



university of
 groningen

faculty of science
 and engineering

mathematics and applied
 mathematics

The Discrete Logarithm Problem on Anomalous Elliptic Curves

Bachelor's Project Mathematics

July 2020

Student: S. J. Hofman

First supervisor: Dr. M. Djukanović

Second assessor: Dr. P. Kılıçer

Abstract

Smart's algorithm solves the discrete logarithm problem on anomalous curves in polynomial time. This thesis will examine the algorithm developed by Smart in detail. Furthermore, it discusses why the same method, with only a slight adaptation, also works on any finite field extension of \mathbb{F}_p . In addition to this, we explain the theory behind a small program we developed to search for anomalous curves with small coefficients over large finite fields.

Keywords— elliptic curves · discrete logarithm problem · anomalous curves · Smart's algorithm · formal groups · p -adic numbers

Contents

1	Introduction	4
2	Elliptic curves and their group law	6
3	General theory of elliptic curves	12
3.1	Isogenies and endomorphisms	12
3.2	Torsion points	21
4	The p-adic numbers and Hensel's lemma	30
4.1	Valuations and absolute values	31
4.2	The construction of the p -adic numbers	33
4.3	The ring of p -adic integers	36
4.4	Hensel's lemma	38
5	The formal group of an elliptic curve over the field \mathbb{Q}_p	43
5.1	The construction of the formal group	44
5.2	The reduction of elliptic curves modulo p	47
5.3	The formal logarithm	50
6	Smart's algorithm	52
6.1	The algorithm over \mathbb{F}_p	53
6.2	The algorithm over \mathbb{F}_q	56
7	Searching for anomalous curves	59
7.1	The j -invariant and quadratic twists	59
7.2	Elliptic curves with complex multiplication	61
7.3	The starting prime and the output	65
8	Discussion and further developments	66
	Appendices	66
A	The implementation of Smart's algorithm	66
A.1	The algorithm	66
A.2	Auxiliary functions	67
B	Searching for anomalous curves: the program	67
C	An anomalous curve of the form $y^2 = x^3 + B$	69
D	An anomalous curve constructed using complex multiplication	69

1 Introduction

Cryptography has a long history going back to around 1900 BC, when in ancient Egypt, unusual hieroglyphic symbols were carved on tombs [Mol04], arguably representing cryptography in one of its simplest forms. Fast-forward to the era of modern cryptography, which revolves around the secret communication between parties. In this period, encryption and decryption methods became more mathematically founded and algorithms were starting to develop that could run on computers. With the introduction of the internet and thus the possibility of exchanging information quickly, globally and, (unfortunately) publicly, security methods were widely called for. Before that, in the mid-1970s, Whitfield Diffie and Martin Hellman published a method that provided a great step towards solving one of cryptography's fundamental problems, namely the distribution of keys [DH76]. The publication of this method induced a completely new class of encryption algorithms, collectively known as public-key cryptography.

The idea of this new cryptographic system is that users can communicate securely without first having to establish a secret channel. In the concept, every user has two keys: one private decryption key and one public encryption key which they publish in some open directory. Any two users who now wish to communicate in private can look up the other user's public key and use their own private key to create a secret link.

The method described by Diffie and Hellman, also known as the Diffie-Hellman key exchange, can be explained using the well-known Alice and Bob example: suppose Alice and Bob want to exchange information privately. They (publicly) agree upon a cyclic group G and a generator g in G . Moreover, they both have secretly chosen numbers a and b that they keep to themselves (their private keys). Alice and Bob now compute g^a and g^b , respectively. These elements are their public keys which they put out in the open. Alice will receive g^b and computes $(g^b)^a$ whereas Bob obtained g^a and computes $(g^a)^b$. At this point, both Alice and Bob have the same shared key, since $g^{ab} = g^{ba}$.

Of course, Alice and Bob were not planning on sharing the value g^{ab} ; they would like to exchange plaintext, for example. In order to do so, they can make a list of values for powers of g and the corresponding alphabetic letter. This is clearly not the most sophisticated method. Over the years, many more advanced algorithms have been developed.

One of the obvious ways in which a third party can intercept the message between Alice and Bob is when they know one of the private keys of either Alice or Bob. This induces the following problem:

Discrete logarithm problem (DLP): for a finite group G and elements g, h in G , find an integer k (assuming it exists) such that

$$g^k = h.$$

In the scenario of Alice and Bob, h equals g^a or g^b . The difficulty of solving this problem depends on the group G . To this day, it remains one of the unsolved problems in computer science whether or not this general problem can be solved in polynomial time.

To lift some of the abstraction, we can consider the additive group $\mathbb{Z}/p\mathbb{Z}$ for G , where p is a prime. Since this group is of prime order, it is cyclic. Therefore, we can take any element as a generator and we denote it by g . For this particular group, the problem can be restated as finding an integer k such that

$$k \cdot g \equiv \underbrace{g + g + \dots + g}_{k \text{ times}} \equiv h \pmod{p}.$$

This means that we need to compute the multiplicative inverse of $g \pmod{p}$, since this gives $k \equiv h \cdot g^{-1} \pmod{p}$. By recalling Fermat's little theorem, which says that $g^p \equiv g \pmod{p}$,

we find that $g^{-1} \equiv g^{p-2} \pmod{p}$. Hence in this case, the problem can be solved very efficiently. Also, observe that here the integer k is uniquely determined modulo p .

A natural next step would be to take the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ instead of the additive group. The DLP then already becomes much harder. However, there exist sub-exponential algorithms to solve this problem, such as the index calculus. This means that, in order to make finding k a difficult task, one needs to consider a very large prime p (of hundreds of bits).

For Alice and Bob, taking $\mathbb{Z}/p\mathbb{Z}$ as their group G would be a very poor choice. For their purposes, a group is required that makes the discrete logarithm problem very difficult to solve. They could take $(\mathbb{Z}/p\mathbb{Z})^\times$ for a large prime p , but, a perhaps safer choice would be to use *elliptic curves*. In 1985, Neal Koblitz and Victor Miller both independently developed the idea of using elliptic curves as a means to improving the security for public-key cryptography [Kob87][Mil85]. An elliptic curve E , defined over a field K , is an equation of the form

$$y^2 = x^3 + Ax + B, \tag{1.1}$$

where A and B are constants in K and we require that $4A^3 + 27B^2 \neq 0$, so that the cubic $x^3 + Ax + B$ has no multiple roots. Moreover, for (1.1) to be a general equation, we require that the field K has characteristic not equal to 2 or 3. It will be shown that by considering a particular operation, the points on an elliptic curve form a group. In this thesis, we will consider a certain class of elliptic curves in more detail. This is the class of so-called *anomalous curves*:

Anomalous curves: an elliptic curve over a finite field of prime order p is called anomalous if its group order equals p .

By considering an elliptic curve over a finite field of large prime order, Koblitz and Miller made the reasonable assumption that the discrete logarithm problem would be very hard to solve. In fact, the company Certicom, which specialises in elliptic curve cryptography (ECC), says that for a prime of order 2^{163} or larger, this problem is ‘believed to be computationally infeasible’ [Cer]. This is one of the reasons why cryptocurrencies such as Bitcoin implement ECC in their algorithms to ensure safe transactions [Bos+14].

It is thus no secret that elliptic curve cryptography is very secure. However, Alice and Bob should watch out when they pick an elliptic curve to safely interact. Nigel P. Smart published a method in 1999 that renders specific elliptic curves very weak for cryptographic purposes [Sma99]. In his paper, Smart showed the following:

Smart’s algorithm: the discrete logarithm problem on anomalous elliptic curves can be solved in polynomial time.

In layman’s terms, this means that the previously discussed ‘infeasibility’ of solving the DLP now just becomes a matter of seconds on an ordinary computer. The algorithm provides a method to reduce the discrete logarithm problem on anomalous curves to the problem of computing the inverse of an element in $(\mathbb{Z}/p\mathbb{Z})^\times$. We have already seen that the latter is not a hard task.

In this thesis, we will look at Smart’s algorithm in detail after discussing some general theory on elliptic curves. To be able to understand the algorithm, we will need to introduce the p -adic numbers and a few of the basic results concerning them. Moreover, the notion of a formal group and its logarithm will prove to be very valuable in our research. One can broaden the definition of being anomalous to elliptic curves over finite field extensions of \mathbb{F}_p . In this case, the elliptic curve must have the same group order as the number of elements in the field extension. By considering an adaptation of the algorithm developed by Smart it allows us to solve the discrete logarithm problem for anomalous curves over finite field extensions as well.

James McKee showed that the density of anomalous curves over \mathbb{F}_p is at most $\mathcal{O}((1/\sqrt{p}) \log(p) \log(\log(p)))$ [McK99]. For large primes p , this becomes relatively small, so anomalous curves over large prime fields can be considered as rare. In the last part of this project, we will design a program that, despite of their scarcity, searches for anomalous curves over relatively large prime fields. Using basic properties of elliptic curves and theory about curves with complex multiplication, this program is made more efficient.

2 Elliptic curves and their group law

In the introduction, we have already seen the general equation of an elliptic curve over a field of characteristic 0 or larger than 3. This equation is also known as the *Weierstrass equation*, named after the German mathematician Karl Weierstrass (1815 - 1897). It should be mentioned that if the characteristic of K is not specified, we require a more generalised form of (1.1) given by the *generalised Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (2.1)$$

It can be shown that any elliptic curve can be represented by a generalised Weierstrass equation (see [Sil09, Section III.3, Proposition 3.1]). From this equation, it only requires a few steps to obtain (1.1) when the characteristic is neither 2 or 3; only completing the square and performing a change of variables twice suffices (cf. [Was08, Section 2.1]).

Remark. Throughout this section, we assume that K is a field with characteristic not equal to 2 or 3 (unless stated otherwise). In this case, we can consider the Weierstrass equation given in (1.1). The notation \bar{K} and $K[x, y, z]$ used in this section denote the algebraic closure of K and the polynomial ring over K in three variables, respectively.

As we are interested in points on E and the way in which we can perform arithmetic operations on these points, we require the following definition:

Definition 2.1. Let E be an elliptic curve defined over a field K . For a field $L \supseteq K$, the set of L -rational points on E , together with a rational point at infinity denoted by \mathcal{O} , is given by

$$E(L) = \{(x, y) \in L \times L : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

More information on \mathcal{O} and why we call it the point at infinity will soon be given. First, to obtain some intuition on what this set represents visually, consider $E(\mathbb{R})$ for the two elliptic curves over \mathbb{Q} that are given in Figure 1.

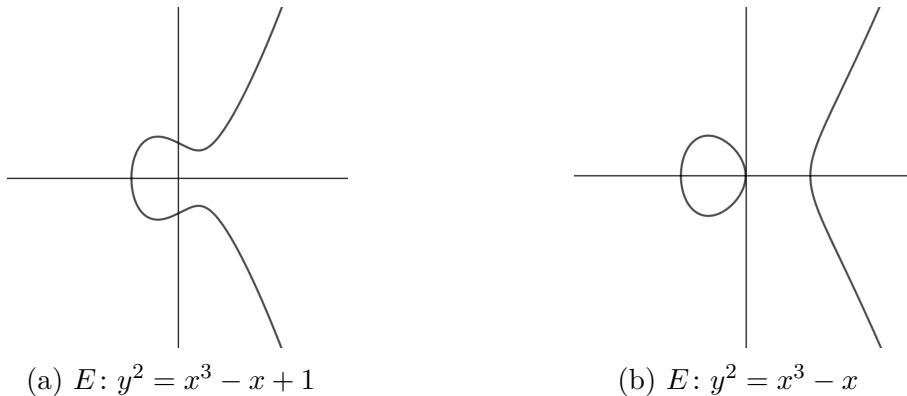


Figure 1: $E(\mathbb{R})$ for two elliptic curves defined over \mathbb{Q} .

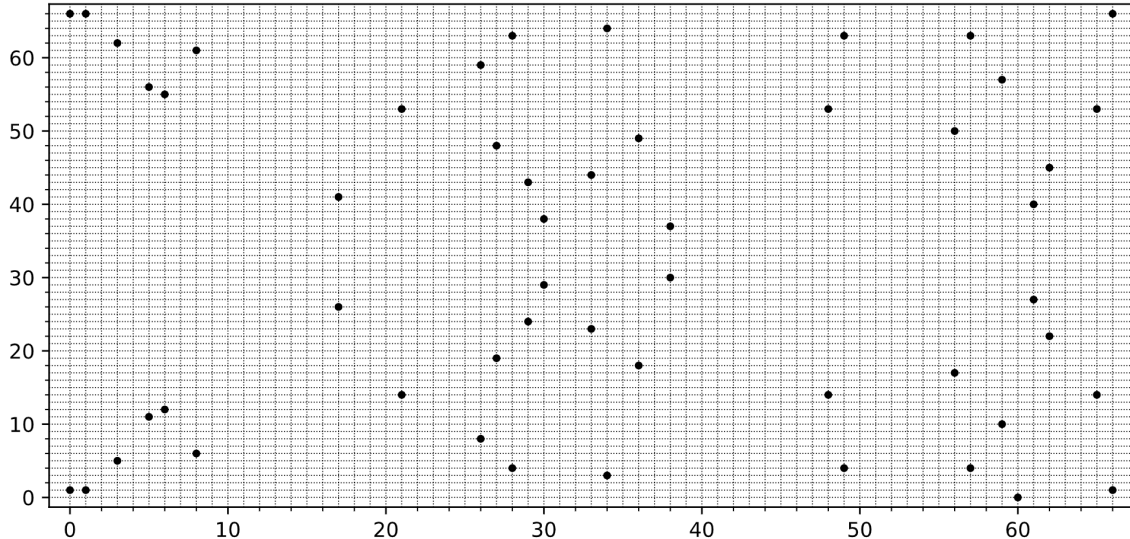


Figure 2: $E(\mathbb{F}_{67})$ with $E: y^2 = x^3 - x + 1$

For points in \mathbb{R} , this set represents a nice curve. However, for most fields this set will not look like one of the figures above. In later sections, we often consider our field to be finite and in this case, the plot of an elliptic curve looks more like a plot of randomly scattered points; see Figure 2 for example. Despite of this, note that the curve still has some symmetry due to the fact that both (x, y) and $(x, -y)$ lie on the curve.

Before we can obtain a clearer understanding of the point \mathcal{O} and define a group law on the set $E(L)$, we need to consider the *affine* and the *projective plane*.

Definition 2.2. Let K be a field. The *affine plane* over K , denoted by $\mathbb{A}^2(K)$, is defined as

$$\mathbb{A}^2(K) := K \times K.$$

The projective plane was constructed to make sure that any two lines meet in exactly one point [ST92]. By adding the so-called points at infinity to the affine plane, it is guaranteed that this condition is indeed satisfied. In fact, the projective plane obtained in this way satisfies a stronger result, called Bézout's theorem (see Theorem 2.7)

Definition 2.3. Let K be a field. The *projective plane* over K , denoted by $\mathbb{P}^2(K)$, is defined as

$$\mathbb{P}^2(K) := \{(x, y, z) : x, y, z \in K, \text{ not all zero}\} / \sim,$$

with the equivalence relation given by

$$(x, y, z) \sim (x', y', z') \quad \text{if and only if} \quad x = \lambda x', \quad y = \lambda y', \quad z = \lambda z',$$

for some nonzero λ in K . The triple $(x : y : z)$ denotes an equivalence class and x, y, z are called *homogeneous coordinates*.

Remark. The equivalence classes are denoted by $(x : y : z)$ as we are merely concerned with the *ratios* of the homogeneous coordinates. Moreover, observe that $(0 : 0 : 0)$ is not a point in the projective plane. This is because all points $(a : b : c)$ in $\mathbb{P}^2(K)$ correspond to planes in K^3 described by $ax + by + cz = 0$. If a, b and c are all zero, this point does not correspond to such a plane, and therefore, it is excluded.

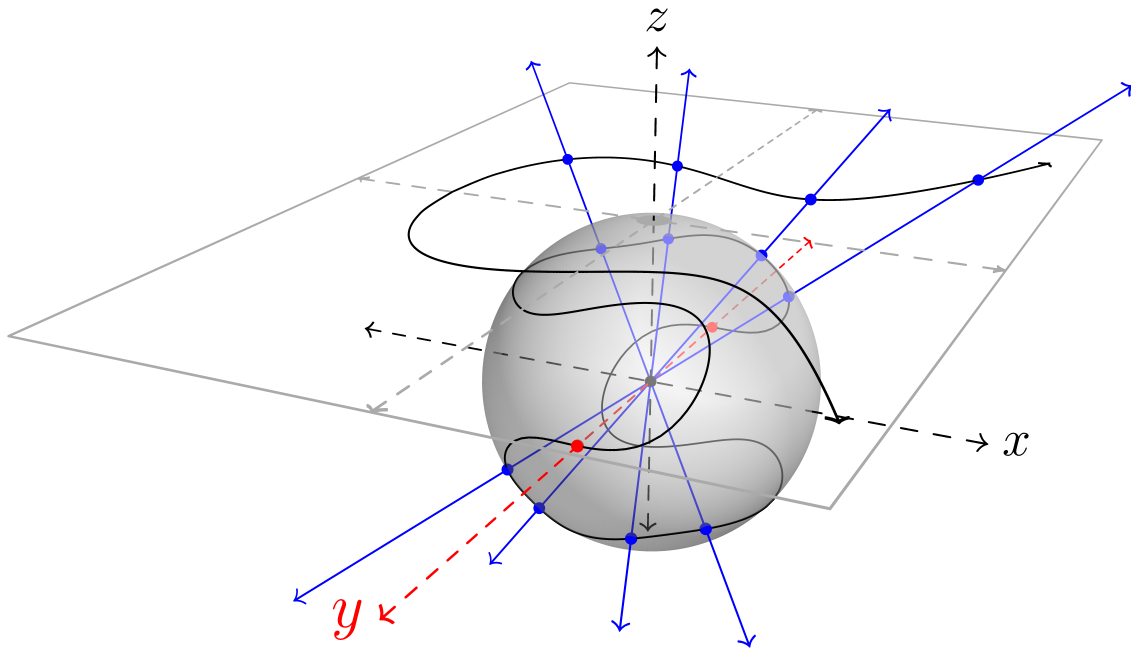


Figure 3: The elliptic curve as a projective and affine plane curve over \mathbb{R} [Cse19].

Intuitively, the points on the projective plane can be thought of as lines going through the origin in different directions. The points $(x : y : z)$, where z is nonzero, are called the *affine points* in $\mathbb{P}^2(K)$. These points can be associated with points in the affine plane $\mathbb{A}^2(K)$, namely via the bijection

$$\begin{aligned} \mathbb{P}^2(K) \setminus \{(x : y : 0) : x, y \in K, \text{ not both zero}\} &\rightarrow \mathbb{A}^2(K), \\ (x : y : z) &\mapsto (x/z, y/z). \end{aligned} \tag{2.2}$$

The projective plane can help us to obtain a more formal definition of rational points on an elliptic curve, especially of the point \mathcal{O} . This is because, although the definition of an elliptic curve we gave in the introduction is convenient, it lacks a bit of formality. To be able to describe all points on the elliptic curve, we need the projective plane. Figure 3 can be used as a means to develop more intuition about the points on an elliptic curve.

In this figure, the line on the sphere is a *projective plane curve* (we will see what this means later) that represents the elliptic curve. Observe that this curve is closed. We can identify a part of the projective plane curve by projecting it onto a plane above the unit sphere. This projection is the elliptic curve as it is defined in (1.1). In order to obtain this *affine plane curve*, we consider a point on the projective plane curve, which is in truth a line going through the origin that intersects the projective plane curve at two points (indicated by the blue points). This line will intersect the plane in some point, and thus corresponds to an affine point (x, y) , as we saw in (2.2). We can do this for almost all points on the projective plane curve and, by doing so, we acquire the affine plane curve lying in the plane, which corresponds to a curve like the one given in Figure 1a. However, if we consider the red line in Figure 3, which is represented by the red points on the projective plane curve, we see that this line is in fact parallel to the y -axis. Due to this, it will not intersect the plane above the unit sphere. Therefore, there is one point¹ on the projective plane curve that cannot be represented by a point on the affine plane curve and this point is denoted by \mathcal{O} .

¹All antipodal points on the sphere are identified to give the projective plane. Thus both red points, and antipodal blue points, are identified.

The reason this point is often called the ‘point at infinity’ of an elliptic curve is due to the fact that, if we consider points further along the affine plane curve in one of the two directions (so further up or down in Figure 1a), then the line it corresponds to in the projective plane tends to the line parallel to the y -axis going through the red points. That is, the line represented by the point \mathcal{O} . This point is not the only point at infinity in the projective plane. In fact, the points with $z = 0$ are precisely all such points.

With this better comprehension of the projective plane, we can now consider the terminology used before in more detail.

Definition 2.4. Let K be a field. An *affine plane curve* is the set of solutions in $\mathbb{A}^2(\bar{K})$ to the polynomial equation

$$f(x, y) = 0,$$

where f in $K[x, y]$ is irreducible over \bar{K} .

There are two complications we need to deal with in order to define curves in the projective plane. Since points in this plane are represented by homogeneous triples, we need to use polynomials in three variables. Moreover, due to the equivalence relation in the projective plane, we need to work with *homogeneous polynomials*.

Definition 2.5. Let K be a field. A polynomial F in $K[x, y, z]$ of degree n is called *homogeneous* if it satisfies

$$F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$$

for all λ in K .

Remark. There is another way to characterise these polynomials: a polynomial of degree n is homogeneous if all monomials have degree n .

We can now define projective plane curves.

Definition 2.6. Let K be a field. A *projective plane curve* is the set of solutions in $\mathbb{P}^2(\bar{K})$ to the polynomial equation

$$F(x, y, z) = 0,$$

where F in $K[x, y, z]$ is a homogeneous polynomial that is irreducible over \bar{K} .

Remark. It is essential that F is homogeneous in the definition above since it makes sure the set of zeros for F is well-defined (that is, the choice of the representative for the equivalence class does not matter). This is due to the fact that $F(x, y, z) = 0$ if and only if $F(\lambda x, \lambda y, \lambda z) = 0$ for all nonzero λ in \bar{K} , so $(x : y : z)$ is on the projective plane curve if and only if $(\lambda x : \lambda y : \lambda z)$ is on the projective plane curve, where λ is nonzero.

This allows us to state Bézout’s theorem, which will help us when we define a group law on the set of points on an elliptic curve. A proof of this result can be found in [ST92, Section A.4].

Theorem 2.7 (Bézout’s theorem). *Let K be a field and let $F(x, y, z) = 0$ and $G(x, y, z) = 0$ be two projective plane curves with degrees m and n , respectively. Suppose that F and G have no common components, then F and G meet in $m \cdot n$ points, counting with multiplicities.*

Before we look at the group law, we want to find homogeneous coordinates for the point \mathcal{O} . To this end, consider an elliptic curve $E: y^2 = x^3 + Ax + B$ over a field K . Define the affine plane curve

$$f(x, y) := y^2 - x^3 - Ax - B = 0,$$

which represents E in the affine plane. By homogenising this curve, we can obtain a projective plane curve for E , given by

$$F(x, y, z) := y^2z - x^3 - Axz^2 - Bz^3 = 0.$$

By the bijection given in (2.2), a point (x, y) on the affine plane curve corresponds to a point $(x : y : 1)$ on the projective plane curve. Since we look for \mathcal{O} , a point at infinity, we set $z = 0$ in F and consequently, we obtain $x^3 = 0$, implying that $x = 0$. Therefore, y must be nonzero and dividing by y gives the only point on E at infinity, namely the triple intersection point $(0 : 1 : 0)$. This is the point \mathcal{O} .

We can avoid a lot of messy notation if we use the equation in (1.1) as our representation of an elliptic curve. Hence, we will often write \mathcal{O} and remember that this is a rational point on the elliptic curve as well. The reason we need this point at infinity is to make sure the group law works, as is discussed below.

Let E be an elliptic curve defined over K and consider two points P and Q in $E(L)$, with $L \supseteq K$ a field. We will define an operation, denoted by \oplus , that adds two points on an elliptic curve. To this end, define the point R as the third intersection of the line through P and Q with E , which exists by Bézout's theorem. Note that this theorem only tells us that $R \in E(\bar{K})$. However it is not hard to show, by applying a few algebraic operations, that this point R is in fact an element of $E(L)$. We now reflect R across the x -axis and define the resulting point as $P \oplus Q$, which thus also in $E(L)$. The process of adding two points is depicted below, using an elliptic curve over \mathbb{Q} and by considering the set $E(\mathbb{R})$.

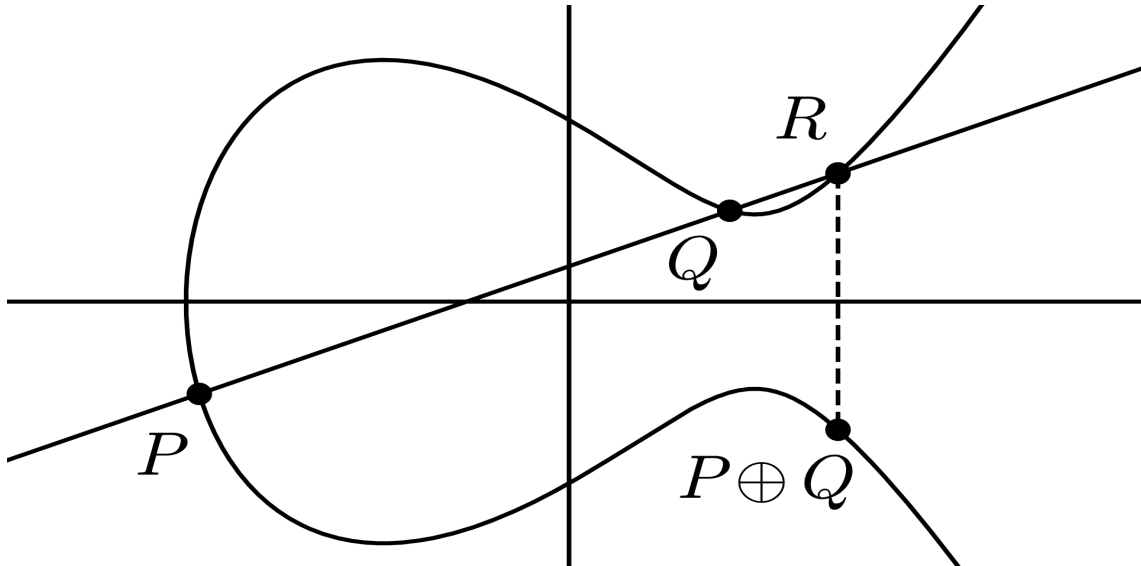


Figure 4: Adding two points on an elliptic curve.

Figure 4 and the process discussed above imply that the points P and Q are distinct and not equal to \mathcal{O} . However, a similar method also makes point addition work in other instances where this is not the case. For example, if two distinct points share the same x -coordinate, then the line through these points is vertical and therefore the third intersection point and final result will be \mathcal{O} , since \mathcal{O} is invariant under reflection over

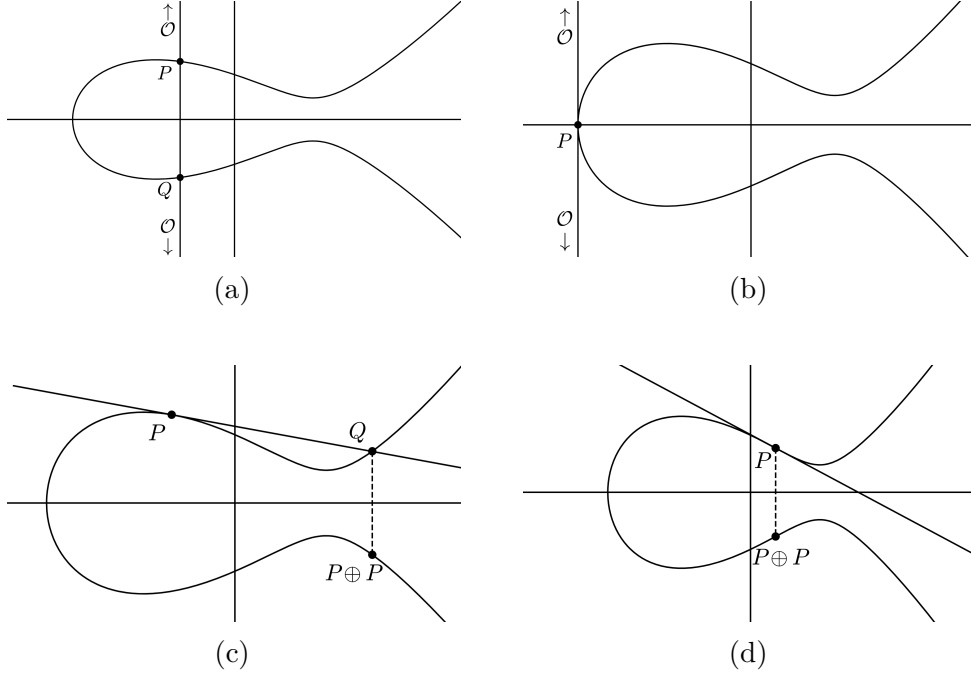


Figure 5: Point addition on an elliptic curve in different situations.

the x -axis (see Figure 5a). If we add a point P to itself (see Figures 5b and 5c), then the line through P is taken to be the tangent of E at P . If the y -coordinate of P is 0, then the tangent line is vertical and therefore the third intersection and final result will be \mathcal{O} (see Figure 5b). When we add \mathcal{O} to P , the line through P and \mathcal{O} also intersects E in the reflection of P across the x -axis. Therefore, the resulting point is P again. This result also holds if P equals \mathcal{O} , by recalling that \mathcal{O} was defined as a triple intersection point. One last remark should be made about the addition of an inflection point P to itself. In this case, the point P is a triple intersection point of the line through P that is tangent to E . Hence $P \oplus P = -P$ (see Figure 5d). The formulas for adding two points on E are summarised in the following definition; their derivations can be found in [Was08, Section 2.2].

Definition 2.8. Let $E: y^2 = x^3 + Ax + B$ be an elliptic curve over a field K . Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, both not equal to \mathcal{O} , denote two points on E . The point $R = (x_3, y_3) = P \oplus Q$ is obtained by applying one of the following rules:

- if $x_1 \neq x_2$, then

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

- if $x_1 = x_2$ and $y_1 \neq y_2$, then $P \oplus Q = \mathcal{O}$.
- if $P = Q$ and $y_1 \neq 0$, then

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where } m = \frac{3x_1^2 + A}{2y_1}.$$

- if $P = Q$ and $y_1 = 0$, then $P \oplus Q = \mathcal{O}$.

Moreover, for any point P on E , define $P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$.

This definition gives rise to the main result of this section.

Theorem 2.9. *Let E be an elliptic curve defined over a field K . For any field $L \supseteq K$, the triple $(E(L), \oplus, \mathcal{O})$ forms an abelian group.*

Proof. It suffices to show that all defining properties of a group hold. For any P in $E(L)$, it follows that $P \oplus \mathcal{O} = P$ by definition. Moreover, $P \oplus P' = \mathcal{O}$, where P' is the point obtained by reflecting P in the x -axis. Hence, every element in $E(L)$ is invertible and we denote the inverse of P by $\ominus P$. Commutativity follows from the fact that for any P, Q in $E(L)$, the line through P and Q is the same as the line through Q and P . The proof of associativity requires a bit more theory; see [Was08, Section 2.4]. \square

Remark. The geometric description of the group law given in this section also holds for the generalised Weierstrass equation. Analogous to Definition 2.8, an algebraic definition for this equation can be found in [Sil09, Section III.2]. One important fact is that for generalised Weierstrass equation, the inverse of a point (x, y) is given by $(x, -y - a_1x - a_3)$.

Observe that, since we have shown the points on an elliptic curve form a group, we can consider the discrete logarithm problem on it. We will come back to this later, and first study general theory of elliptic curves

3 General theory of elliptic curves

This section is mainly concerned with general properties of elliptic curves over fields with characteristic not equal to 2 or 3. Almost all of the results discussed in this section can be found in [Was08, Sections 2.9, 3.1, 3.2] and [Sil09, Sections 3.1-3.4]. We will consider *endomorphisms* and use them as a tool to examine the group structure of an elliptic curve. Moreover, theory about *torsion points* will be discussed, which further develops our understanding of the group formed by points on an elliptic curve. One of the main results provides a lot of information about the group structure of n -torsion points, which are points on an elliptic curve with order dividing n . Another important result is Hasse's theorem, named after German mathematician Helmut Hasse (1898 – 1979), which gives a bound on the group order of an elliptic curve over a finite field. In some cases, this bound can be used to directly determine the group order. Hasse's theorem is essential in Schoof's algorithm, which helps us to find the group order when Hasse's bound on its own does not give us enough information.

Throughout this section, we will assume that the field K has characteristic not equal to 2 or 3, unless specified otherwise. Other notations that will be used are $\bar{K}(X)$ and $\bar{K}(X, Y)$, which denote the field of rational functions over an algebraic closure of K in one or two variables, respectively.

3.1 Isogenies and endomorphisms

As we mentioned before, endomorphisms will play an important role in proving certain results about the group structure of elliptic curves. Before giving the definition of an endomorphism, we first introduce the notion of an *isogeny*.

Definition 3.1. Let E and E' be elliptic curves defined over a field K . An *isogeny* $\phi: E(\bar{K}) \rightarrow E'(\bar{K})$ is a nontrivial rational map and a group homomorphism. More specifically, ϕ satisfies

$$\phi((x, y) \oplus (x', y')) = \phi(x, y) \oplus \phi(x', y')$$

and there exists rational functions ρ_1, ρ_2 in $\bar{K}(X, Y)$ such that

$$\phi(x, y) = (\rho_1(x, y), \rho_2(x, y))$$

for all points $(x, y), (x', y')$ in $E(\bar{K})$.

Remark. It is indeed true that ϕ maps the identity on E to the identity on E' , which is what we would expect from a group homomorphism. A more precise definition of ϕ shows this, but it would require more theory in the field of algebraic geometry, which this thesis will not discuss. Essentially, the definition above says that ϕ is a map that preserves both the geometric structure (that is, being a smooth projective curve) and the algebraic structure (that is, being an abelian group) of an elliptic curve. For more details, see [Sil09, Sections I.3, II.2, III.4].

Remark. Notice that we define an isogeny as a map on the group of an elliptic curve over its algebraic closure. This is because many properties that we can obtain by defining it in this way would not follow if we did not consider the algebraic closure. Take for example Theorem 3.11, which also holds for isogenies. This statement is not necessarily true if we take K instead of \bar{K} .

The definition of an endomorphism is given below.

Definition 3.2. Let E be an elliptic curve defined over a field K . An *endomorphism* of E is an isogeny from E to itself.

Although most of the results below also hold for isogenies, we will only consider endomorphisms from now on.

We need to be careful when we express an endomorphism in terms of rational functions since there might be points where these functions are not defined. We deal with such situations in the following result, which also gives a more specific form for an endomorphism.

Theorem 3.3. Let $E: y^2 = x^3 + Ax + B$ be an elliptic curve defined over K . For any endomorphism $\alpha: E(\bar{K}) \rightarrow E(\bar{K})$, there exists rational functions r_1, r_2 in $\bar{K}(X)$ such that

$$\alpha(x, y) = (r_1(x), r_2(x)y)$$

for all (x, y) in $E(\bar{K})$.

Proof. Take α to be any endomorphism of E , then

$$\alpha(x, y) = (\rho_1(x, y), \rho_2(x, y)).$$

Any rational function ρ in $\bar{K}(X, Y)$ can be written as

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

for all (x, y) in $E(\bar{K})$, where p_1, \dots, p_4 are in $\bar{K}[X]$. This follows from the fact that points in $E(\bar{K})$ satisfy $y^2 = x^3 + Ax + B$, which means that we can replace any even power of y in ρ by a polynomial in x and any odd power of y in ρ by a polynomial in x times y . In this way, we obtain a rational function that equals ρ on the points in $E(\bar{K})$. If we multiply both the numerator and denominator by $p_3 - p_4y$ and use the equation of an elliptic curve, it follows that for all (x, y) in $E(\bar{K})$, we have

$$\rho(x, y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}, \tag{3.1}$$

with q_1, q_2, q_3 in $\bar{K}[X]$. Since α is a group homomorphism and the inverse of a point in $E(\bar{K})$ is given by changing the sign of the y -coordinate, we have

$$\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y).$$

Hence, we see that

$$(\rho_1(x, -y), \rho_2(x, -y)) = -(\rho_1(x, y), \rho_2(x, y)) = (\rho_1(x, y), -\rho_2(x, y)).$$

If we write $\rho_1(x, y)$ in the form given in (3.1), then we obtain that $q_2(x) = 0$ due to the fact that $\rho_1(x, -y) = \rho_1(x, y)$. Similarly, $\rho_2(x, y)$ written in this form implies $q_1(x) = 0$ since $\rho_2(x, -y) = -\rho_2(x, y)$. Thus, we can represent α as

$$\alpha(x, y) = (r_1(x), r_2(x)y),$$

for some rational functions r_1, r_2 in $\bar{K}(X)$. It remains to show that the rational functions in α are defined. First, write

$$\alpha(x, y) = (r_1(x), r_2(x)y) = \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)}y \right),$$

where f_1, g_1, f_2, g_2 in $\bar{K}[X]$ are such that $\gcd(f_1, g_1) = 1$ and $\gcd(f_2, g_2) = 1$ (that is, f_1 and g_1 do not share any roots and f_2 and g_2 do not share any roots in \bar{K}). If (x, y) in $E(\bar{K})$ satisfies $g_1(x) = 0$, we can assume that $\alpha(x, y) = \mathcal{O}$ (see [Har13, Section I.3 and I.4] for detailed reasoning on this). If (x, y) satisfies $g_1(x) \neq 0$, then we claim that $g_2(x) \neq 0$. This would imply that r_2 is defined whenever r_1 is defined, as desired. To prove this claim, we observe that since $\alpha(x, y)$ lies on E , it follows that

$$\left(\frac{f_2(x)}{g_2(x)}y \right)^2 = \left(\frac{f_1(x)}{g_1(x)} \right)^3 + A \frac{f_1(x)}{g_1(x)} + B.$$

Hence

$$\frac{f_2(x)^2(x^3 + Ax + B)}{g_2(x)^2} = \frac{f_1(x)^3 + Af_1(x)g_1(x)^2 + Bg_1(x)^3}{g_1(x)^3} = \frac{u(x)}{g_1(x)^3}, \quad (3.2)$$

where $u(x) := f_1(x)^3 + Af_1(x)g_1(x)^2 + Bg_1(x)^3$. We will first show that $u(x)$ and $g_1(x)$ do not share any roots. Suppose that $u(x_0) = g_1(x_0) = 0$ for some point (x_0, y_0) in $E(\bar{K})$. Then we have

$$0 = u(x_0) = f_1(x_0)^3 + Af_1(x_0)g_1(x_0)^2 + Bg_1(x_0)^3,$$

hence $f_1(x_0)^3 = 0$, which implies that $f_1(x_0) = 0$. This contradicts the assumption that f_1 and g_1 do not share any roots. We conclude that u and g_1 do not share any roots. Now we can prove the claim; assume that $g_2(x'_0) = 0$ for some point (x'_0, y'_0) in $E(\bar{K})$. Then from (3.2) it follows that

$$f_2(x'_0)^2(x'^3_0 + Ax'_0 + B)g_1(x'_0)^3 = u(x'_0)g_2(x'_0)^2 = 0. \quad (3.3)$$

Since f_2 and g_2 do not share any roots, we have

$$(x'^3_0 + Ax'_0 + B)g_1(x'_0)^3 = 0.$$

If $g_1(x'_0)^3 = 0$, then $g_1(x'_0) = 0$ and the claim is shown by contraposition. If $x'^3_0 + Ax'_0 + B = 0$, then we can write

$$x^3 + Ax + B = (x - x'_0)v(x) \quad \text{and} \quad g_2(x) = (x - x'_0)w(x),$$

for some polynomials v, w in $\bar{K}[X]$. Substituting this in (3.2) gives

$$f_2(x)^2(x - x'_0)v(x)g_1(x)^3 = u(x)[(x - x'_0)w(x)]^2,$$

and thus

$$f_2(x)^2 v(x) g_1(x)^3 = u(x)(x - x'_0) w(x)^2.$$

Hence we obtain

$$f_2(x'_0)^2 v(x'_0) g_1(x'_0)^3 = 0.$$

Since $x^3 + Ax + B$ has no double roots, we have that $v(x'_0) \neq 0$. We also have that $f_2(x'_0) \neq 0$ since f_2 and g_2 do not share any roots by assumption. Therefore $g_1(x'_0) = 0$ and thus, by contraposition, the claim follows. \square

Example 3.4. The multiplication-by- n map is an endomorphism for any integer n . In Section 3.2, we construct an explicit rational map for this endomorphism, using the so-called *division polynomials*.

The definition of the *degree* of an endomorphism is given below. We will see later in this section that it can help to indicate the number of elements in its kernel.

Definition 3.5. Let E be an elliptic curve defined over K and $\alpha: E(\bar{K}) \rightarrow E(\bar{K})$ be an endomorphism defined by

$$\alpha(x, y) = (r_1(x), r_2(x)y), \tag{3.4}$$

where $r_1(x) = f_1(x)/g_1(x)$ for some polynomials f_1, g_1 in $\bar{K}[X]$. The *degree* of α , denoted by $\deg(\alpha)$, is defined as

$$\deg(\alpha) := \max\{\deg(f_1), \deg(g_1)\},$$

where $\deg(f_1)$ and $\deg(g_1)$ denote the degrees of the polynomials f_1 and g_1 respectively.

Another property of α that is of importance in our study is the notion of separability, which plays a significant role when we consider elliptic curves over finite fields.

Definition 3.6. Let E be an elliptic curve defined over K and let α be of the form given in (3.4). The map α is defined to be a *separable* endomorphism if the (formal) derivative r'_1 is not the zero polynomial.

A useful equivalent formulation for separability is given in the following lemma.

Lemma 3.7. *Let E be an elliptic curve defined over K . Let α be an endomorphism written as in (3.4). Then α is separable if and only if f'_1 or g'_1 is not the zero polynomial.*

Proof. We will prove the following equivalent statement: the endomorphism α in (3.4) is not separable if and only if both f'_1 and g'_1 are the zero polynomial.

(\Rightarrow) Assume α is not separable. Then $r'_1 = 0$, so we have that

$$r'_1 = \frac{f'_1 g_1 - g'_1 f_1}{g_1^2} = 0$$

and thus

$$f'_1 g_1 = g'_1 f_1. \tag{3.5}$$

Suppose for a contradiction that g'_1 is not zero. Then g_1 is of degree at least 1, so it has a root x_0 in \bar{K} . Since f_1 and g_1 do not have any common roots, we have that x_0 is not a

root of f_1 . Consider the following two cases: $g'_1(x_0) \neq 0$ and $g'_1(x_0) = 0$. First, suppose the former holds. Then from (3.5) we get

$$0 = f'_1(x_0)g_1(x_0) = g'_1(x_0)f_1(x_0),$$

and therefore $f_1(x_0) = 0$, a contradiction. Suppose instead that $g'_1(x_0) = 0$. Then, for some u, v in $\bar{K}[X]$, we can write

$$g_1(x) = (x - x_0)^m u(x), \quad g'_1(x) = (x - x_0)^n v(x),$$

where $m, n \in \mathbb{N}$, $m > n$ and $u(x_0), v(x_0)$ are both nonzero. The equation in (3.5) gives

$$f'_1(x)(x - x_0)^m u(x) = (x - x_0)^n v(x)f_1(x),$$

and therefore

$$f'_1(x)(x - x_0)^{m-n} u(x) = v(x)f_1(x).$$

We evaluate at $x = x_0$ to obtain

$$0 = v(x_0)f_1(x_0).$$

Hence $f_1(x_0) = 0$ and we have reached a contradiction. We can conclude that g'_1 is 0. By symmetry, we conclude that f'_1 must be 0 as well. This proves one direction.

(\Leftarrow) Suppose that f'_1 and g'_1 are both equal to the zero polynomial. Then, by computing the derivative of r_1 , we see that

$$r'_1 = \frac{f'_1 g_1 - g'_1 f_1}{g_1^2} = 0.$$

So $r'_1 = 0$ and therefore α is not separable. This proves the other direction and the statement follows. \square

The *Frobenius*, defined below, is a well-known endomorphism that is used extensively in the theory of elliptic curves over finite fields. Throughout the rest of this thesis, the finite field of order q is denoted by \mathbb{F}_q , where q is the power of a prime. If we explicitly require \mathbb{F}_q to be of prime order, we will write \mathbb{F}_p instead.

Definition 3.8. Let E be an elliptic curve defined over a finite field \mathbb{F}_q . The *Frobenius* $\varphi_q: E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_q)$ is defined by

$$\varphi_q(x, y) = (x^q, y^q).$$

Remark. To see that φ_q is well-defined, consider the generalised Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

We have that $(a + b)^q = a^q + b^q$ (since q is a power of the characteristic of \mathbb{F}_q) and $a^q = a, b^q = b$ for all $a, b \in \mathbb{F}_q$ by Fermat's little theorem. Therefore, raising the equation above to the q -th power gives

$$(y^q)^2 + a_1 x^q y^q + a_3 y^q = (x^q)^3 + a_2 (x^q)^2 + a_4 x^q + a_6.$$

Hence $\varphi_q(x, y) = (x^q, y^q) \in E(\mathbb{F}_q)$.

We will now see that φ_q also respects the group structure of an elliptic curve.

Lemma 3.9. *Let E be an elliptic curve over \mathbb{F}_q . The Frobenius φ_q is an endomorphism of degree q and it is not separable.*

Proof. Clearly, φ_q is a map given by rational functions and has degree q . To show that φ_q is a group homomorphism, let $(x_1, y_1), (x_2, y_2) \in E(\bar{\mathbb{F}}_q)$. If $x_1 \neq x_2$, then the sum equals (x_3, y_3) with

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Raising everything to the power q gives

$$x_3^q = (m')^2 - x_1^q - x_2^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{where } m' = \frac{y_2^q - y_1^q}{x_2^q - x_1^q},$$

using the fact that $(x + y)^q = x^q + y^q$ for all x, y in $\bar{\mathbb{F}}_q$. Therefore, we have

$$\varphi_q(x_3, y_3) = \varphi_q(x_1, y_1) + \varphi_q(x_2, y_2).$$

The cases with $x_1 = x_2$ or with one of the points being equal to \mathcal{O} can be checked in a similar manner. If we add a point (x_1, y_1) to itself, we have that

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{where } m = \frac{3x_1^2 + A}{2y_1}.$$

If we raise this to the q -th power, we obtain

$$x_3^q = (m')^2 - 2x_1^q, \quad y_3^q = m'(x_1^q - x_3^q) - y_1^q, \quad \text{where } m' = \frac{3^q(x_1^q)^2 + A^q}{2^q y_1^q}.$$

Since $2, 3, A \in \mathbb{F}_q$, we have that

$$2^q = 2, \quad 3^q = 3 \quad \text{and} \quad A^q = A.$$

Thus, we obtain $\varphi_q(x_3, y_3) = 2\varphi_q(x_1, y_1)$ as desired. So indeed, φ_q is a group homomorphism given by rational functions, hence an endomorphism. Since q is equivalent to 0 in \mathbb{F}_q , the derivative of x^q is identically 0, hence φ_q is not separable. \square

The following theorem will give a relation between the order of the kernel and the degree of an endomorphism. It is crucial in proving Hasse's theorem, which will be done at the end of this subsection.

Theorem 3.10. *Let E be an elliptic curve defined over K . Let α be a separable endomorphism of E . Then*

$$\#\ker(\alpha) = \deg(\alpha),$$

where $\ker(\alpha)$ denotes the kernel of the group homomorphism α . If α is not separable, then

$$\#\ker(\alpha) < \deg(\alpha).$$

Proof. Write $\alpha(x, y) = (r_1(x), r_2(x)y)$, where $r_1(x) = f_1(x)/g_1(x)$. If α is separable, then we have $r_1 \neq 0$ and thus $f_1 g_1' - g_1 f_1' \neq 0$. Define

$$S := \left\{ x \in \bar{K} : (f_1 g_1' - g_1 f_1')(x) g_1(x) = 0 \right\}.$$

Take (a, b) in $E(\bar{K})$ such that it satisfies the following properties:

- (i) $a \neq 0$, $b \neq 0$ and $(a, b) \neq \mathcal{O}$;
- (ii) $\deg(f_1(x) - a \cdot g_1(x)) = \max\{\deg(f_1), \deg(g_1)\} = \deg(\alpha)$;
- (iii) $a \notin r_1(S)$ (i.e., a is not in the image of S under r_1);
- (iv) $(a, b) \in \alpha(E(\bar{K}))$.

Note that since \bar{K} is algebraically closed, the group $E(\bar{K})$ is of infinite order. Hence, we can certainly find a point (a, b) satisfying the first condition. Clearly, there exist infinitely many values of a such that the second condition is satisfied. Since $r_1(S)$ is finite (because S is finite) and we have infinitely many choices for a , we can satisfy the third condition as well. Moreover, since $r_1(x)$ takes on infinitely many values as x goes through \bar{K} and every x gives a point (x, y) in $E(\bar{K})$, we have that $\alpha(E(\bar{K}))$ is of infinite order. So we can find a point $(a, b) \in \alpha(E(\bar{K}))$ satisfying the first three conditions.

Since we are considering an algebraically closed field, we have that $f_1 - a \cdot g_1$ has $\deg(\alpha)$ roots by condition (ii), counting with multiplicities. We will show that $f_1 - a \cdot g_1$ has no multiple roots. In this case, there exists exactly $\deg(\alpha)$ points (x, y) in $E(\bar{K})$ such that $\alpha(x, y) = (a, b)$. For such a point (x, y) (which exists by condition (iv)), we have that

$$a = \frac{f_1(x)}{g_1(x)} \quad \text{and} \quad b = y \cdot r_2(x).$$

Since we chose $(a, b) \neq \mathcal{O}$, it holds that $g_1(x) \neq 0$. Furthermore, because $b \neq 0$, we have $r_2(x) \neq 0$ and thus $y = b/r_2(x)$. This means that y is determined by x . Therefore, it will suffice check the number of values for x for which $\alpha(x, y) = (a, b)$ holds.

Suppose $x_0 \in \bar{K}$ is a multiple root of $f_1 - a \cdot g_1$. Then

$$f_1(x_0) - a \cdot g_1(x_0) = 0 \quad \text{and} \quad f_1'(x_0) - a \cdot g_1'(x_0) = 0.$$

Since $f_1(x_0) = a \cdot g_1(x_0)$, multiplying the second equation by $f_1(x_0)$ on both sides gives

$$a \cdot f_1(x_0)g_1'(x_0) = a \cdot g_1(x_0)f_1'(x_0).$$

Since $a \neq 0$, we have that x_0 is a root of $f_1g_1' - g_1f_1'$. This means that $x_0 \in S$, thus $a = r_1(x_0) \in r_1(S)$, which contradicts the third condition. Hence $f_1 - a \cdot g_1$ has $\deg(\alpha)$ distinct roots. We can now conclude that the kernel of α has order $\deg(\alpha)$ due to the bijection

$$\begin{aligned} \{(x, y) \in E(\bar{K}) : \alpha(x, y) = (a, b)\} &\rightarrow \ker(\alpha), \\ (x, y) &\mapsto (x, y) - (x_1, y_1), \end{aligned} \tag{3.6}$$

where the point (x_1, y_1) in $E(\bar{K})$ satisfying $\alpha(x_1, y_1) = (a, b)$.

If α is not separable, then all the steps above hold, except that $f_1' - a \cdot g_1'$ will be the zero polynomial by Lemma 3.7. Thus $f_1 - a \cdot g_1$ will always have multiple roots and hence, $f_1(x) - a \cdot g_1(x) = 0$ has less than $\deg(\alpha)$ solutions. Therefore, it follows that the kernel of α has fewer than $\deg(\alpha)$, using (3.6). \square

In addition to the theorem above, we can find another very useful property of endomorphisms.

Theorem 3.11. *Let E be an elliptic curve defined over K . Any endomorphism of E is surjective.*

Proof. Let α be an endomorphism of E and let $(a, b) \in E(\bar{K})$. Since $\alpha(\mathcal{O}) = \mathcal{O}$, we can assume that $(a, b) \neq \mathcal{O}$. Let $r_1(x) = f_1(x)/g_1(x)$ and suppose it is in its simplest form, so that f_1 and g_1 do not share any roots. We consider two cases: $f_1 - a \cdot g_1$ is not constant and $f_1 - a \cdot g_1$ is constant.

If $f_1 - a \cdot g_1$ is not constant, then it has a root $x_0 \in \bar{K}$. Since f_1 and g_1 do not have any roots in common, we must have that $g_1(x_0)$ is nonzero, thus $a = f_1(x_0)/g_1(x_0)$. Pick y_0 in \bar{K} to be one of the square roots of $x_0^3 + Ax_0 + B$. Then $\alpha(x_0, y_0) = (a, b')$ for some b' in \bar{K} . Since

$$(b')^2 = a^3 + Aa + B = b^2,$$

it follows that $b' = \pm b$. If $b' = b$, then $\alpha(x_0, y_0) = (a, b)$ as desired. If $b' = -b$, then take $(x_0, -y_0)$ in $E(\bar{K})$. This gives

$$\alpha(x_0, -y_0) = -\alpha(x_0, y_0) = -(a, b') = (a, -b') = (a, b),$$

as desired.

Suppose instead that $f_1 - a \cdot g_1$ is constant. Since $E(\bar{K})$ is of infinite order and $\ker(\alpha)$ is finite by Theorem 3.10, only finitely many points in $E(\bar{K})$ can map to a point with a given x -coordinate (due to the bijection given in (3.6)). If f_1 and g_1 were both constant, then any element in $E(\bar{K})$ would be mapped to a point with the same x -coordinate under α . This contradicts the reasoning above, hence both f_1 and g_1 must be nonconstant (if only one of them were nonconstant, then $f_1 - a \cdot g_1$ is not constant, contrary to the assumption). If f_1, g_1 are both not constant, then a is the unique element such that $f_1 - a \cdot g_1$ is constant. This follows from the fact that if a' were another such element, then

$$(a' - a)g_1 = f_1 - a \cdot g_1 - (f_1 - a' \cdot g_1),$$

thus g_1 is constant and similarly f_1 is constant, which we assumed is not the case. Hence there are at most two points, (a, b) and $(a, -b)$, that are not in the range of α (for the other points, the first case applies). We can find a point (a_1, b_1) in $E(\bar{K})$ such that $(a_1, b_1) + (a, b) \neq (a, \pm b)$ (since $E(\bar{K})$ is of infinite order). There exists P, Q in $E(\bar{K})$ such that

$$\alpha(P) = (a_1, b_1) \quad \text{and} \quad \alpha(Q) = (a_1, b_1) + (a, b).$$

Now we have that $\alpha(P - Q) = (a, b)$ and $\alpha(Q - P) = (a, -b)$, hence (a, b) and $(a, -b)$ are in the range of α .

Thus, α is surjective as desired. \square

Most of the hard work on general endomorphisms is now done. This brings us close to proving a very important result of this section, called Hasse's theorem.

Theorem 3.12 (Hasse's theorem). *Let E be an elliptic curve defined over \mathbb{F}_q . Then*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

In order to prove this theorem, we need to examine the Frobenius endomorphism a bit further. To this end, we state and prove the following two lemmata.

Lemma 3.13. *Let E be defined over \mathbb{F}_q and let (x, y) in $E(\bar{\mathbb{F}}_q)$ be arbitrary. Then $(x, y) \in E(\mathbb{F}_q)$ if and only if $\varphi_q(x, y) = (x, y)$.*

Proof. We first claim and prove that $\mathbb{F}_q = \{a \in \bar{\mathbb{F}}_q : a^q = a\}$. Note that the multiplicative group \mathbb{F}_q^\times contains all nonzero elements of \mathbb{F}_q and thus has order $q - 1$. This implies that $a^{q-1} = 1$ for all a nonzero. Hence $a^q = a$ for all a in \mathbb{F}_q . All elements in the set on the right-hand side are roots of the polynomial $x^q - x$. Since the (formal) derivative of this polynomial is $qx^{q-1} - 1 = -1 \neq 0$, it follows that $x^q - x$ does not have any double roots. Thus, there are q distinct a in $\bar{\mathbb{F}}_q$ such that $a^q = a$. Since both sets have the same cardinality and $\mathbb{F}_q \subseteq \{a \in \bar{\mathbb{F}}_q : a^q = a\}$, the claim follows. Now we can prove the lemma.

(\Rightarrow) Suppose $(x, y) \in E(\mathbb{F}_q)$, this gives x and y in \mathbb{F}_q . Hence $x^q = x$ and $y^q = y$ by the equality of sets above. Therefore $\varphi_q(x, y) = (x^q, y^q) = (x, y)$.

(\Leftarrow) The assumption $\varphi_q(x, y) = (x, y)$ implies $x^q = x$ and $y^q = y$. So by the equality of sets above, $(x, y) \in E(\mathbb{F}_q)$. \square

Lemma 3.14. *Let E be defined over \mathbb{F}_q and let n be a positive integer. The map $\varphi_q^n - 1: E(\bar{\mathbb{F}}_q) \rightarrow E(\bar{\mathbb{F}}_q)$ is a separable endomorphism of E . Moreover, it satisfies*

$$\ker(\varphi_q^n - 1) = E(\mathbb{F}_{q^n}) \quad \text{and} \quad \#E(\mathbb{F}_{q^n}) = \deg(\varphi_q^n - 1).$$

Proof. It is not hard to show that the composition of endomorphisms gives an endomorphism. Hence $\varphi_q^n = \varphi_q \circ \cdots \circ \varphi_q$ is an endomorphism for all $n \geq 1$. Since multiplication-by-1 is clearly an endomorphism as well, it follows that the linear combination $\varphi_q^n - 1$ is also an endomorphism. Separability follows from [Was08, Section 2.9, Proposition 2.29], since $p \nmid 1$ for any prime p . Lemma 3.13 implies that $\varphi_q^n(x, y) = (x, y)$ precisely when $(x, y) \in E(\mathbb{F}_{q^n})$. Consequently, the first equality follows. The second equality follows from Theorem 3.10, since $\varphi_q^n - 1$ is separable. \square

Before showing the result, we need the lemma below for which a proof can be found in [Was08, Section 3.3, Lemma 3.16].

Lemma 3.15. *Let E be an elliptic curve defined over K . Let α, β be endomorphisms and let a, b be integers. Then*

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

The proof of Hasse's theorem is given below.

Proof. Define $a_q := q + 1 - \#E(\mathbb{F}_q)$. We claim that

$$\deg(r\varphi_q - s) = r^2q + s^2 - rsa_q$$

for all integers r, s . Note that by Lemma 3.15, we have

$$\deg(r\varphi_q - s) = r^2 \deg(\varphi_q) + s^2 \deg(-1) + rs(\deg(\varphi_q - 1) - \deg(\varphi_q) - \deg(-1)).$$

By Lemma 3.9, $\deg(\varphi_q) = q$ and clearly, $\deg(-1) = 1$. Now, by Lemma 3.14, we obtain

$$\deg(r\varphi_q - s) = r^2q + s^2 + rs(\#E(\mathbb{F}_q) - q - 1) = r^2q + s^2 - rsa_q.$$

Since the degree of $r\varphi_q - s$ is nonnegative, it follows that

$$r^2q + s^2 - rsa_q \geq 0.$$

Assume that s is nonzero, then we have

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

The set of rational numbers r/s is dense² in \mathbb{R} . Thus, we have

$$qx^2 - a_q x + 1 \geq 0$$

for all x in \mathbb{R} . The discriminant $a_q^2 - 4q$ must therefore be less than or equal to zero. It follows that $|a_q| \leq 2q$. Recalling the definition of a_q now gives the desired result. \square

Remark. The term a_q is also known as the *trace of Frobenius*.

In some cases, Hasse's theorem can help to determine the group order so that we do not need to resort to a complicated algorithm. The important thing to remember is the fact that the order of any element in the group divides the order of the group. In our case, the *order* of a point P in $E(\mathbb{F}_q)$ is the smallest positive integer k such that $kP = \mathcal{O}$. We can illustrate such a use of Hasse's theorem via an example.

Example 3.16. Consider $E: y^2 = x^3 + x + 2$ over \mathbb{F}_{71} . Hasse's theorem gives us

$$56 \leq \#E(\mathbb{F}_{71}) \leq 88.$$

By some trial-and-error, we find that $(0, 59) \in E(\mathbb{F}_{71})$ with order 40. Now, notice that the order is greater than the interval length, hence only one multiple of 40, namely 80, lies between 56 and 88. We can conclude that the order of the group must be equal to 80. If we cannot find a point with such a specific order, there is still another trick that can be useful; observe that both $(3, 23), (34, 19) \in E(\mathbb{F}_{71})$. These points have orders 8 and 5 respectively. Hence, the group order must be a multiple of $\text{lcm}(8, 5) = 40$. So again, we find that $\#E(\mathbb{F}_{71}) = 80$.

In most cases, the group $E(\mathbb{F}_q)$ will contain a point of order greater than the length of the interval in Hasse's bound, that is, greater than $4\sqrt{q}$. Therefore, in theory, one could often use this method to determine the group order. However, more sophisticated algorithms have been developed that can significantly decrease the effort needed to compute the group order. A few examples are Schoof's algorithm and the baby-step, giant-step algorithm with Mestre's trick. The latter is also used by SageMath [Sag20], a software package we will extensively use when we look for anomalous curves in Section 7. More information on algorithms that can determine the group order can be found in [Was08] and, for more algorithms on elliptic curves in general, see [Coh13].

3.2 Torsion points

Apart from Hasse's theorem, we can obtain more information about the structure of the group of points on an elliptic curve by considering torsion points. These are points that have a finite order. In 1908, Beppo Levi conjectured that the number of torsion points of an elliptic curve over \mathbb{Q} is finite. More specifically, after a slight adaptation by Trygve Nagell and later by Andrew Ogg, it was conjectured that

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4, \end{aligned}$$

were the only possible torsion subgroups of an elliptic curve over \mathbb{Q} . This was later proven by Barry Mazur in [Maz77]. In this subsection, we will examine the torsion subgroup of an elliptic curve over a field K with characteristic not equal to 2 or 3.

²This follows from the fact that we can take s to be powers of 2 and the fact that the numbers $r/2^m$ are dense in \mathbb{R} . These numbers are the so-called dyadic rationals and the proof of their density is very much like showing \mathbb{Q} is dense in \mathbb{R} . The dyadic rationals are *p-adic numbers*. We will discuss such numbers in more detail in Section 4.

Definition 3.17. Let E be an elliptic curve defined over a field K . For a positive integer n , we define the set of n -torsion points as

$$E[n] := \{P \in E(\bar{K}) : nP = \mathcal{O}\}.$$

Remark. The reason why we consider points in the algebraic closure is because we have defined endomorphisms over the algebraic closure as well. This is important since we can now apply the theory of the previous subsection to the multiplication-by- n endomorphism and examine its kernel.

Remark. Note that $E[n]$ does not only contain points of order n in $E(\bar{K})$, but all points in $E(\bar{K})$ with order dividing n .

It is not hard to show that $E[n]$ is a subgroup of $E(\bar{K})$. This section aims to prove the following important result about torsion points.

Theorem 3.18. *Let E be an elliptic curve over a field K with characteristic p and let n be a positive integer. If $p \nmid n$ or $p = 0$, then*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

If $p \mid n$, write $n = p^r m$, where $p \nmid m$ and $r \geq 1$ is an integer. Then

$$E[n] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{or} \quad E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Even though this is already a fascinating statement in itself, it will also help in proving another result about $E(\mathbb{F}_q)$. Together with Hasse's theorem, these give heavy restrictions on the structure of this group. This is because, using Theorem 3.18, we can prove that $E(\mathbb{F}_q)$ is either cyclic, or isomorphic to the product of two cyclic groups. This is captured by the following result.

Theorem 3.19. *Let E be an elliptic curve over \mathbb{F}_q . Then*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z},$$

with n a positive integer, or

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

for positive integers n_1, n_2 with $n_1 \mid n_2$.

Proof. From the structure theorem for finite abelian groups, we have that there exists integers n_1, \dots, n_k , all greater than 1 and $k \geq 1$, such that $n_1 \mid n_2 \mid \dots \mid n_k$ and

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Each group $\mathbb{Z}/n_i\mathbb{Z}$ has precisely n_i elements of order dividing n_i . Thus, $E(\mathbb{F}_q)$ has n_1^k elements with such order. By the theorem above, there are at most n_1^2 elements with order dividing n_1 , hence $r \leq 2$ and the statement follows. \square

In order to prove Theorem 3.18, we first consider the lemma below.

Lemma 3.20. *Let E be an elliptic curve defined over a field K of characteristic $p > 0$ and let $n = p^r m$, with $r \geq 0$ and $p \nmid m$. Then*

$$E[n] \cong E[p^r] \times E[m].$$

Proof. Consider the map

$$\begin{aligned} f: E[p^r] \times E[m] &\rightarrow E[n], \\ (P, Q) &\mapsto P \oplus Q. \end{aligned}$$

This clearly maps to $E[n]$. Moreover, it is a homomorphism since $E[n]$ is abelian and

$$(P, Q) + (P', Q') = (P \oplus P', Q \oplus Q').$$

To prove that it is injective, suppose that $f(P, Q) = f(P', Q')$ for P, P' in $E[p^r]$ and Q, Q' in $E[m]$. Then we have $P \ominus P' = Q \ominus Q'$. Since the order of $P \ominus P'$ now divides p^r and m , and $\gcd(p^r, m) = 1$, we have that $P \ominus P' = \mathcal{O}$. Similarly, $Q \ominus Q' = \mathcal{O}$. This shows that f is injective.

For surjectivity, take an element R in $E[n]$. The order of R either equals n or divides one of the coprime factors p^r or m . If the latter holds, then we have $R = f(R, \mathcal{O})$ or $R = f(\mathcal{O}, R)$, respectively. If the order of R equals n , choose integers a and b satisfying $a \cdot m + b \cdot p^r = 1$. Since $mR \in E[p^r]$ and $p^r R \in E[m]$, it now follows that

$$R = (x \cdot m + y \cdot p^r)R = (x \cdot m)R \oplus (y \cdot p^r)R = f((x \cdot m)R, (y \cdot p^r)R).$$

This proves the result. \square

To construct an explicit rational map for the multiplication-by- n endomorphism, we need to introduce *division polynomials*.

Definition 3.21. The division polynomials ψ_m in $\mathbb{Z}[x, y, A, B]$ are defined recursively as

$$\begin{aligned} \psi_0 &= 0, \\ \psi_1 &= 1, \\ \psi_2 &= 2y, \\ \psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\ \psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad \text{for } m \geq 2, \\ \psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \quad \text{for } m \geq 3. \end{aligned}$$

Remark. Note that in the definition x, y, A and B are variables.

Lemma 3.22. *Let n be a nonnegative integer. The division polynomial ψ_n is in $\mathbb{Z}[x, y^2, A, B]$ for odd n and in $2y\mathbb{Z}[x, y^2, A, B]$ for even n .*

Proof. We prove the statement by induction on n . The statement holds for $n \leq 4$ by definition. First, consider the case when n is even. Let $n = 2m$ for an integer $m > 2$ and suppose that $\psi_i \in 2y\mathbb{Z}[x, y^2, A, B]$ for all $i < n$. Observe that we have $2m > m + 2$, hence all polynomials in the expression of ψ_{2m} satisfy the induction hypothesis. If m is even, then ψ_m, ψ_{m+2} and ψ_{m-2} are all in $2y\mathbb{Z}[x, y^2, A, B]$ and therefore so is $\psi_n = \psi_{2m}$. If m is odd, then $\psi_{m-1}, \psi_{m+1} \in 2y\mathbb{Z}[x, y^2, A, B]$. Hence $\psi_{m-1}^2, \psi_{m+1}^2$ are both in $4y^2\mathbb{Z}[x, y^2, A, B]$, and we have $\psi_n = \psi_{2m}$ is in $2y\mathbb{Z}[x, y^2, A, B]$. Suppose instead that n is odd. Then $n = 2m + 1$ for some integer $m \geq 2$ and thus $2m + 1 > m + 2$. We don't have to consider different cases for m ; we always have that one term of $\psi_n = \psi_{2m+1}$ is in $\mathbb{Z}[x, y^2, A, B]$ and the other term is so as well since both terms in the polynomial have even exponents in total. Hence ψ_n is in $\mathbb{Z}[x, y^2, A, B]$ when n is odd. Thus, the statement follows by induction. \square

Define the polynomials

$$\begin{aligned}\varphi_n &= x\psi_n^2 - \psi_{n-1}\psi_{n+1}, \\ \omega_n &= (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2),\end{aligned}$$

for which we can prove the lemma below.

Lemma 3.23. *Let n be a nonnegative integer. Then $\varphi_n \in \mathbb{Z}[x, y^2, A, B]$. If n is odd, then $\omega_n \in y\mathbb{Z}[x, y^2, A, B]$. Otherwise $\omega_n \in \mathbb{Z}[x, y^2, A, B]$.*

Proof. First, consider the case when n is odd. By the previous lemma, it follows that ψ_{n-1}, ψ_{n+1} are in $2y\mathbb{Z}[x, y^2, A, B]$ and therefore both are in $y\mathbb{Z}[x, y^2, A, B]$ as well and thus their product is in $\mathbb{Z}[x, y^2, A, B]$. Since $x\psi_n^2 \in \mathbb{Z}[x, y^2, A, B]$, we conclude that $\varphi_n \in \mathbb{Z}[x, y^2, A, B]$. Note that $\psi_{n+2}\psi_{n-1}^2$ and $\psi_{n-2}\psi_{n+1}^2$ are both in $4y^2\mathbb{Z}[x, y^2, A, B]$ by Lemma 3.22, hence ω_n is in $y\mathbb{Z}[x, y^2, A, B]$.

Now, consider φ_n when n is even. Then ψ_{n-1}, ψ_{n+1} are in $\mathbb{Z}[x, y^2, A, B]$, thus their product is so as well. Since ψ_n is in $2y\mathbb{Z}[x, y^2, A, B]$, it becomes a polynomial in $\mathbb{Z}[x, y^2, A, B]$ when we square it. Therefore, φ_n is in $\mathbb{Z}[x, y^2, A, B]$.

Lastly, we look at ω_n where n is even. It is clear that $\omega_n \in \frac{1}{2}\mathbb{Z}[x, y^2, A, B]$, but, getting rid of the fraction requires a little bit more effort. It follows by induction that

$$\psi_n \equiv (x^2 + A)^{(n^2-1)/4} \pmod{2}, \text{ when } n \text{ is odd,}$$

and

$$(2y)^{-1}\psi_n \equiv \frac{n}{2}(x^2 + A)^{(n^2-4)/4} \pmod{2}, \text{ when } n \text{ is even.}$$

Hence for even n we have

$$\begin{aligned}\omega_n &= (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2) \\ &\equiv (4y)^{-1}\left(2y\frac{n+2}{2}(x^2 + A)^{((n+2)^2-4)/4}(x^2 + A)^{2((n-1)^2-1)/4}\right) \\ &\quad - (4y)^{-1}\left(2y\frac{n-2}{2}(x^2 + A)^{((n-2)^2-4)/4}(x^2 + A)^{2((n+1)^2-1)/4}\right) \pmod{2} \\ &\equiv \frac{1}{4}\left((n+2)(x^2 + A)^{3n^2/4} - (n-2)(x^2 + A)^{3n^2/4}\right) \pmod{2} \\ &\equiv (x^2 + A)^{3n^2/4} \pmod{2}.\end{aligned}$$

So indeed $\omega_n \in \mathbb{Z}[x, y^2, A, B]$ for even n . This concludes the proof \square

We will consider an arbitrary elliptic curve $E: y^2 = x^3 + Ax + B$, so we do not fix A, B and thus leave them as variables. It follows from the previous lemmata that $\psi_n^2, \varphi_n \in \mathbb{Z}[x, A, B]$ due to the relation $y^2 = x^3 + Ax + B$.

Lemma 3.24. *Let n be a nonnegative integer. The leading term of ψ_n is $nx^{(n^2-1)/2}$ when n is odd and $y \cdot nx^{(n^2-4)/2}$ when n is even.*

Proof. We will prove this by induction on n . Clearly, the statement holds for $n = 0, 1$. First, suppose that $n = 2m$ for $m \geq 0$ and assume the statement holds for all values $i \leq n$. Suppose that m is even. Recall that

$$\psi_{n+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,$$

by definition. Denote the leading term of $\psi_{m+2}\psi_m^3$ by μ_1 . Using the induction hypothesis, we obtain

$$\mu_1 = y^4(m+2)m^3x^{(4m^2+4m-12)/2}.$$

Since $y^2 = x^3 + Ax + B$, it follows that

$$\mu_1 = x^6(m+2)m^3x^{(4m^2+4m-12)/2} = (m+2)m^3x^{(4m^2+4m)/2}.$$

The leading term of $\psi_{m-1}\psi_{m+1}^3$, denoted by μ_2 , is given by

$$\mu_2 = (m-1)(m+1)^3x^{(4m^2+4m)/2},$$

using a similar computation. Thus, subtracting these terms gives

$$\begin{aligned} \mu_1 - \mu_2 &= (m+2)m^3x^{(4m^2+4m)/2} - (m-1)(m+1)^3x^{(4m^2+4m)/2} \\ &= \left((m+2)m^3 - (m-1)(m+1)^3 \right) x^{((2m+1)^2-1)/2} \\ &= (2m+1)x^{((2m+1)^2-1)/2}. \end{aligned}$$

Hence, the leading term of $\psi_{n+1} = \psi_{2m+1}$ is $(2m+1)x^{((2m+1)^2-1)/2}$, as desired. The other cases are similar. \square

Corollary 3.25. *Let n be a nonnegative integer. The leading term of φ_n is x^{n^2} and the leading term of ψ_n^2 is $n^2x^{n^2-1}$.*

Proof. Suppose first that n is odd. Then, clearly, the result holds for ψ_n^2 . Recall that

$$\varphi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1}.$$

By Lemma 3.24, the leading term of $x\psi_n^2$ is given by $n^2x^{n^2}$ and for $\psi_{n-1}\psi_{n+1}$ it is given by

$$y(n-1)x^{((n-1)^2-4)/2}y(n+1)x^{((n+1)^2-4)/2},$$

which, using the equation of an elliptic curve, becomes

$$(n^2 - 1)x^{n^2}.$$

We can subtract both terms to obtain x^{n^2} , as desired.

If n is even, then the leading term of ψ_n^2 becomes $y^2 \cdot n^2x^{n^2-4}$ which gives the term

$$x^3 \cdot n^2x^{n^2-4} = n^2x^{n^2-1},$$

as the statement suggests. For φ_n , we have that $x\psi_n^2$ has leading term $xy^2 \cdot n^2x^{n^2-4}$, thus we obtain

$$x^4 \cdot n^2x^{n^2-4} = n^2x^{n^2}.$$

Similarly, for $\psi_{n-1}\psi_{n+1}$ we have the leading term

$$(n-1)x^{((n-1)^2-1)/2}(n+1)x^{((n+1)^2-1)/2} = (n^2+1)x^{n^2}.$$

Subtracting these two terms gives x^{n^2} , as desired. This concludes the proof. \square

The following theorem gives an explicit expression for the multiplication-by- n endomorphism. The proof can be found in [Was08, Section 9.5, Theorem 9.33] and uses the so-called *Weierstrass \wp -functions*.

Theorem 3.26. *Let E be an elliptic curve defined over a field K . For a positive integer n , the multiplication-by- n endomorphism $n: E(\bar{K}) \rightarrow E(\bar{K})$ is given by*

$$n(x, y) = \left(\frac{\varphi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)} \right).$$

Two corollaries that will be needed in proving Theorem 3.18 are given below.

Corollary 3.27. *Let E be an elliptic curve defined over a field K and let n be a positive integer. The multiplication-by- n endomorphism is separable if $\text{char}(K) \nmid n$.*

Proof. By Lemma 3.7, an endomorphism is separable if and only if $f'_1(x)$ or $g'_1(x)$ is not the zero polynomial, where $r_1(x) = f_1(x)/g_1(x)$. From Theorem 3.26 and Corollary 3.25 it follows that

$$r_1(x) = \frac{x^{n^2} + \dots}{n^2 x^{n^2-1} + \dots}.$$

The derivative of f_1 has leading term $n^2 x^{n^2-1}$, which is nonzero since the characteristic of the field does not divide n . This proves the result. \square

In fact, the converse is also true.

Lemma 3.28. *Let E be an elliptic curve defined over a field K and let n be a positive integer. The multiplication-by- n endomorphism is not separable if $\text{char}(K) \mid n$.*

Proof. [Was08, Section 2.9, Proposition 2.28] \square

Corollary 3.29. *Let E be an elliptic curve defined over a field K . The multiplication-by- n endomorphism in Theorem 3.26 has degree n^2 .*

Proof. From Corollary 3.25, it follows that the maximum of the degrees of φ_n and ψ_n^2 is n^2 . If φ_n and ψ_n^2 do not share any roots, then we can conclude that the degree of the map is n^2 by Definition 3.5.

Suppose, aiming for a contradiction, that φ_n and ψ_n^2 share a root and let n be the smallest index for which this occurs. First, consider case (i), in which we assume n is even, so that $n = 2m$ for some integer $m \geq 1$. Using the definitions of ψ_n and φ_n and the fact that $y^2 = x^3 + Ax + B$, we see that a quick computation gives us

$$\begin{aligned} \varphi_2 &= x^4 - 2Ax^2 - 8Bx + A^2, \\ \psi_2^2 &= 4(x^3 + Ax + B). \end{aligned} \tag{3.7}$$

The map in Theorem 3.26 gives us the following expression in the first argument if we consider the image of (x, y) under the multiplication-by- n endomorphism:

$$n(x, y) = 2m(x, y) = 2 \left(\frac{\varphi_m(x)}{\psi_m^2(x)}, \dots \right) = \left(\frac{\varphi_2(\varphi_m/\psi_m^2)}{\psi_2^2(\varphi_m/\psi_m^2)}, \dots \right).$$

By using the equations from (3.7), we obtain

$$\begin{aligned} \frac{\varphi_{2m}}{\psi_{2m}^2} &= \frac{\varphi_2(\varphi_m/\psi_m^2)}{\psi_2^2(\varphi_m/\psi_m^2)} \\ &= \frac{\varphi_m^4 - 2A\varphi_m^2\psi_m^4 - 8B\varphi_m\psi_m^6 + A^2\psi_m^8}{4\psi_m^2(\varphi_m^3 + A\varphi_m\psi_m^4 + B\psi_m^6)} = \frac{U}{V}, \end{aligned}$$

where U, V are the numerator and denominator of the foregoing expression, respectively. Note that U/V might be a reduced form of φ_{2m}/ψ_{2m}^2 . The next lemma will help us to show that U and V have no common roots.

Lemma 3.30. Let $\Delta = 4A^3 + 27B^2$ and define

$$\begin{aligned} F(x, z) &= x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4, \\ G(x, z) &= 4z(x^3 + Axz^2 + Bz^3), \\ h_1(x, z) &= 12x^2z + 16Az^3, \\ \tilde{h}_1(x, z) &= 3x^3 - 5Axz^2 - 27Bz^3, \\ h_2(x, z) &= 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3, \\ \tilde{h}_2(x, z) &= A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 \\ &\quad - 3A^2(A^3 + 8B^2)z^3. \end{aligned}$$

Then

$$Fh_1 - G\tilde{h}_1 = 4\Delta z^7 \quad \text{and} \quad Fh_2 + G\tilde{h}_2 = 4\Delta x^7.$$

Remark. The functions F and G correspond to U and V , respectively.

Proof. (of Lemma 3.30). It can be shown that $F(x, 1)$ and $G(x, 1)$ do not share any roots. Using the extended Euclidean algorithm, the polynomials $h_1(x)$ and $\tilde{h}_1(x)$ can be found such that $F(x, 1)h_1(x) + G(x)\tilde{h}_1(x) = 1$. Then, by applying the map $x \mapsto x/z$, multiplying everything by $4\Delta z^7$ to homogenise the equation and clearing the denominators, this gives us the first equality. The second one is obtained by switching the roles of x and z (thus, by considering $F(1, z)$ and $G(1, z)$). Both equalities can be verified with straightforward calculations. \square

Evaluating the both equations at $(x, z) = (\varphi_m, \psi_m^2)$ gives us

$$\begin{aligned} Uh_1(\varphi_m, \psi_m^2) - V\tilde{h}_1(\varphi_m, \psi_m^2) &= 4\Delta\psi_m^{14}, \\ Uh_2(\varphi_m, \psi_m^2) - V\tilde{h}_2(\varphi_m, \psi_m^2) &= 4\Delta\varphi_m^7. \end{aligned}$$

This implies that if U and V share a root, then so do φ_m and ψ_m^2 . This contradicts the assumption of $n = 2m$ being the smallest index for which φ and ψ^2 share a root. Hence U and V do not share a root, so the fraction U/V is simplified. We still need to show that the fraction φ_{2m}/ψ_{2m}^2 is in its most reduced form (i.e., $U = \varphi_{2m}$ and $V = \psi_{2m}^2$). Since U and V share no roots, it follows that φ_{2m} is a multiple of U and similarly ψ_{2m}^2 is a multiple of V . By using Corollary 3.25, we obtain that the leading term of U is given by x^{4m^2} and similarly the leading term of φ_{2m} is x^{4m^2} too. Since φ_{2m} is a multiple of U we must have the equality $U = \varphi_{2m}$. It follows that $V = \psi_{2m}^2$ as well. Therefore, φ_{2m} and ψ_{2m}^2 do not share any roots.

Now we consider case (ii), where we suppose that n is odd, so that $n = 2m + 1$ for some integer $m \geq 0$. Let η be a common root of φ_n and ψ_n^2 (which are both polynomials in x since A, B are now determined by E). Recall that

$$\varphi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1}.$$

By Lemma 3.22, the product $\psi_{n-1}\psi_{n+1}$ is a polynomial in x . Hence, we have that

$$(\psi_{n-1}\psi_{n+1})(\eta) = 0.$$

Both $\psi_{n-1}^2, \psi_{n+1}^2$ are polynomials in x and their product is 0 at $x = \eta$ by the equation above. Hence, either $\psi_{n-1}^2(\eta)$ or $\psi_{n+1}^2(\eta)$ is zero. Denote this by $\psi_{n+\delta}^2(\eta) = 0$ for $\delta \in \{-1, 1\}$.

Again, by Lemma 3.22, we have that both ψ_n and $\psi_{n+2\delta}$ are polynomials in x , since n is odd. We also have that

$$(\psi_n \psi_{n+\delta})^2 = \psi_n^2 \psi_{n+\delta}^2,$$

and evaluating both sides at η gives us $(\psi_n \psi_{n+\delta})^2(\eta) = 0$, so that $\psi_n \psi_{n+\delta}(\eta) = 0$. It follows that since

$$\varphi_{n+\delta} = x\psi_{n+\delta}^2 - \psi_n \psi_{n+2\delta},$$

we have $\varphi_{n+\delta}(\eta) = 0$. Therefore $\varphi_{n+\delta}$ and $\psi_{n+\delta}^2$ share a root. Since $n + \delta$ is even, we can apply case (i) to it and conclude that $\varphi_{(n+\delta)/2}$ and $\psi_{(n+\delta)/2}^2$ must share a root. Since n is assumed to be the minimal index for which a shared root occurs, we have that

$$\frac{n + \delta}{2} \geq n$$

which, in turn, implies

$$\delta \geq n.$$

If $\delta = -1$, this directly gives a contradiction. In the other case, when $\delta = 1$, we must have $n = 1$. Clearly, $\varphi_1 = x$ and $\psi_1^2 = 1$ do not have a common root, so we reach a contradiction, again.

In all cases we have shown that φ_n and ψ_n^2 do not share any roots. Hence the degree of the multiplication-by- n endomorphism is n^2 . This completes the proof. \square

We have shown that the polynomials φ_n and ψ_n^2 do not share any roots for any positive integer n . Consequently, we see that the x -coordinates of the points in $E[n]$ are precisely the roots of $\psi_n^2(x)$.

Finally, we are able to prove Theorem 3.18.

Proof. Suppose that $p \nmid n$ or $p = 0$. From the structure theorem for finite abelian groups, we have that there exists integers d_1, \dots, d_k , all greater than 1 and $k \geq 1$, satisfying $d_1 \mid d_2 \mid \dots \mid d_k$ such that

$$E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}.$$

Let ℓ be a prime so that $\ell \mid d_1$, then $\ell \mid d_i$ for all i . Since $d_1 \mid n$, we have that $\ell \mid n$. So $E[\ell] \subseteq E[n]$ and since every group $\mathbb{Z}/d_i\mathbb{Z}$ has ℓ distinct elements of order dividing ℓ , it follows that $\#E[\ell] = \ell^k$. From Theorem 3.10, we have that for every separable endomorphism, the order of its kernel equals its degree. The multiplication-by- ℓ endomorphism is separable by Corollary 3.27 since $p \nmid \ell$. By Corollary 3.29 this map has degree ℓ^2 , so it follows that $E[\ell]$ has order ℓ^2 and therefore $k = 2$. Consequently, we have

$$E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}.$$

We already know that $d_1 \mid d_2 \mid n$. Thus, $\#E[n] = n^2 = d_1 d_2$ implies $n = d_1 = d_2$. Therefore, we can conclude that

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Suppose instead that $p \mid n$. First, assume that $n = p^r$ for some integer $r \geq 1$. By Lemma 3.28, we have that the multiplication-by- p endomorphism is not separable. Hence, by Theorem 3.10 and Corollary 3.29, it follows that

$$\#\ker(p) < \deg(p) = p^2.$$

Since an element in $E[p]$ either has order 1 or p , the size of $E[p]$ must be a power of p and therefore equals either 1 or p .

If $E[p]$ is trivial, then so is $E[p^k]$ for any $k \geq 0$. This follows by the following reasoning: if $Q \in E[p^k]$, then $p^{k-1}Q \in E[p]$, thus $p^{k-1}Q = \mathcal{O}$. This implies that $p^{k-2}Q \in E[p]$, so $p^{k-2}Q$ is trivial. Repeating this argument eventually gives us $Q = \mathcal{O}$. Hence $E[p^k]$ is trivial.

If $E[p]$ is of order p , then it is cyclic. We claim that

$$E[p^k] \cong \mathbb{Z}/p^k\mathbb{Z}$$

for all $k \geq 0$. Note that $E[p^k]$ is cyclic for all k . This follows from the fact that $E[p]$ has order p which implies that $E[p^k]$ cannot be isomorphic to the product of two or more cyclic groups, since otherwise it would contain more than p elements of order dividing p . We claim that $E(\bar{K})$ contains elements of order p^j for all $j \geq 1$. If this is the case, then $E[p^k]$ contains an element of order p^k and since $E[p^k]$ is cyclic we thus have $E[p^k] \cong \mathbb{Z}/p^k\mathbb{Z}$ (if $E[p^k]$ would be of greater size, then there would exist an element of order larger than p^k in $E[p^k]$, which would contradict the definition of the group).

We will prove the claim by induction on j . As a base case, note that $E[p^k]$ contains $E[p]$, which is cyclic and hence there exists an element of order p . Now suppose there exists an element P of order p^j in $E[p^k]$, for some integer $j \geq 1$. Since the multiplication-by- p endomorphism is surjective by Theorem 3.11, there exists Q in $E(\bar{K})$ such that $pQ = P$. Thus, we have

$$p^jQ = p^{j-1}P \neq \mathcal{O} \quad \text{and} \quad p^{j+1}Q = p^jP = \mathcal{O}.$$

Hence the order of Q must be p^{j+1} . By induction, there exists points in $E(\bar{K})$ of order p^j for all $j \geq 1$. More specifically, we have an element in $E[p^k]$ of order p^k as desired. We conclude that in this case, $E[p^k] \cong \mathbb{Z}/p^k\mathbb{Z}$ for all $k \geq 0$.

Lastly, assume that $n = p^r m$ where $r \geq 0$ and $p \nmid m$. Because $p \nmid m$, we know that

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Since $\gcd(p^r, m) = 1$, we can apply the Chinese remainder theorem to obtain

$$\mathbb{Z}/p^r\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p^r m\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}.$$

Using that $E[p^r]$ is trivial or isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$, we can now conclude from Lemma 3.20 that since

$$E[n] \cong E[p^r] \times E[m],$$

we either have

$$E[n] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{or} \quad E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

This completes the proof. □

The following example illustrates some of the results we have seen in this subsection.

Example 3.31. Let $E: y^2 = x^3 + 2x$ over \mathbb{F}_5 . Consider the torsion group $E[5]$. We know by Theorem 3.18 that it is isomorphic to either $\{0\}$ or $\mathbb{Z}/5\mathbb{Z}$. One can compute that

$$\psi_5(x) = 4x^{10} + 4 = 4 \cdot (x+2)^5 \cdot (x+3)^5.$$

Notice that this is already a polynomial in x , so we do not have to consider ψ_5^2 . Moreover, it splits completely over \mathbb{F}_5 . We find that $(2, t) \in E[5]$, with $t \in \bar{\mathbb{F}}_5$ such that $t^2 = 2 \in \mathbb{F}_5$. Therefore, we can conclude that $E[5] \cong \mathbb{Z}/5\mathbb{Z}$. Indeed, we have that

$$E[5] = \{\mathcal{O}, (2, t), (2, 4t), (3, 2t), (3, 3t)\}.$$

Now consider $E: y^2 = x^3 + 1$ over \mathbb{F}_5 . Recall that

$$\psi_5 = \psi_4\psi_2^3 - \psi_1\psi_3^3.$$

Since $A = 0$ and $B = 1$, the computation can be easily done by hand. We have

$$\begin{aligned} \psi_5(x, y) &= 4y(x^6 + 20x^3 - 8)(2y)^3 - (3x^4 + 12x)^3 \\ &\equiv 12y^4(x^6 + 2) - (2x^{12} + 4x^9 + x^6 + 3x^3) \pmod{5} \\ &\equiv 2(x^3 + 1)^2(x^6 + 2) - (2x^{12} + 4x^9 + x^6 + 3x^3) \pmod{5} \\ &\equiv (2x^{12} + 4x^9 + x^6 + 3x^3 + 4) - (2x^{12} + 4x^9 + x^6 + 3x^3) \pmod{5} \\ &\equiv 4 \pmod{5}. \end{aligned}$$

It follows that ψ_5 is constant and therefore it has no roots in $\bar{\mathbb{F}}_5$. This means that $E[5]$ is trivial. Moreover, observe that $\#E(\mathbb{F}_5) = 6$. In general, the elliptic curves over finite fields of characteristic p that have no p -torsion points are called *supersingular elliptic curves*. Using Hasse's theorem, one can show that for $p \geq 5$, the supersingular elliptic curves over \mathbb{F}_p are precisely the curves that satisfy $\#E(\mathbb{F}_p) = p + 1$ (cf. [Was08, Section 4.6, Corollary 4.32]). We discuss these curves briefly in Section 7.2.

4 The p -adic numbers and Hensel's lemma

Most of us are familiar with the field of real numbers \mathbb{R} . This field is constructed by considering the rational numbers \mathbb{Q} with the well-known absolute value

$$|x|_\infty = \begin{cases} x, & \text{if } x \geq 0, \\ -x, & \text{if } x < 0, \end{cases}$$

for all x in \mathbb{Q} . As an example, consider the element $\sqrt{2}$ in \mathbb{R} with decimal expansion $1.4142\dots$. This corresponds to the following sequence of partial sums:

$$\begin{aligned} &1, \\ &1 + 4 \cdot 10^{-1}, \\ &1 + 4 \cdot 10^{-1} + 1 \cdot 10^{-2}, \\ &1 + 4 \cdot 10^{-1} + 1 \cdot 10^{-2} + 4 \cdot 10^{-3}, \\ &1 + 4 \cdot 10^{-1} + 1 \cdot 10^{-2} + 4 \cdot 10^{-3} + 2 \cdot 10^{-4}, \end{aligned}$$

and so on. This is a Cauchy sequence in \mathbb{Q} , since the terms get closer and closer together with respect to the absolute value $|\cdot|_\infty$. However, it does not converge in \mathbb{Q} . In \mathbb{R} it does converge, to the element $\sqrt{2}$. The real numbers are constructed in such a way that any Cauchy sequence of rational numbers converges (with respect to $|\cdot|_\infty$). We call \mathbb{R} a *completion* of \mathbb{Q} with respect to the absolute value $|\cdot|_\infty$. In a similar way, we can construct the field of *p -adic numbers* by completing \mathbb{Q} with respect to a different absolute value (thus, by considering a different notion of distance). In fact, one can show that together with \mathbb{R} ,

the p -adic numbers form all completions of \mathbb{Q} . This section will look at the field of p -adic numbers and its construction in more detail. Moreover, a very useful result, called Hensel's lemma, named after German mathematician Kurt Wilhelm Sebastian Hensel (1861 – 1941), and its use in ‘lifting’ points on an elliptic curve will be discussed. The main source of information is [Gou12, Chapters 1-3], where almost all results can be found. In this section, the field K has arbitrary characteristic, unless specified otherwise.

To consider the p -adic numbers, we must first consider the concept of *valuation*, which is introduced in the following subsection.

4.1 Valuations and absolute values

Definition 4.1. Let K be a field. A *valuation* on K is a function $\nu: K \rightarrow \mathbb{R} \cup \{\infty\}$ satisfying the following properties for all x, y in K :

- (i) $\nu(xy) = \nu(x) + \nu(y)$.
- (ii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.
- (iii) $\nu(x) = \infty$ if and only if $x = 0$.

On the field of rational numbers one can consider the following function.

Definition 4.2. Let p be a prime. For a nonzero rational number a , write $a = p^r b/c$ for some integer r , where p does not divide the integers b and c . Define the valuation $\nu_p: \mathbb{Q} \rightarrow \mathbb{R} \cup \{\infty\}$ by $\nu_p(a) = r$ and set $\nu_p(0) = \infty$.

It remains to show that this function is in fact a valuation.

Proposition 4.3. *The function ν_p is a valuation on \mathbb{Q} for any prime p .*

Proof. Let p be a prime. The third property follows by definition. If x or y are 0, then properties (i) and (ii) are readily satisfied. Thus, take x, y in \mathbb{Q}^\times and write

$$x = p^{\nu_p(x)} \frac{a}{b}, \quad y = p^{\nu_p(y)} \frac{c}{d}.$$

Then $p \nmid ab$ and $p \nmid cd$. We have that

$$\nu_p(xy) = \nu_p\left(p^{\nu_p(x)+\nu_p(y)} \frac{ac}{bd}\right) = \nu_p(x + y),$$

where the second equality follows since $p \nmid acbd$. Hence (i) holds. Now suppose, without loss of generality, that $\nu_p(x) \leq \nu_p(y)$. Observe that

$$x + y = p^{\nu_p(x)} \left(\frac{a}{b} + p^{\nu_p(y)-\nu_p(x)} \frac{c}{d} \right) = p^{\nu_p(x)} \frac{ad + p^{\nu_p(y)-\nu_p(x)} bc}{bd}. \quad (4.1)$$

Since $p \nmid bd$, it follows that $\nu_p(x + y) \geq \nu_p(x) = \min\{\nu_p(x), \nu_p(y)\}$, so (ii) is satisfied. \square

Remark. If $\nu_p(x) \neq \nu_p(y)$, then the numerator in the last expression of (4.1) is not divisible by p , since $p \nmid ad$. We conclude that $\nu_p(x + y) = \min\{\nu_p(x), \nu_p(y)\}$ if $\nu_p(x) \neq \nu_p(y)$.

Definition 4.4. Let K be a field. An *absolute value* on K is a function $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$ satisfying the following properties for all x, y in K :

- (i) $|xy| = |x| \cdot |y|$.
- (ii) $|x + y| \leq |x| + |y|$.
- (iii) $|x| = 0$ if and only if $x = 0$.

If an absolute value satisfies the stronger statement $|x + y| \leq \max\{|x|, |y|\}$ instead of (ii), then it is called *non-archimedean*.

Remark. Note that any absolute value $|\cdot|$ satisfies $|1| = 1$. This follows from the first property which says that $|1|^2 = |1|$. The only nonzero real number satisfying $X^2 = X$ is 1, thus $|1| = 1$.

Recall the usual absolute value $|\cdot|_\infty$ on \mathbb{Q} given at the start of this section. We can extend this absolute value to \mathbb{R} in the trivial way. Note that this function is archimedean, since for any positive real number, we have that $|x+x|_\infty = 2x > x = \max\{|x|_\infty, |x|_\infty\}$. The archimedean property for the real numbers says that for any x and y in \mathbb{R} with x nonzero, there exists a positive integer n such that $|nx|_\infty > |y|_\infty$. This can be reformulated by saying that $\sup\{|n|_\infty : n \in \mathbb{Z}\} = \infty$, that is, there are arbitrarily ‘large’ integers [Gou12, Section 2.2]. Similarly, an absolute value $|\cdot|$ which is non-archimedean can be characterised by $\sup\{|n| : n \in \mathbb{Z}\} = 1$. This uses the fact that

$$|n| = |1 + \cdots + 1| \leq \max\{|1|, \dots, |1|\} = 1$$

for all integers n since $|1| = 1$.

Definition 4.5. Let p be a prime. The *p -adic absolute value* $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$ is defined as $|x|_p = p^{-\nu_p(x)}$ for any x in \mathbb{Q}^\times and $|0|_p = 0$.

Example 4.6. Let $p = 3$. Observe that $27 = 3^3$, $48 = 3 \cdot 2^4$ and $7/12 = 7 \cdot 3^{-1} \cdot 2^{-2}$. Then,

$$|27|_3 = \frac{1}{27}, \quad |48|_3 = \frac{1}{3}, \quad \left| \frac{7}{12} \right|_3 = 3.$$

Moreover, consider the rational numbers 12, 14 and 579. The usual absolute value tells us that 12 and 14 are closer together than 12 and 579. The opposite is true if we take the p -adic absolute value, since

$$|14 - 12|_3 = |2|_3 = 1, \quad |579 - 12|_3 = |567|_3 = \left| 7 \cdot 3^4 \right|_3 = \frac{1}{81}.$$

Remark. The notion of size and distance is thus different when we consider the p -adic absolute value. A rational number is small when it is divisible by a high power of p . Similarly, two rational numbers are close if their difference is divisible by a high power of p .

Using the fact that ν_p is a valuation on \mathbb{Q} , it follows that $|\cdot|_p$ is an absolute value on \mathbb{Q} .

Proposition 4.7. *The function $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$ is a non-archimedean absolute value on \mathbb{Q} for any prime p .*

Proof. Let p be a prime and let $x, y \in \mathbb{Q}$. We have that $|0|_p = 0$ by definition. Conversely, if $|x|_p = 0$, then $x = 0$ since p is not zero, so (iii) is satisfied. If $x = 0$ or $y = 0$, then conditions (i) and (ii) follow immediately. Suppose that both x and y are nonzero and note that

$$|x|_p |y|_p = p^{-\nu_p(x) - \nu_p(y)} = p^{-\nu_p(xy)} = |xy|_p,$$

using property (i) in Definition 4.1. Thus (i) holds. Moreover, observe that (ii) holds by the fact that

$$|x + y|_p = p^{-\nu_p(x+y)} \leq p^{-\min\{\nu_p(x), \nu_p(y)\}} = \max\{|x|_p, |y|_p\}.$$

This completes the proof. □

Remark. Following up on the remark made after Proposition 4.3, we see that if $|x|_p \neq |y|_p$ and thus $\nu_p(x) \neq \nu_p(y)$, then

$$|x + y|_p = \max\{|x|_p, |y|_p\}.$$

Two absolute values $|\cdot|_\star$ and $|\cdot|_\times$ on K are said to be *equivalent* if there exists an $\alpha > 0$ such that $|x|_\star = |x|_\times^\alpha$ for all x in K . It can be shown that any absolute value on \mathbb{Q} is equivalent to either the regular absolute value $|\cdot|_\infty$ discussed earlier or to the p -adic absolute value $|\cdot|_p$. This result is known as Ostrowski's theorem; a proof can be found in [Gou12, Section 3.1, Theorem 3.1.3]. We will study the construction of p -adic numbers in the following subsection.

4.2 The construction of the p -adic numbers

Throughout this section, $|\cdot|_p$ denotes the non-archimedean absolute value for some prime p . We start with recalling a few basic definitions of sequences.

Definition 4.8. Let K be a field and $|\cdot|$ be an absolute value on K .

- A sequence $(x_n)_{n \in \mathbb{N}}$ in K *converges to* x with respect to $|\cdot|$ if for all $\varepsilon > 0$ there exists a natural number N such that $|x_n - x| < \varepsilon$ for all $n \geq N$.
- A sequence $(x_n)_{n \in \mathbb{N}}$ in K is called a *Cauchy sequence* in K if for all $\varepsilon > 0$ there exists a natural number N such that $|x_m - x_n| < \varepsilon$ for all $n, m \geq N$.

If we are working with a non-archimedean absolute value on \mathbb{Q} , such as $|\cdot|_p$, then the characterisation of Cauchy sequences in \mathbb{Q} becomes much simpler. This statement, just as most other results in this section, is not limited to the field \mathbb{Q} ; it holds for an arbitrary field K with a non-archimedean absolute value.

Lemma 4.9. Let $(x_n)_{n \in \mathbb{N}}$ be a sequence in \mathbb{Q} and let $|\cdot|_p$ be a non-archimedean absolute value of \mathbb{Q} . The sequence $(x_n)_{n \in \mathbb{N}}$ is Cauchy in \mathbb{Q} if and only if for all $\varepsilon > 0$, there exists a natural number N such that

$$|x_{n+1} - x_n|_p < \varepsilon$$

for all $n \geq N$.

Proof. (\Rightarrow) Suppose that $(x_n)_{n \in \mathbb{N}}$ is Cauchy in \mathbb{Q} . Take $m = n + 1$ in the definition of a Cauchy sequence. The result then follows.

(\Leftarrow) Assume that for all $\varepsilon > 0$ there exists a natural number N such that

$$|x_{n+1} - x_n| < \varepsilon$$

for all $n \geq N$. Take $n, m \geq N$ and assume, without loss of generality, that $m \geq n$. Write $m = n + r$ for some integer $r \geq 0$. We have that

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \dots + x_{n+1} - x_n| \\ &\leq \max\{|x_{n+r} - x_{n+r-1}|, \dots, |x_{n+1} - x_n|\} < \varepsilon. \end{aligned}$$

Hence $(x_n)_{n \in \mathbb{N}}$ is Cauchy in \mathbb{Q} . □

Remark. The condition that the absolute value is non-archimedean is really necessary. For example, consider the harmonic series

$$x_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}, \quad \text{where } n \in \mathbb{N},$$

with respect to the usual absolute value. This sequence is not Cauchy. However, the difference between consecutive terms does converge to 0.

The following lemma uses the non-archimedean property of $|\cdot|_p$ to show that any Cauchy sequence in \mathbb{Q} that does not converge to zero eventually attains a constant absolute value.

Lemma 4.10. *Let $(x_n)_{n \in \mathbb{N}}$ be a Cauchy sequence in \mathbb{Q} with respect to the absolute value $|\cdot|_p$. Assume that $(x_n)_{n \in \mathbb{N}}$ does not converge to 0. Then, there exists a natural number N such that $|x_n|_p = |x_N|_p \neq 0$ for all $n \geq N$.*

Proof. Since $(x_n)_{n \in \mathbb{N}}$ does not converge to 0, there exists $c > 0$ such that for all natural numbers N' there exists $n' \geq N'$ for which

$$|x_{n'}|_p \geq c > 0. \quad (4.2)$$

By the definition of a Cauchy sequence, it follows that for all $\varepsilon > 0$, there exists a natural number N such that $|x_m - x_n|_p < \varepsilon$ for all $n, m \geq N$. Now take $\varepsilon = c/2$ and pick the corresponding N . Choose n' such that (4.2) holds. Then

$$|x_N|_p \geq |x_{n'}|_p - |x_{n'} - x_N|_p > c - \varepsilon = \varepsilon,$$

by the reverse triangle inequality. Since $|x_N - x_n|_p < \varepsilon < |x_N|_p$ for all $n \geq N$, we have $|x_N|_p \neq |x_N - x_n|_p$ for all $n \geq N$. We now obtain

$$|x_n|_p = |x_n - x_N + x_N|_p = \max\{|x_n - x_N|_p, |x_N|_p\} = |x_N|_p,$$

for all $n \geq N$. Clearly, by (iii) of Definition 4.4, $|x_N|_p \neq 0$ since $(x_n)_{n \in \mathbb{N}}$ does not converge to 0. This completes the proof. \square

We define the sets

$$\begin{aligned} \mathcal{C} &:= \{(x_n)_{n \in \mathbb{N}} \text{ a sequence in } \mathbb{Q} : (x_n)_{n \in \mathbb{N}} \text{ is a Cauchy sequence}\}, \\ \mathcal{I} &:= \{(x_n)_{n \in \mathbb{N}} \in \mathcal{C} : (x_n)_{n \in \mathbb{N}} \text{ converges to } 0\}, \end{aligned}$$

considered with respect to the p -adic absolute value.

Proposition 4.11. *The tuple $(\mathcal{C}, +, \cdot, (0), (1))$ with*

$$(x_n)_{n \in \mathbb{N}} + (y_n)_{n \in \mathbb{N}} = (x_n + y_n)_{n \in \mathbb{N}}, \quad (x_n)_{n \in \mathbb{N}} \cdot (y_n)_{n \in \mathbb{N}} = (x_n y_n)_{n \in \mathbb{N}}$$

and

$$(0) = (0, 0, 0, \dots), \quad (1) = (1, 1, 1, \dots)$$

forms a commutative ring.

Proof. This result can be obtained by showing that \mathcal{C} is a subring of the commutative ring of all sequences in \mathbb{Q} , using the identities

$$\begin{aligned} (x_m + y_m) - (x_n + y_n) &= (x_m - x_n) + (y_m - y_n), \\ x_m y_m - x_n y_n &= x_m (y_m - y_n) + y_n (x_m - x_n), \end{aligned} \quad (4.3)$$

and the fact that every Cauchy sequence is bounded. \square

Since we want to construct an extension of \mathbb{Q} , we should have that \mathcal{C} contains \mathbb{Q} . This follows directly from the trivial inclusion map

$$\mathbb{Q} \hookrightarrow \mathcal{C}, \quad x \mapsto (x, x, x, \dots). \quad (4.4)$$

Proposition 4.12. *The set \mathcal{I} is a maximal ideal of \mathcal{C} .*

Proof. The claim that \mathcal{I} is an ideal follows easily by using the second identity in (4.3) and the fact that every Cauchy sequence is bounded. Showing that \mathcal{I} is maximal requires a little more work. First off, note that $(1) \notin \mathcal{I}$, so that \mathcal{I} is proper. Let \mathcal{J} be any ideal of \mathcal{C} with $\mathcal{I} \subsetneq \mathcal{J} \subseteq \mathcal{C}$. We will show that $\mathcal{J} = \mathcal{C}$. Take $(x_n)_{n \in \mathbb{N}}$ in \mathcal{J} such that it does not converge to 0. By Lemma 4.10, there exists a natural number N_1 so that $|x_n|_p = |x_{N_1}|_p \neq 0$ for all $n \geq N_1$. Hence $x_n > 0$ for all $n \geq N_1$. Define the sequence $(y_n)_{n \in \mathbb{N}}$ as follows:

$$y_n := \begin{cases} 1, & \text{if } n < N_1, \\ x_n^{-1}, & \text{if } n \geq N_1. \end{cases}$$

Let $\varepsilon > 0$. Since $(x_n)_{n \in \mathbb{N}}$ is Cauchy in \mathbb{Q} , there exists a natural number N_2 such that

$$|x_{n+1} - x_n|_p < \varepsilon \cdot |x_{N_1}|_p^2,$$

for all $n \geq N_2$ by Lemma 4.9. Let $M = \max\{N_1, N_2\}$. Then, for all $n \geq M$, we have that

$$|y_{n+1} - y_n|_p = |x_{n+1}^{-1} - x_n^{-1}|_p = \frac{|x_{n+1} - x_n|_p}{|x_n x_{n+1}|_p} = \frac{|x_{n+1} - x_n|_p}{|x_{N_1}|_p^2} < \frac{\varepsilon \cdot |x_{N_1}|_p^2}{|x_{N_1}|_p^2} = \varepsilon.$$

Hence $(y_n)_{n \in \mathbb{N}}$ is Cauchy in \mathbb{Q} by Lemma 4.9. Clearly,

$$(x_n)_{n \in \mathbb{N}} \cdot (y_n)_{n \in \mathbb{N}} = (x_n y_n)_{n \in \mathbb{N}} = (1).$$

Since $(x_n)_{n \in \mathbb{N}} \in \mathcal{J}$, this shows $(1) \in \mathcal{J}$. Therefore, $\mathcal{J} = \mathcal{C}$ and we conclude that \mathcal{I} is a maximal ideal. \square

Just as with the construction of the real numbers, the idea is that every p -adic number is a Cauchy sequence of rational numbers, but with respect to the absolute value $|\cdot|_p$. It could happen that the difference of two sequences in \mathcal{C} converges to 0. If this is the case, we would like to identify these Cauchy sequences to avoid ambiguity. This is done by considering the quotient of the ring \mathcal{C} and the ideal \mathcal{I} , denoted by \mathcal{C}/\mathcal{I} . Recall that if we take the quotient of a ring with a maximal ideal, we obtain a field. This results in the following definition.

Definition 4.13. The field of p -adic numbers, denoted by \mathbb{Q}_p , is defined as \mathcal{C}/\mathcal{I} .

Remark. Note that \mathbb{Q}_p contains \mathbb{Q} . Similar to (4.4), we can consider the map

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p, \quad x \mapsto (x, x, x, \dots).$$

If $x \neq y$, then the difference of (x, x, x, \dots) and (y, y, y, \dots) is a constant sequence not equal to (0) . Hence, this difference does not converge to 0 and thus is not in \mathcal{I} . This shows that the map is an inclusion.

It can be shown that \mathbb{Q}_p is indeed a completion of \mathbb{Q} . This means that the absolute value $|\cdot|_p$ on \mathbb{Q} extends to \mathbb{Q}_p , every Cauchy sequence in \mathbb{Q}_p has a limit in \mathbb{Q}_p and every element in \mathbb{Q}_p is the limit of a sequence in \mathbb{Q} . In fact, this completion is unique up to an absolute value preserving isomorphism of fields. One can show, using the order limit theorem, that the extended absolute value function on \mathbb{Q}_p is non-archimedean as well. A proof of the fact that \mathbb{Q}_p is a completion of \mathbb{Q} can be found in [Gou12, Section 3.2].

4.3 The ring of p -adic integers

This subsection considers the field of p -adic numbers and introduces its ring of integers. By examining the ring of integers more closely, we obtain more information about the structure of this ring and the field \mathbb{Q}_p . For example, we will see a general form in which we can represent p -adic numbers. To this end, we start by observing the following.

Proposition 4.14. *The image of $|\cdot|_p: \mathbb{Q}_p \rightarrow \mathbb{R}_{\geq 0}$ is the set $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$.*

Proof. Let x in \mathbb{Q}_p be nonzero. Since \mathbb{Q}_p is a completion, there exists a sequence of rational numbers $(x_n)_{n \in \mathbb{N}}$ converging to x . We have that $|x_n|_p = p^{-\nu_p(x_n)}$, where $\nu_p(x_n) \in \mathbb{Z}$ for all n in \mathbb{N} . Since $(x_n)_{n \in \mathbb{N}}$ converges, the sequence of integers

$$(\nu_p(x_1), \nu_p(x_2), \nu_p(x_3), \dots)$$

converges to some integer k , thus $\nu_p(x) = k$. This gives us $|x|_p = p^{-\nu_p(x)}$, where $-\nu_p(x) \in \mathbb{Z}$. This completes the proof. \square

The proposition above tells us that the p -adic valuation ν_p extends to \mathbb{Q}_p . We will now define the p -adic integers, followed by a basic result.

Definition 4.15. The p -adic integers, denoted by \mathbb{Z}_p , is the set $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

Proposition 4.16. \mathbb{Z}_p is a commutative subring of \mathbb{Q}_p .

Proof. Clearly, $\mathbb{Z}_p \subseteq \mathbb{Q}_p$. Note that $|1|_p = 1$ so that $1 \in \mathbb{Z}_p$. For every x, y in \mathbb{Z}_p we have (using the fact that $|\cdot|_p$ is non-archimedean) that

$$\begin{aligned} |x + (-y)|_p &\leq \max\{|x|_p, |(-y)|_p\} = \max\{|x|_p, |y|_p\} \leq 1, \\ |xy|_p &= |x|_p |y|_p \leq 1. \end{aligned}$$

Therefore $x + (-y), xy \in \mathbb{Z}_p$. Since \mathbb{Q}_p is commutative, so is \mathbb{Z}_p . This proves the result. \square

The ring \mathbb{Z}_p contains \mathbb{Z} since $\nu_p(k)$ is nonnegative for any integer k and hence $|k|_p = p^{-\nu_p(k)} \leq 1$. Moreover, every rational number a/b with b not divisible by p is in \mathbb{Z}_p by the same reasoning. For a nonzero x in \mathbb{Q}_p to be a unit in \mathbb{Z}_p , we must have $|x|_p \leq 1$ and $|x^{-1}|_p \leq 1$. Note that

$$|x|_p |x^{-1}|_p = |xx^{-1}|_p = |1|_p = 1.$$

Hence, we see that $|x|_p = |x^{-1}|_p = 1$, since absolute values are nonnegative. Consequently, all units in \mathbb{Z}_p must have absolute value equal to 1. Clearly, if an element x in \mathbb{Q}_p satisfies $|x|_p = 1$, then $|x^{-1}|_p = 1$, so x is a unit in \mathbb{Z}_p . The set \mathbb{Z}_p^\times of units in \mathbb{Z}_p thus equals

$$\{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

Every rational number a/b with p not dividing ab is a unit in \mathbb{Z}_p .

It can be shown that \mathbb{Z}_p is a *local ring*, which means it only contains one maximal ideal. This follows from the fact that the set of non-unit elements in \mathbb{Z}_p , that is, $\mathbb{Z}_p \setminus \mathbb{Z}_p^\times$ is an ideal (apply the same reasoning as in the proof of Proposition 4.16). We have that $\mathbb{Z}_p \setminus \mathbb{Z}_p^\times$ is equal to $p\mathbb{Z}_p$ since every element x in $\mathbb{Z}_p \setminus \mathbb{Z}_p^\times$ satisfies $|x|_p < 1$ and therefore $|p^{-1}x|_p \leq 1$. This means that $x \in p\mathbb{Z}_p$. Conversely, for every x in $p\mathbb{Z}_p$ we have $x = p^n y$ for some y in \mathbb{Z}_p^\times and a positive integer n . Thus, $|x|_p < 1$ and hence $x \in \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$. We conclude that \mathbb{Z}_p is a local ring with maximal ideal $p\mathbb{Z}_p$.

Theorem 4.17. *For every element x in \mathbb{Z}_p and every positive integer k , there exists a unique Cauchy sequence $(a_n)_{n \in \mathbb{N}}$ in \mathbb{Z} converging to x such that*

$$\begin{aligned} 0 &\leq a_n < p^n, \\ a_{n+1} &\equiv a_n \pmod{p^n}, \\ x &\equiv a_n \pmod{p^n}, \end{aligned}$$

for all positive integers n .

Proof. Let $x \in \mathbb{Z}_p$ and let n be a positive integer. Recall that \mathbb{Q} is dense in \mathbb{Q}_p since \mathbb{Q}_p is the completion of \mathbb{Q} (with respect to $|\cdot|_p$). Hence, we can find a/b in \mathbb{Q} such that

$$\left| x - \frac{a}{b} \right|_p \leq p^{-n} < 1.$$

Using the non-archimedean property of $|\cdot|_p$, we obtain

$$\left| \frac{a}{b} \right|_p = \left| \left(x - \frac{a}{b} \right) - x \right|_p \leq \max \left\{ \left| x - \frac{a}{b} \right|_p, |x|_p \right\} \leq 1.$$

This implies that $p \nmid b$. Hence, we have that p^n and b are coprime, so there exist integers b' and k such that $bb' - 1 = kp^n$. Consequently, using that $|k|_p \leq 1$, we get

$$\left| ab' - \frac{a}{b} \right|_p = \left| \frac{a}{b} \right|_p |bb' - 1|_p = |1 + kp^n - 1|_p = |kp^n|_p \leq p^{-n}.$$

Now take a_n equal to $ab' + mp^n$, where m is the unique integer such that $0 \leq a_n < p^n$ (thus a_n is uniquely determined). Then

$$\begin{aligned} |x - a_n|_p &= \left| x - \frac{a}{b} - \left(ab' - \frac{a}{b} + mp^n \right) \right|_p \\ &\leq \max \left\{ \left| x - \frac{a}{b} \right|_p, \left| ab' - \frac{a}{b} \right|_p, |mp^n|_p \right\} \\ &\leq p^{-n}. \end{aligned}$$

hence $p^n \mid (x - a_n)$, or equivalently, $x \equiv a_n \pmod{p^n}$. Similarly,

$$|a_{n+1} - a_n|_p = |x - a_{n+1} - (x - a_n)|_p \leq \max \left\{ |x - a_{n+1}|_p, |x - a_n|_p \right\} \leq p^{-n},$$

so $a_{n+1} \equiv a_n \pmod{p^n}$. The only thing left to show is that $(a_n)_{n \in \mathbb{N}}$ is Cauchy and converges to x . Let $\varepsilon > 0$. Pick N in \mathbb{N} such that $p^{-N} < \varepsilon$. It follows from the reasoning above that

$$|a_{n+1} - a_n|_p \leq p^{-n} \leq p^{-N} < \varepsilon$$

for all $n \geq N$, so $(a_n)_{n \in \mathbb{N}}$ is Cauchy by Lemma 4.9. Moreover,

$$|x - a_n|_p \leq p^{-n} \leq p^{-N} < \varepsilon$$

for all $n \geq N$. Hence $(a_n)_{n \in \mathbb{N}}$ converges to x . This proves the result. \square

This theorem gives us the following useful corollary.

Corollary 4.18. *Every element x in \mathbb{Z}_p can be uniquely represented as*

$$x = \sum_{i=0}^{\infty} \alpha_i p^i, \quad \text{where } 0 \leq \alpha_i < p \text{ for all } i.$$

Proof. Let $x \in \mathbb{Z}_p$ and take the corresponding sequence $(a_n)_{n \in \mathbb{N}}$ from Theorem 4.17. Write the elements of this sequence in their p -adic expansion:

$$\begin{aligned} a_1 &= \alpha_0, \\ a_2 &= \alpha_0 + \alpha_1 p, \\ &\vdots \\ a_n &= \alpha_0 + \alpha_1 p + \dots + \alpha_{n-1} p^{n-1} \end{aligned}$$

and so on, where $0 \leq \alpha_0, \alpha_1, \alpha_2, \dots < p$. Note that an infinite series converges if its partial sums converge. In this case, the partial sums equal the elements in the sequence $(a_n)_{n \in \mathbb{N}}$ and this sequence converges to x . Hence we can write

$$x = \sum_{i=0}^{\infty} \alpha_i p^i.$$

This representation is unique since all the a_n are uniquely determined by x and this implies all the α_i are so too. \square

In fact, we can find a unique representation for all p -adic numbers.

Corollary 4.19. *Every element x in \mathbb{Q}_p can be uniquely represented as*

$$x = \sum_{i=n_0}^{\infty} \alpha_i p^i, \quad \text{where } 0 \leq \alpha_i < p \text{ for all } i \text{ and } n_0 = \nu_p(x).$$

Proof. Take x in \mathbb{Q}_p and define $y := p^{-\nu_p(x)} x$. Then $|y|_p = 1$ so $y \in \mathbb{Z}_p$. Now apply Corollary 4.18 to y and multiply the resulting series by the constant $p^{\nu_p(x)}$. This gives the desired result for x . \square

4.4 Hensel's lemma

With Newton's method, one can approximate real roots of a polynomial defined over \mathbb{R} under specific conditions. A similar procedure can give roots in \mathbb{Z}_p of a polynomial with coefficients in \mathbb{Z}_p when certain criteria are met. This is a result known as Hensel's lemma. Just as Newton's method gives the decimal expansion of a real root, Hensel's lemma finds the coefficients that uniquely determine the p -adic integer. We will compare the two more closely later in this section. Moreover, the application of Hensel's lemma to elliptic curves will be discussed. First, before stating the result, we illustrate the method used by Hensel's lemma via an example.

Example 4.20. Consider the polynomial $F(X) = X^2 - 3$ with coefficients in \mathbb{Z}_{11} . Even though its existence is not assured, we can try to find a root α of this polynomial in \mathbb{Z}_{11} . First, write

$$\alpha = \sum_{i=0}^{\infty} c_i \cdot 11^i.$$

Suppose we know that $F(\alpha) \equiv 0 \pmod{11}$. This gives $\alpha^2 \equiv 3 \pmod{11}$. Since $\alpha^2 \equiv c_0^2 \pmod{11}$, we require that

$$c_0^2 \equiv 3 \pmod{11}.$$

It is not hard to show that $c_0 = 5$ is a solution. If we consider the problem modulo $11^2 = 121$, we have

$$\alpha^2 \equiv (c_0 + c_1 \cdot 11)^2 \pmod{121}.$$

Hence, we must have that

$$(5 + c_1 \cdot 11)^2 \equiv 3 \pmod{121}.$$

By expanding the square, it follows that $25 + 10c_1 \cdot 11 \equiv 3 \pmod{121}$ and thus

$$22 + 10c_1 \cdot 11 \equiv 0 \pmod{121}.$$

Since all terms are multiples of 11, we can reduce the problem to $2 + 10c_1 \equiv 0 \pmod{11}$. This gives $c_1 \equiv 2 \pmod{11}$ since $10^{-1} \equiv 2 \pmod{11}$. We see that $5 + 2 \cdot 11$ in \mathbb{Z}_{11} is a solution to $F(X) \equiv 0 \pmod{11^2}$. Continuing with this procedure, we obtain that

$$\alpha \equiv 5 + 2 \cdot 11 + 6 \cdot 11^2 + 8 \cdot 11^3 \pmod{11^4}.$$

We could continue indefinitely with this method. Hensel's lemma assures us that this process uniquely determines α , given certain initial conditions.

One of the most basic forms of Hensel's lemma is given below, with the proof based on [Con15].

Theorem 4.21 (Hensel's lemma). *Let $F(X) \in \mathbb{Z}_p[X]$ and let $F'(X)$ denote the (formal) derivative of $F(X)$. Suppose that there exists an element a in \mathbb{Z}_p satisfying*

$$F(a) \equiv 0 \pmod{p} \quad \text{and} \quad F'(a) \not\equiv 0 \pmod{p}.$$

Then, there exists a unique p -adic integer α such that

$$F(\alpha) = 0 \quad \text{and} \quad \alpha \equiv a \pmod{p}.$$

Proof. We will construct a sequence $(\alpha_n)_{n \in \mathbb{N}}$ in \mathbb{Z}_p such that

$$F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}} \quad \text{and} \quad \alpha_{n+1} \equiv \alpha_n \pmod{p^n}, \tag{4.5}$$

for all positive integers n . First, we show that if for some $n \geq 1$ we have α_n satisfying the conditions above, then we can find α_{n+1} that fulfils the requirements. Let $\alpha_1 = a$. Now suppose α_n satisfies (4.5). For α_{n+1} to satisfy the second condition, we must have that $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$. Therefore, we can express α_{n+1} as

$$\alpha_{n+1} = \alpha_n + \beta_n p^n,$$

for some β_n in \mathbb{Z}_p that we will determine. Write

$$F(X) = \sum_{i=0}^d c_i X^i, \quad \text{with} \quad d := \deg(F).$$

Then, by writing out the first two terms of the binomial expansion of $(X + Y)^i$ in the third equality, we obtain that

$$\begin{aligned}
F(X + Y) &= \sum_{i=0}^d c_i (X + Y)^i \\
&= c_0 + \sum_{i=1}^d c_i (X + Y)^i \\
&= c_0 + \sum_{i=1}^d c_i (X^i + iX^{i-1}Y + G_i(X, Y)Y^2) \\
&\quad \text{where } G_i(X, Y) \in \mathbb{Z}_p[X, Y] \text{ for all } 1 \leq i \leq d \\
&= \sum_{i=0}^d c_i X^i + \left(\sum_{i=1}^d i c_i X^{i-1} \right) Y + G(X, Y) Y^2 \\
&\quad \text{where } G(X, Y) = \sum_{i=1}^d c_i G_i(X, Y) \in \mathbb{Z}_p[X, Y] \\
&= F(X) + F'(X)Y + G(X, Y)Y^2.
\end{aligned}$$

We get the identity

$$F(X + Y) = F(X) + F'(X)Y + G(X, Y)Y^2. \quad (4.6)$$

Clearly, $G(x, y)$ is in \mathbb{Z}_p for all p -adic integers x and y . Using the identity given above and the fact that $2n \geq n + 1$, we evaluate $F(X)$ at α_{n+1} :

$$\begin{aligned}
F(\alpha_{n+1}) &= F(\alpha_n + \beta_n p^n) \\
&= F(\alpha_n) + F'(\alpha_n)\beta_n p^n + G(\alpha_n, \beta_n p^n)\beta_n^2 p^{2n} \\
&\equiv F(\alpha_n) + F'(\alpha_n)\beta_n p^n \pmod{p^{n+1}}.
\end{aligned}$$

By the induction hypothesis, we have $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$ and thus, since $\alpha_{n-1} \equiv \alpha_{n-2} \pmod{p^{n-2}}$, it follows that $\alpha_n \equiv \alpha_{n-2} \pmod{p^{n-2}}$. By continuing this argument, we see that $\alpha_n \equiv a \pmod{p}$, since $\alpha_1 = a$. Therefore, since $F(X) \in \mathbb{Z}_p[X]$, we obtain $F'(\alpha_n) \equiv F'(a) \pmod{p}$. Equivalently, $F'(\alpha_n)p^n \equiv F'(a)p^n \pmod{p^{n+1}}$ and thus

$$F'(\alpha_n)\beta_n p^n \equiv F'(a)\beta_n p^n \pmod{p^{n+1}}.$$

Now we can find an explicit expression for β_n , since $F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}}$ precisely when $F(\alpha_n) + F'(\alpha_n)\beta_n p^n \equiv 0 \pmod{p^{n+1}}$. Rewriting this congruence gives us

$$\beta_n \equiv -\frac{F(\alpha_n)}{F'(a)p^n} \pmod{p}.$$

Notice that $F(\alpha_n)/p^n$ is in \mathbb{Z}_p and $F'(a)$ is invertible since $F(\alpha_n) \equiv 0 \pmod{p^n}$ and $\gcd(F'(a), p) = 1$, respectively, by assumption. This choice for β_n gives us

$$F(\alpha_{n+1}) \equiv 0 \pmod{p^{n+1}} \quad \text{and} \quad \alpha_{n+1} \equiv \alpha_n \pmod{p^n}.$$

Thus, by induction, we have formed a sequence $(\alpha_n)_{n \in \mathbb{N}}$ that satisfies the conditions given in (4.5).

Since $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ for all positive integers n , this sequence is Cauchy in \mathbb{Z}_p . Take α to be its limit, which is in \mathbb{Z}_p since

$$|\alpha|_p = |\alpha - \alpha_n + \alpha_n|_p \leq \max\{|\alpha - \alpha_n|_p, |\alpha_n|_p\} \leq 1.$$

It remains to show that α is the unique element in \mathbb{Z}_p that satisfies

$$F(\alpha) = 0 \quad \text{and} \quad \alpha \equiv a \pmod{p}.$$

Note that $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$ for all n implies $\alpha_m \equiv \alpha_n \pmod{p^n}$ for all $m \geq n$. If we consider $n = 1$, then we obtain $\alpha \equiv a \pmod{p}$ since α is the limit of the sequence $(\alpha_n)_{n \in \mathbb{N}}$. Now, let $\varepsilon > 0$. Choose n in \mathbb{N} such that $1/p^n < \varepsilon$. Then $\alpha \equiv \alpha_n \pmod{p^n}$ implies $F(\alpha) \equiv 0 \pmod{p^n}$, since $F(\alpha_n) \equiv 0 \pmod{p^n}$. Thus

$$|F(\alpha)|_p \leq 1/p^n < \varepsilon.$$

Since ε was arbitrary, this gives $F(\alpha) = 0$ as desired. To show that α is unique, suppose that α' in \mathbb{Z}_p satisfies $F(\alpha') = 0$ and $\alpha' \equiv a \pmod{p}$. We will show by induction that $\alpha' \equiv \alpha \pmod{p^n}$ for all n in \mathbb{N} ; this will give $\alpha' = \alpha$. For $n = 1$, this holds by assumption, since both are congruent to a modulo p . Now suppose the congruence holds for some n . Write $\alpha' = \alpha + p^n \gamma_n$ for some p -adic integer γ_n . By a similar argument as before, using the identity given in (4.6), we get

$$F(\alpha') \equiv F(\alpha) + F'(\alpha)p^n \gamma_n \pmod{p^{n+1}}.$$

Recalling that α and α' are both roots of the polynomial, we see that $F'(\alpha)\gamma_n \equiv 0 \pmod{p}$ and therefore $\gamma_n \equiv 0 \pmod{p}$, since $F'(\alpha) \equiv F'(a) \not\equiv 0 \pmod{p}$. This gives $\alpha' \equiv \alpha \pmod{p^{n+1}}$ and therefore $\alpha' = \alpha$. This completes the proof. \square

Remark. Note that if Hensel's lemma gives us a root α in \mathbb{Z}_p of $F(X) = f(X^2)$ for some polynomial f in $\mathbb{Z}_p[X]$, it does not state that it is the only p -adic integer that is a root of F . Clearly, $-\alpha$ in \mathbb{Z}_p is a root as well. It only says that α is the unique root corresponding to a (i.e., $\alpha \equiv a \pmod{p}$).

Remark. There are many different versions of Hensel's lemma. For example, it could also be stated in the formulation given below (from [Con15, Theorem 4.1]).

Let $F(X) \in \mathbb{Z}_p[X]$ and a in \mathbb{Z}_p satisfy

$$|F(a)|_p < |F'(a)|_p^2.$$

Then, there is a unique p -adic integer α such that

$$F(\alpha) = 0 \quad \text{and} \quad |\alpha - a|_p < |F'(a)|_p.$$

Moreover,

$$|\alpha - a|_p = |F(a)/F'(a)|_p < |F'(a)|_p \quad \text{and} \quad |F'(\alpha)|_p = |F'(a)|_p.$$

Although the version of Hensel's lemma in Theorem 4.21 is more elementary than the statement above, it does the job for us. In fact, it does not really matter which version you use; it can be shown that both formulations are equivalent (see [Con15, Theorem 5.4]).

As can be deduced from the discussion at the start of this subsection, Hensel's lemma bears a close resemblance to Newton's method for approximating real roots of a polynomial defined over \mathbb{R} . In the proof, α_{n+1} was computed by expressing it as $\alpha_n + \beta_n p^n$, where $\beta_n \equiv -F(\alpha_n)/(F'(a)p^n) \pmod{p}$. Now, set $\beta_n = -F(\alpha_n)/(F'(a)p^n)$. This gives

$$\alpha_{n+1} = \alpha_n - F(\alpha_n)/F'(a). \tag{4.7}$$

This is similar to the general formula of Newton's method, which states that

$$x_{n+1} = x_n - F(x_n)/F'(x_n), \tag{4.8}$$

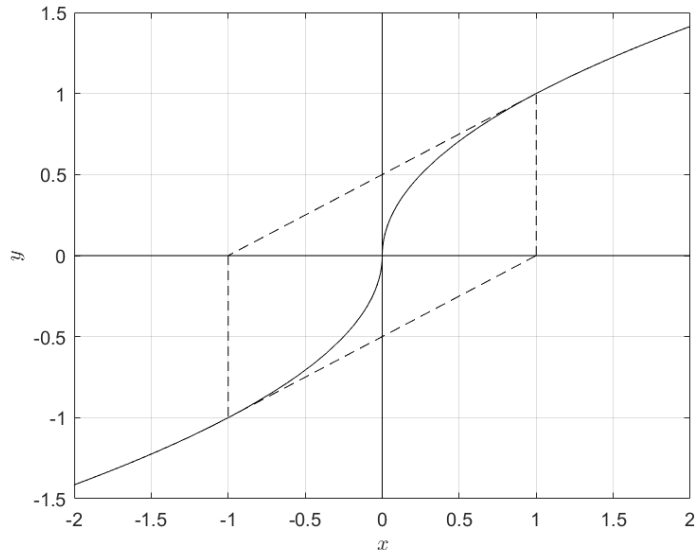


Figure 6: Plot of the function $y(x) = \operatorname{sgn}(x)\sqrt{|x|}$. An initial guess for x_0 of 1 or -1 will not make Newton's method converge.

where x_0 is an initial guess. Note that the denominator in (4.7) is constant, whereas the denominator in (4.8) changes with respect to the new approximation, resulting in a different rate of convergence [Con15, Section 6]. A quick comparison yields a few more differences between the two. For example, in the proof of Hensel's lemma, we showed that the method never leaves \mathbb{Z}_p . In Newton's method, a sequence starting with an integer as the first approximation does not have to stay in \mathbb{Z} . Moreover, the approximation in Hensel's lemma always works; that is, the sequence always converges. This is not necessarily true in the case of Newton's method, where scenarios like in Figure 6 can occur. Lastly, Hensel's lemma gives a bit more information on the distance between the initial 'estimate' and the actual root α . Namely, it says that $|\alpha - a|_p \leq 1/p$.

Although the formal description will be given in Section 5.2, we can look at an example of how Hensel's lemma can be applied to obtain 'lifts' of elliptic curves and points on it. This will be needed in Smart's algorithm, which is explained in Section 6. The notation in the example is used in order to keep consistency with the notation used in the coming sections.

Example 4.22. Consider the elliptic curve $\tilde{E}: y^2 = x^3 + 2x + 3$ defined over \mathbb{F}_7 and the point $\tilde{P} = (3, 1)$ in $\tilde{E}(\mathbb{F}_7)$. Since the integers are contained in \mathbb{Z}_7 , we can lift \tilde{E} in the obvious way to an elliptic curve E defined over \mathbb{Z}_7 . Namely, let $E: y^2 = x^3 + 2x + 3$. In order to lift \tilde{P} to a point P in $E(\mathbb{Q}_7)$, we use Hensel's lemma. Let the x -coordinate of P be equal to 3 and define the polynomial

$$F(Y) := Y^2 - 36 = Y^2 - 3^3 - 2 \cdot 3 - 3,$$

which is in $\mathbb{Z}_7[Y]$. To find the y -coordinate, we need to find α in \mathbb{Z}_7 such that $F(\alpha) = 0$. Clearly, the values for α are 6 and -6 . So in this case, it is not necessary to apply Hensel's lemma, but to show that the method works, we do it anyway.

In our case, we have that $\alpha \equiv 1 \pmod{7}$, therefore Hensel's lemma will give us an expression for -6 in \mathbb{Z}_7 . By construction, we know that $F(1) \equiv 0 \pmod{7}$. Moreover, we have that $F'(1) = 2 \not\equiv 0 \pmod{7}$. Hensel's lemma now assures us that α exists and we can use the method given in the proof to compute it. Since $F'(1)^{-1} = 2^{-1} \equiv 4 \pmod{7}$,

we have that

$$\begin{aligned} \alpha_2 &\equiv \alpha_1 - F(\alpha_1)/F'(a) \pmod{7^2} & \alpha_3 &\equiv \alpha_2 - F(\alpha_2)/F'(a) \pmod{7^3} \\ &\equiv 1 - (-35) \cdot 4 \pmod{7^2} & &\equiv 1 + 6 \cdot 7 - (1813) \cdot 4 \pmod{7^3} \\ &\equiv 1 + 6 \cdot 7 \pmod{7^2}, & &\equiv 1 + 6 \cdot 7 + 6 \cdot 7^2 \pmod{7^3}. \end{aligned}$$

By computing a few more terms, we find that the expression for -6 in \mathbb{Z}_7 is given by

$$1 + 6 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + 6 \cdot 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + \dots$$

From this expression, one could already see that it must be an element of \mathbb{Q} . This follows from the fact that it is eventually periodic, and any p -adic number with an (eventually) periodic expansion represents a rational number (and vice versa). Note the analogy to the real numbers, where the (eventually) periodic real numbers are precisely the rational numbers.

The example showed how to compute the additive inverse of an element in \mathbb{Z}_p . In general, we have that for an element x in \mathbb{Q}_p given by

$$\alpha_{n_0}p^{n_0} + \alpha_{n_0+1}p^{n_0+1} + \dots + \alpha_0 + \alpha_1p + \alpha_2p^2 + \dots,$$

its additive inverse is equal to

$$(p - \alpha_{n_0})p^{n_0} + (p - \alpha_{n_0+1} - 1)p^{n_0+1} + (p - \alpha_{n_0+2} - 1)p^{n_0+2} + \dots$$

In Section 6, we will see that if we really require Hensel's lemma to obtain lifts, we do not need to compute many terms of the p -adic expansion.

If $p = 2$, Hensel's lemma does not assure the existence of a solution in \mathbb{Z}_2 to $F(Y) = 0$ in the previous example. The reason is that the derivative of F is identically zero modulo 2. This does not mean that we can never lift solutions modulo 2^n to solutions modulo 2^{n+1} , it just depends on the specific case that is considered, as the following example illustrates.

Example 4.23. Consider $F(X) = X^2 + 1$ in $\mathbb{Z}_2[X]$. We see that $F(1) \equiv 0 \pmod{2}$ and $F'(1) \equiv 0 \pmod{2}$. Note that $F(1) \not\equiv 0 \pmod{4}$ and $F(3) \not\equiv 0 \pmod{4}$. Therefore, we conclude that it does not lift to a root in \mathbb{Z}_2 ; if α in \mathbb{Z}_2 were such a root, then $\alpha \equiv 1 \pmod{2}$ and thus $\alpha \equiv 1 \pmod{4}$ or $\alpha \equiv 3 \pmod{4}$. However, we checked that neither of these is a root of $F(X)$ modulo 4.

On the other hand, take $F(X) = X^2 - 33$ in $\mathbb{Z}_2[X]$. Then $F(1) \equiv 0 \pmod{2}$ and $F'(1) \equiv 0 \pmod{2}$. Both $F(1) \equiv 0 \pmod{4}$ and $F(3) \equiv 0 \pmod{4}$. Moreover, it can be shown that the number of solutions modulo 2^n for $n \geq 3$ equals 4, which follows from the fact that $33 \equiv 1 \pmod{8}$ (cf. [Kos07, Theorem 11.15]).

In order to enable the use of Hensel's lemma for lifting points on an elliptic curve when the derivative of the quadratic polynomial vanishes modulo p , we can fix the y -coordinate instead and apply the lemma to the cubic equation to obtain the x -coordinate.

The next section looks at the formal group and the formal logarithm of an elliptic curve over the p -adic numbers. Moreover, we consider the reduction modulo p of an elliptic curve over \mathbb{Z}_p and its points.

5 The formal group of an elliptic curve over the field \mathbb{Q}_p

The idea of this section is to describe the group law of an elliptic curve over \mathbb{Q}_p in a 'small neighbourhood' around the identity \mathcal{O} . We will see that the so-called *formal group law* we

obtain helps us when we consider the reduction modulo p of elliptic curves over \mathbb{Z}_p and its points. In addition to this, the formal group law induces a *formal logarithm*, which is an explicit isomorphism that plays a key part in constructing a *p-adic elliptic logarithm* for Smart's attack.

For this section, we generalise a bit and recall the general Weierstrass form for E , which was given by

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (5.1)$$

where a_1, a_2, a_3, a_4, a_6 are in \mathbb{Z}_p . The results in this section are mainly from [Sil09, Sections IV, VII.2].

5.1 The construction of the formal group

Our first task is to find an expression to represent points on E in one parameter in \mathbb{Q}_p around the point \mathcal{O} . To this end, we first put the identity \mathcal{O} at the origin. In order to do so, we consider E as curve in the projective plane, just like we did in Section 2. The homogenisation gives us

$$E: y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Instead of assuming z is nonzero like we usually do to obtain (5.1), we now take y to be nonzero and thus we move the points at infinity. The obvious reason for this is that if we want to talk about the neighbourhood around the identity, it should contain the identity; hence we should not take x or z nonzero since $\mathcal{O} = (0 : 1 : 0)$. Thus, we consider the points $(-x/y : -1 : -z/y)$ (the minus is for notation) and it follows that

$$\begin{aligned} E: \frac{-z}{y} - a_1 \frac{-x}{y} \cdot \frac{-z}{y} - a_3 \left(\frac{-z}{y} \right)^2 &= \left(\frac{-x}{y} \right)^3 + a_2 \left(\frac{-x}{y} \right)^2 \cdot \frac{-z}{y} \\ &\quad + a_4 \frac{-x}{y} \cdot \left(\frac{-z}{y} \right)^2 + a_6 \left(\frac{-z}{y} \right)^3. \end{aligned}$$

We apply the change of variables

$$u = -\frac{x}{y} \quad \text{and} \quad v = -\frac{z}{y},$$

which gives us

$$E: v = u^3 + a_1uv + a_2u^2v + a_3v^2 + a_4uv^2 + a_6v^3.$$

The point \mathcal{O} is now at the origin in the (u, v) -plane. We define

$$f(u, v) := u^3 + a_1uv + a_2u^2v + a_3v^2 + a_4uv^2 + a_6v^3.$$

The equation for E now becomes $v = f(u, v)$. To obtain an expression for v in terms of u , we first collect terms involving powers of v and then recursively substitute the expression into itself, as is done below:

$$\begin{aligned} v &= u^3 + u(a_1 + a_2u)v + (a_3 + a_4u)v^2 + a_6v^3 \\ &= u^3 + u(a_1 + a_2u)(u^3 + u(a_1 + a_2u)v + (a_3 + a_4u)v^2 + a_6v^3) \\ &\quad + (a_3 + a_4u)(u^3 + u(a_1 + a_2u)v + (a_3 + a_4u)v^2 + a_6v^3)^2 \\ &\quad + a_6(u^3 + u(a_1 + a_2u)v + (a_3 + a_4u)v^2 + a_6v^3)^3 \\ &\quad \vdots \\ &= u^3 + a_1u^4 + (a_1^2 + a_2)u^5 + (a_1^3 + 2a_1a_2 + a_3)u^6 + \dots \\ &= u^3(1 + A_1u + A_2u^2 + A_3u^3 + \dots), \end{aligned}$$

where $A_n \in \mathbb{Z}_p$. Using the recursive approach above, we would like to obtain an expression $v(u) \in \mathbb{Z}_p[[u]]$, where $v(u) = f(u, v(u))$. Here, $\mathbb{Z}_p[[u]]$ denotes the ring of formal power series in u with coefficients in \mathbb{Z}_p . The fact that this approach actually gives a formal power series $v(u)$ with $v(u) = f(u, v(u))$ follows from a more general version of Hensel's lemma for rings that are complete with respect to some ideal (analogous to \mathbb{Z}_p , which is complete with respect to the ideal $p\mathbb{Z}_p$). This general version, however, does not require the notion of an absolute value. It is given in [Sil09, Section IV.1, Lemma 1.2] and the proof is similar to that of Theorem 4.21. The formal power series for $v(u)$ thus follows from the recursive substitution we did above, so we have

$$v(u) = u^3(1 + A_1u + A_2u^2 + A_3u^3 + \dots). \quad (5.2)$$

By recalling our change of variables, we obtain the following series for x and y :

$$\begin{aligned} x(u) &= \frac{u}{v(u)} = \frac{1}{u^2} - \frac{a_1}{u} - a_2 - a_3u - (a_4 + a_1a_3)u^2 - \dots, \\ y(u) &= -\frac{1}{v(u)} = -\frac{1}{u^3} + \frac{a_1}{u^2} + \frac{a_2}{u} + a_3 + (a_4 + a_1a_3)u - \dots. \end{aligned} \quad (5.3)$$

Clearly, both $x(u)$ and $y(u)$ have coefficients in \mathbb{Z}_p . If we substitute $x(u)$ and $y(u)$ into both sides of (5.1), then we obtain the same series on both sides. Note that the parameter u can describe points on the curve E only when the series $x(u)$ and $y(u)$ converge. This is the case when $u \in p\mathbb{Z}_p$. To see this, recall that the infinite sum $x(u)$ converges if the sequence of its partial sums converges. Since \mathbb{Q}_p is complete, convergence is assured when the sequence is Cauchy. In Lemma 4.9, we proved that a sequence is Cauchy if the difference between consecutive terms converges to 0 (this also holds in \mathbb{Q}_p , since the absolute value extends from \mathbb{Q} to \mathbb{Q}_p). Note that for every u in $p\mathbb{Z}_p$ and every a in \mathbb{Z}_p , we have $|a|_p|u|_p^n \leq p^{-n}$ for all positive integers n . If we consider the expression for $x(u)$, observe that the difference between two consecutive elements in the sequence of partial sums is just one term in the expression. For every $\epsilon > 0$ we can find an N in \mathbb{N} such that

$$|B_n \cdot u^n|_p = |B_n|_p|u|_p^n \leq p^{-n} \leq p^{-N} < \epsilon,$$

for all $n \geq N$, where B_n corresponds to the coefficient in front of u^n in $x(u)$. This proves that the sequence of partial sums is Cauchy and therefore $x(u)$ converges in \mathbb{Q}_p . Similarly, $y(u)$ converges and hence we obtain the map

$$p\mathbb{Z}_p \rightarrow E(\mathbb{Q}_p), \quad u \mapsto (x(u), y(u)).$$

This map is an injection, since we can find an inverse on its image:

$$(x(u), y(u)) \mapsto -x(u)/y(u).$$

We will now look at the construction of the formal group law of an elliptic curve E given in the generalised Weierstrass form. This will be done in a similar fashion as for the usual addition law. First, take points $(u_1, v_1), (u_2, v_2)$ where $v_i = v(u_i)$, $i = 1, 2$ on E . Recall that $v(u) = f(u, v(u)) \in \mathbb{Z}_p[[u]]$. We construct the 'line' $v = \lambda u + \gamma$ in the (u, v) -plane going through both points. First we compute the λ , for which we have

$$\begin{aligned} \lambda = \lambda(u_1, u_2) &= \frac{v(u_1) - v(u_2)}{u_2 - u_1} \\ &= \frac{v_2 - v_1}{u_2 - u_1} \\ &= \frac{u_2^3(1 + A_1u_2 + A_2u_2^2 + \dots) - u_1^3(1 + A_1u_1 + A_2u_1^2 + \dots)}{u_2 - u_1} \\ &= \sum_{n=3}^{\infty} A_{n-3} \frac{u_2^n - u_1^n}{u_2 - u_1}, \quad \text{where } A_0 = 1. \end{aligned}$$

Note that $\lambda \in \mathbb{Z}_p[[u_1, u_2]]$ and this expression also holds when $u_1 = u_2$ since $u_2 - u_1$ divides $u_2^n - u_1^n$ for all $n \geq 1$. Now we have that

$$v = \lambda u + \gamma, \quad \text{with} \quad \gamma = v(u_1, u_2) = v_2 - \lambda u_2.$$

Substituting this into the equation $v = f(u, v)$ gives us $\lambda u + \gamma = f(u, \lambda u + \gamma)$. From this, the following equation can be derived:

$$u^3 + a_1 u(\lambda u + \gamma) + a_2 u^2(\lambda u + \gamma) + a_3(\lambda u + \gamma)^2 + a_4 u(\lambda u + \gamma)^2 + a_6(\lambda u + \gamma)^3 - (\lambda u + \gamma) = 0.$$

Since the coefficient in front of the quadratic term in a monic cubic polynomial equals $-(u_1 + u_2 + u_3)$ where u_1, u_2 and u_3 are the roots, we expand the squares to obtain

$$(1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3)u^3 + (a_1 \lambda + a_2 \gamma + a_3 \lambda^2 + 2a_4 \lambda \gamma + 3a_6 \lambda^2 \gamma)u^2 + \dots$$

The fact that u_1, u_2 are two known roots yields the third, given by

$$u_3 = -u_1 - u_2 - \frac{a_1 \lambda + a_2 \gamma + a_3 \lambda^2 + 2a_4 \lambda \gamma + 3a_6 \lambda^2 \gamma}{1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3}.$$

Since λ has no constant term, the power series in the denominator has constant term 1, which is invertible in \mathbb{Z}_p , hence the denominator is invertible in $\mathbb{Z}_p[[u_1, u_2]]$ (for a proof, see [BG08]). Therefore, we also have that $u_3(u_1, u_2) \in \mathbb{Z}_p[[u_1, u_2]]$. SageMath [Sag20] confirms our reasoning and we obtain

$$u_3 = -u_1 - u_2 - a_1 u_1^2 - a_1 u_1 u_2 - a_1 u_2^2 - a_1^2 u_1^3 + (-a_1^2 + a_2)u_1^2 u_2 + \dots$$

Using this, we can compute v_3 by filling in u_3 in the equation of the line:

$$v_3 = v(u_3) = v(u_1, u_2) = \lambda(u_1, u_2)u_3(u_1, u_2) + v(u_1, u_2).$$

Note that the points (u_i, v_i) for $i = 1, 2, 3$ are collinear, resulting in \mathcal{O} when adding them. Thus, u_3 is the u -coordinate of $\ominus((u_1, v_1) \oplus (u_2, v_2))$. In general, the inverse of a point (x, y) on E is given by $(x, -y - a_1 x - a_3)$. Let $i_E(u)$ denote the u -coordinate of the inverse of the point (u, v) . Since $u = -x/y$, we obtain

$$\begin{aligned} i_E(u) &= -\frac{x(u)}{-y(u) - a_1 x(u) - a_3} \\ &= \frac{x(u)}{y(u) + a_1 x(u) + a_3} \\ &= -u - a_1 u^2 - a_1^2 u^3 + (-a_1^3 - a_3)u^4 + (-a_1^4 - 3a_1 a_3)u^5 + \dots \\ &\in \mathbb{Z}_p[[u]]. \end{aligned}$$

We now define $F_E(u_1, u_2) := i_E(u_3(u_1, u_2))$. The first few terms of F_E are given by

$$F_E(u_1, u_2) = u_1 + u_2 - a_1 u_1 u_2 - a_2 (u_1^2 u_2 + u_1 u_2^2) - \dots \quad (5.4)$$

One can show, due to properties of the addition law \oplus on the points of an elliptic curve, that F_E satisfies the properties of a formal group law and therefore, forms a formal group over \mathbb{Z}_p . This means that $F_E(X, Y)$ is a formal power series in two variables over the ring \mathbb{Z}_p , satisfying

- (i) $F_E(X, Y) = X + Y +$ terms of higher degree,
- (ii) $F_E(F_E(X, Y), Z) = F_E(X, F_E(Y, Z))$,
- (iii) $F_E(X, Y) = F_E(Y, X)$,
- (iv) $F_E(T, i_E(T)) = 0$ for some unique power series $i_E(T) \in \mathbb{Z}_p[[T]]$,
- (v) $F_E(X, 0) = X$ and $F_E(0, Y) = Y$,

The formal group can be seen as solely a group operation without an underlying group

set. We know that for elements in $p\mathbb{Z}_p$, which have absolute value less than 1, the power series F_E converges. Therefore, we can look at the sets $p^n\mathbb{Z}_p$, for $n \geq 1$, endowed with the group law F_E . Due to the properties of F_E , these sets form groups. This leads to the proposition below.

Proposition 5.1. *Let E be an elliptic curve over \mathbb{Q}_p and let n be a positive integer. The tuple $(p^n\mathbb{Z}_p, \oplus_{F_E}, 0)$ forms an abelian group, denoted by $\hat{E}(p^n\mathbb{Z}_p)$, where for all x, y in $p^n\mathbb{Z}_p$,*

$$x \oplus_{F_E} y := F_E(x, y).$$

The inverse is denoted by \ominus_{F_E} and is defined as $\ominus_{F_E} x := i_E(x)$ for all x in $p^n\mathbb{Z}_p$.

5.2 The reduction of elliptic curves modulo p

Recall from Section 4.3 that \mathbb{Z}_p is a local ring with maximal ideal $p\mathbb{Z}_p$. Hence, we can consider the *residue field* $\mathbb{Z}_p/p\mathbb{Z}_p$, which has p elements and hence is isomorphic to \mathbb{F}_p . We consider the map from \mathbb{Z}_p to \mathbb{F}_p , given by

$$\begin{aligned} \text{red}: \mathbb{Z}_p &\rightarrow \mathbb{F}_p, \\ \sum_{i=0}^{\infty} \alpha_i p^i &\mapsto \alpha_0. \end{aligned}$$

Let E be an elliptic curve over \mathbb{Q}_p in generalised Weierstrass form with coefficients a_1, a_2, a_3, a_4 and a_6 in \mathbb{Z}_p . Define $\tilde{a}_i := \text{red}(a_i)$. Denote the reduced curve over \mathbb{F}_p with coefficients \tilde{a}_i by \tilde{E} . Note that this curve can be singular, which is the case when the discriminant of the elliptic curve has positive valuation, that is, it is 0 modulo p (see [Sil09, Section VII.5]). However, for our purposes, we do not consider this scenario; we always assume to have good reduction. Just like the curve E , a point P in $E(\mathbb{Q}_p)$ can be reduced to a point \tilde{P} in $\tilde{E}(\mathbb{F}_p)$. Let $P \in \mathbb{P}^2(\mathbb{Q}_p)$ and write $P = (x : y : z)$, where we can assume x, y and z are in \mathbb{Z}_p , not all zero. Then the point \tilde{P} is given by $(\tilde{x} : \tilde{y} : \tilde{z}) := (\text{red}(x) : \text{red}(y) : \text{red}(z))$. This point is on the reduced curve \tilde{E} . Using the same notation as above, we obtain the following definition of the *reduction map*.

Definition 5.2. The *reduction modulo p map* is defined as the surjective group homomorphism

$$\begin{aligned} \pi: E(\mathbb{Q}_p) &\rightarrow \tilde{E}(\mathbb{F}_p), \\ P &\mapsto \tilde{P}. \end{aligned}$$

Remark. It requires some substantial work to show that this map is indeed a surjective group homomorphism (see [Sil09, Section VII.2, Proposition 2.1]). This property will be useful later on.

The curve E over \mathbb{Q}_p and a point P in $E(\mathbb{Q}_p)$ are called lifts of a curve E' over \mathbb{F}_p and P' in $E'(\mathbb{F}_p)$, respectively, if $\tilde{E} = E'$ and $\tilde{P} = P'$.

Example 5.3. Consider $E: y^2 = x^3 + 2x + 3$ over \mathbb{Q}_{19} and the point P in $E(\mathbb{Q}_{19})$ given by the homogeneous coordinates

$$\left(10 + 12 \cdot 19 + 7 \cdot 19^2 + O(19^3) : 4 + 6 \cdot 19 + 9 \cdot 19^2 + O(19^3) : 1 + O(19^3)\right),$$

³Due to the fact that any p -adic number has only finitely many negative powers of p in its expansion (cf. Corollary 4.19), this can be done by multiplying the equation by a sufficiently large power of p . Therefore, we assume this is always the case.

where $O(19^3)$ means the approximation is correct up to and including the term with 19^2 . The reduced curve \tilde{E} in \mathbb{F}_{19} has the same coefficients. We have that \tilde{P} equals $(10 : 4 : 1)$, i.e. the point $(10, 4)$ in affine coordinates. It follows that $\tilde{P} \in \tilde{E}(\mathbb{F}_{19})$ since

$$10^3 + 2 \cdot 10 + 3 = 1023 \equiv 16, \quad 4^2 \equiv 16 \pmod{19}.$$

Definition 5.4. Let E be an elliptic curve defined over \mathbb{Q}_p with coefficients in \mathbb{Z}_p . Define

$$E_n(\mathbb{Q}_p) := \{(x, y) \in E(\mathbb{Q}_p) : \nu_p(x) \leq -2n, \nu_p(y) \leq -3n\} \cup \{\mathcal{O}\},$$

for all positive integers n .

Remark. Note that we have the inclusions

$$E(\mathbb{Q}_p) \supseteq E_1(\mathbb{Q}_p) \supseteq E_2(\mathbb{Q}_p) \supseteq \dots$$

For every positive integer n , we add \mathcal{O} to $E_n(\mathbb{Q}_p)$ and, by doing this, it forms a subgroup of $E(\mathbb{Q}_p)$. This can be shown by moving \mathcal{O} to the origin using a similar change of variables as discussed in Section 5 and writing down the formulas for the addition law [ST92, Section 2.4].

Example 5.5. Consider $E: y^2 = x^3 - 4x + 4$ over \mathbb{Q}_3 and the point $P = (10/9, 26/27)$ in $E(\mathbb{Q}_3)$. Representing P with homogeneous coordinates in their 3-adic expansion gives

$$P = \left(3^{-2} + 1 : 2 \cdot 3^{-3} + 2 \cdot 3^{-2} + 2 \cdot 3^{-1} : 1\right).$$

Note that $\nu_p(10/9) = -2$ and $\nu_p(26/27) = -3$, hence $P \in E_1(\mathbb{Q}_3)$. We can multiply the coordinates of P by 3^3 to obtain homogeneous coordinates that are p -adic integers:

$$P = \left(3 + 3^3 : 2 + 2 \cdot 3 + 2 \cdot 3^2 : 3^3\right).$$

Hence we have that $\tilde{P} = (0 : 1 : 0)$.

It is no coincidence that the point in the preceding example reduces modulo p to \mathcal{O} . In fact, it can be shown that the elements of $E_n(\mathbb{Q}_p)$ are precisely the points that reduce modulo p^n to the identity. To establish this result, the following lemma will be helpful.

Lemma 5.6. *Let E be an elliptic curve defined over \mathbb{Q}_p . If a point $P = (x, y)$ in $E(\mathbb{Q}_p)$ satisfies $\nu_p(x) < 0$, then $2\nu_p(y) = 3\nu_p(x)$.*

Proof. See [Win11, Lemma 3.1.3]. □

Remark. It follows from the lemma that the condition on the y -coordinate in Definition 5.4 is redundant.

Now, let n be a positive integer and let $P = (x, y) \in E_n(\mathbb{Q}_p)$. Since $\nu_p(x) < 0$, it follows from Lemma 5.6 that $2\nu_p(y) = 3\nu_p(x)$. Therefore, since ν_p maps to the integers, we have $\nu_p(x) = -2r$ and $\nu_p(y) = -3r$ for some integer $r \geq n$. Observe that $|y|_p x \in p^r \mathbb{Z}_p$ and $|y|_p y \in \mathbb{Z}_p^\times$. Hence, p^n divides $|y|_p x$ and $|y|_p$, but not $|y|_p y$. Write $P = (x : y : 1)$, so that $P = (|y|_p x : |y|_p y : |y|_p)$ and $\tilde{P} = (0 : 1 : 0)$. Thus, we have shown that every point in $E_n(\mathbb{Q}_p)$ reduces modulo p^n to \mathcal{O} . On the other hand, assume that $P = (x : y : 1)$ in $E(\mathbb{Q}_p)$ reduces modulo p^n to \mathcal{O} . In this case, observe that $\nu_p(y) < 0$. The elliptic curve E is given by

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

Suppose that $\nu_p(x) \geq 0$. Since all coefficients are p -adic integers, the expression on the right-hand side clearly has nonnegative valuation. For the left-hand side, note that

$$\begin{aligned}\nu_p(y^2 + a_1xy + a_3y) &= \min\{2\nu_p(y), \nu_p((a_1x + a_3)y)\} \\ &= \min\{2\nu_p(y), \nu_p(a_1x + a_3) + \nu_p(y)\} \\ &= 2\nu_p(y) < 0.\end{aligned}$$

Since the valuations of both expressions must be equal, this gives a contradiction. Therefore, $\nu_p(x) < 0$. Consequently, we can apply Lemma 5.6 to obtain $\nu_p(x) = -2r$ and $\nu_p(y) = -3r$, for some positive integer r . Since P reduces modulo p^n to \mathcal{O} , we must have that $\nu_p(x) - \nu_p(y) \geq n$. Hence, we obtain $r \geq n$ and therefore $P \in E_n(\mathbb{Q}_p)$. This shows that the elements of $E_n(\mathbb{Q}_p)$ are precisely the points that reduce modulo p^n to the identity. As a result, we have that $\ker(\pi) = E_1(\mathbb{Q}_p)$, which will be needed in the following proposition.

Proposition 5.7. *Let E be an elliptic curve over \mathbb{Q}_p . Then*

$$E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \tilde{E}(\mathbb{F}_p).$$

Proof. We have shown that $\ker(\pi) = E_1(\mathbb{Q}_p)$. The fact that π is a surjective group homomorphism now gives us the desired result by applying the homomorphism theorem for groups. \square

The following proposition gives an explicit isomorphism between $E_n(\mathbb{Q}_p)$ and $\hat{E}(p^n\mathbb{Z}_p)$, the group induced by the formal group. For later purposes, we only need this result for n equal to 1 and 2. However, the proof remains exactly the same when we let n be any positive integer.

Proposition 5.8. *Let E be an elliptic curve defined over \mathbb{Q}_p . For every positive integer n , the map*

$$\begin{aligned}\vartheta: E_n(\mathbb{Q}_p) &\rightarrow \hat{E}(p^n\mathbb{Z}_p), \\ (x, y) &\mapsto -x/y, \\ \mathcal{O} &\mapsto 0,\end{aligned}$$

is a group isomorphism.

Proof. Let n be a positive integer. We first show that ϑ indeed maps to $\hat{E}(p^n\mathbb{Z}_p)$. Let (x, y) be in $E_n(\mathbb{Q}_p)$, so that $\nu_p(x) < 0$. From Lemma 5.6, we have that $2\nu_p(y) = 3\nu_p(x)$, hence

$$2\nu_p(-x/y) = 2\nu_p(x) - 2\nu_p(y) = -\nu_p(x) > 2n,$$

so that $\nu_p(-x/y) > n$ and thus $-x/y \in p^n\mathbb{Z}_p$. To prove that ϑ is a homomorphism, take $(x, y), (x', y')$ in $E_n(\mathbb{Q}_p) \setminus \{\mathcal{O}\}$. Assume first that the points are not inverses of each other. Since $\nu_p(y) < 0$ and $\nu_p(y') < 0$, we have that y and y' are nonzero. Recall from (5.3) that we can write

$$(x, y) = \left(\frac{u}{v(u)}, -\frac{1}{v(u)} \right) \quad \text{and} \quad (x', y') = \left(\frac{u'}{v(u')}, -\frac{1}{v(u')} \right),$$

where $u = -x/y$ and $u' = -x'/y'$. By the construction of the formal power series F_E , adding these points gives

$$\left(\frac{F_E(u, u')}{v(F_E(u, u'))}, -\frac{1}{v(F_E(u, u'))} \right)$$

in $E_n(\mathbb{Q}_p)$. We obtain

$$\begin{aligned}
\vartheta((x, y) \oplus (x', y')) &= \vartheta\left(\left(\frac{u}{v(u)}, -\frac{1}{v(u)}\right) \oplus \left(\frac{u'}{v(u')}, -\frac{1}{v(u')}\right)\right) \\
&= \vartheta\left(\frac{F_E(u, u')}{v(F_E(u, u'))}, -\frac{1}{v(F_E(u, u'))}\right) \\
&= F_E(u, u') \\
&= u \oplus_{F_E} u' \\
&= \vartheta(x, y) \oplus_{F_E} \vartheta(x', y').
\end{aligned}$$

Observe that ϑ also preserves inverses; if we have points (x, y) and $\ominus(x, y) = (x', y')$ in $E_n(\mathbb{Q}_p)$ with $u = -x/y$ and $u' = -x'/y'$, then

$$\vartheta((x, y) \oplus (\ominus(x, y))) = 0 = F_E(u, i_E(u)) = F_E(u, u') = \vartheta(x, y) \oplus_{F_E} \vartheta(x', y').$$

If one of the points is trivial, then ϑ straightforwardly satisfies the required properties. We conclude that ϑ is a group homomorphism. To show that it is an isomorphism, consider the map

$$\begin{aligned}
\varphi: \hat{E}(p^n\mathbb{Z}_p) &\rightarrow E_n(\mathbb{Q}_p), \\
u &\mapsto \left(\frac{u}{v(u)}, -\frac{1}{v(u)}\right), \\
0 &\mapsto \mathcal{O}.
\end{aligned}$$

From Section 5, we know that the pair $(u/v(u), -1/v(u))$ satisfies the equation of E . If $u \in p^n\mathbb{Z}_p \subseteq p\mathbb{Z}_p$, then we saw that the series $x(u)$ and $y(u)$ converge and therefore $(u/v(u), -1/v(u)) \in E(\mathbb{Q}_p)$. Moreover, from the formulas in (5.3) it follows that

$$\nu_p(u/v(u)) = -2\nu_p(u) \leq -2n \quad \text{and} \quad \nu_p(-1/v(u)) = -3\nu_p(u) \leq -3n$$

since $u \in p^n\mathbb{Z}_p$. Thus $(u/v(u), -1/v(u)) \in E_n(\mathbb{Q}_p)$.

Note that since $(x, y) = (u/v(u), -1/v(u))$, $u = -x/y$ and we have that

$$\vartheta \circ \varphi = \text{id}_{\hat{E}(p^n\mathbb{Z}_p)} \quad \text{and} \quad \varphi \circ \vartheta = \text{id}_{E_n(\mathbb{Q}_p)},$$

it follows that ϑ has an inverse and therefore it is a group isomorphism. This completes the proof. \square

5.3 The formal logarithm

This subsection will provide an explicit group isomorphism between $\hat{E}(p^n\mathbb{Z}_p)$ and $p^n\mathbb{Z}_p$, with $+$ denoting the addition on the p -adic integers. The map is called the formal logarithm of F_E , denoted by \log_{F_E} . Just as the natural logarithm maps to the additive group of the real numbers, the formal logarithm sends elements to the additive group $p^n\mathbb{Z}_p$. To construct \log_{F_E} , we start by considering a power series $P(T)$ in $\mathbb{Z}_p[[T]]$ satisfying⁴

$$P(F_E(T, S)) \frac{\partial}{\partial X} F_E(T, S) = P(T), \quad (5.5)$$

where $(\partial/\partial X)F_E$ denotes the derivative of F_E with respect to the first argument. Since \log_{F_E} needs to be a homomorphism, we should have that for all u_1, u_2 in $\hat{E}(p^n\mathbb{Z}_p)$, it satisfies

$$\log_{F_E}(u_1 \oplus_{F_E} u_2) = \log_{F_E}(u_1) + \log_{F_E}(u_2). \quad (5.6)$$

⁴The differential form $P(T)dT$ where $P(T)$ satisfies (5.5) is called an *invariant differential*.

Hence, by setting $T = 0$ and recalling that $F_E(0, S) = S$, equation (5.5) becomes

$$P(S) \frac{\partial}{\partial X} F_E(0, S) = P(0).$$

From the expression for F_E in (5.4), we see that $(\partial/\partial X)F_E(0, S)$ has constant term 1 and therefore $[(\partial/\partial X)F_E(0, S)]^{-1}$ exists in $\mathbb{Z}_p[[T]]$. The inverse is given by

$$[(\partial/\partial X)F_E(0, S)]^{-1} = 1 + a_1 S + (a_1^2 + a_2) S^2 + (a_1^3 + 2a_1 a_2 + 2a_3) S^3 + \dots$$

Therefore $P(0)$ completely determines $P(T)$ and every power series satisfying (5.5) is of the form

$$P(T) = a \cdot [(\partial/\partial X)F_E(0, T)]^{-1}$$

for some constant a in \mathbb{Z}_p . In our case, we let $a = 1$ and we obtain⁵

$$P(T) = 1 + a_1 T + (a_1^2 + a_2) T^2 + (a_1^3 + 2a_1 a_2 + 2a_3) T^3 + \dots$$

We now define

$$\log_{F_E}(T) := \int P(T) dT = T + \frac{a_1}{2} T^2 + \frac{a_1^2 + a_2}{3} T^3 + \dots \in \mathbb{Q}_p[[T]].$$

Note the analogy with the natural logarithm, which is defined as the integral of dt/t on $[1, x]$ for some real number $x > 0$.

Clearly, \log_{F_E} maps $\hat{E}(p^n \mathbb{Z}_p)$ to $p^n \mathbb{Z}_p$. To show that it is a group homomorphism, we integrate both sides of (5.5) with respect to T to obtain

$$\log_{F_E}(F_E(T, S)) = \log_{F_E}(T) + C(S),$$

with $C(S)$ any power series in $\mathbb{Q}_p[[S]]$. Take $C(S) = \log_{F_E}(S)$, then

$$\log_{F_E}(F_E(T, S)) = \log_{F_E}(T) + \log_{F_E}(S)$$

and thus (5.6) is satisfied for any u_1, u_2 in $\hat{E}(p^n \mathbb{Z}_p)$. To show that \log_{F_E} is an isomorphism, we prove that it has an inverse map; that is, a power series f in $\mathbb{Q}_p[[T]]$ such that $\log_{F_E}(f(T)) = T$ and $f(\log_{F_E}(T)) = T$. We start by inductively constructing a sequence $(f_m)_{m \in \mathbb{N}}$ of polynomials in $\mathbb{Q}_p[T]$ that satisfy

$$\begin{aligned} \log_{F_E}(f_m(T)) &\equiv T \pmod{T^{m+1}}, \\ f_{m+1}(T) &\equiv f_m(T) \pmod{T^{m+1}}. \end{aligned} \tag{5.7}$$

These conditions imply that there exists a limit f in $\mathbb{Q}_p[[T]]$ of this sequence by Hensel's lemma⁶ and that $\log_{F_E}(f(T)) = T$. As a base case, let $f_1(T) = T$. Now suppose the conditions hold for some f_{m-1} in the sequence. We need to find the value a in \mathbb{Q}_p for which the polynomial f_m in $\mathbb{Q}_p[T]$ with

$$f_m(T) = f_{m-1}(T) + aT^m$$

⁵The differential $P(T)dT$ is equal to the power series expression of the invariant differential ω of an elliptic curve E . See [Sil09, Chapter IV.1].

⁶This follows from the fact that we can complete $\mathbb{Q}_p[[T]]$ via the (T) -adic topology on $\mathbb{Q}_p[[T]]$ and this gives $\mathbb{Q}_p[[T]]$. Alternatively, the completion $\mathbb{Q}_p[[T]]$ is the inverse limit of $\mathbb{Q}_p[T]$ with respect to (T) . See [AM94, Chapter 10] and [Eis13, Chapter 7] for more information on this topic.

satisfies $\log_{F_E}(f_m(T)) \equiv T \pmod{T^{m+1}}$. Using that f_{m-1} has no constant term in (5.8) and in (5.9) that f_{m-1} satisfies first condition from (5.7), we obtain

$$\begin{aligned} \log_{F_E}(f_m(T)) &= \log_{F_E}(f_{m-1}(T) + aT^m) \\ &= (f_{m-1}(T) + aT^m) + \frac{a_1}{2}(f_{m-1}(T) + aT^m)^2 + \dots \\ &\equiv aT^m + f_{m-1}(T) + \frac{a_1}{2}(f_{m-1}(T))^2 + \dots \pmod{T^{m+1}} \end{aligned} \quad (5.8)$$

$$\begin{aligned} &\equiv aT^m + \log_{F_E}(f_{m-1}(T)) \pmod{T^{m+1}} \\ &\equiv aT^m + T + bT^m \pmod{T^{m+1}}, \end{aligned} \quad (5.9)$$

for some b in \mathbb{Q}_p . Let $a = -b$, so that both conditions hold for f_m . By induction, the sequence converges to some f in $\mathbb{Q}_p[[T]]$ satisfying $\log_{F_E}(f(T)) = T$. In order to show that $f(\log_{F_E}(T)) = T$ also holds, we apply the technique above to f and find g in $\mathbb{Q}_p[[T]]$ such that $f(g(T)) = T$. Now we have that

$$f(\log_{F_E}(T)) = f(\log_{F_E}(f(g(T)))) = f(\log_{F_E} \circ f(g(T))) = f(g(T)) = T,$$

as desired. Thus, \log_{F_E} is invertible. Summarising the discussion above leads to the following theorem.

Theorem 5.9. *Let E be an elliptic curve defined over \mathbb{Z}_p and let n be a positive integer. The formal logarithm*

$$\begin{aligned} \log_{F_E} : \hat{E}(p^n\mathbb{Z}_p) &\rightarrow p^n\mathbb{Z}_p, \\ u &\mapsto u + \frac{a_1}{2}u^2 + \frac{a_1^2 + a_2}{3}u^3 + \dots, \end{aligned}$$

is a group isomorphism.

Apart from an explicit expression for the formal logarithm, the theorem above, together with Proposition 5.8, tells us that $E_n(\mathbb{Q}_p) \cong p^n\mathbb{Z}_p$ for all positive integers n . The explicit isomorphism is given by $\psi := \log_{F_E} \circ \vartheta$ and is called the *p -adic elliptic logarithm*. Thus, we have that

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p.$$

Notice that there exists an isomorphism from $p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$ to $\mathbb{Z}/p\mathbb{Z}$, which sends the element $x = p^n \sum_{i=0}^{\infty} \alpha_i p^i + p^{n+1}\mathbb{Z}_p$ to α_0 . Hence we obtain

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong \mathbb{Z}/p\mathbb{Z}. \quad (5.10)$$

The use of this isomorphism and the p -adic elliptic logarithm will become clear in the next section, where Smart's attack will be explained.

6 Smart's algorithm

This section studies the algorithm developed by N. P. Smart that can be used to solve the discrete logarithm problem on anomalous elliptic curves. Recall from the introduction that an elliptic curve \tilde{E} over \mathbb{F}_p is anomalous if

$$\#\tilde{E}(\mathbb{F}_p) = p.$$

Observe that since the group has prime order, it is cyclic. Therefore, as long as \tilde{P} is nontrivial, we can always find $k \pmod{p}$ such that $k\tilde{P} = \tilde{Q}$, for any $\tilde{Q} \in \tilde{E}(\mathbb{F}_p)$. Smart's algorithm provides a method to reduce the discrete logarithm problem on $\tilde{E}(\mathbb{F}_p)$ to the problem of finding the inverse of an element in $(\mathbb{Z}/p\mathbb{Z})^\times$, which is easily solvable.

6.1 The algorithm over \mathbb{F}_p

The theorem describing Smart's algorithm is given below. We refer to Appendix A.1 for an implementation of this method in SageMath.

Theorem 6.1 (Smart's algorithm). *Let \tilde{E} be an anomalous elliptic curve over \mathbb{F}_p . Let \tilde{P}, \tilde{Q} in $\tilde{E}(\mathbb{F}_p)$ be points such that*

$$k\tilde{P} = \tilde{Q}$$

for some integer k . Then the following algorithm finds $k \bmod p$ in polynomial time:

Smart's algorithm
<p>Input: anomalous elliptic curve \tilde{E} over \mathbb{F}_p and points \tilde{P}, \tilde{Q} in $\tilde{E}(\mathbb{F}_p)$, with \tilde{P} nontrivial</p> <p>Output: $k \bmod p$ satisfying $k\tilde{P} = \tilde{Q}$</p> <ol style="list-style-type: none"> 1 $E \leftarrow$ elliptic curve over \mathbb{Q}_p with same coefficients as \tilde{E} 2 $P, Q \leftarrow$ lifts of \tilde{P}, \tilde{Q} 3 $a \leftarrow$ x-coordinate of pP 4 while $\nu_p(a) \leq -4$ do <li style="padding-left: 20px;">5 $E \leftarrow$ random elliptic curve over \mathbb{Q}_p that reduces to \tilde{E} modulo p <li style="padding-left: 20px;">6 $P, Q \leftarrow$ lifts of \tilde{P}, \tilde{Q} <li style="padding-left: 20px;">7 $a \leftarrow$ x-coordinate of pP 8 end 9 $k \leftarrow \psi(pQ)/\psi(pP)$ 10 return $k \bmod p$

Proof. We need to show that

$$k \equiv \frac{\psi(pQ)}{\psi(pP)} \pmod{p}.$$

This will mean that $\psi(pQ)/\psi(pP) \bmod p$ is the solution to the problem. To this end, let E be the elliptic curve over \mathbb{Q}_p with the same coefficients as \tilde{E} and let P, Q in $E(\mathbb{Q}_p)$ be the lifts of \tilde{P}, \tilde{Q} , respectively. Since π is a group homomorphism, it follows that

$$\pi(kP - Q) = k\pi(P) - \pi(Q) = k\tilde{P} - \tilde{Q} = \mathcal{O}$$

and hence $R := kP - Q \in E_1(\mathbb{Q}_p)$. From Proposition 5.7 and (5.10) we have

$$E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \tilde{E}(\mathbb{F}_p) \quad \text{and} \quad E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p) \cong \mathbb{Z}/p\mathbb{Z}.$$

Applying multiplication-by- p to R gives an element in $E_2(\mathbb{Q}_p)$. This follows from the second isomorphism given above, which implies that the order of $E_1(\mathbb{Q}_p)/E_2(\mathbb{Q}_p)$ is p , thus adding an element p times to itself must give $\mathcal{O} + E_2(\mathbb{Q}_p)$, that is, $pR \in E_2(\mathbb{Q}_p)$. By similar reasoning, since the curve \tilde{E} is anomalous, one obtains from the first isomorphism above that $pP, pQ \in E_1(\mathbb{Q}_p)$. Now, using the p -adic elliptic logarithm, we obtain

$$k \cdot \psi(pP) - \psi(pQ) = \psi(pR) \in p^2\mathbb{Z}_p,$$

which gives us

$$k \cdot \psi(pP) - \psi(pQ) \equiv 0 \pmod{p^2}. \tag{6.1}$$

Since both $\psi(pP)$ and $\psi(pQ)$ are in $p\mathbb{Z}_p$, we can write

$$\psi(pP) = \alpha_1 p + \alpha_2 p^2 + \dots \quad \text{and} \quad \psi(pQ) = \beta_1 p + \beta_2 p^2 + \dots$$

The equivalence in (6.1) now gives $k \cdot \alpha_1 \equiv \beta_1 \pmod{p}$ and thus

$$k \equiv \frac{\psi(pQ)}{\psi(pP)} \equiv \frac{\beta_1}{\alpha_1} \pmod{p}.$$

as desired.

For the time complexity, write $N = \log(p)$, that is, N is the number of bits (up to a scalar) of the input. The operations that depend on N are finding the multiplicative inverse of an element modulo p and the multiplication of points P and Q by p . All of these actions can be done in $O(N)$ time;⁷ the former by using Fermat's little theorem and the latter by using the successive doubling algorithm [Was08, Section 2.2]. Therefore, the time complexity of the algorithm is given by $O(N)$; that is polynomial time. \square

Remark. It does not suffice to take new lifts for the points P and Q if the x -coordinate of pP has valuation less than or equal to -4 , that is, $pP \in E_2(\mathbb{Q}_p)$; one really needs to take a different lift E for \tilde{E} .

Remark. The algorithm will have little success when \tilde{E} is not anomalous. In this case, pP need not be an element of $E_1(\mathbb{Q}_p)$. We discuss this in more detail below.

Notice that in the proof we only need to know the values of $\psi(pP)$ and $\psi(pQ)$ modulo p^2 . Hence it suffices to take points P and Q that satisfy the equation for E modulo p^2 and reduce to \tilde{P} and \tilde{Q} modulo p . That is, we do not have to compute complete lifts of \tilde{P} and \tilde{Q} .

The reason for the condition in the while-loop on line 4 of Smart's algorithm is that if $pP \in E_2(\mathbb{Q}_p)$, then the algorithm fails. In this case, $pQ \in E_2(\mathbb{Q}_p)$ as well (since it is a group) and therefore $\psi(pP), \psi(pQ) \in p^2\mathbb{Z}_p$. As a result, the equivalence in (6.1) does not give us any information because we obtain

$$k \cdot 0 - 0 \equiv 0 \pmod{p^2}.$$

Therefore, we need to take a different lift for the curve \tilde{E} . Fortunately, this only happens with probability $1/p$ [Bla+99, Section V.3]. In most cases, the primes that are considered are very large, so the chance of requiring a new lift is very slim.

The key point in this algorithm is that if \tilde{E} is anomalous, then it is assured that pP, pQ are in $E_1(\mathbb{Q}_p)$. Therefore, we can apply the p -adic elliptic logarithm, which is only defined on $E_1(\mathbb{Q}_p)$. If the curve is not anomalous, then we can still compute the discrete logarithm, but it will not be as efficient. To obtain points in $E_1(\mathbb{Q}_p)$, we need to be more specific about the lifts we take. We illustrate this with a simple example.

Example 6.2. Let $\tilde{E} : y^2 = x^3 + 5x + 2$ be an elliptic curve over \mathbb{F}_{97} . We have that $\#\tilde{E}(\mathbb{F}_{97}) = 104$. Consider the points $\tilde{P} = (14, 10)$ and $\tilde{Q} = (6, 65)$ in $\tilde{E}(\mathbb{F}_{97})$. We seek k such that $k\tilde{P} = \tilde{Q}$. First, we define E over \mathbb{Z}_{97} with the same coefficients as \tilde{E} . To lift \tilde{P} and \tilde{Q} modulo 97^2 , we use the same technique as was given in Example 4.22. It follows that

$$P \equiv (14, 10 + 79 \cdot 97) \pmod{97^2} \quad \text{and} \quad Q \equiv (6, 65 + 84 \cdot 97) \pmod{97^2}.$$

⁷The notation $O(f(N))$, for some positive function f , means that the time complexity of an algorithm is bounded by $c \cdot f(N)$, where c is some positive constant.

The correct value of k modulo 97 is 12, however, it follows that

$$12P \equiv (6 + 59 \cdot 97, 65 + 45 \cdot 97) \not\equiv (6, 65 + 84 \cdot 97) \equiv Q \pmod{97^2}.$$

Hence, the relation $kP \equiv Q \pmod{97^2}$ does not hold. We must take a different lift of Q ; instead of fixing the x -coordinate and solving for y , we write

$$Q \equiv (6 + 97m, 65 + 97n) \pmod{97^2},$$

for some integers m and n . To obtain a point on $E \pmod{97^2}$, we need that

$$(65 + 97n)^2 \equiv (6 + 97m)^3 + 5(6 + 97m) + 2 \pmod{97^2},$$

which expands to

$$4225 + 3201n \equiv 248 + 1552m \pmod{97^2}.$$

This gives us the relation $n \equiv 84 + 24m \pmod{97}$. We already know the value of $12P \pmod{97^2}$ and indeed, if $m = 59$, then $n \equiv 45 \pmod{97^2}$. In this case, the congruence $12P \equiv Q \pmod{97^2}$ is satisfied. Thus, let

$$Q \equiv (6 + 59 \cdot 97, 65 + 45 \cdot 97) \pmod{97^2}.$$

Due to this specific choice for Q , we know have that $R \equiv \mathcal{O} \pmod{97^2}$. Thus, it follows that $R \in E_2(\mathbb{Q}_{97})$. We now multiply both P and Q by $\#\tilde{E}(\mathbb{F}_{97}) = 104$ to obtain $104P, 104Q \in E_1(\mathbb{Q}_{97})$ by Proposition 5.7. The rest of the example follows the last part of the proof of Theorem 6.1. We have that

$$k \cdot \psi(104P) - \psi(104Q) = \psi(104R) \in 97^2\mathbb{Z}_{97}.$$

For a point (x, y) in $E_1(\mathbb{Q}_{97}) \cong 97\mathbb{Z}_{97}$, it follows from the expression of \log_{F_E} in Theorem 5.9 that

$$\psi(x, y) = \log_{F_E} \circ \vartheta(x, y) \equiv -\frac{x}{y} \pmod{97^2}.$$

Using successive doubling, we obtain

$$\begin{aligned} 104P &= \left(43 \cdot 97^{-2} + O(97^{-1}), 89 \cdot 97^{-3} + O(97^{-2})\right), \\ 104Q &= \left(36 \cdot 97^{-2} + O(97^{-1}), 22 \cdot 97^{-3} + O(97^{-2})\right). \end{aligned}$$

This gives

$$\begin{aligned} \psi(104P) &= -\frac{43 \cdot 97^{-2}}{89 \cdot 97^{-3}} \equiv 66 \cdot 97 \pmod{97^2}, \\ \psi(104Q) &= -\frac{36 \cdot 97^{-2}}{22 \cdot 97^{-3}} \equiv 16 \cdot 97 \pmod{97^2}. \end{aligned}$$

Since $66^{-1} \equiv 25 \pmod{97}$, we finally have

$$k \equiv \frac{\psi(104Q)}{\psi(104P)} \equiv 16 \cdot 25 \equiv 12 \pmod{97}.$$

As we know, this is the correct answer.

The method used in the example looks quite similar to the approach in Smart's algorithm, however, there is one big setback when the curve is not anomalous. As we have seen, not every lift works in this case. The problem is the following. We want to have lifts P and Q such that multiplying them by a scalar gives points in $E_1(\mathbb{Q}_p)$. From the isomorphism in Proposition 5.7, we see that $\#\tilde{E}(\mathbb{F}_p)$ as the scalar gives the desired points in $E_1(\mathbb{Q}_p)$. We also then need that $R = kP - Q$ multiplied by the group order gives a point in $E_2(\mathbb{Q}_p)$, since this assures the expression in (6.1) for k . However, we will not⁸ get that $\#\tilde{E}(\mathbb{F}_p) \cdot R \in E_2(\mathbb{Q}_p)$. Thus, we require a different approach.

We first compute the lift P as usual, using Hensel's lemma, whereafter we search for a lift Q such that the relation $kP \equiv Q \pmod{p^2}$ is guaranteed. Notice that this lift Q is unique modulo p^2 , for if we have another point Q' satisfying $kP \equiv Q' \pmod{p^2}$, then we obtain $Q \equiv Q' \pmod{p^2}$. Since the relation is preserved, we are certain that $R \in E_2(\mathbb{Q}_p)$ by the reasoning in the example above. Hence, multiplying lifts P and Q by the group order $\#\tilde{E}(\mathbb{F}_p)$ gives points in $E_1(\mathbb{Q}_p)$ and we also have that $\#\tilde{E}(\mathbb{F}_p) \cdot R \in E_2(\mathbb{Q}_p)$ since $R \in E_2(\mathbb{Q}_p)$. From here we can continue by applying the p -adic elliptic logarithm as is done in the proof of Theorem 6.1.

One could argue that, instead of searching for a specific lift, we can just take arbitrary lifts P and Q and multiply both by $\text{lcm}(p, \#\tilde{E}(\mathbb{F}_p)) =: m$ to obtain points mP, mQ in $E_1(\mathbb{Q}_p)$ and mR in $E_2(\mathbb{Q}_p)$. However, by doing so, one in fact obtains that $mP, mQ \in E_2(\mathbb{Q}_p)$ and we saw that in this case, equation (6.1) gives us no information about k .

The problem is finding the specific lift for Q that works. We have seen in the previous example that we have p different lifts for Q . Of course, in general, we do not know the value of k in advance, thus we need to check for every Q if R is in $E_2(\mathbb{Q}_p)$. In a situation where security is of the essence, the prime p is very large; it has order approximately 2^{200} or even higher [KG13, Section D.1]. In this case, sifting through all possible lifts until the correct lift is found takes a lot of work which makes the algorithm impractical as an attack. There are ways to lift points and preserve the relation $P = kQ$ (see [Sil08]), however, all these methods have disadvantages that render them useless as efficient attacks. The condition that \tilde{E} is anomalous is therefore crucial to obtain an efficient algorithm that is based on the method in Theorem 6.1

6.2 The algorithm over \mathbb{F}_q

The natural question to ask is whether this algorithm also works over a finite field \mathbb{F}_q , with $q = p^n$ and $n \in \mathbb{Z}_{>1}$. The short answer is that it works in almost exactly the same way. However, when examining this situation further, we will see that it requires a bit more attention. First, recall the construction of a finite field with nonprime order. Every finite field has prime power order. To construct a field with $q = p^n$ elements, we consider an irreducible polynomial f in $\mathbb{F}_p[X]$ of degree n . Then $\mathbb{F}_p[X]/(f(X))$ is a field of order p^n . It follows that this is the unique field of $q = p^n$ elements up to isomorphism and therefore we denote it by \mathbb{F}_q . Before going into details about the algorithm, we look at an example.

Example 6.3. Consider the irreducible polynomial $X^2 + 7X + 2$ in $\mathbb{F}_{11}[X]$ and the induced field $\mathbb{F}_{121} = \mathbb{F}_{11}[X]/(X^2 + 7X + 2)$. Elements of this field can be represented by $a + b\alpha$, where α is a root of $X^2 + 7X + 2$ in \mathbb{F}_{121} and $a, b \in \mathbb{F}_{11}$. Take $\tilde{E}: y^2 = x^3 + \alpha x + 8\alpha$ over \mathbb{F}_{121} . Then $\#\tilde{E}(\mathbb{F}_{121}) = 121$, so \tilde{E} is anomalous. We want to find $k \pmod{121}$ such that $k\tilde{P} = \tilde{Q}$, for $\tilde{P} = (1, 7\alpha)$ and $\tilde{Q} = (4\alpha, 6\alpha + 6)$ in $\tilde{E}(\mathbb{F}_{121})$, assuming it exists. Instead of \mathbb{Q}_{11} , we now need to lift \tilde{P}, \tilde{Q} to an extension of \mathbb{Q}_{11} , that we will denote by \mathbb{Q}_{121} . This

⁸This could happen if $\#\tilde{E}(\mathbb{F}_p)$ is a multiple of p . But, for $p \leq 5$, we never have that $\#\tilde{E}(\mathbb{F}_p)$ is a multiple of p other than p itself, and for $p > 5$ we have $\#\tilde{E}(\mathbb{F}_p) < 2p$ by the Hasse bound (cf. Theorem 3.12). This means that if \tilde{E} is not anomalous, the group order is never a multiple of p .

is done by taking the polynomial $X^2 + 7X + 2$, but considering it as an element of $\mathbb{Z}_{11}[X]$. Then we define

$$\mathbb{Q}_{121} := \mathbb{Q}_{11}[X]/(X^2 + 7X + 2).$$

Take E to be the elliptic curve over \mathbb{Q}_{121} with the same coefficients as \tilde{E} . We lift \tilde{P}, \tilde{Q} as usual: for \tilde{P} , we have the polynomial $F(Y) := Y^2 - 9\alpha - 1$. To find $Y \pmod{11^2}$, we compute

$$\begin{aligned} F(7\alpha) &= (7\alpha)^2 - 9\alpha - 1 \equiv (\alpha + 2) \cdot 11 \pmod{11^2}, \\ (F'(7\alpha))^{-1} &= (14\alpha)^{-1} \equiv (9\alpha + 8) + (9\alpha + 2) \cdot 11 \pmod{11^2}, \end{aligned}$$

using the fact that $\alpha^2 = -7\alpha - 2$. The y -coordinate of the lift P becomes

$$7\alpha - \frac{F(7\alpha)}{F'(7\alpha)} \equiv 7\alpha + (4\alpha + 2) \cdot 11 \pmod{11^2}.$$

We obtain, by applying the same method to \tilde{Q} , that

$$\begin{aligned} P &\equiv (1, 7\alpha + (4\alpha + 2) \cdot 11) \pmod{11^2}, \\ Q &\equiv (4\alpha, (6\alpha + 6) + (4\alpha + 4) \cdot 11) \pmod{11^2}. \end{aligned}$$

Using the isomorphism in Proposition 5.7, we obtain

$$\begin{aligned} 121P &= \left((2\alpha + 8) \cdot 11^{-2} + O(11^{-1}), 5 \cdot 11^{-3} + O(11^{-2}) \right) \in E_1(\mathbb{Q}_{121}), \\ 121Q &= \left((7\alpha + 6) \cdot 11^{-2} + O(11^{-1}), 3 \cdot 11^{-3} + O(11^{-2}) \right) \in E_1(\mathbb{Q}_{121}). \end{aligned}$$

The same p -adic elliptic logarithm results in

$$\begin{aligned} \psi(121P) &\equiv (4\alpha + 5) \cdot 11 \pmod{11^2}, \\ \psi(121Q) &\equiv (5\alpha + 9) \cdot 11 \pmod{11^2}. \end{aligned}$$

This gives

$$\begin{aligned} k &\equiv \frac{\psi(121Q)}{\psi(121P)} \\ &\equiv \left((5\alpha + 9) \cdot 11 + O(11^2) \right) \cdot \left((8\alpha + 2) \cdot 11^{-1} + O(11^0) \right) \\ &\equiv 4 \pmod{11}, \end{aligned}$$

Thus, we know that $k \equiv 4 \pmod{11}$. However, one can show that the order of \tilde{P} equals 121 and consequently, we have 11 possible choices for $k \pmod{121}$. In our case, it follows that $k \equiv 15 \pmod{121}$. To compute this value, we apply the algorithm again, but now with $\tilde{P}_1 = 11\tilde{P}$ and $\tilde{Q}_1 = \tilde{Q} - 4\tilde{P}$. Solving $k_1\tilde{P}_1 = \tilde{Q}_1$ will give us $k_1 \equiv 1 \pmod{11}$ and therefore $k \equiv 4 + 1 \cdot 11 \equiv 15 \pmod{121}$, as desired.

There are a few points that are worthy of additional elaboration. To make the algorithm work over \mathbb{F}_q , we need an extension K of \mathbb{Q}_p such that $[K : \mathbb{Q}_p] = [\mathbb{F}_q : \mathbb{F}_p]$, that is, the degree of the extension K over \mathbb{Q}_p equals that of \mathbb{F}_q over \mathbb{F}_p . Such an extension is called *unramified*. Before we go into these specific extensions, we will discuss a general finite extension of \mathbb{Q}_p of degree n , denoted by K . First of all, we can extend the p -adic absolute value to K (see [Gou12, Section 5.4] for details). Recall how we defined the p -adic integers \mathbb{Z}_p in Section 4.3. In the same way, we define

$$\mathcal{O}_K := \{x \in K : |x|_p \leq 1\},$$

where $|\cdot|_p$ denotes the extended absolute value. For p -adic integers, we know that the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to \mathbb{F}_p . We have used this fact many times to obtain the unique lift of an element in \mathbb{F}_p . In order to assure that we also have unique lifting over \mathbb{F}_q , an unramified extension K over \mathbb{Q}_p is required. The reason is that such extensions are precisely the extensions that make $\mathcal{O}_K/p\mathcal{O}_K$ into a field. The degree of the extension is n and hence this field has p^n elements, so it is isomorphic to \mathbb{F}_q . This gives us Hensel's lemma as it is given in Theorem 4.21, but with \mathbb{Z}_p replaced by \mathcal{O}_K , which is what we were after. The proof is identical.

It is not hard to find an unramified extension of degree n . To obtain such an extension, take the monic irreducible polynomial of degree n in $\mathbb{F}_p[X]$ that was used to construct \mathbb{F}_q and consider it over \mathbb{Z}_p , as was done in Example 6.3. This polynomial will be irreducible over \mathbb{Q}_p (see [Gou12, Corollary 5.3.8]) and hence, since $\mathbb{Q}_p[X]$ is a principal ideal domain, it follows that $\mathbb{Q}_p[X]/(f(X))$ is a field. Just as for finite extensions of \mathbb{F}_p , there is exactly one finite unramified extension over \mathbb{Q}_p of degree n (up to isomorphism, cf. [Gou12, Proposition 5.4.11]). Due to the uniqueness, we denote this extension by \mathbb{Q}_q .

In addition to this, the algorithm extends in another way from the method over \mathbb{F}_p . In Example 6.3, we compute k by applying the algorithm another time to find the p -adic expansion of $k \bmod 11^2$. In general, when $q = p^n$, we use the algorithm in Theorem 6.1 n times to find the p -adic expansion

$$c_0 + c_1p + \dots + c_{n-1}p^{n-1}$$

of $k \bmod p^n$. For c_0 , we just apply the algorithm as usual. If we know c_0, \dots, c_{i-1} for some $i \leq n-1$, then we can compute c_i as follows: let

$$\tilde{P}_0 = p^{n-1}\tilde{P} \quad \text{and} \quad \tilde{Q}_i = p^{n-i-1} \left(\tilde{Q} - \left(\sum_{j=0}^{i-1} c_j p^j \right) \tilde{P} \right).$$

Now, observe that

$$\begin{aligned} \tilde{Q}_i &= p^{n-i-1} \left(\tilde{Q} - \left(\sum_{j=0}^{i-1} c_j p^j \right) \tilde{P} \right) \\ &= \left(p^{n-i-1} \left(\sum_{j=0}^{n-1} c_j p^j - \sum_{j=0}^{i-1} c_j p^j \right) \right) \tilde{P} \\ &= \left(p^{n-i-1} \left(\sum_{j=i}^{n-1} c_j p^j \right) \right) \tilde{P} \\ &= \left(p^{n-1} \left(\sum_{j=i}^{n-1} c_j p^{j-i} \right) \right) \tilde{P} \\ &= c_i p^{n-1} \tilde{P} + \left(\left(\sum_{j=i+1}^{n-1} c_j p^{j-i-1} \right) p^n \right) \tilde{P} \\ &= c_i \tilde{P}_0 + \mathcal{O} = c_i \tilde{P}_0. \end{aligned}$$

We obtain $c_i \tilde{P}_0 = \tilde{Q}_i$ and thus, by applying Smart's algorithm, we can find $c_i \bmod p$.

For the time complexity, let $N = \log(q)$, the number of bits (up to a scalar) of the input. To calculate $k \bmod p^n$, we need to compute \tilde{Q}_i and then apply Smart's algorithm, for every i . Computing \tilde{Q}_i takes approximately $(n-1)N/n$ operations and Smart's algorithm takes approximately N operations, so $(n-1)N^2/n$ operations combined. We do this n times, so we obtain $(n-1)N^2$ operations in total. If p is fixed, then observe that since $n = \log_p(q) = N/\log(p)$, we have that the time complexity is $O(N^3)$. If n is fixed, then the time complexity is $O(N^2)$. Either way, we obtain a polynomial running time algorithm.

7 Searching for anomalous curves

This section will look at an algorithm to find anomalous curves with small coefficients over relatively large finite fields of prime order. There is no particular reason why we choose to restrict the size of the coefficients; it is mostly due to personal preference and ease of notation. Although a method exists (see [Lep+05]) to construct anomalous curves over arbitrarily large prime fields, it does not provide a way to choose the size of the coefficients. Using an appropriate change of variables (which we will see later), one could slightly adapt the coefficients and their size, however, often they will remain large. We will try to make the program as efficient as possible in order to go over enough primes and find anomalous curves. The code can be found in Appendix B. The first part of this section looks at general theory about the j -invariant and quadratic twists of elliptic curves and how we can apply this to make our code more efficient. A few specific elliptic curves having certain j -invariants will be further discussed in the second subsection, which considers curves with complex multiplication. Finally, we will briefly go into a method that approximates the effectiveness of the program. Moreover, it will give the output of the code. Most of the theory in this section can be found in [Was08, Section 2.7, 4.6], [Sil09, Section C.11] or [Ols76].

7.1 The j -invariant and quadratic twists

In our search, we always assume that both our coefficients are nonzero, since we are not interested in finding anomalous curves of the form

$$y^2 = x^3 + Ax \quad \text{and} \quad y^2 = x^3 + B.$$

In fact, for the curves of the right-hand form, we already know the exact conditions on p and B for which they are anomalous. In Appendix C, one can find an anomalous curve of this form over a very large prime field. The elliptic curves on the left are never anomalous. For proofs of both of these statements, see [Ols76].

A very important quantity of an elliptic curve $E: y^2 = x^3 + Ax + B$ over K is the j -invariant, given by

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2} \in K. \tag{7.1}$$

Recall from Section 2 that the denominator was assumed to be nonzero in the definition of an elliptic curve.

One of the main concepts we consider that involve the j -invariant are the so-called *quadratic twists*. We say that two curves are quadratic twists over K if they have the same j -invariant, not equal to⁹ 0 or 1728, and are not isomorphic over K . Since our curve E is already assumed to have nonzero coefficients, we can deduce from (7.1) that E does not have j -invariant 0 or 1728, so we can consider its quadratic twists; take a square-free element $d \in K$ and apply over $K(\sqrt{d})$ the following change of variables to E :

$$x_1 = dx \quad \text{and} \quad y_1 = d\sqrt{d}y. \tag{7.2}$$

Then, the equation becomes

$$y_1^2 = x_1^3 + d^2Ax_1 + d^3B \tag{7.3}$$

⁹These cases are referred to as quartic and sextic twists, respectively. See [Sil09, Section X.5, Proposition 5.4].

and we denote it by $E^{(d)}$. Observe that this curve has the same j -invariant as E , since

$$j(E^{(d)}) = 1728 \frac{4(d^2 A)^3}{4(d^2 A)^3 + 27(d^3 B)^2} = 1728 \frac{4d^6 A^3}{4d^6 A^3 + 27d^6 B^2} = j(E).$$

So, since d is not a square in K , we have that E and $E^{(d)}$ are not isomorphic over K (the change of variables does not provide a rational map) and hence they are quadratic twists over K . In truth, these are all quadratic twists of E . This follows from the fact that if two curves

$$E: y^2 = x^3 + Ax + B \quad \text{and} \quad E': y^2 = x^3 + A'x + B'$$

have the same j -invariant, then the coordinate transformation in (7.2) takes one equation to the other. To see this, take d in $\overline{\mathbb{F}}_p$ satisfying $A' = d^2 A$. This implies that

$$\frac{4A'^3}{4A'^3 + 27B'^2} = \frac{4A^3}{4A^3 + 27B^2} = \frac{4d^{-6}A'^3}{4d^{-6}A'^3 + 27B^2} = \frac{4A^3}{4A^3 + 27d^6 B^2},$$

so $B' = \pm d^3 B$. The relation $B' = d^3 B$ directly gives us the desired answer. If $B' = -d^3 B$, then take $-d$ instead of d . This gives $B' = -(-d)^3 B = d^3 B$ while preserving $A' = d^2 A$. Note that in fact $d \in K$, since

$$\frac{B'}{B} = d^3 = d \frac{A'}{A}$$

thus $d = (B'/B)(A/A') \in K$. Since the transformations $A' = d^2 A$ and $B' = d^3 B$ follow from the change of variables in (7.2), this means that two curves have the same j -invariant precisely when $x_1 = dx$ and $y_1 = d\sqrt{d}y$ for some d in K , with the change of variables considered over $K(\sqrt{d})$. Now, if d is not a square in K , then this map is not rational (over K) and hence the curves are not isomorphic over K , so they are quadratic twists by definition. This shows that the curves given by (7.3) for a non-square d in K are precisely the quadratic twists of the curve E .

Now let $\tilde{E}: y^2 = x^3 + Ax + B$ denote an elliptic curve over the finite field \mathbb{F}_p . The reason we consider quadratic twists of \tilde{E} is due to the fact that we obtain the following useful equality when our field K equals \mathbb{F}_p :

$$\#\tilde{E}(\mathbb{F}_p) + \#\tilde{E}^{(d)}(\mathbb{F}_p) = 2p + 2. \quad (7.4)$$

To show this, we will first rewrite the general equation for a quadratic twist. Consider the transformation

$$x_2 = \frac{x_1}{d} \quad \text{and} \quad y_2 = \frac{y_1}{d^2}.$$

Then (7.3) becomes

$$d^4 y_2^2 = d^3 x_2^3 + d^3 A x_2 + d^3 B,$$

and therefore

$$dy_2^2 = x_2^3 + Ax_2 + B.$$

Now, let $f(x) := x^3 + Ax + B$. The equality in (7.4) is just a matter of counting the points. If for x in \mathbb{F}_p we have $f(x) = 0$, then both groups $\tilde{E}(\mathbb{F}_p)$ and $\tilde{E}^{(d)}(\mathbb{F}_p)$ get one point. Note that for all other x in \mathbb{F}_p , we have that $f(x)$ is either a square in \mathbb{F}_p or it is not. If x is such that $f(x)$ is a square, then $y^2 = f(x)$ has two solutions while $dy^2 = f(x)$ has none, so two points for $\tilde{E}(\mathbb{F}_p)$ and none for $\tilde{E}^{(d)}(\mathbb{F}_p)$. Similarly, if $f(x)$ is not a square, then $dy^2 = f(x)$

has two solutions (since d is not a square, $f(x)/d$ will be a square) and $y^2 = f(x)$ has none. Therefore, we have two points for $\tilde{E}^{(d)}(\mathbb{F}_p)$ and none for $\tilde{E}(\mathbb{F}_p)$. We see that each element of \mathbb{F}_p contributes two to the sum in (7.4) and, together with the identity counted twice, the relation follows.

Due to this equality, if a curve with a certain j -invariant is not anomalous, we check if the group order is $p + 2$. If this is the case, then we compute a quadratic twist of the curve (with sufficiently small coefficients, for convenience) and the resulting curve will be anomalous.

The reason we only need to consider each j -invariant once is the following. If a curve with a certain j -invariant is anomalous, then any other anomalous curve with the same j -invariant must be isomorphic. For if it were not, both curves would be quadratic twists of each other by definition, but this cannot be the case since both groups have order p and hence the relation in (7.4) is not satisfied.

At the start of this section we mentioned that there was a method to construct anomalous curves over large prime fields, but that it does not provide a way to choose the size of the coefficients. With the change of variables given in (7.2) and a quadratic residue d in \mathbb{F}_p , one could tinker a bit with the coefficients. Unfortunately, most of the time these coefficients will remain very large and hence this is not a feasible option when we want to find anomalous curves over large fields with small coefficients. Despite this, it is a very clever method to construct anomalous curves. In Appendix D, one can find an anomalous curve constructed using the method outlined in [Lep+05]. One of the important concepts behind the theory described in Leprévost et al. is elliptic curves with complex multiplication. Such curves will be examined more closely in the next subsection.

7.2 Elliptic curves with complex multiplication

We will go over the main idea behind elliptic curves with complex multiplication and subsequently go into the use (or rather, non-use) of such curves to slightly improve our code.

Recall the definition of an endomorphism from Section 3.1. The set of all endomorphisms of an elliptic curve E over a field K can be formed into a ring,¹⁰ denoted by $\text{End}(E)$ (see [Sil09, Section III.9]). In general, an elliptic curve over a field K is said to possess *complex multiplication* if its endomorphism ring is larger than \mathbb{Z} .

We have seen that multiplication by an integer is always an endomorphism. Therefore, $\text{End}(E)$ contains a subring that is isomorphic to \mathbb{Z} . In the case that our field K has positive characteristic, the ring of endomorphisms is always bigger than \mathbb{Z} since it contains the Frobenius endomorphism as well (cf. Lemma 3.9), which does not correspond to an element in \mathbb{Z} ; rather, it is an algebraic integer of degree 2 and not real. Formally, elliptic curves over finite fields therefore always possess complex multiplication. For most of the curves over fields of positive characteristic, the endomorphism ring is isomorphic to $\mathbb{Z}[\alpha]$, where α is some algebraic integer and $\mathbb{Z}[\alpha]$ contains $\mathbb{Z}[\varphi_p]$. There is one class of elliptic curves, the supersingular elliptic curves, that contains precisely the curves which have endomorphism ring even larger than $\mathbb{Z}[\alpha]$.

For elliptic curves over fields of characteristic 0, the endomorphism ring can be isomorphic to \mathbb{Z} , or isomorphic to an *order* in an *imaginary quadratic extension* of \mathbb{Q} . In the latter case, these curves are thus said to have complex multiplication. For our purposes, we will consider \mathbb{Q} as our field of characteristic zero.

Our motivation for discussing CM curves stems from the fact that our program was originally developed to look for supersingular elliptic curves as well. It was produced

¹⁰Note that in the definition of an endomorphism, we assumed it to be nontrivial. However, it should be mentioned that the identity in the endomorphism ring is the trivial endomorphism.

together with fellow student Roelien Smit, who did a research project on the discrete logarithm problem on supersingular elliptic curves [Smi20]. It often happens that, for a curve over \mathbb{Q} with complex multiplication, reducing the curve modulo a prime p gives a supersingular curve over \mathbb{F}_p [Sil09, Section V.4]. We wanted to avoid these curves, since it is precisely known for which primes p the reductions modulo p are supersingular. However, since the code checked for anomalous and supersingular curves at the same time, it was not certain if we should leave out the reductions of CM curves completely; perhaps a CM curve could also reduce to an anomalous curve for some primes. It turns out that this is not the case for our range of coefficients, but it is not obvious. To prove this, a more detailed inspection of the endomorphism ring of an elliptic curve over \mathbb{Q} is required.

We mentioned that, for an elliptic curve E over \mathbb{Q} with complex multiplication, the endomorphism ring is isomorphic to an order in an imaginary quadratic extension of \mathbb{Q} . First of all, a *quadratic extension* is an extension of \mathbb{Q} of degree 2. Such extensions can be formed by adjoining a square root of a square-free integer d . They are denoted by $\mathbb{Q}(\sqrt{d})$. When we adjoin the square root of a negative square-free integer, we call such an extension *imaginary*. So, in our case, we look at orders of the field $\mathbb{Q}(\sqrt{-d})$, where d is a positive square-free integer.

Before discussing orders, we will restrict the values d can take. Since we consider an elliptic curve over \mathbb{Q} , it follows from the definition of the j -invariant that it is an element of \mathbb{Q} (cf. (7.1), with $K = \mathbb{Q}$). It can be shown that in this case, the field $\mathbb{Q}(\sqrt{-d})$ has class number 1 (see [Sil09, Section C.11, Example 11.3.2]). This means that the ring of integers (also known as the *maximal order*) of $\mathbb{Q}(\sqrt{-d})$, denoted by $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$, is a principal ideal domain. The ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ consists of elements that are roots of monic polynomials with integral coefficients. Since our extension is of degree 2, these polynomials have degree 2. Therefore we consider roots of

$$X^2 + c_1X + c_2,$$

with $c_1, c_2 \in \mathbb{Z}$. Roots of these polynomials are called *quadratic integers*. Observe that $\sqrt{-d}$ is a quadratic integer. In fact, the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ equals

$$\begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right], & \text{if } d \equiv 3 \pmod{4}, \\ \mathbb{Z}[\sqrt{-d}], & \text{otherwise.} \end{cases}$$

Note that since $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ is a principal ideal domain, it also has unique factorisation (up to the order and up to units).

Due to the fact that our field has class number 1, the number of values for d is heavily reduced; it was conjectured by Gauss, and later proven by Baker, Heegner and Stark (cf. the Baker-Heegner-Stark theorem) that d is equal to one of the following values:¹¹

$$3, 4, 7, 8, 11, 19, 43, 67, 163.$$

For these 9 different values of d , there are 13 corresponding CM j -invariants.¹² We will not go into the computation of these j -invariants. In our case, the only j -invariants that will come up in the program are given in Table 1, together with the corresponding value of d , the *conductor* f (which will be explained soon) and the pair of coefficients (A, B) in our range.

¹¹Sometimes, the values 1 and 2 are written instead of 4 and 8, respectively. This clearly does not change the field extension.

¹²Note that we did not say that the endomorphism ring of an elliptic curve with complex multiplication has to be isomorphic to the *maximal* order of an imaginary quadratic number field.

j -invariant	d	f	(A, B)
54000	3	2	$(-15, 22)$
287496	4	2	$(-11, 14)$
-3375	7	1	$(-35, 98)$
8000	8	1	$(-30, 56)$

Table 1: The considered j -invariants and the corresponding values of d , the conductor f and the coefficients of the elliptic curve $E: y^2 = x^3 + Ax + B$ over \mathbb{Q} .

Our aim is to show that for any prime p , the elliptic curve \tilde{E} over \mathbb{F}_p , obtained by reducing¹³ modulo p an elliptic curve E over \mathbb{Q} defined by a pair of coefficients (A, B) given in Table 1, is not anomalous.

We continue describing the endomorphism ring for a curve with complex multiplication. An *order* of an imaginary number field is a subring of the ring of integers $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ and is denoted by \mathcal{R}_f . It can be written as [Cox89, Section 7.A, Lemma 7.2]

$$\mathcal{R}_f = \mathbb{Z} + f\mathcal{O}_{\mathbb{Q}(\sqrt{-d})},$$

where f is a unique positive integer called the *conductor*. Elements of \mathcal{R}_f are of the form $a + fr$ with $a \in \mathbb{Z}$ and $r \in \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. The ring $\text{End}(E)$ is thus isomorphic to \mathcal{R}_f for some f .

In Section 3.1, we defined $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$. Hence \tilde{E} being anomalous is equivalent to $a_p = 1$. By [Cox89, Section 14.C, Theorem 14.16], it follows that there exists $\pi = b + fr$ in \mathcal{R}_f such that

$$a_p = \pi + \bar{\pi} \quad \text{and} \quad p = \pi\bar{\pi},$$

where $\bar{\pi}$ denotes the conjugate of π . Notice that π corresponds to the Frobenius endomorphism φ_p in $\text{End}(\tilde{E})$; as we mentioned before, φ_p is an algebraic integer and in fact a root of the polynomial (cf. [Was08, Section 4.2, Theorem 4.10])

$$X^2 - a_p X + p = (X - \pi)(X - \bar{\pi}).$$

We can now prove the following.

Proposition 7.1. *Let E be an elliptic curve over \mathbb{Q} and suppose that*

$$j(E) \in \{287496, 8000\}.$$

Then, the reduction \tilde{E} of E is not anomalous for any prime p .

Proof. From Table 1, we have that in this case $d \equiv 0 \pmod{4}$. Thus

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} = \mathbb{Z}[\sqrt{-d}] = \{k + l\sqrt{-d} : k, l \in \mathbb{Z}\}.$$

Let $p = \pi\bar{\pi}$ with $\pi = b + fr \in \mathcal{R}_f$, where $b \in \mathbb{Z}$ and $r \in \mathbb{Z}[\sqrt{-d}]$. We can write $r = k + l\sqrt{-d}$ and therefore

$$\pi = b + fr = b + f(k + l\sqrt{-d}) = (b + fk) + fl\sqrt{-d}.$$

The conjugate $\bar{\pi}$ of π is given by $(b + fk) - fl\sqrt{-d}$. Since $a_p = \pi + \bar{\pi}$, we obtain

$$a_p = (b + fk) + fl\sqrt{-d} + (b + fk) - fl\sqrt{-d} = 2(b + fk).$$

Hence, the trace is always even. Thus, the order of $\tilde{E}(\mathbb{F}_p)$ is never p , which proves the result. \square

¹³As before, we will assume that E has good reduction.

Remark. The theorem also shows that \tilde{E} cannot be a quadratic twist of an anomalous curve, that is, $\#\tilde{E}(\mathbb{F}_p)$ does not equal $p + 2$.

From the result and the remark, it follows that we do not have to check the elliptic curves over \mathbb{F}_p that are given by

$$y^2 = x^3 - 11x + 14 \quad \text{and} \quad y^2 = x^3 - 30x + 56.$$

This leaves us with the other two j -invariants in Table 1. For these, we first introduce the following lemma.

Lemma 7.2. *Let E be an elliptic curve over \mathbb{Q} and p be a prime. Suppose that*

$$j(E) \in \{54000, -3375\},$$

with corresponding values d and f , given in Table 1. If the reduction \tilde{E} of E modulo p is anomalous, then p is of the form

$$\frac{1 + f^2 l^2 d}{4},$$

for some integer l .

Proof. In this case we have that $d \equiv 3 \pmod{4}$ and so

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} = \mathbb{Z} \left[\frac{1 + \sqrt{-d}}{2} \right] = \left\{ k + l \frac{1 + \sqrt{-d}}{2} : k, l \in \mathbb{Z} \right\}.$$

Let $p = \pi \bar{\pi}$ where $\pi = b + fr \in \mathcal{R}_f$, with b in \mathbb{Z} and r in $\mathbb{Z}[\frac{1 + \sqrt{-d}}{2}]$. We write $r = k + l(1 + \sqrt{-d})/2$ to obtain

$$\pi = b + fr = b + f \left(k + l \frac{1 + \sqrt{-d}}{2} \right) = \left(b + fk + \frac{fl}{2} \right) + \frac{fl\sqrt{-d}}{2},$$

and thus $\bar{\pi} = (b + fk + fl/2) - fl\sqrt{-d}/2$. It follows that

$$\begin{aligned} a_p = \pi + \bar{\pi} &= \left(b + fk + \frac{fl}{2} \right) + \frac{fl\sqrt{-d}}{2} \\ &\quad + \left(b + fk + \frac{fl}{2} \right) - \frac{fl\sqrt{-d}}{2} \\ &= 2b + 2fk + fl. \end{aligned}$$

If \tilde{E} is anomalous, then $a_p = 1$, so $b + fk + fl/2 = 1/2$. Observe that

$$\begin{aligned} p = \pi \bar{\pi} &= \left(\left(b + fk + \frac{fl}{2} \right) + \frac{fl\sqrt{-d}}{2} \right) \left(\left(b + fk + \frac{fl}{2} \right) - \frac{fl\sqrt{-d}}{2} \right) \\ &= \left(b + fk + \frac{fl}{2} \right)^2 - \frac{f^2 l^2 (-d)}{4} \\ &= \frac{1 + f^2 l^2 d}{4}, \end{aligned}$$

as desired. □

Notice that if we consider the case $a_p = -1$ in the proof, the result also follows since we square $a_p/2$. This means that Lemma 7.2 also holds when \tilde{E} is the quadratic twist of an anomalous curve. Using this lemma, we can now state and prove the wanted result.

Proposition 7.3. *Let E be an elliptic curve over \mathbb{Q} and let p be a prime. Then*

(a) *if $j(E) = 54000$, then \tilde{E} is not anomalous.*

(b) *if $j(E) = -3375$ and $p > 2$, then \tilde{E} is not anomalous.*

Proof. We first consider the case $j(E) = 54000$. Suppose that \tilde{E} is anomalous for a prime p . From Table 1, we have that $f = 2$ and $d = 3$. By Lemma 7.2, it follows that

$$p = \frac{1 + f^2 l^2 d}{4} = \frac{1 + 12l^2}{4} = \frac{1}{4} - 3l^2.$$

Note that since p and l are integers, this is impossible. Therefore, \tilde{E} is not anomalous.

If $j(E) = -3375$ then we have $f = 1$ and $d = 7$. If \tilde{E} is anomalous, then we obtain from Lemma 7.2 that

$$p = \frac{1 + f^2 l^2 d}{4} = \frac{1 + 7l^2}{4}.$$

Suppose that $p > 2$ and write $p = 2m + 1$ for some m in \mathbb{N} . Since l must be odd, write $l = 2n + 1$, for some n in \mathbb{N} . Observe that $l^2 = 4(n^2 + n) + 1$ and $n^2 + n$ is even. Consequently, we have

$$4 \equiv 4(2m + 1) = 1 + 7(2n + 1)^2 \equiv 1 + 7(4(n^2 + n) + 1) \equiv 1 - 1 \equiv 0 \pmod{8}.$$

This is clearly a contradiction, hence \tilde{E} is not anomalous. \square

The proposition above also holds for quadratic twists of anomalous curves since we can still apply Lemma 7.2 and the reasoning in the proof remains exactly the same. Therefore, we can also completely exclude the curves over \mathbb{F}_p of the form

$$y^2 = x^3 - 15x + 22 \quad \text{and} \quad y^2 = x^3 - 35x + 98$$

from our code, since our prime p is always taken to be very large.

In conclusion, we can safely avoid checking the j -invariants in Table 1. This makes the code a bit more efficient, as we now have to check four j -invariants less for every prime.

7.3 The starting prime and the output

Something that is still undecided is the order of the prime at which we start running the program. There should be some certainty that we at least find one anomalous curve. As an initial condition, one could say the aim is to have a 95% probability of success (that is, finding at least one anomalous curve) within a given time frame. The operation in the code that requires the most computational effort is computing the cardinality of the group. This can be done in $O(\log(p)^6)$. Under the assumption that the distribution of anomalous curves is uniform, Hasse's theorem (Theorem 3.12) implies that the probability of a random curve over \mathbb{F}_p being anomalous is approximately $1/(4\sqrt{p})$. Since we only check each j -invariant once, we assume that every time the code runs, this can be seen as an independent event. Lastly, due to our primes being very large, most of the primes that are checked are of the same bit size, hence the probability will be approximately the same for each event.

Using these assumptions, one can compute the size of p that corresponds to a certain probability of success, say 95%. In our case, we chose our starting prime to be roughly 2^{64} . After running the code for three weeks, we found the anomalous curve $\tilde{E}: y^2 = x^3 - 9x + 18$ over \mathbb{F}_p with $p = 2^{64} + 368817$. The point

$$P = (0, 3917997113888895058)$$

can be taken as a generator for $\tilde{E}(\mathbb{F}_p)$.

8 Discussion and further developments

Although Smart’s algorithm can be implemented with a few lines, understanding all the theory behind it is not an easy task. By dissecting the method developed by Smart, knowledge was obtained on the construction of p -adic numbers. For us, one of the main results used from this theory was how to acquire unique lifts of elements in \mathbb{F}_p to p -adic numbers using Hensel’s lemma. As we have seen, this was proven to be essential in the first step of Smart’s algorithm.

Studying the formal group and its respective logarithm helped us create explicit isomorphisms between subgroups of an elliptic curve over the p -adic numbers and ideals of the p -adic integers. This allowed us to transfer the discrete logarithm problem on $\tilde{E}(\mathbb{F}_p)$ to the problem of computing a multiplicative inverse in \mathbb{F}_p , a fascinating result. Moreover, only a minor change to the original method gave a more general version of the algorithm that works on $\tilde{E}(\mathbb{F}_q)$.

To realise our last goal, namely finding anomalous curves with small coefficients over large prime fields, we looked into the j -invariant and the quadratic twists of an elliptic curve. In addition to this, we also touched on elliptic curves with complex multiplication, a topic that was easier to understand due to our discussion of endomorphisms at the start of the thesis. The designed program proved to be effective since we found a desired curve over a fairly large prime field.

Further research could look into the area of post-quantum cryptography. Although solving the discrete logarithm problem is still very time consuming, the developing quantum computers could bring change into this in a few decades. One of the methods that is claimed to provide security against these powerful computers is called the supersingular isogeny key exchange. In this method, which is also based on the Diffie-Hellman key exchange discussed in the introduction, the underlying security comes from the fact that finding a specific isogeny between two supersingular curves is very difficult; see [GV18] for more information on this topic.

Appendices

A The implementation of Smart’s algorithm

The programs below were constructed using the SageMath software package.

A.1 The algorithm

```
reset()
from time import process_time
get_ipython().magic('run_ functions.ipynb')

p = ...;
A = ...;
B = ...;

E = EllipticCurve(GF(p), [A,B]);
P = randomPoint(E);
Q = randomPoint(E);
```

```

t_start = process_time()

Ep = EllipticCurve(Qp(p,2), [A,B]);
Plift = lift(P,Ep,p);
Qlift = lift(Q,Ep,p);
k = GF(p)(psi(p*Qlift)/psi(p*Plift));

t_stop = process_time()

print("k:",k,"\n")
print("Correct result:",ZZ(k)*P==Q,"\n")
print("Time:",t_stop-t_start,"seconds")

```

A.2 Auxiliary functions

```

from sage.schemes.elliptic_curves.ell_generic import generic

def lift(P,Ep,p):
    xCoord = ZZ(P[0]);
    Plift = Ep.lift_x(xCoord);

    if ZZ(Plift[1])%p != P[1]:
        Plift = -Plift;

    return Plift;

def psi(P):
    return -P[0]/P[1];

def randomPoint(E):
    P = E.random_point();
    while P.is_zero() == True:
        P = E.random_point();
    return P;

```

B Searching for anomalous curves: the program

The program below was constructed using the SageMath software package.

Remark. In the code below, one could also leave out the multiplication-by- p and always compute the cardinality. This would speed up the code for smaller primes, however, if we want to check for primes of order 2^{64} , the program below is significantly faster. This is because multiplication-by- p is more efficient than computing the cardinality.

```

get_ipython().magic('run functions.ipynb')
P = Primes();
CM = cm_j_invariants(QQ);

```

```

p = next_prime(2^64);

while True:
    K = GF(p);
    Checked = set();

    for m in range(1,100):
        for n in range(1,100):

            for e1 in range(0,2):
                for e2 in range(0,2):
                    A = (-1)^(e1)*m;
                    B = (-1)^(e2)*n;
                    a = K(A);
                    b = K(B);
                    disc = 4*a^3+27*b^2;

                    if disc != 0:
                        j = 1728*4*a^3/disc;

                    if j not in Checked and j not in CM:
                        E = EllipticCurve(K, [A,B]);
                        Checked.add(j);
                        Q = randomPoint(E);
                        R = p*Q;

                    if R.is_zero():
                        print('anomalous:', [A,B,p]);
                    elif (R+2*Q).is_zero() and E.cardinality() == p+2:

                        if K(-1).is_square():

                            for d in range(2,p):

                                if not K(d).is_square():
                                    A = d^2*a;
                                    B = d^3*b;
                                    print('anomalous:', [A,B,p]);
                                    break;
                                else:
                                    B = -b;
                                    print('anomalous:', [A,B,p]);

p = P.next(p);

```


References

- [AM94] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Avalon Publishing, 1994. ISBN: 9780813345444.
- [BG08] D. Birmajer and J.B. Gil. “Arithmetic in the ring of formal power series with integer coefficients”. In: *The American Mathematical Monthly* 115.6 (2008), pp. 541–549.
- [Bla+99] I. Blake et al. *Elliptic Curves in Cryptography*. Lecture note series. Cambridge University Press, 1999. ISBN: 9780521653749.
- [Bos+14] J.W. Bos et al. “Elliptic curve cryptography in practice”. In: *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 157–175.
- [Cer] Certicom. *The Certicom ECC Challenge*. URL: <https://www.certicom.com/content/certicom/en/the-certicom-ecc-challenge.html> (visited on 30/06/2020).
- [Coh13] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013. ISBN: 9783662029459.
- [Con15] K. Conrad. “Hensel’s lemma”. In: *Unpublished note, available at <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf>* (2015). (visited on 01/06/2020).
- [Cox89] D.A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Monographs and textbooks in pure and applied mathematics. Wiley, 1989. ISBN: 9780471506546.
- [Cse19] <https://crypto.stackexchange.com/users/49826>. Cryptography Stack Exchange. 2019. URL: <https://crypto.stackexchange.com/questions/70507/in-elliptic-curve-what-does-the-point-at-infinity-look-like/70509> (visited on 15/06/2020).
- [DH76] W. Diffie and M. Hellman. “New directions in cryptography”. In: *IEEE transactions on Information Theory* 22.6 (1976), pp. 644–654.
- [Eis13] D. Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781461253501.
- [Eve11] J.-H. Evertse. “ p -Adic Numbers”. In: *Lecture notes, Leiden University* (2011). URL: <http://www.math.leidenuniv.nl/~evertse/dio2011-padic.pdf> (visited on 20/05/2020).
- [Gou12] F.Q. Gouvea. *p -adic Numbers: An Introduction*. Universitext. Springer Berlin Heidelberg, 2012. ISBN: 9783642590580.
- [GV18] S.D. Galbraith and F. Vercauteren. “Computational problems in supersingular elliptic curve isogenies”. In: *Quantum Information Processing* 17.10 (2018), p. 265.
- [Har13] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781475738490.

- [KG13] C.F. Kerry and P.D. Gallagher. “Digital signature standard (DSS)”. In: *FIPS PUB* (2013), pp. 186–4.
- [Kob12] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Graduate Texts in Mathematics. Springer New York, 2012. ISBN: 9781461211129.
- [Kob87] N. Koblitz. “Elliptic curve cryptosystems”. In: *Mathematics of computation* 48.177 (1987), pp. 203–209.
- [Kos07] T. Koshy. *Elementary Number Theory with Applications*. Elementary Number Theory with Applications. Elsevier Science, 2007. ISBN: 9780080547091.
- [Lep+05] F. Leprévost et al. “Generating anomalous elliptic curves”. In: *Information processing letters* 93.5 (2005), pp. 225–230.
- [Maz77] B. Mazur. “Modular curves and the Eisenstein ideal”. In: *Publications Mathématiques de l’Institut des Hautes Études Scientifiques* 47.1 (1977), pp. 33–186.
- [McK99] J. McKee. “Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field”. In: *Journal of the London Mathematical Society* 59.2 (1999), pp. 448–460.
- [Mil85] V.S. Miller. “Use of elliptic curves in cryptography”. In: *Conference on the theory and application of cryptographic techniques*. Springer. 1985, pp. 417–426.
- [Mol04] R.A. Mollin. “Cryptography-A Brief History”. In: *CUBO, A Mathematical Journal* 6.1 (2004), pp. 23–44.
- [Ols76] L. Olson. “Hasse invariants and anomalous primes for elliptic curves with complex multiplication”. In: *Journal of Number Theory* 8.4 (1976), pp. 397–414.
- [SA+98] T. Satoh, K. Araki et al. “Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves”. In: *Rikkyo Daigaku sugaku zasshi* 47.1 (1998), pp. 81–92.
- [Sag20] Sage Developers. *SageMath, the Sage Mathematics Software System*. Version 9.0. <https://www.sagemath.org>. 2020.
- [Sil08] J.H. Silverman. “Lifting and elliptic curve discrete logarithms”. In: *International Workshop on Selected Areas in Cryptography*. Springer. 2008, pp. 82–102.
- [Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946.
- [Sma99] N.P. Smart. “The discrete logarithm problem on elliptic curves of trace one”. In: *Journal of cryptology* 12.3 (1999), pp. 193–196.
- [Smi20] R. Smit. “The Discrete Logarithm Problem on Supersingular Elliptic Curves”. Bachelor’s Thesis. Rijksuniversiteit Groningen, 2020.
- [ST92] J.H. Silverman and J.T. Tate. *Rational Points on Elliptic Curves*. Structure and Bonding. Springer-Verlag, 1992. ISBN: 9780387978253.
- [Top17] J. Top. *Rijksuniversiteit Groningen, Lecture Notes: Algebraic Structures*. 2017.

- [Was08] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. Discrete Mathematics and Its Applications. CRC Press, 2008. ISBN: 9781420071474.
- [Wen13] S.L. Wenberg. “Elliptic curves and their cryptographic applications”. Master’s Thesis. Eastern Washington University, 2013.
- [Win11] R. Winter. “Elliptic curves over \mathbb{Q}_p ”. Bachelor’s Thesis. Universiteit Leiden, 2011.
- [Wol20] Inc. Wolfram Research. *Mathematica*. Version 12.1. 2020. URL: <https://www.wolfram.com/mathematica>.