Der Rabin Miller Test

erstellt von
Mag. Stefan Hagmann 2007

Allgemeines

Der Rabin Miller Test kann dazu verwendet werden, eine ungerade Zahl N auf Primalität zu testen. Dieser Test ist recht zuverlässig und schnell durchzuführen.

Gilt für eine ungerade Zahl N, die darstellbar ist als $N = s \cdot 2^t + 1$, wobei $s, t \in \mathbb{N}$ und s ungerade sind, mit einer Zahl $a \in \mathbb{Z}\ 1 \leq a < N - 1$

$$a^s \equiv 1 \mod N \tag{1}$$

oder

$$a^{s \cdot 2^r} \equiv -1 \mod N \text{ für } 0 \leq r < t \tag{2}$$

Dann ist N eine Starke Wahrscheinliche Primzahl zur Basis a $(SWP(a))$.

Die Formel (2) ist für ein Computerprogramm in dieser Form nicht zu gebrauchen. Denn N ist größer als 0 und damit ist jedes Ergebnis von Formel (2) > 0. Da aber bei Konqruenzen gilt

$$a \equiv b \mod N \Longleftrightarrow (a - b) \mod N = 0 \tag{3}$$

können wir die Formel (2) umschreiben zu

$$a^{s \cdot 2^r} \equiv -1 \mod N \Longleftrightarrow a^{s \cdot 2^r} + 1 \mod N = 0 \tag{4}$$

Als Beispiel:

$$3 \equiv 24 \mod 7 \Longleftrightarrow (3 - 24) \mod 7 = 0 \tag{5}$$

Es bleibt kein Rest, denn $-21 = -3 \cdot 7$ und daher ist der Modul 0.

Anmerkungen

Falls N eine Primzahl ist, fällt für alle a einer der beiden Teiltests positiv aus, falls N jedoch zusammengesetzt ist, fallen für mindestens Dreiviertel aller a beide Teiltests negativ aus. Wenn man also für so ein gegebenes N eine Zahl a mit $1 \leq a < N - 1$ gleichmäßig zufällig auswählt und die beiden Tests durchführt, kann man bei zwei negativen Antworten sicher sein, dass N keine Primzahl ist, während man bei einer positiven Antwort mit Sicherheit $\frac{3}{4}$ sagen kann, dass N eine Primzahl ist. Durch m-fache Wiederholung des Test's kann man die Sicherheit auf $1 - \left(\frac{1}{4}\right)^m$ hochschrauben.

Zusammenfassung

1. N muss eine ungerade Zahl sein, da nur ungerade Zahlen Primzahlen sein können
2. Zerlege N in die Form $N = s \cdot 2^t + 1$, wobei $s, t \in \mathbb{N}$ und s ungerade sind
3. Wähle eine Basis a im Bereich $1 \leq a < N - 1$
4. Teste nun $a^s \equiv 1 \mod N$

Test bestanden?	
Ja	Nein
N ist prim!	weiter zum nächsten Punkt

5. Teste $a^{s \cdot 2^r} \equiv -1 \mod N$ für $0 \leq r < t$
   Teste solange bis alle r aus $0 \leq r < t$ durchgetestet sind, oder der Test erfüllt wurde.

Test bestanden?	
Ja	Nein
N ist prim!	erhöhe r um 1 teste erneut solange, bis $r < t$ erreicht ist, oder Test bestanden

6. Um die Sicherheit zu steigern, wiederhole den Primzahltest für andere Zahlen a. Wiederholst du den Test m Mal, ist die Sicherheit $1 - \frac{1}{4}^m$

Teilbarkeitsregeln

Bevor man eine Zahl auf Primalität testet, ist es sinnvoll die Teilbarkeitsregeln aus der Schule auf die Zahl anzuwenden. Denn werden die Zahlen sehr groß, kann der Rabin Miller Test schon einige Zeit in Anspruch nehmen.

Teilbarkeit durch 2

Eine Zahl ist durch 2 teilbar, wenn sie mit 0, 2, 4, 6 oder 8 endet, man kann auch sagen: wenn die letzte Ziffer gerade ist.

Teilbarkeit durch 3

Bilde die Quersumme der Zahl (d.h. addiere alle Ziffern).
Wenn die Quersumme durch 3 teilbar ist, dann ist es die ursprüngliche Zahl auch.
Beispiel:
Ist 3 ein Teiler von 2.169.252?
Ja, denn die Quersumme ist $2+1+6+9+2+5+2 = 27$, und 27 ist durch 3 teilbar.
Sollte die erste Quersumme zu groß sein, als daß du die Teilbarkeit durch 3 schon sehen kannst, dann bilde von der Quersumme nochmal die Quersumme. Das kannst du solange machen, bis du eine einstellige Zahl hast.
Beispiel: 9938993948234086886 ist nicht durch 3 teilbar, denn $9+9+3+8+9+9+3+9+4+8+2+3+4+0+8+6+8+8+6 = 116$ und die Quersumme von 116 ist 8.

Teilbarkeit durch 5

Jede Zahl, die mit 0 oder 5 endet ist durch 5 teilbar.

Teilbarkeit durch 7

Multipliziere die letzte Ziffer der Zahl mit 2. Subtrahiere das Ergebnis von der Zahl ohne die letzte Stelle. Wenn das Ergebnis durch 7 teilbar ist, dann ist es die ursprüngliche Zahl auch.
Beispiel: 364 ist durch 7 teilbar, denn die letzte Ziffer ist 4, multipliziert mit 2 ergibt 8. Subtrahiere $36 - 8 = 28$. 28 ist durch 7 teilbar.
Auch diesen Test kann man mehrmals nacheinander durchführen, solange bis man bei einer Zahl endet, von der man weiß, daß sie durch 7 teilbar ist.