Randomisierte Primzahltests

Paul Gamper

Seminar im Wintersemester 2006/07

Probability and Randomization in Computer Science

07.02.2007, Aachen

1 Abstract

Nach einer Einführung, in der ich kurz auf die Geschichte der Primzahlen, die Motivation und die Primzahltests eingehe, werden einige deterministische Primzahltests vorgestellt. Es folgen Sätze, wie der kleine Satz von Fermat, die die mathematische Grundlage für das Miller-Rabin Tests bilden. Anschließend wird das Miller-Rabin Test als Algorithmus vorgestellt und an Beispielen demonstriert.

2 Einführung

2.1 Geschichtliches

Bereits 300 v. Chr. bewies der griechische Mathematiker Euklid in seinem Buch „Elemente“, dass es unendlich viele Primzahlen gibt. Um 200 v. Chr. entdeckte Eratosthenes einen Algorithmus zum berechnen von Primzahlen, dieser wird heute „Sieb des Eratosthenes“ genannt.
Die erste wirklich große Primzahl, 2^{19-1}, wurde schon 1588 von Cataldi entdeckt. Heute, in Zeitalter der Computer findet man immer größere Primzahlen. *Am 4 September 2006 würde die größte bekannte Primzahl mit 9.808.358 Stellen gefunden:* $2^{32582657}$ [1].
Obwohl Primzahlen fundamentale Bausteine der Natürlichen Zahlen sind[1], kannte man fast 2000 Jahre für sie keinen praktischen Nutzen. Heute werden die Primzahlen beispielsweise in der Kryptographie eingesetzt. Für den ersten Primzahlbeweis einer Zahl mit mehr als 10 Millionen Dezimalstellen hat die Electronic Frontier Foundation einen Preis von 100.000 Dollar ausgeschrieben.

[1] In seinem Buch „Elemente“ bewies Euklid eine der wichtigsten Grundlagen der Arithmetik, dass nämlich jede ganze Zahl als das Produkt von Primzahlen geschrieben werden kann.

2.2 Motivation

Wie schon oben erwähnt, werden die Primzahlen in der Kryptographie eingesetzt. Dabei sind die Verfahren mit öffentlichem Schlüssel, wie RSA, ohne Primzahlen unmöglich. Für RSA braucht man sehr große Primzahlen. Es währe unsicher eine Liste dieser Zahlen zu führen, so werden sie jedes mal neu gesucht. Da es ausreichend viele große Primzahlen gibt, ist die Wahrscheinlichkeit, dass zwei Leute zufällig dieselbe Primzahl wählen, praktisch gleich null.

2.3 Primzahltest

Definition 2.1. *Die Primzahltests sind mathematische Verfahren, die für eine gegebene Zahl ermitteln ob es eine Primzahl ist oder nicht.*

Es gibt deterministische und randomisierte Primzahltests. Deterministische Algorithmen liefern zwar ein eindeutiges Ergebnis, brauchen aber in der Regel zu lange. Algorithmen wie RSA(Kryptografie) brauchen 500-stellige Primzahlen, die schnell ausgerechnet werden müssen. Deswegen wird ein randomisierter Primzahltest wie Miller-Rabin Test verwendet. Neben akzeptabler Laufzeit, $O(k * log(N)^3)$, ist der Miller-Rabin Test leicht zu verstehen und zu programmieren.

3 Einige deterministische Primzahltests

3.1 Probedivision:

Eine einfachste Methode eine Zahl n auf Primalität zu prüfen ist es durch alle Zahlen zwischen 2 und $\sqrt{n}$ zu teilen. Wenn es keine Teiler gibt, ist es sicher eine Primzahl. Das Verfahren benötigt aber einen exponentiellen Aufwand [2] und ist für große Zahlen unbrauchbar.

3.2 Sieb des Eratosthenes:

Beim Sieb des Eratosthenes werden alle Primzahlen bis zu einer vorgegebenen Schranke berechnet. Zur Ausführung streiche man in einer zusammenhängenden Liste von natürlichen Zahlen, die bei der 2 beginnt, alle echten Vielfachen der ersten Zahl, also von 2, d.h.: 4, 6, 8, 10,... .

3.3 ASK-Methode

Die AKS-Methode ist ein deterministischer Primzahltest in Polynomialzeit, der im Jahr 2002 von Manindra Agrawal, Neeraj Kayal und Nitin Saxena gefunden und nach ihnen benannt wurde [2]. Eine verbesserte Variante hat eine Laufzeit von nur $O((\log n)^6)$.

[2] Im Binär-System ist die Eingabe-Länge $l = \log 2n$ mit Laufzeit $O(\sqrt{2^l}) = O(2^{l\frac{l}{2}})$

4 Randomisierte Primzahltests

Der kleine fermatsche Satz wurde im 17 Jahrhundert von Pierre de Fermat aufgestellt und dient als Grundlage vieler Primzahltests.

Satz 4.1. *(Der kleine fermatscher Satz) Für alle Primzahlen p gilt:*

$$a^{p-1} \equiv 1 \pmod{p}$$

wobei a eine ganze Zahl ist und kein Vielfaches von p.

Beweis. mithilfe Induktion über a

Behauptung: die Aussage gilt für alle $a \geq 0$ und p ist eine Primzahl
IA: Für a=0; $0^p \equiv 0 \pmod{p}$
IV: $a^p \equiv a$
IS: $a \to a + 1$

$$(a+1)^p = a^p + \binom{p}{1} \cdot a^{p-1} + \ldots + \binom{p}{p-1} \cdot a + 1$$

In der Darstellung:

$$\binom{p}{k} = \frac{p \cdot (p-1) \ldots (p-k+1)}{k!}$$

taucht p nur im Zähler auf, das heißt, dass alle Binomialkoeffizienten für $1 \leq k \leq p$ durch p teilbar sind. Also:

$$\binom{p}{k} \cdot a^n \equiv 0 \pmod{p}$$

daraus folgt:

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

Nach IV:

$$a^p + 1 \equiv a + 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$$

□

4.1 Fermat-Test

Mit Hilfe des kleinen fermatschen Satzes kann man auf eine einfache Weise Zahlen auf primalität testen.

Es gibt aber zusammengesetzte Zahlen, Pseudoprimzahlen genannt, die Fermat-Test überstehen und als Primzahlen erkannt werden. Wenn also ein Fermat-Test die eingegebene Zahl als Prim erkennt, wissen wir nur dass es eine Primzahl sein kann.

Eingabe:	Eine ungerade Zahl p und eine Basis a (mit 1<a<p-1)
Berechne:	$b = a^{p-1} \pmod{p}$
Überprüfe:	Ist b ungleich 1 so ist p sicher zusammengesetzt.
	Ist b=1 so ist p ein Primzahlkandidat

4.2 Pseudoprimzahlen

Pseudoprimzahlen sind zusammengesetzte Zahlen die gewisse Eigenschaften mit Primzahlen gemeinsam haben, selbst aber keine sind. Am Bedeutesten sind die Fermatschen Pseudoprimzahlen.

Definition 4.1. *Eine ungerade, zusammengesetzte, natürliche Zahl n heißt fermatsche Pseudoprimzahl zu Basis a, wenn gilt:*

$$a^{n-1} \equiv 1 \pmod{n}$$

Beispiel: Die Zahl $4 = 2 \cdot 2$ ist fermatsche Pseudoprimzahl zu Basis 5 denn es gilt: $5^{4-1} \equiv 1 \pmod{4}$)

Um die Pseudoprimzahlen zu erkenen wendet man das Fermant-Test mit allen basen zwischen 2 und p an. Es gibt aber fermansche Pseudoprimzahlen die für jede mögliche Basis a den Fermat-Test überstehen. Diese Zahlen heißen Carmichaelzahlen.

4.3 Carmichaelzahlen

Carmichaelzahlen und sind nach dem Mathematiker Robert Daniel Carmichael benannt.

Definition 4.2. *Eine zusammengesetzte, natürliche Zahl n heißt Carmichael-Zahl, wenn für alle natürliche Zahlen b (mit ggT(b,n)=1)* $a^{n-1} \equiv 1 \pmod{n}$ *gilt.*

Beispiel: Die kleinste Carmiaelzahl ist $561 = 3 \cdot 11 \cdot 17$, denn
$2^{561-1} \equiv 1 \pmod{5}61$
$3^{561-1} \equiv 1 \pmod{5}61$
...
$560^{561-1} \equiv 1 \pmod{5}61$

Weitere Carmihaelzahlen sind: 1105, 1729, 2465, 6601 ...

Satz 4.2. *Eine ungerade, zusammengesetzte Zahl* $n \geq 3$ *ist genau dann eine Carmichaelzahl, wenn n quadratfrei ist und für jeden Primteiler p von p die Zahl p-1 ein Teiler von n-1 ist.*

Beweis. Siehe: Carmichael-Zahlen und Miller-Rabin-Test [3] □

Satz 4.3. *Jede Carmichaelzahl besitzt mindestens drei verschiedene Primteiler.*

Beweis. Sei n eine Carmihaelzahl, quadratfrei[3] und nach Definition keine Primzahl. So hat n wenigstens 2 Primteiler. Sei n=pq mit $p, q \in P$, p>q und p-1>q-1>0. Nach Satz 6 gilt auch:

$$p - 1 | a - 1 = (p * q) - 1 = (p - 1)q + q - 1$$

Das würde aber bedeuten, dass p-1 ein Teiler von q-1 ist, was aber im Widerspruch zu p-1>q-1 ist. □

1994 bewiesen Pomerance, Alford und Granville die Existenz unendlich vieler Carmichael-Zahlen.[2]

4.4 Miller-Rabin-Test

1976 entwickelte Gary Miller einen deterministischen Test, der das Problem mit den Carmichael-Zahlen umging.[5] Seine Arbeit fundierte jedoch auf der heute noch unbewiesenen Riemann-Hypothese. *1980 entwickelte Dr. Michael O.Rabin den Miller-Rabin-Test der auf Grundlage von Millers Arbeit basiert aber keine unbewiesenen Hypothesen mehr inhaltet*[5]. Der Miller-Rabin-Test ist ein Monte-Carlo-Algorithmus [4] der eine Verfeinerung des Fermatschen Primzahltestes darstellt.

4.4.1 Nichttriviale Einheitswurzeln

Definition 4.3. *Sei* $1 \leq a < n$. *Wenn* a^2 *mod n =1 dann heißt a Einheitswurzel modulo n.*

Nach der Definition sind die Zahlen 1 und n-1 immer Einheitswurzeln modulo n denn ($(n-1)^2 \equiv (-1)^2 \equiv 1 \mod n$). 1 und n-1 (-1) heißen triviale Einheitswurzeln modulo n.

Satz 4.4. *(Nichtexistenz nichttrivialer Einheitswurzeln) Sei p eine ungerade Primzahl,* $1 \leq a < n$ *und* $a^2 \equiv 1 \pmod{p}$, *dann ist a=1 oder a=-1*

Beweis. Es ist $0 \equiv a^2 - 1 = (a-1)(a+1) \pmod{p}$, dass heißt: p teilt (a-1)(a+1). Da aber p eine Primzahl ist, teilt p (a-1) oder (a+1), so kann entweder a=p-1 oder a=1 sein. □

[3] Alle Primteiler nur bis zur ersten Potenz vorhanden.

[4] Monte-Carlo-Algorithmen sind Randomisierte Algorithmen die mit einer nach oben beschränkten Wahrscheinlichkeit ein falsches Ergebnis liefern dürfen. Durch Wiederholen des Algorithmus mit unabhängigen Zufallsbits kann jedoch die Fehlerwahrscheinlichkeit gesenkt werden.

Beispiel: $p = 5$, $a = 4 = 5 - 1$

$$4^2 = 16 \bmod 5 = 1$$

Wenn also eine nichttriviale Einheitswurzel modulo n existiert, dann ist n sicher zusammengesetzt.

Beispiel: $7^2 \equiv 1 \pmod{48}$. Da 7 keine triviale Einheitswurzel modulo 48 ist ($7 \not\equiv \pm 1 \pmod{48}$), kann 48 keine Primzahl sein.

Wenn a wenige nichttriviale Einheitswurzel hat, ist es leider unnützlich diese zufällig zu suchen. Eine Primzahl n>2 ist ungerade, so ist n-1 gerade und kann als Produkt einer zweier Potenz und einer ungeraden Zahl u geschrieben werden: $n - 1 = u \cdot 2^k$ für $k \geq 1$.

Definition 4.4. *Sei $n \geq 3$ und ungerade mit $n - 1 = u \cdot 2^k$, u ungerade, $k \geq 1$ so heißt eine Zahl a, $1 \leq a < n$ Zeuge für die Zerlegbarkeit von n genau dann wenn $a^u \pmod{n} \neq 1$ und $a^{u \cdot 2^i} \pmod{n} \neq n - 1$ für alle i mit $0 \leq i < k$.*

Satz 4.5. *Wenn es einen Zeugen für die Zerlegbarkeit von n gibt, so ist n sicher zusammengesetzt.*

Beweis. Sei n eine Primzahl und a ein Zeuge für die Zerlegbarkeit von n, so müsste gelten:
$a^n - 1 = a^{2^k \cdot u} = 1 \pmod{n}$ und wegen der Definition eines Zeugen gilt:
$b^n \neq 1 \pmod{n}$ dann gibt es ein maximales Element s mit $0 \leq s < k$ und $b^{2^k \cdot u} \neq 1 \pmod{n}$ da s maximal gild: $b^{2^{s+1} \cdot u} = (b^{2^k \cdot u})^2 \equiv 1 \pmod{n}$
wegen Satz 2 gild: $b^{2^k \cdot u} \equiv \pm 1 \pmod{n} \Rightarrow b^{2^k \cdot u} \equiv -1 \pmod{n}$
was im Wiederspruch zur Definition eines Zeugen ist. □

Beispiel:
$n = 325 = 5^2 \cdot 13$ also ist $n - 1 = 324 = 81 \cdot 2^2$, u=81 und k=2
für a=224 ist 274 eine nichttriviale Einheitswurzel und ist eine Zeuge das 325 zusammengesetzt ist.

Satz 4.6. *(Über die Dichte der Nichtzeugen) Ist n>3 eine ungerade zusammengesetzte Zahl, so gibt es in der Menge {1,2...n-1}, höchstens $\frac{n-1}{4}$ Zahlen, die keine Zeugen für die Zerlegbarkeit von n sind.*

Beweis. Sei $p \geq 3$ eine ungerade zusammengesetzte natürliche Zahl. Wir schätzen die Anzahl der $a \in \{1,2,...,n\text{-}1\}$, die zu p teilerfremd sind (ggT(a,p)=1) und zusätzlich gilt:
a) $a^d \equiv 1 \pmod{p}$ oder
b) $a^{(2^r)d} \equiv 1$ für ein r{0,1,...,s-1}
Wenn es kein solches a gibt, so ist die Aussage des Satzes gezeigt, weil es dann keinen Zeugen gibt.
Angenohmen es gibt einen solchen Nicht-Zeugen. Dann muss auch einer existieren der b) erfüllt. Denn wenn a die Eigenschaft a) erfüllt, so erfüllt -a die

Eigenschaft b).
Sei k der größte Wert von r für den es ein a mit ggT(a,p)=1 und b) gibt. Wir setzen

$$m := 2^k u$$

Die Primfaktorzerlegung von n sei definiert als

$$p = \prod n^{e(n)}$$

mit allen n die p teilen. Die Häufigkeit e mit welcher der Primzeiler p in der Primfaktorzerlegung von n auftauchen muss, wird mit e(p) bezeichnet.

Nun definiert man Untergruppern M,L,K,J von $(\mathbb{Z}/n\mathbb{Z})^*$ mit

$$M \subset L \subset K \subset J \subset (\mathbb{Z}/n\mathbb{Z})^*$$

mit:
$M = \{a + n\mathbb{Z} : ggT(a,p) = 1, a^m \equiv 1 \pmod{p}\}$
$L = \{a + n\mathbb{Z} : ggT(a,p) = 1, a^m \equiv \pm 1 \pmod{p}\}$
$K = \{a + n\mathbb{Z} : ggT(a,p) = 1, a^m \equiv \pm 1 \pmod{n^{e(n)}})\}$ $\forall n$, die p teilen
$J = \{a + n\mathbb{Z} : ggT(a,p) = 1, a^{n-1} \equiv 1 \pmod{p}\}$.

Für jeden Nichtzeugen a mit ggT(a,n)=1 liegt die Restklasse a+n$\mathbb{Z}$ in L. Man kann den Satzt veweisen in dem man zeigt, dass der Index von L in $(\mathbb{Z}/n\mathbb{Z})^*$ mindestens 4 ist, also wenn gilt: $(|(\mathbb{Z}/n\mathbb{Z})^*|/|L|) > 4$, denn dann liegen mindestens viermal soviel Elemente in $(\mathbb{Z}/n\mathbb{Z})^*$ wie in L.
Der Index von M in K ist eine 2er-Potenz, weil das Quadrat jedes Elementes von K in M liegt. Der Index von L in K ist daher auch eine Potenz von 2, etwa 2^c.
- Wenn c>1 ist, dann ist der Satz bewiesen, weil dann 2^c>4 ist.
- Ist c=1, so hat p genau zwei Primteiler und kann nach Satz 3.3 keine Carmichaelzahl sein. Deswegen ist J eine echte Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$, mit $|(\mathbb{Z}/n\mathbb{Z})^*|/|J|=2$. Da $|K|/|L| = 2^w$ gilt, ist $|(\mathbb{Z}/n\mathbb{Z})^*|/|J|=4$.
- Ist c=0, so ist p eine Primpotenz. Hierfür lässt sich nachweisen, dass J genau p-1 Elemente hat, also genau die Elemente der Untergruppe der Ordnung p-1 der Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$. Daher ist der Index von J in $(\mathbb{Z}/n\mathbb{Z})^*$ wenigstens 4, außer für n=9. Aber dies lässt sich direckt überprüfen. Die Abschätzung ist gezeigt. □

4.5 Algorithmus: Miller-Rabin Test

Eingabe: Ungerade, natürliche Zahl $p \geq 3$.
Ausgabe: „Prim“ oder „Zusammengesetzt“

1. wähle a zufälig aus {2,...,p-2}
2. finde u ungerade und $k \geq 1$ so dass $p - 1 = u \cdot 2^k$;

3. Berechne $b = a^u \pmod p$, wenn b=1 oder b=p-1, return „Prim“
4. Berechne $b^{2^i} \pmod p$ für $1 \geq i \geq k$, wenn b=p-1 return „Prim“, wenn b=1 return „Zusammengesetzt“
5. return „Zusammengesetzt“

Beispiel 1:

Eingabe: p=41, a=4.
41-1=5*2^3, also: k=3, u =5
b=$2^5 \pmod{41} = 40$
40=41-1 Ausgabe: „Prim“

Beispiel 2:

Eingabe: p=11*31=341 (Pseudoprimzahl zu basis 2), a=43
341-1=85*2^2, also: k=2, u =85
b=$43^{85} \pmod{341} = 67 \neq 1$ *und* $\neq p-1$
$67^2 \pmod{341} = 56$, $56^4 \pmod{341} = 56$
Ausgabe: „Zusammengesetzt “

Beispiel3:

Eingabe: 1729=7*13*19 (3te Charmichaelzahl), a=3
1729-1=27*2^6, also ist k=6, u=27
b=$3^{27} \pmod{1729}$=664
$664^2 \pmod{1729} = 1$ Ausgabe: „Zusammengesetzt “

Satz 4.7. *Der Miller-Rabin Test hat eine Fehlerwahrscheinlichkeit* $\leq (1/4)$.

Beweis: Der Miller-Rabin Test benutzt den Satz 3.4 in den Schritten 3,4 um die Zeugen für Zerlegbarkeit zu finden und findet nach Satz 3.5 mit einer Wahrscheinlickeit $\leq (1/4)$ keine. □

Um die Fehlerwahrscheinlichkeit zu reduzieren werden mehrere Tests mit zufällig gewählten Basen durchgeführt. Die Wahrscheinlichkeit, dass eine nach k Durchläufen unbelastete Zahl keine Primzahl ist, beträgt $(\frac{1}{4})^k$ ln n. *Miller-Rabin Test ist sehr effizient. Seine Laufzeit ist O((log n)^3), außerdem fällt die Fehlerwahrscheilichkeit in Wirklichkeit noch viel geringer als* $(1/4)^k$ *aus.*[6]

5 Zusammenfassung

Wegen vielen guten Eigenschaften ist Miller-Rabin Test in der Praxis weit verbreitet. *Die Laufzeit ist polynomiel und die Fehlerwahrscheinlichkeit lässt sich bei ausreichender Wiederholung (ca. 30 mal) unter eines Hardware-Fehlers drücken.*[4]

Man kann die Fehler-Wahrscheinlichkeit weiter senken in dem man den Miller-Rabin Test mit der Probedevision kombiniert, in dem mann zuerst die Zahl durch die ersten x Primzahlen teilt.
Man kombiniert Miller-Rabin Test auch mit anderen Verfahren, um z.B., bei der Suche nach sehr großen Primzahlen, zuerst die Kandidaten auszusuchen um dann die deterministische Tests anzuwenden.

Test	Art	Bemerkung
Probedevision	D	Zu langsam
Fermat-Test	R	Wegen Pseudoprimzahlen unzuverläsig, wird aber in Kombination mit anderen Tests genutzt.
Solovay-Strassen-Test	R	Erster probabilistischer Primzahltest(1977) $\epsilon < 1/2$, Laufzeit: O((log n)^3)
Miller-Rabin-Test	R	$\epsilon < 1/2$ und Laufzeit: O((log n)^3), wird neben Kryptographie in Programmen wie Maple oder Mathematica eingesetzt.
Miller-Test	D	Mathematisch nicht bewiesen (Rieman Hypothese)
Lukas-Test	D	Für Zahlen mit bestimmten Formen sehr effizient. Z.B. $2^n - 1$
Pepin - Test	D	Überprüft Fermatsche Zahlen: $2^{2^k} - 1$
Lucas-Lehmer-Test	D	Überprüft Mersenne-Zahlen ($2^p - 1$ wobei p eine Primzahl ist) Die größte bekannte Primzahlen sind Mersenne-Zahlen.
ECPP	P	Elliptic Curve Primality Proving, basierend auf Theorie elliptischer Kurven, Laufzeit O((ln n)^4)
AKS	D	Erster deterministischer Primzahltest in Polynomialzeit (O((log n)^6)

Tabelle 1: Einige Primzahltests, ϵ = Fehlerwahrscheinlichkeit

6 Quellenangabe

1) Martin Dietzfelbinger: Primality Testing in Polynomial Time
2) Wikipedia.de
3) Felix Pape: Carmichael-Zahlen und Miller-Rabin-Test
4) Nicolas Rachinsky: Probabilistische Primzahltests
5) Bernhard Häupler: Miller-Rabin-Primalitätstest
6) www.math.tu-berlin.de/ hess/krypto-ws2006/miller-rabin-einfach.ps

7 Anhang

Zahl	Ziffernanzahl	Jahr	Entdeker
$2^{17}-1$	6	1588	Cataldi
$2^{19}-1$	6	1588	Cataldi
$2^{31}-1$	10	1772	Euler
$2^59-1/179951$	13	1867	Landry
$2^{127}-1$	39	1876	Lucas
$2^{148}+1/17$	44	1951	Ferrier
$2^{521}-1$	157	1952	Robinson(SWAC)
$2^{607}-1$	183	1952	Robinson(SWAC)
$2^{1279}-1$	386	1952	Robinson(SWAC)
$2^{2203}-1$	664	1952	Robinson(SWAC)
$2^{3217}-1$	969	1957	Riesel(BESK)
$2^{4423}-1$	1332	1961	Robinson(IBM7090)
$2^{9689}-1$	2917	1963	Gillies(ILLIAC 2)
$2^{19937}-1$	6002	1971	Tuckerman(IBM360/91)
$2^{44497}-1$	13395	1979	Nelson und Slowinski(Cray 1)
$2^{86243}-1$	25962	1982	Slowinski(Cray 1)
$2^{216091}-1$	65050	1985	Slowinski(Cray X-MP/24)
$2^{756839}-1$	227832	1992	Slowinski und Gage(Cray 2)
$2^{1398269}-1$	420921	1996	Armengaud, Woltman (GIMPS, Pentium 90MHz)
$2^{2976221-1}$	895932	1997	Spence, Woltman (GIMPS, Pentium 100MHz)
$2^{13466917-1}$	4053946	2001	Cameron, Woltman, Kurowski (GIMPS, Athlon 800 Mhz)
$2^{20996011-1}$	6320430	2003	Shafer (GIMPS, Pentium 4 2 GHz)
$2^{30402457-1}$	9152052	2005	Cooper, Boone (GIMPS, Pentium 4 3 GHz)
$2^{32582657-1}$	9808358	2006	Cooper, Boone (GIMPS)

Tabelle 2: Große Primzahlen nache Jahren, verkürzt, [2]