

Pratts Primzahlzertifikat*

Alexander Fischer

14.04.2005

Diese Ausarbeitung basiert auf dem Artikel von Vaughan Pratt [1].

Die mathematischen Grundlagen basieren auf der Vorlesung „*Höhere Mathematik I*“ WS 2004/2005 Prof. G. Kemper und dem Script „*Pratt's primality proofs*“ von Prof. Vasek Chvatal, Rutgers State University of New Jersey.

1 Grundlage

Theorem 1.1 *Ein $m \in \mathbb{N}_{>2}$ ist eine Primzahl, genau dann wenn es ein $a \in \mathbb{N}$ gibt, mit:*

- (1) $a^{m-1} \equiv 1 \pmod{m}$
- (2) $a^x \not\equiv 1 \pmod{m}$ für alle $x = 1, 2, \dots, m-2$

Dieses a wird auch **primitive Wurzel** von m genannt. (Eine primitive Wurzel ist eine Zahl, die in $\mathbb{Z}/(m)$ die multiplikative Ordnung $\varphi(m)$ hat.)

Um nun zu zeigen, dass eine Zahl eine Primzahl ist, muss man nicht alle $m-2$ Werte von $a^x \pmod{m}$ berechnen. Es genügt $a^{(m-1)/p} \not\equiv 1 \pmod{m}$ für alle Primfaktoren p von $m-1$ zu zeigen, denn es gilt:

Theorem 1.2 *Sei R ein Ring, $a \in R$ beliebig. Dann gilt:*

$$\forall i \in \mathbb{N}: a^i = e \iff \text{ord}(a) \mid i$$

Beweis:

- \Leftarrow : Sei $i \in \mathbb{N}$ mit $\text{ord}(a) = n$ und $n \mid i$
 $\Rightarrow i = k * n$ mit $k \in \mathbb{N} \Rightarrow a^i = (a^n)^k = e^k = e$
- \Rightarrow : Sei $i \in \mathbb{N}$ mit $a^i = e$.
Division mit Rest: $i = n * q + r$, $q, r \in \mathbb{N}$, $r < n$
 $\Rightarrow e = a^i = a^{n*q} * a^r \Rightarrow r = 0 \Rightarrow i = n * q \Rightarrow n \mid i$

Hätte nun a eine Ordnung $< m-1$, so wäre $m-1$ ein Vielfaches von $\text{ord}(a)$. Somit wäre auch $(m-1)/p$ für einen Primfaktor p von $m-1$ ein Vielfaches von $\text{ord}(a)$ und es würde gelten: $a^{(m-1)/p} \equiv 1 \pmod{m}$.

*Vortrag gehalten im Rahmen der Vorlesung *Perlen der Informatik 2*, TU München, SS 2005.

Korollar 1.3 Ein $m \in \mathbb{N}_{>2}$ ist eine Primzahl, genau dann wenn es ein $a \in \mathbb{N}$ gibt, mit:

- (1) $a^{m-1} \equiv 1 \pmod{m}$
- (2) $a^{(m-1)/q} \not\equiv 1 \pmod{m}$ für alle Primfaktoren q von $m-1$

Beispiel: Primzahl 1459

$$m-1 = 1458 = 3^6 * 2$$

- (1) $3^{1458} \equiv 1 \pmod{1459}$
- (2) $3^{1458/2} = 3^{729} \equiv 1458 \pmod{1459}$
- $3^{1458/3} = 3^{486} \equiv 339 \pmod{1459}$

2 Das Beweissystem

In dem Beweissystem werden folgende Prädikate verwendet:

- $prime(p)$ kurz: p p ist eine Primzahl
- $aux(p, x, a)$ kurz: (p, x, a) Jeder Primfaktor q von a genügt: $x^{(p-1)/q} \not\equiv 1 \pmod{p}$

Auf diese Prädikate werden folgende Herleitungsregeln angewendet:

- $R_1: (p, x, a), q \vdash (p, x, q * a)$,wenn $x^{(p-1)/q} \not\equiv 1 \pmod{p}$
- $R_2: (p, x, p-1) \vdash p$,wenn $x^{p-1} \equiv 1 \pmod{p}$

Jedes Zertifikat beginnt mit dem Axiom $(p, x, 1)$ (welches immer gilt) und endet mit p

Beispiel:

- (1) $(2, 1, 1)$ Axiom
- (2) 2 $(1), R_2, 1^1 \equiv 1 \pmod{2}$
- (3) $(3, 2, 1)$ Axiom
- (4) $(3, 2, 2)$ $(3), (2), R_1, 2^{2/2} \equiv 2 \pmod{3}$
- (5) 3 $(4), R_2, 2^2 = 4 \equiv 1 \pmod{3}$
- (6) $(5, 2, 1)$ Axiom
- (7) $(5, 2, 2)$ $(6), (2), R_1, 2^{4/2} \equiv 4 \pmod{5}$
- (8) $(5, 2, 4)$ $(7), (2), R_1$
- (9) 5 $(8), R_2, 2^4 \equiv 1 \pmod{5}$
- (10) $(7, 3, 1)$ Axiom
- (11) $(7, 3, 2)$ $(10), (2), R_1, 3^{6/2} \equiv 6 \pmod{7}$
- (12) $(7, 3, 6)$ $(11), (5), R_1, 3^{6/3} \equiv 2 \pmod{7}$
- (13) 7 $(12), R_2, 3^6 \equiv 1 \pmod{7}$
- (14) $(211, 2, 1)$ Axiom
- (15) $(211, 2, 2)$ $(14), (2), R_1, 2^{210/2} \equiv 210 \pmod{211}$
- (16) $(211, 2, 6)$ $(15), (5), R_1, 2^{210/3} \equiv 196 \pmod{211}$
- (17) $(211, 2, 42)$ $(16), (13), R_1, 2^{210/7} \equiv 171 \pmod{211}$
- (18) $(211, 2, 210)$ $(17), (9), R_1, 2^{210/5} \equiv 107 \pmod{211}$
- (19) 211 $(18), R_2, 2^{210} \equiv 1 \pmod{211}$

3 Korrektheit und Vollständigkeit

Theorem 3.1 *p ist eine Primzahl, genau dann wenn p ein Theorem ist.*

Beweis:

\Leftarrow : Wenn „ p “ hergeleitet wurde, so wurde Herleitungsregel R_2 auf das Prädikat $(p, x, p-1)$ angewendet. Somit gilt $x^{p-1} \equiv 1 \pmod{p}$. Um $(p, x, p-1)$ herzuleiten, musste man $x^{(p-1)/q} \not\equiv 1 \pmod{p}$ für alle Primfaktoren q von $(p-1)$ zeigen, da dies die Bedingung für Herleitungsregel R_1 ist. Somit gilt nach Korollar 1.3: p ist eine Primzahl.

\Rightarrow : Induktion über p :

Wenn p eine Primzahl ist, so hat p eine primitive Wurzel x .

Nach der Induktionshypothese gilt: Jeder Primfaktor q von $p-1$ ist ein Theorem. Außerdem gilt $x^{(p-1)/q} \not\equiv 1 \pmod{p}$, für alle q , denn sonst hätte x nicht die multiplikative Ordnung $p-1 \pmod{p}$.

Das Beweissystem lässt jedes Theorem (p, x, a) herleiten, bei dem a ein Produkt von Primfaktoren von $p-1$ ist. Insbesondere also auch $(p, x, p-1)$.

Da nun $x^{p-1} \equiv 1 \pmod{p}$ gilt (Kleiner Satz von Fermat) lässt sich auch p herleiten.

4 Komplexität

4.1 Die Länge des Zertifikats

Theorem 4.1 *Wenn p ein Theorem ist, so hat p einen Beweis von höchstens $\lfloor 4 \log_2 p \rfloor$ Zeilen.*

Beweis: per Induktion:

Induktionshypothese: Jede Primzahl $< p$ kann, den Beweis von 2 und 3 nicht mitgezählt, in höchstens $\lfloor 4 \log_2 p - 4 \rfloor$ Zeilen bewiesen werden.

Für $p = 2$ und $p = 3$ ist dies offensichtlich, denn $\lfloor 4 \log_2 2 \rfloor - 4 \geq 0$ und $\lfloor 4 \log_2 3 \rfloor - 4 \geq 0$. Die Zahlen 2 und 3 müssen gesondert betrachtet werden, da dies die einzigen Primzahlen sind, bei denen $p-1$ unteilbar ist.

Für Primzahlen > 3 : Sei $p-1 = p_1 * p_2 * \dots * p_k$, $k \geq 2$. Dann ist die Länge des Zertifikats nach oben beschränkt durch:

2	für den Start $(p, x, 1)$ und das Ende p des Zertifikats.
k	für das Aufmultiplizieren der Primfaktoren p_i von $p-1$
$\lfloor 4 \log_2 p_i \rfloor - 4$	für den Beweis der einzelnen Primfaktoren p_i nach der Induktionshypothese.

Daraus ergibt sich für das gesamte Zertifikat:

$$\begin{aligned} & 2 + k + \sum_{i=1}^k \lfloor 4 \log_2 p_i \rfloor - 4 \\ & \leq \lfloor 4 \log_2 p_1 p_2 \dots p_k \rfloor - 4, \text{ da } k \geq 2 \\ & \leq \lfloor 4 \log_2 p \rfloor - 4 \end{aligned}$$

Zählt man nun die 5 Zeilen für den Beweis von 2 und 3 dazu, so ergibt sich eine maximale Länge von $\lfloor 4 \log_2 p \rfloor + 1$.

Da $\log_2 p$ für $p > 2$ keine ganze Zahl ist, ist die Länge nach oben durch $\lfloor 4 \log_2 p \rfloor$ beschränkt.

4.2 Der Aufwand des Testens

Das Überprüfen jeder Zeile des Zertifikats erfordert nur eine Potenzierung. Da man jedoch mit sehr großen Werten arbeitet, kann dies zu einem erheblichen Aufwand und Speicherbedarf führen. Daher bedient man sich zweier Verfahren, um diesen Aufwand zu senken:

(1) Potenzieren durch iteriertes quadrieren.

Für die Potenzierung x^b benötigt man mit der herkömmliche Methode $b - 1$ Multiplikationen. Durch den folgenden Algorithmus jedoch kann die Anzahl der nötigen Multiplikationen auf $2 \lfloor \log_2 b \rfloor$ reduziert werden. Eine rekursive Definition des Algorithmus lautet wie folgt:

$$x^b: \quad \begin{aligned} b = 0 &\rightarrow 1, \\ b \text{ ungerade} &\rightarrow x * x^{b-1}, \\ b \text{ gerade} &\rightarrow (x^2)^{b/2}. \end{aligned}$$

Beispiel: 2^{17}

k	2	4	8	16	17
2^k	4	16	256	65536	131072

(2) Multiplizieren modulo p

Um den Speicherbedarf zu reduzieren, werden alle Multiplikationen des oben genannten Algorithmus modulo p durchgeführt.

Um nun das gesamt Zertifikat zu testen, werden höchstens $\lfloor 3 \log_2 p \rfloor$ Potenzierungen benötigt. Dies entspricht also, mit dem oben genannten Algorithmus $6 \log_2^2 p$ Multiplikationen. Zusätzlich werden noch $\lfloor 4 \log_2 p \rfloor$ Multiplikationen für die Anwendung von Ableitungsregel R_1 benötigt.

Fazit dieser Überlegungen ist, dass das vorgestellte Zertifikat nur polynomiale Größe hat und ebenso in polynomialer Zeit getestet werden kann. Somit ist bewiesen, dass:

$$PRIMES \in NP$$

Literatur

- [1] V. R. Pratt. Every prime has a succinct certificate. *SIAM Journal of Computing*, 4:214–220, 1975.