L.J. Perrenet

Decoding CSIDH

A Guide to Isogeny-Based Cryptography

Master thesis,

Mathematisch Instituut, Universiteit Leiden.

Supervised by Dr. S.A. Arpin.

July 22, 2024.

Universiteit Leiden

The Netherlands

An uncompiled, LaTeX version of this thesis is available at
`https://github.com/jorisperrenet/MasterThesis`.

Abstract

In today's digital age, private communication is anchored in robust encryption techniques. As the horizon of quantum computing draws nearer, current encryption methods may soon become vulnerable to quantum attacks, pointing to the need for post-quantum cryptography. The CSIDH encryption scheme [1], grounded in isogeny-based cryptography, emerges as a compelling candidate for such post-quantum cryptography. Understanding CSIDH requires a solid grasp of finite fields, number fields, and particularly elliptic curves. This thesis strives to break down these topics to make the innovative CSIDH approach more accessible, encouraging further exploration in the field of isogeny-based cryptography to ensure digital privacy for years to come.

Introduction

In the world of digital communication, the robustness of encryption algorithms is of great concern. Weak encryption algorithms pose a risk of sensitive information leakage, as messages could be decoded without our consent. The digital era has made information rapidly accessible across great distances. Yet, this convenience comes with a downside: the possibility of unauthorised interception by eavesdroppers. Encrypting our messages is a very reliable measure to prevent such breaches. However, the advent of quantum computing challenges our existing encryption methods, revealing susceptibilities to quantum attacks, highlighting the necessity for encryption methods that are resistant to such threats. CSIDH [1], an encryption scheme founded on isogeny-based cryptography, is believed to be a promising example of such a quantum-resistant encryption scheme. The method relies on mathematical theories and concepts such as finite fields, number fields, and elliptic curves.

Organised into five chapters (see Figure 1), this thesis lays out the groundwork of algebraic structures relevant to CSIDH, aiming to provide an explanation of the CSIDH algorithm. As a result, we hope to make the CSIDH algorithm more accessible in order to encourage further research in the area of isogeny-based cryptography, promoting the privacy of digital communication in the era of quantum computing.

Chapter 1 introduces the concept of finite fields, as well as how to construct them. The subsequent chapter is on number fields, number rings, and ideals, an important concept for understanding the CSIDH algorithm. Chapter 3 focuses on elliptic curves, detailing their properties and establishing a basis for isogeny-based cryptography. Elaborating on this theory, Chapter 4 explores isogenies, isomorphisms, and endomorphisms of elliptic curves. This chapter further explores how ideals can act on elliptic curves, culminating in the introduction of isogeny graphs, an illustrative concept that helps with visualising isogeny-based cryptography.

The final chapter ties together the explored concepts, concentrating on their applications in encryption schemes. It begins with an overview of the Diffie-Hellman key exchange, describing how two parties can reach a shared secret. Subsequently, it presents the CSIDH encryption scheme, using the theory from the previous chapters. Lastly, we discuss a variant of the CSIDH scheme, providing proofs and a way to break this variant if one can break CSIDH.

To further illustrate the inner workings of the CSIDH encryption scheme, we have implemented a generic, unoptimised version of the algorithm using SageMath [2]. The computer code for this implementation is accessible in Appendix A and on `https://github.com/jorisperrenet/MasterThesis`.

An alternative strategy for reading this thesis might be to begin with Section 5.2, which explains the CSIDH encryption scheme. By starting here, readers can grasp the ultimate objective and the requirements for achieving it. They can then decide what sections and chapters to read to supplement their existing knowledge in order to understand the algorithm.

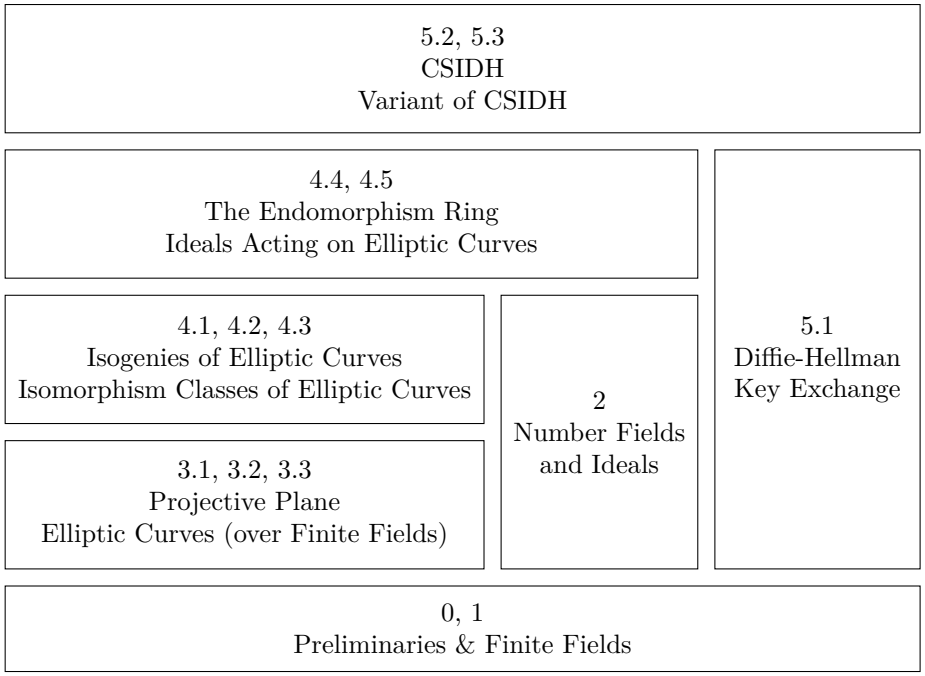

Figure 1: The conceptual hierarchy of sections within this thesis is depicted as a series of rectangles, where a rectangle positioned above another indicates that the understanding of concepts introduced in the upper rectangle necessitates knowledge from the sections outlined in the lower rectangle.

Contents

Chapter 0

Preliminaries

This chapter aims to provide some of the background knowledge that the other chapters of this thesis rely on. Before we move on to a couple of explicit definitions, we first state some topics that we regard as prerequisites to this thesis. If the reader is not familiar with any of these subjects, they are referred to [3], [4], or [5] (depending on the subject). We also note that online resources are readily available for most of these prerequisites. In particular, we assume that the reader is familiar with (and has a thorough understanding of) the following.

- The (set of all) integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, and the reals $\mathbb{R}$.
- Prime numbers, divisors, prime factorisation, greatest common divisors, and the Euler totient function.
- Sets and subsets, as well as unions, intersections, differences, and the Cartesian product of sets together with the corresponding notation.
- The notation surrounding maps, the definition of one-to-one and bijective maps, the composition of maps, and the definitions of homomorphisms, isomorphisms, and endomorphisms.
- Addition and multiplication of polynomials, as well as knowing what coefficients and terms of a polynomial are.
- (Equivalence) relations, equivalence classes and the notation of basic propositional logic.
- Summations, linear combinations, (the dimension and rank of) vector spaces, and (the trace and determinant of) matrices.
- The basics of group actions, i.e., when is something a group action.

0.1 Groups and Rings

Definition 0.1. A *(binary) operation* on a set G is a map $G \times G \to G$.

Definition 0.2. A non-empty set G with a binary operation on G, which we denote here as $\circ : G \times G \to G$, is called a *group* if the following three requirements are met.

- (*Associativity*) For all $a, b, c \in G$, one has $a \circ (b \circ c) = (a \circ b) \circ c$.
- (*Identity element*) There is an $e \in G$ such that, for all $a \in G$, we have that $e \circ a = a \circ e = a$.
- (*Inverse element*) For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$.

If G is a group there is exactly one identity element in G, and every element of G has exactly one inverse [3, Theorem 2.4]. Also, the group G is called *commutative* or *abelian* if it satisfies the following additional requirement.

- (*Commutativity*) For all $a, b \in G$ we have that $a \circ b = b \circ a$.

A non-empty subset H of a group G is called *closed* under the operation $\circ$ if for any pair $(a, b) \in H \times H$ we have that $a \circ b \in H$ (where $\circ$ is the operation of the group G), and for any $a \in H$ we have that $a^{-1} \in H$ (where a^{-1} is the inverse of a in G). In that case, we call H a *subgroup* of G as we can restrict $\circ$ to get a map $\circ : H \times H \to H$, yielding an operation on H.

A *finite group* is a group with only finitely many elements. The number of elements of a finite group is called its *order*.

Definition 0.3. A group G under some operation is said to be *finitely generated* if there is some finite subset of G such that every element of G can be written (under the group operation and taking inverses) as a combination of finitely many elements of the subset.

Definition 0.4. A non-empty set R equipped with two binary operations, which we call *addition* and *multiplication* and denote by $+ : R \times R \to R$ and $\cdot : R \times R \to R$ respectively, is called a *ring* if the following requirements are met.

- The set R is an abelian group under the $+$ operation (with the additive identity element denoted by 0).
- The set R is associative under multiplication and has a multiplicative identity element, which we denote by 1 (also, we require that $0 \neq 1$ in this thesis).
- Multiplication in R is distributive over addition, i.e., for every $a, b, c \in R$ we require that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and that $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

A ring R is called a *commutative ring* if multiplication in R is commutative.

A subset S of the ring R is called a *subring* of R if S contains the multiplicative identity of R and S is closed (Definition 0.2) under the addition and multiplication operation (of the ring R).

Just like with a group, a *finite ring* is a ring with only finitely many elements. The number of elements of a finite ring is called its *order*.

0.2 Modulo Arithmetic

Let $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ be a set under the usual addition and multiplication operations.

Definition 0.5. Let $a, b \in \mathbb{Z}$ with $b > 0$ be arbitrary. Then, there exist unique [3, Theorem 1.3] integers q and r called the *quotient* and *remainder*, respectively, of the division of a by b such that $a = qb + r$ and $0 \leq r < b$.

Fix n to be a positive integer, in order to define the ring $\mathbb{Z}/n\mathbb{Z}$ we let a and b denote positive integers. Define the relation $\sim$ between a and b such that $a \sim b \iff a$ and b have the same remainder after division by n. This relation is an equivalence relation, and we call its equivalence classes *residue classes modulo* n. Since there are n different remainders, there are exactly n different residue classes modulo n. We can now define $\mathbb{Z}/n\mathbb{Z}$ as the set containing the n residue classes modulo n. For any $a \in \mathbb{Z}$ we let $(a \bmod n)$ denote the residue class that contains a. If a and b belong to the same residue class, i.e., $a \sim b$, we say that a and b are *congruent* modulo n, and denote this by $a \equiv b \pmod{n}$. We define the $+$ operator on $\mathbb{Z}/n\mathbb{Z}$ to be the map sending $((a \bmod n), (b \bmod n)) \to ((a + b) \bmod n)$, where the $+$ on the right-hand side is the ordinary addition taken in $\mathbb{Z}$. Similarly, we let the $\cdot$ operator on $\mathbb{Z}/n\mathbb{Z}$ satisfy $(a \bmod n) \cdot (b \bmod n) = ((a \cdot b) \bmod n)$. Under these two operations $\mathbb{Z}/n\mathbb{Z}$ forms a commutative ring.

Chapter 1

Finite Fields

In many mathematical textbooks, the theory of finite fields is considered to be a prerequisite. This causes most books to be unsuitable for learning from top to bottom to the ones that do not grasp the full scope of finite fields. With that in mind, this chapter aims to provide a thorough explanation of the theory on finite fields, as we will use it in later parts of this thesis.

Commencing with fundamental principles that define a finite field, this chapter progressively reveals the existence and creation of finite fields. Although this chapter introduces the subject quite extensively, it is still focused on providing background for the rest of the thesis. Therefore, not all the existing theory on finite fields is stated. If the reader is interested in a more complete theory, they are encouraged to consult [6], [7], and [8].

1.1 Fields

Definition 1.1. A non-empty set F equipped with two binary operations, which we call *addition* and *multiplication* and denote by $+ : F \times F \to F$ and $\cdot : F \times F \to F$ respectively, is called a *field* if the following requirements are met.

- The set F is an abelian group under the $+$ operation (with the additive identity element denoted by 0).
- The set $F \setminus \{0\}$ is an abelian group under the $\cdot$ operation (we usually denote this group as F^* and denote its multiplicative identity element as 1).
- Multiplication in F is distributive over addition, i.e., for every $a, b, c \in F$ we require that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and that $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

A subset K of the field F is called a *subfield* of F if K is a field with respect to the addition and multiplication operation (of the field F). If K is a subfield of F, then F is called an *extension (field)* of K.

Remark. Equivalently, a field F is a commutative ring (Definition 0.4) where $0 \neq 1$ and all elements of $F \setminus \{0\}$ are invertible (i.e., have an inverse element in $F \setminus \{0\}$) under multiplication.

Remark. Similar to groups and rings, a field is called a *finite field* if it has finitely many elements. The number of elements of a finite field F is called its *order*.

With respect to our usual addition and multiplication operation, it can be shown that $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{Z}/7\mathbb{Z}$ are fields.
Additionally, we can see that $\mathbb{Z}$ is not a field as $\mathbb{Z} \setminus \{0\}$ does not contain an inverse element for any numbers except -1 and 1. To motivate this, note that $\mathbb{Z} \subset \mathbb{Q}$. Now, if $\mathbb{Z}$ is a field

then it will be a subfield of $\mathbb{Q}$ as $\mathbb{Q}$ is a field with the same operations. As $\mathbb{Q} \setminus \{0\}$ is a group with respect to multiplication (since $\mathbb{Q}$ is a field) we find that $2 \in \mathbb{Q}$ has a unique inverse. Since 1 is the multiplicative identity of $\mathbb{Q}$ we know that the unique inverse of 2 must equal $1/2 \in \mathbb{Q}$. Now, $1/2 \notin \mathbb{Z}$, contradicting the fact that $\mathbb{Z}$ contains an inverse element for $2 \in \mathbb{Z}$. Therefore, $\mathbb{Z}$ cannot be a subfield of $\mathbb{Q}$, and in turn $\mathbb{Z}$ cannot be a field.
Likewise, $(\mathbb{Z}/12\mathbb{Z})^*$ does not contain an inverse element for the residue class $(3 \bmod 12)$ as we can not find an $x \in \mathbb{Z}$ such that $3x \equiv 1 \pmod{12}$. We can conclude that $\mathbb{Z}/12\mathbb{Z}$ is not a (finite) field.

Theorem 1.2. *Let n be a positive integer. Then $\mathbb{Z}/n\mathbb{Z}$ is a finite field if and only if n is prime.*

Proof. First, let n be a positive integer, but not a prime. To prove necessity, we assume that $\mathbb{Z}/n\mathbb{Z}$ is a finite field and prove that it leads to a contradiction. Since n is not prime, there exists an integer d such that $1 < \gcd(d, n) < n$. For any such d, let $a \in (\mathbb{Z}/n\mathbb{Z})^*$ denote the multiplicative inverse of $(d \bmod n)$, note that this inverse exists by our assumption that $\mathbb{Z}/n\mathbb{Z}$ is a finite field. Since a is the inverse of $(d \bmod n)$ we know that $(d \bmod n) \cdot a = (1 \bmod n)$. Let $a' \in \mathbb{Z}$ be an element of the residue class of a, we find that there exists some integer b such that $d \cdot a' - b \cdot n = 1$. We know that $\gcd(d, n)$ divides both d and n, thus it divides the left-hand side of our equation, implying that it must also divide 1. Since $\gcd(d, n) > 1$ we know that the equation cannot hold, resulting in a contradiction. Therefore, $\mathbb{Z}/n\mathbb{Z}$ can only be a finite field if n is prime. A proof of sufficiency can be found in [9, Theorem 3] and in [10, Theorem 7.5]. □

In our previous example we have stated that $\mathbb{Z}/7\mathbb{Z}$ is a field. In fact, this is a direct consequence of Theorem 1.2. In this example, we will show that $\mathbb{Z}/7\mathbb{Z}$ is a field using brute force calculations.
First, let 0 through 6 denote the elements of $\mathbb{Z}/7\mathbb{Z}$ (where each number is used to denote the residue class that contains it). We will get the following addition and multiplication tables concerning these elements:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

For the abelian group (Definition 0.2) with respect to addition, we verify the following.

- Identity element: It is clear that 0 is our identity element, and that $0+a = a+0 = a$ holds for all $a \in \mathbb{Z}/7\mathbb{Z}$.
- Inverse element: The addition table has one, and exactly one, 0 on each of its rows and columns. Upon looking in the row of some $a \in \mathbb{Z}/7\mathbb{Z}$, there will be an element $b \in (\mathbb{Z}/7\mathbb{Z})$ such that $a+b = 0$ (the element b can be found in the column containing the 0).
- Commutativity: The addition table is symmetric around its main diagonal, we must thus have that for all $a, b \in \mathbb{Z}/7\mathbb{Z}$, the equality $a + b = b + a$ holds.
- Associativity: Let $a, b, c \in \mathbb{Z}/7\mathbb{Z}$, then $(a + b) + c = a + (b + c)$ holds. This can be seen by verifying all possible a, b, and c.

For the abelian group $(\mathbb{Z}/7\mathbb{Z}) \setminus \{0\}$ with respect to multiplication:

- Identity element: It is clear that 1 is our identity element, and that $1 \cdot a = a \cdot 1 = a$ holds for all $a \in \mathbb{Z}/7\mathbb{Z}$.
- Inverse element: The inverse of an element can be found by first finding the 1 in its row and subsequently looking at the column that contains the 1.
- Commutativity: The multiplication table is likewise symmetric around its main diagonal, commutativity follows.
- Associativity: Let $a, b, c \in (\mathbb{Z}/7\mathbb{Z}) \setminus \{0\}$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ holds. This can be seen by verifying all possible a, b, and c.

Finally, the distributive property of $\mathbb{Z}/7\mathbb{Z}$ can be verified by checking all possibilities. We now know that $\mathbb{Z}/7\mathbb{Z}$ is a (finite) field due to Definition 1.1.

As we shall see in Theorem 1.9, it turns out that there only exist finite fields with p^m elements, for any prime p and positive integer m. The finite field of that order is denoted as $\mathbb{F}_{p^m}$. Moreover, any two fields of order p^m are isomorphic. We already know that for $m = 1$ the set $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a finite field due to Theorem 1.2, however constructing finite fields for integers $m > 1$ requires a little more effort.

1.2 Polynomial Rings

For this entire section, we let p denote a prime number and R a commutative ring (Definition 0.4). Note that any field is also a commutative ring.

Definition 1.3. We define the *polynomial ring* $R[x]$ for any commutative ring R as the set of all polynomials in x (with finitely many terms) with coefficients in R (note that x is a variable and its value does not need to be in R). Let n be a non-negative integer, using our definition of $R[x]$ we say that the set

$$\left\{ \sum_{i=0}^{n} a_i x^i, \quad \text{with } a_0, a_1, \ldots, a_{n-1} \in R \text{ and } a_n \in R \setminus \{0\} \right\} \tag{1.1}$$

contains all polynomials $f \in R[x]$ of *degree* n. Generally, the degree of a polynomial $f \in R[x]$ is denoted as $\deg(f)$. Furthermore, we define the degree of the *zero polynomial*, i.e., the polynomial $0 \in R[x]$, to be $-\infty$*. Building on equation (1.1), we call a_n the *lead coefficient* of a polynomial in any such set. A polynomial is called *monic* if its lead coefficient equals 1.

Equivalently, we can define $R[x]$ as the union of all sets from equation (1.1) for arbitrary non-negative integers n together with the zero polynomial.

Remark. If f is a polynomial in a polynomial ring $R[x]$, then we use the notation f and $f(x)$ interchangeably in this thesis to denote the polynomial.

Multiplication and addition (denoted by $\cdot$ and $+$, respectively) in this polynomial ring work as expected.

Define two polynomials $f(x) = 3x^8 + 6 \in \mathbb{F}_7[x]$ and $g(x) = x^2 + 2x + 1 \in \mathbb{F}_7[x]$. Using Definition 1.3 we find that $\deg(f) = 8$, $\deg(g) = 2$, f has lead coefficient 3, and g is monic.

*This definition is not used throughout all literature, sometimes the degree of the zero polynomial is defined to be non-existent.

Also, $f(x)+g(x) = 3x^8+x^2+2x \in \mathbb{F}_7[x]$ and $f(x)\cdot g(x) = 3x^{10}+6x^9+3x^8+6x^2+5x+6 \in \mathbb{F}_7[x]$.

Definition 1.4. Let $f \in R[x]$ be an arbitrary polynomial. For all polynomials $g \in R[x]\setminus\{0\}$ (i.e., excluding the zero polynomial) there exist unique [11, Theorem 3.16] polynomials $q, r \in R[x]$ such that $\deg(r) < \deg(g)$ and $f(x) = q(x)g(x)+r(x)$. These polynomials are called the *quotient* and *remainder*, respectively, of the division of $f(x)$ by $g(x)$ (this division is sometimes denoted as $f(x)/g(x)$).

In this example, we determine the quotient and the remainder of $f(x)/g(x)$ using long division where $f(x) = 9x^5 + 3x^4 + 5x^3 + 6x^2 + 8x + 1$ and $g(x) = 2x^3 + x^2 + 7$ are both elements of $\mathbb{F}_{11}[x]$. For the first step, we note that $10 \cdot (2x^3 + x^2 + 7) = 9x^3 + 10x^2 + 4$. Remember that all coefficients of these polynomials are in $\mathbb{F}_{11}$.[†]

$$
\begin{array}{rl}
2x^3 + x^2 + 7 / & 9x^5 + 3x^4 + 5x^3 + 6x^2 + 8x + 1 \setminus 10x^2 + 2x + 7 \\
& \underline{9x^5 + 10x^4 \qquad + 4x^2} \\
& \qquad 4x^4 + 5x^3 + 2x^2 + 8x + 1 \\
& \qquad \underline{4x^4 + 2x^3 \qquad + 3x} \\
& \qquad\quad 3x^3 + 2x^2 + 5x + 1 \\
& \qquad\quad \underline{3x^3 + 7x^2 \qquad + 5} \\
& \qquad\qquad 6x^2 + 5x + 7
\end{array}
$$

Therefore, we can write $f(x) = q(x)g(x) + r(x)$ with $q(x) = 10x^2 + 2x + 7$ and $r(x) = 6x^2 + 5x + 7$. Note that $\deg(r) < \deg(g)$ indeed holds. If $\deg(r) \geq \deg(g)$, we should have continued the long division by removing additional factors of $g(x)$ from the leftover $r(x)$ until $\deg(r) < \deg(g)$ is satisfied.

[†]This is the Dutch notational variant of long division or "staartdeling". The denominator is written down left of the /, the numerator comes next and after the \ the quotient is denoted element by element. The denominator is multiplied by the first element of the quotient (which one needs to figure out and write down), this is then subtracted from the numerator and the result is written below a long horizontal line. Now the result becomes the new numerator and the process is repeated. At the end you can find the remainder of the division at the bottom and the quotient at the top right.

Definition 1.5. A non-constant (i.e., of degree at least 1) polynomial $f \in R[x]$ is called *irreducible* if there does not exist a polynomial $g \in R[x]$ such that $0 < \deg(g) < \deg(f)$ and the remainder of $f(x)/g(x)$ is the zero polynomial.

Now that we have provided some definitions regarding polynomial rings $R[x]$ for any commutative ring R (which will be needed in upcoming chapters), we start by stating theorems concerning only $\mathbb{F}_p[x]$ (this does not mean that some theorems do not generalise to other polynomial rings).

Similar to how non-zero integers can be uniquely factored into products of prime numbers and -1, non-zero polynomials $f \in \mathbb{F}_p[x]$ can be uniquely factored into products of monic irreducible polynomials and a constant in $\mathbb{F}_p^*$ [12, Theorem 1.2.17].

The polynomial $f(x) = 2x^2 + x + 1$ in $\mathbb{F}_3[x]$ is irreducible. To illustrate this, we write it in the form $q(x)g(x) + r(x)$ where $g(x)$ iterates through all possible polynomials in $\mathbb{F}_3[x]$ with $0 < \deg(g) < \deg(f)$:

$$
\begin{array}{ll}
(2x+1)(x)+1 & (x+2)(2x)+1 \\
(2x+2)(x+1)+2 & (x)(2x+1)+1
\end{array}
$$

$$(2x)(x+2)+1 \qquad (x+1)(2x+2)+2.$$

No remainder equals the zero polynomial, $f(x)$ is thus irreducible.*

The polynomial $f(x) = x^3 + x + 1$ is not irreducible in $\mathbb{F}_3[x]$. It can be expressed as the product of two polynomials $p(x) = x + 2$ and $q(x) = x^2 + x + 2$ of non-zero degree. The remainder of dividing $f(x)$ by either $p(x)$ or $q(x)$ will result in the zero polynomial.

In $\mathbb{F}_{19}[x]$, the polynomial $f(x) = 4x^{11} + 5x^3 + 13x^2 + 7x + 15$ is not irreducible. The unique factorisation (up to permutation of the factors) of $f(x)$ equals

$$(4)(x+9)(x^2+10x+3)(x^3+15x^2+17)(x^5+4x^4+18x^3+9x^2+10x+6)$$

and is thus the product of monic irreducible polynomials in $\mathbb{F}_{19}[x]$ multiplied by the constant $4 \in \mathbb{F}_{19}^*$. Or, as you can also see it, the polynomial $4 \in \mathbb{F}_{19}[x]$ of degree 0.

*A faster way to check irreducibility of a polynomial $f(x) \in \mathbb{F}_p[x]$ with $\deg(f) \geq 2$ is to check for roots. That is, if $f(x)$ is irreducible then there does not exist an $a \in \mathbb{F}_p$ such that $f(a) = 0$. The converse only holds if $f(x)$ is a polynomial of degree 2 or 3.

Definition 1.6. Let $f, g \in \mathbb{F}_p[x]$ be arbitrary and fix $h \in \mathbb{F}_p[x] \setminus \{0\}$. We say that f and g are *congruent* modulo h if the remainder of $f(x)/h(x)$ equals the remainder of $g(x)/h(x)$. This congruence is denoted as $g \equiv f \pmod h$ and forms an equivalence relation. We denote the equivalence classes of this relation by $(f \bmod h)$. The set of all these equivalence classes is denoted by $\mathbb{F}_p[x]/(h)$.

Following the notation of the definition, one can define the $+$ operation on $\mathbb{F}_p[x]/(h)$ by the map $((f \bmod h), (g \bmod h)) \to ((f+g) \bmod h)$, where $f+g$ is evaluated using polynomial addition. Similarly, one can let the $\cdot$ operation satisfy $(f \bmod h) \cdot (g \bmod h) = ((f \cdot g) \bmod h)$. Equipped with the $+$ and $\cdot$ operator, $\mathbb{F}_p[x]/(h)$ forms a commutative ring [12, Theorem 1.3.8].

Let $f(x) = 9x^5 + 3x^4 + 5x^3 + 6x^2 + 8x + 1$ and $g(x) = 2x^3 + x^2 + 7$ be defined over $\mathbb{F}_{11}[x]$ (note that these are the same polynomials as in the long division example). We can write $f(x) = q(x)g(x) + r(x)$ with $q(x) = 10x^2 + 2x + 7$ and $r(x) = 6x^2 + 5x + 7$.
Furthermore,

$$r(x) + g(x) \equiv 2x^3 + 7x^2 + 5x + 3 \equiv 6x^2 + 5x + 7 \equiv r(x) \pmod{g(x)}.$$

Likewise, each intermediate result in the previous long division example is contained in $(r \bmod g)$ as in the process of the long division we only subtracted multiples of g from the original polynomial f.

1.3 Finite Fields of p^m Elements

Combining our theory on fields and polynomial rings, we are able to construct finite fields of p^m elements, where p is a prime number and m is a positive integer.

Theorem 1.7. *Fix p to be a prime number and let $g \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree m. Following the notation from Definition 1.6, we find that $\mathbb{F}_p[x]/(g)$ forms a finite field of order p^m.*

Proof. A proof can be found in [10, Theorem 7.9] or in [12, Theorems 1.3.13, 1.3.15]. □

Theorem 1.8. *There exists at least one irreducible polynomial $g \in \mathbb{F}_p[x]$ of degree m for every integer $m \geq 1$ and every prime p.*

Proof. For a proof, the reader is referred to [12, Theorem 2.6.6] or [6, Lemma 1.4]. □

Theorem 1.9. *Every finite field F is isomorphic to a finite field $\mathbb{F}_p[x]/(g)$ constructed by an irreducible polynomial $g \in \mathbb{F}_p[x]$. Moreover, for every prime p and every integer $m \geq 1$ there exists exactly one finite field with p^m elements up to isomorphism, meaning that one can always find an isomorphism between two finite fields of p^m elements. Finite fields with an order that can not be written as the power of a prime, i.e., in the form p^m, do not exist.*

Proof. Proofs of this theorem can be found in [6, Section 1.1 up to Theorem 1.2], [10, Theorems 7.16, 7.18], and [12, Theorems 2.6.2, 2.8.9]. □

Theorem 1.10. *Under multiplication $\mathbb{F}_{p^m}^*$ forms a cyclic group, i.e., there exists an element $\alpha \in \mathbb{F}_{p^m}^*$ such that $\mathbb{F}_{p^m}^* = \{1, \alpha, \ldots, \alpha^{p^m-2}\}$. Such an element is called a primitive element[†], and there are exactly $\varphi(p^m - 1) > 0$ distinct primitive elements in $\mathbb{F}_{p^m}^*$ where φ denotes Euler's totient function.*

Proof. A proof that $\mathbb{F}_{p^m}^*$ is cyclic and generated by primitive elements is contained in [6, Theorem 1.3]. For the number of distinct primitive elements, the reader is referred to [10, Theorem 7.13]. □

Also, under addition $\mathbb{F}_{p^m}$ is isomorphic to the vector space $(\mathbb{F}_p)^m$, meaning that we can represent every polynomial $g \in \mathbb{F}_p[x]/(f)$ (where f is an irreducible polynomial in $\mathbb{F}_p[x]$ of degree m) as a vector. For example, $g(x) = (x^3 + 2x + 1 \bmod f) \in \mathbb{F}_3[x]/(f)$ with $f = x^4 + x + 2$ can be represented as `1021`, where each term (from highest to lowest degree) has an entry equal to their coefficient in $g(x)$.

We would like to illustrate some properties of $\mathbb{F}_8$ by highlighting them in the following example.
We take the irreducible polynomial $f(x) := x^3 + x^2 + 1 \in \mathbb{F}_2[x]$ and write down the elements of $\mathbb{F}_2[x]/(f)$ (note that by Theorem 1.7 this is a finite field of order 8), to get

$$(0 \bmod f), (1 \bmod f), (x \bmod f), (x+1 \bmod f), (x^2 \bmod f),$$
$$(x^2+1 \bmod f), (x^2+x \bmod f), \text{ and } (x^2+x+1 \bmod f).$$

In vector notation, these can be denoted by `000`, `001`, `010`, `011`, `100`, `101`, `110`, and `111`, respectively. Let $s = (x \bmod f)$, and view 0 and 1 as $(0 \bmod f)$ and $(1 \bmod f)$, respectively. We find that $\mathbb{F}_2[x]/(f)$ can be written as $\{0, 1, s, s+1, s^2, s^2+1, s^2+s, s^2+s+1\}$.
Let $\alpha \in \mathbb{F}_2[x]/(f)$ denote a root of f, implying that we must have $\alpha^3 + \alpha^2 + 1 = 0$. To check whether some choice for α is a root of f, we need to check whether $\alpha^3 + \alpha^2 + 1 = 0$ holds, given that $s^3 + s^2 + 1 = 0$.
For example, in order to check whether $\alpha = s + 1$ is a root, we evaluate

$$(s+1)^3 + (s+1)^2 + 1 = s^3 + s + 1 \neq 0,$$

implying that $s + 1$ is not a root of f. However, if we take $\alpha = s^2 + s + 1$, we get

$$(s^2+s+1)^3 + (s^2+s+1)^2 + 1 = (s^3+s^2+1)(s^3+s+1) = 0.$$

Implying that $s^2 + s + 1$ is a root of f, and thus presents a valid choice for α. Similarly, s and s^2 are also roots of f.

[†]It is said that a primitive element of $\mathbb{F}_{p^m}$ is a *generator* of $\mathbb{F}_{p^m}^*$. Conversely, each generator of $\mathbb{F}_{p^m}^*$ is called a *primitive element* of $\mathbb{F}_{p^m}$.

For the rest of this example we take $\alpha := s \cong \texttt{010}$. Keeping in mind that coefficients of the polynomials are in $\mathbb{F}_2$, we have

$$\begin{aligned}
0 &= && = 0 && \cong \texttt{000},\\
\alpha^0 &= && = 1 && \cong \texttt{001},\\
\alpha^1 &= && = \alpha && \cong \texttt{010},\\
\alpha^2 &= && = \alpha^2 && \cong \texttt{100},\\
\alpha^3 &= && = \alpha^2 + 1 && \cong \texttt{101},\\
\alpha^4 &= && \alpha \cdot \alpha^3 = \alpha(\alpha^2+1) = \alpha^3 + \alpha = \alpha^2 + \alpha + 1 && \cong \texttt{111},\\
\alpha^5 &= && \alpha \cdot \alpha^4 = \alpha(\alpha^2+\alpha+1) = \alpha^2 + 1 + \alpha^2 + \alpha = \alpha + 1 && \cong \texttt{011},\\
\alpha^6 &= && \alpha \cdot \alpha^5 = \alpha(\alpha+1) = \alpha^2 + \alpha && \cong \texttt{110},\\
\alpha^7 &= && \alpha \cdot \alpha^6 = \alpha(\alpha^2+\alpha) = \alpha^2 + 1 + \alpha^2 = 1 && \cong \texttt{001}.
\end{aligned}$$

It can also be seen that $\mathbb{F}_8^* \cong (\mathbb{F}_2)^3 \setminus \{\texttt{000}\}$ is indeed cyclic as $\alpha^7 = \alpha^0 \cong \texttt{001}$. Moreover, α is a primitive element of $\mathbb{F}_2[x]/(f)$ as it generates all of $\mathbb{F}_8^*$. Using vector notation (and the equations above) addition and multiplication can be easily done within $\mathbb{F}_2[x]/(x^3+x^2+1)$. E.g., $\texttt{101} + \texttt{011} = \texttt{110}$ (similar to a bitwise XOR operator since coefficients are in $\mathbb{F}_2$). And $\texttt{101} \cdot \texttt{011} \cong \alpha^3 \cdot \alpha^5 = \alpha^8 = \alpha^1 \cong \texttt{010}$, using the useful cyclic property of $\mathbb{F}_8^*$.

We will also illustrate similar properties of $\mathbb{F}_9$. Define $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$. Since f is irreducible and of degree 2 we know that $\mathbb{F}_3[x]/(f)$ is a finite field of order 9. The elements of $\mathbb{F}_3[x]/(f)$ are

$$\begin{gathered}
(0 \bmod f), (1 \bmod f), (2 \bmod f), (x \bmod f), (x+1 \bmod f),\\
(x+2 \bmod f), (2x \bmod f), (2x+1 \bmod f), \text{ and } (2x+2 \bmod f).
\end{gathered}$$

In vector notation, these can be denoted by $\texttt{00}, \texttt{01}, \texttt{02}, \texttt{10}, \texttt{11}, \texttt{12}, \texttt{20}, \texttt{21}$, and $\texttt{22}$, respectively.
We can already answer questions regarding addition in $\mathbb{F}_9$, such as $\texttt{02} + \texttt{11} = \texttt{10}$, which can also be expressed as $(2 \bmod f) + (x+1 \bmod f) = (x \bmod f)$. Similarly, $\texttt{20} + \texttt{22} = \texttt{12}$, representing $(2x \bmod f) + (2x+2 \bmod f) = (x+2 \bmod f)$. Things get more difficult if we start looking at multiplication. For example, to calculate $\texttt{10} \cdot \texttt{21}$ we would have to find $(x \bmod f) \cdot (2x+1 \bmod f) = (2x^2 + x - 2f \bmod f) = (2x+2 \bmod f)$. Implying that $\texttt{10} \cdot \texttt{21} = \texttt{22}$. This calculation is tedious (and becomes increasingly more tedious in larger finite fields), so we look for a simpler method.
To this end, when necessary, view $0, 1$, and 2 as $(0 \bmod f), (1 \bmod f)$, and $(2 \bmod f)$, respectively, and let $\alpha \in \mathbb{F}_3[x]/(f)$ be a root of f, implying that $\alpha^2 + \alpha + 2 = 0$. In this example we take $\alpha := (x \bmod f) \cong \texttt{10}$, as one can verify that this is indeed a root of f. Assuming that α is a primitive element, we know that $\mathbb{F}_9^*$ forms a cyclic group generated by powers of α.

$$\begin{aligned}
\alpha^0 &= && = 1 && \cong \texttt{01},\\
\alpha^1 &= && = \alpha && \cong \texttt{10},\\
\alpha^2 &= && = 2\alpha + 1 && \cong \texttt{21},\\
\alpha^3 &= && \alpha \cdot \alpha^2 = \alpha(2\alpha+1) = 2\alpha^2 + \alpha = 2\alpha + 2 && \cong \texttt{22},\\
\alpha^4 &= && \alpha \cdot \alpha^3 = \alpha(2\alpha+2) = 2\alpha^2 + 2\alpha = 2 && \cong \texttt{02},\\
\alpha^5 &= && \alpha \cdot \alpha^4 = 2\alpha && \cong \texttt{20},
\end{aligned}$$

$$\begin{aligned}
\alpha^6 &= \alpha \cdot \alpha^5 = 2\alpha^2 = \alpha + 2 && \cong \texttt{12},\\
\alpha^7 &= \alpha \cdot \alpha^6 = \alpha(\alpha+2) = \alpha^2 + 2\alpha = \alpha + 1 && \cong \texttt{11},\\
\alpha^8 &= \alpha \cdot \alpha^7 = \alpha(\alpha+1) = \alpha^2 + \alpha = 1 && \cong \texttt{01}.
\end{aligned}$$

If we want to calculate $(x \bmod f) \cdot (2x + 1 \bmod f)$ at this point we can perform the calculation $(x \bmod f) \cdot (2x + 1 \bmod f) \cong \texttt{10} \cdot \texttt{21} \cong \alpha \cdot \alpha^2 = \alpha^3 \cong \texttt{22} \cong (2x + 2 \bmod f)$ instead.
Now we choose to define $\mathbb{F}_9$ by taking the irreducible polynomial $g(x) = x^2 + 1 \in \mathbb{F}_3[x]$. We expect that the finite field $\mathbb{F}_3[x]/(g)$ has exactly the same properties as our previous finite field $\mathbb{F}_3[x]/(f)$ as we know that both fields are isomorphic due to Theorem 1.9.
Let $\alpha := (x \bmod g) \cong \texttt{10}$, then α is a root of g, giving $\alpha^2 + 1 = 0$. This choice of α is not a primitive element of $\mathbb{F}_9^*$ since we have $(\alpha + 2)^2 = \alpha^2 + \alpha + 1 = \alpha$, meaning that α is a square in $\mathbb{F}_9^*$. A different way to see that α is not a primitive element arises when writing out the powers of α as before, finding that some elements of $\mathbb{F}_9^*$ are missing.
Instead, we let $\beta := \alpha + 1 = (x + 1 \bmod g) \cong \texttt{11}$ generate $\mathbb{F}_9^*$, as, contrary to α, this is a primitive element of $\mathbb{F}_9^*$. Note that β is not a root of g, thus we do not have $\beta^2 + 1 = 0$, however, we still have $\alpha^2 + 1 = 0$, as α is a root of g. We defined β as $\alpha + 1$, thus we have $\alpha = \beta - 1$, substituting this into $\alpha^2 + 1 = 0$ gives the minimal polynomial for β, which equals $\beta^2 - 2\beta + 2 = 0$. Writing out powers of β gives:

$$\begin{aligned}
\beta^0 &= 1 && \cong \texttt{01},\\
\beta^1 &= \alpha + 1 && \cong \texttt{11},\\
\beta^2 &= (\alpha+1) \cdot \beta = \alpha^2 + 2\alpha + 1 = 2\alpha && \cong \texttt{20},\\
\beta^3 &= (\alpha+1) \cdot \beta^2 = 2\alpha^2 + 2\alpha = 2\alpha + 1 && \cong \texttt{21},\\
\beta^4 &= (\alpha+1) \cdot \beta^3 = 2\alpha^2 + 1 = 2 && \cong \texttt{02},\\
\beta^5 &= (\alpha+1) \cdot \beta^4 = 2\alpha + 2 && \cong \texttt{22},\\
\beta^6 &= (\alpha+1) \cdot \beta^5 = 2\alpha^2 + \alpha + 2 = \alpha && \cong \texttt{10},\\
\beta^7 &= (\alpha+1) \cdot \beta^6 = \alpha^2 + \alpha = \alpha + 2 && \cong \texttt{12},\\
\beta^8 &= (\alpha+1) \cdot \beta^7 = \alpha^2 + 2 = 1 && \cong \texttt{01}.
\end{aligned}$$

It may seem that $\mathbb{F}_3[x]/(g)$ gives rise to a different multiplication table as $\mathbb{F}_3[x]/(f)$. For example, evaluating $(x \bmod g) \cdot (2x + 1 \bmod g)$ in $\mathbb{F}_3[x]/(g)$ gives

$$(x \bmod g) \cdot (2x + 1 \bmod g) \cong \texttt{10} \cdot \texttt{21} \cong \beta^6 \cdot \beta^3 = \beta^9 = \beta \cong \texttt{11} \cong (x + 1 \bmod g).$$

However, we know from Theorem 1.9 that these finite fields must be isomorphic. To illustrate that this is indeed true the two tables below are multiplication tables over $\mathbb{F}_3[x]/(f)$ and $\mathbb{F}_3[x]/(g)$, respectively. Notice that the arrangement of colours in both tables is identical, despite some colours representing different elements in each table. This observation confirms that these two finite fields are isomorphic, differing only in the permutation of their elements.

·	01	02	10	11	12	20	21	22
01	01	02	10	11	12	20	21	22
02	02	01	20	22	21	10	12	11
10	10	20	21	01	11	12	22	02
11	11	22	01	12	20	02	10	21
12	12	21	11	20	02	22	01	10
20	20	10	12	02	22	21	11	01
21	21	12	22	10	01	11	02	20
22	22	11	02	21	10	01	20	12

·	01	02	11	12	10	22	20	21
01	01	02	11	12	10	22	20	21
02	02	01	22	21	20	11	10	12
11	11	22	20	01	12	10	21	02
12	12	21	01	10	22	02	11	20
10	10	20	12	22	02	21	01	11
22	22	11	10	02	21	20	12	01
20	20	10	21	11	01	12	02	22
21	21	12	02	20	11	01	22	10

1.4 The Algebraic Closure of Fields

Let R denote a commutative ring and let F denote a field for this section.

Definition 1.11. The monic polynomial in $R[x]$ of the largest possible degree that divides (i.e., the remainder of the division is the zero polynomial) two polynomials $f, g \in R[x]$ (not both the zero polynomial) is called the *greatest common divisor* of f and g and is denoted as $\gcd(f, g)$.

Definition 1.12. A field F is called *algebraically closed* if every non-constant polynomial $f \in F[x]$ has a root in F. An *algebraic extension* of a field F is an extension field K of F (Definition 1.1) such that every element of K is a root of some non-zero polynomial in $F[x]$. A field $\overline{F}$ is called an *algebraic closure* of F if $\overline{F}$ is an algebraic extension of F and $\overline{F}$ is algebraically closed.

Theorem 1.13. *Every field F has exactly one algebraic closure, denoted as $\overline{F}$, up to isomorphism.*

Proof. A proof can be found in [14, Tag 09GP]. □

Remark. Because of this theorem, instead of calling $\overline{F}$ **an** algebraic closure of F, we will call $\overline{F}$ **the** algebraic closure of F.

Let $f(x) = x^2 + 7x + 12 \in \mathbb{Z}[x]$ (remember that $\mathbb{Z}$ is a commutative ring) and $g(x) = 2x + 8 \in \mathbb{Z}[x]$. We have that $f(x) = (x + 3)(x + 4)$ and $g(x) = 2(x + 4)$, so that $\gcd(f, g) = x + 4 \in \mathbb{Z}[x]$.

The set of complex numbers, $\mathbb{C}$, is algebraically closed by the Fundamental Theorem of Algebra [15]. This means that for every non-constant polynomial

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

with $a_0, \ldots, a_n \in \mathbb{C}$, the equation $f(z) = 0$ only admits solutions with $z \in \mathbb{C}$.

The field of rational numbers, $\mathbb{Q}$, is not algebraically closed, as for example the roots of $x^2 - 2 \in \mathbb{Q}[x]$ are not elements of $\mathbb{Q}$.
The field of real numbers, $\mathbb{R}$, is also not algebraically closed, as for example $x^2 + 1 \in \mathbb{R}[x]$ does not contain roots in $\mathbb{R}$.
Since $\mathbb{C}$ is a field containing the field $\mathbb{R}$ we know that $\mathbb{C}$ is an extension field of $\mathbb{R}$. Moreover, arbitrary elements $a+bi \in \mathbb{C}$ are roots of the non-zero polynomial $x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$. Therefore, $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$. Since $\mathbb{C}$ is algebraically closed, we find that $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

Chapter 2

Number Fields and Ideals

CSIDH, a form of isogeny-based cryptography, relies on the intricate relationships between elliptic curves. Isogeny graphs offer a clear lens on how CSIDH functions, marking elliptic curves as nodes and isogenies as edges of the graph. These isogenies are shaped by the actions of ideals on elliptic curves. For those eager to grasp the basics of CSIDH quickly, the first couple of sections of this chapter on number fields, number rings, and ideals provide a solid start. Yet, to truly appreciate the depth of isogeny graphs and the mechanics behind the CSIDH encryption scheme, delving into the entire chapter is recommended.

After establishing the groundwork in the first two sections, Section 2.3 and Section 2.4 discuss norms, traces, discriminants, and (fundamental) units, equipping readers with the analytical tools for the more advanced topics ahead. The journey continues through Section 2.5 and Section 2.6, which explore factorisation of ideals and class groups of number fields. The last section presents an example incorporating all the theories discussed throughout this chapter.

2.1 Number Fields

First off, let us remember from Definition 1.1 what subfields and extension fields are.

Definition 2.1. A subset K of a field F is called a *subfield* of F if K is a field with respect to the addition and multiplication operation of the field F. Similarly, an *extension (field)* of a field K is a field F such that $K \subseteq F$ and the addition and multiplication operation of F are those of K.

Definition 2.2. A *field extension* is defined to be a pair of fields F and K such that F is an extension field of K. The *degree* of the field extension is denoted as $[F : K]$, and equals the dimension of F as a vector space over K.

> The field $\mathbb{C}$ is an extension field of $\mathbb{R}$ as $\mathbb{R}$ is a field and the addition and multiplication operation of $\mathbb{C}$ are inherited from $\mathbb{R}$. We have that $[\mathbb{C} : \mathbb{R}] = 2$ as $\{1, i\}$ is a basis.
> The complex numbers, $\mathbb{C}$, also form an extension field of $\mathbb{Q}$. The degree of this field extension, however, is infinite (as $[\mathbb{C} : \mathbb{Q}]$ is infinite).

Definition 2.3. A *number field* (typically denoted by the capital letter K) is an extension field of the field of rational numbers $\mathbb{Q}$ such that the corresponding field extension has finite degree.

Remark. The *degree* of a number field is said to be the degree of the corresponding field extension.

Definition 2.4. Let α be the root of a monic irreducible polynomial $p \in \mathbb{Q}[x]$ (Definition 1.3) of degree n with rational coefficients. We can *adjoin* α to the field of rational numbers, forming

the number field

$$\mathbb{Q}(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} : c_i \in \mathbb{Q} \text{ for all } 0 \leq i < n\}.$$

Remark. In other literature (such as [16] and [17]) one can find the definition that $\mathbb{Q}[\alpha]$ is the smallest ring containing $\mathbb{Q}$ and α, and that $\mathbb{Q}(\alpha)$ is the smallest field containing $\mathbb{Q}$ and α. That way, $\mathbb{Q}(\alpha)$ automatically becomes a number field. One can then show that $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(p)$ (which is defined similar to finite fields) and prove that $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$. From those results, one can see that our definition of $\mathbb{Q}(\alpha)$ indeed forms a number field.

Constructing a number field using Definition 2.4 will imply that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, and that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$.

Let $\sqrt{2}$ be a root of $x^2 - 2$, a monic irreducible polynomial of degree 2. We can adjoin $\sqrt{2}$ to $\mathbb{Q}$, giving

$$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}.$$

We can verify that this is indeed a field using Definition 1.1. Naturally, we have that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$, confirming that $\mathbb{Q}(\sqrt{2})$ is a number field.
Thus, $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2})$ is an extension field of $\mathbb{Q}$, the degree of the field extension is $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$.

2.2 Number Rings and Ideals

In this section, we will discuss number rings. Generally, all rings (Definition 0.4) discussed in this thesis will be commutative with respect to multiplication.

Definition 2.5. A *number ring* is a subring of a number field K. If the number ring is finitely generated (Definition 0.3) of rank $[K : \mathbb{Q}]$, then we call the number ring an *order* of K.

Definition 2.6. The *ring of integers* of a number field K is denoted as $\mathcal{O}_K$ and contains all orders of K. It is said to be the *maximal order* in K. Conversely, all orders R of K are subrings of $\mathcal{O}_K$ such that $[\mathcal{O}_K : R]$ (the dimension of $\mathcal{O}_K$ as a vector space over R) is finite. Additionally, the ring of integers contains all roots that lie in K of monic polynomials in $\mathbb{Z}[x]$ [18, Theorem 3.20].

Remark. One can find equivalent definitions for the ring of integers and (maximal) orders of a number field. Examples are contained in [19], [20], [18], and [21].

Theorem 2.7. *Let $\mathbb{Q}(\alpha)$ denote the number field of degree n obtained by adjoining α to $\mathbb{Q}$, where α is a root of some monic irreducible polynomial in $\mathbb{Q}[x]$. For every order R of $\mathbb{Q}(\alpha)$, there exists a basis $\{\omega_1, \omega_2, \ldots, \omega_n\}$ of $\mathbb{Q}(\alpha)$ such that*

$$R = \omega_1\mathbb{Z} \times \omega_2\mathbb{Z} \times \cdots \times \omega_n\mathbb{Z}.$$

That is, every element in R is a $\mathbb{Z}$-linear combination of the basis $\{\omega_1, \omega_2, \ldots, \omega_n\}$.

Proof. See [21, Proposition 2.2] and [18, p. 20]. Equivalent definitions of an order using this theorem can be found in [22, pp. 212, 213] and [23, Definition 1]. □

Definition 2.8. Let α be a root of a monic irreducible polynomial in $\mathbb{Z}[x]$ of degree n. Then $\mathbb{Z}[\alpha]$ is defined as

$$\mathbb{Z}[\alpha] = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} : c_i \in \mathbb{Z} \text{ for all } 0 \leq i < n\}.$$

Remark. To avoid confusion, if we write $\mathbb{Z}[\alpha]$ in this thesis, we generally mean that α is the root of a monic irreducible polynomial in $\mathbb{Z}[x]$.

We have that $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a number ring of the number field $\mathbb{Q}(\sqrt{2})$. Since it is finitely generated (by 1 and $\sqrt{2}$) it is also an order of the number field $\mathbb{Q}(\sqrt{2})$. Also, $\mathbb{Z}[\sqrt[3]{5}] = \{a + b\sqrt[3]{5} + c\sqrt[3]{25} : a, b, c \in \mathbb{Z}\}$ is a number ring of $\mathbb{Q}(\sqrt[3]{5})$. However, $S := \{a + b\sqrt[3]{5} : a, b \in \mathbb{Z}\}$ is not a number ring of $\mathbb{Q}(\sqrt[3]{5})$ as it is not closed under multiplication since $(\sqrt[3]{5})^2 \notin S$.

The number field $\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} : a, b \in \mathbb{Q}\}$ has ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ (in Section 2.5 we see how one can compute this). We can see that $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z} \times \frac{1+\sqrt{5}}{2}\mathbb{Z}$. As $\mathbb{Z}[2\sqrt{5}]$ is a subring of $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ and $\left[\mathbb{Z}[\frac{1+\sqrt{5}}{2}] : \mathbb{Z}[2\sqrt{5}]\right] = 4$ is finite, we know that $\mathbb{Z}[2\sqrt{5}]$ is an order of $\mathbb{Q}(\sqrt{5})$. Now, every element in $\mathbb{Z}[2\sqrt{5}]$ is a $\mathbb{Z}$-linear combination of the basis $\{1, 2\sqrt{5}\}$.

Definition 2.9. Number fields of degree 2 are called *quadratic number fields*.

Let D be a squarefree integer (without any squared factors) unequal to 0 and 1. For any positive integer m, we define the quadratic number field $\mathbb{Q}(\sqrt{m^2 D})$. We know that the order $\mathbb{Z}[\sqrt{m^2 D}]$ satisfies $\mathbb{Z}[\sqrt{m^2 D}] = \mathbb{Z}[m\sqrt{D}]$. Therefore, we have that the order $\mathbb{Z}[\sqrt{m^2 D}]$ is a subring of the order $\mathbb{Z}[\sqrt{D}]$. Hence, multiplication and addition of elements in $\mathbb{Z}[\sqrt{m^2 D}]$ can also be carried out in $\mathbb{Z}[\sqrt{D}]$. Therefore, we are typically only interested in the case $m = 1$.

In the integers we are quite familiar with the concept of prime numbers. A positive integer greater than 1 is prime if it cannot be factored into two strictly smaller positive integers. So, one might wonder, what happens in our newly created number rings. It turns out that our old concept of primality does not hold any more, to which end ideals are introduced.

Definition 2.10. Let R be a commutative (number) ring. An *ideal* I of R is an additive subgroup of R satisfying $ra \in I$ for all $r \in R$ and $a \in I$. The ideal generated by 0, i.e., the ideal that only contains the additive identity element of R, is called the *zero ideal* of R.

Remark. Previously, we noted that all rings considered in this thesis will also be commutative. Likewise, all number rings we consider will be finitely generated, so that they become orders. If R is an order in a number field, then every ideal I is a finitely generated subgroup of R. Therefore, we often denote an ideal by its generators (wrapped in brackets to distinguish them from elements in $\mathbb{Z}$).

Let $R = \mathbb{Z}$ be our commutative ring. We find that $I = (3)$ is an ideal in R. The ideal is generated by the element $3 \in \mathbb{Z}$ and thus contains only the numbers in $\mathbb{Z}$ that are divisible by 3.

Let $R = \mathbb{Z}[\sqrt{-11}]$ be an order in the number field $\mathbb{Q}[\sqrt{-11}]$. The ideal $I = (1 + \sqrt{-11})$ is generated by $1 + \sqrt{-11}$, e.g., we have that $\sqrt{-11} \cdot (1 + \sqrt{-11}) \in I$. Let $r = a + b\sqrt{-11}$ with $a, b \in \mathbb{Z}$ denote an arbitrary element of R. We must have $r \cdot (1 + \sqrt{-11}) \in I$.
Suppose that $I = \{r \cdot (1 + \sqrt{-11}) : r \in R\} = \{(a - 11b) + (a + b)\sqrt{-11} : a, b \in \mathbb{Z}\}$. To verify that $ra \in I$ for all $r \in R$ and $a \in I$, we note that $a \in I$ implies that there exists a $t \in R$ such that $t + t\sqrt{-11} = a$. Our constraint thus becomes that $rt \cdot (1 + \sqrt{-11}) \in I$. But, as R is a ring, we know that $rt \in R$. Therefore, the constraint is satisfied, and we indeed have that $I = (1 + \sqrt{-11}) = \{(a - 11b) + (a + b)\sqrt{-11} : a, b \in \mathbb{Z}\}$ is an ideal.

Similarly, the ideal $J = (2)$ is the set of numbers $J = \{2a+2b\sqrt{-11} : a, b \in \mathbb{Z}\}$. For every $r = c+d\sqrt{-11}$ with $c, d \in \mathbb{Z}$ we have $r(2a+2b\sqrt{-11}) = 2(ac-11bd)+2(bc+ad)\sqrt{-11} \in J$.

Choose $R = \mathbb{Z}[\sqrt[3]{5}]$, then the ideal $I = (2 + 3\sqrt[3]{5} + \sqrt[3]{25})$ equals

$$I = \{(2a + 5b + 15c) + (3a + 2b + 5c)\sqrt[3]{5} + (a + 3b + 2c)\sqrt[3]{25} : a, b, c \in \mathbb{Z}\}.$$

Take α to be a root of the polynomial $x^2 + 2x + 6$, then $\mathbb{Z}[\alpha]$ is an order in the number field $\mathbb{Q}(\alpha)$. The ideal $I = (2, \alpha)$ of $\mathbb{Z}[\alpha]$ is generated by 2 and α. Therefore, any element of I can be written as a $\mathbb{Z}[\alpha]$-linear combination of 2 and α.

Another example would be to take the order $\mathbb{Z}[\sqrt{3}, \sqrt{5}]$ of the number field $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ with the ideal $I = (4, 1 + \sqrt{3}, 2 + \sqrt{5}, 3 + \sqrt{15})$.

We see that ideals are actually sets and not numbers. In our previous integer-only world the number 1 divided every other number. One might question whether such an ideal exists for number rings as well. The answer is that that ideal is not the zero ideal containing 1 element, but rather the ideal (1), which equals the whole number ring! In this new realm of ideals, the most trivial ideal we can think of is not the smallest, but rather the largest set. We say that an ideal I *divides* an ideal J if I contains J. In other words, the larger set acts as the divisor. Now, consider the ring $R = \mathbb{Z}$. The ideal (2) of R comprises all even numbers. Notably, (2) divides (4), consisting of all numbers divisible by 4. We also have that the ideal (1), which is equal to $\mathbb{Z}$, contains the even numbers and thus (1) divides (2) which in turn divides (4).

Also, for the remainder of this section, we let R denote a commutative ring.

Definition 2.11. Abstractly, the addition of two ideals I and J of R is defined as $I+J = \{i+j : i \in I, j \in J\}$. Multiplication of two ideals is defined as $IJ = \{\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J, n \in \mathbb{Z}_{\geq 0}\}$, note that the sum is introduced in this product as an ideal must still be closed under addition (since it is defined as an additive subgroup of R).

Theorem 2.12. *If I and J are both ideals in R then so are the sum $I + J$ and the product IJ.*

Proof. See [24, Lemma 2.3] and [18, Prop. 2.4]. □

The ideal I divides $I + I$ as I contains the smaller set $I + I = \{i + i : i \in I\}$.

Define the ring $R = \mathbb{Z}[\sqrt{15}]$ with ideals $I = (2, 1 + \sqrt{15})$, $J = (2)$, and $L = (1 + \sqrt{15})$.

$$\begin{aligned} I &= \{2a + 2b\sqrt{15} : a, b \in \mathbb{Z}\} + \{(a + 15b) + (a + b)\sqrt{15} : a, b \in \mathbb{Z}\} \\ &= (2) + (1 + \sqrt{15}) = J + L. \end{aligned}$$

The product JL is the ideal $(2 + 2\sqrt{15})$. Note that JL is a smaller set than J and since J contains JL we have that J divides JL, similarly L divides JL.

Definition 2.13. An ideal is called *principal* if it can be generated by a single element of R (meaning that it equals an ideal of the form (r) with $r \in R$). If an ideal cannot be generated by only one generator, it is called *non-principal*. We call R a *principal ideal domain* if every ideal of R is principal.

Let $R = \mathbb{Z}[\sqrt{15}]$, the ideal $I = (2, 1+\sqrt{15})$ is non-principal (as we will see in the following example), whereas

$$\begin{aligned} I^2 &= ((2) + (1+\sqrt{15}))^2 = (4, 2+2\sqrt{15}, 2+2\sqrt{15}, 16+2\sqrt{15}) \\ &= (4, 2+2\sqrt{15}, 14) = (4, 2+2\sqrt{15}, 2) = (2) \end{aligned}$$

is principal. Note that in the equation above one must be careful that all the elements of an ideal are still contained in the next ideal and no additional elements are introduced, also, the second equality comes from the distributive law of multiplication of ideals over addition of ideals [18, p. 15].

Definition 2.14. An ideal $I \neq (1)$ of a number ring R is called a *prime ideal* if for any $a, b \in R$ with $ab \in I$, we have that $a \in I$ or $b \in I$.

Similar to how we can factor numbers into products of prime numbers, ideals can also be decomposed into products of prime ideals. We elaborate on this concept in Section 2.5.

2.3 Norm and Trace

Let K be a field and let L be a finite extension of degree n of K (we will use this notation throughout the section). We can choose a basis $\{b_1, b_2, \ldots, b_n\} \in L$ such that L is constructed from K by taking K-linear combinations of that basis. In other words, if $\{b_1, b_2, \ldots, b_n\}$ is a K-basis for L, then $L = \{x_1 b_1 + x_2 b_2 + \cdots + x_n b_n : x_i \in K\}$.

Let $\alpha \in L$ and let V be the vector space spanned by the basis $\{b_1, b_2, \ldots, b_n\}$. Let $m_\alpha : V \to V$ denote multiplication by α. Thus, for any basis element $b_j \in V$ we have $m_\alpha(b_j) = \alpha b_j = \sum_{i=1}^{n} a_{ij} b_i$ for some coefficients $a_{ij} \in K$. We can thus define a matrix, denoted as $[m_\alpha]$, enlisting the coefficients a_{ij}. The following examples compute this matrix for a couple of number fields.

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$ and choose the basis $\{1, \sqrt{2}\}$. Furthermore, let $\alpha = a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$, now we calculate αb_i for all b_i in the chosen basis.

$$\left.\begin{aligned} \alpha \cdot 1 &= a + b\sqrt{2} \\ \alpha \cdot \sqrt{2} &= 2b + a\sqrt{2} \end{aligned}\right\} \implies [m_\alpha] = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}.$$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\gamma)$ where γ is a root of the irreducible polynomial $x^2 + 2x + 6$. Select the basis $\{1, \gamma\}$, note that this is indeed a basis by Definition 2.4. Since γ is a root of $x^2 + 2x + 6$ we have $\gamma^2 + 2\gamma + 6 = 0$ and thus $\gamma^2 = -2\gamma - 6$. Choosing $\alpha = a + b\gamma$ with $a, b \in \mathbb{Q}$, gives that

$$\left.\begin{aligned} \alpha \cdot 1 &= a + b\gamma \\ \alpha \cdot \gamma &= -6b + (a - 2b)\gamma \end{aligned}\right\} \implies [m_\alpha] = \begin{bmatrix} a & -6b \\ b & a - 2b \end{bmatrix}.$$

Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{3}, \sqrt{-5})$. One can verify that $\{1, \sqrt{3}, \sqrt{-5}, \sqrt{-15}\}$ is a K-basis for L. Let $\alpha = a + b\sqrt{3} + c\sqrt{-5} + d\sqrt{-15}$ for $a, b, c, d \in \mathbb{Q}$, we get

$$\left.\begin{aligned} \alpha \cdot 1 &= a + b\sqrt{3} + c\sqrt{-5} + d\sqrt{-15} \\ \alpha \cdot \sqrt{3} &= 3b + a\sqrt{3} + 3d\sqrt{-5} + c\sqrt{-15} \\ \alpha \cdot \sqrt{-5} &= -5c - 5d\sqrt{3} + a\sqrt{-5} + b\sqrt{-15} \\ \alpha \cdot \sqrt{-15} &= -15d - 5c\sqrt{3} + 3b\sqrt{-5} + a\sqrt{-15} \end{aligned}\right\} \implies [m_\alpha] = \begin{bmatrix} a & 3b & -5c & -15d \\ b & a & -5d & -5c \\ c & 3d & a & 3b \\ d & c & b & a \end{bmatrix}.$$

More examples are listed in [25, Ex. 2.3-2.6].

These multiplication matrices come in handy for computations in our fields L and K. To this end, we define the norm, trace, characteristic polynomial, and discriminant. We note that these definitions are independent of the choice of the basis $\{b_1, b_2, \ldots, b_n\}$ [18, § 4] [26].

Definition 2.15. The *norm* and the *trace* from L to K are, respectively, are the maps $\mathrm{N}_{L/K} : L \to K$ and $\mathrm{Tr}_{L/K} : L \to K$ defined by

$$\mathrm{N}_{L/K}(x) = \det\,[m_x] \quad \text{and} \quad \mathrm{Tr}_{L/K}(x) = \mathrm{trace}\,[m_x].$$

Similarly, if $\{b_1, b_2, \ldots, b_n\}$ is a $\mathbb{Z}$-basis for the order R in a number field L and $K = \mathbb{Q}$, we can define the *restricted norm* and *restricted trace* as maps $\mathrm{N}_{R/\mathbb{Z}} : R \to \mathbb{Z}$ and $\mathrm{Tr}_{R/\mathbb{Z}} : R \to \mathbb{Z}$ defined by

$$\mathrm{N}_{R/\mathbb{Z}}(x) = \det\,[m_x] \quad \text{and} \quad \mathrm{Tr}_{R/\mathbb{Z}}(x) = \mathrm{trace}\,[m_x].$$

Remark. It can be seen that the codomain of the norm and trace indeed lie in K by [27] or [26, Proposition 2.8] in combination with [26, Proposition 2.3].

Definition 2.16. The *characteristic polynomial* $f^x_{L/K} \in K[X]$ of $x \in L$ is the characteristic polynomial of $[m_x]$, given by

$$f^x_{L/K}(X) = \det(X \cdot \mathrm{id}_L - [m_x]).$$

Moreover, every $x \in L$ is a root of its characteristic polynomial $f^x_{L/K}$ [25, Theorem 5.6].

Definition 2.17. Let $\{b_1, b_2, \ldots, b_n\}$ be any $\mathbb{Z}$-basis for the order R of a number field. The *discriminant* of R is defined as

$$\Delta(R) = \det(\mathrm{Tr}_{R/\mathbb{Z}}(b_i b_j))_{i,j=1}^n.$$

We define the discriminant of a number field K as $\Delta_K := \Delta(\mathcal{O}_K)$.

Continuing the examples from before we deduce that if $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$, then $\mathrm{Tr}_{L/K}(\alpha) = 2a$ and $\mathrm{N}_{L/K}(\alpha) = a^2 - 2b^2$. Meaning that for $3 + 2\sqrt{2} \in L$ we have $\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(3 + 2\sqrt{2}) = 6$ and $\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(3 + 2\sqrt{2}) = 3^2 - 2 \cdot 2^2 = 1$.
The characteristic polynomial becomes

$$f^\alpha_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(X) = \det \begin{bmatrix} X - a & -2b \\ -b & X - a \end{bmatrix} = X^2 - 2aX + a^2 - 2b^2.$$

Thus, we have $f^{\sqrt{2}}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(X) = X^2 - 2$ and indeed $\sqrt{2}$ is a root of $X^2 - 2$. On a different note $f^{1+\sqrt{2}}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(X) = X^2 - 2X - 1$. We can rewrite $X^2 - 2X - 1 = 0$ as $(X - 1)^2 = 2$, signifying that $1 + \sqrt{2}$ is a root of this characteristic polynomial.
Let $R = \mathbb{Z}[\sqrt{2}]$. The discriminant $\Delta(R)$ can be calculated as

$$\Delta(R) = \det \begin{bmatrix} \mathrm{Tr}_{\mathbb{Z}[\sqrt{2}]/\mathbb{Z}}(1) & \mathrm{Tr}_{\mathbb{Z}[\sqrt{2}]/\mathbb{Z}}(\sqrt{2}) \\ \mathrm{Tr}_{\mathbb{Z}[\sqrt{2}]/\mathbb{Z}}(\sqrt{2}) & \mathrm{Tr}_{\mathbb{Z}[\sqrt{2}]/\mathbb{Z}}(\sqrt{2} \cdot \sqrt{2}) \end{bmatrix} = \det \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix} = 8.$$

Had we taken the order $R' = \mathbb{Z}[2\sqrt{2}]$ in L, we would have found that, using the basis

$\{1, 2\sqrt{2}\}$, for any $a, b \in \mathbb{Z}$ we have $\mathrm{Tr}_{R'/\mathbb{Z}}(a + 2b\sqrt{2}) = 2a$. Therefore,

$$\Delta(R') = \det \begin{bmatrix} \mathrm{Tr}_{\mathbb{Z}[2\sqrt{2}]/\mathbb{Z}}(1) & \mathrm{Tr}_{\mathbb{Z}[2\sqrt{2}]/\mathbb{Z}}(2\sqrt{2}) \\ \mathrm{Tr}_{\mathbb{Z}[2\sqrt{2}]/\mathbb{Z}}(2\sqrt{2}) & \mathrm{Tr}_{\mathbb{Z}[2\sqrt{2}]/\mathbb{Z}}(8) \end{bmatrix} = \det \begin{bmatrix} 2 & 0 \\ 0 & 16 \end{bmatrix} = 32.$$

For $K = \mathbb{Q}$ and $L = \mathbb{Q}(\gamma)$ with γ a root of $x^2 + 2x + 6$ we have $\mathrm{Tr}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\alpha) = 2a - 2b$ and $\mathrm{N}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(\alpha) = a^2 - 2ab + 6b^2$.
The characteristic polynomial becomes

$$f^{\alpha}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(X) = \det \begin{bmatrix} X - a & 6b \\ -b & X - a + 2b \end{bmatrix} = X^2 - (2a - 2b)X + a^2 - 2ba + 6b^2$$

giving $f^{1+\gamma}_{\mathbb{Q}(\gamma)/\mathbb{Q}}(X) = X^2 + 5$ which has the two roots $\pm\sqrt{-5}$. The roots of $x^2 + 2x + 6$ are $-1 \pm \sqrt{-5}$, thus $1 + \gamma = \pm\sqrt{-5}$ is indeed satisfied.
Let $R = \mathbb{Z}[\gamma]$ and denote $\mathrm{Tr}_{\mathbb{Z}[\gamma]/\mathbb{Z}}(x)$ as $\mathrm{Tr}(x)$, then (remembering that $\gamma^2 = -6 - 2\gamma$)

$$\Delta(R) = \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\gamma) \\ \mathrm{Tr}(\gamma) & \mathrm{Tr}(-6 - 2\gamma) \end{bmatrix} = \det \begin{bmatrix} 2 & -2 \\ -2 & -8 \end{bmatrix} = -20.$$

Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{3}, \sqrt{-5})$, then $\mathrm{Tr}_{L/K}(\alpha) = 4a$ by the previous examples. Denote $\mathrm{Tr}_{\mathbb{Z}[\sqrt{3},\sqrt{-5}]/\mathbb{Z}}(x)$ as $\mathrm{Tr}(x)$, the discriminant of $R = \mathbb{Z}[\sqrt{3}, \sqrt{-5}]$ becomes

$$\begin{aligned} \Delta(R) &= \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{3}) & \mathrm{Tr}(\sqrt{-5}) & \mathrm{Tr}(\sqrt{-15}) \\ \mathrm{Tr}(\sqrt{3}) & \mathrm{Tr}(3) & \mathrm{Tr}(\sqrt{-15}) & \mathrm{Tr}(3\sqrt{-5}) \\ \mathrm{Tr}(\sqrt{-5}) & \mathrm{Tr}(\sqrt{-15}) & \mathrm{Tr}(-5) & \mathrm{Tr}(-5\sqrt{3}) \\ \mathrm{Tr}(\sqrt{-15}) & \mathrm{Tr}(3\sqrt{-5}) & \mathrm{Tr}(-5\sqrt{3}) & \mathrm{Tr}(-15) \end{bmatrix} \\ &= 4 \cdot 12 \cdot (-20) \cdot (-60) = 57600. \end{aligned}$$

Theorem 2.18. *Let K be a number field with extension L. The norm map $\mathrm{N}_{L/K} : L \to K$ is multiplicative and the trace map $\mathrm{Tr}_{L/K} : L \to K$ is additive. To put it differently, assume that α and β are elements of L, then $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha) \cdot \mathrm{N}_{L/K}(\beta)$ and $\mathrm{Tr}_{L/K}(\alpha + \beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$.*

Proof. Previously, we defined a way to construct the multiplication matrix $[m_\alpha]$ for some $\alpha \in L$. Using linear algebra, one can show that the determinant is multiplicative [28, Theorem 9.49] and that the trace is additive. Therefore

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha\beta) &= \det\left([m_{\alpha\beta}]\right) = \det\left([m_\alpha][m_\beta]\right) = \det\,[m_\alpha] \cdot \det\,[m_\beta] = \mathrm{N}_{L/K}(\alpha) \cdot \mathrm{N}_{L/K}(\beta), \\ \mathrm{Tr}_{L/K}(\alpha + \beta) &= \mathrm{trace}\left([m_{\alpha+\beta}]\right) = \mathrm{trace}\left([m_\alpha] + [m_\beta]\right) \\ &= \mathrm{trace}\,[m_\alpha] + \mathrm{trace}\,[m_\beta] = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta). \end{aligned}$$

□

Remark. One can also show that the restricted norm map is multiplicative and the restricted trace map is additive by letting K denote an order in a number field and defining $L = \mathbb{Z}$ in the above theorem.

Definition 2.19. For any non-zero ideal I of the order R of some number field K extending $\mathbb{Q}$, we define the *restricted norm* of I, denoted $\mathrm{N}_{R/\mathbb{Z}}(I)$, to be the ideal of $\mathbb{Z}$ equal to the set $\{\mathrm{N}_{R/\mathbb{Z}}(x) : x \in I\}$.

Take $R = \mathbb{Z}[\sqrt{15}]$ and $I = (2)$ as principal ideal in R. This ideal equals the set $\{2a+2b\sqrt{15} : a, b \in \mathbb{Z}\}$. The restricted norm of any element $\alpha = c + d\sqrt{15} \in R$ with $c, d \in \mathbb{Z}$ is $\mathrm{N}_{\mathbb{Z}[\sqrt{15}]/\mathbb{Z}}(\alpha) = c^2 - 15d^2$. Any element in the ideal, e.g., $2a + 2b\sqrt{15}$ with $a, b \in \mathbb{Z}$. will have restricted norm $\mathrm{N}_{\mathbb{Z}[\sqrt{15}]/\mathbb{Z}}(2a + 2b\sqrt{15}) = 4a^2 - 60b^2$. The restricted norm of the ideal will be $\mathrm{N}_{R/\mathbb{Z}}(I) = \mathrm{N}_{R/\mathbb{Z}}((2)) = \{\mathrm{N}_{R/\mathbb{Z}}(x) : x \in (2)\} = (4)$.
The non-principal ideal $J = (2, 1 + \sqrt{15})$ also has a restricted norm. This time the ideal (2) has restricted norm (4) and the ideal $(1 + \sqrt{15})$ has restricted norm (-14). Thus, the restricted norm of the ideal J will be generated by $(4, -14) = (2) \subset \mathbb{Z}$. If there is any ideal that divides J, its restricted norm must thus contain $(2) \subset \mathbb{Z}$.
Suppose now that J equals a principal ideal $(c + d\sqrt{15})$, equating restricted norms then gives us that $c^2 - 15d^2 = \pm 2$ must hold. Looking at the equation modulo 15 we see that such a solution does not exist, thus J is indeed non-principal.

Remark. Often the restricted norm of an ideal is said to just be the generator of the resulting ideal of $\mathbb{Z}$ (which must be a principal ideal) [29, Section I.8]. In the previous example this will mean that the ideal (2) is said to have restricted norm 4 and $(2, 1+\sqrt{15})$ is said to have restricted norm 2. This will also be done for the remainder of this thesis as it simplifies the statement of some theorems later on.

2.4 Units

A *unit* is an element u of a ring R such that an element $v \in R$ exists that satisfies $vu = uv = 1$ where 1 is the multiplicative identity of R. In the ring $\mathbb{Z}$ we had two units, namely ± 1. In number fields we can have an infinite number of units (see Theorem 2.20 below). An element u of an order R is called a *unit* if and only if $\mathrm{N}_{R/\mathbb{Z}}(u) = \{\pm 1\}$ [20, p. 16].

Let $a, b \in \mathbb{Z}$, then from previous examples we know that $\mathrm{N}_{\mathbb{Z}[\sqrt{2}]/\mathbb{Z}}(a+b\sqrt{2}) = a^2-2b^2$. Now, $3+2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is a unit since $(3+2\sqrt{2}) \cdot (3-2\sqrt{2}) = 1$. Indeed, $\mathrm{N}_{\mathbb{Z}[\sqrt{2}]/\mathbb{Z}}(3+2\sqrt{2}) = 1$. Likewise 1, -1, $3-2\sqrt{2}$, $7+5\sqrt{2}$, $1+\sqrt{2}$ are all units of $\mathbb{Z}[\sqrt{2}]$.

Remember from Definition 2.6 that the ring of integers $\mathcal{O}_K$ contains the roots of all monic polynomials in $\mathbb{Z}[x]$. That means that for every element $\alpha \in R$, where R is an order of (and thus contained in) $\mathcal{O}_K$, we have that there exists a non-zero monic polynomial in $\mathbb{Z}[x]$ with the root α. Such a polynomial with the least degree is called a *minimal polynomial* of α. Now, each polynomial $f \in \mathbb{Z}[x]$ is also a polynomial in $\mathbb{C}[x]$. Since $\mathbb{C}$ is algebraically closed (Section 1.4), we know that all roots of f will be contained in $\mathbb{C}$. Roots of $f \in \mathbb{C}[x]$ are either *real* or *complex*, depending on whether the root in question has an imaginary part.

Using this theory on minimal polynomials, we can state an important theorem regarding the *unit group* of R, the group containing all units in R.

Theorem 2.20 (Dirichlet unit theorem, 1846)**.** *Let $R = \mathbb{Z}[\alpha]$ be an order in a number field. Let the minimal polynomial of α admit r real roots and $2s$ complex roots. Write μ_R for the group of roots of unity in R, that is, all solutions to the equation $x^n = 1$ for some positive integer n and $x \in R$. Then μ_R is finite and the unit group of R can be written as*

$$R^\times = \mu_R \times \langle \eta_1 \rangle \times \langle \eta_2 \rangle \times \cdots \times \langle \eta_{r+s-1} \rangle \cong (\mathbb{Z}/\#\mu_R\mathbb{Z}) \times \mathbb{Z}^{r+s-1}.$$

Where $\eta_1, \eta_2, \ldots, \eta_{r+s-1}$ are called fundamental units*, forming a $\mathbb{Z}$-basis for $R^\times/\mu_R$.*

Proof. See [30] or [31, Section 6.2]. □

The case of imaginary quadratic number fields is of special interest in the CSIDH algorithm. Specifically, orders of the form $R = \mathbb{Z}[\sqrt{-p}]$ for primes p are of interest. As $\sqrt{-p}$ is a root of the monic polynomial $x^2 + p \in \mathbb{Z}[x]$, and this polynomial has the least possible degree (as constant polynomials and monic polynomials of degree 1 will never have $\sqrt{-p}$ as a root), we find that $x^2 + p$ is the minimal polynomial of $\sqrt{-p}$. Since $\pm\sqrt{-p}$ are all the roots of the polynomial $x^2 + p \in \mathbb{C}[x]$, both having an imaginary part, we find that $r = 0$ and $s = 1$ in the Dirichlet unit theorem. Therefore, $R^\times = \mu_R \cong \mathbb{Z}/\#\mu_R\mathbb{Z}$, implying that the unit group of R is finite.

The two fundamental units of $\mathbb{Z}[\sqrt{2}]$ are -1 and $1 + \sqrt{2}$.
Let $R = \mathbb{Z}[\sqrt{2}]$ be an order in $\mathbb{Q}(\sqrt{2})$. The minimal polynomial of $\sqrt{2}$ is $x^2 - 2 \in \mathbb{Z}[x]$, which admits 2 real roots and 0 complex roots. Using the Dirichlet unit theorem, we find that $R^\times = \mu_R \times \langle \eta_1 \rangle$ as $r + s - 1 = 2 + 0 - 1 = 1$.
In fact, $\mu_R = \{\pm 1\}$ and $\eta_1 = 1 + \sqrt{2}$. Therefore, all units of R are generated by $\langle -1 \rangle \times \langle 1 + \sqrt{2} \rangle$, that is, they are of the form $\pm(1 + \sqrt{2})^k$ for some $k \in \mathbb{Z}$.
If we rewrite the equation $x^2 - 2y^2 = \pm 1$ in R, we get that $(x - \sqrt{2}y)(x + \sqrt{2}y) = \pm 1$, so that $x - \sqrt{2}y$ and $x + \sqrt{2}y$ must have restricted norms equal to ± 1. As all units have restricted norms equal to ± 1, and are of the form $\pm(1 + \sqrt{2})^k$ we find the units

$$(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}, \qquad (1 + \sqrt{2})^3 = 7 + 5\sqrt{2}, \qquad (1 + \sqrt{2})^4 = 17 + 12\sqrt{2}.$$

Now, these units give the integer solutions $(x, y) \in \{(1, 1), (3, 2), (7, 5), (17, 12)\}$ of the equation $x^2 - 2y^2 = \pm 1$.

Take $R = \mathbb{Z}[\sqrt{7}]$, then $\mu_R = \{\pm 1\}$ are the roots of unity in R. Since the minimal polynomial of $\sqrt{7}$ is $x^2 - 7$, we find that $r = 2$ and $s = 0$, using the notation of Theorem 2.20. Hence, the unit group has the form $R^\times = \langle -1 \rangle \times \langle \eta \rangle$ for some fundamental unit η. For example, $\eta = 8 - 3\sqrt{7} \in R$ is a fundamental unit.

The order $R = \mathbb{Z}[\sqrt{-1}]$ has $\mu_R = \{\pm 1, \pm\sqrt{-1}\}$ as $\pm\sqrt{-1} \in R$ are roots of $x^4 - 1$. Moreover, the minimal polynomial of $\sqrt{-1}$ is $x^2 + 1$, and admits 0 real roots and 2 complex roots. Thus, $R^\times \cong \mathbb{Z}/4\mathbb{Z}$.

Units can be verified to be fundamental if the unit is not equal to an nth power of a different unit where n is a positive integer.

We want to show that $1 + \sqrt{2}$ is a fundamental unit in $\mathbb{Z}[\sqrt{2}]$. Note that we indeed have $\mathrm{N}_{\mathbb{Z}[\sqrt{2}]/\mathbb{Z}}(1 + \sqrt{2}) = -1$. In order to show that the unit $1 + \sqrt{2}$ is fundamental we first assume it is not fundamental. Thus, there exists a unit $t = u + v\sqrt{2}$ and $k \in \mathbb{Z}_{>1}$ such that $1 + \sqrt{2} = t^k$, thus $t^k \approx 2.41$. As the restricted norm of $1 + \sqrt{2}$ is -1, we have that k cannot be even. Therefore, k must be odd and t must have restricted norm equal to -1. Since $t^k > 1$ and $k > 1$ we know that $1 < t < \sqrt{2.41} \approx 1.55$ must hold. We can immediately see that $u, v < 0$ implies that $t < 0$, and thus gives no solutions. In the case that $u > 0$ and $v < 0$ we deduce, from the fact that t is a unit, that $\pm 1 = (u + v\sqrt{2})(u - v\sqrt{2}) = t(u - v\sqrt{2})$. Naturally $u - v\sqrt{2} > t$ as v is negative, so that we reach a contradiction to the equality. Similarly, if $u < 0$ and $v > 0$ we have $t(u - v\sqrt{2}) = \pm 1$, we have $u - v\sqrt{2} < -1$, and since $t > 1$ we again reach a contradiction. Also, if $v = 0$, then t^k would always be an integer and never equal $1 + \sqrt{2}$. Similarly, if $u = 0$, then t^k would either be integral or of the form $x\sqrt{2}$ for some $x \in \mathbb{Z}$, which also never equals $1 + \sqrt{2}$. Therefore, $u, v > 0$ holds. Since $u, v > 0$ and we require $t < 1.55$ such a t does not exist as $t = u + v\sqrt{2} \geq 1 + \sqrt{2} \approx 2.41 \not< 1.55$.

Therefore, the unit $1+\sqrt{2}$ is fundamental and $\mathbb{Z}[\sqrt{2}]^\times = \langle -1 \rangle \times \langle 1+\sqrt{2} \rangle$.

2.5 Ramification and Factorisation

Before we can introduce the subject of ideal factorisation, we need to look at the definition of invertible ideals.

Definition 2.21. An ideal I of an order R is called *invertible* if there exists an ideal J of R such that $I \cdot J$ is a non-zero principal ideal [18, p. 17]. The *regular* prime ideals (Definition 2.14) of R are the primes ideals of R that are invertible; if a prime ideal is not invertible it is called *singular*. A *Dedekind domain* is a number ring in which all ideals are invertible. The smallest extension of $\mathbb{Z}$ that is a Dedekind domain in any number field K is $\mathcal{O}_K$, the *ring of integers* of K [18, Theorem 3.20].

Finding the ring of integers of some number field can be a difficult process. Often a guess is made for $\mathcal{O}_K$ and if there are singular primes left in this domain, then we know that our choice of $\mathcal{O}_K$ was not correct, as $\mathcal{O}_K$ is Dedekind and all ideals must be invertible. Before we look at a few examples there is another important theorem that will help with our understanding of this concept later on.

Theorem 2.22 (Kummer-Dedekind)**.** *Let p be a prime number and let α be a root of a monic irreducible polynomial $f := \sum_{i=1}^{m} c_i x^i \in \mathbb{Z}[x]$ of degree m. First, find the residue classes of the coefficients of f modulo p, to create the polynomial $f' := \sum_{i=1}^{m} (c_i \bmod p) x^i \in \mathbb{F}_p[x]$. Next, factor the polynomial f' into pairwise distinct monic irreducible polynomials $g_1, \ldots, g_n \in \mathbb{F}_p[x]$ with multiplicities $e_1, \ldots, e_n \in \mathbb{Z}_{\geq 1}$, i.e., we are able to write that $f'(x) = g_1(x)^{e_1} \cdots g_n(x)^{e_n}$. Then, for each g_i, take the coefficients of g_i and take some element in the residue class of the coefficient to create a polynomial $g_i' \in \mathbb{Z}[x]$.*

Now, the ideal (p) in the order $R := \mathbb{Z}[\alpha]$ factors into prime ideals as $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ satisfying $\mathfrak{p}_i = (p, g_i'(\alpha))$ and $\mathrm{N}_{R/\mathbb{Z}}(\mathfrak{p}_i) = p^{\deg g_i} = p^{\deg g_i'}$. Also, denote $r_i \in \mathbb{Z}[x]$ to be the remainder of $f \in \mathbb{Z}[x]$ upon division by $g_i' \in \mathbb{Z}[x]$, after writing $q := p \in \mathbb{Z}[x]$ (viewing p as a constant polynomial with integer coefficients), we can state that

$$\mathfrak{p}_i \text{ is singular } \iff e_i > 1 \text{ and } q^2 \text{ divides } r_i \in \mathbb{Z}[x].$$

Proof. See [32] or [18, Theorem 3.1]. □

Corollary 2.23. *Suppose that $\mathfrak{p}_i$ is singular in the Kummer-Dedekind theorem and that the quotient and remainder of the division of f by g_i' equal q and r, respectively, i.e., we can write $f = q \cdot g_i' + r$. Then $\frac{1}{p} q(\alpha)$ is the root of a monic polynomial in $\mathbb{Z}[x]$, but does not lie in $\mathbb{Z}[\alpha]$, that is, it extends $\mathbb{Z}[\alpha]$.*

Proof. See [18, Theorems 3.1, 3.2]. □

Remark. In the next example we will see that the ideal (7) factors in $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ as $(7, \sqrt{2}+3)(7, \sqrt{2}+4)$. To make our notation more compact, we write $(7, \sqrt{2}+3)(7, \sqrt{2}+4) = \mathfrak{p}_7 \cdot \mathfrak{q}_7$ to mean that $\mathfrak{p}_7 := (7, \sqrt{2}+3)$ and $\mathfrak{q}_7 := (7, \sqrt{2}+4)$. We will continue to do this in the rest of our thesis to assign letters to our ideals. Also, we note that this assignment of letters for the ideals will always be in respective order.

Take K to be the number field $\mathbb{Q}(\sqrt{2})$. In a previous example, we found that the characteristic polynomial of $\sqrt{2}$ equals $f := x^2 - 2$ which seems logical as $\sqrt{2}$ is a root of this polynomial. Now, we make the guess that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ (it is in fact true that $\mathbb{Z}[\sqrt{2}]$

equals $\mathcal{O}_K$).
The ideal (7) factors in $\mathcal{O}_K$ as $(7, \sqrt{2}+3)(7, \sqrt{2}+4) = \mathfrak{p}_7 \cdot \mathfrak{q}_7$. Since in $\mathbb{F}_7[x]$ we have $x^2 - 2 = (x+3)(x+4)$.
The ideal (17) factors in $\mathcal{O}_K$ as $(17, \sqrt{2}+6)(17, \sqrt{2}+11) = \mathfrak{p}_{17} \cdot \mathfrak{q}_{17}$. Since in $\mathbb{F}_{17}[x]$ we have $x^2 - 2 = (x+6)(x+11)$.
The ideal (5) does not factorise in $\mathcal{O}_K$ as $x^2 - 2$ is irreducible in $\mathbb{F}_5[x]$, in other words, (5) is a prime ideal. The same goes for (3), (11), (13), and others.

Let K be the number field $\mathbb{Q}(\sqrt{5})$. The characteristic polynomial of $\sqrt{5}$ is $f = x^2 - 5$. Assume that $\mathcal{O}_K = \mathbb{Z}[\sqrt{5}]$. The ideal (2) factors in $\mathcal{O}_K$ as $(2, 1+\sqrt{5})^2 = \mathfrak{p}_2^2$ since $x^2 - 5 = (x+1)^2$ in $\mathbb{F}_2[x]$. The remainder $r_i \in \mathbb{Z}[x]$ of f upon division by $g_i' = x + 1$ can be seen from

$$\frac{x^2 - 5}{x+1} = x + \frac{-5 - x}{x+1} = x - 1 + \frac{4}{x+1}$$

to be equal to the constant polynomial 4. But $q^2 := p^2 = 2^2 = 4 \in \mathbb{Z}[x]$ divides $r_i \in \mathbb{Z}[x]$, thus $\mathfrak{p}_2$ is singular.
We find that $f = (x-1)g_i' + 4$, thus, using Corollary 2.23, we get that $\frac{1}{2}(\sqrt{5} - 1)$ does not lie in $\mathcal{O}_K = \mathbb{Z}[\sqrt{5}]$. We conclude that our original guess for $\mathcal{O}_K$ was insufficient as it did not include $\frac{\sqrt{5}-1}{2} \in \mathbb{Q}(\sqrt{5})$, which is a root of the monic polynomial $x^2 + x - 1 \in \mathbb{Z}[x]$. As, $\mathbb{Z}[\frac{\sqrt{5}-1}{2}]$ contains $\mathbb{Z}[\sqrt{5}]$, we now assume that $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{5}-1}{2}]$ (in fact, this is indeed the ring of integers of K).
Let α denote $\frac{\sqrt{5}-1}{2}$, the characteristic polynomial of α is $f := x^2 + x - 1$. Now, (5) factors in $\mathcal{O}_K$ as $(5, \alpha + 2)^2 = \mathfrak{p}_5^2$ as in $\mathbb{F}_5[x]$ we have $x^2 + x - 1 = (x+3)^2$. The remainder of f upon division by $x + 3$ is 5, so that $\mathfrak{p}_5$ is a regular ideal of $\mathcal{O}_K$.
The ideal (2) does not factor in $\mathcal{O}_K$ as $x^2 + x - 1$ is irreducible in $\mathbb{F}_2[x]$.

Other useful references for the Kummer-Dedekind theorem and its application are [33] and [18, § 3, § 7].

Definition 2.24. Let p be a prime number and let (p) be an ideal of the order R that factors as the product $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$ of prime ideals, using the conventions of Theorem 2.22. We distinguish two cases.

- The order R is called *singular above* p if one of $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ is singular in R.
- The order R is called *regular above* p if all prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are regular in R. We distinguish a few more cases if R is regular above p.
  - If $n = 1$ and $e_1 = 1$, i.e., (p) itself is a prime ideal, we say that p is *inert* in R.
  - If some $e_i > 1$, we say that p is *ramified* in R, moreover, if $n = 1$ also holds, then p is said to be *totally ramified* in R.
  - If $n > 1$, then p is said to be *split* in R (note that p can be both split and ramified in R). Moreover, if all $e_i = 1$, then p is said to be *totally split* in R.

In the above examples we saw that $\mathbb{Z}[\sqrt{5}]$ was singular above 2 as the ideal $\mathfrak{p}_2$ was singular. However, the order $R := \mathbb{Z}[\frac{\sqrt{5}-1}{2}]$ was regular above 2. Since the ideal (2) could not be factored in R, we say that 2 is inert in R. Also, 5 is ramified in R as it factored into a prime ideal with multiplicity greater than one.

Theorem 2.25. *A prime p ramifies in the ring of integers, $\mathcal{O}_K$, of a number field K if and only if p divides Δ_K. Any order R of the number field K can only be singular above some prime p if p^2 divides $\Delta(R)$. Also, Δ_K divides $\Delta(R)$.*

Proof. See [18, Theorem 4.14] for the first statement, the second and third statement follow from [18, Theorems 4.7, 4.10]. □

Take $R = \mathbb{Z}[\sqrt{5}]$, then we can calculate that $\Delta(R) = 20$, meaning that the primes 2 and 5 are ramified in R. From the previous example, we know that R is singular above 2, so we defined $R' = \mathbb{Z}[\frac{\sqrt{5}-1}{2}]$. We can calculate that $\Delta(R') = 5$, meaning that only 5 is ramified in R'.
Also, since $\Delta(R') = 5$, there will be no prime p such that p^2 divides 5. So R' is not singular above any prime, meaning that $\mathcal{O}_K = R'$.

Let $R = \mathbb{Z}[\sqrt{2}]$, we found in previous examples that $\Delta(R) = 8$, implying that only 2 is ramified in R. The ideal (2) factors in R as $(2, \sqrt{2})^2 = (\sqrt{2})^2 = \mathfrak{p}_2^2$ as $x^2 - 2 = x^2$ in $\mathbb{F}_2[x]$. If we divide the characteristic polynomial $x^2 - 2$ by x we get a remainder of -2. Since $2^2 = 4$ does not divide -2, Theorem 2.22 implies that $\mathfrak{p}_2$ is regular. Thus, R is regular above 2 and 2 is ramified in R. Since only 2 is ramified in R, and it is regular in R we know that there are no singular primes in R and thus $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = R = \mathbb{Z}[\sqrt{2}]$.

2.6 Class Groups

Definition 2.26. Let R be a Dedekind domain in a number field K, define a relation $\sim$ on non-zero ideals of R by $I \sim J$ whenever there exist non-zero elements $a, b \in R$ such that $(a)I = (b)J$ where (a) and (b) constitute the ideals generated by a and b. In fact, this relation is an equivalence relation [34] and the equivalence classes are called *ideal classes* of R, denoted as $[L]$ for L an arbitrary ideal of R. We define the addition of $[I]$ and $[J]$ to be the ideal class $[IJ]$ (writing that $[I] + [J] = [IJ]$). In fact, the set of all ideal classes is called the *class group* of R, denoted $\mathrm{Cl}(R)$, and as the name suggests, it forms a group under this addition operation [20, Corollary 1]. Moreover, the class group of the ring of integers $\mathcal{O}_K$ is denoted as $\mathrm{Cl}(K)$. The ideal class containing all principal ideals of R forms the identity element of the class group, thus, if IJ is a principal ideal we write $[I] + [J] = 0$. If all ideals in R are principal, the class group $\mathrm{Cl}(R)$ is trivial, and R is called a *principal ideal domain*.

Theorem 2.27 (Minkowski bound)**.** *Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$ be the ring of integers in a number field K such that $[K : \mathbb{Q}] = n$, where α is the root of some monic irreducible polynomial $f \in \mathbb{Z}[x]$ of degree n. Let f (as a polynomial of $\mathbb{C}[x]$) admit a total of $2s$ complex roots. Then every ideal class contains an ideal of restricted norm not exceeding*

$$M_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} \cdot \sqrt{|\Delta_K|}.$$

In particular, the class group $\mathrm{Cl}(K)$ is generated by the ideal classes of prime ideals of restricted norm at most M_K.

Proof. See [18, Theorem 5.9]. □

Let $K = \mathbb{Q}(\sqrt{-5})$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $\Delta_K = -20$ as well as 2 complex roots and 0 real roots of the minimal polynomial $x^2 + 5$ of $\sqrt{-5}$. This implies that $M_K =$

$\frac{4}{\pi}\frac{2}{4}\sqrt{20} \approx 2.847$. Hence, the class group $\mathrm{Cl}(K)$ is generated by ideal classes of prime ideals of restricted norm at most 2. The ideal (2) factors in $\mathcal{O}_K$ as $(2, 1+\sqrt{-5})^2 = \mathfrak{p}_2^2$, since $x^2+5 = (x+1)^2$ in $\mathbb{F}_2[x]$.
Since $\mathrm{Cl}(K)$ is generated by the ideal class of $\mathfrak{p}_2$, in order to prove that the class group of $\mathcal{O}_K$ has order 2 (since $\mathfrak{p}_2^2$ is principal the class group has order dividing 2) we must show that $[\mathfrak{p}_2] \neq 0$, i.e., that $\mathfrak{p}_2$ is non-principal in $\mathcal{O}_K$.
Suppose that $\mathfrak{p}_2 = (a+b\sqrt{-5})$ with $a, b \in \mathbb{Z}$. Since $\mathfrak{p}_2$ has restricted norm 2 (Theorem 2.22), and we know that $\mathrm{N}_{\mathbb{Z}[\sqrt{-5}]/\mathbb{Z}}(a+b\sqrt{-5}) = a^2+5b^2$, we need to solve the equation $a^2+5b^2 = 2$, which has no solutions, resulting in a contradiction. Thus, $\mathfrak{p}_2$ is non-principal and the class group of K has order 2.

Take $K = \mathbb{Q}(\sqrt{130})$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{130}]$ and $\Delta_K = 520$. The minimal polynomial of $\sqrt{130}$, which is x^2-130, has 2 real roots and 0 complex roots. Therefore, $M_K = \frac{2}{4}\sqrt{520} \approx 11.40$, implying that $\mathrm{Cl}(R)$ is generated by the ideal classes of prime ideals of restricted norm at most 11. We start by factoring some ideals in $\mathcal{O}_K$

$$\begin{aligned}
(2) &= (2, \sqrt{130})^2 = \mathfrak{p}_2^2,\\
(3) &= (3, 1+\sqrt{130})(3, 2+\sqrt{130}) = \mathfrak{p}_3\mathfrak{q}_3,\\
(5) &= (5, \sqrt{130})^2 = \mathfrak{p}_5^2,\\
(7) &= (7, 2+\sqrt{130})(7, 5+\sqrt{130}) = \mathfrak{p}_7\mathfrak{q}_7,\\
(11) &= (11, 3+\sqrt{130})(11, 8+\sqrt{130}) = \mathfrak{p}_{11}\mathfrak{q}_{11}.
\end{aligned}$$

This implies that $2[\mathfrak{p}_2] = 0$, $[\mathfrak{p}_3] + [\mathfrak{q}_3] = 0$, $2[\mathfrak{p}_5] = 0$, $[\mathfrak{p}_7] + [\mathfrak{q}_7] = 0$, and $[\mathfrak{p}_{11}] + [\mathfrak{q}_{11}] = 0$. Now, for $k \in \mathbb{Z}$ we have that $\mathrm{N}_{\mathbb{Z}[\sqrt{130}]/\mathbb{Z}}(k-\sqrt{130}) = k^2-130$. Therefore, the ideal $(11-\sqrt{130})$ has restricted norm -9. From Theorem 2.22 we know that $\mathrm{N}_{\mathbb{Z}[\sqrt{130}]/\mathbb{Z}}(\mathfrak{p}_3) = 3$. As the restricted norm is multiplicative, and units are the only elements of an order with restricted norm equal to ± 1, we know that $(u)\mathfrak{p}_3^2 = (v)(11-\sqrt{130})$, where u and v are units in $\mathcal{O}_K$. Hence, $\mathfrak{p}_3^2$ and $(11-\sqrt{130})$ are in the same ideal class. We write $2[\mathfrak{p}_3] = 0$. Also, $(12-\sqrt{130})$ has restricted norm 14, without loss of generality, factor it as $\mathfrak{p}_2\mathfrak{p}_7$. Then, $[\mathfrak{p}_2] + [\mathfrak{p}_7] = 0$. The class group is thus generated by (the ideal classes of) $\{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5, \mathfrak{p}_{11}\}$. Factoring $(14-\sqrt{130})$ as $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_{11}$ (without loss of generality) gives $[\mathfrak{p}_2] + [\mathfrak{p}_3] + [\mathfrak{p}_{11}] = 0$, implying that the class group is also generated by $\{\mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_5\}$ (as $[\mathfrak{p}_{11}]$ is generated by $[\mathfrak{p}_2]$ and $[\mathfrak{p}_3]$). Additionally, we factor $(5-\sqrt{130})$ as $\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_7$, implying that $[\mathfrak{p}_3] + [\mathfrak{p}_5] = -[\mathfrak{p}_7] = [\mathfrak{p}_2]$ meaning that the class group is generated by $\{\mathfrak{p}_3, \mathfrak{p}_5\}$.
We know that $2[\mathfrak{p}_3] = 0$ and that $2[\mathfrak{p}_5] = 0$. In order to show that the class group $\mathrm{Cl}(K) = \langle[\mathfrak{p}_3]\rangle \times \langle[\mathfrak{p}_5]\rangle \equiv (\mathbb{Z}/2\mathbb{Z})^2$ we need to show that both $\mathfrak{p}_3$ and $\mathfrak{p}_5$ are non-principal and that $[\mathfrak{p}_3] \neq [\mathfrak{p}_5]$.
For some principal ideal $(a+b\sqrt{130})$ with $a, b \in \mathbb{Z}$ we have that $\mathrm{N}_{\mathbb{Z}[\sqrt{130}]/\mathbb{Z}}(a+b\sqrt{130}) = a^2-130b^2$. If $\mathfrak{p}_3$ is principal we must thus have $a^2-130b^2 = 3$ for some $a, b \in \mathbb{Z}$. Looking at the equation modulo 130 we see that we must have $a^2 \equiv 3 \pmod{130}$. But 3 is not a quadratic residue (see Definition 5.1 if the term is unfamiliar) modulo 130, thus $\mathfrak{p}_3$ is non-principal. Since 5 is also not a quadratic residue modulo 130 we also know that $\mathfrak{p}_5$ is non-principal.
If $[\mathfrak{p}_3] = [\mathfrak{p}_5]$ we have $0 = 2[\mathfrak{p}_3] = [\mathfrak{p}_3\mathfrak{p}_5]$, meaning that $\mathfrak{p}_3\mathfrak{p}_5$ is principal. But $15 = a^2-130b^2 \equiv a^2 \pmod{130}$ is not a quadratic residue, meaning that $[\mathfrak{p}_3] \neq [\mathfrak{p}_5]$. We conclude that $\mathrm{Cl}(K) = \langle[\mathfrak{p}_3]\rangle \times \langle[\mathfrak{p}_5]\rangle \equiv (\mathbb{Z}/2\mathbb{Z})^2$.

Many more examples are listed in [35, Ex. 2.1-2.6, 3.1–3.4].

2.7 Overarching Example

As an example combining the theory of ideals and numbers fields we will compute all integer solutions to the equation $x^2 - 109y^2 = 1$. Other such examples are listed in [18, § 7].

To this end, we define the number field $K = \mathbb{Q}(\sqrt{109})$, now, solutions to the equation amount to finding solutions to

$$(x - \sqrt{109}y)(x + \sqrt{109}y) = 1.$$

We see that both parts in brackets must be represented by some element in the unit group of the ring of integers of our number field, that is, they must be an element of $\mathcal{O}_K^\times$. We proceed by computing $\mathcal{O}_K^\times$, to which end we first find $\mathcal{O}_K$.

Take $R = \mathbb{Z}[\sqrt{109}]$, using Section 2.3 we find that the characteristic polynomial of $\sqrt{109}$ is $x^2 - 109$. Section 2.5 now tells us that the ideal (2) factors in R as $(2, 1 - \sqrt{109})^2 = \mathfrak{p}_2^2$. Furthermore, the remainder of $x^2 - 109$ upon division by $x - 1$ is $-108 \in \mathbb{Z}[x]$, sadly $2^2 = 4$ divides -108, thus R is not equal to the ring of integers $\mathcal{O}_K$ by Theorem 2.22. We extend R by using Corollary 2.23 and the fact that $x^2 - 109 = (x - 1)(x + 1) - 108$, giving that the element $\frac{1}{2}(\sqrt{109} + 1)$ extends the order R.

Now, let $\alpha = \frac{\sqrt{109}+1}{2}$ and let $S = \mathbb{Z}[\alpha]$, we know that $R \subset S$ so S indeed extends R. Define $\gamma = a + b\alpha \in S$ with $a, b \in \mathbb{Z}$. Since $\alpha^2 = \frac{(\sqrt{109}+1)^2}{4} = \frac{55+\sqrt{109}}{2} = 27 + \alpha$ we have

$$\left.\begin{aligned} \gamma \cdot 1 &= a + b\alpha \\ \gamma \cdot \alpha &= 27b + (a + b)\alpha \end{aligned}\right\} \implies [m_\gamma] = \begin{bmatrix} a & 27b \\ b & a + b \end{bmatrix}.$$

Denote $\mathrm{Tr}_{\mathbb{Z}[\alpha]/\mathbb{Z}}(x)$ as $\mathrm{Tr}(x)$, then $\mathrm{Tr}(\gamma) = 2a + b$. Also,

$$\Delta(S) = \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(27 + \alpha) \end{bmatrix} = \det \begin{bmatrix} 2 & 1 \\ 1 & 55 \end{bmatrix} = 109.$$

Since 109 is prime, Theorem 2.25 tells us that there S is regular above all primes, implying that $\mathcal{O}_K = S$ and $\Delta_K = \Delta(S) = 109$. Furthermore, α is a root of $x^2 - x - 27$, its characteristic polynomial (as well as a minimal polynomial). There are 2 real roots and 0 pairs of complex roots of this polynomial, the Minkowski bound from Section 2.6 therefore equals $M_K = \frac{1}{2}\sqrt{109} \approx 5.22$, which implies that $\mathrm{Cl}(K)$ is generated by primes of norm at most 5. Since the characteristic polynomial of α is $x^2 - x - 27$, we get that 2 in inert in $\mathcal{O}_K$ as $x^2 - x - 27$ is irreducible in $\mathbb{F}_2[x]$. We also have $(3) = (3, \alpha)(3, \alpha - 1) = \mathfrak{p}_3\mathfrak{q}_3$ and $(5) = (5, \alpha - 2)(5, \alpha + 1) = \mathfrak{p}_5\mathfrak{q}_5$ in $\mathcal{O}_K$. Therefore, only $\mathfrak{p}_3$ and $\mathfrak{p}_5$ are possible generators of $\mathrm{Cl}(K)$.

For $k \in \mathbb{Z}$ we have $\mathrm{N}_{\mathbb{Z}[\alpha]/\mathbb{Z}}(k - \alpha) = k(k - 1) - 27 = k^2 - k - 27 = f(k)$. Since $f(6) = 3$ and $6 - \alpha \in \mathfrak{p}_3$, we know that $(6 - \alpha) = \mathfrak{p}_3$, hence $\mathfrak{p}_3$ is principal. Also, $f(7) = 15$, $7 - \alpha \in \mathfrak{q}_3$, and $7 - \alpha \in \mathfrak{p}_5$, thus $7 - \alpha \in \mathfrak{q}_3\mathfrak{p}_5$ and $(7 - \alpha) = \mathfrak{q}_3\mathfrak{p}_5$, and hence $[\mathfrak{p}_5] = [\mathfrak{p}_3]$, implying that $\mathfrak{p}_5$ is also principal. Therefore, $\mathrm{Cl}(K)$ is trivial and $\mathcal{O}_K$ is a principal ideal domain.

We have $f(1) = -27$, thus $(1 - \alpha) = \mathfrak{q}_3^3 = (27)\mathfrak{p}_3^{-3}$ (as we have that $(3) = \mathfrak{q}_3\mathfrak{p}_3$ and $\mathfrak{p}_3$ is invertible as we are working in a Dedekind domain) and $(6 - \alpha) = \mathfrak{p}_3$. The principal ideal generated by $\eta = (1 - \alpha)^a(6 - \alpha)^b/27^a$ thus factors as $\mathfrak{p}_3^{-3a+b}$ for arbitrary $a, b \in \mathbb{Z}$. If we take $(a, b) = (1, 3)$ we have $-3a + b = 0$ and get the unit ideal

$$\begin{aligned} \eta &= (1 - \alpha)(6 - \alpha)^3/27 = (1 - \alpha)(63 - 11\alpha)(6 - \alpha)/27 \\ &= (33 - 6\alpha)(63 - 11\alpha)/27 = (3861 - 675\alpha)/27 = 143 - 25\alpha. \end{aligned}$$

And indeed $\mathrm{N}_{\mathbb{Z}[\alpha]/\mathbb{Z}}(143 - 25\alpha) = -1$, implying that η is a unit according to the definition in Section 2.4.

It remains to prove that η is a fundamental unit. As η has a negative norm, it cannot be the square of a unit, and must therefore be some odd power of a unit. Since $\eta = 143 - 25\alpha \approx -0.00383$, we know that $\eta^{-1} \approx -1/(-0.00383) \approx 261$. We already know that η cannot be a square, thus if

$\eta = t^k$ for any odd $k \in \mathbb{Z}_{>1}$ and unit $t = u + v\alpha$ with norm -1 and inverse $t^{-1} = u + v - v\alpha$, then $\eta^{-1} = (t^{-1})^k$, thus $1 < t^{-1} = u + v - v\alpha < \sqrt[3]{\eta^{-1}} \approx 6.40$. Taking inverses with respect to -1 then gives that $-1 < t = u + v\alpha < \sqrt[3]{\eta} \approx -0.157$. This relation implies that $-1 - v\alpha < u < \sqrt[3]{\eta} - v\alpha$, substituting this into the relation for t^{-1}, subtracting $v\alpha$ from both sides and dividing by $1 - 2\alpha$ gives $-0.708 < v < -0.109$, which is impossible as v needs to be an integer. Therefore, η is a fundamental unit and we have

$$\mathcal{O}_K^\times = \langle -1 \rangle \times \langle 143 - 25\alpha \rangle.$$

We are almost done with our calculations, except for the fact that we set out to find the integer solutions to $x^2 - 109y^2 = 1$. We know that $\eta = 143 - 25\alpha$ is a fundamental unit in $\mathbb{Z}[\frac{\sqrt{109}+1}{2}]$, but converting this to our original basis $\{1, \sqrt{109}\}$ gives us $\eta = 143 - 25\frac{\sqrt{109}+1}{2}$ which does not give us an integer solution. Therefore, we compute powers of η until the coefficient of α is even.

$$\begin{aligned}
\eta &= 143 - 25\alpha \\
\eta^2 &= 37324 - 6525\alpha \\
\eta^3 &= 9741707 - 1703050\alpha \\
&= 9741707 - 1703050(\sqrt{109} + 1)/2 \\
&= 8890182 - 851525\sqrt{109}.
\end{aligned}$$

Now, the pair $(x, y) = (8890182, 851525)$ satisfies $x^2 - 109y^2 = -1$, but not $x^2 - 109y^2 = 1$. We square our answer to get the correct result.

$$\varepsilon := \eta^6 = (8890182 - 851525\sqrt{109})^2 = 158070671986249 - 15140424455100\sqrt{109}.$$

The powers $\pm 1, \pm\varepsilon^{\pm 1}, \pm\varepsilon^{\pm 2}, \pm\varepsilon^{\pm 3}, \ldots$, written in the form $x + \sqrt{109}y$ represent all solutions (x, y) satisfying $x^2 - 109y^2 = 1$, some examples are listed below.

$$\begin{aligned}
1 &\implies (1)^2 - 109 \cdot (0)^2 = 1, \\
-1 &\implies (-1)^2 - 109 \cdot (0)^2 = 1, \\
\varepsilon &\implies (158070671986249)^2 - 109 \cdot (-15140424455100)^2 = 1, \\
-\varepsilon^{-1} &\implies (-158070671986249)^2 - 109 \cdot (-15140424455100)^2 = 1, \\
\varepsilon^2 &\implies (49972674684368648757690180001)^2 - 109 \cdot (-4786514135549389701035839800)^2 = 1, \\
\varepsilon^{-2} &\implies (49972674684368648757690180001)^2 - 109 \cdot (4786514135549389701035839800)^2 = 1, \\
\varepsilon^3 &\implies (15798428536616731910550597262825995341626249)^2 - \\
&\qquad 109 \cdot (-1513215011755943526709349270967663109365300)^2 = 1.
\end{aligned}$$

Chapter 3

Elliptic Curves

The importance of elliptic curves in contemporary cryptography cannot be overstated. They provide the backbone for several encryption protocols, with the first ones published in 1985 [36] [37]. The theory of elliptic curves provides record-breaking methods to factorise numbers. CSIDH heavily relies on the use of elliptic curves, and computations involving elliptic curves form the backbone of their algorithm.

This chapter starts by introducing the concept of a projective plane, a helpful idea that provides building blocks for other theorems on elliptic curves. Section 3.2 delves into the fundamentals of elliptic curves, particularly focusing on the operation of addition over elliptic curves as defined by the group law. In the final section we combine our theory with Chapter 1 and define elliptic curves over finite fields, forming the foundation for the next chapter which discusses morphisms of elliptic curves.

3.1 Projective Plane

As we will see later on, the projective plane allows us to state formulas and methods regarding elliptic curves. We will look at some definitions regarding the projective plane at the start of this section, after which we will look at an example of a projective line, ending the section with some intuition about projective planes.

Definition 3.1. Let K be a field. Define a *triple* to be an element $(x, y, z) \in K^3$ such that at least one of x, y, z is non-zero. Two triples (x_1, y_1, z_1) and (x_2, y_2, z_2) are said to be equivalent if there exists a non-zero element $\lambda \in K$ such that $(x_1, y_1, z_1) = (\lambda x_2, \lambda x_2, \lambda z_2)$. This relation forms an equivalence relation, and the set of all equivalence classes is called the *projective plane* over K, denoted as $\mathbb{P}^2_K$. The equivalence class of $(x, y, z) \in K^3$ is denoted as $(x : y : z) \in \mathbb{P}^2_K$ and is called a *projective point*. Typically, if K is algebraically closed (Definition 1.12) and it is clear which field we are working in, we denote the projective plane by $\mathbb{P}^2$ instead of $\mathbb{P}^2_{\overline{K}}$.

For the projective plane over a field K we distinguish two cases for projective points $(x : y : z) \in \mathbb{P}^2_K$. If $z \neq 0$, then $(x : y : z) = (x/z : y/z : 1)$. Such projective points are called *finite* points in $\mathbb{P}^2_K$. If $z = 0$, we have $(x : y : z) = (x : y : 0)$. These points are called the *points at infinity*.

Consider the two-dimensional affine plane over K, defined by $\mathbb{A}^2_K := K \times K$. Upon mapping every point $(x, y) \in \mathbb{A}^2_K$ to $(x : y : 1) \in \mathbb{P}^2_K$, we find that $\mathbb{A}^2_K$ is identified with the finite points in $\mathbb{P}^2_K$.

Definition 3.2. Let K be a field. A *line* in $\mathbb{P}^2_K$ is the collection of all points $(x : y : z) \in \mathbb{P}^2_K$ satisfying $ax + by + cz = 0$ for some $a, b, c \in K$.

Remark. Suppose that the triple (x, y, z) is a solution to $ax + by + cz = 0$ for some $a, b, c \in K$. Then, for any $\lambda \in K \setminus \{0\}$, we will also have that the triple $(\lambda x, \lambda y, \lambda z)$ will be a solution to the equation. Hence, we are able to state that an entire equivalence class of these triples (a projective point) can satisfy the equation.

Remark. One can show that if a triple (x, y, z) satisfies $F(x, y, z) = 0$ where F is a homogeneous polynomial of degree n (meaning that $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ for all $\lambda \in K$), then all triples in the equivalence class $(x : y : z)$ will satisfy the equation. Equivalently, polynomials that are the sum of terms of the form $ax^i y^j z^k$ with $a \in K$ and $i + j + k = n$ are homogeneous. Using this, we find that the equations from Definition 3.2 and Definition 3.4 (which comprise all the types of projective equations used in this thesis) can be rewritten into the form $F(x, y, z) = 0$ where F is homogeneous. We will not go deeper into the subject of homogeneity, and instead refer the reader to [38, Section 2.3], [39, Appendix A.2], [40, Section I.2], and [41, Lecture 1].

Definition 3.3. Let L be an algebraic extension (Definition 1.12) of K. A point $(x : y : z) \in \mathbb{P}^2_K$ is called L-rational if $(x : y : z) \in \mathbb{P}^2_L$. Similarly, a point $(x, y) \in \mathbb{A}^2_K$ is called L-rational if $(x, y) \in \mathbb{A}^2_L$.

Let K be the field of rational numbers. We start by writing down all solutions to the projective line (the line in $\mathbb{P}^2_{\mathbb{Q}}$)

$$3x - y + z = 0.$$

We can see that $\{(u : 3u + v : v) \in \mathbb{P}^2_{\mathbb{Q}} : u, v \in \mathbb{Q}\}$ forms a set of all solutions. To get all finite points on the line, we enter the case $v \neq 0$, which gives the points $(\frac{u}{v} : 1 + \frac{3u}{v} : 1) \in \mathbb{P}^2_{\mathbb{Q}}$.
We can also determine all finite points of the projective line using the substitution $x' = x/z$, $y' = y/z$, and $z' = z/z = 1$, which gives

$$3x' - y' + 1 = 0.$$

Such that the $\mathbb{Q}$-rational point $(a, 3a + 1)$ with $a \in \mathbb{Q}$ arbitrary forms a parameterisation of all solutions. Using the (bijective) map $(x, y) \to (x : y : 1)$, we can see that $(a, 3a + 1)$ maps to $(a : 3a + 1 : 1)$. Thus, using this method, we find that all finite points on our projective line are $(a : 3a + 1 : 1) \in \mathbb{P}^2_{\mathbb{Q}}$.
By setting $a = u/v$, we can see that both methods of enumerating the finite points on the projective line give the same answer.

To conclude this section we provide some intuition about projective planes. The main idea is to introduce points at infinity. In affine planes, one can find a unique line through any two distinct points, and parallel lines do not intersect. However, in projective planes we can not only state that there exists a unique line through two distinct points, but we can also state that any two distinct lines intersect in exactly one point. In a projective plane, two lines that are parallel to each other (with respect to the finite points), are defined to intersect at a point at infinity determined by the direction of the lines. Informally, this means that we can write the projective plane as follows.

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{\text{directions in } \mathbb{A}^2\}.$$

The set of directions in $\mathbb{A}^2$ is the set of all the points at infinity.

3.2 Elliptic Curves

Definition 3.4. An *elliptic curve* in short Weierstrass form defined over a field K is the collection of all points $(X : Y : Z) \in \mathbb{P}^2_K$ that satisfy

$$Y^2 Z = X^3 + aXZ^2 + bZ^3, \tag{3.1}$$

for some $a, b \in K$ with $4a^3 + 27b^2 \neq 0$.

If we substitute $Z = 0$ in equation (3.1) we get $X^3 = 0$, which has the triple root $X = 0$. This gives us all points at infinity on the elliptic curve, namely $(0 : 1 : 0)$ (which corresponds to the direction of a vertical line).

Elliptic curves are often written in their *affine form*. Upon setting $x = X/Z$ and $y = Y/Z$, and substituting this into equation (3.1) we can define an elliptic curve over K as the collection of points $(x, y) \in \mathbb{A}^2_K$ satisfying

$$y^2 = x^3 + ax + b$$

plus the projective point at infinity $\mathcal{P}_\infty := (0 : 1 : 0)$. Just as before, we have that $a, b \in K$ and $4a^3 + 27b^2 \neq 0$ must hold.

Let E be the elliptic curve over $\mathbb{Q}$ defined by the affine equation

$$y^2 = x^3 - 5x + 2.$$

Since $-5, 2 \in \mathbb{Q}$ and $4 \cdot (-5)^3 + 27 \cdot 2^2 \neq 0$ we know that E indeed is an elliptic curve.
Take the $\mathbb{Q}$-rational point $P = (2, 0)$, we have that $P \in E$ as $0^2 = 2^3 - 5 \cdot 2 + 2$. The point $Q = (-2, 2) \in \mathbb{A}^2_{\mathbb{Q}}$ also satisfies $Q \in E$. We also have that $(-2, -2) \in E$. The $\mathbb{Q}$-rational point $R = (\frac{113}{16}, \frac{1143}{64})$ is also a point on the elliptic curve.
The $\mathbb{Q}(\sqrt{2})$-rational points $(0, \sqrt{2})$ and $(0, -\sqrt{2})$ are points on the elliptic curve.
The point $(1, \sqrt{2}i) \in \overline{\mathbb{Q}}$ lies on the elliptic curve. Note that $\sqrt{2}i$ is a root of the polynomial $x^2 + 2 \in \mathbb{Q}[x]$ and thus resides in the algebraic closure (Definition 1.12) of $\mathbb{Q}$.

It turns out that we can find a group operator hidden in these elliptic curves.

3.2.1 The Group Law

Definition 3.5. Define an elliptic curve E over a field K and choose two points P and Q on the elliptic curve. By Bézout's theorem [39, Theorem A.1] [41, Theorem 18.3] [42, Chapter 3], the line through P and Q will intersect the elliptic curve in a third point (this specific statement can be found in [38, Section 2.2]), denoted $P * Q$ and called the *composition* of P and Q. See Figure 3.1.

Remark. If the points P and Q are equal, then the line through them is taken to be the tangent line of the elliptic curve at P. We say that the tangent line intersects the curve with multiplicity 2 at P. Points of inflection on the elliptic curve intersect the elliptic curve with multiplicity 3.

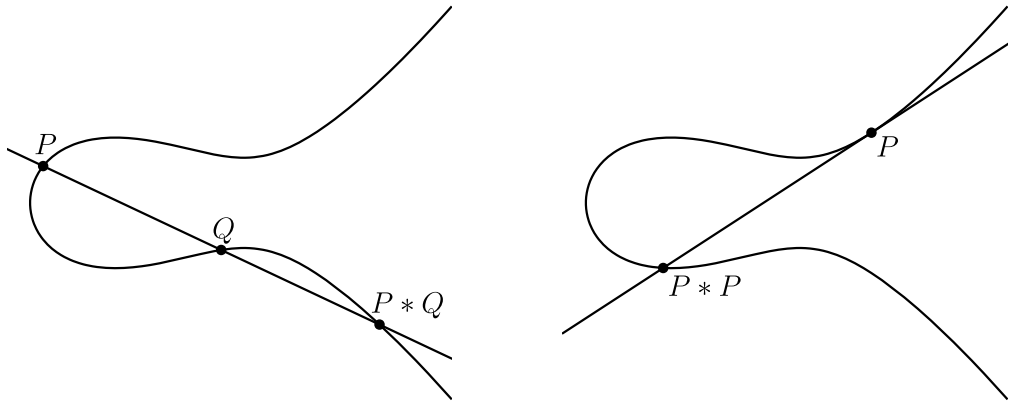

Figure 3.1: The composition of points on the elliptic curve $y^2 = x^3 - \frac{3}{2}x + 2$ plotted over $\mathbb{A}^2_{\mathbb{R}}$.

What about the point at infinity on the elliptic curve, i.e., $\mathcal{P}_\infty = (0:1:0)$, is our definition of composition well-defined at this point? First, we look at $\mathcal{P}_\infty * Q$ for any other point Q on the elliptic curve. The vertical line coming down from $\mathcal{P}_\infty$, crosses $Q := (Q_x, Q_y)$ and $(Q_x, -Q_y)$. Second, a neat consequence of $\mathcal{P}_\infty$ being a triple root in equation (3.1) is that $\mathcal{P}_\infty * \mathcal{P}_\infty = \mathcal{P}_\infty$. Having discussed these special cases, we are assured that Definition 3.5 is indeed well-defined.

There is another nice property of composing points in this way. Namely, if E is defined over $\mathbb{Q}$, and P and Q are points in $\mathbb{P}^2_{\mathbb{Q}}$, then we have that $P * Q \in \mathbb{P}^2_{\mathbb{Q}}$ [43]. So the composition of two rational points is also rational.

Sadly however, the rational points on an elliptic curve under composition do not behave as a group as composition is not associative to start with (see Figure 3.2). On the bright side, without too much effort, we can define a group operation on the rational points on the elliptic curve.

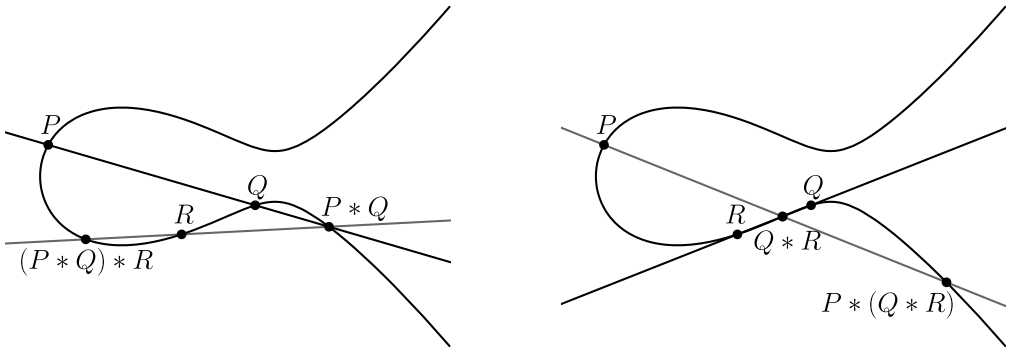

Figure 3.2: The composition of points three points P, Q, and R on the elliptic curve $y^2 = x^3 - \frac{5}{2}x + 2$ plotted over $\mathbb{A}^2_{\mathbb{R}}$ in two different ways.

Definition 3.6. Take an arbitrary point of the elliptic curve to be the identity element of the group, denote it as $\mathcal{O}$. We define the operation $+$ on two points P and Q on the elliptic curve as $P + Q = \mathcal{O} * (P * Q)$.

Under this operation, the rational points on an elliptic curve form an abelian group. The proof that this operation is associative can be found in [38, Section 2.4], computer-assisted proofs using the explicit formulas (we derive these in Section 3.2.2) can be found in [44] and [45]. The following famous theorem gives an important property of this group.

Theorem 3.7 (Mordell's theorem, 1922)**.** *The set of rational points over an elliptic curve is a finitely generated abelian group under the $+$ operator from Definition 3.6.*

Proof. See [46]. □

For the set of rational points on an elliptic curve, being finitely generated means that there exists a set of finitely many rational points on the elliptic curve, such that **every** other rational point on the curve can be found by repetitively applying our $+$ operation to these points (and reflecting points across the x-axis).

We end this subsection by noting something about $\mathcal{O}$, the identity element of our group. The choice of $\mathcal{O}$ is entirely arbitrary, but in most cases it is chosen to be the point at infinity $(0:1:0)$. This simplifies things greatly in terms of visualisation and understanding. Simply draw a line through the two points you want to add, find the other point of intersection with the elliptic curve and reflect it around the x-axis, and you are done. This choice also makes sense as it is the only projective point that lies on every elliptic curve.

3.2.2 Explicit Formulas for the Group Law

Given an elliptic curve over K which, in its affine form, can be written down as

$$y^2 = x^3 + Ax + B. \tag{3.2}$$

We would like to find explicit formulas to add two points $P := (P_x, P_y)$ and $Q := (Q_x, Q_y)$ with $P_x, P_y, Q_x, Q_y \in \overline{K}$ on this elliptic curve, instead of having to draw lines and finding intersection points.

We take the identity $\mathcal{O}$ to be $(0 : 1 : 0)$ for the remainder of this section (and even this thesis). Also, for an arbitrary point $R := (R_x, R_y)$ on the elliptic curve we define $-R := (R_x, -R_y)$, the point R reflected across the x-axis.

There are a couple of cases we can have, we list them below.

- $P = \mathcal{O}$ **and** $Q = \mathcal{O}$**:** We have already seen that $\mathcal{O} * \mathcal{O} = \mathcal{O}$. Hence, we also have $\mathcal{O} + \mathcal{O} = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} * \mathcal{O} = \mathcal{O}$.
- $P \neq \mathcal{O}$ **and** $Q = \mathcal{O}$**:** The line through P and $\mathcal{O}$ is equal to the vertical line through P. This line intersects P in $-P = (P_x, -P_y)$, the point P reflected across the x-axis. Thus, $P * \mathcal{O} = -P$, therefore $\mathcal{O} + \mathcal{P} = \mathcal{O} * (P * \mathcal{O}) = \mathcal{O} * (-P) = P$.
- $P = \mathcal{O}$ **and** $Q \neq \mathcal{O}$**:** Swap P and Q and apply the case $P \neq \mathcal{O}$ **and** $Q = \mathcal{O}$.
- $Q = -P \neq \mathcal{O}$**:** We find that $P + Q = P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O} * \mathcal{O} = \mathcal{O}$. As the line through P and $-P$ will be the vertical line extending to infinity.
- $P \neq \mathcal{O}$**,** $Q \neq \mathcal{O}$**, and** $P \neq \pm Q$**:** We need to find the slope of the lines through both P and Q, this line will have a slope, λ, of

  $$\lambda = \frac{Q_y - P_y}{Q_x - P_x}.$$

  Note that we cannot have $Q_x = P_x$ as we assumed that $P \neq \pm Q$.

  The derivation below these cases then finds the explicit coordinates of $P + Q$.
- $P = Q \neq \mathcal{O}$ **and** $P_y \neq 0$**:** We are trying to find $P + P$, which will be denoted as $[2]P$. Note that if $P_y = 0$, we enter the case $Q = -P \neq \mathcal{O}$. To do this we need to set up the tangent to the elliptic curve at point P. Taking the derivative on both sides of the equation $y^2 = x^3 + Ax + B$, yields $2y\mathrm{d}y = (3x^2 + A)\mathrm{d}x$. The tangent line of the elliptic curve at P will thus have a slope, λ, of

  $$\lambda = \left.\frac{\mathrm{d}y}{\mathrm{d}x}\right|_P = \frac{3P_x^2 + A}{2P_y}.$$

Given λ, the slope of the line through P and Q (which we define the tangent line at P if $P = Q$), we would like to find the third intersection point of the line through P and Q with the elliptic curve.

Define $\mu = P_y - \lambda P_x = Q_y - \lambda Q_x$, then the line through the points P and Q can be written as: $y = \lambda x + \mu$. Plugging this formula into equation (3.2) we get:

$$y^2 = (\lambda x + \mu)^2 = x^3 + Ax + B.$$

We thus need to find the roots of

$$x^3 + Ax + B - (\lambda x + \mu)^2 = x^3 - \lambda^2 x^2 + (A - 2\lambda\mu)x + (B - \mu^2).$$

But, we already know two solutions, namely P_x and Q_x, since the line goes through these two points. Define the x-coordinate of the third intersection point to be x_3, we now state that

$$x^3 - \lambda^2 x^2 + (A - 2\lambda\mu)x + (B - \mu^2) = (x - P_x)(x - Q_x)(x - x_3).$$

Writing the right-hand side out gives us

$$x^3 - (P_x + Q_x + x_3)x^2 + (P_xQ_x + P_xx_3 + Q_xx_3)x - P_xQ_xx_3.$$

Combining both sides of the equation allows us to equate coefficients that belong to identical degrees of x, giving us some direct formulas to calculate x_3:

$$x_3 = \lambda^2 - P_x - Q_x = \frac{A - 2\lambda\mu - P_xQ_x}{P_x + Q_x} = \frac{\mu^2 - B}{P_xQ_x}. \tag{3.3}$$

Thus, $P + Q$ can be written as (note the reflection around the x-axis)

$$P + Q = (\lambda^2 - P_x - Q_x, -\lambda(\lambda^2 - P_x - Q_x) - \mu).$$

Now, remember that we said that elliptic curves defined over the rational numbers with points $P, Q \in \mathbb{P}^2_{\mathbb{Q}}$ on the elliptic curve will have $P * Q \in \mathbb{P}^2_{\mathbb{Q}}$. In other words, the composition of two rational points is also rational. This result is immediate from the explicit formulas that we derived above.

We define an elliptic curve over $\mathbb{A}^2_{\mathbb{Q}}$ with the affine form

$$y^2 = x^3 - 2x + 2. \tag{3.4}$$

Plugging in $\frac{1}{2}$ and $-\frac{3}{2}$ into the equation of the elliptic curve will result in the two points $P = \left(\frac{1}{2}, \sqrt{\frac{1}{2^3} - 1 + 2}\right) = \left(\frac{1}{2}, \frac{3}{\sqrt{8}}\right)$ and $Q = \left(-\frac{3}{2}, -\sqrt{-\frac{3^3}{2^3} + 3 + 2}\right) = \left(-\frac{3}{2}, \sqrt{\frac{13}{8}}\right)$ on the elliptic curve. A visualisation of this addition can be seen in Figure 3.3. Remember that although the elliptic curve is defined over $\mathbb{A}^2_{\mathbb{Q}}$, all points of the elliptic curve reside in $\mathbb{P}^2_{\mathbb{Q}}$.
We get line through P and Q, in the form as $y = \lambda x + \mu$, with coefficients

$$\lambda = \frac{P_y - Q_y}{P_x - Q_x} = \frac{1}{2} \cdot \frac{3 + \sqrt{13}}{2\sqrt{2}}, \quad \mu = P_y - \lambda P_x = \frac{3}{\sqrt{8}} - \frac{1}{2} \cdot \frac{3 + \sqrt{13}}{2\sqrt{2}} \cdot \frac{1}{2} = \frac{9 - \sqrt{13}}{8\sqrt{2}}.$$

The final addition can be written and simplified to

$$P + Q = \left(\frac{27 + 3\sqrt{13}}{16}, -\frac{48 + 7\sqrt{13}}{16\sqrt{2}}\right) \approx (2.36, -3.24).$$

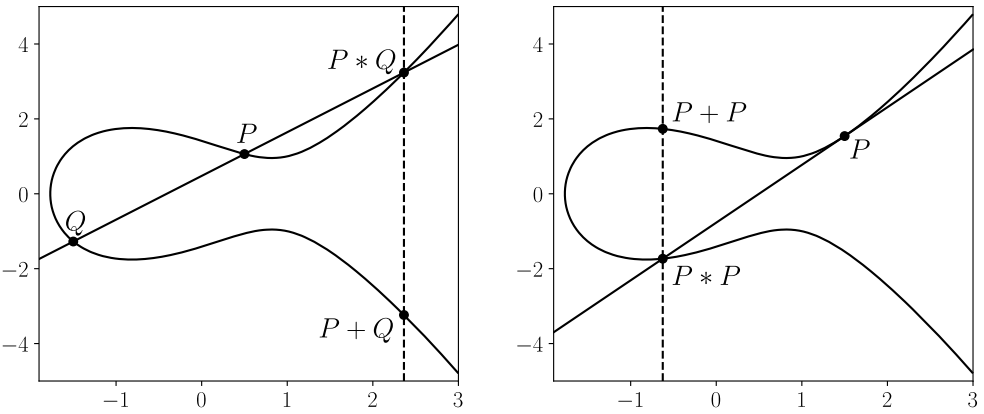

Figure 3.3: Various additions of two points on the elliptic curve from equation (3.4).

As a different example we will add $P = \left(\frac{3}{2}, \sqrt{\frac{3^3}{2^3} - 3 + 2}\right) = \left(\frac{3}{2}, \sqrt{\frac{19}{8}}\right)$ to itself, using the same elliptic curve from equation (3.4). A visualisation of this addition can be seen in Figure 3.3.
We compute the slope λ of the tangent line at P and the parameter μ such that the tangent line at P can be written as $y = \lambda x + \mu$.

$$\lambda = \frac{3P_x^2 + A}{2P_y} = \frac{\frac{27}{4} - 2}{\sqrt{19/2}} = \sqrt{\frac{19}{8}}, \quad \mu = P_y - \lambda P_x = \sqrt{\frac{19}{8}} - \sqrt{\frac{19}{8}} \cdot \frac{3}{2} = -\frac{1}{2}\sqrt{\frac{19}{8}}.$$

The final x-coordinate of $P+P$ can be evaluated in numerous ways according to equation (3.3). The y-coordinate can be calculated using $\lambda([2]P)_x + \mu$, or by plugging the newly found x-coordinate in equation (3.4) and taking the positive solution. All in all, we get the relations

$$(P+P)_x = ([2]P)_x = \lambda^2 - 2P_x = \frac{\mu^2 - B}{P_x^2} = \frac{A - 2\lambda\mu - P_x^2}{2P_x} = -\frac{5}{8},$$
$$(P+P)_y = ([2]P)_y = \lambda([2]P)_x + \mu = -\sqrt{([2]P)_x^3 - 2([2]P)_x + 2} = -\frac{9}{32}\sqrt{38},$$
$$P + P = [2]P = \left(-\frac{5}{8}, -\frac{9}{32}\sqrt{38}\right) \approx (-0.625, -1.734).$$

3.3 Elliptic Curves over Finite Fields

For the remainder of this section, let q be the power of some prime p, such that $q = p^m$ for some positive integer m. Extending Definition 3.4, we find that an elliptic curve (in short Weierstrass form) defined over the finite field $\mathbb{F}_q$ will have coefficients in $\mathbb{F}_q$. We note that the formulas for addition over an elliptic curve derived in Section 3.2.2 can also be evaluated over $\mathbb{F}_q$.

We define an elliptic curve over the finite field $\mathbb{F}_7$ with the affine form

$$y^2 = x^3 - 2x + 2.$$

Using brute force one can find some points on the elliptic curve. For example $P = (1, 1)$ and $Q = (4, 3)$ are both on the elliptic curve. To add P and Q we evaluate (in $\mathbb{F}_7$)

$$\lambda = \frac{P_y - Q_y}{P_x - Q_x} = \frac{-2}{-3} = \frac{2}{3} = 3, \qquad \mu = P_y - \lambda P_x = 1 - 3 = -2.$$

Therefore, $\lambda^2 - P_x - Q_x = 3^2 - 1 - 4 = 4$ and $P+Q = (4, -4\lambda - \mu) = (4, -3 \cdot 4 + 2) = (4, 4)$. Similarly, evaluating $P + P$ gives $\lambda = \frac{3 \cdot 1^2 - 2}{2} = 4$ and $\mu = 1 - 4 = -3$. Therefore, $P + P = (0, 3)$.

In general, points of an elliptic curve E defined over a finite field $\mathbb{F}_q$ are not necessarily contained in the finite field, instead the points belong to $\overline{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, from Definition 1.12.

Take the elliptic curve $E : y^2 = x^3 - 2x + 2$ defined over the finite field $\mathbb{F}_7$.
Let s be a root of the polynomial $x^2+6x+3 \in \mathbb{F}_7[x]$ and define $\mathbb{F}_{7^2}$ to be $\mathbb{F}_7[x]/(x^2+6x+3)$

as in Theorem 1.7. The $\mathbb{F}_{7^2}$-rational (but not $\mathbb{F}_7$-rational) point $P = (2, 6s + 4)$ is on the elliptic curve E as $(6s + 4)^2 = s^2 + 6s + 2 = 6 = 2^3 - 2 \cdot 2 + 2$.

In this example, we have seen that the points of an elliptic curve over $\mathbb{F}_q$ are not always $\mathbb{F}_q$-rational. We denote the subset of points on E that **are** $\mathbb{F}_q$-rational by $E(\mathbb{F}_q)$.

The security of many cryptosystems relies on the difficulty of the *discrete logarithm problem* in a group $(\mathbb{Z}/p\mathbb{Z})$ for some large prime p. We state it as follows. Given $\alpha \in (\mathbb{Z}/p\mathbb{Z})$ and $\beta \in \langle\alpha\rangle$ (that is, β can be generated by α), find any integer x such that $\alpha^x = \beta$

Using our newfound addition of points on elliptic curves we can formulate the *elliptic curve discrete logarithm problem*. The problem is that given a prime p, an elliptic curve E defined over $\mathbb{F}_p$ and the points $P, Q \in E(\mathbb{F}_p)$ (assuming that Q is a multiple of P), find an integer m so that $[m]P = Q$. This problem is the basis for elliptic curve cryptography (ECC), an encryption method that has existed for nearly four decades [36] [37].

Also, Lenstra Elliptic Curve factorisation [39, Section 4.4] [47], can factor positive integers n. Let n denote a number that is not prime (checking primality is a relatively cheap operation compared to factoring), the algorithm starts by finding an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ and a point $P \in E(\mathbb{Z}/n\mathbb{Z})$. Now, it will continue to find multiples of the point P, until, using the addition formulas from Section 3.2.2, we try to invert a residue class in $\mathbb{Z}/n\mathbb{Z}$ that has no inverse (such residue classes exist as n is not prime). We can then retrieve a factor of n using the residue class that has no inverse in $\mathbb{Z}/n\mathbb{Z}$.

Chapter 4

Morphisms of Elliptic Curves

In order to understand the algorithm that drives CSIDH, we must first take a look at mappings between two elliptic curves called morphisms.

In this chapter we will first look at a special type of morphism of elliptic curves called an isogeny. Afterwards, we discuss isomorphism classes of elliptic curves. Intertwining the theory from Chapter 2 allows us to examine the structure of the endomorphism ring of an elliptic curve. It also allows us to define the action of ideal classes on isomorphism classes of elliptic curves, a concept that gives rise to isogeny graphs, a helpful visualisation for isogeny-based cryptography.

The principles covered in this chapter are crucial to understanding CSIDH, linking all previously discussed theories to provide a thorough background on the algorithm introduced in the next chapter.

Warning. Unless stated otherwise, all elliptic curves in this chapter will be defined over the finite field $\mathbb{F}_p$ with $p > 3$ a prime number.

4.1 Isogenies of Elliptic Curves

Defining an isogeny is typically done using algebraic geometry. However, we take a more implicit route to avoid some of this theory. At each step, we try to provide proof that our definitions are equivalent to the definitions using more sophisticated algebraic geometry. Typical definitions of isogenies can be found in [48, Chapter 5, Section 9.6], [49], and [40, Chapters I, II, Section III.4].

Theorem 4.1. *Two elliptic curves E_1 and E_2 over a finite field $\mathbb{F}_p$ are* isogenous *over $\mathbb{F}_p$ if and only if $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$.*

Proof. See [50], [48, Theorem 9.7.4] (only for sufficiency), or [40, Exercise 5.4]. □

Definition 4.2. Let E_1 and E_2 be elliptic curves of the form $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{F}_p$. If E_1 is isogenous to E_2, i.e., $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$, then there exists a map $\phi : E_1 \to E_2$ satisfying $\phi(\mathcal{O}) = \mathcal{O}$ called a *non-zero isogeny* from E_1 to E_2. Every *isogeny* is either the *zero isogeny*, mapping each point $P \in E_1$ to $\mathcal{O} \in E_2$, or a non-zero isogeny between isogenous elliptic curves[†]. Every non-zero isogeny is can be expressed as a rational map

$$\phi(x, y) = \left(\frac{f(x)}{k(x)}, \frac{g(x)}{h(x)} y \right), \tag{4.1}$$

where $f, k, g, h \in \mathbb{F}_p[x]$, $\gcd(f, k) = 1$, and $\gcd(g, h) = 1$ (Definition 1.11). A proof of this can be found in [49, Lemma 4.26] and [48, Lemma 9.6.12]. The *kernel* of any isogeny $\phi : E_1 \to E_2$ is denoted as $\ker(\phi)$ and defined as $\ker(\phi) = \{P \in E_1 : \phi(P) = \mathcal{O}\}$.

[†]In other literature this is said to be an isogeny defined over $\mathbb{F}_p$. Since all isogenies in this thesis will be defined over $\mathbb{F}_p$, we just call them isogenies.

Theorem 4.3. *Let E_1 be isogenous to E_2 and let $\phi : E_1 \to E_2$ be a non-zero isogeny given by equation (4.1). Then, any point $(x_0 : y_0 : 1) \in E_1$ is in the kernel of ϕ if and only if $k(x_0) = 0$*

Proof. This follows directly from [49, Corollary 4.28]. □

Definition 4.4. The *kernel polynomial* of a non-zero isogeny is $k(x) \in \mathbb{F}_p[x]$ from equation (4.1) divided by its lead coefficient (in order for the kernel polynomial to become a monic polynomial). We note that the kernel polynomial is uniquely determined [49, p. 9].

Let $E_1 : y^2 = x^3 + 3x^2 + 2x$ and $E_2 : y^2 = x^3 + 3x^2 + 6x + 4$ be elliptic curves defined over the finite field $\mathbb{F}_7$. As $\#E_1(\mathbb{F}_7) = \#E_2(\mathbb{F}_7) = 8$, we know that E_1 and E_2 are isogenous. Therefore, there exists an isogeny $\phi : E_1 \to E_2$ between them. In fact, such an isogeny is given by the rational map

$$\phi(x, y) = \left(\frac{x^2 + 2}{x}, \frac{x^2 y - 2y}{x^2} \right).$$

Take $P = (4, 1) \in E_1$, then $\phi(P) = \left(\frac{18}{4}, \frac{14}{16}\right) = (1, 0)$ and indeed $(1, 0) \in E_2$. If we would have taken $P = (0, 0) \in E_1$, then $\phi(P) = \mathcal{O} \in E_2$. In fact, one can show that $\ker \phi = \{\mathcal{O}, P\}$.
To show that the isogeny ϕ is not one-to-one note that both $(3, 2) \in E_1$ and $(3, 5) \in E_1$ map to $(6, 0) \in E_2$. Furthermore, no $P \in E_1(\mathbb{F}_7)$ maps to $(2, 1) \in E_2(\mathbb{F}_7)$. However, $P = (6s + 5, 4s + 2) \in E_1(\mathbb{F}_{7^2})$, where both the x and the y coordinate of P are elements of $\mathbb{F}_{7^2} := \mathbb{F}_7[s]/(s^2 + 6s + 3)$ satisfies

$$\begin{aligned}
\phi(6s + 5, 4s + 2) &= \left(\frac{(6s + 5)^2 + 2}{6s + 5}, \frac{(6s + 5)^2 - 2}{(6s + 5)^2}(4s + 2) \right) \\
&= \big(6s + 5 + 2(4s + 2), (1 - 2(4s + 2)^2)(4s + 2)\big) \\
&= (2, (1 - 2(4s + 5))(4s + 2)) \\
&= (2, 1)
\end{aligned}$$

by the long division from Section 1.2 and the relation $(6s + 5)^{-1} = 4s + 2$.

4.2 Isomorphism Classes of Elliptic Curves

Definition 4.5. Let E_1 and E_2 be elliptic curves defined over $\mathbb{F}_p$. We say that E_1 and E_2 are $\mathbb{F}_p$*-isomorphic* if there exist isogenies $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_1$ such that for every point $P \in E_1$ we have that $\phi_2(\phi_1(P)) = P$, i.e., $\phi_2 \circ \phi_1$ is the identity map. The isogenies ϕ_1 and ϕ_2 are then called $\mathbb{F}_p$*-isomorphisms*. Define a relation $\cong$ on arbitrary elliptic curves E_1 and E_2, such that $E_1 \cong E_2$ if and only if E_1 and E_2 are $\mathbb{F}_p$-isomorphic (this notation will come back later). Then this relation forms an equivalence relation. The equivalence classes are called $\mathbb{F}_p$*-isomorphism classes* of elliptic curves.

Define the elliptic curve $E_1 : y^2 = x^3 + 2x + 1$ over $\mathbb{F}_7$ and the elliptic curve $E_2 : y^2 = (x+1)^3 + 2(x+1) + 1 = x^3 + 3x^2 + 5x + 4$ over $\mathbb{F}_7$. These curves are isogenous, so that there exists an isogeny between them. In fact, $\phi_1 : E_1 \to E_2$ given by $\phi_2(x, y) = (x + 1, y)$ and $\phi_2 : E_2 \to E_1$ given by $\phi_2(x, y) = (x - 1, y)$ are two isogenies. We can see that for every point $P \in E_1$ we have that $\phi_2(\phi_1(P)) = P$, proving that E_1 and E_2 are $\mathbb{F}_p$-isomorphic, so that E_1 and E_2 are in the same $\mathbb{F}_p$-isomorphism class.

Besides $\mathbb{F}_p$-isomorphisms, there also exist $\overline{\mathbb{F}}_p$-isomorphisms. Before we state when two curves are $\overline{\mathbb{F}}_p$-ismorphic in Theorem 4.7, we first look at the j-invariant of an elliptic curve.

Definition 4.6. Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve with $a, b, c \in \mathbb{F}_p$. We define $b_2 = 4a$, $b_4 = 2b$, $b_6 = 4c$, and $b_8 = \frac{1}{4}(b_2b_6 - b_4^2)$. The j-invariant of the elliptic curve equals

$$j(E) = \frac{(b_2^2 - 24b_4)^3}{9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2} \in \mathbb{F}_p.$$

Theorem 4.7. *Two elliptic curves E_1 and E_2 are $\overline{\mathbb{F}}_p$-isomorphic (equivalently, there exists an $\overline{\mathbb{F}}_p$-isormorphism between them) if and only if their j-invariants are equal, that is $j(E_1) = j(E_2)$.*

Proof. A proof of this theorem is listed in [40, III.1.4(b)]. □

Theorem 4.8. *An elliptic curve $E' : y^2 = x^3 + A'x + B'$ in short Weierstrass form is $\mathbb{F}_p$-isomorphic to the elliptic curve $E : y^2 = x^3 + Ax + B$ if and only if there exists a $u \in \mathbb{F}_p^*$ such that $A' = u^4A$ and $B' = u^6B$. Moreover, two elliptic curves that are $\mathbb{F}_p$-isomorphic are also $\overline{\mathbb{F}}_p$-isomorphic, the converse does not hold in general.*

Proof. A proof of this theorem can be found in [51, Theorems 2.2.2-2.2.4]. □

Let $E_1 : y^2 = x^3 + 2x + 1$ be an elliptic curve defined over $\mathbb{F}_5$. Similarly, let $E_2 : y^2 = x^3 + 3x + 2$ be an elliptic curve defined over $\mathbb{F}_5$. We have that $j(E_1) \equiv j(E_2) \equiv 4 \pmod 5$, so that the exists an $\overline{\mathbb{F}}_5$-isomorphism between E_1 and E_2 from Theorem 4.7. However, they are not isomorphic due to Theorem 4.8 as there does not exist a $u \in \mathbb{F}_5^*$ such that $3 \equiv 2u^4 \pmod 5$ and $2 \equiv u^6 \pmod 5$.

4.3 Montgomery Curves

A *Montgomery curve* is an elliptic curve over a finite field $\mathbb{F}_p$ with $p > 3$, of the form $y^2 = x^3 + Mx^2 + x$ for some $M \in \mathbb{F}_p$. Here, M is called the *Montgomery coefficient* of the elliptic curve. In CSIDH [1] (which is discussed in Section 5.2) these curves are extensively used as they make calculations easier. Moreover, CSIDH only works with $\mathbb{F}_p$-isomorphism classes that contain exactly one Montgomery curve [1, p. 5]; this allows them to denote an entire $\mathbb{F}_p$-isomorphism class by the Montgomery coefficient of that Montgomery curve.

The curve $E : y^2 = x^3 + 2x + 1$ defined over $\mathbb{F}_{11}$ is isomorphic to the curve $y^2 = x^3 + x^2 + x$ in Montgomery form with a Montgomery coefficient of 1. CSIDH thus denotes the $\mathbb{F}_{11}$-isomorphism class containing E by 1.

An additional use of Montgomery curves for cryptography is that the x-coordinate of $[k]P$ for some $k \in \mathbb{Z}_{>0}$ and point P on the curve can be found significantly faster than for normal elliptic curves [1, p. 26]. This fact is used extensively in CSIDH to speed up computations in their encryption scheme.

4.4 The Endomorphism Ring

In the previous sections we talked about two elliptic curves being isogenous and isomorphic. In this section we will talk about the mappings that map an elliptic curve to itself.

Definition 4.9. Let E be an elliptic curve. An $\mathbb{F}_p$-*endomorphism* is an isogeny ϕ from E to E. The set of all endomorphisms of the elliptic curves is called the $\mathbb{F}_p$-*endomorphism ring* of E, and is denoted as $\mathrm{End}_{\mathbb{F}_p}(E)$. Let ϕ and ψ denote $\mathbb{F}_p$-endomorphisms from E to E. Then the $\mathbb{F}_p$-endomorphism ring forms a ring under the addition operation $(\phi+\psi)(P) = \phi(P)+\psi(P)$ and the multiplication operation $(\phi\cdot\psi)(P) = \phi(\psi(P))$, where P is any point in E [40, Proposition 4.2(c)].

Remark. In this thesis we will only consider $\mathbb{F}_p$-endomorphisms, therefore, we will call them endomorphisms from now on. We will also define $\mathrm{End}(E) := \mathrm{End}_{\mathbb{F}_p}(E)$ and call the $\mathbb{F}_p$-endomorphism ring of E the endomorphism ring of E.

Let E_1 and E_2 be elliptic curves and let $[m] : E_1 \to E_2$ with $m \in \mathbb{Z}$ denote the multiplication-by-m map sending each point $P \mapsto [m]P$, i.e., adding each point to itself a total of m times. We certainly have that the multiplication-by-1 map sends E_1 to itself, i.e., $[1] : E_1 \to E_1$ is an endomorphism. Since $[1] \in \mathrm{End}(E_1)$, we can use the addition operation defined on the endomorphism ring to see that $([1] + [1])(P) = [1]P + [1]P = [2]P$ for any point $P \in E_1$. Thus, the multiplication-by-2 map, $[2]$, is also an endomorphism. Likewise, one can show that every multiplication-by-m map is an endomorphism.

Let $E : y^2 = x^3 + 2x + 1$ be an elliptic curve defined over $\mathbb{F}_7$. The isogeny $\phi : E \to E$ defined by

$$\phi(x, y) = \left(\frac{x^4 - x}{-3x^3 - 3}, \frac{x^6 - x^3 - 1}{x^6 + 2x^3 + 1}y\right)$$

is an endomorphism mapping each point P to $[2]P$ by the formulas from Section 3.2.2.

Definition 4.10. Let $p > 3$ be a prime and let E be an elliptic curve over $\mathbb{F}_p$. The pth power Frobenius map $\pi : E \to E$ defined by the rational map $(x, y) \mapsto (x^p, y^p)$ is an endomorphism. Therefore, we call this map the *pth power Frobenius endomorphism* of E.

Let E be an elliptic curve over $\mathbb{F}_p$. As we have $x^p = x$ for all $x \in \mathbb{F}_p$ (Theorem 5.3), all points in $E(\mathbb{F}_p)$ are fixed by the pth power Frobenius endomorphism. However, the pth power Frobenius endomorphism permutes all points in E that are not in $E(\mathbb{F}_p)$.

Theorem 4.11. *Let E be an elliptic curve, and let G be a finite subgroup (i.e., a subgroup that is a finite group) of the points on E stable under applying the pth power Frobenius endomorphism π, i.e., for each $P \in G$ we have $\pi(P) \in G$. There is a unique elliptic curve E' up to $\mathbb{F}_p$-isomorphism and an isogeny $\phi : E \to E'$ satisfying* $\ker\phi = G$.

Proof. See Proposition III.4.12 and Exercise 3.13(e) of [40]. Also, see [48, Theorem 9.6.19] or [1, Lemma 6]. □

Remark. For a given curve E and subgroup G, Velu [52] found an algorithm that computes explicit formulas for the curve E' and the rational maps of the isogeny $\phi : E \to E'$.

Remark. Note that the kernel of the pth power Frobenius endomorphism is $\{\mathcal{O}\}$, a characteristic that it shares with other (purely) inseparable isogenies. On the contrary, separable isogenies are characterised by their kernel (not uniquely). In following sections we use Theorem 4.11 together with Velu's formulas [52] to convert a non-trivial kernel back into a separable isogeny. Although the separable isogeny we retrieve is not unique, our point of interest, the codomain of the isogeny, is unique up to $\mathbb{F}_p$-isomorphism, which is all we need. Therefore, inseparable isogenies are not very relevant to our use case and separability is not discussed formally in this thesis. For more information regarding the subject the reader is referred to [40, Section II.2] or [48, Sections 9.6, 9.7]. The fact that the kernel of our isogenies is non-trivial, can be seen from [48, Corollary 9.7.3] and [40, Corollaries III.5.3-III.5.5].

Definition 4.12. The *trace* of the pth power Frobenius endomorphism π of an elliptic curve E is the integer t satisfying $\#E(\mathbb{F}_p) = p + 1 - t$. We often call t the *trace of Frobenius* of E.

Theorem 4.13. *Let E be an elliptic curve over $\mathbb{F}_p$. The pth power Frobenius endomorphism π over E satisfies $\pi^2 - [t]\pi + [p] = 0$, that is, the composition of these functions is the zero isogeny.*

Proof. See [40, Theorem V.2.3.1(b)]. □

Another way of stating this theorem is that for **any** point P in $E(\overline{\mathbb{F}}_p)$ (thus even the ones defined over the algebraic closure of $\mathbb{F}_p$) we know that $\pi(\pi(P)) - [t]\pi(P) + [p]P = \mathcal{O}$ as noted in [53, p. 6].

Let $E : y^2 = x^3+3x+2$ be an elliptic curve defined over $\mathbb{F}_5$ and let $\mathbb{F}_{5^2} := \mathbb{F}_5[s]/(s^2+4s+2)$. Furthermore, we define the point $P = (s+4, s+3) \in E(\mathbb{F}_{5^2})$.
For all points $Q := (Q_x, Q_y) \in E(\mathbb{F}_5)$ we have $\pi(Q) = (Q_x^5, Q_y^5) = Q \in E(\mathbb{F}_5)$ by Fermat's little theorem (Theorem 5.3). However, for our point $P = (s+4, s+3) \in E(\mathbb{F}_{5^2})$ we have that $\pi(P) = (4s, 4s+4) \neq P$, and that $\pi(P) = (4s, 4s+4) \in E(\mathbb{F}_{5^2})$. We apply π again to give $\pi^2(P) := \pi(\pi(P))$, essentially performing the map $(x, y) \mapsto (x^{5^2}, y^{5^2})$, to find that $\pi^2(P) = (s+4, s+3) = P$. In fact, one can show that for any $x \in \mathbb{F}_{5^2}$ we have that $x^{5^2} \equiv x$, which implies that all points in $E(\mathbb{F}_{5^2})$ are fixed by applying π^2.
Now, Theorem 4.13 states that $\pi^2 - [t]\pi + [5] = 0$ must hold. For any point $P \in E(\mathbb{F}_{5^2})$ we already know that $\pi^2(P) = P$. We will verify the equation for our point $P := (s+4, s+3) \in E(\mathbb{F}_{5^2})$ by checking whether $\pi(\pi(P)) - [t]\pi(P) + [5]P = \mathcal{O}$ holds. The trace of Frobenius of E equals 1 as $\#E(\mathbb{F}_p) = 5 = 5 + 1 - 1$. Therefore, the equation reduces to checking whether $P - \pi(P) + [5]P = \mathcal{O}$. And indeed $[5+1]P = (4s, 4s+4) = \pi(P)$. We have thus shown that Theorem 4.13 holds for our choice of $P \in E(\overline{\mathbb{F}}_5)$.

Definition 4.14. An elliptic curve E defined over $\mathbb{F}_p$ is called *supersingular* if and only if the trace of Frobenius equals 0, otherwise it is called *ordinary* [54, Theorem 13.4]. Furthermore, the trace of Frobenius is preserved under non-zero isogenies by Theorem 4.1. Therefore, supersingular elliptic curves are never isogenous to ordinary elliptic curves.

The distinction between supersingular and ordinary elliptic curves is important as CSIDH only uses supersingular elliptic curves in their encryption scheme.

The polynomial $x^2 - tx + p \in \mathbb{Z}[x]$ is called the Frobenius polynomial (remember that π satisfies $\pi^2 - [t]\pi + [p] = 0$). From Hasse's theorem [55] we know that $|t| \leq 2\sqrt{p}$, and therefore $t^2 - 4p < 0$. Solving the Frobenius polynomial shows that its roots are imaginary numbers. Those roots can thus *extend* the rationals $\mathbb{Q}$. Building on this, we define the number field $K = \mathbb{Q}(\pi)$, where π is a root of the Frobenius polynomial. Previously we saw that every multiplication-by-m map for $m \in \mathbb{Z}$ is an endomorphism, likewise, the pth power Frobenius endomorphism π of an elliptic curve is also an endomorphism. Thus, we know that the order $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$ for arbitrary elliptic curves E over $\mathbb{F}_p$. Using [54, Theorems 13.6-13.8], we find that ordinary elliptic curves satisfy $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$, implying that $\mathrm{End}(E)$ is an order in the number field K.

4.5 Ideals Acting on Elliptic Curves

This section starts by introducing the concept of ideals acting on $\mathbb{F}_p$-isomorphism classes of elliptic curves; the properties and consequences of these definitions along with their proofs can be found in Section 4.5.1. A visualisation of the action of ideals on $\mathbb{F}_p$-isomorphism classes of elliptic curves can be found in Section 4.5.2, which introduces the concept of isogeny graphs.

Choose an elliptic curve E defined over some fixed finite field $\mathbb{F}_p$ for $p > 3$ prime. Calculate the trace t of the pth power Frobenius endomorphism. Let π be a root of the Frobenius polynomial $x^2 - tx + p$ and define the imaginary quadratic number field $K = \mathbb{Q}(\pi)$.

Let A be a subring of $\mathrm{End}(E)$, that is, $A \subseteq \mathrm{End}(E)$. Then, any $\alpha \in A$ represents an endomorphism of the elliptic curve E, thus $\alpha : E \to E$. Using α we can map every point $P \in E$

to the point $\alpha(P) \in E$. In particular, if some $\alpha \in A$ can be written in the form $a+b\pi$ for $a, b \in \mathbb{Z}$, that is, $\alpha = a + b\pi \in \mathbb{Z}[\pi]$, this sends P to the point $\alpha(P) = (a + b\pi)(P) = [a]P + [b]\pi(P)$.

Definition 4.15. Let $\mathfrak{a}$ be a non-zero ideal of $\mathbb{Z}[\pi]$. We define $\mathfrak{a}E$ to be the $\mathbb{F}_p$-isomorphism class of elliptic curves determined by the codomain of an isogeny $\phi : E \to \mathfrak{a}E$ satisfying

$$\ker \phi = \{P \in E : \alpha(P) = \mathcal{O} \text{ for all } \alpha \in \mathfrak{a}\}.$$

The existence of such an isogeny where the codomain is unique up to $\mathbb{F}_p$-isomorphism is guaranteed by Theorem 4.17. Note that ϕ maps precisely the points P to the point at infinity which all elements of the ideal $\mathfrak{a}$ map to the point at infinity. In fact, we only need to verify that the generators of $\mathfrak{a}$ map P to the point at infinity (as the endomorphism ring is a ring).

As we will see in Lemma 4.20, all ideals in the same ideal class (assuming that $\mathbb{Z}[\pi] = \mathcal{O}_K$) give the same $\mathbb{F}_p$-isomorphism class. Therefore, instead of speaking of the action of an ideal $\mathfrak{a}$ on an $\mathbb{F}_p$-isomorphism class, we often speak of the action of an ideal class on $\mathbb{F}_p$-isomorphism classes of elliptic curves, denoting $\mathfrak{a}E$ as $[\mathfrak{a}]E$.

Let E be the elliptic curve $E : y^2 = x^3 + x + 6$ over $\mathbb{F}_7$. Then $\#E(\mathbb{F}_7) = 11 = 7 + 1 - (-3)$, implying that $t = -3$. Our Frobenius polynomial becomes $x^2 + 3x + 7 = 0$.
Take $K = \mathbb{Q}(\pi)$ where π is the root of $x^2 + 3x + 7$. The ideal (3) is inert in K as $x^2 + 3x + 7$ is irreducible in $\mathbb{F}_3[x]$.
We want to apply the ideal $\mathfrak{a} = (3)$ to the elliptic curve E to get $\mathfrak{a}E$. To do this we aspire to find the set $\ker \phi = \{P \in E : [3]P = \mathcal{O}\}$ as $3 \in \mathfrak{a}$ generates the ideal $\mathfrak{a}$. The isogeny ϕ can be found by evaluating:

```
sage: E = EllipticCurve(GF(7), [1, 6])
sage: E.isogeny(E.scalar_multiplication(3).kernel_polynomial())
```

It turns out that the codomain of this isogeny is the elliptic curve $\mathfrak{a}E : y^2 = x^3 + 4x + 6$. Note that the elliptic curve $\mathfrak{a}E$ is isomorphic to the elliptic curve E due to Theorem 4.8 with $u = 3$. Since $\mathcal{O}_K$ is a principal ideal domain (where only one ideal class exists) and $\mathbb{Z}[\pi] = \mathcal{O}_K$ we can see from Lemma 4.20 that for all ideals $\mathfrak{a}$ of $\mathbb{Z}[\pi]$, the curve E will be $\mathbb{F}_p$-isomorphic to $\mathfrak{a}E$ as the ideal classes $[(1)]$ and $[\mathfrak{a}]$ are identical.

Define $E : y^2 = x^3 + x + 3$ over $\mathbb{F}_7$, the Frobenius polynomial is $x^2 - 2x + 7 = 0$. Let π be a root of $x^2 + 2x + 7$ (and denote the pth power Frobenius endomorphism) and define the order $\mathbb{Z}[\pi]$ of $\mathbb{Q}(\pi)$. We have that (2) factors in $\mathbb{Z}[\pi]$ as $(2) = (2, \pi - 1)^2 = \mathfrak{p}_2^2$. This example aims to find an elliptic curve E' in the same $\mathbb{F}_p$-isomorphism class as $\mathfrak{p}_2 E$. To this end, we will compute the intersection of the two sets $S_2 := \{P \in E : [2]P = \mathcal{O}\}$ and $S_{\pi-1} := \{P \in E : \pi(P) - P = \mathcal{O}\}$ as for the isogeny $\phi : E \to \mathfrak{p}_2 E$ we have that $\ker \phi = S_2 \cap S_{\pi-1}$.
First, we compute $S_{\pi-1}$, for any $P \in E$ we see that $\pi(P) - P = \mathcal{O}$ is equivalent to $\pi(P) = P$. Since P must be fixed by applying π, we see that $S_{\pi-1} = E(\mathbb{F}_p)$. Therefore, $\ker \phi = \{P \in E(\mathbb{F}_p) : [2]P = \mathcal{O}\}$. All points in $\ker \phi$ are thus $\mathbb{F}_p$-rational and roots of the kernel polynomial of the multiplication-by-2 map (Theorem 4.3). Using the following code, we find that the kernel polynomial factors (into irreducible polynomials) as $(x + 2)(x^2 + 5x + 5)$.

```
sage: E = EllipticCurve(GF(7), [1, 3])
sage: E.scalar_multiplication(2).kernel_polynomial().factor()
```

Since $x + 2 \in \mathbb{F}_p[x]$ is the only factor of degree 1 (and therefore the only one providing a root in $\mathbb{F}_p$) we get that the kernel polynomial of ϕ is $x + 2$. And hence $\mathfrak{p}_2 E$, the codomain of ϕ, can be found by the following code:

```
sage: E = EllipticCurve(GF(7), [1, 3])
sage: E.isogeny(x+2)
```

Which returns that $E' \cong \mathfrak{p}_2 E : y^2 = x^3 + 6x + 3$. The curve $E' \cong \mathfrak{p}_2 E$ is not isomorphic to E as $\mathfrak{p}_2$ is a non-principal ideal.

4.5.1 Properties of Ideals Acting on Elliptic Curves

This subsection provides proofs for the action of ideals on elliptic curves. The goal is to shed light on some properties of this action so that the reader (especially one well versed in group actions) can acquire a better understanding of what is possible with these actions. Furthermore, this subsection provides a rigorous foundation which is used to define the CSIDH encryption scheme more abstractly in the next chapter.

In the remainder of this subsection we let E denote an elliptic curve defined over a finite field $\mathbb{F}_p$ for some fixed prime $p > 3$. Also, we let π denote the pth power Frobenius endomorphism of E as well as the root of the Frobenius polynomial $x^2 - tx + p$ and define the number field $\mathbb{Q}(\pi)$ with the order $\mathbb{Z}[\pi]$.

Lemma 4.16. *Let E and E' denote elliptic curves over $\mathbb{F}_p$. Let $\phi : E \to E'$ be an isogeny sending E to E'. Let π denote the pth power Frobenius endomorphism of E. Similarly, let π' denote the pth power Frobenius endomorphism of E'. Then we have $\phi \circ \pi = \pi' \circ \phi$.*

Proof. First, if ϕ is the zero isogeny, this equation holds trivially. Otherwise, by Definition 4.2, ϕ can be expressed as a rational map

$$\phi(x, y) = \left(\frac{f(x)}{k(x)}, \frac{g(x)}{h(x)} y \right),$$

with $f, k, g, h \in \mathbb{F}_p[x]$.

By the Freshman's dream [56, Example 9.42], we have that $f(x^p) = f(x)^p$ for any polynomial $f \in \mathbb{F}_p[x]$, now, $\phi \circ \pi$ is given by the rational map

$$\phi(x^p, y^p) = \left(\frac{f(x^p)}{k(x^p)}, \frac{g(x^p)}{h(x^p)} y^p \right) = \left(\frac{f(x)^p}{k(x)^p}, \frac{g(x)^p}{h(x)^p} y^p \right).$$

which equals the rational map of $\pi' \circ \phi$. □

Theorem 4.17. *There is a unique elliptic curve E' up to $\mathbb{F}_p$-isomorphism and an isogeny $\phi : E \to E'$ satisfying $\ker \phi = \{P \in E : \alpha(P) = \mathcal{O}$ for all $\alpha \in \mathfrak{a}\}$ for any non-zero ideal $\mathfrak{a}$ of $\mathbb{Z}[\pi]$.*

Proof. We need to show that the kernel of the isogeny ϕ as defined in Definition 4.15 satisfies all conditions of G in Theorem 4.11. Let G denote the kernel of ϕ, we must thus show that G is a finite (follows from the fact that $\mathfrak{a}$ is non-zero) subgroup of the points on E such that for all $P \in G$ we have that $\pi(P) \in G$, where π denotes the pth power Frobenius endomorphism.

First off, let α denote an arbitrary element of a non-zero ideal $\mathfrak{a}$ of $\mathbb{Z}[\pi]$. Now, G is naturally a subset of the points on E. Furthermore, G is a subgroup of E, since if $P \in G$ and $Q \in G$, then $\alpha(P) = \alpha(Q) = \mathcal{O} = \alpha(P) + \alpha(Q) = \alpha(P + Q)$, such that $P + Q \in G$, showing that the $+$-operation of E restricts to G (Definition 0.2). Next, for all $P \in G$ we have that $\alpha(P) = \mathcal{O}$, such that $\mathcal{O} = \alpha(P) = \pi(\alpha(P)) = \alpha(\pi(P))$, giving that $\pi(P) \in G$. □

For any elliptic curve E' isogenous to E, we have that $\#E'(\mathbb{F}_p) = \#E(\mathbb{F}_p)$ by Theorem 4.1. Therefore, the Frobenius polynomial of E will equal the Frobenius polynomial of E'. Hence, we can not only identify the order $\mathbb{Z}[\pi]$ as a subring of $\mathrm{End}(E)$ (where π denotes the pth power Frobenius endomorphism of E), but also as a subring of $\mathrm{End}(E')$ (this time π denotes the pth power Frobenius endomorphism of E').

Theorem 4.18. *Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathbb{Z}[\pi]$ be non-zero ideals. Using the notation from Definition 4.15 we have that $(\mathfrak{a} \cdot \mathfrak{b})E$, $\mathfrak{a}(\mathfrak{b}E)$, and $\mathfrak{b}(\mathfrak{a}E)$, all belong to the same $\mathbb{F}_p$-isomorphism class. That is, we can define a left group action where the group of ideals acts on a set of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$.*

Proof. For any elliptic curve E' isogenous to E, and any non-zero ideal $\mathfrak{c}$ of $\mathbb{Z}[\pi]$, after identifying π with the pth power Frobenius endomorphism of E', we get an elliptic curve $\mathfrak{c}E'$ and an isogeny $\phi_{\mathfrak{c}} : E' \to \mathfrak{c}E'$ associated with $\mathfrak{c}$. Also, let the symbol $\forall$ denote "for all", we have

$$\begin{aligned}
\ker(\phi_{\mathfrak{a}} \circ \phi_{\mathfrak{b}}) &= \{P \in E : \phi_{\mathfrak{a}}(\phi_{\mathfrak{b}}(P)) = \mathcal{O}\} \\
&= \{P \in E : (\alpha \circ \phi_{\mathfrak{b}})(P) = \mathcal{O}, \forall \alpha \in \mathfrak{a}\} \\
&= \{P \in E : (\phi_{\mathfrak{b}} \circ \alpha)(P) = \mathcal{O}, \forall \alpha \in \mathfrak{a}\} \\
&= \{P \in E : \alpha(P) \in \ker(\phi_{\mathfrak{b}}), \forall \alpha \in \mathfrak{a}\} \\
&= \{P \in E : \beta(\alpha(P)) = \mathcal{O}, \forall \alpha \in \mathfrak{a}, \forall \beta \in \mathfrak{b}\} \\
&= \{P \in E : (\alpha \cdot \beta)(P) = \mathcal{O}, \forall \alpha \in \mathfrak{a}, \forall \beta \in \mathfrak{b}\} \\
&= \{P \in E : \gamma(P) = \mathcal{O}, \forall \gamma \in (\mathfrak{a} \cdot \mathfrak{b})\} \\
&= \ker(\phi_{\mathfrak{a} \cdot \mathfrak{b}}).
\end{aligned}$$

Therefore, first applying $\phi_{\mathfrak{b}} : E \to \mathfrak{b}E$ and then $\phi_{\mathfrak{a}} : \mathfrak{b}E \to \mathfrak{a}(\mathfrak{b}E)$ is the same as applying $\phi_{\mathfrak{a} \cdot \mathfrak{b}} : E \to (\mathfrak{a} \cdot \mathfrak{b})E$. For the trivial ideal (1) we know that $(1)E = E$ as it sends all points $P \in E$ to themselves. Since $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a}$, the theorem follows. □

Lemma 4.19. *Let $\mathfrak{a} \subseteq \mathbb{Z}[\pi]$ be a non-zero principal ideal. We have $E \cong \mathfrak{a}E$.*

Proof. Let α denote the generator of the principal ideal $\mathfrak{a}$, i.e., $\mathfrak{a} = (\alpha)$. Let $\phi : E \to \mathfrak{a}E$ be the isogeny with kernel $\{P \in E : \beta(P) = \mathcal{O} \text{ for all } \beta \in \mathfrak{a}\}$. This kernel is identical to the set $\{P \in E : \alpha(P) = \mathcal{O}\}$. The endomorphism α has the same kernel as the isogeny ϕ, proving that the codomain of ϕ is $\mathbb{F}_p$-isomorphic to E. □

Lemma 4.20. *Let $\mathfrak{a}, \mathfrak{b} \subseteq \mathbb{Z}[\pi]$ be non-zero ideals. If $[\mathfrak{a}] = [\mathfrak{b}]$, that is, $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same ideal class, we have $\mathfrak{a}E \cong \mathfrak{b}E$.*

Proof. Assume that there are non-zero $\alpha, \beta \in \mathbb{Z}[\pi]$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. For arbitrary elliptic curves E we then have that $((\alpha)\mathfrak{a})E \cong ((\beta)\mathfrak{b})E$. From Theorem 4.18 we deduce that $(\alpha)(\mathfrak{a}E) \cong (\beta)(\mathfrak{b}E)$ must hold. Now Lemma 4.19 gives that $\mathfrak{a}E \cong \mathfrak{b}E$.

It rests us to prove our original assumption. First assume that it is false, thus, for any non-zero $\alpha, \beta \in \mathbb{Z}[\pi]$ we never have $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. In that case $[(\alpha)\mathfrak{a}] \neq [(\beta)\mathfrak{b}]$, which would imply that $[(\alpha)] + [\mathfrak{a}] \neq [(\beta)] + [\mathfrak{b}]$ and consequently $[\mathfrak{a}] \neq [\mathfrak{b}]$, which is a contradiction. □

Theorem 4.21. *The action of the group of ideal classes $\mathrm{Cl}(\mathbb{Z}[\pi])$ on a set of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ is a group action. Therefore, principal ideals $\mathfrak{a}$ of $\mathbb{Z}[\pi]$ satisfy $[\mathfrak{a}]E \cong E$, and we have that $[\mathfrak{a} \cdot \mathfrak{b}]E \cong [\mathfrak{a}]([\mathfrak{b}]E) \cong [\mathfrak{b}]([\mathfrak{a}]E)$ holds for arbitrary non-zero ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathbb{Z}[\pi]$.*

Proof. From Lemma 4.19 we already know that the identity element of $\mathrm{Cl}(\mathbb{Z}[\pi])$, the set of principal ideals, acts on E in a similar fashion as the ideal (1) does, namely trivially. From Theorem 4.18 and Lemma 4.20 we deduce that $[\mathfrak{a} \cdot \mathfrak{b}]E \cong [\mathfrak{a}]([\mathfrak{b}]E) \cong [\mathfrak{b}]([\mathfrak{a}]E)$. Therefore, $\mathrm{Cl}(\mathbb{Z}[\pi])$ indeed defines a group action on a set of isomorphism classes of elliptic curves defined over $\mathbb{F}_p$. □

Remember that for supersingular elliptic curves over $\mathbb{F}_p$ (which we defined in Definition 4.14) the trace of Frobenius equals 0 (as long as $p > 3$ is prime). Therefore, the Frobenius polynomial of such an elliptic curve is of the form $x^2 + p \in \mathbb{Z}[x]$ and $\mathbb{Z}[\pi] = \mathbb{Z}[\sqrt{-p}]$.

In the special case of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$ with $p \equiv 1 \pmod 4$, Theorem 4.21 translates to a free and transitive [57, Definitions 3.6, 3.8]

group action. That is, for two supersingular elliptic curves E_1, E_2 there exists an ideal $\mathfrak{a}$ such that $[\mathfrak{a}]E_1 \cong E_2$, which implies transitivity, and if $[\mathfrak{a}]E_1 \cong E_1$ then the ideal class $[\mathfrak{a}]$ must be trivial, which implies that the action must be free. In other words, the action of $\mathrm{Cl}(\mathbb{Q}(\sqrt{-p}))$ on the set of isomorphism classes of all supersingular curves defined over $\mathbb{F}_p$ is free and transitive. This fact, along with its proof, can be found in [1, Theorem 7].

4.5.2 Isogeny Graphs

Isogeny graphs help with visualising the effect of applying ideals to elliptic curves. In this subsection we will briefly look at an example of an isogeny graph and describe what it signifies.

For this example, we will look at elliptic curves defined over $\mathbb{F}_{59}$. For any $A \in \mathbb{F}_{59}$, let the curve E_A denote the elliptic curve with Montgomery coefficient A, i.e., $E_A : y^2 = x^3 + Ax^2 + x$. We will look at the isogeny graph that results from applying the ideals over 3 and 5 repetitively to the starting curve $E_0 : y^2 = x^3 + x$, see Figure 4.1.

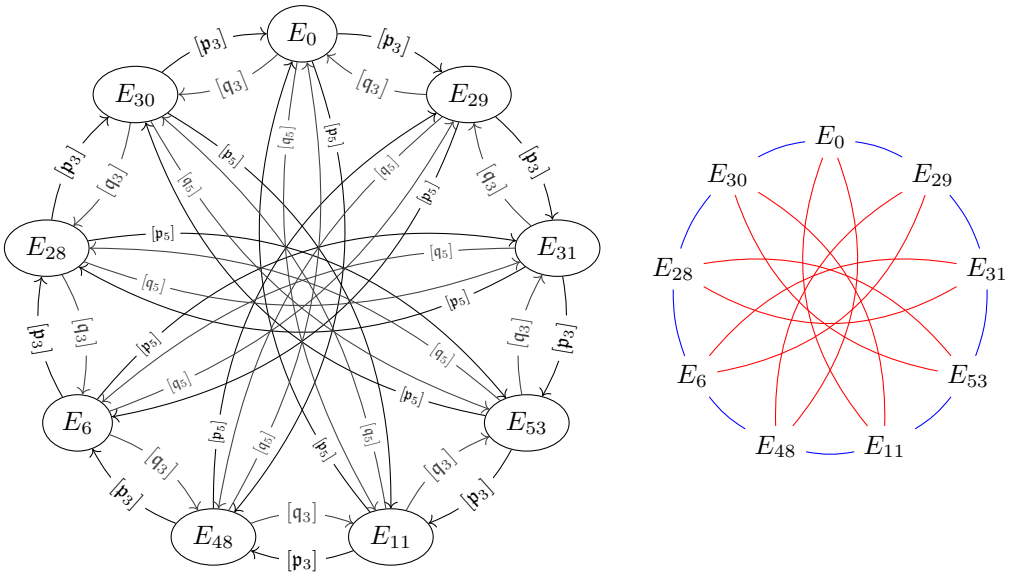

Figure 4.1: Isogeny graphs with starting curve defined by $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{59}$. Nodes in the isogeny graph represent $\mathbb{F}_{59}$-isomorphism classes of supersingular elliptic curves, denoted by the unique Montgomery curve contained in the class. Edges in the graph represent isogenies defined by the actions of the ideals over $\{3, 5\}$. The figure on the left-hand side gives a complete overview of the mappings that some ideals perform. The figure on the right-hand side is a simplified version, merging directional edges of each ideal with its conjugate.

Note that the Frobenius polynomial of E_0, which is supersingular, equals $x^2 + 59$. Therefore, we define $K = \mathbb{Q}(\sqrt{-59})$. Let $\alpha = \sqrt{-59}$, and define the order $R = \mathbb{Z}[\alpha]$ of K. Then, (3) factors in R as $(3, \alpha - 1)(3, \alpha + 1) = \mathfrak{p}_3\mathfrak{q}_3$ and $(5) = (5, \alpha - 1)(5, \alpha + 1) = \mathfrak{p}_5\mathfrak{q}_5$.

Remark. After applying an ideal to an elliptic curve E defined over $\mathbb{F}_q$, the Frobenius polynomial does not change. This is due to the fact that applying an ideal corresponds to an isogeny and Theorem 4.1 states that the resulting curve E' satisfies $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$, which gives the same trace of Frobenius.

As an example, applying the ideal $\mathfrak{p}_3$ to E_0 gives a curve isomorphic to E_{29}, i.e., $[\mathfrak{p}_3]E_0 = E_{29}$. Applying $\mathfrak{p}_3$ to E_{29} gives E_{31}, and so on until we get back to the original curve E_0. A more detailed view is given in Figure 4.1.

Chapter 5

Encryption Schemes

In today's world, secure communication has become paramount, with privacy concerns escalating. This chapter starts by delving into the concept of key exchange (in particular Diffie-Hellman Key Exchange) and how it enables two parties to establish a shared secret. Building on this foundation, we set the stage for understanding the intricacies of the CSIDH algorithm, the culmination of this thesis. Elaborating on this algorithm, we present a variant of CSIDH in Section 5.3, aimed at sparking further exploration and research in this area of cryptography.

5.1 Diffie-Hellman Key Exchange

Suppose Alice and Bob, two people living on different sides of the Earth, want to share sensitive information with each other. Ideally, they wish to send each other messages containing this information securely. However, Eve can intercept and read the contents of that message. This is something that Alice and Bob want to avoid. The Diffie-Hellman key exchange describes how, even if all messages get intercepted, only Alice and Bob are able to read its contents.

First of all, Alice and Bob need to agree on the algorithm they are going to use, an example of applying such an algorithm is listed below. Once they have done this, they can agree on initialisers of the algorithm called the *public parameters* of the key exchange. Alice then computes a *private key* that she keeps to herself, which Bob does as well. Combining public parameters and private key, the algorithm provides a *public key* that Alice sends (via public communication channels) to Bob. Bob also uses his private key and the algorithm to send a public key to Alice. Alice receives Bob's public key and Bob receives Alice's public key. The second stage of the algorithm now uses this public key in combination with their own private key to get to a *shared secret*. Shared secrets are useful, since **only** Alice and Bob know this secret, even if all messages get intercepted. Alice and Bob can use this shared secret to encrypt their sensitive data, which, as long as the shared secret stays a secret to interceptors, can only be read by Alice and Bob.

Suppose Alice and Bob want to exchange sensitive information with each other. To this end, they want to establish a shared secret. See Figure 5.1.
Alice and Bob create a public channel on which they can send messages. On it, they agree to use the Finite Field Diffie-Hellman algorithm to reach a shared secret. To set up their system they agree that they will use the modulus $p = 81233$ and the base $g = (3 \bmod p) \in \mathbb{F}_p$ (nowadays, p is typically chosen to be around 2^{3200} [58]).
Now Alice creates a random private key, which must be an integer < 81233 according to the algorithm. She chooses $a = 75629$. Likewise Bob generates the private key $b = 26921$. Following the algorithm they compute their public using their private key, Alice computes $A := g^a = (21836 \bmod p)$. Bob computes $B := g^b = (63093 \bmod p)$.

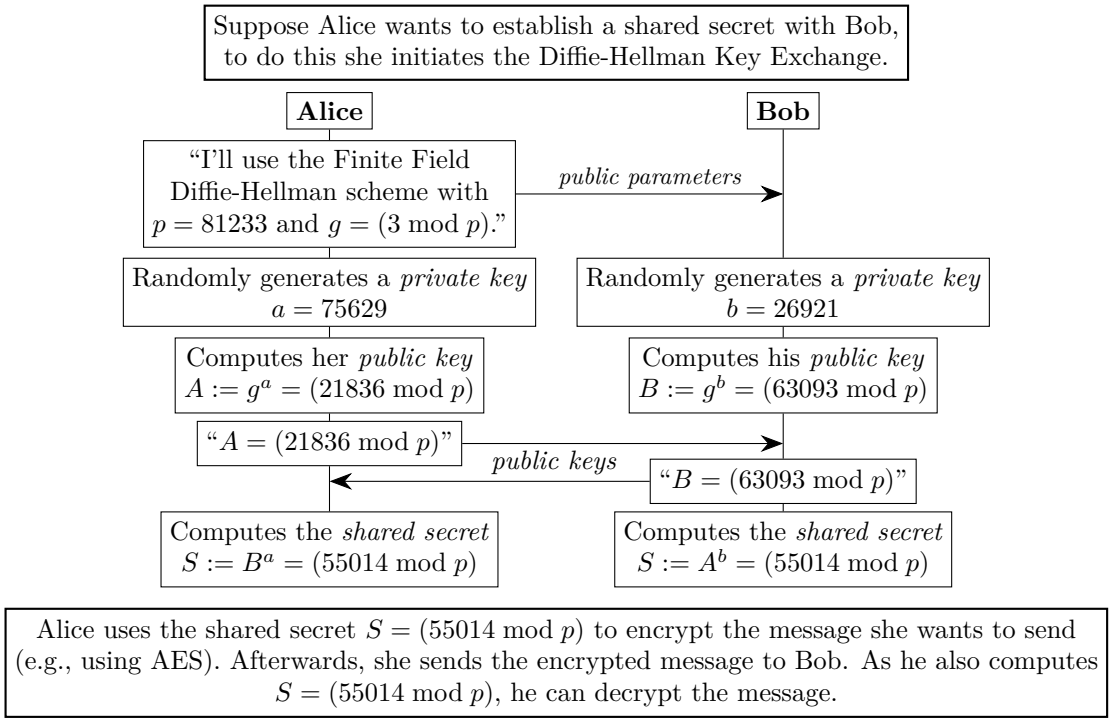

Figure 5.1: An overview of the Diffie-Hellman Key Exchange from the example. Here, an arrow represents sending data across a (public) channel.

At this point, Eve, who intercepted all their messages, only knows which algorithm Alice and Bob use, together with initialisers $p = 81233$ and $g = (3 \bmod p)$.
Bob now sends his result B to Alice and Alice sends A to Bob.
Eve is happy, she intercepts the message and knows that $A = (21836 \bmod p)$ and $B = (63093 \bmod p)$. However, she remains oblivious to the values of a and b which are presumed to be difficult to figure out (if p were a much larger prime) by herself.
According to the algorithm Alice now computes $S_a := B^a = (55014 \bmod p)$. Bob computes $S_b := A^b = (55014 \bmod p)$. We know that $S_a = S_b$ holds as $(g^a)^b = (g^b)^a$ for a and b integers and $g \in \mathbb{F}_p$. Thus, Alice and Bob have a shared secret $S = (55014 \bmod p)$.
Eve knows that $A = (21836 \bmod p)$ and that $B = (63093 \bmod p)$, but if p were a much larger prime it would be difficult to find the shared secret S without the private keys a or b.
Now, Alice can use the shared secret $S = (55014 \bmod p)$ and a different encryption scheme like poly-alphabetic substitution or AES encryption to encrypt her message. She can then send the encrypted message to Bob. He can then decrypt the message by using the shared secret.

To develop a new encryption scheme for the Diffie-Hellman key exchange protocol one must first specify how to generate its public parameters and private keys. The first algorithm of the encryption scheme is then applied to the public parameters and private keys to compute the public keys. The computed public key is then exchanged with the other person. Upon receiving the key, the person uses it as an input for the second stage of the algorithm which finds a shared secret. If a shared secret is obtained the encryption scheme is finalised.

Depending on the strength of the encryption the shared secret is difficult or extremely difficult for an eavesdropper/interceptor Eve to figure out. The strength of certain encryption schemes is not discussed further in this thesis.

5.2 CSIDH

This section describes CSIDH [1] and their encryption scheme. In Table 5.1 a small example of the encryption scheme is worked out.

Initialisation. To start, a prime of the form $p = 4\ell_1 \cdot \ell_2 \cdots \ell_n - 1$ is needed where ℓ_i are small distinct odd primes and $n \in \mathbb{Z}_{\geq 1}$. CSIDH used a 512-bit prime p [1, Section 8.1], i.e., a prime p satisfying $2^{511} \leq p < 2^{512}$. This prime is a public parameter of the encryption scheme. We also define the starting curve to be the (supersingular) elliptic curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$ and define the order $R = \mathbb{Z}[\pi]$ of $\mathbb{Q}(\pi)$ obtained by adjoining a root π of $x^2 + p$ to $\mathbb{Q}$.
Private Key Generation. The private key is an n-tuple $(e_1, \ldots, e_n)$ of integers representing exponents, each sampled randomly from a range $\{-m, \ldots, m\}$ where $2m + 1 \geq \sqrt[n]{\#\mathrm{Cl}(R)}$.
As $x^2 + p = x^2 - 1 = (x - 1)(x + 1)$ in $\mathbb{F}_{\ell_i}[x]$ we get that (ℓ_i) factors in R as $\mathfrak{l}_i\overline{\mathfrak{l}_i}$ where $\mathfrak{l}_i := (\ell_i, \pi - 1)$ and $\overline{\mathfrak{l}_i} := (\ell_i, \pi + 1)$.
Using the n-tuple we define the ideal class $[\mathfrak{a}] = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \in \mathrm{Cl}(R)$, where $[\mathfrak{l}_i^{-1}] := [\overline{\mathfrak{l}_i}]$.
Now, Alice generates a private key and applies $[\mathfrak{a}]$ to the starting curve E_0 and finds an $\mathbb{F}_p$-isomorphism class containing the Montgomery curve (Section 4.3) equal to $E_A = [\mathfrak{a}]E_0 : y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_p$. Bob does the same by generating a private key and applying its respective ideal class to the starting curve, obtaining a different curve E_B. At this point Alice and Bob send their values of A and B to each other over a public channel.
Computing the Shared Secret. Now Alice computes $E_{S_A} := [\mathfrak{a}]E_B$ and Bob computes $E_{S_B} := [\mathfrak{b}]E_A$. Applying ideal classes is commutative (as can be seen in Figure 4.1 and from Theorem 4.18 or Theorem 4.21). Thus, we in fact have $E_S := E_{S_A} = E_{S_B}$. Hence, Alice and Bob share a secret S determined by the elliptic curve $E_S = [\mathfrak{a}][\mathfrak{b}]E_0 = [\mathfrak{b}][\mathfrak{a}]E_0 : y^2 = x^3 + Sx^2 + x$.

		Some Possible Actions $[\mathfrak{a}]$								
		0	$[\mathfrak{l}_3]$	$[\mathfrak{l}_3^2]$	$[\mathfrak{l}_3^3]$	$[\mathfrak{l}_3^4]$	$[\mathfrak{l}_3^5]$	$[\mathfrak{l}_3^6]$	$[\mathfrak{l}_3^7]$	$[\mathfrak{l}_3^8]$
		0	$[\mathfrak{l}_5^2]$	$[\mathfrak{l}_5^4]$	$[\mathfrak{l}_5^6]$	$[\mathfrak{l}_5^8]$	$[\mathfrak{l}_5]$	$[\mathfrak{l}_5^3]$	$[\mathfrak{l}_5^5]$	$[\mathfrak{l}_5^7]$
		$[\overline{\mathfrak{l}_3}\mathfrak{l}_5^2]$	$[\mathfrak{l}_3^4\mathfrak{l}_5^3]$	$[\mathfrak{l}_3\mathfrak{l}_5]$	$[\overline{\mathfrak{l}_3^2}\mathfrak{l}_5]$	$[\mathfrak{l}_3^3\mathfrak{l}_5^2]$	$[\overline{\mathfrak{l}_3}\mathfrak{l}_5^3]$	$[\mathfrak{l}_3\mathfrak{l}_5]$	$[\mathfrak{l}_3^2\mathfrak{l}_5]$	$[\mathfrak{l}_3^2\mathfrak{l}_5^3]$
		Alice's Resulting Montgomery Coefficient A								
		0	29	31	53	11	48	6	28	30
Bob's Coefficient B	0	0	29	31	53	11	48	6	28	30
	29	29	31	53	11	48	6	28	30	0
	31	31	53	11	48	6	28	30	0	29
	53	53	11	48	6	28	30	0	29	31
	11	11	48	6	28	30	0	29	31	53
	48	48	6	28	30	0	29	31	53	11
	6	6	28	30	0	29	31	53	11	48
	28	28	30	0	29	31	53	11	48	6
	30	30	0	29	31	53	11	48	6	28

Table 5.1: Table of shared secrets with $p = 59 = 4 \cdot 3 \cdot 5 - 1$. One can use Figure 4.1 to verify this table.

Let ℓ_1 through ℓ_{11} denote the first 11 odd primes (thus the primes from 3 to 37). Then $p := -1+4\prod_{i=1}^{11}\ell_i = 14841476269619$. Define the starting curve $E_0 : y^2 = x^3+x$ over $\mathbb{F}_p$. We know that the Frobenius polynomial of E_0 equals π^2+p, thus we define $K = \mathbb{Q}(\sqrt{-p})$ and the order $R = \mathbb{Z}[\sqrt{-p}]$.
Evaluating*

```
sage: p = 4*3*5*7*11*13*17*19*23*29*31*37-1
sage: E0 = EllipticCurve(GF(p), [1, 0])
sage: K.<pi> = NumberField(E0.frobenius_polynomial())
sage: K.order(pi).class_number()
```

gives that $\#\mathrm{Cl}(R) = 7617567$. Hence, the isogeny graph that we are working on will have at most 7617567 nodes by Theorem 4.21 (in fact, it has exactly that many nodes).
Moving on with the encryption scheme, we must thus choose a positive integer m such that $2m+1 \geq \sqrt[11]{7617567} \approx 4.223$, we take $m = 2$.
Now, Alice generates a private key by choosing $n = 11$ random integers in the range $\{-2,-1,0,1,2\}$. Let us say that she generates the tuple $(1,0,0,0,-2,2,0,0,-2,1,0)$. She now has to compute $[\mathfrak{a}]E_0 = [\mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_{11}^{e_{11}}]E_0$. Note that in this case

$$\mathfrak{a} = \mathfrak{l}_1\cdot\overline{\mathfrak{l}_5}^2\cdot\mathfrak{l}_6^2\cdot\overline{\mathfrak{l}_9}^2\cdot\mathfrak{l}_{10} = (3,\pi-1)\cdot(13,\pi+1)^2\cdot(17,\pi-1)^2\cdot(29,\pi+1)^2\cdot(31,\pi-1).$$

As an example, we will calculate $[\mathfrak{l}_1]E_0 = [(3,\pi-1)]E_0$.
From Section 4.5 we know that the action of the ideal $\mathfrak{l}_1 = (3,\pi-1)$ is determined by an isogeny $\phi : E \to \mathfrak{l}_1 E$ satisfying $\ker\phi = \{P\in E : [3]P = \mathcal{O}\}\cap\{P\in E : \pi(P)-P = \mathcal{O}\}$. Now, if $\pi(P)-P = \mathcal{O}$, then we will have that $\pi(P) = P$, and we know that π only fixes the points $E(\mathbb{F}_p)$ on the elliptic curve. Hence, $\ker\phi = E(\mathbb{F}_p)\cap\{P\in E : [3]P = \mathcal{O}\}$. All the points in $\{P\in E : [3]P = \mathcal{O}\}$ will have to have an x-coordinate that is a root of $x^4+2x^2+9894317513079 \in \mathbb{F}_p[x]$ which we get from evaluating

```
sage: E0.scalar_multiplication(3).kernel_polynomial()
```

in the same cell as before (we note that this particular computation is relatively slow, for a faster approach see the code in Appendix A). This polynomial factors (into monic irreducible polynomials) as $(x+5672940366292)(x+9168535903327)(x^2+6967967836332)$ which we get from evaluating:

```
sage: x = polygen(GF(p))
sage: (x^4 + 2*x^2 + 9894317513079).factor()
```

Since we are only looking for points in $E(\mathbb{F}_p)$ that are a root of this polynomial, we thus find that the x-coordinate of any point in $\ker\phi$ can only be $(-5672940366292 \bmod p)$ or $(-9168535903327 \bmod p)$. We note that for every point in $E(\mathbb{F}_p)$, the y-coordinate also has to be in $\mathbb{F}_p$. We have that $y^2 = x^3+x$, so that we can determine whether our possible x-coordinates result in y-coordinates in $\mathbb{F}_p$. Using SageMath [2], we verify whether x^3+x is a square in $\mathbb{F}_p$ for each possible choice of x.

```
sage: GF(p)((-5672940366292)^3 + (-5672940366292)).is_square()
sage: GF(p)((-9168535903327)^3 + (-9168535903327)).is_square()
```

We get `False` and `True`, respectively. Therefore, the isogeny ϕ is given by the kernel polynomial $x+9168535903327$.

```
sage: E0.isogeny(x + 9168535903327)
```

which has codomain $E' \cong [\mathfrak{l}_1]E : y^2 = x^3+13583108954376x+8730919815582$. The $\mathbb{F}_p$-isomorphism class can be represented by a Montgomery curve, which we compute using the following code.

```
sage: EllipticCurve(GF(p), [13583108954376, 8730919815582]).montgomery_model()
```

We find the Montgomery curve $E_A : y^2 = x^3 + 3475446217924x^2 + x$.
Now that we have seen the action of $[\mathfrak{l}_1]$ in more detail, we use the computer code from Appendix A to evaluate $[\mathfrak{a}]E = [\mathfrak{l}_1\overline{\mathfrak{l}_5}^2\mathfrak{l}_6^2\overline{\mathfrak{l}_9}^2\mathfrak{l}_{10}]E$ and put the resulting curve in Montgomery form to get $[\mathfrak{a}]E : y^2 = x^3 + 13973923058365x^2 + x$. Thus, Alice will send $A = 13973923058365$ as her public key to Bob. If everything goes well, then with an example using large enough primes (see remark below), no one can figure out that precisely the ideal class $[\mathfrak{a}]$ was applied to the starting curve to get this public key.
Bob also generates a private key and finds the Montgomery curve $[\mathfrak{l}_2^2\mathfrak{l}_3\overline{\mathfrak{l}_5}^2\mathfrak{l}_6\overline{\mathfrak{l}_7}\mathfrak{l}_8^2]E \cong E_B : y^2 = x^3 + 2115215140719x^2 + x$. And thus send his public key $B = 2115215140719$ to Alice.
Alice receives Bob's public key $B = 2115215140719$ and computes $[\mathfrak{a}]E_B : y^2 = x^3 + 12546545727400x^2 + x$, similarly, Bob computes $[\mathfrak{b}]E_A : y^2 = x^3 + 12546545727400x^2 + x$. That is, Alice and Bob compute the shared secret $S = 12546545727400$.

*Only a single SageMath shell should be opened as some commands we present rely on earlier definitions.

Remark. Note that if Eve tries all shared secrets, i.e., she tries $S = 0$, $S = 1$, $S = 2$, ..., $S = p$, she will eventually find $S = 12546545727400$ and crack the encryption of Alice and Bob. CSIDH recommends using at least a 512-bit prime p. To put things in perspective, in [1, Section 8.1] they used

$$\begin{aligned} p = {} & 5326738796327623094747867617954605554069371494832722337612 \cdot \ldots \\ & 4466420540095600265765376268921130263812536246269416439494 \cdot \ldots \\ & 4479266288124162137328894288028806565 9. \end{aligned}$$

If Eve wants to check all shared secrets up to this prime p, using all existing computers of the entire world, each of which could check a single shared secret per a nanosecond, then it would still take her longer than the age of the universe.

5.3 Variant of CSIDH

In this final section we present another encryption scheme based on CSIDH. We did not find any mentions of this encryption scheme, and therefore included it in this thesis. In this section you can find proofs of various theorems regarding this variant of CSIDH. In the final subsection of this chapter, we provide a method to break this encryption scheme, given an oracle that can solve CSIDH.

Instead of denoting the isomorphism classes by their Montgomery representative we remove this restriction entirely by considering two $\mathbb{F}_p$-isomorphic elliptic curves as distinct. As a consequence, we do not let ideal classes act on isomorphism classes of elliptic curves, but let the ideals themselves act on elliptic curves without reducing them in their isomorphism class.

In this encryption scheme we denote elliptic curves (which we define over $\mathbb{F}_p$ with $p > 3$ prime) in short Weierstrass form as $E_{A,B} : y^2 = x^3 + Ax + B$. Therefore, an elliptic curve $E'_{A',B'} : y^2 = x^3 + A'x + B'$ is only considered to be equal to $E_{A,B}$ if and only if $A' = A$ and $B' = B$.

Initialisation. Find a prime of the form $p = 4\ell_1 \cdot \ell_2 \cdots \ell_n - 1$ with ℓ_i distinct odd primes and $n \geq 1$. Define the starting curve to be $E_{1,0} : y^2 = x^3 + x$ over $\mathbb{F}_p$ and define the order $\mathbb{Z}[\pi]$ of $\mathbb{Q}(\pi)$, where π is a root of $x^2 + p$.

Private Key Generation. The private key is a $2n$-tuple $(e_1, \dots, e_{2n})$ of integers representing exponents, each sampled randomly from a range[†] $\{0, \dots, m\}$ with $m \in \mathbb{Z}_{>0}$. Now, using the $2n$-tuple we define the ideal (and not the ideal class!) $\mathfrak{a} = \mathfrak{l}_1^{e_1}\overline{\mathfrak{l}_1}^{e_2} \cdots \mathfrak{l}_n^{e_{2n-1}}\overline{\mathfrak{l}_n}^{e_{2n}}$ where $\mathfrak{l}_i := (\ell_i, \pi - 1)$ and $\overline{\mathfrak{l}_i} := (\ell_i, \pi + 1)$ are ideals of $\mathbb{Z}[\pi]$.
Now, Alice generates a private key and applies $\mathfrak{a}$ to the starting curve $E_{1,0}$ to obtain the elliptic curve $E_{A_1,A_2} = \mathfrak{a}E_{1,0} : y^2 = x^3 + A_1x + A_2$ with $A_1, A_2 \in \mathbb{F}_p$. Bob does the same by generating a private key and applying its respective action to the starting curve, obtaining a different elliptic curve E_{B_1,B_2}. At this point Alice and Bob send their values of A_1, A_2 and B_1, B_2 to each other over a public channel.
Computing the Shared Secret. Now Alice computes $E_{S_A} := \mathfrak{a}E_{B_1,B_2}$ and Bob computes $E_{S_B} := \mathfrak{b}E_{A_1,A_2}$. We assume that both Alice and Bob use the same implementation to compute isogenies, which preserves commutativity, so that $\mathfrak{a}(\mathfrak{b}E) = \mathfrak{b}(\mathfrak{a}E)$ holds instead of only $\mathfrak{a}(\mathfrak{b}E) \cong \mathfrak{b}(\mathfrak{a}E)$ as we have shown in Theorem 4.18. If this holds, we have $E_{S_1,S_2} := E_{S_A} = E_{S_B}$. Thus, Alice and Bob will share a secret $S = (S_1, S_2)$ determined by the curve $E_{S_1,S_2} = \mathfrak{a}\mathfrak{b}E_{1,0} = \mathfrak{b}\mathfrak{a}E_{1,0} : y^2 = x^3 + S_1x + S_2$.

[†]The bound on m is not discussed here.

Remark. The question is whether the used implementation for computing isogenies preserves commutativity. The implementation in Appendix A, using the "Kohel" algorithm from SageMath to compute isogenies from monic kernel polynomials seems to preserve commutativity, however, this fact is not proven. Proving it would require a more careful analysis of the Kohel formulae [59, Section 2.4].

In short, the CSIDH algorithm represented nodes in the isogeny graph by a Montgomery representative of the $\mathbb{F}_p$-isomorphism class, from which commutativity of applying ideal classes followed. In this variant, the nodes are not taken up to isomorphism but the operation is still (or at least seems to be) commutative as we have fixed the algorithm to compute the codomain of applying some ideal.

From Theorem 4.21 we can deduce that applying an ideal class of an ideal over some prime p and then its conjugate results in a scalar multiplication as $[\overline{\mathfrak{a}}]([\mathfrak{a}]E) \cong [(p)]E \cong E$. However, applying the scalar multiplication $\mathfrak{a} = (3)$ within this encryption scheme will give you an elliptic curve that is still isomorphic to E, but is considered to be different from E. The resulting curve can be computed using:

```
sage: from sage.schemes.elliptic_curves.ell_curve_isogeny import compute_codomain_kohel
sage: compute_codomain_kohel(E, E.scalar_multiplication(3).kernel_polynomial())
```

or can be evaluated using Theorem 5.6.

We evaluate the same example as in Section 5.2 with our new encryption scheme. If the reader wants to try to do this computation for themselves they would need to remove all 4 occurrences of `.montgomery_model()` in Appendix A before running the code.
We again take $p = 14841476269619$ and let $E_{1,0} : y^2 = x^3 + x$ be our starting curve defined over $\mathbb{F}_{14841476269619}$.
Alice applies $\mathfrak{a} = \mathfrak{l}_1 \cdot \mathfrak{l}_5^2 \cdot \mathfrak{l}_6^2 \cdot \overline{\mathfrak{l}_9^2} \cdot \mathfrak{l}_{10}$ to $E_{1,0}$ to find $E_{A_1,A_2} : y^2 = x^3 + 7807459824573x + 7370375928529$. Bob applies $\mathfrak{b} = \mathfrak{l}_2^2 \cdot \mathfrak{l}_3 \cdot \overline{\mathfrak{l}_5^2} \cdot \mathfrak{l}_6 \cdot \overline{\mathfrak{l}_7} \cdot \mathfrak{l}_8^2$ to $E_{1,0}$ to find $E_{B_1,B_2} : y^2 = x^3 + 6302721679322x + 10110512071156$. Alice and Bob exchange their public keys $(A_1, A_2) = (17807459824573, 7370375928529)$ and $(B_1, B_2) = (6302721679322, 10110512071156)$.
Upon receiving Bob's public keys Alice applies $\mathfrak{a}$ to E_{B_1,B_2} to get $E_{S_1,S_2} : y^2 = x^3 + 12542399067944x + 2321986802072$. Similarly Bob applies $\mathfrak{b}$ to E_{A_1,A_2} to get the same elliptic curve $E_{S_1,S_2} : y^2 = x^3 + 12542399067944x + 2321986802072$. Thus, both Alice and Bob compute the shared secret $(S_1, S_2) = (12542399067944, 2321986802072)$.

In this new encryption scheme isogeny graphs have a lot more nodes compared to CSIDH. Assuming that $p \equiv 11 \pmod{12}$, Theorem 5.5 gives us that there are at most $\frac{p-1}{2}$ times as many nodes in our isogeny graph compared to CSIDH as there are $\frac{p-1}{2}$ elliptic curves in each $\mathbb{F}_p$-isomorphism class. A lower bound for the amount of nodes in the isogeny graph of our encryption scheme is given in Theorem 5.8. For $p = 59$, instead of having just 9 different nodes in the isogeny graph from Figure 4.1 we expect to have exactly $\operatorname{lcm}(29, 29) \cdot 9 = 29 \cdot 9 = 261$ nodes from Theorem 5.8.

5.3.1 Proofs Regarding Our Variant

We continue this section with some proofs regarding our encryption scheme.

Definition 5.1. A residue class $(x \bmod p) \in \mathbb{F}_p^*$ is called a *quartic residue* if there is some $a \in \mathbb{F}_p^*$ such that $a^4 \equiv x \pmod{p}$. For *sextic residues* the relation $a^6 \equiv x \pmod{p}$ must hold for some $a \in \mathbb{F}_p^*$, for *quadratic residues* $a^2 \equiv x \pmod{p}$ must hold for some $a \in \mathbb{F}_p^*$, and for *cubic residues* $a^3 \equiv x \pmod{p}$ must hold for some $a \in \mathbb{F}_p^*$.

Theorem 5.2 (Quadratic Reciprocity)**.** *Let p and q be odd positive integers with $\gcd(p, q) = 1$, and let $\left(\frac{p}{q}\right)$ denote the Jacobi symbol (see [60, Definition 1.3] and [61, p. 1]). We have that*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. See [61, pp. 5-6] and [60, Section 2]. □

Theorem 5.3 (Fermat's little theorem)**.** *For $x \in \mathbb{F}_p$ we have that $x^p = x$. Equivalently, for $(x \bmod p) \in \mathbb{F}_p$, we have that $x^p \equiv x \pmod{p}$.*

Proof. See for example [62]. □

Lemma 5.4. *Let $p \equiv 11 \pmod{12}$ be a prime number. There are $\frac{p-1}{2}$ quadratic residues in $\mathbb{F}_p^*$. These residues are also quartic and sextic residues.*

Proof. This proof is split into two parts. The first part shows that if $p \equiv 3 \pmod{4}$, then there are as many quadratic residues as there are quartic residues. The other part shows that if $p \equiv 2 \pmod{3}$, then there are $p-1$ cubic residues in $\mathbb{F}_p^*$. We know that $p \equiv 11 \pmod{12}$ satisfies both these conditions and that there are $\frac{p-1}{2}$ quadratic residues in $\mathbb{F}_p^*$ as shown in [63, Theorem 3.1]. Therefore, using these parts gives us that there are $\frac{p-1}{2}$ quartic residues in $\mathbb{F}_p^*$ and $\frac{p-1}{2}$ sextic residues in $\mathbb{F}_p^*$ (as a sixth power is the square of a cube), the fact that these residues are the same can be seen from the fact that quartic and sextic residues must also be quadratic residues.

First, if $p \equiv 3 \pmod{4}$, we know that $(-1 \bmod p)$ is not a quadratic residue from the law of quadratic reciprocity (or directly from [60, Theorem 1.6]). Therefore, for any residue class $x \in \mathbb{F}_p^*$, we either have that $(x \bmod p)$ is a quadratic residue or that $(-x \bmod p)$ is a quadratic residue. Suppose $(r \bmod p)$ is a quadratic residue (remember that there are $\frac{p-1}{2}$ quadratic residues), then there exists an $(a \bmod p) \in \mathbb{F}_p^*$ such that $r \equiv a^2 \pmod{p}$. Now, one of $(a \bmod p)$ and $(-a \bmod p)$ is a quadratic residue, so there exists some $(b \bmod p) \in \mathbb{F}_p^*$ such that $a \equiv b^2 \pmod{p}$ or $-a \equiv b^2 \pmod{p}$. But then $r \equiv a^2 \equiv (\pm a)^2 \equiv b^4 \pmod{p}$, so $(r \bmod p)$ is a quartic residue. Each quadratic residue is thus also a quartic residue, and as there cannot be more quartic residues than quadratic residues, this part is proven.

Every $p \equiv 2 \pmod{3}$ is of the form $3k+2$ with $k \in \mathbb{Z}$. Let $(x \bmod p) \in \mathbb{F}_p^*$ be arbitrary. Then by Fermat's little theorem (Theorem 5.3) we have $x^{2p-1} \equiv x^p x^{p-1} \equiv x \pmod{p}$. Substituting $3k+2$ for p then gives that $x^{6k+3} \equiv (x^{2k+1})^3 \equiv x \pmod{p}$. Therefore, $(x \bmod p)$ is a cubic residue as $a \in (x^{2k+1} \bmod p)$ satisfies $a^3 \equiv x \pmod{p}$. As our residue class $(x \bmod p) \in \mathbb{F}_p^*$ was arbitrary, there are $p-1$ cubic residues in $\mathbb{F}_p^*$, proving the theorem. □

Theorem 5.5. *Each $\overline{\mathbb{F}}_p$-isomorphism class of elliptic curves defined over $\mathbb{F}_p$ contains $p-1$ representatives of the form $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_p$. Moreover, if $p \equiv 11 \pmod{12}$, there are $\frac{p-1}{2}$ representatives of that form in each $\mathbb{F}_p$-isomorphism class.*

Proof. By Theorem 4.7 we know that two elliptic curves over $\mathbb{F}_p$ are isomorphic over $\overline{\mathbb{F}}_p$ if and only if the j-invariants of both curves are equal. Naturally, if two elliptic curves are $\mathbb{F}_p$-isomorphic, they must also be isomorphic over $\overline{\mathbb{F}}_p$ and thus have the same j-invariant (Section 4.2). If $E' : y^2 = x^3 + A'x + B'$ is an elliptic curve over $\mathbb{F}_p$, then we have $j(E) = j(E')$ if and only if

$$\frac{4A^3}{4A^3 + 27B^2} = \frac{4A'^3}{4A'^3 + 27B'^2},$$

which is equivalent to

$$A^3(4A'^3 + 27B'^2) = A'^3(4A^3 + 27B^2),$$

as for elliptic curves we have $4A^3 + 27B^2 \neq (0 \bmod p)$. Distributing the terms gives that this is in turn equivalent to $A^3B'^2 = B^2A'^3$. In other words, we are counting pairs $(A', B') \in (\mathbb{F}_p^*)^2$ such that $A^3B'^2 = B^2A'^3$.

If $A = (0 \bmod p)$ and $B = (0 \bmod p)$, then E is not an elliptic curve. Now, if only $A = (0 \bmod p)$, then A' will have to be $(0 \bmod p)$ as well, giving that $B' \in \mathbb{F}_p^*$ is arbitrary, implying that there exist $p-1$ elliptic curves E' isomorphic over $\overline{\mathbb{F}}_p$ to this choice of E. Similarly if only $B = (0 \bmod p)$, then B' has to be $(0 \bmod p)$, and the equation gives an elliptic curve E' for arbitrary $A' \in \mathbb{F}_p^*$, which has $p-1$ elements.

For the remaining case where $A \neq (0 \bmod p)$ and $B \neq (0 \bmod p)$, we note that $A^3B^{-2} \in \mathbb{F}_p^*$. If $A' = (0 \bmod p)$ or $B' = (0 \bmod p)$, the equation will not hold, or E' will not be an elliptic curve, so we can safely assume that $A', B' \in \mathbb{F}_p^*$. We have $j(E) = j(E')$ if $A^3B^{-2} = A'^3B'^{-2}$, or, upon defining $C' = A'B'^{-1} \in \mathbb{F}_p^*$, if $A^3B^{-2} = A'C'^2$. Now let $\alpha := A^3B^{-2} \in \mathbb{F}_p^*$ be arbitrary, in order to prove that there are $p-1$ elliptic curves E' isomorphic over $\overline{\mathbb{F}}_p$ to E we will show that there are $p-1$ choices for $(A', C') \in (\mathbb{F}_p^*)^2$ such that $\alpha = A'C'^2$. To this end, let $C' \in \mathbb{F}_p^*$ be arbitrary, and compute $\beta := \alpha C'^{-2} \in \mathbb{F}_p^*$. We need to have $\beta = A'$, which implies that there is only one valid choice of A' corresponding to this value of C'. Note that $C' \in \mathbb{F}_p^*$ was arbitrary, implying that there are $p-1$ choices for C' and therefore also $p-1$ elliptic curves E' that are $\overline{\mathbb{F}}_p$-isomorphic to E.

We have thus shown that there are $p-1$ elliptic curves in each $\overline{\mathbb{F}}_p$-isomorphism class. Two elliptic curves E and E' (in short Weierstrass form) are $\mathbb{F}_p$-isomorphic if E' is of the form $y^2 = x^3 + u^4Ax + u^6B$ for some $u \in \mathbb{F}_p^*$, as stated in Theorem 4.8.

For the case that only $A = (0 \bmod p)$, we found that $A' = (0 \bmod p)$ and $B' \in \mathbb{F}_p^*$ is arbitrary. However, since we require the elliptic curves to have an isomorphism over $\mathbb{F}_p$, B' must be of the form u^6B. By Lemma 5.4 there are $\frac{p-1}{2}$ distinct sextic residues modulo p. Therefore, there are precisely $\frac{p-1}{2}$ elliptic curves E' that are $\mathbb{F}_p$-isomorphic to E. Similarly, for the case that only $B = (0 \bmod p)$, we have shown that $B' = (0 \bmod p)$ holds and that $A' \in \mathbb{F}_p^*$ was arbitrary. Now A' has to satisfy $A' = u^4A$, so that Lemma 5.4 implies that there are $\frac{p-1}{2}$ elliptic curves E' that are $\mathbb{F}_p$-isomorphic to E.

Following the notation of the last case, we see that $A' = u^4A$ must hold and that $B' = u^6B$ must hold. But in that case $C' = A'B'^{-1} = u^{-2}AB^{-1} \in \mathbb{F}_p^*$ also holds. This implies that there are only $\frac{p-1}{2}$ valid choices for C'. Each choice of C' then gives only one value of A', showing once more that there are $\frac{p-1}{2}$ elliptic curves E' that are $\mathbb{F}_p$-isomorphic to E. □

Theorem 5.6. *The action of ideals of the form (n) for odd integers n using Kohel's algorithm [59, Section 2.4] will result in mapping $E : y^2 = x^3 + Ax + B$ to $(n)E : y^2 = x^3 + n^4Ax + n^6B$.*

Proof. Using [48, Theorem 9.8.7] or [59, p. 14] we see that the (monic) kernel polynomial of this map equals the division polynomial ψ_n [64, Section 6.5] [48, Definition 9.8.5]. We define the division polynomials $f_n \in \mathbb{Z}[A, B][x]$ for positive integers n as in [65, Equation 1]. These values

for f_n can be derived from the usual values for ψ_n by $f_n = \psi_n$ for odd n and $f_n = \psi_n/y$ for even n. Using [64, Lemma 6.21] for the first coefficient and the main lemma in [65] for the others, we find a relation for the first few coefficients of f_n for odd n:

$$f_n = nx^{\frac{n^2-1}{2}} + \frac{A}{60}n(n^2-1)(n^2+6)x^{\frac{n^2-1}{2}-2} + \left(-\frac{1}{42}n(n^2-1)(n^2-3) + \frac{1}{210}n^3(n^2-1)(n^2+6)\right)Bx^{\frac{n^2-1}{2}-3} + \mathcal{O}\left(x^{(n^2-1)/2-4}\right).$$

To obtain a monic polynomial, we divide f_n by n to obtain (for odd n)

$$\psi_n = x^{\frac{n^2-1}{2}} + s_2x^{\frac{n^2-1}{2}} - s_3x^{\frac{n^2-1}{2}} + \mathcal{O}\left(x^{(n^2-1)/2-4}\right), \text{ where}$$
$$s_2 = \frac{1}{60}(n^2-1)(n^2+6)A, \qquad s_3 = \frac{n^2-1}{210}\left(5(n^2-3) - n^2(n^2+6)\right)B.$$

Now, using the relations from Kohel's algorithm [59, Section 2.4] we find $s_1 = 0$, $t = -12s_2 + (n^2-1)A$, and $w = 30s_3 + 2(n^2-1)B$. Thus, upon defining $E' = (n)E : y^2 = x^3 + A'x + B'$ we find that (for odd n)

$$\begin{aligned} A' &= A - 5t = A + 60s_2 - 5(n^2-1)A = A + (n^2-1)(n^2+1)A = n^4A, \\ B' &= B - 7w = B - 210s_3 - 14(n^2-1)B = B + (n^2-1)B(-5(n^2-3) + n^2(n^2+6) - 14) \\ &= B + (n^2-1)B(n^4+n^2+1) = n^6B. \end{aligned}$$

We have thus proved the theorem. Note that E and $(n)E$ are isomorphic by Theorem 4.8, thus the action of the ideal (n) (for odd n), is indeed an endomorphism. □

For the remainder of this section, we let $\mathrm{ord}(n \bmod p)$ denote the order of $(n \bmod p) \in \mathbb{F}_p^*$, thus, $\mathrm{ord}(n \bmod p)$ equals the first positive integer k such that $n^k \equiv 1 \pmod p$.

Lemma 5.7. *Let $p \equiv 11 \pmod{12}$ be a prime number, then for any odd divisor $q \mid p+1$ we have $\mathrm{ord}(q \bmod p) = \mathrm{ord}(q^4 \bmod p) = \mathrm{ord}(q^6 \bmod p)$.*

Proof. Let $k = \mathrm{ord}(q \bmod p)$, in other words, let $k \in \mathbb{Z}_{>0}$ be the first number such that $q^k \equiv 1 \pmod p$. By Euler's theorem we have that k must divide $\varphi(p) = p-1$, where φ is the Euler totient function. Since $p \equiv 2 \pmod 3$ we know that $3 \nmid \varphi(p)$ and thus $3 \nmid k$. Similarly, $p \equiv -1 \pmod 4$, thus $4 \nmid \varphi(p)$ and thus $4 \nmid k$. Now, if $q = 1$, we have that $\mathrm{ord}(q \bmod p) = \mathrm{ord}(q^4 \bmod p) = \mathrm{ord}(q^6 \bmod p)$, so we can safely assume that $q \geq 3$. Since $q \mid p+1$ we have that $\left(\frac{p}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$ using Theorem 5.2, where the second equality comes from [61, p. 4]. As $p \equiv 3 \pmod 4$, this implies that $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$. Therefore, q is a quadratic residue modulo p, i.e., $q^{\frac{p-1}{2}} \equiv 1 \pmod p$. Thus, $k = \mathrm{ord}(q \bmod p) \mid \frac{p-1}{2}$, which implies that $2 \nmid k$ as $p \equiv 3 \pmod 4$. Since we have $\mathrm{ord}(q^4 \bmod p), \mathrm{ord}(q^6 \bmod p) \mid \mathrm{ord}(q \bmod p) = k$, but $2, 3 \nmid k$ we must have $\mathrm{ord}(q \bmod p) = \mathrm{ord}(q^4 \bmod p) = \mathrm{ord}(q^6 \bmod p)$. □

Theorem 5.8. *Let p be a prime of the form $p = 4\ell_0\ell_1\ell_2\cdots\ell_n - 1$ with $\ell_0 = 3$ and ℓ_i distinct odd primes for $0 \leq i \leq n$ with $n \geq 0$. Furthermore, define the ideals $\mathfrak{l}_i := (\ell_i, \pi - 1)$, $\overline{\mathfrak{l}_i} := (\ell_i, \pi - 1)$. Let S be the set of elliptic curves that can be reached from $E_{1,0}$ by repeatedly applying (using Kohel's algorithm) the ideals $\mathfrak{l}_i$ or $\overline{\mathfrak{l}_i}$ for $0 \leq i \leq n$. Then,*

$$3 \cdot \mathrm{lcm}(\mathrm{ord}(\ell_0 \bmod p), \ldots, \mathrm{ord}(\ell_n \bmod p)) \cdot \#\mathrm{Cl}(\mathbb{Q}(\pi)) \leq \#S \leq \frac{3}{2}(p-1)\#\mathrm{Cl}(\mathbb{Q}(\pi))$$

Proof. The ideal classes of the ideals $\mathfrak{l}_i$ and $\overline{\mathfrak{l}_i}$ give us at least one representative of each $\mathbb{F}_p$-isomorphism class of elliptic curves over $\mathbb{F}_p$. As the CSIDH encryption scheme works on isogeny

graphs with $3\#\mathrm{Cl}(\mathbb{Q}(\pi))$ nodes [66, Section 3], we know that our encryption scheme has at least as many nodes as the CSIDH encryption scheme. Namely, at least one node for each $\mathbb{F}_p$-isomorphism class. As we cannot perform an action that lets us enter an isomorphism class that we could not enter using CSIDH, this encryption scheme contains the same amount of isomorphism classes. Now, combining the fact that $p \equiv 11 \pmod{12}$ with Theorem 5.5 gives us the upper bound of $\frac{3}{2}(p-1)\#\mathrm{Cl}(\mathbb{Q}(\pi))$ elements.

Suppose that the representative of an isomorphism class is $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_p$. Then applying the ideal $\mathfrak{l}_i\overline{\mathfrak{l}_i} = (\ell_i)$ maps E to $(\ell_i)E : y^2 = x^3 + \ell_i^4 Ax + \ell_i^6 B$ from Theorem 5.6. With $(\ell_i)E$ being in the same $\mathbb{F}_p$-isomorphism class as E due to Theorem 4.8.

From Lemma 5.7 we deduce that $\mathrm{ord}(\ell_i \bmod p) = \mathrm{ord}(\ell_i^4 \bmod p) = \mathrm{ord}(\ell_i^6 \bmod p)$ for any $0 \leq i \leq n$. Thus, the first positive integer k that satisfies $(\ell_i)^k E = E$, equals $\mathrm{ord}(\ell_i \bmod p)$.

Iterating over all possible ℓ_i yields that there are at least $\mathrm{lcm}(\mathrm{ord}(\ell_0 \bmod p), \ldots, \mathrm{ord}(\ell_n \bmod p))$ elliptic curves we can "reach" from a representative E in our $\mathbb{F}_p$-isomorphism class of elliptic curves. As there are $3\#\mathrm{Cl}(\mathbb{Q}(\pi))$ such isomorphism classes the theorem follows. □

For $p = 6563 = 4 \cdot 3 \cdot 547 - 1$ we have $\#\mathrm{Cl}(\mathbb{Q}(\pi)) = 23$. Therefore, Theorem 5.8 gives that the number of elliptic curves we can reach from our starting curve $E_{1,0}$ is at least $3 \cdot \mathrm{lcm}(193, 193) \cdot 23 = 13317$ and at most 226389. We verified that the correct number is 13317, which equals the lower bound.
In fact, 6563 is one of the two primes of the form in Theorem 5.8 under 10^4 such that $\mathrm{lcm}(\mathrm{ord}(\ell_0 \bmod p), \ldots, \mathrm{ord}(\ell_n \bmod p)) \neq \frac{p-1}{2}$. The other one is 5531.

5.3.2 Isogeny Graphs Using Our Variant

In Figure 5.2 we visualised the isogeny graph using our encryption method on the left-hand side, and the CSIDH encryption method on the right-hand side. The isogeny graph generated by our method has 21 nodes, compared to the isogeny graph generated by CSIDH of only 3 nodes. We note that Theorem 5.8 does not apply as we have $p = 43$ and $43 \not\equiv 11 \pmod{12}$.

As an example, we look at applying the ideal $\mathfrak{p}_{11} := (11, \pi - 1)$ and the ideal $\overline{\mathfrak{p}_{11}} := (11, \pi + 1)$ to a node in both isogeny graphs (where we take π to be a root of $x^2 + 43$ and we define the order $\mathbb{Z}[\pi]$ of $\mathbb{Q}(\pi)$). In the isogeny graph generated by CSIDH, we see that as the ideal class $[(11)]$ is trivial, therefore applying $[\mathfrak{p}_{11}]$ and then $[\overline{\mathfrak{p}_{11}}]$ will result in the same $\mathbb{F}_p$-isomorphism class of elliptic curves. In the other isogeny graph, we will look at applying (11) to the node $E_{22,25}$. Using the graph one can verify that $(11)E_{22,25} = \overline{\mathfrak{p}_{11}}\mathfrak{p}_{11}E_{22,25} = \overline{\mathfrak{p}_{11}}E_{39,7} = E_{32,14}$. Similarly, $(11)E_{22,25} = \mathfrak{p}_{11}\overline{\mathfrak{p}_{11}}E_{22,25} = \mathfrak{p}_{11}E_{21,0} = E_{32,14}$, ensuring commutativity. This result can also be obtained using Theorem 5.6 as $32 \equiv 11^4 \cdot 22 \pmod{43}$ and $14 \equiv 11^6 \cdot 25 \pmod{43}$.

5.3.3 Strength of Our Encryption Scheme

Let p be a prime and define the order $\mathbb{Z}[\pi]$ of $\mathbb{Q}(\pi)$ where π is a root of $x^2 + p$. In this subsection, we assume that there exists an oracle that can solve the CSIDH encryption scheme to a level that given a public key A and a starting curve E_0, the oracle can find an ideal $\mathfrak{a}$ of $\mathbb{Z}[\pi]$ such that $[\mathfrak{a}]E_0 \cong E_A$. We will provide an unproven method for the oracle to break our variant of CSIDH as well.

Given is Alice's public key A_1, A_2, determined by evaluating $\mathfrak{a}E_{1,0}$, where $\mathfrak{a}$ is the ideal of $\mathbb{Z}[\pi]$ corresponding to the secret key of Alice. Suppose that a CSIDH oracle finds an ideal $\mathfrak{c}$ such that $[\mathfrak{c}]E_{1,0} \cong M_A$ where M_A denotes the Montgomery curve in the $\mathbb{F}_p$-isomorphism class of E_{A_1,A_2}. Now, we can compute the curve $E_{C_1,C_2} := \mathfrak{c}E_{1,0}$ (using the same algorithm that Alice and Bob use) which is $\mathbb{F}_p$-isomorphic to E_{A_1,A_2}. Afterwards, we can find a rational map ψ equal to the $\mathbb{F}_p$-isomorphism from E_{C_1,C_2} to E_{A_1,A_2} (using Theorem 4.8). We write $\phi_{\mathfrak{c}}$ for the isogeny determined by the ideal $\mathfrak{c}$. We thus have that $(\psi \circ \phi_{\mathfrak{c}})E_{1,0} = E_{A_1,A_2} = \mathfrak{a}E_{1,0}$. Now, given Bob's public key B_1, B_2, we can evaluate $(\psi \circ \phi_{\mathfrak{c}})E_{B_1,B_2}$ to find the shared secret $\mathfrak{a}E_{B_1,B_2}$.

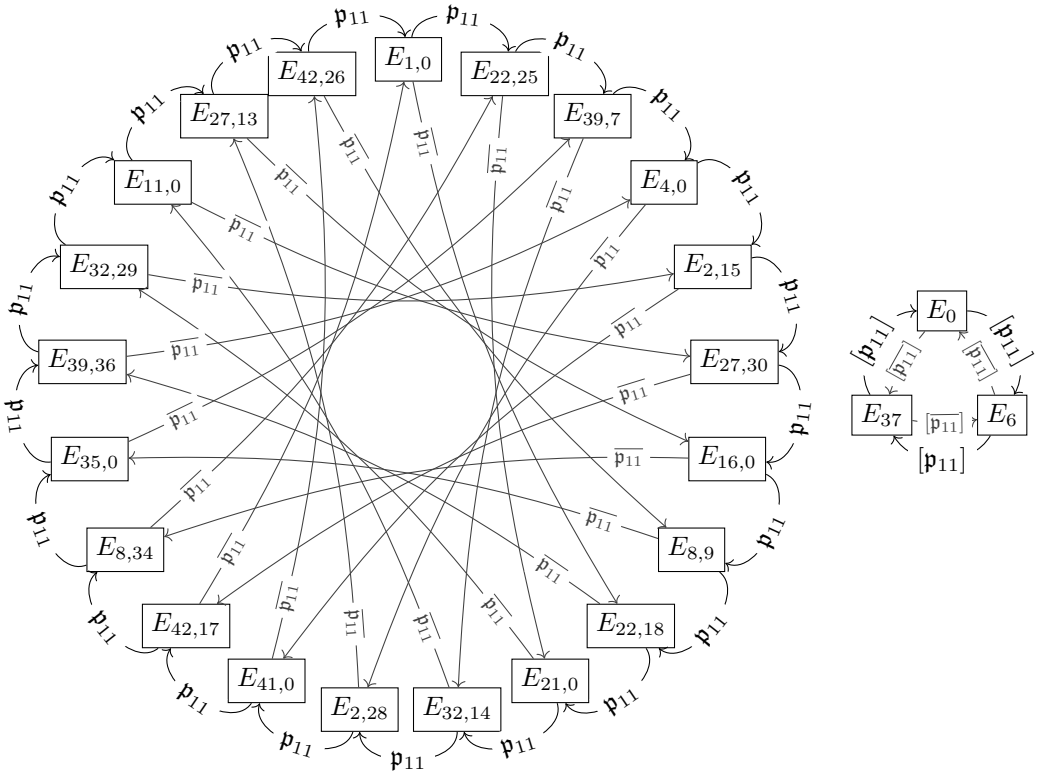

Figure 5.2: Isogeny graphs with the same starting curve $E_{1,0} = E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_{43}$. On the left-hand side nodes in the same $\mathbb{F}_{43}$-isomorphism class are not contracted, giving an isogeny graph generated by the action of the ideals $\mathfrak{p}_{11} := (11, \pi - 1)$ and $\overline{\mathfrak{p}_{11}} := (11, \pi + 1)$ of the order $\mathbb{Z}[\pi]$ of the number field $\mathbb{Q}(\pi)$ where π is a root of $x^2 + 43$ on the elliptic curves. On the right-hand side, nodes in the same $\mathbb{F}_{43}$-isomorphism class are contracted and are denoted by their Montgomery representative, the isogeny graph is generated by the action of the ideal classes $[\mathfrak{p}_{11}]$ and $[\overline{\mathfrak{p}_{11}}]$.

Let $p = 59 = 4 \cdot 3 \cdot 5 - 1$, Theorem 5.8 then gives the lower bound of 261 nodes and the upper bound of 261 nodes. We will thus be working on an isogeny graph with exactly 261 nodes. Alice generates her private key, and reaches $\mathfrak{a} = \mathfrak{l}_3^2\overline{\mathfrak{l}_3^3}\mathfrak{l}_5\overline{\mathfrak{l}_5^3}$. She applies her action to the starting curve $E_{1,0}$ (using Kohel's algorithm) to get the elliptic curve $E_{25,45} : y^2 = x^3 + 25x + 45$. Suppose that there exists a method to break the CSIDH algorithm. Then, after finding the Montgomery representative of $E_{25,45}$ given by $E_{28} : y^2 = x^3 + 28x^2 + x$, the method can find an ideal $\mathfrak{c}$ such that $[\mathfrak{c}]E_{1,0} = E_{28}$. An example of such an ideal class can be found in Table 5.1, which yields $\mathfrak{c} = \mathfrak{l}_3^2\mathfrak{l}_5$.
Now, applying the ideal $\mathfrak{c}$ to $E_{1,0}$ gives the curve $\mathfrak{c}E_{1,0} = E_{35,20} : y^2 = x^3 + 35x + 20$. To find an $\mathbb{F}_p$-isomorphism from $E_{35,20}$ to $E_{25,45}$, we first find the residue classes a, b of $\mathbb{F}_{59}$ such that $(35 \bmod p)a = (25 \bmod p)$ and $(20 \bmod p)b = (45 \bmod p)$. We calculate these to be $(26 \bmod p)$ and $(17 \bmod p)$, respectively. Although we can calculate the actual $\mathbb{F}_p$-isomorphism, these residue classes are enough.
Now, Alice receives Bob's public key $E_{52,30} : y^2 = x^3 + 52x + 30$ and computes the shared secret $\mathfrak{a}E_{52,30} = E_{48,14} : y^2 = x^3 + 48x + 14$. The oracle computes $\mathfrak{c}E_{52,30} = E_{20,39} : y^2 = x^3 + 20x + 39$. Using the residue classes $(26 \bmod p)$ and $(17 \bmod p)$, we can compute $20 \cdot 26 \equiv 48 \pmod p$ and $39 \cdot 17 \equiv 14 \pmod p$, precisely the coefficients of $E_{48,14} = \mathfrak{a}E_{52,30}$, the shared secret.

Appendix A

Computer Code

This is the SageMath code [2] for computing the example in Section 5.2. It can be adapted to evaluate the action of other ideals on elliptic curves. The code is also available on `https://github.com/jorisperrenet/MasterThesis`.

```
from sage.all import *
from sage.schemes.elliptic_curves.ell_curve_isogeny import compute_codomain_kohel


def apply_ideal(E, n, v=-1):
    """Returns (n, pi-1)E, (n)E, or (n, pi+1)E depending on v=-1,0,+1

    Arguments:
        - E, an elliptic curve of the form y^2 = f(x) over F_p for a prime p
               satisfying p>3 and p=3 mod 8.
        - n, an odd prime dividing p+1.
        - v, an integer between -1 and 1, specifying what ideal to apply to
               the elliptic curve.

    Output:
        - E', an elliptic curve in the F_p-isomorphism class of
               (n, pi-1)E, (n)E, or (n, pi+1)E, depending on `v`.
             The resulting elliptic curve is found using Kohel's algorithm.
    """
    assert E.a1() == E.a3() == 0
    assert is_prime(n) and n & 1 and (p+1) % n == 0
    assert -1 <= v <= 1 and int(v) == v

    # Do the case v=0 separately, as this is much faster.
    if v == 0:
        Esw = E.short_weierstrass_model()
        return EllipticCurve([0, 0, 0, n^4 * Esw.a4(), n^6 * Esw.a6()])

    # We find the function f(x) such that E: y^2 = f(x).
    f = E.hyperelliptic_polynomials()[0]

    # We aspire to find a generator Q of the n-torsion points on the elliptic curve, i.e.,
    # a generator of the set {P in E: [n]P = O}
    if v == 1:
        # We want to apply the ideal (n, pi+1) to E.
        # ker phi = {P in E: [n]P = O} {P in E: pi(P)+P = O}
        # If pi(P) + P = O, then pi(P) = -P, and if P=(x,y), then x^p=x and y^p=-y is required.
        # So x in F_p and y^(p-1) = -1, so P in E(F_{p^2}).
        # We go through random points on the curve an check whether they are generators of the
        # n-torsion points of E(F_{p^2}).
        F = GF(p)
        EF2 = E.base_extend(GF(p^2))
        while True:
```

```
            # We still have that x in F_p.
            x_coor = F.random_element()
            # Check whether this point satisfies y^(p-1)=-1, so that since y^2=f(x) we find that
            # f(x)^((p-1)/2) = -1, giving that f(x) is not a quadratic residue.
            if not f(x_coor).is_square():
                # This point is in E(F_{p^2}), find the corresponding coordinates.
                G = EF2.lift_x(x_coor)
                # Assume that G is a generator of the n-torsion points of E(F_{p^2}), so that
                # G has order equal to p+1, then we find that [n]*[(p+1)/n]*G = O as
                # n divides p+1, therefore [(p+1)/n]*G has order n (or a divisor of n).
                Q = ((p+1)//n)*G
                # The only point of order a divisor of n is the point at infinity, check that
                # we did not find this point.
                if Q != EF2.point(0):
                    break
    elif v == -1:
        # The commented code
        # while True:
        #     x_coor = GF(p).random_element()
        #     if f(x_coor).is_square():
        #         G = E.lift_x(x_coor)
        #         Q = ((p+1)//n)*G
        #         if Q != E.point(0):
        #             break
        # is actually the same as the following built-in code.
        G = E.gens()[0]
        Q = ((p+1)//n)*G

    # The multiples [k]*Q = [k*(p+1)/n]*G still satisfy [n]*[k*(p+1)/n]*G = O, such that
    # each of [k]*Q is an n-torsion point, these are in fact all the n-torsion points that
    # we need to check.
    # We only need to know the distinct x-coordinates of [k]*Q.
    # We will repetitively add Q to itself, stopping at [n]*Q (exclusive).
    # Since [n-1]*Q = [-1]*Q = -Q has the same x-coordinate as [1]Q = Q and -Q has the same
    # x-coordinate as Q, we can even stop our search at [n//2]*Q (inclusive).
    P = Q
    xs = {Q.x()}
    for _ in range(n//2-1):
        P += Q
        xs.add(P.x())

    # We are ready to compute the monic kernel polynomial of the isogeny phi, remember that
    # ker phi = {P in E: [n]P = O} {P in E: pi(P) \pm P = O}
    # and `xs` are the x-coordinates of all points in {P in E: [n]P = O}.
    # A monic kernel polynomial of the resulting isogeny will be the product
    # of (x-P_x), where P_x is the x-coordinate of the point in the kernel.
    x = polygen(GF(p))
    if v == -1:
        # If (pi-1)(P) = O, then pi(P) = P, so that if P=(x,y) we require that x^p=x and y^p=y.
        # This gives that both x in F_p and y in F_p. Then, we need y^(p-1)=1. But, y^2=f(x),
        # so that the equality becomes y^(p-1)=f(x)^((p-1)/2)=1, implying that we need f(x)
        # to be a quadratic residue, i.e., a square in F_p.
        kernel_pol = prod(x - px for px in xs if f(px).is_square())
    elif v == 1:
        # If (pi+1)(P) = O, then pi(P) = -P, so that if P=(x,y) we require that x^p=x and y^p=-y.
        # We again get that x in F_p, but require that y^(p-1)=f(x)^((p-1)/2)=-1, implying that
        # f(x) may not be a square in F_p.
        # First, map each x-coordinate in F_{p^2} to a point in F_p (we already know that these
        # are in F_p so that we can apply this mapping).
        F = GF(p)
        xs = [F(px) for px in xs]
        kernel_pol = prod(x - px for px in xs if not f(px).is_square())

    # Specifying the algorithm that SageMath uses to compute the codomain of the isogeny
    # corresponding to the kernel speeds up the calculation significantly over using
    # `E.isogeny`, I presume that this is because SageMath does not need to compute the
```

```
    # isogeny in this case.
    return compute_codomain_kohel(E, kernel_pol)

def apply_ideals(E, ps, mults):
    """Applies the ideal (ps[i], pi-1)**mults[i] to E for all i
    Note: if mults[i] < 0, then we apply (ps[i], pi+1)**(-mults[i])."""
    e = E
    for n, mult in zip(ps, mults):
        if mult < 0:
            for _ in range(-mult):
                e = apply_ideal(e, n, 1)
        else:
            for _ in range(mult):
                e = apply_ideal(e, n, -1)
    return e



### Define your prime `p` here as the product of small primes in `ps`
ps = [3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37]
p = 4*prod(ps)-1

# Make sure that p>3 is prime and p = 3 (mod 8).
# Then, make sure that p is -1+4*[the product of distinct odd primes]
assert is_prime(p)
assert p % 8 == 3 and p > 3
assert factor((p+1)/4).radical_value() == (p+1)/4

# Create the starting curve, E0
E0 = EllipticCurve(GF(p), [1, 0])

# Display some information
print()
print(f'p = {p}, with starting curve {str(E0)[26:-27-len(str(p))]}')
K.<pi> = NumberField(E0.frobenius_polynomial())
print(f'The number of nodes in the isogeny graph is {K.order(pi).class_number()}')
print()

### Applying the ideals to the elliptic curves according to the example.
print()
print("Alice's resulting curve after applying her private key is")
E_A = apply_ideals(E0, (3, 13, 17, 29, 31), (1, -2, 2, -2, 1)).montgomery_model()
print(E_A)

print()
print("Bob's resulting curve after applying his private key is")
E_B = apply_ideals(E0, (5, 7, 13, 17, 19, 23), (2, 1, -2, 1, -1, 2)).montgomery_model()
print(E_B)

print()
print()
print("Alice applies her private key to E_B and gets")
print(apply_ideals(E_B, (3, 13, 17, 29, 31), (1, -2, 2, -2, 1)).montgomery_model())
print()
print("Bob applies his private key to E_A and gets")
print(apply_ideals(E_A, (5, 7, 13, 17, 19, 23), (2, 1, -2, 1, -1, 2)).montgomery_model())
print()
print("They thus get the same curve E_S.")
```

Bibliography

[1] Wouter Castryck et al. *CSIDH: An Efficient Post-Quantum Commutative Group Action*. Cryptology ePrint Archive, Paper 2018/383. https://eprint.iacr.org/2018/383. 2018. URL: https://eprint.iacr.org/2018/383.

[2] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.2)*. https://www.sagemath.org. Dec. 2023.

[3] D.C. Gijswijt. *Algebra 1, Course AM1060*. TUDelft. 2020/2021.

[4] P. Stevenhagen. *Algebra I*. Leiden University. 2023. URL: https://websites.math.leidenuniv.nl/algebra/algebra1.pdf.

[5] S.R. Lay. *Analysis: With an Introduction to Proof*. Prentice Hall, 2000. ISBN: 9780130898791. URL: https://books.google.nl/books?id=cRjvAAAAMAAJ.

[6] X. Hou. *Lectures on Finite Fields*. Graduate Studies in Mathematics. American Mathematical Society, 2018. ISBN: 9781470442897. URL: https://books.google.nl/books?id=lhpfDwAAQBAJ.

[7] R. Lidl and H. Niederreiter. *Finite Fields*. EBL-Schweitzer v. 20,dl. 1. Cambridge University Press, 1997. ISBN: 9780521392310. URL: https://books.google.nl/books?id=xqMqxQTFUkMC.

[8] R. Kochendorffer. *Introduction to Algebra*. Springer, 1972. ISBN: 9789001475505. URL: https://books.google.nl/books?id=bNO1vwEACAAJ.

[9] David Vogan. *Finite fields*. MIT. 2013. URL: https://ocw.mit.edu/courses/18-700-linear-algebra-fall-2013/resources/mit18_700f13_finite_fields/.

[10] David Forney. *6.451 S05: Complete Lecture Notes*. MIT. 2005. URL: https://ocw.mit.edu/courses/6-451-principles-of-digital-communication-ii-spring-2005/resources/mit6_451s05_fulllecnotes/.

[11] Darij Grinberg. *Regular elements of a ring, monic polynomials and "lcm-coprimality"*. 2021. URL: https://www.cip.ifi.lmu.de/~grinberg/algebra/regpol.pdf.

[12] *Eindige Lichamen TW2560*. TUDelft. Mar. 2018.

[13] Jyrki Lahtonen. *Reed Solomon Polynomial Generator*. Mathematics Stack Exchange. [Online; version 2017-04-13]. URL: https://math.stackexchange.com/a/76136/1049661.

[14] The Stacks project authors. *The Stacks project*. https://stacks.math.columbia.edu. 2024.

[15] Matthew Steed. *Proofs of the fundamental theorem of algebra*. 2015. URL: https://math.uchicago.edu/~may/REU2014/REUPapers/Steed.pdf.

[16] J. Wyss-Gallifent. *Math 403 Chapter 21: Algebraic Extensions*. UMD. URL: https://math.umd.edu/~immortal/MATH403/lecturenotes/ch21.pdf.

[17] Hiroshi Suzuki. *Algebra II Chapter 10: Algebraic Extensions*. ICU. 2017. URL: https://icu-hsuzuki.github.io/science/class/algebra2/lecnote/2017/Lecture10.pdf.

[18] Peter Stevenhagen. *Number Rings*. 2019. URL: https://websites.math.leidenuniv.nl/algebra/ant.pdf.

[19] J.F. Brakenhoff. *Counting problems for number rings*. Leiden University. 2009. URL: https://scholarlypublications.universiteitleiden.nl/access/item%3A2925604/view.

[20] D.A. Marcus. *Number Fields*. Universitext. Springer New York, 1995. ISBN: 9780387902791. URL: https://books.google.nl/books?id=DKrf26ogA0UC.

[21] Luke Wolcott. *Maximal and Non-Maximal Orders*. URL: https://wstein.org/wiki/attachments/ant07(2f)projects/wolcott.pdf.

[22] Peter Stevenhagen. "The arithmetic of number rings". In: (Jan. 2008). URL: https://www.math.leidenuniv.nl/~stevenhagenp//ANTproc/08psh.pdf.

[23] Pace Nielsen. *An Introduction to Orders of Number Fields*. May 2002. URL: https://kskedlaya.org/Math254B/Orders.pdf.

[24] B. Hartley and T.O. Hawkes. *Rings, Modules and Linear Algebra*. Chapman and Hall mathematics series. Chapman and Hall Limited, 1974. URL: https://books.google.nl/books?id=AvNewAEACAAJ.

[25] Keith Conrad. *Trace and Norm*. Accessed: 2024-03-14. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/tracenorm.pdf.

[26] Khalid Rian. *The Norm and Trace*. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=481883de7a6b54a258fc496a14cbcff13339ac8c.

[27] Minhyong Kim. *Norm and Trace via matrices*. URL: https://www.ucl.ac.uk/~ucahmki/normtrace.pdf.

[28] S. Axler. *Linear Algebra Done Right*. Undergraduate Texts in Mathematics. Springer International Publishing, 2023. ISBN: 9783031410260. URL: https://books.google.nl/books?id=OdnfEAAAQBAJ.

[29] G.J. Janusz. *Algebraic Number Fields*. Advances in the Mathematical Sciences. American Mathematical Society, 1996. ISBN: 9780821804292. URL: https://books.google.nl/books?id=rw0PCgAAQBAJ.

[30] P.G.L. Dirichlet. *Vorlesungen über Zahlentheorie*. 4th ed. Vieweg und Sohn, Braunschweig, 1894. URL: https://archive.org/details/vorlesungenberz02dirigoog/page/n5/mode/1up.

[31] R.B. Ash. *A Course in Algebraic Number Theory*. Dover books on mathematics. Dover Publications, 2010. ISBN: 9780486477541. URL: https://books.google.nl/books?id=r6DPTJLzfT4C.

[32] R. Dedekind. "Über den Zusammenhang zwischen der Theorie der ideale und der Theorie der höheren Congruenzen". In: *Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen* 23 (1878), pp. 3–38. URL: http://eudml.org/doc/135827.

[33] Keith Conrad. *Factoring After Dedekind*. Accessed: 2024-03-14. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf.

[34] Ila Varma. *MAT415 Assignment 2 Solutions*. University of Toronto. 2020. URL: https://www.math.utoronto.ca/~ila/MAT415%20HW%202%20Solutions.pdf.

[35] Keith Conrad. *Class Group Calculations*. Accessed: 2024-03-14. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/classgpex.pdf.

[36] Victor S. Miller. "Use of Elliptic Curves in Cryptography". In: *Advances in Cryptology — CRYPTO '85 Proceedings*. Ed. by Hugh C. Williams. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. ISBN: 978-3-540-39799-1. DOI: 10.1007/3-540-39799-X_31.

[37] Neal Koblitz. "Elliptic Curve Cryptosystems". In: *Mathematics of Computation* 48.177 (Jan. 1987), pp. 203–209. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-1987-0866109-5.

[38] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Discrete Mathematics and Its Applications. CRC Press, 2003. ISBN: 9780203484029. URL: https://books.google.nl/books?id=vPL19KNdm2wC.

[39] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer New York, 1994. ISBN: 9780387978253. URL: https://books.google.nl/books?id=mAJei2-JcE4C.

[40] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946. URL: https://books.google.nl/books?id=Z90CA_EUCCkC.

[41] J. Harris. *Algebraic Geometry: A First Course*. Graduate texts in mathematics. Springer-Verlag, 1992. ISBN: 9783540977162. URL: https://books.google.nl/books?id=INW6QgAACAAJ.

[42] R.P. Hulst. *A proof of Bézout's theorem using the euclidean algorithm*. Leiden University. 2011. URL: https://hdl.handle.net/1887/3596706.

[43] Brian Lehmann. *Lecture 3: Elliptic Curves*. Boston College. 2023. URL: https://sites.nd.edu/2023cmndthematicprogram/files/2023/06/lecture3-Lehmann-updated.pdf.

[44] Kazuyuki Fujii and Hiroshi Oike. "An Algebraic Proof of the Associative Law of Elliptic Curves". In: *Advances in Pure Mathematics* 07 (Jan. 2017), pp. 649–659. DOI: 10.4236/apm.2017.712040.

[45] Jeroen Spandaw. "Associativity of Addition on Elliptic Curves". In: (Oct. 2022). URL: https://www.ru.nl/publish/pages/1056229/spandaw_associativity_on_elliptic_curve_1.pdf.

[46] Louis Joel Mordell. "On the rational resolutions of the indeterminate equations of the third and fourth degree". In: *Proc. Cambridge Phil. Soc.* Vol. 21. 1922, pp. 179–192.

[47] Daniel Parker. *ELLIPTIC CURVES AND LENSTRA'S FACTORIZATION ALGORITHM*. University of Chicago. 2014. URL: https://math.uchicago.edu/~may/REU2014/REUPapers/Parker.pdf.

[48] S.D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. ISBN: 9781107013926. URL: https://books.google.nl/books?id=owd76BElvosC.

[49] Andrew Sutherland. *18.783 - Elliptic Curves*. MIT. 2022. URL: https://math.mit.edu/classes/18.783/2022/LectureNotes4.pdf.

[50] John Tate. "Endomorphisms of abelian varieties over finite fields". In: *Inventiones mathematicae* 2.2 (1966), pp. 134–144.

[51] Jan Nekovář. *Elliptic functions and elliptic curves*. 2004. URL: https://webusers.imj-prg.fr/~jan.nekovar/co/ln/el/el2.pdf.

[52] J. Vélu. "Isogénies entre courbes elliptiques". In: *Comptes-Rendus de l'Académie des Sciences, Série I* 273 (July 1971), pp. 238–241.

[53] Steven D. Galbraith. *The Ideal Class Group Action on Supersingular Elliptic Curves*. [Online; accessed 16-March-2024]. 2023. URL: https://www.math.auckland.ac.nz/~sgal018/note-on-CSIDH-action.pdf.

[54] Andrew Sutherland. *18.783 - Elliptic Curves*. MIT. 2023. URL: https://math.mit.edu/classes/18.783/2023/LectureNotes13.pdf.

[55] Helmut Hasse. In: *Journal für die reine und angewandte Mathematik* 1936.175 (1936), pp. 193–208. DOI: doi:10.1515/crll.1936.175.193. URL: https://doi.org/10.1515/crll.1936.175.193.

[56] V. Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2005. ISBN: 9780521851541. URL: https://books.google.nl/books?id=-RzJs-mPfX0C.

[57] J.B. Weimar. *Categories of sets with a group action*. Leiden University. 2008. URL: https://hdl.handle.net/1887/3596850.

[58] M. Kojo T. Kivinen. *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*. The Internet Society, 2003. URL: https://www.rfc-editor.org/rfc/pdfrfc/rfc3526.txt.pdf.

[59] David R. Kohel. "Endomorphism rings of elliptic curves over finite fields". In: 1996. URL: https://www.i2m.univ-amu.fr/perso/david.kohel/pub/thesis.pdf.

[60] Awatef Noweafa Almuteri. *Quadratic Reciprocity: Proofs and Applications*. 2019. URL: https://egrove.olemiss.edu/etd/1540.

[61] Bruce Ikenaga. *The Jacobi Symbol*. 2019. URL: https://sites.millersville.edu/bikenaga/number-theory/jacobi-symbol/jacobi-symbol.pdf.

[62] S. W. Golomb. "Combinatorial Proof of Fermat's "Little" Theorem". In: *The American Mathematical Monthly* 63.10 (1956), pp. 718–718. ISSN: 00029890, 19300972. URL: http://www.jstor.org/stable/2309563 (visited on 07/10/2024).

[63] D. Alkema. *The Law of Quadratic Reciprocity: From Fermat to Gauss*. 2016. URL: https://studenttheses.uu.nl/handle/20.500.12932/23450.

[64] Andrew Sutherland. *18.783 - Elliptic Curves*. MIT. 2017. URL: https://math.mit.edu/classes/18.783/2017/LectureNotes6.pdf.

[65] James McKee. "Computing Division Polynomials". In: *Mathematics of Computation* 63.208 (1994), pp. 767–771. ISSN: 00255718, 10886842. URL: http://www.jstor.org/stable/2153297 (visited on 05/11/2024).

[66] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. "CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations". In: *Advances in Cryptology – ASIACRYPT 2019*. Ed. by Steven D. Galbraith and Shiho Moriai. Cham: Springer International Publishing, 2019, pp. 227–247. ISBN: 978-3-030-34578-5.