Einfache Primtests

Autor(en): **Kaup, Burchard**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **48 (1993)**

PDF erstellt am: **26.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-44633

El. Math. *48* (1993) 0013-6018/93/040143-14$1.50 + 0.20/0

Einfache Primtests

Burchard Kaup

Burchard Kaup wurde 1940 in Deutschland geboren, studierte bei H. Behnke und H. Holmann und promovierte 1975 mit einer Arbeit in komplexer Analysis mehrerer Veränderlicher. Er ist Professeur associé an der Universität Freiburg (Schweiz). Sein Hauptarbeitsgebiet ist die komplexe Analysis; darüber hat er zusammen mit seinem Bruder Ludger 1983 das Lehrbuch "Holomorphic Functions" geschrieben. Er interessiert sich ferner für die Fage, wie man gewisse mathematische Probleme computerunterstützt lösen bzw. illustrieren kann.

1 Einleitung

Wenn jemand abklären soll, ob eine gegebene Zahl n prim ist oder nicht, dann erwartet man von ihm üblicherweise eine der folgenden zwei Antworten:

1. n ist keine Primzahl, denn n hat den echten Teiler n_1 (und hier erwartet man, daß der Teiler n_1 auch wirklich angegeben wird)

Die Gegenstände der 'reinen Mathematik' finden ausserhalb der mathematischen Welt selten grösseres Interesse, da sie gewöhnlich als nutzlos, ja als Spielerei angesehen werden. Wie die Geschichte der Mathematik vielfach belegt, ändert sich diese Einstellung jeweils plötzlich, wenn Anwendungen auftauchen. Zahlentheorie und Primzahlen gehörten lange Zeit zu den "reinsten" aller mathematischen Gegenstände; seit es Verschlüsselungssysteme gibt, die auf grossen Primzahlen beruhen, ist das öffentliche und staatliche Interesse an Primzahlen schlagartig gestiegen. — Will man von einer Zahl entscheiden, ob sie prim ist oder nicht, so bietet sich dafür unmittelbar das Verfahren an, der Reihe nach durch kleinere (Prim)Zahlen zu dividieren. Leider ist dies für grosse Zahlen nicht genügend effizient: bereits für 30stellige Zahlen wird die Rechenzeit auch mit grossen Computern unakzeptierbar lang. Effizientere Verfahren sind deshalb gefragt und damit auch Erkenntnisse der Zahlentheorie, die zu solchen Verfahren führen.

Burchard Kaup behandelt in seinem Beitrag eine Reihe von vergleichsweise einfachen solchen Primtests. Bei einigen davon, den schnelleren *probabilistischen*, wird die Antwort jeweils nur mit einer bekannten und steuerbaren Wahrscheinlichkeit richtig sein, während bei anderen, den aufwendigeren *deterministischen*, die Antwort immer richtig ist. Der Beitrag regt an, einige dieser Tests auf einem Kleincomputer zu implementieren. *ust*

2. n ist eine Primzahl, denn keine der Primzahlen p mit $p^2 \leq n$ ist ein Faktor von n.

Für "große" Zahlen ist ein solches Vorgehen unter Umständen sehr problematisch. Zwar ist es im Fall der Antwort 1 verhältnismäßig leicht, von der angegebenen Zahl n_1 zu verifizieren, daß es sich tatsächlich um einen Faktor handelt (man muß nur testen, ob bei der Division von n durch n_1 ein Rest bleibt oder nicht); im Fall der Antwort 2 wird stets ein Unbehagen bleiben, da dieses Ergebnis nur schwer zu kontrollieren ist wegen des ungeheueren Rechenaufwandes: Da es wegen des Primzahl-Satzes (vgl. [7]) etwa $A(n) := \sqrt{n}/\ln(\sqrt{n})$ Primzahlen $p \leq \sqrt{n}$ gibt, sind mindestens $A(n)$ Probedivisionen erforderlich, um n als Primzahl nachzuweisen, für eine zehnstellige Zahl also mindestens $A(10^{10}) \approx 8700$. Wenn die Rechnungen auf einem Computer ausgeführt wurden, müßte man sich das Programm anschauen und verifizieren, ob es fehlerfrei ist. Um dann wirklich sicher zu sein, müßte man das Programm noch einmal laufen lassen, was viele Jahre dauern kann: Wenn z.B. $n \geq 10^{30}$, ist $A(n) \geq A(10^{30}) \approx 3 \cdot 10^{13}$; wenn Sie pro Sekunde eine Million Primfaktoren testen, benötigen Sie immer noch etwa 1 Jahr.

Nehmen wir an, Sie hätten die zwei Zahlen

$$E(23) := \underbrace{11111111111111111111}_{23} \quad \text{und} \quad E(59) := \underbrace{111\ldots111}_{59}$$

zu untersuchen. Hier sei bereits verraten:

- $E(23)$ ist eine Primzahl, vgl. Abschnitt 4,
- der kleinste Teiler von $E(59)$ ist 2559647034361, vgl. [1, Tabelle 10-].

Es ist $A(E(23)) \approx 10^{10}$. Auf einem Macintosh IIsi (bei Benutzung des Programmes MATHEMATICA) kann man $E(23)$ pro Sekunde auf einige Hundert Primfaktoren testen; die total benötigte Zeit wäre also etwa ein Jahr, um durch Probedividieren nachzuweisen, daß $E(23)$ prim ist.

Den oben angegebenen Faktor von $E(59)$ werden Sie (bei systematischem Probieren aller Primzahlen) frühestens nach etwa 90'000'000'000 Probedivisionen finden. Konkret heißt das: Mit der oben erwähnten Software können Sie durch Probedividieren nicht feststellen, ob $E(59)$ eine Primzahl ist oder nicht. Vielleicht werden Sie jedoch nach längerer Zeit, wenn Sie immer noch keinen Faktor gefunden haben, persönlich zu der Überzeugung "$E(59)$ ist wahrscheinlich eine Primzahl" kommen.

Es gibt eine große Anzahl von Algorithmen zum Auffinden von Primfaktoren bzw. zum Beweisen, daß eine gegebene Zahl prim ist (vgl. [1], [8], [13], [14]). Mit dem von Cohen und Lenstra in [2] angegebenen Algorithmus kann angeblich in etwa 10 Minuten entschieden werden, ob eine vorgegebene (≤ 200)-stellige Zahl prim ist oder nicht!

Ziel dieses Textes ist es *nicht*, die modernsten und leistungsfähigsten Algorithmen vorzustellen; vielmehr soll der Leser an Hand einiger einfacher Algorithmen (die leicht auf einem PC bzw. sogar auf einigen programmierbaren Taschenrechnern implementiert werden können) in die Problematik eingeführt und zu eigenen Aktivitäten angeregt werden. Das dadurch wahrscheinlich aufkeimende Bedürfnis nach leistungsfähigeren Algorithmen kann in den oben erwähnten Büchern und der dort angegebenen weiterführenden Literatur gestillt werden.

Die hier behandelten Algorithmen sollen Ihnen Folgendes zeigen:

1. Wenn eine gegebene Zahl n nicht prim ist, dann kann man mit großer Wahrscheinlichkeit in vernünftiger Zeit einen Beweis dafür finden, daß n nicht prim ist (ohne daß man dafür einen Faktor von n zu kennen braucht), vgl. 2.5.
2. Der PP-Test (siehe Abschnitt 3) liefert Ihnen in kurzer Zeit für eine gegebene Zahl n eine der beiden Antworten "n ist nicht prim" oder "sehr wahrscheinlich ist n prim". Dabei kann es (höchstens jedoch mit der Wahrscheinlichkeit $1/4^s$, siehe 2.6) vorkommen, daß n nicht prim ist, obwohl die Antwort "sehr wahrscheinlich ist n prim" lautete (probabilistischer Primtest).
3. Wenn für eine gegebene Zahl n alle Primfaktoren von $n-1$ bekannt sind, dann kann man mit großer Wahrscheinlichkeit in vernünftiger Zeit entscheiden, ob n prim ist oder nicht; die Entscheidung kann mit einem leicht nachvollziehbaren Beweis belegt werden (deterministischer Primtest, vgl. Abschnitt 4).
4. Mit einem zusätzlichen Faktorisierungsprogramm kann man rekursiv auch für gewisse größere Primzahlen n einen leicht nachvollziehbaren Beweis liefern, daß n prim ist. (Dieser Algorithmus ist für große Zahlen "schlecht", weil in ihm große Zahlen faktorisiert werden müssen; große Zahlen in Primfaktoren zu zerlegen verlangt aber nach dem heutigen Stand des Wissens wesentlich mehr Rechenaufwand als der Nachweis, daß eine Zahl prim ist. Ein "gutes" Programm, mit dem man beweisen will, daß eine Zahl prim ist, muß also anders aufgebaut werden).
5. Unter Verwendung des deterministischen Primtests in Abschnitt 4 kann man effektiv große Primzahlen konstruieren (vgl. Abschnitt 5).

Der obige Satz "mit großer Wahrscheinlichkeit in vernünftiger Zeit" soll hier nicht näher präzisiert werden. Was eine "vernünftige Zeit" ist, hängt natürlich wesentlich ab von der Größe der zu untersuchenden Zahl n und der Ihnen zur Verfügung stehenden Hard- und Software.

Wenn Sie selber mit großen Zahlen experimentieren möchten, dann sollten Sie über ein Programm verfügen, das es Ihnen gestattet, mit (beliebig) großen ganzen Zahlen zu rechnen. Wer gerne in PASCAL programmiert, kann die in [14, Appendix 7] explizit angegebenen Programme zum Rechnen mit großen Zahlen abschreiben und darauf eigene Programme aufbauen. Eine andere Möglichkeit ist, daß man z.B. mit MATHEMATICA arbeitet, das mit beliebig großen ganzen Zahlen rechnen kann, viele Funktionen (wie z.B. die Berechnung von $b^k \pmod n$, Zerlegung in Primfaktoren etc.) bereits eingebaut hat und eine äußerst leistungsfähige Programmiersprache zur Verfügung stellt. MATHEMATICA liefert auf Wunsch auch ein "Zertifikat", daß eine gegebene Primzahl n wirklich prim ist (benutze ProvablePrimeQ[n,Certificate $->$ True]).

Zum obigen Punkt 5 sei noch bemerkt, daß die Kenntnis geeigneter (vgl. [5]) großer Primzahlen (mehr als hundert Ziffern) von entscheidender Bedeutung ist in der Kryptographie (Verschlüsseln von Texten mit öffentlich bekanntem Code, vgl. [15], [14], [6]); dadurch wurde dieser Zweig der Zahlentheorie und insbesondere die Frage, wie man eine Zahl faktorisieren kann, die nur große Primfaktoren hat, plötzlich auch für militärische Kreise äußerst wichtig.

2 Zerlegbarkeits-Beweise

Wir benutzen die folgenden Notation:

$$a \underset{n}{\equiv} b \text{ ist eine Abkürzung für } a \equiv b \pmod{n}.$$

Definition 2.1 *Es sei $n \geq 5$ ungerade und $2 \leq b \leq n-2$. Wir sagen:*

$$\textbf{b ist ein F-Zeuge für } \textit{(die Zerlegbarkeit von)} \ \boldsymbol{n} \ :\Longleftrightarrow \ b^{n-1} \underset{n}{\not\equiv} 1.$$

Der Buchstabe F in obiger Definition soll an Fermat erinnern. Die Bedeutung dieser Sprechweise wird deutlich aus dem folgenden

Satz 2.2 *Eine Zahl $n \geq 3$ ist genau dann eine Primzahl, wenn es keinen F-Zeugen für sie gibt.*

Zum *Beweis* vgl. Abschnitt 6. Jede Zahl $n \geq 3$, die einen F-Zeugen besitzt, ist also zerlegbar.

Für praktische Rechnungen ist es wichtig, daß man $b^{n-1} \pmod{n}$ auch wirklich in vernünftiger Zeit berechnen kann.

Insbesondere kann man also durch Angabe eines F-Zeugen für n einen leicht verifizierbaren *Beweis* liefern, daß n nicht prim ist, ohne daß man einen konkreten Faktor von n zu kennen braucht!

Beispiel: $E(59)$ ist nicht prim, weil 2 ein F-Zeuge für $E(59)$ ist (d.h. $2^{E(59)-1} \underset{E(59)}{\not\equiv} 1$).

Für die meisten Zahlen, die keine Primzahlen sind, ist schon 2 ein F-Zeuge:

n	2^{n-1}	$2^{n-1} \pmod{n}$
4	8	0
5	16	1
6	32	2
7	64	1
8	128	0
9	256	4
10	512	2
11	1024	1

Für viele zerlegbare Zahlen n sind die meisten b mit $2 \leq b \leq n-2$ F-Zeugen. Es gibt jedoch zerlegbare Zahlen, die nur verhältnismäßig wenig F-Zeugen besitzen. Da jedes b mit $\mathrm{ggT}(b,n) > 1$ ein F-Zeuge für n ist, können höchstens diejenigen b keine F-Zeugen sein, die zu n teilerfremd sind. Es gibt nun Nicht-Primzahlen n mit der folgenden Eigenschaft:

$$b^{n-1} \underset{n}{\equiv} 1 \iff \mathrm{ggT}(b,n) = 1.$$

Diese Zahlen heißen **Carmichael-Zahlen** (vgl. [6]; erst kürzlich gelang der Nachweis, dass es unendlich viele Carmichael-Zahlen gibt, vgl. [3]), für sie gibt es nur verhältnis-

mäßig wenig F-Zeugen. In der Liste am Ende dieses Abschnittes sind einige Carmichael-Zahlen n aufgeführt mit den Verhältnissen $Z_F(n)/n$ und $Z_{MR}(n)/n$, wobei $Z_F(n)$ und $Z_{MR}(n)$ die Anzahl der F-Zeugen bzw. der MR-Zeugen (vgl. 2.3) für n sind.

Wenn man trotz vieler Versuche keinen F-Zeugen für eine gegebene Zahl n findet, kann das sowohl daran liegen, daß n prim ist (und deshalb überhaupt keinen F-Zeugen besitzt) oder daß n zwar zusammengesetzt ist, aber nur wenig F-Zeugen hat.

Eine Lösung dieses Problems liefert die folgende Verfeinerung des Begriffes eines F-Zeugen:

Definition 2.3 *Es sei $n \geq 3$ ungerade und $n-1 = 2^q m$ mit ungeradem m, ferner sei b eine Zahl mit $2 \leq b \leq n-2$. Es sei*

$$c_k := b^{2^k m} (\mathrm{mod}\, n) \quad \text{für} \quad 0 \leq k \leq q$$

(es ist also $c_0 = b^m (\mathrm{mod}\, n)$, $c_k = c_{k-1}^2 (\mathrm{mod}\, n)$ für $1 \leq k \leq q$ und $c_q = b^{n-1} (\mathrm{mod}\, n)$).
Wir sagen: **b ist ein MR-Zeuge für** *(die Zerlegbarkeit von)* **n** *, wenn $c_0 \underset{n}{\not\equiv} \pm 1$ ist und wenn $c_k \underset{n}{\not\equiv} -1$ gilt für $1 \leq k < q$.*

Die Buchstaben MR in obiger Definition sollen an Miller und Rabin erinnern.

An zwei Beispielen soll der Begriff des MR-Zeugen erläutert werden:

Für $n = 13$ ist $n - 1 = 2^2 \cdot 3$, also $q = 2$ und $m = 3$. Für $b = 2$ ist also

$$\begin{aligned} c_0 &= b^3 (\mathrm{mod}\, 13) = 8 \\ c_1 &= c_0^2 (\mathrm{mod}\, 13) = 64 (\mathrm{mod}\, 13) = 12 \underset{13}{\equiv} -1, \end{aligned}$$

also ist 2 kein MR-Zeuge für 13.

Für $n = 561$ ist $q = 4$ und $m = 35$. Für $b = 2$ ist also

$$\begin{aligned} c_0 &= 2^{35} (\mathrm{mod}\, 561) = 263 \\ c_1 &= c_0^2 (\mathrm{mod}\, 561) = 166 \\ c_2 &= c_1^2 (\mathrm{mod}\, 561) = 67 \\ c_3 &= c_2^2 (\mathrm{mod}\, 561) = 1 \\ c_4 &= c_3^2 (\mathrm{mod}\, 561) = 1 \end{aligned}$$

also ist 2 ein MR-Zeuge für 561, aber kein F-Zeuge (denn $c_4 = 2^{560} (\mathrm{mod}\, 561) = 1$); vgl. auch die Tabelle nach Theorem 2.6.

Analog zu 2.2 gilt nun:

Satz 2.4

1. *Jeder F-Zeuge für n ist auch ein MR-Zeuge für n.*
2. *$n \geq 3$ ist genau dann eine Primzahl, wenn n keine MR-Zeugen besitzt.*

Den *Beweis* findet man in Abschnitt 6. Es gibt also mehr MR-Zeugen als F-Zeugen. Genauer gilt:

Theorem 2.5 (Rabin) *Jede ungerade zerlegbare Zahl n besitzt wenigstens $\frac{3}{4}(n-1)$ MR-Zeugen. Mit anderen Worten: bei zufälliger Auswahl eines b mit $2 \leq b \leq n-2$ ist die Wahrscheinlichkeit, einen MR-Zeugen zu treffen, mindestens gleich $3/4$.*

Zum Beweis vgl. [12], [10], [6, V.1.7]. In Abschnitt 6 finden Sie eine Beweisskizze.

Fassen wir zusammen:

Theorem 2.6 *Es sei $n \geq 3$ eine ungerade Zahl. Es seien $b_1, \ldots, b_s$ zufällig ausgewählte Zahlen mit $2 \leq b_\sigma \leq n-2$.*

1. *Wenn n prim ist, dann gilt für alle σ: $b_\sigma^{n-1} \underset{n}{\equiv} 1$, b_σ ist kein MR-Zeuge für n.*
2. *Wenn n nicht prim ist, dann ist die Wahrscheinlichkeit dafür, daß wenigstens eines der ausgewählten b_σ ein MR-Zeuge für n ist (damit ist dann n als zerlegbar erkannt), mindestens gleich $1-(1/4)^s$.*

In der folgenden Tabelle ist n jeweils eine Carmichael Zahl, $Z_F(n)$ die Anzahl der F-Zeugen für n und $Z_{MR}(n)$ die Anzahl der MR-Zeugen für n:

n	$Z_F(n)/n$	$Z_{MR}(n)/n$
561	0.43	0.98
1105	0.30	0.97
1729	0.25	0.91
2821	0.23	0.90
6601	0.20	0.95
29341	0.12	0.86
9624742921	0.0016	?

Die Zahl $m = 9624742921$ ist also keine Primzahl; die Wahrscheinlichkeit, daß ein zufällig gewähltes b ein F-Zeuge für m ist, ist nur 0.0016. Für die Mengen

$$\begin{aligned} M_1 &:= \{b; 1 \leq b \leq 50000,\ b \text{ ist ein F-Zeuge für } m\} \\ &= \{1171, 2341, 2342, 3511, 3513, \ldots\}, \\ M_2 &:= \{b; 1 \leq b \leq 50000,\ b \text{ ist ein MR-Zeuge für } m\} \\ &= \{2, 3, 4, 5, 6, 7, 8, 10, 11, 13, \ldots\} \end{aligned}$$

gilt: M_1 hat 77 Elemente, M_2 hat 43588 Elemente. Beachte, daß

$$9624742921 = 1171 \cdot 2341 \cdot 3511 .$$

3 Ein probabilistischer Primtest und seine Zuverlässigkeit

Aus 2.6 ergibt sich:

Probabilistischer Prim-Test (PP-Test)
Zu einer gegebenen ungeraden Zahl n wähle zufällig Zahlen $b_1, \ldots, b_s$ mit $2 \leq b_\sigma \leq n-2$. Wenn auch nur eines der b_σ ein MR-Zeuge für n ist, dann erkläre n als nicht prim. Andernfalls erkläre n als prim.

Wie zuverlässig ist dieser Test? Wenn n prim ist, wird der PP-Test mit Sicherheit die Antwort "n ist prim" liefern. Wenn dagegen n zusammengesetzt ist, kann es vorkommen, daß der PP-Test eine Fehldiagnose stellt.

Satz 3.1 *Die Wahrscheinlichkeit, daß bei N Durchführungen des PP-Tests mit jeweils dem gleichen s wenigstens einmal eine Fehldiagnose gestellt wird, ist kleiner als $N/4^s$.*

Beweis. Wenn n zusammengesetzt ist, dann liefert der PP-Test eine richtige Antwort, wenn wenigstens eines der ausgewählten b_σ ein MR-Zeuge ist. Die Wahrscheinlichkeit dafür ist größer als $1 - 1/4^s$. Also ist die Wahrscheinlichkeit, bei N-maliger Anwendung des PP-Tests stets die richtige Antwort zu erhalten, größer als $(1 - 1/4^s)^N$, da in den Fällen, wo n prim ist, sicherlich die richtige Antwort gegeben wird. Also ist die Wahrscheinlichkeit, bei N-maliger Anwendung des PP-Test wenigstens einmal eine falsche Antwort zu erhalten, kleiner als $1 - (1 - 1/4^s)^N < 1 - (1 - N/4^s) = N/4^s$.

Das folgende Beispiel soll erläutern, wie ungeheuer groß die Zuverlässigkeit des PP-Tests ist:

Wenn seit 10 Milliarden Jahren (das heißt etwa seit dem Urknall) 10 Milliarden Mathematiker jede Sekunde 10 Milliarden mal den PP-Test anwenden mit $s = 100$, dann ist die Wahrscheinlichkeit, daß dabei wenigstens einmal eine zerlegbare Zahl fälschlicherweise als prim erklärt wird, kleiner als 10^{-20}, also praktisch gleich Null.

Für "kleine" n wird der probabilistische Primtest zu einem deterministischen Primtest:

Satz 3.2 *Es sei n eine ungerade Zahl.*

1. *Wenn $n < 1373653$ ist, dann ist n genau dann prim, wenn 2 und 3 keine MR-Zeugen für n sind.*
2. *Wenn $n < 25 \cdot 10^9$, dann ist n genau dann prim, wenn $2, 3, 5, 7$ und 11 keine MR-Zeugen für n sind. (Die einzige zusammengesetzte Zahl $n < 25 \cdot 10^9$, für die keine der Zahlen $2, 3, 5$ und 7 eine MR-Zeuge ist, ist $n = 3215031751 = 151 \cdot 751 \cdot 28351$).*

Zum *Beweis* vgl. [11].

Es wäre schön, wenn man entsprechend für beliebige n eine explizite sehr kleine Schranke $S(n)$ hätte mit folgender Eigenschaft:

$$\text{Kein } b \leq S(n) \text{ ist MR-Zeuge für } n \implies n \text{ ist prim .}$$

Wenn die sog. "Verallgemeinerte Riemannsche Vermutung" richtig ist, so gibt es in der Tat eine solche Schranke (man kann dann $S(n) = 2 \cdot (\ln n)^2$ wählen, vgl. [9], [17]), und man hat dann einen deterministischen Primtest, dessen Rechenaufwand polynomial (vom Grad 5, vgl. [8]) ist in Abhängigkeit von der Anzahl Ziffern der zu behandelnden Zahl. Da bei allen bekannten korrekten deterministischen Primtests der Rechenaufwand schneller wächst als polynomial, ist dieser Algorithmus (zumindest für genügend grosse Zahlen) schneller als alle bisher bekannten Algorithmen. Leider ist nicht bekannt, ob er immer das richtige Resultat liefert.

Es sei noch angefügt, daß die oben erwähnte Schranke $S(n) = 2(\ln n)^2$ zumindest für kleine n viel zu groß ist, kann man doch $S(n) = 11$ wählen für $n \leq 25 \cdot 10^9$.

4 Ein deterministischer Primtest mit Zertifikat

Nach "menschlichem Ermessen" wird, wie wir oben gesehen haben, der probabilistische Primtest nie zu einem Fehlentscheid führen, wenn man z.B. $s = 100$ wählt. Der Mathematiker möchte aber absolute Sicherheit haben: Er erkennt n erst dann als Primzahl an, wenn ein Beweis vorliegt, daß n prim ist. In vielen Fällen kann man einen solchen Beweis führen mit

Theorem 4.1 *Eine ungerade Zahl $n \geq 3$ ist genau dann prim, wenn es zu jedem Primteiler p von $n-1$ eine Zahl $b_p < n$ gibt mit*

$$b_p \text{ ist kein MR-Zeuge für } n, \quad b_p^{(n-1)/p} \not\equiv_n 1. \qquad (*)$$

Zum *Beweis* vgl. Abschnitt 6.

Damit ergibt sich nun leicht ein Algorithmus, der entscheidet, ob die gegebene ungerade Zahl n prim ist oder nicht (wenn sie prim ist, wird ein leicht nachvollziehbarer Prim-Beweis mitgeliefert); dazu müssen wir allerdings annehmen, daß wir alle Primteiler von $n-1$ kennen:

Deterministischer Primtest
Für jeden Primfaktor p von $n-1$ suche durch Ausprobieren Zahlen $b_p < n$ mit der Eigenschaft $(*)$. Sobald man bei diesem Suchen ein b findet, welches ein MR-Zeuge für n ist, ist man sicher, daß n nicht prim ist. Wenn man zu jedem p ein b_p mit der Eigenschaft $(*)$ gefunden hat, ist man wegen 4.1 sicher, daß n prim ist.

Wenn dieser Algorithmus zu einer Entscheidung gekommen ist, dann liefert er einen Beweis (Zertifikat) für die Richtigkeit seiner Entscheidung: Wenn n nicht prim ist, dann ist der MR-Zeuge b ein Beweis für die Zerlegbarkeit von n. Wurde dagegen n als prim erkannt, dann ist die Liste aller Paare (p, b_p) wegen 4.1 ein Beweis dafür, daß n prim ist.

Wenn nicht klar ist, daß die angegebenen Faktoren p_σ von $n-1$ wirklich Primzahlen sind, muß man natürlich Primbeweise für die p_σ hinzufügen. Dadurch wird ein Primbeweis ein baumartiges Gebilde, das an zwei Beispielen erläutert werden soll:

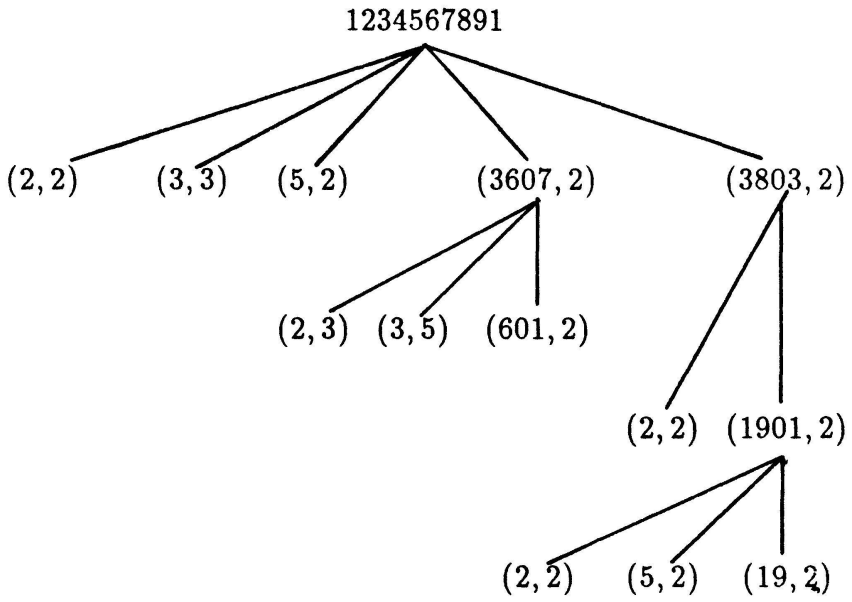

Fig. 1

Die zweite Zeile dieses Primbeweises besagt, daß 1234567890 die Primfaktoren 2, 3, 5, 3607 und 3803 besitzt und daß $(*)$ gilt für die Paare $(p, b_p) = (2,2), (3,3), (5,2),$

(3607, 2) und (3803, 2). Die folgenden Zeilen beweisen, daß 3607 und 3803 prim sind. Es sei speziell darauf verwiesen, daß stets $b_p \leq 3$ gewählt werden kann.

Der folgende Baum beweist, daß $E(23)$ prim ist (dabei kann stets $b_p \leq 11$ gewählt werden):

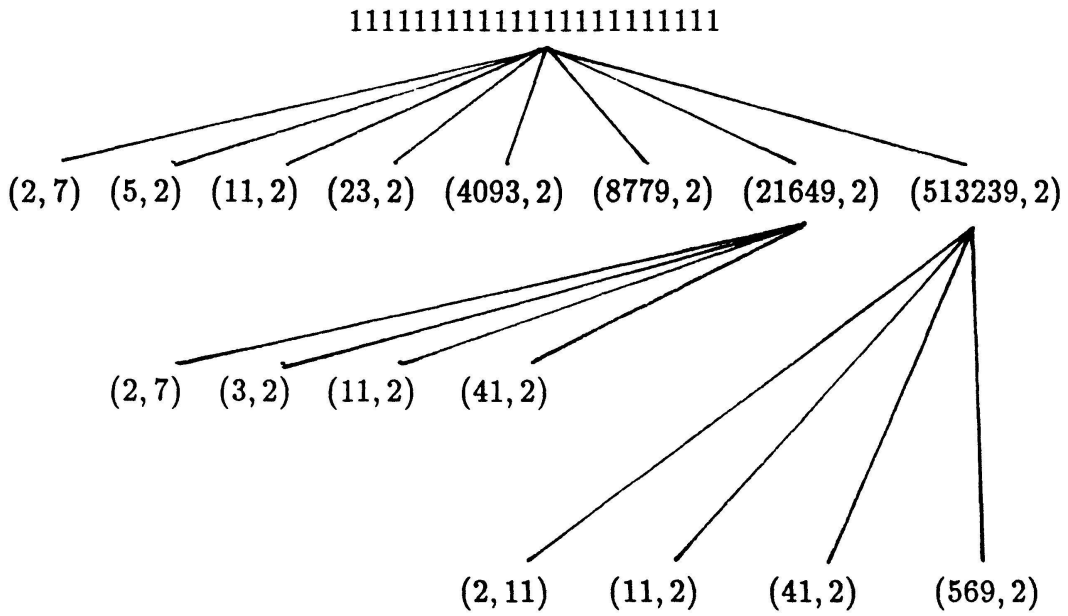

Fig. 2

Der gleiche Primbeweis kann auch in Form einer Liste dargestellt werden (eine solche Ausgabe wird man etwa von einem rekursiven Programm erhalten, welches mit dem oben angegebenen deterministischen Primtest arbeitet; für Primzahlen unter 10000 wurde kein Primbeweis geführt):

$$\{11111111111111111111, \{2,7\}, \{5,2\}, \{11,2\}, \{23,2\}, \{4093,2\}, \{8779,2\},$$
$$\{21649, \{21649, \{2,7\}, \{3,2\}, \{11,2\}, \{41,2\}\}, 2\},$$
$$\{513239, \{513239, \{2,11\}, \{11,2\}, \{41,2\}, \{569,2\}\}, 2\}\}$$

Wie lange muß man suchen, um mit dem deterministischen Primtest auch wirklich zu einer Entscheidung zu kommen (wir setzen voraus, daß alle Primfaktoren von $n-1$ bekannt sind)? Wenn n nicht prim ist, dann ist ein zufällig gewähltes b wenigstens mit der Wahrscheinlichkeit 3/4 ein MR-Zeuge (vgl. 2.6). Wenn n prim ist, dann müssen wir zu jedem p ein b_p mit der Eigenschaft $(*)$ finden. Wieviele solche b_p gibt es? Eine erfreuliche Antwort liefert

Satz 4.2 *Wenn $n < 10^{100}$ (bzw. $n < 10^{600}$) eine Primzahl ist, dann gibt es wenigstens $(n-1)/10$ (bzw. $(n-1)/13$) Zahlen b mit $2 \leq b \leq n-2$ und*

$$b^{n-1} \underset{n}{\equiv} 1, \qquad b^k \underset{n}{\not\equiv} 1 \text{ für } 1 \leq k \leq n-2.$$

Alle diese b können in $(*)$ für jedes p gewählt werden.

Zum *Beweis* siehe Abschnitt 6. Damit erhalten wir die sehr grobe Abschätzung

Korollar 4.3 *Wenn $n < 10^{100}$ prim ist und p ein Primfaktor von $n-1$, dann ist die Wahrscheinlichkeit, daß unter s zufällig ausgewählten Zahlen $b_1, \ldots, b_s$ mit $2 \leq b_\sigma \leq n-2$ wenigstens eine ist mit $b_\sigma^{n-1} \underset{n}{\equiv} 1$ und $b_\sigma^{(n-1)/p} \underset{n}{\not\equiv} 1$, mindestens gleich $1-(9/10)^s$.*

Die Erfahrung zeigt, daß man ruhig einfach die Werte $b = 2, 3, 5, \ldots$ ausprobieren kann (nur sehr selten wird man $b \geq 50$ wählen müssen).

Insgesamt ergibt sich also, daß man mit einer großen Wahrscheinlichkeit erwarten darf, daß der Algorithmus wirklich in vernünftiger Zeit eine Entscheidung liefert, ob die zu untersuchende Zahl prim ist oder nicht.

Wie bereits mehrfach erwähnt, haben wir vorausgesetzt, daß wir alle Primfaktoren von $n-1$ kennen. Wenn das nicht der Fall ist, dann tauchen die folgenden zwei Probleme auf:

1. Wir müssen Faktoren von $n-1$ finden und
2. wir müssen beweisen können, daß die gefundenen Faktoren wirklich prim sind (sonst müssen wir noch weiter zerlegen).

Das zweite Problem läßt sich leicht lösen, indem man ein rekursives Programm schreibt (mit 3.2 sind wir sowieso in der Lage, für $p < 10^9$ ohne 4.1 zu entscheiden, ob n prim ist). Für das erste Problem gibt es viele Algorithmen, auf die hier jedoch nicht eingegangen werden soll. Für nicht zu große n (etwa $n < 10^{20}$) findet man Zerlegungen von $n-1$ z.B. mit der "Pollard'schen ρ-Methode" (vgl. [14]; dort wird ein konkreter Algorithmus in PASCAL angegeben). Mit dieser Methode kann man mit etwas Glück auch Zerlegungen einiger sehr viel größerer Zahlen bekommen. Es sei nochmals darauf hingewiesen (siehe Einleitung), daß ein Primbeweis, welcher große Zahlen faktorisieren muß, für beliebig große Zahlen unbrauchbar ist.

Wir beschließen diesen Abschnitt mit einem Kommentar zu 4.2. Die in 4.2 beschriebenen b sind genau die primitiven Elemente des Körpers $\mathbb{Z}_n := \mathbb{Z}/(n\mathbb{Z})$, d.h. die Elemente, deren Ordnung in der Einheitengruppe $\mathbb{Z}_n^*$ gerade $n-1$ ist. Wegen [16, Theorem 2 in §1.1] gibt es stets solche Elemente. Wenn b die Ordnung $n-1$ hat, dann hat b^k genau dann ebenfalls die Ordnung $n-1$, wenn k und $n-1$ teilerfremd sind. Folglich gibt es genau $\varphi(n-1)$ Elemente der Ordnung $n-1$ (dabei ist φ die Euler'sche Funktion). Ein zufällig gewähltes $b \in \mathbb{Z}_n^*$ hat also mit der Wahrscheinlichkeit $\varphi(n-1)/(n-1)$ die in 4.2 geforderten Eigenschaften.

Keineswegs trivial ist nun die Tatsache, daß der Ausdruck $\varphi(n-1)/(n-1)$ beliebig klein werden kann:

Satz 4.4 *Zu jeder positiven Zahl $\varepsilon > 0$ gibt es eine Primzahl n mit $\varphi(n-1)/(n-1) < \varepsilon$.*

Einen Beweis findet man in Abschnitt 6. Weitere Resultate zu diesem Thema findet man in [13, Seiten 16ff].

5 Konstruktion großer Primzahlen

Mit dem folgenden Verfahren können Sie "neue" Primzahlen konstruieren:

Wählen Sie Primzahlen $p_1, \ldots, p_r$ und positive Exponenten $e_1, \ldots, e_r$ so, daß die Zahl

$$N := p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$$

etwa so viele Stellen hat wie die zu bestimmende Primzahl. Suchen Sie jetzt (durch Ausprobieren) einen kleinen Faktor f, für den

$$n := fN + 1$$

prim ist.

Da Sie (solange f nicht zu groß gewählt ist) alle Primfaktoren von $n - 1 = fN$ kennen, können Sie mit den oben angegebenen Verfahren entscheiden, ob $fN + 1$ prim ist oder nicht. Achten Sie darauf, daß das Produkt fN stets gerade ist (wenn 2 nicht unter den p_ρ ist, dann müßen Sie stets gerade Faktoren f nehmen), weil sonst sicherlich $fN + 1$ keine Primzahl ist.

Die folgende Liste gibt einige Beispiele für das oben genannte Verfahren (wir haben stets $p_1 = 2$, $p_2 = 5$ und $e_1 = e_2 =: k$ gewählt; angegeben wird stets das kleinste f, für das $n := f \cdot 10^k + 1$ prim ist)

k	f	Primbeweis für $n = f \cdot 10^k + 1$
10	3	$\{2,7\},\{3,2\},\{5,5\}$
20	6	$\{2,7\},\{3.2\},\{5,2\}$
30	63	$\{2,17\},\{3,2\},\{5,2\},\{7.3\}$
40	24	$\{2,7\},\{3,2\},\{5,2\}$
50	85	$\{2,3\},\{5,2\},\{17,2\}$
60	19	$\{2,3\},\{5,2\},\{19,2\}$
70	114	$\{2,13\},\{3,2\},\{5,5\},\{19,2\}$
80	12	$\{2,11\},\{3,2\},\{5,2\}$
90	126	$\{2,11\},\{3,2\},\{5,2\},\{7,3\}$
100	111	$\{2,11\},\{3,2\},\{5,2\},\{37,2\}$
200	90	$\{2,7\},\{3,13\},\{5,2\}$
300	231	$\{2,13\},\{3,2\},\{5,2\},\{7,2\},\{11,2\}$

In den obigen Primbeweisen sind jeweils Paare $\{p, b_p\}$ angegeben, für die p ein Primfaktor von $n - 1$ ist und für die $(*)$ von 4.1 gilt.

Wenn Sie Primzahlen zum Verschlüsseln von Texten mit öffentlich bekanntem Code konstruieren wollen, dann sollten Sie (damit Ihr Code nicht einfach zu knacken ist)

gemäß [5, 3.2] die Primzahl n in der folgenden Form wählen:

$$n = fp + 1, \text{ wobei } p = gq + 1, \quad p \text{ und } q \text{ große Primzahlen, } f \text{ und } g \text{ kleine Faktoren.}$$

Konstruieren Sie also zunächst ein q wie oben angegeben, daraus dann p und damit das endgültige n.

6 Beweise

Es sei $\mathbb{N}$ die Menge der natürlichen und $\mathbb{Z}$ die Menge der ganzen Zahlen, $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}_n^*$ die multiplikative Gruppe der Einheiten von $\mathbb{Z}_n$.

Zunächst einige Vorbemerkungen zu den folgenden Beweisen.

Satz 6.1 *Für $2 \leq n \in \mathbb{N}$ wird die Ordnung der Gruppe $\mathbb{Z}_n^*$ gegeben durch*

$$\varphi(n) := \text{ Anzahl derjenigen } b \text{ mit } 1 \leq b < n, \text{ die zu } n \text{ teilerfremd sind .}$$

Die Funktion $\varphi : \mathbb{N}_{n\geq 2} \longrightarrow \mathbb{N}$ wird auch **Eulersche Funktion** *genannt. Sie hat folgende Eigenschaft:*

Es seien p_σ paarweise verschiedene Primzahlen, $\alpha_\sigma \geq 1$. Dann ist

$$\varphi\left(\prod_{\sigma=1}^{s} p_\sigma^{\alpha_\sigma}\right) = \prod_{\sigma=1}^{s} p_\sigma^{\alpha_\sigma - 1}(p_\sigma - 1).$$

Korollar 6.2 *Für $m = \prod_{\sigma=1}^{s} p_\sigma^{\alpha_\sigma}$ ist $\dfrac{m}{\varphi(m)} = \prod_{\sigma=1}^{s} \dfrac{p_\sigma}{p_\sigma - 1}$.*

Insbesondere hängt $m/\varphi(m)$ nur ab von den Primfaktoren von m, nicht von ihrem Exponenten in m. Ferner gilt $m/\varphi(m) \leq n/\varphi(n)$, wenn m ein Teiler von n ist.

Satz 6.3 *Es sei $n \geq 3$ eine Primzahl. Dann ist $\mathbb{Z}_n$ ein Körper, und die multiplikative Gruppe $\mathbb{Z}_n^*$ ist zyklisch von der Ordnung $\varphi(n-1) = n - 1$.*

Zum *Beweis* vgl. [16, Ch. I, Theorem 2].

Beweis von 2.2 n ist genau dann prim, wenn $\mathbb{Z}_n^*$ ein Körper ist, d.h. wenn $\mathbb{Z}_n^*$ aus $n-1$ Elementen besteht. Wenn n prim ist, gilt also $b^{n-1} \underset{n}{\equiv} 1$ für jedes $b \in \mathbb{Z}_n^*$, da die Ordnung eines Elementes stets die Gruppenordnung teilt. Umgekehrt folgt aus $b^{n-1} \underset{n}{\equiv} 1$, daß b eine Einheit ist, also hat $\mathbb{Z}_n^*$ genau $n-1$ Elemente.

Beweis von 2.4 Ad 1. Da $b^{n-1} (\mathrm{mod}\, n) = c_q$ sich aus den c_k durch wiederholtes Quadrieren modulo n ergibt und da $(-1)^2 = 1$, ist b kein F-Zeuge für n, wenn b kein MR-Zeuge für n ist.

Ad 2. Es genügt zu zeigen: Wenn n prim ist, dann hat n keine MR-Zeugen. Es sei also n prim, $2 \leq b \leq n-2$ und $c_0, \ldots, c_q = b^{n-1} (\mathrm{mod}\, n)$ wie in 2.3. Da $\mathbb{Z}_n$ ein Körper ist, hat die Gleichung $x^2 = 1$ in $\mathbb{Z}_n$ höchstens die Lösungen 1 und $n-1$; da (in $\mathbb{Z}_n$) für $1 \leq k \leq q$ gilt $c_{k-1}^2 = c_k$ und $c_q = 1$, ist entweder $c_k = 1$ für $0 \leq k \leq q$ oder es gibt ein $k < q$ mit $c_k = n - 1$; in jedem Fall ist b kein MR-Zeuge.

Beweisskizze von 2.5 Da ein vollständiger Beweis zwar elementar, aber doch etwas länger ist, beschränken wir uns hier auf die Beweisskizze eines Spezialfalles: Wir setzen voraus, dass $n = p^2m$, wobei $p \geq 3$ eine Primzahl ist. In diesem Fall hat n nicht nur wenig MR-Zeugen, sondern auch nur wenig F-Zeugen: Wir zeigen, dass

$$\#\{b \in \mathbb{Z}_n;\ b^{n-1} = 1\} \leq (p-1)m. \qquad (*)$$

Da (wie man leicht nachrechnet) für $p \geq 3$ und $m \geq 1$ stets gilt

$$(p-1)m \leq \frac{p^2m-1}{4} = \frac{n-1}{4},$$

folgt aus $(*)$ also unsere Behauptung.

Beweisskizze von $(*)$: die Einheitengruppe $\mathbb{Z}_{p^2}^*$ ist zyklisch von der Ordnung $p(p-1)$; also hat die Menge

$$\{\beta \in \mathbb{Z}_{p^2}^*;\ \beta^{n-1} = 1\}$$

genau $d := \mathrm{ggT}\,(p(p-1), n-1)$ Elemente. Da p ein Teiler von n ist, ist d ein Teiler von $p-1$, also $d \leq p-1$. Es sei π die kanonische Projektion von $\mathbb{Z}_n$ auf $\mathbb{Z}_{p^2}$; für jedes $\beta \in \mathbb{Z}_{p^2}$ hat $\pi^{-1}(\beta)$ genau m Elemente; folglich hat $\{b \in \mathbb{Z}_n;\ b^{n-1} = 1\}$ höchstens $dm \leq (p-1)m$ Elemente.

Auch für beliebiges ungerades zerlegbares n kann man die Anzahl der MR-Zeugen für n explizit angeben und damit 2.5 beweisen (vgl. Theorem 5 und Proposition 1 in [10]).

Beweis von 4.1 Wenn n prim ist, dann gibt es wegen 6.3 im Körper $\mathbb{Z}_n$ ein Element b der Ordnung $n-1$. Dieses b kann man für alle p nehmen. Zum Beweis der Umkehrung genügt es zu zeigen, daß $n-1$ ein Teiler von $\mathrm{ord}(\mathbb{Z}_n^*)$ ist. Dazu sei p ein Primfaktor von $n-1$ und α der Exponent von p in $n-1$. Nach Voraussetzung gibt es ein b mit $b^{n-1} \underset{n}{\equiv} 1 \underset{n}{\not\equiv} b^{(n-1)/p}$. Dann ist die Ordnung e von b in $\mathbb{Z}_n^*$ ein Teiler von $n-1$, nicht aber von $(n-1)/p$; also ist p^α ein Teiler von e und damit auch ein Teiler von $\mathrm{ord}(\mathbb{Z}_n^*)$, da e die Ordnung von $\mathbb{Z}_n^*$ teilt.

Beweis von 4.2 Die Gruppe $\mathbb{Z}_n^*$ hat genau $\varphi(n-1)$ Elemente der Ordnung $n-1$ (vgl. 6.3). Wir müssen also zeigen, daß $(n-1)/\varphi(n-1) < 10$ gilt, wenn $n < 10^{100}$ eine Primzahl ist (der Beweis für $n < 10^{600}$ verläuft analog).

Dazu seien zunächst $p_1 = 2,\ p_2 = 3, \ldots, p_{54} = 251$ die ersten 54 Primzahlen. Es gilt (Beweis durch brutales Nachrechnen)

$$9 < \frac{R}{\varphi(R)} = \prod_{\sigma=1}^{54} \frac{p_\sigma}{p_\sigma - 1} < 10 \quad \text{für} \quad R := \prod_{\sigma=1}^{54} p_\sigma \approx 6 \cdot 10^{100} \qquad (**)$$

Es sei jetzt $n < 10^{100}$ eine Primzahl, es seien $q_1 < q_2 < \ldots < q_s$ die Primfaktoren von $n-1$. Wegen $(**)$ ist $s \leq 54$. Da $p_k \leq q_k$ für $1 \leq k \leq s$, folgt also mit 6.2

$$\frac{n-1}{\varphi(n-1)} = \prod_{\sigma=1}^{s} \frac{q_\sigma}{q_\sigma - 1} \leq \prod_{\sigma=1}^{s} \frac{p_\sigma}{p_\sigma - 1} \leq \prod_{\sigma=1}^{54} \frac{p_\sigma}{p_\sigma - 1} < 10.$$

Beweis von 4.4 Es sei $p_1 = 2$, $p_2 = 3, \ldots$ die Folge aller Primzahlen. Wegen (zum Beweis dieser Aussage vgl. [16, Ch. VI, § 3, Lemma 5])

$$\lim_{s \searrow 1} \prod_{\sigma=1}^{\infty} \frac{p_\sigma^s}{p_\sigma^s - 1} = \lim_{s \searrow 1} \sum_{k \geq 1} \frac{1}{k^s} = \infty$$

gibt es ein $S \in \mathbb{N}$ mit $P := \prod_{\sigma=1}^{S} p_\sigma/(p_\sigma - 1) > N$. Es bleibt zu zeigen, daß es eine Primzahl n gibt mit $(n-1)/\varphi(n-1) \geq P$: dazu sei $a := \prod_{k=1}^{S} p_k$. Wegen 6.4 gibt es ein $\nu \in \mathbb{N}$ für welches $n := \nu a + 1$ prim ist. Aus 6.2 ergibt sich jetzt $(n-1)/\varphi(n-1) \geq a/\varphi(a) = P$.

Theorem 6.4 (Dirichlet) *Es seien a, b teilerfremde natürliche Zahlen. Dann enthält die arithmetische Progression $\{\nu a + b;\ \nu \in \mathbb{N}\}$ unendlich viele Primzahlen.*

Zum *Beweis* vgl. [16, Ch. VI].

Literatur

[1] Brillhart, J., Lehmer, D.H., Selfridge, J.L., Tuckerman, B., Wagstaff, S.S.: Factorizations of $b^n \pm 1$. Contemporary Math, AMS vol. 22

[2] Cohen, H., Lenstra, H.W. Jr.: Primality Testing and Jacobi sums. Mathematics of Computation **42** (1984), 297–330.

[3] Granville, A.: Primality Testing and Carmichael Numbers. Notices of the AMS **39** (1992), 696–700.

[4] Head, A.K.: Multiplication modulo n, BIT **20** (1980), 115–116.

[5] Hoogendoorn, P.J.: On a secure Public-Key Cryptosystem. in: Computational Methods in Number Theory, Part I. Mathematical Centre Tracts 154. Mathematisch Centrum Amsterdam 1984, edited by H.W. Lenstra Jr. and R. Tijdeman.

[6] Koblitz, N.: A Course in Number Theory and Cryptography. GTM **114**, Springer 1987

[7] Lang, S.: Primzahlen. El. Math. **47** (1992), 49–61.

[8] Lenstra, H.W.Jr.: Primality Testing. in: Computational Methods in Number Theory, Part I. Mathematical Centre Tracts 154. Mathematisch Centrum Amsterdam 1984, edited by H.W. Lenstra Jr. and R. Tijdeman.

[9] Miller, G.: Riemann's Hypothesis and tests for primality. Journal of Computer and System Sciences **13** (1976), 300–317.

[10] Monier, L.: Evaluation and comparison of two efficient probabilistic primality testing algorithms. Theoret. Comp. Sc. **12** (1980), 97–108.

[11] Pomerance, C., Selfridge, J.L., Wagstaff, S.S.: The pseudoprimes to $25 \cdot 10^9$ Math. Comp. **35** (1980), 1003–1026.

[12] Rabin, M.O.: Probabilistic algorithm for testing primality. J. Number Theory **12** (1971), 281–292.

[13] Ribenboim, P.: The Book of Prime Number Records. Springer 1988.

[14] Riesel, H.: Prime Numbers and Computer Methods for Factorisation. Birkhäuser 1985

[15] Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, vol. **21**, Nr. 2 (1978).

[16] Serre, J.P.: A Course in Arithmetic. Graduate Texts in Math. 7 Springer 1973.

[17] Wagon, S.: Primality Testing. The Mathematical Intelligencer, Vol. 8, No. 3 (1986), 58–61.

Burchard Kaup
Math. Inst. der Universität
ch. du Musée 23
CH-1700 Freiburg