Zahlentheorie und Kryptographie

Aloys Krieg

Vortrag im Münsteraner Kolloquium zur Geschichte und Didaktik der Mathematik am 30.11.99

Ziel dieses Vortrags ist es, ausgehend von den Grundvorlesungen der Mathematik einen Einblick in Fragen, Methoden und Probleme der modernen Zahlentheorie zu geben. Insbesondere soll deutlich werden, wie man Oberstufenschüler an diesen Problemkreis heranführen kann.

1. Der Fundamentalsatz der Arithmetik

Wir bezeichnen die Menge der *natürlichen Zahlen* mit

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

Bekanntlich heißt eine natürliche Zahl $p > 1$, die nur durch 1 und p teilbar ist, eine *Primzahl*. Eine natürliche Zahl $n > 1$, die keine Primzahl ist, nennt man *zerlegbar*. Die Bedeutung der Primzahlen liegt in dem folgenden

Fundamentalsatz der Arithmetik. *Jede natürliche Zahl $n > 1$ ist bis auf die Reihenfolge eindeutig als Produkt von Primzahlpotenzen darstellbar, d.h. es existieren $k \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_k$ und $r_1, \ldots, r_k \in \mathbb{N}$ mit der Eigenschaft*

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}.$$

Beispiel.

$$\begin{array}{lll} 28 & = 2^2 \cdot 7 & \\ 286 & = 2 \cdot 11 \cdot 13 & \\ 2^{29} - 1 & = 233 \cdot 1.103 \cdot 2.089 & \approx 5 \cdot 10^8 \\ 2^{32} + 1 & = 641 \cdot 6.700.417 & \approx 4 \cdot 10^9 \\ 3^{59} - 2^{59} & = \quad ? & \approx 10^{28} \end{array}$$

Das letzte Beispiel zeigt, wie schwierig es ist, selbst bei für unser Computerzeitalter mäßig großen Zahlen die konkrete Faktorisierung zu berechnen.

Vom algorithmischen Standpunkt gibt es zwei verschiedene Ansätze:

Problem 1. Wie entscheidet man, ob eine gegebene Zahl $n \in \mathbb{N}$ eine Primzahl ist?

Problem 2. Wie bestimmt man die Primfaktorzerlegung einer gegebenen Zahl $n \in \mathbb{N}$, die zerlegbar ist?

Diese beiden Probleme haben einen unterschiedlichen Schwierigkeitsgrad. Auf dieser Tatsache beruhen die Anwendungen in der Kryptographie.

2. Welche Anwendungen gibt es?

Es gibt eine bedeutsame Anwendung in der Kryptographie, weil man Chiffrierverfahren auf der Grundlage dieser Erkenntnisse entwickeln kann. Die erste Methode dieser Art wurde 1977 von Rivest, Shamir und Adleman angegeben und heißt *RSA-Verfahren*. Es hat sich in der Praxis bewährt und wird heutzutage in der Verschlüsselung auf Geld- und Scheckkarten, für E-Mail und Internet allgegenwärtig eingesetzt.

Das Verfahren beruht auf dem Kleinen Satz von Fermat:

Sei G eine endliche Gruppe mit neutralem Element e. Dann gilt für jedes $a \in G$

$$a^{ord\, G} = e.$$

Diese Aussage wird angewendet auf die prime Restklassengruppe

$$\begin{aligned} G = (\mathbb{Z}/n\mathbb{Z})^{\times} &= \{a + n\mathbb{Z};\ a \in \mathbb{Z},\ ggT(a,n) = 1\} \\ &= \{a\, mod\, n;\ \text{es gibt } b\, mod\, n \text{ mit } ab = 1\, mod\, n\}, \\ ord\, G = \varphi(n) &= \sharp\{m \in \mathbb{N}; 1 \leq m \leq n,\ ggT(m,n) = 1\}, \\ a^{\varphi(n)} &\equiv 1\, mod\, n \quad \text{und} \quad a^{\varphi(n)+1} \equiv a\, mod\, n \quad \text{für } a \in \mathbb{Z},\ ggT(a,n) = 1. \end{aligned}$$

Man nimmt eine Zahl $n = p \cdot q$, wobei p, $q \approx$ 100-stellige Primzahlen sind. Eine Nachricht wird mit Hilfe dieser Zahl n chiffriert. Zum Dechiffrieren benötigt man die Zerlegung $n = p \cdot q$. Wenn nur n bekannt ist, gibt es heute keine Möglichkeit, die Faktorisierung zu berechnen.

Man wählt

$$k, l \in \mathbb{N} \ \text{ mit } k \cdot l = \varphi(n) + 1 = (p-1) \cdot (q-1) + 1.$$

Die zu übermittelnde Nachricht sei $a \in \mathbb{N}, 1 \leq a < n$. Wir schreiben nach Division mit Rest

$$a^k = n \cdot x + r \quad \text{mit} \quad x, r \in \mathbb{N}_0,\ 0 \leq r < n.$$

Übermittelt wird r. Zum Entschlüsseln verwenden wir wieder Division mit Rest

$$r^l = n \cdot y + s \quad \text{mit} \quad y, s \in \mathbb{N}_0,\ 0 \leq s < n.$$

Weil n quadratfrei ist, folgt aus dem Kleinen Satz von Fermat

$$s = a.$$

Selbst wenn n und k bekannt sind, muss man die Faktorisierung $n = p \cdot q$ kennen, um l zu finden und um damit a aus r zu berechnen.

Ein Problem könnte der hohe Exponent sein, den man aber durch sukzessives Quadrieren schnell in den Griff bekommt. Man beachte, dass man nur $a^k mod\, n$ und nicht etwa a^k direkt berechnen muss.

Solche Verfahren nennt man *Public-Key-Krypto-Systeme.*

Beispiel.

$$\begin{array}{lll} n = 11 \cdot 17 = 187; & p = 11,\ q = 17; & \\ \varphi(n) + 1 = 10 \cdot 16 + 1 = 7 \cdot 23; & k = 7,\ l = 23; & \\ a = 3, & 3^7 = 2.187 = 11 \cdot 187 + 130, & r = 130 \\ 130^{23} = 187 \cdot y + 3, & s = 3. & \end{array}$$

Die Berechnung von $130^{23}\, mod\, 187$ soll verdeutlicht werden:

$$\begin{aligned} 23 &= 2^4 + 2^2 + 2 + 1 \\ 130^2 &= 187 \cdot 90 + 70 \equiv 70 \\ 130^4 &\equiv 70^2 = 187 \cdot 26 + 38 \equiv 38 \\ 130^8 &\equiv 38^2 = 187 \cdot 7 + 135 \equiv 135 \\ 130^{16} &\equiv 135^2 = 187 \cdot 97 + 86 \equiv 86 \\ 130^{23} &\equiv 86 \cdot 38 \cdot 70 \cdot 130 = 187 \cdot 159.031 + 3 \equiv 3 \\ 130^{23} &\approx 4 \cdot 10^{48}. \end{aligned}$$

3. Wie erkennt man Primzahlen?

Zu den Standardergebnissen einer Zahlentheorie-Vorlesung gehört das folgende Reduktionsresultat, das wir in 2 Varianten formulieren.

Lemma. *Sei* $n \in \mathbb{N}, n > 1$.
a) *Ist* n *zerlegbar, so besitzt* n *einen Primteiler* $p \leq \sqrt{n}$.
b) *Wird* n *von keiner Primzahl* p *mit* $p \leq \sqrt{n}$ *geteilt, so ist* n *eine Primzahl.*

Beweis. a) Sei $n = u \cdot v, \quad 1 < u \leq v$. Dann gilt

$$u^2 \leq u \cdot v = n, \quad \text{also} \quad u \leq \sqrt{n}$$

Demnach erfüllt jeder Primteiler p von u auch $p \,|\, n$ und $p \leq \sqrt{n}$.
b) Diese Aussage ist äquivalent zu a). □

Dieses Verfahren stößt in der Praxis relativ schnell an seine Grenzen. Sei n etwa eine 40-stellige Primzahl:

$$n \approx 10^{40}, \quad \sqrt{n} \approx 10^{20}.$$

Nach dem Primzahlsatz gibt es etwa $2 \cdot 10^{18}$ Primzahlen $\leq \sqrt{n}$. Also sind $2 \cdot 10^{18}$ Tests erforderlich, um zu beweisen, dass n eine Primzahl ist. Ein Hochleistungsrechner ist in der Lage, pro Sekunde etwa 10^8 Tests durchzuführen. Also benötigen wir

$$\approx 2 \cdot 10^{10}\ sec \approx 634\ Jahre.$$

Auch wesentlich schnellere Rechner erhöhen die Anwendungsmöglichkeit nur geringfügig. Ein konzeptioneller Ansatz bringt dagegen wesentlich mehr.

Dennoch wird die im Lemma beschriebene *Trial Division* in der Praxis stets eingesetzt, um kleine Primteiler auszuschließen.

Die Gleichung $a^{p-1} \equiv 1\, mod\, p$ für jede Primzahl p und $1 \leq a < p$ nach dem Kleinen Satz von Fermat eignet sich, um nachzuweisen, dass eine gegebene Zahl zerlegbar ist.

Kleiner-Fermat-Test auf Zerlegbarkeit natürlicher Zahlen.

Gegeben sei $n \in \mathbb{N}$, $n > 7$.

Schritt 1. *Ist n durch 2, 3, 5 oder 7 teilbar?*
ja $\rightarrow$ zerlegbar, nein $\rightarrow$ Schritt 2.
Schritt 2. *Gilt* $2^{n-1} \equiv 1\, mod\, n$?
nein $\rightarrow$ zerlegbar, ja $\rightarrow$ Schritt 3.
Schritt 3. *Gilt* $3^{n-1} \equiv 1\, mod\, n$ *oder* $5^{n-1} \equiv 1\, mod\, n$ *oder* $7^{n-1} \equiv 1\, mod\, n$?
nein $\rightarrow$ zerlegbar, ja $\rightarrow$ wahrscheinlich Primzahl.

Beispiel. Wir betrachten wieder $n = 187$ und stellen fest

$$2^{186} \equiv 174 \mod 187.$$

Also erkennt dieser Test, dass 187 keine Primzahl ist.

Hierbei handelt es sich um einen sogenannnten probabilistischen Test. Denn eine Zahl n, die von diesem Test nicht als zerlegbar erkannt wird, ist nur wahrscheinlich prim. Es gibt genau 1.770 Zahlen $n \leq 25 \cdot 10^9$, die diesen Test als vermutliche Primzahlen passieren, aber zerlegbar sind. Es gibt aber mehr als $4 \cdot 10^7$ Primzahlen $\leq 25 \cdot 10^9$. Die kleinste Nicht-Primzahl, die diesen Test als vermutlich prim passiert, ist....

Passiert eine Zahl diesen Test, so versucht man mit einem aufwendigeren Test, die Unzerlegbarkeit von n nachzuweisen. Zentral ist dazu der folgende

Satz. *Sei* $n \in \mathbb{N}$, $n > 2$ *und*

$$n - 1 = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

die Primfaktorzerlegung. Dann sind äquivalent:

(i) *n ist eine Primzahl.*

(ii) *Zu jedem $1 \leq j \leq n$ existiert ein $a_j \in \mathbb{N}$ mit den Eigenschaften*

$$a_j^{n-1} \equiv 1 \, mod \, n \quad und \quad a_j^{(n-1)/p_j} \not\equiv 1 \, mod \, n.$$

Beweis. (i) $\Rightarrow$ (ii): Ist n eine Primzahl, so ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper und die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch. Sei $a \, mod \, n$ ein Erzeuger. Wegen $ord(a + n\mathbb{Z}) = ord(\mathbb{Z}/n\mathbb{Z})^\times = n - 1$ gilt $(\mathbb{Z}/n\mathbb{Z})^\times = \{a^m \, mod \, n;\ 1 \leq m \leq n-1\}$, also

$$a^{n-1} \equiv 1 \, mod \, n \quad \text{und} \quad a^{(n-1)/p_j} \not\equiv 1 \, mod \, n, \quad j = 1, \dots, k.$$

Man kann demnach $a_j = a$ wählen.
(ii) $\Rightarrow$ (i): Für $j = 1, \dots, k$ gilt

$$ord(a_j + n\mathbb{Z}) \big| (n-1) \quad \text{und} \quad \tfrac{n-1}{p_j} \nmid ord\,(a_j + n\mathbb{Z}).$$

Daraus folgt mit dem Satz von Lagrange

$$p_j^{r_j} \big| ord(a_j + n\mathbb{Z}) \big| ord(\mathbb{Z}/n\mathbb{Z})^\times.$$

Weil $p_1, \dots, p_k$ paarweise verschieden sind, gilt

$$n - 1 = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k} \big| ord(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n), \quad \text{also} \quad \varphi(n) = n - 1.$$

Daher sind alle Zahlen m mit $1 \leq m < n$ zu n teilerfremd. Demnach ist n eine Primzahl. □

Um die Effektivität dieses Verfahrens zu unterstreichen, betrachten wir wieder das Beispiel $n = 3^{59} - 2^{59}$. Man testet für a_j nacheinander die Zahlen 2, 3, 5:

$$n = 3^{59} - 2^{59} = 14.130.386.091.162.273.752.461.387.579 \approx 1,4 \cdot 10^{28}$$
$$n - 1 = 2 \cdot 3 \cdot 7 \cdot 59 \cdot 1.151 \cdot 58.171 \cdot 123.930.193 \cdot 687.216.767$$

$2^{(n-1)/2}$	$\equiv$	-1	mod n
2^{n-1}	$\equiv$	1	mod n
$2^{(n-1)/3}$	$\equiv$	1	mod n
$3^{(n-1)/3}$	$\equiv$	1	mod n
$5^{(n-1)/3}$	$\equiv$	14.039.524.071.766.095.844.181.052.225	mod n
$5^{(n-1)/7}$	$\equiv$	782.661.097.299.526.754.770.837.537	mod n
$5^{(n-1)/59}$	$\equiv$	10.636.292.038.180.945.801.879.749.999	mod n
$5^{(n-1)/1.151}$	$\equiv$	3.216.430.705.463.480.598.022.736.901	mod n
$5^{(n-1)/58.171}$	$\equiv$	13.450.338.895.656.173.387.977.763.600	mod n
$5^{(n-1)/123.930.193}$	$\equiv$	3.732.507.535.185.619.691.818.435.804	mod n
$5^{(n-1)/687.216.767}$	$\equiv$	9.167.675.531.100.609.270.057.486.746	mod n
5^{n-1}	$\equiv$	1	mod n

Demnach ist $n = 3^{59} - 2^{59}$ eine Primzahl.

Möglichkeiten, $n-1$ zu zerlegen, werden im nächsten Abschnitt beschrieben. Der Nachteil dieses Verfahrens besteht natürlich darin, dass man die Primfaktorzerlegung von $n-1$ kennen muss. Es gibt aber auch andere Methoden, z.B. den Lucas-Test, in den die Primfaktorzerlegung von $n+1$ eingeht.

Mit diesen und ähnlichen Verfahren kann man heutzutage auf Hochleistungsrechnern von einer Zahl bis zu 1.000 Stellen innerhalb vertretbarer Zeit entscheiden, ob sie eine Primzahl ist oder nicht.

Die größte bekannte Primzahl ist aber sehr viel größer

$$p = 2^{6.972.593} - 1 \qquad \text{(Hajratwala, Juni 1999).}$$

p hat genau 2.098.960 Dezimalstellen. Hierbei handelt es sich um eine sog. *Mersennesche Zahl*

$$M_q = 2^q - 1, \quad q \text{ Primzahl.}$$

$M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{11} = 2.047 = 23 \cdot 89$. Wenn M_q prim ist, nennt man M_q eine *Mersennesche Primzahl.* Für M_q sind ganz spezielle Tests entwickelt worden, die für Zahlen dieser Bauart besonders gut funktionieren. Man verwendet stets einen speziellen Lucas-Test, so dass es nur auf die Schnelligkeit der eingesetzten Computer ankommt. Vom mathematischen Standpunkt ist diese Jagd nach Weltrekorden daher uninteressant. Informationen zu den aktuell größten bekannten Primzahlen findet man im Internet:

http://www.utm.edu/research/primes

4. Wie findet man die Primfaktorzerlegung?

Gegeben sei eine natürliche Zahl n, die wir als zerlegbar erkannt haben. Wie findet man nun einen Primteiler und sukzessiv die Faktorisierung? Die erste offensichtliche Methode ist das Probieren, die sog. *Trial Division.* Man testet nacheinander alle Primzahlen $\leq \sqrt{n}$. Diesem Verfahren sind jedoch enge Grenzen gesetzt, wie wir bereits gesehen haben.

Ein anderes Verfahren beruht auf dem folgenden

Lemma. *Sei $n > 1$ ungerade und zerlegbar. Dann gibt es $x, y \in \mathbb{N}_0$ mit*

$$n = x^2 - y^2 = (x-y)(x+y), \quad x - y > 1.$$

Beweis. Sei $n = u \cdot v$ mit $u \geq v > 1$. Dann sind u, v beide ungerade, und $x := \frac{u+v}{2}$, $y := \frac{u-v}{2} \in \mathbb{N}_0$ erfüllen

$$x - y = v, \quad x + y = u, \quad x^2 - y^2 = uv = n.$$

□

Darauf beruht der

Fermatsche Faktorisierungstest. *Sei $n > 1$ ungerade, zerlegbar und m die kleinste natürliche Zahl $\geq \sqrt{n}$. Man testet nacheinander für $x = m, m+1, \ldots$, ob $x^2 - n$ eine Quadratzahl ist. Gilt $x^2 - n = y^2$, so folgt*

$$n = (x - y) \cdot (x + y).$$

Der Test liefert nach dem Lemma mit Sicherheit einen Teiler, jedoch kann die Laufzeit sehr lang sein, weil x groß werden kann.

Es gibt zahlreiche Tests, die tiefliegende Methoden der Algebra verwenden, z.B. Kettenbrüche oder Klassengruppen von Zahlkörpern, um eine Faktorisierung zu finden. Damit kann man heutzutage bis zu 130-stellige Zahlen faktorisieren.

Die Idee des Fermatschen Faktorisierungstests wurde ausgebaut zum quadratischen Sieb und zum Zahlkörpersieb. Diese Verfahren sind parallelisierbar. Beim quadratischen Sieb besteht die Idee darin, Lösungen $x, y \in \mathbb{Z}$ von

$$x^2 \equiv y^2 \, mod \, n, \quad x \not\equiv \pm \, y \, mod \, n$$

zu erzeugen, um so durch ggT $(x - y, n)$ ggfs. einen nicht-trivialen Teiler von n zu erhalten.

Den aktuellen Rekord im Faktorisieren nicht-spezieller Zahlen hat te Riele aufgestellt, als er am 12.08.99 die beiden 78-stelligen Primteiler einer 155-stelligen Zahl aus der RSA-Challenge-Liste gefunden hat. Dazu war eine CPU-Zeit von 35,7 Jahren erforderlich. Die Rechnungen benötigten wegen der Parallelisierung allerdings nur 3 1/2 Monate. Am 08.04.99 wurden die beiden 93- und 118-stelligen Primteiler der Zahl $n = 10^{211} - 1$ gefunden. Hier hat man allerdings bei der Anwendung des Zahlkörpersiebs die spezielle Gestalt der Zahl ausgenutzt.

Ein anderes sehr effektives probabilistisches Verfahren zur Faktorisierung natürlicher Zahlen ist die Methode von Lenstra, die *elliptische Kurven* verwendet.

Seien $a, b \in \mathbb{R}$ mit $\Delta = 4a^3 + 27b^2 \neq 0$ und

$$E_{a,b}(\mathbb{R}) := \{(x, y) \in \mathbb{R} \times \mathbb{R} \,;\, y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

Da das Polynom $x^3 + ax + b$ eine oder drei (verschiedene) reelle Nullstellen haben kann, erhält man die Bilder am Ende des Textes.

Auf der Menge $E_{a,b}(\mathbb{R})$ kann man eine Addition einführen, die $E_{a,b}(\mathbb{R})$ zu einer abelschen Gruppe mit neutralem Element ∞ macht. Für Punkte $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E_{a,b}(\mathbb{R})$ hat man

$$-P_1 = (x_1, -y_1)\ ,\ P_1 + P_2 = (x_3, y_3) \quad \text{für} \quad P_2 \neq -P_1,$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{für} \quad P_2 \neq P_1, \quad \text{bzw.} \quad \lambda = \frac{3x_1^2 + a}{2y_1} \quad \text{für} \quad P_2 = P_1,$$
$$x_3 := \lambda^2 - x_1 - x_2, \quad y_3 := -y_1 - \lambda(x_3 - x_1).$$

Geometrisch kann man sich diese Addition auf den Bildern am Ende des Textes veranschaulichen.

Man erhält auch eine Gruppe, wenn man einen Körper K mit char $K \neq 2, 3$ sowie $a, b \in K$ und nur die Lösungen in $K \times K$ sowie ∞ betrachtet. Insbesondere kann man also $K = \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p wählen.

Ist $n \in \mathbb{N}$ keine Primzahl, so hat man mit obiger Verknüpfung eine Pseudoaddition über $\mathbb{Z}/n\mathbb{Z}$ erklärt, solange der Nenner in λ teilerfremd zu n ist. Andernfalls hat man einen echten Teiler von n gefunden.

Faktorisierungsverfahren von Lenstra.

Seien n, k, $w \in \mathbb{N}$ gegeben.

Schritt 1. *Wähle zufällig $(a, x, y) \in (\mathbb{Z} \cap [0, n))^3$.*
Schritt 2. $b := y^2 - x^3 - ax\ ,\ P := (x, y) \in E_{a,b}(\mathbb{Z}/n\mathbb{Z}),\ \Delta := 4a^3 + 27b^2$.
Gilt ggT $(6\Delta, n) = 1$?
nein $\to$ stop oder zurück zu Schritt 1, ja $\to$ Schritt 3.
Schritt 3. *Kann man mit obiger Formel $P + P + \ldots + P$ (k-mal) in $E_{a,b}(\mathbb{Z}/n\mathbb{Z})$ berechnen?*
nein $\to$ stop, ja $\to$ Schritt 4.
Schritt 4. *Wiederhole das Verfahren w-mal.*

Dann kann man zeigen, dass das Verfahren für ein zerlegbares n mit einer bestimmten Wahrscheinlichkeit einen echten Teiler liefert.

Der größte Primteiler, der mit dieser Methode bestimmt wurde, wurde am 12.10.99 gefunden, hat 50 Dezimalstellen und teilt $3^{1.179} + 1 \approx 10^{526}$. Weitere Informationen über die *Elliptic Curve Method* und Hinweise auf verfügbare Software findet man im Internet:

http://www.loria.fr/~zimmerma/records/ecmnet.html

Beispiel. Wir betrachten wieder $n = 187$ und wählen zufällig

$$\begin{aligned} a = 1,\ x = 1,\ y = 1, &\quad \text{also} \quad b = -1, \\ y^2 = x^3 + x - 1, &\quad P = (1,1) \end{aligned}$$

Mit obigem Verfahren folgt

$$\begin{aligned} P + P &= (2,-3) \quad \text{mit} \quad \lambda = 2, \\ P + 2P &= (13,47) \quad \text{mit} \quad \lambda = -4, \\ P + 3P &= (89,98) \quad \text{mit} \quad \lambda = 35. \end{aligned}$$

Bei der Berechnung von $P + 4P$ erhält man $\lambda = \frac{97}{88}$ und somit 11 als Teiler von 187.

In der Praxis existiert das ideale Faktorisierungsverfahren nicht. Üblicherweise nimmt man eine Kombination aus mehreren Verfahren.

Literatur

D. Boneh: Twenty years of attacks on the RSA cryptosystem. Notices AMS **46** (1999), 203-213.

D. Bressoud: Factorization and primality testing. Springer-Verlag, Berlin-Heidelberg-New York 1989.

H. Cohen: A course in computational algebraic number theory. Springer-Verlag, Berlin-Heidelberg-New York 1993.

O. Forster: Algorithmische Zahlentheorie. Vieweg, Braunschweig-Wiesbaden 1996.

N. Koblitz: Algebraic aspects of cryptography. Springer-Verlag, Berlin-Heidelberg-New York, 1998.

H.W. Lenstra: Factoring integers with elliptic curves. Ann. Math. (2) **126** (1987), 649-673.

H. Müller: Primzahltests und elliptische Kurven, $10^{99} + 289$ ist prim. Mitt. Math. Ges. Hamburg **13** (1993), 155-177.

G. Nebe: Faktorisieren ganzer Zahlen. Jahresber. Deutsche Math.-Ver. **102** (2000).

R. Remmert, P. Ullrich: Elementare Zahlentheorie. Birkhäuser Verlag, Basel-Boston, 1989.

P. Ribenboim: The new book of prime number records. Springer-Verlag, New York-Berlin-Heidelberg 1996.

H. Riesel: Prime numbers and computer methods for factorization. 2. Aufl., Prog. Math. **57**, Birkhäuser, Boston-Basel, 1994.

R.L. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM **21** (1978), 120-126.

Aloys Krieg, Lehrstuhl A für Mathematik, RWTH Aachen, D-52056 Aachen
Tel.: 0241-80-4525, FAX: 0241-8888-212
E-Mail: krieg@mathA.rwth-aachen.de
Internet: http://www.mathA.rwth-aachen.de/