

## Chapter 2

# Mathematical Foundations of Cryptography

This chapter introduces some basic mathematical concepts necessary to understand the design of modern cryptographic algorithms and protocols. It begins with definitions of such algebraic structures as groups, rings, and finite fields, followed by some of their applications. This part also includes fundamental number theoretic definitions and properties playing an important role in cryptographic applications: the integer divisibility relation, the greatest common divisor, the least common multiple, the prime numbers, Euler's totient function, the congruence relation, and their basic properties.<sup>1</sup>

Throughout this book the set of natural numbers will be well ordered by the relation *less than*. This means that every subset of the natural numbers has the least element. Also it will be assumed throughout that zero is a natural number. Thus  $\mathbf{N}$  will denote the set of all natural numbers with zero. To denote the set of positive integers  $\mathbf{N}_+$  will be used.

### 2.1 Basic Concepts in the Theory of Algebraic Structures

Let  $S$  denote a nonempty set and let  $S \times S$  denote the Cartesian product of  $S$  with itself (the Cartesian square of  $S$ ), i.e., the set of all ordered pairs  $(x, y)$  such that  $x \in S$  and  $y \in S$ . Every mapping  $f: S \times S \rightarrow S$  of the Cartesian square of  $S$  into  $S$  is called an operation defined on the set  $S$ . The operation  $f$  is thus given by the function  $f(x, y) = z$ , where the element  $z \in S$  is called the result of  $f$  on the pair of elements  $x$  and  $y$ . In practice, operations are usually not denoted by letters but by operation symbols, e.g.  $+$ ,  $\star$ ,  $\cdot$ ,  $-$ ,  $\odot$ , etc. When using operation symbols, the result of an operation on elements  $x$  and  $y$  is denoted in the same way as when performing standard arithmetic operations on numbers:  $x + y$ ,  $x \star y$ ,  $x \cdot y$ , etc. It is important to note that according to the definition above not all operations on numbers are

---

<sup>1</sup>Further background on mathematical structures in cryptography can be found in [27, 92], and [68].

operations. For example, division is not an operation on the set of integers  $\mathbf{Z}$  (the result is not necessarily an integer) and subtraction is not an operation on the set of natural numbers  $\mathbf{N}$  (which does not contain negative integers). However, addition and multiplication are well-defined operations on those sets.

We will also use the notion of an algebraic structure which is defined as a set  $S$  together with operations defined on this set. Usually structures will contain either one operation, in which case they will be denoted by  $\langle S, + \rangle$ , or two operations when we will denote them by  $\langle S, +, \cdot \rangle$ .

### 2.1.1 Groups

**Definition 2.1** An algebraic structure  $\langle G, \bullet \rangle$  is called a *group* if the following conditions are satisfied:

1. The operation  $\bullet$  is associative, i.e.,

$$\forall_{a,b,c \in G} [a \bullet (b \bullet c) = (a \bullet b) \bullet c].$$

Thanks to associativity an expression  $x_1 \bullet x_2 \bullet \dots \bullet x_k$ , where  $x_i \in G$  and  $1 \leq i \leq k$ , always has the same value, irrespective of the order of operations performed on elements  $x_i$ .

2. There exists an identity element  $e \in G$  which is neutral with respect to the operation  $\bullet$ , i.e.

$$\exists_{e \in G} \forall_{a \in G} [a \bullet e = e \bullet a = a].$$

3. For every element  $a \in G$  there exists an element  $\tilde{a} \in G$  satisfying the following property:

$$\forall_{a \in G} \exists_{\tilde{a} \in G} [a \bullet \tilde{a} = \tilde{a} \bullet a = e].$$

If the operation in a group has the symbol  $+$ , then it is called addition and the group is called additive. In this case the element  $\tilde{a}$  is denoted by  $-a$  and called the inverse element of  $a$ . The identity element of an additive group is called the zero of the group and is denoted by 0. In a multiplicative group the operation is called multiplication and is denoted by a dot  $\cdot$ , which is often neglected in the notation, analogously as in the case of multiplying numbers. In this case the inverse element of  $a$  is denoted by  $a^{-1}$ . The identity element in a multiplicative group has the symbol 1 and is called the unit of the group.

4. Additionally, if the group operation is commutative, i.e.,

$$\forall_{a,b \in G} [a \bullet b = b \bullet a],$$

then the group is called commutative or Abelian (in honor of the Norwegian mathematician N.H. Abel).

Although a group is an algebraic structure consisting of a set and an operation, we will often write just the set symbol to denote the group.

On the basis of the axioms above, it is easy to prove that there exists only one identity element and that for every element of a group there exists a unique inverse element.

In order to simplify expressions in which an operation is performed many times on the same element from an additive (multiplicative) group  $a \in G$ , the following notation and rules will be used:

Additive group	Multiplicative group
$ma = \underbrace{a + a + \dots + a}_{m \text{ arguments}}$	$a^m = \underbrace{aaa \cdots a}_{m \text{ arguments}}$
$(-n)a = n(-a)$	$a^{-n} = (a^{-1})^n$
$na + ma = (n + m)a$	$a^n a^m = a^{n+m}$
$m(na) = (mn)a$	$(a^n)^m = a^{nm}$
$0a = 0$	$a^0 = 1$

where  $m, n, 0, 1 \in \mathbf{Z}$  and the symbols 0 and 1 denote identity elements for operations in additive and multiplicative groups, respectively. Thus, in a multiplicative group powers of elements exist. In an additive group multiples of elements are their analogs.

**Definition 2.2** Let  $G$  be a group consisting of a finite number of elements. We call  $G$  a *finite group* and the number of its elements the *order* of  $G$ . The order of a group  $G$  is denoted by  $|G|$  or  $\text{card } G$ .

**Definition 2.3** A multiplicative group  $G$  is called *cyclic* iff

$$\exists_{g \in G} \forall_{a \in G} \exists_{j \in \mathbf{N}} [a = g^j].$$

The element  $g$  is called a *generator* of the cyclic group, since each element of  $G$  can be represented as some power of  $g$ . We denote this fact by  $G = \langle g \rangle$ . It follows from this definition that every cyclic group is commutative ( $\forall_{x, y \in \mathbf{Z}} [g^x g^y = g^{x+y}]$ , and because  $x + y = y + x$ , we have  $g^{y+x} = g^y g^x = g^x g^y = g^{x+y}$ ) and  $g^{|G|} = 1$  (where 1 is the unit of the group).

**Definition 2.4** Let  $G$  be a finite multiplicative group. The *multiplicative order*  $s$  of an element  $a \in G$  is defined in the following way:

$$s = \min \{m \in \mathbf{N} : a^m = 1\}, \quad \text{where 1 is the unit of } G.$$

Such  $s$  divides the order of  $G$ , i.e.,  $s \mid \text{card } G$ . For instance, if  $\text{card } G = 63$ , then  $G$  contains elements of order 1, 3, 7, 9, 21 and 63.

**Definition 2.5** Let  $G$  be a group and let  $H$  be a subset of  $G$ . An algebraic structure  $\langle H, \bullet \rangle$ , consisting of a set  $H$  and an operation  $\bullet$  defined on  $G$ , is called a *subgroup* of

the group  $G$ , denoted by  $H \subset G$ , if it fulfills the axioms of a group (Definition 2.1). Alternatively, a subgroup may be defined as a structure that satisfies:

$$\forall_{a,b \in H} \begin{cases} a \bullet (-b) \in H & \text{for an additive group,} \\ a \bullet b^{-1} \in H & \text{for a multiplicative group.} \end{cases}$$

There are two trivial subgroups of  $G$ : an algebraic structure  $\langle e, \bullet \rangle$  and the group  $G$  itself. Therefore, if  $\text{card } H \notin \{1, \text{card } G\}$ , then a subgroup  $H$  of  $G$  is called *non-trivial*.

### 2.1.2 Rings and Fields

**Definition 2.6** An algebraic structure  $\langle R, +, \cdot \rangle$  is called a *ring* if the following axioms are satisfied:

1. the structure  $\langle R, + \rangle$  is an Abelian group;
2. the operation  $\cdot$  is associative, i.e.,  $\forall_{a,b,c \in R} [(a \cdot b) \cdot c = a \cdot (b \cdot c)]$ .
3. the operation  $\cdot$  is distributive over  $+$ , i.e.,

$$\forall_{a,b,c \in R} [(a \cdot (b + c) = a \cdot b + a \cdot c) \wedge ((b + c) \cdot a = b \cdot a + c \cdot a)].$$

Operations  $+$  and  $\cdot$  are usually called addition and multiplication, however, they are not necessarily these commonly understood number operations. A neutral element of a structure  $\langle R, + \rangle$  is denoted by 0 and the inverse element of an element  $a \in R$  by  $-a$ . For the sake of simplicity, we commonly use the following convention:  $a + (-b) = a - b$ ,  $a \cdot b = ab$ . On the basis of the definition of a ring, we get that  $\forall_{a \in R} [a0 = 0]$ , since  $a0 = a(b - b) = ab - ab = 0$ . Similarly, it can be proven that  $\forall_{a,b \in R} [(-a)b = a(-b) = -ab]$ .

Depending on the properties of multiplication, we can classify rings as follows:

1. If  $\exists_{e \in R} \forall_{a \in R} [ae = ea]$ , then a ring  $R$  is called a *ring with a unit*.
2. If multiplication in a ring is commutative, then such a ring is called *commutative*.
3. If a ring is commutative and additionally it contains a neutral element of multiplication  $e \neq 0$  and  $ab = 0 \Rightarrow (a = 0) \vee (b = 0)$ , then it is called an *integral domain* or an *integral ring*. A neutral element of multiplication is usually denoted by 1. It follows from the definition that an integral domain does not contain *zero divisors*.
4. Let  $R$  be an integral domain. We call it a *Euclidean ring* if there exists a function  $v : R \setminus \{0\} \rightarrow \mathbf{N} \cup \{0\}$ , called a *norm* of  $R$ , such that

$$\forall_{a,b \neq 0 \in R} \exists_{q,r \in R} [(a = bq + r) \wedge (v(r) < v(b) \vee r = 0)].$$

Here element  $r \in R$  is called a *remainder*, 0 is the zero of the ring  $R$ , and 0 is an integer.

**Table 2.1** Addition table for  $GF(16)$ 

+	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	1	0	3	2	5	4	7	6	9	8	b	a	d	c	f	e
2	2	3	0	1	6	7	4	5	a	b	8	9	e	f	c	d
3	3	2	1	0	7	6	5	4	b	a	9	8	f	e	d	c
4	4	5	6	7	0	1	2	3	c	d	e	f	8	9	a	b
5	5	4	7	6	1	0	3	2	d	c	f	e	9	8	b	a
6	6	7	4	5	2	3	0	1	e	f	c	d	a	b	8	9
7	7	6	5	4	3	2	1	0	f	e	d	c	b	a	9	8
8	8	9	a	b	c	d	e	f	0	1	2	3	4	5	6	7
9	9	8	b	a	d	c	f	e	1	0	3	2	5	4	7	6
a	a	b	8	9	e	f	c	d	2	3	0	1	6	7	4	5
b	b	a	9	8	f	e	d	c	3	2	1	0	7	6	5	4
c	c	d	e	f	8	9	a	b	4	5	6	7	0	1	2	3
d	d	c	f	e	9	8	b	a	5	4	7	6	1	0	3	2
e	e	f	c	d	a	b	8	9	6	7	4	5	2	3	0	1
f	f	e	d	c	b	a	9	8	7	6	5	4	3	2	1	0

5. If an algebraic structure  $\langle R \setminus \{0\}, \cdot \rangle$  is a group, then the ring  $R$  is called a *division ring*.
6. A commutative division ring is called a *field*.

Thus, a field can be defined in the following way:

**Definition 2.7** A structure  $\langle F, +, \cdot \rangle$  is called a *field* iff

1. the structure  $\langle F, + \rangle$  is a commutative group with a neutral element denoted by 0;
2. the structure  $\langle F \setminus \{0\}, \cdot \rangle$  is a commutative group with a neutral element denoted by 1;
3. multiplication is distributive over addition, i.e., the following condition is satisfied:

$$\forall_{a,b,c \in F} ([a(b+c) = ab+ac] \wedge [(b+c)a = ba+ca]).$$

The number of elements of a field is either infinite or equal to a power of some prime. A field with a finite number of elements is called a finite field or a Galois field and is denoted by  $GF(q)$ .

**Example 2.1** A Galois field  $GF(16)$  is a structure  $\langle F_{16}, +, \cdot \rangle$  consisting of a set  $F_{16} = \{0, 1, 2, \dots, 9, 10, a, b, \dots, f\}$  and operations of addition and multiplication defined as in Tables 2.1 and 2.2:

One can verify that this structure satisfies all axioms of a field.

**Definition 2.8** An algebraic structure  $\langle S, +, \cdot \rangle$ , where  $S \subset R$ , is called a *subring* of a ring  $\langle R, +, \cdot \rangle$  if it satisfies all axioms of a ring.

**Table 2.2** Multiplication table for  $GF(16)$ 

·	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
2	0	2	4	6	8	a	c	e	3	1	7	5	b	9	f	d
3	0	3	6	5	c	f	a	9	b	8	d	e	7	4	1	2
4	0	4	8	c	3	7	b	f	6	2	e	a	5	1	d	9
5	0	5	a	f	7	2	d	8	e	b	4	1	9	c	3	6
6	0	6	c	a	b	d	7	1	5	3	9	f	e	8	2	4
7	0	7	e	9	f	8	1	6	d	a	3	4	2	5	c	b
8	0	8	3	b	6	e	5	d	c	4	f	7	a	2	9	1
9	0	9	1	8	2	b	3	a	4	d	5	c	6	f	7	e
a	0	a	7	d	e	4	9	3	f	5	8	2	1	b	6	c
b	0	b	5	e	a	1	f	4	7	c	2	9	d	6	8	3
c	0	c	b	7	5	9	e	2	a	6	1	d	f	3	4	8
d	0	d	9	4	1	c	8	5	2	f	b	6	3	e	a	7
e	0	e	f	1	d	3	2	c	9	7	6	8	4	a	b	5
f	0	f	d	2	9	6	4	b	1	e	c	3	8	7	5	a

**Definition 2.9** An algebraic structure  $\langle I, +, \cdot \rangle$ , where  $I \subset R$ , is called an *ideal* of a ring  $\langle R, +, \cdot \rangle$  if this structure is a subring of  $R$  and  $\forall a \in I \forall r \in R [ar \in I \wedge ra \in I]$ .

**Definition 2.10** An ideal  $\langle I, +, \cdot \rangle$  is called *principal* if there exists an element  $a \in R$  such that  $I = (a)$ , where  $(a)$  stands for the set  $Ra$ . Then we say that  $a$  is a generator of an ideal  $(a)$ . If every ideal  $\langle I, +, \cdot \rangle$  of a ring  $\langle R, +, \cdot \rangle$  is principal, then the ring  $\langle R, +, \cdot \rangle$  is called a *principal ring*.

A structure  $\langle I, + \rangle$ , where  $I = \{0, a_1, a_2, \dots\}$ , is a subgroup of a group  $\langle R, + \rangle$ ; therefore a ring, similarly to a group, can be decomposed into cosets with respect to an ideal:

$$\begin{array}{ccccccc}
 0 & a_1 & a_2 & a_3 \dots, & a_m \dots, & & \\
 r_1 & r_1 + a_1 & r_1 + a_2 & r_1 + a_3 \dots, & r_1 + a_m \dots, & & \\
 r_2 & r_2 + a_1 & r_2 + a_2 & r_2 + a_3 \dots, & r_2 + a_m \dots, & & \\
 \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \dots,
 \end{array}$$

The first row of the table depicting the decomposition of the ring into cosets represents an ideal of the ring and the cosets are called *remainder classes*. Elements of the ring located in the first column of the table are representatives of remainder classes. Addition and multiplication of cosets are defined in the following way:

$$[r_i] \oplus [r_j] = [r_i + r_j], \quad [r_i] \odot [r_j] = [r_i r_j],$$

where  $[r_s]$  denotes the remainder class to which an element  $r_s$  of the ring belongs. Both operations are associative and multiplication of remainder classes is distribu-

**Table 2.3** Addition and multiplication tables for  $\mathbf{Z}/(4)$ 

Addition table for the ring $\langle \mathbf{Z}/(4), \oplus, \odot \rangle$					Multiplication table for the ring $\langle \mathbf{Z}/(4), \oplus, \odot \rangle$				
$\oplus$	[0]	[1]	[2]	[3]	$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[0]	[1]	[0]	[1]	[2]	[3]
[2]	[2]	[3]	[0]	[1]	[2]	[0]	[2]	[0]	[2]
[3]	[3]	[0]	[1]	[2]	[3]	[0]	[3]	[2]	[1]

tive over addition. In this way, from a ring  $\langle R, +, \cdot \rangle$  and its ideal  $\langle I, +, \cdot \rangle$ , we obtain a *remainder class ring*, denoted by  $R/I$ .

**Example 2.2** The set of integers  $\mathbf{Z}$  together with the arithmetical operations of addition and multiplication forms a ring. Let  $(4)$  denote the set of all multiples of 4:

$$(4) = [\dots, -20, -16, -12, -8, -4, 0, 4, 8, 16, \dots].$$

It is easy to prove that the structure  $\langle (4), +, \cdot \rangle$  is an ideal of the ring  $\langle \mathbf{Z}, +, \cdot \rangle$ . Thus, this ring can be decomposed into remainder classes with respect to the ideal  $(4)$ :

$$[0] = 0 + (4) \quad [1] = 1 + (4) \quad [2] = 2 + (4) \quad [3] = 3 + (4).$$

The structure  $\langle \mathbf{Z}/(4), \oplus, \odot \rangle$  is a ring with the following operation tables (Table 2.3):

In this ring  $[2] \odot [2] = [0]$ , thus the remainder class  $[2]$  is a zero divisor.

The ring  $\langle \mathbf{Z}/(n), \oplus, \odot \rangle$  exists for any positive integer  $n$  and is isomorphic to the ring  $\langle \mathbf{Z}_n, \oplus, \odot \rangle$ , i.e., the set  $[0, 1, \dots, n-1]$  in which addition and multiplication are performed modulo  $n$ .

**Theorem 2.1** A ring  $\langle \mathbf{Z}/(p), \oplus, \odot \rangle$  is a finite field if and only if  $p$  is a prime.

**Definition 2.11** Let  $p$  be a prime. Additionally, let

$$GF(p) = \langle F_p, \oplus, \odot \rangle, \quad F_p = [0, 1, \dots, p-1].$$

Then a finite field  $GF(p)$  is called a *Galois field* with  $p$  elements. Thus, we can write:  $GF(p) = \langle \mathbf{Z}_p, \oplus, \odot \rangle$ . Addition and multiplication in this field are performed modulo  $p$ .

**Definition 2.12** Let  $\langle R, +, \cdot \rangle$  be a ring. If

$$\exists_{n \in \mathbf{N}} \forall_{r \in R} [nr = 0],$$

then the least integer  $n$  fulfilling this condition is called the *characteristic* of  $R$ . If such an integer does not exist, the ring  $R$  has characteristic equal to 0.

**Table 2.4** Addition and multiplication tables for  $GF(2)$ 

Addition in $GF(2)$			Multiplication in $GF(2)$		
+	0	1	·	0	1
0	0	1	0	0	0
1	1	0	1	0	1

**Theorem 2.2** *The characteristic of a ring  $\langle R, +, \cdot \rangle$  with a unit, where  $|R| \neq 0$ , and with no zero divisors is equal to some prime  $p$ . Moreover, the following condition is satisfied in such a ring:*

$$\forall a, b \in R \forall n \in \mathbb{N} [(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}].$$

*Example 2.3* The characteristic of the Galois field from Example 1 is equal to 2, since  $\forall a \in GF(16) [a + a = 0]$ .

### 2.1.3 Finite Fields

We have already mentioned that a structure  $\langle F, +, \cdot \rangle$  is a finite field provided the cardinality of  $F$  is a power of some prime. As an example of a finite field we can give the algebraic structure  $\langle \{0, 1\}, +, \cdot \rangle$  in which operations of addition and multiplication are defined in Table 2.4.

This is the two-element field  $GF(2)$ . One can easily verify that the field axioms are satisfied: the structure  $\langle \{0, 1\}, + \rangle$  is a commutative group with 0 as a neutral element and the unit as its own inverse element. The structure  $\langle \{1\}, \cdot \rangle$  is a typical multiplicative group and multiplication is distributive over addition. As another example of a finite field one can give the structure  $\langle \{0, 1, 2, 3, 4, 5, 6\}, \oplus, \odot \rangle$  with operations of multiplication and addition modulo 7. We denote this field by  $GF(7)$ . One can check that the multiplicative group  $GF(7)$  has elements of order 1, 2, 3. Thus, there exist two- and three-element subgroups of the group  $\langle \{1, 2, \dots, 6\}, \odot \rangle$ .

By considering finite fields  $GF(q)$ , it can easily be seen that due to the closure property of addition, the sums  $\sum_{i=1}^k 1$ , where  $k = 1, 2, \dots$ , cannot be different for all  $k$ , since the result of the operation has to be an element of the field. Therefore, there exist two integers  $m, n$ , where  $m < n$  such that  $\sum_{i=1}^n 1 = \sum_{i=1}^m 1$ , which implies that  $\sum_{i=1}^{n-m} 1 = 0$ . This means that there exists the least prime  $p$  such that  $\sum_{i=1}^p 1 = 0$ . Such a prime is called the characteristic of the finite field.

**Theorem 2.3** *The characteristic  $p$  of a finite field is a prime.*

Now let  $a$  denote a nonzero element from  $GF(q)$ . Since the field  $GF(q)$  is closed under multiplication then consecutive powers of  $a$

$$a^1 = a, \quad a^2 = a \cdot a, \quad a^3 = a \cdot a \cdot a, \quad \dots$$



are elements of the field. As in the case of addition, subsequent powers of  $a$  cannot be all different, i.e.,

$$\exists_{m,k}[m > k \wedge a^k = a^m].$$

If we denote the multiplicative inverse element of  $a$  by  $a^{-1}$ , then the element  $(a^{-1})^k = a^{-k}$  is the multiplicative inverse element of  $a^k$ . Multiplying both sides of the equation  $a^k = a^m$  by  $a^{-k}$  we obtain  $1 = a^{m-k}$ . Hence, there exists a least positive integer  $n$  such that  $a^n = 1$ . As we already know, such  $n$  is the multiplicative order of  $a$ . Thus, the sequence of elements

$$a^1, a^2, a^3, \dots, a^n, a^{n+1} = a \dots$$

repeats after the element  $a^n$ , and powers  $a^1, a^2, a^3, \dots, a^{n-1}, a^n = 1$  are all pairwise different. Therefore, if  $i + j < n$ , then

$$a^i \cdot a^j = a^{i+j}.$$

On the other hand, if  $i + j > n$ , then  $i + j = n + r$ ,  $0 \leq r < n$ , and

$$a^i \cdot a^j = a^n \cdot a^r = a^r.$$

**Theorem 2.4** *Let  $a$  be a nonzero element of order  $n$  from the finite field  $GF(q)$ . Then  $n$  is a divisor of  $(q - 1)$ .*

### 2.1.4 Polynomial Ring

Let  $\langle R, +, \cdot \rangle$  be a ring. A *polynomial* over this ring is an expression of the form

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \dots + a_n x^n,$$

where  $n \in \mathbf{N}$ . The *coefficients* of a polynomial are elements from the ring, i.e.,  $a_i \in R$ ,  $0 \leq i \leq n$ , and the symbol  $x$  is called an *independent variable*. It is customary to omit a monomial  $a_i x^i$  in the notation of a polynomial whenever  $a_i = 0$ . Verifying the equality of two polynomials consists of checking whether they have the same coefficients standing at corresponding powers of their independent variables.

Let

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^m b_i x^i, \quad m \leq n.$$

If  $n = m$ , then the condition on the equivalence of two polynomials can be written as follows:

$$f(x) = g(x) \Leftrightarrow a_i = b_i, \quad 0 \leq i \leq n.$$

We define the sum and the product of two polynomials in the following way:

$$f(x) + g(x) = \sum_{i=0}^n (a_i + b_i)x^i,$$

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j, \quad 0 \leq i \leq n, \quad 0 \leq j \leq m.$$

**Definition 2.13** The set of all polynomials over a ring  $\langle R, +, \cdot \rangle$  together with operations of polynomial addition and multiplication is called a *polynomial ring* and we denote it by  $R[x]$ .

The zero polynomial, i.e., the polynomial with only zero coefficients, is the zero of  $R[x]$ . We denote it by 0, thus by the same symbol as the element of  $R$ . Therefore, when considering a ring  $R[x]$  one has to be careful not to confuse the zero of the polynomial ring with the zero of the ring from which coefficients of polynomials are taken.

**Definition 2.14** If

$$f(x) = \sum_{i=0}^n a_i x^i \in R[x], \quad a_n \neq 0,$$

then  $n$  is called the *degree* of the polynomial  $f(x)$ , which is denoted by  $\deg(f(x)) = n$ , whereas  $a_n$  is the *leading coefficient* of the polynomial. If a ring  $R$  has a neutral multiplication element, denoted by 1, and the leading coefficient of a polynomial is equal to 1, then such a polynomial is called *monic*. If  $\deg(f(x)) = 0$ , then the polynomial  $f(x)$  is called *constant*. The coefficient  $a_0$  is called a *free term*. Conventionally, we assume that the degree of the zero polynomial is equal to  $-\infty$ . Constant polynomials are in fact elements of a ring  $R$ , therefore  $R$  is a subring of the ring  $R[x]$  and the latter inherits some properties of the ring  $R$ .

Usually we consider polynomial rings over a field  $F$ , i.e., structures denoted by  $F[x]$ . Every polynomial ring is an integral domain, so if  $f(x), g(x) \in F[x]$ , then

$$\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x)))$$

and

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)).$$

**Definition 2.15** Similarly to the case of division in the ring  $\langle \mathbf{Z}, +, \cdot \rangle$ , we say that polynomial  $f(x)$  divides  $g(x)$  ( $f(x)$  is a divisor of  $g(x)$ ) if and only if there exists a polynomial  $h(x)$  such that  $g(x) = f(x) \cdot h(x)$ . We denote this property by  $f(x) \mid g(x)$ . In symbols:

$$f(x) \mid g(x) \Leftrightarrow \exists_{h(x) \in F[x]} (g(x) = f(x) \cdot h(x)).$$

**Theorem 2.5** *Let  $g(x) \neq 0$ ,  $g(x) \in F[x]$ . Then*

$$\forall f(x) \in F[x] \exists q(x), r(x) \in F[x] [f(x) = q(x)g(x) + r(x)],$$

$$\text{where } \deg(r(x)) < \deg(g(x)).$$

The above theorem describes an algorithm for division in a polynomial ring. One can thus compute the greatest common divisor of two polynomials  $f(x), g(x) \in F[x]$  by means of Euclid's algorithm,<sup>2</sup> repeating the algorithm for polynomial division in the following way:

$$\begin{array}{llll} f(x) & = q_1(x)g(x) & + r_1(x), & \deg(r_1(x)) < \deg(g(x)), \\ g(x) & = q_2(x)r_1(x) & + r_2(x), & \deg(r_2(x)) < \deg(r_1(x)), \\ r_1(x) & = q_3(x)r_2(x) & + r_3(x), & \deg(r_3(x)) < \deg(r_2(x)), \\ \vdots & \vdots & \vdots & \vdots \\ r_{k-1}(x) & = q_{k+1}(x)r_k(x) & + r_{k+1}(x), & \deg(r_{k+1}(x)) < \deg(r_k(x)), \\ r_k(x) & = q_{k+2}(x)r_{k+1}(x), & & \end{array}$$

until the remainder equals zero. If the leading coefficient of the polynomial  $r_{k+1}(x) \in R[x]$  is equal to  $c$ , then  $\gcd(f(x), g(x)) = c^{-1}r_{k+1}(x)$ , since it has to be monic. Of course, Euclidean algorithm can be applied to compute the greatest common divisor of three or more polynomials, for instance:  $\gcd(f_1(x), f_2(x), f_3(x)) = \gcd(\gcd(f_1(x), f_2(x)), f_3(x))$ .

**Theorem 2.6** *If  $\gcd(f(x), g(x)) = h(x)$ , then there exist polynomials  $u(x), v(x) \in R[x]$  such that*

$$u(x)f(x) + v(x)g(x) = h(x).$$

**Definition 2.16** A polynomial  $f(x) \in F[x]$  is called *irreducible* over a field  $F$  if  $\deg(f(x)) > 0$  and  $f(x) = a(x)b(x)$ ,  $a(x), b(x) \in F[x]$ , implies either  $a(x)$  or  $b(x)$  is constant, i.e.,  $(a(x) \in F) \vee (b(x) \in F)$ .

In other words, an irreducible polynomial over  $F$  is divided only by itself and constant polynomials. If neither  $a(x)$  nor  $b(x)$  is a constant polynomial, then the polynomial  $f(x)$  is reducible over  $F$ . Irreducible polynomials over  $F$  are crucial in constructing Galois fields.

**Theorem 2.7** *Every polynomial  $f(x) \in F[x]$ ,  $\deg(f(x)) > 0$ , can be presented in the following form:*

$$f = a \prod_{i=1}^k (g_i(x))^{e_i},$$

---

<sup>2</sup>The detailed presentation of the algorithm can be found in Chap. 3.

where  $a \in F$ ,  $e_1, \dots, e_k \in \mathbf{N}$  and  $g_1(x), \dots, g_k(x) \in F[x]$  are different monic polynomials. Such a decomposition is unique up to the order of the factors.

It can easily be checked that the set of all multiples of a polynomial  $f(x) \in F[x]$  is an ideal in the ring  $F[x]$ , which can be denoted by  $I = (f) = \{f(x)g(x) : g \in F[x]\}$ . We say that the polynomial  $f(x)$  generates the ideal  $(f)$ .

Decomposition of the polynomial ring  $F[x]$  into remainder classes with respect to an ideal generated by an irreducible polynomial plays an important role in applications of Galois fields.

**Theorem 2.8** *Let  $f(x) \in F[x]$ . The ring of remainder classes  $F[x]/(f)$  is a field if and only if  $f(x)$  is irreducible over  $F$ .*

**Definition 2.17** An element  $b \in F$  is called a *root* or a *zero* of a polynomial  $f(x) \in F[x]$  if  $f(b) = 0$ .

**Theorem 2.9** *An element  $b \in F$  is a root of a polynomial  $f(x) \in F[x]$  if and only if  $(x - b) \mid f(x)$ .*

**Theorem 2.10** *Let  $f(x) \in GF(q)[x]$  be a nonzero polynomial of degree  $m \geq 1$  and let  $f(0) \neq 0$ . Then there exists a positive integer  $s \leq q^m - 1$  such that  $f(x) \mid (x^s - 1)$ .*

**Definition 2.18** The least positive integer  $s$  satisfying the assumptions of the above theorem is called the *exponent* of the polynomial  $f(x)$ . If  $f(x) = 0$ , then  $f(x) = x^a g(x)$ ,  $a \in \mathbf{N}$ ,  $g(x) \in GF(q)[x]$ ,  $g(0) \neq 0$ . In such a case we regard the exponent of  $f(x)$  as the exponent of  $g(x)$ .

**Example 2.4** The polynomial ring over the field  $GF(3)$ , denoted by  $GF(3)[x]$ , consists of polynomials of all degrees with coefficients taken from the set  $\{0, 1, 2\}$ . Now, we decompose this ring into remainder classes with respect to the ideal generated by the polynomial  $f(x) = x^2 + x + 2$ . Thus, the ideal constitutes the following set of polynomials:

$$(f) = \{0, f(x), 2f(x), xf(x), (1+x)f(x), (2+x)f(x), 2xf(x), \dots\}$$

In this case we can create the following remainder classes:

$$\begin{aligned} \{0\} &= 0 + (f), \\ \{1\} &= 1 + (f), \\ \{\alpha\} &= x + (f), \\ \{\beta\} &= 1 + 2x + (f), \\ \{\gamma\} &= 2 + 2x + (f), \\ \{\delta\} &= 2 + (f), \\ \{\eta\} &= 2x + (f), \\ \{\kappa\} &= 2 + x + (f), \\ \{\zeta\} &= 1 + x + (f). \end{aligned}$$

**Table 2.5** Addition table for  $GF(9)$ 

+	{0}	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }
{0}	{0}	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }
{1}	{1}	{ $\delta$ }	{ $\zeta$ }	{ $\gamma$ }	{ $\eta$ }	{0}	{ $\beta$ }	{ $\alpha$ }	{ $\kappa$ }
{ $\alpha$ }	{ $\alpha$ }	{ $\zeta$ }	{ $\eta$ }	{1}	{ $\delta$ }	{ $\kappa$ }	{0}	{ $\gamma$ }	{ $\beta$ }
{ $\beta$ }	{ $\beta$ }	{ $\gamma$ }	{1}	{ $\kappa$ }	{ $\alpha$ }	{ $\eta$ }	{ $\zeta$ }	{0}	{ $\delta$ }
{ $\gamma$ }	{ $\gamma$ }	{ $\eta$ }	{ $\delta$ }	{ $\alpha$ }	{ $\zeta$ }	{ $\beta$ }	{ $\kappa$ }	{1}	{0}
{ $\delta$ }	{ $\delta$ }	{0}	{ $\kappa$ }	{ $\eta$ }	{ $\beta$ }	{1}	{ $\gamma$ }	{ $\zeta$ }	{ $\alpha$ }
{ $\eta$ }	{ $\eta$ }	{ $\beta$ }	{0}	{ $\zeta$ }	{ $\kappa$ }	{ $\gamma$ }	{ $\alpha$ }	{ $\delta$ }	{1}
{ $\kappa$ }	{ $\kappa$ }	{ $\alpha$ }	{ $\gamma$ }	{0}	{1}	{ $\zeta$ }	{ $\delta$ }	{ $\beta$ }	{ $\eta$ }
{ $\zeta$ }	{ $\zeta$ }	{ $\kappa$ }	{ $\beta$ }	{ $\delta$ }	{0}	{ $\alpha$ }	{1}	{ $\eta$ }	{ $\gamma$ }

**Table 2.6** Multiplication table for  $GF(9)$ 

·	{0}	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }
{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}	{0}
{1}	{0}	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }
{ $\alpha$ }	{0}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }	{1}
{ $\beta$ }	{0}	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }	{1}	{ $\alpha$ }
{ $\gamma$ }	{0}	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }	{1}	{ $\alpha$ }	{ $\beta$ }
{ $\delta$ }	{0}	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }
{ $\eta$ }	{0}	{ $\eta$ }	{ $\kappa$ }	{ $\zeta$ }	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }
{ $\kappa$ }	{0}	{ $\kappa$ }	{ $\zeta$ }	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }
{ $\zeta$ }	{0}	{ $\zeta$ }	{1}	{ $\alpha$ }	{ $\beta$ }	{ $\gamma$ }	{ $\delta$ }	{ $\eta$ }	{ $\kappa$ }

The polynomial  $f(x) = x^2 + x + 2$  is irreducible over  $GF(3)$  since  $f(0) \neq 0$ ,  $f(1) \neq 0$ ,  $f(2) \neq 0$ , thus the ring of remainder classes  $\langle F_9, +, \cdot \rangle$ , where

$$F_9 = \{ \{0\}, \{1\}, \{\alpha\}, \{\beta\}, \{\gamma\}, \{\delta\}, \{\eta\}, \{\kappa\}, \{\zeta\} \}$$

forms, according to Theorem 2.8, the field  $GF(9)$  with operations defined as in Tables 2.5 and 2.6.

### 2.1.5 Applications of Galois Fields

Galois fields are mostly used as a mathematical tool applied in cryptography (e.g., in algorithms such as AES, IDEA, ElGamal) and in the theory of erasure codes. The

latter constitutes the basis for designing devices used in many systems, for example in radar systems and systems of microwave links, mobile radio and satellite communications. Knowledge of Galois fields is essential when designing data recording systems with the use of magnetic tapes and disks and optical drives. Moreover, Galois fields are applied in designing self-checking arithmetic and logical circuits, high-speed semiconductor memories, digital television systems and Hi-Fi acoustic systems. Galois field arithmetic is applied in spread spectrum radio communication systems. Computation techniques in Galois fields are very useful in developing some types of radio and television antennas, and loudspeakers, and in cryptography and the synthesis of random number generators. Galois fields can also be applied in precise optical and acoustic measurements, in designing concert halls, and even in handicrafts and graphic design.

## 2.2 Elements of Number Theory

### 2.2.1 Divisibility

Let us consider two arbitrary natural numbers  $x$  and  $y$  ( $x, y \in \mathbf{N}$ ).

**Definition 2.19** We say that  $x$  divides  $y$  ( $x$  is a divisor of  $y$ ) if and only if there exists a natural number  $z$  such that  $y = x \cdot z$ . We denote this property by  $x \mid y$ . In symbols,

$$x \mid y \Leftrightarrow \exists_{z \in \mathbf{N}} (y = x \cdot z).$$

*Example 2.5* We have, of course,  $2 \mid 4$ ,  $3 \mid 27$ ,  $1233 \mid 44388$ , but the following relations do not hold:  $2 \nmid 5$ ,  $3 \nmid 26$  and  $123 \nmid 14287$ .

The following properties of divisibility are valid:

**Theorem 2.11** For all  $x, y, z \in \mathbf{N}$  we have

1.  $x \mid x$ ,
2.  $(x \mid y \wedge y \mid z) \Rightarrow x \mid z$ ,
3.  $(x \mid y \wedge y \mid x) \Rightarrow x = y$ ,
4.  $(x \mid y \wedge x \mid z) \Rightarrow (y \geq z \Rightarrow x \mid (y - z))$ ,
5.  $(x \mid y \wedge x \mid z) \Rightarrow \forall_{a, b \in \mathbf{N}} (x \mid (a \cdot y + b \cdot z))$ .

*Proof of 5* Let  $x, y, z \in \mathbf{N}$ . Additionally, let us assume that  $x \mid y \wedge x \mid z$ . It follows that for some natural numbers  $p, q$  we have  $y = p \cdot x$  and  $z = q \cdot x$ . Then

$$a \cdot y + b \cdot z = a \cdot p \cdot x + b \cdot q \cdot x = x \cdot (a \cdot p + b \cdot q),$$

so

$$x \mid (a \cdot y + b \cdot z).$$

Let us recall that if  $x, y \in \mathbf{N}$  and  $y > 1$ , then there exists exactly one pair of natural numbers  $p, r$  such that  $x = p \cdot y + r \wedge r < y$ .

This property is called the *unique factorization* of natural numbers (a similar law is valid for reals). The number  $p$  is simply the result of dividing  $y$  by  $x$ , while  $r$  is the remainder of this division.

Let us introduce the following notation:  $r = x \bmod y$  and  $p = x \operatorname{div} y$ .

We say that  $x$  is a common divisor of  $y$  and  $z$  when  $x \mid y$  and  $x \mid z$ .

The greatest common divisor of natural numbers  $y$  and  $z$  is defined as the natural number  $x$  such that

1.  $x \mid y \wedge x \mid z$ ,
2.  $(p \mid y \wedge p \mid z) \Rightarrow p \mid x$ .

Let us notice that the first condition states that  $x$  is a common divisor, while the second determines that  $x$  is the greatest one.

If  $x$  is the greatest common divisor of  $y$  and  $z$ , then we write  $x = \gcd(y, z)$ .

Natural numbers  $x$  and  $y$  are called coprime if  $\gcd(x, y) = 1$ . This means that they have no common divisors but 1.

It is easy to observe the following fact. □

**Theorem 2.12** *If we divide two natural numbers by their greatest common divisor, then the obtained numbers are coprime. In symbols,*

$$\gcd\left(\frac{x}{\gcd(x, y)}, \frac{y}{\gcd(x, y)}\right) = 1.$$

*Proof* Let  $z = \gcd(x, y)$ . Then there exist two integers  $p, q$  such that  $x = p \cdot z$  and  $y = q \cdot z$  (then, of course,  $p = \frac{x}{\gcd(x, y)}$  and  $q = \frac{y}{\gcd(x, y)}$ ).

Unless  $p$  and  $q$  are coprime, then they have a common divisor greater than 1. Let us denote it by  $d$ . Then the number  $z \cdot d$  is also a divisor of both  $x$  and  $y$ . Since  $d > 1$ , then it must be greater than  $z$ . We arrive at a contradiction.

We say that  $x$  is a common multiple of natural numbers  $y$  and  $z$  if  $y \mid x$  and  $z \mid x$ .

The least common multiple of two natural numbers  $y$  and  $z$  is defined as the natural number  $x$  such that

1.  $y \mid x \wedge z \mid x$ ,
2.  $(y \mid p \wedge z \mid p) \Rightarrow x \mid p$ .

We will denote the least common multiple of  $x$  and  $y$  by  $\operatorname{lcm}(x, y)$ .

The following interesting relation between the gcd and lcm of two natural numbers holds. □

**Theorem 2.13** *The product of two natural numbers  $x$  and  $y$  is equal to the product of the greatest common divisor and the least common multiple of these two numbers.*

In symbols,

$$x \cdot y = \gcd(x, y) \cdot \text{lcm}(x, y).$$

*Example 2.6* Let  $x = 957$  and  $y = 2117$ . Then  $\gcd(x, y) = \gcd(957, 2117) = 29$ , while  $\text{lcm}(x, y) = \text{lcm}(957, 2117) = 69861$ .

Let us notice that  $xy = 957 \cdot 2117 = 2025969$ .

Furthermore,  $\gcd(x, y) \cdot \text{lcm}(x, y) = \gcd(957, 2117) \cdot \text{lcm}(957, 2117) = 29 \cdot 69861 = 2025969$ .

**Corollary** If  $\gcd(x, y) = 1$ , then  $\text{lcm}(x, y) = xy$ .

### 2.2.2 Prime Numbers and Their Properties

**Definition 2.20** A natural number  $p > 1$  is called prime if it has exactly two divisors: 1 and  $p$  itself.<sup>3</sup>

The following theorems about prime numbers are valid.

**Theorem 2.14** Every integer greater than 1 has at least one prime divisor.

*Proof* Let us consider an integer  $x > 1$ . This number has divisors greater than 1 ( $x$  itself is one of these divisors). Let us denote by  $q$  the least of these divisors. We will prove that  $q$  is prime. Let us assume, on the contrary, that there exists  $p$  greater than 1 and smaller than  $q$  that divides the latter. Then  $1 < p < q$ ,  $p \mid q$  and as  $q \mid x$  we have that  $p$  is also a divisor of  $x$ . We get a contradiction with the assumption that  $q$  is the least divisor of  $x$ . Therefore,  $q$  is prime.  $\square$

**Theorem 2.15** Every natural number larger than 1 can be uniquely, up to the order of factors, factorized into the product of primes. In symbols, for a natural number  $n$  we have

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where the  $p_i$  (for  $i = 1, \dots, k$ ) are different primes.

*Proof (sketch)* Let us consider an integer  $x$  greater than 1. According to the previous theorem,  $x$  has at least one prime divisor. Let us denote it by  $q_1$ . Then we have  $x = q_1 \cdot p_1$  for some  $p_1$ . As previously,  $p_1$  has at least one prime divisor, which we denote by  $q_2$ . And so on. As a result we obtain a sequence of prime divisors of  $x$ . It is obvious that this sequence is finite and its last element is prime. Therefore,  $x$  can be represented as a product of primes.  $\square$

---

<sup>3</sup>A comprehensive and interesting study on primes can be found in [85].



**Theorem 2.16** If  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$  and  $m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$ , then

$$\gcd(n, m) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}$$

and

$$\text{lcm}(n, m) = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}.$$

It is easy to notice that natural numbers  $n$  and  $m$  are coprime if for all  $i$  ( $i = 1, \dots, k$ ) we have  $\min(\alpha_i, \beta_i) = 0$ . Then, of course,

$$\gcd(n, m) = p_1^0 \cdot p_2^0 \cdots p_k^0 = 1.$$

*Example 2.7* Let us factorize into primes  $x = 10976$  and  $y = 18772$ .

We have  $x = 10976 = 2^3 \cdot 7^1 \cdot 13^2$  and  $y = 18772 = 2^2 \cdot 13^1 \cdot 19^2$ .

$$p_1 = 2 \quad \alpha_1 = 3 \quad \beta_1 = 2$$

$$p_2 = 7 \quad \alpha_2 = 1 \quad \beta_2 = 0$$

$$p_3 = 13 \quad \alpha_3 = 2 \quad \beta_3 = 1$$

$$p_4 = 19 \quad \alpha_4 = 0 \quad \beta_4 = 2$$

$$\gcd(x, y) = \gcd(10976, 18772) = 2^2 \cdot 7^0 \cdot 13^1 \cdot 19^0 = 52,$$

$$\text{lcm}(x, y) = \text{lcm}(10976, 18772) = 2^3 \cdot 7^1 \cdot 13^2 \cdot 19^2 = 3963236.$$

**Theorem 2.17** There exist infinitely many prime numbers.

*Proof*

- Euclid (5th century BC).

Let us assume that there are finitely many prime numbers. Let  $p_1, p_2, \dots, p_k$  be all of them and let  $P$  denote their product increased by one:  $P = p_1 \cdot p_2 \cdots p_k + 1$ . As we have already shown, each natural number, including  $P$ , has at least one prime divisor. Let us denote a prime divisor of  $P$  by  $q$ . Now the question arises whether  $q$  is one of numbers  $p_1, p_2, \dots, p_k$ . If it were, then we would have  $q \mid p_1 \cdot p_2 \cdots p_k$  and  $q \mid P$ . Since  $P > p_1 \cdot p_2 \cdots p_k$ , thus  $q \mid (P - p_1 \cdot p_2 \cdots p_k)$ . However,  $P - p_1 \cdot p_2 \cdots p_k = 1$ , therefore  $q \mid 1$ , which is obviously impossible.

- Kummer (1878).

Let us suppose that there are finitely many primes. Let  $p_1, p_2, \dots, p_k$  be all of them and let  $P$  denote their product:  $P = p_1 \cdot p_2 \cdots p_k$ . Obviously,  $P > 2$ . Let us notice that  $P - 1$  can be represented as a product of primes. Of course, all factors of this product are taken from the set  $\{p_1, p_2, \dots, p_k\}$ . Therefore, there exists at least one prime  $p_i$  (for some  $i = 1, \dots, k$ ) that divides both  $P$  and  $P - 1$ . However, then we get  $p_i \mid P - 1$  and  $p_i \mid P$ , but since  $P > P - 1$ , we obtain  $p_i \mid (P - (P - 1))$ , thus  $p_i \mid 1$ , which is obviously impossible.

- Stieltjes (1890).

Let us assume that there are finitely many primes. Let  $p_1, p_2, \dots, p_k$  be all of them and let  $P$  denote their product:  $P = p_1 \cdot p_2 \cdots p_k$ . Now, let us represent  $P$  as a product of two natural numbers,  $m$  and  $n$ , greater than or equal 1 ( $m$  and  $n$  are products of some primes taken from the set  $\{p_1, p_2, \dots, p_k\}$ ). Thus, none of  $p_1, p_2, \dots, p_k$  divides both  $m$  and  $n$ . Then, if we consider the sum  $m + n$ , it turns out that it does not have a prime divisor. But since this sum is greater than 1, it has such a divisor. We obtain a contradiction.  $\square$

Below we present more theorems, which imply that there exist infinitely many primes.

**Theorem 2.18** *For every natural number  $n > 2$  there exists at least one prime greater than  $n$  and less than  $n!$ .*

*Proof* Let us observe that  $N = n! - 1$  is greater than 1 (since  $n > 2$ ). Therefore,  $N$  has a prime divisor, which we denote by  $p$ . Let us also notice that  $p$  cannot be less than or equal to  $n$ , as it divides  $n! - 1$ . Thus,  $p$  is greater than  $n$ . On the other hand, we know that  $p \leq N$ , so  $p < N - 1$ . Finally, we get  $n < p < n!$ .  $\square$

**Corollary** *It follows from the above theorem that there are infinitely many primes.*

**Theorem 2.19** (Chebyshev) *For every natural number  $n > 3$  there exists at least one prime greater than  $n$  and less than  $2n - 2$ .*

**Theorem 2.20** (Breusch) *For every natural number  $n > 7$  there exist at least four primes of the forms  $3k + 1, 3k + 2, 4k + 1, 4k + 3$  such that all of them are greater than  $n$  and smaller than  $2n$ .*

It is worth mentioning that despite many efforts no formula for prime numbers has been obtained. Moreover, nobody has proven that such a formula written by means of elementary functions does not exist at all; however, it is assumed that there is no such a formula.

In 1654 Fermat conjectured  $2^{2^n} + 1$  to be a formula for primes. However, in 1732 Euler showed that 641 divides  $2^{2^5} + 1$ . Landry, in 1880, proved that 274177 is another divisor of  $2^{2^5} + 1$ . Now it is also known that 319489 divides  $2^{2^{11}} + 1$  and 114689 divides  $2^{2^{12}} + 1$ . As an interesting fact let us mention that  $2^{2^{38}} + 1$  (which has tens billions of digits) was proven divisible by  $3 \cdot 2^{41} + 1$ . Furthermore, it was shown that numbers  $2^{2^n} + 1$  are composite for  $n = 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73$ .

Another interesting fact concerns the so-called Euler's polynomial  $f(x) = x^2 + x + 41$ , whose values are prime for all integer arguments taken from the interval  $(-40, 39)$ .<sup>4</sup>

---

<sup>4</sup>More information about this polynomial can be found in [85].

**Table 2.7** Values of Euler's function

$\Phi(n)$	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88

### 2.2.3 Euler's Function

Let  $\Phi : \mathbf{N} \rightarrow \mathbf{N}$  be a function which assigns to each natural number  $n$  the number of natural numbers not greater than  $n$  and coprime with it. The function  $\Phi$  is called Euler's function.

*Example 2.8* For  $n = 4$  there exist only two natural numbers not greater than and coprime with 4. These are 1 and 3, hence  $\Phi(4) = 2$ .

Similarly,  $\Phi(13) = 12$ ,  $\Phi(20) = 8$ ,  $\Phi(143) = 120$ .

Euler's function has the following properties.

**Theorem 2.21** *If  $p$  and  $q$  are primes, then*

1.  $\Phi(p) = p - 1$ ,
2.  $\Phi(p \cdot q) = (p - 1) \cdot (q - 1)$ ,
3.  $\Phi(p^a) = (p - 1) \cdot p^{a-1}$ .

**Theorem 2.22** *If  $a$  and  $b$  are coprime, then  $\Phi(ab) = \Phi(a) \cdot \Phi(b)$ . If  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , then  $\Phi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$ .*

Table 2.7 provides the values of Euler's function for natural numbers less than 90.

### 2.2.4 Modular Congruences

Let  $a, b$  and  $n$  be natural numbers ( $a, b, n \in \mathbf{N}, n \neq 0$ ).

If two integers,  $a$  and  $b$ , have the same remainder when divided by  $n$ , then they are said to be congruent modulo  $n$ . We denote this by  $a \equiv b \pmod{n}$ .

In symbols,

$$a \equiv b \pmod{n} \Leftrightarrow (a \bmod n) = (b \bmod n).$$

*Example 2.9*  $19 \equiv 7 \pmod{12}$ ,  $42 \equiv 8 \pmod{17}$ ,  $14 \equiv 18 \pmod{4}$ .

**Theorem 2.23** *The congruence relation is an equivalence relation.*

*Proof (sketch)* Let us notice that for all natural numbers  $a, b, c, n$  the congruence relation  $\equiv$  has the following properties:

1. reflexivity— $a \equiv a \pmod{n}$
2. symmetry— $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
3. transitivity— $[a \equiv b \pmod{n} \wedge b \equiv c \pmod{n}] \Rightarrow a \equiv c \pmod{n}$

Due to the properties of equivalence relations, each congruence relation (modulo  $n$ ) determines a partition of the set of natural numbers into disjoint equivalence classes. These classes are formed by natural numbers congruent modulo  $n$ .  $\square$

*Example 2.10* Let  $n = 4$ . Then the congruence relation partitions the set of natural numbers into four disjoint classes:

$$[0] = \{0, 4, 8, \dots\},$$

$$[1] = \{1, 5, 9, \dots\},$$

$$[2] = \{2, 6, 10, \dots\},$$

$$[3] = \{3, 7, 11, \dots\}.$$

**Definition 2.21** Let  $n$  be a fixed positive natural number.

Then the following implication holds:

$$(a = q \cdot n + r \wedge 0 \leq r < n) \Rightarrow a \equiv r \pmod{n}.$$

We call  $r$  the remainder of  $a$  modulo  $n$ .

**Corollary** *For any equivalence class of  $a$  there exists some  $a_0$  from the set  $\{1, 2, \dots, n-1\}$  such that  $a \equiv a_0 \pmod{n}$ . Such  $a_0$  is called the canonical representative of the equivalence class of  $a$  (the class  $[a]$ ).*

*The set  $Z_n = \{0, 1, 2, \dots, n-1\}$  is called the set of natural numbers modulo  $n$ .*

**Theorem 2.24** *Congruence relations satisfy the following implications:*

1.  $[a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}] \Rightarrow a \pm b \equiv c \pm d \pmod{n}$ ,
2.  $[a \equiv b \pmod{n} \wedge c \equiv d \pmod{n}] \Rightarrow ac \equiv bd \pmod{n}$ ,
3.  $[a \equiv b \pmod{n} \wedge r \mid n] \Rightarrow a \equiv b \pmod{r}$ ,
4.  $[a \equiv b \pmod{n} \wedge a \equiv b \pmod{m} \wedge \gcd(n, m) = 1] \Rightarrow a \equiv b \pmod{n \cdot m}$ .

Concerning computational complexity it should be mentioned that the time cost of addition and subtraction modulo  $n$  of  $k$ -bit integers equals  $O(k)$ , multiplication

and inversion (whenever possible) takes  $O(k^2)$ , while exponentiation costs  $O(k^3)$ .<sup>5</sup> These facts are crucial for the complexity of encryption algorithms presented in subsequent chapters.

### 2.2.5 Simple Modular Equations

Let  $d = \gcd(a, n)$ .

**Theorem 2.25** *The equation  $a \cdot x \equiv b \pmod{n}$  has a solution (or solutions) in  $Z_n$  if and only if  $d \mid b$ . Moreover, there exist exactly  $d$  solutions and all of them are congruent modulo  $\frac{n}{d}$ .*

*Example 2.11*  $3 \equiv 2 \pmod{5}$ .

We have

$$3 \cdot 0 \pmod{5} = 0,$$

$$3 \cdot 1 \pmod{5} = 3,$$

$$3 \cdot 2 \pmod{5} = 1,$$

$$3 \cdot 3 \pmod{5} = 4,$$

$$3 \cdot 4 \pmod{5} = 2.$$

Of course,  $d = \gcd(3, 5) = 1$  and  $1 \mid 2$  (due to the condition  $d \mid b$ ), hence in fact there is only one solution:  $x = 2$ .

*Example 2.12*  $3 \cdot x \equiv 5 \pmod{6}$ .

We get

$$3 \cdot 0 \pmod{6} = 0,$$

$$3 \cdot 1 \pmod{6} = 3,$$

$$3 \cdot 2 \pmod{6} = 0,$$

$$3 \cdot 3 \pmod{6} = 3,$$

$$3 \cdot 4 \pmod{6} = 0,$$

$$3 \cdot 5 \pmod{6} = 3.$$

Obviously,  $d = \gcd(3, 6) = 3$  and it is not true that  $3 \mid 5$ —hence there are no solutions.

---

<sup>5</sup>See Table 2.5 in [68].

*Example 2.13*  $3 \cdot x \equiv 3 \pmod{6}$ .

We get

$$3 \cdot 0 \pmod{6} = 0,$$

$$3 \cdot 1 \pmod{6} = 3,$$

$$3 \cdot 2 \pmod{6} = 0,$$

$$3 \cdot 3 \pmod{6} = 3,$$

$$3 \cdot 4 \pmod{6} = 0,$$

$$3 \cdot 5 \pmod{6} = 3.$$

Obviously,  $d = \gcd(3, 6) = 3$  and  $3 \mid 3$ —therefore there exist 3 solutions.

**Theorem 2.26** (Chinese Remainder Theorem) *If natural numbers  $n_1, n_2, \dots, n_k$  are pairwise coprime, i.e.,  $\gcd(n_i, n_j) = 1$  for any distinct  $i, j \in \{1, 2, \dots, k\}$ , then the system of equations*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \dots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

*has exactly one solution in  $\mathbb{Z}_n$ , where  $n = n_1 \cdot n_2 \cdot \dots \cdot n_k$ .*

*The system can be solved by applying the technique of the Gaussian elimination:*

$$x = \sum_{i=1}^k a_i \cdot N_i \cdot M_i \pmod{n},$$

where  $N_i = \frac{n}{n_i}$ , and  $M_i = N_i^{-1} \pmod{n}$ .

*Example 2.14* Let

$$x \equiv 3 \pmod{7}$$

$$x \equiv 7 \pmod{13}$$

We have

$$n_1 = 7, \quad n_2 = 13, \quad n = 7 \cdot 13 = 91$$

$$N_1 = 13, \quad N_2 = 7$$

$$M_1 = 13^{-1} \pmod{7} = 6^{-1} \pmod{7} = 6$$

$$M_2 = 7^{-1} \pmod{13} = 2$$

$$x = 3 \cdot 13 \cdot 6 + 7 \cdot 7 \cdot 2 \pmod{91} = 234 + 98 \pmod{91} = 332 \pmod{91} = 59.$$

**Corollary** (To the CRT) *If  $\gcd(n_1, n_2) = 1$  and*

$$x \equiv a \pmod{n_1},$$

$$x \equiv a \pmod{n_2},$$

*then  $x \equiv a \pmod{n_1 \cdot n_2}$  is the only solution to the above system of equations.*

### 2.2.6 Euler's Theorem

**Theorem 2.27** (Fermat's Little Theorem) *If  $p$  is a prime, then for all  $a \in \mathbb{Z}_p$  such that  $a \neq 0$  we have*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's little theorem can be generalized to the following one.

**Theorem 2.28** (Euler's Theorem) *For every positive integer  $n$  coprime with  $a$ , where  $a \in \mathbb{Z}_n$  and  $a \neq 0$ , the following modular equation holds*

$$a^{\Phi(n)} \equiv 1 \pmod{n},$$

*where  $\Phi(n)$  is Euler's function on  $n$ .*

## 2.3 Sieve of Eratosthenes, Euclidean Algorithms

Below we present some of most elementary algorithms in number theory applying notions used in cryptography, along with their applications. We start with the so-called sieve of Eratosthenes, which allows us to select primes from a given initial interval of natural numbers. Next, we describe a few versions of the Euclidean algorithm including the basic one that enables us to compute the greatest common divisor of two natural numbers and the extended version that computes inverse elements in rings  $\mathbb{Z}_n$ .<sup>6</sup>

### 2.3.1 Sieve of Eratosthenes

The question of whether there are methods to determine primes in the set of natural numbers was raised already by the ancients. According to current knowledge, the

---

<sup>6</sup>A very intelligible presentation of all these algorithms can be found in [87]. See also [68].

first algorithmic method solving this problem was developed in the second century BC by the ancient Greek mathematician Eratosthenes (276 BC–184 BC).

Its simple idea is to arrange natural numbers in an ascending sequence (or in an array) and eliminate composite numbers by crossing out multiples of, consecutively, two, three, five, and so on.

Let us look at an example that illustrates the search for primes in the set  $\{2, 3, \dots, 60\}$  by means of the sieve of Eratosthenes.

First, we arrange numbers in a sequence (or an array):

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60

The first number in this sequence is equal to 2 (we do not take 1 into consideration, as according to the definition it is not prime), hence 2 is prime. We cross out all multiples of 2 except itself, which gives the following sequence:

	2	3	<del>4</del>	5	<del>6</del>	7	8	9	<del>10</del>	11	<del>12</del>	13	<del>14</del>	15	<del>16</del>	17	<del>18</del>	19	<del>20</del>
21	<del>22</del>	23	<del>24</del>	25	<del>26</del>	27	<del>28</del>	29	<del>30</del>	31	<del>32</del>	33	<del>34</del>	35	<del>36</del>	37	<del>38</del>	39	<del>40</del>
41	<del>42</del>	43	<del>44</del>	45	<del>46</del>	47	<del>48</del>	49	<del>50</del>	51	<del>52</del>	53	<del>54</del>	55	<del>56</del>	57	<del>58</del>	59	<del>60</del>

The next prime turns out to be 3. We cross out its multiples, as well:

	2	3	<del>4</del>	5	<del>6</del>	7	8	9	<del>10</del>	11	<del>12</del>	13	<del>14</del>	<del>15</del>	<del>16</del>	17	<del>18</del>	19	<del>20</del>
<del>21</del>	<del>22</del>	23	<del>24</del>	25	<del>26</del>	<del>27</del>	<del>28</del>	29	<del>30</del>	31	<del>32</del>	<del>33</del>	<del>34</del>	<del>35</del>	<del>36</del>	37	<del>38</del>	<del>39</del>	<del>40</del>
41	<del>42</del>	43	<del>44</del>	<del>45</del>	<del>46</del>	47	<del>48</del>	49	<del>50</del>	<del>51</del>	<del>52</del>	53	<del>54</del>	<del>55</del>	<del>56</del>	<del>57</del>	<del>58</del>	59	<del>60</del>

Afterwards, we continue this procedure with 5 and 7, respectively:

	2	3	<del>4</del>	5	<del>6</del>	7	8	9	<del>10</del>	11	<del>12</del>	13	<del>14</del>	<del>15</del>	<del>16</del>	17	<del>18</del>	19	<del>20</del>
<del>21</del>	<del>22</del>	23	<del>24</del>	<del>25</del>	<del>26</del>	<del>27</del>	<del>28</del>	29	<del>30</del>	31	<del>32</del>	<del>33</del>	<del>34</del>	<del>35</del>	<del>36</del>	37	<del>38</del>	<del>39</del>	<del>40</del>
41	<del>42</del>	43	<del>44</del>	<del>45</del>	<del>46</del>	47	<del>48</del>	<del>49</del>	<del>50</del>	<del>51</del>	<del>52</del>	53	<del>54</del>	<del>55</del>	<del>56</del>	<del>57</del>	<del>58</del>	59	<del>60</del>

Let us observe that in order to find all prime numbers in the set  $\{1, 2, \dots, n\}$ , it is sufficient to apply the sieve algorithm only for primes not greater than  $\sqrt{n}$ . This follows from the fact that every composite number greater than  $\sqrt{n}$  has to have a prime factor which is less than  $\sqrt{n}$ . Therefore, it must have already been crossed out by the sieve. For this reason, in the case of the considered set  $\{2, 3, \dots, 60\}$  we can stop the selection procedure on arriving at 7.

We obtain the following primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59.

### 2.3.2 Euclidean Algorithm

The algorithm presented below is attributed to Euclid (c. 300 BC), who is thought to have been the first chief librarian of the ancient Library of Alexandria and who wrote the famous *Elements*—the first treatise on geometry. The algorithm computes



the greatest common divisor of two natural numbers. Its extended version allows us to determine the inverse of a given natural number in  $Z_n$ .

The first version of the algorithm, presented in *Elements*, concerned the purely geometric problem of determining whether two line segments are commensurable. Later, it was proven that this problem can be expressed in the language of number theory.

The easiest version of the Euclidean algorithm consists of repeatedly subtracting the smaller number from the greater one until zero is obtained. The last nonzero number achieved in this way is equal to the greatest common divisor of the two input numbers. A faster version applies a function that returns the remainder of the division of two natural numbers. There exist also recursive versions of the algorithm. Below we present them written in pseudocode.

**Algorithm 2.1** (Euclid (1))

Input:  $m, n$  (positive integers, for the sake of simplicity let  $m \leq n$ )

Output:  $\gcd(m, n)$

Auxiliary variables: natural numbers  $a, b, c$

```

1  a := n;
2  b := m;
3  if a=b then gcd(a,b) := a
4      else
5          repeat
6              begin
7                  repeat b := b - a until b < a;
8                  (a,b) := (b,a);
9              end
10         until b=0;
11 gcd(n,m) := a;
```

It is easy to notice that this algorithm can be rewritten in a simpler way using the mod function, which finds the remainder of division:

**Algorithm 2.2** (Euclid (2))

Input:  $m, n$  (positive integers, let  $m \leq n$ )

Output:  $\gcd(m, n)$

Auxiliary variables: natural numbers  $a, b, c$

```

1  a := n;
2  b := m;
3  if a=b then gcd(a,b) := a
4      else
5          repeat
6              begin
7                  b := (b mod a)
8                  (a,b) := (b,a);
```

```

9           end
10          until b=0;
11 gcd(a,b) :=a;

```

The algorithm can also be presented in a recursive version:

**Algorithm 2.3** (Euclid (3))

Input:  $m, n$  (positive integers, let  $m \leq n$ )

Output:  $\gcd(m, n)$

Auxiliary variables: natural numbers  $a, b$

```

1  a := n;
2  b := m;
3  if a=b then gcd(a,b) := a
4      else
5          if a<b then gcd(a,b) := gcd(a, b-a)
6              else
7                  gcd(a,b) := gcd(a-b, b);

```

In order to show the correctness of the Euclidean algorithm, we start by proving the following result.

**Theorem 2.29** *For all natural numbers  $a, b$ , where  $b \neq 0$ , the common divisors of  $a$  and  $b$  are the same as the common divisors of  $a$  and  $b \bmod a$ .*

*Proof* Let  $a, b$  be arbitrary numbers satisfying the assumptions of the theorem. Then, for some  $q$  and  $r$ ,

$$b = a \cdot q + r,$$

where

$$q = (b \operatorname{div} a),$$

$$r = (b \bmod a),$$

thus

$$b = a \cdot (b \operatorname{div} a) + (b \bmod a).$$

Let us assume that the above formula holds also for  $a = 1$ . We have

$$(b \operatorname{div} a) = (b \operatorname{div} 1) = b, \quad (b \bmod a) = (b \bmod 1) = 0.$$

Suppose that  $d$  is a divisor of both  $a$  and  $b$ . Then, for some  $x, y$ , we get

$$b = d \cdot x \quad \text{and} \quad a = d \cdot y.$$

We have

$$b = a \cdot q + r = d \cdot y \cdot q + r,$$

hence

$$d \cdot x = d \cdot y \cdot q + r, \quad r = d \cdot (x - y \cdot q),$$

therefore

$$(b \bmod a) = d \cdot (x - y \cdot q).$$

It follows that  $d$  is also a common divisor of  $a$  and  $b \bmod a$ .

The proof of the other direction is analogous.  $\square$

**Corollary** *If the set of divisors of positive integers  $a$  and  $b \bmod a$  is equal to the set of divisors of  $a$  and  $b$ , then the greatest common divisor of both pairs is the same:*

$$\gcd(a, b) = \gcd(a, b \bmod a).$$

Let us take a look at several examples:

*Example 2.15*  $\gcd(45, 12) = \gcd(45 \bmod 12, 12) = \gcd(9, 12) = \gcd(9, 12 \bmod 9) = \gcd(9, 3) = \gcd(9 \bmod 3, 3) = \gcd(0, 3) = 3$ .

*Example 2.16*  $\gcd(20, 63) = \gcd(63 \bmod 20, 20) = \gcd(3, 20) = \gcd(3, 20 \bmod 3) = \gcd(3, 2) = \gcd(3 \bmod 2, 2) = \gcd(1, 2) = \gcd(1, 2 \bmod 1) = \gcd(1, 1) = 1$ .

This shows that 63 and 20 are coprime (indeed, let us notice that  $63 = 3^2 \cdot 7$ , while  $20 = 2^2 \cdot 5$ ).

**Theorem 2.30** *The Euclidean algorithm is correct, i.e., it returns the greatest common divisor of two given positive integers.*

*Proof (for the second version of the algorithm)* In order to prove the theorem, we need to show two facts. Firstly, it is necessary to justify that the algorithm stops, secondly, that its output is correct.

Let us consider two natural numbers  $n, m$  such that  $n \leq m$ .

1. In the case when  $n = m$ , then  $\gcd(n, m) = n = m$ , and hence the algorithm returns the value  $\gcd(n, m)$  (3rd line of the algorithm (2)).
2. Let us assume that  $n < m$ . After executing each loop 6–9, values of the variable  $b$  form a strictly decreasing sequence of natural numbers. Obviously, each strictly decreasing sequence of natural numbers is finite and thus the last value of  $b$  is equal to 0. Therefore, the algorithm always stops.

As concerns the correctness of the result, let us observe that, due to the last theorem,  $\gcd(n, m)$  is constant before and after each loop 6–9. The initial value of  $\gcd(n, m)$  is thus equal to the value after the last execution of the loop, where  $b = 0$ ,

**Table 2.8** Consecutive values of variables  $a, b, q$  and  $-q \cdot b$ 

Loop number	$a$	$b$	$q$	$-q \cdot b$
1	135	40	3	-120
2	40	15	2	-30
3	15	10	1	-10
4	10	5	2	-10
5	5	0		

which gives  $\gcd(n, m) = \gcd(a, 0) = a$ . The last value of the variable  $a$  is the greatest common divisor of  $n$  and  $m$ .

From the viewpoint of the computational complexity, it should be noticed that the time complexity of the above algorithm applied to  $k$ -bit numbers equals  $O(k^2)$ .<sup>7</sup>  $\square$

### 2.3.3 Extended Euclidean Algorithm

Let us consider one more variant of the Euclidean algorithm which applies the function  $\text{div}$  instead of  $\text{mod}$ . This version allows us to present and justify the correctness of the so-called extended Euclidean algorithm.

**Algorithm 2.4** (Euclid (4))

Input:  $m, n$  (positive integers, let  $m \leq n$ )

Output:  $\gcd(m, n)$

Auxiliary variables: natural numbers  $a, b, c$

```

1  a := n;
2  b := m;
3  while b <> 0 do
4      begin
5          q := a div b;
6          (a, b) := (b, a - bq)
7      end;
8  gcd(m, n) := a
```

*Example 2.17* Let us follow the execution of the above algorithm for  $n = 135$  and  $m = 40$ .

Table 2.8 below provides values of variables  $a, b, q$  and  $-q \cdot b$  during the algorithm's execution for the numbers  $n, m$  set as above.

As can be seen in the presented example, the algorithm generates several sequences of natural numbers  $a_0, a_1, a_2, \dots, a_k, b_0, b_1, b_2, \dots, b_k, q_1, q_2, \dots, q_k$  and integers  $-q_1 \cdot b_1, -q_2 \cdot b_2, \dots, -q_k \cdot b_k$  (where  $a_0 = m$ , while  $b_0 = n$ ).

---

<sup>7</sup>See [68], Fact 2.105.

If  $a_{i-1}$  and  $b_{i-1}$  are values of variables  $a$  and  $b$  at the beginning of the loop 4–7, and  $a_i$  and  $b_i$  are values of these variables after the loop's execution, then, for  $i = 1, 2, \dots, k$ , the following properties hold:

1.  $a_i = b_{i-1}$ ,
2.  $q_i = a_{i-1} \operatorname{div} a_i$
3.  $a_{i+1} = b_i = a_{i-1} - q_i \cdot b_{i-1} = a_{i-1} - q_i \cdot a_i$ , hence
4.  $a_{i+1} = a_{i-1} - q_i \cdot a_i$

Let us also notice that  $a_k = \gcd(n, m)$ .

Now, we will construct two useful integer sequences  $(s_n)$  and  $(t_n)$ . Let

$$s_0 = 1, \quad t_0 = 0 \quad \text{and} \quad s_1 = 0, \quad t_1 = 1.$$

Let us observe that for such coefficients  $s_0, t_0, s_1, t_1$  the following relations hold:

$$m = a_0 = s_0 \cdot m + t_0 \cdot n \quad \text{and} \quad n = a_1 = s_1 \cdot m + t_1 \cdot n,$$

as well as  $a_{i-1} = s_{i-1} \cdot m + t_{i-1} \cdot n$  and  $a_i = s_i \cdot m + t_i \cdot n$ .

Now, let us apply formula 4. We get

$$\begin{aligned} a_{i+1} &= a_{i-1} - q_i \cdot a_i = (s_{i-1} \cdot m + t_{i-1} \cdot n) - q_i \cdot (s_i \cdot m + t_i \cdot n) \\ &= (s_{i-1} - q_i \cdot s_i) \cdot m + (t_{i-1} + t_i \cdot q_i) \cdot n \end{aligned}$$

If sequences  $(s_n)$  and  $(t_n)$  are defined as follows:

$$s_{n+1} = s_{n-1} - q_n \cdot s_n$$

$$t_{n+1} = t_{n-1} + q_n \cdot t_n,$$

then we can see that for all  $i = 0, 1, \dots, k-1$  the equation  $a_{i+1} = s_{i+1} \cdot m + t_{i+1} \cdot n$  is valid.

Therefore, this relation does not depend on the number of executions of the loop 4–7.

Now, let us recall that the last value of  $a$  determines  $\gcd(n, m)$ , which results in the following formula:

$$\gcd(n, m) = a_k = s_k \cdot m + t_k \cdot n.$$

We see that the greatest common divisor of two given numbers can be represented as their linear combination with integer coefficients. This observation turns out to be crucial for determining inverses in rings  $Z_n$ .

Finally, we describe the so-called extended Euclidean algorithm, which takes into account our considerations and which determines coefficients  $s$  and  $t$  mentioned above.

**Algorithm 2.5** (Extended Euclidean Algorithm)Input:  $m, n$  (positive integers, let us assume that  $m \leq n$ )Output:  $\gcd(m, n)$ Auxiliary variables: natural numbers  $a, a', q$ , integers  $s, s', t, t'$ 

```

1  a := m;
2  a' := n;
3  s := 1;
4  t := 0;
5  s' := 0;
6  t' := 1;

{We have:  $m = a = sm + tn$  and  $n = a' = s'm + t'n$ }

7  while a <> 0 do
8    begin
9      q := a div a';
10     (a, a') := (a', a - qa');
11     (s, s') := (s', s - qs');
12     (t, t') := (t', t - qt');
13   end
14   gcd(n, m) := a

```

The extended Euclidean algorithm returns the greatest common divisor of two given numbers, and, moreover, it determines the integer coefficients  $s$  and  $t$  of a linear combination such that  $\gcd(n, m) = s \cdot n + t \cdot m$ .

The proof is based on our discussion related to Example 2.17.

The above algorithm allows us, among other things, to find inverses in rings  $Z_n$ .

Let us recall that if for a given number  $z \in Z_n$  there exists  $y \in Z_n$  such that  $x \cdot y \equiv 1 \pmod{n}$ , then we call  $x$  and  $y$  mutually inverse. We adopt the following notation:  $y = x^{-1}$  and  $x = y^{-1}$ .

We say that  $z \in Z_n$  is invertible if and only if there exists its inverse.

We have the following result.

**Theorem 2.31** *A number  $z \in Z_n$  is invertible in  $Z_n$  if and only if  $\gcd(z, n) = 1$ . In particular, if  $p$  is prime, then every number from the set  $\{1, 2, \dots, p-1\}$  is invertible in  $Z_p$ .*

*Example 2.18* Let us consider the following problem. We want to compute the inverse, provided it exists, of 10 in the set  $Z_{37}$  (37 is a prime, so due to the above theorem 10 is invertible in  $Z_{37}$ ). Let us denote this inverse by  $x$ .

The following modular equation has to be satisfied:  $10 \cdot x = 1 \pmod{37}$ .

If we apply the extended Euclidean algorithm to 10 and 37, then we obtain  $\gcd(10, 37) = 1$ ,  $s = -11$  and  $t = 3$ . We have

$$1 = -11 \cdot 10 + 3 \cdot 37,$$

and since  $(-11 = 26) \bmod 37$ , we also get

$$1 = 26 \cdot 10 + 3 \cdot 37 \pmod{37},$$

therefore

$$1 = 26 \cdot 10 \pmod{37}.$$

Thus, 27 is the inverse of 10 in the set  $Z_{37}$ .

It follows from this example that a simple way to determine the inverse of  $x$  in  $Z_n$  is to apply the extended Euclidean algorithm for numbers  $x$  and  $n$ .

The time complexity of the described algorithm applied to  $k$ -bit numbers is also  $O(k^2)$ .<sup>8</sup>

## 2.4 Tests for Primality

This section presents two probabilistic, or randomized, algorithms for testing primality of natural numbers—Fermat’s test and the Miller-Rabin test,<sup>9</sup> both often used in practice today. This is followed by pointing out the theoretic role of one of the most important achievements in computer science of the last decade, namely the AKS deterministic test for primality. The section closes with a brief discussion of two computationally hard number theoretic problems—the integer factorization and the discrete logarithm problem. These issues play a fundamental role when it comes to the cryptographic strength of many of today’s security systems, considered in the following chapters.

### 2.4.1 Fermat’s Test

Let’s recall *Fermat’s little theorem*: If  $p$  is a prime integer, then for any  $a \in Z_p$  and  $a \neq 0$ ,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Unfortunately, the primes are not the only numbers that satisfy the above condition. There are also composite numbers, for which the above holds true.

A composite  $n$  that satisfies condition  $a^{n-1} \equiv 1 \pmod{n}$  for every  $a$  coprime to  $n$  is called a Carmichael number.

The smallest Carmichael number is 561 ( $3 \cdot 11 \cdot 17$ ).

---

<sup>8</sup>See [68], Fact 2.108.

<sup>9</sup>See Sect. 4.2. in [68].

A number  $w$  satisfying the condition

$$w^{n-1} \equiv 1 \pmod{n}$$

for the natural number  $n$  ( $w < n$ ) is called a witness to the primality of  $n$ . Of course, if  $n$  is prime, then all natural numbers less than  $n$  are witnesses to the primality of  $n$ .

It turns out that Fermat's little theorem provides a method for checking primality. The following assertion is true.

**Theorem 2.32** *Every number relatively prime to  $n$  is a witness to the primality of  $n$  or at most half of the numbers relatively prime to  $n$  are witnesses to the primality of  $n$ .*

*Proof* Consider a natural  $n$ . Let  $T$  denote the set of all integers relatively prime to  $n$ . Then for each  $w \in T$ , we have:  $\gcd(w, n) = 1$ . There are two cases: either all the elements of  $T$  are witnesses to the primality of  $n$ , that is, for each  $w \in T$ , we have:  $w^{n-1} \equiv 1 \pmod{n}$ , or a number exists in  $T$  which is not a witness to the primality of  $n$ . In the first case the conclusion is obvious.

Suppose that some  $w \in T$  is not a witness to the primality of  $n$ , i.e.,  $w^{n-1} \not\equiv 1 \pmod{n}$ . Then  $n$  is composite. Let  $T_n = \{w_1, w_2, \dots, w_t\}$  denote the set of those numbers from  $T$  ( $T_n \subseteq T$ ) which are witnesses to the primality of  $n$ . We have, for each  $k \in \{1, 2, \dots, t\}$ :  $w_k^{n-1} \equiv 1 \pmod{n}$ .

Let  $u_i = w \cdot w_i$ , for each  $i \in \{1, 2, \dots, t\}$ . Then any  $i, k \in \{1, 2, \dots, t\}$  satisfy the following relationships:

1.  $u_i \neq u_k$ , for  $i \neq k$ .

Because suppose that for some  $i \neq j$ , we have  $u_i = u_k$ . Then of course  $u_i - u_k = 0$ , therefore  $w \cdot w_i - w \cdot w_k = 0$ , and so  $n \mid (w \cdot w_i - w \cdot w_k)$  and finally  $n \mid w \cdot (w_i - w_k)$ . But  $\gcd(w, n) = 1$ . Therefore  $n \mid (w_i - w_k)$ . It is also true that  $-n < w_i - w_k < n$ . Hence  $w_i = w_k$ , which contradicts the assumption.

2.  $u_i^{n-1} = (w \cdot w_i)^{n-1} = w^{n-1} \cdot w_i^{n-1} = w^{n-1} \not\equiv 1 \pmod{n}$ .

A direct application of these properties is the fact that in the latter case, for  $t$  numbers which are witnesses to the primality of  $n$ , there exist as many numbers in  $T$  which are not witnesses to the primality of  $n$ .  $\square$

### 2.4.2 Fermat's Primality Test

The test consists of  $k$  independent trials carried out for a given number  $n$  being tested.

The parameter  $k$  is chosen by the user, in practice most often  $k$  is not less than 20 and not greater than 50.



We choose a random number  $w$  such that  $w < n$  and

1. we compute  $\gcd(w, n)$ ; if  $\gcd(w, n) > 1$ , then  $n$  is composite;
2. we compute  $w^{n-1} \pmod{n}$ ; if  $w^{n-1} \not\equiv 1 \pmod{n}$ , then  $n$  is composite.

We repeat the test several times. If in  $k$  trials we do not get that  $n$  is composite, the test concludes:  $n$  is prime.

As noted above, there exist composite numbers  $n$  satisfying the congruence  $w^{n-1} \equiv 1 \pmod{n}$ , for each  $w$ . The test may therefore mistakenly declare primality. The question arises, how often the test can be mistaken, and when, and whether the probability of a correct result can be determined.

Obviously, the test always gets it wrong, when we test the Carmichael numbers. The probability of a correct result of Fermat's test is provided as a corollary to the theorem proven above:

**Theorem 2.33** *If  $n$  is not prime and is not a Carmichael number, then, in a single trial a randomly selected number  $a$  ( $a < n$ ) is not a witness to the primality of  $n$  with probability of at least  $\frac{1}{2}$ .*

It follows that, if we repeat the test  $k$  times and we do not hit on a Carmichael number, the probability of a mistaken result is less than  $\frac{1}{2^k}$ . For  $k$  equal to 20, the result is already satisfactory for our purposes.

Carmichael numbers are believed to be very rare. Their distribution has been studied extensively for over 100 years with no definite answer, so far. Their rarity has been proved for the primes up to  $10^{21}$  (as of August 2012), see [80]. The currently interesting cryptographic prime parameters are much bigger, in the range of size between 160 and 4096 bits, (see [30, 82]). These are still very small from the perspective of asymptotic (i.e., for arbitrarily large  $n$ ) conjectures currently discussed in number theory research. The probability of randomly hitting a Carmichael number cannot be precisely estimated with present knowledge. It is often believed that they are sufficiently rare among small primes currently used in cryptography to make the risk due to the fallibility of the Fermat test fallibility small enough in practice. However, according to some researchers (e.g., [68]) this uncertainty makes Fermat's test excessively fallible.

It is interesting to note that Fermat's test is now utilized for testing primality of numbers used as keys in the PGP system (discussed thoroughly in the following chapters).

### 2.4.3 Miller-Rabin Test

This subsection presents the Miller-Rabin test, most often used in practice these days.

**Theorem 2.34** *Let  $n$  be an odd prime, and let  $n - 1 = 2^s \cdot r$  where  $r$  is odd. Let  $a$  be an integer coprime to  $n$ . Then either  $a^r \equiv 1 \pmod{n}$  or  $a^{2^j \cdot r} \equiv -1 \pmod{n}$  for some  $j$ ,  $0 \leq j \leq s - 1$ .*

As before, we will examine primality of a natural number  $n$ . Since there is only one even prime 2, the other primes are odd, we consider only an odd number  $n$ . Of course, the number  $n - 1$  is even, so there exist natural numbers  $r$  and  $s$  such that:

$$n - 1 = 2^s \cdot r \quad \text{where } r \text{ is odd.}$$

As in the previous test, we run  $k$  independent trials:

1. we choose a random number  $1 < a \leq n - 1$  and compute  $x = a^r \pmod{n}$ ;
2. we sequentially compute the powers of  $x$ :  $x^2, x^4, x^8, x^{16}, \dots$ , until
  - (a) the exponent value reaches  $2s$ , then we check if whether the last computed power is equal to  $1 \pmod{n}$ , and if not, then the number  $a$  is not a witness to the primality of  $n$ , therefore  $n$  is composite.
  - (b) any of the powers calculated is equal to  $1 \pmod{n}$ ; if it is 1, then we check whether every previous power is equal to  $-1 \pmod{n}$ , if not, the number  $a$  is not a witness to the primality of  $n$ , therefore  $n$  is composite.

The error probability of the Miller-Rabin test is characterized by the following statements.

**Theorem 2.35** *If  $n$  is prime, the test always gives the correct answer.*

**Theorem 2.36** *If  $n$  is composite, then the probability that the selected number is a witness to the primality and the test with a single trial declares prime is less than  $\frac{1}{4}$ .*

Thus a single positive Miller–Rabin test trial gives twice the confidence that the result is correct than does Fermat’s test. For  $k$  trials the confidence rises  $2^k$ -fold.

The seemingly more complicated Miller-Rabin test is in fact computationally no more time-consuming than the Fermat test. The time complexity of each of the two tests for  $k$ -bit input numbers is  $O(k^3)$ .<sup>10</sup>

### 2.4.4 Algorithm AKS

The tests presented above for primality are probabilistic. This means that the result is correct with a certain large probability but the probability is not equal to 1.

So far, no feasible deterministic algorithm has been developed for checking primality of numbers of size interesting in cryptographic practice these days. Until

---

<sup>10</sup>See Sect. 4.2 in [68].

2002 the only known deterministic algorithms testing primality were of exponential time complexity.

In August 2002, Manindra Agrawal and his two undergraduate students, Neeraj Kayal and Nitin Saxena of the Indian Institute of Technology in Kanpur, published the first polynomial-time algorithm for testing primality.<sup>11</sup> However practical usage of this algorithm for large numbers of current interest is still impossible. The degree of the polynomial is too high. Many research centers are working hard on optimizing this algorithm.

Algorithm AKS (for abbreviation, we omit the names of the coauthors) is based on a generalization of Fermat's little theorem for polynomials.

**Theorem 2.37** *A natural number  $n$  is prime iff*

$$(x - a)^n \equiv (x^n - a) \pmod{n}$$

*for all natural numbers  $a$  such that  $a < n$ .*

Here  $x - a$  and  $x^n - a$  are polynomials with coefficients in the ring  $Z_n$ .

Since the above condition is equivalent to the primality of  $n$ , the AKS test is deterministic. If  $n$  is prime, the algorithm will always return prime. Conversely, if  $n$  is composite, the algorithm will always return composite. There are no liars in this test, and no problem with their probability distribution, unlike in the case of the properties on which the Fermat and Miller-Rabin tests are based. It is much harder to give an intuitive argument for the polynomial run time estimate so we shall not dwell on it here. For a proof of this result and further discussion the interested reader is referred to [4] and [62]. [62] gives a slightly smaller than seventh degree polynomial run time complexity upper bound. It also argues that a fundamentally new idea would be required to obtain a deterministic primality testing algorithm with run time exponent smaller than 6. This leaves the AKS test infeasible for primes in the size range currently used in practical cryptography.

## 2.5 Computationally Hard Problems in Number Theory

Modern cryptography often employs so-called computationally hard mathematical problems. A computational problem is considered *hard* or *intractable* or *infeasible* if there is no known algorithm solving all the problem instances with a polynomial upper bound on the resources required, in particular polynomial time. Any cryptosystem whose security is based on an intractable problem is considered secure. That is, breaking the cryptosystem would imply the existence of a polynomial-resources (e.g., time) algorithm solving all problem instances, including instances with parameters especially carefully chosen. This section presents two of the most famous such problems: the integer factorization problem, justifying the cryptographic strength

---

<sup>11</sup>See [4].

of the RSA algorithm, and the discrete logarithm problem, employed in the Digital Signature Algorithm.

### 2.5.1 Factorization

The integer factorization problem is the problem of splitting any given composite positive integer  $n$  into (preferably prime) non-trivial factors. The multiplication of integers is instantly executed on any computer. But the inverse operation, i.e., factorization, is computationally hard. This subsection summarizes the current status of the integer factorization problem to the extent of its interest for cryptology.

In general running times of the factoring algorithms are functions of the size of  $n$  only. In some special cases, these times may depend also on some specific properties of  $n$ , e.g., on the size of the prime factors of  $n$ . It is advisable to try the algorithms for finding small prime factors first. The hardest case is when  $n$  is the product of two primes of roughly the same size.

In 1991, a global contest was started, the *RSA Factoring Challenge*,<sup>12</sup> organized by *RSA Security* in order to stimulate the scientific community to study efficient algorithms for factoring large integers. A list of numbers was published, which were known to be the products of two primes. These numbers are called *RSA numbers*.

A cash prize was offered for factorization of some of them. The first one, a 100-digit RSA-100 number was factored out within a few days, but most of them still remain unbroken. The contest lasted for sixteen years and was officially closed in May 2007. Some of the smaller prizes had been awarded at the time. The remaining prizes were retracted. Many numbers were factored during the challenge. Even today, these results still determine the bounds of feasible factorization.

Here are some of the challenge details. In August 1999, the cryptological community was electrified to learn that a 512-bit number (155 decimal digits) was factored out into prime factors.

```
10941738641570527421809707322040357612003732945449205990913842131
47634998428893478471799725789126733249762575289978183379707653724
4027146743531593354333897.
```

It turned out to be the product of the following two 78-decimal-digit primes:

```
10263959282974110577205419657399167590071656780803806680334193352
1790711307779
×
10660348838016845482092722036001287867920795857598929152227060823
7193062808643.
```

---

<sup>12</sup>Information about the project can be found at <http://www.rsa.com/rsalabs/node.asp?id=2092>.

Finding these factors took four months. Multiple computers were involved in the calculations.

In March 2002, nCipher Inc. announced that it had developed software that allowed it to break the 512-bit RSA key within six weeks, using tens of computers. A little later, the computing time was shortened to one day.

These are obviously very good results, but it should be noted and emphasized that increasing the number of bits by one doubles the search space.

In December 2003, factorization of the next RSA Challenge number was announced. This time it was RSA-576, a 576-bit (174-decimal-digit) integer. This number is:

```
18819881292060796383869723946165043980716356337941738270076335642
29888597152346654853190606065047430453173880113033967161996923212
05734031879550656996221305168759307650257059.
```

It is the product of the following primes:

```
39807508642406493739712550055038649119906436234252670840638518957
5946388957261768583317
×
47277214610743530253622307197304822463291469530209711645985217113
0520711256363590397527.
```

The team that managed to factorize RSA-576 received the \$10,000 prize, as promised by the RSA Challenge.

As of August 2012, the largest RSA Challenge cryptographically hard integer (i.e., one that was chosen specifically to resist all known factoring attacks, and is a product of two roughly equal primes) that has been factored is RSA-768, a 768-bit (232-decimal-digit) integer:

```
12301866845301177551304949583849627207728535695953347921973224521
51726400507263657518745202199786469389956474942774063845925192557
32630345373154826850791702612214291346167042921431160222124047927
4737794080665351419597459856902143413
=
33478071698956898786044169848212690817704794983713768568912431388
982883793878002287614711652531743087737814467999489
×
36746043666799590428244633799627952632279158164343087642676032283
815739666511279233373417143396810270092798736308917
```

This was the result of a large collaboration across the globe stretching over more than two years and using the general-purpose factoring algorithm called the general number field sieve. The overall effort required more than  $10^{20}$  operations, on the

**Table 2.9** RSA numbers

RSA Number	Digits	Bits	Awards	Decomposed	Solving team
RSA-100	100	330		April 1991	A.K. Lenstra
RSA-110	110	364		April 1992	A.K. Lenstra and M. Manasse
RSA-120	120	397		June 1993	T. Denny and others
RSA-129	129	426	US \$00	April 1994	A.K. Lenstra and others
RSA-130	130	430		April 10, 1996	A.K. Lenstra and others
RSA-140	140	463		February 2, 1999	H.J. te Riele and others
RSA-150	150	496		April 16, 2004	K. Aoki and others
RSA-155	155	512		August 22, 1999	H.J. te Riele and others
RSA-160	160	530		April 1, 2003	J. Franke and others
RSA-576	174	576	US \$10000	3 December 2003	J. Franke and others
RSA-640	193	640	US \$20000	2 November 2005	J. Franke and others
RSA-200	200	663		9 May 2005	J. Franke and others
RSA-704	212	704	US \$30000	prize withdrawn	
RSA-768	232	768	US \$50000	prize withdrawn	
RSA-896	270	896	US \$75000	prize withdrawn	
RSA-1024	309	1024	US \$100000	prize withdrawn	
RSA-1536	463	1536	US \$150000	prize withdrawn	
RSA-2048	617	2048	US \$200000	prize withdrawn	

order of  $2^{67}$  instructions. This is sufficiently low that even for short-term protection of data of little value, 768-bit RSA moduli can no longer be recommended [58].

More RSA numbers are waiting in the queue (Table 2.9). For a person who manages to decompose RSA-704, a US \$30000 award was offered, and for the longest presented number, the RSA-2048, a US \$200000. Table 2.9 shows more on the RSA Challenge.<sup>13</sup>

The longest number presented to the contest was the RSA-2048:

25195908475657893494027183240048398571429282126204032027777137836  
04366202070759555626401852588078440691829064124951508218929855914  
91761845028084891200728449926873928072877767359714183472702618963  
75014971824691165077613379859095700097330459748808428401797429100  
64245869181719511874612151517265463228221686998754918242243363725  
90851418654620435767984233871847744479207399342365848238242811981  
63815010674810451660377306056201619676256133844143603833904414952  
63443219011465754445417842402092461651572335077870774981712577246  
79629263863563732899121548314381678998850404453640235273819513786  
36564391212010397122822120720357.

<sup>13</sup>See also [88].

Comparing this number to RSA-576, one can easily forecast that even using modern technology the factorization will remain an open problem for a very long time. The best algorithms currently used for factorization of  $k$ -bit integers have the time complexity  $O(e^{k \cdot lg(k)})$ <sup>14</sup> (see [68]). The work on them, and on new algorithms, does not give much hope for easy and fast factorization of large numbers. A very nice survey of integer factorization methods and their complexities is given by [68], Chap. 3 and [75].

### 2.5.2 Discrete Logarithm Problem

Another computationally hard problem is the calculation of discrete logarithm. This section gives a brief account of its current status. This is similar to that of factorization, in a way, due to its computational hardness, uncertain future, and its role in modern cryptography.

Let's recall that the logarithm of a number  $a > 0$  to the base  $0 < b \neq 1$  is the number  $c$  such that  $b^c = a$ , i.e.,  $\log_b a = c \Leftrightarrow b^c = a$ . In other words, the search for the logarithm of a number is the search for a suitable exponent by which the base has to be raised to give that number. It is the inverse function to exponentiation.

Discrete logarithm is a direct analog in a finite group of the usual log in the field of reals. In general, in a finite multiplicative group  $G$  the discrete logarithm of  $a \in G$  to the base  $b \in G$  is defined to be  $c \in G$  such that  $b^c = a$  in  $G$ , provided that such a  $c$  exists. In cryptography, only logs in cyclic groups are considered and the base  $b$  is assumed to be a generator of  $G$ . The exponent can only be a positive integer, say  $n$ , and both  $a, b \neq 0$ . The logarithm is well defined for every  $a \in G$  (i.e., there exists such an exponent  $c$ ), under these assumptions. Most often,  $G$  is the multiplicative group of a finite field and the order of  $b$  in  $G$  is known. (This is the case of ElGamal and the Digital Signature Algorithm, for example.)

The discrete logarithm problem (DLP) is the following: given a prime  $p$ , a generator  $g$  of  $Z_p$ , and an element  $x \in Z_p^*$  find the integer  $y$ ,  $0 \leq y \leq p - 2$ , such that  $g^y = x \pmod{p}$ .

Let us recall that  $Z_p^*$  denotes the multiplicative group of  $Z_p$ , and for a prime  $p$ ,  $Z_p^* = \{a \mid 1 \leq a \leq p - 1\}$  with multiplication modulo  $p$ . In particular, if  $p$  is a prime, then  $Z_p$  has a generator; i.e., an element  $g \in Z_p$  such that for each  $y \in Z_p$  there is an integer  $i$  with  $y = g^i \pmod{p}$ . In other words, every finite field of size prime; has at least one generator (also called primitive element)  $g$ ; i.e., all nonzero elements of the field are expressible as powers of  $g$ .

It is easy and fast to calculate the powers in  $Z_n$ , even for large  $n$ . But computing the inverse function to exponentiation, or searching for the discrete logarithm, is computationally hard, similar to integer factorization. To date, nobody knows of a time-efficient algorithm for the discrete logarithm of large enough numbers.

---

<sup>14</sup>The  $lg$  function is the logarithm to base 2.

The most obvious algorithm for DLP is exhaustive search: successively compute  $g^0, g^1, g^2$  until  $y$  is obtained. It takes  $O(p)$  multiplications. This is exponential in the bit-length of  $p$ , and is therefore infeasible if  $n$  is large, i.e., in cases of current cryptographic interest.

In some important applications, in particular in the Digital Signature Algorithm (DSA), operations are performed in a field  $Z_p$  with a prime  $p$  which nowadays is recommended to be of at least 2048 bits. This prime  $p$  is selected so that  $p - 1$  is divisible by a much smaller prime  $q$  specified in the standard *FIPS 186-3* to be of 160-, 224-, or 256-bit length.

The currently best method known for computing discrete logs in finite fields  $Z_p$  is called the number field sieve, with a subexponential expected running time, roughly equal to  $\exp((\log(m))^{\frac{1}{3}})$ , where  $m$  is the order of the group. The currently best general algorithms for computing discrete logs (including probabilistic or parallelized ones) in cyclic groups run in (expected) exponential time  $O(m^{\frac{1}{2}})$ , and with low memory requirements.

The so-far largest discrete log case for a prime field  $Z_p$  (with  $p$  chosen with all the recommended precautions to resist the known simple attacks) that has been solved, up to August 2012, is for a 530-bit (160 decimal digit) prime  $p$ , [57]. The largest finite group discrete log problem with hard parameters that has been solved is that of discrete logs over an elliptic curve modulo a 112-bit prime, i.e., in a group of about  $2^{112}$  elements [21].

The Diffie-Hellman problem (DHP) is the following: given a prime  $p$ , a generator  $g$  of  $Z_p^*$  and elements  $g^a \bmod p$  and  $g^b \bmod p$ , compute  $g^{ab} \bmod p$ . From the complexity theory standpoint, DHP is at most as hard as DLP; i.e., it is polytime reducible to DLP. Whether these problems are computationally equivalent remains unknown.

The hardness of the discrete logarithm problem is the basis for the security justification of the Digital Signature Algorithm, presented in the next section, and for the Diffie-Hellman key exchange protocol. The discrete log problem in elliptic curve groups is not explicitly considered in this book. We mention in passing that, elliptic curve cryptosystems currently use much smaller key sizes than would be required by DSA and RSA with comparable security.

It appears that computing like discrete logs in prime fields or in elliptic curve groups is harder than factoring integers of the same size. However, one of the reasons for this impression might be that much less attention and effort has been given to discrete logs than to integer factorization, while many leading algorithms are similar.

More on the discrete logarithm problem can be found in Sect. 3.6 of [68] and a beautiful survey [74]. For recent advances see [75], and the references therein.



Modern Cryptography Primer

Theoretical Foundations and Practical Applications

Kościelny, C.; Kurkowski, M.; Srebrny, M.

2013, XIV, 238 p. 97 illus., Hardcover

ISBN: 978-3-642-41385-8