Primzahlzertifikat von Pratt

Daniela Steidl
TU München *

17. 04. 2008

Primzahltests in der Informatik

"Dass das Problem, die Primzahlen von den Zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen, zu den wichtigsten und nützlichsten der ganzen Arithmetik gehört und den Fleiß und die Weisheit der Geometer der Antike und der Neuzeit beschäftigt hat, ist so bekannt, dass es überflüssig ist, darüber viel zu sagen."(Carl Friedrich Gauss, 1801) In der Informatik wird die Problemstellung, festzustellen, ob eine Zahl prim ist, als PRIMES bezeichnet. Lange Zeit erhoffte man sich in der Komplexitätstheorie dadurch neue Erkenntnisse in Bezug auf das P-NP-Problem. Bereits 1975 zeigte Pratt: PRIMES $\in$ NP. Offensichtlich liegt PRIMES auch in CoNP und mit der Annahme, dass PRIMES nicht in P liegt, wäre man der Vermutung, dass P echt kleiner als NP sei, einen großen Schritt näher gekommen. 2002 fanden Agrawal, Kayal und Saxena mit dem AKS-Primzahltest jedoch einen polynomiellen Primzahltest und bewiesen damit: PRIMES $\in$ P. Bis heute wurde kein Beispiel gefunden, dass tatsächlich in NP $\cap$ CoNP, aber nicht in P liegt. Dennoch spielen Primzahlen in heutiger Zeit eine bedeutende Rolle. Als Beispiel seien hier nur Kryptosysteme wie RSA genannt, die Primzahlen in einer Größenordnung von 1000 Stellen benötigen und auf der (unbewiesenen) Annahme beruhen, dass das Faktorisieren von großen zusammengesetzten Zahlen ein algorithmisch schwieriges Problem ist. In dieser

*Proseminar im Rahmen der Vorlesung "Perlen der Informatik" von Prof. Nipkow, SS 2008

Ausarbeitung wird nun das Verfahren von Vaughan R. Pratt vorgestellt, mit dem es gelingt, in polynomieller Zeit zu verifizieren, dass eine Zahl prim ist.

Der kleine Satz von Fermat

Um das Primzahlzertifikat von Pratt zu verstehen, wird an dieser Stelle zunächst die Bedeutung des kleinen Satzes von Fermat erläutert. Der Beweis für das Theorem von Fermat benötigt dabei einige algebraische Sätze, diese werden jedoch aus der Vorlesung Diskrete Strukturen (siehe [4]) als bekannt vorausgesetzt und daher ohne Beweis aufgeführt.

Lemma 1. *$\langle \mathbb{Z}_n, +_n, \cdot_n \rangle$ ist ein Körper, genau dann wenn n prim ist.*

Für alle Primzahlen n ist $\mathbb{Z}_n \setminus \{0\}$ bezüglich der Multiplikation also eine Gruppe.

Lemma 2. *Sei G eine Gruppe mit neutralem Element e und $x \in G$ ein Element mit endlicher Ordnung $ord(x)$. Dann gilt: $x^k = e \Leftrightarrow ord(x) \mid k$.*

Korollar 1 (Lagrange)**.** *Ist G eine endliche Gruppe, so teilt die Ordnung eines jeden Elements die Kardinalität der Gruppe.*

Mit Hilfe dieser Sätze kann also der kleine Satz von Fermat bewiesen werden:

Theorem 1 (Kleiner Fermat)**.** *Für alle $n \in \mathbb{N}$ mit $n \geqslant 2$ gilt:*
n Primzahl $\Leftrightarrow x^{n-1} \equiv 1 \pmod{n}$ $\forall x \in \mathbb{Z}_n \setminus \{0\}$

Beweis
$\Leftarrow$
Man betrachte einen beliebigen Teiler g von n. Nach Annahme der rechten Seite gilt $g^{n-1} \equiv 1 \pmod{n}$. Anders geschrieben: Es gibt $k, k' \in \mathbb{N}$, sodass gilt: $g^{n-1} - 1 = k \cdot n = k \cdot k' \cdot g$. Letzteres folgt, weil g ein Teiler von n ist. Vergleicht man nun die linke und rechte Seite, so erkennt man, dass diese Gleichungskette nur für $g = 1$ gelten kann. Wenn n aber keinen von 1 verschiedenen Teiler besitzt, so ist n prim.
$\Rightarrow$
Die Kardinalität der Gruppe $\mathbb{Z}_n \setminus \{0\}$ ist $n-1$. Somit ist für alle $x \in \mathbb{Z}_n \setminus \{0\}$ die Ordnung von x ein Teiler von $n-1$. Woraus $x^{n-1} \equiv 1 \pmod{n}$ folgt. $\square$

Der Satz von Fermat ermöglicht es, für zusammengesetzte Zahlen n sehr einfache Beweise für diese Eigenschaft anzugeben. Keineswegs eindeutig ist jedoch die Frage, ob eine solche Feststellung auch für das komplementäre Problem gilt: Ist es leicht zu überprüfen, dass eine Zahl prim ist? Der Satz von Fermat ist für einen Primalitätstest wenig hilfreich, da man die rechte Seite von Theorem 1 für alle Werte von $1, ..., n-1$ testen muss, was exponentiell viele in der Länge von n sind. Dass tatsächlich die Überprüfung für alle diese Werte notwendig ist, zeigen Pseudoprimzahlen und Carmichael-Zahlen. Pseudoprimzahlen und Carmichael-Zahlen sind zusammengesetzte, natürliche Zahlen, die jedoch eine ähnliche Eigenschaft wie die Primzahlen besitzen: Die Rückrichtung des kleinen Fermats gilt für bestimmte $x \in \mathbb{Z}_n \setminus \{0\}$ (aber nicht für alle).

Definition 1. *Eine zusammengesetzte, natürliche Zahl n heißt Fermatsche Pseudoprimzahl, wenn für eine bestimmte Basis x mit $2 \leqslant x \leqslant n-2$ und* $\mathrm{ggT}(x, n) = 1$ *gilt:* $x^{n-1} \equiv 1 \pmod{n}$

Definition 2. *Eine zusammengesetzte, natürliche Zahl n heißt Carmichael-Zahl, falls für alle zu n teilerfremden Zahlen x gilt:* $x^{n-1} \equiv 1 \pmod{n}$

Die kleinste Carmichaeli-Zahl ist 561. Nachdem sie aus den Primteilern 3, 11 und 17 zusammengesetzt werden kann, ist sie keine Primzahl. Die Bedingung von Fermat $x^{560} \equiv 1 \pmod{561}$ ist jedoch für alle $x \in \mathbb{Z}_{561} \setminus \{0\}$ bis auf die Teiler 3, 11, 17, 33, 51 und 187 erfüllt.

Das Lehmer-Theorem als Grundlage

Mit seinem Verfahren hat Pratt gezeigt, dass es dennoch möglich ist, effizient zu überprüfen, ob eine Zahl prim ist. Pratts Methode beruht dabei auf auf einer verschärften Form des Satzes von Fermat. Die Aussage des kleinen Fermats wurde zunächst von E. Lucas und später von D.H. Lehmer verbessert, wie folgende Theoreme zeigen (siehe [5]).

Theorem 2 (Lucas, 1876)**.** *Ein $n \in \mathbb{N}$ mit $n \geqslant 2$ ist eine Primzahl, wenn es ein $x \in \mathbb{N}$ gibt, mit:*

$$x^{n-1} \equiv 1 \pmod{n} \tag{1}$$

$$x^a \not\equiv 1 \pmod{n} \ \forall a = 1, 2, ..., n-2 \tag{2}$$

Diese Zahl x wird auch primitive Wurzel von n genannt.

Der Beweis für dieses Theorem lässt sich in [2] nachlesen.

Auch hier ist es immer noch zu aufwändig, alle Werte von $1, \ldots, n-2$ in (2) einzusetzen. 1891 gelang es Lucas eine verbesserte Version seines Theorems zu beweisen:

Theorem 3 (Lucas, 1891)**.** *Ein $n \in \mathbb{N}$ mit $n \geqslant 2$ ist eine Primzahl, wenn es ein $x \in \mathbb{N}$ gibt, mit:*

$$x^{n-1} \equiv 1 \pmod{n} \tag{3}$$

$$x^a \not\equiv 1 \pmod{n} \ \forall a = 1, 2, ..., n-2 \text{ mit } a \mid n-1 \tag{4}$$

Begründung: Sei a die kleinste, positive, ganze Zahl, für die gilt:

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

Weiterhin definiere man $c, d \in \mathbb{Z}$, sodass

$$c \cdot a + d = n - 1 \mid 0 \leqslant d < a$$

Damit erhält man:

$$x^{c \cdot a + d} = x^{n-1} \equiv 1 \pmod{n}$$

$$x^{c \cdot a} = (x^a)^c \equiv 1 \pmod{n}$$

Aus beiden Gleichungen folgt:

$$x^{c \cdot a + d} = x^{c \cdot a} \cdot x^d \equiv x^{c \cdot a} \equiv 1 \pmod{n}$$

Also:

$$x^d \equiv 1 \pmod{n}$$

Da aber nach Voraussetung $0 \leqslant d < a$ galt und a minimal gewählt wurde, muss $d = 0$ gelten. Also ist a ein Teiler $n - 1$. Das bedeutet: Es genügt zu zeigen, dass $x^a \not\equiv 1 \pmod{n}$ für alle Teiler von $n - 1$ gilt, da der kleinste Wert, für den $x^a \equiv 1 \pmod{n}$ erfüllt sein kann, ein Teiler von $n - 1$ ist.

Man kann sich leicht überlegen, dass die Anzahl aller Teiler einer Zahl immer noch sehr groß sein kann. Der rechnerische Aufwand lässt sich jedoch noch ein Mal reduzieren, denn es reicht sogar $x^{n-1/q} \not\equiv 1 \pmod{n}$ nur für alle Primfaktoren q von $n - 1$ zu überprüfen.

Begründung: Vorraussetzung ist, dass für alle Primteiler q von $n - 1$ die Eigenschaft $x^{n-1/q} \not\equiv 1 \pmod{n}$ erfüllt ist. Der gesuchte Wert von a ist wie eben gezeigt ein Teiler von $n - 1$. Angenommen, a wäre kleiner als $n - 1$.

Dann muss es einen Primteiler q geben, für den $n-1/q$ ein Vielfaches von a ist. Wenn aber $x^a \equiv 1 \pmod{n}$ gilt, dann gilt auch für jedes Vielfache von a: $x^{k \cdot a} \equiv 1 \pmod{n}$ $(k \in \mathbb{N})$. Also müsste auch $x^{n-1/q} \equiv 1 \pmod{n}$ für ein bestimmtes q erfüllt sein. Dies steht im Widerspruch zur Vorraussetung. Das heißt, der kleinste Wert a, für den $x^a \equiv 1 \pmod{n}$ gilt, ist somit $n-1$. Damit genügt es, (4) nur für alle Primfaktoren von $n-1$ zu zeigen.

Theorem 4 (Lehmer)**.** *Ein $n \in \mathbb{N}$ mit $n \geqslant 2$ ist eine Primzahl, wenn es ein $x \in \mathbb{N}$ gibt, mit:*

$$x^{n-1} \equiv 1 \pmod{n} \tag{5}$$

$$x^{n-1/q} \not\equiv 1 \pmod{n} \text{ } \textit{für alle Primfaktoren } q \textit{ von } n-1 \tag{6}$$

Im Gegensatz zum kleinen Satz von Fermat wird in diesem Theorem nicht die Basis x variiert, sondern nur der Exponent für ein fixes x. Die Anzahl der benötigten Test wird auf die Anzahl der Primteiler von $n-1$ reduziert, was höchstens $\log_2(n-1)$ sind.

Das formale Beweissystem

Um zu zeigen, dass eine Zahl prim ist, verwendet Pratt eine formales Beweissystem. Die Idee dabei ist, Theorem 4, Gleichung (6) sukzessive für alle Primfaktoren $q_1, \ldots, q_k$ von $p-1$ zu zeigen und dabei stets das Produkt aller bereits betrachteten Primfaktoren in einer Zählvariablen zu speichern. Das Beweissystem verwendet dabei folgende zwei Prädikate(siehe [3]):

p:	p ist prim
(p, x, a):	Jeder Primfaktor q von a erfüllt die Eigenschaft $x^{p-1/q} \not\equiv 1 \pmod{p}$.

Dabei ist x die primitive Wurzel von p und a der Zähler.

$(p, x, 1)$ ist für alle positiven, ganzen Zahlen x und p ein Axiom.

Für die beiden Prädikate gelten folgende Herleitungsregeln:

R_1:	$(p, x, a), q \vdash (p, x, a \cdot q)$	falls $x^{p-1/q} \not\equiv 1 \pmod{p}$ und $q \mid (p-1)$
R_2:	$(p, x, p-1) \vdash p$	falls $x^{p-1} \equiv 1 \pmod{p}$

Beispiel: Im Folgenden wird die Primheit der Zahl 79 gezeigt.

(1)	(2,1,1)	Axiom
(2)	2	(1), R_2
(3)	(3,2,1)	Axiom
(4)	(3,2,2)	(2), (3), R_1, da $2^{2/2} \equiv 2 \not\equiv 1 \pmod 3$
(5)	3	(4), R_2, da $2^2 \equiv 1 \pmod 3$
(6)	(13,2,1)	Axiom
(7)	(13,2,2)	(6), (2), R_1, da $2^{12/2} \equiv 12 \not\equiv 1 \pmod{13}$
(8)	(13,2,4)	(7, (2), R_1, da $2^{12/2} \equiv 12 \not\equiv 1 \pmod{13}$
(9)	(13,2,12)	(8), (5), R_1, da $2^{12/3} \equiv 3 \not\equiv 1 \pmod{13}$
(10)	13	(9), R_2, da $2^{12} \equiv 1 \pmod{13}$
(11)	(79,3,1)	Axiom
(12)	(79,3,2)	(11), (2), R_1, da $3^{78/2} \equiv 78 \not\equiv 1 \pmod{79}$
(13)	(79,3,6)	(12), (5), R_1, da $3^{78/3} \equiv 23 \not\equiv 1 \pmod{79}$
(14)	(79,3,78)	(13), (10), R_1, da $3^{78/13} \equiv 18 \not\equiv 1 \pmod{79}$
(15)	79	(14), R_2, da $3^{78} \equiv 1 \pmod{79}$

Korrektheit und Vollständigkeit

Im Folgenden soll nun gezeigt werden, dass Pratts Primzahlzertifikat vollständig und korrekt ist.

Theorem 5. *p ist eine Primzahl, genau dann wenn p ein Theorem ist.*

Hierbei hat das Theorem p einen Beweis, der von gültigen Axiomen $(x, y, 1)$ ausgeht, nur die Herleitungsregeln R_1 und R_2 benutzt und mit Prädikat p endet. Jede Zeile besteht dabei aus einem der beiden möglichen Prädikate.

Beweis

Teil 1 (p Theorem $\Rightarrow$ p prim):

Sei p Theorem. Dann ist die letzte Zeile Z des Beweises Prädikat p. Also muss Z aus Prädikat $\dot{Z} = (p, x, p-1)$ mit Herleitungsregel $R2$ abgeleitet worden sein, wobei $x^{p-1} \equiv 1 \pmod p$ gezeigt wurde. Damit ist Gleichung (5) aus Theorem 4 erfüllt.

Bleibt noch zu zeigen, dass $x^{p-1/q} \not\equiv 1 \pmod p$ für alle Primteiler q von $p-1$ (Theorem 4, (6)), was im Folgenden mit Hilfe einer Induktion geschieht.

Für $p = 2$ ist $\dot{Z} = (2, x, 1)$ und damit Axiom. Nachdem $p - 1 = 1$ in diesem Fall keine Primteiler besitzt, ist die Aussage $x^{p-1/q} \not\equiv 1 \pmod p$ für alle

Primteiler q von $p-1$ allgemein gültig, womit nach Theorem 4 $p = 2$ Primzahl ist.

Sei nun im folgenden $p > 2$. Das Prädikat $\dot{Z} = (p, x, p-1)$ ist somit kein Axiom ($p - 1 \neq 1$). Induktionsannahme sei nun: Für alle natürlichen Zahlen n, die kleiner sind als p, gilt: n Theorem $\Rightarrow$ n ist prim. Das Prädikat $(p, x, p-1)$ wurde mit Hilfe der Faktorisierung $p - 1 = q_1 \cdots q_k$ hergeleitet. Da diese Faktoren q_i alle kleiner sind als p und die Zeilen von Axiom $(q_i, x_i, 1)$ bis Prädikat q_i ein kürzerer Beweis für Theorem q_i sind, folgt nach Induktionsannahme, dass diese Faktoren tatsächlich prim sind. Nach Eindeutigkeit der Primfaktorzerlegung sind $q_1, \ldots, q_k$ alle Primfaktoren von $p - 1$. Damit ist Theorem 4, (6) erfüllt.

Teil 2 (p prim $\Rightarrow$ p Theorem):

Der Beweis folgt durch Induktion über p. Wenn p Primzahl ist, so gibt es eine primitive Wurzel x von p, wobei x die multiplikative Ordnung $p - 1$ aufweist. Die Herleitung von p beginnt stets mit dem Axiom $(p, x, 1)$. Nach Induktionsannahme gilt: Jeder der Primfaktoren von $p - 1$ ist ein Theorem. Für jeden dieser Primfaktoren gilt ferner $x^{p-1/q} \not\equiv 1 \pmod{p}$, anderenfalls wäre die Ordnung von x kleiner als $p - 1$. In dem Beweissystem lässt sich jedes Theorem (p, x, a) herleiten, falls a als Produkt von Primfaktoren von $p - 1$ darstellbar ist, insbesondere also auch $(p, x, p - 1)$. Und da $x^{p-1} \equiv 1 \pmod{p}$ gilt (nach 1), lässt sich p herleiten. □

Effizienz und Optimierung des Testaufwands

Um abschließend zu beweisen, dass in polynomieller Zeit geprüft werden kann, ob eine Zahl prim ist, muss die Länge des Zertifikats abgeschätzt werden. Die Eingabegröße einer Zahl p im Binärsystem entspricht dabei der Bitlänge von p, die mit $\log_2 p$ berechnet wird. Deswegen ist es wichtig, dass die Laufzeit zur Überprüfung des Zertifikats polynomiell von $\log_2 p$ abhängig ist.

Theorem 6. *Wenn eine Zahl p prim ist, dann gibt es einen Beweis dafür mit höchstens $6 \cdot \log_2 p - 4$ Zeilen.*

Folgender Beweis richtet sich nach den Ausführungen von Chvátal (siehe [1]).

Beweis

- Induktionsanfang: Dass die Zahlen 2 und 3 prim sind, lässt sich in zwei bzw. drei Zeilen nachweisen (siehe Zeile (1,2) bzw. (1-5) im Beweis der Primheit von 79). Für $p = 2$ und $p = 3$ gilt das Theorem: $2 = 6 \cdot \log_2 2 - 4$ und $5 < 6 \cdot \log_2 3 - 4$.
- Induktionsannahme: Für jede Primzahl q mit $p > q > 3$ lässt sich ihre Primheit in höchstens $6 \cdot \log_2 q - 4$ Zeilen zeigen.
- Induktionsschritt: Für jede Primzahl p mit $p > 3$ gilt, dass $p - 1$ eine zusammengesetzte Zahl ist, die sich in k Primfaktoren $q_1 \cdots q_k$ zerlegen lässt ($k \geqslant 2$). Der Beweis der Primheit von p besteht aus k Beweisen der Primheit der k Primfaktoren, sowie den $k + 2$ Zeilen $(p, x, q_1), (p, x, q_1 \cdot q_2), \ldots, (p, x, q_1 \cdots q_k)$. Nach Induktionsannahme besteht der Beweis folglich aus höchstens

  $$\sum_{i=1}^{k} (6 \cdot \log_2 q_i - 4) + k + 2$$

  Zeilen. Nachdem $k \geqslant 2$ gilt, kann mit folgender Abschätzung der Induktionsschritt abgeschlossen werden:

$$\sum_{i=1}^{k} (6 \cdot \log_2 q_i - 4) + k + 2 = 6 \cdot \log_2(p-1) - 3 \cdot k + 2 \leqslant 6 \cdot \log_2(p) - 4$$

□

Bei der Umsetzung des Verfahrens ergibt sich folgendes Problem: Um die Potenz x^b zu berechnen, benötigt man auf herkömmliche Art und Weise $b-1$ Multiplikationen, was zu einem ernomen Zeitaufwand und Speicherbedarf führt. Es gibt jedoch zwei Möglichkeiten, das Verfahren zu beschleunigen:

1. Anstatt die Potenz x^b in $b-1$ Schritten zu berechnen, reduziert man den Aufwand auf $2 \cdot \lfloor \log_2 b \rfloor$ Schritte, indem man den folgenden, rekursiven Algorithmus des iterierten Quadrierens verwendet:

$$\begin{array}{lll} x^b: & b = 0 & \to 1 \\ & b \text{ ungerade} & \to x \cdot x^{b-1} \\ & b \text{ gerade} & \to (x^2)^{b/2} \end{array}$$

2. Der Speicherbedarf lässt sich reduzieren, indem alle Multiplikationen des eben genannten Algorithmuses modulo p durchgeführt werden.

Um das vollständige Zertifikat zu testen, werden höchstens $\lfloor 3 \cdot \log_2 p \rfloor$ Potenzierungen benötigt. Nach dem eben genannten Algorithmus ergibt sich eine Gesamtzahl an Multiplikationen von höchstens $\left\lfloor 6 \cdot \log_2^2 p \right\rfloor$. Dazu kommen noch $6 \cdot \log_2 p - 4$ Multiplikationen für die Herleitungsregel R_1. Nach Schönhage und Strassen lässt sich eine Multiplikation in $\mathcal{O}(\log_2 p \cdot \log_2 \log_2 p)$ Schritten durchführen. Damit ergibt sich für die Überprüfung des Zertifikats eine Gesamtlaufzeit von $\mathcal{O}(\log_2^3 p \log_2 \log_2 p)$. Es lässt sich somit feststellen, dass das Zertifikat in polynomieller Zeit getestet werden kann. Also:

$$PRIMES \in NP$$

Und, wie es Vasek Chvátal formuliert ([1]):

Isn‘t that a fine thing to know.

Literatur

[1] V. Chvátal. Pratt's primality proofs. `http://users.encs.concordia.ca/~chvatal/notes/ppp.pdf`.

[2] D. H. Lehmer. *Tests for Primality by the converse of Fermat's Theorem.* Bulletin of the American Mathematical Society. Volume 33, Number 3, p.327-340, 1927. `http://projecteuclid.org`.

[3] V. Pratt. *Every Prime has a succinct Certificate.* Siam Journal on Computing, Volume 4, Issue 3, p. 214-220, 1975.

[4] A. Steger. *Diskrete Strukturen.* Springer-Verlag, 2001.

[5] Wikipedia. Lucas-test (mathematik). 2008. `http://de.wikipedia.org/wiki/Lucas-Test`.