Zusammenfassung

der Bachelor-Arbeit *Vom Kleinen Satz von Fermat zum Lucas-Primzahltest*, vorgelegt von Marcell Dietl, am 20.06.2014, zur Erlangung des akademischen Grades Bachelor of Science – B.Sc.

Der Kleine Satz von Fermat besagt, dass für jede Primzahl N und jede dazu teilerfremde natürliche Zahl a stets

$$a^{N-1} \equiv 1 \pmod{N}$$

gilt. Die Umkehrung gilt jedoch nicht. Es gibt unendlich viele Zahlen N, welche die Kongruenz erfüllen, obwohl sie zusammengesetzt sind: Fermatsche Pseudoprimzahlen (zur Basis a). Da diese selten sind, seltener noch als Primzahlen, und weil die modulare Exponentiation, also die Berechnung von $b = a^{N-1} \bmod N$, auch bei vergleichsweise großen Zahlen effizient ist, ist der Kleine Satz von Fermat prinzipiell als Primzahltest geeignet:

Um zu entscheiden, ob eine Zahl N prim ist, berechnet man für eine Reihe zufällig gewählter Basen $1 < a < N$, ob $b = a^{N-1} \bmod N$ gleich oder ungleich 1 ist. Ist b jedes Mal gleich 1, so ist N vermutlich prim. Andernfalls ist N definitiv zusammengesetzt.

Je mehr Basen man testet, desto wahrscheinlicher ist, dass N tatsächlich prim ist. Problematisch wird es immer dann, wenn N eine Carmichael-Zahl ist, also eine zusammengesetzte Zahl, die zu *jeder* teilerfremden Basis pseudoprim ist, und N keine „kleinen“ Primfaktoren enthält. Solche Zahlen sind zwar überaus selten, aber es gibt unendlich viele von ihnen und sie werden von obigem Verfahren nur mit viel Glück entlarvt.

Eine Möglichkeit, um diesem Problem zu begegnen, bietet der Lucas-Primzahltest, der den Kleinen Satz von Fermat umkehrt, indem er ihm eine weitere Bedingung hinzufügt, dank der sich dann zweifelsfrei feststellen lässt, ob N prim ist. Da diese Bedingung jedoch die Faktorisierung von $N - 1$ voraussetzt, ist der Lucas-Primzahltest nur dann wirklich effizient, wenn die Faktorisierung von $N-1$ bekannt oder leicht zu ermitteln ist.

Eine Eigenart, die im Pépin-Primzahltest Verwendung findet. Jenem Primzahltest, der speziell auf Fermat-Zahlen

$$F_k = 2^{2^k} + 1,$$

mit $k \in \mathbb{N}$, zugeschnitten ist und sich zunutze macht, dass $F_k - 1$ nur einen einzigen Primfaktor enthält: die Zahl 2. Für beliebige Zahlen ist dieser Primzahltest zwar augenscheinlich ungeeignet. Die Leistungsfähigkeit in Bezug auf die rasant wachsenden Fermat-Zahlen, die schnell tausende Dezimalstellen lang sind, ist jedoch beeindruckend.

Ziel der vorliegenden Arbeit ist es, diese und weitere Primzahltests theoretisch wie praktisch zu analysieren, um ihre jeweiligen Vor- bzw. Nachteile herausarbeiten und miteinander vergleichen zu können. Um dies zu erreichen, liegt der Schwerpunkt der Analysen auf den mathematischen Ideen hinter den Primzahltests. Erst wenn diese vollständig verstanden und rigoros bewiesen wurden, folgen Zahlenbeispiele, Pseudocode und eine beispielhafte Implementierung in Python bzw. im Falle des Lucas-Primzahltests in Sage.

Dank dieser kann die Leistungsfähigkeit der Primzahltests im Rahmen einer Laufzeituntersuchung betrachtet und die Frage beantwortet werden, ob der jeweilige Primzahltest dazu geeignet ist, Primzahlen zu finden, die groß genug sind, um bspw. in kryptographischen Verfahren weiterverwendet zu werden. Darüber hinaus bietet diese praktische Komponente die Chance, die Theorie zu reflektieren und leichter nachprüfbar zu machen.