2 CHAPTER Congruences and Residue Class Rings

In this chapter, we show how to compute in residue class rings and their multiplicative groups. We also discuss algorithms for finite abelian groups. These techniques are of great importance in cryptographic algorithms.

In this chapter, m is a positive integer and lowercase italic letters denote integers.

2.1 Congruences

Definition 2.1.1
We say that a is *congruent* to b modulo m, and we write $a \equiv b \bmod m$, if m divides the $b - a$.

Example 2.1.2
We have $-2 \equiv 19 \bmod 21$, $10 \equiv 0 \bmod 2$.

It can be easily verified that congruence modulo m is an equivalence relation on the integers. This means that

1. any integer is congruent to itself modulo m (reflexivity),

2. $a \equiv b \bmod m$ implies $b \equiv a \bmod m$ (symmetry),
3. $a \equiv b \bmod m$ and $b \equiv c \bmod m$ implies $a \equiv c \bmod m$ (transitivity).

Moreover, we have the following characterizations.

Lemma 2.1.3
The following statements are equivalent:
1. $a \equiv b \bmod m$.
2. *There is* $k \in \mathbb{Z}$ *with* $a = b + km$.
3. *When divided by* m, *both* a *and* b *leave the same remainder.*

The *equivalence class* of a consists of all integers that are obtained from a by adding integer multiples of m; i.e.,

$$\{b : b \equiv a \bmod m\} = a + m\mathbb{Z}.$$

This equivalence class is called the *residue class* of a mod m.

Example 2.1.4
The residue class of 1 mod 4 is the set $\{1, 1\pm4, 1\pm2*4, 1\pm3*4, \ldots\} = \{1, -3, 5, -7, 9, -11, 13, \ldots\}$. The residue class of 0 mod 2 is the set of all even integers. The residue class of 1 mod 2 is the set of all odd integers. The residue classes mod 4 are $0+4\mathbb{Z}$, $1+4\mathbb{Z}$, $2+4\mathbb{Z}$, $3+4\mathbb{Z}$.

The set of residue classes mod m is denoted by $\mathbb{Z}/m\mathbb{Z}$. It has m elements, since $0, 1, 2, \ldots, m-1$ are the possible remainders of the division by m. A *set of representatives* for those residue classes is a set of integers that contains exactly one element of each residue class mod m.

Example 2.1.5
A set of representatives mod 3 contains an element of each of the residue classes $3\mathbb{Z}$, $1+3\mathbb{Z}$, $2+3\mathbb{Z}$. Hence, $\{0, 1, 2\}$, $\{3, -2, 5\}$, $\{9, 16, 14\}$ are such sets.

One set of representatives mod m is the set $\{0, 1, \ldots, m-1\}$. Its elements are called the *least nonnegative residues* mod m. This set is denoted by $\mathbb{Z}_m$. Likewise, $\{1, 2, \ldots, m\}$ is a set of representatives mod m. Its elements are called the *least positive residues* mod m. Also, $\{n+1, n+2, \ldots, n+m\}$ with $n = -\lceil m/2 \rceil$ is a set of representatives mod m.

Example 2.1.6

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

is the set of least nonnegative residues mod 13.

We need a few rules for computing with congruences. They will later allow us to define a ring structure on the residue classes mod m.

Theorem 2.1.7
$a \equiv b \bmod m$ *and* $c \equiv d \bmod m$ *implies* $-a \equiv -b \bmod m$, $a + c \equiv b + d \bmod m$, *and* $ac \equiv bd \bmod m$.

Proof. Since m divides $a - b$, m also divides $-a + b$. Therefore, $-a \equiv -b \bmod m$. Since m divides $a - b$ and $c - d$, m also divides $a - b + c - d = (a + c) - (b + d)$. Therefore, $a + c \equiv b + d \bmod m$. To show that $ac \equiv bd \bmod m$, we write $a = b + lm$ and $c = d + km$. Then we obtain $ac = bd + m(ld + kb + lkm)$, as asserted. □

Example 2.1.8
We apply Theorem 2.1.7 to prove that the fifth Fermat number $2^{2^5}+1$ is divisible by 641. First,

$$641 = 640 + 1 = 5 * 2^7 + 1.$$

This implies

$$5 * 2^7 \equiv -1 \bmod 641.$$

From Theorem 2.1.7, we deduce that this congruence remains valid if both sides are raised to the fourth power; i.e.,

$$5^4 * 2^{28} \equiv 1 \bmod 641. \tag{2.1}$$

On the other hand,

$$641 = 625 + 16 = 5^4 + 2^4.$$

This implies

$$5^4 \equiv -2^4 \bmod 641.$$

If we use this congruence in (2.1), we obtain

$$-2^{32} \equiv 1 \bmod 641;$$

hence,

$$2^{32} + 1 \equiv 0 \bmod 641.$$

This proves that 641 is a divisor of the fifth Fermat number.

We want to prove that the residue classes modulo m form a ring. In the following sections, we review a few basic notions of algebra.

2.2 Semigroups

Definition 2.2.1
If X is a set, a map $\circ : X \times X \to X$ which sends a pair (x_1, x_2) of elements from X to the element $x_1 \circ x_2$ is called an *operation* on X.

Example 2.2.2
On the set of real numbers, we already know the operations addition and multiplication.

On the set $\mathbb{Z}/m\mathbb{Z}$ of residue classes mod m, we introduce two operations, addition and multiplication.

Definition 2.2.3
The sum of the residue classes $a + m\mathbb{Z}$ and $b + m\mathbb{Z}$ is $(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}$. The product of the residue classes $a + m\mathbb{Z}$ and $b + m\mathbb{Z}$ is $(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) = (a \cdot b) + m\mathbb{Z}$.

Observe that the sum and product of residue classes modulo m are defined using representatives. From Theorem 2.1.7, it follows, however, that these definitions are independent of the representatives. In practice, the residue classes are represented using fixed representatives. The computations are done with those representatives.

Example 2.2.4
We have $(3+5\mathbb{Z})+(2+5\mathbb{Z}) = (5+5\mathbb{Z}) = 5\mathbb{Z}$ and $(3+5\mathbb{Z})(2+5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$. We can also write this computation in the form $3 + 2 \equiv 0 \bmod 5$ and $3 * 2 \equiv 1 \bmod 5$.

Definition 2.2.5
Let $\circ$ be an operation on the set X. It is called *associative* if $(a \circ b) \circ c = a \circ (b \circ c)$ holds for all $a, b, c \in X$. It is called *commutative* if $a \circ b = b \circ a$ for all $a, b \in X$.

Example 2.2.6
Addition and multiplication on the set of real numbers are associative and commutative. The same is true for addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$.

Definition 2.2.7
A pair $(H, \circ)$ consisting of a set H and an associative operation $\circ$ on H is called a *semigroup*. The semigroup is called *commutative* or *abelian* if the operation $\circ$ is commutative.

Example 2.2.8
Commutative semigroups are $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, \cdot)$.

Let $(H, \circ)$ be a semigroup, and set $a^1 = a$ and $a^{n+1} = a \circ a^n$ for $a \in H$ and $n \in \mathbb{N}$. Then the following are true:

$$a^n \circ a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \quad a \in H, n, m \in \mathbb{N}. \tag{2.2}$$

If $a, b \in H$ and $a \circ b = b \circ a$, then

$$(a \circ b)^n = a^n \circ b^n. \tag{2.3}$$

If the semigroup is commutative, then (2.3) is true in general.

Definition 2.2.9
A *neutral element* of the semigroup $(H, \circ)$ is an element $e \in H$ which satisfies $e \circ a = a \circ e = a$ for all $a \in H$. If the semigroup contains a neutral element, then it is called *monoid*.

A semigroup has at most one neutral element (see Exercise 2.23.3).

Definition 2.2.10
If e is the neutral element of the semigroup $(H, \circ)$ and if $a \in H$, then $b \in H$ is called an *inverse* of a if $a \circ b = b \circ a = e$. If a has an inverse, then a is called *invertible* in the semigroup H.

In a monoid, each element has at most one inverse (see Exercise 2.23.5).

Example 2.2.11

1. The neutral element of the semigroup $(\mathbb{Z}, +)$ is 0. The inverse of a is $-a$.
2. The neutral element of the semigroup $(\mathbb{Z}, \cdot)$ is 1. The only invertible elements are 1 and -1.
3. The neutral element of the semigroup $(\mathbb{Z}/m\mathbb{Z}, +)$ is the residue class $m\mathbb{Z}$. The inverse of $a + m\mathbb{Z}$ is $-a + m\mathbb{Z}$.
4. The neutral element of the semigroup $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ is $1 + m\mathbb{Z}$. The invertible elements will be determined later.

2.3 Groups

Definition 2.3.1

A *group* is a monoid in which any element is invertible. The group is called *commutative* or *abelian* if the monoid is commutative.

Example 2.3.2

1. The monoid $(\mathbb{Z}, +)$ is an abelian group.
2. The monoid $(\mathbb{Z}, \cdot)$ is not a group because not every element is invertible.
3. The monoid $(\mathbb{Z}/m\mathbb{Z}, +)$ is an abelian group.

Let $(G, \cdot)$ be a group. Denote by a^{-1} the inverse of $a \in G$, and set $a^{-n} = (a^{-1})^n$ for each positive integer n. Then (2.2) holds for all integral exponents. If the group is abelian, then (2.3) is true for all integers n.

In a group, the following *cancellation rules* can be easily verified.

Theorem 2.3.3

Let $(G, \cdot)$ be a group and $a, b, c \in G$. Then $ca = cb$ implies $a = b$ and $ac = bc$ implies $a = b$.

Definition 2.3.4

The *order* of a group or a semigroup is the number of its elements.

Example 2.3.5

The additive group $\mathbb{Z}$ has infinite order. The additive group $\mathbb{Z}/m\mathbb{Z}$ has order m.

2.4 Residue Class Ring

Definition 2.4.1

A *ring* is a triplet $(R, +, \cdot)$ such that $(R, +)$ is an abelian group and $(R, \cdot)$ is a semigroup. In addition, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ and $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ for all $x, y, z \in R$. The ring is called *commutative* if the semigroup $(R, \cdot)$ is commutative. A *unit element* of the ring is a neutral element of the semigroup $(R, \cdot)$.

Example 2.4.2

The triplet $(\mathbb{Z}, +, \cdot)$ is a commutative ring with unit element 1. This implies that $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ is a commutative ring with unit element $1 + m\mathbb{Z}$. The latter ring is called the *residue class ring* modulo m.

Instead of writing $(R, +, \cdot)$ for a ring, we also write R if it is clear which operations are meant. For example, we write $\mathbb{Z}/m\mathbb{Z}$ for the residue class ring modulo m.

Definition 2.4.3

Let R be a ring with unit element. An element a of R is called *invertible* or a *unit* if it is invertible in the multiplicative semigroup of R. The element a is called a *zero divisor* if it is nonzero and there is a nonzero $b \in R$ with $ab = 0$ or $ba = 0$.

In Exercise 2.23.9, it is shown that the units of a commutative ring R form a group. It is called the *unit group* of R and is denoted by R^*.

Example 2.4.4

The ring of integers contains no zero divisors.

The zero divisors of the residue class ring $\mathbb{Z}/m\mathbb{Z}$ are the residue classes $a + m\mathbb{Z}$ with $1 < \gcd(a, m) < m$. In fact, if $a + m\mathbb{Z}$ is a zero divisor of $\mathbb{Z}/m\mathbb{Z}$, then there is an integer b with $ab \equiv 0 \bmod m$ but neither $a \equiv 0 \bmod m$ nor $b \equiv 0 \bmod m$. Hence, m is a divisor of ab but neither of a nor of b. This means that $1 < \gcd(a, m) < m$. If, conversely, $1 < \gcd(a, m) < m$ and $b = m/\gcd(a, m)$, then $a \not\equiv 0 \bmod m$, $ab \equiv 0 \bmod m$, and $b \not\equiv 0 \bmod m$. Therefore, $a + m\mathbb{Z}$ is a zero divisor of $\mathbb{Z}/m\mathbb{Z}$.

If p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ contains no zero divisors.

2.5 Fields

Definition 2.5.1
A *field* is a commutative ring in which every nonzero element is invertible.

Example 2.5.2
The set of integers is not a field because most integers are not invertible, but it is contained in the field of rational numbers. Also, the real and complex numbers form a field. As we will see later, the residue class ring modulo a prime number is a field.

2.6 Division in the Residue Class Ring

Divisibility in rings is defined as divisibility in $\mathbb{Z}$. To explain this in more detail, we let R be a ring and let $a, n \in R$.

Definition 2.6.1
We say that a *divides* n if there is a $b \in R$ such that $n = ab$.

If the ring element a divides n, then a is called a *divisor* of n and n is called a *multiple* of a, and we write $a|n$. We also say that n is *divisible* by a. If a is not a divisor of n, then we write $a \nmid n$.

We study which elements of the residue class ring mod m are invertible.

First, we note that the residue class $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if the congruence

$$ax \equiv 1 \bmod m \tag{2.4}$$

is solvable. The next theorem answers the question when this is the case.

Theorem 2.6.2
The residue class $a + m\mathbb{Z}$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ (i.e., the congruence (2.4) is solvable) if and only if $\gcd(a, m) = 1$. *If* $\gcd(a, m) = 1$, *then the inverse of $a + m\mathbb{Z}$ is uniquely determined (i.e., the solution x of (2.4) is uniquely determined mod m).*

Proof. Let $g = \gcd(a, m)$ and let x be a solution of (2.4). Then g is a divisor of m and therefore it is a divisor of $ax - 1$. But g is also a divisor of a. Hence, g is a divisor of 1 (i.e., $g = 1$ because g, being a gcd, is positive). Conversely, let $g = 1$. Then by Corollary 1.7.7 there are numbers x, y with $ax + my = 1$ (i.e., $ax - 1 = -my$). This shows that x is a solution of the congruence (2.4) and that $x + m\mathbb{Z}$ is an inverse of $a + m\mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$.

To prove the uniqueness, let $v + m\mathbb{Z}$ be another inverse of $a + m\mathbb{Z}$. Then $ax \equiv av \bmod m$. Therefore, m divides $a(x - v)$. Because $\gcd(a, m) = 1$, this implies that m is a divisor of $x - v$. This proves $x \equiv v \bmod m$. □

A residue class $a + m\mathbb{Z}$ with $\gcd(a, m) = 1$ is called an *invertible residue class* modulo m. Theorem 2.6.2 implies that a residue class $a + m\mathbb{Z}$ with $1 \leq a < m$ is either a zero divisor or an invertible residue class (i.e., a unit in the residue class ring mod m).

In the proof of Theorem 2.6.2, we have shown how to solve the congruence $ax \equiv 1 \bmod m$ with the extended Euclidean algorithm (see Section 1.9) since it computes the representation $1 = ax + my$. In fact, we only need the coefficient x. By Theorem 1.10.5, the solution of the congruence can be computed efficiently.

Example 2.6.3
Let $m = 12$. The residue class $a + 12\mathbb{Z}$ is invertible in $\mathbb{Z}/12\mathbb{Z}$ if and only if $\gcd(a, 12) = 1$. The invertible residue classes mod 12 are therefore $1 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 11 + 12\mathbb{Z}$. To find the inverse of $5 + 12\mathbb{Z}$, we use the extended Euclidean algorithm. We obtain $5*5 \equiv 1 \bmod 12$. Analogously, we have $7*7 \equiv 1 \bmod 12$ and $11*11 \equiv 1 \bmod 12$.

We also introduce the residue class field modulo a prime number, which is frequently used in cryptography.

Theorem 2.6.4
The residue class ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is a prime number.

Proof. By Theorem 2.6.2, the ring $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if $\gcd(k, m) = 1$ for all k with $1 \leq k < m$. This is true if and only if m is a prime number. □

2.7 Analysis of the Operations in the Residue Class Ring

In all algorithms of public-key cryptography, computing in residue class rings is very time-consuming. Frequently, those computations must be carried out on smart cards. It is therefore important to know how efficiently those computations can be carried out. This is described in this section.

We assume that the elements of the residue class ring $\mathbb{Z}/m\mathbb{Z}$ are represented by their smallest nonnegative representatives. Under this assumption, we estimate the running time of the operations in the residue class ring.

Let $a, b \in \{0, 1, \ldots, m-1\}$.

To compute $(a+m\mathbb{Z})+(b+m\mathbb{Z})$, we must determine $(a+b)$ mod m. First, we compute $c = a+b$. The required sum is $c+m\mathbb{Z}$, but c may be the wrong representative since we only know that $0 \le c < 2m$. If $0 \le c < m$, then c is the correct representative. If $m \le c < 2m$, then the correct representative is $c - m$ because $0 \le c - m < m$. In this case, we replace c by $c-m$. Likewise, $(a+m\mathbb{Z})-(b+m\mathbb{Z})$ is computed. We determine $c = a - b$. Then $-m < c < m$. If $0 \le c < m$, then c is the correct representative of the difference. If $-m < c < 0$, then the correct representative is $c + m$. Hence, c must be replaced by $c + m$. The results in Section 1.5 imply that the sum and difference of two residue classes modulo m can be computed in time $O(\text{size}\, m)$.

Now we wish to compute $(a+m\mathbb{Z})(b+m\mathbb{Z})$. We determine $c = ab$. Then $0 \le c < m^2$. We divide c with remainder by m and replace c by the remainder of this division. For the quotient q of this division, we have $0 \le q < m$. By the results of Section 1.5, we can perform the multiplication and the division in time $O((\text{size}\, m)^2)$. Hence, two residue classes mod m can be multiplied in time $O((\text{size}\, m)^2)$.

Finally, we discuss how to invert $a + m\mathbb{Z}$. Using the extended Euclidean algorithm, we compute $g = \gcd(a, m)$ and x with $ax \equiv g \bmod m$ and $0 \le x < m$. By Corollary 1.10.3, we have $|x| \le m/(2g)$. Possibly, the algorithm yields a negative x. The x is replaced by $x+m$. By Theorem 1.10.5, this computation requires time $O((\text{size}\, m)^2)$. The residue class $a + m\mathbb{Z}$ is invertible if and only if $g = 1$. In this case, x is the least nonnegative representative of the inverse class. The total computing time is $O((\text{size}\, m)^2)$. This implies that the division by an invertible residue class mod m takes time $O((\text{size}\, m)^2)$.

In all algorithms, only constantly many numbers of size $O(\text{size}\, m)$ must be stored. Therefore, the algorithms require space $O(\text{size}\, m)$. We remark that there are algorithms for multiplying and dividing residue classes that are asymptotically more efficient. They require time $O(\log m(\log\log m)^2)$ (see [3]). For numbers of the sizes relevant in cryptography, these algorithms are, however, slower than the ones that we have analyzed here. In many situations, the $O((\text{size}\, m)^2)$ algorithms admit optimizations. An overview can be found in [49].

We have proved the following theorem.

Theorem 2.7.1
Suppose the residue classes modulo m are represented by their least nonnegative representatives. Then two residue classes mod m can be added and subtracted using time and space $O(\text{size}\, m)$. *They can be multiplied and divided using time* $O((\text{size}\, m)^2)$ *and space* $O(\text{size}\, m)$.

2.8 Multiplicative Group of Residues mod m

The following result is of crucial importance in cryptography.

Theorem 2.8.1
The set of all invertible residue classes modulo m is a finite abelian group with respect to multiplication.

Proof. By Theorem 2.6.2, this set is the unit group of the residue class rings mod m. □

The group of invertible residue classes modulo m is called the *multiplicative group of residues* modulo m and is written $(\mathbb{Z}/m\mathbb{Z})^*$. Its order is denoted by $\varphi(m)$. The function

$$\mathbb{N} \to \mathbb{N}, \quad m \mapsto \varphi(m)$$

is called the *Euler φ-function*. Observe that $\varphi(m)$ is the number of integers a in $\{1, 2, \ldots, m\}$ with $\gcd(a, m) = 1$. In particular, $\varphi(1) = 1$.

TABLE 2.1 Values of the Euler φ-function.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Example 2.8.2
The multiplicative group of residues mod 12 is $(\mathbb{Z}/12\mathbb{Z})^* = \{1 + 12\mathbb{Z}, 5 + 12\mathbb{Z}, 7 + 12\mathbb{Z}, 11 + 12\mathbb{Z}\}$. Hence, $\varphi(12) = 4$.

A few values of the Euler φ-function can be found in Table 2.1.

In this table, we see that $\varphi(p) = p - 1$ for the prime numbers p. This is in general true for any prime numbers p because all numbers a between 1 and $p - 1$ are prime to p. This proves the following theorem.

Theorem 2.8.3
If p is a prime number, then $\varphi(p) = p - 1$.

The Euler φ-function has the following useful property.

Theorem 2.8.4

$$\sum_{d|m,d>0} \varphi(d) = m.$$

Proof. We have

$$\sum_{d|m,d>0} \varphi(d) = \sum_{d|m,d>0} \varphi(m/d)$$

because the set of positive divisors of m is $\{m/d : d|m, d > 0\}$. Now $\varphi(m/d)$ is the number of integers a in the set $\{1, \ldots, m/d\}$ with $\gcd(a, m/d) = 1$. Hence, $\varphi(m/d)$ is the number of integers b in $\{1, 2, \ldots, m\}$ with $\gcd(b, m) = d$. Therefore,

$$\sum_{d|m,d>0} \varphi(d) = \sum_{d|m,d>0} |\{b : 1 \leq b \leq m \text{ with } \gcd(b, m) = d\}|.$$

But

$$\{1, 2, \ldots, m\} = \cup_{d|m,d>0}\{b : 1 \leq b \leq m \text{ with } \gcd(b, m) = d\}.$$

This implies the assertion. □

2.9 Order of Group Elements

Next, we introduce element orders and their properties. Let G be a group that is multiplicatively written with neutral element 1.

Definition 2.9.1
Let $g \in G$. If there is a positive integer e with $g^e = 1$, then the smallest such integer is called the *order* of g in G. Otherwise, we say that the order of g in G is infinite. The order of g in G is denoted by $\text{order}_G g$. If it is clear which group we mean, we also write $\text{order} g$.

Theorem 2.9.2
Let $g \in G$ and $e \in \mathbb{Z}$. Then $g^e = 1$ if and only if e is divisible by the order of g in G.

Proof. Let $n = \text{order} g$. If $e = kn$, then

$$g^e = g^{kn} = (g^n)^k = 1^k = 1.$$

Conversely, let $g^e = 1$ and $e = qn + r$ with $0 \leq r < n$. Then

$$g^r = g^{e-qn} = g^e(g^n)^{-q} = 1.$$

Because n is the least positive integer with $g^n = 1$, and since $0 \leq r < n$, we have $r = 0$ and therefore $e = qn$. Hence, n is a divisor of e, as asserted. □

Corollary 2.9.3
Let $g \in G$ and let k, l be integers. Then $g^l = g^k$ if and only if $l \equiv k \bmod \text{order} g$.

Proof. Set $e = l - k$ and apply Theorem 2.9.2. □

Example 2.9.4
We determine the order of $2 + 13\mathbb{Z}$ in $(\mathbb{Z}/13\mathbb{Z})^*$. For this purpose, we use the following table:

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \bmod 13$	1	2	4	8	3	6	12	11	9	5	10	7	1

We see that the order of $2 + 13\mathbb{Z}$ is 12. This order is equal to the group order of $(\mathbb{Z}/13\mathbb{Z})^*$, but this is not true for any group element. For example, the order of $4 + 13\mathbb{Z}$ is 6.

We determine the order of powers.

Theorem 2.9.5
If $g \in G$ is of finite order e and if n is an integer, then $\text{order} g^n = e/\gcd(e,n)$.

Proof. We have

$$(g^n)^{e/\gcd(e,n)} = (g^e)^{n/\gcd(e,n)} = 1,$$

so Theorem 2.9.3 implies that $e/\gcd(e,n)$ is a multiple of the order of g^n. Suppose

$$1 = (g^n)^k = g^{nk}.$$

Then Theorem 2.9.3 implies that e is a divisor of nk. Therefore, $e/\gcd(e,n)$ is a divisor of k, which implies the assertion. □

2.10 Subgroups

We introduce subgroups. By G we denote a group.

Definition 2.10.1
A subset U of G is called a *subgroup* of G if U together with the group operation of G is a group.

Example 2.10.2
For all $g \in G$, the set $\{g^k : k \in \mathbb{Z}\}$ is a subgroup of G. It is called the *subgroup generated* by g and is denoted by $\langle g \rangle$.

If g has finite order e, then $\langle g \rangle = \{g^k : 0 \le k < e\}$. In fact, for any integer x we have $g^x = g^{x \bmod e}$ by Corollary 2.9.3. Corollary 2.9.3 also implies that e is the order of $\langle g \rangle$.

Example 2.10.3
By Example 2.9.4, the subgroup generated by $2 + 13\mathbb{Z}$ in $(\mathbb{Z}/13\mathbb{Z})^*$ is the full group $(\mathbb{Z}/13\mathbb{Z})^*$. The subgroup generated by $4 + 13\mathbb{Z}$ has order 6. It is $\{k + 13\mathbb{Z} : k = 1, 3, 4, 9, 10, 12\}$.

Definition 2.10.4
If $G = \langle g \rangle$ for some $g \in G$, then G is called *cyclic* and g is called a *generator* of G.

Example 2.10.5
The additive group $\mathbb{Z}$ is cyclic. It has two generators, namely 1 and -1.

Theorem 2.10.6
If G is finite and cyclic, then G has exactly $\varphi(|G|)$ generators and they are all of order $|G|$.

Proof. Let $g \in G$ be an element of order e. Then the subgroup generated by g has order e. Hence, an element of G is a generator of G if and only if it is of order $|G|$. We determine the number of elements of order $|G|$ in G. Let g be a generator of G. Then $G = \{g^k : 0 \le k < |G|\}$. By Theorem 2.9.5 an element of this set is of order $|G|$ if and only if $\gcd(k, |G|) = 1$. This means that the number of generators of G is exactly $\varphi(|G|)$. □

Example 2.10.7
Since the order of $2 + 13\mathbb{Z}$ in $(\mathbb{Z}/13\mathbb{Z})^*$ is 12, the group $(\mathbb{Z}/13\mathbb{Z})^*$ is cyclic. We will prove later that $(\mathbb{Z}/p\mathbb{Z})^*$ is always cyclic if p is a prime number. By Example 2.9.4, the generators of this group are the residue classes $a + 13\mathbb{Z}$ with $a \in \{2, 6, 7, 11\}$.

To prove the next result, we need a few notions. A map $f : X \to Y$ is called *injective* if $f(x) = f(y)$ implies $x = y$ for all $x, y \in X$. This means that two different elements of X can never have the same image under f. The map is called *surjective* if for any $y \in Y$ there is $x \in X$ with $f(x) = y$. The map is called *bijective* if it is injective and surjective. A bijective map is also called a *bijection*. If there is a bijection between two finite sets, then the sets have the same number of elements.

Example 2.10.8
Consider the map $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto f(n) = n$. This map is obviously bijective.

Consider the map $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto f(n) = n^2$. Since positive integers have pairwise distinct squares, the map is injective. But since 3 is not the square of a positive integer, the map is not surjective.

Consider the map $f : \{1, 2, 3, 4, 5, 6\} \to \{0, 1, 2, 3, 4, 5\}$, $n \mapsto f(n) = n \bmod 6$. Since both sets are sets of representatives modulo 6, the map is bijective.

We prove a theorem of Lagrange.

Theorem 2.10.9
If G is a finite group, then the order of each subgroup of G divides the order of G.

Proof. Let H be a subgroup of G. We say that two elements a and b of G are equivalent if $a/b = ab^{-1}$ belongs to H. This is an equivalence relation. In fact, $a/a = 1 \in H$; hence the relation is reflexive. Since $a/b \in H$, the inverse b/a also belongs to H, so the relation is symmetric. Finally, since $a/b \in H$ and $b/c \in H$, it follows that $a/c = (a/b)(b/c) \in H$. This proves the transitivity of the relation.

We show that all the equivalence classes have the same cardinality. The equivalence class of $a \in G$ is $\{ha : h \in H\}$. Let a, b be two elements of G. Consider the map

$$\{ha : h \in H\} \to \{hb : h \in H\}, ha \mapsto hb.$$

The map is injective because in the group G cancellation is possible by Theorem 2.3.3. Moreover, the map is surjective. Therefore, all equivalence classes have the same number of elements. Since G is the disjoint union of all the equivalence classes, the number of elements in one equivalence class must divide $|G|$. But the equivalence class of 1 is H; hence $|H|$ divides $|G|$. □

Definition 2.10.10
If H is a subgroup of G, then the positive integer $|G|/|H|$ is called the *index* of H in G.

2.11 Fermat's Little Theorem

We formulate the famous theorem of Fermat.

Theorem 2.11.1
If $\gcd(a, m) = 1$, *then* $a^{\varphi(m)} \equiv 1 \bmod m$.

This theorem is proved below. If $\gcd(a, m) = 1$, then by Theorem 2.11.1 we have

$$a^{\varphi(m)-1} \cdot a \equiv 1 \bmod m.$$

This implies that $a^{\varphi(m)-1} + m\mathbb{Z}$ is the inverse residue class of $a + m\mathbb{Z}$. Hence, we have a new method for computing inverses mod m. If we apply fast exponentiation as explained in Section 2.12, this method can compete with the algorithm that is based on the extended Euclidean algorithm.

We prove Fermat's little theorem in a more general context. Let G be a finite group of order $|G|$, multiplicatively written, with neutral element 1.

Theorem 2.11.2
The order of every group element divides the group order.

Proof. The order of a group element g is the order of the subgroup generated by g. Therefore, the assertion follows from Theorem 2.10.9. □

From this result, we deduce the following general version of Fermat's little theorem.

Corollary 2.11.3
We have $g^{|G|} = 1$ *for all* $g \in G$.

Proof. The assertion follows from Theorem 2.11.2 and Theorem 2.9.3. □

Since $(\mathbb{Z}/m\mathbb{Z})^*$ is a finite abelian group of order $\varphi(m)$, Theorem 2.11.1 follows from Corollary 2.11.3.

2.12 Fast Exponentiation

Theorem 2.11.1 shows that an integer x with $x \equiv a^{\varphi(m)-1} \bmod m$ solves the congruence (2.4). In order for this new method of solving (2.4) to be efficient, we must be able to compute quickly powers mod m.

We now describe an efficient algorithm for computing powers in a monoid G. This algorithm and its variants are central ingredients of many cryptographic protocols. Let $g \in G$ and e be a positive integer.

Let

$$e = \sum_{i=0}^{k} e_i 2^i$$

be the binary expansion of e. Observe that the coefficients e_i are either 0 or 1. Therefore,

$$g^e = g^{\sum_{i=0}^{k} e_i 2^i} = \prod_{i=0}^{k} (g^{2^i})^{e_i} = \prod_{0 \le i \le k, e_i = 1} g^{2^i}.$$

From this formula, we obtain the following idea for computing g^e.

1. Compute the successive squares g^{2^i}, $0 \le i \le k$.
2. Determine g^e as the product of those g^{2^i} for which $e_i = 1$.

Observe that

$$g^{2^{i+1}} = (g^{2^i})^2.$$

Therefore, $g^{2^{i+1}}$ can be computed from g^{2^i} by one squaring. Before we explain the algorithm in more detail, we give an example to show that this method is much faster than the naive one.

Example 2.12.1
We determine 6^{73} mod 100. We write the binary expansion of the exponent:

$$73 = 1 + 2^3 + 2^6.$$

Then we determine the successive squares of 6, $6^2 = 36$, $6^{2^2} = 36^2 \equiv -4 \bmod 100$, $6^{2^3} \equiv 16 \bmod 100$, $6^{2^4} \equiv 16^2 \equiv 56 \bmod 100$, $6^{2^5} \equiv 56^2 \equiv 36 \bmod 100$, $6^{2^6} \equiv -4 \bmod 100$. Hence, $6^{73} \equiv 6 * 6^{2^3} * 6^{2^6} \equiv 6 * 16 * (-4) \equiv 16 \bmod 100$. We have only computed 6 squares and two products $(\mathbb{Z}/m\mathbb{Z})^*$ to obtain the result. If we would have computed 6^{73} mod 100 as $6 * 6 * \cdots * 6 \bmod 100$, 72 multiplications modulo 100 would have been necessary.

Figure 2.1 shows an implementation of fast exponentiation.

This program works as follows. The variable `result` contains the current value of the result. The variable `base` contains the successive squares. The new square is obtained by squaring the old one. The result is multiplied by that square if the corresponding bit in the


```
pow(goupElement base, int exponent, groupElement result)
begin
  result = 1
  while (exponent > 0)
    if (isEven(exponent) == false)
      result = result * base
    base = base*base
    exponent = exponent/2
  end while
end
}
```

FIGURE 2.1 Fast exponentiation

exponent is 1. The following theorem states the complexity of the fast exponentiation algorithm.

Theorem 2.12.2
Algorithm `pow` *computes* $\text{base}^{\text{exponent}}$ *using at most* size(exponent) − 1 *squarings and multiplications. Algorithm* `pow` *only stores a constant number of group elements.*

From Theorem 2.12.2 and Theorem 2.7.1, we obtain an estimate for the time necessary to compute powers in the multiplicative group of residues mod m.

Corollary 2.12.3
If e is an integer and $a \in \{0, \ldots, m-1\}$, then the computation of a^e mod *m requires time $O((\text{size } e)(\text{size } m)^2)$ and space $O(\text{size } e + \text{size } m)$.*

We see that exponentiation in the multiplicative group of residues mod m is possible in polynomial time. Variants of the fast exponentiation algorithm are described in [49] and [53]. Under certain circumstances, they may be more efficient than the basic variant.

2.13 Fast Evaluation of Power Products

Let G be a finite abelian group, $g_1, \ldots, g_k$ be elements of G, and $e_1, \ldots, e_k$ be nonnegative integers. We want to evaluate the power product

$$A = \prod_{i=1}^{k} g_i^{e_i}.$$

We need the binary expansion of the exponents e_i. They are normalized to equal length. Let

$$b_{i,n-1} b_{i,n-2} \ldots b_{i,0}, \quad 1 \le i \le k$$

be the binary expansion of e_i. For at least one i, let $b_{i,n-1}$ be nonzero. For $1 \le i \le k$ and $0 \le j < n$, let $e_{i,j}$ be the integer with binary expansion $b_{i,n-1} b_{i,n-2} \ldots b_{i,j}$. Moreover, let $e_{i,n} = 0$ for $1 \le i \le k$. Then $e_i = e_{i,0}$ for $1 \le i \le k$. Finally, set

$$A_j = \prod_{i=1}^{k} g_i^{e_{i,j}}, 0 \le j \le n.$$

Then $A_0 = A$ is the required power product. We compute $A_n, A_{n-1}, \ldots, A_0 = A$ iteratively. Observe that

$$e_{i,j} = 2 * e_{i,j+1} + b_{i,j}, \quad 1 \le i \le k, 0 \le j < n.$$

Therefore,

$$A_j = A_{j+1}^2 \prod_{i=1}^{k} g_i^{b_{i,j}}, \quad 0 \le j < n.$$

For all $\mathbf{b} = (b_1, \ldots, b_k) \in \{0,1\}^k$, we determine

$$G_{\mathbf{b}} = \prod_{i=1}^{k} g_i^{b_i}.$$

Then

$$A_j = A_{j+1}^2 G_{(b_{1,j}, \ldots, b_{k,j})}, \quad 0 \le j < n.$$

We analyze this algorithm. The computation of the $G_{\mathbf{b}}$, $\mathbf{b} \in \{0,1\}^k$ requires $2^k - 2$ multiplications in G. The $G_{\mathbf{b}}$ can be precomputed and

used in any power product evaluation. The actual computation of A requires $n-1$ squarings and multiplications in G. Therefore, the following result is proved.

Theorem 2.13.1
Let $k \in \mathbb{N}$, $g_i \in G$, $e_i \in \mathbb{Z}_{\ge 0}$, $1 \le i \le k$, and let n be the maximal binary length of the e_i. Then the power product $\prod_{i=1}^{k} g_i^{e_i}$ can be computed using $2^k + n - 3$ multiplications and $n-1$ squarings in G.

For the case $k = 1$, the algorithm just described is an alternative method for fast exponentiation. Whereas in the method from Section 2.12 the binary expansion of the exponents is scanned from right to left, here we work from left to right.

2.14 Computation of Element Orders

In cryptographic protocols, group elements of large order are frequently used. In this section, we discuss the problem of finding the order of an element g of a finite group G or to check whether a given positive integer is the order of g.

The following theorem shows how to compute the order of g if the prime factorization

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

of the order of G is known. If this prime factorization is unknown, then it is not easy to find the order of g. However, in public-key cryptography, the group order and its factorization are frequently known.

Theorem 2.14.1
For a prime divisor p of $|G|$, let $f(p)$ be the greatest integer such that $g^{|G|/p^{f(p)}} = 1$. Then

$$\operatorname{order} g = \prod_{p||G|} p^{e(p)-f(p)}. \tag{2.5}$$

Proof. Exercise 2.23.22. □

Theorem 2.14.1 yields an algorithm that computes the order of an element $g \in G$.

Example 2.14.2
Let G be the multiplicative group of residues modulo 101. Its order is $100 = 2^2 * 5^2$. Hence,

$$e(2) = e(5) = 2.$$

We compute the order of $2 + 101\mathbb{Z}$. First, we compute the numbers $f(p)$ from Theorem 2.14.1. We obtain

$$2^{2*5^2} \equiv 2^{50} \equiv -1 \bmod 101.$$

Hence, $f(2) = 0$. Moreover,

$$2^{2^2*5} \equiv 2^{20} \equiv -6 \bmod 101.$$

Hence, $f(5) = 0$, so the order of $2 + 101\mathbb{Z}$ is 100. This means that $\mathbb{Z}/101\mathbb{Z}$ is cyclic and $2 + 101\mathbb{Z}$ is a generator of this group.

The algorithm for computing the order of g determines the numbers $f(p)$ for all prime divisors p of $|G|$. Then it determines the element order. The implementation details are left to the reader.

Next, we discuss the problem of testing whether a given number is the order of $g \in G$. This is necessary if we want to find a generator of a cyclic group. We need the following result, which is an immediate consequence of Theorem 2.14.1.

Corollary 2.14.3
Let $n \in \mathbb{N}$. If $g^n = 1$ and $g^{n/p} \neq 1$ for each prime divisor p of n, then n is the order of g.

We illustrate the verification algorithm in an example.

Example 2.14.4
We claim that 25 is the order of the residue class $5 + 101\mathbb{Z}$ in the multiplicative group of residues modulo 101. In fact, $5^{25} \equiv 1 \bmod 101$ and $5^5 \equiv -6 \bmod 101$. Hence, the assertion follows from Corollary 2.14.3.

2.15 The Chinese Remainder Theorem

Let $m_1, \ldots, m_n$ be positive integers that are pairwise co-prime. Let $a_1, \ldots, a_n$ be integers. We explain how to solve the following *simultaneous congruence*:

$$x \equiv a_1 \bmod m_1, \quad x \equiv a_2 \bmod m_2, \quad \ldots, \quad x \equiv a_n \bmod m_n. \tag{2.6}$$

Set

$$m = \prod_{i=1}^{n} m_i, \quad M_i = m/m_i, \quad 1 \leq i \leq n.$$

We will see that the solution of the congruence (2.6) is unique modulo m. Since the m_i are pairwise co-prime, we have

$$\gcd(m_i, M_i) = 1, \quad 1 \leq i \leq n.$$

We use the extended Euclidean algorithm to compute numbers $y_i \in \mathbb{Z}$, $1 \leq i \leq n$ with

$$y_i M_i \equiv 1 \bmod m_i, \quad 1 \leq i \leq n. \tag{2.7}$$

Then we set

$$x = \left(\sum_{i=1}^{n} a_i y_i M_i \right) \bmod m. \tag{2.8}$$

We show that x is a solution of the simultaneous congruence (2.6). From (2.7), we obtain

$$a_i y_i M_i \equiv a_i \bmod m_i, \quad 1 \leq i \leq n, \tag{2.9}$$

and because for $j \neq i$ the integer m_i is a divisor of M_j, we have

$$a_j y_j M_j \equiv 0 \bmod m_i, \quad 1 \leq i, j \leq n, i \neq j. \tag{2.10}$$

From (2.8), (2.9), and (2.10), we deduce

$$x \equiv a_i y_i M_i + \sum_{j=1, j\neq i}^{n} a_j y_j M_j \equiv a_i \bmod m_i, \quad 1 \leq i \leq n. \tag{2.11}$$

Hence, x solves the congruence (2.6).

Example 2.15.1
We solve the simultaneous congruence

$$x \equiv 2 \bmod 4, \quad x \equiv 1 \bmod 3, \quad x \equiv 0 \bmod 5.$$

We have $m_1 = 4$, $m_2 = 3$, $m_3 = 5$, $a_1 = 2$, $a_2 = 1$, $a_3 = 0$. Therefore, $m = 60$, $M_1 = 60/4 = 15$, $M_2 = 60/3 = 20$, $M_3 = 60/5 = 12$. We solve $y_1 M_1 \equiv 1 \bmod m_1$ (i.e., $-y_1 \equiv 1 \bmod 4$). A solution is $y_1 = -1$. We solve $y_2 M_2 \equiv 1 \bmod m_2$ (i.e., $-y_2 \equiv 1 \bmod 3$). A solution is $y_2 = -1$. Finally, we solve $y_3 M_3 \equiv 1 \bmod m_3$ (i.e., $2y_3 \equiv 1 \bmod 5$). A solution is $y_3 = 3$. Therefore, $x \equiv -2 * 15 - 20 \equiv 10 \bmod 60$ (i.e., $x = 10$ is a solution of the simultaneous congruence).

Observe that in the algorithm just described, the numbers y_i and M_i do not depend on the a_i. Therefore, if the integers y_i and M_i are precomputed, then (2.8) can be used to solve (2.6) for any selection of the a_i. An implementation can be found in Figure 2.2.

Now we formulate the *Chinese remainder theorem*.

Theorem 2.15.2
Let $m_1, \ldots, m_n$ be pairwise co-prime positive integers and let $a_1, \ldots, a_n$ be integers. Then the simultaneous congruence (2.6) has a solution x which is unique mod $m = \prod_{i=1}^{n} m_i$.

Proof. The existence has been proved in (2.11). Hence, we must prove the uniqueness. Let x and x' be two such solutions. Then $x \equiv x' \bmod m_i$, $1 \le i \le n$. Because the numbers m_i are pairwise co-prime, it follows that $x \equiv x' \bmod m$. □

The following theorem estimates the effort that is necessary to construct a solution of a simultaneous congruence.

Theorem 2.15.3
The algorithm for solving the simultaneous congruence (2.6) requires time $O((\text{size } m)^2)$ and space $O(\text{size } m)$.

Proof. By the results of Section 1.5, the computation of m requires time $O(\text{size } m \sum_{i=1}^{n} \text{size } m_i) = O((\text{size } m)^2)$. The computation of all M_i and y_i and of x takes the same time. This follows from the results of Section 1.5 and from Theorem 1.10.5. The upper bound for the space is easy to verify. □


```
crtPrecomp(int moduli[], int numberOfModuli, int modulus,
                         int multipliers[])
begin
  int i, m, M, inverse, gcd, y
  modulus = 1;
  for(i = 0; i < numberOfModuli; i=i+1)
    modulus = modulus*moduli[i]
  end for
  for(i = 0; i < numberOfModuli; i=i+1)
    m = moduli[i];
    M = modulus/m;
    xeuclid(M,m,gcd,inverse,y);
    multipliers[i] = inverse*M%modulus;
  end for
end

crt(int moduli[], int x[], int numberOfModuli, int result)
begin
  int multipliers[numberOfModuli]
  int result = 0
  int modulus, i
  crtPrecomp(moduli, numberOfModuli, modulus, multipliers)
  for(i = 0; i < numberOfModuli; i=i+1)
    result = (result + multipliers[i]*x[i])%modulus;
  end for
end
```

FIGURE 2.2 The Chinese remainder algorithm

2.16 Decomposition of the Residue Class Ring

We use the Chinese remainder theorem to decompose the residue class ring $\mathbb{Z}/m\mathbb{Z}$. Using this decomposition, we can reduce computations in a large residue class ring $\mathbb{Z}/m\mathbb{Z}$ to computations in many small residue class rings $\mathbb{Z}/m_i\mathbb{Z}$. Frequently, this is more efficient. This method can, for example, be used to speed up decryption in the RSA cryptosystem.

We define the *product of rings*.

Definition 2.16.1
Let $R_1, R_2, \ldots, R_n$ be rings. Their *direct product* $\prod_{i=1}^{n} R_i$ is the set of all tuples $(r_1, r_2, \ldots, r_n) \in R_1 \times \cdots \times R_n$ together with component-wise addition and multiplication.

It is easy to verify that $R = \prod_{i=1}^{n} R_i$ is a ring. If the R_i are commutative rings with unit elements e_i, $1 \le i \le n$, then R is a commutative ring with unit element $(e_1, \ldots, e_n)$.

The direct product of groups is defined analogously.

Example 2.16.2
Let $R_1 = \mathbb{Z}/2\mathbb{Z}$ and $R_2 = \mathbb{Z}/9\mathbb{Z}$. Then $R = R_1 \times R_2$ consists of all pairs $(a + 2\mathbb{Z}, b + 9\mathbb{Z})$, $0 \le a < 2$, $0 \le b < 9$. Hence, $R = R_1 \times R_2$ has exactly 18 elements. The unit element in R is $(1 + 2\mathbb{Z}, 1 + 9\mathbb{Z})$.

We also need the notion of a homomorphism and an isomorphism.

Definition 2.16.3
Let $(X, \bot_1, \ldots, \bot_n)$ and $(Y, \top_1, \ldots, \top_n)$ be sets with n operations. A map $f : X \to Y$ is called a *homomorphism* if $f(a \bot_i b) = f(a) \top_i f(b)$ gilt for all $a, b \in X$ and $1 \le i \le n$. If the map is bijective, it is called an *isomorphism*.

If we know an isomorphism between two rings which can be efficiently computed in both directions, then computational tasks in the one ring can be solved in the other ring. This may result in a more efficient algorithm.

Example 2.16.4
If m is a positive integer, then the map $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $a \mapsto a + m\mathbb{Z}$ is a ring homomorphism.

If G is a cyclic group of order n with generator g, then $\mathbb{Z}/n\mathbb{Z} \to G$, $e + n\mathbb{Z} \mapsto g^e$ is an isomorphism of groups (see Exercise 2.23.24).

Theorem 2.16.5
Let $m_1, \ldots, m_n$ be pairwise coprime integers and let $m = m_1 m_2 \cdots m_n$. Then the map

$$\mathbb{Z}/m\mathbb{Z} \to \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}, \quad a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z}) \quad (2.12)$$

is an isomorphism of rings.

Proof. First, we note that (2.12) is well defined. In fact, if $a \equiv b \bmod m$, then $a \equiv b \bmod m_i$ for $1 \le i \le n$. It is easy to verify that (2.12) is a homomorphism of rings. To prove surjectivity, let $(a_1 + m_1\mathbb{Z}, \ldots, a_n + m_n\mathbb{Z}) \in \prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$. Then Theorem 2.15.2 implies that this tuple has an inverse image under (2.12). The injectivity follows from the uniqueness in Theorem 2.15.2. □

Theorem 2.16.5 shows that computations in $\mathbb{Z}/m\mathbb{Z}$ can be reduced to computations in $\prod_{i=1}^{n} \mathbb{Z}/m_i\mathbb{Z}$. For a residue class mod m, the corresponding tuple of residue classes mod m_i is determined. The computation is carried out using those tuples, and the Chinese remainder theorem is used to compute the residue class mod m that corresponds to the result of the computation.

2.17 A Formula for the Euler φ-Function

We prove a formula for the Euler φ-function.

Theorem 2.17.1
Let $m_1, \ldots, m_n$ be pairwise co-prime positive integers and $m = \prod_{i=1}^{n} m_i$. Then $\varphi(m) = \varphi(m_1)\varphi(m_2) \cdots \varphi(m_n)$.

Proof. Theorem 2.16.5 implies that the map

$$(\mathbb{Z}/m\mathbb{Z})^* \to \prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z})^*, a + m\mathbb{Z} \mapsto (a + m_1\mathbb{Z}, \ldots, a + m_n\mathbb{Z}) \quad (2.13)$$

is an isomorphism of groups. In particular, this map is bijective. Therefore, the number $\varphi(m)$ of the elements of $(\mathbb{Z}/m\mathbb{Z})^*$ is equal to the number $\prod_{i=1}^{n} \varphi(m_i)$ of elements of $\prod_{i=1}^{n} (\mathbb{Z}/m_i\mathbb{Z})^*$. □

Theorem 2.17.2
Let m be a positive integer and $m = \prod_{p|m} p^{e(p)}$ its prime factorization. Then

$$\varphi(m) = \prod_{p|m} (p-1)p^{e(p)-1} = m \prod_{p|m} \frac{p-1}{p}.$$

Proof. By Theorem 2.17.1,

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

Hence, we only need to compute $\varphi(p^e)$ for a prime number p and a positive integer e. By Theorem 1.3.3, any $a \in \{0, 1, 2, \ldots, p^e - 1\}$ can be uniquely written as

$$a = a_e + a_{e-1}p + a_{e-2}p^2 + \ldots + a_1 p^{e-1}$$

with $a_i \in \{0, 1, \ldots, p-1\}$, $1 \leq i \leq e$. Moreover, $\gcd(a, p^e) = 1$ if and only if $a_e \neq 0$. This implies

$$\varphi(p^e) = (p-1)p^{e-1} = p^e\left(1 - \frac{1}{p}\right),$$

so the assertion is proved. □

Example 2.17.3
We have $\varphi(2^m) = 2^{m-1}$, $\varphi(100) = \varphi(2^2 * 5^2) = 2 * 4 * 5 = 40$.

If the factorization of m is known, then $\varphi(m)$ can be computed using Theorem 2.17.2 in time $O((\text{size}\, m)^2)$.

2.18 Polynomials

In Section 2.22, we want to prove that for any prime number p the multiplicative group of residues $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$. For this purpose, we need polynomials, which we introduce in this section. We also need polynomials to introduce finite fields.

Let R be a commutative ring with unit element $1 \neq 0$. A *polynomial* in one variable over R is an expression

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

where X is the variable and the *coefficients* $a_0, \ldots, a_n$ of the polynomial are elements of R. The set of all polynomials over R in the variable X is denoted by $R[X]$.

Let $a_n \neq 0$. Then n is called the *degree* of the polynomial. We write $n = \deg f$. Moreover, a_n is called the *leading coefficient* of f. If all coefficients except for the leading one are zero, then f is called a *monomial* .

Example 2.18.1
The polynomials $2X^3 + X + 1$, X, 1 are elements of $\mathbb{Z}[X]$. The first polynomial has degree 3, the second has degree 1, and the third has degree 0.

If $r \in R$, then

$$f(r) = a_n r^n + \cdots + a_0$$

is the *value* of f at r. If $f(r) = 0$, then r is called *zero* of f.

Example 2.18.2
The value of the polynomial $2X^3 + X + 1 \in \mathbb{Z}[X]$ at -1 is -2.

Example 2.18.3
Denote the elements of $\mathbb{Z}/2\mathbb{Z}$ by 0 and 1. Then $X^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[X]$. This polynomial has the zero 1.

Let

$$g(X) = b_m X^m + \cdots + b_0$$

be another polynomial over R and let $n \geq m$. If we set the missing coefficients to zero, we can write

$$g(X) = b_n X^n + \cdots + b_0.$$

The *sum* of the polynomials f and g is the polynomial

$$(f+g)(X) = (a_n + b_n)X^n + \cdots + (a_0 + b_0).$$

Example 2.18.4
If $g(X) = X^2 + X + 1 \in \mathbb{Z}[X]$ and $f(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Z}[X]$, then $(f+g)(X) = X^3 + 3X^2 + 2X + 3$.

The addition of f and g requires at most $O(\max\{\deg f, \deg g\} + 1)$ additions in R.

The *product* of the polynomials f and g is

$$(fg)(X) = c_{n+m}X^{n+m} + \cdots + c_0,$$

where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}, \quad 0 \le k \le n+m.$$

In this formula, the undefined coefficients a_i and b_i are set to 0.

Example 2.18.5
Let $f(X) = X^2 + X + 1 \in \mathbb{Z}[X]$ and $g(X) = X^3 + 2X^2 + X + 2 \in \mathbb{Z}[X]$. Then $(fg)(X) = (X^2+X+1)(X^3+2X^2+X+2) = X^5+(2+1)X^4+(1+2+1)X^3+(2+1+2)X^2+(2+1)X+2 = X^5+3X^4+4X^3+5X^2+3X+2$.

We estimate the number of operations necessary for the multiplication of f and g. We compute the products $a_i b_j$, $0 \le i \le \deg f$, $0 \le j \le \deg g$. There are $(\deg f + 1)(\deg g + 1)$ many of those products. The sum of all products $a_i b_j$ for which $i + j$ has the same value is the coefficient of X^{i+j}. Since every product appears in exactly one sum, those coefficients can be computed using at most $(\deg f + 1)(\deg g + 1)$ additions. In total, the multiplication of f and g requires at most $O((\deg f + 1)(\deg g + 1))$ additions and multiplications in R. Faster polynomial operations based on fast Fourier transformations are described in [3]. See also [37].

It is easy to see that $(R[X], +, \cdot)$ is a commutative ring with unit element 1.

2.19 Polynomials over Fields

Let K be a field. The following lemmas are easy to prove.

Lemma 2.19.1
The ring $K[X]$ of polynomials over K contains no zero divisors.

Lemma 2.19.2
If $f, g \in \mathbb{K}[x]$, $f, g \neq 0$, then $\deg(fg) = \deg f + \deg g$.

As in the ring of integers, in the polynomial ring also $K[x]$ division with remainder is possible.

Theorem 2.19.3
Let $f, g \in K[x]$, $g \neq 0$. Then there are uniquely determined polynomials $q, r \in K[x]$ with $f = qg + r$ and $r = 0$ or $\deg r < \deg g$.

Proof. If $f = 0$, then set $q = r = 0$. Assume that $f \neq 0$. If $\deg g > \deg f$, then set $q = 0$ and $r = f$. We assume that $\deg g \le \deg f$.

We prove the existence of q and r by induction on the degree of f.

If $\deg f = 0$, then $\deg g = 0$. Hence, $f, g \in K$ and we can set $q = f/g$ and $r = 0$.

Assume that $\deg f = n > 0$, $\deg g = m$, $n \ge m$, and

$$f(x) = a_n x^n + \cdots + a_0, \quad g(x) = b_m x^m + \cdots + b_0.$$

Set

$$f_1 = f - a_n/b_m x^{n-m} g.$$

Then either $f_1 = 0$ or $\deg f_1 < \deg f$. By the induction hypothesis, there are polynomials q_1 and r with $f_1 = q_1 g + r$ and $r = 0$ or $\deg r < \deg g$. This implies

$$f = (a_n/b_m x^{n-m} + q_1)g + r.$$

The polynomials $q = a_n/b_m x^{n-m} + q_1$ and r from earlier satisfy the assertion.

We prove uniqueness. Let $f = qg + r = q'g + r'$ be two representations as described in the theorem. Then $(q - q')g = r' - r$. If $r = r'$, then $q = q'$ because $g \neq 0$ and $K[x]$ contains no zero divisors. If $r \neq r'$, then $q - q' \neq 0$ and since $\deg g > \deg r$ and $\deg g > \deg r'$, Lemma 2.19.2 implies $\deg(q - q')g > \deg(r' - r)$. This is impossible because $(q - q')g = r' - r$. □

In the situation of Theorem 2.19.3, we call q the *quotient* and r the *remainder* of the division of f by g, and we write $r = f \bmod g$.

From the proof of Theorem 2.19.3, we obtain an algorithm for dividing a polynomial f by another polynomial g with remainder. First, we set $r = f$ and $q = 0$. While $r \neq 0$ and $\deg r \ge \deg g$, we set $h(x) = (a/b)x^{\deg r - \deg g}$, where a is the leading coefficient of r, and b is the leading coefficient of g. Then r is replaced by $r - hg$ and q by $q + h$. As soon as $r = 0$ or $\deg r < \deg g$, the algorithm returns the

quotient q and the remainder r. This is illustrated in the following example.

Example 2.19.4
Let $K = \mathbb{Z}/2\mathbb{Z}$ be the residue class ring mod 2. This ring is a field. The elements are represented by their least nonnegative representatives, so we write $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

Let

$$f(x) = x^3 + x + 1, \quad g(x) = x^2 + x.$$

We divide f with remainder by g. We first set $r = f$ and $q = 0$. Then we eliminate x^3 in r. We set $h(x) = x$ and replace r by $r - hg = x^3+x+1-x(x^2+x) = x^2+x+1$ and q by $q+h = x$. Then $\deg r = \deg g$. Hence, the algorithm requires another iteration. Again, we eliminate the leading coefficient in r. We set $h(x) = 1$, and we replace r by $r - hg = 1$ and q by $q + h = x + 1$. Now $0 = \deg r < \deg g = 2$, so we are finished and have found the quotient $q = x + 1$ and the remainder $r = 1$.

We estimate how many operations in K are necessary to divide f by g with remainder. The computation of the monomials h requires one operation in K. The number of monomials h is at most $\deg q + 1$ because their degree is strictly decreasing. Every time h is computed, $r - hg$ is also determined. The computation of hg requires $\deg g + 1$ multiplications in K. The degree of the polynomials r and hg is the same, and the number of nonzero coefficients in hg is at most $\deg g + 1$. Therefore, the computation of $r - hg$ requires at most $\deg g+1$ additions in K. In total, the division with remainder requires $O((\deg g + 1)(\deg q + 1))$ operations in K.

Theorem 2.19.5
If $f, g \in K[x]$ with $g \neq 0$, then the division with remainder of f by g requires $O((\deg g + 1)(\deg q + 1))$ operations in K, if the quotient q of the division is nonzero and $O(\deg g)$ operations in K otherwise.

Theorem 2.19.3 implies the following.

Corollary 2.19.6
If f is a nonzero polynomial in $K[x]$ and if a is a zero of f, then $f = (x-a)q$ with $q \in K[x]$ (i.e., f is divisible by the polynomial $x - a$).

Proof. By Theorem 2.19.3, there are polynomials $q, r \in K[x]$ with $f = (x - a)q + r$ and $r = 0$ or $\deg r < 1$. This implies $0 = f(a) = r$; hence $f = (x - a)q$. □

Example 2.19.7
The polynomial $x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ has the zero 1 and therefore $x^2 + 1 = (x - 1)^2$.

Corollary 2.19.8
A nonzero polynomial $f \in K[x]$ has at most $\deg f$ zeros.

Proof. We prove the assertion by induction on $n = \deg f$. For $n = 0$, the assertion holds because $f \in K$ and $f \neq 0$. Let $n > 0$. If f has no zeros, then the assertion is true. If f has a zero a, Corollary 2.19.6 implies $f = (x-a)q$ and $\deg q = n-1$. By the induction hypothesis, q has at most $n - 1$ zeros. Therefore, f has at most n zeros. □

In the following example, we show that the upper bound in Corollary 2.19.8 is not always sharp.

Example 2.19.9
The polynomial $x^2 + x \in (\mathbb{Z}/2\mathbb{Z})[x]$ has the zeros 0 and 1 in $\mathbb{Z}/2\mathbb{Z}$. By Corollary 2.19.8, it cannot have more zeros.

The polynomial $x^2 + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ has the only zero 1 in $\mathbb{Z}/2\mathbb{Z}$. By Corollary 2.19.8, it could have at most two zeros.

The polynomial $x^2 + x + 1 \in (\mathbb{Z}/2\mathbb{Z})[x]$ has no zeros in $\mathbb{Z}/2\mathbb{Z}$. By Corollary 2.19.8, it could also have at most two zeros.

2.20 Construction of Finite Fields

In this section we describe a method for constructing a finite field with p^n elements for any prime p and any positive integer n. Up to isomorphy, this field is uniquely determined. It is denoted by $\mathrm{GF}(p^n)$. The abbreviation GF stands for *Galois field*. We already know from Theorem 2.6.4 that $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements. It is denoted by $\mathrm{GF}(p)$. The prime number p is called the *characteristic* of the field $\mathrm{GF}(p^n)$. The field $\mathrm{GF}(p)$ is called a *prime field*. The construction of $\mathrm{GF}(p^n)$ for $n > 1$ is very similar to the construction of the field $\mathbb{Z}/p\mathbb{Z}$

for a prime number p. We only sketch the construction here. Details and proofs can be found, for example, in [4] and in [72].

Let p be a prime number, let n be a positive integer, and let f be a polynomial with coefficients in $\mathbb{Z}/p\mathbb{Z}$ of degree n. Assume that this polynomial is *irreducible*; that is, it cannot be written as a product $f = gh$, where g and h are polynomials in $(\mathbb{Z}/p\mathbb{Z})[X]$ of degree > 0. If a polynomial is not irreducible then it is called *reducible*.

Example 2.20.1
Let $p = 2$.

The polynomial $f(X) = X^2+X+1$ is irreducible in $(\mathbb{Z}/2\mathbb{Z})[X]$. We prove this statement. Assume that f is reducible. Then by Lemma 2.19.2 it can be written as the product of two polynomials of degree one in $(\mathbb{Z}/2\mathbb{Z})[X]$. So f has a zero in $\mathbb{Z}/2\mathbb{Z}$. But $f(0) \equiv f(1) \equiv 1 \bmod 2$. So f is in fact irreducible.

Since $X^2 + 1 \equiv (X + 1)^2 \bmod 2$, the polynomial $f(X) = X^2 + 1$ is reducible in $(\mathbb{Z}/2\mathbb{Z})[X]$

The elements of the finite field, which is constructed now, are residue classes mod f. The construction of those residue classes corresponds to the construction of residue classes in $\mathbb{Z}$. The residue class of a polynomial $g \in (\mathbb{Z}/p\mathbb{Z})[X]$ consists of all polynomials h in $(\mathbb{Z}/p\mathbb{Z})[X]$ such that $g - h$ is a multiple of f. For this residue class we write $g + f(\mathbb{Z}/p\mathbb{Z})[X]$. So we have

$$g + f(\mathbb{Z}/p\mathbb{Z})[X] = \{g + hf : h \in (\mathbb{Z}/p\mathbb{Z})[X]\}.$$

It follows from Theorem 2.19.3 that each residue class mod f contains a uniquely determined representative which is either zero or which is of degree $< \deg f$. This representative can be determined using division with remainder. Hence, in order to decide whether two residue classes are equal, those representatives are computed and compared. If they are equal, then the residue classes are equal. Otherwise, the residue classes are different.

Since the residue classes of all polynomials of degree $< n$ are different and since each residue class contains a representative of degree $< n$, the number of different residue classes mod f is p^n.

TABLE 2.2 Addition in GF(4).

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

TABLE 2.3 Multiplication in GF(4).

*	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

Example 2.20.2
The residue classes in $(\mathbb{Z}/2\mathbb{Z})[X]$ mod $f(X) = X^2+X+1$ are $f(\mathbb{Z}/2\mathbb{Z})$, $1 + f(\mathbb{Z}/2\mathbb{Z})$, $X + f(\mathbb{Z}/2\mathbb{Z})$, $X + 1 + f(\mathbb{Z}/2\mathbb{Z})$.

Let $g, h \in (\mathbb{Z}/p\mathbb{Z})[X]$. Then the sum of the residue classes of g and h mod f is defined as the residue class of $g + h$. The product of the residue classes of g and h is the residue class of the product of g and h. With this addition and multiplication, the set of residue classes mod f becomes a commutative ring with unit element $1 + f(\mathbb{Z}/p\mathbb{Z})[X]$.

Example 2.20.3
Let $p = 2$ and $f(X) = X^2 + X + 1$.

The residue classes mod f are the residue classes of the polynomials 0, 1, X and $X + 1$ mod f. In Table 2.2 and Table 2.3 we present the addition and multiplication tables of those residue classes. In those tables, we denote by α the residue class of $X + f(\mathbb{Z}/2\mathbb{Z})[X]$. Note that α is a zero of f in the residue class ring mod f, that is, $\alpha^2 + \alpha + 1 = 0$.

In Example 2.20.3 the residue class ring mod f is a field since nonzero residue classes mod f have a multiplicative inverse. We show that this is true for any irreducible polynomila f. Let $g \in (\mathbb{Z}/p\mathbb{Z})[X]$, then an analogue of the extended Euclidean algorithm is

used to determine a polynomial $r \in (\mathbb{Z}/p\mathbb{Z})[X]$ such that $gr + fs = 1$ for a polynomial $s \in (\mathbb{Z}/p\mathbb{Z})[X]$. Then the residue class of r is the inverse of the residue class of g. If f is reducible, then there are nonzero residue classes that have no inverse. In this case the residue class ring mod f is a commutative ring with zero divisors.

Example 2.20.4
Let $p = 2$ and let $f(X) = x^8 + x^4 + x^3 + x + 1$. This polynomial is reducible in $(\mathbb{Z}/2\mathbb{Z})[X]$ (see Exercise 2.23.26). Let α be the residue class of X mod f. We determine the inverse of $\alpha+1$. For this purpose, we use the extended Euclidean algorithm. We have

$$f(X) = (X + 1)q(X) + 1$$

with

$$q(X) = X^7 + X^6 + X^5 + X^4 + X^2 + X.$$

As in Example 1.9.2 we obtain the following table

k	0	1	2	3
r_k	f	$X+1$	1	0
q_k		$q(X)$	$X+1$	
x_k	1	0	1	$X^8 + X^4 + X^3$
y_k	0	1	$q(X)$	$X \cdot q(X)$

So we have

$$f(X) - q(X)(X + 1) = 1.$$

Therefore, the residue class $\alpha^7 + \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha$ of $q(X)$ is the inverse of $\alpha + 1$.

It can be shown that the fields that are obtained using the described construction with two different irreducible polynomials $f, g \in (\mathbb{Z}/p\mathbb{Z})[X]$ of degree n are isomorphic. Any such field is denoted by $\mathrm{GF}(p^n)$. Also, for any positive integer n there is an irreducible polynomial of degree n in $(\mathbb{Z}/p\mathbb{Z})[X]$. Therefore, the field $\mathrm{GF}(p^n)$ exists for all p and n.

2.21 The Structure of the Unit Group of Finite Fields

We now study the structure of the unit group of a finite field (i.e., of the multiplicative group of nonzero elements in a field with finitely many elements). We prove that this group is always cyclic. This it is particularly interesting for cryptography because in cryptography groups with elements of high order are used. We already know the finite field $\mathbb{Z}/p\mathbb{Z}$ for a prime number p. Its unit group is of order $p - 1$. Later, we will also construct other finite fields.

The unit group K^* of a field K with q elements has order $q - 1$ because all nonzero elements in K are units in K. We prove the following general result which implies that K^* is cyclic.

Theorem 2.21.1
Let K be a finite field with q elements. Then for any divisor d of $q - 1$ there are exactly $\varphi(d)$ elements of order d in the unit group K^*.

Proof. Let d be a divisor of $q - 1$. Denote by $\psi(d)$ the number of elements of order d in F.

Assuming that $\psi(d) > 0$, we prove that $\psi(d) = \varphi(d)$. Later, we will show that in fact $\psi(d) > 0$. Let a be an element of order d in K^*. The powers a^e, $0 \le e < d$, are pairwise distinct and are all zeros of the polynomial $x^d - 1$. By Corollary 2.19.8, there are at most d zeros of this polynomial in F. Hence, that polynomial has exactly d zeros and they are all powers of a. Now each element of F of order d is a zero of $x^d - 1$ and is therefore a power of a. By Theorem 2.9.5, a power a^e is of order d if and only if $\gcd(d, e) = 1$. Hence, we have shown that $\psi(d) > 0$ implies $\psi(d) = \varphi(d)$.

We will now show that $\psi(d) > 0$. Suppose $\psi(d) = 0$ for a divisor d of $q - 1$. Then

$$q - 1 = \sum_{d|q-1} \psi(d) < \sum_{d|q-1} \varphi(d).$$

This contradicts Theorem 2.8.4. □

Example 2.21.2
Consider the field $\mathbb{Z}/13\mathbb{Z}$. Its unit group is of order 12. In this group, there is one element of order 1, one element of order 2, two elements

of order 3, two elements of order 4, two elements of order 6, and four elements of order 12. In particular, this group is cyclic and has four generators.

If K is a finite field with q elements, then by Theorem 2.21.1 it contains exactly $\varphi(q-1)$ elements of order $q-1$. This implies the following.

Corollary 2.21.3
If K is a finite field with q elements, then its unit group K^* is cyclic of order $q-1$. It has exactly $\varphi(q-1)$ generators.

2.22 Structure of the Multiplicative Group of Residues Modulo a Prime Number

Let p be a prime number. Corollary 2.21.3 implies the following result.

Corollary 2.22.1
The multiplicative group of residues mod p is cyclic of order $p-1$.

An integer a for which the residue class $a+p\mathbb{Z}$ generates the multiplicative group of residues $(\mathbb{Z}/p\mathbb{Z})^*$ is called a *primitive root* mod p.

Example 2.22.2
For $p=13$, we have $p-1=12$. Theorem 2.17.2 implies that $\varphi(12)=4$. Therefore, there are four primitive roots mod 13, namely 2, 6, 7, and 11.

We describe how primitive roots modulo a prime number p can be computed. We have seen in Theorem 2.21.3 that there are $\varphi(p-1)$ primitive roots mod p. Now

$$\varphi(n) \geq n/(6 \ln \ln n)$$

for any positive integer $n \geq 5$ (see [61]). Hence, the number of generators of a cyclic group of order n is at least $\lceil n/(6 \ln \ln n) \rceil$. If $n = 2*q$ with a prime number q, then the number of generators is $q-1$. Hence, almost half of all group elements generate the group. If we randomly choose an integer g with $1 \leq g \leq p-1$, then we have a good chance that g is a primitive root mod p. We only need to check whether g is in fact a primitive root mod p. If we know the factorization of $p-1$, then Corollary 2.14.3 can be used efficiently to carry out this test. If $p-1=2q$ with a prime number q, then we only need to check whether $g^2 \equiv 1 \bmod p$ or $g^q \equiv 1 \bmod p$. If neither of these congruences is satisfied, then g is a primitive root mod p.

Example 2.22.3
Let $p=23$. Then $p-1=22=11*2$. To check whether an integer g is a primitive root modulo 23, we must verify that $g^2 \bmod 23 \neq 1$ and that $g^{11} \bmod 23 \neq 1$. Here is a table with the corresponding remainders for the prime numbers between 2 and 17.

g	2	3	5	7	11	13	17
$g^2 \bmod 23$	4	9	2	3	6	8	13
$g^{11} \bmod 23$	1	1	-1	-1	-1	1	-1

It follows that 5, 7, 11, and 17 are primitive roots mod 23 and that 2, 3, and 13 are not primitive roots mod 23.

2.23 Exercises

Exercise 2.23.1
Prove (2.2) and (2.3).

Exercise 2.23.2
Determine all semigroups that are obtained by defining an operation on $\{0,1\}$.

Exercise 2.23.3
Prove that in a semigroup there is at most one neutral element.

Exercise 2.23.4
Which of the semigroups of Exercise 2.23.2 are monoids? Which are groups?

Exercise 2.23.5
Prove that in a monoid each element can have at most one inverse.

Exercise 2.23.6
Let n be a positive divisor of the positive integer m. Prove that the map $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a + m\mathbb{Z} \mapsto a + n\mathbb{Z}$ is a surjective homomorphism of rings.

Exercise 2.23.7
Construct an example which shows that in the semigroup $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ cancellation is in general not possible.

Exercise 2.23.8
Determine the unit group and the zero divisors of the ring $\mathbb{Z}/16\mathbb{Z}$.

Exercise 2.23.9
Prove that the invertible elements of a commutative ring with unit element form a group.

Exercise 2.23.10
Solve $122x \equiv 1 \bmod 343$.

Exercise 2.23.11
Prove that the congruence $ax \equiv b \bmod m$ is solvable if and only if $\gcd(a, m)$ is a divisor of b. When solvable, determine all solutions.

Exercise 2.23.12
Let $d_1 d_2 \ldots d_k$ be the decimal expansion of a positive integer d. Prove that d is divisible by 11 if and only if $\sum_{i=1}^{k} (-1)^{k-i}$ is divisible by 11.

Exercise 2.23.13
Determine all invertible residue classes modulo 25, and compute their inverses.

Exercise 2.23.14
The least common multiple of two nonzero integers a, b is the least positive integer k that is a multiple of a and a multiple of b. It is denoted by $\operatorname{lcm}(a, b)$.

1. Prove the existence and uniqueness of $\operatorname{lcm}(a, b)$.
2. How can $\operatorname{lcm}(a, b)$ be computed using the Euclidean algorithm?

Exercise 2.23.15
Let X and Y be finite sets and $f : X \to Y$ a bijection. Prove that the number of elements in X and Y is equal.

Exercise 2.23.16
Compute the subgroup generated by $2 + 17\mathbb{Z}$ in $(\mathbb{Z}/17\mathbb{Z})^*$.

Exercise 2.23.17
Compute the order of 2 mod 1237.

Exercise 2.23.18
Determine the order of all elements in $(\mathbb{Z}/15\mathbb{Z})^*$.

Exercise 2.23.19
Compute $2^{20} \bmod 7$.

Exercise 2.23.20
Let G be a finite cyclic group. Prove that for every divisor d of $|G|$ there is exactly one subgroup G of order d.

Exercise 2.23.21
Let p be a prime number, $p \equiv 3 \bmod 4$. Let a be an integer which is a square mod p (i.e., the congruence $a \equiv b^2 \bmod p$ has a solution). Show that $a^{(p+1)/4}$ is a square root of a mod p.

Exercise 2.23.22
Prove Theorem 2.14.1.

Exercise 2.23.23
Construct an element of order 103 in the multiplicative group of residues mod 1237.

Exercise 2.23.24
Let G be a cyclic group of order n with generator g. Prove that $\mathbb{Z}/n\mathbb{Z} \to G$, $e + n\mathbb{Z} \mapsto g^e$ is an isomorphism of groups.

Exercise 2.23.25
Solve the simultaneous congruence $x \equiv 1 \bmod p$ for all $p \in \{2, 3, 5, 7\}$.

Exercise 2.23.26
Prove that the polynomial $f(X) = x^8 + x^4 + x^3 + x + 1$ is irreducible in $(\mathbb{Z}/2\mathbb{Z})[X]$.

Exercise 2.23.27
For $g = 2, 3, 5, 7, 11$ determine a prime number $p > g$ such that g is a primitive root mod p.

Exercise 2.23.28
Find all multiplicative groups of residues that have four elements.

3 CHAPTER Encryption

The traditional topic of cryptography is encryption. Encryption schemes are used to keep messages or stored data secret. In this chapter, we introduce fundamental notions that we need to describe encryption schemes. As a first example, we present affine linear ciphers and their cryptanalysis.

3.1 Encryption Schemes

We define encryption schemes.

Definition 3.1.1
An *encryption scheme* or *cryptosystem* is a tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ with the following properties:

1. $\mathcal{P}$ is a set. It is called the *plaintext space*. Its elements are called *plaintexts*.
2. $\mathcal{C}$ is a set. It is called the *ciphertext space*. Its elements are called *ciphertexts*.
3. $\mathcal{K}$ is a set. Is is called the *key space*. Its elements are called *keys*.