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 $561 = 3 \cdot 11 \cdot 17$.

Die folgende Definition gibt ein spezielleres, notwendiges Kriterium für eine Primzahl N an. Wir werden zeigen, daß es für dieses Kriterium stets Zeugen für die Zerlegbarkeit von N gibt.

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 $\mathrm{ord}(a^q) = 2^t$ 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 kein Zeuge für die Zerlegbarkeit von N, 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. Für $N = 9$ sind die Nichtzeugen für die Zerlegbarkeit von N gleich $1, -1$, wie man leicht von Hand nachrechnet oder unter Verwendung von Lemma 9 und der Bemerkung danach beweist. Die Anzahl der Nichtzeugen ist also $\leq N/4$. Wir wollen diese Schranke auch für größere N beweisen.

Im folgenden sei $v_P(N)$ den Exponent von p in der Primfaktorisierung von N. Es gilt also $N = \prod_{p \text{ Primzahl}} p^{v_p(N)}$. Mit $\phi(N)$ wird die Eulersche Phi-Funktion, also die Kardinalität von $(\mathbb{Z}/N\mathbb{Z})^\times$ bezeichnet.

4 Satz. *Sei $N \geq 11$ ungerade und zerlegbar, und sei u die Anzahl der verschiedenen Primfaktoren von N. Die Anzahl der Nichtzeugen für die Zerlegbarkeit von N ist dann kleiner oder gleich*

$$(1/2)^{u-1} \prod_{p|N} \gcd(N-1, p-1) \leq N/4.$$

Beweis. Für Nichtzeugen gilt $a \neq 0$ und $\gcd(a, N) = 1$, also $a + N\mathbb{Z} \in (\mathbb{Z}/N\mathbb{Z})^\times$. Falls es keinen Nichtzeugen 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 einen

Nichtzeugen 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. Daher ist $m > -\infty$. Für jeden Nichtzeugen 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 ein Nichtzeuge, so gilt $a \in I_3$ nach Definition von m. Wir verwenden folgende Aussagen:

$$(I_2 : I_3) = 2^{u-1} \tag{5}$$

$$\#I_1 = \prod_{p|N} \gcd(N-1, p-1). \tag{6}$$

Mit diesen Aussagen ergibt sich

$$\begin{aligned}
\#I_3 &= (I_2 : I_3)^{-1} \#I_2 \le (I_2 : I_3)^{-1} \#I_1\\
&\le (1/2)^{u-1} \prod_{p|N} \gcd(N-1, p-1),
\end{aligned}$$

womit die erste Behauptung des Satzes bewiesen wäre.

Zum Beweis von (5). 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. Um dies zu zeigen 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 $x^m \equiv (b^m)^{(1-\lambda_p)/2} \equiv (-1)^{(1-\lambda_p)/2} \equiv \lambda_p \bmod p^{v_p(N)}$ und $x^{N-1} \equiv (x^m)^{2^{s-r}} \equiv (\pm 1)^{2^{s-r}} \equiv 1 \bmod p^{v_p(N)}$ wegen $s - r \ge 1$ nach Definition von m,

also $x^m \equiv 1 \bmod N$ und $x \in I_2$. Konkret gilt $f(x) = (\lambda_p)_p$, 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 $(I_2 : I_3) = 2^{u-1}$. Damit ist (5) bewiesen.

Zum Beweis von (6). Nach dem chinesischen Restsatz gilt

$$\#I_1 = \prod_{p|N} \#\{a \in (\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times \mid a^{N-1} \equiv 1 \bmod p^{v_p(N)}\}.$$

Wir müssen daher die Anzahl der Elemente der Ordnung $N-1$ in $(\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times$ bestimmen. Wegen $\gcd(N-1,p) = 1$ sind dies nach Lemma 9 genau $\gcd(N-1,p-1)$ Elemente, womit (6) bereits bewiesen wäre.

Es bleibt zu zeigen, daß $(1/2)^{u-1}\prod_{p|N}\gcd(N-1,p-1) \le N/4$ gilt. Wir zeigen genauer $(1/2)^{u-1}(\prod_{p|N}\gcd(N-1,p-1))/\phi(N) \le 1/4$, wobei dann wegen $\phi(N) \le N$ die Aussage folgt. Mit $\phi(N) = \prod_{p|N}(p-1)p^{v_P(N)-1}$ müssen wir also

$$(1/2)^{u-1}\prod_{p|N}\big(\gcd(N-1,p-1)/(p-1)\big)p^{-v_P(N)+1} \tag{7}$$

nach oben durch $1/4$ abschätzen. Für $u \ge 3$ ist (7) bereits aufgrund des Vorfaktors $(1/2)^{u-1}$ kleiner gleich $1/4$. Für $u = 2$ ist der Vorfaktor gleich $1/2$ und mindestens einer der Faktoren $\gcd(N-1,p-1)/(p-1) \le 1/2$, so daß (7) ebenfalls kleiner gleich $1/4$ ist. Die Aussage über den gcd sieht man wie folgt: Ist $N = p_1p_2$ mit $p_1 < p_2$, so folgt aus $\gcd(N-1,p_2-1)/(p_2-1) = 1$ auch $N \equiv 1 \bmod (p_2-1)$ und $p_1 \equiv 1 \bmod (p_2-1)$. Wegen $p_1 < p_2$ ergibt sich $p_1 = 1$, im Widerspruch zur Wahl von p_1. Da sich der gcd nur um ganzzahlige Vielfache ändert, ist also $\gcd(N-1,p_2-1)/(p_2-1) \le 1/2$. Für $u = 1$ sei $N = p^e$ mit $e = v_P(N) \ge 2$, da N nach Voraussetzung zerlegbar ist. Aufgrund der Voraussetzungen $N \ge 11$ und N ungerade gilt dann $p^{e-1} \ge 4$, so daß (7) wieder kleiner gleich $1/4$ ist. □

8 Bemerkung. Nach dem Beweis von Satz 4 ist $(1/2)^{u-1}\#I_2$ eine obere Schranke für die Anzahl der Nichtzeugen. Auf der anderen Seite ist $(1/2)^u\#I_2$ eine untere Schranke für die Anzahl der Nichtzeugen: Die Elemente aus $I_3\backslash I_4$ sind nämlich Nichtzeugen, und es gilt $(I_3 : I_4) = 2$. Daher erhalten wir in der Tat die untere Schranke $(1/2)\#I_3 = (1/2)^u\#I_2$. Mit einem genaueren Ausdruck für $\#I_2$ läßt sich die Anzahl der Nichtzeugen also genauer bestimmen.

9 Lemma. *Sei p eine Primzahl und $e \geq 1$. Dann gilt*

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \cong G_1 \times G_2$$

mit einer zyklischen Gruppe G_1 der Ordnung $p-1$ und einer abelschen Gruppe G_2 der Ordnung p^{e-1}.

Beweis. Es gilt $\#(\mathbb{Z}/p^e\mathbb{Z})^\times = (p-1)p^e$, 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 $\#G_2 = p^{e-1}$. Wir können ohne Einschränkung annehmen, daß G_1 und G_2 Untergruppen von $(\mathbb{Z}/p^e\mathbb{Z})^\times$ sind, so daß $(\mathbb{Z}/p^e\mathbb{Z})^\times = G_1G_2$ mit $G_1 \cap G_2 = \{1\}$ gilt. Es bleibt zu zeigen, daß G_1 zyklisch ist.

Hierzu betrachten wir den kanonischen Epimorphismus $f : \mathbb{Z}/p^e\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Nach den obigen Überlegungen erhalten wir daraus einen Epimorphismus $g : (\mathbb{Z}/p^e\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. Es gilt $\ker(g) = \{a + p^e\mathbb{Z} \in \mathbb{Z}/p^e\mathbb{Z} \,|, a \equiv 1 \bmod p\}$. Wir schreiben $U_{p^e}^{(1)} = \ker(g)$. Nun ist $(\mathbb{Z}/p\mathbb{Z})^\times$ zyklisch mit der Ordnung $p-1$, und $U_{p^e}^{(1)}$ abelsch mit der Ordnung p^{e-1}. Wegen $(\mathbb{Z}/p^e\mathbb{Z})^\times \cong G_1 \times G_2$, $\#G_1 = p-1$ und $\#U_{p^e}^{(1)} = p^{e-1}$ ergibt sich $U_{p^e}^{(1)} = G_2$. Wegen $\ker(g) \cap G_1 = U_{p^e}^{(1)} \cap G_1 = G_2 \cap G_1 = \{1\}$ ergibt sich, daß die Einschränkung $g : G_1 \to (\mathbb{Z}/p\mathbb{Z})^\times$ ein Isomorphismus ist. Also ist G_1 zyklisch. □

Der Beweis des Lemmas zeigt genauer, daß die kanonische exakte Sequenz

$$1 \to U_{p^e}^{(1)} \xrightarrow{i} (\mathbb{Z}/p^e\mathbb{Z})^\times \xrightarrow{g} (\mathbb{Z}/p\mathbb{Z})^\times \to 1$$

zerlegt ist, daß es also einen Epimorphismus $j : (\mathbb{Z}/p^e\mathbb{Z})^\times \to U_{p^e}^{(1)}$ und einen Monomorphismus $h : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p^e\mathbb{Z})^\times$ mit $j \circ i = \mathrm{id}$ und $g \circ h = \mathrm{id}$ gibt. Wir können dann

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times U_{p^e}^{(1)}$$

schreiben, wobei der Isomorphismus durch $a \mapsto (g(a), j(a))$ mit Inversem $(x, y) \mapsto h(x)i(y)$ gegeben wird.

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.

10 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“.*

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

Beweis. Schritt 1 gibt für $N \leq 8$ oder N gerade 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 und der Bemerkung für $N = 9$ vor 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: Für „zufällige“ N sind die $\gcd(N-1, p-1)$ deutlich kleiner als $p - 1$, so daß sich in der Abschätzung am Ende des Beweises von Satz 4 deutlich kleinere obere Schranken für (7) als $1/4$ ergeben.

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.