Miller-Rabin Test

Primzahl- und Zerlegbarkeitstests

Sei N eine positive ganze Zahl. Wie kann man möglichst effizient feststellen, ob N eine Primzahl oder zerlegbar ist? Dies ist die Aufgabe von Primzahl- und Zerlegbarkeitstests.

Sei A ein (probabilistischer) Algorithmus. Wir nennen A einen Primzahltest, wenn aus $A(N) =$ wahr folgt, daß N eine Primzahl ist, und wenn für eine feste Primzahl N bei wiederholten Aufrufen $A(N) =$ falsch nur mit geringer Wahrscheinlichkeit $< 1/2$ eintritt. Entsprechend nennen wir A einen Zerlegbarkeitstest, wenn aus $A(N) =$ wahr folgt, daß N zerlegbar ist, und wenn für eine feste zerlegbare Zahl N bei wiederholten Aufrufen $A(N) =$ falsch nur mit geringer Wahrscheinlichkeit $< 1/2$ eintritt. Ist A deterministisch, so müssen die Fehlerwahrscheinlichkeiten also Null sein.

Liefert A zusätzliche Informationen, anhand derer (effizient) überprüft werden kann, ob N für einen Primzahltest wirklich eine Primzahl, und für einen Zerlegbarkeitstest wirklich zerlegbar ist, so heißt diese Zusatzinformation Zeuge für die Primzahleigenschaft beziehungsweise Zeuge für die Zerlegbarkeit von N.

Die Laufzeit von Primzahl- und Zerlegbarkeitstest soll polynomiell in $\log(N)$ mit möglichst kleinem Exponent sein.

Die Idee eines Zeugen ist tritt auch bei Problemen in NP auf. Hier sind Lösungen unter Umständen schwierig zu berechnen, aber, wenn bekannt, leicht zu verifizieren.

Zeugen für die Zerlegbarkeit ganzer Zahlen

Ist N eine Primzahl und $a \neq 0$ eine ganze Zahl, so gilt $a^{N-1} \equiv 1 \bmod N$. Findet man also ein $a \neq 0$ mit $a^{N-1} \not\equiv 1 \bmod N$, so ist N zerlegbar und a ein Zeuge für die Zerlegbarkeit von N. Hat N höchstens zwei verschiedene Primfaktoren, so kann leicht gezeigt werden, daß es stets solche Zeugen für die Zerlegbarkeit gibt. Bei mehr als drei Primfaktoren ist dies aber nicht

mehr der Fall, und die zugehörigen Zahlen N heißen Carmichaelzahlen. Die kleinste Carmichaelzahl ist $561 = 3 \cdot 11 \cdot 17$.

1 Definition. Sei N ungerade, $a \neq 0$ und $N = 2^r q + 1$ mit $q > 0$ ungerade. Wir nennen N eine starke Pseudoprimzahl zur Basis a, wenn $a^q \equiv 1 \bmod N$ gilt oder wenn es $0 \leq s \leq r-1$ mit $a^{2^s q} \equiv -1 \bmod N$ gibt.

2 Lemma. *Ist N eine ungerade Primzahl und $a \neq 0$, so ist N eine starke Pseudoprimzahl zur Basis a.*

Beweis. Gilt $a^q \equiv 1 \bmod N$, sind wir fertig. Für $a^q \not\equiv 1 \bmod N$ gilt $\operatorname{ord}(a^q) = 2^t$ mit $1 \leq t \leq r$. Für $s = t-1$ und $b = a^{2^s q}$ gilt dann $b \not\equiv 1 \bmod N$ und $b^2 \equiv 1 \bmod N$. Da $\mathbb{Z}/N\mathbb{Z}$ ein Körper ist, folgt $b \equiv -1 \bmod N$ (das Polynom $x^2 - 1$ faktorisiert in $(\mathbb{Z}/N\mathbb{Z})[x]$ eindeutig in $(x-1)(x+1)$). □

3 Definition. Sei $a \neq 0$. Ist N keine starke Pseudoprimzahl zur Basis a, so heißt a Zeuge für die Zerlegbarkeit von N. Ist a eine Basis, so nennen wir a auch einen Nichtzeugen für die Zerlegbarkeit von N.

Gilt für $a \neq 0$ zum Beispiel $\gcd(a, N) \neq 1$, so ist a ein Zeuge für die Zerlegbarkeit von N.

4 Satz. *Sei $N \geq 9$ ungerade. Ist N zerlegbar, so gibt es $\geq 3N/4$ Zeugen für die Zerlegbarkeit von N.*

Beweis. Wir beweisen, daß es $< N/4$ Elemente $a + N\mathbb{Z} \in (\mathbb{Z}/N\mathbb{Z})^\times$ gibt, so daß N eine starke Pseudoprimzahl zur Basis a ist.

Falls es kein solches a gibt, sind wir fertig. Andernfalls sei m das Maximum der Exponenten $2^s q$ mit $0 \leq s \leq r-1$, für die es eine Basis a mit $a^{2^s q} \equiv -1 \bmod N$ gibt. Diese Exponentenmenge ist nicht leer, da wir $(-a)^{2^0 q} = -1 \bmod N$ aus $a^q \equiv 1 \bmod N$ erhalten. Für jede Basis a gilt dann $a^m \equiv \pm 1 \bmod N$.

Wir definieren folgende Untergruppen von $(\mathbb{Z}/N\mathbb{Z})^\times$:

$$
\begin{aligned}
I_1 &= \{a + N\mathbb{Z} \in (\mathbb{Z}/N\mathbb{Z})^\times \mid a^{n-1} \equiv 1 \bmod N\},\\
I_2 &= \{a + N\mathbb{Z} \in I_1 \mid a^m \equiv \pm 1 \bmod p^{v_p(N)} \text{ für alle } p|N\},\\
I_3 &= \{a + N\mathbb{Z} \in I_2 \mid a^m \equiv \pm 1 \bmod N\},\\
I_4 &= \{a + N\mathbb{Z} \in I_3 \mid a^m \equiv 1 \bmod N\}.
\end{aligned}
$$

Ist a eine Basis, so gilt $a \in I_3$ nach Definition von m. Es genügt daher zu zeigen, daß $((\mathbb{Z}/N\mathbb{Z})^\times : I_3) \geq 4$ ist. Die Multiplikativität des Index liefert

$$
\begin{aligned}
((\mathbb{Z}/N\mathbb{Z})^\times : I_1)(I_1 : I_2)(I_2 : I_3)(I_3 : I_4) &= ((\mathbb{Z}/N\mathbb{Z})^\times : I_3)(I_3 : I_4)\\
&= ((\mathbb{Z}/N\mathbb{Z})^\times : I_4).
\end{aligned}
$$

Der Index $(I_1 : I_4)$ ist eine Potenz von 2. Dies folgt zum Beispiel mit dem Hauptsatz für endlich erzeugte abelsche Gruppen, da für $a \in I_1$ auch $a^{2^r} \in I_4$ gilt und die endliche abelsche Gruppe I_1/I_4 also Exponent 2^r besitzt.

Für den Index $(I_2 : I_4)$ gilt $(I_2 : I_4) = 2^u$, wobei u die Anzahl der verschiedenen Primzahlen p mit $p|N$ ist. Zum Beweis definieren wir

$$f : I_2 \to \prod_{p|N} \{-1, 1\}$$

mit $\prod_{p|N}\{-1,1\} \subseteq \prod_{p|N}(\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times$ durch $a + N\mathbb{Z} \mapsto (a^m + p^{v_p(N)}\mathbb{Z})_p$. Es ist unmittelbar einsichtig, daß f ein Homomorphismus mit $\ker(f) = I_4$ ist. Sei b eine Basis mit $b^m \equiv -1 \bmod N$ (existiert nach Definition von m) und sei $(\lambda_p + p^{v_p(N)}\mathbb{Z})_p \in \prod_{p|N}\{-1,1\}$ mit $\lambda_p = \pm 1$ beliebig. Nach dem chinesischen Restsatz gibt es ein $x \in \mathbb{Z}$ mit $x \equiv b^{(1-\lambda_p)/2} \bmod N$ für alle $p|N$. Dann gilt $f(x + N\mathbb{Z}) = (\lambda_p)_p$, so daß f also auch surjektiv ist. Nach dem Homomorphiesatz liefert f einen Isomorphismus $I_2/I_4 \cong \prod_{p|N}\{-1,1\} \cong (\mathbb{Z}/2\mathbb{Z})^u$, so daß $(I_2 : I_4) = 2^u$ folgt.

Für den Index $(I_2 : I_3)$ gilt $(I_2 : I_3) = 2^{u-1}$. Das Bild von I_3 unter f ist gleich der von $(-1, \ldots, -1)$ erzeugten Untergruppe von $\prod_{p|N}\{-1,1\}$ der Ordnung 2, da es eine Basis b mit $b^m \equiv -1 \bmod N$ gibt. Entsprechend besitzt I_3/I_4 die Ordung 2 und es ergibt sich $(I_2 : I_3) = 2^{u-1}$.

Wir unterscheiden nun drei Fälle, nämlich $u \geq 3$, $u = 2$ und $u = 1$. Gilt $u \geq 3$, so folgt $(I_2 : I_3) = 2^{u-1} \geq 4$, also $((\mathbb{Z}/N\mathbb{Z})^\times : I_3) \geq 4$. Für $u = 2$ gilt nur $(I_2 : I_3) \geq 2$. Da N dann keine Carmichaelzahl ist, ergibt sich nach den Bemerkungen vom Anfang des Abschnitts $((\mathbb{Z}/N\mathbb{Z})^\times : I_1) \geq 2$, also zusammen $((\mathbb{Z}/N\mathbb{Z})^\times : I_3) \geq 4$ wie gewünscht. Gilt schließlich $u = 1$, so ist N von der Form $N = p^e$ mit $e \geq 2$. Wir haben $\#(\mathbb{Z}/p^e\mathbb{Z})^\times = (p-1)p^{e-1}$, denn jedes Element a mit $0 \leq a \leq p^e - 1$ und $\gcd(a, p^e) = 1$ läßt sich eindeutig schreiben als $\sum_{i=0}^{e-1} a_i p^i$ mit $a_0 \in \{1, \ldots, p-1\}$ und $a_i \in \{0, \ldots, p-1\}$. Dies sind genau $(p-1)p^{e-1}$ Elemente. Da $p-1$ und p^{e-1} teilerfremd sind, gilt nach dem Hauptsatz über endlich erzeugte abelsche Gruppen $(\mathbb{Z}/p^e\mathbb{Z})^\times \cong G_1 \times G_2$ mit $\#G_1 = p - 1$ und $\#G_2 = p^{e-1}$. Wegen $\gcd(p^e - 1, (p-1)p^{e-1}) = p - 1$ enthält die Unterguppe I_1 genau die Elemente der Ordnung $p - 1$ von $(\mathbb{Z}/p^e\mathbb{Z})^\times$ und entspricht unter der Isomorphie der Untergruppe $G_1 \times \{0\}$ von $G_1 \times G_2$. Es folgt $\#I_1 = \#(G_1 \times \{0\}) = \#G_1 = p - 1$ und $((\mathbb{Z}/p^e\mathbb{Z})^\times : I_1) = (p-1)p^{e-1}/(p-1) = p^{e-1}$. Für $p \geq 5, e \geq 2$ oder $p = 3, e \geq 3$ gilt damit $((\mathbb{Z}/p^e\mathbb{Z})^\times : I_3) \geq 5$. Es bleibt daher nur der Fall $p = 3, e = 2$, also $N = 9$ zu behandeln. Hier kann die Aussage des Satzes aber direkt von Hand nachgerechnet werden (es gibt genau 2 Basen, nämlich ± 1). Damit ist die Aussage des Satzes vollständig bewiesen. $\square$

Miller-Rabin Test

Der Miller-Rabin Test ist ein Zerlegbarkeitstest und ist in der Praxis wegen seiner guten Eigenschaften sehr weit verbreitet. Er ergibt sich mit den Aussagen des vorherigen Abschnitts wie folgt.

5 Algorithmus. *(Miller-Rabin Test)*

Eingabe: *Ganze Zahlen $N > 1$ und $k \geq 1$.*

Ausgabe: *„N ist zerlegt“ und ein Zeuge a für die Zerlegbarkeit von N, oder „N ist eine Primzahl“.*

1. *Falls $N \in \{2, 3, 5, 7\}$, dann Ausgabe von „N ist eine Primzahl“. Falls N gerade ist, Ausgabe von „N ist zerlegt“ und 2.*
2. *Wähle $a \in \{1, \ldots, N-1\}$ zufällig und gleichverteilt.*
3. *Falls a ein Zeuge für die Zerlegbarkeit von N ist (hierfür $\gcd(a, N) \neq 1$ und Bedingungen testen), Ausgabe von „N ist zerlegt“ und a.*
4. *Schritte 2 und 3 werden k-mal wiederholt. Falls kein Zeuge gefunden wurde, Ausgabe von „N ist eine Primzahl“.*

6 Satz. *Der Miller-Rabin Test ist ein Zerlegbarkeitstest mit Fehlerwahrscheinlichkeit $\leq (1/4)^k$.*

Beweis. Schritt 1 gibt für $N \leq 8$ das korrekte Ergebnis aus. Die nachfolgenden Schritte werden dann für $N \geq 9$ und N ungerade ausgeführt.

Wenn der Miller-Rabin Test in Schritt 3 „N ist zerlegt“ ausgibt, so ist N nach Lemma 2 in der Tat zerlegbar. Wenn der Miller-Rabin Test in Schritt 4 „N ist eine Primzahl“ ausgibt, so ist N nach Satz 4 mit Wahrscheinlichkeit $\leq (1/4)^k$ keine Primzahl. □

Der Miller-Rabin Test ist sehr effizient. Seine Laufzeit ist $O(k \log(N)^3)$ unter Verwendung von „Schulbuchintegerarithmetik“ und $O^{\sim}(k \log(N)^2)$ unter Verwendung von asymptotisch schneller Integerarithmetik, wie unschwer zu sehen ist. Außerdem fällt die Fehlerwahrscheinlichkeit in Wirklichkeit noch viel geringer als $(1/4)^k$ aus.

In der Kryptographie verwendet man den Miller-Rabin Test als Primzahltest, zum Beispiel bei der Erzeugung von RSA Moduln. Man wählt hier k so, daß die Wahrscheinlichkeit einer falschen Ausgabe vernachlässigbar klein wird. Dies ist für kryptographische Zwecke ausreichend.

Der Miller-Rabin Test wird aber auch bei eigentlichen Primzahltests eingesetzt. Man überprüft damit in einer Vorberechung, ob N zumindest mit hoher Wahrscheinlichkeit eine Primzahl ist. Erst danach wird der eigentliche Primzahltest auf N angewendet.

Andere Primzahl- und Zerlegbarkeitstests

Es gibt eine ganze Reihe weiterer Primzahl- und Zerlegbarkeitstests. Hervorzuheben ist vielleicht der AKS Primzahltest (nach Agrawal, Kayal und Saxena), der erst 2002 entdeckt wurde. Es handelt sich hierbei um ein deterministisches Verfahren mit Laufzeit $O(\log(N)^6)$.

Zwei Gesichtspunkte sind beim AKS Primzahltest bemerkenswert: Erstens die Eigenschaft, daß er deterministisch ist („Primes in P“). Alle zuvor bekannten Verfahren waren probabilistisch („Primes in BPP“). Zweitens kam seine Entdeckung sehr überraschend, da Primzahltests schon relativ lange untersucht werden und die Methodik des AKS Primzahltest irgendwie übersehen wurde.