University of Groningen

Bachelor's Project Mathematics

Schoof's algorithm: Point counting on elliptic curves

February 26, 2020

Author:
Janet Visser

First supervisor:
Pınar Kılıçer

Second assessor:
Steffen Müller

Contents

Abstract

The goal of this paper is to prove Schoof's algorithm; a clever application of the Chinese Remainder Theorem, which counts the number of points on an elliptic curve defined over a finite field $\mathbb{F}_q$. These points form a finite group. It is in fact a union of torsion subgroups, each of which is the exact set zeros of a division polynomial. The thesis concludes with the proof of the algorithm, which concerns finite fields with characteristic larger than 3.

1 Introduction

More than ever, the internet plays a significant role in almost all aspects of our society. Its intentional, and also its most important purpose is to exchange knowledge with other people from all over the world. This information is usually shared between two parties over a public channel. To prevent misuse of the knowledge that is exchanged, any interference from other parties should be nearly impossible. It is therefore desirable that this exchange can be done in a secure way. In other to ensure this, a reliable method would be to use Elliptic Curve Cryptography (ECC). We will devote this first section to get a general understanding of its origins and importance.

1.1 Relevant cryptography

The security of public key cryptosystems is based on a special property of *one-way trapdoor functions* $f : A \to B$. Such functions are injective and easily computable. Most importantly, their inverse f^{-1} is very hard to compute in general. However, this difficulty is drastically reduced if someone has an extra piece of information k, called a

cryptographic key. This means that if Alice knows the value of k, then Bob can send her a message $a \in A$ by sending her the quantity $b = f(a)$. Alice easily recovers $a = f^{-1}(b)$, since she knows k. A person who does not know k is unable to compute $f^{-1}(b)$, in a reasonable amount of time.

The search for one-way trapdoor functions is still an open problem in mathematics. However, it has been proposed that the *Discrete Logarithm Problem* (DLP) could be a solid basis for such functions.

Discrete Logarithm Problem. Given a group $(G, \cdot)$ and elements $g, h \in G$, find an integer n such that $g^n = h$, assuming it exists.

It should be emphasized that the difficulty of the DLP depends on the chosen group. For practical reasons, it is desirable that the DLP is hard to solve. Moreover, for implementation purposes, we require that the group operation should be easily computable. We will shortly discuss the DLP for a number of groups.

Besides the DLP, some other hard problems are used as a secure basis for cryptosystems. As an example, the first practical public key cryptosystem bases its security on the difficulty of factoring large numbers. It is known as the *RSA cryptosystem* and was introduced in 1977. The abbreviation stands for Rivest, Shamir, and Adleman [1], who designed the algorithm.

The first paper on public key cryptography was published by Diffie and Hellman [2] in 1976, although they were not able to find a practical method to implement their idea. However, they did describe a key exchange algorithm that bears their name. Its security relies on the DLP in $\mathbb{F}_q^*$. Based on this key exchange, ElGamal [3] created a public key cryptosystem in 1985.

The *Diffie-Hellman key exchange* makes it possible for two persons, which we will call Alice and Bob, to securely exchange a piece of information whose value neither one of them knows in advance. Below, a step-by-step description of how the key exchange is given for an arbitrary group.

Diffie-Hellman key exchange

1. Alice randomly generates an integer $a \in \{0, 1, \cdots, \#G - 1\}$ and publicly sends g^a to Bob.
2. Bob randomly generates an integer $b \in \{0, 1, \cdots, \#G - 1\}$ and publicly sends g^b to Alice.
3. Alice computes $(g^a)^b = g^{ab}$. Bob computes $(g^b)^a = g^{ba} = g^{ab}$.
4. The element $g^{ab} =: h$ is the encryption key.

Eve only knows the elements g, g^a and g^b. If Eve is able to determine g^{ab} from these elements, then Eve solved the *Diffie-Hellman problem* (DHP).

Diffie-Hellman problem Given three elements g, g^a and g^b of G, compute the element g^{ab}.

It is important to note that the DLP is stronger then the Diffie-Hellman problem. If Eve can solve the DLP, then Eve is able to solve the DHP as well. When this occurs, we say that the Diffie-Hellman scheme is broken.

1.2 Discrete Logarithm Problem for some specific groups

We recall that the hardness of both the DLP and the DHP depends on the group used. To illustrate this we will discuss the DLP for some particular groups.

For $(\mathbb{Z}_n, +)$ the DLP is relatively easy. The congruence $gn \equiv h \pmod{N}$ can be solved using the Euclidean algorithm, which takes $O(\log(n))$ steps.

We denote by $\mathbb{F}_q^*$ the unit group of the finite field $\mathbb{F}_q$, where $q = p^r$ for some prime p and $r \in \mathbb{Z}_{\geq 1}$. There are no known algorithms which solve the DLP for this group in polynomial time. The fastest algorithms solve the problem in *subexponential* time. The number of steps required for the best known algorithm equals

$$\exp\left(c\sqrt[3]{(\log q)(\log\log q)^2}\right).$$

Here c is a small absolute constant. This is already an improvement compared to the DLP for $\mathbb{Z}_n$, but we are about to encounter a group for which the DLP is even harder.

1.3 Elliptic Curve Cryptography (ECC)

In an attempt to find a group for which the DLP is harder than it is in the group $\mathbb{F}_q^*$, Koblitz [4] and Miller [5] suggested to replace $\mathbb{F}_q^*$ by the group $(E(\mathbb{F}_q), +)$. This group consists of all rational points of an elliptic curve E (a notion that we will thorougly explore later) over a finite field $\mathbb{F}_q$. This idea led to the creation of *Elliptic Curve Cryptography* (ECC). The security of an elliptic curve cryptosystem relies on the hardness of the *Elliptic Curve Discrete Logarithm Problem* (ECDLP).

Elliptic Curve Discrete Logarithm Problem. For two given points $P, Q \in E(\mathbb{F}_q)$, find the integer m such that $[m]P = P + \cdots + P = Q$.

The best known algorithm to solve the DLP in $E(\mathbb{F}_q)$ take exponential time. It requires $O\left(2^{n/2}\right)$ steps, where $n = \log_2 q$.

The use of elliptic curves in favor of other groups has one main advantage. With our current knowledge, it is much harder to solve the DLP in $E(\mathbb{F}_q)$ than it is to solve the DLP in $\mathbb{F}_q^*$. In practice, this means that elliptic curve cryptography has key and message sizes that are 5 to 10 times smaller than those for other systems, including $\mathbb{F}_q^*$-based DLP systems. This is why ECC is widely used.

1.4 Point counting on elliptic curve

We have established that the DLP is notoriously hard for the group $E(\mathbb{F}_q)$. To take maximum advantage of this fact, we need to have curves on our disposal which contain a large number of points. Essential tools for checking this requirement are point-counting algorithms.

At first, the *Baby Step, Giant Step* algorithm (BSGS) by Shanks [6] was the most conventional. It requires $O(q^{1/4})$ steps. Until 1985, there were no sub-exponential point-counting algorithms. Schoof made a breakthrough in this matter by introducing the first such algorithm in his paper [7]. It requires $O(\log^8(q))$ steps, and it utilizes the Chinese Remainder Theorem in a clever way. We will write its main steps below. In this description, $a := q + 1 - \#E(\mathbb{F}_q)$.

Schoof's algorithm
Input: An elliptic curve E defined over a finite field $\mathbb{F}_q$.
Output: $\#E(\mathbb{F}_q)$.

1. Find primes ℓ such that $\prod \ell > 4\sqrt{q}$.
2. Determine $a \bmod \ell$.
3. Compute $a \bmod (\prod \ell)$.
4. Choose a such that $|a| \leq 2\sqrt{q}$.
5. $\#E(\mathbb{F}_q) = q + 1 - a$.

In the 1990s, Atkin [8] and Elkies [9, 10] made some improvements to Schoof's algorithm, which are incorporated in the SEA-algorithm (Schoof-Elkies-Atkin). The maximum number of steps required is reduced to $O(\log^6 q)$.

The bulk of this thesis will be used to introduce all essential theory required to properly dissect Schoof's algorithm. To this regard, we will first introduce the concept to which all theory will be applied.

2 Elliptic curves

Elliptic curves will form the foundation of this thesis. It is easy to see that a proper understanding of them will be absolutely essential. Prior to stating the exact definition of an elliptic curve, we will introduce the notions of *the projective plane, the affine plane*, and *the Weierstrass equations*. Their definitions will be provided in the next few subsections.

2.1 The projective plane and the affine plane

Unless specified differently, K is understood to be field, and $\bar{K}$ will denote an algebraic closure of K.

Definition 2.1. The *projective plane over* K, denoted by $\mathbb{P}^2_{\bar{K}}$, consists of equivalence classes of ordered triples (x, y, z). (When K is fixed, it is sometimes denoted by $\mathbb{P}^2$ instead of $\mathbb{P}^2_{\bar{K}}$). Here, $x, y, z \in \bar{K}$, and at least one of x, y and z is nonzero. The equivalence relation is given by the multiplication by a nonzero scalar $\lambda \in K^*$. If (x_0, y_0, z_0) is such an ordered triple, its equivalence class is denoted $(x : y : z)$ and we have

$$(x : y : z) := \{(\lambda x_0, \lambda y_0, \lambda z_0) \mid \lambda \in \bar{K}^*\}.$$

An equivalence class $(x : y : z)$ is then referred to as a point in $\mathbb{P}^2_{\bar{K}}$. Note that $(0 : 0 : 0)$ is *not* a point in $\mathbb{P}^2_{\bar{K}}$, since $\bar{K}$ does not contain zero divisors. When $z \neq 0$, the point $(x : y : z)$ equals $(x/z : y/z : 1)$. Points of this form make up the *affine points* in $\mathbb{P}^2_{\bar{K}}$. If $z = 0$, such a normalization of coordinates cannot be made without dividing by zero. This operation can be thought of as assigning the value ∞ to either the x- or y-coordinate. For this reason, the points $(x : y : 0)$ are said to be *points at infinity* in $\mathbb{P}^2_{\bar{K}}$. Choosing $z = 0$ is simply a convention, as there is nothing special about the variable z.

We will now introduce a specific subset of $\mathbb{P}^2$. We will later see that its defining property allows us to find subgroups of the points on elliptic curves.

Definition 2.2. The K-rational points in $\mathbb{P}^2$ is the set

$$\mathbb{P}^2_K = \{(x : y : z) \in \mathbb{P}^2_{\bar{K}} \mid x, y, z \in K\}.$$

We will now introduce a different kind of plane, referred to as the *affine plane*. This plane can be embedded in the projective plane.

Definition 2.3. The *affine plane* $\mathbb{A}^2_{\bar{K}}$ is defined to be the following set.

$$\mathbb{A}^2_{\bar{K}} = \{(x, y) \in \bar{K} \times \bar{K}\}.$$

When K is fixed, we will sometimes denote $\mathbb{A}^2_{\bar{K}}$ by $\mathbb{A}^2$.

Just as with the projective plane, $\mathbb{A}^2$ has K-rational points.

Definition 2.4. The K-rational points of $A^2(\bar{K})$ form the set

$$\mathbb{A}^2_K = \{(x, y) \in \mathbb{A}^2_{\bar{K}} \mid (x, y) \in K \times K\}.$$

We can define an inclusion map $\mathbb{A}^2_{\bar{K}} \hookrightarrow \mathbb{P}^2_{\bar{K}}$ as follows:

$$(x, y) \mapsto (x : y : 1). \tag{1}$$

This map shows us that the affine plane can be identified with the affine points of $\mathbb{P}^2_{\bar{K}}$.

Remark 2.5. We remark that the inclusion map restricted to $\mathbb{A}^2_K$ maps into $\mathbb{P}^2_K$.

We will soon provide a different method to obtain points in the projective plane. Prior to this, we will require the following definition. It will allow us to define zeros of a polynomials in the projective plane.

Definition 2.6. Let F be a polynomial in variables X, Y and Z with coefficients in K. Recall that each term of F is of the form $cx^i y^j z^k$, with $c \in K$ and positive integers $i, j, k \geq 0$. Then F is said to be *homogeneous of degree* n if $i + j + k = n$ for each term of F.

Every non-homogeneous polynomial in X and Y can be made homogeneous by adding suitable powers of Z. For example, the polynomial $g(x, y) = x^3 + y^2$ is not homogeneous. Inserting appropriate powers of z results in the polynomial

$$G(x, y, z) = x^3 + y^2 z,$$

which is homogeneous of degree 3.

If $F(x, y, z)$ is a polynomial over K which is homogeneous of degree n, then it can easily be seen that $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ for any $\lambda \in K^*$. Note that this does not hold if F is not homogeneous. In particular this shows that the roots of F in $\mathbb{P}^2_K$ do not depend on the choice of representative for the equivalence class $(x : y : z)$. Therefore, the set of zeros of F in $\mathbb{P}^2_K$ is well-defined.

The inclusion map (1) serves as helpful tool to transform polynomials in the affine plane into homogeneous polynomials in the projective plane. Let $f(x, y)$ be a polynomial and let F be the corresponding homogeneous polynomial of degree n. Then it holds that $F(x : y : z) = z^n f(x/z, y/z)$. By setting $z = 1$, this equality establishes that $f(x, y) = F(x : y : 1)$.

We will now see that two parallel lines in the affine plane actually intersect in a unique point in the projective plane. Assume we have two distinct parallel lines $by = ax + r$, and $dy = cx + s$. Their homogeneous equations are given by $by = ax + rz$ and $dy = cx + sz$. We now have two cases to consider.

- *Case 1:* $b \neq 0$. Since we assumed the lines to be parallel, we can immediately deduce that $d \neq 0$. Therefore, we can write $y = (ax + rz)/b$ and $y = (cx + sz)/d$. Equating both expressions forces either $r/b = s/d$ or $z = 0$. If the first equation holds, then the lines are equal. We assumed that they are not, so we must have that $z = 0$. This implies $y = (a/b)x = (c/d)x$. Definition 2.1 of the projective space does not allow x, y and z to vanish simultaneously, so $x \neq 0$. It follows that the lines only intersect at the point $(1 : (a/b) : 0) = (b : a : 0)$.

- *Case 2:* $b = 0$. Lines in the xy-plane with $b = 0$ are *vertical lines*. Using the same argument as above, we directly see that $d = 0$. Recall that we are dealing with lines in the xy-plane, so both a and c have to be nonzero. Thus, we can write $x = -(r/a)z$ and $x = -(s/c)z$. Equating both lines forces either $(r/a) = (s/c)$ or $z = 0$. The first equation implies that the lines are equal, so we must have that $z = 0$. Therefore we also have that $x = 0$. It follows that the y-coordinate of the intersection point in $\mathbb{P}^2$ is nonzero. This implies that distinct vertical lines have a single intersection, namely $(0 : y : 0) = (0 : 1 : 0)$.

Remark 2.7. In the second case, we also showed that the projective point $(0 : 1 : 0)$ lies on every vertical line in the xy-plane, as all lines in the proof were arbitrarily chosen. This is a result we will use later.

2.2 Weierstrass equations

There is one concept left to be introduced before we can start our treatment of elliptic curves, namely the *Weierstrass equations*. This will be done in the first part of this subsection. After this matter is handled, we will finally provide a formal definition of elliptic curves. Most of the concepts in this subsection will be presented in the same way as they appear in Washington [11] and Silverman [12].

Definition 2.8. A *Weierstrass equation* is a homogeneous equation of the following form:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2}$$

where the coefficients a_i are elements of the field K. In the remainder of the thesis, we will refer to this equation as the *homogeneous Weierstrass equation*. Notice that the point $(0 : 1 : 0)$ satisfies equation (2) for all possible choices of the a_i's.

By applying the substitutions $x = X/Z$ and $y = Y/Z$, we write the equation in an *affine* form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3}$$

In the rest of the thesis, the notion *Weierstrass equation* will refer to this affine version. The notation (x, y) will be used for any ordered pair in $\mathbb{A}^2$ satisfying (3).

Note that this substitution can be regarded as the inverse of the inclusion map (1), as it maps the point $(x : y : 1)$ on (2) to the point (x, y) satisfying (3). Just like the inclusion map hits all the affine points and none of the points at infinity, the substitutions can only be applied to the affine points.

We will now look for the points at infinity associated with equation (3). Its homogeneous form is given by (2). To find the points at infinity, we set $Z = 0$ to obtain $X^3 = 0$. Hence, Y is an arbitrary nonzero scalar. Therefore the only point at infinity is $(0 : y : 0) = (0 : 1 : 0)$.

Remark 2.9. We already established that the point $(0 : 1 : 0)$ lies on each vertical line. Since (3) also contains this point, every vertical line intersects the curve at this point.

In order to represent the points at infinity in the environment of the affine plane, we will give a distinct notation to the point $(0 : 1 : 0)$. We will denote it by $\mathcal{O}$ and refer to it as the *point at infinity*. For all intents and purposes, we think of $\mathcal{O}$ as satisfying the affine Weierstrass equation.

We will now introduce a concept intrinsic to the Weierstrass equation. It will turn out to be a defining property of an elliptic curve.

Definition 2.10. Rewrite the Weierstrass equation to obtain the form $f(x, y) = 0$. Then, the equation is said to be *nonsingular* if $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ do not vanish simultaneously at any point on $\{(x, y) : f(x, y) = 0\}$.

All notions mentioned in the beginning of this subsection are now properly introduced. This means that we are fully prepared to state two of the most important definitions in this thesis.

Definition 2.11. An *elliptic curve* defined over a field K is a pair $(E, \mathcal{O})$ such that

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ with } a_i \in K \tag{4}$$

is a nonsingular equation and $\mathcal{O}$ is the point at infinity. For an elliptic curve E, the set of *K-rational points* $E(K)$ is defined to be

$$E(K) = \{(x, y) \in \mathbb{A}^2_K \mid (x, y) \text{ is a solution to } E\} \cup \{\mathcal{O}\}. \tag{5}$$

Remark 2.12. We sometimes use the notation E/K to emphasize that the coefficients of the elliptic curve E are elements of K. If we write $P \in E$, we mean $P \in E(\bar{K})$.

Example 2.13. As an example, consider the following elliptic curve E defined over $\mathbb{Q}$:

$$E : y^2 = x^3 + 3x.$$

As Definition 2.11 requires, this curve is indeed nonsingular. We will later show how this can be deduced. Note that the points $(1, \pm 2)$ are in $E(\mathbb{Q})$ (whereas the points $(-1, \pm 2i)$ are not).

For later use, we will define the following values associated to an elliptic curve in Weierstrass form. All the coefficients a_i are understood to be elements of K.

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned} \tag{6}$$

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

As we mentioned earlier, there exist useful tools which help to determine whether a curve is nonsingular or not. It will be introduced in the definition below.

Definition 2.14. The *discriminant* of an elliptic curve E/K is defined as

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{7}$$

If it is clear from the context which elliptic curve we mean, $\Delta(E)$ will be denoted as Δ.

The discriminant provides an easy way to check whether a Weierstrass equation is also an elliptic curve. This will be the content of the next theorem. Its proof is omitted.

Theorem 2.15. A curve defined by the Weierstrass equation (3) is elliptic if and only if $\Delta \neq 0$.

The next concept will later prove to be a nice tool to classify maps between elliptic curves. More on this matter will follow in the next subsection.

Definition 2.16. Let E be an elliptic curve defined over K. If Δ is nonzero, the *j-invariant* of the elliptic curve E is defined as

$$j(E) = \frac{c_4^3}{\Delta}. \tag{8}$$

If it is clear which elliptic curve we are referring to, we will write j instead of $j(E)$.

We now introduced some of the intrinsic properties of elliptic curves. However, we have not yet verified whether the representation of an elliptic curve is unique. This question will concern us in the start of the next subsection.

2.3 Isomorphisms between Weierstrass equations

The Weierstrass equation for an elliptic curve is not precisely unique. However it can be shown that the only possible change of variables preserving the Weierstrass form of the equation and fixing $\mathcal{O}$ has to be of a certain form.

In order to find those transformations, we will first require the definitions of some specific kinds of maps. We will start by introducing the most general type, which is the morphism. Its definition is stated as by Smith [13].

Definition 2.17. A *morphism of elliptic curves* $\phi : E \to E'$ is a polynomial mapping

$$\phi : (X : Y : Z) \mapsto (\phi_1(X, Y, Z) : \phi_2(X, Y, Z) : \phi_3(X, Y, Z)),$$

where the ϕ_i are homogeneous polynomials of equal degree, satisfying the defining equation of E' up to a scaling. A morphism has the property that if for $P \in E(\bar{K})$ we have that $\phi_1(P), \phi_2(P)$ and $\phi_3(P)$ are not all zero, it follows that $(\phi_1(P) : \phi_2(P) : \phi_3(P))$ lies on E'.

In affine coordinates, ϕ will be a *rational* map (with denominators).

$$\phi : (x, y) \mapsto \left(\frac{\phi_1(x, y, 1)}{\phi_3(x, y, 1)}, \frac{\phi_2(x, y, 1)}{\phi_3(x, y, 1)} \right).$$

This rational map extends automatically to a polynomial map when we 'complete' the curves in projective space. By cleaning up the denominators, an equivalent definition by Orzech [14] in affine coordinates can be obtained. It is provided below.

Definition 2.18. Let E and E' be two elliptic curves defined over K. A *morphism of elliptic curves* is a map $\phi : E \to E'$ for which there exists polynomials $\phi_1, \phi_2 \in K[X, Y]$ satisfying

$$\phi(x, y) = (\phi_1(x, y), \phi_2(x, y))$$

for all $P = (x, y) \in E_1$.

The next theorem establishes that morphisms of elliptic curves are divided into two categories. We will later see that this distinction is useful, as some definitions and theorems only discuss one of the two types. The theorem, as found in Silverman [12] will be presented without proof.

Theorem 2.19. A morphism of elliptic curves is either a constant function or a surjective function.

We will now list definitions for three different types of morphisms. Without exception, the definitions are stated in the same way as is Silverman [12].

Definition 2.20. Let E and E' be two elliptic curves defined over K and let the map $\phi : E \to E'$ be a morphism. We say that ϕ is an *isomorphism of elliptic curves* if there exists a morphism $\phi^{-1} : E' \to E$ such that $\phi \circ \phi^{-1}$ is the identity map on E, and $\phi^{-1} \circ \phi$ is the identity map on E'. If an isomorphism exists, we refer to E and E' as being *isomorphic*. This is denoted by $E \simeq E'$.

Remark 2.21. If ϕ in Definition 2.20 is an isomorphism, it immediately follows that ϕ^{-1} is an isomorphism as well.

Definition 2.22. Let E be an elliptic curve defined over K. A morphism from E to itself is called an *endomorphism* if it fixes $\mathcal{O}$. An endomorphism that is also an isomorphism is said to be an *automorphism*.

In affine coordinates, isomorphisms can shown to be of a particular form. This fact is formalized in the next theorem, as found in Silverman [12]. We will present it without proof.

Theorem 2.23. Let E and E' be elliptic curves defined over K. Then, every isomorphism $\phi : E \to E'$ over $\bar{K}$ is of the form

$$\phi(x, y) = (u^2 x + r, u^3 y + u^2 s x + t), \tag{9}$$

where r, s, t and $u \in \bar{K}$, and u is nonzero. For an ϕ to be an isomorphism over K, it is required that $r, s, t \in K$ and $u \in K^*$.

In Theorem 2.23, the restrictions on the constants r, s, t, and u ensure that the transformation is invertible. Therefore, its inverse also defines an admissible change of variables mapping E' to E. It is given by

$$\phi^{-1}(x', y') = \left(\frac{x' - r}{u^2}, \frac{y' - u^2 s x' - t}{u^3} \right).$$

The change of coordinates given by (9) is called an *admissible change of variables*. It is important to note that this transformation preserves the j-invariant, although proving this result requires a rather tedious calculation, which can be found in [12].

Theorem 2.24. Two elliptic curves E and E' (over K) are isomorphic over $\bar{K}$ if and only if $j(E) = j(E')$. In other words, the j-invariant classifies elliptic curves up to isomorphisms.

Remark 2.25. In the next subsection, we will prove Theorem 2.24 in the case that $\mathrm{char}(K) \neq 2, 3$. For the proof of the remaining cases we refer to Silverman [12].

We will now focus on isomorphisms between elliptic curves defined over K such that $\mathrm{char}(K) \neq 2, 3$.

2.3.1 Isomorphisms of E with char$(K) \neq 2, 3$.

Suppose that the characteristic of K is different from 2 and 3. In this case the Weierstrass equation can be simplified. In particular, the following change of variables is properly defined since we can divide the coefficients by multiples of 2 or 3.

$$(x, y) \to \left(x - \frac{b_2}{12}, y - \frac{a_1}{2}\left(x - \frac{b_2}{12} \right) - \frac{a_3}{2} \right).$$

This results in a different Weierstrass equation of the given curve, which is called a *short Weierstrass form*, namely

$$E : y^2 = x^3 - 27c_4 x - 54c_6 := x^3 + Ax + B. \tag{10}$$

Because of its simpler form, we will often assume that $\text{char}(K) \neq 2, 3$ as it allows us to work with this shorter expression.

For convenience, we state the equations for j and Δ corresponding to the short Weierstrass form.

$$\Delta = -16(4A^3 + 27B^2) \quad \text{and} \quad j = -1728\frac{(4A)^3}{\Delta}.$$

Lemma 2.26. Let E and E' be elliptic curves over a field K, given by short Weierstrass equations. Let $u \in \bar{K}^*$. Then every isomorphism ϕ over $\bar{K}$ between those curves assumes the form

$$\phi(x, y) = \left(u^2 x, u^3 y \right).$$

Proof. The coordinate transformation (9) acts on the short Weierstrass equation (10) as follows:

$$\begin{aligned} y^2 &\to (u^3 y + u^2 sx + t)^2 \\ &= u^6 y^2 + 2u^5 sxy + 2u^3 ty + u^4 s^2 x^2 + 2u^2 stx + t^2, \end{aligned}$$

and

$$\begin{aligned} x^3 + Ax + B &\to (u^2 x + r)^3 + A(u^2 x + r) + B \\ &= u^6 x^3 + u^4 r x^2 + 3u^2 r^2 x + r^3 + u^2 Ax + Ar + B. \end{aligned}$$

In the short Weierstrass form, the terms xy, y and x^2 do not appear. Therefore

$$\begin{aligned} 2u^5 sxy &= 0 \\ 2u^3 ty &= 0 \\ u^4 s^2 x^2 &= 0 \\ u^4 r x^2 &= 0. \end{aligned}$$

As u (and its powers) are nonzero, the above equations force $r = s = t = 0$. Substituting these values in (9) then yields the lemma. □

In Theorem 2.24, we stated that two elliptic curves E and E', both defined over K, are isomorphic over $\bar{K}$ if and only if $j(E) = j(E')$. However, this is not necessarily true over K. This subtlety is illustrated in the next example.

Example 2.27 (Twist of elliptic curves)**.** Suppose $\mathrm{char}(K) \neq 2, 3$ and consider the curves E and $E^{(d)}$ over K, defined below.

$$\begin{aligned} E : y^2 &= x^3 + Ax + B, \\ E^{(d)} : y'^2 &= x'^3 + Ad^2x' + Bd^3, \\ d^{-3}y'^2 &= d^{-3}x'^3 + Ad^{-1}x' + B. \end{aligned}$$

The coefficient d is an element of K^*. The j-invariants of E and E' are equal, as can be seen in the following calculation.

$$j(E) = \frac{(4A)^3}{4A^3 + 27B^2} = \frac{d^3(4A)^3}{d^3(4A^3 + 27B^2)} = j(E^{(d)}).$$

By comparing both curve equations, we deduce that $y = d^{-3/2}y'$ and $x = d^{-1}x'$. If d is a square in K, then both coordinate transformations are defined over K. If d is not a square in K, then the transformation of the y-coordinate requires a transformation over the field $K(\sqrt{d})$. Therefore, when two curves defined over K have equal j-invariants, this does not ensure that they are isomorphic over K.

As promised in the previous subsection, will now prove Theorem 2.24 with some restriction on the characteristic of the field K.

Proof of Theorem 2.24. Let E and E' be elliptic curves over K, with $\mathrm{char}(K) \neq 2, 3$. Then, both curves allow a short Weierstrass form. Their equations are given as follows.

$$\begin{aligned} E : y^2 &= x^3 + Ax + B, \\ E' : y'^2 &= x'^3 + A'x' + B'. \end{aligned}$$

Suppose that the curves are isomorphic, so that $x = u^2x'$ and $y = u^3y'$ as stated by Lemma 2.26. We then obtain the following equations.

$$\begin{aligned} y^2 &= x^3 + Ax + B, \\ u^6y'^2 &= u^6x'^3 + Au^2x' + B, \\ y'^2 &= x'^3 + Au'^{-4}x' + u^{-6}B. \end{aligned} \tag{11}$$

Comparing this last expression with the curve equation of E', we deduce that $A'u^4 = A$ and $B'u^6 = B$. We further calculate

$$\begin{aligned} \Delta(E) &= -16(4A^3 + 27B^2) = -16(4u^{12}A^3 + 27u^{12}B') = u^{12}\Delta(E') \\ j(E) &= -1728\frac{(4A)^3}{\Delta(E)} = -1728\frac{u^{12}(4A')^3}{u^{12}\Delta(E')} = j(E'). \end{aligned}$$

This shows that the j-invariant is indeed preserved under isomorphisms.

Now suppose we have $j(E) = j(E')$, and let the curve equations be given as in the beginning of the proof. The condition on the j-invariant implies that

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

From this we can deduce that $A^3B'^2 = A'^3B^2$. We now have several cases to consider.

1. *Case 1:* $A = 0$. Note that $B \neq 0$, since otherwise $\Delta(E) = 0$. This forces $A' = 0$. In turn, the system of equations (11) implies that $B = u^6 B$. Therefore $u = (B/B')^{1/6}$.

2. *Case 2:* $B = 0$. Following the same reasoning as in Case 1, we quickly deduce that $A \neq 0$ and $B' = 0$. Implementing these constraints on the system of equations (11) forces $Au^2 = A'u^6$. Taking $u = (A/A')^{1/4}$ will do the job.

3. *Case 3:* $AB \neq 0$. This condition immediately forces that $A'B' \neq 0$. The value $u = (A/A')^{1/4} = (B/B')^{1/6}$ provides the required change of variables.

In each case it follows that a suitable change of coordinates can be defined. This concludes our proof. □

2.4 Addition law on elliptic curves

Up to now, we have seen how elliptic curves can be represented, and how these representations are related. The inner structure of the points on an arbitrary elliptic curve is yet to be discussed. This will soon change, as we are about to define a group structure on them. We will first do this geometrically, but explicit formulas will be provided in the latter part of this subsection.

2.4.1 The geometric construction

Let E be an elliptic curve over given by a Weierstrass equation and let L be a line in the projective plane. The curve E and L have exactly three intersection points, as the defining equation of E has degree three. This fact is a special case of Bézout's Theorem which is discussed in Hartshorne [15]. We will label these intersection points by P, Q and R. In the case that L is tangent to E, these points are not distinct.

We will now define a composition law on E, that we will denote by $+$. We emphasize that the law will be constructed geometrically, without regard for the field in which

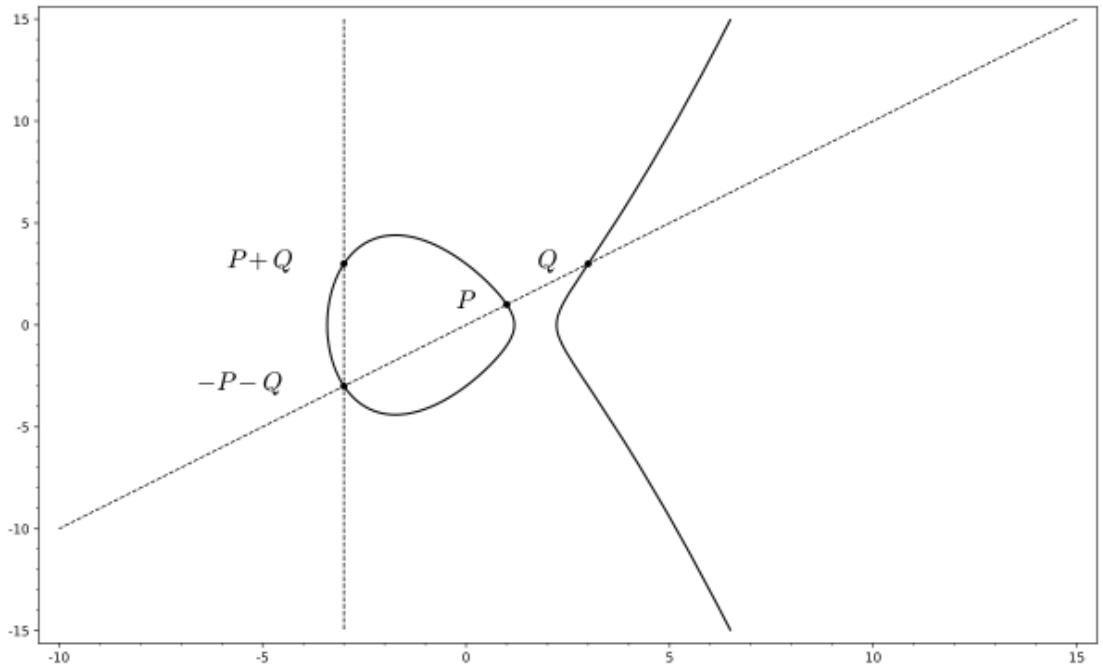

Figure 1: The addition of the points $P = (1, 1)$ and $Q = (3, 3)$ on the elliptic curve $y^2 = x^3 - 9x + 9$

the coordinates of the points lie. The composition law will therefore not mention any particular field.

Composition law. Let $P, Q \in E$ and let L be the line through P and Q. If P and Q coincide, let L be the tangent line of E at P. Let R denote the additional point of intersection of L with E. Let L' be the vertical line through R (and $\mathcal{O}$). The third intersection point of L' and E is defined to be $P + Q$.

The procedure we just described to determine $P + Q$ is often referred to as the *chord-tangent law*. An example of this process can be seen in Figure 1. It can be shown that this method defines an additive abelian group law on E, with $\mathcal{O}$ as the zero element.

Theorem 2.28. $(E(\bar{K}), +, \mathcal{O})$ is an abelian group.

Proof. Let P, Q and R be arbitrary points of the elliptic curve $(E, \mathcal{O})$. We will show that all abelian group axioms are satisfied.

1. $P + Q = Q + P$: The line through P and Q is of course the same as the line through Q and P, so the chord-tangent process yields $P + Q = Q + P$.

2. $P + \mathcal{O} = P$: Let L be the line through $\mathcal{O}$ and P. Note that this line is vertical. Denote by R the third point of intersection of L and E. Then it is easy to see that the line through $\mathcal{O}$ and R also intersects P.

3. *There is a point* $-P$ *such that* $P + (-P) = \mathcal{O}$: Denote by R the intersection point of E with the vertical line through P. Then the line L through P and R additionally intersects E at $\mathcal{O}$. Therefore, $P + R = \mathcal{O}$, so $(-P) = R$. Note that $\mathcal{O} + P = P$ for all points on E. Since the tangent of E at $\mathcal{O}$ has a triple intersection with E, it follows that $-\mathcal{O} = \mathcal{O}$.

4. $(P + Q) + R = P + (Q + R)$: The proof of this property is nontrivial, but it can be found in Silverman [12]. A more geometric proof is given in Fulton [16].

This shows that $(E(\bar{K}), +)$ is an abelian group with $\mathcal{O}$ as the identity element. □

2.4.2 Explicit formulas

With the geometric construction of the group in mind, we will now provide explicit algebraic formulas for the group law we just defined. We will first do this for the complete Weierstrass equation. Later, we will list the addition formulas which solely apply to elliptic curves in short Weierstrass form.

Let E be an elliptic curve over K, given by a Weierstrass equation.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Furthermore, let $P = (x, y)$ be an arbitrary point on E. Also, let P_1, P_2 and P_3 be points on E. Let their respective coordinates be given by $P_i = (x_i, y_i)$. Suppose $P_1 + P_2 = P_3$. The formulas which make up the addition law on E will be listed below. While doing this, we will closely follow the notation as used by Silverman [12].

(a) $-P = (x, -y - a_1x - a_3)$.

(b) If $P_1 = -P_2$, then $P_1 + P_2 = \mathcal{O}$.

(c) If $P_1 \neq -P_2$, then define λ and ν by the following formulas:

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

When $P_1 \neq P_2$, then the line $M : y = \lambda x + \nu$ passes through both P_1 and P_2. If $P_1 = P_2$, then M is the tangent line at P_1. The coordinates of P_3 are as follows:

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3. \end{aligned}$$

As announced at the start of this subsection, we will now list the addition formulas specifically for elliptic curves which admit a short Weierstrass form. This requires the additional assumption that the defining field K satisfies $\mathrm{char}(K) \neq 2, 3$. If E is such a curve, then it can be written as follows.

$$E : y^2 = x^3 + Ax + B.$$

Just as it is with the Weierstrass equation, the addition laws become simpler, which makes them easier to deal with.

Let $P = (x, y) \in E$. Moreover, consider the points P_1, P_2 and $P_3 \in E$, with $P_i = (x_i, y_i)$. Suppose $P_1 + P_2 = P_3$.

(a) $-P = (x, -y)$.

(b) If $P_1 = -P_2$, then $P_1 + P_2 = \mathcal{O}$.

(c) If $P_1 \neq -P_2$, then define λ and ν by the following formulas.

	λ	ν
$x_1 \neq x_2$	$\frac{y_2 - y_1}{x_2 - x_1}$	$\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$
$x_1 = x_2$	$\frac{3x_1^2 + A}{2y_1}$	$\frac{-x_1^3 + Ax_1 + 2B}{2y_1}$

Table 1: Formulas for λ and ν.

The line $M : y = \lambda x + \nu$ passes through P_1 and P_2. In the case that $P_1 = P_2$, the line M is the tangent line at P_1. The coordinates of the point P_3 are as follows:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= -\lambda x_3 - \nu. \end{aligned} \tag{12}$$

To get more familiar with the formulas, we will demonstrate the addition law on a particular curve defined over $\mathbb{Q}$.

Example 2.29 (Adding two points on a curve)**.** Let the short Weierstrass equation of the elliptic curve $E/\mathbb{Q}$ be given as

$$E : y^2 = x^3 - 34x + 37.$$

Let $P = (x_1, y_1) = (1, 2)$ and $Q = (x_2, y_2) = (6, 7)$. Using the formulas in Table 1, we calculate

$$\lambda = \frac{7-2}{6-1} = 1.$$

By equations (12), it follows that

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 = 1 - 1 - 6 = -6, \\ y_3 &= \lambda(x_1 - x_3) - y_1 = 1 - -6 - 2 = 5. \end{aligned}$$

Hence, $P + Q = (-6, 5)$.

Note that for all cases in any characteristic, the addition law on a curve E is entirely expressed by rational functions consisting solely of elements of K. This fact implies that the K-rational points of E form a subgroup.

Theorem 2.30. Let E be an elliptic curve defined over K. Then $E(K)$ is a subgroup of $E(\bar{K})$.

Proof. We need to show that all subgroup axioms are satisfied.

1. $\mathcal{O} \in E(K)$: This holds trivially because of Definition 2.11.
2. *If* $P, Q \in E(K)$ *then* $P + Q \in E(K)$*:* The action of the addition law on both coordinates can be expressed by rational functions of elements in K, as noted earlier. This implies that if $P, Q \in E(K)$, then indeed $P + Q \in E(K)$.
3. *If* $P \in E(K)$ *then* $-P \in E(K)$*:* From the formulas of the addition law, it can easily be deduced that if P has coordinates in K, then the same holds for $-P$.

Indeed, not a single axiom is violated. This concludes the proof. □

Remark 2.31. The isomorphisms described by (9) become group isomorphisms between $E(K)$ and $E'(K)$, as they preserve the group structure. This in particular holds when $\mathrm{char}(K) \neq 2, 3$. We recall that the form of these isomorphisms can be found in Lemma 2.26.

2.5 Endomorphisms

As we established the group structure of elliptic curves, we are now in the position to study the maps on these groups. Especially, we are interested in maps that preserve the group structure.

Definition 2.32. Let E and E' be two elliptic curves defined over K. A *homomorphism of elliptic curves* is a morphism $\alpha : E \to E'$ such that for all $P, Q \in E(K)$, we have that $\alpha(P + Q) = \alpha(P) + \alpha(Q)$.

Remark 2.33. Note that a homomorphism α necessarily fixes $\mathcal{O}$. We see this by noting that $\alpha(\mathcal{O}) = \alpha(\mathcal{O} + \mathcal{O}) = \alpha(\mathcal{O}) + \alpha(\mathcal{O})$. This equality only holds when $\alpha(\mathcal{O}) = \mathcal{O}$.

It turns the we have already encountered homomorphisms earlier in this thesis. This notion is formalized below. The proof can be found in Silverman [12], but is omitted here.

Theorem 2.34. Any morphism of elliptic curves that fixes $\mathcal{O}$ is a homomorphism.

Remark 2.35. Recall that any nonconstant morphism is surjective. Therefore, any nonconstant morphism is automatically a surjective homomorphism.

We now have all the tools required to define a very specific kind of homomorphism. This map will be the main topic of this section.

Definition 2.36. An *endomorphism* of an elliptic curve E is a surjective homomorphism $\alpha : E(\bar{K}) \to E(\bar{K})$. Equivalently, this entails that

$$\alpha(x, y) = \big(R_1(x, y), R_2(x, y)\big),$$

where R_1 and R_2 are both rational functions in x and y.

Remark 2.37. In the previous section, another definition of endomorphism was provided (see Definition 2.22). It should come as no surprise that it is in fact equivalent to Definition 2.36. We will not prove this here.

In what follows, we list a number of different examples of endomorphisms.

Example 2.38 (Trivial endomorphism)**.** Suppose E is an elliptic curve over K. Then, the constant function $\alpha(x, y) = \mathcal{O}$ is an endomorphism. Indeed, for any two points P and Q on E, we have that $\alpha(P + Q) = \mathcal{O}$, and $\alpha(P) + \alpha(Q) = \mathcal{O} + \mathcal{O} = \mathcal{O}$. We will refer to this map as the *trivial endomorphism*.

Example 2.39 (Involution)**.** Let E be an elliptic curve over K given by a short Weierstrass equation. (Note that this means that we assume $\mathrm{char}(K) \neq 2, 3$). Let $P = (x, y)$ and $Q = (x', y')$ be points on E. We define

$$\begin{aligned} \iota : E(K) &\to E(K), \\ (x, y) &\mapsto (x, -y). \end{aligned}$$

We first assume that $P \neq Q$. To show that ι is an endomorphism, we calculate $\iota(P+Q)$ and $\iota(P)+\iota(Q)$.

$$\begin{aligned}\iota(P+Q) &= \iota(\lambda^2 - x - x', \lambda(x - \lambda^2 + x + x') - y),\\ &= (\lambda^2 - x - x', \lambda(\lambda^2 - 2x - x') + y).\end{aligned}$$

$$\begin{aligned}\iota(P)+\iota(Q) &= \iota(x,y) + \iota(x',y'),\\ &= (x,-y) + (x',-y'),\\ &= ((-\lambda)^2 - x - x', -\lambda(-\lambda^2 + 2x + x') + y),\\ &= ((-\lambda)^2 - x - x', \lambda(\lambda^2 - 2x - x') + y).\end{aligned}$$

Both calculations yield the same result. In the case that $P = Q$, this result can be shown by this same method. The proof in the case $P = -Q$ is trivial. For this reason, both calculations are omitted.

So indeed ι defines an endomorphism. Note that ι composed with itself yields the identity map. Any map with this property is referred to as an *involution*. Since in our case ι is specifically applied to points on elliptic curves, ι is called an *elliptic curve involution*.

Example 2.40 (Multiplication by an integer)**.** For a positive integer m we denote by $[m]$ the *multiplication-by-m* map from an elliptic curve E to itself. This map is indeed an endomorphism. It is a fact which we will not prove, but still often refer to. It is defined as follows. Let $P \in E$.

$$\begin{aligned}[m] : E &\to E\\ P &\mapsto \underbrace{P + P + \cdots + P}_{m \text{ summands}}\end{aligned}$$

This definition can be extended to all integers, by defining $[0]P = \mathcal{O}$ and setting $[-m]P = -[m]P$. This map plays an essential role in elliptic curve cryptography. Its properties and computation will keep recurring throughout the remainder of the thesis.

Example 2.41 (Complex multiplication by ζ_3)**.** Let $E : y^2 = x^3 + B$ be an elliptic curve over a field K, which contains an nontrivial root of unity ζ_3. The map

$$\begin{aligned}[\zeta_3] : E(K) &\to E(K)\\ (x,y) &\mapsto (\zeta_3 x, y)\end{aligned}$$

is well-defined, as the image is always a point in $E(K)$. This can easily be seen by noting that $(\zeta_3 x)^3 = x^3$. We will show that $[\zeta_3]$ is an automorphism of E. To this end, let $P_1 = (x_1, y_2)$ and $P_2 = (x_2, y_2)$ be points in $E(K)$.

In case $x_1 \neq x_2$, the formulas in Table 1 and the equations (12) say that

$$[\zeta_3](P_1 + P_2) = (\zeta_3\lambda^2 - \zeta_3 x_1 - \zeta_3 x_2, -\lambda\zeta_3(2x_1 - x_2) + y_1).$$

We will now compute $[\zeta_3](P_1) + [\zeta_3](P_2)$. To make this easier, we will first determine λ' (the equivalent of λ) for the points $[\zeta_3](P_1)$ and $[\zeta_3](P_2)$.

$$\begin{aligned}\lambda' &:= \frac{y_2 - y_1}{\zeta_3 x_2 - \zeta x_1} \\ &= \frac{1}{\zeta_3}\lambda.\end{aligned}$$

It follows that

$$\begin{aligned}[\zeta_3](P_1) + [\zeta_3](P_2) &= (\frac{1}{{\zeta_3}^2}\lambda^2 - \zeta_3 x_1 - \zeta_3 x_2, \frac{-\zeta_3\lambda}{\zeta_3}(2\zeta_3 x_1 + \zeta_3 x_2) + y_1) \\ &= (\zeta_3\lambda^2 - \zeta_3 x_1 - \zeta_3 x_2, -\lambda(2x_1 + x_2) + y_1) \\ &= [\zeta_3](P_1 + P_2).\end{aligned}$$

The proof for the case $x_1 = x_2$ follows the same steps, and yields the same result. This proves that $[\zeta_3]$ is indeed an endomorphism. Since $\zeta_3 \notin \mathbb{R}$, we say that E has *complex multiplication by* ζ_3.

A very similar proof will show that the map $[\zeta_3^2] : (x, y) \to (x\zeta_3^2, y)$ also defines an endomorphism on E. It is easy to see that both $[\zeta_3] \circ [\zeta_3^2]$ and $[\zeta_3^2] \circ [\zeta_3]$ are the identity map on E. This establishes that $[\zeta_3]$ defines an automorphism on E.

2.6 Properties of endomorphisms

In the previous subsection, we defined an endomorphism as an ordered pair of coordinate functions in two variables. It turns out that, in a sense, we can reduce this number to one. Proving this matter will be our concern in the first part of this subsection. However, we should note that this reduction can only be made when the elliptic curves involved admit a short Weierstrass form. Therefore, any elliptic curve E (defined over a field K with $\mathrm{char}(K) \neq 2, 3$) mentioned in this subsection is given in the form

$$E : y^2 = x^3 + Ax + B.$$

The reduction in the number of variables subsequently means that proving theorems about endomorphisms will be easier. We will repeatedly exploit this simplification in the latter part of this subsection.

Let α be an arbitrary endomorphism of the curve E. We know that α can be written as $\alpha(x, y) = (R_1(x, y), R_2(x, y))$, where the R_i denote rational functions. We will now illustrate how and why it is possible to write both R_i as functions in one variable.

We first take $R(x, y)$ to be any rational function. If an even power of y occurs in either its numerator or its denominator, we can replace it by a suitable power of $x^3 + Ax + B$. This

fact simply follows from the definition of the short Weierstrass form (10). Therefore, we may assume that $R(x, y)$ takes the following form:

$$R(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

We can cancel out the y in the denominator by multiplying both its denominator and numerator by $p_3(x) - p_4(x)y$, and performing substitutions of the powers of y. We obtain the following expression.

$$R(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{13}$$

We recall that if P is a point on E, then the addition law forces $-P = -(x, y) = (x, -y)$. Thus, $\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y)$. In terms of the coordinate functions, this has the following implications.

$$R_1(x, -y) = R_1(x, y) \text{ and } R_2(x, -y) = -R_2(x, y).$$

The condition imposed on R_1 requires that $q_2(x)$ in Equation (13) vanishes. Furthermore, the constraint on R_2 implies that q_1 vanishes as well. This reduces R_1 to a rational function in the single variable x, and it reduces R_2 to a rational function in x multiplied by y. We will formalize the result below.

Theorem 2.42. Let E be an elliptic curve which admits a short Weierstrass form. Let α be any endomorphism on E. Then α can be assumed to have the following form:

$$\alpha(x, y) = (r_1(x), r_2(x)y). \tag{14}$$

In the above equations, both r_i denote rational functions.

What happens when one of the denominators of either r_i vanishes? Let $r_1(x) = p(x)/q(x)$ and assume p and q have no common factors. If $q(x)$ vanishes at a certain $a \in \bar{K}$, we set $\alpha(a, b) = \mathcal{O}$. As the following theorem shows, r_2 is defined whenever $q(x) \neq 0$, so α is completely defined.

Theorem 2.43. Let E be an elliptic curve admitting a short Weierstrass form. Let $\alpha(x, y) = (p(x)/q(x), ys(x)/t(x))$ be any endomorphism of E. Assume that p and q have no common roots and that s and t have no common roots. Then $t(x)$ is defined whenever $q(x)$ is defined.

Proof. We first note that $r_2(x) = s(x)/t(x)$ is only defined when $t(x)$ does not vanish. We then note that both (x, y) and $\alpha(x, y)$ are points on E, which means that they both satisfy the same Weierstrass equation. We obtain the following equalities, where the

variable x is left out to improve readability.

$$\begin{aligned}\frac{y^2s^2}{t^2} &= \frac{p^3}{q^3} + \frac{pAx}{q} + B \\ &= \frac{p^3 + pq^2Ax + Bq^3}{q^3} \\ &=: \frac{u(x)}{q^3}.\end{aligned} \tag{15}$$

In the last equality, $u(x) = p^3+pq^2Ax+Bq^3 = p^3+q(pqAx+Bq^2)$. We now substitute y^2 with the cubic from the short Weierstrass equation and we obtain the following:

$$\frac{(x^3 + Ax + B)s^2}{t^2} = \frac{u}{q^3}$$

We now show that u and q have no common roots. Assume for contradiction that $b \in \bar{K}$ is a common root. Then $q^3 = m(x)(x-b)^3$ and $u = f(x)(x-b)$. In order to factor u like this, all summands of u have to contribute the factor $q = (x-b)$. This requires that $p^3 = g(x)(x-b)$. Since p^3 has only triple roots, we must have that $p^3 = h(x)(x-b)^3$. In particular, it follows that p^3 and q^3 share a root, implying that p and q share a root. This contradicts the assumption in the statement of Theorem 2.43, which states that they do not share a root. It follows that u and q have no common roots.

We moreover note that t^2 and y^2 have no common roots. Every root of t^2 has to be a double one, but Definition 2.11 prohibits y^2 to have a double root. Using the last equality of (15), we have that

$$y^2s^2q^3 = ut^2.$$

If $t(x_0) = 0$ then $t^2(x_0) = 0$. This automatically implies that both $y^2(x_0)$ and $s^2(x_0)$ do not vanish. In order to preserve the equality, we must have $q^3(x_0) = 0$ and therefore $q(x_0) = 0$. Hence $t(x_0) = 0$ implies $q(x_0) = 0$. Conversely, $q(x_0) \neq 0$ forces $t(x_0) \neq 0$, which is what we wanted to prove. □

We will now introduce some useful properties of endomorphisms. As a reminder, we still assume that the elliptic curve E admits a short Weierstrass form. For this exact reason, the concepts that we will introduce only apply to such curves.

Definition 2.44. Let E be an elliptic curve, and let $\alpha = (r_1(x), r_2(x)y)$ be any endomorphism on E. If α is nontrivial, then the *degree* of α is defined as follows.

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}.$$

In the case that α is the trivial endomorphism, we set $\deg(\alpha) = 0$.

Definition 2.45. Let α be as in Definition 2.44. If α is nontrivial, then α is said to be *separable* if the derivative of $r_1(x)$ is not identically zero.

The following lemma is provides a useful criterion to check whether Definition 2.45 is satisfied.

Lemma 2.46. Let E and α be as in Definition 2.44, and write $r_1(x) = p(x)/q(x)$. If α is a nontrivial endomorphism, then it is separable if either $p'(x)$ or $q'(x)$ is nonzero.

Proof. By Definition 2.45, α is separable if $r_1'(x) \neq 0$. This condition can be written as follows.

$$\frac{d}{dx}\left(\frac{p}{q}\right) = \frac{p'q - pq'}{q^2} \neq 0.$$

Note that we can prove the lemma by showing that the equivalence holds for the negation of both statements. This means that it is sufficient to prove that $r_1'(x) = 0$ if and only if both p and q are constant functions. If that is the case, then $p' = q' = 0$. This implies that $pq' - p'q$ vanishes, so $r_1'(x) = 0$.

Now we will prove the other direction of the equivalence. To this end, assume that $p'q - pq' = 0$. Note the we can assume that p and q do not have any roots in $\bar{K}$, as we can always cancel out any common factors. It follows from our assumption that every root of p in $\bar{K}$ must also be root of p', and it must have at least the same multiplicity. Because $\deg(p') < \deg(p)$, this can only occur when $p' = 0$. Similarly, we can deduce that $q' = 0$. This shows that both p and q are constant functions. □

The following theorem describes the relation between the degree of an endomorphism and the order of its corresponding kernel. A good proof of this can be found in Washington [11].

Theorem 2.47. Let E denote an elliptic curve, and let α any nontrivial endomorphism on E. If α is separable, then the following equality holds.

$$\deg(\alpha) = \#\mathrm{Ker}(\alpha).$$

In the case that α is not separable, this previous expression will be an inequality, namely

$$\deg(\alpha) > \#\mathrm{Ker}(\alpha).$$

Remark 2.48. Actually, Theorem 2.47 also holds for elliptic curves not in the short Weierstrass form, as can be seen in Silverman [12]. Since we have not defined the notion of degree for those curves, we will not provide it here.

3 Torsion points and the Weil pairing

3.1 Torsion points

When discussing any group, elements of finite order are always of special interest. They are usually referred to as *torsion elements*. The term *torsion group* is commonly used when talking about the subgroups of elements of finite order.

We will devote the first part of this subsection to define the torsion subgroups of $E(\bar{K})$. We will subsequently characterize their structure, and we will study how homomorphisms on those groups can be represented. We want to emphasize that we again only consider elliptic curves E admitting a short Weierstrass form.

Definition 3.1. Let E be an elliptic curve over a field K. Take n to be any positive integer. Then, the *n-torsion group* consists of the following points.

$$E[n] = \{P \in E \mid [n]P = \mathcal{O}\}$$

Note that $E[n]$ consists of all points whose order divides n. Moreover, we underline the fact that the coordinates of the points in $E[n]$ do not necessarily belong to K.

As we announced, we will now focus on the structure of $E[n]$. It can be characterized by the following theorem, whose proof can be found in Washington [11].

Theorem 3.2. Let E be an elliptic curve defined over K, and take n to be any positive integer. If $\mathrm{char}(K) \nmid n$, or if $\mathrm{char}(K) = 0$, then

$$E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n.$$

If $\mathrm{char}(K) = p \mid n$, then write $n = p^r n'$, with $p \nmid n'$. In that case,

$$E[n] \simeq \mathbb{Z}_{n'} \times \mathbb{Z}_{n'} \text{ or } E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_{n'}.$$

Using the terminology introduced in Theorem 3.2, we will now define some specific kinds of elliptic curves, which will be classified by the structure of particular torsion groups.

Definition 3.3. Let E be an elliptic curve defined over K. Suppose that $\mathrm{char}(K) = p$. Then, E is a *supersingular* curve if $E[p] \simeq \{\mathcal{O}\}$. In the case that $E[p] \simeq \mathbb{Z}_p$, we refer to E as an *ordinary* curve.

Definition 3.3 will not appear anywhere in the remainder of this thesis, but it is still useful to be aware of these particular notions.

As mentioned in the start of this paragraph, we will now study how torsion groups can be used to represent homomorphisms. Prior to this, we want to ensure that any homomorphism on E maps torsion points to torsion points.

Theorem 3.4. Let E be an elliptic curve and let α be any homomorphism on E. Let n be any positive integer such that $\text{char}(K) \nmid n$. Then, α maps $E[n]$ to $E[n]$.

Proof. We want to emphasize that both α and the multiplication-by-n map are homomorphisms. In particular, this implies that for an arbitrary $P \in E[n]$ we have that $n\alpha(P) = \alpha(nP) = \alpha(\mathcal{O}) = \mathcal{O}$. This means that $\alpha(P) \in E[n]$. □

Just as in Theorem 3.4, we take n to be any positive integer such that $\text{char}(K) \nmid n$. By Theorem 3.2 it follows that $E[n]$ is of the form $\mathbb{Z}_n \times \mathbb{Z}_n$. This allows us to fix a 2-element basis, which we will denote by $\{T_1, T_2\}$, so that every element of $E[n]$ is of the form $s_1T_1 + s_2T_2$, where both s_i are uniquely determined modulo n.

The action of α on the basis can be written as follows:

$$\alpha(T_1) = \alpha_{11}T_1 + \alpha_{21}T_2, \quad \alpha(T_2) = \alpha_{12}T_1 + \alpha_{22}T_2. \tag{16}$$

As both $\alpha(T_i)$ are elements of $E[n]$, all the α_{ij} belong to $\mathbb{Z}_n$. Another representation will be provided in the next theorem, which can also be found in Washington [11].

Theorem 3.5. Let E be an elliptic curve over K. Let $\alpha : E \to E$ be a homomorphism. Its action on a basis of $E[n]$ can be expressed by a matrix with elements in $\mathbb{Z}_n$.

$$\alpha_n := \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.$$

As we will now encounter, we can compose homomorphisms by simply multiplying their representative matrices.

Corollary 3.6. Let α and β be homomorphisms on E. Denote by α_n and β_n their respective matrices, when restricted to $E[n]$. Then the matrix of $\alpha \circ \beta$ equals $\alpha_n \cdot \beta_n$.

Proof. Let

$$\alpha_n = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \text{ and } \beta_n = \begin{pmatrix} \beta_{11} & \beta_{12} \\ \\ \beta_{21} & \beta_{22} \end{pmatrix}.$$

A straightforward calculation shows

$$\alpha_n\beta_n = \begin{pmatrix} \alpha_{11}\beta_{11} + \alpha_{12}\beta_{21} & \alpha_{11}\beta_{12} + \alpha_{12}\beta_{22} \\ \\ \alpha_{21}\beta_{11} + \alpha_{22}\beta_{21} & \alpha_{21}\beta_{12} + \alpha_{22}\beta_{22} \end{pmatrix}.$$

Applying the map $\alpha \circ \beta$ on $\{T_1, T_2\}$ yields

$$\begin{aligned} \alpha(\beta(T_1)) &= \alpha(\beta_{11}(T_1)) + \alpha(\beta_{21}(T_2)) \\ &= \beta_{11}(\alpha(T_1)) + \beta_{21}(\alpha(T_2)) \\ &= \alpha_{11}\beta_{11}T_1 + \alpha_{21}\beta_{11}T_2 + \alpha_{12}\beta_{21}T_1 + \alpha_{22}\beta_{21}T_2 \\ &= (\alpha_{11}\beta_{11} + \alpha_{12}\beta_{21})T_1 + (\alpha_{21}\beta_{11} + \alpha_{22}\beta_{21})T_2 \\ &=: c_{11}T_1 + c_{21}T_2. \end{aligned}$$

$$\begin{aligned} \alpha(\beta(T_2)) &= \alpha(\beta_{12}(T_1)) + \alpha(\beta_{22}(T_2)) \\ &= \beta_{12}\alpha(T_1) + \beta_{22}(\alpha(T_2)) \\ &= \alpha_{11}\beta_{12}T_1 + \alpha_{21}\beta_{12}T_2 + \alpha_{12}\beta_{22}T_1 + \alpha_{22}\beta_{22} \\ &= (\alpha_{11}\beta_{12} + \alpha_{12}\beta_{22})T_1 + (\alpha_{21}\beta_{21} + \alpha_{22}\beta_{22})T_2 \\ &=: c_{12}T_1 + c_{22}T_2. \end{aligned}$$

Comparing the expressions c_{ij} with the coefficients of $\alpha_n\beta_n$ leads us to conclude that the action matrix of $\alpha \circ \beta$ is indeed represented by $\alpha_n\beta_n$. Therefore, this shows that the composition of homomorphisms is indeed equivalent to the multiplication of their corresponding matrices. □

If we wish to get an even better understanding of torsion groups, it is necessary to take a closer look at the multiplication maps on elliptic curves by an integer m. We will make these maps explicit in the next section.

3.2 Division Polynomials

As we have already seen in Example 2.40, the multiplication-by-n map on an elliptic curve E is an endomorphism. An explicit form of such a map is yet to be provided, but we will soon state a theorem which will do exactly that.

The building blocks of these maps, the *division polynomials*, deserve some more attention. In particular, their relation to torsion points is quite remarkable. The study of these polynomials will be done in the latter part of this subsection.

Unlike the previous subsection, E will denote an elliptic curve defined over a field K which does not necessarily admit a short Weierstrass form, i.e.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The corresponding constants b_2, b_4, b_6 and b_8 are defined as in (6). We are now ready to give state the explicit form of an arbitrary multiplication-by-n map. The proof of this is far from trivial and it is demonstrated in Silverman [12].

Theorem 3.7. Let E be an elliptic curve defined over a field K, and let m be any positive integer. There exist polynomials ψ_m, θ_m, $\omega_m \in K[X,Y]$ such that, for all points $P = (x,y) \in E(\bar{K})$ such that $P \notin E[m]$, we have that

$$[m]P = \left(\frac{\theta_m(x,y)}{\psi_m(x,y)^2}, \frac{\omega_m(x,y)}{\psi_m(x,y)^3} \right) \tag{17}$$

When expressing the map $[m]$ like this, it becomes easier to imagine what the degree of this map might be. The exact degree is provided by the following theorem, the proof of which can be found in Silverman [12] and is omitted here.

Corollary 3.8. Let E be an elliptic curve and let m any positive integer. Then the multiplication-by-m endomorphism has degree m^2.

The polynomial ψ_m as in Theorem 3.7 is the *m-th division polynomial* of the curve E. We will later demonstrate how the polynomials θ_m and ω_m are recursively defined in terms of ψ_m.

We will now list the exact expressions of ψ_m. We emphasize that these apply to any elliptic curve, even those which do not admit a short Weierstrass equation. The coefficients b_i are as defined in (6).

$$\begin{aligned}
\psi_0 &= 0, \\
\psi_1 &= 1, \\
\psi_2 &= 2Y + a_1X + a_3, \\
\psi_3 &= 3X^4 + b_2X^3 + 3b_4X^2 + 3b_6X + b_8, \\
\psi_4 &= \psi_2 \cdot \left(2X^6 + b_2X^5 + 5b_4X^4 + 10b_6X^3 + 10b_8X^2 + (b_2b_8 - b_4b_6)X + (b_4b_8 - b_6^2)\right), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2, \\
\psi_{2m} &= (\psi_2)^{-1}(\psi_m)(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 3.
\end{aligned} \tag{18}$$

As we mentioned earlier, the torsion groups and division polynomials are related in a very special way. In particular, a relation exists between m-torsion points and the roots of the m-th division polynomial, where $m \in \mathbb{Z}_{\geq 1}$. It is formalized in the next corollary, whose proof can also be found in Blake [17].

Theorem 3.9. Let E be an elliptic curve defined over a field K and let $m \in \mathbb{Z}_{\geq 1}$. Let $P = (x,y) \in E(\bar{K}) - \{\mathcal{O}\}$. We have that $P \in E[m]$ if and only if $\psi_m(x,y) = 0$.

One of the key properties of a polynomial is its degree. For our purposes, we are especially interested in the degree of the m-th division polynomial, where m is odd. The next theorem will be useful in that regard. We will present it without proof, which can be found in Blake [17].

Theorem 3.10. Suppose E is an elliptic curve over K, with $\mathrm{char}(K) = p$. Let m be odd, and suppose that $p \nmid m$. Then,

$$\deg \psi_m = \frac{m^2 - 1}{2}$$

Remark 3.11. If m is even, then we have that $\deg(\psi_m/\psi_2) = (m^2 - 4)/2$. We do not need this fact in the remainder of thesis, but we provide it here for completeness.

Theorem 3.9 and Theorem 3.10 form the main ingredients for our next corollary. It concerns the multiplicity of the roots of ψ_m.

Corollary 3.12. Let E be an elliptic curve over K with $\mathrm{char}(K) = p$. Suppose m is odd, and suppose that $p \nmid m$. Then, the roots of ψ_m are simple.

Proof. By Theorem 3.9, we have that the roots of ψ_m are exactly the x-coordinates of the points in $E[m]^*$. As $p \nmid m$, Theorem 3.2 says that $\#E[m] = m^2$. This implies that $\#E[m]^* = m^2 - 1$, which corresponds to $(m^2 - 1)/2$ distinct x-coordinates. By Theorem 3.9, these are all roots of ψ_m. By Theorem 3.10, we have that $\deg \psi_m = (m^2 - 1)/2$. This implies that all the roots of ψ_m are distinct, so they are simple. □

Looking at the list of equations (18), we see that Y only appears in the division polynomials via ψ_2. The following lemma about ψ_2 soon turn out to be quite useful.

Lemma 3.13. The polynomial $(\psi_2)^2$ is independent of Y.

Proof.

$$\begin{aligned}
\psi_2^2(x, y) &= (2Y + a_1X + a_3)^2, \\
&= 4Y^2 + 4Y(a_1X + a_3) + a_1X + a_3, \\
&= 4(Y^2 + a_1XY + a_3Y) + a_1X + a_3, \\
&= 4(X^3 + a_2X^2 + a_4X + a_6) + a_1X + a_3.
\end{aligned}$$

In the 4th equation, we used the fact that the left hand side of the Weierstrass equation (3) can be expressed as a polynomial in X. □

As we stated earlier, Lemma 3.13 will prove to be quite useful. Its result allows us to show that the division polynomials ψ_m can be represented in terms of univariate polynomials.

Theorem 3.14. If m is odd, then $\psi_m \in \mathbb{Z}[a_1, \cdots, a_6, X]$. If m is even, then we have $\frac{1}{(2\psi_2)}(\psi_m) \in \mathbb{Z}[a_1, \cdots, a_6, X]$.

Proof. We will prove it by using induction on m. We can see that the statement holds for all $0 \leq m \leq 4$. Suppose the statement holds for all $m < 2n$. Note that we can assume that $2n > 4$, so $n > 2$, and consequently $2n > n + 2$. Note that all subscripts in the recurrence relation for both ψ_{2m} ψ_{2m+1} do not exceed $m + 2$. The induction hypothesis then states that the theorem holds for all polynomials appearing in their respective expressions. We now have two cases to consider:

1. *m is odd:* By the induction hypothesis, it follows that the expressions for both ψ_{m+2} and ψ_{m-2} do not contain Y. Moreover, the hypothesis states that both $(\psi_{m-1})^2$ and $(\psi_{m+1})^2$ contain the factor $4\psi_2^2$. The induction hypothesis also entails that the variable Y does not occur in the product $(\psi_2)^{-1}(\psi_m)$. Therefore, ψ_{2m} is a multiple of ψ_2^2. The lemma directly forces that in this case $\psi_{2m} \in Z[a_1, \cdots, a_6, X]$.

2. *m is even:* By the hypothesis we have that both ψ_{m-1}^2 and ψ_{m+1}^2 are polynomials solely in the variable X. The induction hypothesis tells us that ψ_m ψ_{m-2} and ψ_{m+2} are elements of $(2\psi_2)\mathbb{Z}[a_1, \cdots a_6, X]$. All these factors considered, it follows that $\psi_{2m} \in (2\psi_2)\,\mathbb{Z}[a_1, \cdots, a_6, X]$. Therefore, $(2\psi_2)^{-1}\psi_{2m} \in \mathbb{Z}[a_1, \cdots, a_6, X]$.

It follows that the statement holds for $m = 2n$. In a similar matter, it can be shown that the theorem holds for $2m + 1$. □

So far in this subsection, we provided a quite lengthy list of properties division polynomials. Recall that the expression for multiplication endomorphism by equation (17) also contains two other polynomials, denoted as θ_m and ω_m. We will now briefly focus on those. In particular, we will show how both polynomials are recursively defined in terms of ψ_m. This relation can also be found in Silverman [12] and Blake [17].

Definition 3.15. Let $m \in \mathbb{Z}_{\geq 1}$. The recursive formulae for θ_m and ω_m are stated below.

$$\theta_m = X\psi_m^2 - \psi_{m-1}\psi_{m+1}, \tag{19}$$

$$2\psi_2\omega_m = \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2. \tag{20}$$

After having dealt with curves in the long Weierstrass form, we will conclude this subsection by providing a list division polynomials especially for curves admitting a short Weierstrass form. The coefficients a_i and b_i as provided by the equations (6) can all be reduced. From this process, we obtain the following system of equations.

$$
\begin{aligned}
a_1 &= 0 & b_2 &= 4a_2 = 0\\
a_2 &= 0 & b_4 &= 2a_4 = 2A\\
a_3 &= 0 & b_6 &= 4a_6 = 4B\\
a_4 &= A & b_8 &= -a_4^2 = -A^2.\\
a_6 &= B
\end{aligned}
$$

Using these expressions, the division polynomials assume the following form.

$$
\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2Y,\\
\psi_3 &= 3X^4 + 6AX^2 + 12BX - A^2,\\
\psi_4 &= 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - A^3 - 8B^2),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2,\\
\psi_{2m} &= (2Y)^{-1}(\psi_m)(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 3.
\end{aligned}
\tag{21}
$$

3.3 The Weil Paring

As the title of this subsection suggests, we will study the *Weil pairing*, a map with a lot of useful properties. In particular, it will allow us to relate the degree of an endomorphism to the determinant of its matrix representative. More about the origins of the Weil pairing can be found in Washington [11], which also includes the proof of the next theorem.

Any elliptic curve E we encounter will admit a short Weierstrass form

$$E : y^2 = x^3 + Ax + B.$$

Theorem 3.16. Let n be a positive integer such that $\text{char}(K) \nmid n$. Then there is a map

$$e_n : E[n] \times E[n] \to \mu_n$$

called the *Weil pairing*, which satisfies all of the following properties.

(a) e_n is linear in both variables. This means that for arbitrary elements S, S_1, S_2, T, T_1, T_2 of $E[n]$, it satisfies the following equations:

$$
\begin{aligned}
e_n(a_1S_1 + a_2S_2, T) &= e_n(S_1, T)^{a_1} e_n(S_2, T)^{a_2},\\
e_n(S, b_1T_1 + b_2T_2) &= e_n(S, T_1)^{b_1} e_n(S, T_2)^{b_2}
\end{aligned}
$$

With a_i and $b_i \in \mathbb{Z}$.

(b) e_n is non-degenerate in each variable. This means that if $e_n(S,T) = 1$ for all $T \in E[n]$, then $S = \mathcal{O}$. Moreover, if $e_n(S,T) = 1$ for all $S \in E[n]$, then $T = \mathcal{O}$.

(c) $e_n(T,T) = 1$ for all $T \in E[n]$.

(d) $e_n(\sigma S, \sigma T) = \sigma(e_n(S,T))$ for all automorphisms σ over $\bar{K}$ which fix the elements in K.

(e) $e_n(\alpha(S), \alpha(T)) = e_n(S,T)^{\deg(\alpha)}$ for all separable endomorphisms α of E.

Note that part (c) implies that $e_n(S,T) = e_n(T,S)^{-1}$. This can be seen by noting that

$$\begin{aligned} 1 =& e_n(S+T, S+T) \\ =& e_n(S+T, T+S) \\ =& e_n(S, T+S) \cdot e_n(T, T+S) \\ =& e_n(S,T) \cdot e_n(S,S) \cdot e_n(T,T) \cdot e_n(T,S) \\ =& e_n(S,T) \cdot e_n(T,S) \end{aligned}$$

We now immediately get the first helpful consequence of the properties of the Weil pairing, stated below.

Theorem 3.17. Let E be an elliptic curve over K, and let n be an integer such that $\mathrm{char}(K) \nmid n$. Let $\{T_1, T_2\}$ denote a basis for $E[n]$. In that case, $e_n(T_1, T_2)$ is a primitive n-th root of unity.

Proof. Recall that x is a primitive n-th root of unity when $x^d = 1$ if and only if $n \mid d$. Assume that $e_n(T_1, T_2) = \mu$, with $\mu^d = 1$. Property (1) of the Weil pairing implies that $e_n(T_1, dT_2) = e_n(T_1, T_2)^d = 1$. We also note that property (3) allows us to deduce that $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$. For any $T \in E[n]$, the the following equality holds:

$$e_n(T, dT_2) = e_n(aT_1 + bT_1, dT_2) = e_n(T_1, dT2)^a e_n(T_2, dT_2)^b = 1.$$

Because the Weil pairing is non-degenerate, this equality states that $dT_2 = \mathcal{O}$. It follows that d must be a multiple of n by recalling that $T_2 \in E[n]$. This proves the theorem. □

As we already announced at the start of this subsection, the properties of the Weil pairing allow us to relate the degree of an endomorphism α on E to the determinant of the corresponding matrix α_n. This result will be formalized in the next proposition. We will repeat here that α_n represents the action of α on a basis $\{T_1, T_2\}$ of $E[n]$.

Proposition 3.18. Let E be an elliptic curve defined over K. Let α be an endomorphism on E, and let $n \in \mathbb{Z}$ be such that $n \nmid \mathrm{char}(K)$. In that case, we have $\det(\alpha_n) \equiv \deg(\alpha) \mod n$.

Proof. Let $\{T_1, T_2\}$ be a basis for $E[n]$. Then Theorem 3.17 tells us that $e_n(T_1, T_2) = \mu_n$, where μ_n is a primitive n-th root of unity. Let $\alpha_n = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then, we have

$$\begin{aligned}
\mu_n^{\deg \alpha} &= e_n(\alpha(T_1), \alpha(T_2)), \\
&= e_n(aT_1 + cT_2, bT_1 + dT_2), \\
&= e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{cd}, \\
&= e_n(T_1, T_2)^{ad} e_n(T_1, T_2)^{-bc}, \\
&= e_n(T_1, T_2)^{ad-bc}, \\
&= \mu_n^{\det(\alpha_n)}.
\end{aligned}$$

The first equality follows from (e) of the Weil pairing, the second one is from (16). The third and fourth equality follow from part (a) and (c) of Theorem 3.16, respectively. So we get $\deg \alpha \equiv \det(\alpha_n) \mod n$. Since we have just shown that μ is a primitive nth root of unity, the proposition follows. □

This result can be generalized a bit. If a, b are both positive integers and α, β denote two endomorphisms on a curve E, then we can define a new endomorphism pointwise. If we consider an arbitrary $P \in E$, this endomorphism is constructed as follows:

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

In the above expression, both a and b denote multiplication endomorphisms on E. The next proposition can be found in Washington [11]. Its result will help us to calculate easily the degree of the composite endomorphism we just introduced.

Proposition 3.19. Let a, b, α and β be as stated above. Then the following equality holds:

$$\deg(a\alpha + b\beta) = a^2 \deg(\alpha) + b^2 \deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta).$$

Remark 3.20. The proof only suffices for certain types of endomorphisms, namely separable endomorphisms and the Frobenius endomorphism ϕ_q. (We are still unfamiliar with this latter map, but we will make up for this in the next section). However, the proposition holds for all endomorphisms.

Proof. Let $n \in \mathbb{Z}$ be positive and such that $\mathrm{char}(K) \nmid n$. We emphasize here that infinitely many such n exist. Furthermore, let the matrices α_n and β_n denote the action of α and β, respectively, on a basis $\{T_1, T_2\}$ of $E[n]$. Hence $(a\alpha_n + b\beta_n)$ represents the action of $(a\alpha + b\beta)$. Let

$$\alpha_n = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}, \quad \beta_n = \begin{pmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{pmatrix}. \tag{22}$$

With this representation, one easily calculates

$$\det(\alpha_n) = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}, \quad \det(\beta_n) = \beta_{11}\beta_{22} - \beta_{12}\beta_{21}. \tag{23}$$

For later convenience, we will explicitly calculate the determinant of $(\alpha_n + \beta_n)$. This computation is skipped in the proof by Washington [11]. We have

$$\begin{aligned}\det(\alpha_n + \beta_n) &= (\alpha_{11} + \beta_{11})(\alpha_{22} + \beta_{22}) - (\alpha_{12} + \beta_{12})(\alpha_{21} + \beta_{21}) \\ &= \alpha_{11}\alpha_{22} + \alpha_{11}\beta_{22} + \alpha_{22}\beta_{11} + \beta_{11}\beta_{22} - \alpha_{12}\alpha_{21} - \alpha_{12}\beta_{21} - \alpha_{21}\beta_{12} - \beta_{12}\beta_{21}.\end{aligned} \tag{24}$$

To ease notation, we denote

$$\begin{aligned}M &:= a\alpha_n + b\beta_n \\ &= \begin{pmatrix} a\alpha_{11} + b\beta_{11} & a\alpha_{12} + b\beta_{12} \\ a\alpha_{21} + b\beta_{21} & a\alpha_{22} + \beta_{22} \end{pmatrix}.\end{aligned}$$

Then, we have that

$$\begin{aligned}\det(M) = a^2(\alpha_{11}\alpha_{22}) + b^2(\beta_{11} + \beta_{22}) + ab(\alpha_{11}\beta_{22} + \alpha_{22}\beta_{11}) \\ - a^2(\alpha_{12}\alpha_{21}) - b^2(\beta_{12}\beta_{21}) - ab(\alpha_{12}\beta_{21} + \alpha_{21}\beta_{12}).\end{aligned}$$

Some rewriting yields

$$\begin{aligned}\det(M) = a^2(\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}) + b^2(\beta_{11}\beta_{22} - \beta_{12}\beta_{21}) \\ + ab(\alpha_{11}\beta_{22} + \alpha_{22}\beta_{11} - \alpha_{12}\beta_{21} - \alpha_{21}\beta_{12}).\end{aligned}$$

Substituting the identities given by (23) gives the following:

$$\begin{aligned}\det(M) = a^2\det(\alpha_n) + b^2(\alpha_n) + ab(\alpha_{11}\alpha_{22} - \alpha_{11}\alpha_{22} + \alpha_{11}\beta_{22} + \alpha_{22}\beta_{11} + \beta_{11}\beta_{22} - \\ \beta_{11}\beta_{22} - \alpha_{12}\alpha_{21} + \alpha_{12}\alpha_{21} - \alpha_{12}\beta_{21} - \alpha_{21}\beta_{12} - \beta_{12}\beta_{21} + \beta_{12}\beta_{21})\end{aligned}$$

We now rearrange the terms once more, which yields

$$\begin{aligned}\det(M) = a^2\det(\alpha_n) + b^2(\alpha_n) + ab\big[\alpha_{11}\alpha_{22} + \alpha_{11}\beta_{22} + \alpha_{22}\beta_{11} + \beta_{11}\beta_{22} \\ - \alpha_{12}\alpha_{21} - \alpha_{12}\beta_{21} - \alpha_{21}\beta_{12} - \beta_{12}\beta_{21}) - \{(\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}) + (\beta_{11}\beta_{22} - \beta_{12}\beta_{21})\}\big].\end{aligned}$$

Finally, inserting the identity given by (24) allows us to write the desired result:

$$\begin{aligned}\det(a\alpha_n + b\beta_n) &= \det(M), \\ &= a^2\det(\alpha_n) + b^2\det(\beta_n) + ab(\det(\alpha_n + \beta_n) - \det(\alpha_n) - \det(\beta_n)).\end{aligned}$$

Using Proposition (3.18) then yields

$$\deg(a\alpha_n + b\beta_n) \equiv a^2\deg(\alpha) + b^2\deg(\beta) + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)) \mod n.$$

As we mentioned earlier, this congruence is satisfied for infinitely many integers. This is only possible if the above expression is an equality and the subscript n can be dropped. This concludes the proof. □

4 Elliptic curves over finite fields

In what follows, we will focus on elliptic curves over a particular set of fields, namely the finite fields. Before we can study elliptic curves over finite fields, we will first need to get familiar with finite fields themselves.

In particular, we will devote this section to study some noteworthy properties of the Frobenius endomorphism. This map will play a major role in the remainder of the thesis. Its importance stems from the fact that it possesses some special properties. Among other things, it can be used to construct other endomorphisms.

Here is an example of an elliptic curve over a finite field:

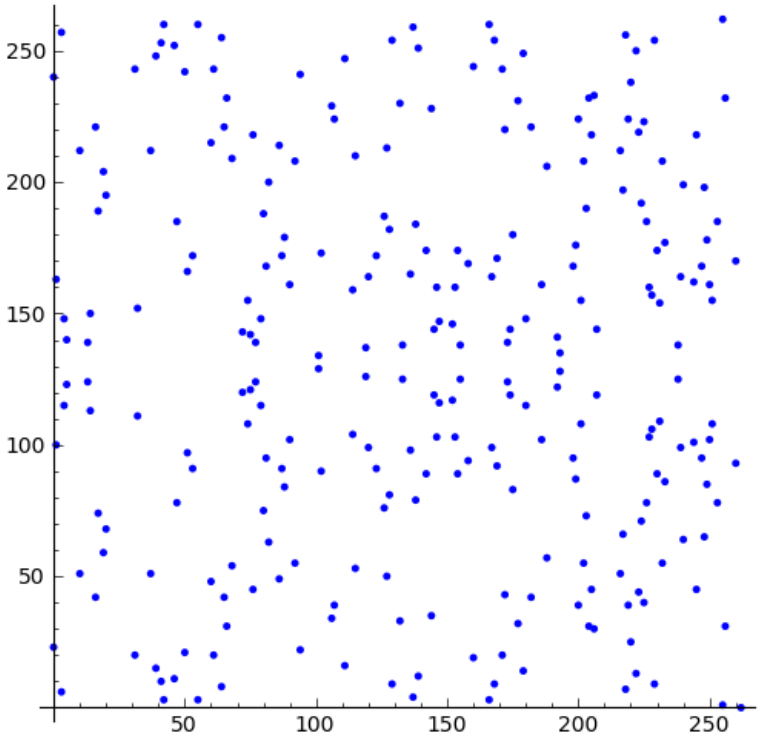

Figure 2: The elliptic curve $E : Y^2 = X^3 + 2X + 3$ over the finite field $\mathbb{F}_{263}$ (Bauer, [18])

Remark 4.1 (Notation)**.** Unless specified differently, we will use $\mathbb{F}_q$ to denote a finite field consisting of q elements, where $q = p^n$ for a prime p and positive integer n. We will denote by $\bar{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$. Furthermore, $\mathbb{F}_p$ represents a field with p elements, where p is a prime. Its algebraic closure will be denoted by $\bar{\mathbb{F}}_p$.

4.1 The Frobenius map on $\bar{\mathbb{F}}_q$

Definition 4.2. The *Frobenius map* ϕ_q on $\bar{\mathbb{F}}_q$ is defined as follows:

$$\begin{aligned} \phi_q : \bar{\mathbb{F}}_q &\to \bar{\mathbb{F}}_q, \\ x &\mapsto x^q. \end{aligned} \tag{25}$$

In what follows, the next well-known result will be used. We will omit the proof.

Theorem 4.3.

$$\bar{\mathbb{F}}_p = \bigcup_{n \geq 1} \mathbb{F}_{p^n}. \tag{26}$$

Remark 4.4. This in particular implies that $\mathbb{F}_q \subset \bar{\mathbb{F}}_p$. In fact, it holds that $\bar{\mathbb{F}}_q = \bar{\mathbb{F}}_p$. A proof of this fact can be found in Washington [11].

The following theorem will explicitly state what this embedding looks like.

Theorem 4.5.

$$\mathbb{F}_q = \{x \in \bar{\mathbb{F}}_p \mid \phi_q(x) = x\}. \tag{27}$$

Proof. Denote by S the set of roots of $f(X) = X^q - X$. It is trivial to note that $0^q = 0$. Recall that the multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ has order $q-1$, so by Fermat's Little Theorem we have that $x^q = x^{q-1}x = x$ for all $x \in \mathbb{F}_q^*$. Therefore, we get $\mathbb{F}_q \subset S$.

We recall the fact that a polynomial has a multiple root if and only if it shares a root with its derivative. We calculate

$$\frac{d}{dX}(X^q - X) = qX^{q-1} - 1 = -1 \mod p.$$

This shows that $f'(X)$ has no roots, so particular it has no roots in common with $f(X)$. From this we may conclude that $f(X)$ has q distinct roots. We thus have that S has the same order as $\mathbb{F}_q$. Considering the fact that $\mathbb{F}_q \subset S$, it follows that the sets must be equal. □

Furthermore, we will prove the following useful result.

Theorem 4.6. The map ϕ_q is an automorphism of $\bar{\mathbb{F}}_q$. In particular,

$$\phi_q(x+y) = \phi_q(x) + \phi_q(y) \text{ and } \phi_q(xy) = \phi_q(x)\phi_q(y). \tag{28}$$

Proof. Indeed, for all $x, y \in \bar{\mathbb{F}}_q$ we have that $\phi(xy) = (xy)^q = x^q y^q = \phi_q(xy)$.

Note that the binomial coefficient $\binom{p}{j}$ has a factor p in its numerator, which is not cancelled in the denominator when $1 \leq j \leq p-1$. Equivalently, all binomial coefficients vanish in $\mathbb{F}_p$ when $j \neq 0$ or p. Therefore,

$$\begin{aligned}(x+y)^p &= \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}x^{p-1}y + \binom{p}{p}y^p \\ &= x^p + y^p.\end{aligned}$$

Now we use induction on the power n of p to derive this same result for $\mathbb{F}_q$. Obviously, it holds that $(x+y)^{p^1} = x^{p^1} + x^{p^1}$. Now assume that $(x+y)^{p^n} = x^{p^n} + x^{p^n}$. We then calculate

$$\begin{aligned}(x+y)^{p^{n+1}} &= \left((x+y)^{p^n}\right)^p \\ &= (x^{p^n} + y^{p^n})^p \\ &= (x^{p^n})^p + (y^{p^n})^p \\ &= x^{p^{n+1}} + y^{p^{n+1}}.\end{aligned}$$

It follows by induction that $(x+y)^{p^n} = x^{p^n} + x^{p^n}$ for all $n \in \mathbb{Z}_{n\geq 1}$. In particular, this shows that $(x+y)^q = x^q + y^q$. We conclude that ϕ_q is a homomorphism of fields. To show that ϕ_q is moreover an automorphism, we still need to prove that it is bijective.

We will first see that ϕ_q is injective. We know that $0^q = 0$. Now, let x be a nonzero element of $\bar{\mathbb{F}}_q$. As ϕ_q is a homomorphism, we have that $1 = \phi_q(x)\phi_q(x^{-1}) = \phi_q(x)\phi_q(x)^{-1}$. From this we deduce that $\phi_q(x)$ has a multiplicative inverse which implies that $\phi_q(x) \neq 0$. It follows that $\phi_q(x) = 0$ if and only $x = 0$, which establishes the injectivity of the Frobenius map.

It now only remains to show that ϕ_q is surjective. If $x \in \bar{\mathbb{F}}_q$, then by Remark 4.4 we have that $x \in \bar{\mathbb{F}}_p$, which means that there exists n such that $x \in \mathbb{F}_{q^n}$. This implies that $\phi_q^n(x) = x$. We therefore have that x lies in the image of ϕ_q. As x was arbitrary, we conclude that ϕ_q is surjective. □

4.2 The Frobenius map on $E(\bar{\mathbb{F}}_q)$

In this section, we will study the Frobenius map on the points of $E(\bar{\mathbb{F}}_q)$. On coordinates, the map is defined as follows:

$$\begin{aligned}\phi_q : E(\bar{\mathbb{F}}_q) &\to E(\bar{\mathbb{F}}_q) \\ (x,y) &\mapsto (x^q, y^q)\end{aligned} \tag{29}$$

By convention, we set $\phi_q(\mathcal{O}) = \mathcal{O}$. We call this map *Frobenius map on an elliptic curve.*

Remark 4.7. Note that the notation for the Frobenius map is identical for $\bar{\mathbb{F}}_q$ and $E(\mathbb{F}_q)$. However, the field over which the map acts will always be clear form the context.

Lemma 4.8. Let $E/\mathbb{F}_q$ be an elliptic curve, and let $(x, y) \in E(\bar{\mathbb{F}}_q)$. The following two results hold.

1. $\phi_q(x, y) \in E(\bar{\mathbb{F}}_q)$.
2. $(x, y) \in E(\mathbb{F}_q)$ if and only if $\phi_q(x, y) = (x, y)$.

Proof of (1): We recall the homogeneous Weierstrass equation (2):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If we raise both sides to the power q, we use the results of Theorems 4.5 and 4.6 to obtain

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6.$$

. This shows that $(x^q, y^q) \in E(\bar{\mathbb{F}}_q)$.

Proof of (2). The result of Theorem 4.5 allows us to write the following equivalences:

$$\begin{aligned} \phi_q(x, y) = (x, y) &\Leftrightarrow \phi_q(x) = x \text{ and } \phi_q(y) = y \\ &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow (x, y) \in E(\mathbb{F}_q). \end{aligned}$$

. □

Remark 4.9. Note that part (2) of Lemma 4.8 implies that $\phi_q^n(x, y) = (x, y)$ if and only if $(x, y) \in E(\mathbb{F}_{q^n})$. This shows us that ϕ_q^n is the Frobenius map on $\mathbb{F}_{q^n}$.

As the Frobenius map is an endomorphism on $\mathbb{F}_q$, it would be a logical step to see whether it is an endomorphism on $E(\mathbb{F}_q)$. The next Lemma will answer this question, and will also provide some additional properties of ϕ_q.

Lemma 4.10. Let E be a curve defined over the finite field $\mathbb{F}_q$. In that case, ϕ_q is a surjective endomorphism on $E(\bar{\mathbb{F}}_q)$ of degree q which is not separable.

Remark 4.11. We give the proof of this lemma only for elliptic curves admitting a short Weierstrass form because we have provided no notion of degree for elliptic curves which do not admit a short Weierstrass form. Nevertheless, Lemma 4.10 also holds for these curves. A proof of this result can be found in Silverman [12].

Proof. As we explained in the remark above, we will assume that E is given by a short Weierstrass form. We will first prove that $\bar{\mathbb{F}}_q$ is a homomorphism given by rational functions. To this end, we will show that $\phi_q(P_1 + P_2) = \phi_q(P_1) + \phi_q(P_2)$ for all $P_1, P_2 \in$

$E(\bar{\mathbb{F}}_q)$. Denote the coordinates of $P_i \in E(\bar{\mathbb{F}}_q)$ by (x_i, y_i). We first assume that $P_1 \neq P_2$, and $P_3 := P_1 + P_2$. Using the formulas in Table 1, we have that

$$\begin{aligned}\lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1.\end{aligned}$$

We now apply ϕ_q to all 3 equations. This results in the following three expressions. We will use the notation λ' to refer to λ^q.

$$\begin{aligned}\lambda' &= \frac{y_2^q - y_1^q}{x_2^q - x_1^q} \\ x_3^q &= \lambda'^2 - x_1^q - x_2^q \\ y_3^q &= \lambda'(x_1^q - x_3^q) - y_1^q.\end{aligned}$$

Since $\phi_q(x_i, y_i) = (x_i^q, y_i^q)$, This shows that $\phi_q(P_1 + P_2) = \phi_q(P_1) + \phi_q(P_2)$. In case $x_1 = x_2$, or at least one of P_1 and P_2 equals $\mathcal{O}$, the result can be verified in a similar way.

We will now check whether the lemma holds in case $P_1 = P_2$. Using the equations in Table 1, we then obtain the following equations.

$$\begin{aligned}\lambda &= \frac{3x_1^2 + A}{2y_1} \\ x_3 &= \lambda^2 - 2x_1 \\ y_3 &= \lambda(x_1 - x_3) - y_1\end{aligned}$$

We emphasize that $2, 3, A \in \mathbb{F}_q$, so they are fixed by ϕ_q. Having said that, raising the equations above to the q-th power yields the following result. As before, we denote λ^q by λ'.

$$\begin{aligned}\lambda' &= \frac{3(x_1^q)^2 + A}{2y_1^q} \\ x_3^q &= \lambda'^2 - 2x_1^q \\ y_3^q &= \lambda'(x_1^q - x_3^q) - y^q.\end{aligned}$$

Indeed, this shows that $\phi_q(2P_1) = \phi_q(P_1) + \phi_q(P_1)$. Therefore, we conclude that ϕ_q is a homomorphism on E.

We note that ϕ_q is rational, as both x^q and y^q are rational functions. This establishes that the Frobenius map is an endomorphism on $E(\bar{\mathbb{F}}_q)$. Since $r_1(x) = x^q$, it is trivial to note that $\deg \phi_q = q$. We also have that $r_1'(x) = qx^{q-1} = 0$, since $q = 0$ in F_q. It follows that ϕ_q is not separable. Theorem 2.19 allows us to conclude that ϕ_q is surjective, by noting that it is a nontrivial morphism. $\square$

Remark 4.12. We would like to repeat the last property of the Weil pairing here:

$$e_n(\alpha(S), \alpha(T)) = e_n(S,T)^{\deg(\alpha)} \text{ for all separable endomorphisms } \alpha \text{ of } E.$$

If the elliptic curve E is defined over $\mathbb{F}_q$, this property also applies when $\alpha = \phi_q$, even though we have just shown that ϕ_q is not separable. Actually, the statement holds for all endomorphisms α, separable of not. (See Washington [11]).

We will now illustrate some other characteristics of ϕ_q. They will involve the notions of division polynomials and torsion group, which we encountered in the previous section.

Theorem 4.13. Let E be an elliptic curve defined over $\mathbb{F}_q$ given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and let ψ_m be the m-th division polynomial. For all points $P \in E(\bar{\mathbb{F}}_q)$, we have that $\psi_m(x^q, y^q) = \psi_m(x,y)^q$.

Proof. We will prove this by induction on m. We have that $0^q = 0$ and $1^q = 1$, so the proof trivially holds for ψ_0 and ψ_1.

Let $(x,y) \in E(\bar{\mathbb{F}}_q)$. By utilizing the results of Theorems 4.5 and 4.6, we have that

$$\begin{aligned}
\psi_2(x,y)^q &= (2y + a_1x + a_3)^q \\
&= (2y + a_1x)^q + a_3^q \\
&= (2y)^q + (a_1x)^q + a_3^q \\
&= 2^q y^q + a_1^q x^q + a_3^q \\
&= 2y^q + a_q x^q + a_3 \\
&= \psi_2(x^q, y^q).
\end{aligned}$$

The proofs for ψ_3 and ψ_4 are similar, so we will omit them here. The result for all integers $n \geq 4$ can be proven by induction. It is analogous to the proof of Theorem 3.14. □

We will now see that the torsion group $E[m]$ of an elliptic curve E over $\mathbb{F}_q$ is invariant under the Frobenius map.

Corollary 4.14. Let E be an elliptic curve over $\mathbb{F}_q$. If $P = (x,y) \in E[m]$, then $(x^q, y^q) \in E[m]$.

Proof. Let $P = (x,y) \in E[m]$. By Theorem 3.9, it follows that $\psi_m(x,y) = 0$. By Theorem 4.13, it follows that $\psi_m(x^q, y^q) = \psi_m(x,y)^q = 0^q = 0$. Again by Theorem 3.9, this implies that $(x^q, y^q) \in E[m]$. □

4.3 Other endomorphisms on $E(\mathbb{F}_q)$

As mentioned earlier, the Frobenius map can be used to construct new endomorphisms on $E(\mathbb{F}_q)$. These endomorphisms are polynomials in ϕ_q of degree 1 or 2, with coefficients in $\mathbb{Z}$. These coefficients are the multiplication endomorphisms, as introduced in Example 2.40. We will use this section to illustrate useful properties about those maps, and also study particular examples of these constructed endomorphisms. We will first focus on endomorphisms of the form $r\phi_q + s$.

Theorem 4.15. Let E be an elliptic curve over $\mathbb{F}_q$ given by $y^2 = x^3 + Ax + B$. Take any two integers r, s, with at least one of them being nonzero. The endomorphism $r\phi_q + s$ is separable if and only if $p \nmid s$.

To prove this theorem, we first require the result of the following two lemmas.

Lemma 4.16. Let E be an elliptic curve over $\mathbb{F}_q$ given by $y^2 = x^3 + Ax + B$. Let α_1, α_2 and α_3 be three nontrivial endomorphisms of E and suppose $\alpha_1 + \alpha_2 = \alpha_3$. We denote $\alpha_j(x, y) = (R_{\alpha_j}(x), yS_{\alpha_j}(x))$. Assume that there are constants c_{α_1} and c_{α_2} such that

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1} \quad \text{and} \quad \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}.$$

Then

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}.$$

Lemma 4.17. Let E be an elliptic curve over K and let n be any positive integer. Denote $p = \mathrm{char}(K)$. Assume that for all $(x, y) \in E(\bar{K})$, multiplication by n on E can be expressed as

$$n(x, y) = (R_n(x), yS_n(x)),$$

where R_n and S_n are rational functions. Then

$$\frac{R'_n(x)}{S_n(x)} = n.$$

Equivalently, we have that multipliciation-by-n map is separable if and only if $p \nmid n$.

Now we have gathered all the tools needed to prove the theorem.

Proof of Theorem 4.15. Write the multiplication-by-r endomorphism as

$$r(x, y) = (R_r(x), yS_r(x)).$$

Then

$$\begin{aligned}(R_{r\phi_q}(x), yS_{r\phi_q}(x)) &= (\phi_q r)(x, y) = (R_r^q(x), y^q S_r^q(x)) \\ &= \big(R_r^q(x), y(x^3 + Ax + B)^{(q-1)/2} S_r^q(x)\big).\end{aligned}$$

It follows that

$$c_{r\phi_q} := R'_{r\phi_q}/S_{r\phi q} = qR_r^{q-1}R'_r/S_{r\phi_q} = 0.$$

By Lemma 4.17, $c_s := R'_s/S_s = s$. Using the result of Lemma 4.16 we have that

$$R'_{r\phi_q+s}/S_{r\phi_q+s} = c_{r\phi_q} + c_s = 0 + s = s.$$

This implies that $R'_{r\phi_q+s} \neq 0$ if and only if $p \nmid s$. □

Remark 4.18. We will now apply Theorem 4.15 in the case where $r = 1$ and $s = -1$. As $p \nmid 1$, we have that $\phi_q - 1$ is separable. Since $\mathrm{char}(\mathbb{F}_{q^n}) = p$ for all integers $n \geq 1$, we also have that $\phi_q^n - 1$ is separable.

Remark 4.19. By Remark 4.9, we know that $\mathrm{Ker}(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$. Since ϕ_q^n is separable by Remark 4.18, we can use the result of Theorem 2.47 to deduce that $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$.

We will now introduce an important constant. In this section, it will mainly serve as a coefficient of polynomials of ϕ_q with degree 2. This will not be its only useful property, as we will see in the following sections.

Definition 4.20. Let E a curve over $\mathbb{F}_q$. Then, the *trace of Frobenius* at q, denoted by a, is defined to be the constant

$$a := q + 1 - \#E(\mathbb{F}_q). \tag{30}$$

This freshly defined constant will immediately play its part in the following lemma.

Lemma 4.21. Let r, s be integers with $\gcd(s, q) = 1$. Then $\deg(r\phi_q - s) = r^2q + s^2 - rsa$.

Remark 4.22. The condition $\gcd(s, q) = 1$ is not necessary. The requirement is included here as we proved Proposition 3.19 only for the Frobenius map and separable endomorphisms.

Proof. We know the degree of ϕ_q by Lemma 4.10. Moreover, we note that the endomorphism $[-1]$ has degree 1. Using Theorem 3.18, we now have the following equality:

$$\begin{aligned}\deg(r\phi_q - s) &= r^2 \deg(\phi_q) + s^2 \deg(-1) + rs\left(\deg(\phi_q - 1) - \deg(\phi_q) - \deg(-1)\right),\\ &= r^2q + s^2 - rs\left(q + 1 - \deg(\phi_q - 1\right),\\ &= r^2q + s^2 - rsa.\end{aligned}$$

By Remark 4.19, we know that $\deg(\phi_q - 1) = \#E(\mathbb{F}_q)$. The third equality then follows from Definition 4.20. □

We will now study polynomials in ϕ_q of degree 2. In particular, we will focus on one specific occurrence of this type of endomorphism. A key aspect of this map will be highlighted in the theorem below.

Theorem 4.23. Let E be an elliptic curve defined over $\mathbb{F}_q$. Let a be the trace of Frobenius. Then

$$\phi_q^2 - a\phi_q + q = 0 \tag{31}$$

as endomorphisms of E, and a is the unique integer k such that

$$\phi_q^2 - k\phi_q + q = 0.$$

In other words, if $(x, y) \in E(\bar{\mathbb{F}}_q)$, then

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = \mathcal{O},$$

and a is the unique integer such that this relation holds for all $(x, y) \in E(\bar{\mathbb{F}}_q)$. Moreover, a is the unique integer satisfying

$$a \equiv \text{Trace}((\phi_q)_m) \mod m \tag{32}$$

for all m with $\gcd(m, q) = 1$.

Proof. Theorem 2.47 states that every nonzero, separable endomorphism has a finite kernel. To show that our endomorphism is trivial, we will prove that its kernel is infinite. Let $m \in Z_{n\geq 1}$ such that $\gcd(m, q) = 1$. Since ϕ_q is a homomorphism, Theorem 3.5 implies that the action of ϕ_q on $E[m]$ can be represented by the matrix $(\phi_q)_m$. We denote

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}.$$

We easily calculate that $\det((\phi_q)_m) = sv - tu$ and $\text{Trace}((\phi_q)_m) = s + v$. We know that $\phi_q - 1$ is separable by Proposition 4.15. Moreover, the results of Theorem 2.47 and Proposition 3.18 allow us to write the following equalities:

$$\begin{aligned} \#\text{Ker}(\phi_q - 1) &= \deg(\phi_q - 1), \\ &\equiv \det((\phi_q)_m - I), \\ &= sv - tu - (s + v) + 1 \mod m. \end{aligned}$$

Note that $sv - tu = \det((\phi_q)_m) = \deg(\phi_q)$ by Proposition 3.18. By Lemma 4.21 it follows that $\#\text{Ker}(\phi_q - 1) = q + 1 - a$. Therefore we can write

$$q + 1 - a \equiv q + 1 - \text{Trace}(\phi_q)_m \mod m.$$

We immediately see that $\text{Trace}((\phi_q)_m) \equiv a \mod m$. Note that the characteristic polynomial of $(\phi_q)_m - I$ is given by $X^2 - aX + q$. Now the Cayley-Hamilton Theorem states that

$$(\phi_q)_m^2 - a(\phi_q)_m + qI \equiv 0 \mod m.$$

This shows that the endomorphism $\phi_q^2 - a\phi_q + q$ is the zero map on $E[m]$. Since we have infinitely many choices for m, it follows that the kernel consists of the union of all sets $E[m]$, which is infinite. As we remarked at the start of the proof, this implies that the endomorphism $\phi_q^2 - aq + q$ is indeed trivial.

We now show that a is unique. Suppose $b \neq 0$ also satisfies $\phi^2 - bq + q = 0$. It follows that

$$(a-b)\phi_q = (\phi^2 - q - bq + q) + (\phi^2 - q - bq + q) = 0.$$

We recall Lemma 4.10 which states that ϕ_q is a surjective endomorphism on $E(\bar{\mathbb{F}}_q)$. This means that the multiplication-by-$(a-b)$ map sends every element of $E(\bar{\mathbb{F}}_q)$ to 0. In particular we have that $E[m]$ gets mapped to 0. Since there are points in $E[m]$ of order m such that $\gcd(m, q) = 1$, we have that $(a-b) \equiv 0 \mod m$ for such m. Again, we note that m can be any positive integer, which forces $a - b = 0$. This proves that a is unique. □

In the following proposition, we want to emphasize two notable results from the previous proof. It also nicely illustrates where the trace of Frobenius a got its name from.

Proposition 4.24. Let E be an elliptic curve over $\mathbb{F}_q$ and let $(\phi_q)_m$ denote the matrix giving the action of the Frobenius ϕ_q on $E[m]$. Let a be the trace of Frobenius. Then

$$\text{Trace}((\phi_q)_m) \equiv a \mod m, \qquad \det((\phi_q)_m) \equiv q \mod m. \tag{33}$$

The polynomial $X^2 - aX + q$ is referred to as the *characteristic polynomial of Frobenius.*

4.4 Structure and order of $E(\mathbb{F}_q)$

After having studied their endomorphisms, it is now time to look at the group $E(\mathbb{F}_q)$ itself. This section will be used to study their structure and cardinality. We will start with the former.

The following theorem reduces the possible structures of $E(\mathbb{F}_q)$ to only two options. We use the formulation given by Washington [11], which we will also refer to for the proof.

Theorem 4.25. Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then $E(\mathbb{F}_q) \simeq \mathbb{Z}_n$ for some integer $n \geq 1$, or $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} + \mathbb{Z}_{n_2}$ for some integers $n_1, n_2 \geq 1$ with $n_1 \mid n_2$.

We will now study the cardinality of $E(\mathbb{F}_q)$. The simple fact that the field $\mathbb{F}_q$ has finitely many elements ensures that the number of points on $E(\mathbb{F}_q)$, denoted by $\#E(\mathbb{F}_q)$, is finite as well. Of course, we are interested in the exact order of $E(\mathbb{F}_q)$. Hasse's Theorem proves to be very useful in this regard. Its remarkable result reduces the number of possible orders to a small interval.

Theorem 4.26 (Hasse, [19])**.** Let E be an elliptic curve defined over $\mathbb{F}_q$. The trace of Frobenius a satisfies

$$|a| < 2\sqrt{q}. \tag{34}$$

Proof. We note that $\deg(r\phi_q - s) \geq 0$. Using Lemma 4.21, this implies that

$$\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0.$$

We will now use the fact that the set of fractions (r/s) with $\gcd(s, q) = 1$ is dense in $\mathbb{R}$. The number s can be taken to be either a power of 2 or a power of 3, one of which must be coprime with q. The sets of rationals of the form $r/2^m$ or $r/3^m$ are both dense in $\mathbb{R}$. From this notion, we can deduce that the following inquality holds for all $x \in \mathbb{R}$.

$$qx^2 - ax + 1 \geq 0.$$

In order for this inequality to be satisfied, the discriminant of the polynomial is either negative or 0. Therefore we require that $a^2 - 4q \leq 0$. The result of Hasse's Theorem follows directly from this inequality. □

The result of Hasse's Theorem can also be stated in terms of *Legendre symbols*, a somewhat general notion which is widely used in group theory.

Definition 4.27. For an odd prime p, the *Legendre symbol* is defined as follows:

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{if } t^2 \equiv x \mod p \text{ has no solution } t \not\equiv 0 \mod p, \\ -1 & \text{if } t^2 \equiv x \mod p \text{ has no solution } t, \\ 0 & \text{if } x \equiv 0 \mod p. \end{cases}$$

This notion can be generalized to any finite field $\mathbb{F}_q$ with q odd by defining, for $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^\times, \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q^\times, \\ 0 & \text{if } x = 0. \end{cases}$$

Theorem 4.28. Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Then

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right).$$

Corollary 4.29. Let $x^3 + Ax + B$ be a polynomial with $A, B \in \mathbb{F}_q$, where q is odd. Then

$$\left| \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right) \right| \leq 2\sqrt{q}.$$

Proof. Recall that the trace of Frobenius $a := \#E(\mathbb{F}_q) - (q+1)$. By Theorem 4.28, this implies that

$$a = \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right).$$

By Hasse's Theorem, the result of Corollary 4.29 immediately follows. □

A well-known fact from group theory is that $\text{ord}(g) | \#G$ for all elements g of a group G. In particular this also holds for an arbitrary point $P \in E(\mathbb{F}_q)$.

5 Point-counting algorithms

This section will be the accumulation of all the previous sections and the previously introduced theory will be applied here.

A naive way to find multiples of $\text{ord}(P)$ would be to check whether $kP = \mathcal{O}$ for every integer k in the interval $[q+1-2\sqrt{q},\ q+q+2\sqrt{q}]$. This procedure is sometimes referred to as the *brute force* method, and requires up to $4\sqrt{q}$ steps. We can do much better then that.

5.1 Baby Step, Giant Step algorithm

Of course, it is desirable that the number of steps be as low as possible. The following algorithm is therefore more suitable than brute force, as it reduces the maximum number of steps by a factor of $q^{1/4}$.

Baby Step, Giant Step
Input: An elliptic curve E over $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$
Output: $\text{ord}(P)$
Maximal number of steps: $4q^{1/4}$

1. Compute $Q = (q+1)P$.
2. Choose an integer m such that $m > q^{1/4}$. Compute and store the points jP for $j = 0, 1, \ldots, m$.
3. Compute the points
$$Q + k(2mP) \text{ for } k = -m, -(m-1), \ldots, m$$
until there is a match $Q + k(2mP) = \pm jP$ with a point (or its inverse) in the stored list.
4. Conclude that $(q + 1 + 2mk \mp j)P = \mathcal{O}$. Let $M = q + 1 + 2mk \mp j$.
5. Factor M and let $p_1, \ldots, p_r$ be the distinct prime factors of M.
6. Compute $(M/p_i)P$ for $i = 1, \ldots, r$. If $(M/p_i)P = \mathcal{O}$ for some i, replace M with M/p_i and go back to step (5). If $(M/p_i)P \neq \mathcal{O}$ for all i, then M is the order of the point P.

Before the algorithm is proved, we first require the result two useful lemmas. The proofs as displayed below can both be found in Washington [11].

Lemma 5.1. Let m be as in the algorithm. Let a be an integer with $|a| \leq 2m^2$. There exist integers a_0 and a_1 with $-m < a_0 \leq m$ and $-m \leq a_1 \leq m$ such that
$$a = a_0 + 2ma_1.$$

Proof. Let $a_0 \equiv a \pmod{2m}$, with $-m < a_0 \leq m$ and $a_1 = (a - a_0)/2m$. Then
$$|a_1| \leq (2m^2 + m)/2m < m + 1.$$
□

Lemma 5.2. Let G be an additive group and let $g \in G$. Suppose $Mg = 0$ for some positive integer M. Let $p_1, \ldots, p_r$ be the distinct primes dividing M. If $(M/p_i)g \neq 0$ for all i, then M is the order of g.

Proof. Let k be the order of g. Then $k \mid M$. Suppose $k \neq M$. Let p_i be a prime dividing M/k. Then $p_i k \mid M$ so $k \mid (M/p_i)$. Therefore $(M/p_i)g = 0$, contrary to assumption. It follows that $k = M$. □

Proof of the algorithm. Steps 1, 2, 4 and 5 are straightforward. We therefore start with the proof of Step 3, which requires us to show that there is indeed a match. Since $q^{1/4} < m$, we have that $2\sqrt{q} < 2m^2$. Let a the trace of Frobenius. Hasse's Theorem

implies that $|a| \leq 2m^2$. We can write $a = a_0 + 2ma_1$, as in Lemma 5.1. Note that $|a_1| \leq m$. This means the algorithm could require us to calculate $Q + k(2m)P$ for $k = -a_1$. This is done as follows:

$$\begin{aligned} Q + k(2m)P &= (q + 1 - 2ma_1)P \\ &= (q + 1 - a - a_0)P \\ &= \#E(\mathbb{F}_q) - a_0P \\ &= a_0P \\ &= \pm jP \end{aligned}$$

where $j = |a_0| \leq m$. This establishes that Step 3 will always yield a match.

Step 6 is proved by noting that $\#E(\mathbb{F}_q)$ is an additive group and applying the the result of Lemma 5.2. □

Remark 5.3. The Baby Step, Giant Step algorithm is a useful tool for determining the order of the group $E(\mathbb{F}_q)$. For this, we apply the algorithm to randomly chosen points on $E(\mathbb{F}_q)$. This should be done until the least common multiple (lcm) of the orders of these points divides a unique integer in the interval $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$.

The reason that this approach works is a combination of basic group theory and Hasse's Theorem. If we have found several orders of points in $E(\mathbb{F}_q)$, then we know from group theory that lcm of these orders divides $\#E(\mathbb{F}_q)$. If the lcm exceeds $4\sqrt{q}$, then Hasse's Theorem says there is a unique multiple of the lcm which is the group order.

5.2 Schoof's algorithm

Even the Baby Step Giant Step algorithm can be improved upon. The genius of the algorithm we are about to present lies in the clever use of the Chinese Remainder Theorem. We will provide the namesake of this thesis directly below.

Algorithm.
Input: An elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$ where $q = p^r$
Output: $\#E(\mathbb{F}_q)$

1. Choose a small set of primes $S = \{2, 3, 5, \cdots, L\}$ with $p \notin S$ and $\prod_{\ell \in S} \ell > 4\sqrt{q}$.
2. Let $a := q + 1 - \#E(\mathbb{F}_q) \in \mathbb{Z}$. Using a sub-algorithm, compute $a \mod \ell$ for every $\ell \in S$.
3. Using the Chinese Remainder Theorem, compute $a \mod \prod \ell$. Determine the integer $a \in \mathbb{Z}$ with $|a| \leq 2\sqrt{q}$ that satisfies this congruence.
4. Output $\#E(\mathbb{F}_q) = q + 1 - a$.

Proof. Suppose that we know $a \mod \ell$ for each $\ell \in S$. Then by the Chinese Remainder Theorem, we can lift $a \mod \ell$ to $a \mod \prod_{\ell \in S} \ell$. Then Hasse's Theorem 4.26 implies that $a \mod \prod_{\ell \in S} \ell$ lifts uniquely to $a \in \mathbb{Z}$. Then we compute $\#E(\mathbb{F}_q) = q + 1 - a$. $\square$

The sub-algorithm.
Input: An elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$ where $q = p^r$ and a prime $\ell \neq p$
Output: $(a \mod \ell)$

1. $a \equiv 0 \mod 2$ if $\gcd(x^3 + Ax + B, x^q - x) \neq 1$ and $(a \equiv 1 \mod 2)$ if $\gcd(x^3 + Ax + B, x^q - x) = 1$.
2. If ℓ is odd, do the following: Let $q_\ell \equiv q \mod \ell$ with $|q_\ell| < \ell/2$
   (a) Compute the x-coordinate of
   $$(x', y') = (x^{q^2}, y^{q^2}) + q_\ell(x, y) \mod \phi_\ell.$$
   (b) For $j = 1, 2, \ldots, (\ell - 1)/2$, do the following.
      (1) Compute the x-coordinate x_j of $(x_j, y_j) = j(x, y)$.
      (2) If $x' - x^q - j \equiv 0 \mod \psi_l$, go to step (3). If not, try the next value of j (in step (c)). If all values $1 \leq j \leq (\ell - 1)/2$ have been tried, go to step (d).
      (3) Compute y' and y_j. If $(y' - y_j{}^q)/y \equiv 0 \mod \phi_\ell$, then $a \equiv j \mod \ell$. If not then $a \equiv -j \mod \ell$.
   (c) If all values $1 \leq j \leq (\ell - 1)/2$ have been tried without success, let $w^2 \equiv q \mod \ell$. If w does not exist, then $a \equiv 0 \mod \ell$.
   (d) If $\gcd(\text{numerator}(x^q - x_w), \phi_\ell) = 1$, then $a \equiv 0 \mod \ell$. Otherwise, compute
   $$\gcd\left(\text{numerator}((y^q - y_w)/y), \phi_\ell\right).$$
   If this gcd is not 1, then $a \equiv 2w \mod \ell$. Otherwise, $a \equiv -2w \mod \ell$.

Proof. Let $\ell = 2$. Recall that a point $P = (x, y)$ has order 2 only when $y = 0$. Therefore, we need to find a root e of $X^3 + AX + B$. For $P = (e, 0)$ to be an element of $E(\mathbb{F}_q)$, we require that $e \in \mathbb{F}_q$, so e also needs to be a root of $X^q - X$. To check whether both conditions hold, it suffices to check whether

$$\gcd(X^3 + AX + B, X^q - X) \neq 1.$$

If this is indeed the case, it follows that $\#E(\mathbb{F}_q) = q+1-a \equiv 0 \mod 2$. Since we assumed q to be odd, it follows that $a \equiv 0 \mod 2$. This proves Step 1 of the sub-algorithm.

Suppose now that ℓ is an odd prime such that $\ell \neq p$. We assume that $P = (x, y) \in E[\ell]$ and $P \neq \mathcal{O}$, unless explicitly stated otherwise. Let E be the given elliptic curve over $\mathbb{F}_q$. Then Theorem 4.23 says that the Frobenius automorphism satisfies the equality

$$\phi_q^2 - a\phi_q + q = 0, \tag{35}$$

where $a = q + 1 - \#E(\mathbb{F}_q)$.

Let $(\phi_q)_\ell$ denote the matrix of the action of ϕ_q on $E[\ell]$. Then by Proposition 4.24, we know that $\mathrm{Trace}(\phi_q)_\ell = a \mod \ell$. So to determine $(a \mod \ell)$ we compute $\mathrm{Trace}(\phi_q)_\ell$ for every odd prime $\ell \in S$.

Note that we have that $aP = bP$ when $a \equiv b \mod \ell$. This allows us to replace q by q_ℓ in (35), where $q_\ell \equiv q \mod \ell$ and $|q_\ell| < \ell/2$. Working with smaller numbers is much more convenient for implementation purposes, so replacing q by q_ℓ is desirable.

Applying the identity (35) to P yields the following equality.

$$a\phi_q(P) = \phi_q^2(P) + q_\ell P. \tag{36}$$

By Corollary 4.14, we have $\phi_q(P)$, $\phi_q^2(P) \in E[\ell]$. Since q_ℓ and ℓ are coprime, it also holds that $q_\ell P \in E[\ell]$. Hence from equation (36) we can derive $(a \mod \ell)$. In order to do this, our aim is now to determine all terms in (36). Before we do this, we will set some notational conventions. For integers j, we will use the following notation:

$$jP = j(x, y) = (x_j, y_j).$$

We can determine both coordinates of jP using the division polynomials by Theorem 3.7 and Definition 3.15. As the multiplication-by-j map is an endomorphism, (14) says we can write $x_j = r_{1,j}(x)$ and $y_j = r_{2,j}(x)y$, where $r_{1,j}$ and $r_{2,j}$ are rational functions. In particular, we can do this when $j = q_\ell$.

We now will determine all terms of (36). First assume that $\phi_q^2(P) \neq \pm q_\ell(P)$. We define

$$(x', y') := \phi_q^2(P) + q_\ell(P) = (x^{q^2}, y^{q^2}) + q_\ell(x, y) \neq \mathcal{O}.$$

In this case, we have $a\phi_q(P) \neq \mathcal{O}$, so $a \neq 0 \mod \ell$. By assumption, we also have that the x-coordinates of $\phi_q^2(P)$ and $q_\ell(P)$ differ, so we can calculate x' by excluding the possibility that the line through $\phi_q^2(P)$ and $q_\ell(P)$ is tangent.

$$x' = \left(\frac{x^{q^2} - x_{q_\ell}}{y^{q^2} - y_{q_\ell}}\right)^2 - x^{q^2} - x_{q_\ell}.$$

We moreover calculate

$$\begin{aligned}\left(y^{q^2} - y_{q_\ell}\right)^2 &= y^2 \left(y^{q^2-1} - r_{2,q_\ell}(x)\right)^2 \\ &= \left(x^3 + Ax + B\right)\left(\left(x^3 + Ax + B\right)^{(q^2-1)/2} - r_{2,q_\ell}(x)\right)^2.\end{aligned}$$

Since we already know that x_{q_ℓ} is a rational function in x, this last calculation shows that x' can be written as a rational function in x.

We will now also explicitly calculate y'. Note that (14) allows us to write $y_{q_\ell} = y r_{2,q_\ell}(x)$. Moreover, we recall that q^2 is odd. We use these two results to calculate

$$\begin{aligned} y' &= \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}}\right)(x' - x^{q^2}) - y^{q^2} \\ &= \left(\frac{y(x^3 + Ax + B)^{(q^2-1)/2} - y r_{2,q_\ell}(x)}{x^{q^2} - x_{q_\ell}}\right)(x' - x^{q^2}) - (x^3 + Ax + B)^{(q^2-1)/2} y \\ &= y\left[\left(\frac{(x^3 + Ax + B)^{(q^2-1)/2} - r_{2,q_\ell}(x)}{x^{q^2} - x_{q_\ell}}\right)(x' - x^{q^2}) - (x^3 + Ax + B)^{(q^2-1)/2}\right] \end{aligned}$$

Since we have already shown that x' is a function of x, it follows that y'/y is a function of x.

As our goal is to find $(a \mod \ell)$ in equation (36), we now want to find the integer j such that

$$(x_j^q, y_j^q) = (x', y'). \tag{37}$$

For such j, we have that $j\phi^q(P) = a\phi^q(P)$. Recalling that $\phi^q(P) \in E[\ell]^*$, this allows us to conclude that $a \equiv j \mod \ell$.

We first start by comparing the x-coordinates of (37). We have $(x', y') = \pm(x_j^q, y_j^q)$ if and only if $x_j^q = x'$. This last equality comes from the fact that (x_j^q, y_j^q) and $-(x_j^q, y_j^q)$ have the same x-coordinate. This fact is very useful, since we then only need to check the x-coordinates of the terms in (37) for $j \in \{1, 2, \ldots, (\ell-1)/2\}$. If the equation holds for $P = (x, y)$, it follows that it holds for all points in $E[\ell]^*$ as P was chosen arbitrarily. As $\ell \neq 2$, Corollary 3.9 says that the roots of ψ_ℓ are the x-coordinates of all points in $E[\ell]^*$. We note that the roots of ψ_ℓ are simple, which follows from Corollary 3.9 and our assumption that $\ell \neq p$. Both statements together imply that $x' - x_j^q \equiv 0 \mod \psi_\ell$. If the roots of ψ_ℓ are not simple, we would in fact only obtain that ψ_ℓ divides some power of $x' - x_j^q$.

Suppose now that we have found an integer j such that (37) is satisfied. Then, only the sign of the y-coordinate is left to be determined. Before we do this, we will show that y_j^q/y is a rational function of x. Recall that we can write $y_j = r_{2,j}(x)y$. Using the fact that q is odd, we can calculate

$$\begin{aligned} (y_j)^q &= r_{2,j}^q(x) y^q \\ &= r_{2,j}^q(x)(x^3 + Ax + B)^{(q-1)/2} y \end{aligned}$$

Therefore, y_j^q/y is a function of x (the x-coordinate of $P \in E[\ell]^*$).

We have therefore established that y_j^q/y and y'/y are both rational functions of x, Therefore we are now able to explicitly calculate both terms, which allows us to determine whether $y'/y = y_j^q/y$ or $y'/y = -y_j^q/y$ for all points of $E[\ell]^*$. Using the same reasoning we applied when comparing x' and x_j^q, it is only required to verify one of the equations modulo ψ_ℓ. If $(y' - y_j^q)/y \equiv 0 \mod \psi_\ell$, then we conclude that $y'/y = y_j^q/y$. This implies that $a \equiv j \mod \ell$. If $(y' - y_j^q) \not\equiv 0 \mod \psi_\ell$, then we have that $a \equiv -j \mod \ell$. This finishes the proof of part (b) of the sub-algorithm.

If (37) does not hold for any $j \in \{1, 2, \ldots, (\ell-1)/2\}$, it has to be the case that $j \equiv 0 \mod \ell$. This forces $\phi_q^2(P) = \pm q_\ell P$ for all $P \in E[\ell]$. We will now determine $(a \bmod \ell)$ for both scenarios. After that, we will provide a criterion which determines which of the two cases we are dealing with.

Case 1: $\phi_q^2 P = q_\ell P$. If $a = 0 \mod \ell$, then by (36), we get $2q_\ell P = \mathcal{O}$ for all $P \in E[\ell]$. This only holds if $\ell = 2$ or $\ell = p$, however we assumed that ℓ is an odd prime and not p. So in this case $a \neq 0 \mod \ell$.

By the equality (36), it follows that $a\phi_q P = \phi_q^2 P + q_\ell P = 2q_\ell P$, so $a^2 q_\ell(P) = (a\phi_q)^2(P)$ for all $P \in E[\ell]$. Therefore, we get $a^2 q \equiv 4q^2 \mod \ell$. Here if q is not a square modulo ℓ, we get $a = 0 \mod \ell$ and $\ell = 2$ or $\ell = p$. So we cannot be in this case.

So let us suppose that q is a square modulo ℓ and set $w^2 = q$. Therefore, we can write for all $P \in E[\ell]$ that $\mathcal{O} = (\phi_q^2 - q)P = (\phi_q + w)(\phi_q - w)P$. It must be the case that either $(\phi_q - w)P = \mathcal{O}$ or $(\phi_q + w)P' = \mathcal{O}$, where $P' = (\phi_q - w)P$. This establishes the existence of a point $P \in E[\ell]$ satisfying $\phi_q P = \pm wP$. The sign of $\pm wP$ can then be determined in the exact same way as we did in the proof of step (b), where w replaces the role of j.

Again, we have two possibilities to consider. We first explore the case that $\phi_q P = wP$. Then $\mathcal{O} = (\phi_q^2 - a\phi_q + q)P = (q - aw + q)P = (2q - aw)P$. It follows that $aw \equiv 2q \equiv 2w^2 \mod \ell$. This shows that $a \equiv 2w \mod \ell$. In the case that $\phi_q P = -wP$, an almost identical calculation yields $a \equiv -2w \mod \ell$.

Case 2: $\phi_q^2 P = -q_\ell P$. The equality (36) gives us $a\phi_q P = \mathcal{O}$ for all $P \in E[\ell]$. So this implies $a \equiv 0 \mod \ell$.

We now need a criterion which determines whether we are dealing with Case 1 or 2. If we are in Case 1, then we proved that q is a square mod p. (This implies we can write $w^2 = q$ for some integer w). Therefore we are dealing with Case 1 if q is a square. If not, then we are in Case 2. This proves step (c) of the sub-algorithm.

If we are in Case 1, then we have already showed that there is a point $P \in E[\ell]$ which satisfies $\phi_q P = \pm wP$. As the x-coordinates of these points are equal, it holds that $x^q - x_w = 0$. This expression is a rational function of x by (14). Therefore we are in Case 1 if we are able to find a point $P \in E[\ell]$ satisfying $\phi_q P = \pm wP$. To see if such a

point exists, we need to check whether

$$\gcd(\text{numerator}(x^q - x_w), \psi_\ell) \neq 1.$$

If this gcd is different from 1, then we are in Case 1. If the gcd is 1, then we are dealing with Case 2. In both cases, the value of $(a \bmod \ell)$ is then calculated in the way we illustrated earlier in the proof. This concludes the proof of step (d), which also concludes the proof of Step 2 of the sub-algorithm. □

6 Conclusion

The last line of the proof of Schoof's algorithm also concludes our thesis; an accumulation of different branches of mathematics, all providing essential building blocks to prove an incredibly useful application of the Chinese Remainder Theorem. It is fascinating to observe how an ancient result in mathematics continues to be very relevant today.

References

[1] R. L. Rivest, A. Shamir, and L. Adelman, "A method for obtaining public-key cryptosystems and digital signatures," tech. rep., Technical Report MIT/LCS/TM-82, 1977.

[2] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[4] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[5] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*, pp. 417–426, Springer, 1985.

[6] D. Shanks, "Class number, a theory of factorization, and genera," in *Proc. of Symp. Math. Soc., 1971*, vol. 20, pp. 41–440, 1971.

[7] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," *Mathematics of computation*, vol. 44, no. 170, pp. 483–494, 1985.

[8] A. O. Atkin, "The number of points on an elliptic curve modulo a prime," *preprint*, 1988.

[9] N. D. Elkies *et al.*, "Elliptic and modular curves over finite fields and related computational issues," *AMS/IP Studies in Advanced Mathematics*, vol. 7, pp. 21–76, 1998.

[10] N. D. Elkies, "Explicit isogenies," *preprint*, 1991.

[11] L. C. Washington, *Elliptic curves: number theory and cryptography*. Boca Raton: Chapman and Hall/CRC, 2nd ed. ed., 2008.

[12] J. H. Silverman, *The arithmetic of elliptic curves*. New York: Springer-Verlag, 2nd ed. ed., 2009.

[13] B. Smith, "Mappings of elliptic curves," in *DIAMANT-Summer School on Elliptic and Hyperelliptic Curve Cryptography*, (Eindhoven), 2008.

[14] C. Orzech, *Plane algebraic curves*, vol. 61. CRC Press, 1981.

[15] R. Hartshorne, *Algebraic Geometry. Graduate Texts in Math. 52*. 1977.

[16] W. Fulton, *Algebraic curves: an introduction to algebraic geometry*. Advanced book classics, Addison-Wesley Pub. Co., Advanced Book Program, 1989.

[17] I. F. Blake, G. Seroussi, and N. P. Smart, *Elliptic curves in cryptography*. Cambridge: Cambridge University Press, 1999.

[18] J. Bauer, *Sage plot of an elliptic curve over a finite field*. Sep 2011.

[19] H. Hasse, "Zur theorie der abstrakten elliptischen funktionenkörper i. die struktur der gruppe der divisorenklassen endlicher ordnung.," *Journal für die reine und angewandte Mathematik*, vol. 175, pp. 55–62, 1936.