

Zwei Probabilistische Primzahltests

Thomas Rupp*

Version 1.0[†]

15. Januar 2001

1 Der Fermat'sche Test

Satz 1.1 (kleiner Fermat) *Sei n prim. Dann gilt:*

$$a^{n-1} \equiv 1 \pmod{n} \text{ für alle } a \in [1, n-1].$$

Ein einfacher Ansatz um eine Zahl n auf ihre Primeigenschaft hin zu untersuchen, wäre es, zufällig Zahlen $a \in [2, n-2]$ zu ziehen und darauf den kleinen Satz von Fermat anzuwenden.

Definition 1.2 (pseudoprim) *Eine Zahl n für die $a^{n-1} \equiv 1 \pmod{n}$ erfüllt ist, nennen wir pseudoprim zur Basis a . Trifft das auf alle zu n teilefremde a zu¹, nennen wir sie pseudoprim.*

Ist n eine Zahl, die nicht pseudoprim ist, dann kann sie keine Primzahl sein und \mathbb{Z}_n^* enthält zumindest $\left\lfloor \frac{\mathbb{Z}_n^*}{2} \right\rfloor$ Elemente, für die diese Eigenschaft nicht erfüllt ist². Demzufolge wird eine nicht pseudoprime Zahl bei zufälliger Ziehung von t Zahlen aus $[2, n-2]$ mit einer Wahrscheinlichkeit $< (\frac{1}{2})^{-t}$ als pseudoprim deklariert³. Unser Algorithmus $F(n, t)$ sieht also für eine Zahl n und t Durchläufe so aus:

1. tue folgendes t -mal:

- (a) wähle a gleichmäßig verteilt aus $[2, n-2]$
- (b) Wenn $a^{n-1} \not\equiv 1 \pmod{n}$ dann ist n nicht prim

2. deklariere n als prim

*thomas@7t7.de

[†]Quellen: Handbook of applied cryptography, A. Menezes, P. van Oorschot, S. Vanstone; Prime Glossary, <http://www.utm.edu/research/primes/glossary/>; Randomized Algorithms, Rajeev Motwani, Probhaka Roghavan; Skript Diskrete Mathematik, Günter Bartsch

¹die Einschränkung auf $a \in \mathbb{Z}_n^*$ reicht aus, da $a \notin \mathbb{Z}_n^* \Leftrightarrow \text{ggT}(a, n) > 1 \Rightarrow a^{n-1} \not\equiv 1 \pmod{n}$; siehe nächste Seite

²mit $a_i^{n-1} \equiv 1$ und $b^{n-1} \not\equiv 1$ folgt auch $(a_i b)^{n-1} \not\equiv 1$; es gibt sogar nur $< \frac{\phi(n)}{2}$ Basen zu denen n pseudoprim ist

³bzw. sogar $< (\frac{\phi(n)}{2n})^{-t}$

1.1 Carmichael-Zahlen

Ein kleines Problem stellen jedoch die Carmichael-Zahlen da.

Definition 1.3 Eine zusammengesetzte pseudoprime Zahl heisst Carmichael-Zahl.

Satz 1.4 n ist eine Carmichael-Zahl genau dann, wenn sie quadratfrei ist (d.h. alle Faktoren p_i der Primzahlzerlegung sind einfach) und für alle p_i gilt: $p_i - 1 | n - 1$.

Beweis

Sei $n = \prod_1^m p_i^{k_i}$ die Primfaktorzerlegung. Nach dem CRT ist $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}$. Mit $a = (a_1, \dots, a_m)$ und $a^{n-1} \equiv 1 \pmod n$ folgt für jedes i : $\text{ord } \mathbb{Z}_{p_i^{k_i}} = (p_i - 1)p_i^{k_i-1} | (n - 1) \stackrel{k_i \geq 1}{\cong} p_i | (n - 1)$. Nach Konstruktion von n gilt aber auch $p_i | n$. Widerspruch. Also treten alle Primfaktoren nur einfach auf und für diese gilt $(p_i - 1) | (n - 1)$.

Die Rückrichtung ist trivial.

□

Bemerkung 1.5 Eigenschaften der Carmichael-Zahlen

- Jede Carmichael-Zahl hat mindestens 3 Primfaktoren
- Es gibt unendlich viele Carmichael-Zahlen; die kleinste ist $561 = 3 \cdot 11 \cdot 17$.

Von dem Fermat'schen Primzahltest werden also Carmichael-Zahlen für Primzahlen gehalten, solange nicht zufällig a als beliebiges Produkt der Primfaktoren gezogen wurde⁵. Dies ist aber in der Praxis nicht allzu tragisch, da es viel weniger Carmichael-Zahlen als Primzahlen gibt. Jedoch wird beim Fermat'schen Test eine Carmichael-Zahl mit Wahrscheinlichkeit $\frac{\phi(n)}{n}$ nicht entlarvt.

1.1.1 Fermat-Schnelltest

In bestimmten Fällen könne wir schon mit erstaunlicher Geschwindigkeit eine Primzahl mit ansehnlicher Wahrscheinlichkeit 'erkennen':

Unter den ersten 25.000.000.000 Zahlen gibt es lediglich 21853 nichtprime Zahlen die pseudoprime zur Basis 2 sind. Testen wir also nur einmal zur Basis 2, so beträgt die Chance auf eine solche Zahl zu treffen lediglich 0.0000874%. Das kann unter Umständen schon ausreichen und ist somit ein äusserst schneller Test.

⁴ da $\text{ggT}(p_i^{k_i}, p_j^{k_j}) = 1, \forall i \neq j$

⁵ der kleine Fermat ist nicht erfüllt, wenn $\text{ggT}(a, n) > 1$: mit dem CRT sehen wir, dass dann in der jeweiligen Komponente eine 0 statt einer 1 steht. Dies trifft deshalb auf $n - \phi(n)$ viele Zahlen aus $[1, n - 1]$ zu.

1.1.2 Verteilung von Prim- und Carmichael-Zahlen

Für große x gilt für die Anzahl $\text{car}(x)$ der Carmichael-Zahlen unterhalb von x :

$$x^{\frac{2}{7}} < \text{car}(x) < x^{1-(1+o(1))\frac{\ln \ln \ln x}{\ln \ln x}}$$

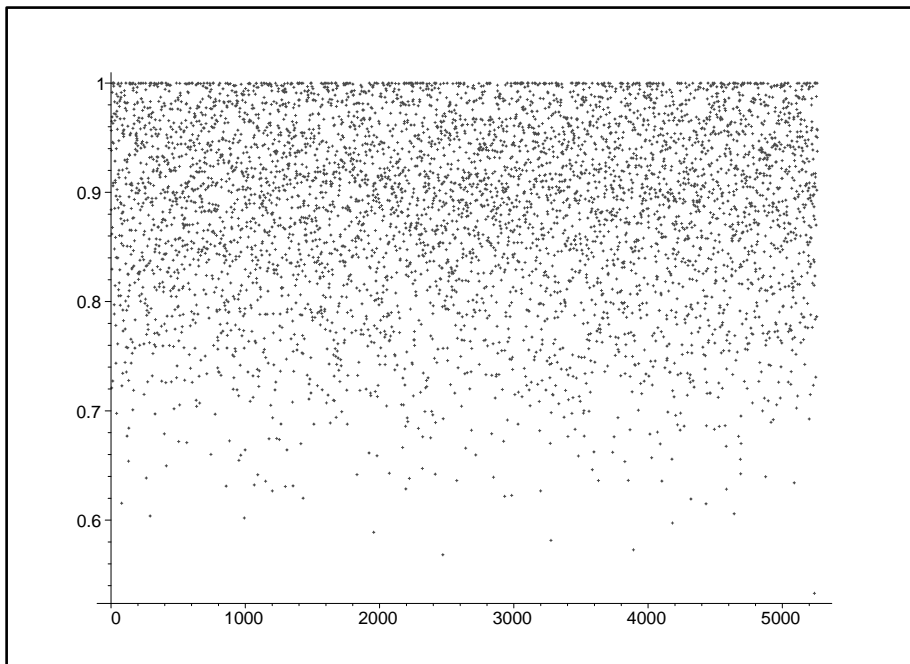
Bekanntermaßen gilt analog für die Anzahl der Primzahlen

$$\frac{x}{\ln x} < \pi(x) < 1.22506 \frac{x}{\ln x}.$$

Sehen wir uns die Anzahl der Primzahlen unterhalb von 10^{15} an, so befinden sich darunter ca. $2.9 \cdot 10^{13}$ Primzahlen, aber lediglich 105212 Carmichael-Zahlen. Die Wahrscheinlichkeit eine solche Carmichael-Zahl anstatt einer Primzahl zu erwischen⁶ beträgt also lediglich etwa $3.6 \cdot 10^{-9}$. Bei größeren Primzahlen fällt diese dann konsequenterweise weiter ab. Heute werden 1000-bittige Primzahlen benutzt; von diesen gibt es $6 \cdot 10^{190}$ mal mehr als 1000-bittige Carmichael-Zahlen.

Der Fermat'sche Test zeichnet sich durch sehr geringen Rechenaufwand aus und besticht durch seine Einfachheit. Seine Schwächen sind das Vorhandensein 'besserer' Tests und dass die Erkennungswahrscheinlichkeit von Carmichael-Zahlen sehr gering ist bzw. überhaupt berücksichtigt werden muss.

Bei den ersten 105212 Carmichael-Zahlen beträgt die Irrtumswahrscheinlichkeit⁷ im Mittel 88.89%. Es gibt zwar einzelne Ausreisser, wie z.B. $1.886.616.373.665 = 3 \cdot 5 \cdot 17 \cdot 23 \cdot 83 \cdot 353 \cdot 10979$, bei der ein Irrtum nur zu 47.2965% auftritt, sonst ist sie jedoch meist sehr hoch, wie die Verteilung der Irrtumswahrscheinlichkeit bei einer zufälligen Auswahl von 5% der ersten 105212 Carmichael-Zahlen nahelegt:



Ein Test, der keine Sonderbetrachtungen erfordert und 'besser' ist, ist eine Erweiterung des Fermat'schen Tests, der Miller-Rabin-Test.

⁶also eine pseudoprime Zahl, welche nicht prim ist

⁷also eine Carmichael-Zahl nicht als zusammengesetzt zu erkennen; pro Durchlauf

2 Der Miller-Rabin-Test

Satz 2.1 Sei n prim ($n > 2$) und $n - 1 = 2^s r$ mit r ungerade. Sei $1 < a < n$. Dann ist entweder $a^r \equiv 1 \pmod{n}$ oder $a^{2^j r} \equiv -1 \pmod{n}$ für ein $j : 0 \leq j \leq s - 1$.

Beweis Entweder ist $a^r \equiv 1 \pmod{n}$ und besitzt in \mathbb{Z} keine Quadratwurzel oder, wenn dem nicht so ist, so ist nach dem kleinen Fermat $a^{n-1} = a^{2^s r} \equiv 1 \pmod{n}$ und $a^{2^s r}$ besitzt in \mathbb{Z} eine Quadratwurzel. Diese ist dann modulo n entweder kongruent 1 oder -1 (sonst besäße die 1 mind. 4 Quadratwurzeln).

Also gibt es ein $j : 0 \leq j \leq s - 1$ so dass $a^{2^j r} \equiv -1 \pmod{n}$ ist.

□

Fakt 2.1 Es gibt (für $n \neq 9$) maximal $\frac{\phi(n)}{4}$ Zahlen $\in [1, n-1]$, die diese Eigenschaft erfüllen, wenn n nicht prim ist.

Der Algorithmus M-R(n, t) sieht dann für eine Primzahl $n > 9$ und t Testläufen so aus:

1. bestimme s, r so, dass $n - 1 = 2^s r$ mit r ungerade
2. tue folgendes t -mal:
 - (a) wähle a gleichmäßig verteilt aus $[2, n - 2]$
 - (b) $y := a^r \pmod{n}$
 - (c) Wenn $y \not\equiv 1 \pmod{n}$ und $y \not\equiv -1 \pmod{n}$ dann tue folgendes
 - i. bestimme j so, dass $y^{2^j} \not\equiv 1 \pmod{n}$ und j minimal ist
 - ii. Wenn $y^{2^j} \not\equiv -1 \pmod{n}$ dann ist n nicht prim
3. deklariere n als prim

In Schritt (c) wird abgefragt, ob $a^r \equiv \pm 1 \pmod{n}$ ist. Ist dies der Fall, so wird n in diesem Durchlauf als prim deklariert (Fakt 2.1 trifft zu). Trifft Abfrage (ii.) zu, so gibt es das geforderte j aus Fakt 2.1 nicht ($y \not\equiv -1, y^2 \equiv 1 \pmod{n}$).

Deklariert der Algorithmus n als nicht prim, dann stimmt das auch. Gibt er die Zahl als prim aus, so ist die Irrtumswahrscheinlichkeit

$$< \left(\frac{1}{4}\right)^t \text{ bzw. sogar } < \left(\frac{\phi(n)}{4n}\right)^t.$$

Der Miller-Rabin-Test ist dem Fermat'schen Test deutlich überlegen, da er nicht-prime Zahlen mit doppelter Wahrscheinlichkeit erkennt, eine gleichwertige Laufzeit besitzt, ebenfalls noch einfach zu implementieren ist und die Carmichael-Zahlen hier keine gesonderte Rolle mehr spielen.

Er zählt (in dieser oder einer abgewandelten Form) zu den wichtigsten probabilistischen Primzahltests.