# Primzahltest nach Goldwasser und Kilian

Vortrag im Rahmen des Seminars der WE A$\ell$ZAGK im
Sommersemester 2007 an der Universität Bremen

Arne & Gerrit Grenzebach

31. Mai 2007

## Einleitung

Für viele kryptographische Anwendungen benötigt man große Primzahlen – wie beispielsweise für die RSA-Verschlüsselung. Dabei beruht die Sicherheit von RSA auf der Annahme, daß es sehr viel einfacher ist, zwei große Primzahlen zu finden, als eine aus zwei großen Primzahlen zusammengesetzte Zahl zu faktorisieren. Allerdings ist der explizite Nachweis der Primzahl-Eigenschaft sehr viel schwieriger als zu zeigen, daß eine Zahl zusammengesetzt ist. Dafür gibt es nämlich einen einfachen Test, der auf dem Kleinen Satz von Fermat basiert:

**Satz:** *Sei $n$ eine Primzahl, $a \in \mathbb{N}$ mit $\mathrm{ggT}(a,n) = 1$. Dann gilt stets:*

$$a^{n-1} \equiv 1 \bmod n. \tag{*}$$

Findet man also zu einem $n$ ein solches $a$ mit $a^{n-1} \not\equiv 1 \bmod n$, so ist $n$ zusammengesetzt. Der Vorteil dieses Tests ist, daß man keinen Faktor von $n$ kennen muß.

Um zu zeigen, daß eine Zahl $n$ prim ist, gibt es ebenfalls einfache, aber im allgemeinen ungeeignete Verfahren:

- Trivialer Test: Teile $n$ durch jede Primzahl $p \leq \sqrt{n}$. Wenn stets $p \nmid n$, ist $n$ prim. Dieser Test ist allerdings nur für kleine Primzahlen geeignet.
- Probabilistischer Test mit dem Kleinen Satz von Fermat: Wähle zufällig *viele* verschiedene $a$ mit $\mathrm{ggT}(a,n) = 1$. Wenn stets $a^{n-1} \equiv 1 \bmod n$, könnte $n$ vermutlich prim sein.

Der probabilistische Test ist unbefriedigend, da er nur eine Wahrscheinlichkeitsaussage bietet. Trotzdem wollen wir uns mit der Idee dieses Tests – ausgehend vom Kleinen Satz von Fermat, einen Primzahltest zu entwickeln – kurz beschäftigen:

**Definition:** *Eine zusammengesetzte Zahl $n \in \mathbb{N}$ heißt **(Fermat)-Pseudoprimzahl** zur Basis $b \in \mathbb{N}$, falls $\mathrm{ggT}(b,n) = 1$ ist und $b$ (*) erfüllt.*

Die Zahl 15 ist demnach zur Basis 11 pseudoprim, aber nicht zur Basis 2, denn $11^{15-1} \equiv 1 \bmod 15$ und $2^{15-1} \equiv 4 \bmod 15$.

Gäbe es nun eine endliche Menge $M \subset \mathbb{N}$, so daß **jede** zusammengesetzte Zahl $n$ für mindestens ein $a \in M$ nicht pseudoprim ist (also $a^{n-1} \not\equiv 1 \bmod n$), hätte man einen einfachen rechnerischen Primzahlnachweis:

$$\forall\, a \in M\colon a^{n-1} \equiv 1 \bmod n \quad \Rightarrow \quad n \text{ prim.}$$

Doch leider existiert so eine Menge nicht, wie der amerikanische Mathematiker Robert Daniel Carmichael im Jahre 1910 durch die Zahl $561 = 3 \cdot 11 \cdot 17$ zeigte; sie ist die kleinste der nach ihm benannten *Carmichael-Zahlen*:

**Definition:** *Eine **Carmichael-Zahl** ist eine zusammengesetzte Zahl $n \in \mathbb{N}$, für die für jedes $a \in \mathbb{N}$ gilt: $a^n \equiv a \bmod n$.*

In Alford et alii (1994) wird sogar bewiesen, daß es unendlich viele Carmichael-Zahlen gibt.

Bereits 11 Jahre bevor Carmichael das erste Beispiel brachte, formulierte der deutsche Mathematiker Alwin Reinhold Korselt 1899 ein Testkriterium. Möglicherweise wollte Korselt damit zeigen, daß keine derartigen Zahlen existieren.

> **Satz** (Korselt-Kriterium)**:** *$n \in \mathbb{N}$ ist genau dann eine Carmichael-Zahl, wenn $n$ positiv, zusammengesetzt sowie quadratfrei ist und für jeden Primteiler $p$ von $n$ gilt: $p - 1$ teilt $n - 1$.*

*Beweis:* Siehe Crandall & Pomerance, Prime numbers. A computational perspective (1999), S. 122, Kap. 3.4, Theorem 3.3.6. ∎

Die bereits erwähnte Zahl $561 = 3 \cdot 11 \cdot 17$ ist damit tatsächlich eine Carmichael-Zahl, denn $560 = 2^4 \cdot 5 \cdot 7$ ist teilbar durch $3 - 1, 11 - 1, 17 - 1$.

Besser als obige simple Verfahren ist ein Primzahlbeweis, der im Idealfall auch für große Zahlen angewendet werden kann. Davon gibt es ebenfalls verschiedene:

- Für Primzahlen mit ein paar 100 Stellen haben Cohen & Lenstra Tests entwickelt, die Jacobi-Summen benutzen.
- Für Primzahlen mit einigen 1000 Stellen und mehr werden meistens Tests eingesetzt, die elliptische Kurven verwenden.
- Für spezielle Primzahlen existieren besondere Tests, etwa der sehr schnelle Lucas-Lehmer-Test für die *Mersenne*-Primzahlen.

*Bemerkung:* Primzahlen der Form $M_q = 2^q - 1$ heißen *Mersenne-Primzahlen*. Dabei kann $M_q$ nur dann prim sein, wenn $q$ prim ist, denn für zusammengesetztes $q = cd$ hat man:

$$\sum_{j=0}^{c-1} \left(2^d\right)^j = \frac{\left(2^d\right)^c - 1}{2^d - 1} = \frac{2^q - 1}{2^d - 1},$$

weshalb für jeden echten Teiler $d$ von $q$ auch $2^d - 1$ echter Teiler von $2^q - 1$ ist.

Die Mersenne-Primzahl $2^{32.582.657} - 1$ mit 9.808.358-Ziffern ist die zurzeit größte bekannte Primzahl. Sie ist die 44. bekannte Mersenne-Primzahl und wurde am 4. September 2006 von Dr. Curtis Cooper und Dr. Steven Boone im Rahmen des GIMPS-Projektes* unter Verwendung des Lucas-Lehmer-Tests entdeckt.

*GIMPS: The Great Internet Mersenne Prime Search

Wir wollen den Primzahltest nach Goldwasser* und Kilian† vorstellen. Bei diesem Test handelt es sich um eine „Elliptische-Kurven-Version“ des klassischen *Pocklington-Lehmer-Primzahltests*; daher betrachten wir diesen zuerst.

## Pocklington-Lehmer-Primzahltest

**Satz** (Pocklington-Lehmer-Test)**:** *Sei $n \in \mathbb{N}, n > 1$, und sei $n-1 = rs$ mit $r \geq \sqrt{n}$. Wenn es für jeden Primteiler $q$ von $r$ ein $a = a(q) \in \mathbb{N}$ gibt, so daß*

$$a^{n-1} \equiv 1 \bmod n \quad \& \quad \mathrm{ggT}\Big(a^{\frac{n-1}{q}} - 1, n\Big) = 1$$

*gilt, dann ist $n$ prim.*

Beachte: Beim trivialen Test werden alle Prim**zahlen** $\leq \sqrt{n}$ verwendet, hier hingegen nur alle Prim**teiler** einer Zahl $\geq \sqrt{n}$.

*Beweis:* Sei $p$ ein Primteiler von $n$. Dann gilt für $b \equiv a^{\frac{n-1}{r}} \bmod n$:

$$b^r \equiv a^{n-1} \bmod n \equiv 1 \bmod p, \quad \text{da } a^{n-1} \equiv 1 \bmod n \text{ und } p \mid n.$$

Folglich ist die Ordnung von $(b \bmod p)$ in der Gruppe $\mathbb{F}_p^\times$ ein Teiler von $r$. Für jeden Primteiler $q$ von $r$ folgt aber:

$$b^{\frac{r}{q}} \equiv a^{\frac{n-1}{q}} \bmod p \not\equiv 1 \bmod p, \quad \text{da } \mathrm{ggT}\big(a^{\frac{n-1}{q}} - 1, n\big) = 1,$$

weshalb die Ordnung von $(b \bmod p)$ für jedes $q$ nicht $\frac{r}{q}$ teilt. Daher ist nur $\mathrm{ord}\big(b \bmod p\big) = r$ möglich. Weil die Ordnung eines Gruppenelementes stets die Gruppenordnung teilt, hat man: $r \mid \#\mathbb{F}_p^\times = p - 1$. Also genügt **jeder** Primteiler $p$ von $n$ der Ungleichung $p > r \geq \sqrt{n}$, weshalb $n$ prim ist. ∎

**Beispiel:** Für $n = 153533$ gilt: $n - 1 = 4 \cdot 131 \cdot 293$. Dann ist $r := 4 \cdot 131 \geq \sqrt{n}$. Zu den Primfaktoren 2 und 131 von $r$ suchen wir geeignete $a_q \in \mathbb{N}$. Betrachte:

$$\begin{aligned} q = 2: \quad & 2^{n-1} \equiv 1 \bmod n, \quad \mathrm{ggT}(2^{\frac{n-1}{2}} - 1, n) = 1 \quad \Rightarrow \quad a_2 := 2, \\ q = 131: \quad & 2^{n-1} \equiv 1 \bmod n, \quad \mathrm{ggT}(2^{\frac{n-1}{131}} - 1, n) = 1 \quad \Rightarrow \quad a_{131} := 2. \end{aligned}$$

Nach dem Pocklington-Lehmer-Test ist also $n = 153533$ prim.

Strenggenommen müssen wir auch noch zeigen, daß 2 und 131 ebenfalls Primzahlen sind. Für 2 ist das klar; für 131 können wir das Verfahren erneut anwenden:

$$\begin{aligned} 131 - 1 = 2 \cdot 5 \cdot 13 \quad & \Rightarrow \quad r := 13 \geq \sqrt{131}, \\ 2^{130} \equiv 1 \bmod 131, \quad \mathrm{ggT}(2^{\frac{131}{13}} - 1, 131) = 1 \quad & \Rightarrow \quad a_{13} := 2. \end{aligned}$$

Offenbar ist auch 131 eine Primzahl.

*Shafrira Goldwasser (*1958): US-amerikanische Informatikerin am Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts

†Joe Kilian: NEC Research Institute, Princeton, New Jersey

*Bemerkung:* Leider ist obiger Beweis nicht konstruktiv. Um zu zeigen, daß $n$ prim ist, genügt es zwar, die Primteiler $q$ von $r$ mit den zugehörigen $a_q$ anzugeben, allerdings wissen wir weder, wie man die $a_q$ findet, noch, wie man $r$ faktorisiert.

Problematisch wird es, wenn man sehr große $n$ (mehrere tausend Stellen) untersuchen will. Denn dann findet man oft nicht genügend Faktoren von $n-1$, um $r \geq \sqrt{n}$ zu erreichen, so daß man auch nicht alle Primteiler $q$ von $r$ kennt. Glücklicherweise helfen uns elliptische Kurven.

## Goldwasser-Kilian-Primzahltest

**Satz** (Goldwasser-Kilian-Test)**:** *Sei $E$ eine elliptische Kurve modulo $n > 1$. Es gebe verschiedene Primzahlen $\ell_1, \ldots, \ell_k$ und endliche Punkte $P_i \in E(\mathbb{Z}_n)$, so daß:*

$$\text{I: } \ell_i P_i = \infty, \qquad \text{II: } \prod_{i=1}^{k} \ell_i > (\sqrt[4]{n}+1)^2.$$

*Dann ist $n$ eine Primzahl.*

*Bemerkung:* Sei $E$ eine elliptische Kurve, gegeben durch $y^2 = x^3 + Ax + B$. Die Kurve $E$ mod $n = E(\mathbb{Z}_n)$ betrachtet man im projektiven Raum $\mathbb{P}^2(\mathbb{Z}_n)$; es gilt:

- $\mathbb{P}^2(\mathbb{Z}_n)$ ist die Menge der Äquivalenzklassen
  $(x:y:z) = \{(x',y',z') \in \mathcal{P}(\mathbb{Z}_n^3) \mid \exists\, u \in \mathbb{Z}_n^\times : (x',y',z') = (ux,uy,uz)\}$
  mit $\mathcal{P}(\mathbb{Z}_n^3) = \{(x,y,z) \in \mathbb{Z}_n^3 \mid (x,y,z) \text{ primitiv, d. h. } \mathrm{ggT}(n,x,y,z) = 1\}$.
- $E(\mathbb{Z}_n) = \{(x:y:z) \in \mathbb{P}^2(\mathbb{Z}_n) \mid y^2z = x^3 + Axz^2 + Bz^3\}$.
- $(x:y:0)$: unendliche Punkte in $\mathbb{P}^2(\mathbb{Z}_n)$; dabei $(0:1:0) = \infty$ auf $E$.
- $(x,y)$ auf $E$ entspricht $P = (x:y:1)$ auf $E(\mathbb{Z}_n)$. Das ist ein endlicher Punkt auf $E(\mathbb{Z}_n)$, und es ist $P$ mod $k$ endlich für $k|n$.
- $(x:y:z)$ mit $\mathrm{ggT}(z,n) = k > 1$ liefert $(x \bmod k : y \bmod k : 0)$ auf $E(\mathbb{Z}_k)$, also unendlich.

Für den Beweis des Satzes benötigen wir die Hasse-Ungleichung:

**Lemma:** *Sei $E$ eine elliptische Kurve über $\mathbb{F}_q$. Für die Ordnung der Gruppe $E(\mathbb{F}_q)$ gilt dann:*

$$|q+1-\#E(\mathbb{F}_q)| \leq 2\sqrt{q}, \quad \textit{also: } \#E(\mathbb{F}_q) \leq q+1+2\sqrt{q} = (\sqrt{q}+1)^2.$$

*Beweis:* Siehe Washington (2003), S. 91, Kap. 4.1, Theorem 4.2. ∎

*Beweis des Satzes:* Sei $p$ ein Primteiler von $n$. Dann ist $n = p^f n_1$ mit $p \nmid n_1$ und man hat:

$$E(\mathbb{Z}_n) \simeq E(\mathbb{Z}_{p^f}) \oplus E(\mathbb{Z}_{n_1}).$$

Da $P_i$ endlich ist in $E(\mathbb{Z}_n)$, ist also auch $P_i$ mod $p^f$ endlich in $E(\mathbb{Z}_{p^f})$. Eine weitere Reduzierung führt zu endlichem Punkt $P_{i,p} = P_i$ mod $p$ in $E(\mathbb{F}_p)$.

Da $\ell_i P_i = \infty \bmod n$, ist auch $\ell_i P_i = \infty \bmod s$ für jedes $s \mid n$. Insbesondere gilt $\ell_i P_i = \infty$ also in $\mathbb{F}_p$, d. h. ord $P_{i,p} = \ell_i$. Damit folgt:

$$\forall\, i\colon \ell_i \mid \#E(\mathbb{F}_p) \quad \Rightarrow \quad \prod_{i=1}^{k} \ell_i \mid \#E(\mathbb{F}_p)$$

Das liefert:

$$(\sqrt[4]{n}+1)^2 \overset{\text{II}}{<} \prod_{i=1}^{k} \ell_i \leq \#E(\mathbb{F}_p) \leq (\sqrt{p}+1)^2,$$

weshalb stets $p > \sqrt{n}$ gilt. Es können aber nur dann alle Primfaktoren von $n$ größer als $\sqrt{n}$ sein, wenn $n$ selbst eine Primzahl ist. ∎

**Beispiel:** Für $n = 907$ sei $E$ die elliptische Kurve $y^2 = x^3 + 10x - 2 \pmod{n}$. Sei $\ell = 71$; es gilt dann: $\ell > (\sqrt[4]{907}+1)^2 \approx 42{,}1$. Sei $P = (819, 784) \in E(\mathbb{Z}_{907})$. Da $\ell P = 71P = \infty$, folgt mit obigem Satz: 907 ist eine Primzahl.

Für diesen Test müssen wir noch wissen, daß 71 eine Primzahl ist. Dieses läßt sich durch direktes Nachrechnen (trivialer Test) oder durch erneutes Anwenden des Goldwasser-Kilian-Tests nachweisen.

In dem obigen Beispiel bleibt noch eine Frage offen: Wie findet man eine Kurve $E$ und einen Punkt $P$? Man muß dazu mehrere elliptische Kurven $E(\mathbb{Z}_n)$ betrachten, bis man eine findet, deren Ordnung von einer Primzahl $\ell$ geteilt wird, die nicht viel größer als $(\sqrt[4]{n}+1)^2$ ist.* Wie dieses Verfahren praktisch aussieht, zeigt die folgende Tabelle:

| Verfahren allgemein | Beispiel |
|---|---|
| Man betrachtet Kurven $E(\mathbb{Z}_n)$, auf denen man jeweils einen Punkt $Q_E$ kennt. | Auf $E$: $y^2 = x^3 + 10x - 2 \pmod{907}$ liegt der Punkt $(1,3)$. |
| Mit dem Verfahren „Baby Step, Giant Step“ erhält man die jeweilige Ordnung ord $Q_E$. | $\text{ord}(1,3) = 923 = 13 \cdot 71$ |
| Mit etwas Glück hat ein ord $Q_E$ einen Primteiler $\ell > (\sqrt[4]{n}+1)^2$. Es ist dann ord $Q_E = \ell \cdot k$; der Punkt $P = k \cdot Q_E$ hat also Ordnung $\ell$. | Verwende den Punkt $P = 13 \cdot (1,3)$, dieser hat Ordnung 71. |

Gegebenenfalls reicht es nicht, nur einen Punkt auf den Kurven $E$ zu kennen. In dem Fall funktioniert dieses Verfahren analog; es muß im dritten Schritt lediglich $\prod \ell_i > (\sqrt[4]{n}+1)^2$ sein.

Man sieht schon an diesem Beispiel, daß es der schwierigste Teil von diesem Algorithmus ist, eine elliptische Kurve mit geeigneten Punkten $P_i$ zu finden. Eine Möglichkeit dafür ist, zufällige elliptische Kurven $E(\mathbb{Z}_n)$ zu generieren und dann deren Ordnung beispielsweise mit dem Algorithmus von Schoof zu berechnen. Dieses muß man so lange fortführen, bis die Ordnung einer Kurve einen geeigneten Primfaktor besitzt.

*Wäre die Primzahl $\ell \approx n$, so hätte man nichts gewonnen. Denn man müßte immer noch nachweisen, daß $\ell$ prim ist.

Einen anderen effizienteren Weg, der komplexe Multiplikation verwendet, findet man bei Atkin & Morain (1993). Die wesentliche Verbesserung besteht darin, daß hier von vornherein elliptische Kurven mit schon bekannter Ordnung gewählt werden; der Algorithmus von Schoof wird dabei nicht mehr benötigt. Wir wollen aber an dieser Stelle nicht näher darauf eingehen.

## Literatur

ALFORD, W. R.; GRANVILLE, Andrew; POMERANCE, Carl:
„There are infinitely many Carmichael numbers“.
In: *Annals of Mathemmticx* 140 (1994), S. 703 – 722.

ATKIN, A. O. L.; MORAIN, F.:
„Elliptic Curves and Primality Proving“.
In: *Mathematics of Computation* 61 (1993), July, Nr. 203, S. 29 – 68.

CRANDALL, Richard; POMERANCE, Carl:
*Prime numbers. A computational perspective*.
1st.
New York; Berlin; Heidelberg: Springer, 1999.

GOLDWASSER, Shafi; KILIAN, Joe:
„Primality Testing Using Elliptic Curves“.
In: *Journal of the ACM* 46 (1999), July, Nr. 4, S. 450 – 472.

KOBLITZ, Neal:
*Graduate Texts in Mathematics*. Bd. 114: *A course in number theory and cryptography*.
2nd Printing.
New York; Berlin; Heidelberg: Springer, 1987.

LENSTRA, H. W. jr.:
„Elliptic Curves and Number-Theoretic Algorithms“.
In: GLEASON, Andrew M. (Hrsg.): *Proceedings of the International Congress of Mathematicians (ICM), August 3–11, 1986, Berkeley/California* Bd. 1.
Providence, Rhode Island: American Mathematical Society (AMS), 1987, S. 99 – 120.

WASHINGTON, Lawrence C.:
*Discrete Mathematics and Its Applications*. Bd. 24: *Elliptic Curves. Number Theory and Cryptography*.
Boca Raton: Chapman and Hall/CRC, 2003.