# 7 CHAPTER Prime Number Generation

In many public-key cryptosystems, large random prime numbers are used. They are produced by generating random numbers of the right size and by testing whether those random numbers are prime. In this chapter, we explain how we can efficiently decide whether a given positive integer is a prime number. All algorithms that are presented in this chapter are implemented in the library *LiDIA* [46].

M. Agraval, N. Kayal and N. Saxena [2] have found a determinstic polynomial time algorithm that decides whether or not a positive integer is a prime number. However in practice that algorithm is still too inefficient. We will not describe it here.

Lower case italic letters denote integers.

## 7.1 Trial Division

Let $n$ be a positive integer. We want to know whether $n$ is a prime number. A simple algorithm is based on the following theorem.

**Theorem 7.1.1**
*If $n$ is a composite positive integer, then $n$ has a prime divisor $p$ which is less than or equal to $\sqrt{n}$.*

*Proof.* Since $n$ is composite, we can write $n = ab$ with $a > 1$ and $b > 1$. Now we have $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, since otherwise $n = ab > \sqrt{n}\sqrt{n} = n$. Suppose that $a \leq \sqrt{n}$. By Theorem 1.11.2, $a$ has a prime divisor $p$ which also divides $n$. Then $p \leq a \leq n$, and this proves the assertion. □

Theorem 7.1.1 suggests the following algorithm to test whether $n$ is prime. The algorithm checks, for all prime numbers $p$ that are less than or equal to $n$, whether they divide $n$. If a prime divisor of $n$ is found, then $n$ is composite. Otherwise, $n$ is prime. The prime numbers $p \leq \sqrt{n}$ can either be generated by the sieve of Eratosthenes (see [4]) or be obtained from a precomputed table. It is also possible to test whether $n$ is divisible by any odd, positive integer $m \leq \sqrt{n}$. This procedure is called *trial division*.

**Example 7.1.2**
We use trial division to decide whether $n = 15413$ is prime. We have $\lfloor\sqrt{n}\rfloor = 124$. Hence, we must test whether one of the prime numbers $p \leq 124$ divides $n$. The odd primes $p \leq 124$ are 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. None of them divides $n$. Therefore, $n$ is a prime number.

Trial division can also be used to find the prime factorization of $n$. If a prime factor $p$ is found, then $n$ is replaced by $n/p$ and trial division is applied again. This is repeated until $n$ is proven prime.

**Example 7.1.3**
We factor 476 by trial division. The first prime divisor that we find is 2 and $476/2 = 238$. The next prime factor is again 2 and $238/2 = 119$. The next prime factor is 7 and $119/7 = 17$. The number 17 is prime. Hence, the prime factorization of 476 is $476 = 2^2 * 7 * 17$.

If $n$ is large, then trial division becomes very inefficient. In factoring algorithms, trial division is typically used to find all prime factors that are less than $10^6$.



To estimate the running time of trial division, we need an estimate for the number of primes below a given bound. We use the following notation.

**Definition 7.1.4**
If $x$ is a positive real number, then $\pi(x)$ denotes the number of primes that are less than or equal to $x$.

**Example 7.1.5**
We have $\pi(1) = 0$, $\pi(4) = 2$. As we have seen in Example 7.1.2, we also have $\pi(124) = 30$.

The following theorem is presented without proof. For the proof, see [61].

**Theorem 7.1.6**
1. *For $x \geq 17$, we have $\pi(x) > x/\log x$.*
2. *For $x > 1$, we have $\pi(x) < 1.25506(x/\log x)$.*

It follows from Theorem 7.1.6 that at least $\lceil\sqrt{n}/\log\sqrt{n}\rceil$ divisions are necessary to prove $n$ prime. For the RSA cryptosystem, we need primes that are greater then $10^{75}$. To prove the primality of such a number, more than $10^{75/2}/\log 10^{75/2} > 0.36 * 10^{36}$ divisions are necessary. This is impossible. In the following sections, we describe more efficient primality tests.

## 7.2 Fermat Test

It is very expensive to prove that a given positive integer is prime. But there are very efficient algorithms that prove the primality of a positive integer with high probability. Such algorithms are called *primality tests*.

A first example of a primality test is the *Fermat test*. It is based on Fermat's theorem (2.11.1) in the following version.

**Theorem 7.2.1 (Fermat's theorem)**
*If $n$ is a prime number, then $a^{n-1} \equiv 1 \bmod n$ for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.*

This theorem can be used to determine that a positive integer is composite. We choose a positive integer $a \in \{1, 2, \ldots, n-1\}$. We use fast exponentiation from Section 2.12 to compute $y = a^{n-1} \bmod n$. If $y \neq 1$, then $n$ is composite by Theorem 7.2.1. If $y = 1$, then we do not know whether $n$ is prime or composite, as the following example shows.

**Example 7.2.2**
Consider $n = 341 = 11 * 31$. We have

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

although $n$ is composite. Therefore, if we use the Fermat test with $n = 341$ and $a = 2$, then we obtain $y = 1$, which proves nothing. On the other hand, we have

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

If we use the Fermat test with $n = 341$ and $a = 3$, then $n$ is proven composite.

If the Fermat test proves that $n$ is composite, it does not find a divisor of $n$. It only shows that $n$ lacks a property that all prime numbers have. Therefore, the Fermat test cannot be used as a factoring algorithm.

## 7.3 Carmichael Numbers

The Fermat test can prove that a positive integer $n$ is composite, but it cannot prove that $n$ is prime. However, if the Fermat test was not able to find a proof for the compositeness of $n$ for many bases $a$, then it seems likely that $n$ is prime. Unfortunately, there are composite integers that cannot be proven composite by the Fermat test with any basis. They are called *Carmichael numbers* and we discuss them now.

We need two definitions. If $n$ is an odd composite number and if $a$ is an integer that satisfies

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



then $n$ is called a *pseudoprime* to the base $a$. If $n$ is a pseudoprime to the base $a$ for all integers with $\gcd(a, n) = 1$, then $n$ is called a *Carmichael number*. The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$. It has been shown that there are infinitely many Carmichael numbers. Because of the existence of Carmichael numbers, the Fermat test is not optimal for practical use. A better choice is the Miller-Rabin test, which will be described shortly. For the analysis of the Miller-Rabin test, we need the following characterization of Carmichael numbers.

**Theorem 7.3.1**
*An odd composite number $n \geq 3$ is a Carmichael number if and only if it is square free (i.e., it has no multiple prime divisors, and for each prime divisor $p$ of $n$ the integer $p - 1$ divides $n - 1$).*

*Proof.* Let $n \geq 3$ be a Carmichael number. Then

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

for any integer $a$ that is prime to $n$. Let $p$ be a prime divisor of $n$, and let $a$ be a primitive root mod $p$ that is prime to $n$. Such a primitive root can be constructed using the Chinese remainder theorem. Then (7.1) implies

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

By Theorem 2.9.2, $p - 1$, the order of $a$, divides $n - 1$. It remains to be shown that $p^2$ does not divide $n$. We use a similar argument. Suppose that $p^2$ divides $n$. Then $(p-1)p$ divides $\varphi(n)$, and it can even be shown that the multiplicative group of residues mod $n$ contains an element of order $p(p-1)$. This follows from the structure of the multiplicative group of residues mod $n$, which is a product of cyclic groups of prime power order. As earlier, we find that $p(p-1)$ is a divisor of $n-1$. In particular, $p$ is a divisor of $n-1$. This is impossible because $p$ is a divisor of $n$.

Conversely, let $n$ be square-free and assume that $p - 1$ divides $n - 1$ for all prime divisors $p$ of $n$. Let $a$ be an integer that is prime to $n$. Then

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

by Fermat's little theorem, and therefore

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

since $n-1$ is a multiple of $p-1$. This implies

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

because the prime divisors of $n$ are pairwise distinct. □

## 7.4 Miller-Rabin Test

In this section, we describe the Miller-Rabin test. Contrary to the Fermat test, the Miller-Rabin test can prove the compositeness of any composite positive integer. In other words, there is no analog of Carmichael numbers for the Miller-Rabin test.

The Miller-Rabin test is based on a modification of Fermat's little theorem. The situation is the following. Let $n$ be an odd, positive integer and let

$$s = \max\{r \in \mathbb{N} : 2^r \text{ divides } n-1\},$$

so $2^s$ is the largest power of 2 that divides $n-1$. Set

$$d = (n-1)/2^s.$$

Then $d$ is odd.

**Theorem 7.4.1**
*If $n$ is a prime and if $a$ is an integer that is prime to $n$, then with the previous notation we have either*

$$a^d \equiv 1 \bmod n \tag{7.2}$$

*or there exists $r$ in the set $\{0, 1, \ldots, s-1\}$ with*

$$a^{2^r d} \equiv -1 \bmod n. \tag{7.3}$$

*Proof.* Let $a$ be an integer that is prime to $n$. The order of the multiplicative group of residues mod $n$ is $n-1 = 2^s d$ because $n$ is a prime number. Therefore, the order $k$ of the residue class $a^d + n\mathbb{Z}$ is a power of 2. If this order is $k = 1 = 2^0$, then

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

If $k > 1$, then $k = 2^l$ with $1 \le l \le s$. Therefore, the residue class $a^{2^{l-1}d} + n\mathbb{Z}$ has order 2. By Exercise 2.23.20, the only element of order 2 in $(\mathbb{Z}/n\mathbb{Z})^*$ is $-1 + n\mathbb{Z}$. This implies

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

for $r = l-1$. □

If $n$ is a prime, then at least one of the conditions from Theorem 7.4.1 holds. Therefore, if we find an integer $a$ that is prime to $n$ and that satisfies neither (7.2) nor (7.3) for some $r \in \{0, \ldots, s-1\}$, then $n$ is proven composite. Such an integer is called a *witness* for the compositeness of $n$.

**Example 7.4.2**
Let $n = 561$. Since $n$ is a Carmichael number, the Fermat test cannot prove its compositeness. But $a = 2$ is a witness for the compositeness of $n$, as we will now show. We have $s = 4$, $d = 35$ and $2^{35} \equiv 263 \bmod 561$, $2^{2*35} \equiv 166 \bmod 561$, $2^{4*35} \equiv 67 \bmod 561$, $2^{8*35} \equiv 1 \bmod 561$. Therefore, Theorem 7.4.1 proves that 561 is composite.

For the efficiency of the Miller-Rabin test, it is important that there are sufficiently many witnesses for the compositeness of a composite number. This is shown in the next theorem.

**Theorem 7.4.3**
*If $n \ge 3$ is an odd composite number, then the set $\{1, \ldots, n-1\}$ contains at most $(n-1)/4$ numbers that are prime to $n$ and not witnesses for the compositeness of $n$.*

*Proof.* Let $n \ge 3$ be an odd, composite positive integer.

We want to estimate the number of elements $a \in \{1, 2, \ldots, n-1\}$ with $\gcd(a, n) = 1$ and

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

or

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

for some $r \in \{0, 1, \ldots, s-1\}$. If such an $a$ does not exist, then we are finished. Suppose such a nonwitness exists. Then there is one for which (7.5) holds. In fact, if $a$ satisfies (7.4), $-a$ satisfies (7.5). Let $k$ be the maximum value of $r$ for which there is an integer $a$ that satisfies $\gcd(a, n) = 1$ and (7.5). We set

$$m = 2^k d.$$

Let

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

be the prime factorization of $n$. We define the following subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$:

$$J = \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^{n-1} \equiv 1 \bmod n\},$$

$$K = \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^m \equiv \pm 1 \bmod p^{e(p)} \text{ for all } p|n\},$$

$$L = \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^m \equiv \pm 1 \bmod n\},$$

$$M = \{a + n\mathbb{Z} : \gcd(a, n) = 1, a^m \equiv 1 \bmod n\}.$$

We have

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

For each $n$ that is prime to $a$ and is not a witness for the compositeness of $n$, the residue class $a + n\mathbb{Z}$ belongs to $L$. We will prove the assertion of the theorem by proving that the index of $L$ in $(\mathbb{Z}/n\mathbb{Z})^*$ is at least four.

The index of $M$ in $K$ is a power of 2 because the square of each element of $K$ belongs to $M$. Therefore, the index of $L$ in $K$ is also a power of 2, say $2^j$. If $j \geq 2$, then we are finished.

If $j = 1$, then $n$ has two prime divisors. It follows from Exercise 7.6.5 that $n$ is not a Carmichael number. This implies that $J$ is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ and the index of $J$ in $(\mathbb{Z}/n\mathbb{Z})^*$ is at least 2. By definition of $m$, the index of $L$ in $K$ is also 2. Therefore, the index of $L$ in $(\mathbb{Z}/n\mathbb{Z})^*$ is at least 4.

Finally, let $j = 0$. Then $n$ is a prime power. In this case, it can be verified that $J$ has precisely $p - 1$ elements, namely the elements of



the subgroup of order $p - 1$ of the cyclic group $(\mathbb{Z}/p^e\mathbb{Z})^*$. Therefore, the index of $J$ in $(\mathbb{Z}/n\mathbb{Z})^*$ is at least 4 unless we have $n = 9$. For $n = 9$, the assertion can be verified directly. □

**Example 7.4.4**

We determine all witnesses for the compositeness of $n = 15$. We have $n - 1 = 14 = 2 * 7$. Therefore, $s = 1$ and $d = 7$. An integer $a$, which is prime to 15, is a witness for the compositeness of $n$ if and only if $a^7 \bmod 15 \neq 1$ and $a^7 \bmod 15 \neq -1$. The following table contains the corresponding residues:

| $a$ | 1 | 2 | 4 | 7 | 8 | 11 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|
| $a^{14} \bmod 15$ | 1 | 4 | 1 | 4 | 4 | 1 | 4 | 1 |
| $a^7 \bmod 15$ | 1 | 8 | 4 | 13 | 2 | 11 | 7 | 14 |

The integers prime to 15 in $\{1, 2, \ldots, 14\}$ that are nonwitnesses are $1, 2 \leq (15 - 1)/4 = 7/2$.

To apply the Miller-Rabin test to an odd, positive integer $n$, we choose a random number $a \in \{2, 3, \ldots, n-1\}$. If $\gcd(a, n) > 1$, then $n$ is composite. Otherwise, we compute $a^d, a^{2d}, \ldots, a^{2^{s-1}d}$. If we find a witness for the compositeness of $n$, then we have proved that $n$ is composite. By Theorem 7.4.3, the probability that $n$ is composite and we do not find a witness is at most $1/4$. If we repeat the Miller-Rabin test $t$ times and if $n$ is composite, then the probability of not finding a witness is at most $(1/4)^t$. For $t = 10$, this probability is at most $1/2^{20} \sim 1/10^6$. This is very unlikely. A more detailed analysis of the Miller-Rabin test has shown that the error probability is in fact even smaller.

## 7.5 Random Primes

In many public-key systems, random primes of a fixed bit length are required. We describe the construction of such random primes.

We want to generate a random prime of bit length $k$. We generate a random odd $k$-bit number (see Section 4.6). For this purpose, we set the first and last bit of $n$ to 1, and the remaining $k - 2$ bits are chosen randomly with uniform distribution. Then we test whether

$n$ is prime. First, we check whether $n$ is divisible by a prime number below a predefined bound $B$, typically $B = 10^6$. If no prime divisor of $n$ is found, then we apply the Miller-Rabin test $t$ times. The choice $t = 3$ suffices to make the error probability less than $(1/2)^{80}$ if $k \geq 1000$. If this test finds no witness for the compositeness of $n$, then $n$ is considered prime. If trial division is much more efficient than the Miller-Rabin test, then a larger $B$ can be chosen.

## 7.6 Exercises

**Exercise 7.6.1**
Use the Fermat test to show that 1111 is not a prime number.

**Exercise 7.6.2**
Determine $\pi(100)$. Compare your result with the bounds from Theorem 7.1.6.

**Exercise 7.6.3**
Determine the smallest pseudoprime to the base 2.

**Exercise 7.6.4**
Use the Fermat test to prove that the fifth Fermat number $F_5 = 2^{2^5}+1$ is composite. Prove that any Fermat number is a pseudoprime to the base 2.

**Exercise 7.6.5**
Prove that a Carmichael number has at least three different prime factors.

**Exercise 7.6.6**
Use the Miller-Rabin test to prove that the fifth Fermat number $F_5 = 2^{2^5} + 1$ is composite. Compare the efficiency of the test with the efficiency of the Fermat test (see Exercise 7.6.4).

**Exercise 7.6.7**
Use the Miller-Rabin test to prove that the pseudoprime $n$ from Exercise 7.6.3 is composite. Determine the smallest witness for the compositeness of $n$.



**Exercise 7.6.8**
Determine the number of Miller-Rabin witnesses for the compositeness of 221 in $\{1, 2, \ldots, 220\}$. Compare your result with the bound in Theorem 7.4.3.

**Exercise 7.6.9**
Write a program that implements the Miller-Rabin test and use it to determine the smallest 512-bit prime.