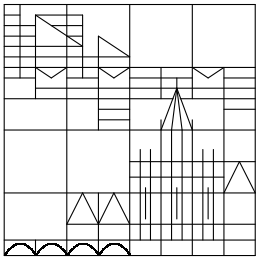

Universität Konstanz

Zufalls–Primzahlen und Kryptographie

Volker Strassen

Konstanzer Schriften in Mathematik und Informatik
Nr. 7, März 1996

ISSN 1430–3558

Zufalls-Primzahlen und Kryptographie*

V. Strassen, Universität Konstanz
Fakultät Mathematik und Informatik

7/1996

Dieser Vortrag handelt von algorithmischen Problemen der elementaren Zahlentheorie und einer Revolution der Kryptographie in den siebziger Jahren. Es werden kaum Mathematik- und überhaupt keine Informatik-Kenntnisse vorausgesetzt.

Ringe und Körper

Ich beginne mit der Diskussion einer grundlegenden mathematischen Struktur, der eines *kommutativen Rings*. Ein solcher Ring ist eine Menge, für deren Elemente eine Addition und eine Multiplikation erklärt sind, so dass sämtliche Rechenregeln gelten, die Sie für das Rechnen mit ganzen Zahlen kennen. Der Prototyp eines solchen Rings ist also der Ring $\mathbf{Z}$ der ganzen Zahlen.

Es gibt neben $\mathbf{Z}$ noch viele für die Mathematik und ihre Anwendungen wichtige Ringe, z.B. die Ringe $\mathbf{Z}_n$ (n eine positive ganze Zahl), die ich jetzt definieren möchte. Als Menge besteht $\mathbf{Z}_n$ einfach aus den natürlichen Zahlen kleiner als n,

$$\mathbf{Z}_n := \{0, 1, \ldots n-1\}.$$

Wie wird addiert und multipliziert? Wir multiplizieren zwei Zahlen a, b in $\mathbf{Z}_n$ so, dass wir sie zunächst als ganze Zahlen, also in $\mathbf{Z}$ multiplizieren. Damit erhalten wir in der Regel natürlich eine Zahl, die viel zu gross ist, um als Element von $\mathbf{Z}_n$ in Frage zu kommen. Wir ziehen dann so oft n ab, bis wir eine Zahl in $\{0, 1, \ldots n-1\}$ erhalten und erklären diese (eindeutig bestimmte) Zahl zum Produkt von a und b im Ring $\mathbf{Z}_n$. Mit anderen Worten: Das Produkt von a, b im Ring $\mathbf{Z}_n$ ist der Rest, den das gewöhnliche Zahlenprodukt von a und b nach (ganzzahliger) Division durch n übrig lässt. Bezeichnen wir, wie es üblich ist, den Rest einer Zahl a nach Division durch n mit $a \; mod \; n$, so können wir die Ringmultiplikation in $\mathbf{Z}_n$ durch

$$\underbrace{a \cdot b}_{in \; \mathbf{Z}_n} \quad := \quad \underbrace{a \cdot b}_{in \; \mathbf{Z}} \; mod \; n$$

*Der vorliegende Artikel ist bis auf geringfügige Änderungen die Ausarbeitung eines Vortrages, den der Autor am 10. Oktober 1995 vor der Deutschen Akademie der Naturforscher Leopoldina in Halle gehalten hat. Die Ausarbeitung wird im Jahrbuch 1995 der Akademie veröffentlicht.

beschreiben. Ebenso ist die Addition erklärt: Wir addieren a und b in $\mathbf{Z}$ und nehmen den Rest der Summe nach Division durch n. Das ist hier natürlich besonders leicht, da wir höchstens einmal n abziehen müssen.

In Konstanz gibt es einen Studenten, der sich ein T-Shirt angefertigt hat, das vorne so beschriftet ist:

$$5 \cdot 9 = 1.$$

Kommt er auf einen zu, so möchte man in Erregung geraten ob dieser Provokation. Aber wie beim Doppler-Effekt beruhigt sich die Pulsfrequenz, sobald der junge Mann vorübergeht, denn auf der Rückseite erkennt man die Weisheit des Hemdes:

$$in \quad \mathbf{Z}_{11}.$$

In der Tat, das gewöhnliche Zahlenprodukt von 5 und 9 ist 45, nach Division durch 11 erhalten wir also 1. Ebenso hätte er $3 \cdot 4 = 1$ oder $1 \cdot 1 = 1$ schreiben können. (Letzteres wäre ihm wohl zu wenig provokativ.) Natürlich kommt nicht immer 1 heraus, 4^2 z.B. ist 5 in $\mathbf{Z}_{11}$.

Wie schon bemerkt, können Sie mit Addition und Multiplikation in $\mathbf{Z}_n$ unbekümmert umgehen, denn die Rechenregeln, wie Sie sie für die ganzen Zahlen kennen, gelten auch hier. Z.B. ist immer $(a+b)+c = a+(b+c)$ und $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, ferner $a+b = b+a$ und $a \cdot b = b \cdot a$, ferner $0+a = a$ und $1 \cdot a = a$ sowie $a \cdot (b+c) = a \cdot b + a \cdot c$. Ausserdem gibt es zu jeder Zahl a in $\mathbf{Z}_n$ genau eine additive Inverse, d.h. eine Zahl in $\mathbf{Z}_n$, die mit ihr die Summe 0 gibt und die man deshalb mit $-a$ bezeichnet. -1 etwa ist die Zahl $n-1$, denn $1+(n-1) = 0$ nach unserer oben gegebenen Definition der Summe in $\mathbf{Z}_n$. Natürlich kommt die gewöhnliche ganze Zahl -1 in $\mathbf{Z}_n$ gar nicht vor. -1 als Element des Rings $\mathbf{Z}_n$ ist einfach eine Notation für $n-1$, die auf die Richtigkeit der Gleichung $1+(-1) = 0$ hindeutet.

Weil jede Zahl in $\mathbf{Z}_n$ eine additive Inverse besitzt, kann man in $\mathbf{Z}_n$ (und in jedem andern Ring) nicht nur addieren und multiplizieren, sondern auch subtrahieren ($a - b := a + (-b)$), und für die Subtraktion gelten wieder die vertrauten Regeln. Unter den kommutativen Ringen sind die sogenannten *Körper* dadurch ausgezeichnet, dass man ausserdem noch dividieren kann. Anders ausgedrückt: Jedes von 0 verschiedene Element a eines Körpers besitzt eine multiplikative Inverse, das ist ein Element b mit $a \cdot b = 1$. Die multiplikative Inverse b ist dann eindeutig bestimmt und wird mit a^{-1} (oder mit $1/a$) bezeichnet. Aus dem Alltag wissen Sie, wie bequem es ist ist, dividieren zu können. Körper sind also besonders bequeme Ringe.

$\mathbf{Z}$ ist kein Körper. Es gibt z.B. keine ganze Zahl b mit $7 \cdot b = 1$. Der Prototyp eines Körpers ist der Körper der rationalen Zahlen, dessen *raison d'etre* ja gerade darin besteht, eine möglichst eng anliegende Erweiterung des Rings der ganzen Zahlen zu einem Körper zu sein, zu einem Ring also, der die Division gestattet.

Natürlich stellt sich die Frage, welche von den Ringen $\mathbf{Z}_n$ Körper sind. Sicher nicht alle! $\mathbf{Z}_{12}$ z.B. ist kein Körper. In $\mathbf{Z}_{12}$ gilt nämlich die Gleichung

$$3 \cdot 4 = 0.$$

Wäre $\mathbf{Z}_{12}$ ein Körper, so könnten wir beide Seiten der Gleichung mit 4^{-1}, der multiplikativen Inversen von 4, multiplizieren und erhielten mit den üblichen Rechenregeln $3 = 0$, was nicht der Fall ist.

Die Schlussweise lässt sich verallgemeinern: In einem Körper ist das Produkt zweier von Null verschiedener Zahlen stets wieder $\neq 0$. Auf die Ringe $\mathbf{Z}_n$ angewandt bedeutet dies, dass $\mathbf{Z}_n$ sicher dann kein Körper ist, wenn sich n als Produkt zweier kleinerer positiver Zahlen darstellen lässt (wie oben $12 = 3 \cdot 4$), also wenn n keine Primzahl ist. Umgekehrt zeigen wir nun, dass $\mathbf{Z}_n$ für primes n tatsächlich immer ein Körper ist, so dass wir das schöne Kriterium

$$n \ \textit{prim} \quad \Longleftrightarrow \quad \mathbf{Z}_n \ \textit{Körper} \tag{1}$$

erhalten. Der klassische Beweis (aus dem 17. Jahrhundert) der Körpereigenschaft bezwingt durch seine Einfachheit und Eleganz: Wir nehmen an, n sei eine Primzahl, und zeigen, dass jede von 0 verschiedene Zahl a in $\mathbf{Z}_n$ eine multiplikative Inverse besitzt, also ein b mit $a \cdot b = 1$ in $\mathbf{Z}_n$. Dazu multiplizieren wir a der Reihe nach mit allen Zahlen aus $\mathbf{Z}_n$ im Sinne der Ring-Multiplikation von $\mathbf{Z}_n$. Die so erhaltenen Zahlen

$$a \cdot 0, a \cdot 1, \ldots, a \cdot (n-1)$$

liegen nach Konstruktion alle in $\mathbf{Z}_n$. Ich behaupte: Sie sind sämtlich voneinander verschieden. Andernfalls hätten wir etwa $a \cdot b = a \cdot c$ für gewisse b, c mit $0 \leq b < c < n$. Da in $\mathbf{Z}_n$ die üblichen Rechenregeln gelten, folgt hieraus $a \cdot (c - b) = 0$. Diese Gleichung ist in $\mathbf{Z}_n$ zu interpretieren. Auf Grund der Definition der Multiplikation in $\mathbf{Z}_n$ kommen wir zu dem Schluss, dass die in $\mathbf{Z}$ berechnete ganze Zahl $a \cdot (c-b)$ bei Division durch n den Rest 0 liefert, also ein Vielfaches von n ist. Es gibt deshalb eine positive ganze Zahl x mit

$$a \cdot (c - b) = x \cdot n.$$

Dies ist nun eine Gleichung im Ring $\mathbf{Z}$ der ganzen Zahlen. Auf beiden Seiten stehen nur positive Zahlen, und die Zahlen auf der linken Seite sind beide $< n$. Zerlegen wir deshalb a, $(c-b)$ und x in Primfaktoren, so entsteht links ein Produkt aus lauter Primzahlen $< n$, während rechts die Primzahl n vorkommt. Das ist ein Widerspruch zur Eindeutigkeit (bis auf die Reihenfolge) der Primfaktorzerlegung natürlicher Zahlen. Damit haben wir gezeigt, dass die n Zahlen $a \cdot 0, a \cdot 1, \ldots, a \cdot (n-1)$ in $\mathbf{Z}_n$ tatsächlich alle verschieden sind, also ganz $\mathbf{Z}_n = \{0, \ldots, n-1\}$ ausfüllen:

$$\{a \cdot 0, a \cdot 1, \ldots, a \cdot (n-1)\} = \{0, 1, \ldots, n-1\}. \tag{2}$$

Nun sind wir aber fertig, denn die Zahl 1 kommt in der rechten Menge vor, also auch in der linken, lässt sich also als Produkt $a \cdot b$ in $\mathbf{Z}_n$ darstellen, was zu zeigen war.

Sie sehen: Primzahlen sind nicht nur wegen des Satzes über die eindeutige Primfaktorzerlegung interessant, sondern z.B. auch, weil die Primalität von n darüber entscheidet, ob der endliche Ring $\mathbf{Z}_n$ ein Körper ist.

Primzahlen

Wir wollen uns in diesem Abschnitt mit der Frage beschäftigen, wie man einer natürlichen Zahl n ansieht, ob sie prim ist oder nicht. Wir können davon ausgehen, dass n ungerade ist, denn unter den geraden Zahlen ist 2 die einzige Primzahl. Für ungerades n ist $\frac{n-1}{2}$ wieder eine ganze Zahl, und ich möchte in diesem Vortrag annehmen, dass auch $\frac{n-1}{2}$ ungerade sei. Das bedeutet $n \; mod \; 4 = 3$, schliesst also jedes zweite ungerade n von der Betrachtung aus. Es vereinfacht aber die folgenden Überlegungen. Ungerade Zahlen n, für die auch $\frac{n-1}{2}$ ungerade ist, wollen wir zur Abkürzung *erlaubt* nennen.

Eine Zahl n ist prim, gewenn[1] sie keinen echten Teiler hat, und das können wir dadurch prüfen, dass wir n durch jede ganze Zahl a mit $1 < a < n$ teilen und nachsehen, ob wir stets einen von 0 verschiedenen Rest erhalten. Schon ERATHOSTENES (etwa 276 bis 194 v.Chr.) hat bemerkt, dass man sich dabei auf Zahlen $1 < a \leq \sqrt{n}$ beschränken kann. Ist nämlich n keine Primzahl, so gibt es eine Produktdarstellung $n = a \cdot b$ mit $1 < a, b < n$. Die Zahlen a und b können aber nicht beide grösser als $\sqrt{n}$ sein (sonst wäre ja das Produkt grösser als $\sqrt{n} \cdot \sqrt{n} = n$). Also hat n einen Teiler $\leq \sqrt{n}$.

Zusammen mit anderen Vereinfachungen, die ERATHOSTENES vorgeschlagen hat[2], ist das oben beschriebene Divisionsverfahren recht effizient für Zahlen n etwa in der Grössenordnung von einer Million oder auch einer Milliarde, also für sechs- oder auch neun-stellige Zahlen. Mein Interesse gilt nun aber viel grösseren Zahlen, sagen wir tausend-stelligen. Erinnern wir uns daran, dass die Anzahl der Atome im Weltall auf weniger als 10^{80} geschätzt wird und dass 10^{80} eine 80-stellige Zahl ist, so sehen wir: 1000-stellige Zahlen kommen in der Natur als Anzahlen (disjunkter Objekte) nicht vor, und die Mathematik dieser Zahlen ist keine Naturwissenschaft. Solche Zahlen codieren vielmehr mathematische Strukturen wie die Ringe $\mathbf{Z}_n$ und andere (z.B. geheime) Informationen. Ihre Mathematik ist Strukturwissenschaft.

Wie testen wir eine 1000-stellige Zahl n auf Primalität? Sicher nicht mit dem obigen Divisionsverfahren: Eine Division mit Rest 1000-stelliger Zahlen ist für einen modernen Computer zwar kein Problem, wohl aber die Anzahl der durchzuführenden Divisionen, nach ERATHOSTENES ungefähr $\sqrt{n}$, also eine etwa 500-stellige Zahl. Allein schon das Zählen bis zu einer solchen Zahl ist völlig unmöglich und wird es, unabhängig von zukünftigen Technologien, wohl auch bleiben. Im Anblick dieser Riesen-Zahlen müssen wir unsere Schulerfahrung auf den Kopf stellen: Dividieren ist einfach, Zählen unmöglich.

Um bei der Suche nach einem brauchbaren Primtest auf neue Ideen zu kommen, ziehen wir einen alten Satz[3] von FERMAT (1601-1665) zu Rate:

Satz (FERMAT)

$$n \; prim \quad \Longrightarrow \quad \left.\begin{array}{c} a^{n-1} = 1 \\ \text{für alle } a \neq 0 \end{array}\right\} \; in \; \mathbf{Z}_n$$

Für den Nicht-Mathematiker klingt dieses Resultat vielleicht etwas skurril: Ist n eine Primzahl und nimmt man irgendeine von 0 verschiedene Zahl aus $\mathbf{Z}_n$ in die $(n-1)$-te Potenz (im Sinne der für $\mathbf{Z}_n$ erklärten Multiplikation), so kommt immer 1 heraus. Was kann man damit anfangen? Wir werden es später sehen. Zuvor möchte ich den FERMATschen Satz *beweisen*. Erinnern wir uns daran, dass wir die Mengengleichung (2) genau unter den jetzigen Voraussetzungen an n und a hergeleitet haben. Natürlich stehen die Zahlen von 0 bis $n-1$ auf der linken Seite von (2) in irgendeiner unordentlichen Reihenfolge. Auf beiden Seiten der Gleichung steht aber am Anfang die Zahl 0. Diese beiden Nullen lassen wir weg und multiplizieren auf jeder Seite die verbleibenden Zahlen in $\mathbf{Z}_n$. Da wir uns auf die gewohnten Rechenregeln stützen können, kommt es auf Klammerung und Reihenfolge nicht an und wir erhalten nach Vertauschung der Seiten

$$\begin{aligned} 1 \cdot \ldots \cdot (n-1) &= a \cdot 1 \cdot \cdot \ldots \cdot a \cdot (n-1) \\ &= a^{n-1} \cdot 1 \cdot \ldots \cdot (n-1). \end{aligned}$$

Nun ist n eine Primzahl, also $\mathbf{Z}_n$ ein Körper. Wir können deshalb die Zahlen $n-1, n-2, \ldots, 2$ der Reihe nach aus der Gleichung kürzen (indem wir mit ihren multiplikativen Inversen multiplizieren) und erhalten

$$1 = a^{n-1} \cdot 1 = a^{n-1},$$

die Behauptung des FERMATschen Satzes.

Als erste Anwendung ergibt sich eine Formel für die multiplikative Inverse in Körpern $\mathbf{Z}_n$: Ist n prim und a in $\mathbf{Z}_n$ von 0 verschieden, so gilt nach FERMAT $a \cdot a^{n-2} = a^{n-1} = 1$ in $\mathbf{Z}_n$. Nach Definition der multiplikativen Inversen ist also

$$a^{-1} = a^{n-2} \quad in \ \ \mathbf{Z}_n. \tag{3}$$

Z.B. ist in $\mathbf{Z}_{11}$

$$5^{-1} = 5^9 = ((5^2)^2)^2 \cdot 5 = 9, \tag{4}$$

ein Ergebnis, dessen Richtigkeit schon auf dem Konstanzer T-Shirt konstatiert wird.

Bei der (kurzen) Herleitung der Inversenformel (3) haben wir gar nicht benutzt, dass n eine Primzahl ist, sondern nur, dass die Konklusion des FERMATschen Satzes gilt. Aus dieser folgt deshalb schon, dass jedes von 0 verschiedene a in $\mathbf{Z}_n$ eine multiplikative Inverse besitzt, dass also $\mathbf{Z}_n$ ein Körper und damit n eine Primzahl ist. Diese Überlegung zeigt, dass wir den Implikationspfeil $\Rightarrow$ im Satz von FERMAT auch umkehren können und damit ein weiteres Primalitätskriterium gewonnen haben. Was ist das wert?

Zunächst führen wir eine suggestive, wenn auch etwas ungenaue Sprachregelung ein: Wir wollen Algorithmen[4], die sich auf n beziehen, *effizient* nennen, wenn sie für 1000-stelliges n praktisch durchführbar sind. Z.B. lässt sich die Multiplikation im Ring $\mathbf{Z}_n$ effizient berechnen, weil für die gewöhnliche Multiplikation 1000-stelliger Zahlen und für die Division mit Rest einer 2000-stelligen durch eine 1000-stellige Zahl praktikable Algorithmen zur Verfügung stehen. Das

Gleiche gilt für Addition und Subtraktion in $\mathbf{Z}_n$. Wie steht es mit einer Potenzierung vom Typ a^{n-1}? Hier sieht es so aus, als müssten wir a etwa 10^{1000} mal in $\mathbf{Z}_n$ mit sich selbst multiplizieren, was sicher nicht möglich ist. Nehmen wir aber einmal an, der Exponent $n-1$ sei selbst eine Zweierpotenz: $n-1=2^s$. Dann können wir doch $a^{n-1}=a^{2^s}$ ausgehend von a durch s-faches Quadrieren in $\mathbf{Z}_n$ berechnen, und das ist ein effizientes Verfahren, denn s ist für 1000-stelliges n nur 4-stellig. Dieser Gedanke lässt sich ohne grosse Schwierigkeiten auf Exponenten verallgemeinern, die keine Zweierpotenzen sind (vergleiche (4)) und führt so zu einem effizienten Algorithmus zur Berechnung von a^{n-1}. Ebenso lässt sich natürlich $a^{-1}=a^{n-2}$ in $\mathbf{Z}_n$ effizient berechnen, und wir merken uns: In einem Ring $\mathbf{Z}_n$ sind Addition, Subtraktion, Multiplikation und die Berechnung hoher Potenzen effizient, in einem Körper $\mathbf{Z}_n$ ausserdem die Division[5] .

Wie wir gerade gesehen haben, ist jede einzelne Potenzberechnung im FERMATschen Primtest effizient. Wie beim Test des ERATHOSTENES scheitern wir aber auch hier an der riesigen Anzahl der Einzelprüfungen: Es steht uns nicht einmal die Reduktion von n auf $\sqrt{n}$ zur Verfügung.

Zufall

Einen Ausweg aus dieser Schwierigkeit bietet ein Paradigma, das in den angewandten Wissenschaften schon seit langem seinen festen Platz hat, die Idee des *statistischen Tests*. Die Grundlage eines solchen Primtests bildet der folgende Satz, dessen erster Teil von EULER (1707-1783) stammt. Ich erinnere daran, dass wir n 'erlaubt' nennen, wenn n und $\frac{n-1}{2}$ beide ungerade sind, und dass -1 in $\mathbf{Z}_n$ die additive Inverse von 1, also eine Abkürzung für $n-1$ ist.

Satz: *Sei n eine erlaubte Zahl. Dann gilt:*

1.	*n prim*	$\Longrightarrow$	$a^{\frac{n-1}{2}}=\pm 1$ *für alle* $a\neq 0$
2.	*n nicht prim*	$\Longrightarrow$	$a^{\frac{n-1}{2}}=\pm 1$ *für höchstens die Hälfte der* $a\neq 0$.

(Die Gleichungen sind in $\mathbf{Z}_n$ zu lesen.) Die erste Aussage folgt aus dem Satz von FERMAT: Mit der Abkürzung $b:=a^{\frac{n-1}{2}}$ haben wir in $\mathbf{Z}_n$ unter Verwendung der üblichen Rechenregeln

$$(b-1)(b+1)=b^2-1=a^{n-1}-1=0.$$

Aber $\mathbf{Z}_n$ ist ein Körper, also können wir eine schon früher benutzte Schlussweise anwenden: Ist $(b+1)\neq 0$, so multiplizieren wir die obige Gleichung in $\mathbf{Z}_n$ mit $(b+1)^{-1}$ und erhalten $(b-1)=0$. Also ist entweder $(b+1)=0$ oder $(b-1)=0$, also $b=\pm 1$, was zu zeigen war[6].

Schon dieser erste Teil des Satzes hat eine überraschende Konsequenz. Er liefert eine einfache Formel zur Berechnung von Quadratwurzeln in $\mathbf{Z}_n$ (für erlaubte n). Freilich ist nicht jedes a in $\mathbf{Z}_n$ ein Quadrat (z.B. ist 6 in $\mathbf{Z}_{11}$ keins, wie Sie durch Quadrieren aller Elemente von $\mathbf{Z}_{11}$ nachprüfen können). Wir müssen deshalb *voraussetzen*, a sei ein Quadrat in $\mathbf{Z}_n$, etwa $x^2=a$. Dann ist auch $(-x)^2=a$, denn es gelten die gewohnten Rechenregeln. Weil $\mathbf{Z}_n$ ein Körper ist, sind $\pm x$ die einzigen Quadratwurzeln von a. Denn ist y eine Wurzel, so ist $(y-x)(y+x)=$

$y^2 - x^2 = 0$, also $y - x = 0$ oder $y + x = 0$, also $y = \pm x$. Wir stellen uns jetzt vor, dass wir a kennen, $\pm x$ aber nicht. Erlauben Sie mir, ein Kaninchen aus dem Hut zu ziehen: $w := a^{\frac{n+1}{4}}$. Weil n erlaubt ist, ist $\frac{n+1}{4}$ eine ganze Zahl. Ausserdem ist w effizient aus a berechenbar. Hier ist die Überraschung:

$$w = a^{\frac{n+1}{4}} = (x^2)^{\frac{n+1}{4}} = x^{\frac{n+1}{2}} = x^{\frac{n-1}{2}} \cdot x = \pm x \tag{5}$$

nach dem schon bewiesenen ersten Teil des Satzes. Also: Wenn a überhaupt eine Quadratwurzel besitzt, dann ist w eine. Wir können im Nachhinein unsere Voraussetzung, a sei ein Quadrat, wieder fallenlassen. Wir berechnen einfach w und sehen nach, ob $w^2 = a$ gilt oder nicht. Im ersten Fall haben wir eine Quadratwurzel, im zweiten ist a kein Quadrat. In $\mathbf{Z}_{11}$ z.B. ist

$$6^{\frac{n+1}{4}} = 6^3 = 7, \;\; 7^2 \neq 6,$$

also 6 kein Quadrat. Andererseits ist

$$5^{\frac{n+1}{4}} = 5^3 = 4, \;\; 4^2 = 5,$$

also 4 eine Quadratwurzel von 5.

Die Implikation im ersten Teil des Satzes lässt sich umkehren, denn aus $a^{\frac{n-1}{2}} = \pm 1$ folgt durch Quadrieren beider Seiten $a^{n-1} = 1$ (für alle $a \neq 0$ in $\mathbf{Z}_n$), und daraus nach der Umkehrung des Satzes von FERMAT die Primalität von n. Das können wir auch so formulieren: Ist n *nicht* prim, so gilt $a^{\frac{n-1}{2}} = \pm 1$ *nicht* für alle $a \neq 0$ in $\mathbf{Z}_n$. Es gibt also wenigstens ein Gegenbeispiel. Der zweite Teil des Satzes verschärft diese Feststellung zu einer statistischen Aussage über die Gegenbeispiele: Sie sind in der Mehrheit.

Um diese Aussage zu beweisen, müssen wir die Struktur des Rings $\mathbf{Z}_n$ (für nicht primes n) genauer untersuchen. Zur Vereinfachung wollen wir annehmen, $n = p \cdot q$ sei das Produkt zweier verschiedener Primzahlen p und q. Wir betrachten zunächst das *direkte Produkt* $\mathbf{Z}_p \times \mathbf{Z}_q$ der Ringe $\mathbf{Z}_p$ und $\mathbf{Z}_q$. Das ist ein neuer Ring, dessen Elemente keine Zahlen sind, sondern Zahlenpaare (a_1, a_2), wo a_1 aus $\mathbf{Z}_p$ und a_2 aus $\mathbf{Z}_q$ ist. Addition und Multiplikation sind (wie in der Vektorrechnung) komponentenweise erklärt: Ist z.B. $p = 7$ und $q = 11$, so sind $(5, 7)$ und $(4, 5)$ Elemente von $\mathbf{Z}_7 \times \mathbf{Z}_{11}$ und es ist $(5, 7) + (4, 5) = (5 + 4, 7 + 5) = (2, 1)$ und $(5, 7) \cdot (4, 5) = (5 \cdot 4, 7 \cdot 5) = (6, 2)$. Klar ist, dass wieder die gewohnten Rechenregeln gelten, dass also $\mathbf{Z}_p \times \mathbf{Z}_q$ ein kommutativer Ring ist. (Das Paar $(0, 0)$ übernimmt die Rolle von 0, $(1, 1)$ die Rolle von 1.)

Die Anzahl der Elemente von $\mathbf{Z}_p \times \mathbf{Z}_q$ ist offenbar $p \cdot q = n$. Also sind die Ringe $\mathbf{Z}_n$ und $\mathbf{Z}_p \times \mathbf{Z}_q$ gleich gross. Es gilt noch viel mehr: Die beiden Ringe sind Kopien voneinander. Wir können nämlich jeder Zahl a in $\mathbf{Z}_n$ ein Zahlenpaar (a_1, a_2) in $\mathbf{Z}_p \times \mathbf{Z}_q$ so zuordnen, dass jedes Element aus $\mathbf{Z}_p \times \mathbf{Z}_q$ genau einmal getroffen wird (sodass wir eine umkehrbare Abbildung erhalten), und dass sich Addition und Multiplikation der beiden Ringe bei dieser Zuordnung entsprechen. Man schreibt

$$\mathbf{Z}_n \;\; \simeq \;\; \mathbf{Z}_p \times \mathbf{Z}_q \tag{6}$$

und nennt die beiden Ringe *isomorph*. Die Zuordnung ist ganz einfach: a_1 ist der Rest von a nach Division mit p, also $a_1 := a \ mod \ p$, und ebenso ist $a_2 := a \ mod \ q$. Wählen wir z.B. $n = 77 = 7 \cdot 11$, so entspricht der Multiplikation $40 \cdot 60 = 13$ in $\mathbf{Z}_{77}$ gerade die oben angeführte Multiplikation $(5,7) \cdot (4,5) = (6,2)$.

Die Isomorphie (6) wird als *chinesischer Restsatz* bezeichnet[7]. Wir wissen, dass $\mathbf{Z}_n$ kein Körper ist. Der chinesische Restsatz führt die Struktur von $\mathbf{Z}_n$ aber vollständig und übersichtlich auf die Struktur der beiden Körper $\mathbf{Z}_p$ und $\mathbf{Z}_q$ zurück. Einsichten über $\mathbf{Z}_p$ und $\mathbf{Z}_q$ liefern automatisch Einsichten über $\mathbf{Z}_n$. Z.B. können wir mühelos zeigen, dass eine Quadratzahl in $\mathbf{Z}_n$ in der Regel nicht 2 (wie in Körpern), sondern 4 Quadratwurzeln besitzt. Wir ersetzen $\mathbf{Z}_n$ einfach durch seine isomorphe Kopie $\mathbf{Z}_p \times \mathbf{Z}_q$ und bemerken, dass $(x_1, x_2)^2 = (a_1, a_2)$ in $\mathbf{Z}_p \times \mathbf{Z}_q$ dasselbe bedeutet wie $x_1^2 = a_1$ in $\mathbf{Z}_p$ und $x_2^2 = a_2$ in $\mathbf{Z}_q$. Gibt es also ein (x_1, x_2) mit $(x_1, x_2)^2 = (a_1, a_2)$, so hat (a_1, a_2) genau die Wurzeln $(\pm x_1, \pm x_2)$ (die nicht alle verschieden sein müssen).

Es ist klar, dass die Zuordnung des chinesischen Restsatzes effizient ist. Tatsächlich ist auch die Umkehrabbildung effizient[8], wir können also zu einem Zahlenpaar (a_1, a_2) in $\mathbf{Z}_p \times \mathbf{Z}_q$ auf effiziente Weise die korrespondierende Zahl a in $\mathbf{Z}_n$ berechnen. Das bedeutet z.B., dass wir in $\mathbf{Z}_n$ effizient Quadratwurzeln ziehen können, wenn p und q erlaubte Primzahlen sind. (Ausgehend von einem a in $\mathbf{Z}_n$ berechnen wir zunächst das zugeordnete Paar (a_1, a_2) in $\mathbf{Z}_p \times \mathbf{Z}_q$, bestimmen davon sämtliche Wurzeln, indem wir das unter (5) angegebene Verfahren auf die Komponenten a_1 und a_2 anwenden, und kehren mit diesen Wurzeln wieder zurück in den Ring $\mathbf{Z}_n$.) Freilich können wir dieses Verfahren nur dann anwenden, wenn wir die Zerlegung $n = p \cdot q$ wirklich kennen und nicht nur wissen, dass es eine solche gibt.

Wir kommen nun zum Nachweis der zweiten Aussage des Satzes im Fall $n = p \cdot q$, wo p und q verschiedene Primzahlen sind. Wir können $\mathbf{Z}_n$ durch seine isomorphe Kopie $\mathbf{Z}_p \times \mathbf{Z}_q$ ersetzen. Den beiden Zahlen ± 1 entsprechen die beiden Zahlenpaare $(1,1)$ und $(-1,-1)$. Nennen wir ein Element (a_1, a_2) von $\mathbf{Z}_p \times \mathbf{Z}_q$ Eulersch, wenn $(a_1, a_2)^{\frac{n-1}{2}} = (1,1)$ oder $= (-1,-1)$ ist, so müssen wir zeigen: Die Mehrheit der (a_1, a_2) ist nicht EULERsch. Nun ist aber $\frac{n-1}{2}$ ungerade. Ist also (a_1, a_2) EULERsch, so ist $(a_1, -a_2)^{\frac{n-1}{2}} = (a_1^{\frac{n-1}{2}}, -a_2^{\frac{n-1}{2}}) = (1,-1)$ oder $= (-1,1)$, also ist $(a_1, -a_2)$ nicht EULERsch. Die Menge $\mathbf{Z}_p \times \mathbf{Z}_q$ zerfällt demnach in lauter ein- oder zwei-elementige Teilmengen $\{(a_1, a_2), (a_1, -a_2)\}$, von denen stets mindestens ein Element nicht EULERsch ist. Daraus folgt die Behauptung[9].

Den obigen Satz verwenden wir als Grundlage für einen statistischen Primtest. Dazu bringen wir den Zufall ins Spiel mittels unabhängiger Zufallszahlen[10]mit Werten in $\{1, \ldots, n-1\}$. Wie lassen sich solche Zufallszahlen realisieren? Im wesentlichen dadurch, dass wir ihre Binärziffern zufällig wählen: Sei s die Anzahl der Binärziffern von n. Wir erzeugen s unabhängige Zufallsbits (z.B. durch Werfen einer fairen Münze[11]) und fassen die Ergebnisse α_i als die Binärziffern einer Zahl, nämlich $\sum_{i=0}^{s-1} \alpha_i 2^i$ auf. Falls nötig, wiederholen wir das Experiment, bis die erhaltene Zahl zum ersten Mal in $\{1, \ldots, n-1\}$ liegt. Diese Zahl ist dann unsere erste Zufallszahl a_1. Es

ist nicht schwer zu sehen, dass wir im Durchschnitt mit einer Wiederholung auskommen und dass a_1 jeden Wert in $\{1, \ldots, n-1\}$ mit der Wahrscheinlichkeit $\frac{1}{n-1}$ annimmt. Auf die gleiche Weise konstruieren wir (mit neuen Zufallsbits) weitere Zufallszahlen $a_2, \ldots, a_k$. Dabei ist k ein positiv-ganzzahliger Parameter, mit dem wir Zuverlässigkeit und Zeitaufwand des folgenden Verfahrens steuern. Wenn wir ganz sicher gehen wollen, setzen wir z.B. $k = 100$.

Statistischer Primtest[12] *für erlaubte n:*

1. *Wähle Zufallszahlen $a_1, \ldots, a_k$ in $\{1, \ldots, n-1\}$*
2. *Berechne $a_i^{\frac{n-1}{2}}$ in $\mathbf{Z}_n$*
3. *Falls alle $a_i^{\frac{n-1}{2}} = \pm 1$, entscheide: n prim*
   Sonst entscheide: n nicht prim.

Wir bemerken zunächst, dass das Verfahren (etwa für $k = 100$) effizient ist, denn die Erzeugung von einigen hunderttausend zufälligen Bits lässt sich technisch bewerkstelligen, und die Bildung einer hohen Potenz in $\mathbf{Z}_n$ ist, wie wir gesehen haben, ein effizienter Prozess[13].

Nehmen wir nun an, n sei (in Wirklichkeit) prim. Dann folgt aus dem obigen Satz $a^{\frac{n-1}{2}} = \pm 1$ für *jedes* a in $\{1, \ldots, n-1\}$, insbesondere für die zufällig gewählten a_i. Wir treffen in diesem Fall also *mit Sicherheit* die richtige Entscheidung.

Was passiert, wenn n in Wahrheit nicht prim ist? In diesem Fall könnte es sein, dass beim Potenzieren der Zufallszahlen trotzdem immer ± 1 herauskommt und wir deshalb falsch entscheiden. Aber wie wahrscheinlich ist das? Nach dem obigen Satz gilt $a^{\frac{n-1}{2}} = \pm 1$ für höchstens die Hälfte aller a in $\{1, \ldots, n-1\}$. Also ist die Wahrscheinlichkeit, dass dies für ein zufällig gewähltes a passiert, höchstens $\frac{1}{2}$. Weil unsere Zufallszahlen a_i unabhängig sind, ist die Wahrscheinlichkeit dafür, dass wir immer $a_i^{\frac{n-1}{2}} = \pm 1$ erhalten, höchstens $(\frac{1}{2})^k = 2^{-k}$. Wir haben also gezeigt:

$$\begin{array}{rcl} n \text{ prim} & \Longrightarrow & \text{Entscheidung richtig} \\ n \text{ nicht prim} & \Longrightarrow & \text{Irrtumswahrscheinlichkeit} \leq 2^{-k}. \end{array}$$

Für $k = 100$ ist die Irrtumswahrscheinlichkeit $\leq 2^{-100} \approx 10^{-30}$. Ich denke, ich muss höchstens die Mathematiker davon überzeugen, dass diese Wahrscheinlichkeit nicht 0 ist.

Beachten Sie auch, dass die Wahrscheinlichkeitsaussage nicht etwa so lautet: Für fast alle (erlaubten) Zahlen n liefert unser Primtest das richtige Ergebnis, nur für ganz wenige ein falsches. Eine solche Aussage wäre wertlos, denn die Zahl n könnte uns von einem Gegner (etwa mit dem Ziel einer Wette) zugespielt worden sein.

Wir haben gerade gesehen, wie man (erlaubte) Zahlen effizient auf Primalität testet. Im Gegensatz dazu ist bis heute kein effizientes Verfahren zur Zerlegung von Zahlen in ihre Primfak-

toren bekannt. Konkreter: Es ist nach heutigem Stand der Technik[14] und der algorithmischen Kunst unmöglich, 1000-stellige Zahlen n, die das Produkt zweier etwa 500-stelliger 'zufällig gewählter' Primzahlen p und q sind, in ihre Primfaktoren zu zerlegen, also aus der Kenntnis von n allein auf die Faktoren p und q zu schliessen. Auf dieser algorithmischen Diskrepanz zwischen Primalität und Primfaktorzerlegung beruht das kryptographische Verfahren des nächsten Abschnitts.

Geheimnisse

Hier möchte ich Ihnen kurz über eine Revolution in der Kryptographie[15]berichten, die in den späten siebziger Jahren stattgefunden hat und in der grosse Primzahlen eine Rolle spielen. Die Revolution wurde ausgelöst von DIFFIE und HELLMAN (1976), von denen die grundlegende Idee eines 'public key cryptosystem' stammt. Sie wurde zum Erfolg geführt von RIVEST et al. (1978) mit einem Verfahren, das Eleganz mit mathematischer Strenge verknüpft und heute in verschiedenen Bereichen praktische Verwendung findet (RSA-System). Ein Grenzfall des RSA-Systems, der von RABIN (1979) vorgeschlagen wurde, ist für unsere Darstellung besonders geeignet.

Stellen wir uns vor, eine Bank in Halle möchte mit einer Sparkasse in Konstanz ein Börsengeschäft abwickeln, dessen Erfolg entscheidend vom Tempo der Vorbereitung und von der Geheimhaltung des Projekts abhängt. Das Tempo erzwingt die Benutzung öffentlicher Telefonnetze, die freilich von der Konkurrenz in Zürich abgehört werden. Wir nehmen ferner an, dass die beiden Geldinstitute zuvor keinen Geschäftskontakt hatten, insbesondere über keinen gemeinsamen Schlüssel zum Chiffrieren ihrer Gespräche verfügen. Jede Botschaft, die Halle an Konstanz sendet, und jede, die Konstanz nach Halle schickt, wird also von Zürich gelesen. Zur Vereinfachung unserer Diskussion wollen wir annehmen, dass Zürich selbst keine Botschaften (unter dem Deckmantel von Halle oder Konstanz) verschicken kann. Ist geheime Kommunikation möglich?

Wohl kaum! Ein Beweis könnte so aussehen: Alles, was Halle und Konstanz einander mitteilen, ist auch Zürich bekannt. Weder Halle noch Konstanz können deshalb einen Informationsvorsprung vor Zürich gewinnen.

Tatsächlich ist dieser Schluss nicht zwingend. Es gibt eine Asymmetrie zwischen Deutschen und Eidgenossen: Halle und Konstanz können die Initiative ergreifen und das Gespräch nach Gutdünken lenken, während Zürich in Passivität verharren muss.

Wir wollen annehmen, Halle möchte Konstanz eine erste ausführliche Botschaft senden. Diese denken wir uns von vorneherein auf eine standardisierte (und damit auch den Zürchern bekannte) Weise als 1000-stellige Dezimalzahl x codiert. Diese Zahl x ist also der zu übermittelnde *Klartext*.

Die Sparkasse in Konstanz hat für ihre Geschäftskontakte ein für alle mal zwei (verschie-

dene) zufällige 501-stellige erlaubte Primzahlen p und q gewählt und als Geschäftsgeheimnis gespeichert. Wie kommt sie zu solchen Primzahlen? Einfach dadurch, dass ihr Rechner so oft zufällige erlaubte 501-stellige Zahlen erzeugt, bis er darunter zwei Primzahlen gefunden hat. Nach klassischen Sätzen über die Häufigkeit von grossen Primzahlen und wegen der Existenz effizienter Primtests ist das praktikabel.

Konstanz ergreift die Initiative und sendet das Zahlenprodukt $n := p \cdot q$ nach Halle. (p und q selbst werden von der Sparkasse niemals preisgegeben.) Halle notiert n. Zürich notiert n ebenfalls. Die Zahl n ist 1001- oder 1002-stellig. Halle interpretiert den 1000-stelligen Klartext x als Element von $\mathbf{Z}_n$ und berechnet x^2 in $\mathbf{Z}_n$. Dieses x^2 ist das *Chiffrat*, welches Halle nach Konstanz übermittelt. Die Verschlüsselung besteht also im Quadrieren des Klartextes in $\mathbf{Z}_n$. Konstanz notiert x^2. Zürich notiert x^2 ebenfalls.

Die Informationen sind jetzt so verteilt: Halle kennt n und den Klartext x in $\mathbf{Z}_n$, Zürich kennt n und das Chiffrat x^2 in $\mathbf{Z}_n$, Konstanz kennt ebenfalls n und das Chiffrat x^2, zusätzlich aber noch die Primfaktorzerlegung $n = p \cdot q$.

Wie wir im letzten Kapitel ausgeführt haben, kann Konstanz mit Hilfe von (6) und (5) die (in der Regel 4) Wurzeln von x^2 berechnen. Unter diesen muss sich der Klartext x befinden, und nur er wird einen Sinn ergeben. Konstanz kann also das Chiffrat entschlüsseln.

Zürich kann das nicht, denn es ist nicht im Besitz der Primfaktorzerlegung $n = p \cdot q$. Wie wir ebenfalls im letzten Kapitel bemerkt haben, sind keine effizienten Methoden zur Primfaktorzerlegung von Zahlen wie n bekannt. Die Kenntnis des Chiffrats x^2 ist für die Faktorzerlegung nutzlos, denn Zürich kann sich selbst nach Belieben Paare y, y^2 in $\mathbf{Z}_n$ herstellen, auch mit sinnvollen Klartexten y. Gibt es vielleicht effiziente Verfahren zur Berechnung von Wurzeln, die ohne die Kenntnis der Primfaktorzerlegung auskommen? Rabin (1979) hat gezeigt, dass jeder solche Algorithmus eine effiziente Primfaktorzerlegung nach sich zieht[16].

Anmerkungen

1. ', gewenn' steht für 'genau dann, wenn'

2. Haben wir eine Zahl a (mit negativem Ergebnis) auf die Teilereigenschaft getestet, so können wir alle Vielfachen von a aus der Testliste streichen, da sie n erst recht nicht teilen. Dies ist als *Sieb des* Erathostenes bekannt. Erathostenes hat übrigens als erster die Erdkrümmung und daraus den Erdumfang bestimmt, und zwar mit einem sehr genauen Ergebnis.

3. Es handelt sich hier um den sogenannten 'kleinen Fermat', im Gegensatz zur 'grossen Fermatschen Vermutung', die sehr viel tiefer liegt und erst vor kurzem vollständig bewiesen wurde.

4. Dieses Synonym für 'Rechenverfahren' ist dem Eigennamen des islamischen Mathematikers AL-KHWARISMI (etwa 780–850) entlehnt. Der Titel eines seiner Werke hat ausserdem zur Bezeichnung 'Algebra' geführt.

5. Es gibt noch eine andere Möglichkeit, multiplikative Inverse effizient zu berechnen, die auf dem EUKLIDschen Algorithmus beruht, siehe IRELAND und ROSEN (1990).

6. Wir haben bisher nicht verwendet, dass $\frac{n-1}{2}$ ungerade ist. EULER hat für $a \neq 0$ in $\mathbf{Z}_n$ genauer bewiesen, dass $a^{\frac{n-1}{2}} = 1$ gilt, falls a eine Quadratzahl in $\mathbf{Z}_n$ ist, sonst $a^{\frac{n-1}{2}} = -1$, siehe IRELAND und ROSEN (1990).

7. Es handelt sich genauer um einen Spezialfall des chinesischen Restsatzes. Der Beweis von (6) ist nicht schwierig, siehe IRELAND und ROSEN (1990).

8. Man verwendet den EUKLIDschen Algorithmus, siehe IRELAND und ROSEN (1990).

9. Diesen Beweis können wir auch so formulieren: Nennen wir eine Zahl a in $\mathbf{Z}_n$ Eulersch, wenn $a^{\frac{n-1}{2}} = \pm 1$ gilt, so genügt es, ein im Ring $\mathbf{Z}_n$ invertierbares nicht Eulersches b zu finden. (Denn die Multiplikation mit b ist eine Einbettung der Menge der Eulerschen in die Menge der nicht Eulerschen Elemente von $\mathbf{Z}_n$.) Ersetzen wir $\mathbf{Z}_n$ durch $\mathbf{Z}_p \times \mathbf{Z}_q$, so sehen wir, dass $(1, -1)$ die gewünschten Eigenschaften hat.
Der gleiche Beweis lässt sich auf beliebiges n anwenden, solange n keine Potenz einer Primzahl ist. Ist dagegen $n = p^e$, so kann man $b := 1 - p$ nehmen.

10. In mathematischer Sprache sind das unabhängige und in $\{1, \ldots, n-1\}$ gleichverteilte Zufallsvariable.

11. Tatsächlich arbeitet man heute meist mit Pseudo-Zufallszahlen, ohne gesicherte Grundlage und mit bestem Erfolg. Gute physikalische Zufallsquellen wären weisses Widerstandsrauschen oder langlebiger radioaktiver Zerfall. (Ich danke Herrn W. WEYRICH für diese Information.)

12. Es handelt sich hier um eine vereinfachte Variante (für erlaubte n) des Primtests von SOLOVAY und STRASSEN (1977) sowie des heute meist verwendeten Tests von MILLER und RABIN (siehe RABIN (1980)). Die erstgenannte Arbeit musste übrigens fast drei Jahre auf ihre Veröffentlichung warten, weil sich ein Referee mit der Idee eines zufälligen Primtests nicht anfreunden konnte. Heute sind Zufallsverfahren in der algorithmischen Zahlentheorie an der Tagesordnung.

13. Aus Gründen der Übersichtlichkeit habe ich das obige Verfahren in einer Weise dargestellt, wie man es nicht wirklich verwenden wird. Vielmehr wird man die Zufallszahl a_{i+1} nur erzeugen, wenn man $a_i^{\frac{n-1}{2}}$ schon berechnet und das Ergebnis ± 1 erhalten hat.

14. Eine neue Situation entstünde, wenn es gelänge, Quanten-Computer mit gewissen Eigenschaften technisch zu realisieren, siehe SHOR (1994), BENNETT et al. (1992).

15. Kryptographie ist die Lehre von der geheimen Datenübermittlung. Siehe etwa KRANAKIS (1986).

16. Man wählt ein zufälliges x in $\mathbf{Z}_n$ und berechnet eine Wurzel y von x^2. Dieses Zufallsexperiment wiederholt man so oft, bis $y \neq \pm x$ ist. (Im Durchschnitt reicht etwa eine Wiederholung.) Dann ist $y + x$ durch p oder q, aber nicht durch $n = p \cdot q$ teilbar. (Man argumentiere in $\mathbf{Z}_p \times \mathbf{Z}_q$.) Der grösste gemeinsame Teiler von $y+x$ und n ist also entweder p oder q. Genaueres findet man in KRANAKIS (1986).

Ich danke Franz Mauch und Michael Nüsken für ihre Hilfe bei der Abfassung des Manuskripts.

Schriftenverzeichnis

1. BENNETT, C.H., BRASSARD, G., and EKERT, A.K.: Quantum cryptography. Scientific American, Oct 1992, 50-57.

2. DIFFIE, W., and HELLMAN, M.: New Directions in Cryptography. IEEE Transactions on Information Theory, IT *22*, 644-654 (1976).

3. IRELAND, K., and ROSEN, M.: A Classical Introduction to Modern Number Theory. 2. ed. New York, Berlin, Heidelberg: Springer 1990.

4. KRANAKIS, E.: Primality and Cryptography (Wiley-Teubner Series in Computer Science). Stuttgart: B.G. Teubner; Chichester, New York, Brisbane, Toronto, Singapore: Wiley 1986.

5. RABIN, M. O.: Digitalized Signatures and Public Key Functions as Intractable as factorization. MIT Laboratory for Computer Science, Jan 1979, TR 212.

6. RABIN, M.O.: Probabilistic Algorithm for Testing Primality. Journal of Number Theory *12*, 128-138 (1980).

7. RIVEST, R., SHAMIR, A., and ADLEMAN, L.: A Method for Obtaining digital Signatures and Public Key Cryptosystems. Comm. ACM *21*, 120-126 (1978).

8. SHOR, P.: Algorithms for quantum computation: Discrete log and factoring. Ann. IEEE Symp. on Found. of Computer Science (FOCS) 1994.

9. SOLOVAY, R., and STRASSEN, V.: A Fast Monte Carlo Test for Primality. SIAM J. Comp. *6*, 84-85 (1977), erratum 7, 118 (1978).