausenden.

Einen Unterschied zur Schule sollten wir freilich machen: Während uns in der Grundschule das kleinen Einmaleins eingepaukt wird, also die Produkte der Zahlen von Eins bis Zehn untereinander, sind in den CPUs unserer Computer Algorithmen implementiert, die zwei 32-Bit-Zahlen zu einer 64-Bit-Zahl multiplizieren oder, falls der Computer hinreichend neu ist, zwei 64-Bit-Zahlen zu einer 128-Bit-Zahl. Wir sollten die Zahlen also nicht im Zehnersystem betrachten, sondern im Ziffernsystem mit Basis 2^{32} oder 2^{64}.

Nach jeder Multiplikation muß das Ergebnis modulo N reduziert werden; wir müssen also durch N dividieren. Auch dazu können wir *im Prinzip* genauso vorgehen wie in der Schule, haben dabei allerdings das

Problem, daß das in der Schule gelehrte Divisionsverfahren kein Algorithmus ist: Wir müssen schließlich in jedem Schritt die nächste Ziffer des Quotienten *erraten* und sehen erst nach Multiplikation mit dem Divisor oder sogar erst nach Subtraktion dieses Produkts vom Dividenden, ob wir das korrekte Ergebnis haben.

Zum Glück läßt sich dieses „Erraten“ selbst für beliebige Basen des Ziffernsystems zumindest insoweit algorithmisch machen, daß das Ergebnis nie um mehr als zwei danebenliegt, und auch ein Fehler von zwei nur mit verschwindend geringer Wahrscheinlichkeit auftritt. Da es inzwischen viele Unterprogrammpakete und auch Programme gibt, in denen Algorithmen zum Rechnen mit Langzahlen implementiert sind, sei hier nicht auf Einzelheiten eingegangen; Interessenten finden diese zusammen mit allen Beweisen z.B. in Abschnitt 4.3 des bereits im Zusammenhang mit der Aufwandsabschätzung für den EUKLIDischen Algorithmus zitierten Buchs

> DONALD E. KNUTH: The Art of Computer Programming, *vol. 2:* Seminumerical Algorithms, *Addison Wesley,*, ^{3}1997

Ein großer Vorteil eines Verfahrens mit öffentlichen Schlüsseln gegenüber einem klassischen Kryptoverfahren ist die Möglichkeit elektronischer Unterschriften. Angenommen, der Besitzer des privaten Exponenten d zum öffentlichen Schlüsseln (N, e) möchte eine Nachricht x unterschreiben. Dann kann er dazu einfach $u = x^d \bmod N$ berechnen. Da niemand außer ihm d kennt, kann nur er diese Zahl bestimmen. Jeder, der den öffentlichen Schlüssel kennt, kann aber $u^e \equiv x^{de} \equiv x \bmod N$ berechnen und sich davon überzeugen, daß er wirklich das Ergebnis x erhält. Solche elektronischen Unterschriften sind innerhalb der Europäischen Union rechtsverbindlich sofern sie den jeweils geltenden Vorschriften genügen. Derzeit ist das die sogenannte eIDAS-Verordnung *(**e**lectronic **ID**entification, **A**uthentication and Trust **S**ervices)* vom 23. Juli 2014.

Der Wert einer elektronischen Unterschrift steht und fällt damit, daß der korrekte öffentliche Schlüssel des Unterschreibenden bekannt ist: Falls es jemandem gelingt, einem anderen einen falschen Schlüssel für eine

Person zu unterschieben, kann er beliebig viele Unterschriften in deren Namen leisten. Zu elektronischen Unterschriften (und allgemein zur Kryptographie mit öffentlichen Schlüsseln) gehört daher eine *public key infrastructure* mit zertifizierten Schlüsseln. An der Spitze stehen einige wenige Zertifizierungsagenturen, deren öffentliche Schlüssel weithin bekannt sind (insbesondere sind sie in den gängigen Browsern gespeichert), und diese unterschreiben für Ihre Kunden Zertifikate, die Namen, öffentlichen Schlüssel, *usw.* enthalten. Oft ist das Verfahren mehrstufig, d.h. der Inhaber eines Zertifikats kann auf dessen Grundlage selbst Zertifikate ausstellen. Erst mit zertifizierten Unterschriften wird ein sicherer Handel über das Internet möglich: Da RSA zur Verschlüsselung langer Texte zu aufwendig ist, verwendet man dazu symmetrische Verfahren, typischerweise den sogenannten *Advanced Encryption Standard* AES, der mit eine Schlüssellänge von 128 Bit arbeitet. Wenn der Kunde ein Zertifikat mit dem öffentlichen Schlüssel des Händlers bekommt, kann er ihm einen damit verschlüsselten AES-Schlüssel schicken, den die beiden dann zur weiteren Kommunikation verwenden. (Das tatsächlich verwendete Verfahren TLS/SSL ist aufwendiger; hier wirken beide Seiten an der Erstellung des Schlüssels mit.)

Zum Schluß dieses Kapitels möchte ich noch darauf hinweisen, daß sichere Kryptographie keineswegs nur Mathematik ist; auch das beste Kryptoverfahren wird wertlos, wenn sich ein Gegner Zugriff auf Ihren Computer verschafft oder die Routine zur Erzeugung einer „zufälligen“ Zahl als Ausgangspunkt zur Primzahlsuche manipuliert oder . . .
Nicht nur NSA hat viele Möglichkeiten.