Discrete Mathematics

Prof. Dr. Tanja Lange
Coding Theory and Cryptology
Eindhoven University of Technology

March 2022

Contents

Chapter 1

Introduction

As the name "Discrete Mathematics" suggests this module deals with discrete objects like problems over the naturals or the integers as opposed to continuous structures like the reals.
We first consider problems in Combinatorics - questions about the number of different possibilities to choose k objects out of n. This is the basis to express simple probabilities like the chance to win at lotto. Simultaneously this chapter provides an introduction in mathematical logic and proof techniques. (12.5h)
The second part is concerned with concepts of number theory and algebra. Groups, fields and vector spaces are introduced and explained with examples. In number theory we deal with modular arithmetic and prime numbers. (15h)
The third part is about algorithms and running time analysis. (7.5h)
Finite fields play an important role in public key cryptography. The 4th part provides mathematical background, ways to construct finite fields and an introduction to efficient arithmetic in finite fields. (15h)
Elliptic curves are an interesting field of Algebraic Geometry which found applications in cryptography. The 5th part defines elliptic curves, the group law and shows how to compute efficiently on elliptic curves. Some theorems on the structure of elliptic curves over finite fields complete the introduction. (12.5h)
In all previous chapters we took for granted that primes are easy to find. This part provides insight on factorization of integers and shows how primality testing and proving work. (7.5h)
For each part references to the literature are given.

Acknowledgement

Thanks go to past teaching assistants and students for pointing out typos and errors, in particular Tibor Jager, Peter Birkner, Simon Hoerder, Jan-Jaap Oosterwijk, Marc Kleffmann, Christian Mrugalla, Melanie Alwardt, Dominik Leichtle, Florian Weber und Daniel Thewes. All remaining typos and errors are of course my responsibiliy. I would also like to thank Christof Paar and Jan Pelzl for providing the latex style file.

Chapter 2

Combinatorics and Proofs

For this year the first chapter is replaced by several chapters from E.A. Bender and S.G. Wiliamson "A Short Course in Discrete Mathematics". The book in general offers good background for the first half of this course and thus reading it is educational in any case. Most of what we need later on is covered in any first semester course on mathematics for engineers, so I hope the following is easy reading just to recall the notions. From the book, please read Sections 1 and 2 of Unit SF; Section 1 of Unit EO and Section 1 and Example 11 of Unit IS.

More precisely we will need the following concepts from the respective sections.

Unit SF:

- set, subset
- intersection, union, difference, complement
- product, Cartesian product
- algebraic rules for sets
- ordered sets
- binomial coefficient, binomial recursion, power sets
- function, domain, range, codomain, image
- relation, functional relation
- types of function: surjective (onto), injective (into), bijective

Unit EO:

- equivalence relation, equivalence class,

Unit IS:

- induction
- sum of first n integers
- geometric series

We will also use base-2 representations later on. This concept is covered in more generality in Unit BF in Section 2. We use a slightly different notation, namely

$$(1001010)_2 = 2^6 + 2^3 + 2^1,$$

i.e. with parentheses.

Exercise 2.0.1 *a) Let A, B, C be sets contained in the set U. Prove or disprove*

(a) $(A \cap B) \cup C = A \cap (B \cup C)$.
(b) $(A \cup B) \cap C = A \cup (B \cap C)$.
(c) If A is a subset of B and C is a subset of $U \setminus B$ then $A \cap C = \emptyset$.

b) Use the set notation to write the set of

(a) all even integers;
(b) all integers that are divisible by 5 and larger than 29;
(c) all negative integers that are squares of an integer;
(d) all 3rd powers in $\mathbb{R}$.

c) Write out all possible orderings of the elements a, b, c, d.

d) How many ways are there to order 10 elements. Give the result as an integer.

e) How many ways are there to select 3 elements out of 10 different elements if

(a) we distinguish the order of the selected elements.
(b) we do not distinguish the order of the selected elements.

f) How many ways are there to distribute 8 identical lollipops to 4 different children?

g) Consider the function $f(x) = x^{-3}$. State image and domain of f, where the domain should be a subset of $\mathbb{R}$

h) Give the maximal domain of g, where $g(x) = \sqrt{x^3 + x}$ and the domain and image are subsets of $\mathbb{R}$.

i) Define $f : \mathbb{N} \to \mathbb{N}$ by $f(x) = x^2 + x$. Is f injective? Is f surjective?

j) Give an example of a surjective function from $\{1, 2, 3, 4\}$ to $\{3, 4, 5\}$. Is it possible to define a bijection between these sets? If yes, give one; if no, show why.

k) Give an example of an injective function from $\{3,4,5\}$ *to* $\{1,3,5,7,9\}$*. Is it possible to define a bijection between these sets? If yes, give one; if no, show why.*

l) Find a bijection from $\{0,1,2,3,4,\dots\}$ *to* $\{\dots,-2,-1,0,1,2,\dots\}$*, i.e. from* $\mathbb{N}$ *to* $\mathbb{Z}$*.*

m) Prove: If $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$ *then* $a = c$ *and* $b = d$*.*

n) Show that $a \equiv b$ *if and only if* $a - b$ *is divisible by* 5 *is an equivalence relation on the integers. Write down the equivalence classes as sets.*

o) Compute $\sum_{k=0}^{15}(1/4)^k$*. Prove by induction that*

$$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$$

for any $n \in \mathbb{N}$ *and any real* $q \neq 1$*.*

p) Prove by induction that

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

for any $n \in \mathbb{N}$*.*

q) Prove by induction and using the binomial recursion that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

r) Write 974394 *in binary. Write* $(10010010)_2$ *as a decimal number.*

Chapter 3

Number Theory and Algebra

Most of the concepts of discrete mathematics belong to the areas of combinatorics, number theory and algebra. In Chapter 2 we studied the first area. Now we turn our attention to algebra and number theory and introduce the concepts in increasing level of complexity, starting with groups, rings and fields, providing the ring of polynomials as a long example and concluding with vector spaces. In the examples and applications of the theory we obtain almost all the necessary number-theoretic background as well.
The material of this chapter is very standard and can be found in any textbook on algebra or number theory. Some recommended references are:

- K. Ireland, M. Rosen "A Classical Introduction to Modern Number Theory", Springer.
- N. Jacobson, "Basic Algebra", W. H. Freeman.
- S. Lang, "Algebra", Springer.
- S. Lang, "Undergraduate Algebra", Springer.

3.1 Introduction to groups

In the previous chapter we introduced sets. Some of the most familiar sets like the integers or the reals come with more structure. We are used to adding or subtracting numbers to obtain their sum or difference respectively, which is again a number; we note that addition is inverse to subtraction. When we multiply or divide two non-zero reals we obtain another real; we note that multiplication is inverse to division. So there is some similarity between the ways of operating in a set. Algebra is about identifying such common structures and classifying them. One big advantage of this approach is that theorems that can be shown to hold, using only the definition of the abstract concept automatically apply to every concrete instantiation – let it be the integers with the operation addition, the reals with the operation multiplication or, as we will see, the rotations and reflections of an equilateral triangle with the operation of composition.

Definition 3.1.1 (Group)
A set G is a group *with respect to the operation $\circ$ if*

1. *G is closed under $\circ$: for all $a, b \in G$ one has $a \circ b \in G$.*
2. *Associativity: for all $a, b, c \in G$ one has $(a \circ b) \circ c = a \circ (b \circ c)$.*
3. *Neutral element: there exists an element $e \in G$ so that for all $a \in G$ one has $a \circ e = e \circ a = a$.*
4. *Inverse: for all $a \in G$ there exists an element $\mathrm{inv}(a) \in G$ with $a \circ \mathrm{inv}(a) = e$ and $\mathrm{inv}(a) \circ a = e$.*

We use $(G, \circ)$ as a shorthand to state that G is a group with respect to $\circ$.
A group G is called commutative *or* abelian *if for all $a, b \in G$ one has*

$$a \circ b = b \circ a.$$

Note that associativity allows any rearrangement of parentheses, e.g.

$$(a \circ b) \circ (c \circ d) = a \circ (b \circ (c \circ d)) = a \circ ((b \circ c) \circ d).$$

The neutral element of a group is unique; assume on the contrary that both e and e' satisfy $a \circ e = e \circ a = a$ and $a \circ e' = e' \circ a = a$ for any group element $a \in G$. Letting e' and then e play the role of a we obtain

$$e' = e \circ e' = e, \text{ i.e. } e = e'.$$

The inverse of an element is unique, i.e. if $\mathrm{inv}(a)$ and $\mathrm{inv}'(a)$ are both inverses of a, then $\mathrm{inv}(a) = e \circ \mathrm{inv}(a) = \mathrm{inv}'(a) \circ a) \circ \mathrm{inv}(a) = \mathrm{inv}'(a) \circ (a \circ \mathrm{inv}(a)) = \mathrm{inv}'(a) \circ e = \mathrm{inv}'(a)$.
The inverse of the neutral element is the neutral element itself since by definition of the inverse element $e \circ \mathrm{inv}(e) = e$ while the definition of the neutral element gives $e \circ \mathrm{inv}(e) = \mathrm{inv}(e)$, so $e = \mathrm{inv}(e)$.
Inversion changes the order of the elements $\mathrm{inv}(a \circ b) = \mathrm{inv}(b) \circ \mathrm{inv}(a)$; we show that by direct computation using associativity:

$$(a \circ b) \circ (\mathrm{inv}(b) \circ \mathrm{inv}(a)) = a \circ (b \circ \mathrm{inv}(b)) \circ \mathrm{inv}(a) = a \circ e \circ \mathrm{inv}(a) = a \circ \mathrm{inv}(a) = e.$$

Applying $\mathrm{inv}(\cdot)$ twice leads to the original element:

$$\mathrm{inv}(\mathrm{inv}(a)) = \mathrm{inv}(\mathrm{inv}(a))(\circ \mathrm{inv}(a) \circ a) = (\mathrm{inv}(\mathrm{inv}(a)) \circ \mathrm{inv}(a)) \circ a = e \circ a = a.$$

Example 3.1.2 *The integers $\mathbb{Z}$ form a group with respect to $+$:*

1. *If we add two integers $a, b \in \mathbb{Z}$ the result is again an integer, so the integers are closed under addition.*
2. *Associativity: We have $(a + b) + c = a + (b + c)$.*

3. *Neutral element: Adding* 0 *to an integer does not change its value and* $0 \in \mathbb{Z}$*, so* $0 \in \mathbb{Z}$ *is the neutral element.*

4. *Inverse element: The negative of an integer* $a \in \mathbb{Z}$ *is again an integer (by the very definition of the integers) and we have* $a + (-a) = 0$ *and thus* $\mathrm{inv}(a) = -a$*.*

5. *Since the order of summation does not matter,* $a+b = b+a$ *for all* $a, b \in \mathbb{Z}$*, we even have that* $\mathbb{Z}$ *is commutative.*

The natural numbers $\mathbb{N}$ do not form a group with respect to $+$ since there are no inverse elements. Consider $\mathbb{N}$ as subset of $\mathbb{Z}$; if $a \in \mathbb{N}\backslash\{0\}$, i.e. $a > 0$, then $-a < 0$ and thus not in $\mathbb{N}$ which means that that $\mathbb{N}$ does not fulfill the fourth condition. Sets which are closed under an operation which is associative are referred to as *semigroups*. A *monoid* is a semigroup with a neutral element, so the natural numbers form a monoid. Another example of a monoid is that the integers form a monoid with respect to multiplication since no element other than 1 has an inverse, but $\mathbb{Z}$ is closed under $\cdot$ and the operation is associative.

We now state some very common examples to show that groups are quite familiar objects. We use 'abelian group' and 'commutative group' interchangeably; this is common practice in mathematics.

Example 3.1.3 1. *The rationals* $\mathbb{Q}$ *form an abelian group with respect to* $+$*.*

2. *The reals* $\mathbb{R}$ *form an abelian group with respect to* $+$*.*

3. *The complex numbers* $\mathbb{C}$ *form an abelian group with respect to* $+$*.*

4. *The set obtained by removing 0 from* $\mathbb{Q}$ *is usually denoted by* $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$*. Similarly one defines* $\mathbb{R}^*$ *and* $\mathbb{C}^*$*.*

   We observe that the product of two rationals is again rational, that $1 \cdot a = a$*, that every fraction* $a/b \neq 0$ *can be inverted to* b/a *with* $(a/b) \cdot (b/a) = 1$*, and that* $(a/b) \cdot (c/d) = (c/d) \cdot (a/b)$*. So* $\mathbb{Q}^*$ *is a commutative group with respect to multiplication.*

5. $\mathbb{R}^*$ *is a commutative group with respect to multiplication.*

6. $\mathbb{C}^*$ *is a commutative group with respect to multiplication.*

We have not yet defined polynomials. Readers not familiar with this concept should skip this example but for the others it might be enlightening. We provide an extensive study of polynomials over a field in Section 3.7.

Example 3.1.4 *The set of polynomials* $\mathbb{C}[x]$ *in one variable* x *over the complex numbers* $\mathbb{C}$ *is a commutative group with respect to coefficientwise addition.*

1. *The set is closed under the operation $+$:*

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

where the undefined coefficients a_i for $i > n$ and b_i for $i > m$ are put to zero. The result is again a polynomial and the coefficients are in $\mathbb{C}$, since $\mathbb{C}$ forms a group with respect to the same addition $+$.

2. *Associativity is inherited from $(\mathbb{C}, +)$ as*

$$\begin{aligned}\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i\right) + \sum_{i=0}^{l} c_i x^i &= \sum_{i=0}^{\max\{m,n,l\}} ((a_i + b_i) + c_i)\, x^i \\ = \sum_{i=0}^{\max\{m,n,l\}} (a_i + (b_i + c_i))\, x^i &= \sum_{i=0}^{n} a_i x^i + \left(\sum_{i=0}^{m} b_i x^i + \sum_{i=0}^{l} c_i x^i\right),\end{aligned}$$

where the missing coefficients are put to zero.

3. *Neutral element:*

$$e = \sum_{i=0}^{0} 0 x^i = 0 \in \mathbb{C}[x].$$

4. *Inverse element: The inverse of $\sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x]$ is given by $\sum_{i=0}^{n} (-a_i) x^i \in \mathbb{C}[x]$.*

Example 3.1.5 *We consider the set of multiples of 3, which is defined by $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$. We now show that this set forms a group under addition.*
Let a and b be in $3\mathbb{Z}$, so there exist $a', b' \in \mathbb{Z}$ with $a = 3a'$ and $b = 3b'$.

1. *$a + b = 3a' + 3b' = 3(a' + b')$ which is again in $3\mathbb{Z}$ as $3(a' + b')$ is a multiple of 3.*

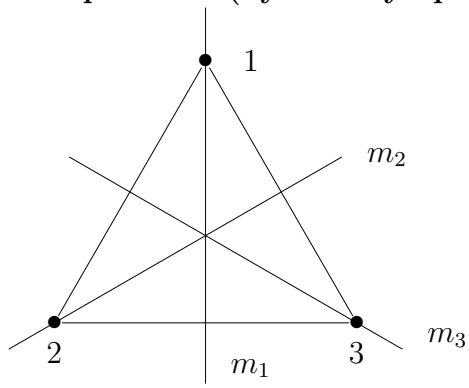
2. *Associativity follows from the associativity in $\mathbb{Z}$.*

3. *The neutral element is 0 as in the integers. Since 0 is divisible by 3 we have $0 \in 3\mathbb{Z}$.*

4. *The inverse of $a = 3a'$ is $-a = 3(-a') \in 3\mathbb{Z}$.*

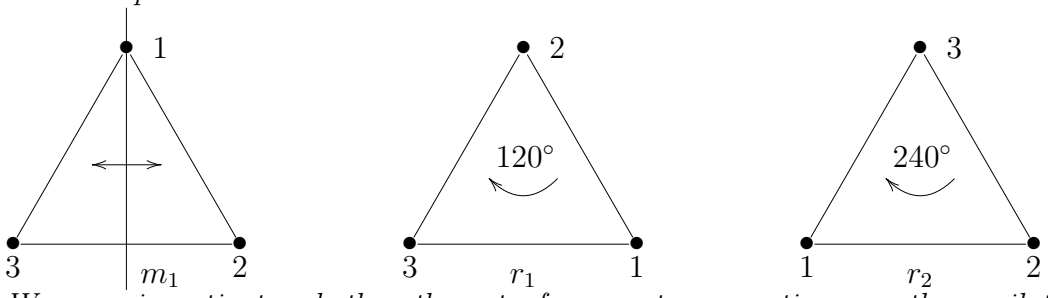
5. *Commutativity follows from the commutativity in $\mathbb{Z}$.*

Example 3.1.6 (Symmetry operations of equilateral triangle)



Symmetry operations of the equilateral triangle are maps that do not change the shape of the triangle. There are 6 *different such maps:*
id: identity map,
m_1*: reflection in axis through* 1,
m_2*: reflection in axis through* 2,
m_3*: reflection in axis through* 3,
r_1*: clockwise rotation by* 120° *mapping* 1 *to* 3,
r_2*: clockwise rotation by* 240° *mapping* 1 *to* 2.

For example:



We now investigate whether the set of symmetry operations on the equilateral triangle forms a group with respect to composition. The set is closed under composition: There are no other symmetry operations, so the result of the composition of two operations must again be one of these operations. For further reference we give a table with all results of composing two transformations. The symbol for composition is $\circ$*. We recall that for maps we write* $r_1 \circ m_1$ *if first* m_1 *and then* r_1 *is executed. The table is to be read as follows: each table entry is the result of performing the operation stated in the same row in the leftmost column first, followed by the one in the same column in the top row. E.g.* $r_1 \circ m_1$ *is found in the row of* m_1 *and the column of* r_1 *and equals* m_2*, which can be checked directly.*

$\circ$	id	m_1	m_2	m_3	r_1	r_2
id	id	m_1	m_2	m_3	r_1	r_2
m_1	m_1	id	r_1	r_2	m_2	m_3
m_2	m_2	r_2	id	r_1	m_3	m_1
m_3	m_3	r_1	r_2	id	m_1	m_2
r_1	r_1	m_3	m_1	m_2	r_2	id
r_2	r_2	m_2	m_3	m_1	id	r_1

Proving associativity with such a group table is cumbersome but possible since we have only finitely many group elements. As an example let us check

$$m_1 \circ (m_2 \circ m_1) = m_1 \circ r_1 = m_3 = r_2 \circ m_1 = (m_1 \circ m_2) \circ m_1$$

which shows associativity in this case. The remaining cases can be checked the same way.
The table shows that the identity map id is the neutral element of the group.
For each symmetric transformation there exists an inverse one. This can be seen

from the table – and by direct inspection. The reflections $m_i = \mathrm{inv}(m_i)$ *are their own inverses while* $\mathrm{inv}(r_1) = r_2$ *and* $\mathrm{inv}(r_2) = r_1$.
So the symmetric transformations on a equilateral triangle form a group with respect to $\circ$. *It is commonly called* S_3, *the symmetry group of a triangle. It is interesting to note that* $(S_3, \circ)$ *is not commutative:*

$$m_1 \circ m_2 = r_2 \neq r_1 = m_2 \circ m_1.$$

We will encounter group tables like in the previous example more often in the course. They offer a convenient way of stating group laws for finite groups. For an entertaining example have a look at "Group Theory in the Bedroom – An insomniac's guide to the curious mathematics of mattress flipping" by Brian Hayes which appeared in American Scientist, September-October 2005, volume 93, page 395.

Example 3.1.7 *Let* $(G_1, \circ_1)$ *and* $(G_2, \circ_2)$ *be groups. The* Cartesian product $G_1 \times G_2$ of G_1 and G_2 *is defined to be the set*

$$G_1 \times G_2 = \{(a_1, a_2) | a_1 \in G_1, a_2 \in G_2\}.$$

The operation $\circ$ *defined by*

$$(a_1, a_2) \circ (b_1, b_2) = ((a_1 \circ_1 b_1), (a_2 \circ_2 b_2))$$

turns $G_1 \times G_2$ *into a group, called the* direct product of G_1 and G_2 . *The detailed proof is posed as Exercise 3.1.27 g) below.*
The same holds for products of finitely many groups.

A useful tool is the cancellation rule.

Lemma 3.1.8 (Cancellation rule)
Let $(G, \circ)$ *be a group and let* $a, b, c \in G$. *If* $a \circ b = a \circ c$ *then* $b = c$.

Proof. The proof is posed as Exercise 3.1.27 f). □

Definition 3.1.9 (Subgroup)
Let $(G, \circ)$ *be a group. A subset* G' *of* G *is a* subgroup of G *if* G' *is a group with respect to* $\circ$.

Lemma 3.1.10 *Let* $(G, \circ)$ *be a group. A subset* $G' \subseteq G$ *is a subgroup of* G *if and only if the following three conditions are satisfied:*

1. *The neutral element* e *of* G *is in* G'.
2. *For all* $a, b \in G'$ *we have* $a \circ b \in G'$.
3. *For all* $a \in G'$ *we have* $\mathrm{inv}(a) \in G'$.

If G *is commutative then so is* G'.

Proof. Let $G' \subseteq G$ be a group. Then it must have a neutral element and by the uniqueness of the neutral element we obtain $e \in G'$. The other two conditions are the same as in the definition of a group.
Conversely, let $G' \subseteq G$ satisfy the above conditions. The only condition of the definition that is missing is associativity. We know that G' is contained in G which is associative, so by the associativity of G we have for all $a', b', c' \in G' \subseteq G$ $a \circ (b \circ c) = (a \circ b) \circ c$ which gives associativity in G'. Similarly, if G is commutative then this property is inherited by the subgroup. □

Remark 3.1.11 *The converse of the last statement in the lemma does not hold; there are non-commutative groups which have commutative subgroups. See Example 3.1.16.*

There is an equivalent version which is sometimes easier to use.

Lemma 3.1.12 *Let $(G, \circ)$ be a group. A subset $G' \subseteq G$ is a subgroup of G if and only if the following two conditions are satisfied:*

1. *The neutral element e of G is in G'.*
2. *For all $a, b \in G'$ we have $a \circ \mathrm{inv}(b) \in G'$.*

Proof. Let $G' \subseteq G$ be a group. Like before we get $e \in G'$. For every $b \in G'$ we must have $\mathrm{inv}(b) \in G'$ and since a group is closed and $a, \mathrm{inv}(b) \in G'$ we must have $a \circ \mathrm{inv}(b) \in G'$.
Assume now that $G' \subseteq G$ satisfies the conditions. Like in the previous lemma we obtain associativity for G'. We need to show that G' is closed under $\circ$ and that inverses exist in G'. The latter one is seen since $e \in G'$ and by the second condition thus $e \circ \mathrm{inv}(b) = \mathrm{inv}(b) \in G'$. Consequently, for any $a, b \in G'$ we have $a, \mathrm{inv}(b) \in G'$ and by the second condition we obtain $a \circ \mathrm{inv}(\mathrm{inv}(b)) = a \circ b \in G'$, so G' is closed. □

Example 3.1.13 *Let G be a group and let $e \in G$ be the neutral element. We have two (trivial) subgroups of G, namely $G_1 = \{e\} \subset G$ and $G_2 = G$ itself. The latter one is clearly a group. Let us check G_1 now. Since $e \circ e = e$ we have $\mathrm{inv}(e) = e$ and so using the criterion from Lemma 3.1.12 we only need to see that $e \circ \mathrm{inv}(e) = e \circ e = e$ is indeed in $G_1 = \{e\}$ which obviously holds.*

If we want to exclude the *trivial* subgroups considered in the previous example we speak of *proper subgroups*.

Example 3.1.14 *We have seen that $(\mathbb{C}, +)$ forms a group. With Lemma 3.1.10, the observation that $0 \in \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, and checking that in all these sets addition and inversion is closed we get the earlier obtained result that $(\mathbb{Z}, +), (\mathbb{Q}, +)$, and $(\mathbb{R}, +)$ are groups.*

Example 3.1.15 *We have seen that* $(\mathbb{Z}, +)$ *forms a group and that* $5\mathbb{Z} \subset \mathbb{Z}$. *The neutral element of* $\mathbb{Z}$ *is* 0 *which is also in* $5\mathbb{Z}$ *as* $0 = 5 \cdot 0$. *Let* $a, b \in 5\mathbb{Z}$, *i.e.* $a = 5a', b = 5b'$. *Then*

$$a \circ \text{inv}(b) = a + (-b) = 5a' - 5b' = 5(a' - b') \in 5\mathbb{Z}$$

and so $(5\mathbb{Z}, +)$ *forms a subgroup of* $(\mathbb{Z}, +)$ *by Lemma 3.1.12.*

Example 3.1.16 (Subgroups of S_3)
In Example 3.1.6 we considered S_3, *the group of symmetric transformations of the equilateral triangle, as an example of a non-abelian group. We now state all subgroups of* S_3.
Clearly $(\{id\}, \circ)$ *satisfies the criteria of Lemma 3.1.12 and thus is a subgroup.*
The reflections are self-inverse and thus $(\{id, m_1\}, \circ)$, $(\{id, m_2\}, \circ)$, *and* $(\{id, m_3\}, \circ)$ *are further subgroups.*
If we want a subgroup containing r_1 *then it must also contain* $r_1 \circ r_1 = r_2$ *by the second criterion and any combination of them. Since the rotations are inverse to each other and* $r_2 \circ r_2 = r_1$ *these three elements are sufficient leading to the subgroup* $(\{id, r_1, r_2\}, \circ)$.
As soon as we combine two different reflections or one reflection with a rotation and try to obtain a subgroup containing them, the second criterion dictates that we obtain the whole group. Thus the sixth and last subgroup is the full group $(\{id, m_1, m_2, m_3, r_1, r_2\}, \circ) = (S_3, \circ)$.
It is interesting to note that all proper subgroups are commutative while the full group is not.

In the example we constructed subgroups starting from one element $a \in G$ and considering the elements obtained as $a \circ a$ etc. For a natural number $m \in \mathbb{N}$ we introduce the notation $[m]a$ to denote the m-fold composition of a with itself:

$$[m]a = \underbrace{a \circ a \circ \cdots \circ a}_{m- \text{ copies of } a} .$$

We extend this to negative scalars m as $[m]a = [-m]\text{inv}(a)$ for $m < 0$.
The set of all such scalar multiples of a is denoted by

$$\langle a \rangle = \{[m]a \mid m \in \mathbb{Z}\} .$$

Definition 3.1.17 (Cyclic group)
A group $(G, \circ)$ *is called a* cyclic group *if there exists an element* $g \in G$ *so that*

$$G = \langle g \rangle .$$

A group element g *with* $G = \langle g \rangle$ *is called a* generator of G.
Let $a \in G$. *The set* $\langle a \rangle$ *is called the* cyclic subgroup generated by a.

The following lemma shows that the notion "subgroup" is justified since $\langle a \rangle$ is indeed a subgroup of G.

Lemma 3.1.18
Let $(G, \circ)$ *be a group and let* $a \in G$. *The set* $\langle a \rangle$ *is a commutative subgroup of* G.

Proof. The neutral element $e = [0]a$ is contained in $\langle a \rangle$. Since $\text{inv}(a) = [-1]a$ we have $\text{inv}([m]a) = [-m]a$ and

$$[m]a \circ \text{inv}([n]a) = [m]a \circ [-n]a = [m-n]a \in \langle a \rangle$$

as $m - n \in \mathbb{Z}$ and the result follows by Lemma 3.1.12.
Since $\mathbb{Z}$ is abelian and $[m]a \circ [n]a = [m+n]a = [n]a \circ [m]a$ also $\langle a \rangle$ is abelian. □

Example 3.1.19 *1. Any integer m can be written as $m = 1 + 1 + \cdots + 1 = [m]1$. So the group $(\mathbb{Z}, +)$ is cyclic and generated by 1. Similarly also -1 is a generator.*

2. $(3\mathbb{Z}, +)$ is cyclic and generated by 3.

3. For any integer n the set $(n\mathbb{Z}, +)$ is a cyclic group and generated by n.

4. $(\mathbb{Q}, +)$ is not cyclic; one cannot find a generator for this group. It contains $(\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$ as cyclic subgroups.

5. The subgroup $(\{id, r_1, r_2\}, \circ)$ of S_3 is generated by r_1. Another generator is r_2.

Definition 3.1.20 (Order of element)
Let $(G, \circ)$ be a group and let $a \in G$. If there exists an $m \in \mathbb{N}$ such that $[m]a = e$ then a has finite order*. The smallest such m is called the* order of a*, denoted by* $\text{ord}(a) = m$.
If no such number exists then a has infinite order*.*

Example 3.1.21 *In S_3 every element has finite order. Since $m_1 \circ m_1 = id$ we have $\text{ord}(m_1) = 2 = \text{ord}(m_2) = \text{ord}(m_3)$. The rotations have order 3 since $r_1 \circ r_1 = r_2 \neq id$ but $r_1 \circ r_1 \circ r_1 = r_2 \circ r_1 = id$.*

Definition 3.1.22 (Order of group)
Let $(G, \circ)$ be a group. The order of G *is the cardinality of G.*

If a group has finite order then there are only finitely many elements in it and thus each element must have finite order. The converse does not hold: There are infinite groups which contain elements of finite order.
For discrete mathematics finite groups are particularly interesting. Therefore, we now investigate some details of finite groups. The groups we encounter later on are mostly abelian, so we give some results only for this case. The interested reader may consult any of the algebra books mentioned in the introduction for the general case.
There is a nice connection between the order of a group and the order of an element given by the following lemma.

Lemma 3.1.23 *Let $(G, \circ)$ be a finite abelian group of order $|G| = n$.*
For all $a \in G$ one has $[n]a = e$.

Proof. Let $a \in G$. Since G is finite of order n, it can be written as $G = \{a_1, a_2, \ldots, a_n\}$.
The results $a \circ a_1$, $a \circ a_2, a \circ a_3, \ldots, a \circ a_n$ are all distinct as from $a \circ a_i = a \circ a_j$ the cancellation rule gives $a_i = a_j$. There are n results, so we can also write G as $G = \{a \circ a_1, a \circ a_2, a \circ a_3, \ldots, a \circ a_n\}$.
We now take the product over all elements of G – the left side in the representation involving a and the right side without – and use that the group is abelian so that we can re-arrange the order of the elements.

$$\begin{aligned}(a \circ a_1) \circ (a \circ a_2) \circ (a \circ a_3) \circ \cdots \circ (a \circ a_n) &= a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_n, \\ ([n]a) \circ (a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_n) &= a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_n.\end{aligned}$$

Using the cancellation rule we obtain

$$[n]a = e$$

which proves the claim. □

The lemma is actually a special case of Lagrange's Theorem (Theorem 3.3.8) which also holds for non-commutative groups.

Lemma 3.1.24 *Let $(G, \circ)$ be a group and let $a \in G$. If $[m]a = e$ then $\operatorname{ord}(a) \mid m$. In particular if G is finite and abelian with $|G| = n$ then for all $a \in G$ one has $\operatorname{ord}(a) | n$.*

Proof. Assume on the contrary that $m = k \operatorname{ord}(a) + r$ for $0 < r < \operatorname{ord}(a)$. Then

$$e = [m]a = [k \operatorname{ord}(a) + r]a = [k \operatorname{ord}(a)]a \circ [r]a = e \circ [r]a = [r]a,$$

so $e = [r]a$ which contradicts the minimality of $\operatorname{ord}(a)$.
By Lemma 3.1.23 for all group elements a we have $[n]a = e$. By the first part of the lemma we obtain $\operatorname{ord}(a) | n$. □

The converse of this lemma is not true in general. For $m | \operatorname{ord}(G)$ there need not exist an element $a \in G$ of order m. Only for prime numbers Cauchy's Theorem (Theorem 3.3.17) guarantees the existence of an element with that order.
The second part holds also for non-abelian groups by Langrange's theorem. Lagrange's and Cauchy's theorems will both be presented in Section 3.3.

Definition 3.1.25 (Exponent)
Let $(G, \circ)$ be a finite group. The smallest $m \in \mathbb{N}$ such that $[m]a = e$ for all $a \in G$ is called the exponent of G.

Example 3.1.26 *The symmetry group $(S_3, \circ)$ is finite. The elements have order 2 and 3, therefore $[6]a = id$ for any $a \in S_3$. No smaller integer with this property exists since it must be divisible by 2 and 3, thus S_3 has exponent 6.*

In more generality let $g_1, g_2, \ldots, g_k$ be elements of a group G with orders $m_1, m_2, \ldots, m_k$ respectively. The exponent of G must be divisible by the least common multiple $\operatorname{lcm}(m_1, m_2, \ldots, m_k)$ of the orders.

Exercise 3.1.27 *a) Consider the subset $\mathbb{Z}[i]$ of the complex numbers given by*

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z}\}.$$

Show that $(\mathbb{Z}[i], +)$ is a subgroup of $(\mathbb{C}, +)$.

b) Find all symmetric transformations of the square and show that they form a group with respect to composition. Give the group table. State all subgroups. Compute the order of this group and the exponent.

c) Find all symmetry operations of a rectangle which is not a square and show that they form a group with respect to composition. Give the group table. State all subgroups.
Compute the order of this group and the exponent. You do not need to prove associativity.

d) Define the following equivalence relation

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c$$

on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Let $M = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$ be the set of residue classes under $\sim$. Define the operation $\circ$ on M as follows:

$$(a, b) \circ (c, d) = (a \cdot d + c \cdot b, b \cdot d).$$

(a) Show that $\sim$ is indeed an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, i.e. show that $\sim$ is reflexive, symmetric and transitive.

(b) Show that $(M, \circ)$ is a group.

(c) Investigate whether $(M, \circ)$ is a commutative group.

e) Define the following operation $\circ$ on the set of rational numbers

$$a \circ b = a \cdot b - 3 \cdot (a + b) + 12,$$

where $+$ and $\cdot$ denote the regular addition and multiplication in $\mathbb{Q}$.

(a) Find the neutral element in $\mathbb{Q}$ with respect to the operation $\circ$.

(b) Determine all invertible elements in $\mathbb{Q}$ with respect to the operation $\circ$.

(c) Determine the maximal subset M of $\mathbb{Q}$ that forms a group with respect to $\circ$. Show that $(M, \circ)$ is a group.
Note: the expressions in the proof of associativity get very long, you may skip this part if you are sure that you can prove associativity.

f) Prove the cancellation rule, Lemma 3.1.8.

g) Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups. Give all details of the proof that the Cartesian product $G_1 \times G_2$ is a group.

3.2 Modular arithmetic

We briefly pause our algebraic considerations and introduce modular arithmetic in $\mathbb{Z}$ and consider quotient groups in general.
We have seen that the relation $a \sim b \Leftrightarrow 3|(a-b)$ is an equivalence relation. We now study such relations systematically for arbitrary numbers n in place of 3 and introduce names for the different concepts.

Definition 3.2.1 (Modulus)
Let n, a, b be integers. If n divides $(a-b)$ we write

$$a \equiv b \bmod n,$$

read "a is equivalent to b modulo n". In such a relation, the integer n is called the modulus*.*
The equivalence classes under $\equiv$ are called residue classes modulo n*.*

Example 3.2.2 *We have* $12 \equiv 27 \bmod 5$ *since* $12 - 27 = -15$ *is divisible by 5.*

Since any number which is divisible by n is also divisible by $-n$ we restrict to positive integers n in most of the following considerations.
We have $a \equiv b \bmod n$ exactly if a and b have the same remainder under division by n, i.e. if we write $a = a'n + r_a$ and $b = b'n + r_b$ with minimal remainders $0 \leq r_a, r_b < n$ then $r_a = r_b$.
We often represent the residue classes by the smallest non-negative integer in the class, i.e. for $0 \leq r < n$ we let

$$\bar{r} = \{a \in \mathbb{Z} | a = a'n + r\},$$

where the notation assumes that the modulus n is fixed.
One can combine the operations $+$ and $\cdot$ with modular reduction. The following lemma shows that this is compatible.

Lemma 3.2.3 *Let $a, b, n \in \mathbb{Z}$ with $a = a'n + r_a, b = b'n + r_b$, where the remainders are not necessarily minimal. We have the following equivalences*

1. $(a + b) \equiv (r_a + r_b) \bmod n$,
2. $(a \cdot b) \equiv (r_a \cdot r_b) \bmod n$.

Proof. The proof is left to the reader as Exercise 3.2.11 a. □

So we can also define operations + and · on the residue classes and the lemma shows that one can work with any representative of the class.

Example 3.2.4 *1. Let $n = 6$. A complete set of residue classes is given by*

$$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}.$$

To determine the value of $\bar{3} + \bar{4}$, we find one element in the resulting class, e.g. $3 + 4 = 7$ and then reduce it modulo 6 to find the smallest remainder, here $7 \equiv 1 \bmod 6$. So, as classes: $\bar{3} + \bar{4} = \bar{1}$.

Multiplication works the same: To find the resulting class of $\bar{3} \cdot \bar{4}$ we multiply the representatives of the classes $3 \cdot 4 = 12$ and reduce the result modulo 6, so $\bar{3} \cdot \bar{4} = \bar{0}$.

The complete tables of addition and multiplication of classes look as follows:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

The set $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ forms an abelian group under addition – the table shows that the set is closed under this operation, $\bar{0}$ is the neutral element and each element has an inverse. Associativity and commutativity are inherited from $\mathbb{Z}$.

The set does not does not form a group under multiplication. The neutral element is $\bar{1}$ but there are elements that do not have an inverse, namely there are no inverses of $\bar{0}, \bar{2}, \bar{3}$, and $\bar{4}$.

The subset $\{\bar{1}, \bar{5}\}$ forms a group under multiplication with $\bar{1}$ as neutral element and $\bar{5} \cdot \bar{5} = \bar{1}$.

2. We now do the same considerations modulo 3 and demonstrate, that one can also use other representatives for the classes, e.g. $\{-\bar{1}, \bar{0}, \bar{1}\}$ can be used just as well as the more standard choice $\{\bar{0}, \bar{1}, \bar{2}\}$.

+	$-\bar{1}$	$\bar{0}$	$\bar{1}$
$-\bar{1}$	$\bar{1}$	$-\bar{1}$	$\bar{0}$
$\bar{0}$	$-\bar{1}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$-\bar{1}$

·	$-\bar{1}$	$\bar{0}$	$\bar{1}$
$-\bar{1}$	$\bar{1}$	$\bar{0}$	$-\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$-\bar{1}$	$\bar{0}$	$\bar{1}$

We see that $(\{-\bar{1}, \bar{0}, \bar{1}\}, +)$ and $(\{-\bar{1}, \bar{1}\}, \cdot)$ are both abelian groups.

These examples can be generalized.

Lemma 3.2.5 *Let $n \in \mathbb{Z}$ be positive. The residue classes modulo n form a commutative group with respect to addition, where the addition is defined as*

$$\bar{r}_1 + \bar{r}_2 = \bar{r}_3 \Leftrightarrow r_1 + r_2 \equiv r_3 \bmod n$$

and r_3 is the unique representative of the class containing $r_1 + r_2$.

Proof. We first have to show that the operation is well-defined, i.e. that for any element in the class of $\bar{r}_1$ and for any element in the class of $\bar{r}_2$ the result is in the same class $\bar{r}_3$. So let $a \in \bar{r}_1, b \in \bar{r}_2$, then there exist integers a' and b' so that $a = a'n + r_1$ and $b = b'n + r_2$. Their sum is in the class of $a + b = (a'n + r_1) + (b'n + r_2) = (a' + b')n + r_1 + r_2 \equiv r_1 + r_2 \equiv r_3 \bmod n$ by definition of r_3.
The neutral element is $\bar{0}$ and the inverse of $\bar{r}$ is the residue class containing $-r$. If one uses representatives $0 \leq r < n$ then for $r \neq 0$ the inverse is $\overline{n - r}$.
Associativity and commutativity follow from $\mathbb{Z}$. □

The example with $n = 6$ demonstrated that one cannot hope for the same generality for multiplication. Analyzing which elements besides $\bar{0}$ do not have an inverse one sees that those are exactly the elements which have a factor in common with 6.

Lemma 3.2.6 *Let $a, n \in \mathbb{Z}$ be integers. The class containing a is invertible modulo n with respect to multiplication $\cdot$ if and only if*

$$\gcd(n, a) = 1.$$

Proof. Let $a = a'n + r_a$ with $0 \leq r_a < n$. We first observe that $\gcd(a, n) = \gcd(r_a, n)$ because any divisor of a and n also divides linear combinations of them like $a - a'n = r_a$. Similarly any divisor of r_a and n also divides $a'n + r_a = a$.
Let $b = b'n + r_b$ with $0 \leq r_b < n$ be a candidate multiplicative inverse. Their product is

$$a \cdot b = (a'n + r_a) \cdot (b'n + r_b) = (a'b'n + a'r_b + b'r_a)n + r_a r_b.$$

Let $r_a r_b$ be in the residue class of $0 \leq r_c < n$. By the same considerations, $\gcd(a, n)$ also divides $r_a r_b$ and r_c. So if $\gcd(a, n) = k \neq 1$ is non-trivial then k divides r_c which therefore cannot be 1 no matter which b is chosen.
Now let $\gcd(a, n) = 1$. Let $\{r_0, r_1, \ldots, r_{n-1}\}$ be a complete set of remainders modulo n. The products $a \cdot r_i$ are all different modulo n; because if $a \cdot r_i \equiv a \cdot r_j \bmod n$ then $n | a(r_i - r_j)$ and since $\gcd(a, n) = 1$ it must be that $n | (r_i - r_j)$ which by the size restrictions implies $r_i = r_j$. This means that there is one r_l such that $ar_l \equiv 1 \bmod n$ and so a is invertible. □

Definition 3.2.7 (Euler φ-function)
Let $n \in \mathbb{Z}$ be positive. We define the Euler φ-function $\varphi(n)$ *of n as the number of integers a with $0 \leq a < n$ and $\gcd(a, n) = 1$.*

Sometimes the Euler φ-function is also called *Euler's totient function*.

Example 3.2.8 *1. We have $\varphi(7) = 7 - 1 = 6$ since all positive integers < 7 are coprime to 7.*

2. Let p be a prime. Like in the previous example we have $\varphi(p) = p - 1$.

3. Let $n = p^2$ be the square of a prime. The integers $0 \leq a < n$ which have $\gcd(a, n) \neq 1$ are exactly the multiples of p, i.e. $p, 2p, 3p, \ldots, (p-1)p$. There are $p^2 - 1 - (p-1) = p(p-1)$ numbers $0 \leq a < n$ with $\gcd(a, n) = 1$.

4. Let $n = pq$ be the product of two different primes p and q. The integers a with $1 \leq a \leq pq - 1$ and $\gcd(a, n) \neq 1$ are multiples of p or q, precisely the numbers $p, 2p, 3p, \ldots, (q-1)p, q, 2q, 3q, \ldots (p-1)q$. I.e. there are $pq - 1 - (q-1) - (p-1) = pq - p - q + 1 = (p-1)(q-1)$ positive integers coprime to pq and smaller than pq.

The Euler φ-function is a typical function of elementary number theory. The examples in Example 3.2.8 can be generalized to the following lemma which we will not prove here but in Section 3.4 after stating the Chinese Remainder Theorem 3.4.20.

Lemma 3.2.9 *Let $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_r^{e_r}$ with $p_1, p_2, \ldots, p_r$ distinct primes and positive exponents $e_1, e_2, \ldots, e_r \in \mathbb{Z}$. We have*

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

The following lemma gives a nice illustration of the use of modular reduction in proofs.

Lemma 3.2.10 *For any nonzero $a, b \in \mathbb{Z}$ there exist $m, n \in \mathbb{Z}$ with $|m| < |b|$ and $|n| < |a|$ so that*

$$\gcd(a, b) = ma + nb.$$

Proof. Let $d = \gcd(a, b)$. For simplicity assume that a and b are positive. Put $p = a/d$ and $q = b/d$, then p and q are coprime. The $q - 1$ multiples $p, 2p, 3p, \ldots, (q-1)p$ of p are all not divisible by q and all in distinct residue classes modulo q. Since there are $q - 1$ non-zero residue classes modulo q one of the multiples, say pm, is in the class of 1 modulo q, i.e. $pm \equiv 1 \bmod q$. This implies $1 = pm + qn$ for some $1 \leq n < p$. Multiplying both sides of this equation by d we obtain the desired equation $d = am + bn$, where $1 \leq m < q \leq b$ and $1 \leq n < p \leq a$. For negative values of a or b similar considerations hold. □

This representation is often called *Bézout's identity* and is obtained using the *Extended Euclidean Algorithm* 4.3.1 which we will state later in this chapter and consider in detail in Chapter 4. It is possible to extend Bézout's identity to give a linear combination of any number of elements.

Exercise 3.2.11 *a) Prove Lemma 3.2.3.*

b) Write addition and multiplication tables for arithmetic modulo 4 and modulo 8. How many elements are invertible modulo 4 and modulo 8 respectively.

c) Compute $\varphi(1001)$. You may use Lemma 3.2.9.

3.3 Advanced concepts of groups

Modular arithmetic as considered in the previous section is one example of considering one group modulo a subgroup, in this case the group $\mathbb{Z}$ modulo $n\mathbb{Z}$ for some integer n. In this section we generalize the approach and show some properties of the resulting constructs. The whole section is rather technical and the proofs can be skipped on first reading but the results will be needed in later sections and chapters.
Let $(G, \circ)$ be a group and let G' be a subgroup. We define a relation $\sim$ on G by

$$a \sim b \Leftrightarrow a \circ \mathrm{inv}(b) \in G'. \tag{3.1}$$

We observe that $\sim$ is an equivalence relation as it is

reflexive: $a \sim a$ as $a \circ \mathrm{inv}(a) = e \in G'$ since G' is a subgroup.

symmetric: If $a \sim b$ then also $b \sim a$, because with $a \circ \mathrm{inv}(b) = c \in G'$ also $\mathrm{inv}(c) = \mathrm{inv}(a \circ \mathrm{inv}(b)) = b \circ \mathrm{inv}(a)$ must be in G' by the second criterion in Lemma 3.1.12.

transitive: If $a \sim b$ and $b \sim c$ then also $a \sim c$ because $a \circ \mathrm{inv}(c) = a \circ (\mathrm{inv}(b) \circ b) \circ \mathrm{inv}(c) = (a \circ \mathrm{inv}(b)) \circ (b \circ \mathrm{inv}(c))$ must be in G' as combination of the two group elements $a \circ \mathrm{inv}(b)$ and $b \circ \mathrm{inv}(c)$.

The set of equivalence classes is denoted by G/G' and we have

$$G/G' = \{a \circ G' | a \in G\}.$$

Example 3.3.1 *In Example 3.2.4 we considered $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.*

Lemma 3.3.2 *Let $(G, \circ)$ be an abelian group and let G' be a subgroup. The set of equivalence classes G/G' forms an abelian group under the operation*

$$\circ' : (a \circ G') \circ' (b \circ G') = (a \circ b) \circ G'$$

inherited from G.

Proof. We first need to show that the operation is well defined on the classes. Let $a' \in a \circ G'$ and $b' \in b \circ G'$, so there exist $c, d \in G'$ so that $a' = a \circ c$ and $b' = b \circ d$. The result of $a' \circ b'$ is

$$a' \circ b' = (a \circ c) \circ (b \circ d) = (a \circ b) \circ (c \circ d) \in (a \circ b) \circ G',$$

where in the last step we used associativity and commutativity of G and that $c \circ d \in G'$. So the resulting class is independent of the chosen representative.
The set G/G' is closed under $\circ'$, associativity and commutativity are inherited from G. The neutral element is $G' = e \circ G'$ since $(a \circ G') \circ' (e \circ G') = (a \circ e) \circ G' = a \circ G'$. The inverse element to $a \circ G'$ is $\mathrm{inv}(a) \circ G'$. □

Because $\circ'$ is so closely related to $\circ$ we drop the extra notation and use the same symbol $\circ$ for the group operation in G/G'.

Definition 3.3.3
Let $(G, \circ)$ be an abelian group and let G' be a subgroup. The group $G/G' = \{a \circ G' | a \in G\}$ is called the quotient group *of G modulo G'.*

With this theoretical background, the earlier proven fact that $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group follows as an easy corollary from Lemma 3.3.2.

Example 3.3.4 *In Example 3.1.13 we saw that every group G has trivial subgroups, namely $G_1 = \{e\}$ and $G_2 = G$. The first one leads to equivalence classes which contain only one element each, since $a \sim b$ requires $a \circ \mathrm{inv}(b) \in G_1$, i.e. $a \circ \mathrm{inv}(b) = e$ and thus $a = b$. This means that $G/\{e\}$ behaves like G itself.*
The same considerations for G_2 show that there is only one equivalence class which contains all of G, so the quotient group G/G has only one element.

The integers are not a group with respect to multiplication, so we cannot use this lemma to deduce anything about $\mathbb{Z}/n\mathbb{Z}$ under multiplication. Example 3.2.4 showed that there are subsets of $\mathbb{Z}/n\mathbb{Z}$ of elements that are invertible modulo n and that these subsets formed groups.

Definition 3.3.5 (Multiplicative group modulo n)
Let $n \in \mathbb{N}$. We denote by $(\mathbb{Z}/n\mathbb{Z})^\times$ the set of multiplicatively invertible elements modulo n. By Lemma 3.2.6 we have with unique representatives for the equivalence classes

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid 0 \leq a < n, \gcd(a, n) = 1\}.$$

Lemma 3.3.6 *Let $n \in \mathbb{N}$. The set $(\mathbb{Z}/n\mathbb{Z})^\times$ forms a commutative group under multiplication. It is called the* multiplicative group modulo n. *We have $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.*

Proof. We use the definition and Lemma 3.2.6. Let $a+n\mathbb{Z}, b+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, i.e. $\gcd(a,n) = \gcd(b,n) = 1$. Since ab is coprime to n, so is the remainder of ab modulo n and thus the set is closed under multiplication. Associativity and commutativity follow from the same properties in $\mathbb{Z}$. The neutral element is $1 + n\mathbb{Z}$ which is clearly in the set. By definition, the a's are exactly those integers which are invertible modulo n and so there exists a b with $ab \equiv 1 \bmod n$ and $(a + n\mathbb{Z})^{-1} = b + n\mathbb{Z}$. The second claim follows from the definition of the Euler φ-function. □

Since $\varphi(n)$ is the cardinality of the multiplicative group modulo n we get Fermat's little theorem as a corollary of Lemma 3.1.23

Corollary 3.3.7 (Fermat's Little Theorem)
Let $n \in \mathbb{N}$. For all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ one has $a^{\varphi(n)} \equiv 1 \bmod n$.

The proof of the following theorem is rather technical and can be skipped on first reading. However, the result is important.

Theorem 3.3.8 (Lagrange's Theorem)
Let $(G, \circ)$ be a finite group of order $|G| = n$.
Let G' be a subgroup of G. The order of G' divides n.

Proof. We use again the equivalence relation (3.1) $a \sim b$ if and only if $a \circ \mathrm{inv}(b) \in G'$ and decompose G into disjoint equivalence classes

$$G = H_1 \cup H_2 \cup \cdots \cup H_k,$$

for some number k. Since G' is closed under $\circ$, the equivalence class of any $b \in G'$ equals G' and so we can assume $H_1 = G'$.
For each equivalence class we can define a bijection between it and G'. Let $c \in H_i$ for some $1 \leq i \leq k$, i.e.

$$H_i = \{a \in G | c \circ \mathrm{inv}(a) \in G'\}$$

and this gives us a map

$$\psi_c : H_i \to G',\ a \mapsto c \circ \mathrm{inv}(a).$$

By the definition of H_i we have $c \circ \mathrm{inv}(a) \in G'$ and so the map indeed maps to G'. It is easy to give the inverse map $\psi_c^{-1}$of ψ_c as

$$\psi_c^{-1} : G' \to H_i,\ b \mapsto \mathrm{inv}(b) \circ c.$$

Indeed

$$\psi_c^{-1}(\psi_c(a)) = \psi_c^{-1}(c \circ \mathrm{inv}(a)) = \mathrm{inv}(c \circ \mathrm{inv}(a)) \circ c = a \circ \mathrm{inv}(c) \circ c = a$$

and

$$\psi_c(\psi_c^{-1}(b)) = \psi_c(\mathrm{inv}(b) \circ c) = c \circ \mathrm{inv}(\mathrm{inv}(b) \circ c) = c \circ \mathrm{inv}(c) \circ b = b.$$

So $|H_i| = |G'|$ for any $1 \leq i \leq k$ and from the above partition we have

$$|G| = |H_1| + |H_2| + \cdots + |H_k| = k \cdot |G'|$$

which proves the claim. □
So we have that the order of any subgroup divides the group order.
The ψ_c's in the previous proof were maps between sets. We now consider maps that respect the group operation.

Definition 3.3.9 (Group homomorphism)
Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be two groups and let $\psi : G_1 \to G_2$ be a map between them.
It is a group homomorphism *(or* homomorphism*) if for all $a_1, b_1 \in G_1$ one has*

$$\psi(a_1 \circ_1 b_1) = \psi(a_1) \circ_2 \psi(b_1).$$

A group homomorphism is an isomorphism *if it is bijective.*
Two groups G_1, G_2 are isomorphic*, written $G_1 \cong G_2$, if there exists an isomorphism between them.*

Example 3.3.10 *1. The map $[3] : \mathbb{Z} \to 3\mathbb{Z},\ a \mapsto 3a$ is a group homomorphism between $(\mathbb{Z}, +)$ and $(3\mathbb{Z}, +)$. First we observe that the map is well-defined since each element of $\mathbb{Z}$ is indeed mapped into $3\mathbb{Z}$. Since for all integers a and b we have $3(a+b) = (3a)+(3b)$ the map is a homomorphism. It is easy to give the inverse map $[1/3] : 3\mathbb{Z} \to \mathbb{Z}, a \mapsto a/3$. This map is actually well-defined since any $a \in 3\mathbb{Z}$ is divisible by 3. So in fact $\mathbb{Z}$ and $3\mathbb{Z}$ are isomorphic $\mathbb{Z} \cong 3\mathbb{Z}$.*

2. Let $(G, \circ)$ be a group. For any integer n the map

$$[n] : G \to G,\ a \mapsto [n]a$$

is a group homomorphism. Clearly, $[n]a \in G$ for any $a \in G$ and by the definition of $[n]$ it is a homomorphism.

A group homomorphism might map some elements to the neutral element in the target group. These elements will play a special role later on.

Definition 3.3.11 (Image and kernel of homomorphism)
Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be two groups and let $\psi : G_1 \to G_2$ be a group homomorphism.
The image of ψ*, denoted* $\mathrm{Im}(\psi)$*, is the subset of G_2 defined by*

$$\mathrm{Im}(\psi) = \{\psi(a_1) \in G_2 | a_1 \in G_1\}.$$

The kernel of ψ*, denoted* $\mathrm{Ker}(\psi)$*, is the subset of G_1 that is mapped to the neutral element e_2 of G_2*

$$\mathrm{Ker}(\psi) = \{a_1 \in G_1 | \psi(a_1) = e_2\}.$$

Theorem 3.3.12 (First isomorphism theorem) *Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be abelian groups and let $\psi : G_1 \to G_2$ be a group homomorphism. The kernel of ψ is a subgroup of G_1 and $\mathrm{Im}(\psi) \cong G_1/\mathrm{Ker}(\psi)$.*

Proof. We use Lemma 3.1.12. Since $e_1 \circ_1 a_1 = a_1$ for any $a_1 \in G_1$ and by the definition of homomorphisms we have

$$\psi(a_1) = \psi(e_1 \circ_1 a_1) = \psi(e_1) \circ_2 \psi(a_1).$$

By the cancellation rule we get $\psi(e_1) = e_2$, the neutral element in G_2. So $e_1 \in \mathrm{Ker}(\psi)$.
We remark that for $a_1 \in G_1$ we have $\psi(\mathrm{inv}_1(a_1)) = \mathrm{inv}_2(\psi(a_1))$, where the first inverse is with respect to $\circ_1$ and the second one with respect to $\circ_2$, as $e_2 = \psi(e_1) = \psi(a_1 \circ_1 \mathrm{inv}_1(a_1)) = \psi(a_1) \circ_2 \psi(\mathrm{inv}_1(a_1))$.
Let $a_1, b_1 \in \mathrm{Ker}(\psi)$, i.e. $\psi(a_1) = \psi(b_1) = e_2$. We see that

$$\psi(a_1 \circ_1 \mathrm{inv}_1(b_1)) = \psi(a_1) \circ_2 \psi(\mathrm{inv}_1(b_1)) = e_2 \circ_2 \mathrm{inv}_2(\psi(b_1)) = \mathrm{inv}_2(e_2) = e_2$$

and so $a_1 \circ_1 \mathrm{inv}_1(b_1) \in \mathrm{Ker}(\psi)$.
To prove the isomorphism we construct a homomorphism between the sets and show that an inverse map exists. Let

$$\psi' : G/\mathrm{Ker}(\psi) \to \mathrm{Im}(\psi),\ \psi'(a_1 \circ \mathrm{Ker}(\psi)) = \psi(a_1).$$

By definition of $\mathrm{Im}(\psi)$ indeed ψ' maps to $\mathrm{Im}(\psi)$ and the map is well-defined since for $k \in \mathrm{Ker}(\psi)$ we have $\psi'((a_1 \circ k) \circ \mathrm{Ker}(\psi)) = \psi(a_1 \circ k) = \psi(a_1) \circ \psi(k) = \psi(a_1)$ and so the image is independent of the representative. Since ψ is a homomorphism so is ψ'. If $a_2 \in \mathrm{Im}(\psi)$ there must exist an $a_1 \in G$ with $a_2 = \psi(a_1)$; a_1 is unique up to elements from $\mathrm{Ker}(\psi)$: If $\psi(a_1) = \psi(b_1) = a_2$ then $\psi(b_1 \circ \mathrm{inv}_1(a_1)) = \psi(b_1) \circ \mathrm{inv}_2(\psi(a_1)) = e_2$ and so $b_1 \circ \mathrm{inv}_1(a_1) \in \mathrm{Ker}(\psi)$ and a_1 and b_1 are in the same residue class modulo $\mathrm{Ker}(\psi)$. This allows to define the inverse map $(\psi')^{-1} : \mathrm{Im}(\psi) \to G/\mathrm{Ker}(\psi)$ as $(\psi')^{-1}(a_2) = a_1 \circ \mathrm{Ker}(\psi)$ if $\psi(a_1) = a_2$. □

Example 3.3.13 *Let $\psi : G \to H$ be an isomorphism, i.e. ψ is injective and so $\mathrm{Ker}(\psi) = \{e\}$ and surjective, i.e. $\mathrm{Im}(\psi) = H$. Theorem 3.3.12 says that*

$$H = \mathrm{Im}(\psi) \cong G/\{e\} \cong G,\ \textit{i.e. } H \cong G$$

which we knew already from ψ being an isomorphism. So the lemma fits with our expectation.

Example 3.3.14 *Let $(G, \circ)$ be a group. The elements of order n for some integer n form a group as they are the kernel of the homomorphism*

$$[n] : G \to G,\ a \mapsto [n]a.$$

Definition 3.3.15 (Product of groups)
Let $(G, \circ)$ be a group and let G' and G'' be subgroups of G. The set

$$G'G'' = \{a' \circ a'' | a' \in G', a'' \in G''\}$$

is called the product of G' and G''.

Lemma 3.3.16 *Let $(G, \circ)$ be an abelian group and let G' and G'' be subgroups of G. The product $G'G''$ is a subgroup of G and*

$$|G'G''| = |G'| \cdot |G''| / |G' \cap G''|.$$

Proof. We use Lemma 3.1.12. Since G' and G'' are subgroups of G they both contain e and thus $e = e \circ e \in G'G''$.
Let $a', b' \in G'$ and $a'', b'' \in G''$. We show that with $a' \circ a'' \in G'G''$ and $b' \circ b'' \in G'G''$ also $(a' \circ a'') \circ \mathrm{inv}(b' \circ b'')$ is in $G'G''$. Since G is abelian we can rearrange the last expression to

$$(a' \circ a'') \circ \mathrm{inv}(b' \circ b'') = (a' \circ \mathrm{inv}(b')) \circ (a'' \circ \mathrm{inv}(b'))$$

and use that $(a' \circ \mathrm{inv}(b')) \in G'$ and $(a' \circ \mathrm{inv}(b')) \in G''$ so that the result is indeed in $G'G''$.
To prove the statement about the cardinality of $G'G''$ we consider the following map between the Cartesian product $G' \times G''$ and $G'G''$:

$$\psi : G' \times G'' \to G'G'', \ (a', a'') \mapsto a' \circ \mathrm{inv}(a'').$$

Since all groups involved are abelian and subgroups of G, this is a group homomorphism and in particular $G'G'' = \mathrm{Im}(\psi)$. The kernel consists of

$$\mathrm{Ker}(\psi) = \{(a', a'') \in G' \times G'' | a' \circ \mathrm{inv}(a'') = e\},$$

in other words of the tuples (a, a) such that $a \in G' \cap G''$ and so the proof follows by Theorem 3.3.12 and taking cardinalities. □

The next theorem provides a partial inverse to Lagrange's Theorem. The proof needs all the concepts introduced so far.

Theorem 3.3.17 *Cauchy's Theorem*
Let $(G, \circ)$ be a finite abelian group of order n and let p be a prime dividing n. There exists an element $a \in G$ with $\mathrm{ord}(a) = p$. The subgroup generated by this a is cyclic of order p.

Proof. Let $G = \{g_1, g_2, \ldots, g_n\}$ and consider the finite product of groups $P_m = \langle g_1 \rangle \langle g_2 \rangle \langle g_3 \rangle \cdots \langle g_m \rangle$ for some $m \leq n$, which by $m - 1$-fold application of Lemma 3.3.16 is a subgroup of G. By the same lemma the cardinality is

$$|P_m| = |\langle g_1 \rangle||\langle g_2 \rangle||\langle g_3 \rangle| \cdots |\langle g_m \rangle|/k_m,$$

where k_m is an integer taking care of the cardinalities of the intersections.
By construction P_n contains all g_i and since P_n is a subgroup of G we actually have $G = P_n$, so we get

$$|G| = |P_n| = |\langle g_1 \rangle||\langle g_2 \rangle||\langle g_3 \rangle| \cdots |\langle g_n \rangle|/k_n.$$

Since p is a prime and divides $|G|$ it must also divide the product on the right hand side, and by the primality it must divide one of the factors $|\langle g_i \rangle|$ for one $1 \leq i \leq n$. Let $c = |\langle g_i \rangle|/p$ and put $a = [c]g_i$. By construction $[p]a = [p]([c]g_i) = [\mathrm{ord} g_i]g_i = e$ and $a \neq e$. □

Corollary 3.3.18 *Every finite abelian group of prime order is cyclic.*

Proof. Let $|G| = p$ be a prime. There exists an element $g \in G$ of order $\mathrm{ord}(g) = p$ and thus $G = \langle g \rangle$. □

Example 3.3.19 *Let $(G, \circ)$ be a cyclic group of order m. How many generators does G have?*
Since G is cyclic there exists a generator g, so let $G = \langle g \rangle = \{[n]g \mid n \in \mathbb{Z}\}$. For any $a = [n]g \in G$ we have $[m]a = [n]([m]g) = e$ but if n has a non-trivial common divisor with m then a $\mathrm{ord}(a) < m$. So there are exactly $|\{0 \leq n < m \mid \gcd(n, m) = 1\}| = \varphi(m)$ generators.

Example 3.3.20 *In Exercise 3.2.11 we considered the multiplicative group modulo 8 and found that $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ has order 4. The multiplication table shows that there is no element of order 4 but that the orders are $\mathrm{ord}(\bar{1}) = 1, \mathrm{ord}(\bar{3}) = 2, \mathrm{ord}(\bar{5}) = 2, \mathrm{ord}(\bar{7}) = 2$.*
This structure – a non-cyclic group of order 4 – is a famous example in the theory of finite groups. It is called the Klein four-group.

Exercise 3.3.21 *a) Let $(G, \circ)$ be a group and let G_1, G_2 be two subgroups of it. Show that their intersection is also a subgroup of G.*
In fact one can even show that the intersection of arbitrarily many subgroups is a subgroup.

b) Consider the group $(\mathbb{Z}/12\mathbb{Z}, +)$. Find all subgroups. Note that Lagrange's Theorem helps to determine possible group orders.

c) The multiplicative group $(\mathbb{Z}/299\mathbb{Z})^\times$ is of order $(13-1)(23-1) = 264$ which is divisible by 11. Find an element of order 11.

d) Let G be an abelian group of order $13 \cdot p$, where $p \neq 13$ is a prime. State a randomized algorithm to find an element of order p in G.

3.4 Rings

We have seen that the integers form an abelian group with respect to addition and only a semigroup with respect to multiplication and we have seen other sets on which we can define more than one operation. Such structures are called rings if they satisfy some extra conditions. The integers are a particularly familiar example of a ring. In the following section we study fields, which are rings in which both are sets which are closed under two different operations.

Definition 3.4.1 (Ring)
A set R is a ring *with respect to two operations $\circ, \diamond$ denoted by $(R, \circ, \diamond)$ if*

1. *$(R, \circ)$ is an abelian group.*
2. *$(R, \diamond)$ is a semi-group (closed under $\diamond$ and the associative rule holds).*

3. *The distributive laws hold in R:*

   Let $a, b, c \in R$. Then we must have

$$\begin{aligned} a \diamond (b \circ c) &= (a \diamond b) \circ (a \diamond c), \\ (a \circ b) \diamond c &= (a \diamond c) \circ (b \diamond c). \end{aligned}$$

If there exists a neutral element $e_\diamond$ with respect to $\diamond$ then R is called a ring with unity.
If $\diamond$ is commutative in R then R is called a commutative ring.

Example 3.4.2 *The integers $(\mathbb{Z}, +, \cdot)$ form a ring. We have already seen that $(\mathbb{Z}, +)$ is an abelian group and that $(\mathbb{Z}, \cdot)$ is a semi-group. It remains to be shown that the distributive laws hold. We first observe that multiplication is commutative as can be seen in rearranging $a \cdot b = b + b + \cdots + b$ (a times) and $b = 1 + 1 + \cdots + 1$ (b times) to $a \cdot b = b \cdot a$. This implies that only one of the two laws need to be checked explicitly.*
By definition and commutativity of $(\mathbb{Z}, +)$ we have $a \cdot (b+c) = (b+c) + \cdots + (b+c) = (b + \cdots + b) + (c + \cdots + c) = ab + ac$.
The number 1 is the neutral element with respect to multiplication since $1 \cdot a = a \cdot 1 = a$.
To sum up, the integers form a commutative ring with unity.

Example 3.4.3

1. *The rational numbers $(\mathbb{Q}, +, \cdot)$, the reals $(\mathbb{R}, +, \cdot)$ and the complex numbers $(\mathbb{C}, +, \cdot)$ form commutative rings with 1.*

2. *Let $n \in \mathbb{N}$. The set $n\mathbb{Z}$ of multiples of n forms a ring with addition and multiplication as in $\mathbb{Z}$: associativity, commutativity, and the distributive laws follow from $\mathbb{Z}$. We have shown that $(n\mathbb{Z}, +)$ is a group. The only thing we need to check is that the set is closed under multiplication which holds since $an \cdot bn = (abn)n$ is a multiple of n.*

3. *In Example 3.1.4 we considered the additive group of polynomials $\mathbb{C}[x]$ over $\mathbb{C}$. We can define multiplication of polynomials by*

$$\left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(\sum_{i=0}^{m} b_i x^i \right) = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i,$$

   where $a_i = 0$ for $i > n$ and $b_i = 0$ for $i > m$. The set $\mathbb{C}[x]$ is closed under multiplication since all coefficients are again in $\mathbb{C}$. Associativity can be checked by direct computation and follows from associativity in $\mathbb{C}$. The polynomial $1 \in \mathbb{C}[x]$ is the neutral element with respect to multiplication and the operation is commutative. So, $\mathbb{C}[x]$ is a commutative ring with unity. We study polynomial rings in more detail in Section 3.7.

4. *Let $n \in \mathbb{N}$ and consider the set $\mathbb{Z}/n\mathbb{Z}$. We have seen in Lemma 3.2.5 that $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group. Multiplication of residue classes is well-defined and closed by Lemma 3.2.3. Associativity follows from associativity of $(\mathbb{Z}, \cdot)$. The residue class $1 + n\mathbb{Z}$ is the neutral element of multiplication. Commutativity and distributive laws are inherited from $(\mathbb{Z}, \cdot)$. So $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with unity for any n.*

5. *Let $(R, \circ_R, \diamond_R)$ and $(S, \circ_S, \diamond_S)$ be rings. The Cartesian product $R \times S$ is defined by*

$$R \times S = \{(r, s) | r \in R, s \in S\}.$$

With the operations $\circ$ and $\diamond$ defined by

$$\begin{aligned}(r_1, s_1) \circ (r_2, s_2) &= ((r_1 \circ_R r_2), (s_1 \circ_S s_2)) \\ (r_1, s_1) \diamond (r_2, s_2) &= ((r_1 \diamond_R r_2), (s_1 \diamond_S s_2))\end{aligned}$$

the Cartesian product $R \times S$ is a ring. If both R and S are commutative rings then so is $R \times S$; if both are rings with unity then so is $R \times S$.

This example can be generalized to arbitrarily many rings.

In a ring we have the following useful computation laws which we know very well for the integers.

Lemma 3.4.4 *Let $(R, \circ, \diamond)$ be a ring and let $e_\circ$ be the neutral element with respect to $\circ$. If R is a ring with unity, let $e_\diamond$ be the neutral element of $\diamond$. We have for arbitrary $a, b \in R$:*

1. $e_\circ \diamond a = a \diamond e_\circ = e_\circ$.
2. $\mathrm{inv}_\circ(e_\diamond) \diamond a = a \diamond \mathrm{inv}_\circ(e_\diamond) = \mathrm{inv}_\circ(a)$.
3. $\mathrm{inv}_\circ(a) \diamond b = a \diamond \mathrm{inv}_\circ(b) = \mathrm{inv}_\circ(a \diamond b)$.

Proof. By the distributive laws we have

$$(e_\circ \diamond a) \circ (e_\circ \diamond a) = (e_\circ \circ e_\circ) \diamond a = e_\circ \diamond a = (e_\circ \diamond a) \circ e_\circ.$$

By the cancellation rule, Lemma 3.1.8, it follows that

$$e_\circ \diamond a = e_\circ.$$

Similarly one proves $a \diamond e_\circ = e_\circ$.
For the second result we use the definitions of $e_\circ$ and $e_\diamond$, the first result and the distributive laws on

$$e_\circ = e_\circ \diamond a = (e_\diamond \circ \mathrm{inv}_\circ(e_\diamond)) \diamond a = (e_\diamond \diamond a) \circ (\mathrm{inv}_\circ(e_\diamond) \diamond a) = a \circ (\mathrm{inv}_\circ(e_\diamond) \diamond a)$$

and add $\mathrm{inv}_\circ(a)$ on both sides from the left giving $\mathrm{inv}_\circ(a) = \mathrm{inv}_\circ(e_\diamond) \diamond a$ as claimed. The proof for $a \diamond \mathrm{inv}_\circ(e_\diamond) = \mathrm{inv}_\circ(a)$ follows along the same lines.

The last result follows from the second and associativity

$$\mathrm{inv}_\circ(a) \diamond b = (a \diamond \mathrm{inv}_\circ(e_\diamond)) \diamond b = a \diamond (\mathrm{inv}_\circ(e_\diamond) \diamond b) = a \diamond \mathrm{inv}_\circ(b)$$

and

$$\mathrm{inv}_\circ(a) \diamond b = (\mathrm{inv}_\circ(e_\diamond) \diamond a) \diamond b = \mathrm{inv}_\circ(e_\diamond) \diamond (a \diamond b) = \mathrm{inv}_\circ(a \diamond b).$$

□

Definition 3.4.5 (Divisibility)
Let $(R, \circ, \diamond)$ be a ring and let $a, b \in R$. We say that a divides *b, written $a|b$, if there exists $c \in R$ with*

$$a \diamond c = b.$$

Definition 3.4.6 (Domain, zero-product property)
Let $(R, \circ, \diamond)$ be a ring with unity. It is called a domain *if $e_\circ \neq e_\diamond$ and there are no zero divisors, i.e. if*

$$a \diamond b = e_\circ \text{ implies } a = e_\circ \text{ or } b = e_\circ.$$

This last property is called the zero-product property*.*

Definition 3.4.7 (Greatest common divisor)
Let R be a commutative ring and let $a, b \in R$. A greatest common divisor *d of a and b is a common divisor of a and b so that for all common divisors c of a and b one has that $c|d$.*

In the integers we have that if $a|b$ then also $-a|b$ and the factorization of an integer is unique only up to factors of -1 – even though one usually restricts to positive primes. In general rings, greatest common divisors and factorizations can be unique only up to invertible elements from R.

Definition 3.4.8 (Units)
Let $(R, \circ, \diamond)$ be a commutative ring with unity $e_\diamond$. An element $a \in R$ is called a unit *if there exists an element $b = \mathrm{inv}_\diamond(a) \in R$ so that $a \diamond b = e_\diamond$.*
The set of units in R is denoted by $R^\times$ and we have

$$R^\times = \{a \in R | \text{ there exists an element } b \in R \text{ so that } a \diamond b = e_\diamond\}.$$

Example 3.4.9 *The invertible elements in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ are exactly the elements in the multiplicative group modulo n, so the notation $(\mathbb{Z}/n\mathbb{Z})^\times$ is consistent with these elements being the units in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$.*

Lemma 3.4.10 *Let $(R, \circ, \diamond)$ be a commutative ring with unity $e_\diamond$. The set of units $R^\times$ of R forms a group under $\diamond$.*

Proof. Left to the reader as Exercise 3.4.21 d. □

Lemma 3.4.11 *Let $(R, \circ, \diamond)$ be a domain and let $e_\circ \neq a, b \in R$. If $a|b$ and $b|a$ then there exists a unit $u \in R^\times$ so that $a = b \diamond u$.*

Proof. By the definition of divisibility, $a|b$ and $b|a$ imply that there exist $c, d \in R$ with $b = a \diamond c$ and $a = b \diamond d$. The combination leads to

$$a \diamond e_\diamond = a = b \diamond d = (a \diamond c) \diamond d = a \diamond (c \diamond d).$$

Using distributive laws this gives $a \diamond (e_\diamond \circ \mathrm{inv}_\circ(c \diamond d)) = e_\circ$. Since R is a domain and $a \neq e_\circ$, the zero-product property gives $e_\diamond \circ \mathrm{inv}_\circ(c \diamond d)) = e_\circ$, i.e. $e_\diamond = c \diamond d$, and so $c, d \in R^\times$ are units. □

Modular arithmetic (cf. Section 3.2) is about computing with remainders of division by an integer n. For the integers it is very easy to find unique representatives for the residue classes, namely one uses the non-negative integers $< n$ to represent their respective classes and all classes are distinct. In general one cannot hope to find a canonical representative for each class and so rings in which we can define a division with remainder in a unique way deserve a special name.

Definition 3.4.12 (Euclidean domain)
Let $(R, \circ, \diamond)$ be a commutative domain and let $v : R\backslash\{e_\circ\} \to \mathbb{Z}_+$ be a function. The ring R is called a Euclidean domain *with respect to v if for each $a, b \in R$ with $b \neq e_\circ$ one can find $q, r \in R$ with*

$$a = q \diamond b \circ r \text{ and } r = e_\circ \text{ or } v(r) < v(b).$$

In Euclidean domains any two elements have a greatest common divisor and one can give an algorithm to determine it. The method to find greatest common divisors makes extensive use of the following lemma.

Lemma 3.4.13 *Let $(R, \circ, \diamond)$ be a Euclidean domain. Let $a, b, q, r \in R$ with $a = q \diamond b \circ r$.*
The set of common divisors of a and b equals the set of common divisors of b and r.

Proof. Let $d|a$ and $d|b$ which implies that $d|(a \circ \mathrm{inv}_\circ(q \diamond b))$, i.e. $d|r$ and so every divisor of a and b also divides r. Reversing the same argument gives that every common divisor f of b and r also divides the linear combination $q \diamond b \circ r = a$. □

As a shorthand we speak of computing modulo b when using the remainder r of division by b instead of a itself, so we write $a \equiv r \bmod b$ and speak of r as the remainder. Since R is Euclidean we can find a remainder r such that $v(r) < v(b)$ or $r = e_\circ$. We use $(a \bmod b)$ to denote this (smallest) remainder.
Repeated application of this lemma leads to remainders r_i with strictly decreasing values under v and since v maps to the non-negative integers this process

must eventually lead to a remainder $r_j = 0$. This recursive algorithm is known as *Euclidean algorithm* and will be studied in much more algorithmic detail in Chapter 4.

Lemma 3.4.14 *Let $(R, \circ, \diamond)$ be a Euclidean domain. For any two elements $a, b \in R$ there exists a greatest common divisor $d = \gcd(a, b)$ and d is unique up to units from $R^\times$.*

Proof. The sequence of values $v(r_i)$ of the remainders r_i in the following algorithm is strictly decreasing and consists of non-negative integers so it must terminate which means that $r_j = e_\circ$ for some j. By Lemma 3.4.13 we have that each two consecutive remainders r_{i-1} and r_i have the same common divisors as a and b. Since $r_j = e_\circ$ the common divisors of a and b are the same as those of r_{j-1} and $e_\circ$. These are precisely all divisors of r_{j-1} and a greatest common divisor is thus given by r_{j-1} itself.
Let d be another greatest common divisor of a and b. Then we have $r_{j-1}|d$ since d is greatest common divisor and $d|r_{j-1}$ since r_{j-1} is greatest common divisor. By Lemma 3.4.11 this means that there exists a unit $u \in R^\times$ with $d = u \diamond r_{j-1}$. □

Algorithm 3.4.15 (Euclid's Algorithm)
IN: $e_\circ \neq a, b \in R$
OUT: $\gcd(a, b)$

1. $i \leftarrow 0$
2. $r_{-1} \leftarrow a$
3. $r_0 \leftarrow b$
4. `while` $r_i \neq e_\circ$
   (a) $i \leftarrow i + 1$
   (b) $r_i \leftarrow (r_{i-2} \bmod r_{i-1})$ *where* $r_{i-2} = q_i \diamond r_{i-1} \circ r_i$ *with* $r_i = e_\circ$ *or* $v(r_i) < v(r_{i-1})$
5. `return` r_{i-1}

This algorithm must terminate since the size of the remainder is strictly decreasing until $r_i = e_\circ$ is reached. This implies that $r_{i-1}|r_{i-2}$ and by Lemma 3.4.13 this r_{i-1} is the greatest common divisor of the input values a and b.
In Section 3.2 we gave a special version of the following result as Lemma 3.2.10. With the help of the Euclidean algorithm we can not only generalize the result to arbitrary Euclidean rings but also give a constructive proof of Bézout's identity.

Lemma 3.4.16 *Let R be a Euclidean domain with respect to v. For any non-zero $a, b \in R$ there exist $m, n \in R$ so that*

$$\gcd(a, b) = m \diamond a \circ n \diamond b.$$

Proof. Algorithm 3.4.15 produces a sequence of remainders r_i and (implicitly) of quotients q_i with the property that $r_{i-2} = q_i \diamond r_{i-1} \circ r_i$. When the algorithm terminates we have $r_i = e_\circ$ and before that $r_{i-3} = q_{i-1} \diamond r_{i-2} \circ r_{i-1}$, i.e. $\gcd(a,b) = r_{i-3} \circ \mathrm{inv}_\circ(q_{i-1} \diamond r_{i-2})$. Recursively replacing r_{i-2}, r_{i-3} etc. by these linear combinations leads to an equation of the requested form since the first equation was $a = r_{-1} = q_1 \diamond r_0 \circ r_1 = q_1 \diamond b \circ r_1$. □

Example 3.4.17 *Bézout's identity leads to an efficient way of computing modular inverses. Let $a, n \in \mathbb{N}$ and let $\gcd(a,n) = 1$. By Lemma 3.2.6 a is invertible modulo n and indeed the previous lemma shows that there exists b, m such that*

$$1 = \gcd(a,n) = ab + nm, \text{ i.e. } 1 \equiv ab \bmod n,$$

so the b computed in Bézout's identity is the inverse of a modulo n.

Lemma 3.4.18 *Let R be a Euclidean domain and let $a, b \in R$ so that a and b have no non-trivial common divisor and let $c \in R$. If $a|c$ and $b|c$ then also $(a \diamond b)|c$.*

Proof. There exist k, l with $c = a \diamond k$ and $c = b \diamond l$. If a and b are co-prime we have $\gcd(a,b) = e_\diamond$ and by Lemma 3.4.16 there exist $m, n \in R$ so that $e_\diamond = m \diamond a \circ n \diamond b$. This leads to $c = a \diamond k = (a \diamond k) \diamond e_\diamond = (a \diamond k) \diamond (m \diamond a \circ n \diamond b) = (b \diamond l) \diamond (m \diamond a) \circ (a \diamond k) \diamond (n \diamond b) = (a \diamond b) \diamond ((m \diamond l) \circ (n \diamond k))$, so $a \diamond b$ divides c. □

Example 3.4.19 *In recreational mathematics one often encounters stories like the following example:*
A Chinese general has a fast way of "counting" the number of soldiers in his army. He first lets them line up in rows of 11 and counts the number of soldiers in the last, incomplete row. He then repeats the process with rows of 13 and rows of 17.
One morning, he finds that there are 3 soldiers left when the rest are in rows of 11, 4 soldiers left when the rest are in rows of 13, and 9 soldiers left when the rest are in rows of 17. He knows that there are 1000 soldiers in his army. How many of the soldiers are present this morning?
We fist look what the numbers would look like if all 1000 were present. We have

$$1000 \equiv 10 \bmod 11; 1000 \equiv 12 \bmod 13; 1000 \equiv 14 \bmod 17,$$

so clearly not all soldiers are present. So we are asked to find a number X such that the following systems of equivalences is satisfied

$$\begin{aligned} X &\equiv 3 \bmod 11; \\ X &\equiv 4 \bmod 13; \\ X &\equiv 9 \bmod 17. \end{aligned}$$

From the last equivalence we get $X = 17Y + 9$ *for some* Y*. From the second we get* $X = 17Y + 9 \equiv 4Y + 9 \overset{!}{\equiv} 4 \bmod 13$*, i.e.,* $4Y \equiv 8 \bmod 13$*. In this case we can divide both sides by 4 and get* $Y \equiv 2 \bmod 13$*; in general we could use Bézout's identity to compute the inverse of* 4 *modulo* 13*, namely* $4 \cdot 10 \equiv 1 \bmod 13$*, to obtain* $Y \equiv 2 \bmod 13$*. This means that with some* Z *we have*

$$X = 17 \cdot 13Z + 17 \cdot 2 + 9 = 17 \cdot 13Z + 43$$

as combination of the last two equations. Continuing to the first we get $X = 17 \cdot 13Z + 43 \equiv Z + 10 \overset{!}{\equiv} 3 \bmod 11$ *which immediately gives* $Z \equiv 4 \bmod 11$ *and thus for some* A

$$X = 17 \cdot 13 \cdot 11A + 17 \cdot 13 \cdot 4 + 43 = 2431A + 927.$$

From the story we know that the number of soldiers is positive and at most 1000 *and so* $A = 0$ *is the only possibility leading to* $X = 927$*.*
So apparently the general got a very bad day to count his soldiers since 73 *were absent (which is a sufficiently high number to avoid students guessing the correct solution).*

In the following section we show a generalization of this example to arbitrary rings; to conclude this section we state the *Chinese Remainder Theorem* only for the integers.

Theorem 3.4.20 (Chinese Remainder Theorem)
Let $r_1, \ldots, r_k \in \mathbb{Z}$ *and let* $0 \neq n_1, \cdots, n_k \in \mathbb{N}$ *such that the* n_i *are pairwise coprime. The system of equivalences*

$$\begin{aligned} X &\equiv r_1 \bmod n_1, \\ X &\equiv r_2 \bmod n_2, \\ &\vdots \\ X &\equiv r_k \bmod n_k, \end{aligned}$$

has a solution X *which is unique up to multiples of* $N = n_1 \cdot n_2 \cdots n_k$*. The set of all solutions is given by* $\{X + aN | a \in \mathbb{Z}\} = X + N\mathbb{Z}$*.*

Proof. To prove the theorem we state a homomorphism between $\mathbb{Z}/N\mathbb{Z}$ and the Cartesian product $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ and show it to be an isomorphism. That implies that every set of equations (right hand side of the map) has a unique preimage $X \in \mathbb{Z}/N\mathbb{Z}$.
Define $\psi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$; $X + N\mathbb{Z} \mapsto ((X \bmod n_1) + n_1\mathbb{Z}, (X \bmod n_2) + n_2\mathbb{Z}, \ldots, (X \bmod n_k) + n_k\mathbb{Z})$. The map ψ is homomorphic with respect to $+$ and to $\cdot$ since by Lemma 3.2.3 we have $X + Y \equiv (X \bmod n_i) + (Y \bmod n_i)$ and $X \cdot Y \equiv (X \bmod n_i) \cdot (Y \bmod n_i)$ and each n_i divides N.
The image and the domain have the same cardinality N and so the map is an isomorphism if it is injective. The kernel of ψ consists of those elements which

map to $(n_1\mathbb{Z}, n_2\mathbb{Z}, \ldots, n_k\mathbb{Z})$, which are exactly those $X + N\mathbb{Z}$ where X is divisible by $n_1, n_2, \ldots, n_k$. Since the n_i are coprime, X must be divisible by their product, i.e. by N, which implies $X \equiv 0 \bmod N$ and so ψ is an isomorphism. □

If the n_i are not all coprime the system might not have a solution at all. E.g. the system $X \equiv 1 \bmod 8$ and $X \equiv 2 \bmod 6$ does not have a solution since the first congruence implies that X is odd while the second one implies that X is even. If the system has a solution then it is unique only modulo $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$. E.g. the system $X \equiv 4 \bmod 8$ and $X \equiv 2 \bmod 6$ has solutions and the solutions are unique modulo 24. Replace $X \equiv 2 \bmod 6$ by $X \equiv 2 \bmod 3$; the system still carries the same information and we obtain $X = 8a + 4 \equiv 2a + 1 \overset{!}{\equiv} 2 \bmod 3$, thus $a \equiv 2 \bmod 3$ and $X = 8(3b + 2) + 4 = 24b + 20$. The smallest positive solution is thus 20.

We can now prove Lemma 3.2.9 which states that for $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_r^{e_r}$ with $p_1, p_2, \ldots, p_r$ distinct primes and positive exponents $e_1, e_2, \ldots, e_r \in \mathbb{Z}$ we have

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Proof. We first observe that the two expressions are equal as $p_i^{e_i} - p_i^{e_i - 1} = p_i^{e_i}(1 - 1/p_i)$ and $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_r^{e_r}$.
We prove the main result by induction on the number of prime factors r. For $r = 1$, i.e. $n = p_1^{e_1}$ a prime power, there are $p_1^{e_1} - p_1^{e_1 - 1}$ positive numbers coprime to n and $< n$ because there are $p_1^{e_1 - 1}$ multiples of p_1 in $\{0, 1, 2, \ldots, n - 1\}$.
By assumption we have $\varphi\left(p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_{r-1}^{e_{r-1}}\right) = \prod_{i=1}^{r-1} (p_i^{e_i} - p_i^{e_i - 1})$ and $\varphi\left(p_r^{e_r}\right) = p_r^{e_r} - p_r^{e_r - 1}$. Let $0 \le a < p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_{r-1}^{e_{r-1}}$ and $0 \le b < p_r^{e_r}$. The system of equations

$$\begin{aligned} X &\equiv a \bmod p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_{r-1}^{e_{r-1}}, \\ X &\equiv b \bmod p_r^{e_r}, \end{aligned}$$

has a unique solution $0 \le X < n$. So for each of the $\varphi\left(p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_{r-1}^{e_{r-1}}\right)$ values of a coprime to $p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_{r-1}^{e_{r-1}}$ and each of the $\varphi\left(p_r^{e_r}\right)$ values of b coprime to $p_r^{e_r}$ there is exactly one solution $0 \le X < n$ which shows that

$$\varphi(n) = \left(p_r^{e_r} - p_r^{e_r - 1}\right) \prod_{i=1}^{r-1} (p_i^{e_i} - p_i^{e_i - 1}) = \prod_{i=1}^{r} (p_i^{e_i} - p_i^{e_i - 1}).$$

□

Exercise 3.4.21 *a) The Gaussian integers $\mathbb{Z}[i]$ are a subset of the complex numbers, defined as*

$$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}.$$

We define addition and multiplication as in $\mathbb{C}$ *by*

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)i,\\ (a+bi)\cdot(c+di) &= (ac-bd)+(ad+bc)i.\end{aligned}$$

Show that $(\mathbb{Z}[i],+,\cdot)$ *is a commutative ring with unity.*

b) Let $(R,\circ,\diamond)$ *be a commutative ring with unity and let* $a,b\in R$, $n\in\mathbb{N}$. *Show that*

$$(a\circ b)^n=\sum_{i=0}^{n}\left[\binom{n}{i}\right]a^i b^{n-i},$$

where $[n]g = g\circ g\circ\cdots\circ g$ *(n-times), the binomial coefficients are as in Chapter 2, and the exponentiation* a^i *denotes the i fold product of a with itself:* $a^i = a\diamond a\diamond\cdots\diamond a$ *(i-times).*
Hint: Use induction on n.

c) Show that the set

$$\mathbb{C}[x,y]=\left\{\sum_{i=0}^{n}\sum_{j=0}^{m}a_{ij}x^i y^j\,\middle|\, a_{ij}\in\mathbb{C},n,m\in\mathbb{N}\right\}$$

is a ring with respect to the usual addition and multiplication.

d) Prove Lemma 3.4.10. Note that the proof is completely analogous to the considerations for the special case $(\mathbb{Z}/n\mathbb{Z})^\times$.

3.5 Further reading on rings

This section introduces ideals and subrings. These concepts are important in algebra and the proofs in the previous section could be stated more elegantly and in full generality using these notations but we decided to go for a more direct approach of proving results for special cases only. We include this section for the interested reader. The exercises are optional.
In Example 3.4.3 we considered the ring $n\mathbb{Z}$ which is a subset of $\mathbb{Z}$ and forms a ring with respect to the same operations. So we can define subrings analogously to subgroups. However, even more is true: we can multiply an element $an\in n\mathbb{Z}$ by *any* integer $b\in Z$ and obtain $an\cdot b=(ab)n$, a multiple of n. Subrings with this property are called *ideals*.
For simplicity and since all examples we encounter are commutative, we from now on work with commutative rings R.

Definition 3.5.1 (Subring, ideal)
Let $(R,\circ,\diamond)$ *be a ring and let* $R'\subseteq R$ *be a subset of* R. *If* $(R',\circ,\diamond)$ *is a ring then* R' *is a* subring of R.
Let $I\subseteq R$ *be a subset of the commutative ring* R. *If* I *is a subring of* R *and closed under* $\diamond$ *with arbitrary elements from* R, *i.e.* $I\diamond R\subseteq I$ *then* I *is called an* ideal of R.

Example 3.5.2 *1. Let $n \in \mathbb{N}$. The set $n\mathbb{Z}$ of multiples of n is a ring and thus a subring of $\mathbb{Z}$. Since $an \cdot b = (ab)n$ a multiple of n for arbitrary integers b, the set $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.*

2. Consider the ring of polynomials $\mathbb{C}[x]$ in x over $\mathbb{C}$ and the subset

$$x\mathbb{C}[x] = \left\{ x \sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{C}, n \in \mathbb{N} \right\}.$$

Sums and differences of such polynomials are of the same form

$$x \sum_{i=0}^{n} a_i x^i - x \sum_{i=0}^{m} b_i x^i = x \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i$$

and if we multiply a polynomial in $x\mathbb{C}[x]$ by an arbitrary one, the resulting polynomial is a multiple of x since

$$x \left(\sum_{i=0}^{n} a_{i+1} x^i \right) \cdot \left(\sum_{i=0}^{m} b_i x^i \right) = x \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i.$$

So $x\mathbb{C}[x]$ not only forms a subring of $\mathbb{C}[x]$ but even an ideal.

Ideals are an important concept particularly since they allow to generalize the concept of quotient groups to rings.

Definition 3.5.3 (Quotient ring)
Let $(R, \circ, \diamond)$ be a commutative ring and let I be an ideal of R. The quotient ring R/I of R modulo I *is defined as*

$$R/I = \{a \circ I | a \in R\}.$$

We have the analogue of Lemma 3.3.2 in the setting of rings:

Lemma 3.5.4 *Let $(R, \circ, \diamond)$ be a commutative ring and let I be an ideal in R. The quotient ring R/I is a commutative ring with respect to the following operations inherited from R:*

$$\begin{aligned} (a \circ I) \circ (b \circ I) &= (a \circ b) \circ I \\ (a \circ I) \diamond (b \circ I) &= (a \diamond b) \circ I. \end{aligned}$$

Proof. Since an ideal is in particular a subgroup with respect to the first operation $\circ$ we get from Lemma 3.3.2 that $(R/I, \circ)$ is a group. If R is abelian with respect to $\circ$ then so is R/I.
For the second operation we first need to show that the operation is well-defined. Let $a' \circ I = a \circ I$ and $b' \circ I = b \circ I$, i.e. there exist $i_a, i_b \in I$ so that $a' = a \circ i_a$ and $b' = b \circ i_b$. We have $(a' \circ I) \diamond (b' \circ I) = ((a \circ i_a) \circ I) \diamond ((b \circ i_b) \circ I) = (((a \circ i_a) \diamond (b \circ i_b))) \circ I = (a \diamond b) \circ (a \diamond i_b) \circ (i_a \diamond b) \circ (i_a \diamond i_b) \circ I = (a \diamond b) \circ I$ since $a \diamond i_b, i_a \diamond b, i_a \diamond i_b \in I$ by the definition of an ideal. So the resulting residue class is independent of the representatives chosen.
Since R is closed under $\diamond$ so is R/I and associativity, commutativity, and the distributive laws are inherited, too. □

Remark 3.5.5 *Note that this lemma does not hold if the conditions on I are released and only a subring is required.*
Let R' be a subring, then the operation $\diamond$ need not necessarily be well-defined on R/R' since we have no reason to assume that $a \diamond i_b$ and $i_a \diamond b$ (expressions from the proof of Lemma 3.5.4) are in R'. This is where the property that ideals are closed under $\diamond$ with arbitrary elements is crucial.

Example 3.5.6 *Since for any $n \in \mathbb{N}$ we have that $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$, Lemma 3.5.4 directly gives that $\mathbb{Z}/n\mathbb{Z}$ is a ring for any n.*

Definition 3.5.7 (Ring homomorphism)
Let $(R, \circ, \diamond)$ and $(R', \circ', \diamond')$ be rings and let ψ be a map $\psi : R \to R'$. If for any $a, b \in R$ the map ψ satisfies

$$\begin{aligned} \psi(a \circ b) &= \psi(a) \circ' \psi(b) \\ \psi(a \diamond b) &= \psi(a) \diamond' \psi(b) \end{aligned}$$

then ψ is a ring homomorphism.
A homomorphism ψ is an isomorphism *if it is bijective.*

Similar to the group case one can study the kernel and image of this map.

Theorem 3.5.8 *Let $(R, \circ, \diamond)$ and $(R', \circ', \diamond')$ be rings with unity and let ψ be a homomorphism. The kernel $\mathrm{Ker}(\psi)$ of ψ is an ideal in R and $\mathrm{Im}(\psi) \cong R/\mathrm{Ker}(\psi)$.*

Proof. Theorem 3.3.12 shows that $(\mathrm{Ker}(\psi), \circ)$ is a subgroup of $(R, \circ)$. Let $a \in \mathrm{Ker}(\psi)$, i.e. $\psi(a) = e_{\circ'}$. We have to show that for any $r \in R$ we have $r \diamond a \in \mathrm{Ker}(\psi)$:

$$\psi(r \diamond a) = \psi(r) \diamond' \psi(a) = \psi(r) \diamond' e_{\circ'} = e_{\circ'},$$

where the last result followed by Lemma 3.4.4. So $\mathrm{Ker}(\psi)$ is indeed an ideal.
To show the isomorphism the same construction as in Theorem 3.3.12 works. □

Remark 3.5.9 *A different way to motivate ideals is to start from the properties a ring homomorphisms should have and obtain, that the kernel of that map is not only a subring but has additional multiplicative structure.*

Definition 3.5.10 (Generator, principal ideal)
Let $(R, \circ, \diamond)$ be a commutative ring and let I be an ideal.
If there exist elements $g_1, \ldots, g_l$ such that

$$I = \{(g_1 \diamond r_1) \circ \cdots \circ (g_l \diamond r_l) | r_1, \ldots r_l \in R\}$$

then I is generated by $g_1, \ldots, g_l$ *written*

$$I = (g_1, \ldots, g_l).$$

If there exists a single element $g \in I$ such that

$$I = (g) = \{g \diamond r | r \in R\}$$

then I is called a principal ideal. *In this case, I is the ideal* generated by g *and g is called the* generator of I.
The ring R is called a principal ideal domain (PID) *if every ideal is a principal ideal.*

Lemma 3.5.11 *Let $(R, \circ, \diamond)$ be a commutative ring and let $g \in R$. The set $(g) = \{g \diamond r | r \in R\}$ forms an ideal in R.*
In more generality, let $g_1, \ldots, g_l \in R$. The set $(g_1, \ldots, g_l)$ is an ideal.

Proof. The proof is left to the reader as Exercise 3.5.14 a. □

Example 3.5.12 *1. Consider the ring of integers Z. We have seen that the subrings $n\mathbb{Z}$ for $n \in \mathbb{N}$ are ideals in $\mathbb{Z}$. This gives*

$$n\mathbb{Z} = \{nz | z \in \mathbb{Z}\} = (n),$$

and so $n\mathbb{Z}$ is a principal ideal generated by n.

We now show that every *ideal in $\mathbb{Z}$ is a principal ideal and thus $\mathbb{Z}$ is a principal ideal domain. We have to distinguish two cases, $I = \{0\} = (0)$ which is generated by 0 and $I \neq \{0\}$.*

Let $g \in I$ be the smallest positive integer in I. We now show that $I = (g)$. Since I is an ideal all multiples of g are in I and thus $I \supseteq (g)$. Assume that there is an element $b \in I \backslash (g)$. Then we can divide b by g with remainder $0 < r < g$ and obtain $b = qg + r$. Since b and qg are in I so is $r = b - qg$ by the definition of ideals. This contradicts the minimality of g.

So $\mathbb{Z}$ is a principal ideal domain.

2. *The Gaussian integers $\mathbb{Z}[i] \subset \mathbb{C}$ are a principal ideal domain. As for the integers we can define greatest common divisors and the proof follows along the same lines.*

3. *The set*
$$\mathbb{C}[x,y] = \left\{ \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j \mid a_{ij} \in \mathbb{C}, n, m \in \mathbb{N} \right\}$$
is a ring, the polynomial ring in two variables (cf. Exercise 3.4.21 c). The ideal (x,y) generated by x and y is not a principal ideal. Assume on the contrary that there exists some $f(x,y) \in \mathbb{C}[x,y]$ such that $(f) = (x,y)$, so in particular there must exist f_x and f_y such that $x = f_x \cdot f$ and $y = f_y \cdot f$. The first condition limits f to constants $f \in \mathbb{C}$ or constant multiples of x, i.e. $f \in x\mathbb{C}$, while the second condition eliminates the latter possibility. So $f \in \mathbb{C}$ but since (x,y) does not contain any constant except for 0 we must have $f = 0$ which contradicts that f can generate a non-trivial ideal.

In the previous section we showed the Chinese remainder theorem for the integers. Now that we have the vocabulary of quotient rings and homomorphisms we can state the general version.

Theorem 3.5.13 (Chinese Remainder Theorem)
Let R be a Euclidean domain and let $n_1, \ldots, n_k \in R$ be pairwise coprime. Let $n = n_1 \diamond n_2 \diamond \cdots \diamond n_k$. The quotient ring R/nR and the product ring $R/n_1R \times R/n_2R \times \cdots \times R/n_kR$ are isomorphic via the map

$$\psi : R/nR \to (R/n_1R \times \cdots \times R/n_kR);\ \psi(x \circ nR) = (x \circ n_1R, \ldots, x \circ n_kR).$$

Proof. The proof is similar to the integer case. We first note that ψ is a homomorphism since $\circ$ and $\diamond$ are compatible with computing modulo principal ideals.
For the integers we could argue with the cardinalities of the domain and image. In the general case it is easier to give the inverse map to show that ψ is an isomorphism. Let l_i be defined by $l_i \diamond n_i = n$. Since l_i and n_i are coprime, Bézout's identity (Lemma 3.4.16) says that there exist elements $a_i, b_i \in R$ such that $a_i \diamond l_i \circ b_i \diamond n_i = e_\diamond$. Put $c_i = a_i \diamond l_i$. The inverse map is given by

$$\psi^{-1} : (R/n_1R \times \cdots \times R/n_kR) \to R/nR;\ (x_1 \circ n_1R, \ldots, x_k \circ n_kR) \mapsto \left(\sum_{i=1}^{k} x_i \diamond c_i \right) \circ nR,$$

where the summation sign stands for repeated application of $\circ$. To see that ψ^{-1} is well defined note that $((x_i \circ (n_i \diamond r_i)) \diamond c_i) \circ nR = ((x_i \diamond c_i) \circ ((n_i \diamond r_i) \diamond c_i)) \circ nR = ((x_i \diamond c_i) \circ ((n_i \diamond r_i) \diamond (a_i \diamond l_i))) \circ nR = (x_i \diamond c_i) \circ nR$ since $(n_i \diamond r_i) \diamond (a_i \diamond l_i) = (n_i \diamond l_i) \diamond (a_i \diamond r_i)$ is a multiple of n.
We have

$$\psi(\psi^{-1}(x \circ n_1R, \ldots, x \circ n_kR)) = \psi\left(\left(\sum_{i=1}^{k} x_i \diamond c_i \right) \circ nR \right) = (x \circ n_1R, \ldots, x \circ n_kR),$$

since for every $1 \leq j \leq k$ we have $\left(\sum_{i=1}^{k} x_i \diamond c_i\right) \circ n_j R = \left(\sum_{i=1}^{k} x_i \diamond (a_i \diamond l_i)\right) \circ n_j R = x_j \diamond (a_j \diamond l_j) \circ n_j R = x_j \diamond e_\diamond \circ n_j R = x_j \circ n_j R$. Here we used that $l_i \in n_j R$ for $i \neq j$.
Likewise we have

$$\begin{aligned} \psi^{-1}(\psi(x \circ nR)) &= \psi^{-1}(x \circ n_1 R, \ldots, x \circ n_k R) = \left(\sum_{i=1}^{k} (x \circ (n_i \diamond r_i)) \diamond c_i\right) \circ nR \\ &= \left(\sum_{i=1}^{k} ((x \diamond c_i) \circ ((n_i \diamond r_i) \diamond (a_i \diamond l_i)))\right) \circ nR = x \sum_{i=1}^{k} c_i \circ nR. \end{aligned}$$

To show that $\sum_{i=1}^{k} c_i \circ nR = e_\diamond \circ nR$ we show that $n \left| \left(\left(\sum_{i=1}^{k} c_i\right) \circ \mathrm{inv}_\circ(e_\diamond)\right)\right.$. By definition of $c_i = a_i \diamond l_i$ we have for every factor n_j of n that $n_j | a_i \diamond l_i$ for $i \neq j$ and $n_j | a_j \diamond l_j \circ \mathrm{inv}_\circ(e_\diamond)$. So for every $1 \leq j \leq k$ we have $n_j \left| \left(\left(\sum_{i=1}^{k} c_i\right) \circ \mathrm{inv}_\circ(e_\diamond)\right)\right.$. Since the n_j are co-prime the claim follows from Lemma 3.4.18. □

Exercise 3.5.14 *a) Prove Lemma 3.5.11.*

3.6 Fields

Fields are special rings in which also the second operation $\diamond$ is commutative and in which every element $\neq e_\circ$ has an inverse with respect to $\diamond$. Familiar examples are the rational numbers, the reals and the complex numbers. This section is kept very short since most of the concepts are only needed for finite fields with are studied separately in Chapter 5.

Definition 3.6.1 (Field)
A set K is a field *with respect to two operations $\circ, \diamond$ denoted by $(K, \circ, \diamond)$ if*

1. *$(K, \circ)$ is an abelian group.*
2. *$(K^*, \diamond)$ is an abelian group, where $K^* = K \backslash \{e_\circ\}$ is all of K except for the neutral element with respect to $\circ$.*
3. *The distributive law holds in K:*

$$a \diamond (b \circ c) = a \diamond b \circ a \diamond c \text{ for all } a, b, c \in K.$$

Let L be a field and $K \subseteq L$. If K is a field itself it is a subfield of L *and L is an* extension field of K.

An alternative definition is to say that a field is a commutative ring with unity in which every element in K^* has an inverse with respect to $\diamond$.
We start with an easy but important observation

Lemma 3.6.2 *Let $(K, \circ, \diamond)$ be a field and let $e_\circ$ be the neutral element with respect to $\circ$.*
For any $a \in K$ we have:

$$a \diamond e_\circ = e_\circ.$$

Fields are free of zero divisors, i.e. if for $a, b \in K$ one has $a \diamond b = e_\circ$ then either $a = e_\circ$ or $b = e_\circ$ or both.

Proof. The first part was shown already in Lemma 3.4.4. To prove the second part assume $a \neq e_\circ$. Thus $a \in K^*$ has an inverse $\mathrm{inv}_\diamond(a) \neq e_\circ$ since K^* is closed under $\diamond$. So we get:

$$\begin{aligned} e_\circ &= \mathrm{inv}_\diamond(a) \diamond (a \diamond b) \\ &= (\mathrm{inv}_\diamond(a) \diamond a) \diamond b = b, \end{aligned}$$

i.e. $e_\circ = b$. □

Example 3.6.3

1. *The rational numbers $(\mathbb{Q}, +, \cdot)$ form a field. We have already seen that they form a commutative ring with unity so the only thing to show is that in $(\mathbb{Q}^*, \cdot)$ every element has an inverse. By the very construction of the rationals the inverse of $0 \neq \frac{a}{b}$ is given by $\frac{b}{a}$ since $\frac{a}{b} \cdot \frac{b}{a} = 1$. If $a \neq 0$ then the inverse exists and since 0 is the neutral element of addition it is not in $\mathbb{Q}^*$.*

2. *Further fields are $(\mathbb{C}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$, where $\mathbb{R}$ is an extension field of $\mathbb{Q}$ and a subfield of $\mathbb{C}$ while $\mathbb{C}$ is an extension field of both.*

3. *The integers form a commutative ring with unity but not a field since only 1 and -1 are invertible.*

4. *Let $p \in \mathbb{N}$ be a prime number. The set of residue classes modulo p $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field:*
   We have seen that $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with unity for any integer n. By Lemma 3.2.6 we have that the invertible elements $a + p\mathbb{Z}$ are exactly those classes for which a is coprime to p. Since p is prime these are all nonzero classes, so $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ and so $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field.

   This is the first example of a finite field. *We will study finite fields in much more detail in Chapter 5.*

For those readers who read the previous section on ideals we would like to add the following lemma.

Lemma 3.6.4 *Let $(K, \circ, \diamond)$ be a field and let $I \subset K$ be an ideal. Then $I = K$ or $I = \{e_\circ\}$.*

Proof. We first note that a field is also a ring, so speaking of an ideal makes sense. Let us first consider the case that there is an element $a \neq e_\circ$ in I. Since K is a field there exists $\text{inv}_\diamond(a) \in K$ and by the multiplicative property of ideals we must have $a \diamond \text{inv}_\diamond(a) = e_\diamond \in I$. Again by the multiplicative property every $b \in K$ is also in I as $e_\diamond \diamond b = b$, so $I = K$.
We have seen earlier that $I = \{e_\circ\}$ is an ideal for any ring with unity, so this also holds for a field. □

Exercise 3.6.5 *Consider the subset $\mathbb{Q}(i) \subset \mathbb{C}$ defined by*

$$\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}.$$

Show that $(\mathbb{Q}(i), +, \cdot)$ is a field, where addition and multiplication are defined as in $\mathbb{C}$.

3.7 Polynomials

Polynomials become very important in the construction of finite fields in the following chapter. They are also a nice example of a ring and share many properties with the ring of integers.

Definition 3.7.1 (Polynomial)
Let K be a field. A polynomial in one variable x over K *is a finite sum of powers of x with* coefficients f_i *in the field K*

$$f(x) = \sum_{i=0}^{n} f_i x^i, \ f_i \in K.$$

We denote the set of polynomials in x over K by $K[x]$ and have

$$K[x] = \left\{ \sum_{i=0}^{n} f_i x^i | n \in \mathbb{N}, f_i \in K \right\}.$$

Example 3.7.2 *$f(x) = 3x^7 + \sqrt{2}x^4 - 27x^3 + 2x + 100$ and $g(x) = 1024x^{10} + 256x^8 + 32x^5 + 16x^4 + 4x^2 + 1$ are polynomials over the reals $f(x), g(x) \in \mathbb{R}[x]$. Instead of calling the variable x one can also define $K[y]$ or $K[t]$, e.g. $h(t) = 23t^{12} - 4t + 3 \in \mathbb{Q}[t]$.*

Note that $\sum_{i=0}^{n} f_i x^i$ and $0 \cdot x^{n+1} + \sum_{i=0}^{n} f_i x^i$ define the same polynomial just as one can also write 0127 instead of 127. It would be more correct to introduce polynomials as equivalence classes which can be filled up with leading zeros. We usually omit leading zeros.

Definition 3.7.3 (Degree and leading term)
Let $f \in K[x]$ be a nonzero polynomial over a field K. Let n be the largest integer with $f_n \neq 0$, then n is called the degree of f, *denoted by* $\deg(f) = n$, *and f_n is called the* leading coefficient of f, *denoted by $LC(f) = f_n$. The* leading term of f *is $LT(f) = f_n x^n$.*
A polynomial f is called monic *if $LC(f) = 1$.*

All the definitions carry through for the case that the coefficients are from a ring R rather than from a field K. However, if K is a field one can normalize each polynomial to make it monic by dividing by $LC(f)$. Over a ring the leading term need not be invertible.

Example 3.7.4 *Consider $f, g \in \mathbb{R}[x]$ as defined in Example 3.7.2. We have*

$$f(x) = 3x^7 + \sqrt{2}x^4 - 27x^3 + 2x + 100, \deg(f) = 7, LC(f) = 3$$

and

$$g(x) = 1024x^{10} + 256x^8 + 32x^5 + 16x^4 + 4x^2 + 1, \deg(g) = 10, LC(g) = 1024.$$

Lemma 3.7.5 *Let $(K, +, \cdot)$ be a field. The polynomials $K[x]$ form a ring with the operations*

$$\begin{aligned} f(x) + g(x) = \sum_{i=0}^{n} f_i x^i + \sum_{i=0}^{m} g_i x^i &= \sum_{i=0}^{\max\{n,m\}} (f_i + g_i) x^i, \\ f(x) \cdot g(x) = \sum_{i=0}^{n} f_i x^i \cdot \sum_{i=0}^{m} g_i x^i &= \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} f_j g_{i-j} \right) x^i, \end{aligned}$$

where $f, g \in K[x]$ and $f_i = 0$ for $i > n$ and $g_i = 0$ for $i > m$.
Furthermore, multiplication in $K[x]$ is commutative and $K[x]$ is a ring with unity, namely $1 \in K \subset K[x]$ is the neutral element with respect to multiplication. There are no zero divisors in $K[x]$.

Proof. Obviously the results are sums of powers of x of finite lengths ($\max\{n, m\}$ and $n + m$). Since K is a field, the new coefficients $(f_i + g_i)$ and $\sum_{j=0}^{i} f_j g_{i-j}$ are in K as well. So $K[x]$ is closed under addition and multiplication.
Associativity and commutativity of $+$ and $\cdot$ follow from the same properties of K. The neutral element of addition is $0 \in K \subset K[x]$ and of multiplication $1 \in K \subset K[x]$ as can be seen directly.
The additive inverse of $f(x) = \sum_{i=0}^{n} f_i x^i$ is $-f(x) = \sum_{i=0}^{n} (-f_i) x^i$ which is in $K[x]$ since $-f_i \in K$ for $0 \leq i \leq n$.
The distributive laws can be checked by direct inspection. We leave that part of the proof as an exercise to the reader.
Let $f(x) \cdot g(x) = 0$, i.e. $\sum_{j=0}^{i} f_j g_{i-j} = 0$ for all $0 \leq i \leq m + n$. Since K is a field we obtain for $i = 0$ that either $g_0 = 0$ or $f_0 = 0$ or both. Assume first $f_0 = 0$ and

$g_0 \neq 0$. For $i = 1$ we obtain that $f_0g_1 + f_1g_0 = f_1g_0 = 0$ and so $f_1 = 0$. For $i = 2$ we obtain that $f_0g_2 + f_1g_1 + f_2g_0 = f_2g_0 = 0$ and so $f_2 = 0$. Repeating the same argument leads to $f(x) = 0$. If both $f_0 = g_0 = 0$ then $i = 1$ does not lead to any condition on f_1 or g_1. For $i = 2$ we obtain that $f_0g_2 + f_1g_1 + f_2g_0 = f_1g_1 = 0$ and so either $f_1 = 0$ or $g_1 = 0$ or both. Eventually we obtain $f(x) = 0$ or $g(x) = 0$ or both, so there are no zero divisors in $K[x]$. □

Example 3.7.6 *With $f, g \in \mathbb{R}[x]$ as in Example 3.7.2 we have*

$$f(x)+g(x) = 1024x^{10}+256x^8+3x^7+32x^5+(16+\sqrt{2})x^4-27x^3+4x^2+2x+101.$$

and

$$\begin{aligned} f(x)\cdot g(x) \;=\; & 3072x^{17} + 768x^{15} + 1024\sqrt{2}x^{14} - 27648x^{13} + (96 + 256\sqrt{2})x^{12} - 4816x^{11} + \\ & 102400x^{10} + (524 + 32\sqrt{2})x^9 + (24736 + 16\sqrt{2})x^8 - 429x^7 + (64 + 4\sqrt{2})x^6 + \\ & 3124x^5 + (1600 + \sqrt{2})x^4 - 19x^3 + 400x^2 - 2x + 100. \end{aligned}$$

Definition 3.7.7 (Roots)
One can consider a polynomial $f(x) = \sum_{i=0}^{n} f_i x^i \in K[x]$ as a function

$$f : K \to K, \alpha \mapsto f(\alpha) = \sum_{i=0}^{n} f_i \alpha^i.$$

Computing $f(\alpha)$ is called evaluating $f(x)$ in $x = \alpha$.
A root of f *is an element $\alpha \in K$ such that $f(\alpha) = 0$. So the roots form the kernel of the map f defined above.*

Lemma 3.7.8 *Let $f \in K[x]$. If $\alpha \in K$ is a root of f then*

$$(x - \alpha) | f(x).$$

The proof is left to the reader as Exercise 3.7.17. An immediate consequence of this lemma is the following corollary.

Corollary 3.7.9 *Let $f \in K[x]$ be a polynomial of degree n. It has at most n roots.*

Sometimes it is helpful to change the variables in a reversible way, e.g. in the polynomial $g(x)$ in Example 3.7.2 one can substitute $y = 2x$ and obtain $\tilde{g}(y) = y^{10} + y^8 + y^5 + y^4 + y^2 + 1$. A transformation of the form $y = ax + b$ does not change the degree and there is a simple linear relation between the roots of the original and the resulting polynomial. In this example the relation between g and $\tilde{g}$ is particularly simple.

There are many similarities between the ring of integers and the ring of polynomials over a field, in particular we find "primes" and show that each polynomial can be factored uniquely into a product of them. These so-called "irreducible polynomials" play an important role in constructing finite fields as we will see in Chapter 5.

Definition 3.7.10 (Irreducible polynomial)
Let K be a field. A polynomial $f(x) \in K[x]$ of degree at least 1 is irreducible *if it cannot be written as a product of polynomials of lower degree over the same field, i.e. if $u(x)|f(x)$ implies u is constant or $u(x) = f(x)$.*
Otherwise $f(x)$ is reducible.

Example 3.7.11 *Consider polynomials over the rational numbers $\mathbb{Q}$.*

a) $f(x) = x^2+2x-8$ has roots 2 and -4 and thus splits as $f(x) = (x-2)(x+4)$. The factors $x-2$ and $x+4$ are both irreducible.

b) $g(x) = x^2 + 2x + 8$ does not split over $\mathbb{Q}$ but only over $\mathbb{C}$. Therefore, g is irreducible as polynomial in $\mathbb{Q}[x]$.

c) $h(x) = x^4 + 4x^3 + 20x^2 + 32x + 64$ does not have a root over $\mathbb{Q}$ but factors into $x^4 + 4x^3 + 20x^2 + 32x + 64 = (x^2 + 2x + 8)^2 = g(x)^2$.

Note that for a polynomial of degree less than 4 it is enough to check for roots to determine whether it is irreducible or not. For polynomials of larger degree there can be non-linear factors as in the last example.
A prominent example of Euclidean domains is the ring of integers which, as we mentioned in the introduction, shares many properties with the ring of polynomials over a field. We now show that the polynomial ring is also a Euclidean domain. That means that one can define division with remainder and has an algorithm to compute greatest common divisors, namely the Euclidean algorithm.

Lemma 3.7.12 *Let K be a field. The ring of polynomials over K is a Euclidean domain with respect to the degree function $v(f) = \deg(f)$, i.e. $K[x]$ is a ring with unity and without zero divisors, $\cdot$ is commutative and one can define division with remainder so that the remainder has smaller degree than the divisor or equals 0.*

Proof. We have already seen in Lemma 3.7.5 that $K[x]$ is a domain with unity 1 and that $\cdot$ is commutative. Consider the division with remainder of f by g, where both $f, g \in K[x]$. Let $r \in K[x]$ be the remainder. Let the leading term of f be $LT(f) = ax^n$ and of g be $LT(g) = bx^m$. If $n < m$ then $r = f$ is the remainder and obviously $\deg(r) < \deg(g)$. Otherwise there exists a polynomial $q \in K[x]$ with $LT(q) = (a/b)x^{n-m}$ (note that a/b is defined since $a, b \in K \setminus \{0\}$) such that f splits as $f = q \cdot g + r$. The coefficient of x^n in r equals $a - (a/b) \cdot b = 0$ and so the degree of r is strictly smaller than n. Clearly it is possible that more coefficients in r vanish and the degree drops dramatically, for example if $g|f$ then $r = 0$. □

This lemma implies in particular that greatest common divisors are defined and computable via the Euclidean algorithm.
As in the integers $\mathbb{Z}$ we have that in $K[x]$ irreducible is the same as prime.

Lemma 3.7.13 *Let $p, f, g \in K[x]$ and let p be irreducible. Then one has*

$$p|f \cdot g \Rightarrow p|f \text{ or } p|g.$$

Proof. Let $d = \gcd(p, f)$, then $d|p$. Since p is irreducible, we must have $d = 1$ or $d = p$, where we use the convention that the gcd is monic.
If $d = p$ then $p|f$ by the definition of gcd. So $p|f$ and we are done.
In case $d = 1$ we use Lemma 3.4.16 and know that there exist $u, v \in K[x]$ with $d = 1 = u \cdot p + v \cdot f$. Multiplying both sides by g gives the expression

$$g = u \cdot p \cdot g + v \cdot f \cdot g.$$

Both summands on the right are divisible by p. For the second one note that by assumption $p|f \cdot g$. Thus also the left hand side must be divisible by p and thus $p|g$. □

We are used to factoring integers $n \in \mathbb{Z}$ into powers of primes in a unique manner. The following lemma shows that the ring of polynomials over a field has the same property of unique factorization that every non-zero element can be written as a product of irreducible elements.

Lemma 3.7.14 *For all $f \in K[x]$ there exist monic irreducible polynomials $p_1, \ldots, p_r \in K[x]$ all distinct and exponents $e_1, \ldots, e_r \in \mathbb{N}$ so that f can be written as*

$$f = k \prod_{i=1}^{r} p_i^{e_i},$$

where $k \in K$.

Proof. We first show that such a representation exists and then consider uniqueness.
There are two cases, either f itself is irreducible, in which case we put $p_1 = f/LC(f)$ and $k = LC(f)$, or it splits as $f = a \cdot b$ with $\deg(a), \deg(b) < \deg(f)$ and we continue separately with $f = a$ and $f = b$. In the latter case both parts have strictly smaller degree than f which means that this process terminates with *some* factorization into irreducible polynomials

$$f = k \prod p_i^{e_i}.$$

We now assume that the representation is not unique, i.e. there exist monic irreducible polynomials $q_1, \ldots, q_s \in K[x]$, exponents $a_1, \ldots, a_s \in \mathbb{N}$, and a field element $l \in K$ so that f can be written as

$$f = k \prod_{i=1}^{r} p_i^{e_i} = l \prod_{j=1}^{s} q_j^{a_j}.$$

The irreducible polynomial p_1 must divide one of the polynomials on the right hand side by Lemma 3.7.13. So there is some q_j with $p_1|q_j$. Since q_j is also irreducible they must be equal up to constants from K and since both are monic we even have $p_1 = q_j$. The left side is divisible by $p_1^{e_1}$ and so must be the right hand side. Since the q_j are all distinct we must have $e_1 \leq a_j$. By reversing the

arguments we obtain the opposite inclusion and thus $e_1 = a_j$. We divide both sides by $p_1^{e_1}$ and repeat the same considerations for p_2.
Since the exponents coincide we must have $r = s$ which concludes the proof. □

Remark 3.7.15 *It is worth mentioning that the property of having unique factorization is weaker than being Euclidean. In fact every Euclidean ring has unique factorization. Since we did not show the general statement we had to prove the result in the special case of polynomial rings.*

Example 3.7.16 *Let $K = \mathbb{Z}/2\mathbb{Z}$ be the field of integers modulo 2. We consider the residue classes of $K[x]$ modulo $f(x) = x^n + 1$ for some integer n, $R = K[x]/(x^n + 1)K[x]$. In this important example we show that R is a commutative ring with unity.*
We represent each residue class in R by the polynomial of smallest degree in it

$$R = \left\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \mid a_i \in K \right\}.$$

1. *$(K[x]/fK[x], +)$ is a group: obviously it is closed under addition, associativity is inherited from $K[x]$, the neutral element is $0 + fK[x]$, and additive inverses exist* $\operatorname{inv}\left(\left(\sum_{i=0}^{n-1} a_i x^i\right) + fK[x]\right) = \left(\sum_{i=0}^{n-1} (-a_i)\, x^i\right) + fK[x]$.

2. *$(K[x]/fK[x], \cdot)$ is a commutative monoid with 1: the product of two classes is another class, associativity is inherited from $K[x]$, and the neutral element with respect to multiplication is $1 + fK[x]$.*

3. *The distributive laws are inherited from $K[x]$.*

The same proof works for any field K and any polynomial f.

Exercise 3.7.17 *Prove Lemma 3.7.8. Hint: divide $f(x)$ by $x - \alpha$ and study the remainder.*

3.8 Vector spaces

The last algebraic concept we introduce in this chapter is one that most readers will be familiar with from introductory courses on linear algebra and solving of linear equations. Vector spaces also appear in daily life since we are living in a three dimensional space and thus positions can be specified by giving the height and extensions in width and length.

Definition 3.8.1 (Vector space)
A set V is a vector space *over a field $(K, \circ, \diamond)$ with respect to one operation $\oplus$ if*

1. *$(V, \oplus)$ is an abelian group.*

2. *There exists an operation* $\odot : K \times V \to V$ *such that for all* $a, b \in K$ *and for all* $\underline{v}, \underline{w} \in V$ *we have*

$$\begin{aligned} (a \circ b) \odot \underline{v} &= a \odot \underline{v} \oplus b \odot \underline{v} \\ a \odot (\underline{v} \oplus \underline{w}) &= a \odot \underline{v} \oplus a \odot \underline{w} \\ e_\diamond \odot \underline{v} &= \underline{v}, \end{aligned}$$

where $e_\diamond$ *is the neutral element with respect to* $\diamond$.

Example 3.8.2 *Consider the field* $(\mathbb{R}, +, \cdot)$ *and define an operation on the* 3*-tuples* $(x, y, z) \in \mathbb{R}^3$ *by componentwise addition*

$$(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$$

and for $a \in \mathbb{R}$ *let*

$$a \odot (x_1, y_1, z_1) = (ax_1, ay_1, az_1).$$

Since $\mathbb{R}$ *is closed under addition and multiplication and since the distributive laws hold we have that* $\mathbb{R}^3$ *forms a vector space over* $\mathbb{R}$ *with these operations.*
The same holds for $\mathbb{R}^n$ *for any integer* n.
To ease notation we replace $\oplus$ *by* $+$ *and omit* $\odot$ *in* $\mathbb{R}^n$.

Example 3.8.3 *The complex numbers* $\mathbb{C}$ *form a vector space over the reals* $(\mathbb{R}, +, \cdot)$ *where the operations are defined as follows:*
$\oplus$ *is the standard addition of complex numbers, i.e.*

$$(a + bi) \oplus (c + di) = (a + c) + (b + d)i,$$

and $\odot$ *is the standard multiplication, i.e.*

$$a \odot (b + ci) = (a \cdot b) + (a \cdot c)i,$$

in which the first argument is restricted to $\mathbb{R}$.
This fulfills the definition since we have already seen that $(\mathbb{R}, +, \cdot)$ *and* $(\mathbb{C}, +, \cdot)$ *are both fields. The last three conditions are automatically satisfied since* $\mathbb{C}$ *is a field.*

The previous section dealt extensively with polynomials. They are also a good example of vector spaces.

Example 3.8.4 *Let* K *be a field and consider the polynomial ring* $K[x]$ *over* K.
We define $\oplus$ *to be the coefficientwise addition, i.e. the usual addition in* $K[x]$ *and* $\odot$ *as the multiplication of each coefficient by a scalar from* K*, i.e. polynomial multiplication restricted to the case that one input polynomial is constant.*
Since $K[x]$ *forms a ring and* K *is a field,* $K[x]$ *also forms a vector space over* K.

Example 3.8.5 *Let K be a field, $n \in \mathbb{N}$ and consider the subset P_n of $K[x]$ defined by*

$$P_n = \{f(x) \in K[x] | \deg(f) \leq n\}.$$

Since addition of polynomials and multiplication by constants do not increase the degree, P_n is closed under addition and multiplication by scalars from K and is thus a vector space over K.

The example of $\mathbb{C}$ being a vector space over $\mathbb{R}$ can be generalized to arbitrary extension fields.

Example 3.8.6 *Let $(K, \circ, \diamond)$ be a field and let $L \supseteq K$ be an extension field of K. Then L is a vector space over K, where $\oplus = \circ$ and $\odot = \diamond$.*

Definition 3.8.7 (Linear combination, basis, dimension)
Let V be a vector space over the field K and let $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n \in V$.
A linear combination *of the vectors $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ is given by*

$$\sum_{i=1}^{n} \lambda_i \odot \underline{v}_i,$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$, where the summation sign stands for repeated application of $\oplus$.
The elements $\underline{v}_1, \ldots, \underline{v}_n$ are linearly independent *if $\sum_{i=1}^{n} \lambda_i \odot \underline{v}_i = e_\oplus$ implies that for all $1 \leq i \leq n$ we have $\lambda_i = e_\circ$.*
A set $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$ is a basis of V *if $\underline{v}_1, \ldots, \underline{v}_n$ are linearly independent and each element can be represented as a linear combination of them, i.e.*

$$V = \left\{ \sum_{i=1}^{n} \lambda_i \odot \underline{v}_i \mid \lambda_i \in K \right\}.$$

The cardinality of the basis is the dimension of V*, denoted by* $\dim_K(V)$.

An alternative definition of basis are that $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n\}$ is a minimal set of generators, meaning that there are no fewer elements of V such that each element can be represented as a linear combination of them.
Yet another definition states that a basis is a maximal set of linearly independent vectors.

Example 3.8.8 *Consider the vector space $\mathbb{R}^3$. The vectors $(1,0,0)$ and $(0,1,0)$ are linearly independent since*

$$\lambda_1(1,0,0) + \lambda_2(0,1,0) = (\lambda_1, \lambda_2, 0) \stackrel{!}{=} (0,0,0)$$

forces $\lambda_1 = \lambda_2 = 0$. They do not form a basis since, e.g., the vector $(0,0,3)$ cannot be represented as a linear combination of them.
Since $2(1,0,0) = (2,0,0)$ the vectors $(1,0,0)$ and $(2,0,0)$ are linearly dependent.

The vectors $(1,0,0),(0,1,0)$*, and* $(1,3,0)$ *are linearly dependent since a non-trivial linear combination is given by*

$$(1,0,0)+3(0,1,0)-(1,3,0)=(0,0,0).$$

The vectors $(1,0,0),(0,1,0)$*, and* $(0,0,1)$ *are linearly independent and every other vector* $(x,y,z)\in\mathbb{R}^3$ *can be represented as a linear combination of them as*

$$(x,y,z)=x(1,0,0)+y(0,1,0)+z(0,0,1).$$

So we have that a basis of $\mathbb{R}^3$ *is given by* $\{(1,0,0),(0,1,0),(0,0,1)\}$ *and that the dimension is* $\dim_{\mathbf{R}}(\mathbb{R}^3)=3$.
In general $\dim_{\mathbf{R}}(\mathbb{R}^n)=n$.

Example 3.8.9 *We have already seen that the complex numbers form a vector space over the reals. A basis is given by* $\{1,i\}$ *and so the dimension is* $\dim_{\mathbf{R}}(\mathbb{C})=2$.

Example 3.8.10 *Let* K *be a field and let* $P_n\subset K[x]$ *be the set of polynomials of degree at most* n*. A basis is given by* $\{1,x,x^2,x^3,\ldots,x^n\}$ *and so the dimension is* $\dim_K(P_n)=n+1$.
Alternative bases are easy to give. Since K *is a field,* x^i *can be replaced by* a_ix^i *for any nonzero* $a_i\in K$*, also linear combinations are possible. So another basis is given by* $\{5,3x-1,-x^2,2x^3+x,\ldots,x^n+x^{n-1}+x^{n-2}+\cdots+x+1\}$*, since the degrees are all different and so none can be a linear combination of the others, while using linear algebra we can get every element as a linear combination.*

Definition 3.8.11 (Subspace)
Let V *be a vector space over the field* K*. A subset* $W\subseteq V$ *is a* subspace *if* W *is a vector space with respect to the same operations.*

Vector spaces will be an important tool in constructing finite fields. Our interest in their general properties is, however, rather limited. We state some results on fields that need the definition of vector spaces.

Definition 3.8.12 (Extension degree)
Let L *be a field and let* K *be a subfield of* L*. The* extension degree *of* L *over* K *is defined as* $[L:K]=\dim_K(L)$.
If $\dim_K(L)$ *is finite,* L *is a* finite extension of K*. Otherwise* L *is a* infinite extension of K.

Lemma 3.8.13 *Let* L *be a finite extension field of* K *and let* F *be a finite extension field of* L*, so* $K\subseteq L\subseteq F$*. Then*

$$[F:K]=[F:L]\cdot[L:K].$$

Let $[F:L]=n$ *and* $[L:K]=m$*. Let* $f_1,f_2,\ldots,f_n$ *be a basis of* F *over* L *and* $l_1,l_2,\ldots,l_m$ *be a basis of* L *over* K*. A basis of* F *over* K *is given by*

$$\{l_1\diamond f_1,l_2\diamond f_1,\ldots,l_m\diamond f_1,l_1\diamond f_2,l_2\diamond f_2,\ldots,l_m\diamond f_2,\ldots,l_1\diamond f_n,l_2\diamond f_n,\ldots,l_m\diamond f_n\}.$$

Proof. Once we have proved the second claim the first one follows automatically since the basis has $\dim_K(F) = nm = \dim_L(F)\dim_K(L)$ elements.
We first show that every element of F can be represented by a K-linear combination of $l_1 \diamond f_1, l_2 \diamond f_1, \ldots, l_m \diamond f_1, l_1 \diamond f_2, l_2 \diamond f_2, \ldots, l_m \diamond f_2, \ldots, l_1 \diamond f_n, l_2 \diamond f_n, \ldots, l_m \diamond f_n$. Since $f_1, f_2, \ldots, f_n$ is a basis of F over L, for every element $f \in F$ there exist $c_1, c_2, \ldots, c_n \in L$ so that $f = \sum_{i=1}^{n} c_i \diamond f_i$. Likewise every $c_i \in L$ can be written as a K-linear combination of $l_1, l_2, \ldots, l_m$ as $c_i = \sum_{j=1}^{m} d_{ij} \diamond l_j$ with coefficients $d_{ij} \in K$. So

$$f = \sum_{i=1}^{n} c_i \diamond f_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} d_{ij} \diamond l_j \right) \diamond f_i = \sum_{i=1}^{n} \sum_{j=1}^{m} d_{ij} \diamond (l_j \diamond f_i).$$

Assume now that $l_1 \diamond f_1, l_2 \diamond f_1, \ldots, l_m \diamond f_1, l_1 \diamond f_2, l_2 \diamond f_2, \ldots, l_m \diamond f_2, \ldots, l_1 \diamond f_n, l_2 \diamond f_n, \ldots, l_m \diamond f_n$ are linear dependent, i.e. there exist a nontrivial linear combination

$$\sum_{i=1}^{n} \sum_{j=1}^{m} d_{ij} \diamond (l_j \diamond f_i) = e_\circ$$

and not all $d_{ij} = e_\circ$. Put $c_i = \sum_{j=1}^{m} d_{ij} \diamond l_j$ then $\sum_{i=1}^{n} c_i \diamond f_i = e_\circ$. Since the f_i form a basis and are thus linearly independent we must have $c_i = e_\circ$ for all $1 \leq i \leq n$. However, since $l_1, l_2, \ldots, l_m$ form a basis the equality $\sum_{j=1}^{m} d_{ij} \diamond l_j = e_\circ$ implies that all $d_{ij} = e_\circ$ which contradicts the assumption. □

Chapter 4

Algorithms and their Complexity

Algorithms are like recipes for how to compose big computations out of smaller ones. In the extreme case the steps can be individual machine instructions for a specified computer but usually more complex arithmetic operations like addition or multiplication are used as smallest units. It is up to the programmer to instantiate these lowest level operations in an implementation. An algorithm has specified inputs and outputs, it might use randomness for its operations. Algorithms state in a step-by-step manner how to obtain the desired output from the input.

This chapter serves two purposes – it introduces algorithms that are important to implement efficient cryptographic algorithms and it provides the concepts and tools necessary to analyze the running time of algorithms.

We use sorting algorithms to explain the basics of time and space complexity – and because they are used in many applications.

We introduce different integer recodings which are useful to compute exponentiations and scalar multiplications, the main operations in discrete logarithm based cryptosystems. The Euclidean algorithm was introduced in the previous chapter. Here we consider efficient implementations, particularly of the extended Euclidean algorithm which is used to compute modular inverses. In Chapter 5 we work in finite fields. The extended Euclidean algorithm is the main way of computing inverses in such fields. Finally, we consider an explicit version of the nhinese Remainder theorem 3.4.20 over the integers.

Several books deal with algorithms and efficient implementations. The bible in this area is certainly Knuth's "Art of Computer Programming". For the contents of this course Volume 2 "Seminumerical algorithms" is particularly interesting. Our first examples are sorting algorithms which are treated in Volume 3 "Sorting and Searching". The below-mentioned handbook contains a very nice chapter by A. K. Lenstra and H. W. Lenstra titled "Algorithms in number theory" which covers the more advanced algorithms discussed here. Most of the material presented here is also already well covered in online resources.

- A. Aho, J. Hopcraft and J. Ullman, "The Design and Analysis of Computer Algorithm", Addison-Wesley.

- D. E. Knuth, "The art of computer programming", Addison-Wesley.
- J. van Leeuwen, "Handbook of theoretical computer science, Volume A, algorithms and complexity", Elsevier.

4.1 Sorting and complexity

The objective of sorting algorithms is to take an unsorted list of objects and transform it into a sorted list according to some ordering. The reader may think of a list of words to be sorted like in a dictionary or of a list of merchants to be sorted according to the price they offer. For simplicity we stick to sorting numbers by size with the smallest number put first.
Let L be an unsorted list of m integers, i.e. $L[i] = n_i$ for $0 \leq i < m$ and $n_i \in \mathbb{Z}$. The idea of this sorting algorithm is to iteratively produce a sorted sublist so that the list $L[0], \ldots, L[i-1]$ is sorted before $L[i]$ is processed. The next element $L[i]$ is then *inserted*, hence the name *insertion sort*, at the correct position into the sorted list and the entries are relabeled accordingly.

Algorithm 4.1.1 (Insertion sort)
IN: *unsorted list L of length m.*
OUT: *sorted list L' with $L = L'$ as sets.*

1. `for` $i = 1$ `to` $m - 1$
   (a) $d \leftarrow L[i]$
   (b) $j \leftarrow i$
   (c) `while` $j > 0$ *and* $L[j-1] > d$
      i. $L[j] \leftarrow L[j-1]$
      ii. $j \leftarrow j - 1$
   (d) $L[j] \leftarrow d$
2. `return` L

The variable d is used as dummy variable to carry $L[i]$, because this position is taken by the largest element in the so far sorted list. All elements larger than d are shifted so that d can be inserted at the right place, here $L[j]$ at the end of the while loop.
For any list of length m this algorithm will do $m-1$ rounds in the outer loop and the inner loop takes at most $m - 1$ comparisons and shifts. The worst case for this sorting algorithm is if the starting list is sorted with the element in opposite order because then the inner loop uses $i - 1$ comparisons and shifts. So the worst case needs

$$\sum_{i=2}^{m}(i-1) = \sum_{i=1}^{m-1} i = m(m-1)/2$$

comparisons and shifts. A random unsorted list will require less operations but still in the order of magnitude of m^2 many. If the list is already sorted then each inner loop consists of only one comparison, so then only $m-1$ steps are needed.
When comparing different algorithms one wants to choose the most efficient one which usually means the one with the best *performance*. While performance is related to an actual execution of the algorithm on given data and on a given machine, the *complexity* of an algorithm is the theoretical measure of how the algorithm scales with larger inputs.
Counting the number of comparisons in terms of the length of the list m gives a measure of the time complexity of a sorting algorithm. Often not only the time is important but also the space complexity is considered.
For insertion sort we stated how many comparisons are needed in the worst case. We can also look at the best case, namely the case where the input is already sorted. In this case $m-1$ comparisons and no swaps are performed.

Definition 4.1.2 (Complexities)
Consider an algorithm with input size growing in some parameter n.

- *The* worst-case complexity *of the algorithm is the function defined by the maximum number of steps taken on any instance of size n.*
- *The* best-case complexity *of the algorithm is the function defined by the minimum number of steps taken on any instance of size n.*
- *The* average-case complexity *of the algorithm is the function defined by the average number of steps taken on any instance of size n.*

Not only the time is important but also the space requirements. Some algorithms might not be implementable on small devices such as smart cards. When stating the space complexity in terms of the input size we use the same terminology, i.e. worst-case, average-case, and best-case as for the time complexity.
In the insertion sort we took into account the storage requirements by sorting the results into the same list. It would have been easier to state the algorithm with a separate output list into which the elements are inserted in the correct relative location. This would avoid some shifts in the original list on the cost of twice as much storage space.
While for an actual execution of the algorithm a factor of 2 in the execution time or space requirement matters, it does not influence the growth in the parameter. To capture the asymptotic behavior appropriately we introduce the *big-O* notation.

Definition 4.1.3 (big-O)
A function $g(n)$ is $O(f(n))$ if for some positive constant c and for values of n greater than some value n_0 we have

$$g(n) \leq cf(n).$$

Note that the big-O expressions do not involve constants or low-order terms and consider growth in the parameter n. The statements are of asymptotic nature and clearly, if n gets large enough, constants and low-order terms do not matter. In the context of algorithms the function $g(n)$ is thought of as the exact complexity of an algorithm as a function of the problem size n. The function $f(n)$ inside the big-O gives an *upper bound* on that complexity.

Example 4.1.4 *The easiest case is when $g(n)$ is a polynomial in n, e.g. $g(n) = 10n^2 + 30n + 5000$. The highest order term, here $10n^2$, dominates the asymptotic behavior and so determines the function f in the big-O. In this example $g(n)$ is $O(n^2)$, which can be checked easily for $c = 5040$ and $n_0 = 1$.*
We could have stated just as well that g is $O(n^3)$ or $O(n^{2000})$ but these functions n^3 and n^{2000} grow much faster than g. In practice we try to find tight bounds, i.e. the smallest possible upper bound.

We say that an algorithm has *linear complexity* if its running time is $O(n)$. Analogously we speak of quadratic complexity for $O(n^2)$ and in general of *polynomial complexity* if there exists a polynomial $f(n)$ so that the complexity is $O(f(n))$. If the complexity is $O(\exp(f(n))$ for some polynomial f, where exp is the exponential function, then the algorithm has *exponential complexity*.

Example 4.1.5 *Insertion sort as presented in Algorithm 4.1.1 has worst-case complexity in $O(m^2)$ and best-case complexity in $O(m)$. In the big-O estimates the constants do not matter and so we analyze the version with two lists to determine the average-case complexity. When the i-th element is inserted in the sorted list, on average $(i-1)/2$ elements have to shift to create space. So instead of summing up over $i-1$ as in the worst-case complexity we sum up over this value of half the size. However, constants are neglected and so we obtain that insertion sort takes $O(m^2)$ on average.*
The space complexity is $m+1$ elements – m to hold the list and one for the intermediate variable d. This is $O(m)$. If we only consider the extra *storage needed then insertion sort needs $O(1)$ storage.*
Note that the counters i and j also require space, but this is typically neglected and we only count space for the elements we sort. An example would be that the $L[i]$ are movies of several GB and there are only 1024 of them, so the counters have 10 bits.

The big-O estimates are important to get a feeling for the performance of an algorithm. Apart from constants, they give an upper bound on the performance. In most of this book and in cryptography constants do matter and a factor 2 speed-up is worth a lot. It might be that for a concrete parameter size n an asymptotically faster algorithm performs worse because the constants hidden in the big-O might be much larger. So special care is needed to select the appropriate algorithm for given sizes.

We now present some more sorting algorithms and analyze their complexities. The following *bubble sort* algorithm predates insertion sort. In practice it is less efficient but we state it for historic reasons.
The name *bubble sort* comes from the idea that the comparison bubbles through the list. At each moment two adjacent elements are compared and the order of the pair is swapped if $L[i-1] > L[i]$.

Algorithm 4.1.6 (Bubble sort)
IN: *unsorted list L of length m.*
OUT: *sorted list L' with $L = L'$ as sets.*

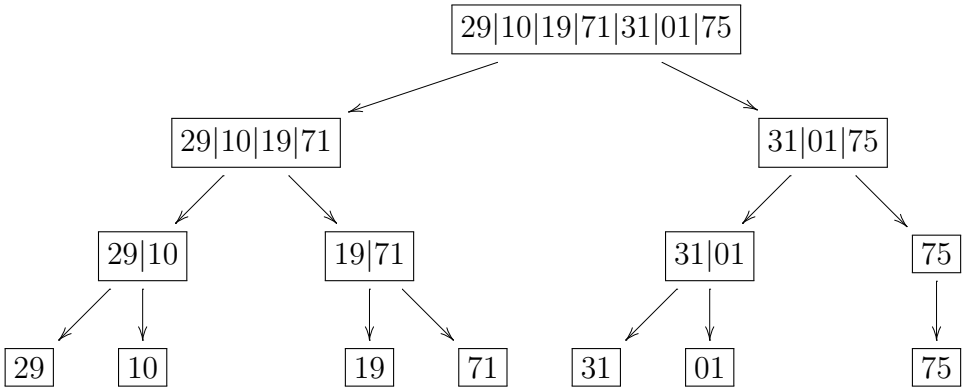
1. `for` $i = m-1$ `downto` 0
   (a) `for` $j = 1$ `to` i
      i. `if` $L[j-1] > L[j]$
         A. $d \leftarrow L[j-1]$
         B. $L[j-1] \leftarrow L[j]$
         C. $L[j] \leftarrow d$
2. `return` L

A big element "bubbles" towards the $(m-1)$-th position in the list by moving forward one position in each comparison. While "insertion sort" creates a sorted sublist into which the handled element is inserted at the correct position, the bubble sort algorithm creates a sublist starting with $L[m-1]$ which is no longer touched; each iteration handles a position, not an element as in insertion sort.
If the input list is sorted starting with the largest element, then bubble sort performs just as good (or bad) as insertion search. Again this case is the worst case and determines the worst-case complexity to $O(n^2)$. The average-case complexity is also $O(n^2)$ while the best-case complexity is $O(n)$ for just reading through an already sorted list. Bubble sort needs only one extra element storage space, namely the intermediate variable d, so the space requirement is just the same as in insertion sort.
From the big-O expressions insertion sort and bubble sort are equally fast, however in practice, insertion sort is twice as fast.

We now present our first *recursive algorithm*. Such an algorithm calls itself as a subroutine, usually on a problem of smaller size so that eventually the innermost call finishes, passes its result to the calling routine which processes the output and finishes etc.
The *merge sort* function recursively chops the list into two sublists of half size which are in turn fed to merge sort. Finally, a sublist consists of only 1 element and is thus sorted.

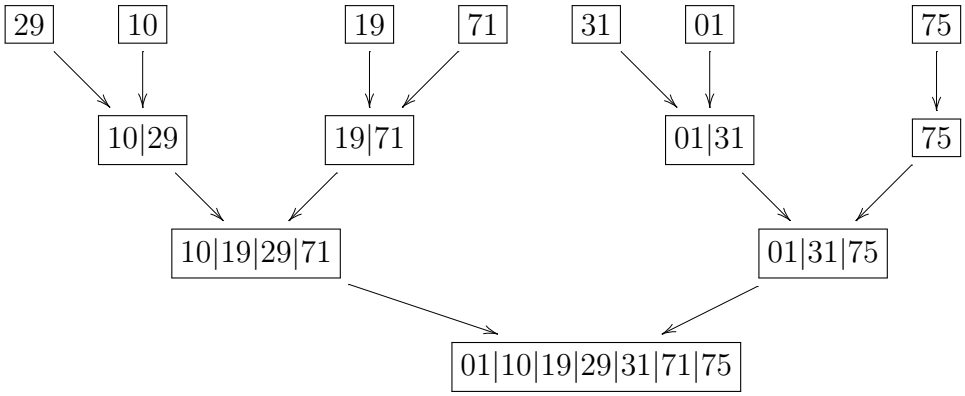
Example 4.1.7 *This example shows the division into sublists of (approximately) half size and the ordering of the resulting lists with only* 1 *or* 2 *elements starting*

from a list with 7 entries.



The algorithm uses a second routine to merge two sorted sublists to form one sorted sublist. Merging two sorted lists is easy since only the initial elements need to be compared. The smaller one is selected and inserted in the new list and so on.

Example 4.1.8 *We continue with the previous example sorting a list with 7 entries.*



To understand why merge sort is faster than the two previously discussed sorting algorithms, note that the resulting tree has $\log m$ levels, where m is the length of the list and log denotes the base 2 logarithm. The outer loop runs through the number of levels, so has length $\log m$. For each level, merges between sorted sublists are needed and in the worst case, each of the m elements takes part in a comparison. This leads to a running time of $m \log m$ comparisons. We note that with the implementation as sketched here, also the best-case needs $O(m \log m)$ comparisons, even though the constants are smaller.
We now state the algorithm in two functions – `mergesort` which calls itself recursively on the lists of half size and `merge` which merges two sorted lists to one.

Algorithm 4.1.9 (`mergesort`)
IN: *unsorted list L of length m.*
OUT: *sorted list L' with $L = L'$ as sets.*

1. `if` $m \leq 1$
   `return` L
2. `else`
   (a) $m' = m/2$
   (b) `for` $i = 0$ `to` $m' - 1$
   $L_l[i] \leftarrow L[i]$
   (c) `for` $i = 0$ `to` $m - m' - 1$
   $L_r[i] \leftarrow L[i + m']$
   (d) $L_l \leftarrow$ `mergesort`(L_l)
   (e) $L_r \leftarrow$ `mergesort`(L_r)
   (f) $L' \leftarrow$ `merge`(L_l, L_r)
   (g) `return` L'

Algorithm 4.1.10 (`merge`)
IN: *sorted lists* L_l *and* L_r *of lengths* m_l *and* m_r.
OUT: *sorted list* L *with* $L = L_l \cup L_r$ *as sets.*

1. $i \leftarrow 0, i_l \leftarrow 0, i_r \leftarrow 0$
2. `while` $i_l < m_l - 1$ *and* $i_r < m_r - 1$
   (a) `if` $L_l[i_l] \leq L_r[i_r]$
   i. $L[i] \leftarrow L_l[i_l]$
   ii. $i \leftarrow i + 1, i_l \leftarrow i_l + 1$
   (b) `else`
   i. $L[i] \leftarrow L_r[i_r]$
   ii. $i \leftarrow i + 1, i_r \leftarrow i_r + 1$
3. `if` $i_l < m_l - 1$
   (a) `for` $j = 0$ `to` $< m_l - i_l - 1$
   $L[i + j] \leftarrow L_l[i_l + j]$
4. `if` $i_r < m_r - 1$
   (a) `for` $j = 0$ `to` $< m_r - i_r - 1$
   $L[i + j] \leftarrow L_r[i_r + j]$
5. `return` L

We first analyze the space requirement of this naive way of writing the algorithm and then show how to improve the space complexity.
We have written the algorithm like in the example, so using fresh arrays for each layer. While `mergesort` is splitting the input list it allocates space for two new

lists of lengths m' and $m - m'$, so at total of m elements. There are $\log m$ layers, so in the current implementation space for $m \log m$ elements would be needed. The way `merge` is stated it also allocates new space for the resulting list. At each layer a total of m elements is stored, adding another $m(\log m - 1)$ elements, so that the algorithm uses a total of $2m \log m$ elements.
It is not hard to get rid of the factor $\log m$ in the space complexity by using one additional list of length m and alternating between the two lists for writing and reading. This version uses $2m$ elements.
Much more tricky to implement, but possible, is *in-place-merge-sort* in which only one extra element is used like the d in insertion or bubble sort. One has to be very careful not to spoil the $O(m \log m)$ running time by using too many shifts in the implementation.
There are many other nice sorting algorithms, particularly the *heap sort* and *radix sort* algorithms. Heap sort also runs in $O(m \log m)$ and needs only one extra element for storage. Radix sort takes into account the length of the numbers to be sorted and is faster than all methods presented here. Giving a complete study of sorting algorithms is way beyond the scope of this script. Knuth is using almost an entire volume on sorting. Readers are encouraged to check the related literature given in the introduction of this chapter.

Exercise 4.1.11 *a) Give big-O estimates for* $g(n) = 100n^3 - 30000n^2 + 1200123n + 1$, $h(n) = \sin(n)$, *and* $l(n) = (50n^6 + 30n^3 + 20n + 1)/(40000n^4 - 40n^3 + 2n - 10)$.

b) Write out explicitly all steps of insertion sort and of bubble sort to sort the list $\boxed{29|10|19|71|31|01|75}$.

4.2 Integer recodings

The main purpose of integer recodings is to improve the speed of exponentiation and scalar multiplication algorithms. The naive way of computing $[n]P$ for some integer n and some group element $P \in (G, \oplus)$ is to iteratively add $\oplus P$ to the intermediate result, which needs $n-1$ group operations. This approach corresponds to viewing n as $n = 1 + 1 + \cdots + 1$. The running time of scalar multiplication algorithms can be enormously reduced by using another representation of n, e.g. binary or NAF, which we introduce in this section. To ease notation we refer to the group operation $\oplus$ as addition. If the two inputs to the addition are the same we speak of doubling.
Assuming the integer n is given in *binary form* as

$$n = \sum_{i=0}^{l-1} n_i 2^i = (n_{l-1} n_{l-2} \dots n_1 n_0)_2,$$

we can perform the scalar multiplication $[n]P$ using the (left-to-right) double-and-add algorithm with $l - 2$ doublings and at most $l - 1$ additions, where $l =$

$\lfloor \log_2 n \rfloor + 1$. The number of necessary additions depends on the number of non-zero bits n_i. The algorithm works as follows:

Algorithm 4.2.1 (Left-to-right binary)
IN: $P \in (G, \oplus)$, *positive integer* $n = (n_{l-1} \dots n_0), n_{l-1} = 1$.
OUT: $[n]P$.

1. $Q \leftarrow P$
2. `for` $i = l - 2$ `downto` 0
   (a) $Q \leftarrow [2]Q$
   (b) `if` $n_i = 1$
   $Q \leftarrow Q \oplus P$
3. `return` Q

Note, there is also a right-to-left version of the above algorithm where the bits are scanned in opposite order.

Example 4.2.2 *We want to compute* $[45]P$. *The binary representation of* 45 *is* $(101101)_2$. *So we perform the left-to-right binary as follows:*

$$[2]([2]([2]([2]([2]P) \oplus P) \oplus P)) \oplus P = [45]P.$$

This computations needs 5 *doublings and* 3 *additions. The naive method would need* 44 *additions instead.*

Averaging over all integers of length l, the probability of a digit n_i being one or zero is one half. So on average there are $l/2$ non-zero digits. The *Hamming weight* of a vector is the number of non-zero entries. If all representations have the same length we care about the *density* which is defined as the Hamming weight divided by the length. The average Hamming weight of the binary representations of length l is $l/2$. Thus, on average one needs $l-2$ doublings and $(l-1)/2$ additions to compute the scalar multiple.
We now consider alternative representations which need the same number of doublings but fewer additions, i.e. we find representations with a lower average Hamming weight. This requires extending the digit set. In particular we deal with signed digits – this is not good in the context of exponentiations since then a negative digit corresponds to an inversion but we will see in Chapter 6 that on elliptic curve an addition takes about as much time as a subtraction.

Definition 4.2.3 (non-adjacent form (NAF))
Let n *be a positive integer. The* non-adjacent form (NAF) *representation of* n *is the representation* $n = \sum_{i=0}^{l-1} n_i 2^i$ *with* $n_i \in \{0, \pm 1\}$ *such that no two consecutive digits are nonzero, i.e.* $n_i n_{i-1} = 0$ *for* $l - 1 \leq i \leq 1$. *To indicate that a representation is in NAF we write* $(n_{l-1} \dots n_0)_{NAF}$.

As the definition indicates, the NAF of an integer is unique. We will comment on this later. The following algorithm computes the NAF of an integer given in binary form.

Algorithm 4.2.4 (Signed-binary representation in non-adjacent form)

IN: *positive integer* $n = (n_l n_{l-1} \dots n_0)_2$ *with* $n_l = n_{l-1} = 0$.
OUT: *NAF of* n *as* $(n'_{l-1} \dots n'_0)_{NAF}$.

1. $c_0 \leftarrow 0$
2. `for` $i = 0$ `to` $\ell - 1$
   (a) $c_{i+1} \leftarrow \lfloor (c_i + n_i + n_{i+1})/2 \rfloor$
   (b) $n'_i \leftarrow c_i + n_i - 2c_{i+1}$
3. `return` $(n'_{\ell-1} \dots n'_0)_{NAF}$

Example 4.2.5 *We want to compute the NAF of* $15 = (1111)_2$. *Here we go through the steps of the previous algorithm.*

i	c_i	c_{i+1}	n_i	n_{i+1}	n'_i
0	*0*	*1*	*1*	*1*	*-1*
1	*1*	*1*	*1*	*1*	*0*
2	*1*	*1*	*1*	*1*	*0*
3	*1*	*1*	*1*	*0*	*0*
4	*1*	*0*	*0*		*1*

The NAF of 15 *is* $(1, 0, 0, 0, -1)_{NAF}$ *as can be seen in the last column of the table. The density is* $2/5$.

Observe, that there are other signed digit representations of 15, e.g. $15 = (1, 0, -1, 1, 1)$, but one can show that the NAF form is unique and that it has minimal Hamming weight (i.e. the number of non-zero digits) among all representations with digit set $\{0, \pm 1\}$. Note that the length can increase by 1 compared to the binary representation.
A value in NAF form has an average density of 1/3, i.e. one-third of the digits are (on average) non-zero. To see this we determine the ratio of non-zero to zero digits in the NAF representation. According to the definition of the (unique) NAF form we know that after a non-zero value there is always a zero. The probability of a second zero is 1/2 since we have only the choices zero or non-zero and the definition does not give any restriction (note, that the next coefficient deals with divisibility by 8; while divisibility by 4 is imposed due to the choice of digit, divisibility by 8 is at random). The probability of a third zero in row is then 1/4 etc. If we sum up the probabilities we get

$$1 + 1/2 + 1/4 + 1/8 + \dots = \sum_{i=0}^{\infty} 1/2^i = 2.$$

(See the first chapter for the geometric series.) So the ratio of non-zero to zero digits is $1:2$ which implies that $1/3$ of all digits are non-zero and the so we have a density of $1/3$.
Using the NAF form of an integer n we can compute the scalar multiplication $[n]P$ by a variant of the left-to-right binary algorithm, where we need to distinguish the non-zero coefficients.

Algorithm 4.2.6 (Left–to–right NAF)
IN: $P \in (G, \oplus)$, *positive integer* $n = (n_{l-1} \dots n_0)_{NAF}, n_{l-1} = 1$.
OUT: $[n]P$.

1. $Q \leftarrow P$
2. `for` $i = l - 2$ `to` 0
   (a) $Q \leftarrow [2]Q$
   (b) `if` $n_i = 1$
   $Q \leftarrow Q \oplus P$
   (c) `if` $n_i = -1$
   $Q \leftarrow Q \ominus P$
   (d) $i \leftarrow i - 1$
3. `return` Q

Example 4.2.7 *We compute again* $[15]P$ *but this time using the NAF of* 15. *The NAF form of* 15 *is* $(1, 0, 0, 0, -1)_{NAF}$. *So we compute*

$$([2]([2]([2]([2]P)))) \ominus P = [15]P.$$

This computations needs 4 *doublings and* 1 *subtraction.*

The average case complexity of scalar multiplication by scalars of binary size l using the NAF representation is $4/3l$ group operations while the binary method needs $3/2l$ group operations on average. The worst case complexity for the NAF is $3/2l$ additions while for the binary representation it is $2l$.

To further reduce the number of additions it is possible to extend the set of coefficients. For a literature search the key words are *signed* and *unsigned windowing methods* and *sliding windows*. If a coefficient $|n_i| > 1$ appears then adding (or subtracting) $[n_i]P$ requires that either this value has been precomputed or that the additions are done at that moment. We refer the reader to the literature.

In the context of elliptic curves we will encounter Montgomery coordinates. To use them most efficiently one needs to ensure that, when adding two elements $P \oplus Q$, one knows the difference $Q \ominus P$. One easy way of achieving this for a scalar multiplication $[n]P$ is known as *Montgomery's ladder* in which two intermediate results Q and R are used with the property that at any moment $R = Q \oplus P$.

Clearly, one could compute this by applying the left-to-right algorithm twice but we now show how to obtain the same results with fewer doublings.
Let $Q_j = \sum_{i=j}^{l} [n_i 2^{i-j}]P$ be the intermediate result after $l-j$ rounds; accordingly $R_i = Q_i \oplus P$. To compute Q_{j-1} from Q_j and R_j we have several possibilities as in

$$Q_{j-1} = [2]Q_j \oplus [n_{j-1}]P = Q_j \oplus R_j \oplus [n_{j-1}]P \ominus P = [2]R_j \oplus [n_{j-1}]P \ominus [2]P.$$

This implies that the next intermediate results are computed as follows:

$$(Q_{j-1}, R_{j-1}) = \begin{cases} ([2]Q_j, Q_j \oplus R_j) & \text{if } n_{j-1} = 0, \\ (Q_j \oplus R_j, [2]R_j) & \text{if } n_{j-1} = 1. \end{cases}$$

Example 4.2.8 *We show how to compute* $[13]P$ *using Montgomery's ladder. The binary representation of* 13 *is* $13 = (1101)_2$ *and so the intermediate steps are*

$$\begin{array}{lcll} (Q_3, R_3) & = & (P, [2]P), & \\ (Q_2, R_2) & = & ([3]P, [4]P) & n_2 = 1, \\ (Q_1, R_1) & = & ([6]P, [7]P) & n_1 = 0, \\ (Q_0, R_0) & = & ([13]P, [14]P) & n_0 = 1. \end{array}$$

For any integer of binary length l, this method needs l additions and l doublings independent of the binary representation of the integer. So, if this method is used, there is no need to start with a NAF representation.

If one wants to compute $[n_1]P_1 \oplus [n_2]P_2 \oplus \cdots \oplus [n_m]P_m$, *multi-scalar multiplication methods* are available. We concentrate on the case $m = 2$ here. Let

$$\begin{array}{lcccccccc} n_1 & = & n_{1,l-1}2^{l-1} & +n_{1,l-2}2^{l-2} & +n_{1,l-3}2^{l-3} & \ldots & +n_{1,1}2 & +n_{1,0}, \\ n_2 & = & n_{2,l-1}2^{l-1} & +n_{2,l-2}2^{l-2} & +n_{2,l-3}2^{l-3} & \ldots & +n_{2,1}2 & +n_{2,0}. \end{array}$$

The first observation is that one can share the doublings and compute

$$[2]\left([2](n_{1,l-1}P_1 \oplus n_{2,l-1}P_2) \oplus (n_{1,l-2}P_1 \oplus n_{2,l-2}P_2)\right) \oplus \cdots$$

If we start with binary representations, i.e. the $n_{i,j}$ are in $\{0, 1\}$, then any addition is with P_1, P_2 or $P_1 \oplus P_2$. The last value should be precomputed so that in any case only one addition is needed. The joint Hamming weight is defined as the number of non-zero columns, where the i-th digits $n_{1,i}, n_{2,i}$ together form the i-th column. The average joint density, i.e. the average joint Hamming weight divided by the length of the representation, is $3/4$. On average $7/4l$ group operations are needed which is much less than the $2 \cdot 3/2l$ used by individually computing $[n_1]P_1$ and $[n_2]P_2$.
If both integers are given in NAF and both combinations $P_1 \oplus P_2$ and $P_1 \ominus P_2$ are precomputed, then at most one addition is performed between two doublings. To determine the density, observe that the initial NAFs have density $1/3$ and are independent, so with probability $2/3 \cdot 2/3$ both $n_{1,i}$ and $n_{2,i}$ are 0 leading to

a joint density of 5/9.

One can do better! Solinas introduced the *Joint Sparse Form (JSF)* which has a joint density of only 1/2. It is defined by the following conditions.

(JSF 1) Of any three consecutive columns at least one is a zero column.
(JSF 2) It is never the case that $n_{i,j+1}n_{i,j} = -1$.
(JSF 3) If $n_{i,j+1}n_{i,j} \neq 0$ then $n_{1-i,j+1} = \pm 1$ and $n_{1-i,j} = 0$.

Example 4.2.9 *Let $n_1 = 403$ and $n_2 = 334$, the NAF expansions of n_1 and n_2 are given on the left, while the JSF is on the right.*

$$\begin{array}{rcl} n_1 & = & (1\ 0\ -1\ 0\ 0\ 1\ 0\ 1\ 0\ -1)_{NAF} \\ n_2 & = & (0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ -1\ 0)_{NAF} \end{array} \quad = \quad \begin{array}{l} (1\ 0\ -1\ 0\ 0\ 1\ 0\ 0\ 1\ 1) \\ (1\ 0\ -1\ -1\ 0\ 1\ 0\ 0\ -1\ 0) \end{array}$$

One can show that the Joint Sparse Form of any two integers exists and is unique. It has minimal joint Hamming weight among all joint signed binary expansions. If n_1 and n_2 have maximal length l, then the joint double and add algorithm computes $[n_1]P_1 \oplus [n_2]P_2$ from the JSF with an average of l doubles and $l/2$ additions of either $\pm P_1$, $\pm P_2$, $\pm(P_1 \oplus P_2)$ or $\pm(P_1 \ominus P_2)$.

Exercise 4.2.10 *a) Compute the NAFs of* 31 *and* 33.

b) Look up the algorithm to compute the JSF and compute the JSF of 31 *and* 33.

4.3 Euclidean algorithm

In the previous chapter we considered the Euclidean algorithm for arbitrary Euclidean rings R in Algorithm 3.4.15. We briefly recall the algorithm as we presented it earlier and then give a more efficient version of the extended Euclidean algorithm. The main purpose of the Euclidean algorithm is to compute greatest common divisors. The extended version is heavily used in the arithmetic of finite fields to compute inverses. For this exposition we concentrate on the case that R is the polynomial ring $K[x]$ over a field K.
On input $f, g \in K[x]$ the algorithm computes the greatest common divisor d of them and also shows how to compute $u, v \in K[x]$ such that

$$\begin{array}{rcl} d(x) & = & \gcd(f(x), g(x)) \\ d(x) & = & u(x)f(x) + v(x)g(x). \end{array}$$

We briefly repeat the recursive version, for proofs see Section 3.4. The algorithm uses division with remainder as subroutine.
Let f split as $f(x) = g(x) \cdot q_1(x) + r_1(x)$ with $\deg(r_1) < \deg(g)$. Interchanging the roles of (f, g) with (g, q_1) we continue as

$$\begin{array}{rcl} g(x) & = & r_1(x) \cdot q_2(x) + r_2(x),\ \deg(r_2) < \deg(r_1) \\ & \vdots & \\ r_{n-2}(x) & = & r_{n-1}(x) \cdot q_n(x) + r_n(x),\ \deg(r_n) < \deg(r_{n-1}) \\ r_{n-1}(x) & = & r_n(x) \cdot q_{n+1}(x) + 0, \end{array}$$

where $r_n \neq 0$.
The greatest common divisor $\gcd(f, g)$ equals $d = r_n$, the last non-zero remainder. It is common to make the gcd monic to work with unique values.
The algorithm works since from $r_{n+1} = 0$ one has $r_n | r_{n-1}$. Inserting that in the previous equation one gets $r_n | r_{n-2}$ which eventually leads to $r_n | g$ and $r_n | f$. So clearly r_n is a divisor of both f and g. Any polynomial $e \in K[x]$ which also divides f and g must divide r_1 and therefore r_2 etc. and thus is a divisor of $d = r_n$, so d is the greatest common divisor of f and g where size is measured in terms of the degree of the polynomial.
Starting from the bottom row, repeatedly inserting leads to two polynomials u and v satisfying $d = u \cdot f + v \cdot g$. Checking their degrees, one sees that $\deg(u) < \deg(g)$ and $\deg(v) < \deg(f)$.
While this description allows to compute the polynomials d, u, and v it will not be very efficient and in particular a lot of storage is needed to store all the intermediate values q_i and r_i. The following algorithm computes u and v along with the computation of d.

Algorithm 4.3.1 (Extended Euclidean algorithm)
IN: $f(x), g(x) \in K[x]$
OUT: $d(x), u(x), v(x) \in K[x]$ *with* $d(x) = u(x)f(x) + v(x)g(x)$

1. $a \leftarrow [f(x), 1, 0]$
2. $b \leftarrow [g(x), 0, 1]$
3. `repeat`
   (a) $c \leftarrow a - (a[1] \operatorname{div} b[1])b$
   (b) $a \leftarrow b$
   (c) $b \leftarrow c$

   `while` $b[1] \neq 0$
4. $l \leftarrow LC(a[1])$, $a \leftarrow (1/l)a$
5. $d(x) \leftarrow a[1]$, $u(x) \leftarrow a[2]$, $v(x) \leftarrow a[3]$
6. `return` $d(x), u(x), v(x)$

In this algorithm, div denotes division with remainder. The first component of c is thus easier written as $c[1] \leftarrow a[1] \bmod b[1]$ but by operating on the whole vector we get to update the values leading to u and v, too. At each step we have

$$a[1] = a[2]f + a[3]g \text{ and } b[1] = b[2]f + b[3]g.$$

To see this, note that this holds trivially for the initial conditions. If it holds for both a and b then also for c since it computes a linear relation of both vectors. So each update maintains the relation and eventually when $b[1] = 0$, we have that $a[1]$ holds the previous remainder, which is the gcd of f and g. At the end the gcd is made monic by dividing by the leading coefficient $LC(a[1])$.

Example 4.3.2 *Let* $K = \mathbb{R}$ *and* $f(x) = x^5 + 3x^3 + x^2 + 2x + 1$, $g(x) = x^4 - 5x^3 - 5x^2 - 5x - 6$. *So at first we have* $a = [f, 1, 0], b = [g, 0, 1]$.

We have $(a[1] \operatorname{div} b[1]) = x + 5$ *and so end the first round with*

$$\begin{aligned} a &= [g, 0, 1], \\ b &= [33x^3 + 31x^2 + 33x + 31, 1, -x - 5]. \end{aligned}$$

Indeed $b[1] = f(x) + (-x - 5)g(x)$.

With these new values we have $(a[1] \operatorname{div} b[1]) = 1/33x - 196/1089$ *and so the second round ends with*

$$\begin{aligned} a &= [33x^3 + 31x^2 + 33x + 31, 1, -x - 5], \\ b &= [-458/1089x^2 - 458/1089, -1/33x + 196/1089, 1/33x^2 - 31/1089x + 109/1089]. \end{aligned}$$

In the third round we have $(a[1] \operatorname{div} b[1]) = -35937/458x - 33759/458$ *and obtain*

$$\begin{aligned} a &= [-458/1089x^2 - 458/1089, -1/33x + 196/1089, 1/33x^2 - 31/1089x + 109/1089], \\ b &= [0, -1089/458x^2 + 5445/458x + 3267/229, 1089/458x^3 + 1089/229x + 1089/458]. \end{aligned}$$

Since $b[1] = 0$ *the loop terminates. We have* $LC(a[1]) = -458/1089$ *and thus normalize to*

$$a = [x^2 + 1, 33/458x - 98/229, -33/458x^2 + 31/458x - 109/458].$$

We check that indeed

$$x^2+1 = (\frac{33}{458}x-\frac{98}{229})(x^5+3x^3+x^2+2x+1)+(\frac{-33}{458}x^2+\frac{31}{458}x-\frac{109}{458})(x^4-5x^3-5x^2-5x-6).$$

Exercise 4.3.3 *a) Compute the extended* gcd *of* $f(x) = x^5 + 3x^3 - x^2 - 4x + 1$ *and* $g(x) = x^4 - 8x^3 + 8x^2 + 8x - 9$ *in* $\mathbb{Q}[x]$ *using Algorithm 4.3.1.*

b) If one skips the one to last step of making $a[1]$ *monic, the same algorithm works for computing extend greatest common divisors of integers. Use it to compute the inverse of* 71 *modulo the prime* 101.

4.4 Chinese remainder computations

Let R be a ring. For our considerations, it is either the ring of integers or the polynomial ring over a field K, so coprimality is easily defined. Theorems 3.4.20 and 3.5.13 show that for coprime elements $n_1, \ldots, n_k \in R$ the system of equivalences

$$\begin{aligned} X &\equiv r_1 \bmod n_1, \\ X &\equiv r_2 \bmod n_2, \\ &\vdots \\ X &\equiv r_k \bmod n_k, \end{aligned}$$

has a solution X which is unique up to multiples of $N = n_1 \cdot n_2 \cdots n_k$.
We now present a constructive algorithm to find this solution, making heavy use of the extended Euclidean algorithm presented in the previous section. Since all n_i are coprime, we have $\gcd(n_i, N/n_i) = 1$ and we can use Algorithm 4.3.1 to compute u_i and v_i with

$$u_i n_i + v_i(N/n_i) = 1.$$

Let $e_i = v_i(N/n_i)$, then this equation becomes $u_i n_i + e_i = 1$ or $e_i \equiv 1 \bmod n_i$. Furthermore, since all $n_j | (N/n_i)$ for $j \neq i$ we also have $e_i = v_i(N/n_i) \equiv 0 \bmod n_j$ for $j \neq i$.
Using these values e_i a solution to the system of equivalences is given by

$$X = \sum_{i=1}^{k} r_i e_i,$$

since X satisfies $X \equiv r_i \bmod n_i$ for each $1 \leq i \leq k$.

Example 4.4.1 *Consider the system of integer equivalences*

$$\begin{aligned} X &\equiv 1 \bmod 3, \\ X &\equiv 2 \bmod 5, \\ X &\equiv 5 \bmod 7. \end{aligned}$$

The moduli are coprime and we have $N = 105$. *For* $n_1 = 3, N_1 = 35$ *we get* $v_1 = 2$ *by just observing that* $2 \cdot 35 = 70 \equiv 1 \bmod 3$. *So* $e_1 = 70$.

Next we compute $N_2 = 21$ *and see* $v_2 = 1$ *since* $21 \equiv 1 \bmod 5$. *This gives* $e_2 = 21$.

Finally, $N_3 = 15$ *and* $v_3 = 1$ *so that* $e_3 = 15$.
The result is $X = 70 + 2 \cdot 21 + 5 \cdot 15 = 187$ *which indeed satisfies all* 3 *congruences. To obtain the smallest positive result we reduce* 187 *modulo* N *to obtain* 82.

For easier reference we phrase this approach as an algorithm.

Algorithm 4.4.2 (Chinese remainder computation)
IN: *system of* k *equivalences as* $(r_1, n_1), (r_2, n_2), \ldots (r_k, n_k)$ *with pairwise coprime* n_i
OUT: *smallest positive solution to system*

1. $N \leftarrow \prod_{i=1}^{k} n_i$
2. $X \leftarrow 0$
3. `for` $i = 1$ `to` k
   (a) $M \leftarrow N \operatorname{div} n_i$
   (b) $v \leftarrow (M^{-1} \bmod n_i)$ *(use Algorithm 4.3.1)*

(c) $e \leftarrow vM$

(d) $X \leftarrow X + r_i e$

4. $X \leftarrow X \bmod N$

Alternatively M can be computed as $\prod_{\substack{j=1 \\ j \neq i}}^{k} n_j$.

Exercise 4.4.3 *a) Find the smallest positive integer X satisfying*

$$\begin{aligned} X &\equiv 1 \bmod 2, \\ X &\equiv 4 \bmod 7, \\ X &\equiv 2 \bmod 11. \end{aligned}$$

b) Find the polynomial $f(x) \in \mathbb{F}_2[x]$ of smallest degree satisfying

$$\begin{aligned} f(x) &\equiv 1 \bmod (x+1), \\ f(x) &\equiv x+1 \bmod (x^2+x+1), \\ f(x) &\equiv x \bmod (x^3+x^2+1). \end{aligned}$$

Chapter 5

Finite Fields

Finite fields are one of the essential building blocks in coding theory and cryptography and thus appear in many areas in IT security. This section introduces finite fields systematically stating for which orders finite fields exist, shows how to construct them and how to compute in them efficiently.
For applications 3 types of fields are particularly interesting – fields with a prime number of elements, extension fields of the minimal field $\{0, 1\}$ and optimal extension fields. We met *prime fields*, the first kind of fields, already in Chapter 3 as $\mathbb{Z}/p\mathbb{Z}$, the second one appeared as an example of a vector space and we also defined some multiplicative structure on it which lead to a ring but not to a field. Here were show how one constructs a *binary field*. These fields are particularly suitable for hardware implementations as the arithmetic involves basic bit operations. If, however, software implementations are the focus then it might be interesting to go for yet another construction in which the size of the elements is tailored to the word size of the processor, such fields are called *optimal extension fields*.
References for this chapter are:

- T. Høholdt and J. Justesen, "A Course In Error-Correcting Codes", Springer Verlag. Contains details for binary fields.
- R. Lidl and H. Niederreiter, "Finite Fields, Encyclopedia of Mathematics and its Applications 20", Addison-Wesley.
- R. Lidl and H. Niederreiter, "Introduction to finite fields and their applications", Cambridge University Press.
- A. Menezes, "Applications of Finite Fields", Kluwer.
- T. Murphy, "Finite Fields", Script online at https://www.maths.tcd.ie/pub/Maths/Courseware/FiniteFields/GF.pdf
- V. Shoup, "A Computational Introduction to Number Theory and Algebra", Cambridge University Press. This book is also available online for download at http://www.shoup.net/ntb/ntb-b5.pdf

In this chapter we first assume that finite fields exist and study their properties. We show that for any prime p and for any natural number n there exists a field with p^n elements. We then detail constructions of finite fields and go into the arithmetic properties.

5.1 First definitions

Definition 5.1.1 (Finite field) *A field with finitely many elements is called a* finite field. *We denote a finite field with q elements by $\mathbb{F}_q$.*

Finite fields are also called *Galois fields*, named after Évariste Galois, and several books and scientific papers thus use $GF(q)$ to denote a finite field with q elements.

Definition 5.1.2 (Characteristic) *Let K be a field. The smallest natural number $n > 0$ such that*

$$n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n\ -times} = 0$$

is called the characteristic of K, *denoted by* $\mathrm{char}(K) = n$.
If no such n exists one puts $\mathrm{char}(K) = 0$.

We have already encountered the following example in the previous chapter but state it again here as the first example of a finite field.

Example 5.1.3 *The ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field of characteristic p. Obviously $\mathbb{F}_p$ has exactly p elements and is thus finite, we have seen that it is a field and every element vanishes under multiplication by p, thus the characteristic is p.*

The following lemma gives useful properties of the characteristic.

Lemma 5.1.4 *Let K be a field.*

1. *If the characteristic of K is positive,* $\mathrm{char}(K)$ *is prime.*
2. *Finite fields have* $\mathrm{char}(K) > 0$. *By the first part of this lemma we even have that a finite field has prime characteristic.*

Proof.

1. Assume on the contrary that there exists a nontrivial factorization $\mathrm{char}(K) = n = p \cdot q$. Then

   $$0 = n{\cdot}1 = (p \cdot q){\cdot}1 = p{\cdot}(q{\cdot}1) = (p{\cdot}1){\cdot}(q{\cdot}1) = \underbrace{(1 + 1 + \cdots + 1)}_{p\text{ -times}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{q\text{ -times}}.$$

   We encountered earlier that fields have no zero divisors, that means that one of the terms in the product must be zero which contradicts the minimality of the characteristic.

2. In a *finite* field not all of $1, 2 \cdot 1, 3 \cdot 1, \ldots$ can be distinct, e.g. $r \cdot 1 = s \cdot 1$ for some $s > r$. Then $\Rightarrow (s - r) \cdot 1 = 0$ and so $\text{char}(K) | s - r > 0$

□

Lemma 5.1.5 *Let K be a field. Then there exists a smallest subfield of K.*

Proof. Let F_1, F_2 be subfields of K, then their intersection $F_1 \cap F_2$ is also a subfield of K.
This holds for arbitrary many subfields, thus also for the intersection of all subfields of K. Obviously, the resulting intersection is the smallest subfield of K. □

This smallest subfield is an important concept and thus deserves a name.

Definition 5.1.6 (Prime subfield)
The smallest subfield of a field K is called the prime subfield *or short* prime field *of K.*

Depending on K the prime subfield can be finite or infinite. If the characteristic of the field is zero one finds a copy isomorphic to $\mathbb{Q}$ the rational numbers by observing that all "integer" multiples of 1 must be in the field and that the field must be closed under division. For finite fields – and generally for fields of positive characteristic – one can always find a subfield of the type encountered in Example 5.1.3.

Lemma 5.1.7 *Let K be a finite field of characteristic p. The prime subfield of K is isomorphic to $\mathbb{F}_p$, the finite field with p elements.*

Proof. We represent $\mathbb{F}_p$ as $\{0, 1, 2, \ldots, p-1\}$ and define a map into K as

$$\varphi : \mathbb{F}_p \mapsto K, r \mapsto r \cdot 1 = \underbrace{1 + \ldots + 1}_{r \text{ -times}}$$

where 1 is the multiplicative unit in K and $+$ denotes addition in K.
One easily checks that φ is additive and multiplicative, thus a field homomorphism. To show that the field $\mathbb{F}_p$ is embedded into K it remains to show that the map is injective. Assume on the contrary that for some $p > r > s \geq 0$ we have $\varphi(r) = \varphi(s)$. Put $c = r - s > 0$. By the definitions of r and s one can consider c as an element of $\mathbb{F}_p^*$ and thus it has a multiplicative inverse c^{-1} in $\mathbb{F}_p$. We obtain

$$\varphi(1) = \varphi\left(c \cdot c^{-1}\right) = \varphi(c) \cdot \varphi\left(c^{-1}\right) = (\varphi(r) - \varphi(s)) \cdot \varphi\left(c^{-1}\right) = 0.$$

However, by the definition of φ one has $\varphi(1) = 1 \neq 0$ since K is a field. Because of this contradiction, φ is an isomorphism between $\mathbb{F}_p$ and the image of the homomorphism $\text{Im}(\varphi) \subset K$.

This isomorphism proves that $\mathrm{Im}(\varphi)$ is a subfield of K (the image contains 0 and 1 and the field operations are inherited). Since $\mathbb{F}_p$ has no non-trivial subfield, it is its own prime subfield and the argument carries over to $\mathrm{Im}(\varphi)$. So $\mathrm{Im}(\varphi)$ is the prime field of K. □

We already used the notation $\mathbb{F}_p$ as if this would be a unique field. Indeed this holds true up to isomorphism.

Corollary 5.1.8 *Let p be a prime. Up to isomorphism there is only one finite field with p elements, denoted by $\mathbb{F}_p$.*

The proof follows from Lemma 5.1.7 by observing that $\mathbb{F}_p$ is isomorphic to its own prime subfield.
Finite fields with a prime number of elements are often referred to as *prime fields*.

Exercise 5.1.9 *Let K be a field of characteristic p, where p is prime. Show that for any integer n one has*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

for all $a, b \in K$.

5.2 The additive structure of finite fields

So far we do not know whether fields other than $\mathbb{F}_p$ exist but we can find criteria a more general finite field has to satisfy. That reduces the search space and actually gives rise to a construction method.
In the Section 3.8 we considered extension fields as vector spaces over their subfield. This approach helps to determine the additive structure of finite fields and limits the possible sizes for which finite fields can exist.
Let K be a finite field of characteristic $\mathrm{char}(K) = p, |K| > p$. By Lemma 5.1.7 there exists a subfield of K isomorphic to $\mathbb{F}_p$. For ease of notation we identify this field with $\mathbb{F}_p$.
K is a vector space over $\mathbb{F}_p$ and so there must exist a basis of linearly independent elements $a_1, \ldots, a_n$ for some dimension n. This is the main observation leading to the proof of the following lemma.

Lemma 5.2.1 *Let K be a finite field of $\mathrm{char}(K) = p$. There exists an integer $n \geq 1$ so that $|K| = p^n$.*

Proof. Consider K as vector space over $\mathbb{F}_p$. Let $\dim_{\mathbb{F}_p}(K : \mathbb{F}_p) = n$ and let $\{\xi_1, \ldots, \xi_n\}$ be a basis.
Then every element $a \in K$ can be represented via a linear combination of the basis elements with coefficients in $\mathbb{F}_p$. So there exist $c_1, \ldots, c_n \in \mathbb{F}_p$ satisfying $a = c_1\xi_1 + \cdots + c_n\xi_n$.
Each c_i can have p different values, since we consider linear combinations over a basis all these p^n elements in K are distinct. Again by the property of a basis each element of K can be represented as linear combination this way. Thus $|K| = p^n$. □

So for any finite field the number of elements must be a prime or a prime power. E.g. there exists no finite field with 6 elements since 6 is not a prime or prime power. In the following q denotes a prime power $q = p^n$.
We also get conditions on the relative sizes of subfields.

Lemma 5.2.2 *Let L be a finite field with $|L| = p^n$ and let K be a subfield of L. There exists an integer $n \geq 1$ so that $|K| = p^m$ and $m|n$.*
The extension degree of L over K is $[L : K] = n/m$.

Proof. Left to the reader as Exercise 5.2.4. □

We now have a necessary condition on the number of elements in a finite field. The following example studies one finite field which is not a prime field.

Example 5.2.3 *The number 4 is a prime power, so there could be a finite field with 4 elements. What would $\mathbb{F}_4 = \mathbb{F}_{2^2}$ look like? For the moment let us assume that $\mathbb{F}_4$ exists (we will later see that this is indeed the case).*
Let 0 be the additive and 1 be the multiplicative neutral element. Let a be one of the other two elements. Since $\mathbb{F}_4$ is closed under addition the other element must equal $a + 1$, so $\mathbb{F}_4 = \{0, 1, a, a + 1\}$. We now give the addition table which follows easily from the fact that the characteristic is 2, thus $x + x = 0$ for any $x \in \mathbb{F}_4$. Since every element must appear in each row and each column of the table we obtain $a \cdot a = a + 1$ and consequently $a \cdot (a + 1) = 1$.

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

$\cdot$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

We were able to fill the tables completely using just necessary conditions. We note that a basis of $\mathbb{F}_4$ over $\mathbb{F}_2$ could be given by $\{1, a\}$ or likewise by $\{1, a + 1\}$. But: do these tables actually form a field? To answer this we need to check associativity of $+$ and $\cdot$ and prove that the distributive laws hold. Since the number of elements is very small we could check these by explicitly considering all possible cases. The next section provides us with a better understanding of finite fields and their multiplicative structure so that we skip this tedious work here.

Let $\xi_1, \xi_2, \ldots, \xi_n$ be a basis of the finite field K with $|K| = p^n$ over $\mathbb{F}_p$. We can state K as a set as

$$K = \{a_1\xi_1 + a_2\xi_2 + \cdots + c_n\xi_n | a_i \in \mathbb{F}_p \text{ for } 1 \leq i \leq n\}.$$

It is very easy to add two field elements by using the vector space structure: Let $a = \sum_{i=1}^{n} a_i\xi_i$ and $b = \sum_{i=1}^{n} b_i\xi_i$ be elements of K. Their sum is given by

$$a + b = \sum_{i=1}^{n} (a_i + b_i)\xi_i,$$

where $a_i + b_i$ is computed as an element of $\mathbb{F}_p$, i.e. modulo p.

However, we are not able to multiply in this representation unless we know the value of $\xi_i \cdot \xi_j$ expressed in this basis for all $1 \leq i, j \leq n$. Apparently one can store all $n(n+1)/2$ results of the multiplication of the basis vectors and perform multiplications with table lookups but that seems rather tedious. The following section suggests a representation which is particularly suitable for multiplications and Section 5.5 gives the representation which we will use for most applications.

Exercise 5.2.4 *Prove Lemma 5.2.2. Hint: consider L as vector space over K and follow the proof of Lemma 5.2.1.*

5.3 The multiplicative structure of finite fields

The previous section gave us insight in the number of elements of a finite field and determined the additive structure. Given a basis of a finite field K over its prime subfield we are able to perform additions. We now turn our attention to the study of K^*, the multiplicative group of K.

Lemma 5.3.1 *Let K be a finite field with $|K| = p^n$. The multiplicative group $K^* = K \setminus \{0\}$ is cyclic.*

Proof. For ease of notation put $q = p^n$. Since K is a field, K^* consists of all elements of K but 0. So $|K^*| = q - 1$.
According to Lagrange's Theorem (Theorem 3.3.8) for each $a \in K^*$ we have $a^{q-1} = 1$ and $\mathrm{ord}(a) | q - 1$.
If K^* is cyclic then there must exist at least one element g with $\mathrm{ord}(g) = q - 1$. Let e be the exponent of K^*. By the definition of e the order of every element divides e, i.e. $a^e = 1$ for all $a \in K^*$. This implies that all $a \in K^*$ are roots of $F(x) = x^e - 1$. Thus $F(x)$ is a non-zero polynomial of degree e which has at least $q - 1$ different roots which implies $q - 1 \leq e$ by Corollary 3.7.9.
Since the exponent of a group divides its order we have $e | q-1$ and thus $e \leq q-1$. Together this gives $e = q - 1$, i.e. the exponent is the full group order which implies that there is at least one element of order $q - 1$. □

Definition 5.3.2 (Primitive element)
Let K be a finite field. A generator of K^* is called primitive element.

An obvious consequence of Lemma 5.3.1 is the following:

Corollary 5.3.3 *Every finite field contains at least one primitive element. More precisely there are exactly $\varphi(q-1)$ primitive elements.*

This gives a second possibility of representing finite fields. Let g be a primitive element of K then

$$K = \{0, 1, g, g^2, \ldots, g^{q-2}\} = \{0\} \cup \langle g \rangle.$$

In this representation it is very easy to multiply two elements $a = g^i$ and $b = g^j$ as

$$a \cdot b = g^i \cdot g^j = g^{i+j},$$

where the exponent $i + j$ is taken modulo $q - 1$. However, we don't know how to add a and b. Assume $j \leq i$. We observe that

$$a + b = g^i + g^j = g^j(g^{i-j} + 1)$$

and so it would be enough to tabulate all $q - 1$ values of $g^k + 1, 1 \leq k \leq q - 2$ expressed as a power of g to be able to add in this representation.
The lemma also allows to obtain properties of power maps and find possible orders.

Corollary 5.3.4 *Let K be a finite field with $|K| = q$ elements. There exist elements of order k if and only if $k|(q-1)$.*
The power map $\tau : K \to K; a \mapsto a^k$ is a bijection if and only if $\gcd(k, q-1) = 1$.

The following section deals with polynomials over finite fields. We obtain necessary knowledge to find a representation of finite fields that allows to perform addition and multiplication without keeping a big table.

Exercise 5.3.5 *a) Corollary 5.3.3 also holds for the prime fields $\mathbb{F}_p$. Find primitive elements of $\mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}, \mathbb{F}_{13}$ and $\mathbb{F}_{17}$.*

b) State all primitive elements of $\mathbb{F}_7$.

c) Let $\mathbb{F}_{16}^* = \langle g \rangle$. State all primitive elements in terms of g.

d) Prove Corollary 5.3.3.

5.4 Polynomials over finite fields

This section studies polynomials over finite fields. In Section 3.7 we introduced many properties of polynomials over a field. We refer to that section for general background and concentrate here on the case that the coefficients come from a finite field.
We recall the definition of an irreducible polynomial (Definition 3.7.10). A polynomial $f(x) \in K[x]$ is *irreducible* if it cannot be written as a product of polynomials of lower degree over the same field, i.e. $u(x)|f(x)$ implies u is constant or $u(x) = f(x)$. Otherwise it is called *reducible*.

Example 5.4.1 *Consider the following polynomials in* $\mathbb{F}_2[x]$*:* $f_1(x) = x$, $f_2(x) = x^2 + 1$, $f_3(x) = x^2 + x + 1$, *and* $f_4(x) = x^4 + x^2 + 1$.

a) Apparently f_1 *is irreducible.*

b) A non-trivial factor of f_2 *must be linear, one sees that* $(x + 1)|f_2(x)$, *actually* $f_2(x) = (x + 1)^2$.

c) There are only two linear polynomials, x *and* $x+1$, *over* $\mathbb{F}_2$. *One easily checks that none of them divides* f_3, *so* f_3 *is irreducible.*

d) The last polynomial is not divisible by a linear factor. However, it is not irreducible since $f_4(x) = (x^2 + x + 1)^2 = f_3^2(x)$. *which cannot be factored further since* f_3 *is irreducible.*

For functions over the reals, the derivative gives information about the slope of the tangent in a point. In the discrete setting of finite fields we lose this interpretation but we can still define the derivative of a polynomial.

Definition 5.4.2 *Let* K *be a field and* $f(x) = \sum_{i=0}^{n} f_i x^i \in K[x]$ *be a polynomial. The* derivative f' of f *is given by*

$$f'(x) = \sum_{i=1}^{n} i \cdot f_i x^{i-1}.$$

Note that if K has characteristic p then the derivative of all terms x^{mp} vanishes. One can show that for this derivative the usual rules hold.

Corollary 5.4.3 *Let* $f, g \in K[x]$. *One has*

$$(f + g)' = f' + g', \tag{5.1}$$
$$(f \cdot g)' = f' \cdot g + f \cdot g', \tag{5.2}$$
$$(f^a)' = a f^{a-1} \cdot f'. \tag{5.3}$$

Exercise 5.4.4 *a) Let* $f(x) = x^{17} + 3x^{15} - 2x^{12} + x^{11} - x^{10} - 2x^8 + x^5 + 3x^2 + 2 \in \mathbb{F}_5[x]$. *Compute the derivative* f' *of* f.

b) Let $f \in K[x]$ be a polynomial. Show that if α is a multiple root of f then $(x-\alpha) | \gcd(f, f')$.

c) Let $f \in K[x]$ be a polynomial. Let L be an extension field of K so that $f(x)$ factors completely into linear factors, i.e., all roots of f are defined over L. Show that $\gcd(f, f') \in K^*$ if and only if f has no multiple roots.

5.5 Polynomial representation of finite fields

In this section we show how to construct finite fields with p^n, $n > 1$, elements by using an irreducible polynomial of degree n over $\mathbb{F}_p$. The same considerations can be used to construct an extension field of K with $|K| = p^m$ in which case the polynomial must be irreducible over K.
We start by investigating relations between a finite field and a subfield of it.

Lemma 5.5.1 *Let K, L be finite fields with $K \subset L$, $|K| = q$, $|L| = q^n$.*
Every element $\alpha \in L$ is a root of a uniquely defined monic polynomial $m_\alpha \in K[x]$, $\deg m_\alpha \leq n$. This polynomial m_α satisfies that if α is a root of some polynomial $f \in K[x]$ then $m_\alpha | f$.

Proof. We start by considering L as a vector space over K. Since the dimension $\dim_K(L:K)$ is n, any $n+1$ or more elements are linearly dependent.
So the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent and there exist coefficients $c_0, \ldots, c_n \in K$ so that $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$.
We just constructed a polynomial $f(x) = \sum_{i=0}^{n} c_i x^i \in K[x]$ of degree n such that $f(\alpha) = 0$. This proves the existence part of the lemma.
Now that we know that there is at least one polynomial of degree $\leq n$ over K which has α as root and since we can make each polynomial monic as K is a field, let m_α be the monic polynomial of minimal degree so that $m_\alpha(\alpha) = 0$. From the first part we know $\deg(m_\alpha) \leq \deg(f) \leq n$.
We first note that m_α must be irreducible because if it would split as $m_\alpha = a \cdot b$ with $\deg(a), \deg(b) > 1$ would give $0 = m_\alpha(\alpha) = a(\alpha) \cdot b(\alpha)$ and because there are no zero divisors either $a(\alpha) = 0$ or $b(\alpha) = 0$ which contradicts the minimality of the degree of m_α.
Let $f(\alpha) = 0$, and let $r(x), \deg(r) < \deg(m_\alpha)$ be the remainder of f by division by m_α, i.e. $f(x) = q(x)m_\alpha(x) + r(x)$. Evaluating both sides at α gives the identity

$$0 = f(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha),$$

so $r(\alpha) = 0$. Again by the minimality of $\deg(m_\alpha)$ we obtain $r(x) = 0$ which means $m_\alpha | f$. □

Definition 5.5.2 (Minimal polynomial)
Let K be a field, L be a finite extension field of K and $\alpha \in L$. The polynomial $m_\alpha \in K[x]$ constructed in Lemma 5.5.1 is called the minimal polynomial of α over K.

The prime fields $\mathbb{F}_p$ are constructed as residue classes of the integers modulo a prime p. We have seen that the ring of polynomials over a field shares many similarities with the ring of integers and so we consider the polynomial ring modulo an irreducible polynomial.

Theorem 5.5.3 *Let K be a finite field and let $L = K[x]/fK[x]$ be the residue classes modulo a polynomial $f \in K[x]$.*
L is a field if and only if f is irreducible.

Proof. In Example 3.7.16 we considered the case $K = \mathbb{F}_2$ and $f(x) = x^n + 1$ in detail and showed that $\mathbb{F}_2[x]/(x^n+1)\mathbb{F}_2$ is a commutative ring with unity. The same proof works for any field K and any polynomial f.
Let $\deg(f) = n$. Like in the example we represent each residue class in L by the polynomial of smallest degree in it $L = \{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \mid a_i \in K\}$. Given that L is a commutative ring with unity for any field K and any polynomial f it remains to show the equivalence

$$L \text{ is a field } \iff f \text{ is irreducible.}$$

Let f be irreducible and let $0 \neq a(x) \in K[x]$ be a polynomial of degree $\deg(a) < n$. In $K[x]$ we have $\gcd(a(x), f(x)) = 1$ and Bézout's identity 3.4.16 leads to a representation

$$1 = a(x)u(x) + f(x)v(x), \text{ with } \deg(u) < n.$$

This implies $(a(x))^{-1} \equiv u(x) \bmod f(x)$ and because of the degrees, a and u are both representatives of classes in L and we obtain the identity of classes $(a(x))^{-1} = u(x)$.
To prove the other implication assume on the contrary that f splits as $f(x) = g(x) \cdot h(x)$, with $1 \leq \deg(g), \deg(h) < n$. Because of the degrees, g and h are representatives of their respective classes in L and they both do not represent the class of 0. However, we have $g \cdot h = f \equiv 0 \bmod f$ and thus $g \cdot h = 0$ in L which contradicts that fields do not have zero divisors. □

This theorem is the most important tool to construct finite fields of cardinality p^n with $n > 1$. All we need is to find is an irreducible polynomial of degree n over $\mathbb{F}_p$. Let us first consider some examples.

Example 5.5.4 *Let $K = \mathbb{F}_2$.*

a) The polynomial $f(x) = x$ is obviously irreducible but the residue class field $\mathbb{F}_2[x]/x\mathbb{F}_2[x] \cong \{a_0 \in \mathbb{F}_2\}$ is isomorphic to the field $\mathbb{F}_2$ itself.

b) Consider $f(x) = x^2 + 1$. We know from Example 5.4.1 that $f(x) = (x+1)^2$ is not irreducible. Consider the addition and multiplication tables modulo f.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

Since $(x+1)\cdot(x+1)=0$ this is not a field but only a ring.

c) Let $f(x)=x^2+x+1$; f is irreducible. By the previous lemma, $\mathbb{F}_2[x]/f\mathbb{F}_2[x]$ is a field. Given that the number of elements in

$$L=\mathbb{F}_2[x]/(x^2+x+1)\mathbb{F}_2[x]=\{a_0+a_1x|a_i\in\mathbb{F}_2, 0\leq i\leq 1\}$$

is 4 we have that L is a finite field with 4 elements. In Example 5.2.3 we investigated what the field $\mathbb{F}_4$ would look like. Note that the addition and multiplication tables we presented there apply directly to L with a representing the class of x and so we have now established that they define addition and multiplication in $\mathbb{F}_4$.

Exercise 5.5.5 *a) Show that $h(x)=(x^3+x+1)\in\mathbb{F}_2[x]$ defines a field with 8 elements. Give addition and multiplication tables of $\mathbb{F}_8\cong\mathbb{F}_2[x]/h\mathbb{F}_2[x]$.*

b) Let $\mathbb{F}_4$ be defined using the irreducible polynomial $f(x)=x^2+x+1$. Show by direct inspection that $k(y)=(y^3+y+1)$ has no roots over $\mathbb{F}_4$.

5.6 Existence and uniqueness of finite fields

We have now obtained a way of constructing finite fields by using irreducible polynomials over prime fields and mentioned that the same construction can also be used for an arbitrary base field. This raises the need to question whether the constructed fields are the same and whether we can always find an irreducible polynomial of the desired degree. This section is rather technical in nature but establishes a major result towards proving the existence and uniqueness of finite fields of prime power order.
The following definition and lemma hold in the context of arbitrary fields.

Definition 5.6.1 (Splitting field)
Let K be a field and let $f(x)\in K[x]$ be a polynomial. The splitting field of f *is the smallest field extension L of K so that f splits into linear factors in $L[x]$.*

We state the following lemma without proof. It is an important piece in the construction of finite fields but its proof is rather technical.

Lemma 5.6.2 *Let K be a field and let $f(x)\in K[x]$ be a polynomial. The splitting field of f exists and is unique up to isomorphism.*

Example 5.6.3 *a) The splitting field of $f(x)=x+1\in\mathbb{F}_2[x]$ is $\mathbb{F}_2$ itself since f is linear.*

b) The splitting field of $g(x) = x^2 + x + 1$ is $\mathbb{F}_4$ – by construction the class of x in $L = \mathbb{F}_2[x]/g\mathbb{F}_2[x]$ is a root of g. To see this consider $g(y) = y^2 + y + 1$ as polynomial in $L[y]$ and note that we compute modulo $x^2 + x + 1$ in L

$$(y + x)(y + x + 1) = y^2 + (x + x + 1)y + x^2 + x = y^2 + y + 1 = g(y).$$

c) Put $h(x) = (x^3 + x + 1) \in \mathbb{F}_2[x]$. This polynomial is irreducible over $\mathbb{F}_2$ and it thus allows to define a field with 8 elements as $\mathbb{F}_8 \cong \mathbb{F}_2[x]/h\mathbb{F}_2[x]$. By the same considerations as above the splitting field of h is $\mathbb{F}_8$.

d) Put $j(x) = (x^2 + x + 1)(x^3 + x + 1) \in \mathbb{F}_2[x]$. Over $\mathbb{F}_2$ the polynomial splits but not into linear factors. As seen right before the first factor splits in $\mathbb{F}_4$ while the second one splits only in $\mathbb{F}_8$. We know from Lemma 5.2.2 that $\mathbb{F}_4$ is not a subfield of $\mathbb{F}_8$ as $2 \nmid 3$ and so the splitting field of j must be $\mathbb{F}_{2^6}$, the smallest extension field of $\mathbb{F}_2$ containing both $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^3}$.

We now provide a *reducible* polynomial which is very important for the existence proof of finite fields.

Lemma 5.6.4 *Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ for some integer n. The splitting field of f is a finite field K with $|K| = p^n$ elements and f splits as*

$$x^{p^n} - x = \prod_{a \in K} (x - a).$$

Proof. We use the result of Exercise 5.4.4 c that a polynomial f has no multiple roots if and only if $\gcd(f, f') = 1$ when made monic. Here $f'(x) = p^n x^{p^n - 1} - 1 = -1$ since we are working in a field of characteristic p and thus $\gcd(f, f') = 1$. Put $q = p^n$.
The splitting field K of f exists by Lemma 5.6.2 and it contains the set $S = \{a \in K | a^q = a\}$. We just showed $|S| = q = p^n$. We now show that S is a subfield of K and by the minimality of the splitting field we obtain that $S = K$ is the splitting field of f.
The elements 0 and 1 are in S since they are roots of f.
Let $a, b \in S$. By Exercise 5.1.9 we have

$$(a - b)^q = a^q + (-b)^q = a^q - b^q = a - b \text{ and thus } (a - b) \in S,$$

where the second equality holds apparently in odd characteristic while in characteristic 2 there is no difference between $+$ and $-$. The third equality uses that $a, b \in S$.
The respective considerations for the multiplicative group are even easier. Let $a, b \in S$ then

$$\left(\frac{a}{b}\right)^q = \frac{a^q}{b^q} = \frac{a}{b} \text{ and thus } \frac{a}{b} \in S$$

and so indeed S is a subfield of K. □

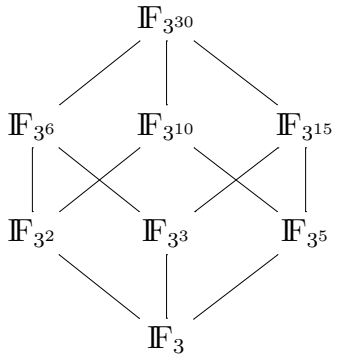
We now have all the knowledge needed to prove that finite fields of any prime power order q exist and that they are unique up to isomorphisms.

Theorem 5.6.5 (Existence and uniqueness of finite fields)
For any prime p and any natural number n there exists a finite field with p^n elements.
Every field with p^n elements is isomorphic to the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{F}_p$.

Proof. We start by noticing that for $n = 1$ the theorem is true as $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ exists and is unique up to isomorphism by Corollary 5.1.7.
Obviously the polynomial $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$ can be stated for any prime p and integer n. The existence and uniqueness of a field with p^n elements follows from the uniqueness of the splitting field of a polynomial, Lemma 5.6.2, and Lemma 5.6.4 showing that the splitting field of $f(x)$ is a finite field with p^n elements. □

It is also easy to give the complete list of subfields of a finite field $\mathbb{F}_q$ and the relations between the subfields by using Lemma 5.2.2. This is best done in a Hasse-diagram in which the largest field, in this case $\mathbb{F}_q$, is situated in the top row. The next row contains the direct subfields of $\mathbb{F}_q$, each of then connected with a line to $\mathbb{F}_q$ etc. The bottom level contains only the prime subfield $\mathbb{F}_q$.

Example 5.6.6 *Consider the finite field $\mathbb{F}_{3^{30}}$. By Lemma 5.2.2 any subfield $\mathbb{F}_{3^m}$ must satisfy $m|30$ and thus there are only the following subfields: $\mathbb{F}_3, \mathbb{F}_{3^2}, \mathbb{F}_{3^3}, \mathbb{F}_{3^5}, \mathbb{F}_{3^6}, \mathbb{F}_{3^{10}}$ and $\mathbb{F}_{3^{15}}$. This leads to the following Hasse-diagram:*



This easily allows to read off that $\mathbb{F}_{3^5}$ is a subfield of $\mathbb{F}_{3^{10}}, \mathbb{F}_{3^{15}}$ and $\mathbb{F}_{3^{30}}$ but not of $\mathbb{F}_{3^6}$ or any field on the same or a lower level.

Exercise 5.6.7 *State all subfields of $\mathbb{F}_{2^{24}}$ and their relations in a Hasse-diagram.*

5.7 Construction of finite fields

We have obtained that for any prime p and any natural number n there exists a finite field with p^n elements. We have a description of this field as splitting field of $x^{p^n} - x$; we also learned how to define a field as the ring of polynomials modulo an irreducible polynomial; and starting from an extension field we defined the minimal polynomial of an element – which is an irreducible polynomial. This section highlights the connections between these approaches.

Definition 5.7.1 *Let K be a field, let L be an extension field of K, and let $\theta \in L$. The smallest extension field of K containing θ is denoted by $K(\theta)$. It is called the* field obtained by adjoining θ to K.

Example 5.7.2 *a) The first example does not deal with finite fields but shows that we know the concept of adjoining elements to fields from other contexts.*

$$\mathbb{R}(i) = \{a + b \cdot i \mid a, b \in \mathbb{R}\} \cong \mathbb{C}\,.$$

b) Let α be a root of $j(x) = (x^2+x+1)(x^3+x+1)$ in $\mathbb{F}_{2^6}$. Depending on whether $\alpha^2 + \alpha + 1 = 0$ or $\alpha^3 + \alpha + 1 = 0$ we have $\mathbb{F}_2(\alpha) \cong \mathbb{F}_4$ or $\mathbb{F}_2(\alpha) \cong \mathbb{F}_8$.

We now highlight the connection between constructing fields by adjoining elements from extension fields and by using the ring of polynomials modulo an irreducible polynomial.

Lemma 5.7.3 *Let $\theta \in L$ and let $m_\theta(x)$ be the minimal polynomial of θ over K and $\deg(m_\theta) = m$. We have*

1. *$K(\theta) \cong K[x]/m_\theta K[x]$,*
2. *$\dim_K(K(\theta) : K) = m$, a basis of $K(\theta)$ over K is given by $\{1, \theta, \theta^2, \ldots, \theta^{m-1}\}$,*
3. *For every $\alpha \in K(\theta)$ there exists a minimal polynomial $m_\alpha(x) \in K[x]$, with $\deg(m_\alpha) | m$.*

Proof.

1. The evaluation at θ map $\tau : K[x] \to K(\theta)$, $f \mapsto f(\theta)$ is a ring homomorphism. The kernel of this map $\mathrm{Ker}(\tau)$ consists of the elements mapped to 0 in $K(\theta)$

   $$\mathrm{Ker}(\tau) = \{h(x) \in K[x] \mid h(\theta) = 0\} = (m_\theta(x))\,,$$

   where $(m_\theta(x))$ denotes the ideal generated by m_θ (that is all multiples of $m_\theta(x)$ in $K[x]$).

   According to Theorem 3.3.12 the image of τ is isomorphic to $K[x]/(\mathrm{Ker}(\tau)) \cong \mathrm{Im}(\tau)$. The set $\mathrm{Im}(\tau)$ contains θ (as image of $\tau(x) = \theta$). Therefore $K(\theta) = \mathrm{Im}(\tau)$.

2. From the first part we have that $\alpha \in K(\theta)$ is in the image of τ and can thus be represented as $f(\theta)$ for some $f \in K[x]$. Since all polynomials are reduced modulo m_θ it is enough to consider polynomials f with $\deg(f) < m$. So α equals a linear combination of $1, \theta, \ldots, \theta^{m-1}$ with coefficients from K and so each element is a linear combination of $1, \theta, \ldots, \theta^{m-1}$.

   To show that $1, \theta, \ldots, \theta^{m-1}$ form a basis we need to show that they are linearly independent over K. Assume on the contrary that there would be

coefficients $a_i \in K$, not all $a_i = 0$ for $0 \leq i < m$ so that $a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1} = 0$. The polynomial $h(x) = \sum_{i=0}^{m-1} a_i x^i$ would have θ as root and strictly lower degree than $m = \deg(m_\theta)$ which contradicts the definition of minimal polynomial.

3. According to Definition 5.5.2, α has a minimal polynomial over K. We have the following inclusion of finite extension fields $K \subseteq K(\alpha) \subseteq K(\theta)$. According to Lemma 5.2.2 the degrees of the extension fields divide each other leading to $\deg(m_\alpha) | \deg(m_\theta) = m$.

□

If we use an irreducible polynomial f of degree n to define an extension field there are n different roots of f over the splitting field which can be adjoined to the ground field. The following corollary which follows from the previous lemma shows that all choices are isomorphic.

Corollary 5.7.4 *Let $f(x) \in K[x]$ be irreducible and let L be the splitting field of f over K. Let α and β be roots of $f(x)$ over L.*
We have $K(\alpha) \cong K(\beta)$.

This shows that all m roots have the same effect on the splitting field. This is no surprise since we work modulo $f(x)$ and thus consider all m roots simultaneously.

Lemma 5.7.5 *Let $f(x) \in \mathbb{F}_q[x]$ be irreducible and let α be a root of $f(x)$ in some extension field $\mathbb{F}_{q^m}$. If a polynomial $h(x) \in \mathbb{F}_q[x]$ also has α as root, $h(\alpha) = 0$ then we have that $f(x)|h(x)$.*

Proof. According to Lemma 5.5.1 the minimal polynomial of α divides any polynomial $h(x)$ with $h(\alpha) = 0$. Let $LT(f) = a$ be the leading coefficient of f. The polynomial $a^{-1} \cdot f$ is monic and irreducible with root α and thus equals the minimal polynomial of α. □

Lemma 5.7.6 *Let $f(x) \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ of $\deg(f) = m$. Then $f(x)$ divides $x^{q^n} - x$ if and only if $m|n$.*

Proof. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ be the roots of $f(x)$ in the splitting field $L \cong \mathbb{F}_{q^m}$ of f over $\mathbb{F}_q$.
If $f(x) \mid x^{q^n} - x$ then $\alpha^{q^n} = \alpha$, and so L is a subfield of $\mathbb{F}_{q^n}$.
Since $[L : \mathbb{F}_q] = m$ and $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ one must have $m|n$ by Lemma 3.8.13.
If $m|n$ then $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ and so $\alpha \in \mathbb{F}_{q^n}$ and satisfies $\alpha^{q^n} = \alpha$ which implies $x^{q^n} \equiv x \bmod (x - \alpha)$. This holds not only for α but for all roots $\alpha_i, 1 \leq i \leq m$ of f. By the Chinese Remainder Theorem 3.5.13 it also holds modulo the product $f(x) = \prod_{i=1}^{m}(x - \alpha_i)$ and thus $f(x) | x^{q^n} - x$. □

We already know that an irreducible polynomial f of degree m over $\mathbb{F}_q$ can be used to construct $\mathbb{F}_{q^m}$. Since $\mathbb{F}_{q^m}$ is the splitting field of $x^{q^m} - x$ we now know that all roots of f are contained in $\mathbb{F}_{q^m}$.

Corollary 5.7.7 *Let $f \in \mathbb{F}_q[x]$ be irreducible of $\deg(f) = m$. Then $\mathbb{F}_{q^m}$ is the splitting field of f.*

The previous lemma is very useful as it states that every irreducible polynomial over $\mathbb{F}_p$ of degree n is a factor of $x^{p^n} - x$.
Even more is true:

Lemma 5.7.8 *The polynomial $f(x) = x^{q^n} - x$ is product of all monic, irreducible polynomials over $\mathbb{F}_q$ of degree dividing n.*

Proof. This lemma holds as each irreducible polynomial of degree m with $m|n$ divides f by Lemma 5.7.6, the polynomials are co-prime, and every irreducible polynomial of degree $m|n$ constructs a subfield of $\mathbb{F}_{q^n}$ and so its roots must satisfy f. □
However, the degree of this polynomial grows very quickly so that it is not possible to obtain irreducible polynomials by factoring it.
We know already that for any degree m and any finite field $\mathbb{F}_q$ there exists at least one irreducible polynomial over $\mathbb{F}_q$ since the finite field $\mathbb{F}_{q^m}$ exists and has dimension m over $\mathbb{F}_q$. Now we can compute the number of irreducible polynomials of a given degree.

Corollary 5.7.9 *Let $N_q(d)$ be the number of monic, irreducible polynomials over $\mathbb{F}_q$ of degree d. Then*

$$q^n = \sum_{d|n} dN_q(d).$$

In particular for all d and q we have $N_q(d) > 0$.

Corollary 5.7.4 shows that all roots (over some extension field) of a fixed irreducible polynomial give rise to the same field if adjoined to the ground field. Since for each order there is only one field up to isomorphism the resulting field is even independent of the choice of the polynomial.

Corollary 5.7.10 *Let $f, g \in \mathbb{F}_q[x]$ be irreducible, of the same degree $\deg(f) = \deg(g)$. Then their splitting fields are isomorphic.*

Exercise 5.7.11 *a) Find all irreducible polynomials of degree 1 and 2 over $\mathbb{F}_3$ and verify directly Lemma 5.7.8.*

b) Verify directly Lemma 5.7.8 for $n = 3$ and $q = 2$.

5.8 Conjugates, trace and norm

This section investigates connections between the roots of an irreducible polynomial and defines two important maps, the trace and the norm.

Lemma 5.8.1 *Let $f \in \mathbb{F}_q[x]$ be irreducible of degree m. Then f has a root α in $\mathbb{F}_{q^m}$ and all roots of f in $\mathbb{F}_{q^m}$ are different and given by*

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}} \in \mathbb{F}_{q^m}.$$

Proof. By Corollary 5.7.7 f splits completely over $\mathbb{F}_{q^m}$ and it has m roots. Let β be some root of f, we now show that then also $f(\beta^q) = 0$. Let $f(x) = \sum_{i=0}^{m} a_i x^i$.

$$\begin{aligned} f(\beta^q) &= a_0 + a_1\beta^q + a_2(\beta^q)^2 + \ldots + a_m(\beta^q)^m,\ a_i \in \mathbb{F}_q \Rightarrow a_i^q = a_i \\ &= a_0^q + a_1^q\beta^q + a_2^q(\beta^2)^q + \ldots + a_m^q(\beta^m)^q \\ &= \left(a_0 + a_1\beta + a_2\beta^2 + \ldots + a_m\beta^m\right)^q \\ &= (f(\beta))^q = 0^q = 0. \end{aligned}$$

This shows that with α also α^q is a root and thus also $\alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are roots of $f(x)$.
If any two of these powers would coincide, e.g. $\alpha^{q^i} = \alpha^{q^j}$ for some $0 \le i < j \le m-1$, then we would have $\alpha^{q^{m-j+i}} = \alpha^{q^m} = \alpha$ and α would satisfy $x^{q^{m-j+i}} - x$. By Lemma 5.7.5 this means that f divides $x^{q^{m-j+i}} - x$ and by Lemma 5.7.6 this implies that $m|(m-j+i)$ contradicting $0 \le i < j \le m-1$. □

The roots are thus q-th powers of one-another.

Definition 5.8.2 (Conjugates)
Let $\mathbb{F}_{q^m}$ be an extension field of $\mathbb{F}_q$ and let $\alpha \in \mathbb{F}_{q^m}$.
The elements $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ are called the conjugates of α.

We know the term "conjugates" from the complex numbers. Indeed there it refers to the same concept:

Example 5.8.3 *The field of complex numbers has degree $[\mathbb{C} : \mathbb{R}] = 2$ over the reals and we obtain $\mathbb{C}$ as $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$. The roots of x^2+1 are $i = \sqrt{-1}$ and $-i$. For $a_0 + a_1 i \in \mathbb{C}$ the conjugate is traditionally defined as $\overline{(a_0 + a_1 i)} = a_0 - a_1 i$. So the conjugate is obtained by changing the root of the irreducible polynomial.*

Example 5.8.4 *Let $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$ and let $f(x) \in \mathbb{F}_q[x]$ be irreducible of degree m and let the roots of $f(x)$ be $\beta, \beta^q, \ldots, \beta^{q^{m-1}}$. By Lemma 5.7.4 we have $\mathbb{F}_{q^m} \cong \mathbb{F}_q[x]/f\mathbb{F}_q[x] \cong \mathbb{F}_q(\beta)$. Let $\alpha = a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{m-1}\beta^{m-1}$. The conjugate α^q of α is given by*

$$\begin{aligned} \alpha^q &= a_0^q + a_1^q\beta^q + a_2^q\beta^2 + \ldots + a_{m-1}^q\left(\beta^q\right)^{m-1},\ a_i \in \mathbb{F}_q \\ &= a_0 + a_1\beta^q + a_2\left(\beta^q\right)^2 + \ldots + a_{m-1}\left(\beta^q\right)^{m-1} \end{aligned}$$

and so also in the case of finite fields the conjugates are obtained by changing the root in the representation.

We note that computing q-powers is a homomorphism of the field to itself. In the context of extension fields we need a more detailed definition.

Definition 5.8.5 (Automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$)
An automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is an isomorphism of $\mathbb{F}_{q^m}$ that leaves every element of $\mathbb{F}_q$ invariant.

Note that it is not enough that the field $\mathbb{F}_q$ is kept invariant, each individual element must remain fixed.

Lemma 5.8.6 *The automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are exactly the maps $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, where $\sigma_i(\alpha) = \alpha^{q^i}$ for $\alpha \in \mathbb{F}_{q^m}$ and $0 \leq i \leq m-1$.*

Proof. The maps σ_i are field homomorphisms by Exercise 5.1.9.
For any $0 \leq i \leq m-1$ one has that the only element α with $\sigma_i(\alpha) = \alpha^{q^i} = 0$ is $\alpha = 0$ and thus the maps are injective. Since they operate of finite sets of the same cardinality they are also surjective and thus they are isomorphisms.
The elements of $a \in \mathbb{F}_q$ are exactly those elements in $\mathbb{F}_{q^m}$ which satisfy $a^q = a$ and thus each σ_i leaves any element of $\mathbb{F}_q$ fix.
On a finite set every isomorphism can be described as a polynomial. The field $\mathbb{F}_q$ is defined as the set of roots of $x^q - x$ and so every automorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ must be a power of σ_1. Since $\sigma_m = \sigma_0$ these are all possibilities. □

Definition 5.8.7 (Frobenius automorphism)
The automorphism $\sigma = \sigma_1$ is called the Frobenius automorphism. *It operates by raising each element to the q-th power.*

Definition 5.8.8 (Trace)
Let $\alpha \in \mathbb{F}_{q^m}$. The relative trace of α over $\mathbb{F}_q$ *denoted by $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ is given by*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

If $\mathbb{F}_q = \mathbb{F}_p$ is a prime field then $\mathrm{Tr}_{\mathbb{F}_{p^m}/\mathbb{F}_p}$ is called the absolute trace *or just* trace. *In this case the index of* Tr *is often skipped.*

With the notation from above the trace $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ of α is the sum of all conjugates of α over $\mathbb{F}_{q^m}$. We now define the multiplicative analogue.

Definition 5.8.9 (Norm)
Let $\alpha \in \mathbb{F}_{q^m}$. The relative norm of α over $\mathbb{F}_q$ *denoted by $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha)$ is given by*

$$N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \alpha \cdot \alpha^q \cdot \ldots \cdot \alpha^{q^{m-1}}.$$

If $\mathbb{F}_q = \mathbb{F}_p$ is a prime field then $\mathrm{N}_{\mathbb{F}_{p^m}/\mathbb{F}_p}$ is called the absolute norm *or just* norm. *In this case the index of* N *is often skipped.*

Lemma 5.8.10 *The images of the relative trace map and of the relative norm map are contained in $\mathbb{F}_q$*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q, \ \mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q,$$

for all $\alpha \in \mathbb{F}_{q^m}$.

Proof. Let $m_\alpha(x) \in \mathbb{F}_q[x]$ be the minimal polynomial of α over $\mathbb{F}_q$ and let $m_\alpha(x) = \sum_{i=0}^{r} a_i x^i$ for some $r = [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. By Lemma 5.7.3 we have $r|m$ and m_α defines an extension field $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$. Lemma 5.8.1 we have

$$\begin{aligned}\prod_{i=0}^{m-1}\left(x-\alpha^{q^i}\right) &= \prod_{i=0}^{r-1}\left(x-\alpha^{q^i}\right)\cdot\prod_{i=0}^{r-1}\left(x-\alpha^{q^{i+r}}\right)\cdot\ldots\cdot\prod_{i=0}^{r-1}\left(x-\alpha^{q^{i+r(\frac{m}{r}-1)}}\right)\\ &= \underbrace{\prod_{i=0}^{r-1}\left(x-\alpha^{q^i}\right)\cdot\ldots\cdot\prod_{i=0}^{r-1}\left(x-\alpha^{q^i}\right)}_{\frac{m}{r}\text{ times}}\\ &= m_\alpha(x)^{\frac{m}{r}}\end{aligned}$$

Since $m_\alpha \in \mathbb{F}_q[x]$ also its $\frac{m}{r}$-th power has all coefficients in $\mathbb{F}_q$. The coefficient of the second highest term equals $-(\alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}) = -\mathrm{Tr}(\alpha)$ while the constant term equals the norm.
By comparison we obtain

$$r\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = -ma_{m-1} \in \mathbb{F}_q$$

and

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = a_0^{\frac{m}{r}} \in \mathbb{F}_q.$$

□

We note some properties of the trace.

Lemma 5.8.11 *Let L be a finite extension of K with $[L : K] = m$ and let $\alpha, \beta \in L, c \in K$. For the relative trace $\mathrm{Tr}_{L/K}$ we have:*

1. $\mathrm{Tr}_{L/K}(\alpha + \beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$,
2. $\mathrm{Tr}_{L/K}(c \cdot \alpha) = c \cdot \mathrm{Tr}_{L/K}(\alpha)$,
3. $\mathrm{Tr}_{L/K}(c) = m \cdot c$,
4. $\mathrm{Tr}_{L/K}(\alpha^q) = \mathrm{Tr}_{L/K}(\alpha)$.

Proof. Given below as homework. □

One also has the corresponding properties of the norm.

Lemma 5.8.12 *Let L be a finite extension of K with $[L : K] = m$ and let $\alpha, \beta \in L, c \in K$. For the relative norm $\mathrm{N}_{L/K}$ we have:*

1. $\mathrm{N}_{L/K}(\alpha \cdot \beta) = \mathrm{N}_{L/K}(\alpha) \cdot \mathrm{N}_{L/K}(\beta)$,
2. $\mathrm{Im}(\mathrm{N}_{L/K}) = K$ *and* $\mathrm{Im}(\mathrm{N}_{L/K}|_{L^*}) = K^*$
3. $\mathrm{N}_{L/K}(c) = c^m$,
4. $\mathrm{N}_{L/K}(\alpha^q) = \mathrm{N}_{L/K}(\alpha)$.

Proof. Given below as homework. □

Exercise 5.8.13 *a) Prove Lemma 5.8.11 by just using the definition.*

b) Prove Lemma 5.8.12 by just using the definition.

5.9 Irreducible polynomials

As stated before it is too expensive to factor $x^{q^m} - x$ over $\mathbb{F}_q$ to find an irreducible polynomial of degree m over $\mathbb{F}_q$ and to construct the extension field $\mathbb{F}_{q^m}$. A more careful analysis of the number $N_q(d)$ of irreducible polynomials of degree d over $\mathbb{F}_q$ given in Corollary 5.7.9 gives the probability that a randomly chosen polynomial of degree d is irreducible.
In this section we state a criterion to determine whether a given polynomial is irreducible. There is a vast literature on factorization of polynomials over finite fields and on constructing irreducible polynomials. We would like to refer the interested reader to a few books covering this topic.

- H. Cohen, "A Course in Computational Algebraic Number Theory", Springer
- J. von zur Gathen and J. Gerhard, "Modern Computer Algebra", Cambrigde University Press.
- M. Pohst and H. Zassenhaus, "Algorithmic Algebraic Number Theory", Cambridge University Press.

and the books by Lidl and Niederreiter and by Shoup mentioned in the introduction to this chapter.
We present here the *Rabin test* which allows to test whether a polynomial is irreducible.

Lemma 5.9.1 (Rabin test)
The polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $\deg(f) = m$ is irreducible if and only if

$$f(x) \Big| x^{q^m} - x$$

and for all divisors $d|m, d < m$ one has

$$\gcd(f(x), x^{q^d} - x) = 1.$$

Proof. We first note that all conditions hold for an irreducible polynomial of degree m. It remains to be shown that they are sufficient. Let f split into factors $f = f_1 \cdots f_r$ over $\mathbb{F}_q$, where $r \geq 1$.
By Lemma 5.7.8 $x^{q^m} - x$ is the product of all irreducible polynomials of degree dividing m. So if the first property holds we must have $\deg(f_i)|m$ for $1 \leq i \leq r$. If $r > 1$ the degree $\deg(f_1)$ equals one of the d in the second round of tests and $f_1|x^{q^d} - x$ for this d. So f is irreducible only if also the second property holds. Since any factor of f must lead to a non-trivial gcd for some d we also have that this condition is sufficient. □

For efficiency it might be interesting to note that one can release the second property to testing only that for all prime divisors $\ell|m$ one has

$$\gcd(f, x^{q^{m/\ell}} - x) = 1.$$

For a random polynomial it is likely that the condition $\gcd(f, x^{q^d} - x) = 1$ fails for some small d so that it is computationally more efficient to have an early abort after it. If, however, the candidate polynomial is likely to be irreducible and thus all checks are expected to be done anyway this observation saves running time.

Example 5.9.2 *Find an irreducible polynomial of the form $x^3 - a$ over $\mathbb{F}_7$. This can still be done by a naive approach since a polynomial of degree 3 is irreducible if and only if it does not have a root. In this case if $a \neq 0, 1, -1$. So $x^3 - 2$ is irreducible.*
Use of the Magma online calculator available at http://magma.maths.usyd.edu.au/calc/ *makes it easy to implement the Rabin test and it even comes with a built-in in function* `IsIrreducible`.

Irreducible polynomials with only two terms as considered in this example are interesting for constructing finite fields. In low weight polynomials have special names.

Definition 5.9.3 (Binomial, trinomial, pentanomial) *A polynomial of the form $x^n + a_0$ with two non-zero coefficients is called a* binomial.
A polynomial of the form $x^n + a_m x^m + a_0$ with three non-zero coefficients is called a trinomial.
A polynomial of the form $x^n + a_m x^m + a_l x^l + a_k x^k + a_0$ with five non-zero coefficients is called a pentanomial.

We first note that over $\mathbb{F}_2$ there cannot be an irreducible binomial as 0 or 1 would be a root. It is a bit more surprising that there cannot be an irreducible binomial of even degree over $\mathbb{F}_2^n$.
The following lemma considers irreducible binomials over arbitrary finite fields.

Lemma 5.9.4 *Let n be prime. An irreducible binomial $f(x) = x^n + a_0$ of degree n over $\mathbb{F}_q$ exists if and only if $n|q - 1$.*

Proof. If $n \nmid q-1$ then the map $\tau : \mathbb{F}_q \to \mathbb{F}_q; a \mapsto a^n$ is a bijection by Corollary 5.3.4 and thus every element a_0 is an n-th power and any binomial of degree n has a linear factor over $\mathbb{F}_q$.

If, however, $n|q-1$ then τ has a non-trivial kernel and each element in the image has n pre-images. Choose $a_0 \notin \mathrm{Im}(\tau)$ and so f has no linear factor over $\mathbb{F}_q$. Then the last property of the Rabin test holds since n is prime.

For the first property note that $n|q-1$ implies that there is some integer k with $q = 1+kn$ and thus $q^n - 1 = (1+kn)^n - 1 = 1+nkn+\binom{n}{2}(kn)^2+\cdots(kn)^n - 1 = n^2k\ell = n(q-1)\ell$ for some ℓ.To show that $f(x) = x^n + a_0$ divides $x^{q^n} - x$ note

$$x^{q^n} - x = x(x^{q^n-1}-1) = x(x^{n(q-1)\ell}-1) \equiv x(a_0^{(q-1)l}-1) = x(1-1) = 0 \bmod x^n + a_0$$

using $a_0^{q-1} = 1$. □

5.10 Arithmetic in binary fields

In Section 5.5 we have seen that an extension field $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$ can be represented using a polynomial basis. Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n. Then we have by Lemma 5.7.3 that

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/f(x)\mathbb{F}_q[x] = \left\{ \sum_{i=0}^{n-1} a_i x^i + f(x)\mathbb{F}_q[x] \middle| a_i \in \mathbb{F}_q \right\}.$$

In this section we consider the special case $q = 2$ which is very important for applications, particularly for hardware implementations. An advantage of such *binary fields* is that additions are `XOR`s and that in squarings no mixed terms need to be considered as by Exercise 5.1.9 we have $(a+b)^2 = a^2 + b^2$.

For multiplications and squarings it is necessary to reduce the resulting polynomial of degree $\geq n$ modulo the irreducible polynomial $f(x)$ to obtain the unique remainder modulo f of degree less than n.

Example 5.10.1 *The polynomial* $f(x) = x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1 \in \mathbb{F}_2[x]$ *is irreducible. To compute the product* $(x^9+x^7+x^4+x^2+1)\cdot(x^8+x^6+x^5+x^3+x^2)$ *in* $\mathbb{F}_{2^{10}}$ *we first compute the product in* $\mathbb{F}_2[x]$ *and then*

reduce the result modulo $f(x)$. The steps are as follows:

$$
\begin{aligned}
&(x^9+x^7+x^4+x^2+1)\cdot(x^8+x^6+x^5+x^3+x^2)=\\
&x^{17}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2=\\
&x^7\cdot x^{10}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2=\\
&(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+\\
&\qquad +x^8+x^7)+x^{14}+x^{13}+x^{12}+x^{11}+\\
&\qquad +x^{10}+x^4+x^3+x^2=\\
&x^{16}+x^{15}+x^9+x^8+x^7+x^4+x^3+x^2=\\
&x^6\cdot x^{10}+x^{15}+x^9+x^8+x^7+x^4+x^3+x^2=\\
&x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^6+x^4+x^3+x^2=\\
&x^4\cdot x^{10}+x^{13}+x^{12}+x^{11}+x^{10}+x^6+x^4+x^3+x^2=\\
&x^9+x^8+x^7+x^5+x^3+x^2.
\end{aligned}
$$

Note, that $g(x)=x^{10}+x^3+1$ is an irreducible polynomial of degree 10 over $\mathbb{F}_2$. Reducing modulo g has much easier iterations since x^{10} is replaced by only two terms x^3+1. Since g is sparse it also becomes useful to replace more than one power simultaneously.

$$
\begin{aligned}
&(x^9+x^7+x^4+x^2+1)\cdot(x^8+x^6+x^5+x^3+x^2)=\\
&x^{17}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2=\\
&x^7\cdot x^{10}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2=\\
&(x^{10}+x^7)+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^4+x^3+x^2=\\
&x^{14}+x^{13}+x^{12}+x^{11}+x^7+x^4+x^3+x^2=\\
&(x^4+x^3+x^2+x)\cdot x^{10}+x^7+x^4+x^3+x^2=\\
&x^6+x^5+x^4+x.
\end{aligned}
$$

We deduce from this example that it is useful to choose irreducible polynomials with as few terms as possible.

Lemma 5.10.2 *For all $n,m\in\mathbb{N}, n>1$ the binomial $x^n+x^m\in\mathbb{F}_2[x]$ is not irreducible.*
More generally, there is no irreducible polynomial over $\mathbb{F}_2$ with an even number of nonzero terms.

Proof. If $m>0$ then x^n+x^m is divisible by x^m and thus not irreducible. If $m=0$ we see that 1 is a root of x^n+1.
Consider $f(x)=\sum_{i=1}^{2m}x^{k_i}$, where $k_i<k_{i+1}$ for all $1\le i\le 2m-1$. If $k_1>0$ we have that x^{k_0} divides $f(x)$ while otherwise 1 is a root of it since we are working in characteristic 2. □

As the example showed, there are extension degrees n for which there exists an irreducible trinomial. To construct $\mathbb{F}_{2^n}$ for a given n, it is best to use an

irreducible trinomial if one exists. Note that if an irreducible trinomial exists there is one $x^n + x^m + 1$ for which $m \leq n/2$.
By the lemma we know that there are no irreducible polynomials with 4 nonzero coefficients, so if no suitable trinomial exists one should search for an irreducible *pentanomial*. It is conjectured that for all binary fields for which there is no irreducible trinomial one can find an irreducible pentanomial. Even though this is not proven, all fields of cryptographic interest have been checked. So in applications we can always find an irreducible trinomial or pentanomial.
For a table of irreducible polynomials consult Gadiel Seroussi's paper "Table of Low-Weight Binary Irreducible Polynomials".

Remark 5.10.3 *For more details on the implementation of binary fields the reader is encouraged to check the literature for* normal basis *representations. A normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is a basis of the form $\{\theta, \theta^2, \theta^{2^2}, \theta^{2^3}, \ldots, \theta^{2^{n-1}}\}$. Note that for most values $\alpha \in \mathbb{F}_{2^n}$ the conjugates of α do not form a basis, so* normal elements *are special.*
An advantage of normal bases is that they lead to very fast squarings:

$$\text{If } a = \sum_{i=0}^{n-1} a_i \theta^{2^i} \text{ then } a^2 = \sum_{i=0}^{n-1} a_{i-1} \theta^{2^i},$$

where the index i of a_i is considered modulo n. This means that a squaring can be implemented as a cyclic shift of the coordinates from $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ to $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$. Likewise, squareroots can be implemented by a cyclic left-shift. On the downside, in software multiplications are usually less efficient than in a polynomial basis. So it depends on the application and in particular on the importance of squarings in it whether a normal basis or a polynomial basis representation should be chosen. In hardware implementation the situation is yet again different and normal bases can be the clear winner.

Exercise 5.10.4 *a) State all irreducible polynomials of degree 3 and of degree 4 over $\mathbb{F}_2$.*

b) The polynomial $f(x) = x^{97} + x^6 + 1$ is irreducible over $\mathbb{F}_2$. We can use it to construct $\mathbb{F}_{2^{97}} \cong \mathbb{F}_2[x]/f(x)\mathbb{F}_2[x]$. Compute $(x^{86} + x^{25} + x^{13} + x^4 + x^2 + x + 1) \cdot (x^{83} + x^{31} + x^{17} + x^7 + x^3)$ modulo $f(x)$.

c) The polynomial $g(x) = x^{89} + x^6 + x^5 + x^3 + 1$ is irreducible over $\mathbb{F}_2$. We can use it to construct $\mathbb{F}_{2^{89}} \cong \mathbb{F}_2[x]/g(x)\mathbb{F}_2[x]$. Compute $(x^{86} + x^{25} + x^{13} + x^4 + x^2 + x + 1) \cdot (x^{83} + x^{31} + x^{17} + x^7 + x^3)$ modulo $g(x)$. Compare the time you needed for the multiplication in this exercise and in the previous one. Note that the previous one deals with a larger finite field.

5.11 Arithmetic in prime fields

There exists a vast amount of literature on fast implementations of prime fields. We do not go into the details here but comment that to speed up modular reductions it is useful to choose primes which are close to a power of 2, or even better

close to a power of 2^w, where w is the word size, i.e. $p = (2^w)^k - c$, where $c \in \mathbb{N}$ is small. This approach is analogous to choosing irreducible trinomials in binary fields.

5.12 Arithmetic in optimal extension fields

Optimal extension fields (OEFs) are finite fields $\mathbb{F}_{q^n}$ where the base field $\mathbb{F}_q$ and the extension degree n are chosen such that arithmetic in $\mathbb{F}_q$ can be implemented particularly fast. A common choice for the base field is $\mathbb{F}_q = \mathbb{F}_p$, a prime field, such that p fits into the word size and is close to a power of two, i.e. $p = \texttt{PreviousPrime}(2^w)$, where w is the word-size. The extension degree n is often chosen to be prime, particularly in applications to elliptic curve cryptography – we will not go into the details here but mention that Weil descent attacks on elliptic curves may apply when the extension degree is not prime. As we have seen in the section on binary fields, it is interesting to work with irreducible polynomials with few nonzero coefficients. If q is odd we can hope for irreducible *binomials*.

Lemma 5.12.1 *Let n and p be primes such that $p \equiv 1 \bmod n$. The binomial $x^n - a$ is irreducible over $\mathbb{F}_p$ if and only if a is not an nth power in $\mathbb{F}_p$.*

Proof. If a is an nth power in $\mathbb{F}_p$, i.e. there exists a $b \in \mathbb{F}_p$ with $b^n = a$, then clearly $x^n - a$ is not irreducible since b is a root.
If a is not an nth power then there is no root of $f(x) = x^n - a$ over $\mathbb{F}_p$. The condition $n \equiv 1 \bmod p$ means that the nth roots of unity are in $\mathbb{F}_p$, i.e. there are n elements $u_i \in \mathbb{F}_p, 1 \leq i \leq n$ with $u_i^n = 1$. To fix notation let $u_1 = 1$. Let α be a root of $f(x)$ over some extension field $\mathbb{F}_{p^m}$. The multiples $u_i\alpha$ for $2 \leq i \leq n$ are distinct from α, are defined over the same extension field $\mathbb{F}_{p^m}$ and are also roots of $f(x)$ because

$$(u_i\alpha)^n = u_i^n\alpha^n = \alpha^n = a.$$

Since there are n of them they are exactly the roots of $f(x)$ and so they are the conjugates of α. This means that α is defined over a field of extension degree no less than n, and so α is defined exactly over $\mathbb{F}_{p^n}$. We have $\mathbb{F}_{p^n} \cong \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(x^n - a)\mathbb{F}_p$. □

Following this lemma, optimal extension fields are finite fields $\mathbb{F}_{p^n}$ for which p is a prime closely related to the word-size, n satisfies $n \equiv 1 \bmod p$ and the extension field is constructed with an irreducible binomial $f(x) = x^n - a$.

Chapter 6

Elliptic Curves

In public key cryptography elliptic curves over finite fields are of ever-growing importance. Now that we know the theoretical background of finite fields and algebra we are ready to define them and show how to compute efficiently on them. In this chapter we consider curves given by an equation of the form

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6, \tag{6.1}$$

where the a_i are elements of a field K and where we have some additional requirements on the coefficients. For a pictorial description we first consider the case $K = \mathbb{R}$. This is not used in cryptography but has the advantage that we can easily sketch the curve and define a group law on the set of points. In the second section we give the mathematical background to curves over arbitrary fields, then we specialize to finite fields. If the group of points is used in a cryptosystem, the group operation need to be as fast as possible. We give optimized formulae for prime fields $\mathbb{F}_p$ with $p > 3$, binary fields $\mathbb{F}_{2^n}$ and briefly comment on optimal extension fields (OEFs).

It is hard to find suitable text books. For the reader interested in mathematics the books by Silverman contain a lot of interesting material. An easier introduction is provided in Silverman and Tate. All these books are not specific to cryptographic applications. Koblitz – one of the proposers of elliptic curve cryptography – wrote two textbooks which contain material on elliptic curves. The Certicom tutorial does not go beyond the material covered in this chapter. The java applets for actively playing with an elliptic curve are worth a visit to that page. Recently, 4 books on elliptic (and more general hyperelliptic) curve cryptography have been published. They all contain the material covered here and are strongly recommended for further reading; however, none of them is a text book.

- R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press.
- I. F. Blake, G. Seroussi, N. P. Smart, Elliptic Curves in Cryptography, Cambridge University Press.

- I. F. Blake, G. Seroussi, N. P. Smart, Advances in Elliptic Curve Cryptography, Cambridge University Press
- Certicom, Online Elliptic Curve Cryptography Tutorial, at https://www.certicom.com/content/certicom/en/ecc-tutorial.html
- D. Hankerson, A. J. Menezes, S. A. Vanstone, Guide to Elliptic Curve Cryptography, Springer.
- N. Koblitz, A Course in Number Theory and Cryptography, Springer.
- N. Koblitz, Algebraic Aspects of Cryptography, Springer.
- J. H. Silverman, The Arithmetic of Elliptic Curves, Springer.
- J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer.
- J. H. Silverman, J. Tate, Rational Points on Elliptic Curves, Springer.

6.1 Considerations over the real numbers

This section is meant to provide an intuitive understanding of elliptic curves. All definitions are repeated in the next section in more generality.

Definition 6.1.1 (Elliptic curve over the reals) *An* elliptic curve over the real numbers $\mathbb{R}$ *can be defined by an equation of the form*

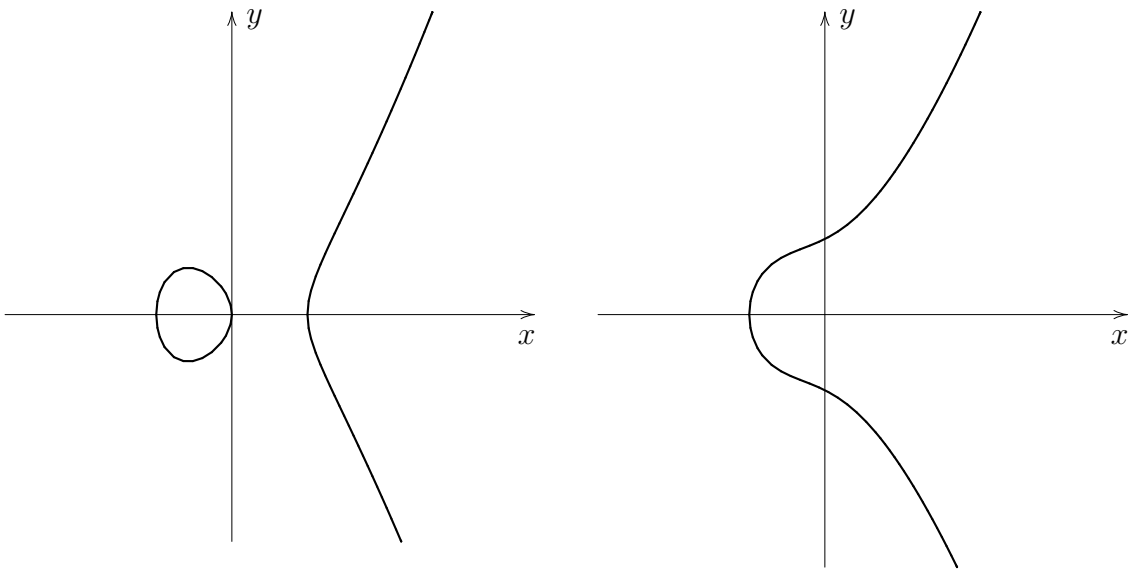
$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \quad \textit{where } a_2, a_4, a_6 \in \mathbb{R}. \tag{6.2}$$

Vice versa, if $x^3 + a_2x^2 + a_4x + a_6$ is square-free, then (6.2) defines an elliptic curve.

Note that the above means that equation (6.2) does not define an elliptic curve, if $x^3 + a_2x^2 + a_4x + a_6$ has a repeated root.
As a shorthand we write $f(x) = x^3 + a_2x^2 + a_4x + a_6$. We consider real solutions to equations of the form (6.2), i.e. points $P = (x_P, y_P)$, with $x_P, y_P \in \mathbb{R}$, which satisfy the curve equation. To sketch the set of solutions in $\mathbb{R}^2$, we first observe that there are either 1 or 3 points with y-coordinate 0, i.e. points on the x-axis, depending on whether $f(x)$ has 1 or 3 real roots. If $f(b) = 0$ then $(b, 0)$ is a point on the curve since indeed $0^2 = f(b) = 0$.
The curve equation is symmetric with respect to the x-axis. If $P = (x_P, y_P)$ satisfies the curve equation then so does the coordinate tuple $(x_P, -y_P)$.
Let $f(x)$ split as $f(x) = (x - b_1)(x - b_2)(x - b_3)$ with $b_1 < b_2 < b_3$. In $\mathbb{R}$ every positive number has two squareroots while negative numbers do have no squareroots. If $x_P < b_1$ then $f(x_P) < 0$ since all three factors are negative. This means that there are no points with x-coordinates smaller than b_1. For $b_1 < x_P < b_2$ we have $f(x_P) > 0$ and thus there are two points with x-coordinate

x_P. Between b_2 and b_3 there are no points while for $x_P > b_3$ we obtain $f(x_P) > 0$ and thus there exist points for all values larger than the largest root of f.

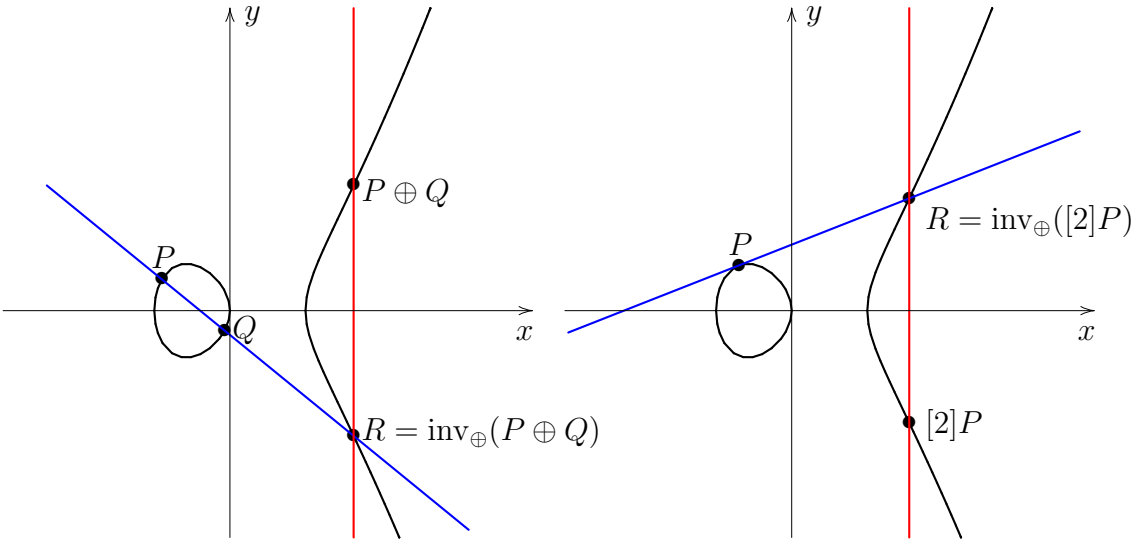
The following two pictures correspond to the cases of $x^3 + a_2x^2 + a_4x + a_6$ having 1 or 3 real roots, in particular the equations $y^2 = (x+1)x(x-1)$ and $y^2 = (x+1)(x^2+1)$ were drawn.



It is possible to define a group law on the points of an elliptic curve and describe the rules in a very pictorial way.

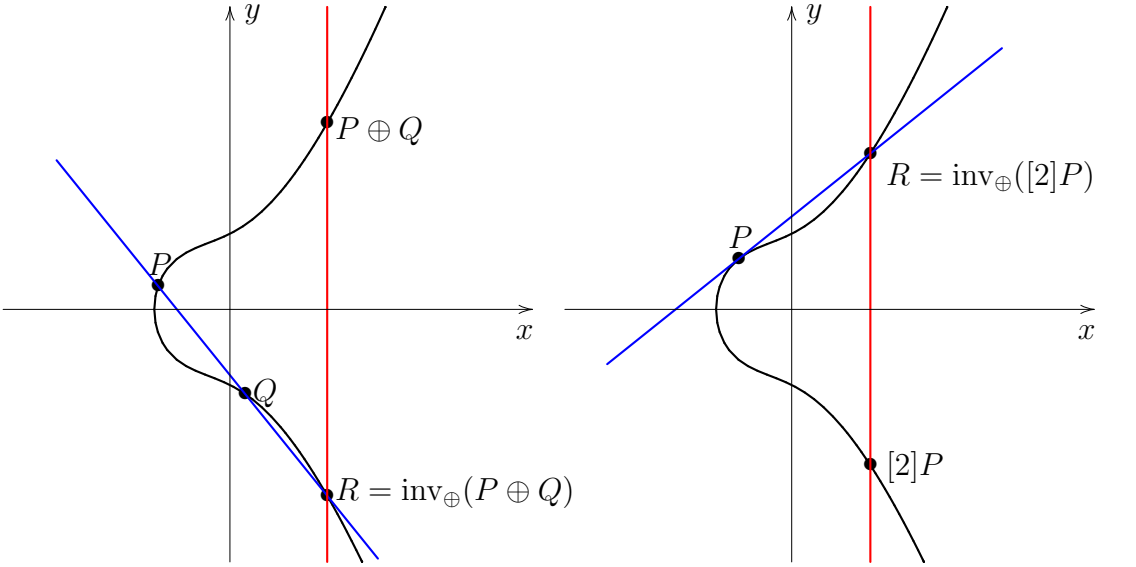
Let $\{P = (x_P, y_P) \mid x_P, y_P \in \mathbb{R} \text{ with } y_P^2 = x_P^3 + a_2x_P^2 + a_4x_P + a_6\}$ be the set of real points on the curve. To define a group law we need to include one further point, P_∞. In the picture it should be thought of as lying in the direction of the y-axis infinitely far out so that every line through the y-axis intersects it. Readers familiar with non-Euclidean geometry will recognize this as the point at infinity in which all lines parallel to the y-axis intersect. Let G be the union of the *affine points* (given by 2 coordinates) and the point at infinity. We define the group operation $\oplus$ on points $P, Q \in G$ by the following procedures for adding two different points $P, Q \neq P_\infty$ and for doubling one point $P \neq P_\infty$. We will deal

with the special cases after the general description.



1. To add the points P and Q draw the line connecting them. This line is intersecting the curve in exactly one more point R.
2. Draw a line parallel to the y-axis through R.
3. The other point of intersection with the curve is $P \oplus Q$.
4. To double the point P draw the tangent line to the curve at the point P in place of the connecting line and proceed as above.

The following picture shows the same group law for the other form of curve where there is only one real root of $x^3 + a_2x^2 + a_4x + a_6$.



Now we go into the details of this operation and handle special cases. We first notice that the procedure is totally symmetric, so the roles of P and Q can be interchanged, i.e. $P \oplus Q = Q \oplus P$ for all $P, Q \in G$, and we have an abelian group

The procedure for adding two points fails if we have $P = (x_P, y_P)$ and $Q = (x_P, -y_P)$ since their connecting line is vertical and there is no visible point in which this line would intersect the curve. Remember that the point at infinity P_∞ should be seen as way out on the y-axis and so it is the third point. Since all vertical lines go through P_∞ *the* vertical line through it, requested by the adding operation, is not an ordinary line. We define that the resulting point is P_∞, i.e. $(x_P, y_P) \oplus (x_P, -y_P) = P_\infty$.
The addition $P \oplus P_\infty$ is similarly not covered by the pictorial description. Like before, the connecting line is the vertical line trough P. The third point of intersection is the point $(x_P, -y_P)$ which has the same x-coordinate as P and negative y-value. The last step of mirroring the intermediate result on the x-axis leads to P as the resulting point. So, for any $P \in G \backslash \{P_\infty\}$ we have

$$P \oplus P_\infty = P \text{ and likewise } P_\infty \oplus P = P.$$

Finally, we define $P_\infty \oplus P_\infty = P_\infty$, so P_∞ operates as neutral element.
Since we noticed in the last paragraph that $(x_P, y_P) \oplus (x_P, -y_P) = P_\infty$, we have that $\text{inv}_\oplus(x_P, y_P) = (x_P, -y_P)$. We include $inv_\oplus(P_\infty) = P_\infty$ in the descriptions.
If P has a vertical tangent – in this example if P is one of $(-1, 0), (0, 0)$ and $(1, 0)$ – then $P = \text{inv}_\oplus(P)$ and so $[2]P = P_\infty$. So the points with vertical tangent have order $\text{ord}(P) = 2$.
We now have defined a group operation on all elements of G and if the statement holds true, that there always is a third point on the line, then G is closed under the operation $\oplus$. In the next section we will introduce formulae to compute the coordinates of $P \oplus Q$ given the coordinates of P and Q. The computations make clear that indeed there is always exactly one more point of intersection. Note, that we count the point twice if the line is tangent to it. If the point is a point of inflection (the curvature of the curve changes sign, so the tangent crosses the curve) then we count the point even three times.
We have identified P_∞ as the neutral element and know that $\text{inv}_\oplus(x_P, y_P) = (x_P, -y_P)$ and $P \oplus Q = Q \oplus P$. To summarize, we have shown all group properties except for associativity. Proving it is cumbersome with the methods we have at hand. Clearly, one can take the formulae developed in the next section and show that $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ for any $P, Q, R \in G$ but going through all possible cases takes a lot of time and is not instructional. We therefore skip the proof and refer to the literature, in particular to the "Handbook of Elliptic and Hyperelliptic Curve Cryptography".

Exercise 6.1.2 *a) Sketch the curve given by $E_1 : y^2 = x^3 - 3x^2 - x + 3$ over the reals. Does E_1 define an elliptic curve?*

b) Sketch the curve given by $E_2 : y^2 = x^3$ over the reals. Does E_2 define an elliptic curve?

c) Show that the points $P = (0, \sqrt{3})$ and $Q = (1, 0)$ are on E_1. Draw the computation of $[2]P$ and $P \oplus Q$.

d) State the coordinates of $\text{inv}_\oplus(P)$ and $\text{inv}_\oplus(Q)$. Find the coordinates of at least one more point which is not equal to its inverse or to $\text{inv}_\oplus(P)$.

6.2 Formulae for group operation over the reals

To enable a computer to perform the group operation we need to translate this pictorial description into operations involving the curve coefficients a_2, a_4, and a_6 and the coordinates of the two points P and Q. Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, and $P \oplus Q = S = (x_S, y_S)$. We first derive the formulae for addition of two general points P and $Q \neq P, P_\infty, \mathrm{inv}_\oplus(P)$ and then consider doubling.

Addition The line connecting P and Q is of the form $y = \lambda x + \mu$, where λ is the slope and μ is the intercept. Inserting the coordinates we obtain

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

for the slope. Since P is a point on the line, i.e. $y_P = \lambda x_P + \mu$, we get

$$\mu = y_P - \lambda x_P = y_P - \frac{y_Q - y_P}{x_Q - x_P} x_P.$$

The points P, Q, and R are the points in which the line intersects the curve. This means that their coordinates satisfy both, the curve equation and the equation of the line. To find the coordinates of R we equate the expressions for y^2 and obtain

$$(\lambda x + \mu)^2 = x^3 + a_2 x^2 + a_4 x + a_6.$$

We transform this equation to obtain 0 on the left-hand side. Recall, that the equation was constructed so that x_P, x_Q and x_R are the roots of the resulting polynomial. By Lemma 3.7.8 this means that the polynomial is divisible by $(x - x_P), (x - x_Q)$, and $(x - x_R)$. Since the polynomial is of degree 3 it must be equal to $(x - x_P)(x - x_Q)(x - x_R)$ so that we obtain

$$\begin{aligned} 0 &= x^3 + (a_2 - \lambda^2)x^2 + (a_4 - 2\lambda\mu)x + a_6 - \mu^2 \\ &= (x - x_P)(x - x_Q)(x - x_R) \\ &= x^3 - (x_P + x_Q + x_R)x^2 + (x_P x_Q + x_P x_R + x_Q x_R)x - x_P x_Q x_R. \end{aligned}$$

By equating the coefficients of x^2 we obtain $x_R = \lambda^2 - a_2 - x_P - x_Q$. By symmetry we get $x_S = x_R$. and from the line $y_S = -(\lambda x_S + \mu) = \lambda(x_P - x_S) - y_P$, where we already took care of the sign change from the last mirroring operation.

Doubling As we have seen before the formulas for doubling differ only in the way the line was obtained. We recall from "Mathematics for Engineers" courses the rules for implicit differentiation. Let $F(x, y)$ be a function in two variables x and y. The equality $F(x, y) = 0$ implicitly defines y as a function of x so that locally one can write $y = g(x)$. If the partial derivative with respect to y is non-zero the derivative of g is given by $-F_x(x, y)/F_y(x, y)$, where $F_x(x, y) = \partial F(x, y)/\partial x$ denotes the partial derivative with respect to x and $F_y(x, y) = \partial F(x, y)/\partial y$ the

one with respect to y. Here we have $F(x,y) = y^2 - (x^3 + a_2x^2 + a_4x + a_6)$ and thus $F_x(x,y) = -(3x^2 + 2a_2x + a_4)$ and $F_y(x,y) = 2y$ leading to

$$\lambda = \frac{3x^2 + 2a_2x + a_4}{2y}.$$

A different approach is to locally solve the equation for y which gives

$$\begin{aligned} y(x) &= \pm\sqrt{x^3 + a_2x^2 + a_4x + a_6} \\ y'(x) &= \pm\left(3x^2 + 2a_2x + a_4\right)\frac{1}{2\sqrt{x^3 + a_2x^2 + a_4x + a_6}} \\ &= \frac{3x^2 + 2a_2x + a_4}{2y}, \end{aligned}$$

where we kept the same sign for the replacement of y in the last step. The definition of μ in terms of λ and the point P remains the same as in addition.

Remark 6.2.1 *Let E be a curve given by $y^2 = x^3+a_2x^2+a_4x+a_6$ with $a_2, a_4, a_6 \in \mathbb{R}$ and let $P, Q \neq P_\infty$ be points on the curve. The addition of P and Q works as follows:*

1. *Compute the slope*

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & Q \neq P, \mathrm{inv}_\oplus(P);\ P, Q \neq P_\infty. \\ \frac{3x_P^2 + 2a_2x_P + a_4}{2y_P} & P = Q, P \neq \mathrm{inv}_\oplus(P);\ P \neq P_\infty. \end{cases}$$

2. *Put $x_S = \lambda^2 - a_2 - x_P - x_Q$.*

3. *Put $y_S = \lambda\,(x_P - x_S) - y_P$.*

4. *We have $P \oplus Q = S$.*

Starting from these formulae one can actually prove that the chord-and-tangent method leads to a group. The longest part of the proof is to show associativity.

Exercise 6.2.2 *a) The points $P = (0, \sqrt{3})$ and $Q = (1, 0)$ are on the elliptic curve given by $E_1 : y^2 = x^3 - 3x^2 - x + 3$. Compute the coordinates of $[2]P$, $[3]P$, and $P \oplus Q$.*

b) Let the curve E_3 be defined by $E_3 : y^2 = x^3 + 2x^2 - x - 2$. Check that E_3 is an elliptic curve. Find all points of order 2, i.e. all points P so that $[2]P = P_\infty$.

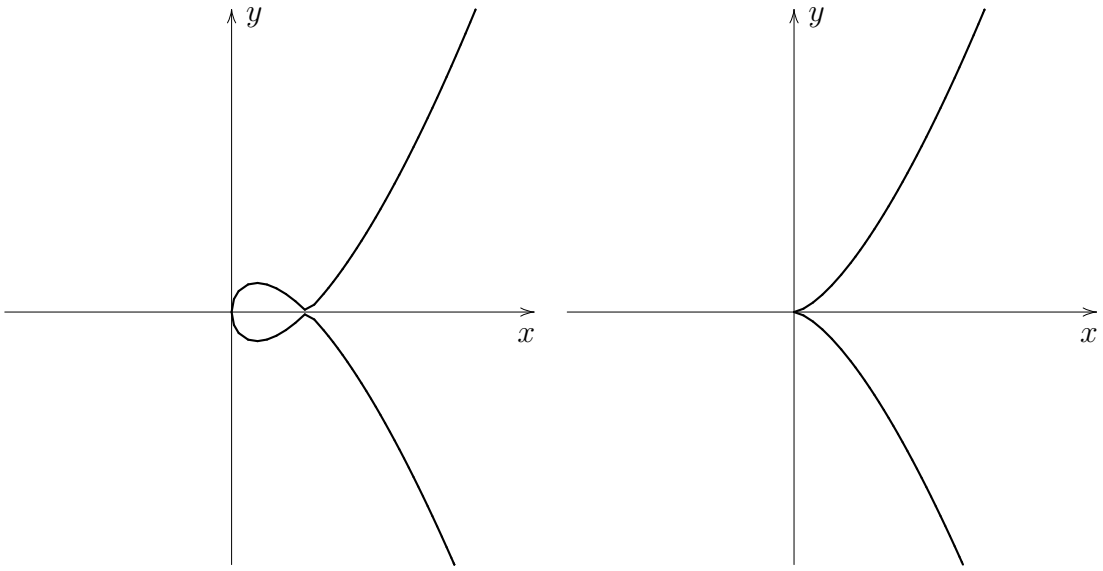
6.3 Elliptic curves

The last section helped to get an idea of elliptic curves. We now consider a more general curve equation and also explain where the point at infinity comes from. We start by explaining where the condition on f in (6.2) comes from. In the doubling formula it was important that we were able to draw a unique tangent at every point of the curve. Looking ahead a few lines we see two examples of curves with points in which tangents are not uniquely defined. Our definition of an elliptic curve must avoid such points if we want to use the same procedure for doubling. We first give a semi-formal definition and then state a mathematical criterion which could just as well be taken as the definition.

Definition 6.3.1 (Singularities)
Let C be a curve over a field K. A point $P \in C$ is singular *if the tangent to the curve at that point is not defined.*
A curve is called singular *if it contains at least one singular point. If there is no singular point over K and any of its extension fields then the curve is* nonsingular.

The following example shows two different types of singularities.

Example 6.3.2 *The elliptic curves we considered in the last two sections were symmetric to the x-axis. We stick to this shape for the moment and draw two possible cases of singularities, i.e. curves with points in which the tangent at that point is not defined. The first picture shows a node, characterized by having two candidate tangents at that point. The second picture shows a cusp. The tangents at points next to the singularity have opposite slopes.*



On the left-hand side we draw the graph of $y^2 = (x-1)^2 x$ which has a node, the right curve is $y^2 = x^3$ having a cusp.

There is a further extreme case which we obtain by changing the curve coefficients, namely a double root of f which is the smallest root. In that case, the "circular" part of the curve becomes a single point. This is impossible to draw and we highly recommend playing with the java applet on the Certicom page (under "2.3 Experiment" on their page).

The following lemma is very useful to detect singularities. We state it without proof. As a motivation remember that the implicit differentiation used to find the slope of the tangent requires the partial derivatives to exist and at least one of them to be non-zero.

Lemma 6.3.3 (Jacobi criterion) *Let C be a curve over a field K given by an equation $F(x,y) = 0$. The curve is singular at a point $P = (x_P, y_P)$ with $F(x_P, y_P) = 0$ if and only if it also satisfies both partial derivative equations $F_x(x_P, y_P) = 0$ and $F_y(x_P, y_P) = 0$.*

Example 6.3.4 *Consider the curves given in the previous example. We now show that their singularities are indeed detected by the Jacobi criterion. We first consider $y^2 = (x-1)^2 x$. From the picture we see that the possible singularity is in $P = (1,0)$ which indeed satisfies the curve equation. The partial derivatives of $F(x,y) = y^2 - (x-1)^2 x$ are $F_x(x,y) = -(2(x-1)x + (x-1)^2)$ and $F_y(x,y) = 2y$. Inserting P gives $F_x(1,0) = 0$ and $F_y(1,0) = 0$. So P is a singular point according to the Jacobi criterion and the curve is singular, since it contains one singular point.*
For the second curve the equation is even simpler, namely $F(x,y) = y^2 - x^3$, and the point $(0,0)$ is on the curve and satisfies both partial derivatives $F_x(x,y) = -3x^2$ and $F_y(x,y) = 2y$.

Example 6.3.5 *In the previous section we considered curves of the form $E : y^2 = f(x)$ over the real numbers and required that $f(x)$ has only single roots. We now show that this is equivalent to having a nonsingular curve. Namely, consider the partial derivative equations*

$$\begin{aligned} F_x(x,y) &= f'(x), \\ F_y(x,y) &= 2y. \end{aligned}$$

A singular point $S = (x_S, y_S)$ must satisfy both these equations and the curve equation, so in particular it must have $y_S = 0$. Inserting this into the curve equation we obtain $0 = f(x_S)$ and so x_S is a root of $f(x)$. From the first partial derivative we see that also $f'(x_S) = 0$. By Exercise 5.4.4c we know that this means that x_S is a multiple root of $f(x)$. This can be rephrased by saying that there are singularities on E if and only if $f(x)$ has multiple roots.

We now have all the necessary vocabulary to define elliptic curves.

Definition 6.3.6 (Elliptic Curve)
An elliptic curve over a field K *is a nonsingular curve defined by an equation of the form*

$$E : y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in K$ *for* $1 \leq i \leq 6$ *and every nonsingular curve defined by such an equation is an elliptic curve. We put* $h(x) = a_1x + a_3$ *and* $f(x) = x^3 + a_2x^2 + a_4x + a_6$.
The set of points defined over K *is given by*

$$E(K) = \left\{(x_P, y_P) \in K^2 \;\middle|\; y_P^2 + (a_1x_P + a_3)y_P = x_P^3 + a_2x_P^2 + a_4x_P + a_6\right\} \cup \{P_\infty\}.$$

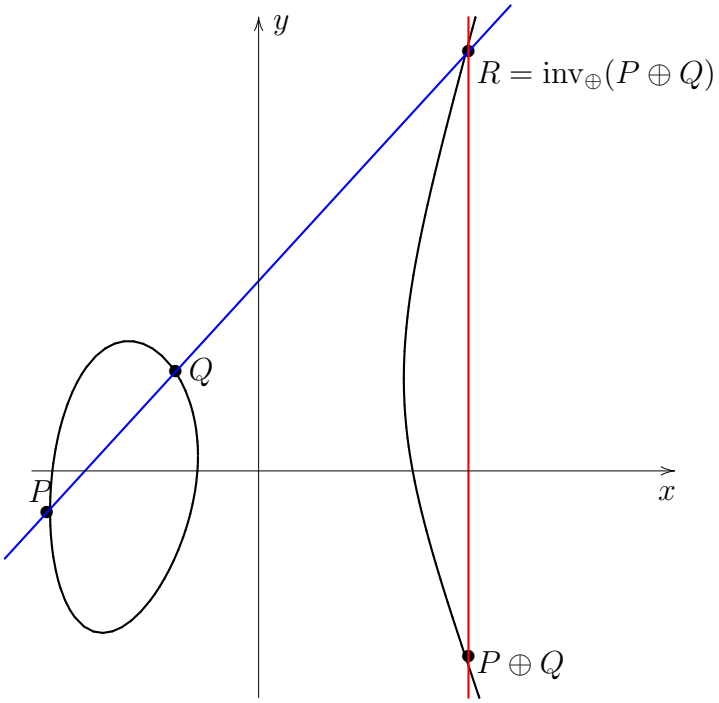
It is called the set of K-rational points of E.
Let L *be an extension field of* K. *The set* $E(L)$ *of* L*-rational points is given by*

$$E(L) = \left\{(x_P, y_P) \in L^2 \;\middle|\; y_P^2 + (a_1x_P + a_3)y_P = x_P^3 + a_2x_P^2 + a_4x_P + a_6\right\} \cup \{P_\infty\}.$$

The set of K*-rational points is a subset of the set of* L*-rational points.*

This definition gives curves of a more general shape than those considered in the previous sections.

Example 6.3.7 *In general we cannot assume that* $a_1 = a_3 = 0$. *The following shows addition on the curve* $y^2 + (-0.75x - 1)y = x^3 + 1.5x^2 - 5x - 4.5$ *following the same chord-and-tangent rule as before.*



The point P_∞ *is the neutral element but now the opposite of a point is no longer obtained by changing the sign of* y. *The picture shows that there are still two*

points which have the same x-coordinate. If $P = (x_P, y_P)$ *is on the curve then the other point with the same x-coordinate is* $(x_P, -y_P - a_1x_P - a_3)$ *since*

$$(-y_P-a_1x_P-a_3)^2+(a_1x_P+a_3)(-y_P-a_1x_P-a_3) = y_P^2+(a_1x_P+a_3)y_P = x_P^3+a_2x_P^2+a_4x_P+a_6,$$

where the last equality follows from $P \in E(K)$*. So we have* $\mathrm{inv}_\oplus(P) = (x_P, -y_P - a_1x_P - a_3)$*.*

To obtain formulae for the group operations we follow the same road as in the last section. Note, that now K is a general field which might be of characteristic $\neq 0$. This might imply that some of the expressions that we state in the sequel contain zero expressions, like $2y$ in characteristic 2. Here we aim at finding the most general formulae; in later sections we specify the field of definition to obtain more efficient formulae for the group operation. Let again $P \oplus Q = S$.

Addition Like in the special case, the line connecting P and Q has slope

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

and intercept

$$\mu = y_P - \lambda x_P = y_P - \frac{y_Q - y_P}{x_Q - x_P}x_P.$$

We substitute y by $\lambda x + \mu$ in the general curve equation and obtain:

$$(\lambda x + \mu)^2 + (a_1x + a_3)(\lambda x + \mu) = x^3 + a_2x^2 + a_4x + a_6.$$

Like before this is a polynomial of degree 3 in x and we know 3 roots, namely x_P, x_Q and x_R. We transform this equation to obtain 0 on the left-hand side and obtain

$$\begin{aligned} 0 &= x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\mu - a_3\lambda)x + a_6 - \mu^2 - a_3\mu \\ &= (x - x_P)(x - x_Q)(x - x_R) \\ &= x^3 - (x_P + x_Q + x_R)x^2 + (x_Px_Q + x_Px_R + x_Qx_R)x + x_Px_Qx_R. \end{aligned}$$

By equating the coefficients of x^2 we obtain $x_R = \lambda^2 - a_2 + a_1\lambda - x_P - x_Q = x_S$ and from the line $y_iS = -(\lambda x_S + \mu) = \lambda(x_P - x_S) - y_P - a_1x_S - a_3$, where we already took care of the mirroring operation.

Doubling The formulae for doubling depend more on the curve coefficients than those for addition. The slope of the tangent at a point $P = (x_P, y_P)$ is given by

$$\lambda = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}.$$

The use and definition of μ is like in the case of addition.

We state the following theorem without proof. Most parts have been motivated in the past paragraphs.

Theorem 6.3.8 *Let E be an elliptic curve over a field K given by $y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$ with $a_1, a_2, a_3, a_4, a_6 \in K$. The set of K-rational points of E forms a group under the operation $\oplus$ given by:*

$$\begin{aligned} P \oplus P_\infty &= P_\infty \oplus P \\ \mathrm{inv}_\oplus(x_P, y_P) &= (x_P, -y_P - a_1x_P - a_3) \\ (x_P, y_P) \oplus (x_Q, y_Q) &= (x_S, y_S) \\ &= (\lambda^2 - a_2 + a_1\lambda - x_P - x_Q, \lambda\,(x_P - x_S) - y_P - a_1x_S - a_3), \end{aligned}$$

where for $(x_P, y_P) \neq \mathrm{inv}_\oplus(x_Q, y_Q)$ we have

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & (x_P, y_P) \neq (x_Q, y_Q) \\ \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} & (x_P, y_P) = (x_Q, y_Q) \end{cases}.$$

Exercise 6.3.9 *a) Let $K = \mathbb{F}_{2^n}$ for some integer n. Is $E_1 : y^2 = x^3 + x + 1$ an elliptic curve over K? For which $a_2, a_4, a_6 \in K$ is $E_2 : y^2 = x^3 + a_2x^2 + a_4x + a_6$ an elliptic curve?*

b) Let $K = \mathbb{F}_{2^n}$ for some integer n. For which $a_2, a_3, a_4, a_6 \in K$ is $E_3 : y^2 + a_3y = x^3 + a_2x^2 + a_4x + a_6$ an elliptic curve?

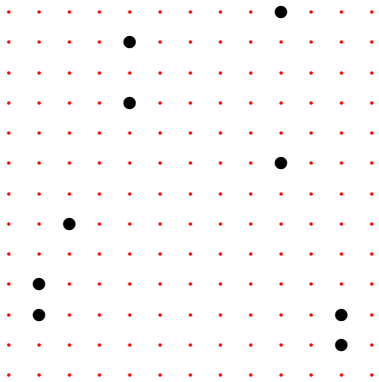
c) Let $E_4 : y^2 + 3xy + y = x^3 + 4x + 4$ be defined over $\mathbb{F}_5$. Verify that E_4 is an elliptic curve and that $P = (4, 1)$ and $Q = (2, 3)$ are points of the curve. Compute $[2]P$, $[2]Q$, and $P \oplus Q$.

6.4 Elliptic curves over finite fields

In this section we focus on elliptic curves over finite fields $\mathbb{F}_q$, $q = p^n$. In the exercises in the last section we already worked over finite fields using the general formulae. Here we provide some graphs of elliptic curves over finite fields and study the number of $\mathbb{F}_q$-rational points.

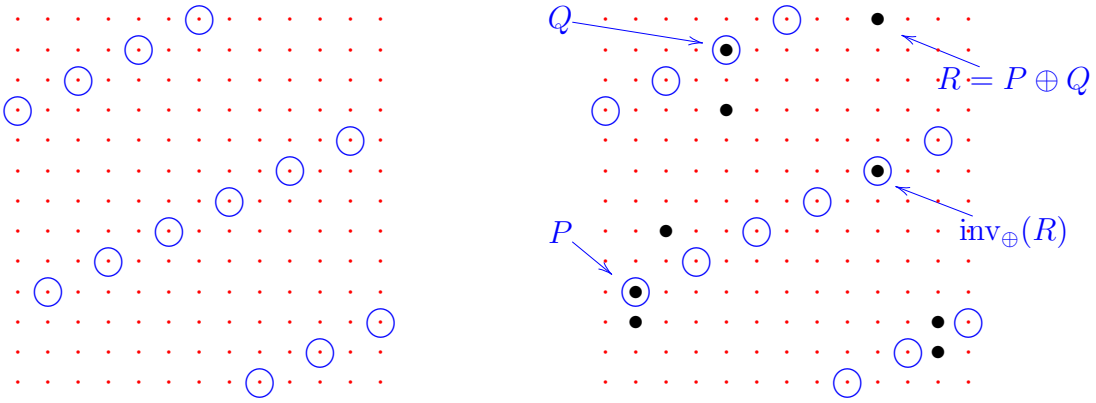
Consider the curve $E : y^2 - 5xy = x^3 - 7$ defined over $\mathbb{F}_{13}$. We first note that E is an elliptic curve since there is no point over $\mathbb{F}_{13}$ or any of its extension fields satisfying both partial derivatives $F_x(x, y) = 3x^2 + 5y, F_y(x, y) = 2y - 5x$ and the curve equation since $(0, 0)$ and $(11, 8)$ are the only solutions to the system of partial derivatives but they both are not a points on the curve.

The graph of this set of points looks as follows

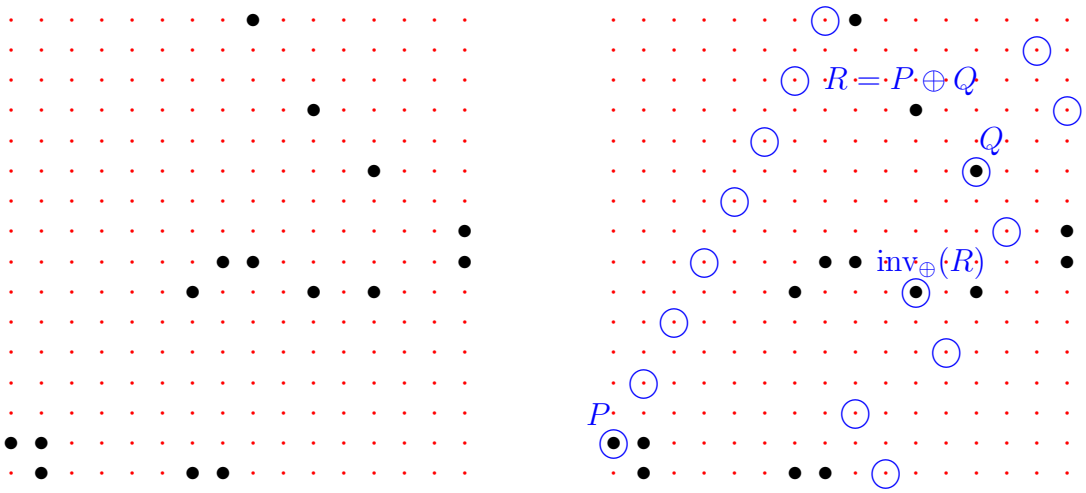


where each of the red dots is a coordinate tuple in $\mathbb{F}_{13}^2$ starting from $(0,0)$ in the lower left corner. Note, that like before points usually occur in pairs having the same x-coordinate, however the symmetry is harder to see since only discrete values exist. In addition to the depicted points we have P_∞ which – as usual – we think of as lying far out on the y-axis.

A line in $\mathbb{F}_{13}$ still has a noticeable similarity with what we usually think of as a line. The following picture shows on the left the line $y = 7x + 9$ and on the right the intersection of the curve with that line leading to $P \oplus Q = R$.



To depict binary fields $\mathbb{F}_{2^n}$ we choose the polynomial basis $\{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ and encode the field element $\sum_{i=0}^{n-1} c_i \xi^i$ by the integer $\sum_{i=0}^{n-1} c_i 2^i$ between 0 and $2^n - 1$. The following picture shows on the left the elliptic curve $y^2 + xy = x^3 + 1$ over $\mathbb{F}_{16} \cong \mathbb{F}_2[\xi]/(\xi^4 + \xi + 1)\mathbb{F}_2[\xi]$ and on the right an addition on this curve using the line $y = \xi x + 1$. Note how for x-values "less" than ξ^3 the line is nicely noticeable while for "larger" values the reduction modulo $\xi^4 - \xi - 1$ is very noticeable.



Since for both of the coordinates there are only q possible values the set of $\mathbb{F}_q$-rational points of an elliptic curve is finite. In a finite field of odd characteristic half of the elements are squares and as a rule of thumb one can expect that about half of the x-coordinates lead to quadratic expressions in y which have roots. Thus about $q/2$ values lead to two points each and there is also P_∞. So we can expect to find approximately q points on an elliptic curve over $\mathbb{F}_q$. For fields of even characteristic similar considerations hold. Note that by Exercise 6.3.9.a any elliptic curve over a binary field must have $h(x) \neq 0$ and so similar considerations hold. Hasse's theorem provides a more accurate statement which we are not able to prove in this course.

Theorem 6.4.1 (Hasse's theorem) *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. There exists an integer t so that for the number of $\mathbb{F}_q$-rational points we have*

$$|E(\mathbb{F}_q)| = q + 1 - t, \text{ where } |t| \leq 2\sqrt{q}.$$

Example 6.4.2 *Consider $E : y^2 - 5xy = x^3 - 7$ over $\mathbb{F}_{13}$. We can see from the picture at the beginning of this section that*

$$E(\mathbb{F}_{13}) = \{(1,2),(1,3),(2,5),(4,9),(4,11),(9,7),(9,12),(11,1),(11,2),P_\infty\}.$$

So we have $|E(\mathbb{F}_{13})| = 10 = 13 + 1 - t$ and $t = 4$ is indeed $\leq 2\sqrt{13}$.

Example 6.4.3 *Consider $E : y^2 + xy = x^3 + 1$ over $\mathbb{F}_2$. By trying out the possible values $0, 1$ for the x-coordinate we see*

$$E(\mathbb{F}_2) = \{(0,1),(1,0),(1,1),P_\infty\}.$$

So we have $|E(\mathbb{F}_2)| = 4 = 2 + 1 - t$ and $t = -1$. The absolute value of t is $\leq 2\sqrt{2}$.
At the beginning of this section we considered the same curve over $\mathbb{F}_{2^4}$. We count $|E(\mathbb{F}_{2^4})| = 16$ on the picture taking into account the point at infinity. In this case $t_4 = 1$, where the index 4 refers to the extension of degree 4 of $\mathbb{F}_2$. Later we will obtain a relation between the number of points on the curve over the ground field and over extension fields.

Let E be defined over $\mathbb{F}_q$ and let $m \in \mathbb{N}$. The set of $\mathbb{F}_{q^m}$-rational points $E(\mathbb{F}_{q^m})$ contains $E(\mathbb{F}_q)$ as a subset. In Chapter 5 we introduced the Frobenius automorphism σ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. By Definition 5.8.7 it operates by raising every element to the q-th power. We extend σ to $E(\mathbb{F}_{q^m})$ by

$$\sigma(P) = \sigma(x_P, y_P) = (x_P^q, y_P^q)$$

and note that $P \in E(\mathbb{F}_{q^m})$ implies that $\sigma(P) \in E(\mathbb{F}_{q^m})$. To see this we notice that the curve coefficients a_i are defined over $\mathbb{F}_q$ and thus $\sigma(a_i) = a_i$ so that by Exercise 5.1.9 we have the system of equivalences

$$\begin{aligned}
\sigma(y_P)^2 + (a_1\sigma(x_P) + a_3)\sigma(y_P) &= \sigma(x_P)^3 + a_2\sigma(x_P)^2 + a_4\sigma(x_P) + a_6 \\
\sigma(y_P^2) + (\sigma(a_1 x_P) + \sigma(a_3))\,\sigma(y_P) &= \sigma(x_P^3) + \sigma(a_2 x_P^2) + \sigma(a_4 x_P) + \sigma(a_6) \\
\sigma\left(y_P^2 + (a_1 x_P + a_3) y_P\right) &= \sigma\left(x_P^3 + a_2 x_P^2 + a_4 x_P + a_6\right) \\
\sigma\left(y_P^2 + (a_1 x_P + a_3) y_P - \left(x_P^3 + a_2 x_P^2 + a_4 x_P + a_6\right)\right) &= 0,
\end{aligned}$$

which shows that $\sigma(P)$ is in $E(\mathbb{F}_{q^m})$ if and only if P is.
Similarly $\sigma^2(P), \sigma^3(P), \ldots$ are on the curve. Note that since the coordinates x_P and y_P are in $\mathbb{F}_{q^m}$ and $x_P^{q^m} = x_P$ we have $\sigma^m(P) = P$.

Example 6.4.4 *Consider $E : y^2 + xy = x^3 + 1$ over $\mathbb{F}_{2^4}$. The point $P = (\xi^2 + \xi, \xi^2 + \xi)$ is in $E(\mathbb{F}_{2^4})$ and so is the point*

$$\sigma(P) = \big(\sigma(\xi^2 + \xi), \sigma(\xi^2 + \xi)\big) = (\xi^2 + \xi + 1, \xi^2 + \xi + 1)$$

as can be checked directly or seen from the picture.

For a fixed field $\mathbb{F}_{q^m}$ one can invert σ by computing the $(q^m - 1)/q$-th power. However, there is no such polynomial map which works for *all* extension fields. Therefore σ is seen as an endomorphism of E and not as an automorphism. It is called the *Frobenius endomorphism*.

Definition 6.4.5 (Frobenius endomorphism) *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. The* Frobenius endomorphism σ of E *operates on $E(\mathbb{F}_{q^m})$ for any $m \in \mathbb{N}$ via $\sigma(x_P, y_P) = (x_P^q, y_P^q)$.*

In the section on efficient arithmetic on elliptic cures over binary fields we will make use of the following dependence which we cannot prove in this course.

Theorem 6.4.6 *Let E be an elliptic curve over a finite field $\mathbb{F}_q$. For any extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ and for every $\mathbb{F}_{q^m}$-rational point P we have for the Frobenius endomorphism σ that*

$$\sigma^2(P) \oplus [-t]\sigma(P) \oplus [q]P = P_\infty.$$

The polynomial

$$\chi(T) = T^2 - tT + q \tag{6.3}$$

is the characteristic polynomial of the Frobenius endomorphism.

Example 6.4.7 *Consider again* $E : y^2 + xy = x^3 + 1$ *over* $\mathbb{F}_{2^4}$ *and in particular* $P = (\xi^2 + \xi, \xi^2 + \xi) \in E(\mathbb{F}_{2^4})$. *We have* $\sigma(P) = (\xi^2 + \xi + 1, \xi^2 + \xi + 1)$ *and so* $[-t]\sigma(P) = [+1]\sigma(P) = (\xi^2 + \xi + 1, \xi^2 + \xi + 1)$. *Note that we used the* t *from the ground field, not* t_4 *from the extension field. We have* $\sigma^2(P) = \sigma(\xi^2 + \xi + 1, \xi^2 + \xi + 1) = (\xi^2 + \xi, \xi^2 + \xi) = P$. *To check the statement of the theorem we need to compute*

$$P \oplus (\xi^2 + \xi + 1, \xi^2 + \xi + 1) \oplus [2]P = (\xi^2 + \xi + 1, \xi^2 + \xi + 1) \oplus [3]P$$

and check whether this gives the point at infinity. This is equivalent to checking whether $[3]P = \mathrm{inv}_{\oplus}(\xi^2 + \xi + 1, \xi^2 + \xi + 1) = (\xi^2 + \xi + 1, 0)$.
Put $R = [2]P$. *We have*

$$\lambda = \frac{x_P^2 + y_P}{x_P} = \frac{(\xi^2 + \xi + 1) + (\xi^2 + \xi)}{\xi^2 + \xi} = \frac{1}{\xi^2 + \xi} = \xi^2 + \xi + 1.$$

So $x_R = \lambda^2 + \lambda = (\xi^2 + \xi + 1)^2 + \xi^2 + \xi + 1 = 1$ *and* $y_R = \lambda(x_P + x_R) + y_P + x_R = (\xi^2 + \xi + 1)\left((\xi^2 + \xi) + 1\right) + (\xi^2 + \xi) + 1 = (\xi^2 + \xi) + (\xi^2 + \xi + 1) = 1$, *i.e.* $R = (1, 1)$.
Put $S = R \oplus P = [3]P$. *We have*

$$\lambda = \frac{(\xi^2 + \xi) + 1}{(\xi^2 + \xi) + 1} = 1$$

and thus $x_S = \lambda^2 + \lambda + x_P + x_R = 1 + 1 + \xi^2 + \xi + 1 = \xi^2 + \xi + 1$ *and* $y_S = \lambda(x_P + x_S) + y_P + x_S = 1\left((\xi^2 + \xi) + (\xi^2 + \xi + 1)\right) + (\xi^2 + \xi) + (\xi^2 + \xi + 1) = 0$.
So indeed $[3]P = (\xi^2 + \xi + 1, 0)$.

Theorem 6.4.6 shows that the Frobenius endomorphism satisfies a quadratic polynomial. One can show that every endomorphism on an elliptic curve satisfies a quadratic polynomial, so the *characteristic polynomial* of a curve endomorphism has degree 2.

Definition 6.4.8 (Trace of the Frobenius)
Let E *be an elliptic curve over a finite field* $\mathbb{F}_q$ *with* $|E(\mathbb{F}_q)| = q + 1 - t$. *The integer* t *is called the* trace of the Frobenius endomorphism.

For large finite fields one cannot determine the number of points by trying all possible coordinate tuples. If the curve is defined over a small finite field and then considered over an extension field the following relation between the numbers of points is helpful. Again we refer to the literature for a proof.

Lemma 6.4.9 *Let* E *be an elliptic curve defined over the finite field* $\mathbb{F}_q$ *and let the characteristic polynomial of the Frobenius endomorphism on* E *be* $\chi(T) = T^2 - tT + q$.
The two complex roots τ_1 *and* τ_2 *of* $\chi(T)$ *satisfy* $\overline{\tau_1} = \tau_2$ *and* $\tau_1\tau_2 = q$. *For the number of points over an extension field* $\mathbb{F}_{q^m}$ *we have*

$$\left|E\left(\mathbb{F}_{q^m}\right)\right| = \left(1 - \tau_1^m\right)\left(1 - \tau_2^m\right).$$

Example 6.4.10 *For $E: y^2+xy=x^3+1$ we found that $\chi(T)=T^2+T+2$. The complex roots are $\tau_1=(-1+\sqrt{-7})/2$ and $\tau_2=(-1-\sqrt{-7})/2$. Over $\mathbb{F}_{2^2}$ we thus expect to find $\left(1-((-1+\sqrt{-7})/2)^2\right)\left(1-((-1-\sqrt{-7})/2)^2\right)$ points. We simplify the expression to*

$$\begin{aligned}
&\left(1-((-1+\sqrt{-7})/2)^2\right)\left(1-((-1-\sqrt{-7})/2)^2\right)\\
=\;& 1-((-1+\sqrt{-7})/2)^2-((-1-\sqrt{-7})/2)^2+((-1+\sqrt{-7})/2)^2((-1-\sqrt{-7})/2)^2\\
=\;& 1-2(1-7)/4+((-1+\sqrt{-7})(-1-\sqrt{-7}))^2/16\\
=\;& 1+3+64/16=8
\end{aligned}$$

and thus $|E(\mathbb{F}_{2^2})|=8$.
Likewise, we compute $|E(\mathbb{F}_{2^4})|=\left(1-((-1+\sqrt{-7})/2)^4\right)\left(1-((-1-\sqrt{-7})/2)^4\right)=1-((-1+\sqrt{-7})/2)^4-((-1-\sqrt{-7})/2)^4+((-1+\sqrt{-7})/2)^4((-1-\sqrt{-7})/2)^4=1-2(1-42+49)/16+16=1-1+16=16$ which coincides with what we had obtained by direct computation.

The following example is again a curve over a field of characteristic 2 but this time the curve is not defined over the field $\mathbb{F}_2$.

Example 6.4.11 *Represent $\mathbb{F}_4$ with a polynomial basis $\mathbb{F}_4=\{0,1,\alpha,\alpha+1\}\cong\mathbb{F}_2[x]/(x^2+x+1)\mathbb{F}_2[x]$ and consider the curve $E: y^2+y=x^3+\alpha x+1$. We first check whether E is nonsingular, i.e. an elliptic curve. The partial derivative with respect to y is 1 which is always nonzero, so there cannot be a singular point.*
We find all points of E over $\mathbb{F}_4$ by trying all possible values for the x-coordinate.

$$E(\mathbb{F}_4)=\{(0,\alpha),(0,\alpha+1),(\alpha+1,\alpha),(\alpha+1,\alpha+1),P_\infty\}.$$

Thus $|E(\mathbb{F}_4)|=5$, and $5=4+1-t=5-t$ leads to $t=0$.
The characteristic polynomial of the Frobenius endomorphism σ is thus given by $\chi(T)=T^2+4=(T-2i)(T-(-2i))$, i.e. $\tau_1=2i$.
For the number of points on extension fields of $\mathbb{F}_4$ we obtain

$$|E(\mathbb{F}_{4^m})|=(1-(2i)^m)(1-(-2i)^m).$$

Since χ has a particularly simple form we can even obtain closed formulae for the number of points. To do so we need to distinguish between even and odd values of m.
Let first m be even, i.e. $m=2m'$ for some integer m'. We obtain

$$|E(\mathbb{F}_{4^m})|=(1-(2i)^m)(1-(-2i)^m)=(1-(-4)^{m'})(1-(-4)^{m'})=(1-(-4)^{m'})^2.$$

For odd $m=2m'+1$ we have

$$|E(\mathbb{F}_{4^m})|=(1-(2i)(-4)^{m'})(1-(-2i)(-4)^{m'})=1+4\cdot 4^{2m'}=1+4^m.$$

Remark 6.4.12 *We would like to stress that the curves studied in the last example and some of the exercises were chosen because they lead to nice formulas for the number of points. They are not useful for cryptographic applications if one wants to construct a discrete logarithm system. The interested reader is advised to consult the web or books for "supersingular curves" and "pairings".*

We are not able to cover point counting for curves defined over large fields in this manuscript. The books recommended in the introduction of this chapter consider *Schoof's algorithm* for curves defined over fields of large characteristic and p-adic point counting methods like *Satoh's algorithm* in small characteristic.

Exercise 6.4.13 *a) Let $E_4 : y^2 + 3xy + y = x^3 + 4x + 4$ be defined over $\mathbb{F}_5$. State $E(\mathbb{F}_5)$ by trying all values for the x-coordinate; make sure not to forget the point at infinity. Determine the characteristic polynomial of the Frobenius endomorphism and use it to compute the number of points in $E(\mathbb{F}_{25})$.*

b) Let $E : y^2 + y = x^3 + 1$ be defined over $\mathbb{F}_2$. Compute $|E(\mathbb{F}_2)|, |E(\mathbb{F}_{2^2})|, |E(\mathbb{F}_{2^3})|$, and $|E(\mathbb{F}_{2^n})|$.

c) Compute all extension degrees n between 160 and 240 so that $|E_a(\mathbb{F}_{2^n})|$ is almost prime where

$$E_a : y^2 + xy = x^3 + ax^2 + 1,\ a \in \mathbb{F}_2.$$

Note: this exercise should be solved with the help of a computer.

6.5 Arithmetic on elliptic curves over fields of large characteristic

To obtain the most efficient arithmetic one needs to specify whether the characteristic is even or odd. We consider odd characteristic fields in the following and concentrate on elliptic curves defined over fields $\mathbb{F}_q$ of characteristic > 3.
We start by obtaining a simpler curve equation. This is done through *isomorphic transformations*.

Definition 6.5.1 *Let C and C' be two elliptic curves over a field K. The curves C and C' are isomorphic if there exists an invertible map given by polynomials that maps the points of C to the points of C'.*

Particularly we consider isomorphic transformations that do not change the shape of the equation, i.e. the highest powers x^3 and y^2 are maintained and the highest power of a mixed term is xy. This means that we can only replace x by $ax + b$ and y by $cy + dx + e$. Obviously these maps are invertible provided that $a, c \neq 0$. The shape of the curve is unchanged if $a^3 = c^2$, i.e. $a = m^2$, $c = m^3$ for some m since then both sides can be made monic.

Lemma 6.5.2 *Let E be an elliptic curve over a finite field of odd characteristic given by a Weierstrass equation $E : y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$. There exists an isomorphic transformation which leads to an isomorphic curve of the form*

$$E' : y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ *and* $b_6 = a_3^2 + 4a_6$.
If the characteristic of $\mathbb{F}_q$ *is larger than* 3 *there is an isomorphic curve of the shape*

$$E : y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864},$$

where c_4 *and* c_6 *are expressed in terms of* b_2, b_4, b_6 *as*

$$c_4 = b_2^2 - 24b_4 \text{ and } c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Proof. Choosing $m = 1, b = 0, d = -a_1/2$, and $e = -a_3/2$ in the first transformation we obtain (in the new coordinates)

$$(y^2 - a_1xy - a_3y + a_1^2x^2/4 + a_1a_3x/2 + a_3^2/4) + (a_1xy + a_3y - a_1^2x^2/2 - a_1a_3x - a_3^2/2) = x^3 + a_2x^2 + a_4x + a_6.$$

Sorting according to the desired shape leads to

$$y^2 = x^3 + (a_2 + a_1^2/4)x^2 + (a_4 + a_1a_3/2)x + a_6 + a_3^2/4.$$

If the characteristic is not 3 then $b_2/12$ exists and we can additionally change x to $x - b_2/12$. Taking care of the powers of 2 and 3 we obtain the claim. □

In Remark 6.2.1 we derived the formulae for addition and doubling in the slightly more general case $b_2 \neq 0$. Now, that we know that we can always work with $f(x) = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$ as right hand side we give a short criterion for the curve to be nonsingular and briefly reconsider the arithmetic. For ease of notation we rename the coefficients and study curves of the form

$$E : y^2 = x^3 + ax + b, a, b \in \mathbb{F}_q. \tag{6.4}$$

For this shape of curve we can compute $\gcd(f, f')$ for $f = x^3 + ax + b$ in terms of a and b and derive an easier criterion for singularity. Remember that by Exercise 5.4.4c we have that $\gcd(f, f') \in \mathbb{F}_q^*$ if and only if f has only simple roots, i.e. if and only if the curve is nonsingular.

$$\begin{aligned} f &= x^3 + ax + b = x/3(3x^2 + a) + 2ax/3 + b \\ f' &= 3x^2 + a = (9x/(2a) - 27b/(4a^2))(2ax/3 + b) + a + 27b^2/(4a^2) \end{aligned}$$

The gcd is trivial if $a + 27b^2/(4a^2) \neq 0$, in other words if

$$\Delta = 4a^3 + 27b^2 \neq 0. \tag{6.5}$$

The expression Δ in (6.5) is called the *discriminant*.

Remark 6.5.3 (Affine coordinates)
The representation of points as a tuple $P = (x_P, y_P)$ *is called* affine coordinates. *For a curve in form (6.4) the formulae for addition* $P \oplus Q = R$ *of* $P \neq \mathrm{inv}_\oplus(Q), P_\infty$ *are given by*

$$x_R = \lambda^2 - x_P - x_Q, y_R = \lambda(x_P - x_R) - y_P, \text{ where } \lambda = \begin{cases} \frac{y_P - y_Q}{x_P - x_Q} & \text{for } P \neq Q \\ \frac{3x_P^2 + a}{2y_P} & P = Q \end{cases}$$

and we have $\mathrm{inv}_\oplus(x_P, y_P) = (x_P, -y_P)$.
This means that an addition takes 1I (inversion), 2M (multiplication), 1S (squaring) while a doubling needs 1I, 2M, 2S. Note that a division A/B is computed by first inverting B and then multiplying the result by A, so one division is counted as $I + Mo$.

For most platforms inversions are much more expensive than multiplications and thus inversion-free coordinate systems are interesting. They are best understood when thinking of arithmetic in the rationals. When adding two fractions a/b and c/d one first needs to write them as equivalent fractions with equal denominators. If no further information on joint factors of b and d is available it is easiest to compute the sum as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Even if one knows that all fractions are actually integers there is no need to reduce the fractions during the computations, the result will be the same.
In *projective coordinates* one avoids inversions at the expense of an extra coordinate Z which holds the "denominator". Whenever an inversion occurs in the computation, Z is multiplied with this value and all values are adjusted so that they have the same denominator. A point is now represented by a triple $P = (X_P : Y_P : Z_P)$, where this representation corresponds to the affine point $P = (X_P/Z_P, Y_P/Z_P)$. The colons indicate that the representation in projective coordinates is not unique. Obviously, the same affine point is obtained from $(kX_P : kY_P : kZ_P)$, where $k \in \mathbb{F}_q$ is some field element, since the contribution of k simply cancels out.
Projective coordinates are actually the proper way of defining elliptic curves and with them the point at infinity can be easily explained; it is given by the triple $(0 : 1 : 0)$. Note, that there is no affine point corresponding to this since we would divide by 0. For more details consult any of the books listed at the end of the introduction.

Remark 6.5.4 (Projective coordinates)
Let $P = (X_P : Y_P : Z_P), Q = (X_Q : Y_Q : Z_Q)$ so that $P \neq Q, \mathrm{inv}_\oplus(Q), P_\infty$. The formulae for addition $P \oplus Q = R$ are as follows:
Addition:

$$A = Y_Q Z_P - Y_P Z_Q;\ B = X_Q Z_P - X_P Z_Q;\ C = A^2 Z_P Z_Q - B^3 - 2B^2 X_P Z_Q;$$
$$X_R = BC;\ Y_R = A(B^2 X_P Z_Q - C) - B^3 Y_P Z_Q;\ Z_R = B^3 Z_P Z_Q.$$

Doubling*:*

$$A = aZ_P^2 + 3X_P^2;\ B = Y_P Z_P;\ C = X_P Y_P B;\ D = A^2 - 8C;$$
$$X_R = 2BD;\ Y_R = A(4C - D) - 8Y_P^2 B^2;\ Z_R = 8B^3.$$

One addition needs 12M, 2S while a doubling needs 7M, 5S.

It is very obvious that the number of extra multiplications needed to avoid the inversion is much larger for additions than for doublings. This is easily explained by the observation that denominators Z_P and Z_Q of the input point are totally unrelated and so a lot of multiplications are needed to adjust the values to have the same denominator.
In applications we often have the situation that we are starting with a point in affine coordinates and just want to avoid inversions during the scalar multiplication. Unless a windowing method is used (cf. Chapter 4) all additions are between the intermediate point and the base point. If the input points are in different coordinate systems or the output is in a different system one speaks of *mixed coordinates*. Addition in mixed coordinates is likely to be faster than projective addition.
Consider the special case of addition where one input point Q is given in affine coordinates – usually the base point P in a scalar multiplication – while the other is in projective coordinates and the result is supposed to be in projective coordinates, too. The obvious savings are that all multiplications by Z_Q disappear, since the affine coordinates of $Q = (x_Q, y_Q)$ translate to the projective point $(x_Q : y_Q : 1)$. The operation count for such additions is 9M and 2S.
When inspecting the formulae and their connection to the affine group operations one notices that some multiplications are used because the denominator of x contains the denominator of λ as a square while y needs the third power and so adjustments are needed. Jacobian coordinates take this into account by having the coordinate triple $(X_P : Y_P : Z_P)$ represent the affine point $P = (X_P/Z_P^2, Y_P/Z_P^3)$. This system has faster doublings than projective coordinates while additions are more expensive. Note, that sometimes the notations are confused and Jacobian coordinates are incorrectly referred to as projective coordinates.

Remark 6.5.5 (Jacobian coordinates)
Let $P = (X_P : Y_P : Z_P), Q = (X_Q : Y_Q : Z_Q)$ so that $P \neq Q, \mathrm{inv}_\oplus(Q), P_\infty$. The formulae for addition $P \oplus Q = S$ are as follows:
Addition:

$$A = X_P Z_Q^2;\ B = X_Q Z_P^2;\ C = Y_P Z_Q^3;\ D = Y_Q Z_P^3;\ E = B - A;\ F = D - C$$
$$X_S = -E^3 - 2AE^2 + F^2;\ Y_S = -CE^3 + F(AE^2 - X_S);\ Z_S = Z_P Z_Q E.$$

Doubling*:*

$$A = 4X_P Y_P^2;\ B = 3X_P^2 + a_4 Z_P^4$$
$$X_S = -2A + B^2;\ Y_S = -8Y_P^4 + B(A - X_S);\ Z_S = 2Y_P Z_P.$$

We have $\mathrm{inv}_\oplus((X_P : Y_P : Z_P)) = (X_P : -Y_P : Z_P)$. *One addition needs 12M, 4S while a doubling needs 4M, 6S. If one of the input points is in affine coordinates only 8M and 3S are needed for an addition.*

The elliptic curves chosen in the NIST standard all have $a_4 = -3$. This has algorithmic advantages. In the doubling operation one can compute $B = 3X_P^2 + a_4 Z_P^4$ as $B = 3(X_P - Z_P^2)(X_P + Z_P^2)$ and the total operation count for a doubling ends

up as 4M and 4S.

There are more coordinate systems, e.g. Chudnovsky Jacobian coordinates, and the reader is advised to consult the literature before implementing a system. For a close to exhaustive overview of all coordinate systems and the formulae we refer to Chapter 11 of the "Handbook of Elliptic and Hyperelliptic Curve Cryptography".

Remark 6.5.6 *We like to remark that the coordinate system should be chosen with the finite field in mind. Optimal extension fields are attractive since the prime field size can be chosen to fit into one word. On top of the optimizations discussed in Section 5.12 one can use semi-projective coordinates. Let $q = p^n$ and consider an elliptic curve over $\mathbb{F}_q$. Use projective (or Jacobian) coordinates and keep the "denominator" Z in $\mathbb{F}_p$. This implies that the adjustments due to multiplications with the denominator are much cheaper than usual multiplications.*

Remark 6.5.7 (Montgomery coordinates)
Another interesting coordinate system is Montgomery coordinates. *A curve is in* Montgomery form *if it is written as*

$$By^2 = x^3 + Ax^2 + x.$$

To define efficient formulae for scalar multiplication on a curve in Montgomery form we start by putting $x_1 = x(P)$, the x-coordinate of P, and $z_1 = 1$. Define sequences $(x_1, x_2, \ldots)$ and $(z_1, z_2, \ldots)$ recursively by the equations

$$\begin{aligned}
x_{2n} &= (x_n - z_n)^2 (x_n + z_n)^2, \\
z_{2n} &= \left((x_n + z_n)^2 - (x_n - z_n)^2\right)\left((x_n + z_n)^2 + \frac{A-2}{4}((x_n + z_n)^2 - (x_n - z_n)^2)\right), \\
x_{2n+1} &= \left((x_n - z_n)(x_{n+1} + z_{n+1}) + (x_n + z_n)(x_{n+1} - z_{n+1})\right)^2 z_1, \\
z_{2n+1} &= \left((x_n - z_n)(x_{n+1} + z_{n+1}) - (x_n + z_n)(x_{n+1} - z_{n+1})\right)^2 x_1.
\end{aligned}$$

The value x_n/z_n is the x-coordinate of $[n]P$.
Clearly, it would be very slow – complexity $O(n)$ rather than $O(\log n)$ – if we needed to compute the whole sequence just to obtain some individual scalar multiple $[n]P$. Inspecting the formulae above we notice that to compute the x-coordinate of $[2n]P$ the knowledge of x_n and z_n is sufficient. To compute the x-coordinate of $[2n+1]P$ we need to know x_n, x_1, z_n, and z_1. This is a nice application of Montgomery's ladder considered in Chapter 4. Note, that the y-coordinates do not appear in the formulae. This is one of the reasons why Montgomery coordinates are fastest for curves where they can be applied.
However, not every elliptic curve is isomorphic to one in Montgomery form. One requirement is that the group order must be divisible by 4.

Exercise 6.5.8 *a) Check whether*

$$E_1 : y^2 = x^3 - 3x + 2 \text{ and } E_2 : y^2 = x^3 + x + 3$$

are elliptic curves over $\mathbb{F}_{17}$.

b) Compute the 31st multiple of $(1,7)$ on the elliptic curve $y^2 = x^3 - 3x$ over $\mathbb{F}_{17}$. Use the result to compute the order of $(1,7)$?

c) Let E be an elliptic curve over $\mathbb{F}_{13}$ given by $E : y^2 = x^3 + 6x^2 + x$ and put $P = (11,12)$. Compute $[7]P$ in affine coordinates.
Compute the x-coordinate of $[7]P$ using Montgomery coordinates.
Check your result with the previous part of the exercise.

d) Let E be an elliptic curve over $\mathbb{F}_{11}$ given by $E : y^2 = x^3 - 3x + 4$ and put $P = (0,2)$. Compute $[6]P$ in projective coordinates coordinates.
Compute $[6]P$ in Jacobian coordinates.
Check your result with the previous part of the exercise.

6.6 Arithmetic on elliptic curves over fields of characteristic two

In this section we deal with elliptic curves defined over fields $\mathbb{F}_{2^n}$. Like in the previous section we start by introducing isomorphic transformations to simplify defining the equation of the curve and make the arithmetic faster.
Let E be an elliptic curve in Weierstrass form by $E : y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$ defined over $\mathbb{F}_{2^n}$. The values of a_1 and a_3 determine which transformations can be applied.
We consider three cases; $a_1 = a_3 = 0$, $a_1 = 0, a_3 \neq 0$, and $a_1 \neq 0$.
Case $a_1 = a_3 = 0$. We show that E is singular, thus it is not an elliptic curve. The partial derivatives are $x^2 + a_4$ and 0 since we are working in characteristic 2. Let b be a root of $x^2 + a_4$ which must exist in some extension field of $\mathbb{F}_{2^n}$. Compute $c = \sqrt{b^3 + a_2b^2 + a_4b + a_6}$ which is defined in some extension field of $\mathbb{F}_{2^n}$. The point (b,c) is a singular point of E and so E is singular.
Case $a_1 = 0$, $a_3 \neq 0$. One can show that every curve is isomorphic to one of the form

$$y^2 + a_3y = x^3 + a_4x + a_6.$$

Proving the details is left to the reader as Exercise 6.6.5.a.
We remark that curves of this shape are supersingular. This means that they are good choices for pairing based cryptography but are weak under the MOV attack which uses the existence of pairings. Please consult the literature about this case.
Case $a_1 \neq 0$. Replacing x by $a_1^2x + a_3/a_1$ and y by $a_1^3y + a_3^2/a_1^3 + a_4/a_1$ we obtain on the left-hand side

$$a_1^6y^2 + \frac{a_3^4}{a_1^6} + \frac{a_4^2}{a_1^2} + a_1^3x\left(a_1^3y + \frac{a_3^2}{a_1^3} + \frac{a_4}{a_1}\right)$$

and on the right-hand side

$$a_1^6x^3 + \left(a_1^4a_2 + \frac{a_1^4a_3}{a_1}\right)x^2 + \left(a_1^2a_4 + \frac{a_1^2a_3^2}{a_1^2}\right)x + a_6 + \frac{a_3^3}{a_1^3} + \frac{a_2a_3^2}{a_1^2} + \frac{a_3a_4}{a_1}.$$

After dividing by a_1^6 and rearranging this becomes

$$y^2 + xy = x^3 + \left(\frac{a_1a_2 + a_3}{a_1^3}\right)x^2 + \frac{a_1^4a_2a_3^2 + a_1^3a_3^3 + a_1^5a_3a_4 + a_1^4a_4^2 + a_1^6a_6 + a_3^4}{a_1^{12}}.$$

So every binary curve with $a_1 \neq 0$ can be transformed to have the form

$$E : y^2 + xy = x^3 + \tilde{a}_2x^2 + \tilde{a}_6. \tag{6.6}$$

Finally, we check when a curve given by (6.6) is nonsingular. The partial derivative with respect to y is x, so a singular point must have x-coordinate 0. The partial derivative with respect to x is given by $y + x^2$. Inserting 0 for x shows that y must also be 0. So, if $(0, 0)$ is a point on E then that point is a singularity and thus E is singular. The point is on E if and only if $\tilde{a}_6 = 0$. So a curve given by (6.6) is an elliptic curve for all choices of $\tilde{a}_2 \in \mathbb{F}_{2^n}$ and $\tilde{a}_6 \in \mathbb{F}_{2^n}^*$.

We summarize these results in a lemma.

Lemma 6.6.1 *Let E be an elliptic curve over a field $\mathbb{F}_{2^n}$ of characteristic two and let $a_1, a_2, a_3, a_4,$ and a_6 be the coefficient of its Weierstrass equation. Through isomorphic transformations E can be transformed to one of the following two forms.*
If $a_1 = 0, a_3 \neq 0$ the curve is supersingular *and can be transformed to*

$$y^2 + a_3y = x^3 + a_4x + a_6.$$

If $a_1 \neq 0$ the curve is isomorphic to

$$y^2 + xy = x^3 + a_2x^2 + a_6, \tag{6.7}$$

where $a_6 \neq 0$. Curves of this form are not supersingular.

In this book we concentrate on providing the basis for implementing efficient discrete logarithm systems. Therefore, we concentrate on the non-supersingular case for describing the curve arithmetic.

Remark 6.6.2 (Affine coordinates) *The representation of points as a tuple $P = (x_P, y_P)$ is called* affine coordinates. *For a curve in form (6.7) the formulae for addition $P \oplus Q = S$ of $P \neq \text{inv}_\oplus(Q), P_\infty$ are given by*

$$x_S = \lambda^2 + \lambda + x_P + x_Q + a_2, y_S = \lambda(x_P + x_S) + x_S + y_P,$$

where

$$\lambda = \begin{cases} \frac{y_P + y_Q}{x_P + x_Q} & \text{for } P \neq Q \\ x_P + \frac{y_P}{x_P} & \text{for } P = Q \end{cases}$$

and we have $\text{inv}_\oplus(x_P, y_P) = (x_P, x_P + y_P)$.
This means that an addition and a doubling cost 1I, 2M , and 1S each.

Like in the case of odd characteristic one can define several inversion-free coordinate systems for elliptic curves over binary fields. We state the formulae without proof. The reader is advised to consult the literature for more details.

Remark 6.6.3 (Projective coordinates)
Let $P = (X_P : Y_P : Z_P), Q = (X_Q : Y_Q : Z_Q)$ *so that* $P \neq Q, \mathrm{inv}_\oplus(Q), P_\infty$. *The formulae for addition* $P \oplus Q = S$ *are as follows:*
Addition:

$$A = Y_P Z_Q + Z_P Y_Q;\ B = X_P Z_Q + Z_P X_Q;\ C = B^2;$$
$$D = Z_P Z_Q;\ E = (A^2 + AB + a_2 C)D + BC;$$
$$X_S = BE;\ Y_S = C(AX_P + Y_P B)Z_Q + (A + B)E;\ Z_S = B^3 D.$$

Doubling*:*

$$A = X_P^2;\ B = A + Y_P Z_P;\ C = X_P Z_P;$$
$$D = C^2;\ E = (B^2 + BC + a_2 D);$$
$$X_S = CE;\ Y_S = (B + C)E + A^2 C;\ Z_S = CD.$$

We have $\mathrm{inv}_\oplus(X_P : Y_P : Z_P) = (X_P : X_P + Y_P : Z_P)$. *One addition needs 16M, 2S while a doubling needs 8M, 4S. If one of the input points to the addition is in affine coordinates only 12M and 2S are needed. So, also here mixed coordinates are faster.*
Note that multiplications by a_2 *are counted; if* a_2 *is chosen so that multiplications by it are cheap then 1M is saved in doubling.*

Like in the case of odd characteristic the correspondence between Jacobian coordinates and affine coordinates is that $(X_P : Y_P : Z_P)$ represent the affine point $P = (X_P/Z_P^2, Y_P/Z_P^3)$.

Remark 6.6.4 (Jacobian coordinates)
Let $P = (X_P : Y_P : Z_P), Q = (X_Q : Y_Q : Z_Q)$ *so that* $P \neq Q, \mathrm{inv}_\oplus(Q), P_\infty$. *The formulae for addition* $P \oplus Q = S$ *are as follows:*
Addition:

$$A = X_P Z_Q^2;\ B = X_Q Z_P^2;\ C = Y_P Z_Q^3;\ D = Y_Q Z_P^3;\ E = A + B;$$
$$F = C + D;\ G = EZ_P;\ H = FX_Q + GY_Q;\ Z_S = GZ_Q;\ I = F + Z_S;$$
$$X_S = a_2 Z_S^2 + FI + E^3;\ Y_S = IX_S + G^2 H.$$

Doubling*:*

$$A = X_P^2;\ B = A^2;\ C = Z_P^2;$$
$$X_S = B + a_6 C^4;\ Z_S = X_P C;\ Y_S = BZ_S + (A + Y_P Z_P + Z_S)X_S.$$

We have $\mathrm{inv}_\oplus(X_P : Y_P : Z_P) = (X_P : X_P Z_P + Y_P : Z_P)$. *One addition needs 16M, 3S while a doubling needs 5M, 5S. If one of the input points to the addition is in affine coordinates only 11M and 3S are needed. So also here mixed coordinates are faster.*
Note that multiplications by a_2 *are counted; if* a_2 *is chosen so that multiplications by it are cheap then 1M is saved in addition.*

It was noted that in the case of even characteristic, the powers of Z used in Jacobian coordinates are not optimally fitting. Lopez and Dahab suggested a new system in which $(X_P : Y_P : Z_P)$ represent the affine point $P = (X_P/Z_P, Y_P/Z_P^2)$. Since the optimal formulae for these coordinates depend a lot on the curve coefficients a_2 and a_6 we omit the formulae here. The "Handbook" gives a long discussion.
Koblitz suggested to use special binary curves for particularly fast arithmetic. His proposal is included in the NIST standard. The curves are considered over $\mathbb{F}_{2^n}$ for some integer $n \geq 160$ but all coefficients are in $\mathbb{F}_2$. In Exercise 6.4.13.c we found all such curves of cryptographic interest. In fact all non-supersingular elliptic curves over $\mathbb{F}_2$ are isomorphic to one of the E_a and the range of n is what is currently considered to be secure.

The main reason that *Koblitz curves* are interesting is that the Frobenius endomorphism operates by squaring each coordinate which is very cheap in a binary field. We have already seen that for $P \in E(\mathbb{F}_{2^n})$ also $\sigma(P) \in E(\mathbb{F}_{2^n})$. Applying this argument repeatedly one sees that $\sigma^i(P) \in E(\mathbb{F}_{2^n})$ for any positive integer i. Furthermore, there exists an integer s so that $\sigma(P) = [s]P$ and the integer is unique modulo the order of P.
Koblitz showed that for each integer k one can find a sequence of coefficients $k_i \in \{0, 1\}$ so that $[k]P = \sum_{i=0}^{n-1}[k_i]\sigma^i(P)$, where the summation refers to the group operation $\oplus$. This was improved by several authors culminating in a paper by Solinas in which he provides an analogue of the NAF expansion of integers. So, he chooses the coefficients k_i in the larger set $\{-1, 0, 1\}$ and additionally requires that $k_i k_{i+1} = 0$, i.e. there are no two adjacent nonzero coefficients. The key idea is to use the characteristic polynomial of the Frobenius endomorphism (6.3) and read it as

$$[2]P = \mathrm{inv}_{\oplus}\left(\sigma^2(P) \oplus [-t]\sigma(P)\right).$$

This is an example of representing a scalar multiplication by a sum of $\sigma^i(P)$. In this case there is no cost reduction due to this approach. In general this leads to huge savings since the expansions are similar to binary NAF expansions and applying the Frobenius endomorphism is much cheaper than a doubling. We do not go into the details on how to compute the expansions; the interested reader should consult the literature and the NIST standard.

Exercise 6.6.5 *a) Show that an elliptic curve of the form* $E : y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, a_3 \in \mathbb{F}_{2^n}^*, a_2, a_4, a_6 \in \mathbb{F}_{2^n}$ *is nonsingular.*
Show that E *is isomorphic to a curve of the form* $y^2 + \bar{a}_3 y = x^3 + \bar{a}_4 x + \bar{a}_6$.
We remark that curves of this form are supersingular.

b) We consider the elliptic curve $y^2 + xy = x^3 + x^2 + 1$ *over* $\mathbb{F}_{2^4} \cong \mathbb{F}_2[w]/(w^4 + w + 1)\mathbb{F}_2[w]$. *Show that* $P = (w^2 + w + 1, 1)$ *is on the curve and compute* $[5]P$. *Use the computations to find the order of* P.

Compute $\sigma^5(P) \oplus \sigma^2(P) \oplus P$. *Which multiple of* P *is this?*

Chapter 7

Primes

Prime numbers play an important role in cryptography – as factors of RSA numbers as well as basis for finite fields. So far we have ignored the question how to find primes and how to prove that an integer is actually prime.

Showing that a number n is composite can be easy – one can just provide a nontrivial factor $1 < m < n$ and verify that $n \equiv 0 \bmod m$. Showing that a candidate number is prime turns out to be much harder. In this chapter we present some primality tests which more or less efficiently and reliable solve this problem. Note, that these tests do only provide a "yes or no" type of answer and not an actual factor in the composite case.

We consider practical tests with a "good" running time. We only comment on elliptic curve primality testing and proving since we have not provided enough background knowledge to explain them. From a theoretical point of view the paper "Primes is in P" giving a polynomial time deterministic algorithm for proving primality was a breakthrough. Readers are highly recommended to read that paper and subsequent improvements. In practice, however, probabilistic tests are used as they provide better performance.

These tests are probabilistic in the sense that they detect composites (or primes, depending on the test) with a certain probability. The first interesting test we present is based on Fermat's little theorem. If a number is prime then it will always pass the test. A composite number passes the test with probability at most $1/2$. If the test outputs "composite" we know for sure that the number is composite. Otherwise we can run the test again to increase the probability of false positives. For this particular test there is another class of numbers that always passes the test, so we have to exclude them as well.

If one wants to be sure that a given number is prime and cannot rely on the statement, that it is very likely to be prime, then one needs to use a different type of test. Namely one that detects primes with a certain probability, so that the answer "prime" is true for sure when given.

In practice, both types of tests are used to find primes. One first identifies a candidate prime with a (repeated) test of the first type and then proves with a test of the second type, that the number is actually prime.

Primality and compositeness tests and proves are considered in number theory

and are covered by many books on algorithmic number theory. We give a short list of some publications that are also interesting for the other chapters.

- R. M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press.
- J. Buchmann, Introduction to Cryptography, Springer.
- H. Cohen, A Course in Computational Algebraic Number Theory, Springer.
- R. Crandall, C. Pomerance, Prime Numbers: A Computational Perspective, Springer.
- N. Koblitz, A Course in Number Theory and Cryptography, Springer.

7.1 Naive tests

In this and the following section we deal with an integer n and want to determine whether it is (likely to be) prime or not. Since divisibility by 2 is easy to detect we assume n to be odd.
Naively we can perform a trial division n mod a for each number a up to $\sqrt{a}$. If n factors as $n = km$ then at least one of k, m must be $\leq \sqrt{n}$.

Algorithm 7.1.1 (Naive test)
IN: *Odd* $n \in \mathbb{N}$.
OUT: *Answer to "Is* n *prime?" and if not a divisor of* n.

1. $a \leftarrow 3$, $bool \leftarrow 0$
2. `while` $bool = 0$ *do*
   (a) `if` $n \bmod a = 0$
      i. $bool = 1$
      ii. `return` *"no"*, a
   (b) `else if` $a < \sqrt{n}$
      i. $a \leftarrow a + 2$
   (c) `else`
      i. $bool = 1$
      ii. `return` *"yes"*

Clearly, this test works and will deterministically find a factor of n if it is composite. However, the running time is $O(\sqrt{n})$ modular reductions. One drawback of this very naive method is that the algorithm tries *all* numbers a and not only the possible prime divisors. If a number is not divisible by 3 then it certainly will

not be divisible by 9 so that test as well as all further tests involving multiples of 3 should be skipped.
The *Sieve of Eratosthenes* works this way and allows to find all prime numbers below n and also factors of n. Since we are interested in finding out whether a single given integer is prime, we skip the details and move on to more efficient tests which do no longer provide the factors of n.

7.2 Tests proving compositeness

This section considers tests which are always passed by prime numbers while composite numbers have a non-negligible chance of being detected in which case the test proves that the number is composite.
In Corollary 3.3.7 we stated Fermat's little theorem. Let n be the integer we want to test. The theorem says that for all $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ one has $a^{\varphi(n)} \equiv 1 \bmod n$. If n is prime then $\gcd(a, n) = 1$ for all $1 < a < n$ and $\varphi(n) = n - 1$. Therefore

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

for all $1 < a < n$ if n is prime. If this fails for some a then we know for sure that n is not prime. Repeated application of this *Fermat test* with random choices of a turns the test into an algorithm for compositeness proving. We first analyze whether there are other numbers than prime numbers that always pass the test. For that we first need to introduce some terminology.

Definition 7.2.1 (Pseudo-prime)
Let n be a composite integer and let $a \in \mathbb{Z}$ with $1 < a < n$ and $\gcd(a, n) = 1$. Then n is called a pseudo-prime to the basis *a if $a^{n-1} \equiv 1 \bmod n$, i.e. if it passes the Fermat test using a.*

Are there composite numbers that are pseudo-primes for all bases? If we would run through all $1 < a < n$ deterministically then we would clearly find a factor due to the gcd computation. However, we hope that random choices of a identify composite numbers quickly.

Lemma 7.2.2 *Let n be a composite integer and let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.*

1. *Let $\mathrm{ord}(a)$ denote the multiplicative order of a modulo n. The integer n is pseudo-prime to the basis a if and only if $\mathrm{ord}(a) | n - 1$.*

2. *If n is pseudo-prime to the bases a_1 and a_2 then it is also pseudo-prime to the bases $a_1 a_2 \bmod n$ and $a_1 \cdot a_2^{-1} \bmod n$.*

3. *If there exists an $1 < a < n$ with $\gcd(a, n) = 1$ and $a^{n-1} \not\equiv 1 \bmod n$, then this holds for at least half of all possible bases.*

Proof. If $\mathrm{ord}(a)|n-1$, i.e. $n-1 = \mathrm{ord}(a)n'$ then

$$a^{n-1} = \left(a^{\mathrm{ord}(a)}\right)^{n'} \equiv 1 \bmod n.$$

To prove the other inclusion we assume on the contrary that $a^{n-1} \equiv 1 \bmod n$ and $n-1 = \mathrm{ord}(a)n' + r$ for some $0 < r < \mathrm{ord}(a)$. Then

$$1 \equiv a^{n-1} = a^{\mathrm{ord}(a)n'+r} = \left(a^{\mathrm{ord}(a)}\right)^{n'} a^r = a^r,$$

which gives a contradiction to the minimality of $\mathrm{ord}(a)$.
Let a_1 and a_2 be such that $a_1^{n-1} \equiv 1 \bmod n$ and $a_2^{n-1} \equiv 1 \bmod n$. We have

$$(a_1 a_2)^{n-1} = a_1^{n-1} a_2^{n-1} \equiv 1 \cdot 1 \equiv 1 \bmod n.$$

Likewise

$$(a_1 a_2^{-1})^{n-1} \equiv 1 \cdot 1^{-1} \equiv 1 \bmod n.$$

To prove the third statement let $A = \{a_1, \ldots, a_k\}$ be the set of all bases for which n is pseudo-prime. Let $1 < a < n$ with $\gcd(a, n) = 1$ be such that $a^{n-1} \not\equiv 1 \bmod n$. Then n is not pseudo-prime to the all bases aa_i for $1 \leq i \leq k$ because

$$(aa_i)^{n-1} \equiv a^{n-1} a_i^{n-1} \equiv a^{n-1} \not\equiv 1 \bmod n,$$

where we used that n is a pseudo-prime to the basis a_i. This means that every $a_i \in A$ gives rise to at least one aa_i which detects compositeness and so at least half of all bases detect. □

This results gives an estimate on the probability that a composite number is detected

Remark 7.2.3 *If there is at least one basis that detects compositeness of n then the third result implies that after trying k bases a composite number is detected with probability at least $1 - \frac{1}{2^k}$.*

Unfortunately it turns out that there are composite numbers that pass the Fermat test for all bases, the smallest number being 561. The reader is encouraged to try a few bases.

Definition 7.2.4 (Carmichael number)
If n is a composite integer that is pseudo-prime to all bases then n is called a Carmichael number.

From the first part of Lemma 7.2.2 we see that for each prime factor p of a Carmichael number n we must have that the order of a modulo p divides $n-1$. By Lemma 5.3.1 elements of order $p-1$ exist and thus for each factor p it must hold that $p-1|n-1$.
This holds true in the example $n = 561 = 3 \cdot 11 \cdot 17$ since $2, 10$, and 16 divide 560. The only way to detect compositeness of a Carmichael is by selecting an a such that $\gcd(a, n) \neq 1$ in which case even a factor is found.

Algorithm 7.2.5 (Fermat's compositeness test)
IN: *Odd* $n \in \mathbb{N}$, $k \in \mathbb{N}$
OUT: *"n is composite" or "n is prime with probability at least* $1 - \frac{1}{2^k}$ *or a Carmichael number"*

1. `for` $i = 1$ `to` k
   (a) *choose* $a \in \mathbb{Z}$ *randomly with* $1 < a < n$
   (b) `if` $\gcd(a, n) \neq 1$ `return` *"n is composite"*
   (c) `else if` $a^{n-1} \not\equiv 1 \bmod n$ `return` *"n is composite"*
2. `return` *"n is prime with probability at least* $1 - \frac{1}{2^k}$ *or a Carmichael number"*

Example 7.2.6 *We now use this algorithm to test* $n = 711$ *for compositeness. We have* $\gcd(2, 711) = 1$*, so* $a = 2$ *is an allowed basis. We compute*

$$2^{710} \equiv 256 \bmod 711,$$

which is not equal to 1. Hence, 711 is composite and we only needed one round. As a second example we consider $n = 341$ *and also choose the basis* $a = 2$*. We have*

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

But

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

showing that n *is not prime. So* n *is a pseudo-prime to the base* 2*.*
Finally, we choose $n = 561$*. We have*

$$2^{560} \equiv 1 \bmod 561,\ 5^{560} \equiv 1 \bmod 561,\ 7^{560} \equiv 1 \bmod 561, \ldots$$

However, $3 \mid n$ *and so* n *is not prime. It is pseudo-prime to the bases* $2, 5,$ *and* 7*. Actually as mentioned earlier,* 561 *is the smallest Carmichael number and so* n *is pseudo-prime to all bases* a *with* $\gcd(a, n) = 1$*.*

We would like to have a compositeness test that does detect all composite numbers and for which there is no family of numbers for which it fails. To state such a test we first need some more definitions.

Definition 7.2.7 (Quadratic residue)
Let n *be an integer and let* $0 \leq a < n$*. Then* a *is a* quadratic residue modulo n *if there exists an integer* $0 \leq b < n$ *with* $a \equiv b^2 \bmod n$*.*
Otherwise a *is a* quadratic non-residue modulo n*.*

Definition 7.2.8 (Legendre symbol)
Let $p > 2$ *be a prime and* $a \in Z$*. The* Legendre symbol $\left(\frac{a}{p}\right)$ of a modulo p $\left(\frac{a}{p}\right)$ *is defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ 1, & \text{if } a \text{ is quadratic residue modulo } p \\ -1, & \text{if } a \text{ is quadratic non-residue modulo } p \end{cases}$$

We have seen in Lemma 5.3.1 that the multiplicative group of a finite field is cyclic, so there exists a $1 < g < p$ so that $\mathbb{F}_p^* = \langle g \rangle$. Since every even power g^{2m} of g is a square while every odd power g^{2m+1} is not we have that there are as many squares as non-squares in $\mathbb{F}_p^*$. So if we restrict a to $1 \leq a < p$ then the Legendre symbol modulo p assumes the value 1 as often as the value -1.

Lemma 7.2.9 *Let p be an odd prime and $a \in \mathbb{Z}$. We have*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof. If $p|a$ then both sides equal 0.
From Fermat's little theorem 3.3.7 we have for any b with $\gcd(b, n) = 1$ that $b^{p-1} \equiv 1 \bmod p$.
If a is a quadratic residue modulo p then there exists an integer b with $a \equiv b^2 \bmod p$ and so

$$a^{\frac{p-1}{2}} \equiv \left(b^2\right)^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \bmod p.$$

If a is a quadratic non-residue modulo p, i.e., $a = g^{2j+1}$ for some generator g modulo p, then $a^{\frac{p-1}{2}} = g^{(2j+1)\frac{p-1}{2}} = g^{j(p-1)} \cdot g^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \not\equiv 1 \bmod p$, as otherwise g would have order dividing $p-1$ contradicting that it is a generator, but $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \bmod p$ and so the result is a root of $x^2 - 1$. This polynomial has degree 2 and since p is odd, 1 and -1 are its two distinct roots. So we must have

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p$$

if a is a quadratic non-residue modulo p. □

This property holds for all primes p and will replace the Fermat test in the Solovay-Strassen test. To use this equality as a test we need to find an efficient way to compute the Legendre symbol. The following lemmata collect properties of the Legendre symbol.

Lemma 7.2.10 *Let p be an odd prime number and let $a, b \in \mathbb{Z}$. We have the following properties of the Legendre symbol modulo p:*

1. *If $a \equiv b \bmod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. *If b is not divisible by p we have*

$$\left(\frac{a \cdot b^2}{p}\right) = \left(\frac{a}{p}\right).$$

4. $\left(\frac{1}{p}\right) = 1$; $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Proof. The first property follows immediately from the definition.
If p divides a or b then p divides the product ab and so both sides equal zero.
Now let $\gcd(ab, n) = 1$. We use Lemma 7.2.9 and get

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \bmod p.$$

Since the symbol can only be 1 or -1 the left- and right-hand side are actually equal.
The third property follows from the second and from $\left(\frac{b^2}{p}\right) = 1$ because b^2 apparently is a quadratic residue modulo p.
Lemma 7.2.9 immediately gives the last property. □

We state the following rule without proof.

Lemma 7.2.11 *Let p be an odd prime. We have for the Legendre symbol of 2 modulo p that*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

To significantly reduce the running time of evaluating the Legendre symbol the quadratic reciprocity law is very important. We state it without proof and refer the reader to the literature, e.g. Koblitz' book mentioned in the introduction.

Lemma 7.2.12 (Quadratic reciprocity law)
Let p and q be odd primes. We have the equality

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{q}{p}\right), & p \equiv q \equiv 3 \bmod 4, \\ \left(\frac{q}{p}\right), & \text{otherwise.} \end{cases}$$

Example 7.2.13 *Is 7411 a quadratic residue modulo 9283? Both numbers are prime, which can be proven by e.g. the naive test.*
By the quadratic reciprocity law we have $\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right)$ since both numbers are congruent to 3 modulo 4.
We use the first, the second, and then the third property of Lemma 7.2.10 with $9283 \equiv 1872 \bmod 7411$ and $1872 = 2^4 \cdot 3^2 \cdot 13$ to see $\left(\frac{9283}{7411}\right) = \left(\frac{1872}{7411}\right) = \left(\frac{2^4 \cdot 3^2 \cdot 13}{7411}\right) = \left(\frac{2^4}{7411}\right) \cdot \left(\frac{3^2}{7411}\right) \cdot \left(\frac{13}{7411}\right) = \left(\frac{2}{7411}\right)^4 \cdot \left(\frac{3}{7411}\right)^2 \cdot \left(\frac{13}{7411}\right) = \left(\frac{13}{7411}\right)$.
Since $13 \equiv 1 \bmod 4$ the reciprocity law gives $\left(\frac{13}{7411}\right) = \left(\frac{7411}{13}\right)$ and then $7411 \equiv 1 \bmod 13$. Since $1 = 1^2$ is a quadratic residue the result is 1 and with the previous steps we get

$$\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1}{13}\right) = -1.$$

This means that 7411 is not a square modulo 9283; as a side result we obtained that 1872 is a square modulo 7411.

The Legendre symbol requires the bottom entry to be prime and to apply the reciprocity law both inputs need to be prime. The generalization is given by the Jacobi Symbol.

Definition 7.2.14 (Jacobi symbol)
Let n be an odd integer and let n factor as $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, where the p_i are distinct primes and the exponents α_i are positive integers. Let a be an integer. The Jacobi-Symbol of a modulo n *is defined as*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_r}\right)^{\alpha_r},$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol of a modulo the prime p_i.

Lemma 7.2.15 *Let n, m be odd integers. We have the following rules for the Jacobi symbol:*

$$\begin{aligned}
\left(\frac{ab}{n}\right) &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \\
\left(\frac{2}{n}\right) &= (-1)^{\frac{n^2-1}{8}} \\
\left(\frac{n}{m}\right) &= (-1)^{\frac{(n-1)(m-1)}{4}} \left(\frac{m}{n}\right)
\end{aligned}$$

Proof. The proof is left to the reader as Exercise 7.2.24.c. □

Remark 7.2.16 *Note that we do no longer have the interpretation that $\left(\frac{a}{n}\right) = 1$ implies that a is a square modulo n.*
Consider the case $n = pq$, where p and q are distinct primes, and let a be a quadratic non-residue modulo p and modulo q. Then we have

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = (-1)(-1) = 1.$$

However, a cannot be a square modulo n as $a \equiv b^2 \bmod n$ would imply $a \equiv b^2 \bmod p$.
In fact we will see below that only a quarter of all numbers is a square modulo n.

Lemma 7.2.17 *Let n be a composite odd integer.*
For at least half of all possible bases a with $\gcd(a, n) = 1$ we have that the Solovay-Strassen test *fails, i.e.*

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n.$$

Proof. Let $A = \{a_1, \ldots, a_k\}$ be the set of a_i for which $\left(\frac{a_i}{n}\right) \equiv a_i^{\frac{n-1}{2}} \bmod n$ with $1 \leq a_i < n$ and $\gcd(a_i, n) = 1$.
If there exists an integer $1 \leq b \leq n$ with $\gcd(b, n) = 1$ and $\left(\frac{b}{n}\right) \not\equiv b^{\frac{n-1}{2}} \bmod n$ then we have by the first property in Lemma 7.2.15 that

$$\left(\frac{b \cdot a_i}{n}\right) = \left(\frac{b}{n}\right) \cdot \left(\frac{a_i}{n}\right)$$

while

$$(b \cdot a_i)^{\frac{n-1}{2}} = b^{\frac{n-1}{2}} \cdot a_i^{\frac{n-1}{2}}$$

and so

$$\left(\frac{b \cdot a_i}{n}\right) \not\equiv (b \cdot a_i)^{\frac{n-1}{2}} \bmod n.$$

Therefore, the Solovay-Strassen test detects compositeness with at least 50% of all values a if such a number b exists.
Now we show that such a number b exists. Note, that this proof uses the factorization of n, so it does not help in the actual test.
Let n factor as $n = p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$, where the p_i are distinct odd primes and the exponents α_i are positive integers. We consider two cases.
Let first one of the the exponents α_i be larger than 1, e.g. $p_1^2 \mid n$, and put $n' = n/p_1^2$.
For $b = 1 + \frac{n}{p_1} = 1 + p_1 n'$ we have

$$\left(\frac{b}{n}\right) = \left(\frac{1 + p_1 n'}{n}\right) = \left(\frac{1 + p_1 n'}{p_1}\right)^2 \left(\frac{1 + p_1 n'}{n'}\right) = \left(\frac{1 + p_1 n'}{n'}\right) = \left(\frac{1}{n'}\right) = 1.$$

To show that $b^{\frac{n-1}{2}} \not\equiv 1 \bmod n$ we consider powers of b using the binomial formula. Let $j \in \mathbb{N}$. We have

$$\begin{aligned} b^j &= (1 + p_1 n')^j = \sum_{i=0}^{j} \binom{j}{i} (p_1 n')^i \\ &\equiv 1 + j p_1 n' + \binom{j}{2} (p_1 n')^2 + \ldots \\ &\equiv 1 + j p_1 n' \bmod n, \end{aligned}$$

because $(p_1 n')^2 = n' n \equiv 0 \bmod n$ and the same holds for higher powers. This implies that $b^j \equiv 1 \bmod n$ if and only if $j p_1 n' \equiv 0 \bmod n$, i.e. if and only if $p_1 \mid j$. Because p_1 divides n it does not divide $n - 1$ and therefore also not $(n-1)/2$. Accordingly

$$\left(\frac{b}{n}\right) \not\equiv b^{\frac{n-1}{2}} \bmod n.$$

We now consider the case that the exponents $\alpha_i = 1$, i.e. $n = p_1 \cdots p_r$ is product of distinct primes. Let $1 \leq a < p_1$ be a quadratic non-residue modulo p_1. Put

$n' = n/p_1$. By the Chinese remainder theorem 3.4.20 there exists an integer b in $1 \leq b < n$ which solves the system of equivalences

$$\begin{aligned} b &\equiv a \bmod p_1, \\ b &\equiv 1 \bmod n'. \end{aligned}$$

For this b we have

$$\left(\frac{b}{n}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{n'}\right) = (-1)\left(\frac{1}{n'}\right) = -1$$

but we cannot have $b^{\frac{n-1}{2}} \equiv -1 \bmod n$ since n' divides n and

$$b^{\frac{n-1}{2}} \equiv 1 \bmod n'.$$

So for both cases we have constructed a number b which fails the test. □

We now have presented all the properties required for the Solovay-Strassen test.

Algorithm 7.2.18 (Solovay-Strassen compositeness test)
IN: *Odd* $n \in \mathbb{N}$, $k \in \mathbb{N}$
OUT: *"n is composite" or "n is prime with probability at least* $1 - \frac{1}{2^k}$*"*

1. `for` $i = 1$ `to` k
   (a) *choose* $a \in \mathbb{Z}$ *randomly with* $1 < a < n$
   (b) `if` $\gcd(a, n) \neq 1$ `return` *"n is composite"*
   (c) `else`
      i. $c \leftarrow \left(\frac{a}{n}\right)$ *(computed using Lemma 7.2.15)*
      ii. $d \leftarrow a^{\frac{n-1}{2}} \bmod n$ *(using a representative in* $-n/2 < d < n/2$*)*
      iii. `if` $c \neq d$ `return` *"n is composite"*
2. `return` *"n is prime with probability at least* $1 - \frac{1}{2^k}$*"*

Example 7.2.19 *Let* $n = 711$*. Like before we choose* $a = 2$ *and compute*

$$c = \left(\frac{2}{711}\right) = (-1)^{(711^2-1)/8} = (-1)^{63190} = 1$$

using Lemma 7.2.15. Next we compute $2^{\frac{710}{2}} \equiv 569 \bmod 711$ *and so* $d = 569$*. Since* $c \neq d$ *we see that* n *is composite.*
As a second example we consider $n = 341$ *and again choose the basis* $a = 2$*. We have*

$$c = \left(\frac{2}{341}\right) = (-1)^{(341^2-1)/8} = (-1)^{14535} = -1.$$

While $2^{170} \equiv 1 \bmod 341$ *and so* $c \neq d$ *and already* $a = 2$ *detects* n *as composite. For the Carmichael number* $n = 561$ *we have*

$$c = \left(\frac{2}{561}\right) = (-1)^{(561^2-1)/8} = (-1)^{39340} = 1$$

and $2^{280} \equiv 1 \bmod 561$*; so* n *is a pseudo-prime under the Solovay-Strassen test to the basis* $a = 2$*.*
For $a = 5$ *we obtain:*

$$c = \left(\frac{5}{561}\right) = \left(\frac{561}{5}\right) = \left(\frac{1}{5}\right) = 1$$

and $5^{280} \equiv 67 \bmod 561$*; and so* n *is detected as composite.*

Both of these tests have probability 1/2 of detecting a composite number for each iteration. The Fermat test needs one modular exponentiation per iteration while the Solovay-Strassen test needs one modular exponentiation and the computation of one Jacobi symbol per iteration. In return there are no exceptions to the Solovay-Strassen test while the Carmichael numbers are pseudo-prime for any basis in the Fermat test in spite of being composite.
The compositeness test of Miller and Rabin has probability of detecting a composite number at least 3/4 per iteration. It uses the observation that modulo a prime p there are only two solutions a of $x^2 \equiv 1 \bmod p$ for $-p/2 < a < p/2$. Let $p - 1 = 2^r t$, where t is an odd integer and let $b \in \mathbb{Z}$ with $1 \leq b < p$. Then either $b^t \equiv 1 \bmod p$ or there exists an $r' < r$ so that $b^{2^{r'}t} \equiv -1 \bmod p$.
If n is composite then there are more than two solutions $1 \leq a < n$. Let e.g. $n = pq$ with p, q prime then the Chinese remainder theorem 3.4.20 leads to one solution for each of the 4 choices of sign in

$$\begin{aligned} a &\equiv \pm 1 \bmod p, \\ a &\equiv \pm 1 \bmod q, \end{aligned}$$

and so there are 4 solutions. If n has more factors then there are more solutions. Let n split as $n-1 = 2^r t$, where t is an odd integer. Let $b \in \mathbb{Z}$ with $\gcd(b, n) = 1$. If n is pseudo-prime to the basis b then $b^{n-1} \equiv 1 \bmod n$ but this does not imply that either $b^t \equiv 1 \bmod n$ or that there exists an $r' < r$ so that $b^{2^{r'}t} \equiv -1 \bmod n$ because there are more elements a which are equivalent to 1 modulo n when squared. So if a subsequent squaring of b^t reaches 1 without having reached -1 we know that n is composite. On top of that we detect compositeness of n if it is not pseudo-prime for a chosen basis, namely if $b^{2^r t} \not\equiv 1 \bmod n$.
This motivates the definition of strong pseudo-primes.

Definition 7.2.20 (Strong pseudo-prime)
Let n *be an odd composite integer and let* $n - 1 = 2^r t$*, with* t *odd.*
Let $b \in \mathbb{Z}$ *with* $\gcd(b, n)$*. If either* $b^t \equiv 1 \bmod n$ *or if there exists* $0 \leq r' < r$ *so that* $b^{2^{r'}t} \equiv -1 \bmod n$ *then* n *is a* strong pseudo-prime to the basis b*.*

The above considerations have motivated the following lemma which we present without proof. The interested reader is referred to Koblitz' book mentioned in the introduction to this chapter.

Lemma 7.2.21 *Let n be an odd composite integer. It is a strong pseudo-prime to at most one quarter of all possible bases b.*

Algorithm 7.2.22 (Miller-Rabin compositeness test)
IN: *Odd $n \in \mathbb{N}$, $k \in \mathbb{N}$ with $n-1 = 2^r t$ and t odd*
OUT: *"n is composite" or "n is prime with probability at least $1 - \frac{1}{4^k}$"*

1. `for` $i = 1$ `to` k
   (a) *choose $a \in \mathbb{Z}$ randomly with $1 < a < n$*
   (b) `if` $\gcd(a, n) \neq 1$ `return` *"n is composite"*
   (c) `else if` $a^t \not\equiv \pm 1 \bmod n$
      i. $j \leftarrow 1$
      ii. `while` $a^{2^j \cdot t} \not\equiv \pm 1 \bmod n$ *and* $j < r$
         $j \leftarrow j + 1$
      iii. `if` $a^{2^j \cdot t} \equiv 1 \bmod n$ `return` *"n is composite"*
      iv. `if` $j = r$ `return` *"n is composite"*
2. `return` *"n is prime with probability at least $1 - \frac{1}{4^k}$"*

Example 7.2.23 *Let $n = 711$. We have $n - 1 = 710 = 2^1 \cdot 355$, so $r = 1$ and $t = 355$. We chose again $a = 2$.*
We have $a^t = 2^{355} \equiv 569 \not\equiv 1 \bmod 711$, so the iteration starts. However, $j = 1 = r$ is reached immediately and we obtain n is composite as answer. Note that it is correct to stop the test here because either the next squaring leads to a value $\neq 1$ in which case the Fermat test detects n as composite or n is pseudo-prime to the basis a but reaches the value 1 without having reached -1 which we identified as another criterion for compositeness.
Now consider $n = 341$ with $n - 1 = 340 = 2^2 \cdot 85$, so $r = 2$ and $t = 85$. For the basis $a = 2$ we have

$$2^{85} \equiv 32 \not\equiv 1 \bmod 341, \; 2^{2 \cdot 85} \equiv 1 \bmod 341,$$

and so n is detected as composite since 1 was reached as square of $85 \not\equiv -1 \bmod 341$.
Finally, let $n = 561$ with $n - 1 = 560 = 2^4 \cdot 35$. We have

$$2^{35} \equiv 263 \bmod 561, \; 2^{2 \cdot 35} \equiv 166 \bmod 561, \; 2^{2^2 \cdot 35} \equiv 67 \bmod 561, \; 2^{2^3 \cdot 35} \equiv 1 \bmod 561,$$

which in the last round on the first basis a detects n as composite.

Exercise 7.2.24 *a) Let $n_1 = 717$. Check compositeness of n_1 using the Fermat test.*

b) Compute $\left(\frac{7001}{14175}\right)$.

c) Prove Lemma 7.2.15 using the properties of the Legendre symbol. Hint: study how remainders modulo 8 and 16 behave under multiplication and squaring.

d) Let $n_2 = 709$ and $n_3 = 721$. Use the Miller-Rabin test to check compositeness of n_2 and n_3 for $k = 2$.

7.3 Tests proving primality

This section considers tests which are always passed by composite numbers while prime numbers have a non-negligible chance of being detected in which case the test proves that the number is prime. We present in detail the Pocklington primality test and sketch the idea behind elliptic curve primality proving.
The following test relates primality of n to the primality of a divisor q of $n-1$. So, to apply it one needs to be able to find a factor of $n-1$ and one needs to know that q is prime. This leads to a recursive primality proof where one finally finds a q small enough that the naive test proves primality.

Lemma 7.3.1 *Let n be an odd integer. If there exists a prime factor q of $n-1$ with $q > \sqrt{n}-1$ and if there exists a basis $1 \leq a < n$ with*

1. $a^{n-1} \equiv 1 \bmod n$
2. $\gcd\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$,

then n is prime.

Proof. Let $q > \sqrt{n}-1$ be a prime divisor of $n-1$. If n is not prime there must exist a prime factor p with $p \leq \sqrt{n}$. Since q is prime and $p < q$ we have $\gcd(p-1, q) = 1$. By Bezout's identity (Lemma 3.2.10) there exists an integer u so that $uq \equiv 1 \bmod p-1$.
This implies that for any $1 < a < n$ which satisfies $a^{n-1} \equiv 1 \bmod n$ (so in particular $p \nmid a$) we have

$$a^{\frac{n-1}{q}} \equiv a^{uq\frac{n-1}{q}} = a^{u(n-1)} \equiv 1 \bmod p.$$

Which, in turn, implies

$$p \mid \gcd\left(a^{\frac{n-1}{q}} - 1, n\right),$$

so that no a can satisfy both criteria if n is composite. □

First of all we point out that for n a prime the first part of the Pocklington test is always satisfied. The second one is not satisfied if and only if $a^{(n-1)/q} \equiv 1 \bmod n$.

Lemma 7.3.2 *Let n be a prime so that $n-1$ has a prime factor $q > \sqrt{n}-1$. For a fraction of $1/q$ of all bases a we have $\gcd\left(a^{(n-1)/q} - 1, n\right) = n$.*

Proof. The bound $q > \sqrt{n} - 1$ on q implies in particular that $q^2 \not| n-1$. Since n is prime, the multiplicative group modulo n is cyclic and generated by some $1 < g < n$. The powers g^j of g for which $(g^j)^{(n-1)/q} \equiv 1 \bmod n$ are exactly those j which are divisible by q, i.e. the $(n-1)/q$ multiples of q less than $n-1$. This corresponds to a fraction of $1/q$ of all bases. □

Note that the proof did not use the bound on q other than in the consequence that $q^2 \not| n-1$.
This lemma implies that a large fraction of all bases a serve as *witnesses* of the primality of n, i.e. they detect n as prime. Repeated use of this criterion with random choices of the basis a makes it likely that a *witness* is found which proves n to be prime. Since for each a also $a^{n-1} \equiv 1 \bmod n$ is checked, the test can also lead to proving compositeness.

Algorithm 7.3.3 (Pocklington primality test)
IN: *Odd* $n \in \mathbb{N}$, $k \in \mathbb{N}$, *prime* q *with* $q|n-1$ *and* $q > \sqrt{n} - 1$
OUT: *"n is prime" or "n is composite" or "n is composite with probability at least* $1 - \frac{1}{q^k}$*"*

1. `for` $i = 1$ `to` k
   (a) *choose* $a \in \mathbb{Z}$ *randomly with* $1 < a < n$
   (b) `if` $\gcd(a, n) \neq 1$ `return` *"n is composite"*
   (c) `else if` $a^{n-1} \not\equiv 1 \bmod n$ `return` *"n is composite"*
   (d) `else if` $\gcd\left(a^{(n-1)/q} - 1, n\right) = 1$ `return` *"n is prime"*
2. `return` *"n is composite with probability at least* $1 - \frac{1}{q^k}$*"*

Example 7.3.4 *Consider* $n = 283$. *We have* $282 = 6 \cdot 47$ *and will prove in the next step that* 47 *is a prime. The condition that* $47 > \sqrt{283} - 1 > 15.82$ *is satisfied so that the test can be applied. Pick* $a = 2$ *and compute* $2^{282} \equiv 1 \bmod 283$ *and* $2^6 \equiv 64 \bmod 283$. *This means that* $\gcd(2^6 - 1, 283) = \gcd(63, 283) = 1$ *and so the basis* 2 *is a witness to* 283 *being prime, where we assume that* 47 *is prime.*
Now consider $nm = 47$. *We have* $46 = 2 \cdot 23$ *and* $23 > \sqrt{47} - 1 > 5.85$. *We could repeat all previous steps to show that* $23 = 2 \cdot 11 + 1$ *and* $11 = 2 \cdot 5 + 1$ *are prime, thus linking the primality of* 283 *to that of* 5 *but we skip the further steps and only show the next round. Again we choose* 2 *as he basis. We have* $2^{46} \equiv 1 \bmod 47$ *and* $2^2 \equiv 4 \bmod 47$, *so that* $\gcd(2^2 - 1, 47) = \gcd(3, 47) = 1$ *and* $a = 2$ *detects* 47 *as prime.*

A problem with applying Pocklington's test as stated is that $n-1$ needs to have a large prime factor. There are different versions of this test, including the historically earliest due to Lucas, which deal with other cases but require more knowledge on the factorization of $n-1$. We state one test without proof.

Lemma 7.3.5 *Let $k, m, n \in \mathbb{Z}$ with $n-1 = km$, where $m > k$ and $\gcd(k, m) = 1$, and suppose the factorization of m is known. If for every prime factor q of m there exists an integer $a > 1$ such that*

1. $a^{n-1} \equiv 1 \bmod n$
2. $\gcd\left(a^{\frac{n-1}{q}} - 1, n\right) = 1$,

then n is prime.

Notice that different a's can be used for each prime q.

Looking at what we have done in an abstract way we notice that we are using the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ and the conditions are about divisors of the alleged group order $|(\mathbb{Z}/n\mathbb{Z})^\times| = n - 1$. An alternative is to use an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ and working with an alleged group order which one obtains assuming that n is prime. We do not treat point counting algorithms in this manuscript and so the following has to remain sketchy. For the moment assume that we are able to find an m so that $[m]P = P_\infty$ if one uses the affine group operations as in Chapter 6. For details we refer to the literature.

Lemma 7.3.6 *Let n be an odd integer. Let E denote the set of solutions to*

$$y^2 \equiv x^3 + ax + b \bmod n,$$

where $\gcd(4a^3 + 27b^2, n) = 1$. Let $m \in \mathbb{N}$ and let q be prime with $q|m$ and $q > (n^{1/4} + 1)^2$. If there exists a point $P \in E$ with

1. $[m]P = P_\infty$,
2. $[\frac{m}{q}]P \neq P_\infty$ *and* $[\frac{m}{q}]P$ *defined,*

then n is prime.

Exercise 7.3.7 *a) Use the Pocklington test to prove that $n_2 = 709$ is prime. You can take for granted that 7 is prime.*

Notation Index

I

K

L

M

N

P

Q

R

S

T

Z

General Index

W

Z