Primzahlerzeugung

7

Für Public-Key-Kryptosysteme braucht man häufig zufällige große Primzahlen. Dazu erzeugt man natürliche Zahlen der richtigen Größe und prüft, ob sie Primzahlen sind. In diesem Kapitel zeigen wir, wie man effizient entscheiden kann, ob eine natürliche Zahl eine Primzahl ist. Wir diskutieren außerdem, wie man die natürlichen Zahlen erzeugen muss, um annähernd eine Gleichverteilung auf den Primzahlen der gewünschten Größe zu erhalten.

M. Agraval, N. Kayal und N. Saxena [2] stellen einen deterministischen Polynomzeitalgorithmus vor, der entscheidet, ob eine vorgelegte natürliche Zahl eine Primzahl ist. Dieser Algorithmus ist aber für die Praxis noch zu ineffizient.

Mit kleinen lateinischen Buchstaben werden ganze Zahlen bezeichnet.

7.1 Probedivision

Sei n eine natürliche Zahl. Wir möchten gerne wissen, ob n eine Primzahl ist oder nicht. Eine einfache Methode, das festzustellen, beruht auf folgendem Satz.

Theorem 7.1 *Wenn n eine zusammengesetzte natürliche Zahl ist, dann hat n einen Primteiler p, der nicht größer ist als $\sqrt{n}$.*

Beweis Da n zusammengesetzt ist, kann man $n = ab$ schreiben mit $a > 1$ und $b > 1$. Es gilt $a \leq \sqrt{n}$ oder $b \leq \sqrt{n}$. Andernfalls wäre $n = ab > \sqrt{n}\sqrt{n} = n$. Nach Theorem 1.6 haben a und b Primteiler. Diese Primteiler teilen auch n und daraus folgt die Behauptung. □

Um festzustellen, ob n eine Primzahl ist, braucht man also nur für alle Primzahlen p, die nicht größer als $\sqrt{n}$ sind, zu testen, ob sie n teilen. Dazu muss man diese Primzahlen bestimmen oder in einer Tabelle nachsehen. Diese Tabelle kann man mit dem Sieb des

J. Buchmann, *Einführung in die Kryptographie*, Springer-Lehrbuch,
DOI 10.1007/978-3-642-39775-2_7

Eratosthenes berechnen (siehe [4]). Man kann aber auch testen, ob n durch eine ungerade Zahl teilbar ist, die nicht größer als $\sqrt{n}$ ist. Wenn ja, dann ist n keine Primzahl. Andernfalls ist n eine Primzahl. Diese Verfahren bezeichnet man als *Probedivision*.

Beispiel 7.1 Wir wollen mit Probedivision feststellen, ob $n = 15413$ eine Primzahl ist. Es gilt $\lfloor \sqrt{n} \rfloor = 124$. Also müssen wir testen, ob eine der Primzahlen $p \leq 124$ ein Teiler von n ist. Die Primzahlen $p \leq 124$ sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113. Keine dieser Primzahlen teilt n. Daher ist n selbst eine Primzahl.

Probedivision kann man auch verwenden, um die Primfaktorzerlegung einer natürlichen Zahl zu finden. Man hört dann nicht auf, wenn ein Primteiler gefunden ist, sondern man sucht den nächsten Primteiler, den übernächsten usw., bis man fertig ist.

Beispiel 7.2 Mit Probedivision wollen wir die Zahl 476 faktorisieren. Der erste Primteiler, den wir finden, ist 2 und $476/2 = 238$. Der nächste Primteiler ist wieder 2 und $238/2 = 119$. Der nächste Primteiler ist 7 und $119/7 = 17$. Die Zahl 17 ist eine Primzahl. Also ist $476 = 2^2 * 7 * 17$ die Primfaktorzerlegung von 476.

In Faktorisierungsalgorithmen verwendet man Probedivision mit Primzahlen bis 10^6, um die kleinen Primteiler zu finden.

Um den Aufwand der Probedivision mit Primzahlen zu bestimmen, geben wir eine Abschätzung für die Anzahl der Primzahlen unterhalb einer Schranke an. Man benutzt folgende Bezeichnung:

Definition 7.1 Ist x eine positive reelle Zahl, so bezeichnet $\pi(x)$ die Anzahl der Primzahlen, die nicht größer als x sind.

Beispiel 7.3 Es ist $\pi(1) = 0$, $\pi(4) = 2$. Wie wir in Beispiel 7.1 gesehen haben, ist $\pi(124) = 30$.

Folgenden Satz erwähnen wir ohne Beweis (siehe [62]). Darin bezeichnet log den natürlichen Logarithmus.

Theorem 7.2
1. *Für* $x \geq 17$ *gilt* $\pi(x) > x/\log x$.
2. *Für* $x > 1$ *gilt* $\pi(x) < 1.25506(x/\log x)$.

Aus Theorem 7.2 folgt, dass man wenigstens $\sqrt{n}/\log\sqrt{n}$ Probedivisionen braucht, um zu beweisen, dass eine natürliche Zahl n eine Primzahl ist. Im RSA-Verfahren benutzt man Primzahlen, die größer als 10^{154} sind. Um die Primalität einer solchen Zahl zu beweisen,

müsste man mehr als $10^{154/2}/\log 10^{154/2} > 5.8 * 10^{71}$ Probedivisionen machen. Das ist nicht durchführbar. In den nächsten Abschnitten geben wir effizientere Verfahren an, die die Primalität einer Zahl überprüfen.

7.2 Der Fermat-Test

Verfahren, die beweisen, dass eine Zahl n eine Primzahl ist, sind aufwendig. Es gibt aber eine Reihe von Verfahren, die feststellen können, dass eine natürliche Zahl mit hoher Wahrscheinlichkeit eine Primzahl ist. Solche Verfahren heißen Primzahltests. Der Fermat-Test ist ein solcher Primzahltest. Er beruht auf dem kleinen Satz von Fermat (siehe Theorem 2.13). Dieser Satz wird in folgender Version benötigt.

Theorem 7.3 (Kleiner Satz von Fermat) *Ist n eine Primzahl, so gilt $a^{n-1} \equiv 1 \bmod n$ für alle $a \in \mathbb{Z}$ mit $\gcd(a, n) = 1$.*

Dieses Theorem eröffnet die Möglichkeit festzustellen, dass eine natürliche Zahl n zusammengesetzt ist. Man wählt eine natürliche Zahl $a \in \{1, 2, \ldots, n-1\}$. Man berechnet unter Verwendung der schnellen Exponentiation aus Abschn. 2.12 den Wert $y = a^{n-1} \bmod n$. Ist $y \neq 1$, so ist n nach Theorem 7.3 keine Primzahl, also zusammengesetzt. Ist dagegen $y = 1$, so kann n sowohl eine Primzahl als auch zusammengesetzt sein, wie das folgende Beispiel zeigt.

Beispiel 7.4 Betrachte die Zahl $n = 341 = 11 * 31$. Es gilt

$$2^{340} \equiv 1 \bmod 341$$

obwohl n zusammengesetzt ist. Dagegen ist

$$3^{340} \equiv 56 \bmod 341.$$

Nach dem kleinen Satz von Fermat ist 341 also zusammengesetzt.

Wenn der Fermat-Test bewiesen hat, dass n zusammengesetzt ist, dann hat er damit noch keinen Teiler von n gefunden. Er hat nur gezeigt, dass n eine Eigenschaft fehlt, die alle Primzahlen haben. Daher kann der Fermat-Test auch nicht als Faktorisierungsalgorithmus verwendet werden.

7.3 Carmichael-Zahlen

Der Fermat-Test kann also zeigen, dass eine Zahl n zusammengesetzt ist. Er kann aber nicht beweisen, dass n eine Primzahl ist. Wenn der Fermat-Test aber für viele Basen a keinen Beweis gefunden hat, dass n zusammengesetzt ist, scheint es wahrscheinlich zu

sein, dass n eine Primzahl ist. Wir werden nun zeigen, dass es natürliche Zahlen gibt, deren Zusammengesetztheit der Fermat-Test nicht feststellen kann.

Wir brauchen zwei Begriffe. Ist n eine ungerade zusammengesetzte Zahl und gilt für eine ganze Zahl a die Kongruenz

$$a^{n-1} \equiv 1 \bmod n,$$

so heißt n *Pseudoprimzahl* zur Basis a. Ist n eine Pseudoprimzahl zur Basis a für alle ganzen Zahlen a mit $\gcd(a,n) = 1$, dann heißt n *Carmichael-Zahl*. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$. Man kann beweisen, dass es unendlich viele Carmichael-Zahlen gibt. Weil es Pseudoprimzahlen und Carmichael-Zahlen gibt, ist der Fermat-Test für die Praxis nicht besonders geeignet. Besser geeignet ist der Miller-Rabin-Test, den wir unten beschreiben. Um dessen Gültigkeit zu beweisen, brauchen wir aber noch eine Charakterisierung von Carmichael-Zahlen.

Theorem 7.4 *Eine ungerade zusammensetzte Zahl $n \geq 3$ ist genau dann eine Carmichael-Zahl, wenn n quadratfrei ist, also keinen mehrfachen Primfaktor hat, und wenn für jeden Primteiler p von n die Zahl $p-1$ ein Teiler von $n-1$ ist.*

Beweis Sei $n \geq 3$ eine Carmichael-Zahl. Dann gilt

$$a^{n-1} \equiv 1 \bmod n \tag{7.1}$$

für jede ganze Zahl a, die zu n teilerfremd ist. Sei p ein Primteiler von n und sei a eine Primitivwurzel mod p, die zu n teilerfremd ist. Eine solche Primitivwurzel kann man nach dem Chinesischen Restsatz konstruieren. Dann folgt aus (7.1)

$$a^{n-1} \equiv 1 \bmod p.$$

Nach Theorem 2.9 muss die Ordnung $p-1$ von a ein Teiler von $n-1$ sein. Wir müssen noch zeigen, dass p^2 kein Teiler von n ist. Dazu benutzt man ein ähnliches Argument. Angenommen, p^2 teilt n. Dann ist $(p-1)p$ ein Teiler von $\varphi(n)$ und man kann sogar zeigen, dass es in der primen Restklassengruppe mod n ein Element der Ordnung p gibt. Daraus folgt wie oben, dass p ein Teiler von $n-1$ ist. Das geht aber nicht, weil p ein Teiler von n ist.

Sei umgekehrt n quadratfrei und sei $p-1$ ein Teiler von $n-1$ für alle Primteiler p von n. Sei a eine zu n teilerfremde natürliche Zahl. Dann gilt

$$a^{p-1} \equiv 1 \bmod p$$

nach dem kleinen Satz von Fermat und daher

$$a^{n-1} \equiv 1 \bmod p$$

weil $n-1$ ein Vielfaches von $p-1$ ist. Dies impliziert

$$a^{n-1} \equiv 1 \bmod n$$

weil die Primteiler von n paarweise verschieden sind. □

7.4 Der Miller-Rabin-Test

Im Gegensatz zum Fermat-Test findet der Miller-Rabin-Test nach hinreichend vielen Versuchen für jede natürliche Zahl heraus, ob sie zusammengesetzt ist oder nicht.

Der Miller-Rabin-Test verwendet eine Verschärfung des kleinen Satzes von Fermat. Die Situation ist folgende. Es sei n eine ungerade natürliche Zahl und es sei

$$s = \max\{r \in \mathbb{N} : 2^r \text{ teilt } n-1\}. \tag{7.2}$$

Damit ist also 2^s die größte Potenz von 2, die $n-1$ teilt. Setze

$$d = (n-1)/2^s. \tag{7.3}$$

Dann ist d eine ungerade Zahl. Folgendes Resultat ist für den Miller-Rabin-Test fundamental.

Theorem 7.5 *Ist n eine Primzahl und ist a eine zu n teilerfremde ganze Zahl, so gilt mit den Bezeichnungen von oben entweder*

$$a^d \equiv 1 \bmod n \tag{7.4}$$

oder es gibt ein r in der Menge $\{0, 1, \ldots, s-1\}$ mit

$$a^{2^r d} \equiv -1 \bmod n. \tag{7.5}$$

Beweis Sei a eine ganze Zahl, die zu n teilerfremd ist. Die Ordnung der primen Restklassengruppe mod n ist $n-1 = 2^s d$, weil n eine Primzahl ist. Nach Theorem 2.10 ist die Ordnung k der Restklasse $a^d + n\mathbb{Z}$ eine Potenz von 2. Ist diese Ordnung $k = 1 = 2^0$, dann gilt

$$a^d \equiv 1 \bmod n.$$

Ist $k > 1$, dann ist $k = 2^l$ mit $1 \leq l \leq s$. Nach Theorem 2.10 hat die Restklasse $a^{2^{l-1}d} + n\mathbb{Z}$ die Ordnung 2. Nach Übung 2.20 ist das einzige Element der Ordnung 2 aber $-1 + n\mathbb{Z}$. Also gilt für $r = l-1$

$$a^{2^r d} \equiv -1 \bmod n.$$

Man beachte, dass $0 \leq r < s$ gilt. □

Wenigstens eine der Bedingungen aus Theorem 7.5 ist notwendig dafür, dass n eine Primzahl ist. Findet man also eine ganze Zahl a, die zu n teilerfremd ist und für die weder (7.4) noch (7.5) für ein $r \in \{0, \ldots, s-1\}$ gilt, so ist bewiesen, dass n keine Primzahl, sondern zusammengesetzt ist. Eine solche Zahl a heißt *Zeuge* gegen die Primalität von n.

Beispiel 7.5 Sei $n = 561$. Mit Hilfe des Fermat-Tests kann nicht festgestellt werden, dass n zusammengesetzt ist, weil n eine Carmichael-Zahl ist. Aber $a = 2$ ist ein Zeuge gegen die Primalität von n, wie wir jetzt zeigen. Es ist $s = 4$, $d = 35$ und $2^{35} \equiv 263 \bmod 561$, $2^{2*35} \equiv 166 \bmod 561$, $2^{4*35} \equiv 67 \bmod 561$, $2^{8*35} \equiv 1 \bmod 561$. Also ist 561 nach Theorem 7.5 keine Primzahl.

Im nächsten Satz wird die Anzahl der Zeugen gegen die Primalität einer zusammengesetzten Zahl abgeschätzt.

Theorem 7.6 *Ist $n \geq 3$ eine ungerade zusammengesetzte Zahl, so gibt es in der Menge $\{1, \ldots, n-1\}$ höchstens $(n-1)/4$ Zahlen, die zu n teilerfremd und keine Zeugen gegen die Primalität von n sind.*

Beweis Sei $n \geq 3$ eine ungerade zusammengesetzte natürliche Zahl.

Wir wollen die Anzahl der $a \in \{1, 2, \ldots, n-1\}$ abschätzen, für die $\gcd(a, n) = 1$ gilt und zusätzlich

$$a^d \equiv 1 \bmod n \tag{7.6}$$

oder

$$a^{2^r d} \equiv -1 \mod n \tag{7.7}$$

für ein $r \in \{0, 1, \ldots, s-1\}$. Wenn es kein solches a gibt, sind wir fertig. Angenommen es gibt einen solchen Nicht-Zeugen a. Dann gibt es auch einen, für den (7.7) gilt. Erfüllt a nämlich (7.6), dann erfüllt $-a$ die Bedingung (7.7). Sei k der größte Wert von r, für den es ein a mit $\gcd(a, n) = 1$ und (7.7) gibt. Wir setzen

$$m = 2^k d.$$

Die Primfaktorzerlegung von n sei

$$n = \prod_{p|n} p^{e(p)}.$$

Wir definieren die folgenden Untergruppen von $(\mathbb{Z}/n\mathbb{Z})^*$:

$$\begin{aligned}
J &= \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^{n-1} \equiv 1 \bmod n\},\\
K &= \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^m \equiv \pm 1 \bmod p^{e(p)} \text{ für alle } p|n\},\\
L &= \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^m \equiv \pm 1 \bmod n\},\\
M &= \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^m \equiv 1 \bmod n\}.
\end{aligned}$$

Dann gilt

$$M \subset L \subset K \subset J \subset (\mathbb{Z}/n\mathbb{Z})^*.$$

Für jedes zu n teilerfremde a, das kein Zeuge gegen die Primalität von n ist, gehört die Restklasse $a + n\mathbb{Z}$ zu L. Wir werden die Behauptung des Satzes beweisen, indem wir zeigen, dass der Index von L in $(\mathbb{Z}/n\mathbb{Z})^*$ wenigstens 4 ist.

Der Index von M in K ist eine Potenz von 2, weil das Quadrat jedes Elementes von K in M liegt. Der Index von L in K ist daher auch eine Potenz von 2, etwa 2^j. Ist $j \geq 2$, sind wir fertig.

Ist $j = 1$, so hat n zwei Primteiler. Nach Übung 7.5 ist n keine Carmichael-Zahl und daher ist J eine echte Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$, der Index von J in $(\mathbb{Z}/n\mathbb{Z})^*$ wenigstens 2. Weil der Index von L in K nach Definition von m ebenfalls 2 ist, ist der Index von L in $(\mathbb{Z}/n\mathbb{Z})^*$ wenigstens 4.

Sei schließlich $j = 0$. Dann ist n eine Primzahlpotenz. Man kann für diesen Fall verifizieren, dass J genau $p-1$ Elemente hat, nämlich genau die Elemente der Untergruppe der Ordnung $p-1$ der zyklischen Gruppe $(\mathbb{Z}/p^e\mathbb{Z})^*$. Daher ist der Index von J in $(\mathbb{Z}/n\mathbb{Z})^*$ wenigstens 4, es sei denn, $n = 9$. Für $n = 9$ kann man die Behauptung aber direkt verifizieren. □

Beispiel 7.6 Wir bestimmen alle Zeugen gegen die Primalität von $n = 15$. Es ist $n - 1 = 14 = 2 * 7$. Mit den Bezeichnungen aus (7.2) und (7.3) gilt $s = 1$ und $d = 7$. Eine zu 15 teilerfremde Zahl a ist nach Theorem 7.5 genau dann ein Zeuge gegen die Primalität von n, wenn $a^7 \bmod 15 \neq 1$ und $a^7 \bmod 15 \neq -1$. Folgende Tabelle enthält die entsprechenden Reste:

a	1	2	4	7	8	11	13	14
$a^7 \bmod 15$	1	8	4	13	2	11	7	14

Die Anzahl der zu 15 teilerfremden Zahlen in $\{1, 2, \ldots, 14\}$, die keine Zeugen gegen die Primalität von n sind, ist $2 \leq (15-1)/4 = 7/2$.

Wenn man den Miller-Rabin-Test auf die ungerade Zahl n anwenden will, wählt man zufällig und gleichverteilt eine Zahl $a \in \{2, 3, \ldots, n-1\}$. Ist $\gcd(a, n) > 1$, dann ist n zusammengesetzt. Andernfalls berechnet man $a^d, a^{2d}, \ldots, a^{2^{s-1}d}$. Findet man dabei einen Zeugen gegen die Primalität von n, dann ist bewiesen, dass n zusammengesetzt ist. Nach Theorem 7.6 ist die Wahrscheinlichkeit dafür, dass man keinen Zeugen findet und dass n zusammengesetzt ist, höchstens $1/4$. Wiederholt man den Miller-Rabin-Test t-mal und ist n zusammengesetzt, so ist die Wahrscheinlichkeit dafür, dass kein Zeuge gegen die Primalität gefunden wird, höchstens $(1/4)^t$. Für $t = 10$ ist dies $1/2^{20} \approx 1/10^6$. Dies ist sehr unwahrscheinlich. Genauere Analysen des Verfahrens haben gezeigt, dass die Fehlerwahrscheinlichkeit noch kleiner ist.

7.5 Zufällige Wahl von Primzahlen

In vielen Public-Key-Verfahren müssen bei der Schlüsselerzeugung zufällige Primzahlen mit fester Bitlänge erzeugt werden. Wir beschreiben ein Verfahren zur Konstruktion solcher Primzahlen.

Wir wollen eine zufällige Primzahl erzeugen, deren Bitlänge k ist. Dazu erzeugen wir zuerst eine zufällige ungerade k-Bit-Zahl n. Wir setzen das erste und letzte Bit von n auf 1 und die restlichen $k-2$ Bits wählen wir unabhängig und zufällig gemäß der Gleichverteilung. Danach überprüfen wir, ob n eine Primzahl ist. Zunächst prüfen wir, ob n durch eine Primzahl unterhalb einer Schranke B teilbar ist. Man nennt das *Probedivision*. Diese Primzahlen stehen in einer Tabelle. Typischerweise ist $B = 10^6$. Wurde kein Teiler von n gefunden, so wird der Miller-Rabin-Test auf n (mit t Wiederholungen) angewendet. Wenn dabei kein Zeuge gegen die Primalität von n gefunden wird, so gilt n als Primzahl. Andernfalls ist bewiesen, dass n zusammengesetzt ist, und der Test muss mit einer neuen Zufallszahl gemacht werden. Die Wiederholungszahl t wird so gewählt, dass die Fehlerwahrscheinlichkeit des Miller-Rabin-Tests hinreichend klein ist. Bei der Suche nach einer Primzahl mit mehr als 1000 Bits reicht es für eine Fehlerwahrscheinlichkeit von weniger als $(1/2)^{80}$ aus, $t = 3$ zu wählen. Die Auswahl der Primzahlschranke B hängt davon ab, wie schnell bei der verwendeten Hard- und Software eine Probedivision im Verhältnis zu einem Miller-Rabin-Test ausgeführt werden kann.

7.6 Übungen

Übung 7.1 Beweisen Sie mit dem Fermat-Test, dass 1111 keine Primzahl ist.

Übung 7.2 Bestimmen Sie $\pi(100)$. Vergleichen Sie ihr Resultat mit den Schranken aus Theorem 7.2.

Übung 7.3 Bestimmen Sie die kleinste Pseudoprimzahl zur Basis 2.

Übung 7.4 Beweisen Sie mit dem Fermat-Test, dass die fünfte Fermat-Zahl $F_5 = 2^{2^5} + 1$ zusammengesetzt ist. Beweisen Sie, dass jede Fermat-Zahl eine Pseudoprimzahl zur Basis 2 ist.

Übung 7.5 Zeigen Sie, dass eine Carmichael-Zahl wenigstens drei verschiedene Primteiler hat.

Übung 7.6 Verwenden Sie den Miller-Rabin-Test, um zu beweisen, dass die fünfte Fermat-Zahl $F_5 = 2^{2^5} + 1$, die in Beispiel 1.13 definiert ist, zusammengesetzt ist. Vergleichen Sie die Effizienz dieser Berechnung mit der Berechnung in Übung 7.4.

Übung 7.7 Beweisen Sie mit dem Miller-Rabin-Test, dass die Pseudoprimzahl n aus Übung 7.3 zusammengesetzt ist. Bestimmen Sie dazu den kleinsten Zeugen gegen die Primalität von n.

Übung 7.8 Bestimmen Sie die Anzahl der Miller-Rabin-Zeugen für die Zusammengesetztheit von 221 in $\{1, 2, \ldots, 220\}$. Vergleichen Sie Ihr Resultat mit der Schranke aus Theorem 7.6.

Übung 7.9 Schreiben Sie ein Programm, dass den Miller-Rabin-Test implementiert und bestimmen Sie damit die kleinste 512-Bit-Primzahl.