Universität Siegen

Der quadratische Frobenius-Test

Autor:
Gary Colin Benner

Gutachter:
PD Dr. Jörg Jahnel
Dr. Jan Fricke

16. November 2014

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel 1

Einleitung

Die erste Frage, die sich bei der Betrachtung des vorliegenden Themas stellt, ist, warum man sich überhaupt mit probabilistischen Primzahltests auseinandersetzen sollte.

Zunächst einmal ist klar, dass es für vielerlei Zwecke nötig ist festzustellen, ob eine gegebene natürliche Zahl n eine Primzahl ist. Dies ist etwa für das korrekte Funktionieren kryptographischer Verfahren unerlässlich. Man kann dafür selbstverständlich einen deterministischen Test, etwa Probedivision oder den AKS-Primzahltest, verwenden. Auf den ersten Blick erscheint dies auch sinnvoll, schließlich bekommt man so sicher heraus, ob n prim ist.

In der Praxis ist es jedoch so, dass diese Tests, verglichen mit probabilistischen Tests, sehr hohe Laufzeiten haben. Muss man sich nicht absolut sicher sein, dass n prim ist, sondern ist man schon damit zufrieden, dies mit sehr hoher Wahrscheinlichkeit sagen zu können, ist es somit möglich, bei dem Test viel Zeit zu sparen. Zum Teil geht es dabei um so viel Zeit, dass die Verwendung eines (der bekannten) deterministischen Tests überhaupt nicht praktikabel wäre.

In der Kryptographie etwa begnügt man sich fast immer damit, dass die Wahrscheinlichkeit, dass eine Nachricht von Unbefugten entschlüsselt werden kann, sehr klein ist; so klein, dass man in der Praxis davon ausgehen kann, dass dies nicht geschieht. Es ist also nicht abwegig, sich bei der Verifikation eines Schlüssels darauf zu verlassen, dass ein probabilistischer Primzahltest mit ausreichend hoher Wahrscheinlichkeit eine zusammengesetzte Zahl als solche erkennen würde.

In dieser Arbeit soll ein moderner probabilistischer Primzahltest, der von Jon Grantham entwickelte *randomisierte quadratische Frobenius-Test* (RQFT) behandelt werden. Dieser Test ist grob vergleichbar mit dem Miller-Rabin-Primzahltest.

Aufgrund der theoretischen Laufzeitabschätzung sollte der RQFT bei gleicher Laufzeit wie drei Iterationen Miller-Rabin-Test eine Fehlerwahrscheinlichkeit von weniger als $\frac{1}{7710}$ bei zusammengesetzten Zahlen garantieren, wohingegen drei Iterationen des Miller-Rabin-Tests nur garantieren können, dass die Fehlerwahrscheinlichkeit kleiner als $\frac{1}{64}$ ist.

In dieser Arbeit werden zum einen die Beweise aus Granthams Artikel detailliert ausgearbeitet und nebenher einige kleinere Fehler korrigiert. Zum anderen wird der Algorithmus in `C` mithilfe von `GMP`[1] implementiert und getestet. Insbesondere wird die reale Laufzeit gemessen und mit der des Miller-Rabin-Tests verglichen.

[1] GNU Multiple Precision Arithmetic Library

1.1 Gliederung der Arbeit

Zunächst finden sich in Kapitel 2 relevante Definitionen und Sätze aus der Zahlentheorie, sowie eine Beschreibung des Miller-Rabin-Primzahltests. In Kapitel 3 wird der quadratische Frobenius-Test beschrieben und wichtige Eigenschaften desselben bewiesen, etwa, dass er Primzahlen stets als *wahrscheinlich prim* erkennt und dass zusammengesetzte Zahlen mit einer Wahrscheinlichkeit kleiner als $\frac{1}{7710}$ nicht als solche erkannt werden. Zudem werden wir dort eine asymptotische Abschätzung für die Laufzeit beweisen. In Kapitel 4 geht es dann um die Laufzeit und andere Eigenschaften der Implementierung. Schließlich folgt in Kapitel 5 eine kurze Zusammenfassung der Ergebnisse.

Kapitel 2

Grundlagen

Im Folgenden werden einige für den quadratischen Frobenius-Test benötigte Grundlagen aus der Zahlentheorie und der etablierte Miller-Rabin-Primzahltest behandelt. Anders als beim Miller-Rabin-Test genügt es für den Frobenius-Test nicht, Eigenschaften des endlichen Körpers $\mathbb{F}_p$ für eine Primzahl p zu benutzen. Stattdessen müssen wir den Erweiterungskörper $\mathbb{F}_{p^2} \cong \mathbb{F}_p(\sqrt{\Delta})$ über $\mathbb{F}_p$ für einen quadratischen Nichtrest Δ modulo p betrachten.

Da die zu testende Zahl auch zusammengesetzt sein kann, wird allgemein mit Polynomen vom Grad kleiner zwei über $\mathbb{Z}_n$ gerechnet. Gemeint ist damit der Restklassenring

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, \ldots, n-1 + n\mathbb{Z}\}.$$

Insbesondere sind, für Primzahlen p, mit $\mathbb{Z}_p$ niemals die p-adisch ganzen Zahlen gemeint.

Statt $x + n\mathbb{Z}$ schreiben wir der Einfachheit halber x. Damit ist außer der Restklasse auch der kleinste nicht-negative Repräsentant von $x + n\mathbb{Z}$ zu verstehen. Wir könnten also auch sagen, alle Zahlen aus $\mathbb{Z}_n$ seien modulo n reduziert.

2.1 Wichtige Definitionen und Sätze

Definition 2.1 (Eulersche φ-Funktion)**.** Die *Eulersche φ-Funktion* ist gegeben durch

$$\varphi(n) := \#\{\, x \in \mathbb{Z}_n \mid \mathrm{ggT}(n, x) = 1 \,\}.$$

Satz 2.2. *Sind p prim, $b, c \in \mathbb{Z}$ und ist $b^2 + 4c$ ein quadratischer Nichtrest modulo p, so ist*

$$\mathbb{Z}[x]/(p, x^2 - bx - c) \cong \mathbb{F}_p\big(\sqrt{b^2 + 4c}\big) \cong \mathbb{F}_{p^2}.$$

Beweis. Offensichtlich ist

$$\mathbb{Z}[x]/(p, x^2 - bx - c) \cong \mathbb{Z}_p[x]/(x^2 - bx - c) \cong \mathbb{F}_p[x]/(x^2 - bx - c).$$

Da die Lösungen von $x^2 - bx - c$ algebraisch vom Grad 2 über $\mathbb{F}_p$ sind, ist dies ein Modell für den endlichen Körper $\mathbb{F}_{p^2}$. □

Definition 2.3. Die *Norm* $N(x)$ von $x \in \mathbb{F}_q$ ist definiert durch

$$N(x) := \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \sigma(x),$$

wobei $q = p^k$ für eine Primzahl p und eine natürliche Zahl k ist.

Für diese Arbeit relevant ist der Fall $q = p^2$ für eine Primzahl p. Die Elemente von $\mathbb{F}_{p^2} \cong \mathbb{F}_p(\sqrt{\Delta})$, wobei Δ ein quadratischer Nichtrest modulo p ist, können wir dann schreiben als $x + \sqrt{\Delta}y$ mit $x, y \in \mathbb{F}_p$. Damit ist

$$N\big(x + \sqrt{\Delta}y\big) = \big(x + \sqrt{\Delta}y\big)\big(x - \sqrt{\Delta}y\big) = x^2 - \Delta y^2.$$

Definition 2.4 (Jacobi-Symbol)**.** Seien $m, p \in \mathbb{Z}$ und p eine ungerade Primzahl. Dann ist das *Jacobi-Symbol* $\left(\frac{m}{p}\right)$ definiert durch

$$\left(\frac{m}{p}\right) := \begin{cases} 1 & \text{falls } m \text{ ein quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{falls } m \text{ ein quadratischer Nichtrest modulo } p \text{ ist,} \\ 0 & \text{falls } p \text{ ein Teiler von } m \text{ ist.} \end{cases}$$

Für ein Produkt $n = p_1 \cdots p_k$ von ungeraden Primzahlen ist das Jacobi-Symbol $\left(\frac{m}{n}\right)$ definiert durch

$$\left(\frac{m}{n}\right) := \prod_{i=1}^{k} \left(\frac{m}{p_i}\right).$$

Aus der Definition folgt sofort, dass $\left(\frac{m}{n^2}\right) = \left(\frac{m}{n}\right)^2 \neq -1$ ist für alle $m, n \in \mathbb{Z}$, wobei n ungerade ist.

Da $\mathbb{F}_{p^2}$ eine algebraische Körpererweiterung zweiten Grades über $\mathbb{F}_p$ ist, ist die Galois-Gruppe $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ von Ordnung 2, also isomorph zu $\mathbb{Z}_2$. Den Erzeuger der Galois-Gruppe beschreibt der folgende Satz.

Satz 2.5 (Frobenius-Automorphismus)**.** *Seien p eine Primzahl und $\mathbb{F}_p(\alpha)$ eine einfache algebraische Erweiterung zweiten Grades des endlichen Körpers $\mathbb{F}_p$. Die Abbildung*

$$\phi\colon \mathbb{F}_p(\alpha) \to \mathbb{F}_p(\alpha),\ a \mapsto a^p$$

definiert einen Automorphismus von $\mathbb{F}_p(\alpha)$, den Frobenius-Automorphismus*.*

Der Frobenius-Automorphismus permutiert die Nullstellen des Minimalpolynoms von α und lässt die Elemente von $\mathbb{F}_p$ unverändert.

Beweis. Seien $a, b \in \mathbb{F}_p(\alpha)$ beliebig. Dann gilt

$$\phi(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = \phi(a) \cdot \phi(b)$$

und mit dem Binomischen Lehrsatz, wegen $p \mid \binom{p}{k}$ für alle $k \in \{1, \ldots, p-1\}$, auch

$$\phi(a + b) = (a + b)^p = a^p + b^p = \phi(a) + \phi(b).$$

Damit ist ϕ ein Körperhomomorphismus.

Weiterhin muss $\ker \phi = \{0\}$ sein, denn $\mathbb{F}_p(\alpha)$ ist ein Körper, hat also keine Nullteiler. Damit ist ϕ injektiv. Eine injektive Abbildung $A \to B$ zwischen zwei endlichen Mengen A und B gleicher Kardinalität ist aber schon bijektiv. Damit ist ϕ ein Automorphismus.

Da $\mathbb{F}_{p^2}$ eine algebraische Körpererweiterung vom Grad 2 über $\mathbb{F}_p$ ist, muss die Galois-Gruppe $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ (zyklisch) vom Grad 2 sein. Wir müssen also nur noch zeigen, dass ϕ nicht die identische Abbildung ist.

Wäre $\phi = \mathrm{id}$, dann hätten wir $a = \phi(a) = a^p$ für alle $a \in \mathbb{F}_{p^2}$. Dann wären alle $a \in \mathbb{F}_{p^2}$ Nullstellen des Polynoms $x^p - x$. Es gibt aber p^2 solche a, doch das Polynom hat nur Grad p. Da $\mathbb{F}_{p^2}$ ein Körper ist, kann das also nicht sein. Somit muss $\phi \neq \mathrm{id}$ sein.

Der einzige andere Automorphismus von $\mathbb{F}_{p^2}$ ist aber durch $\alpha \mapsto \beta$ gegeben, wobei β die zweite Nullstelle des Minimalpolynoms von α ist. ϕ vertauscht also die Nullstellen des Minimalpolynoms von α. □

Insbesondere bedeutet dies, dass der Frobenius-Automorphismus $\phi\colon \mathbb{F}_p(\sqrt{\Delta}) \to \mathbb{F}_p(\sqrt{\Delta})$ für einen quadratischen Nichtrest Δ modulo p charakterisiert ist durch $\phi(\sqrt{\Delta}) = -\sqrt{\Delta}$. Damit ist stets $N(x) = x \cdot \phi(x) = x^{p+1}$.

Lemma 2.6. *Seien $b, c \in \mathbb{F}_p$ mit $\left(\frac{-c}{p}\right) = 1$ und $\left(\frac{b^2+4c}{p}\right) = -1$ gegeben. Dann ist*

$$-c \equiv x^{p+1} \mod (p, x^2 - bx - c).$$

Beweis. Sei x_0 eine Nullstelle von $x^2 - bx - c$. Es gilt also $x_0^2 = bx_0 + c$. Nach Vieta ist die andere Nullstelle dann $b - x_0$. Laut Satz 2.5 auf der vorherigen Seite vertauscht der Frobenius-Automorphismus $x \mapsto x^p$ die beiden Nullstellen. Also ist

$$x_0^{p+1} \equiv x_0 x_0^p \equiv x_0(b - x_0) \equiv bx_0 - x_0^2 \equiv bx_0 - bx_0 - c \equiv -c \mod (p, x^2 - bx - c),$$

was zu zeigen war. □

Lemma 2.7. *Seien p eine Primzahl und $k \in \mathbb{N}$. Dann gibt es genau $\operatorname{ggT}(n, p^k - 1)$ Lösungen der Gleichung $x^n = 1$ in $\mathbb{F}_{p^k}$. Ist -1 eine n-te Potenz in $\mathbb{F}_{p^k}$, so gibt es auch genau $\operatorname{ggT}(n, p^k - 1)$ Lösungen der Gleichung $x^n = -1$ in $\mathbb{F}_{p^k}$.*

Beweis. Bekanntermaßen gibt es einen Isomorphismus $\log\colon \mathbb{F}_{p^k}^* \to \mathbb{Z}_{p^k-1}$, der gegeben ist durch $1 \mapsto 0$ und $g \mapsto 1$ für eine Primitivwurzel $g \in \mathbb{F}_{p^k}^*$. Jede Lösung x von $x^n = 1$ erfüllt also $n \cdot y \equiv 0 \bmod (p^k - 1)$, wobei $y = \log x$ ist. Die Lösungen y dieser Kongruenz sind offenbar $m \cdot \frac{p^k-1}{\operatorname{ggT}(n,p^k-1)}$ für $m = 1, \ldots, \operatorname{ggT}(n, p^k - 1)$. Es gibt damit auch genau $\operatorname{ggT}(n, p^k - 1)$ Lösungen der ursprünglichen Gleichung.

Nehmen wir nun an, dass -1 eine n-te Potenz in $\mathbb{F}_{p^k}$ ist, etwa $\zeta^n = -1$. Dann ist $x^n = -1$ genau dann, wenn $(\zeta x)^n = -x^n = 1$. Da $\mathbb{F}_{p^k}$ ein Körper ist, ist die Multiplikation mit ζ eine Bijektion. Durch die Substitution $\widetilde{x} = \zeta x$ stellen wir fest, dass es $\operatorname{ggT}(n, p^k - 1)$ Lösungen von $x^n = -1$ in $\mathbb{F}_{p^k}$ gibt, da es ebensoviele Lösungen von $\widetilde{x}^n = 1$ gibt. □

Definition 2.8. Sei $n \in \mathbb{Z}$ beliebig und k die Anzahl der Primfaktoren von n. Dann ist die *Möbius-Funktion* μ definiert durch

$$\mu(n) := \begin{cases} (-1)^k & \text{falls } n \text{ quadratfrei ist,} \\ 0 & \text{falls } n \text{ nicht quadratfrei ist.} \end{cases}$$

Lemma 2.9. *Sei $n \in \mathbb{N}$ ungerade. Dann gibt es genau $\varphi(n)^2$ Paare $(b, c) \in \mathbb{Z}_n^2$, so dass $\left(\frac{b^2+4c}{n}\right) \neq 0$ und $\left(\frac{-c}{n}\right) \neq 0$ ist.*

Beweis. Aus der Definition der Eulerschen φ-Funktion folgt sofort, dass es genau $\varphi(n)$ Zahlen $c \in \mathbb{Z}_n$ gibt, so dass n und $(-c)$ teilerfremd sind. Damit gibt es laut Definition des Jacobi-Symbols genau $\varphi(n)$ Zahlen $c \in \mathbb{Z}_n$, so dass $\left(\frac{-c}{n}\right) \neq 0$ ist.

Fall 1. Sei zunächst $n = p^k$, wobei $k \in \mathbb{N}$ und p eine Primzahl ist. Es ist

$$\left(\frac{b^2+4c}{p^k}\right) = \left(\frac{b^2+4c}{p}\right)^k = 0$$

genau dann, wenn $p \mid b^2 + 4c$. Wir müssen also die Anzahl der Nullstellen von $b^2 + 4c$ als Polynom in b über $\mathbb{Z}_p$ zählen.

Fall 1.1. Sei $(-c)$ ein Quadrat modulo p^k. Dann ist $b^2 + 4c = (b + 2\sqrt{-c})(b - 2\sqrt{-c})$. Als Polynom in b hat $b^2 + 4c$ also zwei Nullstellen über $\mathbb{Z}_p$, denn $2c$ und p sind, nach Voraussetzung, teilerfremd. Da $\mathbb{Z}_p$ ein Körper und $b^2 + 4c$ ein Polynom zweiten Grades ist, kann es keine weiteren Nullstellen geben. Es gibt also in $\mathbb{Z}_p$ genau $p - 2$ Zahlen b, so dass $\left(\frac{b^2+4c}{p^k}\right) \neq 0$ ist. Zu jedem solchen $b \in \mathbb{Z}_p$ gibt es in $\mathbb{Z}_{p^k}$ genau p^{k-1} Zahlen b' mit der gleichen Eigenschaft. Insgesamt gibt als also in $\mathbb{Z}_{p^k}$ genau $p^{k-1}(p-2)$ Zahlen $b \in \mathbb{Z}_{p^k}$ mit $\left(\frac{b^2+4c}{p^k}\right) \neq 0$.

Fall 1.2. Sei $(-c)$ kein Quadrat modulo p^k. Dann hat $b^2 + 4c \in \mathbb{Z}_p[b]$ keine Nullstellen. Damit ist für alle $b \in \mathbb{Z}_{p^k}$ automatisch $\left(\frac{b^2+4c}{p^k}\right) \neq 0$. Es gibt in diesem Fall also genau p^k Elemente $b \in \mathbb{Z}_{p^k}$, so dass $\left(\frac{b^2+4c}{p^k}\right) \neq 0$ ist.

Nun ist $-c$ ein Quadrat in genau der Hälfte der Fälle, in denen $\left(\frac{-c}{p^k}\right) \neq 0$ ist. Damit können wir zusammenfassend sagen, dass es

$$\frac{1}{2}\varphi(p^k)p^{k-1}(p-2) + \frac{1}{2}\varphi(p^k)p^k = \frac{1}{2}\varphi(p^k)p^{k-1}(2p-2) = \varphi(p^k)^2$$

Paare $(b, c) \in \mathbb{Z}_{p^k}^2$ gibt, so dass $\left(\frac{-c}{p^k}\right) \neq 0$ und $\left(\frac{b^2+4c}{p^k}\right) \neq 0$ sind.

Fall 2. Betrachten wir nun beliebige ungerade $n \in \mathbb{N}$. Diese können wir mit ungeraden Primzahlen p_i und natürlichen Zahlen ℓ_i, $i = 1, \ldots, k$, schreiben als $n = \prod_{i=1}^k p_i^{\ell_i}$.

Dann gibt es für jedes i in $\mathbb{Z}_{p_i^{\ell_i}}$ genau $\varphi(p_i^{\ell_i})^2$ Paare (b_i, c_i), so dass $\left(\frac{b_i^2+4c}{p_i^{\ell_i}}\right)$ und $\left(\frac{-c_i}{p_i^{\ell_i}}\right) \neq 0$ sind. Mit dem Chinesischen Restsatz können wir aus jeder Kombination solcher Paare $(b_1, c_1) \in \mathbb{Z}_{p_1^{\ell_1}}, (b_2, c_2) \in \mathbb{Z}_{p_2^{\ell_2}}, \ldots, (b_k, c_k) \in \mathbb{Z}_{p_k^{\ell_k}}$ ein Paar $(b, c) \in \mathbb{Z}_n^2$ konstruieren, so dass $(b, c) \equiv (b_i, c_i) \bmod (p_i^{\ell_i})$ für alle $-3 \leq i \leq k$ ist. Damit gibt es genau

$$\prod_{i=1}^k \varphi(p_i^{\ell_i})^2 = \varphi(n)^2$$

Paare $(b, c) \in \mathbb{Z}_n^2$, so dass $\left(\frac{b^2+4c}{n}\right) \neq 0$ und $\left(\frac{-c}{n}\right) \neq 0$ ist. □

Lemma 2.10. *Sei $(b, c) \in \mathbb{Z}_p^2$ ein zulässiges Paar, also $\left(\frac{b^2+4c}{p}\right) = -1$ und $\left(\frac{-c}{p}\right) = 1$. Dann ist x ein Quadrat modulo $(p, x^2 - bx - c)$.*

Beweis. Wir haben $\left(\frac{b+2\sqrt{-c}}{p}\right)\left(\frac{b-2\sqrt{-c}}{p}\right) = \left(\frac{b^2+4c}{p}\right) = -1$, so dass $b + 2\sqrt{-c}$ oder $b - 2\sqrt{-c}$ modulo p ein Quadrat ist.

Fall 1. Sei $b + 2\sqrt{-c}$ ein Quadrat modulo p und $\beta^2 = b + 2\sqrt{-c}$. Dann ist

$$\left(\frac{1}{\beta}x + \frac{\sqrt{-c}}{\beta}\right)^2 \equiv \frac{1}{b+2\sqrt{-c}}(x^2 + 2\sqrt{-c}x - c) \equiv \frac{1}{b+2\sqrt{-c}}(bx + c + 2\sqrt{-c}x - c)$$
$$\equiv \frac{b+2\sqrt{-c}}{b+2\sqrt{-c}}x \equiv x \mod (p, x^2 - bx - c),$$

also x ein Quadrat modulo $(n, x^2 - bx - c)$.

Fall 2. Ist $\beta^2 = b - 2\sqrt{-c}$ für ein $\beta \in \mathbb{Z}_p$, so haben wir, analog zu Fall 1,

$$\left(\frac{1}{\beta}x + \frac{\sqrt{-c}}{\beta}\right)^2 \equiv x \mod (p, x^2 - bx - c). \qquad \square$$

2.2 Der Miller-Rabin-Test

In aller Kürze definieren wir noch den starken Pseudoprimzahl- oder Miller-Rabin-Test.

Algorithmus 2.11 (Miller-Rabin-Test)**.** Sei eine ungerade ganze Zahl $n = 2^r s + 1 \in \mathbb{Z}$ gegeben, wobei s ungerade ist.

Wähle zufällig eine ganze Zahl a mit $1 \leq a < n$. Ist $a^s \equiv 1 \bmod n$ oder $a^{2^j} s \equiv -1 \bmod n$ für ein $0 \leq j < r$, so könnte n prim sein, andernfalls ist n zusammengesetzt.

Definition 2.12. (a) Ein Testparameter ist ein *Zeuge* für die Zusammengesetztheit von n, wenn der Test bei Verwendung dieses Parameters das Ergebnis *zusammengesetzt* liefert.

(b) Eine Zahl n *besteht* den starken Pseudoprimzahl-Test mit Parameter a, wenn a kein Zeuge für die Zusammengesetztheit von n ist.

Satz 2.13. *Für jede ungerade Primzahl $p = 2^r s + 1$ und eine beliebige ganze Zahl $1 \leq a < p$ ist $a^s \equiv 1 \bmod p$ oder $a^{2^j s} \equiv -1 \bmod p$ für ein $0 \leq j < r$.*

Beweis. Sei $a \in \mathbb{F}_p^*$ beliebig. Mit $\#\mathbb{F}_p^* = p - 1$ folgt aus dem Satz von Lagrange, dass $a^{2^r s} = a^{p-1} = 1$ ist. Weil $\mathbb{F}_p$ ein Körper und $y^2 - 1$ ein Polynom zweiten Grades in y ist, gibt es genau zwei $x \in \mathbb{F}_p$, so dass $x^2 = 1$ ist. Dies sind offensichtlich $x = 1$ und $x = -1$. Dann folgt aber, für alle $1 \leq j \leq r$, aus $a^{2^j s} = 1$, dass $a^{2^{j-1} s} \in \{-1, 1\}$ ist. Also haben wir entweder $a^{2^{j-1} s} = 1$ für jedes solche j und damit insbesondere $x^{2^0 s} = x^s = 1$, oder es muss ein $0 \leq j < r$ geben, so dass $x^{2^j s} = -1$ ist. Also besteht jede Primzahl den Miller-Rabin-Test mit einem beliebigen Parameter a. $\square$

Satz 2.14. *Sei $n \in \mathbb{N}$ eine ungerade zusammengesetzte Zahl. Die Wahrscheinlichkeit, dass eine zufällig gewählte Zahl $1 \leq a < n$ kein Zeuge für die Zusammengesetztheit von n ist, ist höchstens $\frac{1}{4}$.*

Beweis. Siehe [Rab80, Theorem 1]. $\square$

Kapitel 3

Der Quadratische Frobenius-Test

Zunächst werden in diesem Kapitel der (randomisierte) quadratische Frobenius-Test und einige Begriffe eingeführt. Anschließend wird gezeigt, dass der Test Primzahlen niemals für zusammengesetzt hält, dass geeignete Parameter mit sehr hoher Wahrscheinlichkeit gewählt werden können und zuletzt eine obere Schranke für die Wahrscheinlichkeit dafür, dass der Test eine zusammengesetzte Zahl fälschlicherweise nicht als solche erkennt.

3.1 Definitionen und Korrektheit

Definition 3.1. Ein Paar $(b, c) \in \mathbb{Z}_n^2$ heißt *zulässig*, falls $\left(\frac{b^2+4c}{n}\right) = -1$ und $\left(\frac{-c}{n}\right) = 1$ ist.

Beginnen wir zunächst mit der Beschreibung des deterministischen Teils des Tests.

Algorithmus 3.2 (Vorberechnung)**.** Sei $n > 1$ eine ungerade ganze Zahl und sei $B \in \mathbb{N}$. Dann besteht die *Vorberechnung* für den quadratischen Frobenius-Test aus den Schritten

(1) Ist n durch eine der Primzahlen $p \leq \min\{B, \sqrt{n}\}$ teilbar, so ist n *zusammengesetzt.*

(2) Ist n eine Quadratzahl, so ist n *zusammengesetzt.*

Diese Vorberechnung ist aus zwei Gründen wichtig. Zum einen gibt es für Quadratzahlen n keine zulässigen Parameterpaare $(b, c) \in \mathbb{Z}_n^2$, da $\left(\frac{x}{k^2}\right) = \left(\frac{x}{k}\right)^2 \neq -1$ für alle $x \in \mathbb{Z}$ ist. Dadurch müsste der probabilistische Teil des Tests diese stets als *wahrscheinlich prim* klassifizieren. Zum anderen setzen die Beweise der oberen Schranken für die Fehlerwahrscheinlichkeit in Abschnitt 3.3 voraus, dass n keine Primfaktoren p unterhalb einer gewissen Schranke B hat. Durch die Probedivision wird sichergestellt, dass zusammengesetzte Zahlen n mit solchen kleinen Primfaktoren stets als zusammengesetzt erkannt werden.

Algorithmus 3.3 (Quadratischer Frobenius-Test (QFT))**.** Seien $b, c \in \mathbb{Z}_n \setminus \{0\}$ und $B \in \mathbb{N}$. Angenommen $n > 1$ ist ungerade, $\left(\frac{b^2+4c}{n}\right) = -1$ und $\left(\frac{-c}{n}\right) = 1$.

Der *quadratische Frobenius-Test (QFT) mit Parametern* (b, c) besteht aus den folgenden Schritten, die der Reihe nach ausgeführt werden, bis entweder ein Schritt das Ergebnis n *ist zusammengesetzt* liefert, oder alle Schritte abgearbeitet wurden.

Wird n bei der Vorberechnung als zusammengesetzt erkannt, so ist n *zusammengesetzt.*

(3) Ist $\left(x^{\frac{n+1}{2}} \bmod (n, x^2 - bx - c)\right) \notin \mathbb{Z}_n$, so ist n *zusammengesetzt.*

(4) Ist $x^{n+1} \not\equiv -c \bmod (n, x^2 - bx - c)$, so ist n *zusammengesetzt*.

(5) Sei $n^2 - 1 = 2^r s$, wobei s ungerade ist. Ist sowohl $x^s \not\equiv 1 \bmod (n, x^2 - bx - c)$, als auch $x^{2^j s} \not\equiv -1 \bmod (n, x^2 - bx - c)$ für alle $0 \leq j \leq r-2$, so ist n *zusammengesetzt*.

Wurde in keinem dieser Schritte festgestellt, dass n zusammengesetzt ist, so ist n *wahrscheinlich prim*.

Bemerkung 3.4. Im Beweis zu Theorem 3.16 werden wir sehen, dass wir $B = 44\,958$ wählen können.

Definition 3.5. (a) Wir nennen ein Paar $(b, c) \in \mathbb{Z}_n^2$ einen *Zeugen* für die Zusammengesetztheit von n, wenn der Quadratische Frobenius-Test mit Parametern (b, c) angewandt auf n das Ergebnis *zusammengesetzt* liefert.

(b) Ist (b, c) kein solcher Zeuge, so sagen wir, dass n den QFT mit Parametern (b, c) *besteht*.

Nun können wir aus den Schritten (1) bis (5) auf die folgende Art einen probabilistischen Primzahltest konstruieren.

Algorithmus 3.6 (Randomisierter Quadratischer Frobenius-Test (RQFT))**.** Die folgenden Schritte beschreiben k Iterationen des *Randomisierten Quadratischen Frobenius-Tests* für eine ungerade ganze Zahl $n > 1$.

(i) Wird bei der deterministischen Vorberechnung n als zusammengesetzt erkannt, so beende den Test mit dem Ergebnis *zusammengesetzt*.

(ii) Führe die folgenden Schritte höchstens k mal aus. Wurde n bei keiner dieser k Iterationen als zusammengesetzt erkannt, so beende den Test mit dem Ergebnis *wahrscheinlich prim*.

(iii) Wähle bis zu B mal ein zufälliges Paar $(b, c) \in \{1, 2, \ldots, n-1\}^2$. Ist in einem dieser Fälle $\operatorname{ggT}(b^2 + 4c, n)$, $\operatorname{ggT}(b, n)$ oder $\operatorname{ggT}(c, n)$ nicht in $\{1, n\}$, so beende den Test mit dem Ergebnis *zusammengesetzt*. Ist $\left(\frac{b^2+4c}{n}\right) = -1$ und $\left(\frac{-c}{n}\right) = 1$, so fahre fort mit Schritt (iv).

(iv) Führe die Schritte (3), (4) und (5) des QFT mit den Parametern (b, c) durch.

Beende den Test mit dem Ergebnis *zusammengesetzt*, falls der QFT das Ergebnis *zusammengesetzt* liefert. Gehe andernfalls zu Schritt (iii).

Bemerkung 3.7. (a) Der hier beschriebene Algorithmus unterscheidet sich leicht von dem in [Gra98]. In jenem wird ein Parameterpaar (b, c) gesucht, bevor die Schritte (1) und (2) durchgeführt werden. Ein solches Paar gibt es aber für eine Quadratzahl n nicht, denn $\left(\frac{b^2+4c}{m^2}\right)$ ist nicht-negativ für alle ungeraden $m \in \mathbb{Z}$. Dadurch werden alle Quadratzahlen fälschlicherweise als *wahrscheinlich prim* deklariert.

(b) Die Konstante B wird hier in zwei Rollen benutzt. Zum einen wird per Probedivision die Teilbarkeit von n durch jede der Primzahlen $p < B$ getestet. Zum anderen ist die maximale Anzahl der Versuche, ein zulässiges Parameterpaar (b, c) zu finden durch B gegeben. Für den zweiten Zweck könnte man eine weitere Konstante C einführen, von der man lediglich fordern muss, dass sie hinreichend groß ist. Schon $C = 10\,000$ wäre möglich. C größer zu machen macht die Abschätzungen in den folgenden Beweisen etwas einfacher, so dass wir zur Vereinfachung auch $C := B$ wählen können.

Im Folgenden soll die Korrektheit des Algorithmus nachgewiesen werden. Dazu wird zunächst gezeigt, dass alle ungeraden Primzahlen den QFT mit beliebigen Parametern und damit auch den RQFT bestehen.

Satz 3.8 (Korrektheit)**.** *Jede ungerade Primzahl p mit $\left(\frac{b^2+4c}{p}\right) = -1$ und $\left(\frac{-c}{p}\right) = 1$ für ein Paar $(b, c) \in \mathbb{Z}_p^2$ besteht den Quadratischen Frobenius-Test mit Parametern (b, c).*[1]

Beweis. Beweis durch Fallunterscheidung nach den einzelnen Schritten des Algorithmus:

Da p eine Primzahl ist, ist p sicherlich durch keine Zahl $1 < k < p$ teilbar. Damit kann p weder von Schritt (1) noch von Schritt (2) als zusammengesetzt deklariert werden.

Schritt (3): Aus Lemma 2.6 auf Seite 5 wissen wir, dass $-c \equiv x^{p+1} \bmod (p, x^2 - bx - c)$ ist. Da p ungerade ist, ist $p + 1$ gerade. Es ist also $-c \equiv (\pm x^k)^2 \bmod (p, x^2 - bx - c)$ mit $k = \frac{p+1}{2} \in \mathbb{Z}$. Da $\mathbb{F}_p$ und $\mathbb{F}_{p^2}$ Körper sind, gibt es jeweils höchstens zwei Lösungen der Gleichung $x^2 = -c$. Wir haben gesehen, dass es in $\mathbb{F}_{p^2}$ zwei Lösungen gibt. Da sich beide Lösungen nur durch ein Vorzeichen unterscheiden, sind entweder beide, oder keine der beiden Lösungen in $\mathbb{F}_p$. Die Voraussetzung $\left(\frac{-c}{p}\right) = 1$ besagt gerade, dass es eine Lösung in $\mathbb{F}_p$ gibt. Damit ist $x^{\frac{p+1}{2}} \in \mathbb{F}_p$, p besteht also Schritt (3).

Schritt (4): Nach Lemma 2.6 besteht p offensichtlich auch diesen Schritt.

Schritt (5): Wir wissen aus Lemma 2.10 auf Seite 6, dass x ein Quadrat modulo p ist, etwa $y^2 \equiv x$ für ein $y \in \mathbb{Z}[x]/(p, x^2 - bx - c)$. Mit dem Satz von Lagrange erhalten wir also, da $\mathbb{Z}[x]/(p, x^2 - bx - c) \cong \mathbb{F}_{p^2}$ und $\#\mathbb{F}_{p^2}^* = p^2 - 1$ ist,

$$x^{2^{r-1}s} \equiv y^{2^r s} = y^{p^2-1} \equiv 1 \mod (p, x^2 - bx - c).$$

Dann ist natürlich auch $x^{2^r s} = 1^2 = 1$. Nun gibt es, da $\mathbb{Z}_p$ ein Körper und $y^2 - 1$ ein Polynom zweiten Grades ist, genau die zwei Lösungen $y_1 = 1$ und $y_2 = -1$ von $y^2 - 1 = 0$. Ist $x^{2^j s} = 1$ für ein $j \in \{1, \ldots, r\}$, so ist $x^{2^{j-1}s} \in \{-1, 1\}$. Somit muss entweder für alle $0 \leq j < p - 1$ gelten, dass $x^{2^j s} \equiv 1 \bmod (p, x^2 - bx - c)$ ist, also insbesondere $x^s \equiv 1 \bmod (p, x^2 - bx - c)$, oder $x^{2^j s} \equiv -1 \bmod (p, x^2 - bx - c)$ für ein $j \in \{0, \ldots, p - 2\}$. Dies bedeutet schlicht, dass p auch Schritt (5) besteht. □

3.2 Zulässige Parameterpaare

In diesem Abschnitt wird eine untere Schranke für die Anzahl der zulässigen Parameterpaare (b, c) modulo n bestimmt. Dazu wird eine Schranke für die Anzahl zulässiger Parameterpaare für Primzahlen (Satz 3.9), quadratfreie Zahlen (Satz 3.10) und schließlich für zusammengesetzte Zahlen, die keine Quadrate sind (Satz 3.11), gezeigt.

Satz 3.9. *Seien $p \neq 2$ prim und $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$. Ist $\varepsilon_1 \neq \varepsilon_2$, so gibt es $\frac{(p-1)^2}{4}$ Paare (b, c) modulo p, so dass $\left(\frac{b^2+4c}{p}\right) = \varepsilon_1$ und $\left(\frac{-c}{p}\right) = \varepsilon_2$, andernfalls sind es $\frac{(p-1)^2}{4} - \varepsilon_1 \frac{p-1}{2}$ derartige Paare.*[2]

Beweis. Sei r ein beliebiger quadratischer Nichtrest modulo p, also $r \in \mathbb{Z}$ und $\left(\frac{r}{p}\right) = -1$. Setze

$$R := \begin{cases} 1 & \varepsilon_2 = 1 \\ r & \varepsilon_2 = -1 \end{cases} \text{ und } S := \begin{cases} 1 & \varepsilon_1 = 1 \\ r & \varepsilon_1 = -1 \end{cases}.$$

[1] vgl. Proposition 2.1 in [Gra98].
[2] vgl. Proposition 2.2 in [Gra98].

Dann gibt es 4 Paare (x, y) mit

$$-c = Rx^2 \qquad (3.1) \qquad \text{und} \qquad b^2 + 4c = Sy^2. \qquad (3.2)$$

R ist so gewählt, dass es eine Lösung x von Gleichung (3.1) gibt. Dann ist $(-x)$ ebenfalls eine Lösung der Gleichung. Entsprechend haben wir S so gewählt, dass es eine Lösung y von Gleichung (3.2) gibt. Also gibt es genau vier simultane Lösungen, nämlich (x, y), $(x, -y)$, $(-x, y)$ und $(-x, -y)$. Da $\mathbb{Z}_p$ ein Körper ist und die Lösungen Nullstellen von Polynomen zweiten Grades sind, kann es keine weiteren Lösungen geben.

Andersherum folgt aus Gleichung (3.1) und Gleichung (3.2) sofort, dass $\left(\frac{-c}{p}\right) = \varepsilon_2$ beziehungsweise $\left(\frac{b^2+4c}{p}\right) = \varepsilon_1$ ist.

Durch Einsetzen von (3.1) in (3.2) erhält man $b^2 = R(2x)^2 + Sy^2$. Die Anzahl N der Paare $(b, c) \in \mathbb{Z}_p^2$ mit der geforderten Eigenschaft können wir also bestimmen durch

$$N_{\varepsilon_1,\varepsilon_2} = \frac{1}{4}\#\Big\{ (b, x, y) \in \mathbb{Z}_p^3 \;\Big|\; x, y \neq 0,\ b^2 = R(2x)^2 + Sy^2 \Big\},$$

wobei aus (3.1) und $\left(\frac{-c}{p}\right) \neq 0$, also $-c \neq 0$, folgt, dass $x \neq 0$ sein muss. Entsprechend erhalten wir aus $\left(\frac{b^2+4c}{p}\right) \neq 0$ und (3.2), dass $y \neq 0$ sein muss.

Fall 1. Sei $\varepsilon_1 \neq \varepsilon_2$. Hier müssen wir also die Anzahl der Lösungen von $x^2 + ry^2 = z^2$ für $\varepsilon_1 = 1$ beziehungsweise $rx^2 + y^2 = z^2$ für $\varepsilon_1 = -1$ zählen. Aufgrund der offensichtlichen Symmetrie ist also

$$\begin{aligned}
N_{1,-1} = N_{-1,1} &= \frac{1}{4}\#\{ (x, y, z) \in \mathbb{Z}_p^3 \mid x, y \neq 0,\ rx^2 + y^2 = z^2 \} \\
&= \frac{1}{4}\#\{ (x, y, z) \in \mathbb{Z}_p^3 \mid x, y \neq 0,\ (z + y)(z - y) = rx^2 \} \\
&= \frac{1}{4}\#\{ (x, a, b) \in \mathbb{Z}_p^3 \mid x, a - b \neq 0,\ ab = rx^2 \} \\
&= \frac{1}{4}\#\{ (x, a, b) \in \mathbb{Z}_p^3 \mid x, a \neq 0,\ b = rx^2a^{-1} \} \\
&= \frac{1}{4}\#\{ (x, a) \in \mathbb{Z}_p^2 \mid a, x \neq 0 \} \\
&= \frac{(p-1)^2}{4},
\end{aligned}$$

wobei wir $a := z + y$ und $b := z - y$ setzen. Dann ist $y = 0 \iff a \neq b$.

Fall 2. Für $\varepsilon_1 = \varepsilon_2 = 1$ haben wir $S = R = 1$, also

$$N_{1,1} = \frac{1}{4}\#\{ (x, y, z) \in \mathbb{Z}_p^3 \mid x, y \neq 0,\ x^2 + y^2 = z^2 \}.$$

Nun ist $x^2 + y^2 = z^2$ äquivalent zu $(z + y)(z - y) = x^2$. Setzen wir auch hier $a := z + y$ und $b := z - y$. Da genau dann $x \neq 0$ ist, wenn wir $a, b \neq 0$ haben, folgt daraus

$$\begin{aligned}
N_{1,1} &= \frac{1}{4}\#\{ (x, a, b) \in \mathbb{Z}_p^3 \mid a, b \neq 0,\ a \neq b,\ ab = x^2 \} \\
&= \frac{1}{4}\#\{ (x, a, b) \in \mathbb{Z}_p^3 \mid a, x \neq 0,\ b = x^2a^{-1},\ b \neq x \} \\
&= \frac{1}{4}\#\{ (x, a) \in \mathbb{Z}_p^2 \mid x \neq 0,\ 0 \neq a \neq \pm x \}
\end{aligned}$$

$$= \frac{1}{4}\sum_{a=1}^{p-1} \#\{\, x \in \mathbb{Z}_p \mid x \neq 0, a, -a \,\}$$
$$= \frac{(p-1)(p-3)}{4} = \frac{(p-1)^2}{4} - \frac{p-1}{2}.$$

Fall 3. Aus Lemma 2.9 auf Seite 5 wissen wir, dass

$$N_{1,1} + N_{1,-1} + N_{-1,1} + N_{-1,-1} = \varphi(p)^2 = (p-1)^2$$

ist. Damit erhalten wir

$$\begin{aligned} N_{-1,-1} &= (p-1)^2 - N_{1,1} - N_{1,-1} - N_{-1,1} \\ &= (p-1)^2 - \frac{(p-1)^2}{4} + \frac{p-1}{2} - \frac{(p-1)^2}{4} - \frac{(p-1)^2}{4} \\ &= \frac{(p-1)^2}{4} - \varepsilon_1 \frac{p-1}{2}, \end{aligned}$$

was zu zeigen war. □

Satz 3.10. *Sei n ungerade und quadratfrei und seien $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$. Ist $\varepsilon_1 \neq \varepsilon_2$, so gibt es $\frac{1}{4}\varphi(n)^2$ Paare (b, c) modulo n mit $\left(\frac{b^2+4c}{n}\right) = \varepsilon_1$ und $\left(\frac{-c}{n}\right) = \varepsilon_2$. Andernfalls sind es $\frac{1}{4}\varphi(n)^2 + \frac{\varepsilon_1}{2}\mu(n)\varphi(n)$ solche Paare.*[3]

Beweis. Sei $n = p_1 \cdots p_k$ für Primzahlen $p_1, \ldots, p_k$. Beweis durch Induktion über k.

Induktfionsanfang. Sei $k = 1$. Nach Satz 3.9 gilt für die Anzahl $N_{\varepsilon_1,\varepsilon_2}(p)$ von Paaren (b, c) modulo p mit $\left(\frac{b^2+4c}{p}\right) = \varepsilon_1$ und $\left(\frac{-c}{p}\right) = \varepsilon_2$, dass

$$N_{\varepsilon_1,\varepsilon_2}(p) = \frac{(p-1)^2}{4} = \frac{1}{4}\varphi(p)^2$$

ist, falls $\varepsilon_1 \neq \varepsilon_2$ und andernfalls

$$N_{\varepsilon_1,\varepsilon_2}(p) = \frac{(p-1)^2}{4} - \varepsilon_1\frac{p-1}{2} = \frac{1}{4}\varphi(p)^2 + \frac{\varepsilon_1}{2}(-1)\varphi(p)$$

und somit, da $\mu(p) = -1$ ist für jede Primzahl p,

$$N_{\varepsilon_1,\varepsilon_2}(p) = \frac{1}{4}\varphi(p)^2 + \frac{\varepsilon_1}{2}\mu(p)\varphi(p).$$

Induktionsschritt. Sei $m = p_1 \cdots p_k$ und $p = p_{k+1}$ für ein $k \in \mathbb{N}$ und eine Primzahl p_{k+1}. Die Behauptung gelte für k, dass heißt

$$\begin{aligned} N_{1,1}(m) &= \frac{1}{4}\varphi(m)^2 + \frac{1}{2}\mu(m)\varphi(m) \\ N_{-1,-1}(m) &= \frac{1}{4}\varphi(m)^2 - \frac{1}{2}\mu(m)\varphi(m) \\ N_{1,-1}(m) &= N_{-1,1}(m) = \frac{1}{4}\varphi(m)^2. \end{aligned}$$

[3] vgl. Proposition 2.3 in [Gra98].

Fall 1. Sei $\varepsilon_1 = \varepsilon_2$. Nach Induktionsvoraussetzung ist

$$\begin{aligned}
N_{\varepsilon_1,\varepsilon_2}(mp) &= N_{\varepsilon_1,\varepsilon_2}(m)N_{1,1}(p) + N_{-\varepsilon_1,\varepsilon_2}(m)N_{-1,1}(p) \\
&\quad + N_{\varepsilon_1,-\varepsilon_2}(m)N_{1,-1}(p) + N_{-\varepsilon_1,-\varepsilon_2}(m)N_{-1,-1}(p) \\
&= \left(\frac{1}{4}\varphi(m)^2 + \frac{\varepsilon_1}{2}\mu(m)\varphi(m)\right)\left(\frac{\varphi(p)^2}{4} - \frac{\varphi(p)}{2}\right) + \frac{1}{4}\varphi(m)^2\frac{\varphi(p)^2}{4} \\
&\quad + \frac{1}{4}\varphi(m)^2\frac{\varphi(p)^2}{4} + \left(\frac{1}{4}\varphi(m)^2 - \frac{\varepsilon_1}{2}\mu(m)\varphi(m)\right)\left(\frac{\varphi(p)^2}{4} + \frac{\varphi(p)}{2}\right) \\
&= \frac{1}{4}\varphi(m)^2\varphi(p)^2 - \frac{\varepsilon_1\mu(m)\varphi(m)\varphi(p)}{2} \\
&= \frac{1}{4}\varphi(mp)^2 + \frac{\varepsilon_1}{2}\mu(mp)\varphi(mp).
\end{aligned}$$

Hierbei verwenden wir die Voraussetzung, dass n quadratfrei sein soll, denn dies impliziert, dass m und p teilerfremd sind. Damit ist $\varphi(m)\varphi(p) = \varphi(mp)$. Weiterhin verwenden wir, dass in diesem Fall $\mu(m) = -\mu(mp)$ ist.

Fall 2. Sei $\varepsilon_1 \neq \varepsilon_2$. Analog zum vorherigen Fall erhält man nach Induktionsvoraussetzung

$$\begin{aligned}
N_{\varepsilon_1,\varepsilon_2}(mp) &= N_{\varepsilon_1,\varepsilon_2}(m)N_{1,1}(p) + N_{-\varepsilon_1,\varepsilon_2}(m)N_{-1,1}(p) \\
&\quad + N_{\varepsilon_1,-\varepsilon_2}(m)N_{1,-1}(p) + N_{-\varepsilon_1,-\varepsilon_2}(m)N_{-1,-1}(p) \\
&= \frac{1}{4}\varphi(m)^2\left(\frac{\varphi(p)^2}{4} - \frac{\varphi(p)}{2}\right) + \left(\frac{1}{4}\varphi(m)^2 - \frac{\varepsilon_1}{2}\mu(m)\varphi(m)\right)\frac{\varphi(p)^2}{4} \\
&\quad + \left(\frac{1}{4}\varphi(m)^2 + \frac{\varepsilon_1}{2}\mu(m)\varphi(m)\right)\frac{\varphi(p)^2}{4} + \frac{1}{4}\varphi(m)^2\left(\frac{\varphi(p)^2}{4} + \frac{\varphi(p)}{2}\right) \\
&= \frac{1}{4}\varphi(m)^2\varphi(p)^2 = \frac{1}{4}\varphi(mp)^2.
\end{aligned}$$

□

Satz 3.11. *Sei n ungerade, zusammengesetzt und kein Quadrat. Sei $M(n)$ die Anzahl der Paare (b,c) modulo n mit $\left(\frac{b^2+4c}{n}\right) = -1$ und $\left(\frac{-c}{n}\right) = 1$, oder $n > \mathrm{ggT}(b^2+4c, n) > 1$ oder $n > \mathrm{ggT}(c,n) > 1$. Dann ist $M(n) > \frac{n^2}{4}$.*[4]

Beweis. Wir schreiben $n = n_0\prod_{i=1}^{k} p_i^2$ mit $k \in \mathbb{N}_0$, $n_0 \in \mathbb{N}$ quadratfrei und p_i Primzahlen für $i \in \{1,\ldots,k\}$. Seien $\varepsilon_1 := \left(\frac{b^2+4c}{n}\right)$ und $\varepsilon_2 := \left(\frac{-c}{n}\right)$.

Sei $\widetilde{M}(n) := n^2 - M(n)$ die Anzahl der Paare $(b,c) \in \mathbb{Z}_n^2$, so dass $(\varepsilon_1,\varepsilon_2) \neq (-1,1)$ und $\mathrm{ggT}(b^2+4c,n), \mathrm{ggT}(c,n) \in \{1,n\}$.

Induktionsanfang. Laut Lemma 2.9 auf Seite 5 gibt es genau $\varphi(n)^2$ Paare $(b,c) \in \mathbb{Z}_n^2$, so dass $\varepsilon_1, \varepsilon_2 \neq 0$ sind, wovon genau $\frac{1}{4}\varphi(n)^2$ die Eigenschaft $(\varepsilon_1,\varepsilon_2) = (-1,1)$ haben. Damit gibt es $\frac{3}{4}\varphi(n)^2$ Paare (b,c) mit $(\varepsilon_1,\varepsilon_2) \neq (-1,1)$ und $\mathrm{ggT}(b^2+4c,n) = \mathrm{ggT}(c,n) = 1$, also $\varepsilon_1, \varepsilon_2 \neq 0$.

Zusätzlich gibt es genau die n Paare $(b, -4^{-1}b^2)$ mit $n \mid b^2+4c$ und genau die n Paare $(b,0)$ mit $n \mid c$. Das Paar $(0,0)$ ist in beiden Fällen enthalten. Damit gibt es exakt $2n-1$

[4] vgl. Proposition 2.4 in [Gra98].

Paare $(b,c) \in \mathbb{Z}_n^2$, so dass $\mathrm{ggT}(b^2+4c,n) = n$ oder $\mathrm{ggT}(c,n) = n$. Also ist

$$\widetilde{M}(n) = \frac{3}{4}\varphi(n)^2 + 2n - 1 \leq \frac{3}{4}(n-2)^2 + 2n - 1 = \frac{3}{4}n^2 - n + 2 < \frac{3}{4}n^2,$$

da $n > 2$ ist. Daraus folgt sofort $M(n) > \frac{n^2}{4}$.

Induktionsschritt. Sei $n = n_0 \prod_{i=1}^{k-1} p_i^2$ und $M(n) > \frac{n^2}{4}$. Sei $p := p_k$. Wir müssen zeigen, dass $M(np^2) > \frac{(np^2)^2}{4}$ ist. Dafür genügt es zu zeigen, dass $\widetilde{M}(np^2) < \frac{3}{4}(np^2)^2$ ist.

Fall 1. Ist p kein Teiler von n, so können wir $\widetilde{M}(np^2)$ mithilfe des Chinesischen Restsatzes berechnen. Es gilt dann

$$\frac{\varphi\big(np^2\big)^2}{\varphi(n)^2} = \frac{\varphi(n)^2\varphi\big(p^2\big)^2}{\varphi(n)^2} = \varphi\big(p^2\big)^2,$$

also $\widetilde{M}(np^2) = \varphi\big(p^2\big)^2 \frac{3}{4}\varphi(n)^2 = \frac{3}{4}\varphi\big(np^2\big)^2$. Wegen $n^2 = M(n) + \widetilde{M}(n)$ für alle n, folgt in diesem Fall die Behauptung.

Fall 2. Sei p ein Teiler von n. Schreibe $n = n_0 p^\ell$ mit $p \nmid n_0$ und $\ell \in \mathbb{N}$. Sei weiterhin $(b',c') \in \mathbb{Z}_n^2$ ein zulässiges Paar.

Wir können jedes $x \in \mathbb{Z}_{p^\ell}$ eindeutig schreiben als

$$x = x_0 + px_1 + p^2x_2 + \cdots + p^{\ell-1}x_{\ell-1}$$

mit $x_0, \ldots, x_{\ell-1} \in \mathbb{Z}_p$. Ebenso können wir jedes $y \in \mathbb{Z}_{p^{\ell+2}}$ schreiben als

$$y = y_0 + py_1 + p^2y_2 + \cdots + p^{\ell-1}y_{\ell-1} + p^\ell y_\ell + p^{\ell+1}y_{\ell+1}.$$

mit $y_0, \ldots, y_{\ell+1} \in \mathbb{Z}_p$. Offensichtlich gibt es also zu jedem $x \in \mathbb{Z}_{p^\ell}$ genau p^2 Zahlen $y \in \mathbb{Z}_{p^{\ell+2}}$ mit $x \equiv y \bmod p^\ell$. Nach dem Chinesischen Restsatz gibt es also zu jeder Zahl $x \in \mathbb{Z}_n$ genau p^2 Zahlen $y \in \mathbb{Z}_{np^2}$, so dass $x \equiv y \bmod np^2$. Zu jedem Paar $(b',c') \in \mathbb{Z}_n^2$ gibt es daher $\big(p^2\big)^2 = p^4$ Paare $(b,c) \in \mathbb{Z}_{np^2}^2$, so dass $(b,c) \equiv (b',c') \bmod n$.

Damit ist

$$\widetilde{M}(np^2) = p^4\widetilde{M}(n) < p^4\frac{3}{4}\varphi(n)^2 = \frac{3}{4}\big(\varphi\big(n_0p^\ell\big)p^2\big)^2 = \frac{3}{4}\varphi\big(n_0p^{\ell+2}\big)^2 = \frac{3}{4}\varphi\big(np^2\big)^2,$$

woraus unsere Behauptung $M(np^2) = n^2 - \widetilde{M}(np^2) > \frac{(np^2)^2}{4}$ folgt. □

Korollar 3.12. *Die Wahrscheinlichkeit kein geeignetes Paar* $(b,c) \in \{1,\ldots,n-1\}^2$ *in Schritt* (iii) *des* RQFT *zu finden ist kleiner als* $\big(\frac{3}{4} + \frac{2}{B^2}\big)^B$.[5]

Beweis. Nach Satz 3.11 ist mehr als $\frac{1}{4}$ aller Paare (b,c) modulo n als Parameter für den QFT geeignet. Bei gleichverteilter Auswahl ist also die Wahrscheinlichkeit, bei einem Versuch kein geeignetes Paar zu finden kleiner als $\frac{3}{4}$.

Da wir jedoch in Schritt (iii) des RQFT die Parameterpaare aus $\{1,\ldots,n-1\}^2$ statt $\mathbb{Z}_n^2$ wählen, müssen wir noch die Fälle mit $b = 0$ beziehungsweise $c = 0$ betrachten. In Satz 3.11

[5] vgl. Corollary 2.5 in [Gra98]. GRANTHAM betrachtet die Wahrscheinlichkeit für $(b,c) \in \mathbb{Z}_n^2$, wählt aber im Algorithmus die Parameter aus $\{1,\ldots,n-1\}^2$. Dadurch kommt er zu der geringfügig kleineren Schranke $\big(\frac{3}{4}\big)^B$.

zählen wir nämlich die Paare $(b,0) \in \mathbb{Z}_n^2$, bei denen $\mathrm{ggT}(b^2+4c,n) = \mathrm{ggT}(b^2,n)$ nicht-trivial ist. Dies sind, nach Definition der Eulerschen φ-Funktion, die $n-\varphi(n)$ Paare (b,c), in denen b und n einen gemeinsamen Teiler $1 < g < n$ haben. Beachte, dass $(0,0)$ kein solches Paar ist. Entsprechend zählen wir auch die Paare $(0,c) \in \mathbb{Z}_n^2$, für die $\mathrm{ggT}(c,n)$ nicht-trivial ist. Auch das sind $n-\varphi(n)$ Paare.

Die Anzahl der Paare $(b,c) \in \{1,\dots,n-1\}$, die entweder zulässig sind, oder bei denen einer der größten gemeinsamen Teiler $\mathrm{ggT}(b^2+4c,n)$, $\mathrm{ggT}(c,n)$ und $\mathrm{ggT}(b,n)$ nicht-trivial ist, ist somit $M(n) - 2n + 2\varphi(n) < M(n) - 2n$. Da wir aufgrund von Schritt (1) alle ungeraden zusammengesetzten Zahlen $n \leq B^2$ stets als solche erkennen, können wir $n > B^2$ voraussetzen. Damit erhalten wir, dass die Wahrscheinlichkeit bei B Versuchen kein einziges geeignetes Paar (b,c) zu finden kleiner als $\left(\frac{3}{4} + \frac{2}{n}\right)^B < \left(\frac{3}{4} + \frac{2}{B^2}\right)^B$ ist. □

3.3 Fehlerwahrscheinlichkeit bei zusammengesetzten Zahlen

Nun betrachten wir die Wahrscheinlichkeit, dass eine ungerade zusammengesetzte Zahl $n > 3$ den quadratischen Frobenius-Test mit einem zufällig ausgewählten Paar zulässiger Parameter (b,c) besteht.

Definition 3.13. Eine ungerade zusammengesetzte Zahl n *besteht den* RQFT *mit Wahrscheinlichkeit* α, wenn die Anzahl der Paare $(b,c) \in \{1,\dots,n-1\}^2$, so dass n den QFT mit Parametern (b,c) besteht $\alpha M(n)$ ist.[6]

Bemerkung 3.14. Wie in Satz 3.8 gezeigt, bestehen alle ungeraden Primzahlen p den quadratischen Frobenius-Test mit beliebigen Paaren zulässiger Parameter.

In diesem Fall kann man natürlich weder durch Probedivision noch durch den Test, ob p ein Quadrat ist, zu dem Ergebnis kommen, dass p zusammengesetzt sein könnte. Weiterhin wird entweder ein zulässiges Parameterpaar gefunden, womit der QFT dann ausgeführt werden kann und somit das Ergebnis *wahrscheinlich prim* liefern wird, oder es wird keines gefunden. Wird kein zulässiges Parameterpaar gefunden, so liefert der RQFT nach Definition das Ergebnis *wahrscheinlich prim*. Damit besteht p den RQFT mit Wahrscheinlichkeit 1.

Definition 3.15. Wir sagen, n *besteht den* QFT *mit Parametern* $((b,c) \bmod p)$, falls es ein Parameterpaar (b',c') mit $(b,c) \equiv (b',c') \bmod p$ gibt, so dass n den QFT mit Parametern (b',c') besteht.

Theorem 3.16. *Eine ungerade zusammengesetzte Zahl besteht den* RQFT *mit Wahrscheinlichkeit kleiner als* $\frac{1}{7710}$.[7]

Um diesen Satz zu beweisen, werden zunächst einige Lemmata gezeigt. Diese sind wie folgt gegliedert: Zunächst wird in Lemma 3.17 der Fall behandelt, dass n nicht quadratfrei ist. Anschließend geht es nur noch um quadratfreie zusammengesetzte Zahlen. In Lemma 3.20 beweisen wir eine Schranke für den Fall, dass b^2+4c ein quadratischer Rest modulo eines Primteilers p von n ist. Dabei wird unterschieden nach der Anzahl k der Primfaktoren von n. Dies liefert unterschiedliche Schranken für den Fall, dass k gerade ist, und den Fall, dass k ungerade ist. Für den Fall, dass k gerade ist, liefert Korollar 3.21 eine Abschätzung für die Fehlerwahrscheinlichkeit. Ist k hingegen ungerade, so ist etwas mehr Arbeit nötig. Für alle ungeraden k wird in Lemma 3.23 eine Schranke für die Fehlerwahrscheinlichkeit bewiesen. Diese ist von k abhängig und für $k = 3$ nicht scharf genug. Daher wird dieser Fall in Lemma 3.22 gesondert behandelt.

[6] GRANTHAM benutzt hier „$(b,c) \in \mathbb{Z}_n^2$“, doch im Algorithmus ist $(b,c) \in \{1,\dots,n-1\}^2$.
[7] vgl. Theorem 2.6 in [Gra98].

Lemma 3.17. *Sei $n \in \mathbb{Z}$ ungerade und p prim mit $p^2 \mid n$. Dann besteht n den* RQFT *mit einer Wahrscheinlichkeit $\alpha < \frac{4}{p}$.*[8]

Beweis. Wegen Schritt (2) besteht keine Quadratzahl den RQFT.

Es sei $k \in \mathbb{N}$ so gewählt, dass $p^k \mid n$ und $p^{k+1} \nmid n$. Nehmen wir an, n bestehe den QFT mit Parametern (b, c). Dann muss n die Schritte (4) und (5) bestehen. Es gilt daher sicherlich

$$x^{n+1} \equiv -c \mod (n, x^2 - bx - c)$$

und

$$x^{n^2-1} \equiv 1 \mod (n, x^2 - bx - c),$$

also $1 \equiv x^{n^2-1} = x^{(n+1)(n-1)} \equiv (-c)^{n-1} \bmod (n, x^2 - bx - c)$. Da $-c \in \mathbb{Z}$ ist, ist dies äquivalent dazu, dass $(-c)^{n-1} = 1$ in $\mathbb{Z}_n$ und folglich gilt auch $(-c)^{n-1} = 1$ in $\mathbb{Z}_{p^k}$ ist. Nach Lemma 2.7 auf Seite 5 gibt es höchstens

$$\operatorname{ggT}\left(n-1, \varphi\left(p^k\right)\right) = \operatorname{ggT}\left(n-1, p^{k-1}(p-1)\right) = \operatorname{ggT}(n-1, p-1)$$

Lösungen c dieser Gleichung in $\mathbb{Z}_{p^k}$, denn $p \mid n$ impliziert $p \nmid n-1$.

Es gibt also nicht mehr als $p-1$ Zahlen $c \in \mathbb{Z}_{p^k}$, so dass n den QFT mit den Parametern (b, c) für einen beliebigen zulässigen Parameter b bestehen könnte. Weiterhin existieren in $\mathbb{Z}_{p^k}$ sicherlich nicht mehr als p^k solcher b.

Insgesamt kann also n den QFT mit weniger als $p^k(p-1) = p^{k+1} - p^k$ der Parameterpaare (b, c) modulo p^k bestehen. Zu jedem Paar (b, c) modulo p^k gibt es nach dem Chinesischen Restsatz genau $\frac{n^2}{p^{2k}}$ Paare $(b', c') \in \mathbb{Z}_n^2$ mit $(b, c) \equiv (b', c') \bmod p^k$. Also besteht n den QFT mit weniger als

$$\left(p^{k+1} - p^k\right) \frac{n^2}{p^{2k}} = \left(1 - \frac{1}{p}\right) \frac{n^2}{p^{k-1}} \underset{\substack{\text{Satz} \\ 3.11}}{<} \left(1 - \frac{1}{p}\right) \frac{4M(n)}{p^{k-1}} < \frac{4}{p^{k-1}} M(n) \leq \frac{4}{p} M(n)$$

Paaren (b, c) modulo n da, nach Voraussetzung, $k \geq 2$ ist.

Nach Definition besteht dann n den RQFT mit einer Wahrscheinlichkeit $\alpha < \frac{4}{p}$. □

Lemma 3.18. *Sei p eine ungerade Primzahl und n ein ungerades Vielfaches von p. Es gibt genauso viele $(b, c) \in \mathbb{Z}_p^2$ mit $b^2 + 4c \not\equiv 0$, so dass jede Lösung x von $x^2 - bx - c \equiv 0 \bmod p$ die Bedingung $x^n \equiv b - x \bmod (p, x^2 - bx - c)$ erfüllt, wie es ungeordnete Paare $\{a_1, a_2\}$ modulo p gibt mit $a_1^n \equiv a_2 \bmod p$ und $a_2^n \equiv a_1 \bmod p$.*[9]

Beweis. Sei ein Paar $\{a_1, a_2\}$, $a_1 \not\equiv a_2$, gegeben mit $a_1^n \equiv a_2 \bmod p$ und $a_2^n \equiv a_1 \bmod p$. Dann sind a_1 und a_2 genau die Nullstellen des Polynoms

$$(x - a_1)(x - a_2) = x^2 - (a_1 + a_2)x + a_1 a_2 = x^2 - bx - c,$$

wobei $b = a_1 + a_2$ und $c = -a_1 a_2$ ist. Es gilt nun $a_1^n \equiv a_2 = a_1 + a_2 - a_1 = b - a_1 \bmod p$ nach Voraussetzung und Definition von b. Entsprechend erhalten wir $a_2^n \equiv b - a_2 \bmod p$. Das so konstruierte Paar (b, c) modulo p hat also genau die gesuchte Eigenschaft.

Umgekehrt seien (b, c) gegeben, so dass für die Lösungen a_i von $a_i^2 - ba_i - c \equiv 0 \bmod p$ gilt, dass $a_i^n \equiv b - a_i \bmod p$. Nach Vieta gilt dann für die Lösungen, dass $a_1 \equiv b - a_2 \bmod p$ und, äquivalent dazu, $a_2 \equiv b - a_1 \bmod p$. Zusammen mit $x^n \equiv b - x \bmod p$ für alle $x \in \{a_1, a_2\}$ erhält man $a_1 \equiv a_2^n \bmod p$ und $a_2 \equiv a_1^n \bmod p$. □

[8] vgl. Lemma 2.7 in [Gra98].

[9] Ausgegliedert aus dem Beweis von Lemma 2.8 in [Gra98].

Lemma 3.19. *Sei $n \in \mathbb{N}$ ungerade und p ein Primfaktor von n. Es gibt höchstens $\frac{p-1}{2}$ verschiedene Paare $(b,c) \in \mathbb{Z}_p^2$ mit $\left(\frac{b^2+4c}{p}\right) = 1$, so dass n den* QFT *mit den Parametern $((b,c) \bmod p)$ besteht.*[10]

Beweis. Nach Voraussetzung besteht n den QFT, insbesondere Schritt (4). Also können wir eine obere Schranke für die gesuchte Anzahl durch die Betrachtung der Paare $(b,c) \in \mathbb{Z}_p^2$ mit $\left(\frac{b^2+4c}{p}\right) = 1$ und $x^{n+1} \equiv -c \bmod (p, x^2 - bx - c)$ erhalten.

Weil $\mathbb{Z}_p$ ein Körper ist, besitzen quadratische Polynome über $\mathbb{Z}_p$ höchstens zwei Nullstellen. Da $\sqrt{b^2+4c} \in \mathbb{Z}_p$ ist wegen $\left(\frac{b^2+4c}{p}\right) = 1$, müssen alle Nullstellen von $x^2 - bx - c$ schon in $\mathbb{Z}_p$ liegen. Aufgrund der Voraussetzung $b^2 + 4c \not\equiv 0 \bmod p$ kann weiterhin $x^2 - bx - c$ keine doppelte Nullstelle haben, so dass es also genau zwei Lösungen a_1 und a_2 der Gleichung $x^2 - bx - c = 0$ in $\mathbb{Z}_p$ gibt.

Wegen $x^2 - bx - c \equiv (x - a_1)(x - a_2) \bmod p$ ist nach dem Chinesischen Restsatz

$$x^{n+1} \equiv -c \mod (p, x - a_1) \qquad \text{und} \qquad x^{n+1} \equiv -c \mod (p, x - a_2).$$

Mit $x \equiv a_i \bmod (p, x - a_i)$ folgt daraus $-c \equiv a_i^{n+1} \bmod (p, x - a_i)$, also, da $(-c)$ und a_i ganze Zahlen sind, auch $-c \equiv a_i^{n+1} \bmod p$.

Durch Koeffizientenvergleich von $x^2 - bx - c$ und $(x - a_1)(x - a_2)$ erhält man jedoch $-c \equiv a_1 a_2 \bmod p$ und es folgt $a_i^{n+1} \equiv a_1 a_2 \bmod p$. Da p eine Primzahl ist und $a_i \not\equiv 0 \bmod p$ ist, gibt es Inverse a_i^{-1} von a_i und Multiplikation mit diesen Inversen liefert

$$a_1^n \equiv a_2 \bmod p \quad \text{und} \quad a_2^n \equiv a_1 \bmod p.$$

Nach dem Wurzelsatz von Vieta ist $b \equiv a_1 + a_2$, also $a_1 \equiv b - a_2$ und $a_2 \equiv b - a_1$. Nun ist, mit Frobenius,

$$a_1^p \equiv (b - a_2)^p \equiv b^p - a_2^p \equiv b - a_1 \mod p.$$

Laut Lemma 3.18 genügt es somit die Anzahl der Paare $\{a_1, a_2\}$, $a_1 \not\equiv a_2$, zu zählen mit $a_1^n \equiv a_2$ und $a_2^n \equiv a_1 \bmod p$.

Wegen $a_2 \equiv a_1^n \bmod p$ ist a_2 durch a_1 eindeutig festgelegt. Da $b^2 + 4c \not\equiv 0 \bmod p$ ist, müssen a_1 und a_2 stets verschieden sein. Wäre $a_1 \equiv 0 \bmod p$, so müsste auch $a_2 \equiv 0 \bmod p$ sein. Dies ist ein Widerspruch. Es gibt daher nur $p - 1$ verschiedene a_1 in $\mathbb{Z}_p$.

Aufgrund der Symmetrie in a_1, a_2 gibt es für jedes ungeordnete Paar $\{a_1, a_2\}$ genau zwei geordnete Paare $(\alpha, \beta) \in \{1, \ldots, p-1\}^2$, nämlich $\alpha \equiv a_1$, $\beta \equiv a_2$ und $\alpha \equiv a_2$, $\beta \equiv a_1$.

Die Anzahl der geordneten Paare (a_1, a_2) und damit auch die Anzahl der Paare $(b,c) \in \mathbb{Z}_p^2$, so dass n Schritt (4) des QFT mit den Parametern $((b,c) \bmod p)$ besteht, ist damit $\frac{p-1}{2}$. Daher gibt es also höchstens $\frac{p-1}{2}$ Paare $(b,c) \in \mathbb{Z}_p^2$, so dass n den gesamten QFT mit den Parametern $((b,c) \bmod p)$ besteht. □

Im folgenden Lemma benutzen wir die Tatsache, dass B eine gerade Zahl ist, so dass die kleinste Primzahl $p \geq B$ nicht kleiner als $B + 1$ sein kann.

Lemma 3.20. *Sei n eine ungerade, quadratfreie Zahl mit genau k Primfaktoren. Die Anzahl der zulässigen Paare $(b,c) \in \mathbb{Z}_n^2$, so dass zum einen $\left(\frac{b^2+4c}{p}\right) = 1$ ist für einen Primteiler p von n, und zum anderen n den* QFT *mit den Parametern (b,c) besteht, ist kleiner oder gleich $\frac{n\varphi(n)}{2(B+1)} < \frac{n\varphi(n)}{2B}$ falls k gerade und kleiner als $\frac{n\varphi(n)}{B^2}$ falls k ungerade ist.*[11]

[10] vgl. Lemma 2.8 in [Gra98].

[11] vgl. Lemma 2.9 in [Gra98]. Der hier bewiesene Satz ist geringfügig stärker als GRANTHAMs Variante. Diese Verschärfung wird im Beweis von Korollar 3.21 benutzt.

Beweis. Sei $n = p_1 \cdots p_k$ mit k paarweise verschiedenen Primzahlen $p_1, \ldots, p_k$. Der Beweis erfolgt durch Fallunterscheidung nach der Anzahl ℓ der Indizes $i \in \{1, \ldots, k\}$ mit $\left(\frac{b^2+4c}{p_i}\right) = 1$. Nun ist nach Voraussetzung

$$-1 = \left(\frac{b^2+4c}{n}\right) = \prod_{j=1}^{k}\left(\frac{b^2+4c}{p_j}\right) = (-1)^{k-\ell},$$

weshalb k genau dann gerade sein muss, wenn ℓ ungerade ist.

Im folgenden betrachten wir zum einen den Fall, dass $\left(\frac{b^2+4c}{p_i}\right) = 1$ ist für genau ein $i \in \{1, \ldots, k\}$, und zum anderen den Fall, dass es mindestens zwei solche Indizes i gibt.

Fall 1. Sei $\left(\frac{b^2+4c}{p_i}\right) = 1$ für genau ein $i \in \{1, \ldots, k\}$.

Modulo p_i gibt es nach Lemma 3.19 nur höchstens $\frac{p_i-1}{2}$ Paare (b, c), so dass n den QFT mit Parametern $((b, c) \bmod p_i)$ besteht, wobei $\left(\frac{b^2+4c}{p_i}\right) = 1$.

Sei $j \neq i$ beliebig. Insgesamt existieren p_j^2 Paare (b, c) modulo p_j. Von diesen haben p_j die Eigenschaft $b^2 + 4c \equiv 0 \bmod p_j$ im Widerspruch zur Annahme, dass (b, c) zulässige Parameter sind. Von den verbleibenden Paaren sind genau die Hälfte solche, für die $b^2 + 4c$ ein Quadrat modulo p_j ist (das muss ja nach Voraussetzung für alle $j \neq i$ gelten). Damit gibt es höchstens $\frac{p_j^2-p_j}{2}$ solcher Paare $((b, c) \bmod p_j)$.

Mit Hilfe des Chinesischen Restsatzes folgt daraus, dass es für jedes feste $i \in \{1, \ldots, k\}$ nicht mehr als

$$\frac{1}{p_i}\prod_{\ell=1}^{k}\frac{p_\ell^2 - p_\ell}{2} = \frac{1}{2^k p_i}\left(\prod_{\ell=1}^{k} p_\ell\right)\left(\prod_{\ell=1}^{k}(p_\ell - 1)\right) = \frac{n\varphi(n)}{2^k p_i}$$

Parameterpaare (b, c) modulo n gibt, mit denen n den quadratischen Frobenius-Test besteht. Insgesamt gibt es also maximal

$$\sum_{i=1}^{k}\frac{n\varphi(n)}{2^k p_i} \leq \sum_{i=1}^{k}\frac{n\varphi(n)}{2^k(B+1)}$$

solcher Parameterpaare (b, c) modulo n, da $p_i > B$ für alle $i \in \{1, \ldots, k\}$ ist.

Fall 2. Es gelte $\left(\frac{b^2+4c}{p_i}\right) = 1$ für mindestens zwei $i \in \{1, \ldots, k\}$. Sei $L(b, c)$ das k-Tupel $L(b, c) := \left(\left(\frac{b^2+4c}{p_i}\right)\right)_{i=1,\ldots,k}$ und sei

$$V := \Big\{ L = (L_1, \ldots, L_k) \in \{-1, 1\}^k \;\Big|\; \exists i, j, i \neq j : \; L_i = L_j = 1 \Big\}.$$

Sei $L \in V$ beliebig und seien i und j die beiden größten Indizes, so dass $L_i = L_j > 1$ mit $i < j$, also $j := \max\{\, j \in \{1, \ldots, k\} \mid L_j = 1 \,\}$ und $i := \max\{\, i \in \{1, \ldots, j-1\} \mid L_i = 1 \,\}$.

Laut Lemma 3.19 gibt es höchstens $\frac{p_\ell-1}{2}$ Paare $((b, c) \bmod p_\ell)$, so dass n den quadratischen Frobenius-Test mit Parametern $((b, c) \bmod p_\ell)$ besteht für $\ell = i, j$. Für alle weiteren Primteiler p_ℓ von n gibt es wiederum höchstens $\frac{p_\ell(p_\ell-1)}{2}$ solcher Paare. Mit dem Chinesischen Restsatz erhalten wir also

$$\frac{p_i - 1}{2} \cdot \frac{p_j - 1}{2} \cdot \prod_{\substack{\ell=1 \\ \ell \neq i,j}}^{k}\frac{p_\ell(p_\ell - 1)}{2} = \frac{n\varphi(n)}{2^k p_i p_j}$$

als obere Schranke für die Anzahl der Paare (b, c) modulo n mit $L(b, c) = L$, so dass n den quadratischen Frobenius-Test mit den Parametern (b, c) besteht.

Damit ist die Anzahl aller Paare (b, c) modulo n mit $L(b, c) \in V$, und so dass n den quadratischen Frobenius-Test mit Parametern (b, c) besteht, kleiner als

$$\sum_{L \in V} \frac{n\varphi(n)}{2^k p_i p_j} \leq \frac{n\varphi(n)}{(B+1)^2} < \frac{n\varphi(n)}{B^2},$$

da alle Primteiler größer B sind und da $\#V < 2^k$ ist.

Fassen wir also zusammen:

- Ist $k = 2$, so kann nur Fall 1 vorliegen, sonst müsste ja $\left(\frac{b^2+4c}{n}\right) = 1$ sein. Setzen wir nun $k = 2$ in die Schranke ein, die wir in Fall 1 erhalten haben, so folgt in diesem Fall die Behauptung.
- Ist $k > 2$ gerade, so können sowohl Fall 1, als auch Fall 2 vorliegen. Wir können als Schranke also nichts besseres als die Summe der beiden Schranken erreichen. Damit erhalten wir als Schranke

$$n\varphi(n)\left(\frac{k}{2^k(B+1)} + \frac{1}{B^2}\right) = \frac{n\varphi(n)}{2(B+1)}\left(\frac{2k}{2^k} + \frac{2}{B+1}\right) < \frac{n\varphi(n)}{2(B+1)}.$$

- Ist k ungerade, so muss Fall 2 vorliegen und wir erhalten $\frac{n\varphi(n)}{B^2}$ als Schranke. □

Es fällt auf, dass wir in Fall 2 eine schärfere Schranke erhalten könnten, wenn mehr als zwei Indizes i mit $\left(\frac{b^2+4c}{p_i}\right) = 1$ existieren. Wäre die Anzahl solcher Indizes nämlich m, so erhielten wir als obere Schranke für die Anzahl der zulässigen Parameterpaare $(b, c) \in \mathbb{Z}_n^2$ nicht $\frac{n\varphi(n)}{B^2}$, sondern $\frac{n\varphi(n)}{B^m}$.

Korollar 3.21. *Eine ungerade quadratfreie Zahl $n \in \mathbb{Z}$ mit einer geraden Anzahl von Primfaktoren besteht den* RQFT *mit Wahrscheinlichkeit $\alpha < \frac{2}{B}$.*[12]

Beweis. Nach Definition besteht n den RQFT genau dann, wenn entweder bei keinem der B Versuche ein zulässiges Parameterpaar gefunden wird, oder n den QFT mit einem zulässigen Parameterpaar (b, c) besteht. Laut Korollar 3.12 ist die Wahrscheinlichkeit, kein gültiges Parameterpaar zu finden kleiner als $P := \left(\frac{3}{4} + \frac{2}{B^2}\right)^B$. Gemäß Lemma 3.20 gibt es weniger als $\frac{n\varphi(n)}{2(B+1)}$ zulässige Paare (b, c), so dass n den QFT mit den Parametern (b, c) besteht.

Da $\left(\frac{3}{4} + \frac{2}{B^2}\right)^B < 10^{-5616}$ sehr viel kleiner als $\frac{2}{B(B+1)} > 10^{-10}$ ist für $B = 44\,958$, erhalten wir somit

$$\alpha < P + \frac{4n\varphi(n)}{2(B+1)n^2} < P + \frac{2}{B+1} = P + \frac{2}{B} - \frac{2}{B(B+1)} < \frac{2}{B}.$$ □

Lemma 3.22. *Für eine ungerade quadratfreie Zahl n mit genau drei Primfaktoren ist die Wahrscheinlichkeit, dass n den* RQFT *besteht, kleiner als $\frac{4}{B^2} + \frac{3(B^2+1)}{2(B^4-3B^2)}$.*[13]

[12] vgl. Corollary 2.10 in [Gra98].
[13] vgl. Lemma 2.11 in [Gra98].

Beweis. Sei $n = p_1p_2p_3$, wobei p_1, p_2, p_3 drei verschiedene Primzahlen sind. Nach Lemma 3.20 und Satz 3.11 auf Seite 14 besteht n den quadratischen Frobenius-Test nur mit höchstens $\frac{4M(n)}{B^2}$ Parameterpaaren $(b, c) \in \mathbb{Z}_n^2$ mit $\left(\frac{b^2+4c}{n}\right) = -1$ und $\left(\frac{b^2+4c}{p_i}\right) = 1$ für ein i. Es genügt also zu zeigen, dass n den QFT für höchstens $\frac{3(B^2+1)}{2(B^4-3B^2)}\frac{n^2}{4}$ Paare mit $\left(\frac{b^2+4c}{p_i}\right) = -1$ für alle i besteht.

Wenn n den QFT besteht, ist

$$x^{n+1} \equiv -c \mod (p_i, x^2 - bx - c) \quad \text{und} \quad x^{p_i+1} \equiv -c \mod (p_i, x^2 - bx - c).$$

Da c modulo n invertierbar ist (es gilt ja $\left(\frac{-c}{n}\right) \neq 0$), ist auch x modulo $(n, x^2 - bx - c)$ invertierbar, denn es gilt $x^{n-p_i} \equiv 1$, also $x^{-1} \equiv x^{n-p_i-1}$.

Nach Lemma 2.7 auf Seite 5 gibt es genau $k_i := \text{ggT}(n - p_i, p_i^2 - 1)$ Lösungen y der Gleichung $y^{n-p_i} = 1$ in $\mathbb{F}_{p_i^2}$. Jedes Paar $(b, c) \in \mathbb{Z}_{p_i}^2$ entspricht zwei Nullstellen x_1, x_2 von $x^2 - bx - c$, die, wie eben gezeigt, beide $x_j^{n-p_i} \equiv 1 \mod (p_i, x^2 - bx - c)$ erfüllen.

Also gibt es höchstens $\frac{k_i}{2}$ Paare $(b, c) \in \mathbb{Z}_{p_i}$ mit $x^{n-p_i} \equiv 1 \mod (p_i, x^2 - bx - c)$. Nach dem Chinesischen Restsatz gibt es also höchstens $\frac{k_1k_2k_3}{8}$ Paare $(b, c) \in \mathbb{Z}_n^2$, so dass n den QFT mit den Parametern (b, c) besteht und $\left(\frac{b^2+4c}{p_i}\right) = -1$ für $i = 1, 2, 3$ ist.

Da p_i und $p_i^2 - 1$ teilerfremd sind, folgt

$$k_i = \text{ggT}(n - p_i, p_i^2 - 1) = \text{ggT}\left(p_i \cdot \left(\frac{p_1p_2p_3}{p_i} - 1\right), p_i^2 - 1\right) = \text{ggT}\left(\frac{p_1p_2p_3 - p_i}{p_i}, p_i^2 - 1\right).$$

Definieren wir nun $j_i := \frac{p_i^2-1}{k_i}$ und $r_i := \frac{p_1p_2p_3-p_i}{p_ik_i}$. Dann haben wir offenbar für alle i

$$r_i(p_i^2 - 1) = j_i\left(\frac{p_1p_2p_3 - p_i}{p_i}\right). \tag{3.3}$$

Für $(i, j) \in \{(1, 2), (1, 3), (2, 3)\}$ ist

$$(p_i^2 - 1)(p_j^2 - 1) = p_i^2p_j^2 - p_i^2 - p_j^2 + 1 < p_i^2p_j^2 - 2p_ip_j + 1 = (p_ip_j - 1)^2.$$

Multiplizieren wir diese Ungleichung mit den verschiedenen Belegungen von i und j, so erhalten wir

$$\begin{aligned} &(p_1^2 - 1)(p_2^2 - 1)(p_2^2 - 1)(p_3^2 - 1)(p_1^2 - 1)(p_3^2 - 1) < (p_1p_2 - 1)^2(p_2p_3 - 1)^2(p_1p_3 - 1)^2 \\ \iff\ &(p_1^2 - 1)^2(p_2^2 - 1)^2(p_3^2 - 1)^2 < (p_1p_2 - 1)^2(p_2p_3 - 1)^2(p_1p_3 - 1)^2. \end{aligned}$$

Da alle auftretenden Faktoren positiv sind, folgt daraus

$$\begin{aligned} &(p_1^2 - 1)(p_2^2 - 1)(p_3^2 - 1) < (p_1p_2 - 1)(p_2p_3 - 1)(p_1p_3 - 1) \\ \iff\ &\frac{(p_1^2 - 1)(p_2^2 - 1)(p_3^2 - 1)}{k_1k_2k_3} < \frac{(p_1p_2 - 1)(p_2p_3 - 1)(p_1p_3 - 1)}{k_1k_2k_3}, \end{aligned}$$

also $j_1j_2j_3 < r_1r_2r_3$.[14]

Sei $C := j_1j_2j_3$. Laut Gleichung (3.3) wissen wir, dass

$$\frac{r_1r_2r_3}{j_1j_2j_3} = \frac{(p_2p_3 - 1)(p_1p_3 - 1)(p_1p_2 - 1)}{(p_1^2 - 1)(p_2^2 - 1)(p_3^2 - 1)}$$

[14] GRANTHAM betrachtet stattdessen getrennt die Fälle $j_1j_2j_3 < r_1r_2r_3$ und $j_1j_2j_3 > r_1r_2r_3$ und zeigt dann, dass $j_1j_2j_3 \neq r_1r_2r_3$ ist.

ist, woraus wir durch Ausmultiplizieren

$$\frac{r_1r_2r_3}{j_1j_2j_3} = \frac{p_1^2p_2^2p_3^2 - p_1^2p_2p_3 - p_1p_2^2p_3 - p_ip_2p_3^2 + p_ip_2 + p_2p_3 + p_1p_3 - 1}{p_1^2p_2^2p_3^2 - p_i^2p_2^2 - p_1^2p_3^2 - p_2^2p_3^2 + p_i^2 + p_2^2 + p_3^2 - 1}$$

erhalten. Daraus folgt sofort

$$\frac{r_1r_2r_3}{j_1j_2j_3} < \frac{n^2 + p_1p_2 + p_2p_3 + p_1p_3}{n^2 - p_1^2p_2^2 - p_1^2p_3^2 - p_2^2p_3^2}. \tag{3.4}$$

Mit $\frac{r_1r_2r_3}{j_1j_2j_3} = \frac{r_1r_2r_3}{C} \geq \frac{C+1}{C} = 1 + \frac{1}{C}$ folgt weiterhin

$$\begin{aligned}
1 + \frac{1}{C} &\leq \frac{r_1r_2r_3}{j_1j_2j_3} \\
&< \frac{1 + (p_1p_2 + p_2p_3 + p_1p_3)/n^2}{1 - (p_1^2p_2^2 + p_2^2p_3^2 + p_2^2p_3^2)/n^2} \\
&= \frac{1 + \frac{p_1p_2}{p_1^2p_2^2p_3^2} + \frac{p_2p_3}{p_1^2p_2^2p_3^2} + \frac{p_1p_3}{p_1^2p_2^2p_3^2}}{1 - \frac{p_1^2p_2^2}{p_1^2p_2^2p_3^2} - \frac{p_2^2p_3^2}{p_1^2p_2^2p_3^2} - \frac{p_1^2p_3^2}{p_1^2p_2^2p_3^2}} \\
&= \frac{1 + \frac{1}{p_1p_2p_3^2} + \frac{1}{p_1^2p_2p_3} + \frac{1}{p_1p_2^2p_3}}{1 - \frac{1}{p_3^2} - \frac{1}{p_2^2} - \frac{1}{p_1^2}},
\end{aligned}$$

woraus wiederum mit $p_i > B$ für alle $i = 1, 2, 3$ folgt, dass

$$1 + \frac{1}{C} < \frac{1 + \frac{3}{B^4}}{1 - \frac{3}{B^2}} = \frac{B^4 + 3}{B^4 - 3B^2},$$

weshalb

$$C > \frac{B^4 - 3B^2}{B^4 + 3 - (B^4 - 3B^2)} = \frac{B^4 - 3B^2}{3B^2 + 3}$$

ist.

Nach Definition von C ist nun $\frac{k_1k_2k_3}{8} < \frac{n^2}{8C}$ und wir haben $\frac{n^2}{8C}\frac{4}{n^2} = \frac{1}{2C}$, woraus mit $C > \frac{B^4-3B^2}{3(B^2+1)}$ die Behauptung folgt. □

Es erscheint auf den ersten Blick, als könne man das vorherige Lemma auf den Fall mit $k > 3$ Primfaktoren erweitern. Dann hätte jedoch Ungleichung (3.4) die Form

$$\prod_{i=1}^{k} \frac{r_i}{j_i} < \frac{n^{k-1} + \ldots}{n^2 - \ldots},$$

was es nicht erlaubt, den Beweis analog fortzusetzen. Dieser funktioniert ausschließlich für den Fall $k - 1 = 2$.

Lemma 3.23. *Sei $k \in \mathbb{N}$ ungerade und n eine ungerade quadratfreie Zahl mit genau k Primfaktoren. Dann besteht n den* RQFT *mit Wahrscheinlichkeit $\alpha < \frac{1}{2^{3k-2}} + \frac{1}{2^{4k-3}} + \frac{4}{B^2}$.*[15]

[15] vgl. Lemma 2.12 in [Gra98].

Beweis. Laut Lemma 3.20 gibt es weniger als $\frac{n^2}{B^2}$ Paare $(b,c) \in \mathbb{Z}_n^2$, so dass n den QFT mit den Parametern (b,c) besteht, wobei $\left(\frac{b^2+4c}{p}\right) = 1$ für ein $p \mid n$. Mit Lemma 3.11 ist die Wahrscheinlichkeit, dass n den QFT mit solchen zufällig gewählten Parametern $(b,c) \in \mathbb{Z}_n^2$ besteht, kleiner als $\frac{n^2}{B^2} \cdot \frac{4}{n^2} = \frac{4}{B^2}$.

Betrachten wir nun den Fall, dass $\left(\frac{b^2+4c}{p}\right) = -1$ für alle Primzahlen $p \mid n$ ist. Dazu schreiben wir $n = p_1 p_2 \cdots p_k$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_k$.

Sei J maximal mit der Eigenschaft, dass $2^{J+1} \mid \operatorname{ggT}(p_1^2 - 1, \ldots, p_k^2 - 1)$. Dann ist

$$p_i^2 \equiv 1 \mod 2^{J+1}$$

für alle $i = 1, \ldots, k$. Multiplizieren wir diese k Kongruenzen, so erhalten wir

$$n^2 \equiv 1 \mod 2^{J+1}.$$

Wir wählen nun $r, s \in \mathbb{N}$ so, dass $2^r s = n^2 - 1$ und s ungerade ist. Dann ist sicherlich $J < r$.

Sei $p := p_i$ für ein beliebiges i. Die Anzahl der Lösungen von $y^{2^j s} = -1$ in $\mathbb{F}_{p^2}$ ist 0, wenn (-1) keine 2^j-te Potenz ist, und andernfalls $\operatorname{ggT}(p^2 - 1, 2^j s)$ gemäß Lemma 2.7 auf Seite 5. Es gibt also eine Lösung genau dann, wenn es ein $\alpha \in \mathbb{F}_{p^2}$ mit $\alpha^{2^j} = -1$ gibt.

Da $\alpha^{2^{j+1}} = 1$, ist sicherlich $\operatorname{ord} \alpha \mid 2^{j+1}$, also $\operatorname{ord} \alpha = 2^\ell$ für ein $\ell \leq j+1$. Mit $\alpha, \alpha^2, \ldots, \alpha^{2^{j-1}} \neq 1$, was aus $\alpha^{2^j} = -1$ folgt, erhalten wir zudem $\ell \notin \{1, 2, 3, \ldots, j-1\}$ und damit $\operatorname{ord} \alpha = 2^{j+1}$. Weil die multiplikative Gruppe $\mathbb{F}_{p^2}^*$ die Ordnung $p^2 - 1$ hat, muss 2^{j+1}, nach dem Satz von Lagrange, ein Teiler von $p^2 - 1$ sein. Damit gibt es keine Paare (b,c) mit $x^{2^j s} \equiv -1 \bmod (n, x^2 - bx - c)$ für $j > J$.

Laut der Definition von J gibt es ein $p := p_i$, so dass $2^{J+1} \mid p^2 - 1$, aber $2^{J+2} \nmid p^2 - 1$. Besteht n den quadratischen Frobenius-Test mit den Parametern (b,c), so ist wegen Schritt (4) klar, dass $(-c)$ ein Quadrat modulo n, also auch modulo p sein muss. Da p, gemäß Satz 3.8, den quadratischen Frobenius-Test mit den Parametern (b,c) besteht, ist

$$x^{\frac{p^2-1}{2}} \equiv 1 \mod (p, x^2 - bx - c),$$

also, mit $p^2 - 1 = 2^{J+1}\ell$, $\operatorname{ord} x$ ein Teiler von $2^J \ell$ für eine ungerade Zahl $\ell \in \mathbb{N}$. Wäre nun $x^{2^J s} \equiv -1 \bmod (p, x^2 - bx - c)$, so folgte $2^{J+1} \mid \operatorname{ord} x$, was offensichtlich ein Widerspruch ist. Es kann also keine Paare (b,c) modulo n geben, so dass $x^{2^J s} \equiv -1 \bmod (n, x^2 - bx - c)$.

Betrachten wir nun den verbleibenden Fall $0 \leq j < J$. Für alle $i = 1, \ldots, k$ gibt es genau $\operatorname{ggT}(p_i^2 - 1, 2^j s)$ Lösungen von $y^{2^j s} = -1$ in $\mathbb{F}_{p_i^2}$. Jede Lösung $y \notin \mathbb{F}_{p_i}$ liefert eine Lösung x von $x^{2^j s} \equiv -1 \bmod (p_i, x^2 - bx - c)$, wobei $x^2 - bx - c$ das Minimalpolynom von y ist. Wegen $\left(\frac{b^2+4c}{n}\right) \neq 0$ hat dieses Polynom in $\mathbb{F}_{p_i^2}$ genau zwei Nullstellen. Damit gibt es höchstens $\frac{1}{2} \operatorname{ggT}(p_i^2 - 1, 2^j s)$ Paare (b,c) modulo p_i, für welche $x^{2^j s} \equiv -1 \bmod (p_i, x^2 - bx - c)$ ist. Laut dem Chinesischen Restsatz gibt es also modulo n höchstens

$$\prod_{i=1}^{k} \frac{\operatorname{ggT}(p_i^2 - 1, 2^j s)}{2} = 2^{-k} \prod_{i=1}^{k} \operatorname{ggT}(p_i^2 - 1, 2^j s)$$

Paare (b,c) mit $x^{2^j s} \equiv -1 \bmod (n, x^2 - bx - c)$.

Da $2^J \mid p_i^2 - 1$ impliziert, dass $2^j \mid p_i^2 - 1$ für alle $j < J$ ist, haben wir

$$2^{-k} \prod_{i=1}^{k} \operatorname{ggT}(p_i^2 - 1, 2^j s) = 2^{-k} \prod_{i=1}^{k} 2^j \operatorname{ggT}(p_i^2 - 1, s) = 2^{(j-1)k} G,$$

mit $G := \prod_{i=1}^{k} \operatorname{ggT}(p_i^2 - 1, s)$.

Analog zu den Paaren (b, c) mit $x^{2^j s} \equiv -1 \bmod (p_i, x^2 - bx - c)$ gibt es höchstens $\frac{1}{2} \operatorname{ggT}(p_i^2 - 1, s)$ Paare (b, c) modulo p_i, für die $x^s \equiv 1 \bmod (p_i, x^2 - bx - c)$ ist. Mit dem Chinesischen Restsatz erhalten wir also, dass die Anzahl der Paare (b, c) modulo n mit $x^s \equiv 1 \bmod (n, x^2 - bx - c)$ höchstens $2^{-k}G$ ist.

Damit gibt es insgesamt höchstens

$$\frac{G}{2^k} + \sum_{j=0}^{J-1} 2^{(j-1)k} G = \frac{G}{2^k} \left(1 + \frac{2^{Jk} - 1}{2^k - 1}\right)$$

Paare (b, c) modulo n, so dass n den quadratischen Frobenius-Test mit den Parametern (b, c) besteht.

Da s ungerade und, nach Voraussetzung, $2^{J+1} \mid p_i^2 - 1$ ist, gilt

$$\operatorname{ggT}\left(p_i^2 - 1, s\right) = \operatorname{ggT}\left(\frac{p_i^2 - 1}{2^{J+1}}, s\right) \leq \frac{p_i^2 - 1}{2^{J+1}} < \frac{p_i^2}{2^{J+1}}.$$

Daraus erhalten wir

$$\left(1 + \frac{2^{Jk} - 1}{2^k - 1}\right) \frac{G}{2^k} < \left(1 + \frac{2^{Jk} - 1}{2^k - 1}\right) \frac{\prod_{i=1}^{k} p_i^2}{2^{(J+1)k} 2^k} = \left(1 + \frac{2^{Jk} - 1}{2^k - 1}\right) \frac{n^2}{2^{(J+1)k} 2^k}$$

als obere Schranke für die Anzahl der Paare (b, c) modulo n, so dass n den quadratischen Frobenius-Test mit den Parametern (b, c) besteht. Es gilt $n^2 - 1 = (n - 1)(n + 1)$. Da n ungerade ist, ist entweder 2 ein Teiler von $n - 1$ und 4 ein Teiler von $n + 1$ oder andersherum. Damit muss $8 = 2^{2+1}$ ein Teiler von $n^2 - 1$ sein. Also ist $J \geq 2$.

Die Schranke nimmt ihr Maximum bei $J = 2$ an, denn die Schranke ist monoton fallend in J, da

$$\begin{aligned}
& \left(1 + \frac{2^{Jk} - 1}{2^k - 1}\right) \frac{n^2}{2^{(J+1)k} 2^k} > \left(1 + \frac{2^{(J+1)k} - 1}{2^k - 1}\right) \frac{n^2}{2^{(J+2)k} 2^k} \\
\iff & \left(2^k - 1 + 2^{Jk} - 1\right) 2^k > 2^k - 1 + 2^{(J+1)k} - 1 \\
\iff & \left(2^k - 2\right) 2^k + 2^{(J+1)k} > 2^k - 2 + 2^{(J+1)k} \\
\iff & 2^k > 1,
\end{aligned}$$

was im hier vorliegenden Fall $k \geq 3$ sicherlich korrekt ist.

Setzen wir $J = 2$ ein, so erhalten wir

$$\left(1 + \frac{2^{2k} - 1}{2^k - 1}\right) \frac{n^2}{2^{3k} 2^k} = \frac{n^2}{2^{4k}} \left(1 + 2^k + 1\right) = \frac{n^2}{2^{4k}} \left(2^k + 2\right) = n^2 \left(\frac{1}{2^{3k}} + \frac{1}{2^{4k-1}}\right).$$

Nun gibt es, laut Satz 3.11, weniger als $\frac{n^2}{4}$ zulässige Parameterpaare (b, c) modulo n. Die Wahrscheinlichkeit, unter diesen eines auszuwählen, so dass n den quadratischen Frobenius-Test mit den Parametern (b, c) besteht, ist damit kleiner als

$$\left(\frac{1}{2^{3k}} + \frac{1}{2^{4k-1}}\right) \frac{4n^2}{n^2} = \frac{1}{2^{3k-2}} + \frac{1}{2^{4k-3}},$$

was zu zeigen war. □

Damit haben wir alle benötigten Teile gezeigt und können nun den Beweis von Theorem 3.16 auf Seite 16 formulieren.

Beweis von Theorem 3.16.

Fall 1. Besitzt n einen Primfaktor $p < B$, so ist die Wahrscheinlichkeit, dass n als zusammengesetzt erkannt wird, gleich 1 wegen Schritt (1). Die Fehlerwahrscheinlichkeit in diesem Fall ist also 0.

Fall 2. Ist n eine Quadratzahl, so ist, wegen Schritt (2), ebenfalls die Fehlerwahrscheinlichkeit gleich 0.

Fall 3. Besitze n keine Primfaktoren $p < B$ und sei n kein Quadrat. Dann ist die Wahrscheinlichkeit, dass kein zulässiges Parameterpaar (b, c) modulo n gefunden wird, laut Korollar 3.12, kleiner als $P := \left(\frac{3}{4} + \frac{2}{B^2}\right)^B$. Diese Wahrscheinlichkeit ist extrem klein und ändert dadurch in den folgenden Fällen die Schranke nicht, denn schon für $B = 30\,840$ ist $P < 10^{-3853}$.

Fall 3.1. Sei p eine Primzahl und p^2 ein Teiler von n, also n nicht quadratfrei. Dann ist die Fehlerwahrscheinlichkeit des RQFT laut Lemma 3.17 kleiner als $P + (1-P)\frac{4}{p} < P + \frac{4}{B} < \frac{1}{7710}$ für alle $B > 4 \cdot 7710 = 30\,840$ ist.

Fall 3.2. Sei n quadratfrei mit einer geraden Anzahl von Primfaktoren. Dann besagt Korollar 3.21, dass die Fehlerwahrscheinlichkeit kleiner als $P + (1-P)\frac{2}{B} < P + \frac{2}{B} < \frac{1}{7710}$ ist für alle $B > 2 \cdot 7710$, insbesondere für alle $B > 30\,840$.

Fall 3.3. Sei n quadratfrei mit genau drei Primfaktoren. Dann ist die Fehlerwahrscheinlichkeit laut Lemma 3.22 kleiner als

$$P + (1-P)\left(\frac{4}{B^2} + \frac{3(B^2+1)}{2(B^4-3B^2)}\right) = P + (1-P)\frac{11B^2-21}{2B^2(B^2-3)} < P + \frac{11B^2-21}{2B^2(B^2-3)}.$$

Nun ist $\frac{11B^2-21}{2B^2(B^2-3)} < \frac{1}{7710}$ genau dann, wenn $3855(11B^2-21) < B^4 - 3B^2$ ist. Diese Ungleichung wird von jedem $B > 205$ gelöst.

Fall 3.4. Sei n quadratfrei mit genau k Primfaktoren, wobei $k > 3$ ungerade ist. Für diesen Fall haben wir in Lemma 3.23 gezeigt, dass die Fehlerwahrscheinlichkeit kleiner als $P + (1-P)\left(\frac{4}{B^2} + \frac{1}{2^{3k-2}} + \frac{1}{2^{4k-3}}\right) < P + \frac{4}{B^2} + \frac{17}{131072} = P + \frac{4}{B^2} + \frac{1}{7710{,}1176\ldots}$ ist. Dies ist kleiner als $\frac{1}{7710}$, sofern $B > 44\,957$ ist.

Setzen wir $B = 44\,958$, so ist die Fehlerwahrscheinlichkeit stets kleiner als $\frac{1}{7710}$. □

Man kann natürlich auch, wie in [Gra98], $B = 50\,000$ setzen. Nutzt man die schärfere Schranke, so reduziert sich die Anzahl der Primzahlen, durch die man n in Schritt (1) teilt von 5132 auf 4669. Da Schritt (1) bei großen Zahlen jedoch kaum ins Gewicht fällt, verursacht dies keinen wesentlichen Geschwindigkeitsunterschied.

In keinem der Beweise der Lemmata, die die verschiedenen Fälle des obigen Beweises behandeln, wird benutzt, dass jede zusammengesetzte Zahl n, die den RQFT besteht, auch jeden der Schritte bestehen muss. Es ist also naheliegend, anzunehmen, dass die Schranke $\frac{1}{7710}$ deutlich verbessert werden könnte, wenn man bei jedem Fall alle Schritte des Tests benutzt.

Zudem erhält man für den Fall, dass n das Produkt von $k = 3$ verschiedenen Primzahlen ist, eine sehr viel bessere Fehlerabschätzung in Lemma 3.22 als man im allgemeineren

Lemma 3.23 für eine ungerade Anzahl von Primfaktoren erhält. Könnte man auch für $k = 5$ eine Schranke beweisen, die signifikant besser ist als die aus Lemma 3.23, so dass die schärfste Schranke diejenige aus Lemma 3.23 für $k = 7$ wäre, wäre eine Verbesserung der gesamten Schranke auf $< \frac{1}{500\,000}$ möglich. Die Fehlerschranken der übrigen Lemmata ließen sich dann durch eine passende Wahl von B entsprechend verschärfen.

3.4 Theoretische Analyse der Laufzeit

Für den Vergleich der Laufzeiten des Miller-Rabin- und des randomisierten quadratischen Frobenius-Tests definieren wir zunächst eine Einheit für die Laufzeit.

Definition 3.24. Ein Algorithmus mit einer Eingabe n der Länge $N = \log_2 n$ hat eine Laufzeit von k selfridge, falls er in der Zeit ausgeführt werden kann, die für die Durchführung von $(k + o(1))N$ Multiplikationen modulo n nötig ist.

Dabei zählen wir $I \in \mathcal{O}(1)$ Multiplikationen für die Berechnung von Inversen modulo n und die Berechnung des Jacobi-Symbols $(\frac{\cdot}{n})$. Weiterhin gehen wir davon aus, dass eine Addition, ebenso wie ein Bit-Shift, also eine Verschiebung der Bits um (in unserem Fall) eine Stelle nach rechts, die Laufzeit von $o(1)$ Multiplikationen benötigt.

Die letzte Annahme basiert darauf, dass eine Addition in Zeit $\mathcal{O}(\log n)$ ausgeführt werden kann, wohingegen angenommen wird, dass die Laufzeit für eine Multiplikation größer als $\mathcal{O}(\log n)$ ist. Dies ist nicht für jedes Rechnermodell richtig. Für Turing-Maschinen mag es richtig sein [Knu69, S. 275], doch für Zeiger-Maschinen („pointer machines“) ist es laut [Knu97, S. 311] nicht korrekt. Da jedoch heutige Computer nicht dem Modell solcher Zeiger-Maschinen entsprechen, werden wir diese Einschränkung ignorieren.

Wir werden im Folgenden davon ausgehen, dass alle Exponenten mittels optimaler Additionsketten berechnet werden. Dies ergibt, gegenüber der tatsächlichen Implementierung mit der sehr viel einfacheren binären Exponentiation, eine Einsparung von höchstens $\log_2 n$ Multiplikationen.

Satz 3.25. *Der Miller-Rabin-Test hat eine Laufzeit von* 1 selfridge.[16]

Beweis. Wir schreiben $n = 2^r s - 1$, wobei s ungerade ist. Dann benötigt der Miller-Rabin-Test die Berechnung einer s-ten Potenz modulo n, sowie von höchstens r weiteren Quadraten. Für die Berechnung einer t-ten Potenz modulo n sind $(1+o(1)) \log_2 t$ Multiplikationen ausreichend laut [Knu69, Abschnitt 4.6.3]. Da $\log_2 n > \log_2 s + r$, ist die Laufzeit des Miller-Rabin-Tests höchstens $(1 + o(1)) \log_2 n$ Multiplikationen, also 1 selfridge. □

Für den RQFT müssen wir Multiplikationen modulo $(n, x^2 - bx - c)$ ausführen. Das folgende Lemma zeigt, wie sich diese durch Multiplikationen modulo n darstellen lassen.

Lemma 3.26. *Eine Multiplikation modulo $(n, x^2 - bx - c)$ kann innerhalb von $5 + o(1)$ Multiplikationen modulo n durchgeführt werden.*[17]

Beweis. Wir können beliebige $\alpha, \beta \in \mathbb{Z}[x]/(n, x^2 - bx - c)$ als $\alpha = dx + e$ und $\beta = fx + g$ mit $d, e, f, g \in \mathbb{Z}_n$ schreiben. Dann ist

$$\begin{aligned}(dx + e)(fx + g) &\equiv dfx^2 + (dg + ef)x + eg \\ &\equiv df(bx + c) + (dg + ef)x + eg\end{aligned}$$

[16] vgl. Proposition 3.1 in [Gra98].
[17] vgl. Proposition 3.2 in [Gra98].

$$\equiv (dg + ef + bdf)x + eg + cdf \mod (n, x^2 - bx - c).$$

Dies können wir aus df, eg, $b(df)$, $c(df)$ und $(d+e)(f+g)$ berechnen als

$$(dg + ef + bdf)x + eg + cdf = ((d+e)(f+g) + b(df) - df - eg)x + eg + c(df).$$

Es sind also zur Berechnung einer Multiplikation modulo $(n, x^2 - bx - c)$ genau 5 Multiplikationen modulo n nötig, sowie 6 Additionen, die wir als $o(1)$ Multiplikationen zählen. □

Lemma 3.27. *Für eine Multiplikation von $dx + e \in \mathbb{Z}[x]/(n, x^2 - bx - c)$ mit x sind $2 + o(1)$ Multiplikationen modulo n nötig.*

Beweis. Wir haben

$$(dx + e)x = dx^2 + ex \equiv d(bx + c) + ex = (bd + e)x + cd \mod (n, x^2 - bx - c),$$

wofür wir nur die Produkte bd und cd berechnen müssen. Damit genügen $2 + o(1)$ Multiplikationen modulo n. □

Definition 3.28. Seien $(A_j)_j, (B_j)_j, (C_j)_j \subseteq \mathbb{Z}[x]/(n, x^2 - bx - c)$ Folgen. Nehmen wir an, wir können (A_{2j}, B_{2j}, C_{2j}) aus (A_j, B_j, C_j) berechnen. Diese Art von Berechnung nennen wir *Verdopplung*. Können wir für $j \neq k$ das Tripel $(A_{j+k}, B_{j+k}, C_{j+k})$ aus (A_j, B_j, C_j) und (A_k, B_k, C_k) berechnen, so nennen wir diese Berechnung eine *Kettenaddition*.

Lemma 3.29. *Die Inverse α^{-1} eines Elements $\alpha \in \mathbb{Z}[x]/(n, x^2 - bx - c)$, $f \neq 0$, können wir, sofern sie existiert, in höchstens $7 + I + o(1)$ Multiplikationen modulo n berechnen.*

Beweis. Seien $d, e \in \mathbb{Z}_n$ gegeben, so dass $\alpha = dx + e$ ist.

Fall 1. Sei $d = 0$, $e \neq 0$. Die Inverse ist gegeben durch e^{-1}, sofern e invertierbar ist. Dafür sind I Multiplikationen nötig.

Fall 2. Sei $d \neq 0$, $e = 0$. Ist d invertierbar, so ist $\alpha^{-1} = \frac{1}{cd}x - \frac{b}{cd}$, denn

$$dx\left(\frac{1}{cd}x - \frac{b}{cd}\right) \equiv d\frac{1}{cd}x^2 - d\frac{b}{cd}x \equiv \frac{b}{c}x + \frac{c}{c} - \frac{b}{c}x \equiv 1 \mod (n, x^2 - bx - c).$$

In diesem Fall sind also nur $2 + I + o(1)$ Multiplikationen nötig.

Fall 3. Seien $d, e \neq 0$. Dann ist die Inverse von α gegeben durch $\alpha^{-1} = -df^{-1}x + (bd+e)f^{-1}$, wobei $f := bde + e^2 - cd^2$ ist, denn wir haben

$$\begin{aligned}(dx + e)(-df^{-1}x + (bd + e)f^{-1}) &\equiv f^{-1}(-d^2(bx + c) + d(bd + e)x - dex + e(bd + e)) \\ &\equiv f^{-1}((-bd^2 + bd^2 + de - de)x + bde + e^2 - cd^2) \\ &\equiv f^{-1}f \equiv 1 \mod (n, x^2 - bx - c).\end{aligned}$$

Hierfür sind somit die folgenden Produkte zu berechnen: bd, $(bd)e$, e^2, d^2, d^2c, df^{-1} und $(bd + e)f^{-1}$. Damit sind $7 + I + o(1)$ Multiplikationen nötig. □

Ist eine der Zahlen $\alpha, \beta, \gamma < n$ in den obigen Fällen von Null verschieden, aber nicht invertierbar, so muss n zusammengesetzt sein. Tritt dieser Fall ein, können wir also den Test mit dem Ergebnis *zusammengesetzt* vorzeitig beenden.

Das folgende Lemma erlaubt es uns, die Laufzeitabschätzung in Lemma 3.31 gegenüber [Gra98] zu verbessern.

Lemma 3.30. *Sei n ungerade. Das Produkt $(2^{-1}d \mod n)$ lässt sich für jedes $d \in \mathbb{Z}_n$ innerhalb von $o(1)$ Multiplikationen modulo n berechnen.*

Beweis. Ist d gerade, so können wir $2^{-1}d$ durch einen Rechtsshift von d um ein Bit berechnen. Da n ungerade ist, ist sonst $d+n$ gerade und $2^{-1}(d+n) \equiv 2^{-1}d + 2^{-1}n \equiv 2^{-1}d \bmod n$. Also genügt in diesem Fall ein Rechtsshift und eine Addition um $(2^{-1}d \mod n)$ zu berechnen. □

Lemma 3.31. *Für alle $j \in \mathbb{N}$ seien*

$$\begin{aligned} A_j &\equiv x^j + (b-x)^j \mod (n, x^2 - bx - c), \\ B_j &\equiv \frac{x^j - (b-x)^j}{2x-b} \mod (n, x^2 - bx - c) \text{ und} \\ C_j &\equiv c_j \mod (n, x^2 - bx - c). \end{aligned}$$

Kennen wir $b^2 + 4c$, so können wir $(A_{j+k}, B_{j+k}, C_{j+k})$ für beliebige $j, k \in \mathbb{N}$, $j \neq k$, aus (A_j, B_j, C_j) und (A_k, B_k, C_k), sowie (A_{2j}, B_{2j}, C_{2j}) aus (A_j, B_j, C_j) bestimmen.

Die Kettenaddition benötigt dabei $6 + o(1)$ Multiplikationen modulo n, die Verdopplung $3 + o(1)$. Wir können aus (A_1, B_1, C_1) das Tupel (A_j, B_j, C_j) berechnen in $(3 + o(1)) \log_2 j$ Multiplikationen modulo n.

Aus (A_j, B_j) können wir zudem x^j mit $1 + o(1)$ Multiplikationen berechnen.[18]

Beweis. Es gilt

$$\begin{aligned} A_{j+k} &= x^{j+k} + (b-x)^{j+k} \\ &= 2^{-1}\Big(x^{j+k} + x^j(b-x)^k + (b-x)^j x^k + (b-x)^{j+k} \\ &\qquad + x^{j+k} - x^j(b-x)^k - (b-x)^j x^k + (b-x)^{j+k}\Big) \\ &= 2^{-1}\left(A_jA_k + \frac{b^2+4c}{b^2+4c}\left(x^j - (b-x)^j\right)\left(x^k - (b-x)^k\right)\right) \\ &= 2^{-1}\left(A_jA_k + \left(b^2+4c\right)B_jB_k\right), \\ B_{j+k} &= \frac{x^{j+k} - (b-x)^{j+k}}{2x-b} \\ &= \frac{1}{2(2x-b)}\Big(x^{j+k} + (b-x)^j x^k - x^j(b-x)^k - (b-x)^{j+k} \\ &\qquad + x^{j+k} + (b-x)^k x^j - x^k(b-x)^j - (b-x)^{j+k}\Big) \\ &= 2^{-1}\left(\left(x^j + (b-x)^j\right)\frac{x^k - (b-x)^k}{2x-b} + \left(x^k + (b-x)^k\right)\frac{x^j - (b-x)^j}{2x-b}\right) \\ &= 2^{-1}(A_jB_k + A_kB_j) \end{aligned}$$

und $C_{j+k} = C_jC_k$. Zählt man nun die nötigen Multiplikationen, so kommt man, unter Verwendung von Lemma 3.30, auf $6 + o(1)$, nämlich 3 für die Berechnung von A_{j+k}, 2 für

[18] vgl. Proposition 3.3 in [Gra98]. Die hier bewiesene Laufzeitabschätzung ist etwas besser als Granthams, was auf die Ersparnis bei der Multiplikation mit 2^{-1} zurückzuführen ist. So erhält Grantham zwar auch $3 + o(1)$ Multiplikationen pro Verdopplung, aber $8 + o(1)$ Multiplikationen pro Kettenaddition und $2 + o(1)$ Multiplikationen für die Berechnung von x^j aus (A_j, B_j).

die Berechnung von B_{j+k} und 1 für die Berechnung von C_{j+k}. 2^{-1} kann man zu Beginn des Tests berechnen und speichern.

Für die Verdopplung haben wir

$$\begin{aligned} A_{2j} &= A_{2j} + 2(-c)^j - 2(-1)^j c^j \\ &\equiv A_{2j} + 2(bx - (bx+c))^j - 2(-1)^j c^j \\ &= x^{2j} + (b-x)^{2j} + 2(bx - x^2)^j - 2(-1)^j c^j \\ &= x^{2j} + 2x^j(b-x)^j + (b-x)^{2j} - 2(-1)^j c^j \\ &= A_j^2 - 2(-1)^j C_j, \end{aligned}$$

$B_{2j} = x^{2j} - (b-x)^{2j} = \left(x^j + (b-x)^j\right)\left(x^j - (b-x)^j\right) = A_j B_j$ und $C_{2j} = C_j^2$. Wegen $2(-1)^j C_j = \pm(C_j + C_j)$ kommen wir bei einer Verdopplung mit $3 + o(1)$ Multiplikationen aus.

Offenbar ist $A_1 = x + (b-x) = b \in \mathbb{Z}_n$, $B_1 = \frac{x-(b-x)}{2x-b} = \frac{2x-b}{2x-b} = 1 \in \mathbb{Z}_n$ und $C_1 = c \in \mathbb{Z}_n$. Angenommen $A_j, B_j \in \mathbb{Z}_n$. Dann ist nach der Formel für die Kettenaddition

$$\begin{aligned} A_{j+1} &= 2^{-1}\left(A_j A_1 + (b^2 + 4c) B_j B_1\right) \in \mathbb{Z}_n, \\ B_{j+1} &= 2^{-1}\left(A_j B_1 + A_1 B_j\right) \in \mathbb{Z}_n \quad \text{und} \\ C_{j+1} &= C_j C_1 \in \mathbb{Z}_n. \end{aligned}$$

Damit sind $A_j, B_j, C_j \in \mathbb{Z}_n$ für alle $j \in \mathbb{N}$.

Da $A_j, B_j \in \mathbb{Z}_n$, haben wir $x^j = B_j x + 2^{-1}(A_j - bB_j)$. Wir können also x^j, gemäß Lemma 3.30, aus (A_j, B_j) in $1 + o(1)$ Multiplikationen berechnen. Man beachte, dass für $B_j x$ keine Multiplikation nötig ist, da $B_j \in \mathbb{Z}_n$ ist.

Beginnend mit (A_1, B_1, C_1) können wir (A_j, B_j, C_j) laut [Knu97] mit $(1 + o(1)) \log_2 j$ Schritten (Verdopplungen und Kettenadditionen) berechnen. Nun sind $o(\log n)$ dieser Schritte keine Verdopplungen, da die durchschnittle Anzahl der 1-Bits durchschnittlich für große j sehr deutlich kleiner als $\log_2 j$ ist. Also können wir (A_j, B_j, C_j) in $(3+o(1)) \log_2 j$ Multiplikationen berechnen. Asymptotisch ist also die durchschnittliche Laufzeit 3 selfridge. □

Bei der binären Exponentiation treten, außer Verdopplungen, nur Kettenadditionen mit $k = 1$ auf. Daher liegen in diesem Fall die Kosten für eine Kettenaddition statt $6 + o(1)$ Multiplikationen bei nur $4 + o(1)$ Multiplikationen modulo n.

Satz 3.32. *Der* RQFT *hat eine Laufzeit von* 3 selfridge.[19]

Beweis. Sei $n \in \mathbb{N}$ eine beliebige ungerade Zahl mit $n > 3$. Die Schritte (1) und (2) können wir in einer konstanten Anzahl von Multiplikationen modulo n erledigen. Ebenso beläuft sich der zeitliche Aufwand für das Finden eines gültigen Parameterpaars auf eine konstante Anzahl von Multiplikationen. Wird kein solches Paar gefunden, hat n einen Primfaktor $p < B$ oder ist n ein Quadrat, so ist der Test hier schon beendet, hat also eine Laufzeit von $\mathcal{O}(1)$ Multiplikationen modulo n.

Sei (b, c) ein gültiges Parameterpaar. Für die Schritte (3), (4) und (5) des quadratischen Frobenius-Tests betrachten wir getrennt die Fälle $n \equiv 1 \bmod 4$ und $n \equiv 3 \bmod 4$.

[19] vgl. Theorem 3.4 in [Gra98].

Fall 1. Sei $n \equiv 1 \bmod 4$. Schreiben wir $n-1 = 2^{r'}s'$ mit einer ungeraden Zahl s'. Dann ist $n^2-1 = (n-1)(n+1) = 2^{r'}s'(2^{r'}s'+2) = 2^{r'+1}(2^{r'-1}s'^2+s') = 2^r s$ mit $r = r'+1$ und $s = 2^{r'-1}s'^2 + s'$. Sei $t = \frac{s'-1}{2}$.

Laut Lemma 3.31 können wir (A_t, B_t, C_t) in $(3+o(1))\log_2 t$ Multiplikationen berechnen. Daraus können wir $(A_{s'}, B_{s'}, C_{s'})$ in $3+8+o(1)$ Multiplikationen modulo n bestimmen. Mit $r'-1$ Verdopplungen können wir nun $\left(A_{\frac{n-1}{2}}, B_{\frac{n-1}{2}}, C_{\frac{n-1}{2}}\right)$ in $(3+o(1))(r'-1)$ Multiplikationen modulo n berechnen. Weitere $1+o(1)$ Multiplikationen liefern $x^{\frac{n-1}{2}}$, woraus wir durch Multiplikation mit x in $2+o(1)$ Multiplikationen $x^{\frac{n+1}{2}}$ ermitteln können. Alle Berechnungen für Schritt (3) sind damit erledigt.

Für Schritt (4) müssen wir lediglich $x^{\frac{n+1}{2}}$ quadrieren. Da Schritt (4) nur ausgeführt wird, wenn $x^{\frac{n+1}{2}} \equiv d \mod (n, x^2-bx-c)$ ist für ein $d \in \mathbb{Z}$, ist zur Berechnung von $x^{n+1} = d^2$ nur 1 Multiplikation modulo n nötig.

Schritt (5) wird nur dann ausgeführt, wenn $x^{n+1} \equiv -c \bmod (n, x^2-bx-c)$ ist. Daraus folgt, wie in Lemma 2.6 gezeigt, dass $x^n \equiv b-x \bmod (n, x^2-bx-c)$ ist. Sei

$$\sigma\colon \mathbb{Z}[x]/(n, x^2-bx-c) \to \mathbb{Z}[x]/(n, x^2-bx-c)$$

der durch $x \mapsto b-x$ definierte Homomorphismus. Dann ist

$$x^{nt} = (x^n)^t \equiv (b-x)^t \equiv \sigma(x)^t \equiv \sigma(x^t) \mod (n, x^2-bx-c).$$

Nun haben wir

$$\begin{aligned} s = 2^{r'-1}s'^2 + s' &= \frac{(2^{r'}s'+2)(s'-1) + 2^{r'}s' + 2}{2} \\ &= (2^{r'}s'+1)\frac{s'-1}{2} + \frac{s'-1}{2} + \frac{2^{r'}s'+2}{2} = nt + t + \frac{n+1}{2}. \end{aligned}$$

Also gilt für alle $0 \le e < r$

$$\begin{aligned} 2^{e+1}s = 2^{e+1}\left((n+1)t + \frac{n+1}{2}\right) &= 2^{e+1}(n+1)\frac{s'-1}{2} + 2^{e+1}\frac{n+1}{2} \\ &= 2^e ns' - 2^e n + 2^e s' - 2^e + 2^e n + 2^e = n2^e s' + 2^e s'. \end{aligned}$$

Damit können wir x^s schreiben als $x^s \equiv x^{nt}x^t x^{\frac{n+1}{2}} \equiv \sigma(x^t)x^t x^{\frac{n+1}{2}} \bmod (n, x^2-bx-c)$. $x^{\frac{n+1}{2}}$ haben wir bereits berechnet. Da wir auch (A_t, B_t) schon berechnet haben, können wir x^t in $1+o(1)$ Multiplikationen bestimmen. Seien nun $d, e \in \mathbb{Z}_n$ gegeben, so dass $x^t \equiv dx+e \bmod (n, x^2-bx-c)$ ist. Somit können wir $\sigma(x^t)$ berechnen als

$$\sigma(x^t) \equiv \sigma(dx+e) \equiv \sigma(d)\sigma(x) + \sigma(e) \equiv d(b-x) + e \equiv -dx + bd + e \mod (n, x^2-bx-c),$$

wofür eine Addition, eine Subtraktion und eine Multiplikation, also $1+o(1)$ Multiplikationen modulo n nötig sind.

Das Produkt $x^s \equiv \sigma(x^t)x^t x^{\frac{n+1}{2}}$ können wir mit weiteren 2 Multiplikationen modulo (n, x^2-bx-c), also $2(5+o(1)) = 10+o(1)$ Multiplikationen modulo n, berechnen.

Es sind also noch höchstens $x^{2s}, x^{2^2 s}, \ldots, x^{2^{r-1}s}$ zu berechnen. Da

$$x^{2^{e+1}s} \equiv x^{n2^e s'} x^{2^e s'} \equiv \sigma\left(x^{2^e s'}\right) x^{2^e s'} \bmod (n, x^2-bx-c)$$

ist und da wir $(A_{2^e s'}, B_{2^e s'})$ im Rahmen der Berechnung von x^{n+1} bereits berechnet haben, können wir, statt diese Potenzen von x^s durch wiederholtes Quadrieren eine nach der

anderen zu berechnen, einzelne dieser Potenzen direkt berechnen. Um zu entscheiden, ob n eine Primzahl sein könnte, ist festzustellen, ob $x^{2^j s} \equiv -1 \bmod (n, x^2 - bx - c)$ ist für ein $0 \le j \le r-2$. Weil aus $x^{2^j s} \equiv -1 \bmod (n, x^2-bx-c)$ folgt, dass $x^{2^k s} \equiv 1 \bmod (n, x^2-bx-c)$ für alle $k > j$, können wir nach einem solchen Index mithilfe einer binären Suche Ausschau halten.

Wir berechnen also $x^{2^e s'}$ für $e = \lfloor \frac{r'-1}{2} \rfloor - 1$ aus $(A_{2^e s'}, B_{2^e s'})$ in $1+o(1)$ Multiplikationen, daraus $\sigma\big(x^{2^e s'}\big)$ in $1+o(1)$ Multiplikationen und das Produkt der beiden in weiteren $5+o(1)$ Multiplikationen modulo n.

Ist $x^{2^{e+1}s'} \equiv \sigma\big(x^{2^e s'}\big) x^{2^e s'} \equiv -1 \bmod (n, x^2-bx-c)$, so wissen wir, dass (b, c) kein Zeuge für die Zusammengesetztheit von n ist und können die Berechnung beenden. Wenn jetzt $x^{2^{e+1}s'} \equiv 1 \bmod (n, x^2 - bx - c)$ ist, wissen wir sicher, dass $x^{2^j s'} \equiv -1 \bmod (n, x^2 - bx - c)$ nur für $j \le e$ gelten kann. Wir setzen also die Suche bei $\lfloor \frac{e}{2} \rfloor$ fort. Falls $x^{2^{e+1}s'} \not\equiv \pm 1$ ist, so kann $x^{2^j s'} \equiv -1 \bmod (n, x^2 - bx - c)$ nur für $j > e+1$ gelten und wir setzen die Suche bei $\lfloor \frac{e+r'-1}{2} \rfloor$ fort. Dies wiederholen wir, bis wir auf ein j mit $x^{2^j s'} \equiv -1 \bmod (n, x^2 - bx - c)$ stoßen, oder uns sicher sein können, dass es kein solches j gibt.

Da wir maximal $\log_2(r-2)$ der Potenzen von x^s berechnen müssen, sind für die binäre Suche nicht mehr als $(7+o(1))\log_2 r'$ Multiplikationen modulo n nötig.

Ist $n \equiv 1 \bmod 4$, so sind alles in Allem

$$\begin{aligned}
&\underbrace{\mathcal{O}(1)}_{\text{Schritt (1), (2)}} + \underbrace{(3+o(1))\log_2 t + (3+8+o(1)) + (3+o(1))(r'-1) + (1+o(1)) + (2+o(1))}_{(3)} \\
&\quad + \underbrace{1}_{(4)} + \underbrace{(1+o(1)) + (1+o(1)) + (10+o(1)) + (7+o(1))\log_2 r}_{(5)} \\
&= \mathcal{O}(1) + (3+o(1))\log_2 t + (7+o(1))\log_2 r + (3+o(1))(r'-1)
\end{aligned}$$

Multiplikationen nötig. Ferner sind $\log_2 t, \log_2 r \in \Theta(\log\log n)$ und $r' - 1 \in \Theta(\log n)$. Die gesamte Laufzeit ist somit $(3+o(1))\log_2 n$, also 3 selfridge.

Fall 2. Sei $n \equiv 3 \bmod 4$. Wir schreiben nun $n+1 = 2^{r'} s'$ und setzen $t = \frac{s'-1}{2}$. Dann ist $n^2 - 1 = 2^{r'+1}(2^{r'-1}s'^2 - s')$, also $r = r'+1$ und $s = 2^{r'-1}s'^2 - s'$ wie oben.

Nun können wir (A_t, B_t, C_t) und $(A_{s'}, B_{s'}, C_{s'})$ wie im vorherigen Fall in insgesamt $(3+o(1))\log_2 t$ Multiplikationen berechnen. Daraus können wir mit $r'-1$ Verdopplungen $\big(A_{\frac{n+1}{2}}, B_{\frac{n+1}{2}}, C_{\frac{n+1}{2}}\big)$ berechnen, was wiederum $(3+o(1))(r'-1)$ Multiplikationen erfordert. Aus diesem Tupel können wir $x^{\frac{n+1}{2}}$ in $1+o(1)$ Multiplikationen berechnen. Dadurch sind wir mit Schritt (3) fertig. Nun erhalten wir x^{n+1} durch einmaliges Quadrieren und auch Schritt (4) ist erledigt. Die Laufzeit ist also, bis hierher, 3 selfridge, wie bei $n \equiv 1 \bmod 4$.

Für Schritt (5) haben wir nun[20]

$$\begin{aligned}
s &= 2^{r'-1}s'^2 - s' = 2^{r'-1}s'^2 - 2^{r'-1}s' + 2^{r'-1}s' - s' \\
&= 2^{r'-1}s'(s'-1) - \frac{s'-1}{2} + 2^{r'-1}s' + \frac{s'-1}{2} - s' \\
&= (2^{r'}s' - 1)\frac{s'-1}{2} + 2^{r'-1}s' + \frac{s'-1}{2} - s' \\
&= nt + \frac{n+1}{2} + t - (2t+1) = nt + \frac{n+1}{2} - (t+1).
\end{aligned}$$

[20] In [Gra98, S. 12] steht an dieser Stelle fälschlicherweise $s = nt + t + \frac{n+1}{2}$, weshalb Grantham die Laufzeit für die Berechnung der Inversen nicht betrachtet.

Wieder können wir $x^{nt} = \sigma(x^t)$ berechnen. Aus x^t können wir x^{t+1} mit 5 Multiplikationen berechnen. Die Inverse x^{-t-1} kann nun, laut Lemma 3.29, in $7 + I + o(1)$ Multiplikationen berechnet werden. Zu den $(3 + o(1)) \log_2 n$ Multiplikationen, die wir auf in Fall 1 erhalten, kommen also nur $\mathcal{O}(1)$ Multiplikationen hinzu.

Weiterhin ist, wie im vorherigen Fall, $2^{e+1}s = n2^e s' - 2^e s'$.[21] Das erlaubt auch hier die Verwendung einer binären Suche, für die wiederum höchstens $\mathcal{O}(\log \log n)$ Multiplikationen modulo n nötig sind. Dies ist jedoch in $o(1) \log_2 n$ enthalten, so dass die gesamte Laufzeit auch in diesem Fall 3 selfridge beträgt. □

Bei Eingaben mit hohem Hamming-Gewicht,[22] wie etwa bei Mersenne-Zahlen, sind etwa gleich viele Kettenadditionen wie Verdopplungen nötig. In solchen Fällen werden also die $4 + o(1)$ Multiplikationen pro Kettenaddition, die zusätzlich zu den $3 + o(1)$ Multiplikationen pro Verdopplung anfallen, durchaus ins Gewicht fallen. Es ist dann mit einer Laufzeit von bis zu 7 selfridge zu rechnen. Dies werden wir in Abschnitt 4.2 auch bei der realen Implementierung beobachten können.

[21] Bei GRANTHAM fehlt „+1“ im Exponenten

[22] Das *Hamming-Gewicht* einer Zahl k ist die Anzahl der 1-Bits in der Binärdarstellung.

Kapitel 4

Experimentelle Resultate

Zur Auswertung wurde im Rahmen dieser Arbeit der RQFT mithilfe der GNU Multiple Precision Arithmetic Library (`GMP`) in `C` implementiert. Ferner wurde, zum Vergleich, eine in gleichem Maße optimierte Implementierung des Miller-Rabin-Tests erstellt.

Im Wesentlichen ist die Implementierung des Miller-Rabin-Tests eine direkte Übersetzung des in Kapitel 2 beschriebenen Algorithmus. Beim RQFT wurde der Algorithmus aus Kapitel 3 mithilfe der in Abschnitt 3.4 beschriebenen Optimierungen implementiert.

Verzichtet wurde zum einen auf die Verwendung der binären Suchen in Schritt (5). Zu durchsuchen sind, bei den in dieser Arbeit getesteten Eingaben, Indizes $0 \leq j < r - 1$ für $r \in \Theta(\log \log n)$, wobei $\log \log n$ stets kleiner als 17 ist. Damit sind also für Schritt (5) bei linearer Suche höchstens 17 Quadrate zu berechnen. Die Ersparnis durch die Verwendung einer binären Suche ist also keinesfalls mehr als $(17-1)(5+o(1)) = 80+o(1)$ Multiplikationen modulo n. Verglichen mit den zehntausenden Multiplikationen modulo n, die für den gesamten RQFT anfallen, können wir den Einfluss der binären Suche auf die Laufzeit vernachlässigen.

Zum anderen werden statt dem Optimum näher kommenden Additionsketten relativ einfache, der binären Exponentiation entsprechende, Additionsketten verwendet. Wie in Abschnitt 3.4 schon erwähnt wirkt sich dies ungünstig auf die Anzahl der durchzuführenden Kettenadditionen aus. Dafür wird die Laufzeit pro Kettenaddition von $6 + o(1)$ auf $4 + o(1)$ Multiplikationen gesenkt.

Zusätzlich wurde die Laufzeit der `GMP`-Funktion `mpz_probab_prime_p` getestet, die, wie die beiden anderen Tests, eine Zahl daraufhin untersucht, ob sie zusammengesetzt ist. Dazu wird zunächst der Fermat-Test mit Basis 210 ausgeführt, dann die Teilbarkeit durch die Primzahlen p mit $2 < p < \log_2 n$ per Probedivision getestet. Falls die zu testende Zahl dabei noch nicht als zusammengesetzt erkannt wurde, wird schließlich der Miller-Rabin-Test durchgeführt.

4.1 Eingaben

Für die Messung der Laufzeit wurden vier verschiedene Eingabemengen verwendet.

- Zum einen wurden Primzahlen verschiedener Größe generiert, indem für verschiedene $k \in \mathbb{N}$ die kleinste Primzahl $p > 2^k$ gewählt wurde. Diese haben also ein führendes 1-Bit gefolgt von vielen Nullen und am Ende eine kleine Anzahl von Nullen und Einsen, besitzen also ein geringes Hamming-Gewicht.

  Möchte man die n-te (oder $(n \pm 1)$-te) Potenz einer solchen Zahl berechnen, sind also mit dem verwendeten binären Exponentiationsverfahren nur recht wenige Kettenadditionen

nötig. In diesem Fall ist also der Vorteil, der durch die Verwendung eines anderen Exponentiationsverfahrens erreicht werden könnte, relativ gering. Das Gleiche gilt für die Berechnung von (n^2-1)-ten Potenzen.

- Eine weitere Menge von Eingaben n waren die 21 Mersenne-Primzahlen $M_p = 2^p - 1$ mit $p = 61, 89, \ldots, 110\,503$. Diese haben, aufgrund ihrer Form, eine Binärdarstellung, die nur aus Einsen besteht.

  Die Berechnung der $(n+1)$-ten Potenz für die Schritte (3) und (4) ist in diesem Fall sehr günstig, schließlich ist $n + 1 = 2^p - 1 + 1 = 2^p$, es muss also nur quadriert werden. Für die Berechnung der (n^2-1)-ten Potenz erhält man wegen

  $$n^2 - 1 = (n-1)(n+1) = 2^p(2^p - 2) = 2^{p+1}(2^{p-1} - 1)$$

  eine Zahl, die in ihrer Binärdarstellung etwa zur Hälfte aus Einsen besteht. Der maximal zu erwartende Speedup durch einen anderen Algorithmus ist also kleiner als $\frac{1}{3}$.

- Getestet wurden zudem die kleinsten zusammengesetzten Zahlen $n > 2^k$ für einige $k \in \mathbb{N}$, die keine Primfaktoren $p < 44\,958$ haben. Dadurch ist sichergestellt, dass die Tests nicht schon bei der Probedivision feststellen, dass n zusammengesetzt ist, da dies zwar für die Best-Case-Laufzeit, aber nicht für die Worst-Case-Laufzeit relevant ist. Wie die kleinsten Primzahlen größer als 2^k, haben auch diese zusammengesetzten Zahlen ein sehr kleines Hamming-Gewicht und verursachen so beim Potenzieren wenig Arbeit.

- Zuletzt wurden noch die Mersenne-Zahlen M_p mit Primzahlen $p = 61, 67, \ldots, 1999$ getestet. Hier handelt es sich, bis auf sieben Ausnahmen (M_{61}, M_{89}, M_{107}, M_{127}, M_{521}, M_{607} und M_{1279}), um zusammengesetzte Zahlen. Wie die Mersenne-Primzahlen, haben diese Zahlen ein hohes Hamming-Gewicht, sorgen also beim Potenzieren für viel Arbeit.

4.2 Laufzeit-Messungen

Nun zur Messung der Laufzeiten. Zur Messung werden die drei Algorithmen auf die verschiedenen Zahlen angewendet, und zwar jeweils so oft, dass für jede Zahl die kombinierte Laufzeit mindestens in der Größenordnung von einer Sekunde liegt. Dadurch wird der Einfluss kleiner Ungenauigkeiten bei der Bestimmung der genauen Zeit auf die Genauigkeit des Ergebnisses verhindert. Vor einer Messung werden dazu einige Iterationen durchgeführt, um zu ermitteln, wie viele Iterationen zum Erreichen einer Laufzeit von etwa einer Sekunde nötig sind. Dieses vorherige Ausführen des Tests sorgt dafür, dass sowohl die Daten, als auch der Maschinencode für den Test in den jeweiligen Caches liegen, soweit das möglich ist.

Es werden dann zehn Messungen gemacht, bei denen jeweils die nach obigem Prinzip festgelegte Anzahl von Wiederholungen des Tests durchgeführt werden. Dabei wird der gesamte Test wiederholt ausgeführt, anstatt die Vorberechnung nur einmal auszuführen. Dies ist insbesondere bei zusammengesetzten Zahlen mit Primfaktoren kleiner als B wichtig. Bei diesen würde sonst keine einzige Iteration des Haupttests und die Vorberechnung nur einmal durchgeführt.

Der bei den Laufzeitmessungen aufgetretene Messfehler ist sehr gering, wie man in Abbildung A.1 erkennen kann. Auf die Messfehler gehen wir daher im Hauptteil dieser Arbeit nicht weiter ein.

Man kann bereits erkennen, dass die Laufzeit des selbst implementierten Miller-Rabin-Tests etwa die Hälfte der Laufzeit von `GMP`s `mpz_probab_prime_p` ist. Ebenso kann man

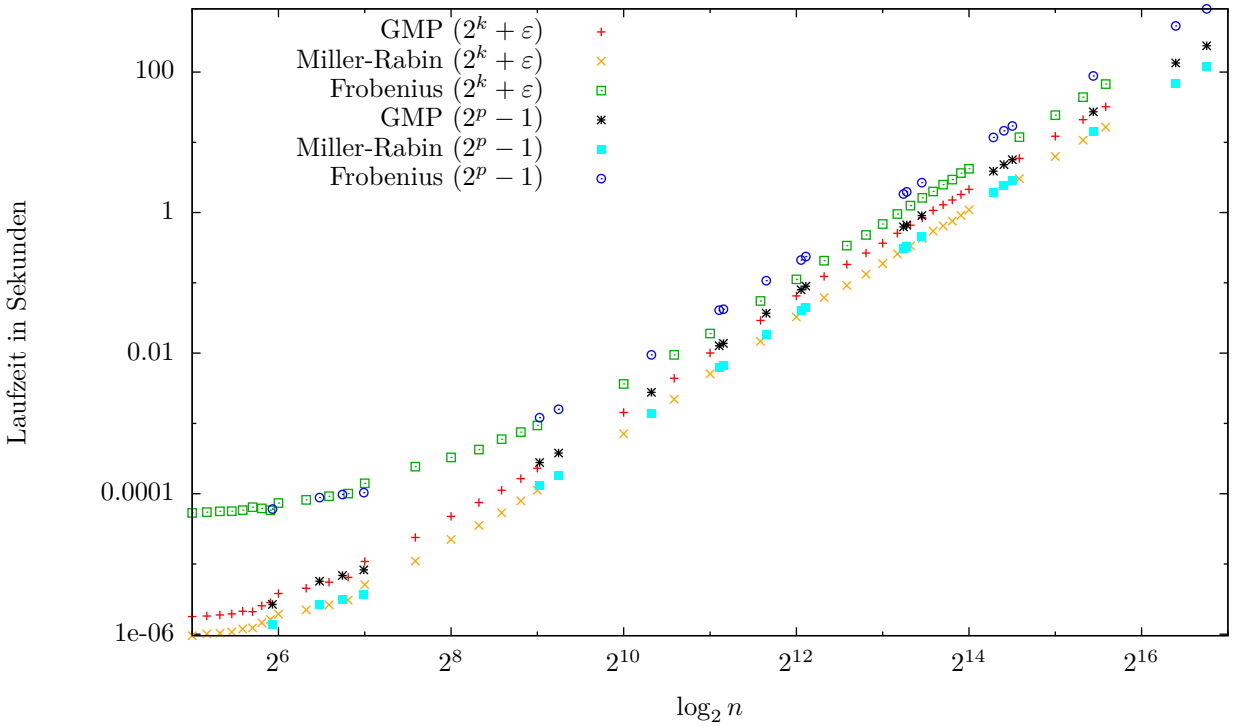

Abbildung 4.1: Hier sind die Laufzeiten der Tests bei Primzahlen der Form $2^k + \varepsilon$, sowie bei Mersenne-Primzahlen zu sehen.

sehen, dass der quadratische Frobenius-Test stets erheblich länger läuft als die anderen Tests. Bei genauerem Hinschauen kann man zudem sehen, dass die Laufzeit bei den Mersenne-Primzahlen, also Zahlen mit großem Hamming-Gewicht, etwas größer ist als die bei den Primzahlen mit kleinem Hamming-Gewicht.

Besser erkennen können wir diesen Unterschied in der Laufzeit in Abbildung 4.2 auf der nächsten Seite, in dem die bezüglich des Miller-Rabin-Tests normalisierte Laufzeit zu sehen ist. Hier ist erkennbar, dass die Laufzeit des RQFT für hinreichend große Zahlen von kleinem Hamming-Gewicht etwa die vierfache des Miller-Rabin-Tests ist. Bei großem Hamming-Gewicht liegt dieser Faktor bei etwa 6.5. Wir haben $\frac{1}{4^7} < \frac{1}{7710} < \frac{1}{4^6}$. Damit bringt also der RQFT bei vergleichbarer Laufzeit keine wesentlich geringere Fehlerwahrscheinlichkeit bei Zahlen von großem Hamming-Gewicht. Im Gegensatz dazu ist die Fehlerwahrscheinlichkeit bei vier Iterationen des Miller-Rabin-Tests $\frac{1}{4^4} = \frac{1}{256}$ und damit deutlich größer, als die Fehlerwahrscheinlichkeit bei einer Iteration des RQFT, obwohl die Laufzeiten bei Zahlen mit kleinem Hamming-Gewicht in etwa übereinstimmen.

In Abbildung 4.3 auf Seite 37 kann man sehen, wie sich der Aufbau einer Zahl auf die Anzahl der durchzuführenden Multiplikationen beim RQFT auswirkt. Bei den Primzahlen der Form $2^k + \varepsilon$ für ein kleines ε ist die Anzahl der Multiplikationen dadurch, dass diese Zahlen ein geringes Hamming-Gewicht haben, kleiner als bei den Mersenne-Primzahlen, die ein recht hohes Hamming-Gewicht haben. Ebenso kann man erkennen, dass die Anzahl der durchzuführenden Multiplikationen bei sämtlichen zusammengesetzten Zahlen erheblich kleiner als bei den Primzahlen ist. Dies ist darauf zurückzuführen, dass der Test bei zusammengesetzten

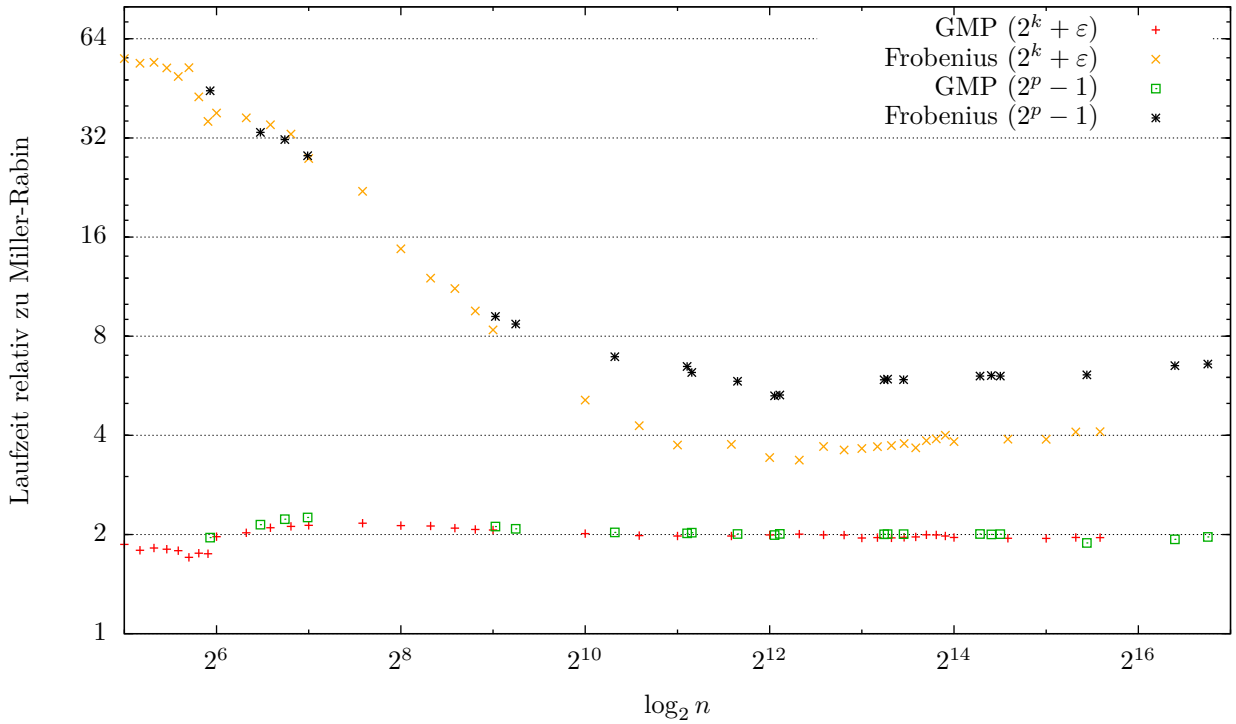

Abbildung 4.2: Normalisierte Laufzeit bei Primzahlen

Zahlen vorzeitig abbrechen kann, etwa schon nach Schritt (3), was bei Primzahlen nicht möglich ist.

4.3 Andere Messergebnisse

False positives Bei den insgesamt 11 525 571 035 Iterationen der verschiedenen Tests, die bei den zusammengesetzten Zahlen durchgeführt wurden, sind nur 2 false positives aufgetreten. Aufgetreten sind diese bei der Anwendung des Miller-Rabin-Tests auf kleine zusammengesetzte Zahlen. Dort gibt es zum einen weniger Basen, die ausgewählt werden könnten, zum anderen werden bei kleinen Zahlen mehr Iterationen des Tests durchgeführt, da die Zeit, die für eine Iteration benötigt wird, deutlich kleiner als bei großen Zahlen ist.

Ebenfalls getestet wurden die 3771 zusammengesetzten Zahlen n mit $3 \leq n < 10\,000$ mit allen möglichen Parameterpaaren. Auch die in der Beschreibung des Algorithmus eigentlich ausgeschlossenen Paare mit $b = 0$ wurden dabei getestet. Dabei sind insgesamt 1938 false positives aufgetreten. Von den Parameterpaaren (b, c) bei den false positives, war nur bei 54 Stück $b \neq 0$. Weiterhin fällt auf, dass nur für $n \equiv 3 \bmod 4$ false positives aufgetreten sind. Insbesondere ist für $n \equiv 3 \bmod 4$ das Paar $(0, n-1)$ stets zulässig, aber nie ein Zeuge für die Zusammengesetztheit von n. Da wir aber $b = 0$ explizit ausschließen, bleiben kaum noch false positives übrig. Die verbleibenden Nichtzeugen (b, c) treten, zumindest in den getesteten Fällen, paarweise auf. Ist nämlich (b, c) ein Nichtzeuge, so ist auch $(n - b, c)$ ein Nichtzeuge.

Die Wahrscheinlichkeit bei der Auswahl eines Parameterpaars $(b, c) \in \mathbb{Z}_n^2$ keinen Zeugen

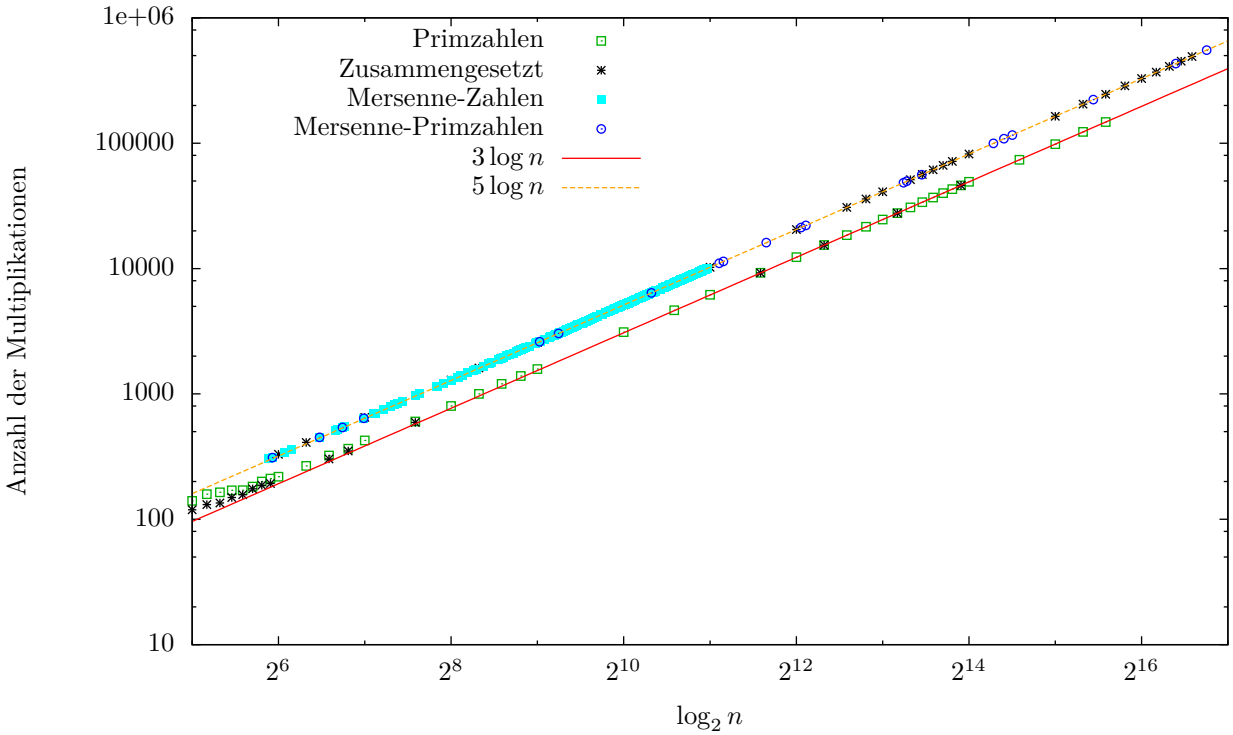

Abbildung 4.3: Anzahl der Multiplikationen

für die Zusammengesetztheit von n zu finden ist für $n = 455$ maximal. In diesem Fall gibt es 3 Nichtzeugen, aber $\varphi(455)^2 - 3 = 82\,941$ Zeugen für die Zusammengesetztheit von 455. Die Fehlerwahrscheinlichkeit ist also $\frac{3}{82941} = \frac{1}{27647}$, was deutlich kleiner als $\frac{1}{7710}$ ist. Letztere Schranke basiert auf der Annahme, dass die Primteiler von n alle größer als $B = 44\,958$ sind. Für Zahlen, die, wie etwa 455, sehr kleine Primteiler haben, könnten wir mit den in Kapitel 3 gezeigten Fehlerabschätzungen nur eine sehr viel schwächere Schranke für die Fehlerwahrscheinlichkeit beweisen. Ersetzen wir $B = 44\,958$ durch $B' = 4$, so erhalten wir unter Verwendung der Lemmata zu Theorem 3.16 folgende Abschätzung für die Fehlerwahrscheinlichkeit α:

$$\alpha < \begin{cases} \frac{4}{5} & \text{falls } n \text{ nicht quadratfrei ist (Lemma 3.17),} \\ \frac{1}{2} & \text{falls } n \text{ quadratfrei ist mit einer geraden Anzahl von Primfaktoren (Korollar 3.21),} \\ \frac{155}{416} & \text{falls } n \text{ quadratfrei mit genau drei Primfaktoren ist (Lemma 3.22),} \\ \frac{1}{2^{13}} + \frac{1}{2^{17}} + \frac{1}{4} & \text{falls } n \text{ quadratfrei ist mit genau } k \text{ Primfaktoren, wobei } k \text{ ungerade ist (Lemma 3.23).} \end{cases}$$

Selbst für quadratfreie Zahlen erhalten wir so also $\frac{1}{2}$ als obere Schranke für die Fehlerwahrscheinlichkeit. Auch für die ebenfalls getesteten Zahlen mit quadratischen Teilern scheint die tatsächliche Fehlerwahrscheinlichkeit sehr viel geringer zu sein. Nicht einmal für Vielfache von 9 war die tatsächliche Fehlerwahrscheinlichkeit größer als $\frac{1}{7710}$. Durch eine genauere

Analyse könnte man die bewiesene Schranke möglicherweise erheblich verbessern, wie auch Grantham in [Gra98, §4] vermutet.

Speicherbedarf Für den Miller-Rabin-Test müssen folgende Zahlen, die alle kleiner oder gleich n sind, gespeichert werden:

- die zu testende Zahl n selbst,
- eine ungerade Zahl s, so dass $2^r s = n - 1$,
- die zufällig gewählte Basis a und
- die aktuell betrachtete Potenz $a^{2^j d}$ für ein $j \in \{0, \ldots, r-1\}$.

Bei der Berechnung von a^d modulo n wird von `GMP` zusätzlich dazu Speicher für eine temporäre Variable belegt, die ebenfalls kleiner oder gleich n ist.

Wenn wir noch den Speicherbedarf für den auszuführenden Maschinencode und kleinere temporäre Variablen, etwa 64-Bit-Ganzzahlen, betrachten, so ist dieser in $o(1) \log_2 n$, da er unabhängig von n ist.

Damit liegt der Speicherbedarf bei etwa $(5 + o(1)) \log_2 n$ Bit.

Beim Frobenius-Test ist mehr Speicher nötig. Allein durch die Tatsache, dass modulo $(n, x^2 - bx - c)$ statt modulo n gerechnet wird, verdoppelt sich der Speicherbedarf an einigen Stellen. Aufgrund des komplexeren Algorithmus sind zudem mehr temporäre Variablen nötig.

Zu speichern sind

- die zu testende Zahl n und die beiden Parameter b und c,
- A_j, B_j, C_j für das aktuelle j,
- je zwei Koeffizienten für die Polynome $x^t, x^{(n+1)/2}$
- fünf temporäre Variablen.

Zusammen mit den Maschinen-Ganzzahlen und dem Maschinencode kommen wir somit auf einen Speicherbedarf von $(15 + o(1)) \log_2 n$ Bit.

Für alle getesteten Zahlen ist $\log_2 n < 110\,503$, so dass sich der gesamte Speicherbedarf auf etwa 202 kiB zuzüglich kleiner Variablen und Maschinencode beläuft. Das ist hinreichend wenig, um in den L2-Cache zu passen, der bei der verwendeten CPU 256 kiB groß ist. Andernfalls wäre auch, bei Überschreitung der Cache-Größe, ein sprunghafter Anstieg der Laufzeit zu erwarten.

Kapitel 5

Fazit

Wir können also zusammenfassend sagen, dass der RQFT für große Zahlen (ab etwa 1024 Bit) von kleinem Hamming-Gewicht dem Miller-Rabin-Test hinsichtlich der Fehlerwahrscheinlichkeit im Verhältnis zur Laufzeit überlegen ist. Für ebenso große Zahlen von hohem Hamming-Gewicht ist die vorliegende Implementierung vergleichbar mit mehreren Iterationen des Miller-Rabin-Tests. Wenn man jedoch, wie in Abschnitt 3.4 angenommen, bessere Additionsketten verwendet, die, verglichen mit dem binären Verfahren, mit weniger Multiplikationen auskommen, wäre wohl auch für Zahlen von hohem Hamming-Gewicht der RQFT überlegen.

Da heute für das RSA-Verschlüsselungsverfahren Schlüssel der Länge 2048 oder 4096 empfohlen werden, für welche man 1024 beziehungsweise 2048 Bit lange Primzahlen finden muss, ist der RQFT auch von praktischem Interesse.

Die obere Schranke für die Fehlerwahrscheinlichkeit des RQFT erscheint bei Betrachtung der Beweise in Abschnitt 3.3 nicht optimal zu sein. Eine genauere Untersuchung des Falls, dass n quadratfrei ist mit 5, 7 oder allgemein k Primfaktoren, wobei k ungerade ist, könnte eine erheblich schärfere Schranke zur Folge haben. Diese Vermutung wird auch durch die experimentelle Untersuchung der Anzahl der Nichtzeugen für zusammengesetzte Zahlen $9 \leq n < 10\,000$ untermauert.

Literaturverzeichnis

[Gra98] Grantham, Jon: A probable prime test with high confidence. In: *Journal of Number Theory* 72 (1998), Nr. 1, S. 32–47

[Knu69] Knuth, Donald E.: *The Art of Computer Programming, Volume 2 (1st Ed.): Seminumerical Algorithms*. Reading, MA, USA : Addison-Wesley Publishing Co., Inc., 1969. – ISBN 0–201–03802–1

[Knu97] Knuth, Donald E.: *The Art of Computer Programming, Volume 2 (3rd Ed.): Seminumerical Algorithms*. Reading, MA, USA : Addison-Wesley Longman Publishing Co., Inc., 1997. – ISBN 0–201–89684–2

[Rab80] Rabin, Michael O.: Probabilistic algorithm for testing primality. In: *Journal of Number Theory* 12 (1980), Nr. 1, S. 128–138

Anhang A

Messungen

A.1 Messfehler

Wie klein die bei der Messung der Laufzeit aufgetretenen Messfehler sind, kann man an Abbildung A.1 gut erkennen. Das Konfidenzintervall wurde folgendermaßen bestimmt. Sei μ das arithmetische Mittel der gemessenen Laufzeiten, σ die anhand der Messungen geschätzte Standardabweichung. Dann ist das Konfidenzintervall gegeben durch $[\mu - 5\sigma, \mu + 5\sigma]$.

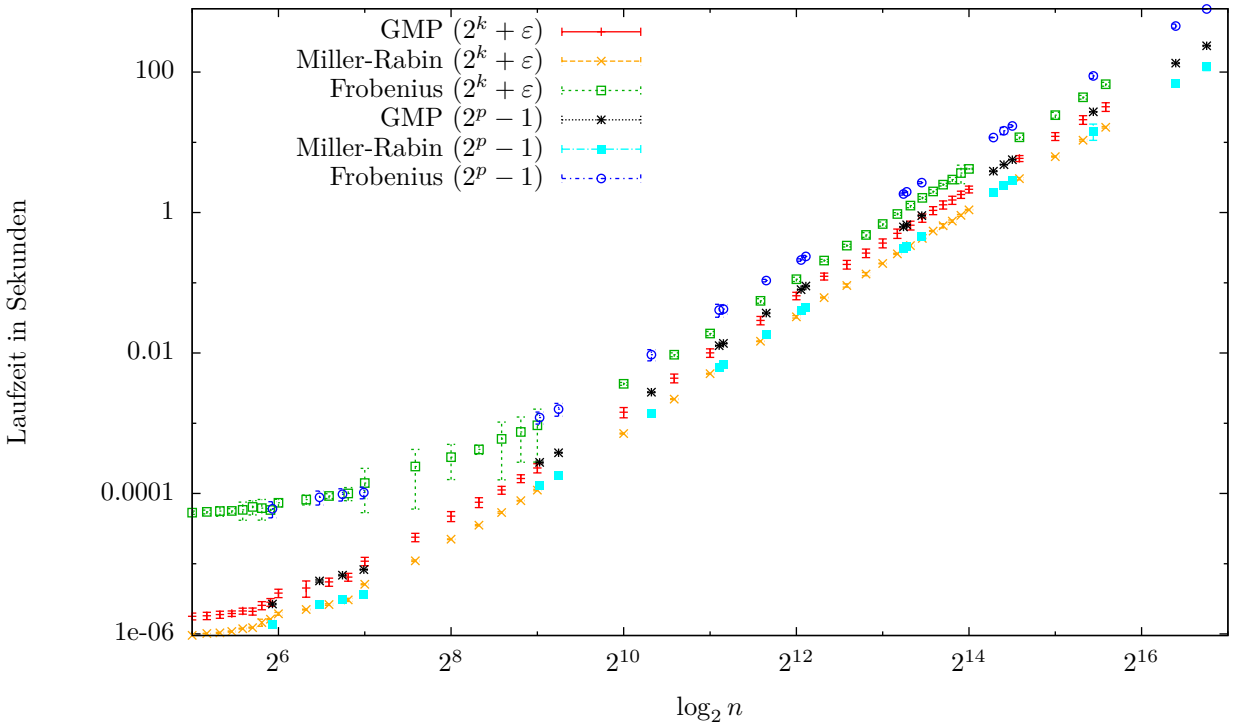

Abbildung A.1: Laufzeit mit Fehlerschranken bei Primzahlen

Wie in Abschnitt 4.2 beschrieben, ist der RQFT für Zahlen $n > 2^{10}$ schneller als der

Miller-Rabin-Test für n mit kleinem Hamming-Gewicht und etwa gleich schnell für Zahlen mit großem Hamming-Gewicht. Für diese Eingaben sind die, anhand der Verteilung der gemessenen Laufzeiten geschätzten, Messfehler sehr klein, die Unterschiede also statistisch signifikant. Genauer ist die Wahrscheinlichkeit, dass die tatsächliche Laufzeit, unter der Annahme einer Gleichverteilung der Messergebnisse, außerhalb des Konfidenzintervalls liegt, kleiner als 10^{-6}. Für zusammengesetzte Zahlen werden die Laufzeiten eine höhere Varianz aufweisen, da der Test, je nach gewähltem Parameterpaar, an unterschiedlichen Stellen beendet werden kann. Die Laufzeit bei Primzahlen ist also in gewissem Sinne die worst-case-Laufzeit, da stets *alle* Schritte des RQFT durchgeführt werden müssen.

A.2 Weitere Messergebnisse

Zusätzlich zu den in Kapitel 4 zu findenden Messergebnissen sind noch einige weitere Messungen gemacht worden.

Dazu zählt etwa die in Abbildung A.2 zu sehende Laufzeit bei zusammengesetzten Zahlen der Form $2^k + \varepsilon$, die keine Primfaktoren kleiner als $B = 44\,958$ haben. Die Laufzeiten ähneln denen bei den Primzahlen in Abbildung 4.1 auf Seite 35 aus, was nicht weiter verwundert. Schließlich ist es in jedem Fall nötig große Potenzen von x in $\mathbb{Z}[x]/(n, x^2 - bx - c)$ zu berechnen.

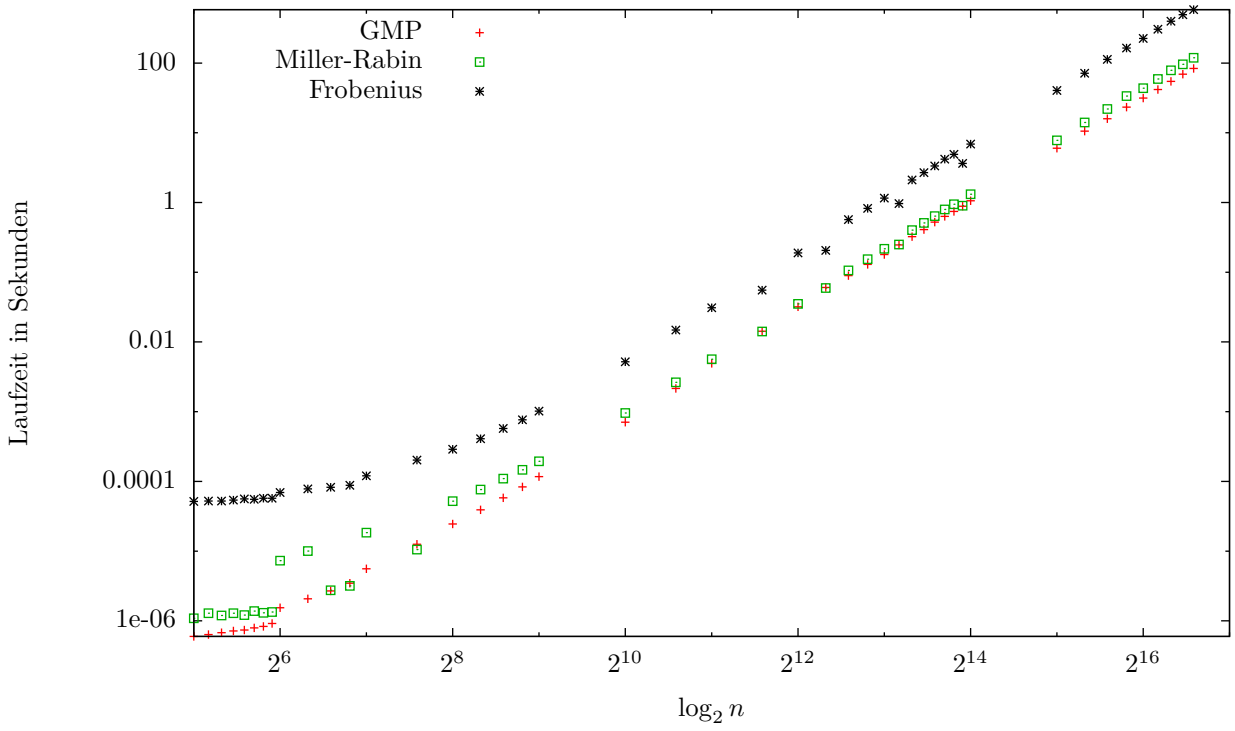

Abbildung A.2: Laufzeit bei zusammengesetzten Zahlen ohne kleine Primfaktoren

In Abbildung A.3 auf der nächsten Seite kann man deutlich die, im Vergleich zu den zusammengesetzten Mersenne-Zahlen, längere Laufzeit bei den Mersenne-Primzahlen erkennen.

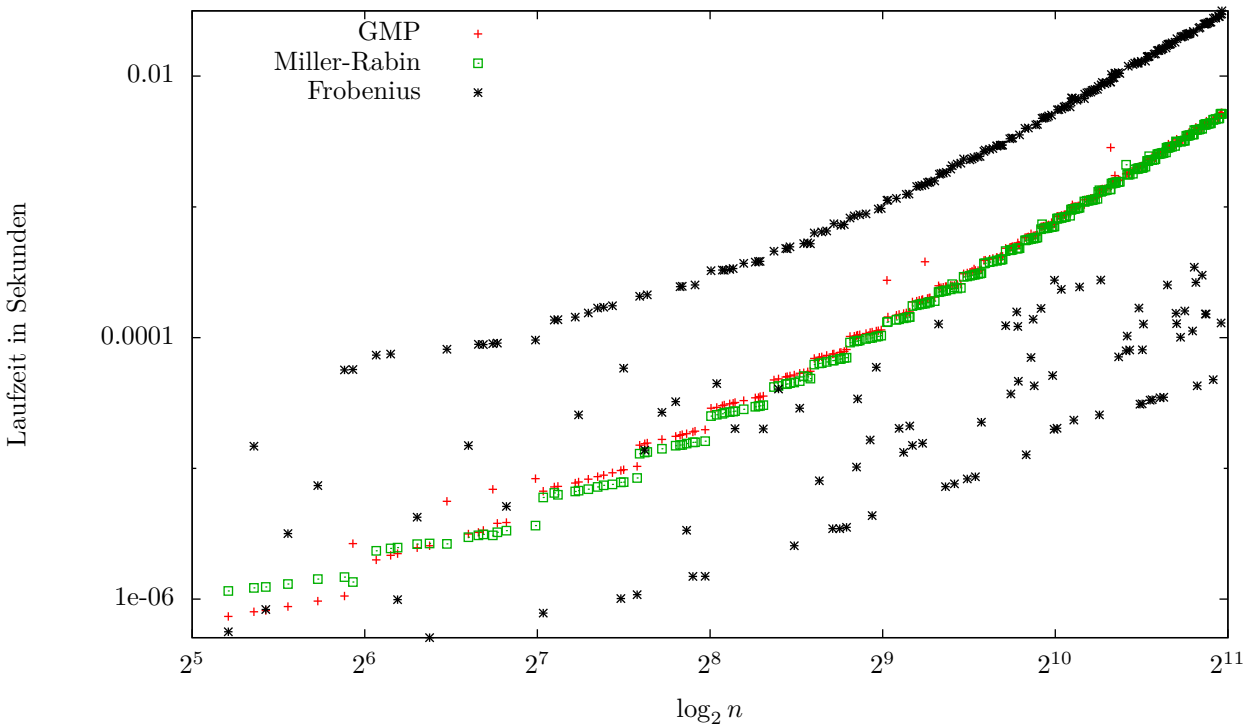

Abbildung A.3: Laufzeit bei Mersenne-Zahlen

Bei den beiden auf dem Miller-Rabin basierenden Tests kann man in dieser Abbildung gut sehen, dass die Laufzeit bei Vielfachen von 64 Bit sprunghaft größer wird. Beim Frobenius-Test ist davon kaum etwas zu erkennen, was aufgrund der deutlich höheren Gesamtlaufzeit zu erwarten ist. Die teilweise sehr kurze Laufzeit beim RQFT ist darauf zurückzuführen, dass einige der Zahlen durch Primzahlen $p < 44\,958$ teilbar sind. Diese Zahlen werden also schon in Schritt (1) als zusammengesetzt erkannt, so dass der Test extrem schnell beendet ist.

In Abbildung A.4 auf der nächsten Seite können wir sehen, dass die Laufzeiten bei Zahlen bis etwa $2^{2^{15}}$ gut zur Karatsuba-Multiplikation, die größeren eher zur Toom-Cook-Multiplikation passen. Dies deckt sich mit der Verwendung dieser Multiplikationsalgorithmen durch `GMP`. Dabei wird die Laufzeitabschätzung aus [Knu97, S. 302] zugrunde gelegt.

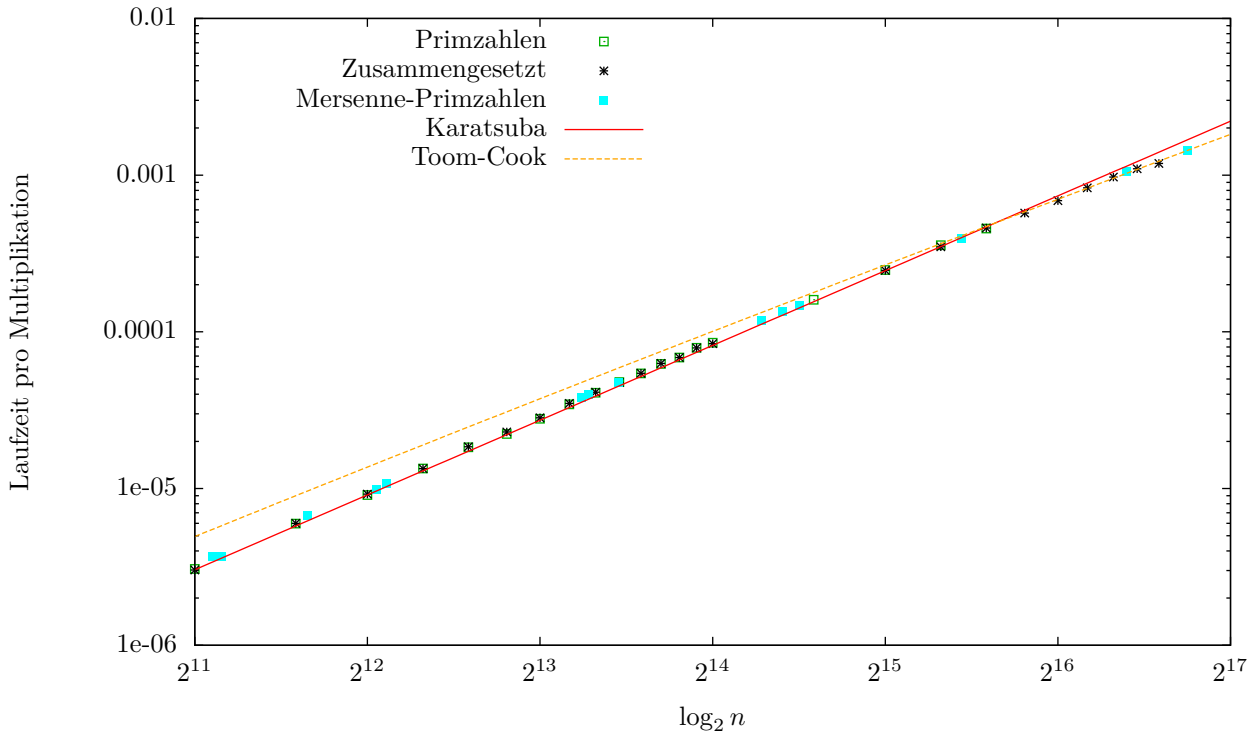

Abbildung A.4: Zeit pro Multiplikation

Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe, dass alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht sind und dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegt wurde.

Kreuztal, den 16. November 2014 _____