Pratts Primzahlzertifikate

Markus Englert

16.04.2009

Technische Universität München
Fakultät für Informatik
Proseminar: Perlen der Informatik 2
SoSe 2009
Leiter: Prof. Dr. Nipkow

1 Primzahltest

Ein Primzahltest ist ein Algorithmus mit dem die Primalität einer Zahl überprüft werden kann. Primzahltests werden in der Praxis vor allem bei Verschlüsselungsverfahren in der Kryptographie eingesetzt. Verfahren, wie zum Beispiel RSA, benötigen Primzahlen in der Größenordnung von ca. 1000 Stellen. Da es kein effizientes Verfahren zum Ermitteln von Primzahlen gibt, bestimmen Algorithmen nach dem Zufallsprinzip Zahlen und überprüfen dann die Primalität mit Hilfe eines Primzahltests.
Das Thema dieser Arbeit ist die Zertifizierung von Primzahlen, d.h. es ist mit Hilfe von Zusatzinformationen (Zertifikaten) sehr leicht zu überprüfen, ob eine Zahl eine Primzahl ist. Das Konzept von Primzahlzertifikaten wurde 1975 von Vaughan Pratt entwickelt, der ebenfalls bewies, dass damit die Verifikation der Primalität in polynomieller Zeit möglich ist. (vgl. Quelle [7])

2 Lehmers Theorem

Das Primzahlzertifikat von Pratt basiert auf den Lehmer Theorem, das oft auch als Umkehrung des "Kleinen fermatschen Satzes" bezeichnet wird:

Theorem 1: Ein $m \in \mathbb{N}$ ist eine Primzahl, gdw. es ein $a \in \mathbb{N}$ gibt, sodass:

$$a^{m-1} \equiv 1 \ (mod\ m) \tag{1}$$

$$\forall x < m-2 : a^x \not\equiv 1 \ (mod\ m) \tag{2}$$

Beweis: Der Beweis des Lehmer Theorems verwendet das sogenannte Generator-Lemma sowie den „Kleinen Satz von Fermat".

Definition 1: $g \in \mathbb{Z}_p \setminus \{0\}$ heißt Generator von $\mathbb{Z}_P \setminus \{0\}$ gdw. $\mathbb{Z}_p \setminus \{0\} = \{g^0, g^1, ..., g^{p-2}\}$.

Mit Hilfe der Definition des Generators einer Gruppe lässt sich nun das Generator-Lemma aufstellen:

Lemma 1 (Generator Lemma): g ist ein Generator von $\mathbb{Z}_p \setminus \{0\}$ gdw.

$$\forall x \in \{1, ..., p-2\} : g^x \not\equiv 1 \tag{3}$$

$$g^{n-1} \equiv 1 \ (mod\ p) \tag{4}$$

Der Beweis befindet sich auf Seite 256 in Quelle [3].
Beispiel: Der Generator der Gruppe $\mathbb{Z}_5$

$$3^0 = 1 \tag{5}$$

$$3^1 = 3 \tag{6}$$

$$3^2 = 9 \equiv 4 \ (mod\ 5) \tag{7}$$

$$3^3 = 27 \equiv 2 \ (mod\ 5) \tag{8}$$

$$3^4 = 81 \equiv 1 \ (mod\ 5) \tag{9}$$

Somit ist 3 ein Generator von $\mathbb{Z}_5$.
Nach dem Generator-Lemma besitzt eine Gruppe $\mathbb{Z}_p(\mathbb{Z}_p = [0, p-1])$ somit genau dann einen Generator wenn (1),(2) gilt. Mit Hilfe des "Kleinen Satzes von Fermat" lässt sich nun zeigen, dass p genau dann eine Primzahl ist wenn $\mathbb{Z}_p$ einen Generator besitzt.

Theorem 2 (Der kleine Satz von Fermat): Für alle $p \in \mathbb{N}$ mit $p \geq 2$ gilt: p ist eine Primzahl gdw.

$$\forall a \in \mathbb{Z}_P \setminus \{0\} : a^{p-1} \equiv 1 \ (mod\ p) \tag{10}$$

Der Beweis findet sich vielfach in der Literatur (z.B. Quelle [4]). Das Theorem besagt, dass in einer Gruppe $\mathbb{Z}_P$ mit p ist Prime jedes Element $a \in \mathbb{Z}_P$ ein Generator ist. Dies ist ein Spezialfall des Satzes: $\langle \mathbb{Z}_N, +_N, .{}_N \rangle$ ist genau dann ein Körper wenn n eine Primzahl ist.

Aus dem „Kleinen Satz von Fermat“ lässt sich folgendes Lemma ableiten:

Lemma 2: p ist eine Primzahl, gdw. $\mathbb{Z}_P$ einen Generator besitzt.

Der Beweis soll nun im Folgenden geführt werden, er befindet sich auch in Quelle [3].
Beweis:
$\Leftarrow$: Sei g ein Generator von $\mathbb{Z}_P \setminus \{0\}$:

$$\forall a \in \mathbb{Z}_P : \exists k \in \{0, ..., p-2\} : a = g^k \tag{11}$$

$$g^{p-1} \equiv 1 \ (mod\ p) \text{ gilt für jeden Generator (Generator-Lemma)} \tag{12}$$

$$a^{p-1} = (g^k)^{p-1} = (g^{p-1})^k = (1)^k = 1 \tag{13}$$

$$\Rightarrow \forall a \in \mathbb{Z}_P \setminus \{0\} : a^{p-1} \equiv 1 \ (mod\ p) \text{ (Kleiner Satz von Fermat)} \tag{14}$$

$$\Rightarrow p \text{ ist eine Primzahl} \tag{15}$$

$\Rightarrow$: Sei p eine Primzahl, dann ist $< \mathbb{Z}_P, +_P, *_P >$ ein Körper (siehe Satz 5.82 in Quelle [2]).
Da die multiplikative Gruppe des Körpers $< \mathbb{Z}_P, +_P, *_P >$ einen Generator hat (vgl. Satz 5.92 in Quelle [2]), besitzt somit $\mathbb{Z}_P$ ebenfalls einen Generator.

Aus Lemma 1 und Lemma 2 folgt Theorem 2. q.e.d.

Beispiel für die Anwendung von Lehmers Theorem

zu zeigen: 11 ist eine Primzahl

Beweis mit Lehmers Theorem:

Gesucht ist ein a mit $a^{10} \equiv 1 \ (mod\ 11)$ und $\forall x < 9 : a^x \not\equiv 1 \ (mod\ 11)$. Sei $a = 3$:

$$3^{10} \ (mod\ 11) = 1 \tag{16}$$

$$\forall x \in \{1, \ldots, 9\} : 3^x \not\equiv 1 \ (mod\ 11) \tag{17}$$

Somit ist 11 nach Lehmers Theorem eine Primzahl.

3 Erweiterung von Lehmers Theorem

Das Beispiel zeigt, dass ein Primalitätsbeweis mit Hilfe des „Lehmer Theorems“ sehr aufwendig ist. Der Aufwand kann durch das sogenannte „Erweiterte Lehmer Theorem“ stark reduziert werden.

Korrolar 1: Ein $p \in \mathbb{N}_{>2}$ ist eine Primzahl, gdw. es ein $g \in \mathbb{N}$ gibt mit:

$$g^{p-1} \equiv 1 \ (mod\ p) \tag{18}$$

$$g^{\frac{p-1}{q}} \not\equiv 1 \ (mod\ p) \text{ für alle Primfaktoren } q \text{ von } p-1 \tag{19}$$

Beweis des Korrolars: Ein Beweis dieses Korrolars befindet sich in den Notizen von Cheval (vergleiche Quelle [2]).

Sei x die kleinste natürliche Zahl, so dass gilt:

$$g^x \equiv 1 \ (mod\ m) \tag{20}$$

$$c * x + d = m - 1 \tag{21}$$

Es gilt: $0 \leq d < x$, $c = \lfloor \frac{m-1}{x} \rfloor$, $d \equiv (m-1) \ (mod\ x)$.

$$g^{c*x+d} = g^{m-1} \equiv 1 \ (mod\ m) \tag{22}$$

$$g^{c*x} = (g^x)^c \equiv 1 \ (mod\ m) \tag{23}$$

$$\Rightarrow g^d \equiv 1 \ (mod\ m) \tag{24}$$

Da $0 \leq d < x$ und x mininal ist folgt, dass $d = 0$. Somit ist x ein Teiler von $m-1$. Aus der Bedingung des erweiterten Lehmer Theorems (19) folgt nun, dass $x = m - 1$.
Da x so gewählt wurde, dass es die kleinste natürliche Zahl ist, für die $g^x \equiv 1 \ (mod\ m)$, gilt somit: $\forall x < m-2 : a^x \not\equiv 1 \ (mod\ m)$. Zusammen mit (18) sind daher die Bedingungen für Lehmers Theorem erfüllt und m ist eine Primzahl.

Anwendung des Korrolars:
Wir wollen zeigen, dass 1783 eine Primzahl ist.
Beweis:

$$10^{1782} \equiv 1 \ (mod\ 1783) \tag{25}$$

$$\forall x < 1781 : 10^x \not\equiv 1 \ (mod\ 1783) \tag{26}$$

(26) lässt sich nun mit der Erweiterung von Lehmers Theorem leicht zeigen:
Primfaktorzerlegung: $1782 = 2 * 3^4 * 11$
$10^{1782/2} \ (mod\ 1783) = 10^{891} \ (mod\ 1783) = 1782$
$10^{1782/3} \ (mod\ 1783) = 10^{594} \ (mod\ 1783) = 1589$
$10^{1782/11} \ (mod\ 1783) = 10^{162} \ (mod\ 1783) = 367$

Aus Lehmers Theorem folgt die Primalität von 1783.

4 Verfahren nach Pratt

Um die Primalität einer Zahl p nach dem Lehmer Theorem zu beweisen, muss die Primfaktorzerlegung von $p-1$ bestimmt werden. Es ist jedoch kein Verfahren bekannt, welches eine Zahl in polynomieller Zeit in seine Primteiler zerlegt. Pratt löst dieses Problem durch Angabe eines sogenannten Primzahlzertifikates, das auf dem erweiterten Lehmer Theorem basiert. Seine Idee ist ein rekursiver Ansatz: Man errät sowohl g als auch die Primteiler q von $p-1$ und überprüft rekursiv, dass es sich tatsächlich um Primzahlen handelt.

Im Gegensatz zum Fermat-Test oder dem Lucas-Test ist Pratts Primzahlzertifikat ein deterministischer Primzahltest. Ein deterministischer Primzahltest beweist eindeutig die Primalität bzw. die Zusammengesetztheit einer Zahl. Mit Hilfe eines prohabilistischer Primzahltest dagegen kann nur die Zusammengesetztheit einer Zahl eindeutig nachgewiesen werden nicht aber die Primalität. Ein Primzahlzertifikat ist ein Inferenzsystem, mit Hilfe dessen die Primalität einer Zahl eindeutig und korrekt nachgewiesen werden kann. (vgl. Quelle [12], Seite 29)
Pratt benutzt in seiner Arbeit:

Prädikate

- Prime p: p ist eine Primzahl
- (p, g, x): für jeden Primteiler q von x gilt $g^{p-1/q} \not\equiv 1 \ (mod\ p)$

Axiome

- $R1: \ p, g \in \mathbb{N} \vdash (p, g, 1)$

Inferenzregeln

- $R2: \ g^{p-1/q} \not\equiv 1 (mod\ p) \ , \ (p, g, x), \ Prime\ q \vdash (p, g, xq)$
- $R3: \ g^{p-1} = 1 \ (mod\ p), \ (p, g, p-1) \vdash Prime\ p$

Eine Herleitung mit diesen Inferenzregeln nennt Pratt Primzahlzertifikat der Zahl p, wenn in der letzten Zeile der Herleitung Prime p steht.

Erläuterung der Kalkülregeln: Die Regeln erschließen sich aus dem „Erweiterten Lehmer Theorem“.

R2: (p, g, xq) ist äquivalent zu $\forall$ Primteiler q' von $xq : g^{p-1/q'} \not\equiv 1 \ mod\ p$.
Die Menge der Primteiler q' besteht aus den Primteilern von x und der Primzahl q.
Somit gilt: (p, g, xq)
$\Leftrightarrow \forall$ Primteiler q' von $x : g^{p-1/q'} \not\equiv 1 \ (mod\ p) \wedge \ g^{p-1/q} \not\equiv 1 (mod\ p)$.
Daraus folgt die Inferenzregel: $g^{p-1/q} \not\equiv 1 (mod\ p) \ , \ (p, g, x), \ Prime\ q \vdash (p, g, xq)$.

R3: Diese Inferenzregel folgt direkt aus dem „Erweiterten Lehmer Theorem“.

4.1 Beispiel: Beweis der Primalität von 1783

Mit Hilfe von Pratts Inferenzsystem:

Nr.	Herleitung	Regel
1	(2,1,1)	R1 (Axiom)
2	Prime 2	(1), $1^1 \equiv 1 \ (mod\ 2)$, R3
3	(3,2,1)	R1 (Axiom)
4	(3,2,2)	(2), (3), $2^{2/2} \not\equiv 1 \ (mod\ 3)$, R2
5	Prime 3	(4), $2^2 \equiv 1 \ (mod\ 3)$, R3
6	(5,2,1)	R1 (Axiom)
7	(5,2,2)	(2), (6), $2^{4/2} \not\equiv 1 \ (mod\ 5)$
8	(5,2,4)	(7), (2), $2^{4/2} \not\equiv 1 \ (mod\ 5)$
9	Prime 5	(8), $2^4 \equiv 1 \ (mod\ 5)$, R3
10	(11,2,1)	R1 (Axiom)
11	(11,2,2)	(10), (2), $2^{10/2} \not\equiv 1 \ (mod\ 11)$, R2
12	(11,2,10)	(11), (9), $2^{10/5} \not\equiv 1 \ (mod\ 11)$, R2
13	Prime 11	(12), $2^{10} \equiv 1 \ (mod\ 11)$, R3

Nr.	Herleitung	Regel
14	(1783,10,1)	R1(Axiom)
15	(1783,10,2)	(14), (2), $10^{1782/2} \not\equiv 1$ (*mod* 1783), R2
16	(1783,10,6)	(15), (5), $10^{1782/3} \not\equiv 1$ (*mod* 1783), R2
17	(1783,10,18	(16), (5), $10^{1782/3} \not\equiv 1$ (*mod* 1783), R2
18	(1783,10,54)	(17), (5), $10^{1782/3} \not\equiv 1$ (*mod* 1783), R2
19	(1783,10,162)	(18), (5), $10^{1782/3} \not\equiv 1$ (*mod* 1783), R2
20	(1783,10,1782)	(19), (13), $10^{1782/11} \not\equiv 1$ (*mod* 1783), R2
21	Prime 1783	(20), $10^{1782} \equiv 1$ (*mod* 1783), R3

4.2 Erläuterungen zu Pratts Zertifikat

Das Zertifikat $C(n)$ in Pratts Primzahlbeweis besteht somit aus (siehe Quelle [5]):

- Der Angabe einer Faktorisierung von $n-1$:
  $n-1 = p_1^{e_1} * p_2^{e_2} * ... * p_S^{e_S}$
  Bsp.: $C(1783) : 2 * 3^4 * 11$
- Dem Nachweis, dass die Zahlen $p_1, ..., p_S$ Primzahlen sind, indem Zertifikate $C(p_i)$ für alle $p_i > 2$ angegeben werden.
  Bsp.: $C(1783) : C(2)$, $C(3)$, $C(11)$.
- Der Angabe eines Elements $g \in \mathbb{Z}_n$ mit $ord(g) = n-1$.
  Bsp.: $C(1783)$: 10

Ein Zertifikat lässt sich neben der obigen Tabellenschreibweise auch noch wie folgt schreiben: $C(n) = (\text{Prime } n, g, C(p_1), C(p_2), C(p_3), ..., C(p_S))$. Mit Hilfe dieser Schreibweise lässt sich Pratts Zertifikat nun induktiv definieren (vgl. Quelle [12]):

Definition 2: $C(n)$ ist genau dann ein Primzahlzertifikat nach Pratt, wenn:

- $C(n) = (2, x, 1)$ und $x \in \mathbb{N}$
- $C(n) = (Prime\ n, g, C(p_0), C(p_1), C(p_2), ..., C(p_S))$ falls $\forall i < s : g^{n-1/p_i} \not\equiv 1\ (mod\ n)$, $g^{n-1} \equiv 1\ (mod\ n)$, $n-1$ sich als Produkt von Potenzen p_i schreiben lässt und falls C(p_i) ein Zertifikat ist.

Aufstellen des Primzahlzertifikates
Beim Aufstellen des Primzahlzertifikates $C(n)$ nach Pratt werden die Primzahlfaktoren q der Zahl $p-1$ benötigt. Da kein effizienter Faktorisierungsalgorithmus bekannt ist, werden zum Bestimmen der Primfaktoren beliebige Faktoren erraten und dann mittels eines Primzahlzertifikates auf Primalität überprüft. Dieses rekursive Verfahren ist offensichtlich nicht effizient durchführbar. Pratts Absicht war es jedoch auch nicht einen effizienten Primzahltest zu finden, sondern ein Verfahren mit Hilfe dessen die Primalität einer Zahl effizient zu verifizieren ist. Dieses Ziel erreichte er im Jahr 1975 durch die Angabe seiner Primzahlzertifikate (siehe 4.4).

Das Primzahlzertifikat von Pratt stellt einen deterministischen Beweis der Primalität von Zahlen dar. Daher lässt sich mit Hilfe des Zertifikats auch die Nicht-Primalität bzw. Zusammengesetzheit von Zahlen beweisen. Dies soll nun im Folgenden anhand zweier Beispiele demonstriert werden. (Die Beweise werden dabei in umgekehrter Reihenfolge geführt, d.h. es wird mit der Behauptung begonnen.)

- Zertifikat für die Zahl 6

Nr.	Herleitung	Regel
1	Prime 6	R3: (2), $g^5 = 1$ $(mod\ 6)$

  Für die Zahl 6 ist kein Beweis möglich, da $\forall x \not\equiv 1\ (mod\ 6):\ x^5 \not\equiv 1\ (mod\ 6)$. Somit ist R3 nicht erfüllt.

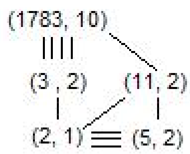
- Zertifikat für die Zahl 99

Nr.	Herleitung	Regel
1	Prime 99	R3: (2), $10^{98} = 1$ $(mod\ 99)$
2	(99,10,98)	R2: Prime 7, (99,10,14), $10^{98/7} \equiv 1$ $(mod\ 99)$

  Somit sind die Vorraussetzungen für R2 nicht erfüllt und das Zertifikat kann nicht aufgestellt werden.

Veranschaulichung der Zertifikate:

1) Mit Hilfe eines Graphen



Die Zeichnung kann als mathematischer Graph interpretiert werden. Die Einträge stellen die Knoten des Baumes dar. Knoten von denen keine Kanten ausgehen, werden als Blätter bezeichnet und die Behauptung, in diesem Fall $(1783, 10)$ als Wurzel. Die Kanten verdeutlichen die Abhängigkeit der Zertifikate voneinander. So benutzt beispielsweise das Zertifikat $(1783, 10)$ an vier Stellen das Zertifikat $(3, 2)$ und einmal das Zertifikat $(11, 2)$.

2) Mit Hilfe eines Kalkülbaums

Die Herleitungen für *Prime* 2 sowie *Prime* 3 wurden hier aus Übersichtlichkeitsgründen weggelassen.

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{(1783,10,1)}\quad\overline{Prime\ 2}}{(1783,10,2)}\quad\overline{Prime\ 3}}{(1783,10,6)}\quad\overline{Prime\ 3}}{(1783,10,18)}\quad\overline{Prime\ 3}}{(1783,10,54)}\quad\overline{Prime\ 3}}{(1783,10,162)}\qquad\dfrac{\dfrac{\dfrac{\overline{(11,2,1)}\quad\overline{Prime\ 2}}{(11,2,2)}\quad\dfrac{\dfrac{\dfrac{\overline{(5,2,1)}\quad\overline{Prime\ 2}}{(5,2,2)}\quad\overline{Prime\ 2}}{(5,2,4)}}{Prime\ 5}}{(11,2,10)}}{Prime\ 11}}{(1783,10,1782)}}{Prime\ 1783}$$

4.3 Korrektheit und Vollständigkeit des Zertifikats

Theorem 3: p ist eine Primzahl, genau dann wenn p ein Zertifikat hat.

Beweis:

$\Leftarrow$: Wurde „Prime p“ hergeleitet, so wurde die Inferenzregel R3 auf das Prädikat $(p, x, p-1)$ angewandt. Somit gilt ebenfalls die Vorraussetzung für R3: $x^{p-1} \equiv 1\ (mod\ p)$.
$(p, x, p-1)$ kann nur durch mehrfache Anwendung der Inferenzregel R2 hergeleitet worden

sein. Dabei muss diese Regel für jeden Primfaktor q von $p-1$ angewandt worden sein. Daraus folgt, dass bei der Herleitung von „Prime p“ ebenfalls $x^{(p-1)/q} \not\equiv 1 \ (mod\ p)$ für alle Primfaktoren q von $p-1$ gezeigt wurde.
Zur Herleitung von „Prime p“ wurden somit

$$x^{p-1} \equiv 1 \ (mod\ p) \tag{27}$$

und

$$x^{(p-1)/q} \not\equiv 1 \ (mod\ p) \text{ für alle Primfaktoren } q \text{ von } p-1 \tag{28}$$

gezeigt.
Aus dem erweiterten Lehmer Theorem folgt daraus, dass p eine Primzahl ist. Somit ist p eine Primzahl, wenn p ein Zertifikat hat. q.e.d.

⇒: **Beweis durch Induktion über p:**

Induktionsanfang

Es gilt $(p, g, 1)$ - Axiom von Pratts Inferenzsystem. Aus Lehmers Theorem folgt, dass wenn p eine Primzahl ist, dann hat p eine primitive Wurzel. Somit hat $\mathbb{Z}_P$ einen Generator g (siehe Definition 1) und es gilt $g^{p-1} \equiv 1 \ (mod\ p)$. Nach R3 lässt sich daher Prime p ableiten. Sei $p = 2$. Aus (2,1,1) und $1^1 \equiv 1 \ (mod\ 2)$ lässt sich nach R3 Prime 2 ableiten.

Induktionsschritt:

Annahme: Jeder Primfaktor q von $p-1$ ist als Theorem ableitbar, d.h $\vdash$ Prime q.
Für jeden Primfaktoren q gilt $g^{p-1/q} \not\equiv 1 \ (mod\ p)$, weil $p - 1/q \in \{1, ..., p-2\}$ und g ein Generator von $\mathbb{Z}_P$ ist. Eine Deduktion von (p, g, x) wo x ein Produkt von Primfaktoren der Zahl $p-1$ ist, ist daher mit Inferenzregel R2 möglich. Es folgt $(p, g, p-1)$ kann abgeleitet werden. Da nach dem Generator-Lemma ebenfalls $g^{p-1} \equiv 1 \ (mod\ p)$ gilt, kann mit R3 „Prime p“ abgeleitet werden. q.e.d.

4.4 Effizienz

Pratt gelang es im Jahr 1975 erstmals mit Hilfe seines Primzahlzertifikates zu beweisen, dass sich die Primalität einer Zahl effizient verifizieren lässt. Das bedeutet: Wie kann man sich effizient davon überzeugen, dass eine gegebene Zahl eine Primzahl ist?
Beispielsweise lässt sich die Nicht-Primalität bzw. Zusammengesetztheit einer Zahl durch Angabe ihrer Primteiler sehr schnell verifizieren. Es wird dabei nicht verlangt, dass sich diese Teiler in polynomieller Zeit finden lassen.
Pratt gelingt es zu zeigen, dass ein bereits vorhandenes Primzahlzertifikat sich in polynomieller Zeit, also effizient, verifizieren lässt. Der Aufwand für das Finden des Zertifikats wird dabei wiederum nicht beachtet. Er kann wie in 4.2 angesprochen sehr groß sein, da kein effizientes Verfahren für das Finden der Zahl g und der Primfaktorzerlegung bekannt ist.
Pratt zeigt in seiner Arbeit, dass falls Prime p gilt, es immer eine Herleitung mit $6 * lg(p) - 4$ Zeilen gibt.

Beweis durch Induktion:

Behauptung: Der Beweis der Primalität von m benötigt höchstens $6 * lg(m) - 4$ Zeilen.

I. Induktionsanfang:
$m = 2$: $6 * lg(2) - 4 = 2$: Aus dem Beispiel in 4.1 ist abzulesen, dass der Beweis der Primalität von 2 zwei Zeilen beträgt. Somit ist die Behauptung für $m = 2$ erfüllt.
$m = 3$: Aus dem obigen Beispiel geht ebenfalls hervor, dass der Beweis für Prime 3 fünf Zeilen lang ist. Somit ist zu zeigen:

$$6 * lg(3) - 4 \geq 5 \Leftrightarrow 6 * log(3) \geq 9 \tag{29}$$

$$\Leftrightarrow 3^6 \geq 2^9 \Leftrightarrow 729 \geq 512 \tag{30}$$

II. Induktionsschritt
Sei m eine beliebige Primzahl. So gilt: $m - 1 = p_1 * p_2 * ... * p_k$, $k \geq 2$ und p_i ist eine Primzahl.
Ein Beweis der Primalität von m setzt sich aus den Beweisen der Primalität von p_i und den Zeilen $(m, a, 1)$, (m, a, p_1), (m, a, p_1p_2), ... ,$(m, a, p_1p_2...p_k)$, Prime m zusammen.
Aus der Induktionsannahme folgt, dass der Beweis aus höchstens

$$\sum_{i=1}^{k}(6 * lg(p_i) - 4) + k + 2 \tag{31}$$

Zeilen besteht.

$$\sum_{i=1}^{k}(6 * lg(p_i) - 4) + k + 2 \tag{32}$$

$$= 6 * lg(m - 1) - 3k + 2 \leq 6 * lg(m - 1) - 4 \tag{33}$$

.

Damit ist garantiert, dass das Überprüfen eines Primzahlzertifikats in polynomieller Zeit effizient möglich ist. Somit gelang es Pratt 1975 erstmals zu zeigen:

$$\text{PRIMES} \in \text{NP}$$

4.5 Algorithmus zum Überprüfen der Korrektheit eines Zertifikats

Mit Hilfer der Darstellung des Beweises als Graph lässt sich die Korrektheit des Zertifikats einfach überprüfen. Diese Methode nennt Vaughan Pratt in seiner Arbeit VELP - Methode (vertices, edges, leaves, products). Ein Zertifikat der Zahl p ist genau dann korrekt, wenn:

- Für jede Wurzel (p, x) gilt, $x^{p-1} \equiv 1 \ (mod\ p)$
- Für jeden Knoten (p, x) bis (q, x) gilt,
  $x^{(p-1)/q} \not\equiv 1 (mod\ p)$ und $q|p - 1$
- Jedes Blatt ist $(2, 1)$.
- für jede Wurzel (p, x) mit den unmittelbaren Nachfolgern $(p_1, x_1), ..., (p_k, x_k)$ gilt:
  $p = p_1 * p_2 * ...p_k + 1$.

5 Schluss

Vaughan Pratt konnte mit Hilfe seiner Primzahlzertifikate zeigen, dass sich die Primheit einer Zahl effizient, d.h. in polynomieller Zeit verifizieren lässt.

$$\text{PRIMES} \in \text{NP}$$

Im August 2002 schafften es Agrawal, Kayal und Saxena sogar zu zeigen, dass Primheit sich effizient entscheiden lässt, d.h.

$$\text{PRIMES} \in \text{P}.$$

Es gelang ihnen einen 20-zeiligen Algorithmus anzugeben, der als Eingabe eine beliebige Zahl n erhält und in polynomieller Zeit ausgibt, ob diese Zahl eine zusammengesetzte Zahl oder eine Primzahl ist.

6 Literaturverzeichnis

1. PRATT, V.R. (1975): Every prime has a succinct sertificate. In: SIAM J. Computing 4, 214-220
2. CHVATAL, Vasek: Pratts primality proofs. Rutgers State University of New Jersey. http://users.encs.concordia.ca/ chvatal/notes/ppp.pdf (Stand 05.03.2009)
3. STEGER, A. (2001): Diskrete Strukturen - Band 1. Springer Verlag
4. BRÜNNER, Arndt: Der kleine Satz von Fermat www.arndt-bruenner.de/mathe/Allgemein/fermatklein.htm (Stand 05.03.2009)
5. VIERGUTZ, Christian: Primheitszertikate, Pocklington-Lemma und der Test von Proth www-math.uni-paderborn.de/ aggathen/vorl/2003ss/sem/Christian-Viergutz-Folien.pdf (Stand 02.03.2009)
6. http://de.wikipedia.org/wiki/Primzahlen (Stand 02.03.2009)
7. http://de.wikipedia.org/wiki/Primzahltest (Stand 02.03.2009)
8. http://en.wikipedia.org/wiki/Primality-certificate (Stand 02.03.2009)
9. http://en.wikipedia.org/wiki/Vaughan-Pratt (Stand 02.03.2009)
10. STREHL, V.: Die Primheit von Zahlen kann man effizient verifizieren http://www8.informatik.uni-erlangen.de/IMMD8/Lectures/THINF3/Folien0405/primesinnp4.pdf (Stand 02.03.2009)
11. LOEBENBERGER, Daniel: Primtest http://www.loebenberger.de/tutorials/primetests/primetests.htm (Stand 10.03.2009)
12. TUENGERTHAL, Max: Algorithmische Zahlentheorie und Kryptographie http://www.kuertz.name/files/Zahlentheorie.pdf (Stand 10.03.2009)