Probabilistische Primzahltests

Alexander von Felbert

06.12.2006

Inhaltsverzeichnis

Motivation, Überblick und Notation

Am 6 August 2002 veröffentlichten M. Agrawal, N. Kayal und N. Saxena ein Arbeit mit dem Titel „**PRIMES is in P**“ auf ihrer Institutswebseite der Universität Kanpur (Indien). Zwei Tage später machte sogar die New York Times diese spektakuläre wissenschaftliche Erkenntnis unter dem Titel '*New Method Said to Solve Key Problem In Math*' zum Thema.

> Three Indian computer scientists devise way for computers to tell quickly and definitively whether number is prime; existing algorithms are faster, but have small chance of giving either wrong answer or no answer at all; new algorithm is work of Manindra Agrawal, Neeraj Kayal and Nitin Sexena.

Bis zu diesem Zeitpunkt war kein *deterministischer* Algorithmus bekannt, welcher in polynomieller Zeit entscheiden konnte, ob eine vorgegebene (ganze) Zahl eine Primzahl oder eine zusammengesetzte Zahl ist. Diese Problemstellung bezeichnet man auch als „*primality problem*“ und Agrawal, Kayal sowie Sexena beschrieben in ihrer Ausarbeitung eine mögliche Lösung für diese Problemstellung - den nach den Initialen der Entdecker benannte AKS-Algorithmus.

Um Kryptosysteme sinnvoll einsetzen zu können, müssen diese gegenüber der Zeit- und Platzkomplexität gewisse Anforderungen erfüllen, insbesondere sollten sie effizient zu berechnen sein. Bei einigen Kryptosystemen (wie z.B. RSA) werden große Primzahlen benötigt, die somit als Teil eines Kryptoverfahrens ebenfalls effizient berechenbar sein müssen.

Das „primality problem“ beschäftigt die Menschheit bereits seit Jahrtausenden. Eratosthenes von Cyrene (276-196 v.Chr.), der im Jahr 235 v.Chr. Vorsteher der Bibliothek in Alexandria wurde, hat ein Verfahren beschrieben, mit welchem man alle Primzahlen unterhalb einer Schranke N bestimmen kann. Dieses Verfahren heißt zu Ehren seines Erfinders „Sieb des Eratosthenes“. Allerdings ist dieses, wie auch die Brute-Force-Methode (überprüfen der Definition), nicht effizient möglich.

Bemerkung 1*:*
Ist n eine zusammengesetzte Zahl, dann existiert ein Primteiler p von n mit $p \leq \sqrt{n}$.

Möchte man also prüfen, ob eine vorgegebene natürliche Zahl $n \in \mathbb{N}$ prim ist, so muss

lediglich festgestellt werden, ob sie durch eine (Prim-)Zahl $\leq \sqrt{n}$ teilbar ist. Bei einem naiven Ansatz testen wir also, ob die natürlichen Zahlen $1, 2, \ldots, \sqrt{n}$ Teiler der zu prüfenden Zahl n sind. Nun könnte man zunächst vermuten, dass die daraus resultierenden Kosten polynomiell beschränkt sind, da wir $\sqrt{n}$-mal eine Teilereigenschaft überprüfen müssen: Es stellt sich jedoch heraus, dass die Kosten zwar polynomiell beschränkt sind, allerdings in dem Eingabewert n, und *nicht* in der Eingabegröße (i.d.R. $\mathcal{O}(2^{log(n)})$).

Probabilistische Primzahltests können effizient, jedoch mit dem scheinbar bitteren Beigeschmack eines „Unsicherheitsfaktor“, entscheiden, ob eine vorgegebene Zahl prim ist. D.h. diese Testarten können diesbezüglich lediglich Aussagen treffen wie „Die Zahl ist wahrscheinlich prim“ oder aber „Die Zahl ist nicht prim“.

Namentlich werden wir folgende drei Primzahltests beschreiben

- Fermat-Test,
- Miller-Rabin-Test,
- Solovay-Strassen-Test.

Der Letztgenannte ist von gewisser historischer Bedeutung für die Mathematik und die Informatik, da dieser Test einen der ersten überhaupt bekannten probabilistischen Algorithmen beschreibt.

Wir werden zunächst den Fermat- und Miller-Rabin-Test behandeln, da diese eng miteinander verwandt sind bzw. aufeinander aufbauen. Dazu werden wir einige bedeutende Sätze der modularen Arithmetik, der Zahlentheorie und der Algebra benötigen und sie deshalb auch sogleich beweisen.

Das „Sahnestück“, den Solovay-Strassen-Test, werden wir abschließend untersuchen. Hierbei werden insbesondere die so genannten Jacobi- und Legendre-Symbole benötigt. Da eine umfassende Untersuchung dieses schönen Gebiets der Zahlentheorie allerdings den Rahmen dieser Arbeit sprengen würde, beschränken wir uns bescheiden, doch neugierig, auf die grundlegenden Ideen dieses Testverfahrens.

Elementare Definitionen oder Sätze, wie z.B. den Primzahlsatz, werden wir in diesem Dokument nicht wiederholen. Dem Leser sollten also Begriffe wie „Primzahl“ oder „Einheitengruppe“ bekannt sein und er sollte auch die elementarsten Sätze in diesem Kontext beherrschen. Wir bezeichnen eine natürliche Zahl n abkürzend als *prim*, wenn n eine Primzahl ist. Entsprechend bezeichnen wir eine Zahl als nicht prim, wenn diese Zahl entweder zusammengesetzt oder aber eine (additive oder multiplikative) Einheit ist. Restklassenringe notieren wir entweder mit $(\mathbb{Z}/n\mathbb{Z})$ oder abkürzend durch $\mathbb{Z}_n$. Das Kongruenz-Zeichen $\equiv \mod n$ werden wir auch häufig mit $\equiv_n$ abkürzend notieren.

Teil I.

Drei Primzahltests

Fermat-, Miller-Rabin- und der Solovay-Strassen-Test...

1. Grundsätzliches Vorgehen

Die Sicherheit der meisten Kryptosysteme basiert u.a. auf der *zufälligen* Wahl einer oder mehrerer großer Primzahlen.

Dabei soll die Wahl einer beliebigen Zahl n des Ausgangsraums $\mathbb{N}$ gleich wahrscheinlich und (stochastisch) unabhängig von einer evtl. vorhergegangen Wahl sein. In der Praxis stellen allein diese Forderungen nicht zu unterschätzende Hindernisse dar, da man „echte“ Zufallsexperimente auf Rechnern nicht simulieren kann. In der Regel muss man sich deshalb mit Pseudo-Zufallszahlen zufrieden geben.

Nach Wahl einer „zufälligen“ Zahl $n \in \mathbb{N}$ testet man, ob n eine Primzahl ist. Dabei können wir uns den eigentlich Test noch als 'Black-Box' vorstellen. Ist die Zahl n gemäß Test eine Primzahl, so sind wir bereits fertig. Ansonsten führen wir einen erneuten Test mit der Zahl $(n + 2)$ aus. Dieses Verfahren iterieren wir so lange bis gemäß Test eine Primzahl gefunden wurde. Wir testen also bei $k - 1$ nicht erfolgreich verlaufenen Tests (d.h. die Zahlen sind nicht prim) nacheinander $n, n + 2, n + 4, \ldots, n + 2k$ mit $k \in \mathbb{N}$.

Dieses Vorgehen kann im Hinblick auf den Primzahlsatz optimiert werden, da die „Dichte der Primzahlen“ nach oben hin immer dünner wird. Genauer: Es gibt ungefähr gleich $\frac{n}{ln(n)}$ Primzahlen kleiner oder gleich n. Da ln für natürliche Zahlen eine stetige, positive und monoton steigende Funktion ist, ist eine Optimierung unter gewissen Voraussetzungen denkbar. Hierbei kann man auch das *Betrandsche Postulat* berücksichtigen, was besagt, dass für jede natürliche Zahl $n \in \mathbb{N}$ eine Primzahl p existiert, welche zwischen n und $2n$ liegt.

Daneben muss natürlich auch sichergestellt sein, dass wir ab einem beliebig hohen $n \in \mathbb{N}$ auch stets eine Primzahl finden können. Da die Menge $\mathbb{P}$ der Primzahlen abzählbar unedlich ist, was bereits Euklid vor zwei Jahrtausenden bewiesen hat, ist auch dies sichergestellt.

Wie bereits angesprochen, haben alle drei probabilistischen Primzahltests angewendet auf eine vorgegebene Zahl $n \in \mathbb{N}$ zwei mögliche Ausgänge:

- Besteht die Zahl n den Test nicht, so ist diese *zusammengesetzt* bzw. eine Einheit.
- Besteht die Zahl n den Test, so ist diese *wahrscheinlich prim*, wobei die Wahrscheinlichkeit durch wiederholtes Testen beliebig gesenkt werden kann.

Alle drei im Folgenden vorgestellten Tests basieren auf *notwendigen*, aber *nicht hinreichenden* Kriterien für eine Primzahl. So ist auch die Unbestimmtheit zu erklären. Entscheidend wird jedoch die Größe der Fehlerwahrscheinlichkeit eines jeden Primzahltests sein. Ist die Fehlerwahrscheinlichkeit eines Primzahltests „sehr klein“, so kann man diese vernachlässigen.

2. Der Fermat-Test

2.1. Satz von Euler und Pseudoprimzahlen

Die zentralen Sätze sowohl für den Fermat- als auch für den Miller-Rabin-Test sind der Satz von Euler bzw. eine direkte Folgerung aus diesem - der „kleine“ Satz von Fermat. Mit ϕ sei die Eulersche Phi-Funktion notiert; ferner unterscheiden wir nur dann streng zwischen den Repräsentanten einer Restklasse und den entsprechenden Äquivalenzklassen, wenn Unklarheiten zu befürchten sind.

SATZ 2.1.1: (Satz von Euler)
Es sei $b \in \mathbb{Z}$, $n \in \mathbb{N}$. *Sei weiter* $ggT(b,n) = 1$, *dann gilt:*

$$b^{\phi(n)} \equiv 1 \mod n. \tag{2.1}$$

Beweis. Es sei $\mathbb{Z}_n^* = \{j_1, j_2, \ldots, j_{\phi(n)}\}$ die Einheitengruppe des Restklassenrings $\mathbb{Z}_n$. Da b teilerfremd zu n ist, ist auch $b \cdot j_i \in \mathbb{Z}_n^*$ für alle $i \in \{1, \ldots, \phi(n)\}$. Außerdem gilt $b \cdot j_i \mod n \neq b \cdot j_k \mod n$ für $i \neq k$, wie wir in folgendem Widerspruch zeigen werden:
Angenommen $b \cdot j_i \mod n = b \cdot j_k \mod n \Rightarrow b(j_i - j_k) \equiv 0(\mod n)$, d.h. n ist ein Teiler von $b(j_i - j_k)$. Da aber nach Voraussetzung b und n teilerfremd sind und wir uns in einem Integritätsring bewegen, muss n bereits $(j_i - j_k)$ teilen. Dies ist aber nur dann möglich, wenn $(j_i - j_k) = 0$ gilt, denn j_i und j_k sind kleiner als n, und damit ist auch die betragsmäßige Differenz kleiner als n. Daraus ergibt sich ein Widerspruch zur Voraussetzung und damit ist die Teilbehauptung bewiesen.

$$\begin{aligned} \prod_{i=1}^{\phi(n)} b \cdot j_i &\equiv \prod_{i=1}^{\phi(n)} j_i (\mod n) \\ \Rightarrow b^{\phi(n)} \prod_{i=1}^{\phi(n)} j_i &\equiv \prod_{i=1}^{\phi(n)} j_i (\mod n) \\ \Rightarrow b^{\phi(n)} &\equiv 1 \mod n. \end{aligned}$$

□

Aus dem Satz von Euler könnte man nun ohne großen weiteren Aufwand ein Korollar folgern, welches uns die Korrektheit des RSA-Algorithmus versichern würde. Unser Ziel ist jedoch ein anderes:

SATZ 2.1.2: (Kleiner Satz von Fermat)
Es sei p prim und $b \in \mathbb{Z}$ mit $ggT(b,p) = 1$. Dann gilt:

$$b^{p-1} \equiv 1 \mod p. \tag{2.2}$$

Beweis. Der Beweis ist offensichtlich: Man ersetze die Zahl n im Satz von Euler durch p und beachte, dass $\phi(p) = p - 1$ ist. □

Wie wir im letzten Beweis erkennen konnte ist der kleine Satz von Fermat ein Spezialfall des allgemeineren Satzes von Euler.

Beispiel:
Es ist $5^{\phi(6)} \mod 6 = 5^2 \mod 6 = 25 \mod 6 = 1$. Gleiches ergibt sich durch die Erkenntnis $ggT(5,6) = 1$ und die Anwendung des Satzes von Euler. Bei der Berechnung des letzten Wertes hätte man den Satz von Euler nicht unbedingt benötigt, um schnell ans Ziel zu kommen.

Anders verhält es sich bei $31^{\phi(853)} \mod 853$. Es lässt sich effizient bestimmen, dass $ggT(853,31) = 1$ gilt. Somit folgt mit dem Satz von Euler direkt $31^{\phi(853)} \equiv 1(\mod 853)$. Wie Sie vielleicht bemerkt haben, ist 853 prim, d.h. es gilt $\phi(853) = 852$, d.h. wir hätten hier auch den kleinen Satz von Fermat anwenden können.

Ohne es vielleicht zu merken, haben wir mit dem kleinen Satz von Fermat bereits das erste notwendige Kriterium für den Fermat-Test gefunden. Für Primzahlen $p \in \mathbb{P}$ wissen wir nach 2.1, dass für *geeignete* Zahlen b stets gilt $b^{p-1} \mod p = 1$. Leider gilt die Umkehrung dieses Sachverhalts nicht, wie uns das folgende Beispiel zeigt:

Beispiel:
Wir wählen $n := 91 = 7 \cdot 13$ und $b := 3$, dann ist $3^{90} \mod 91 = 1$, obwohl 91 offensichtlich zusammengesetzt ist.

Das letzte Beispiel motiviert die folgende

Definition:
Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl und sei $b \in \mathbb{Z}_n^*$. Wir nennen n eine **Pseudoprimzahl zur Basis** b, falls $b^{n-1} \mod n = 1$ gilt.

Beispiel:
Es dürfte klar sein, dass damit 91 eine Pseudoprimzahl zur Basis 3 ist. Es ist jedoch $2^{90} \mod 91 = 64$, d.h. 91 ist keine Pseudoprimzahl zur Basis 2.

Eine Aussage, dass die Zahl n eine Pseudoprimzahl ist, ergibt also ohne Nennung der Basis b keinen Sinn. Dabei kann die Basis b nur „Werte“ aus der Einheitengruppe $\mathbb{Z}_n^*$ des Restklassenringes annehmen. Dass die Basis aus der Einheitengruppe gewählt werden muss wird klar, wenn man folgende Äquivalenz berücksichtigt:

Es sei $b \in \mathbb{Z}_n^* \ \{\bar{0}\}$. Dann gilt die Äquivalenz:

$$b \text{ ist eine Einheit im Ring } \mathbb{Z}_n \Leftrightarrow ggT(n, b) = 1.$$

Beweis. „$\Leftarrow$“:
Wende das Lemma von Bézout (auch Vielfachsummendarstellung genannt) an und reduziere sodann modulo n. Damit haben wir die Rückrichtung gezeigt.

„$\Rightarrow$“:
Die „Hinrichtung“ ist auch nicht schwer: Es sei b eine Einheit im Ring $\mathbb{Z}_n$, dann besitzt die Gleichung $xb \equiv_n 1$ eine Lösung, d.h. es existiert eine $y \in \mathbb{Z}$, so dass $xb = yn + 1$ gilt. Angenommen $ggT(b, n) > 1$, dann würde $d|(xb - yn)$ bzw. $d|1$ gelten. Doch daraus folgt $d = 1$, was im Widerspruch steht zur Annahme. □

Ein bedeutender algebraischer Zusammenhang ist der Folgende:

Lemma 2.1.3: *Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl. Die Menge*

$$B := \{b \in \mathbb{Z}_n^* | n \text{ ist Pseudoprimzahl zur Basis } b\}$$

ist eine Untergruppe von $(\mathbb{Z}_n^*, \odot)$, wobei $\odot$ die modulare Multiplikation ist.

Beweis. Seien $a, b \in B$. Dann gilt $a^{n-1} \equiv 1 \mod n$ und $b^{n-1} \equiv 1 \mod n$. Es folgt

$$(ab^{-1})^{n-1} \equiv a^{n-1}(b^{-1})^{n-1} \equiv 1 \cdot (b^{n-1})^{-1} \equiv 1 \mod n,$$

womit auch das Produkt ab^{-1} in B liegt. Mit dem Untergruppenkriterium folgt damit die Behauptung. □

Wir haben bereits auf die Bedeutung des „Unsicherheitsfaktors“ eines Primzahltests hingewiesen. Das nächste Lemma wird uns Näheres zu diesem verraten:

Lemma 2.1.4: *Sei n eine zusammengesetzte Zahl. Entweder*

- *ist n eine Pseudoprimzahl für alle Basen $b \in \mathbb{Z}_n^*$ oder*
- *n ist keine Pseudoprimzahl zur Basis b für mindestens die Hälfte aller $b \in \mathbb{Z}_n^*$.*

Beweis. Aufgrund des letzten Lemmas wissen wir, dass die Menge aller Basen $B := \{b \in \mathbb{Z}_n^* | n \text{ ist Pseudoprimzahl zur Basis } b\}$ eine Untergruppe der Einheitengruppe $\mathbb{Z}_n^*$ ist. Nach einem Korollar aus dem Satz von Lagrange wissen wir, dass die Ordnung $|U|$ einer Untergruppe U, die Gruppenordnung $|G|$ von G teilt - vorausgesetzt U existiert überhaupt. Wenden wir dies auf die Gruppe $\mathbb{Z}_n^*$ und deren Untergruppe B an, so ergibt sich damit direkt die Behauptung. □

Besteht eine Basis $b \in \mathbb{Z}_n^*$ den Test also nicht, d.h. $b^{n-1} \not\equiv 1 \mod n$, so steht fest, dass es sich um eine zusammengesetzte Zahl handelt. Viele Autoren geben Basen dieser Art einen eigenen sprechenden Namen in diesem Kontext.

Definition:
Ist $n \in \mathbb{N}$ eine ungerade natürliche Zahl, so heißt $b \in \mathbb{Z}_n^*$ ein **Zeuge für die Zerlegbarkeit von** n, wenn $b^{n-1} \not\equiv 1 \mod n$ gilt.

Im Englischen heißen derartige Basen „witness“ und die Gegenstücke, d.h. diejenigen Basen $b \in \mathbb{Z}_n^*$, für welche $b^{n-1} \equiv 1 \mod n$ gilt, werden „liar“ genannt.

2.2. Die Carmichael-Zahlen

Wie im letzten Lemma des letzten Abschnitts proklamiert, existieren in der Tat zusammengesetzte Zahlen $n \in \mathbb{N}$, für die $B = \mathbb{Z}_n^*$ gilt. Die kleinste derartige Zahl ist $561 = 3 \cdot 11 \cdot 17$. Man kann durch Rechnung nachweisen, dass 561 Pseudoprimzahl für alle möglichen Basen $b \in \{1, 2, 4, \cdots, 560\}$ ist.

R. D. Carmichael berechnete Anfang des 20. Jahrhunderts erstmals einige Beispiele derartiger Zahlen:

Definition:
Eine zusammengesetzte Zahl $n \in \mathbb{N}$ heißt **Carmichael-Zahl**, falls $b^{n-1} \mod n = 1$ für alle Basen $b \in \mathbb{Z}_n^*$ gilt.

Beispiel:

7 ersten Carmichael-Zahlen:		
$561 = 3 \cdot 11 \cdot 17$	$1105 = 5 \cdot 13 \cdot 17$	$1729 = 7 \cdot 13 \cdot 19$
$2465 = 5 \cdot 17 \cdot 29$	$2821 = 7 \cdot 13 \cdot 31$	$6601 = 7 \cdot 23 \cdot 41$
$8911 = 7 \cdot 19 \cdot 67$		

Den restlichen Teil dieses Abschnitts werden wir nutzen und die Carmichael-Zahlen etwas näher zu untersuchen. Die dabei entwickelte Theorie ist nicht unbedingt notwendig für das Verständnis des Fermat-Tests, welcher im nächsten Abschnitt behandelt wird.

Alwin Reinhold Korselt, ein deutscher Mathematiker, entdeckte bereits 1899 (ohne jedoch konkrete Beispiele anzugeben) die heute so genannten Carmichael-Zahlen und charakterisierte diese wie im nächsten Satz angegeben. Zum Beweis benötigen wir die Erkenntnis aus der Algebra/Zahlentheorie, dass die Einheitengruppe von $(\mathbb{Z}/p^m\mathbb{Z}), m \in \mathbb{N}, p > 2$ und p Primzahl, zyklisch ist. Diese Einsicht ergibt sich entweder durch Fallunterscheidungen oder aber durch die Theorie der endlichen Körper: man kann zeigen, dass die Einheitengruppe K^* eines endlichen Körper K mit p^m Elementen (p prim) isomorph ist zu $(\mathbb{Z}/(p^m - 1)\mathbb{Z}, +)$ -also insbesondere zyklisch.

SATZ 2.2.1: (Satz von Korselt)
Sei $n \in \mathbb{N}$ eine ungerade, zusammengesetzte Zahl.

1. *Sei p prim und $p^2 | n \Rightarrow n$ ist keine Carmichael-Zahl.*
2. *Sei n nicht durch eine Quadratzahl teilbar. Dann gilt:*
   n ist eine Carmichael-Zahl $\Leftrightarrow$ für jeden Primteiler p von n gilt $(p-1)|(n-1)$.

Beweis. Wir beweisen zunächst etwas mehr als die Aussage des zweiten Punktes, womit implizit auch der erste Punkt gezeigt wird:

„$\Leftarrow$“:
Es sei $n = p_1 p_2 \dots p_k$, wobei $p_1, \dots, p_k$ verschiedene ungerade Primzahlen sind mit $(p_i - 1)|(n-1), i \in \mathbb{N}_k$. Sei nun $a \in \mathbb{Z}_n^*$ und damit $ggT(a,n) = 1 \Rightarrow ggT(a, p_i) = 1, i \in \mathbb{N}_k$, d.h. wir können den kleinen Satz von Fermat anwenden:

$$\forall i \in \mathbb{N}_k : a^{p_i-1} \equiv 1 \mod p_i \tag{2.3}$$

Auf die Gleichungen aus (2.3) können wir den Chinesischen Restsatz anwenden, denn wir haben k modulare Gleichungen mit teilerfremden p_i. Sei nun $t \in \mathbb{Z}$ derart gewählt, so dass $(p_i - 1)t = n - 1$ gilt; dazu wähle man $t := \frac{(n-1)}{(p_i-1)}$.

Damit folgt

$$a^{n-1} \equiv a^{(p_i-1)t} \equiv 1^t \mod p_i \text{ mit } i \in \mathbb{N}_k$$

Da wir, wie bereits erwähnt, den Chinesischen Restsatz auf obige Kongruenzkette anwenden können, ergibt sich für jedes zu n teilerfremde $a \in \mathbb{Z}_n^*$ die Kongruenz $a^{n-1} \equiv 1 \mod n$, was bedeutet, dass n eine Carmichael-Zahl ist.

„⇒“:
Wir nehmen nun an, dass n eine Carmichael-Zahl ist. Zunächst zeigen wir, dass n eine ungerade Zahl sein muss. Nehmen wir dazu an, dass n eine gerade Zahl ist $\Rightarrow (-1)^{n-1} = -1$, da dann $n - 1$ ungerade ist.

Wir setzen $a := (-1) \equiv (n-1) \mod n$ und da nach Voraussetzung n eine Carmichael-Zahl ist, muss sodann gelten $(-1)^{n-1} \equiv 1 \equiv -1$. Durch Anwendung der Definition ergibt sich daraus $n|(1-(-1))$ bzw. man könnte auch folgern $(n|(-1-1))$. Jedenfalls kann (bis auf die Zahl $n = 2$) keine gerade Zahl diese Gleichungen erfüllen, womit folgt, dass n ungerade sein muss.

Als nächstes zeigen wir, dass n quadratfrei ist, d.h. es existiert keine Primzahl p, so dass $p^2|n$. Es sei p ein Primteiler von n und $p^\alpha|n$ mit einem geeigneten natürlichen α. Dann ist $a^{n-1} \equiv 1 \mod p^\alpha$. Da n ungerade und daher $p \neq 2$ existieren primitive Restklassen $\mod p^\alpha$ mit maximal möglicher Ordnung $\phi(p^\alpha)$. Also gibt es ein Element $c \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ mit $ord(c) = ord((\mathbb{Z}/p^\alpha\mathbb{Z})^*) = \phi(p^\alpha)$. Mit Hilfe des im Chinesischen Restsatz angegebenem surjektiven Isomorphismus folgt damit

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p^\alpha\mathbb{Z})^* \times F \tag{2.4}$$

mit $F := (\mathbb{Z}/\frac{n}{p^\alpha}\mathbb{Z})^*$. Es ist damit $(c, 1) \in F$ und es gilt $ord((c,1)) = ord(c)$, da ein entsprechender Isomorphismus angegeben werden kann. Wegen des Isomorphismus (2.4) muss es ein $b \in (\mathbb{Z}/n\mathbb{Z})^*$ mit $ord(b) = ord(c) = \phi(p^\alpha)$. Also gilt

$$b^{\phi(p^\alpha)} \equiv 1 \mod n.$$

Da weiter $b \nmid n$ (b ist Element aus $(\mathbb{Z}/n\mathbb{Z})^*$), gilt nach Voraussetzungen

$$b^{n-1} \equiv 1 \mod n.$$

Insgesamt ergibt sich also $\phi(p^\alpha)|(n-1)$. Aus $p|n$ und $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ folgt $\alpha = 1$, denn sonst würde p sowohl n als auch $n-1$ teilen, was zu einem Widerspruch führen würde.

Sei $n = pq$ mit Primzahlen p und q. Mit dem eben Gezeigten (setze $\alpha = 1$) folgt damit $(p-1)|(n-1)$ und $(q-1)|(n-1)$. Wegen $n-1 = pq-1 = p(q-1)+(p-1)$ folgt $p-1|q-1$ und analog $q-1|p-1$, d.h. $p = q$, was einen Widerspruch zur Voraussetzung darstellt. D.h. eine Carmichael-Zahl kann niemals ein Produkt aus zwei Primzahlen sein.

□

Nach diesem etwas längeren Beweis wollen wir uns das Hauptergebnis an einem Beispiel vor Augen führen und damit die Erkenntnisse festigen:

Beispiel:
Die kleinste Carmichael-Zahl, $561 = 3 \cdot 11 \cdot 17$, erfüllt natürlich die Bedingungen im Satz 2.2.1 (von Korselt). Sie ist ungerade, setzt sich aus mindestens 3 Primzahlen zusammen und es gilt $2|560, 10|560$ und $16|560$.

2.3. Der Algorithmus

Alford, Granville und Pomerance zeigten in ihrem Arktiel *There are infinitely many Carmichael numbers*, veröffentlicht in der Zeitschrift *Annals of Mathematics* im Jahre 1994, dass unendlich viele Carmichael-Zahlen existieren. Der Beweis ist recht aufwendig (ein mir bekannter Beweis beansprucht mehrere Seiten) und wird deshalb hier nicht gezeigt.

Es stellte sich jedoch glücklicherweise heraus, dass die Carmichael-Zahlen innerhalb der natürlichen Zahlen $\mathbb{N}$ recht „weit gestreut liegen“ - es gibt zum Beispiel gerade einmal 646 Carmichael-Zahlen kleiner als 10^9 und unterhalb von 10^{15} existieren gerade einmal 105212 Carmichael-Zahlen. Wir können uns also diejenigen Carmichael-Zahlen unterhalb einer maximalen Zahl in einer Datenstruktur merken und damit vom Test ausschließen. Wir umgehen hiermit das eigentliche Problem der Existenz der Camichael-Zahlen.

Besteht ein zufällig gewähltes ungerades $n \in \mathbb{N}$ den Test, d.h. gilt $b^{n-1} \mod n = 1$ für ein ebenso zufällig gewähltes $b \in \mathbb{Z}_n^*$, so kann die Zahl n entweder

(i) eine Primzahl sein,

(ii) eine Carmichael-Zahl sein oder

(iii) eine zusammengesetzte Zahl sein, und die Wahrscheinlichkeit ein solches b zu wählen, war höchstens $\frac{1}{2}$.

Wie bereits beschrieben, kann der Fall (ii) durch eine Speicherung der Carmichael-Zahlen bis zu einem maximalen Wert 'abgefangen' werden. Im folgenden Algorithmus setzen wir also voraus, dass n keine Carmichael-Zahl ist - dies könnte man mit einer bedingten Anweisung in den Algorithmus integrieren.

Fermat-Test:

Input: $n \in \mathbb{N}, n > 3, n$ ungerade.
Output: „n ist wahrscheinlich prim.“ oder
„n ist zusammengesetzt!“

Wähle zufällig $b \in \{2, \ldots, n-2\}$;
IF $(ggT(b,n) \neq 1)$ **THEN** „n ist zusammengesetzt!“
ELSE

tmp $:= b^{n-1} \mod n$;
IF (tmp $\neq 1$) **THEN** „n ist zusammengesetzt!“
ELSE „n ist wahrscheinlich prim.“
FI

FI

Natürlich sollte man einem Algorithmus, der die richtige Antwort nur mit einer Wahrscheinlichkeit von $\approx 0,5$ ausgiebt, nicht ohne weiteres vertrauen. Da wir die Basen $b \in \mathbb{Z}_n^*$ stochastisch unabhängig wählen, können wir jedoch den Fermat-Test iterativ ausführen: Dabei wählen wir nacheinander $b_0, b_1, \ldots, b_k$, wobei diese Zahlen paarweise verschieden sein müssen. Somit kann man die Wahrscheinlichkeit, eine zusammengesetzte Zahl als Primzahl zu identifizieren, auf $\frac{1}{2^k}$ drücken. Bereits für $k > 25$ ist es wahrscheinlicher vom Blitz getroffen zu werden oder aber dass ein Hardwarefehler auftritt, als dass der Fermat-Test ein falsches Ergebnis „ausspuckt“.

Die aufwendigste Operation des Fermat-Tests ist sicherlich die Berechnung von $b^{n-1} \mod n$. Entsprechend ergibt sich eine Laufzeit von $\mathcal{O}(log^2(n))$.

3. Der Miller-Rabin-Test

3.1. Polynome und starke Pseudoprimzahlen

Das Problem der Carmichael-Zahlen haben wir beim Fermat-Test dadurch in den Griff bekommen, dass wir uns den relevanten Teil der „Ausreißer"-Zahlen bis zu einer Höchstgrenze gemerkt haben. Sehr elegant ist diese Lösung sicherlich nicht, und so machten sich Michael O. Rabin und Garry Miller daran und verbesserten den Fermat-Test.

Wir erinnern uns: beim Fermat-Test wird die zu testende Zahl auf die für eine Primzahl notwendige Bedingung $b^{n-1} \equiv 1 \mod n$ geprüft mit $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Nimmt man die Carmichael-Zahlen aus, so kann man durch Iteration des einfachen Fermat-Tests die Fehler-Wahrscheinlichkeit beliebig senken.

Ist $n \neq 2$ eine Primzahl und damit $(n-1)$ gerade, so kann man für $b \in (\mathbb{Z}/n\mathbb{Z})^*$ auch $b^{\frac{n-1}{2}} \mod n$ bilden und es muss $b^{\frac{n-1}{2}} \equiv_n \pm 1$ gelten. Ist der Exponent von $b^{\frac{n-1}{2}}$ gerade, so können wir wieder entsprechend vorgehen und $b^{\frac{n-1}{4}}$ berechnen. Galt $b^{\frac{n-1}{2}} \equiv_n 1$ so muss auch $b^{\frac{n-1}{4}} \equiv_n \pm 1$ gelten. Dieses Verfahren können wir iterieren so lange bis der Exponent schließlich ungerade ist.

Dies stellt auch schon die Grundidee des Miller-Rabin-Tests dar! Eine formale Herleitung ergibt sich durch die folgenden Umformungen:

$$\begin{aligned} & b^{n-1} \equiv 1 \mod n \\ \Leftrightarrow\ & b^{n-1} - 1 \equiv 0 \mod n. \end{aligned}$$

Da man o.B.d.A. n als ungerade voraussetzen darf, kann man $n-1$ als $2t, t \in \mathbb{N}$, darstellen.

$$\begin{aligned} & b^{n-1} \equiv 1 \mod n \\ \Leftrightarrow\ & b^{2t} - 1 \equiv (b^t - 1)(b^t + 1) \equiv 0 \mod n. \end{aligned}$$

Durch Substitution $2t := (n-1)$ und Faktorisierung ergibt sich die letzte Gleichung - dabei können *nicht beide* Faktoren gleich 0 sein: Wäre dem so, dann würde die Differenz $(b^t + 1) - (b^t - 1) = 2$ von n geteilt werden. Das kann jedoch nicht sein, da dies im Widerspruch zur Voraussetzung n ungerade stünde.

Der erste Faktor $(b^t - 1)$ kann durch dasselbe Prinzip zerlegt (d.h. faktorisiert) werden, jedoch immer nur unter der Annahme, dass t wieder gerade ist. Letztlich erhalten wir eine Faktorisierung der Form

$$b^{n-1} - 1 \equiv (b^s - 1)(b^s + 1)(b^{2s} + 1)(b^{4s} + 1) \dots (b^{2^{r-1}s} + 1) \equiv 0 \mod n \qquad (3.1)$$

mit ungeradem s, d.h. $s \equiv 1 \mod 2$. Es wird der erste Faktor Null, wenn $b^s \equiv_n 1$ und die übrigen Faktoren werden gleich Null, wenn $b^{2^i s} \equiv_n -1$ für ein $0 \leq i < r$.

Da man in Restklassenringen leichter quadrieren als Quadratwurzel ziehen kann, fängt man andersherum an: Man berechnet $r, s \in \mathbb{N}$, so dass $n - 1 = 2^r s$ gilt, wobei s ungerade ist. Das kann man effizient mit höchstens r Divisionen durch 2 erledigen, und $r \leq log_2(n)$. Nun berechnet man nacheinander

- $x_0 := b^s \mod n$,
- $x_1 := b^{2^1 s} \mod n = x_0^2 \mod n$,
- $x_2 := b^{2^2 s} \mod n = x_1^2 \mod n$,
- ...
- $x_r := b^{2^r s} \mod n$,

also berechnen wir quasi die Nullstellen der Faktoren aus (3.1). Im Folgenden notieren wir die eben definierten Werte als Vektor $x := (x_0, x_1, \dots, x_r)$. Der Vektor x kann dabei folgende Formen annehmen:

- $(x_0, x_1, \dots, x_r) = (1, \dots, 1)$ oder
  $(x_0, x_1, \dots, x_r) = (\star, \dots, \star, n-1, 1, \dots, 1)$,
  wobei $\star \neq 1$ bzw. $\star \neq n - 1 = -1$ ist. *Dann ist n wahrscheinlich prim.*
- $(x_0, x_1, \dots, x_r) = (\star, \dots, \star, 1, \dots, 1)$ oder
  $(x_0, x_1, \dots, x_r) = (\star, \dots, \star)$ oder
  $(x_0, x_1, \dots, x_r) = (\star, \dots, \star, n-1)$,
  wobei $\star \neq 1$ bzw. $\star \neq n - 1 = -1$ ist. *Dann ist n zusammengesetzt.*

Beispiel:
Wir berechnen den Vektor $x = (x_0, \dots, x_r)$ für die Zahl $n = 341 = 31 \cdot 11$, also für eine zusammengesetzte Zahl. Dazu berechnen wir zunächst $n - 1 = 2^r s$, wobei s ungerade ist. Es ist $341 - 1 = 2^2 \cdot 85$, d.h. $r = 2$ und $s = 85$, weiter sezten wir die Basis $b := 2$. Nun berechnen wir, wie oben beschrieben, nacheinander die Werte $x_0 = 2^{85} \mod 341 = 32$, $x_1 = 2^{2 \cdot 85} \mod 341 = 1 = (x_0)^2 \mod 341$, $x_2 = 2^{4 \cdot 85} \mod 341 = 1 = (x_1)^2 \mod 341$. Es ergibt sich damit der Vektor $x = (32, 1, 1)$, die Zahl $n = 341$ wird also nach diesem Schema als zusammengesetzt erkannt.

Offensichtlich kann man $b^{\frac{n-1}{2}} = b^t$ als „Variable“ interpretieren und damit $(b^t)^2 - 1$ als Polynom auffassen, da die zu Grunde gelegte Menge $(\mathbb{Z}/n\mathbb{Z})^*$ ein kommutativer Ring ist[1]. Damit liegt ein algebraischer Beweis des oben beschriebenen Kriteriums nahe:

Beweis. Nach dem kleinen Fermat gilt für Primzahlen n und beliebiges $b \in \mathbb{Z}_n^*$ stets die Kongruenz

$$b^{n-1} \equiv_n 1 \Leftrightarrow b^{n-1} - 1 \equiv_n 0 \Leftrightarrow b^{2t} - 1 \equiv_n 0$$
$$\hookrightarrow X^2 - 1 \equiv_n 0.$$

Das Polynom $X^2 - 1$ besitzt über endlichen Körpern $\mathbb{F}_n$ ausschließlich die beiden Nullstellen[2] ± 1, wobei in $\mathbb{F}_n$ gilt: $-1 \equiv_n n - 1$. □

Ist n eine Primzahl, dann besitzt die Kongruenz $X^2 - 1 \equiv_n 0$ also ausschließlich die so genannten **trivialen Wurzeln** (Nullstellen). Ist n eine zusammengesetzte Zahl, dann kann es auch noch mehr Lösungen (sog. nicht triviale Wurzeln) geben:

Beispiel:
Für die zusammengesetzte Zahl $8 = 2^3$ hat das Polynom $F(X) := X^2 - 1$ über $(\mathbb{Z}/8\mathbb{Z})$ die Nullstellen 1, 3, 5 und 7.[3]

Dagegen hat dasselbe Polynom $F(X) = X^2 - 1$ über $(\mathbb{Z}/5\mathbb{Z})$ ausschließlich die Nullstellen ± 1: Es ist $F(0) \equiv_5 -1$, $F(1) \equiv_5 0$, $F(2) \equiv_5 3$, $F(3) \equiv_5 3$, $F(4) \equiv_5 0$. Zu beachten ist, dass $4 \equiv_5 -1$ in $(\mathbb{Z}/5\mathbb{Z}) = \mathbb{F}_5$ ist, schließlich liegen 4 und -1 in derselben Restklasse.

Finden wir also nicht triviale Wurzeln von 1 mod n, dann muss n *sicher* zusammengesetzt sein.

Die erste Frage, die sich nach den Erfahrungen mit dem Fermat-Test stellt, ist, ob das o.g. Kriterium auch *hinreichend* für den Nachweis einer Primzahl ist - diese Frage muss leider verneint werden. D.h. es existieren zusammengesetzte Zahlen, welche ebenfalls dieses notwendige Kriterium (für Primzahlen) erfüllen.

Beispiel:
Sei $n = 2047 = 23 \cdot 89$ eine zusammengesetzte Zahl. Wir wählen $b = 2$ und können sodann

[1] Es kann dann für den kommutativen Ring R die Ringerweiterung $R[X]$ aller Polynome einer Variablen X über R erklärt werden. Dabei bezeichnet $R[X]$ die Menge aller Abbildungen $f : \mathbb{N} \to R$, für die $f(i) = 0$ für fast alle $i \in \mathbb{N}$ gilt.

[2] Dies folgt aus der Äquivalenz: Ein Polynom f besitzt die Nullstelle $\lambda \in K \Leftrightarrow \exists g \in K[T]$, so dass $f = (X - \lambda)g$ und $Grad(g) = Grad(f) - 1$.

[3] Beachten Sie, dass der Satz über die Anzahl der Nullstellen eines Polynoms vom Grad n für Integritätsringe gilt. Offensichtlich ist $(\mathbb{Z}/8\mathbb{Z})$ kein Integritätsring, da bspw. $2 \cdot 4 \equiv_8 0$ gilt.

$x_0 := 2^{\frac{2047-1}{2}} = 2^{1023} \mod 2047 = 1$ berechnen. Es ist aber auch $x_1 := (x_0)^2 = 2^{2046} \mod 2047 = 1$.

Wie bereits bei den Pseudoprimzahlen führt auch dieses Beispiel zur folgenden

Definition:
Eine zusammengesetzte ungerade Zahl n heißt **starke Pseudoprimzahl zur Basis** $b \in (\mathbb{Z}/n\mathbb{Z})^*$ mit $n-1 = 2^r s$ und s ungerade, falls

- entweder $b^s \mod n = 1$ ist mit s ungerade **oder**
- es ein i mit $0 \leq i < r$ gibt, so dass $b^{2^i s} \equiv_n \pm 1$ gilt.

Erfreulich ist aber, dass es zu den *starken* Pseudoprimzahlen kein Analogon zu den Carmichael-Zahlen gibt, d.h. der Miller-Rabin-Test ist in der Tat eine Weiterentwicklung des Fermat-Tests!

Es dürfte klar sein, dass die Zahl $n = 2047$ aus dem letzte Beispiel eine starke Pseudoprimzahl zur Basis 2 ist.

***Bemerkung** 2:*

1. Gilt $b^s \mod n = 1$, dann ist natürlich auch $b^{2^i s} \mod n = 1$ für alle $1 \leq i \leq r$, d.h. der Vektor x hat die Form $(1, \ldots, 1)$.
2. Gilt $b^{2^i s} \mod n = n-1$, dann ist $b^{2^j s} \mod n = 1$ für $j > i$, d.h. der Vektor hat dann die Form $(x_0, \ldots, x_r) = (\star, \ldots, \star, n-1, 1, \ldots, 1)$.
3. Ist n eine *starke* Pseudoprimzahl zur Basis b, dann ist n auch eine Pseudoprimzahl zur Basis b, denn in beiden Fällen ist $b^{n-1} \equiv_n 1$.
4. Es gibt 14884 Pseudoprimzahlen zur Basis 2, die kleiner als 10^{10} sind, und im selben Zahlenbereich lediglich 3291 starke Pseudoprimzahlen zur Basis 2.

Rabin hat gezeigt, dass eine zusammengesetzte Zahl n für höchstens $\frac{1}{4}$ aller Elemente $b \in (\mathbb{Z}/n\mathbb{Z})^*$ eine starke Pseudoprimzahl zur Basis b ist. Der Beweis dieses Satzes ist ebenfalls zu aufwendig und wird deshalb hier nicht aufgeführt. Allerdings trösten wir uns mit einer etwas schwächeren Aussage, die wir auch beweisen werden:

SATZ 3.1.1: *Sei n eine zusammengesetzte ungerade Zahl. Dann gilt für höchstens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^*$, dass n eine starke Pseudoprimzahl zur Basis b ist.*

Beweis. Es sei n keine Carmichael-Zahl, dann gilt für mindestens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^*$, dass n keine Pseudoprimzahl und damit auch keine starke Pseudoprimzahl zur Basis b ist, da jede starke Pseudoprimzahl auch eine Pseudoprimzahl ist.

Sei also n eine Carmichael-Zahl, dann ist n das Produkt aus mindestens drei verschiedenen Primzahlen, d.h. $n = \Pi_{i=1}^{k} p_i, k \geq 3, k \in \mathbb{N}$. Sei $n - 1 = 2^r s$ mit $r, s \in \mathbb{N}$ und s ungerade. Betrachten wir sodann

$$I := \{i \in \mathbb{N}_0 | 0 \leq i \leq r \text{ und für alle } b \in (\mathbb{Z}/n\mathbb{Z})^* \text{ gilt } b^{2^i s} \mod n = 1\}.$$

Da n eine Carmichael-Zahl ist, gilt $r \in I$, denn $b^{2^r s} \mod n = 1$ für alle $b \in (\mathbb{Z}/n\mathbb{Z})^*$ gemäß Definition. Außerdem folgt aus $i \in I, 0 \leq i < r$, auch $i + 1 \in I$, denn aus $b^{2^i s} \mod n = 1$ folgt $b^{2^{i+1} s} \mod n = (b^{2^i s})^2 \mod n = 1$ für alle $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Vergleichen Sie diese Erkenntnis mit Bemerkung 1.

Sei jetzt $g \in \mathbb{N}$ so, dass $g \mod p_1$ ein Erzeuger von $(\mathbb{Z}/p_1\mathbb{Z})^*$ ist - dieses Element muss existieren, da die Einheitengruppe $(\mathbb{Z}/p_1\mathbb{Z})^*$ zyklisch ist. Dann gilt $ord(g \mod p_1) = p_1 - 1$, also ist die Ordnung gerade, da p_1 prim und ungleich 2 ist. Nun ist s aber ungerade, das heißt, $p_1 - 1 \nmid s$, und $g^s \mod p_1 \neq 1$. Mit dem Chinesischen Restsatz folgt, dass es ein $b \in \mathbb{Z}$ gibt mit $b^s \mod n \neq 1$. Also gilt $0 \in I$. Es gibt also ein $l \in \mathbb{N}$ mit $0 \leq l < r$ und $l \notin I$, aber $l + 1 \in I$. Sei dann

$$G := \{b \in (\mathbb{Z}/n\mathbb{Z})^* | b^{2^l s} \mod n \equiv_n \pm 1\}.$$

Die Menge G zusammen mit der modularen Multiplikation ist eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$, denn $1 \in G$ und sind $a, b \in G$, dann ist

$$\begin{aligned}(ab^{-1})^{2^l s} &\equiv_n a^{2^l s}(b^{-1})^{2^l s} \\ &\equiv_n \pm 1 \cdot (b^{2^l s})^{-1} \\ &\equiv_n \pm 1 \cdot \pm 1 \\ &\equiv_n \pm 1,\end{aligned}$$

also $ab^{-1} \in G$. Mit dem Untergruppenkriterium folgt, dass G eine Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$ ist.

Wir zeigen nun, dass $G \neq (\mathbb{Z}/n\mathbb{Z})^*$ gilt und folgern dann mit Hilfe des Satzes von Lagrange die Behauptung. Da $l \notin I$ gilt, gibt es ein $a \in (\mathbb{Z}/n\mathbb{Z})^*$, so dass $a^{2^l s} \mod n \neq 1$

gilt. D.h., es gibt ein $i \in \mathbb{N}_k$, so dass $a^{2^l s} \mod p_i \neq 1$ gilt. Mit dem Chinesischen Restsatz existiert ein $b \in \mathbb{Z}$ mit $b \equiv_{p_i} a$ und $b \equiv_{p_j} 1$ für $i \neq j$. Dann ist $b \mod n \notin G$, denn $b^{2^l s} \not\equiv_{p_i} 1$ und $b^{2^l s} \not\equiv_{p_j} -1$ für $i \neq j$. Also gilt $b^{2^l s} \not\equiv_n \pm 1$. Es folgt $G \neq (\mathbb{Z}/n\mathbb{Z})^*$.

Andererseits sind die Elemente $b \in (\mathbb{Z}/n\mathbb{Z})^* \setminus G$ gerade so, dass n keine starke Pseudoprimzahl zur Basis b ist, denn $b^{2^l s} \not\equiv_n \pm 1$, weil $b \notin G$ und $b^{2^{l+1} s} \equiv_n 1$ - beachte, dass $l+1 \in I$ gilt. Da G eine Untergruppe ist, die nicht ganz $(\mathbb{Z}/n\mathbb{Z})^*$ beinhaltet, ist also mindestens die Hälfte der Elemente aus $(\mathbb{Z}/n\mathbb{Z})^*$ nicht in G, und damit ist n für mindestens die Hälfte der Elemente $b \in (\mathbb{Z}/n\mathbb{Z})^*$ keine Pseudoprimzahl zur Basis b. □

3.2. Der Algorithmus

Im letzten Abschnitt haben wir alle notwendigen Bausteine für den Miller-Rabin-Test entwickelt und bereits einen ersten Eindruck der Funktionsweise dieses Primzahltests gewährt. Vergleichen Sie die Semantik des nun folgenden Algorithmus mit den Erkenntnissen aus Kapitel 3.1 auf Seite 13.

Miller-Rabin-Test:

Input: $n \in \mathbb{N}, n \geq 3, n$ ungerade.
Output: „n ist wahrscheinlich prim.“ oder „n ist zusammengesetzt!“

Bestimme die Zahlen $r, s \in \mathbb{N}$, so dass $n - 1 = 2^r s$ und s ungerade;
wähle zufällig $b \in \{2, \ldots, n-2\}$;
$x_0 := b^s \mod n$;

IF $(x_0 = \pm 1)$ **THEN** „n ist wahrscheinlich prim!“
ELSE
    FOR $i := 1$ **TO** $r - 1$;
        $x_i := (x_{i-1})^2 \mod n$;
        IF $x_i = -1$ **THEN** „n ist wahrscheinlich prim!“
        ELSE „n ist zusammengesetzt!“
        FI
FI

Der Miller-Rabin-Test lässt sich, ebenso wie der Fermat-Test, sehr effizient ausführen: höchstens $log(n)$ Divisionen sind nötig, um s und r zu finden. Durch Shiften der binären Ziffern lässt sich die Laufzeit sogar noch verbessern. Die Berechnung modularer Potenzen

kann in Zeit $\mathcal{O}(log^2(n))$ durchgeführt werden. In der **FOR**-Schleife ist insbesondere die Multiplikation von Gewicht - insgesamt wird diese maximal k-mal durchgeführt, wobei $k \leq log(n)$ gilt. Insgesamt ergibt sich damit also eine Laufzeit von $\mathcal{O}(log^2(n))$.

4. Der Solovay-Strassen-Test

4.1. Quadratische Reste

Ein Schmuckstück der elementaren Zahlentheorie ist die Theorie der quadratischen Reste, welche den hauptsächlichen Anlass zur Entwicklung der höheren Zahlentheorie gegeben hat. In diesem Abschnitt werden wir die Grundlagen dieser Theorie elementar vermitteln. Den eigentlichen Höhepunkt, das quadratische Reziprozitätsgesetzt werden wir jedoch nur nennen, aber nicht beweisen, da dieses für das reine Verständnis des Algorithmus nicht vonnöten ist.

Definition:
Sei $n \in \mathbb{N}, n > 1$, vorgegeben. Eine zu n teilerfremde Zahl $a \in \mathbb{Z}_n^*$ heißt **quadratischer Rest** modulo n, wenn ein $x \in \mathbb{Z}$ existiert, so dass $x^2 \equiv_n a$.
Zwei modulo n quadratische Reste $a, a' \in \mathbb{Z}$ heißen **verschieden**, wenn $a \not\equiv_n a'$ gilt. Eine zu n teilerfremde Zahl a heißt **quadratischer Nichtrest** modulo n, wenn a kein quadratischer Rest modulo n ist.

Beispiel:
Sei $n := 9$, dann sind 1, 4, 7 verschiedene quadratische Reste modulo 9. Der naive Weg ist, alle Elemente aus $(\mathbb{Z}/9\mathbb{Z})^*$ zu berechnen. Gemäß Definition kommen für quadratische Reste nur die zu $n = 9$ teilfremden Zahlen kleiner 9 in Frage. Insgesamt existieren davon $\phi(9) = 6$ Stück und im Einzelnen sind dies: 1, 2, 4, 5, 7, 8. Entsprechend berechnen wir die Quadrate:

$$\begin{aligned} 1^2 &\equiv_9 1, & 2^2 &\equiv_9 4, \\ 4^2 &\equiv_9 7, & 5^2 &\equiv_9 7, \\ 7^2 &\equiv_9 7, & 8^2 &\equiv_9 1. \end{aligned}$$

Wir sehen, dass 1, 4 und 7 quadratische Reste, dagegen 2,5 und 8 quadratische Nichtreste sind.

Für unsere Bedürfnisse reicht es jedoch, sich auf quadratische Reste modulo p, p eine Primzahl, zu beschränken. Für eine Primzahl p ist $a \in \mathbb{Z}_p^*$ genau dann ein quadratischer Rest mod p, wenn ein $x \in \mathbb{Z}$ existiert, so dass die Kongruenz $x^2 \equiv_p a$ lösbar ist.

Unser Hauptaugenmerk liegt dabei auf der Frage nach der *Anzahl der quadratischen Reste* zu vorgegebenem $p \in \mathbb{P}$. Genauer:

> *Wieviele $a \in \mathbb{Z}_p^*$ sind Quadratwurzeln, also von der Form $a = b^2 \mod p$ für ein $b \in \mathbb{Z}_p^*$?*

Eine Antwort auf diese Frage gibt folgendes

Lemma 4.1.1: *Sei $p > 2$ eine Primzahl. Dann sind die Hälfte der Elemente in $\mathbb{Z}_p^*$ quadratische Reste, und die andere Hälfte sind quadratische Nichtreste modulo p.*

Beweis. Sei g ein primitives Element von $(\mathbb{Z}/p\mathbb{Z})^*$, dann ist $a = g^j \mod p$ eine Quadratzahl genau dann, wenn $j \in \mathbb{Z}$ gerade ist:

„$\Rightarrow$“: Ist nämlich $j \in \mathbb{Z}$ gerade, d.h. $j = 2k$ für ein $k \in \mathbb{Z}$, dann gilt $a \equiv_p g^j \equiv_p (g^k)^2 \equiv_p g^{2k}$, also eine Quadratzahl.

„$\Leftarrow$“: Ist andererseit a eine Quadratzahl, also $a = b^2 \mod p$ mit $b \in (\mathbb{Z}/p\mathbb{Z})^*$, dann gilt $b = g^k \mod p$ für ein $k \in \mathbb{Z}$, und $a \equiv_p b^2 \equiv_p (g^k)^2 \equiv_p g^{2k}$, also ist $a = g^j \mod p$ für ein $k \in \mathbb{Z}$.

Da p nach Voraussetzungen stets eine ungerade Primzahl ist, folgt damit unmittelbar, dass die Hälfte, also insgesamt $\frac{p-1}{2}$ der Elemente aus $(\mathbb{Z}/p\mathbb{Z})^*$ quadratische Reste sind. Dies sind gerade die Elemente, welche sich mit Hilfe eines primitiven Elements g und geradem Exponenten $j = 2k$ darstellen lassen. □

Wir haben also festgestellt, dass mit obiger Notation $g^1, g^3, \ldots, g^{p-2}$ quadratische Nichtreste und $g^2, g^4, \ldots, g^{p-1}$ quadratische Reste $\mod p$, p prim, sind. Insbesondere ist also eine primitive Restklasse kein Quadrat - ansonsten würde obiges Lemma seine Gültigkeit verlieren, was nicht sein kann.

Definition:
Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Das **Legendre-Symbol** $\left(\frac{a}{p}\right)$ ist definiert als

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{, falls } p|a \\ 1 & \text{, falls } a \mod p \text{ quadratischer Rest modulo } p \\ -1 & \text{, falls } a \mod p \text{ quadratischer Nichtrest modulo } p \end{cases}$$

Das Legendre-Symbol ist nach dem französischen Mathematiker ADRIEN-MARIE LEGENDRE (1752-1833) benannt. Beachten Sie, dass das Legendre-Symbol für Primzahlen definiert ist. Eine Fortführung dieser Definition werden wir weiter unten mit dem Jacobi-Symbol einführen.

Beispiel:
Sei $p = 7$, also prim. Dann besteht die Einheiten-Gruppe $(\mathbb{Z}/7\mathbb{Z})^*$ aus $\phi(7) = 6$ Elementen, nämlich aus den Restklassen $\{1, 2, 3, 4, 5, 6\}$. Es gilt

$$\begin{aligned} 1^2 &\equiv_7 6^2 \equiv_7 \mathbf{1}, & 2^2 &\equiv_7 5^2 \equiv_7 \mathbf{4} \\ 3^2 &\equiv_7 4^2 \equiv_7 \mathbf{2}, & 0^2 &\equiv_7 7^2 \equiv_7 0 \end{aligned}$$

Es sind also $\left(\frac{0}{7}\right) = 0$ und $\left(\frac{1}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right) = 1$ und $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$.

Um also festzustellen, *für welche* von $0 \mod p$ verschiedene Restklassen $a \mod p$ die Kongruenz

$$x^2 \equiv a \mod p \tag{4.1}$$

lösbar ist, berechnen wir $i^2 \mod p$ für $i = 1, 2, \ldots, (p-1)$.

Im obigen Beispiel haben wir festgestellt, dass die Kongruenz $x^2 \equiv a \mod 7$ für $a \equiv_7 1, 2$ und 4 lösbar ist. Sie besitzt dann jeweils *zwei* differente Lösungen, denn $x^2 \equiv i^2 \mod 7$ ist äquivalent mit $x \equiv i \mod 7$ oder $x \equiv -i \mod 7$, wobei $i \not\equiv -i \mod 7$ und $i \not\equiv 0 \mod 7$.

Bilden wir also die Quadratzahlen von $1, 2, \ldots, (p-1)$, so erhalten wir $\frac{1}{2}(p-1)$ verschiedene Werte, wobei $x^2 \equiv_p (p-x)^2$ gilt:

$$\begin{aligned} & x^2 \equiv_p y^2 && \text{mit } 1 \le x \le y \le \frac{1}{2}(p-1) \\ \Rightarrow & p|(y^2 - x^2) \Rightarrow p|(x+y)(y-x) && \text{mit } 0 \le y - x < x + y < p \\ \Rightarrow & y = x \text{ oder } y = (p-x). \end{aligned}$$

So ist auch klar, warum die Quadrate von $1, \ldots, \frac{1}{2}(p-1)$ alle paarweise verschieden sind.

Die Restklassen $a \mod p$ für welche die Kongruenz (4.1) lösbar ist, findet man auch mit Hilfe einer primitiven Restklasse $\mod p$. Allerdings bereitet das Auffinden einer solchen in der Regel große Schwierigkeiten.

Der folgende Satz geht auf Euler und Legendre zurück und ist ein weiteres *notwendiges*, aber *nicht hinreichendes* Kriterium für Primzahlen p.

SATZ 4.1.2: (Kriterium von Euler)
Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Dann gilt

$$a^{\frac{p-1}{2}} \equiv_p \left(\frac{a}{p}\right) \tag{4.2}$$

Beweis. Gilt $p|a$, dann ist $a \mod p = 0$, also auch $a^{\frac{p-1}{2}} \equiv_p 0 \equiv_p \left(\frac{a}{p}\right)$. Wir müssen also noch zeigen, dass (4.2) auch für $p \nmid a$ gilt. Es sei nun $p \nmid a$, dann ist $a \mod p \in (\mathbb{Z}/p\mathbb{Z})^*$. Sei g ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^*$, dann ist $a \mod p$ ein quadratischer Rest modulo p, dann gilt $a \equiv_p g^{2k}$ für ein $k \in \mathbb{N}_0$. Also folgt

$$a^{\frac{p-1}{2}} \equiv_p (g^{2k})^{\frac{p-1}{2}} \equiv_p (g^{p-1})^k \equiv_p 1^k \equiv_p 1.$$

Ist $a \mod p$ ein quadratischer Nichtrest modulo p, dann gilt $a \equiv_p g^{2k+1}$ für ein $k \in \mathbb{N}_0$. Also folgt

$$a^{\frac{p-1}{2}} \equiv_p (g^{2k+1})^{\frac{p-1}{2}} \equiv_p g^{k(p-1)+\frac{p-1}{2}} \equiv_p (g^{p-1})^k \cdot g^{\frac{p-1}{2}} \equiv_p 1^k \cdot g^{\frac{p-1}{2}} \equiv_p g^{\frac{p-1}{2}}.$$

Nun ist aber $g^{\frac{p-1}{2}} \not\equiv_p 1$, denn die Ordnung von g in $(\mathbb{Z}/p\mathbb{Z})^*$ ist $p-1$. Andererseits ist $(g^{\frac{p-1}{2}})^2 \equiv_p g^{p-1} \equiv_p 1$, also ist $g^{\frac{p-1}{2}} \equiv_p \pm 1$. Insgesamt folgt also $g^{\frac{p-1}{2}} \equiv_p -1$, also $a^{\frac{p-1}{2}} \equiv_p -1 \equiv_p \left(\frac{a}{p}\right)$. □

Sei $ggT(a,p) = 1$, d.h. a ist kein Vielfaches von p, dann muss nach dem Eulerschen Kriterium $a^{\frac{p-1}{2}} \equiv_p \pm 1$ gelten. Die wichtigsten Rechenreglen für Legendre-Symbolen lauten:

Lemma 4.1.3: *Sei $p > 2$ eine Primzahl, und seien $a, b \in \mathbb{Z}$.*

(i) *Gilt $a \equiv b \mod p$, dann ist $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) $\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ , falls } p \mod 4 = 1 \\ -1 \text{ , falls } p \mod 4 = 3. \end{cases}$

Beweis. (i) Sei $a \equiv b \mod p$. Dann ist $a^{\frac{p-1}{2}} \equiv_p b^{\frac{p-1}{2}}$, also folgt mit Satz 4.1.2, dass $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) Es gilt $\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) Es gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Also ist $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow \frac{p-1}{2}$ ist gerade $\Leftrightarrow \frac{p-1}{2} = 2k$ für ein $k \in \mathbb{N}_0 \Leftrightarrow p-1 = 4k$ für ein $k \in \mathbb{N}_0 \Leftrightarrow p = 4k+1$ für ein $k \in \mathbb{N}_0 \Leftrightarrow p \mod 4 = 1$. Da p ungerade ist, gilt entweder $p \mod 4 = 1$ oder $p \mod 4 = 3$.

□

Beispiel:
Mit den eben gewonnenen Rechenregeln kann ein Großteil der Legendre-Symbole einfach berechnet werden: $\left(\frac{40}{31}\right) = \left(\frac{9}{31}\right) = \left(\frac{3}{31}\right)^2 = 1$. Außerdem
$\left(\frac{-1}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{4}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right)^2 = -1$, denn $31 \mod 4 = 3$.

4.2. Das Jacobi-Symbol und Eulersche Pseudoprimzahlen

Wie bereits angedeutet erweitern wir nun die Definition des Legendre-Symbols auf beliebige *ungerade* Zahlen.

Definition:
Sei $n > 2$ eine ungerade Zahl und sei $a \in \mathbb{Z}$. Sei $n = \sum_{i=1}^{r} p_i^{\alpha_i}$ die Primfaktorzerlegung von n, wobei $p_i \neq p_j$ für $j \neq i$ und $1 \leq i, j \leq r$ gilt. Das **Jacobi-Symbol** ist definiert als

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{\alpha_r}.$$

Das Jacobi-Symbol ist nach Gustav Carl Jacob Jacobi (1804-1851) benannt.

Ist n eine Primzahl, dann stimmen Jacobi- und Legendre-Symbol überein. Ist n jedoch zusammengesetzt, dann macht das Jacobi-Symbol *keine* Aussage mehr darüber, ob $a \mod n$ in $(\mathbb{Z}/n\mathbb{Z})^*$ ein quadratischer Rest ist oder nicht, obwohl wir in $(\mathbb{Z}/n\mathbb{Z})^*$ quadratische Reste definiert haben.

Beispiel:
Es sei $n := 15$ und $a := 2$, dann ist $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, denn 2 ist ein quadratischer Nichtrest in $(\mathbb{Z}/3\mathbb{Z})^*$ und in $(\mathbb{Z}/5\mathbb{Z})^*$. Allerdings ist 2 ebenfalls ein quadratischer Nichtrest in $(\mathbb{Z}/15\mathbb{Z})^*$, da es kein $b \in (\mathbb{Z}/15\mathbb{Z})^*$ gibt, so dass $b^2 \mod 15 = 2$ gilt.

Ist also $n > 2$ eine ungerade zusammengesetzte Zahl und $a \in (\mathbb{Z}/n\mathbb{Z})^*$ vorgegeben. Wie wir im letzten Beispiel gezeigt haben, kann aufgrund von

$$\left(\frac{a}{n}\right) = 1 \tag{4.3}$$

keine Aussage darüber getroffen werden, ob a ein quadratischer Rest bzw. Nichtrest in $(\mathbb{Z}/n\mathbb{Z})^*$ ist. Mit anderen Worten: Bedingung (4.3) ist *nicht hinreichend*, wie wir aber sehen werden, ist (4.3) eine *notwendige* Bedingung dafür, dass a ein quadratischer Rest ist.

Lemma 4.2.1: *Sei $n > 2$ ungerade und zusammengesetzt und sei $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Ist a ein quadratischer Rest in $(\mathbb{Z}/n\mathbb{Z})^*$, d.h. es gibt ein $b \in (\mathbb{Z}/n\mathbb{Z})^*$ mit $b^2 \mod n = a$, dann muss $\left(\frac{a}{n}\right) = 1$ gelten.*

Beweis. Sei $n = \sum_{i=1}^{r} p_i^{\alpha_i}$ die Primfaktorzerlegung von n. Für $1 \leq i \leq r$ gilt dann $b^2 \equiv_{p_i} a$, also ist a ein quadratischer Rest modulo p_i. Es folgt damit

$$\begin{aligned}\left(\frac{a}{n}\right) &= \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r} \\ &= 1^{\alpha_1} \ldots 1^{\alpha_r} = 1.\end{aligned}$$

□

Für das Jacobi-Symbol gelten ähnliche Eigenschaften wie für das Legendre-Symbol:

Lemma 4.2.2: *Sei $n > 2$ eine ungerade Zahl und seien $a, b \in \mathbb{Z}$.*

(i) Gilt $a \equiv_n b$, dann folgt $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(iii) $\left(\frac{1}{n}\right) = 1$.

Beweis. Sei $n = \sum_{i=1}^{r} p_i^{\alpha_i}$ die Primfaktorzerlegung von n.

(i) Es gelte $a \equiv_n b$, dann ist $a \equiv_{p_i} b$ für $1 \leq i \leq r$ und

$$\begin{aligned}\left(\frac{a}{n}\right) &= \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{b}{p_1}\right)^{\alpha_1} \cdots \left(\frac{b}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{b}{n}\right).\end{aligned}$$

Mit Lemma 4.1.3 folgt damit die Behauptung.

(ii) Es gilt

$$\begin{aligned}\left(\frac{ab}{n}\right) &= \left(\frac{ab}{p_1}\right)^{\alpha_1} \cdots \left(\frac{ab}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{b}{p_1}\right)^{\alpha_1} \cdots \left(\frac{b}{p_r}\right)^{\alpha_r} \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r} \\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)\end{aligned}$$

und die Behauptung folgt wieder durch Anwendung von Lemma 4.1.3.

(iii) Es gilt $\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)^{\alpha_1} \cdots \left(\frac{-1}{p_r}\right)^{\alpha_r} = 1$, denn 1 ist immer ein quadratischer Rest.

□

Auch der Solovay-Strassen-Test stützt sich wieder auf ein notwendiges Kriterium für Primzahlen, das jedoch nicht hinreichend ist. Konkret:

Für eine ungerade Zahl $n > 2$ wird ein $2 \leq b \leq n-2$ und $ggT(b,n) = 1$ gewählt und getestet, ob

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \mod n \tag{4.4}$$

gilt. Ist n prim, dann gilt dieses Kriterium gemäß Satz 4.1.2 (siehe Abschnitt 4.1).

Allerdings existieren zusammengesetzte Zahlen n und $b \in \mathbb{N}$ mit $0 < b < n$ und $ggT(b,n) = 1$, so dass Bedingung (4.4) erfüllt wird.

Beispiel:
Die Zahl $n := 2047 = 23 \cdot 89$ ist offensichtlich zusammengesetzt, doch für $b := 2$ gilt $2^{1023} \equiv 1 = \left(\frac{2}{2047}\right) \mod 2047$.

Dies führt zu folgender

Definition:
Sei $n > 2$ ungerade und zusammengesetzt. Sei $b \in (\mathbb{Z}/n\mathbb{Z})^*$. Die Zahl n heißt **Eulersche Pseudoprimzahl zur Basis** b, wenn $b^{\frac{n-1}{2}} \equiv_n \left(\frac{b}{n}\right)$ gilt.

Das Lemma 4.2.3 zeigt, dass es wie bei den starken Pseudoprimzahlen kein Analogon zu den Carmichael-Zahlen gibt:

Lemma 4.2.3: *Sei $n > 2$ eine ungerade, zusammengesetzte Zahl. Dann gilt für mindestens die Hälfte aller $b \in (\mathbb{Z}/n\mathbb{Z})^*$, dass n keine Eulersche Pseudoprimzahl zur Basis b ist.*

Einen Beweis bleiben wir an dieser Stelle schuldig.

4.3. Der Algorithmus

Im vorhergegangenen Abschnitt haben wir alles Notwendige für die praktische Durchführung des Solovay-Strassen-Tests entwickelt und zu großen Teilen auch bewiesen. Auch dieser Test ist von stochastischer Natur, d.h. auch dieser Primzahltest belegt nur mit einer gewissen (sehr kleinen) Fehlerwahrscheinlichkeit, dass eine vorgelegte Zahl eine Primzahl ist. So dürfte klar sein, dass auch beim Solovay-Strassen-Test durch mehrmalige Ausführung die Wahrscheinlichkeit eines Fehlers beliebig gesenkt werden kann.

Die Grundidee des Solovay-Strassen-Primzahltests wurde bereits genannt, nun folgt der konkrete Algorithmus.

Solovay-Strassen-Test:

Input: $n \in \mathbb{N}, n \geq 3$, n ungerade.
Output: „n ist wahrscheinlich prim.“ oder „n ist zusammengesetzt!“

Wähle zufällig $b \in \{2, \ldots, n-2\}$;

IF $(ggT(b,n) = 1)$ **THEN**
  berechne $b^{\frac{n-1}{2}} \mod n$ und $\left(\frac{b}{n}\right)$;
  IF $(b^{\frac{n-1}{2}} \mod n \equiv_n \left(\frac{b}{n}\right))$ **THEN**
    „n ist wahrscheinlich prim.“
  Else „n ist zusammengesetzt!“
ELSE „n ist zusammengesetzt!“
FI

Die Komplexitätsuntersuchung beim Solovay-Strassen-Test ist weitaus aufwendiger als bei den beiden anderen in diesem Dokument behandelten Primzahltests. Die Schwierigkeit liegt insbesondere im Nachweis, dass das Jacobi-Symbol effizient berechnet werden kann. Für einen formalen Beweis wäre einiges zusätzlich an Theorie notwendig, wie bspw. das quadratische Reziprozitätsgesetz, dem „Theorema Aureum“ wie Gauß es nannte. Wir üben uns in Askese und verzichten auf dieses schöne Stück Zahlentheorie.

Literaturverzeichnis

[1] Mathematischer Grundlagen der Kryptographie, Silke Hartlieb und Luise Unger, 2004, FernUniversität Hagen.

[2] Primality Testing, Martin Dietzfelbinger, 2004, Springer-Verlag.

[3] Modern Computer Algebra, Joachim von zur Gathen and Jürgen Gerhard, 1999, Cambridge University Press.

[4] Algebra, Siegfried Bosch, 2003, Springer-Verlag.

[5] Algebra - Teil 1, Kurt Meyberg, 1980, Hanser-Verlag.

[6] Algebra - Erster Teil, B.L. van der Waerden, 1966, Springer-Verlag.

[7] Zahlentheorie, Harald Scheid und Andreas Frommer, 2007, Spektrum.

[8] Elementare Zahlentheorie, Reinhold Remmert und Peter Ullrich, 1995, Birkhäuser-Verlag.

[9] A Computational Introduction to Number Theory and Algebra, Victor Shoup, Cambridge University Press, eBook version (http://www.shoup.net/ntb/ntb-v1.pdf).