University of Groningen

Bachelor's Project
Mathematics

Sieving on elliptic curves

Bachelor's Project Mathematics

Author:
Thomas Dijk (S3210057)

First supervisor:
Francesca Bianchi

Second assessor:
Steffen Müller

August 29, 2020

Contents

Chapter 1

Introduction

An elliptic curve over a field K is a projective curve over K that comes equipped with a group structure. We can think of an elliptic curve over K as the set of solutions in $\mathbb{P}^2$ to an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. If we let C be an elliptic curve over the field $\mathbb{Q}$, then Mordell's theorem tells us that, under the group law on C, the set $C(\mathbb{Q})$ has the structure of a finitely generated abelian group. This gives us that the group of rational points of C over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}^r \times T$ for some non-negative integer r, which we call the rank of C, and a finite group T, which we call the torsion subgroup. Although Mordell's theorem gives us that $C(\mathbb{Q})$ is finitely generated, it may still be the case that we have infinitely many rational points on C if $r \geq 1$.

If we fix an equation for C of the form (1.1) with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, then the integral points with respect to this choice of equation are the solutions $(X, Y, 1)$ with $X, Y \in \mathbb{Z}$. We might wonder which of the rational points on C are integral points and whether there are infinitely many of them. It turns out that Siegel's theorem tells us that the set of integral points of an elliptic curve over $\mathbb{Q}$ is always finite. Nevertheless, we do not know these integral points and how many points there are.

In this project, we extend the results of Appendix A of [1]. The problem that is stated in Appendix A of [1] is as follows:

Problem: Let C be an elliptic curve over $\mathbb{Q}$ of rank 1 and trivial torsion. Given a collection of odd primes $p_1, \ldots, p_l$ of good reduction and finite subsets $S_i \subset C(\mathbb{Q}_{p_i})$, we want to show that there is no point in $C(\mathbb{Q})$ which belongs to S_i for all i.

Combining this with a technique called "quadratic Chabauty", which is discussed in the rest of [1], this would result into an algorithm to compute integral points on elliptic curves. To approach **Problem**, we combine information coming from the group structure of $C(\mathbb{Q})$ with information coming from reducing points modulo p_i and information of the logarithm function log_P on $C(\mathbb{Q}_p)$, where $P \in C(\mathbb{Q})$ denotes a generator of $C(\mathbb{Q})$ and $log_P(nP) = n$. To obtain comparable information from the different primes, the authors of [1] consider prime sequences with certain properties. For instance:

1. two odd primes p_1, p_2 of good reduction such that $p_1 | ord(red_{p_2}(P))$ and $p_2 | ord(red_{p_1}(P))$,
2. a sequence of odd primes $p_1, \ldots, p_l$ of good reduction such that $p_{i+1} | ord(red_{p_i}(P))$ for $i \in \{1, \ldots, l-1\}$ and $p_1 | ord(red_{p_l}(P))$.

In this project, we found an example where the first strategy of Appendix A of [1] fails, so we looked at a different prime pattern, namely the following case:

3. three odd primes p_1, p_2, p_3 of good reduction such that $p_1 | ord(red_{p_2}(P))$ and $p_2 | ord(red_{p_1}(P))$ and $p_1 \cdot p_2 | ord(red_{p_3}(P))$.

We are also going to prove that the assumption that the elliptic curve must be torsion free is necessary for these methods to work.

The outline of this report is as follows. In Chapter 2 of the report, we will first introduce the projective plane, which is the plane where our elliptic curves are in, and will explain more generally what algebraic curves are in it.

After this we will work towards Bezout's theorem and the Cayley-Bacharach theorem, which are important theorems for the proof of the group law of elliptic curves, which will be discussed in Chapter 3.

In Chapter 3 we show that every non-singular cubic curve over a field K with a K-rational point can be transformed with a coordinate transformation into an elliptic curve, which is a non-singular curve that satisfies the Weierstrass equation. After this, we will define addition on these elliptic curves. We also show how the addition gives an abelian group law on the curves and we will give explicit formulas to compute the coordinates of the addition of two points. At the end of this chapter we will also state Mordell's theorem and Siegel's theorem.

Before we can start sieving p-adic points on elliptic curves, we first have to take a look at some basics about elliptic curves over finite fields $\mathbb{F}_p$ and elliptic curves over the set of p-adic numbers. After this, we introduce the reduction modulo p map and the logarithm map, which are important maps that we need to sieve the potential integral points that we get after using quadratic Chabauty for several primes.

In the last chapter, we will discuss the three sieving methods (1,2,3 above) and provide examples for them. In this chapter, we will also prove that the elliptic curve must be torsion free for these methods to work.

At the end of the report one can find a code in Sagemath that is used to find the integral points on elliptic curves of rank 1 and with trivial torsion for the first and third case.

Chapter 2

Projective plane and projective curves

In this thesis, we are mostly working with elliptic curves. Before we can do that, we have to define the projective plane and algebraic curves in it. This has to be done because an elliptic curve is an algebraic curve in the projective plane. In this chapter we are going to define projective planes, projective curves and talk about intersection points of projective curves. To do this, we will mostly follow [5, Section 1.1], [10, Chapter 1], [11, Section I.2] and [12, Appendix A.1, A.2 and A.3].

2.1 Projective Plane

In this section, we will introduce two constructions of the projective plane, one algebraic and one geometric. A projective plane is defined over a field K. We define a field as follows:

Definition 2.1.1. [3, Definition 0.66] Let K be a set with two binary operations $+, \times$. K is a *field* if:

1. $(K, +, 0)$ is an abelian group,
2. $(K\backslash\{0\}, \times, 1)$ is an abelian group,
3. For all $a, b \in K$, we get $a \times (b + c) = a \times b + a \times c$.

The fields we are mostly working with are $\mathbb{Q}$, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Q}_p$, where p is prime. For any field K, we let K^* denote the group of nonzero elements of K under $\times$. We say that a field is *algebraically closed* if every non-constant polynomial $p(x) \in K[x]$ contains a root in K. Note that for every field K there exists a field $\bar{K}$, which is called the *algebraic closure* of K, which is the smallest algebraically closed field that contains K.

Now that we have defined what a field is, we are almost able to give the algebraic definition of a projective plane over a field. But before we can do that, we need an equivalence relation. We call two coordinates (a, b, c) and (a', b', c'), where all entries are elements in $\bar{K}$, with a, b, c not all zero and a', b', c' not all zero, equivalent to each other if there exists a non-zero $t \in \bar{K}^*$ such that $a = ta', b = tb', c = tc'$. By $[a, b, c]$ we denote the equivalence class $\{(ta, tb, tc) : t \in \bar{K}^*\}$. We can now use this equivalence relation to define the projective plane.

Definition 2.1.2. The *projective plane over* K, denoted by $\mathbb{P}^2(\bar{K})$, is the set of equivalence classes of coordinate triples $[a, b, c]$ with $a, b, c \in \bar{K}$ not all zero. So we have that

$$\mathbb{P}^2(\bar{K}) := \frac{\{[a, b, c] : a, b, c \in \bar{K} \text{ are not all zero}\}}{\sim}.$$

We will call the elements a, b, c the *homogeneous coordinates* for the point $[a, b, c]$ in $\mathbb{P}^2(\bar{K})$. If it is clear what field we are using, we might write $\mathbb{P}^2$ instead of $\mathbb{P}^2(\bar{K})$. The set of *K-rational points* in $\mathbb{P}^2(\bar{K})$ is defined to be the set

$$\mathbb{P}^2(K) := \{[a, b, c] \in \mathbb{P}^2 : \exists\, (e, f, g) \in K^3 \text{ with } [a, b, c] = [e, f, g]\}.$$

On a similar way we can define

$$\mathbb{P}^1(\bar{K}) := \frac{\{[a,b] : a,b \in \bar{K}, \text{ are not both zero}\}}{\sim},$$

where $[a,b] \sim [a',b']$ if there is a $t \in \bar{K}^*$ such that $a = ta'$ and $b = tb'$, which is useful for the second definition of the projective plane.

The second way to look at the projective plane is called the geometric definition of the projective plane. We can look at the projective plane $\mathbb{P}^2(\bar{K})$ as $\mathbb{A}^2(\bar{K}) \cup \mathbb{P}^1(\bar{K})$, where $\mathbb{A}^2(\bar{K})$ denotes the Euclidean plane (also called the affine plane) over K. To see this, we follow [5, Remark 1.1.5]. Note that

$$\mathbb{P}^2(\bar{K}) = \frac{\{[a,b,c] : a,b,c \in \bar{K}, c \neq 0\}}{\sim} \bigcup \frac{\{[a,b,0] : a,b \in \bar{K}, a,b \text{ are not both zero}\}}{\sim}.$$

We will denote this as $U \cup V$, where

$$U = \frac{\{[a,b,c] : a,b,c \in \bar{K}, c \neq 0\}}{\sim} \text{ and } V = \frac{\{[a,b,0] : a,b \in \bar{K}, a,b \text{ are not both zero}\}}{\sim}.$$

From U, we can make a map $\phi : U \to \mathbb{A}^2(\bar{K})$, where $\phi([a,b,c]) = (\frac{a}{c}, \frac{b}{c})$. We can also make a map $\psi : \mathbb{A}^2(\bar{K}) \to U$ where $\psi((a,b)) = [a,b,1]$. Note that ϕ and ψ are well defined maps which are inverse to each other. Hence we can identify U as $\mathbb{A}^2(\bar{K})$. For V, we can easily see that the correspondence $V \leftrightarrow \mathbb{P}^1(\bar{K}) : [a,b,0] \leftrightarrow [a,b]$ is well defined and bijective. Now we will give a geometric meaning to the algebraic definition described above. As stated above, we first identify U to be $\mathbb{A}^2(\bar{K})$, whereas V is identified with $\mathbb{P}^1(\bar{K})$. The maps that give this relation are represented by Figure 2.1.

Algebraic definition of $\mathbb{P}^2$		Geometric definition of $\mathbb{P}^2$
$\frac{\{[a,b,c] : a,b,c \text{ not all zero}\}}{\sim}$	$\longleftrightarrow$	$\mathbb{A}^2 \cup \mathbb{P}^1$
$[a,b,c]$	$\longrightarrow$	$\begin{cases} (a/c, b/c) \in \mathbb{A}^2 & \text{if } c \neq 0 \\ [a,b] \in \mathbb{P}^1 & \text{if } c = 0 \end{cases}$
$[x,y,1]$	$\longleftarrow$	$(x,y) \in \mathbb{A}^2$
$[A,B,0]$	$\longleftarrow$	$[A,B] \in \mathbb{P}^1$

Figure 2.1: Maps identifying the two descriptions of $\mathbb{P}^2$ [12, Table A.1].

So we now have that the projective plane can be seen as the affine plane together with some extra points, which we call *points at infinity*. These points are given in such a way that two parallel lines will intersect in one of these points. But now we want to know how many of these extra points we need. Would it be sufficient to add only one extra point P? To check this, we take two parallel lines L_1 and L_2 and let them intersect in the extra point P. If we now take two other parallel lines L_1' and L_2' such that they are not parallel to L_1 and L_2, then we let them intersect in P'. Since L_1 and L_1' are not parallel, we get that they intersect in the affine plane. We will denote this intersection with Q. If we added only one point at infinity, then we would have that $P = P'$, which makes L_1 and L_1' intersect in two different points, namely $P = P'$ and Q, where $Q \neq P$. But two lines only have one intersection point, so it is not enough to have only one point at infinity. Instead of one extra point, we need to add an extra point for every direction in the affine plane. All the points at infinity themselves also give a line, which we will call the *line at infinity*. This line will be denoted by L_∞.

2.2 Curves in the projective plane

Now that we have defined what the projective plane is, we can define curves on the plane. But first, let us recall the definition of a curve in the affine plane.

Definition 2.2.1. In the affine plane $\mathbb{A}^2$ over a field K, we define an *affine algebraic curve over* K as the set of solutions of a non-constant polynomial equation $f(x, y) = 0$ in two variables with coefficients in K, so $C_0(\bar{K}) := \{(x, y) \in \mathbb{A}^2(\bar{K}) : f(x, y) = 0\}$.

We will now define a curve in the projective plane, but before we can do that, we have to state that if a polynomial with three variables with coefficients in K satisfies $F(tX, tY, tZ) = t^d F(X, Y, Z)$ for every non-zero t, then we say that F is a *homogeneous polynomial of degree* d. Since we have that a point $[a, b, c] = [ta, tb, tc]$ for any nonzero t, we need that the polynomial representing a projective curve should be homogeneous.

Definition 2.2.2. In the projective plane $\mathbb{P}^2$ over a field K, we define a *projective algebraic curve over* K as the set of solutions of a non-constant homogeneous polynomial equation $F(X, Y, Z) = 0$ in three variables with coefficients in K, so $C(\bar{K}) := \{[a, b, c] \in \mathbb{P}^2(\bar{K}) : F(a, b, c) = 0\}$. We say that C is a curve of degree d if F is a polynomial of degree d. If it is clear that we are working in $\mathbb{P}^2(\bar{K})$, we might just call the curve C instead of $C(\bar{K})$.

Note that affine algebraic curves can be mapped to projective algebraic curves. This can be done by homogenization, which we define as follows.

Definition 2.2.3. Let $f(x, y) = \sum_{i,j} a_{i,j} x^i y^j$ be a polynomial of degree d. Then the *homogenization* of f is defined as $F(X, Y, Z) = \sum_{i,j} a_{i,j} X^i Y^j Z^{d-i-j}$.

From this definition it is easy to see that F is homogeneous of degree d. Note that $F(X, Y, 0)$ is not identically zero, so we obtain that $F(X, Y, Z)$ does not fully contain the line at infinity.

It is also possible to invert this process. This process is called dehomogenization, which we define as follows.

Definition 2.2.4. Let $F(X, Y, Z)$ be a homogeneous polynomial of degree d. Then the *dehomogenization* of F with respect to Z is defined as $f(x, y) = F(x, y, 1)$. Here, we call $C_0 : f(x, y) = 0$ the *affine part* of the projective curve C, where $C : F(X, Y, Z) = 0$.

Note that it is also possible to dehomogenize with respect to the variables X and Y. Then the dehomogenizations are given by $f(y, z) = F(1, y, z)$ and $f(x, z) = F(x, 1, z)$. This is sometimes useful to do if we are interested in a specific point at infinity on the projective curve C. By dehomogenizing with respect to different variables, we split a projective curve C into distinct overlapping affine parts. If we combine the affine parts, we get the entire projective curve.

Since the points $[a, b, 0] \in C$ are not a part of the affine part of the curve, we now would like to know how we could interpret these point in terms of the affine part of the curve. In the projective plane, we had that these points $[a, b, 0]$ are sent to the points at infinity $[a, b] \in \mathbb{P}^1$. Our claim is that these points are the tangent directions of the affine curve if we move towards infinity.

In the study of number theory, we are interested in finding solutions of polynomial equations where the coordinates are in $\mathbb{Q}$, or even $\mathbb{Z}$. To do this, it is useful to take a look at curves where the coefficients and solutions of our curve have specific properties.

We call a curve a rational curve if it is a curve over $\mathbb{Q}$. Note that for any rational curve, we are able to clear the denominators of all coefficients since the solutions of $F(X, Y, Z) = 0$ and $cF(X, Y, Z) = 0$ are

the same for some non-zero c. This gives us that any rational curve can be written as the zero set of a polynomial with integer coordinates.

Definition 2.2.5. Let $C : F(X, Y, Z) = 0$ be a projective curve over a field K. Then we define the *set of K-rational points on C*, denoted by $C(K)$, as

$$C(K) = \{[a, b, c] \in \mathbb{P}^2(K) : F(a, b, c) = 0\}.$$

If we take a look at the affine part of a projective curve, then we let $C_0(K)$ denote the set of K-rational points on $C_0 : f(x, y) = 0$, which is given by

$$C_0(K) = \{(x, y) \in \mathbb{A}^2(\bar{K}) : f(x, y) = 0 \text{ and } x, y \in K\}.$$

Note that we have that $C(K)$ consists of $C_0(K)$ together with the K-rational points at infinity.

If we let C_0 be an affine curve over $\mathbb{Q}$, then we can define the *set of integer points of C*, which we denote by $C_0(\mathbb{Z})$, as

$$C_0(\mathbb{Z}) = \{(x, y) \in \mathbb{A}^2 : f(x, y) = 0 \text{ and } x, y \in \mathbb{Z}\}.$$

These points are also called *integral points*.

2.3 Intersections of Projective Curves

Recall that the the projective plane was constructed in such a way that any two distinct lines would intersect in exactly one point. Now we would like to know how curves of higher degree intersect. Bezout's theorem will tell us the answer to this, but we first have to define a few concepts. The first concept that we will introduce is the one for singular points.

Definition 2.3.1. Let $C : F(X, Y, Z) = 0$ be a projective curve over a field K and let $P = [a, b, c]$ be a point on C. We call P a *singular point* of C if $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$. Otherwise P is called a *non-singular point* of C. If all points of C are non-singular, we call C a *non-singular curve*.

The second concept that has to be introduced is the one of irreducible polynomials.

Definition 2.3.2. Let $C : F(X, Y, Z) = 0$ be a projective curve over a field K. Then we are able to factor F into a product of irreducible polynomials, so

$$F(X, Y, Z) = p_1(X, Y, Z) \cdot p_2(X, Y, Z) \cdots p_n(X, Y, Z).$$

Then we call $p_1(X, Y, Z) = 0, \ldots, p_n(X, Y, Z) = 0$ the *irreducible components of the curve C*. If F is an irreducible polynomial itself, we say that the curve C is irreducible. We say that two curves C_1 and C_2 *have no common components* if they have no common irreducible component.

Now that we have the needed definitions, we can work towards Bezout's theorem. But before we will give Bezout's theorem, we will first take a look at what one might expect to happen.

First suppose that we have two projective curves $C_1 : F_1(X, Y, Z) = 0$ and $C_2 : F_2(X, Y, Z) = 0$ of degree d_1 and d_2 respectively with no common components. Now let $P = (X_0, Y_0, Z_0)$ be an intersection point of C_1 and C_2. Then we can compute the multiplicity of the intersection by some association with the affine curve. Since $P \in \mathbb{P}^2$, we have that at least one of X_0, Y_0, Z_0 is non-zero. If we assume that $Z_0 \neq 0$, then the multiplicity of the intersection of P in $\mathbb{P}^2$ is the same as the one of $(\frac{X_0}{Z_0}, \frac{Y_0}{Z_0})$ on the affine curves $(C_1)_0 : f_1(x, y) = F_1(x, y, 1) = 0$ and $(C_2)_0 : f_2(x, y) = F_2(x, y, 1) = 0$, where $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. Note that the curves $(C_1)_0$ and $(C_2)_0$ also have no common components. In the case where $Z_0 = 0$ we do the same as before, but then with $X_0 \neq 0$ or $Y_0 \neq 0$, but without loss of generality, we will only look at the case where

$Z_0 \neq 0$.
In the affine part, we now have that $(C_1)_0 \cap (C_2)_0$ are the points (x, y) such that $f_1(x, y) = f_2(x, y) = 0$. If we first look at f_1 as a polynomial of y with coefficients as polynomials in x, we should get that it has d_1 roots $y_1, \dots y_{d_1}$ in $\bar{K}$. By substituting the solutions in f_2, one gets d_1 equations for x. Each of these solutions should have d_2 solutions, because each equation is a polynomial in x of degree d_2. This gives us in total $d_1 d_2$ pairs (x, y) such that $f_1(x, y) = f_2(x, y) = 0$. This is the case if we allow coordinates in $\bar{K}$ and count the intersection multiplicity of solutions correctly.

We can almost state Bezout's theorem, but before we do that we have to assign for every point $P \in \mathbb{P}^2$ and curves C_1 and C_2 with no common component an *intersection index* $I(C_1 \cap C_2, P)$. A formal definition of $I(C_1 \cap C_2, P)$ is given on page 295 of [12], but we will only use three properties to sketch an idea of what it is.

1. $I(C_1 \cap C_2, P) = 0$ if $P \notin C_1 \cap C_2$,
2. $I(C_1 \cap C_2, P) = 1$ if $P \in C_1 \cap C_2$, P is a non-singular point of C_1 and C_2, and C_1 and C_2 do not have the same tangent directions at P.
3. $I(C_1 \cap C_2, P) \geq 2$ if $P \in C_1 \cap C_2$ and P is either a singular point of C_1 or C_2, or C_1 and C_2 have the same tangent direction at P.

We can state Bezout's theorem by using the intersection index.

Theorem 2.3.1. *(Bezout's Theorem) [10, Theorem 1.9]. Let C_1 and C_2 be two projective curves over a field K of degree d_1 and d_2 respectively, with no common components. Then*

$$\sum_{P \in C_1(K) \cap C_2(K)} I(C_1 \cap C_2, P) \leq d_1 \cdot d_2.$$

If our field K is algebraically closed, then we will always get equality.

This theorem tells us for example that a cubic curve over K, which is a curve with degree three, and a line over K will have three intersection points, provided that the line is not a component of the cubic curve. This will be useful for the proof of the group law on elliptic curves.

Another important theorem for the proof of the group law of elliptic curves is the Cayley-Bacharach Theorem, which is stated as follows:

Theorem 2.3.2. *(Cayley-Bacharach Theorem) [12, Theorem A.2] Assume that C_1 and C_2 are two projective curves over K of degree d_1 and d_2 respectively with no common components. Assume that the curves intersect in $d_1 d_2$ distinct points. Now let C_3 be another projective curve over K of degree $d_1 + d_2 - 3$ which goes through $d_1 d_2 - 1$ points of the intersection of C_1 and C_2. Then it follows that C_3 also passes through the last intersection point of C_1 and C_2.*

Note that some points might appear with higher multiplicity, so not all intersection points have to be different. If we apply the Cayley-Bacharach theorem to two cubic curves C_1 and C_2 with 9 intersection points $P_1, \dots P_9$, we will get that if a third cubic curve C_3 goes through 8 of the intersection points $P_1, \dots P_8$, then it will also go through P_9.

Chapter 3

Group law on elliptic curves

In this chapter, we are going to define an elliptic curve is, which is a curve with an explicitly defined group law, which we will introduce. We will also give explicit formulas to calculate the addition of two points of the elliptic curve.

3.1 Elliptic curves

In this section, we are going to define elliptic curves. It is also possible to put elliptic curves in a specific form, which we call the Weierstrass normal form, we will show this later in this section.

Definition 3.1.1. Let K be a field. Then we define an *elliptic curve* over K, denoted by $C(\bar{K})$, to be a non-singular projective curve over K with an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. We call equation (3.1) a *Weierstrass equation*.

It is also possible to put equation (3.1) in its affine form. Then we get $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, which only has one point at infinity. This point can be found by taking the intersections of the homogeneous equation with the line at infinity $Z = 0$. If we now substitute $Z = 0$ into the homogeneous equation, we are left with $X^3 = 0$, which has a triple root at $X = 0$. From this we get that there is only one point at infinity, which is represented by $[0, 1, 0]$. Note that, for all $a_1, a_2, a_3, a_4, a_6 \in K$, we have that $[0, 1, 0]$ is always a solution of equation (3.1).

It is important to know that any non-singular cubic curve with a K-rational point can be transformed into an elliptic curve. This can be done by a coordinate transformation. But before we can show this, we have to give a formula for the tangent line of a projective curve.

Definition 3.1.2. Let $C : F(X, Y, Z) = 0$ be a non-singular curve with point $P = [a, b, c]$. Then the *tangent line* of F at P is given by

$$\frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y + \frac{\partial F}{\partial Z}(P) \cdot Z = 0.$$

We will now show that any cubic curve can be transformed into an elliptic curve. To do this, we follow [6] together with [12, Section 1.3]. Let us begin with an affine cubic curve given by $f(u, v) = 0$ with a K-rational point $P = (\frac{a}{c}, \frac{b}{c})$. The first step that we make is to put the curve in homogeneous form $C : F(U, V, W) = 0$. The next step is to find the tangent line of C at P. We will apply a coordinate transformation so that the tangent line to C at P is given by $Z = 0$ in our new coordinate system.

By Bezout's Theorem (Theorem 2.3.1), we get that the tangent line should also intersect the curve in

another point, which we will call Q. Now we have to find the tangent line of C at Q and make this $X = 0$ in our new coordinate system. This gives us that $Q = [0, 1, 0]$ in the new coordinate system. All we have to do now is take an arbitrary line through P that is not the tangent line, and choose it to be the axis $Y = 0$. This gives us that $P = [1, 0, 0]$ in our new coordinate system. From this coordinate transformation we get a curve of the form $C' : F'(X, Y, Z) = F'(m_1U + m_2V + m_3W, m_4U + m_5V + m_6W, m_7U + m_8V + m_9W) = 0$, where m_i are chosen in such a way that all the above holds. Note that C' contains $P = [1, 0, 0]$ and $Q = [0, 1, 0]$, and that the coordinate transformation gives a one-to-one correspondence between $C(K)$ and $C'(K)$ if all m_i are K-rational. Hence the problem of finding K-rational points on C is equivalent to finding the K-rational points in C'.

C' is still a cubic curve, so we can write it as

$$C' : F'(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hxZ^2 + iYZ^2 + jZ^3 = 0,$$

where it follows that a, b and d are zero, which we will show now. Since $[1, 0, 0]$ and $[0, 1, 0]$ are on the curve, we get that $F'(1, 0, 0) = a = 0$ and $F'(0, 1, 0) = d = 0$. If we take the intersection of C' with $Z = 0$, we get that it intersects twice in P and once in Q, which are the roots of the equation $F'(X, Y, 0) = XY(bX + cY) = 0$ (we already know that a and d are zero). Since $F'(X, Y, 0)$ intersects the curve twice in P and once in Q, it follows that Q satisfies $X = 0$ and that P satisfies $Y = 0$ and $bX + cY = 0$. If we substitute the first relation satisfied by P into the second one, we get that $b = 0$. This gives us that

$$C' : F'(X, Y, Z) = cXY^2 + eX^2Z + fXYZ + gY^2Z + hxZ^2 + iYZ^2 + jZ^3 = 0,$$

The next step is to dehomogenize C' with respect to Z. So by taking $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ and dividing both sides with c, we get that the equation of C' becomes of the following form

$$f(x, y) = xy^2 + a'x^2 + b'xy + c'y^2 + d'x + e'y + f' = 0.$$

This can be rewritten as follows.

$$f(x, y) = (x + c')y^2 + a'x^2 + b'xy + d'x + e'y + f' = 0.$$

If we substitute $x = (x' - c')$ and shuffle a bit, we get a equation of the form

$$x'y^2 + (a''x' + b'')y = c''x'^2 + d''x' + e''.$$

By multiplying the whole equation by x' and then substituting $y = \frac{y'}{x'}$, we get

$$y'^2 + (a''x' + b'')y' = c''x'^3 + d''x'^2 + e''x'.$$

If we now substitute $y' = (c'')^2y''$ and $x' = c''x''$, divide by $(c'')^4$ and then homogenize the resulting equation, we obtain that our curve is indeed of the form $C' : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$.

If the characteristic of K is different from 2 and 3, then it is also possible to write our Weierstrass equation in a simpler affine form, which we call the *Weierstrass normal form*, given by $y^2 = x^3 + Ax + B$. This equation is obtained by first dehomogenizing with respect to Z, which gives us

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6.$$

If we complete the square on the left hand side, we obtain that

$$\left(y + \frac{1}{2}(a_1x + a_3)\right)^2 = x^3 + a_2x^2 + a_4x + a_6 + \frac{1}{4}(a_1x + a_3)^2.$$

By substituting $y = y' - \frac{1}{2}(a_1x + a_3)$, one gets

$$y'^2 = x^3 + (a_2 + \frac{1}{4}a_1^2)x^2 + (a_4 + \frac{1}{2}a_1a_3)x + a_6 + \frac{1}{4}a_3^2.$$

To get rid of the x^2 term, one can substitute $x = x' - \frac{4a_2+a_1^2}{12}$ to get

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

An example might make things clearer.

Example 3.1.1. Let us start with the cubic curve over $\mathbb{Q}$ given by

$$y^2 + xy + y = x^3 + x^2 - 21x - 45.$$

If we complete the square on the left hand side, we get that

$$\left(y + \frac{1}{2}(x+1)\right)^2 = x^3 + x^2 - 21x - 45 + \frac{1}{4}(x+1)^2 = x^3 + \frac{5}{4}x^2 - \frac{41}{2}x - \frac{179}{4}.$$

If we now substitute $y = y' - \frac{1}{2}(x+1)$ and $x = x' - \frac{5}{12}$, one finds

$$\begin{aligned} y'^2 &= (x' - \frac{5}{12})^3 + \frac{5}{4}(x' - \frac{5}{12})^2 - \frac{41}{2}(x' - \frac{5}{12}) - \frac{179}{4} \\ &= x'^3 + (-\frac{5}{4} + \frac{5}{4})x^2 + (\frac{75}{144} - \frac{25}{24} - \frac{41}{2})x' - \frac{125}{1728} + \frac{125}{576} + \frac{205}{24} - \frac{179}{4} \\ &= x'^3 - \frac{1009}{48}x' - \frac{31159}{864}, \end{aligned}$$

which is in the form $y^2 = x^3 + Ax + B$. It is also possible to obtain an equation with integral A and B. This is done by substituting $y = \frac{y'}{36}$ and $x = \frac{x'}{216}$ and then multiplying the whole equation by 6^6. By doing this, one obtains

$$y^2 = x^3 - 27243x - 1682586.$$

In general the rational points on one curve have a one-to-one correspondence with the rational points of another curve that is obtained by a coordinate transformation defined over $\mathbb{Q}$, so we get that the problem of rational points on a general cubic curve having a rational point is reduced to studying rational points on cubic curves in Weierstrass normal form.

3.2 Group Law on elliptic curves

In this section, we are going to define a group law for elliptic curves geometrically. We will do this by following the composition law $*$ from [11, Section III.2]. Note that $*$ is denoted as $\oplus$ in [11].

First, let C be an elliptic curve over K given by

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. The affine part of this curve is given by

$$C_0 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Note that C_0 contains every point of C, except the point at infinity $[0, 1, 0]$. We are going to define a group law with identity element $\mathcal{O} = [0, 1, 0]$, since it is on every elliptic curve C. Note that this point is a K-rational point, for every field K.

Now that we have an identity element, we can define addition of the two points $P_1 := (x_1, y_1)$ and $P_2 := (x_2, y_2)$ on elliptic curves, where $P_3 = P_1 + P_2 = (x_3, y_3)$. We will do this for all distinct cases, which are stated as follows:

1. P_1 and P_2 are not the point at infinity, $P_1 \neq P_2$ and $x_1 \neq x_2$,
2. P_1 and P_2 are not the point at infinity, $P_1 = P_2$,
3. P_1 and P_2 are not the point at infinity, $x_1 = x_2$ and $y_1 \neq y_2$,
4. P_1 and P_2 are both the point at infinity,
5. exactly one of P_1 and P_2 is the point at infinity.

Case 1: If we want to find $P_3 := P_1 + P_2$ for two points P_1 and P_2 on the elliptic curve where P_1 and P_2 are not the point at infinity, $P_1 \neq P_2$ and $x_1 \neq x_2$, we will first take the line through P_1 and P_2. From Bezout's theorem (Theorem 2.3.1) it follows that this line has a third intersection point with the curve in the projective plane, if we count multiplicities. Since P_1 and P_2 are affine points and since $x_1 \neq x_2$, it follows that the third intersection point is also affine. We will call this point $P_1 * P_2$. Note that if P_1 and P_2 are defined over K, it follows that $P_1 * P_2$ is also defined over K. If we now take the line through $P_1 * P_2$ and $\mathcal{O}$, which is the vertical line through $P_1 * P_2$, it follows again by Bezout's theorem (Theorem 2.3.1) that this line has a third intersection point with the curve in the projective plane, counting multiplicities. Again, since P_1 and P_2 are affine points and since $x_1 \neq x_2$, it follows that the third intersection point is also affine. This point will be denoted by $P_3 = P_1 + P_2 := (P_1 * P_2) * \mathcal{O}$. Note that if P_1 and P_2 are defined over K, then it follows that P_3 is also defined over K. Since the line through P_1 and P_2 is the same as the line through P_2 and P_1, it follows that $P_1 + P_2 = P_2 + P_1$, which will make the group law commutative.

Case 2: If we want to find P_3 where $P_1 = P_2$ in the affine plane, we will first take the tangent line of the curve at P_1. From Bezout's theorem (Theorem 2.3.1), it follows that this line intersects at another point, if we count multiplicities. We denote this point by $P_1 * P_1$. Then we again take the line through $P_1 * P_1$ and $\mathcal{O}$ and take the third intersection to be $P_1 + P_1 = 2P_1$. Note that if the tangent line of C at P_1 is vertical, then we get that $P_1 + P_1 = \mathcal{O}$.

Case 3: It is also a possibility for two affine points P_1 and P_2 that the x-coordinates are the same, but that the y-coordinates are different. In this case we have that $P_1 * P_2 = \mathcal{O}$. Now we have to take the line through $\mathcal{O}$ and $\mathcal{O}$, which is the line at infinity. This line again intersects in the point $\mathcal{O}$, since it is the only point at infinity on the curve. Then we get that $P_1 + P_2 = \mathcal{O} * \mathcal{O} = \mathcal{O}$.

Case 4: In the rare case that $P_1 = P_2 = \mathcal{O}$, it follows that $P_1 + P_2 = \mathcal{O}$, by the same reasoning as in case 3.

Note that the cases 2, 3 and 4 show that every point P_1 of the curve has an inverse point on the curve $(-P_1)$, such that $P_1 + (-P_1) = \mathcal{O}$, where the inverse of $P_1 \neq \mathcal{O}$ is the point with the same x-coordinate.

Case 5: Now we will take a look at the case where exactly one of P_1 and P_2 is the point at infinity. Assume, without loss of generality, that $P_1 = \mathcal{O}$. Then the line through $\mathcal{O}$ and P_2 is the vertical line through P_2, which intersects in $\mathcal{O} * P_2$. If we now again take the vertical line through $\mathcal{O} * P_2$ and $\mathcal{O}$, we find that $\mathcal{O} + P_2 = (\mathcal{O} * P_2) * \mathcal{O} = P_2$. Since the group law is commutative it follows that $\mathcal{O} + P_2 = P_2 + \mathcal{O} = P_2$, so $\mathcal{O}$ is indeed the identity element.

To prove that the addition really is an abelian group law, we have to prove that + has closure and that it is associative. By the way how we defined the addition it directly follows that adding point of an elliptic curve returns to another point on the curve, which gives us that + has closure. So the only thing left to prove that + really defines an abelian group law is to prove that + is associative. For + to be associative, we need that $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. Note that $(P_1 + P_2) + P_3 = ((P_1 + P_2) * P_3) * \mathcal{O}$ and $P_1 + (P_2 + P_3) = (P_1 * (P_2 + P_3)) * \mathcal{O}$, so to prove that + is associative, it is sufficient to prove that $(P_1 + P_2) * P_3 = P_1 * (P_2 + P_3)$. To get $(P_1 + P_2) * P_3$, we first need $P_1 + P_2$, which is the third intersection of the line through $P_1 * P_2$ and $\mathcal{O}$. By taking the third intersection of the line through $(P_1 + P_2)$ and P_3, we find $(P_1 + P_2) * P_3$. In a similar way, we can find $P_1 * (P_2 + P_3)$. Figure 3.1 gives a visualization of the

lines that are needed to find $(P_1 + P_2) * P_3$ and $P_1 * (P_2 + P_3)$ for the curve $y^2 = x^3 - 8x + 4$ over $\mathbb{R}$. We can now see that the points

$$\mathcal{O}, P_1, P_2, P_3, P_1 * P_2, P_1 + P_2, P_2 * P_3, P_2 + P_3 \tag{3.2}$$

are all on a dashed line and a solid line ($\mathcal{O}$ is on a dashed line and a solid line because we have a dashed vertical line and a solid vertical line). To see if $(P_1 + P_2) * P_3 = P_1 * (P_2 + P_3)$, we have to check whether the line through $P_1 + P_2$ and P_3 intersect the curve at the same point as the line through P_1 and $P_2 + P_3$. Note that each line is given by a linear equation. If we now define C_1 to be the curve obtained by multiplying the three linear equations of the solid lines and C_2 to be the curve obtained by multiplying the three linear equations of the dashed lines, we get that C_1 and C_2 are two cubic curves with no common component and nine intersection points, namely the eight of (3.2) and the intersection of the line through $P_1 + P_2$ and P_3 and the line through P_1 and $P_2 + P_3$. Since C goes through the eight points listed in (3.2), it follows from Cayley-Bacharach theorem (Theorem 2.3.2) that C must also go through the ninth intersection. From this it follows that $(P_1 + P_2) * P_3 = P_1 * (P_2 + P_3)$, which proves that $+$ is indeed associative, so $+$ really defines an abelian group law.

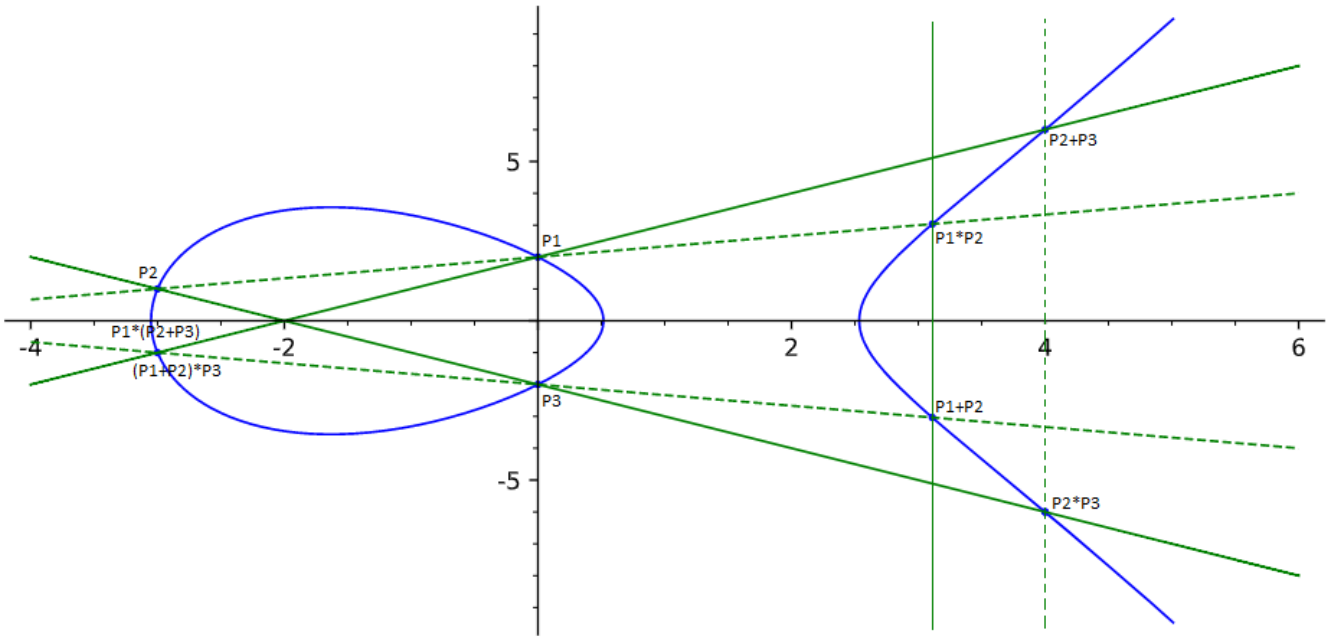

Figure 3.1: Visualization of Associativity law of the elliptic curve $y^2 = x^3 - 8x + 4$ over $\mathbb{R}$.

3.3 Explicit formulas

Now that we have defined a group law on elliptic curves, one might ask whether or not there are explicit formulas to compute $-P_1$ and $P_3 = P_1 + P_2$ for the elliptic equation. The answer is yes, but there are a few different cases we have to keep in mind [11, Group Law Algorithm 2.3]. A few of these cases were already discussed when we defined the addition law, namely the cases where $P_2 = -P_1$ and the one where at least one of P_1 and P_2 was the point at infinity. In the following part, we will not be looking at those cases.

First we want to find for any point $P_1 = (x_1, y_1) \in C - \mathcal{O}$ the point $-P_1 = (x_{-1}, y_{-1}) \in C$. We already know that P_1 and $-P_1$ have the same x-coordinate, so $x_{-1} = x_1$. If we substitute this coordinate in C_0, one gets

$$y^2 + a_1 x_1 y + a_3 y = x_1^3 + a_2 x_1^2 + a_4 x_1 + a_6.$$

Bringing everything to one side gives

$$y^2 + (a_1x_1 + a_3)y - x_1^3 - a_2x_1^2 - a_4x_1 - a_6 = 0.$$

This equation has two roots, namely y_1 and y_{-1}, so

$$y^2 + (a_1x_1 + a_3)y - x_1^3 - a_2x_1^2 - a_4x_1 - a_6 = (y - y_1)(y - y_{-1}).$$

If we look at the coefficient in front of the y term, we get that

$$a_1x_1 + a_3 = -y_1 - y_{-1}.$$

From this it follows that

$$y_{-1} = -y_1 - a_1x_1 - a_3.$$

This gives us that $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$.

We are now going to find the explicit formulas for $P_3 = P_1 + P_2$, where $P_i = (x_i, y_i) \in C_0$, for $i = 1, 2, 3$ and $P_i * P_j = (x_{i,j}, y_{i,j}) \in C_0$ for $i, j = 1, 2$. To do this, we have to distinguish between two cases, one for which $P_1 \neq P_2$ and one for which $P_1 = P_2$, where in both cases we have that $P_1 \neq -P_2$ and neither P_1 nor P_2 is the point at infinity.
We will first take a look at the case $P_1 \neq P_2$. Then the line through P_1 and P_2 is given by the equation

$$y = \lambda x + \mu, \text{ where } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \mu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

If we now substitute $y = \lambda x + \mu$ into the equation, we get

$$(\lambda x + \mu)^2 + a_1x(\lambda x + \mu) + a_3(\lambda x + \mu) = x^3 + a_2x^2 + a_4x + a_6.$$

If we bring everything to one side, we can find that

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

This equation has three roots, namely x_1, x_2 and $x_{1,2}$, so

$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\mu - a_3\lambda)x + a_6 - \mu^2 - a_3\mu = (x - x_1)(x - x_2)(x - x_{1,2}).$$

If we now look at the coefficient in front of the x^2 term, we see that

$$a_2 - \lambda^2 - a_1\lambda = -x_1 - x_2 - x_{1,2}.$$

From this it follows that

$$x_{1,2} = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{and} \quad y_{1,2} = \lambda x_{1,2} + \mu.$$

Since P_3 is the inverse of $P_{1,2}$ it follows that $x_3 = x_{1,2} = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ and $y_3 = -y_{1,2} - a_1x_{1,2} - a_3 = -\lambda x_3 - \mu - a_1x_3 - a_3$.

Before we discuss the case where $P_1 = P_2$, we are going to make an observation. Recall that C_0 is given by the equation

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

If we take the derivative on both sides with respect to x, we get that

$$2y\frac{dy}{dx} + a_1y + a_1x\frac{dy}{dx} + a_3\frac{dy}{dx} = 3x^2 + 2a_2x + a_4.$$

By bringing the $\frac{dy}{dx}$ terms to the left hand side and the other terms to the right hand side, we get that

$$(2y + a_1x + a_3)\frac{dy}{dx} = 3x^2 + 2a_2x + a_4 - a_1y.$$

From this we can obtain that

$$\frac{dy}{dx} = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}.$$

Now we are ready to find $P_3 = P_1 + P_2$ for the case where $P_1 = P_2$. In this case, we will call $P_3 = 2P_1$. The "line through" P_1 and P_2, is the tangent line to the cubic at P_1, which is given by the equation $y = \lambda x + \mu$, where

$$\lambda = \left.\frac{dy}{dx}\right|_{P_1} = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

The remaining formulas are the same as the case where $P_1 \neq P_2$, so $\mu = y_1 - \lambda x_1$, $x_3 = \lambda^2 + a_1\lambda - a_2 - 2x_1$ and $y_3 = -\lambda x_3 - \mu - a_1x_3 - a_3$.

3.4 Mordell's Theorem and Siegel's Theorem.

As stated before, we are interested in finding the integral points of elliptic curves over $\mathbb{Q}$. But we will first take a look at rational points on elliptic curves over $\mathbb{Q}$, since we get useful information from it. The first useful information is coming from Mordell's theorem, which is stated as follow:

Theorem 3.4.1. *(Mordell's Theorem)[12, Page 16] Let C be an elliptic curve over $\mathbb{Q}$ with a rational point. Then $C(\mathbb{Q})$ is finitely generated.*

This gives us that if we have a specific finite set of rational solutions for an elliptic curve C, we can obtain every rational point on C by adding points of this finite set.
Mordell's theorem also gives us that the group of rational points of an elliptic curve over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}^r \times T$, for some non-negative integer r, which is called the *rank*, and a finite group T, which is the group of elements of finite order and is called the *torsion subgroup*.

Although Mordell's theorem gives us that the group of rational points is finitely generated, it may still be the case that the elliptic curve C has infinitely many rational points. We might ask ourselves which of those points are integer points and whether there are infinitely many of them or not. One might think that there are infinitely many integer points on C, but the next theorem shows us that this is not the case.

Theorem 3.4.2. *(Siegel's Theorem)[12, Theorem 5.1] Let $C : f(x, y) = 0$ be an affine elliptic curve over $\mathbb{Q}$ with integer coefficients. Then C has only a finite set of points with integer coordinates.*

Note that this set is not a group, because the point at infinity is never an integral point. Although Siegel's theorem gives us that there are finitely many integral points, it sadly does not give us the integral points. In this project, we will be interested in situations where $r = 1$ and $T = \mathcal{O}$, so that there is only a single generator.

Chapter 4

Elliptic curves over $\mathbb{F}_p$ and $\mathbb{Q}_p$

4.1 Rational points over Finite Fields

We will now take a look at some basics about elliptic curves over finite fields $\mathbb{F}_q$, where $q = p^n$ for a prime p and a positive integer n. In this project, we are only considering the case where $n = 1$. On these finite fields, we define for elliptic curves an addition law on it in the same way as we did in the previous chapter, where we see $\frac{y}{x}$ as yx^{-1}. This addition law will again define an abelian group.

Now we let C be an elliptic curve over $\mathbb{F}_p$ given by the equation

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

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_p$.
We want to estimate the number of $\mathbb{F}_p$-rational points on the elliptic curve over $\mathbb{F}_p$. But before we do that, we will take a look at an example.

Example 4.1.1. Let C be the elliptic curve given by

$$C : f(x, y) = y^2 - (x^3 - 8x + 4) = 0.$$

If we take this curve over the field $\mathbb{F}_5$, we obtain the following equation:

$$C : y^2 - (x^3 + 2x + 4) = 0.$$

If we want to find the set of $\mathbb{F}_5$-rational points of the curve, we get that x and y must be in $\mathbb{F}_5$, so we only have 5 possibilities for x and 5 for y. First we will substitute all possibilities for x in the equation x^3+2x+4. Now we will check whether the result gives a square in $\mathbb{F}_5$. If we do this, and include the point at infinity $\mathcal{O}$, we obtain the following 7 points:

$$C(\mathbb{F}_5) = \{(0, \pm 2), (2, \pm 1), (4, \pm 1), \mathcal{O}\}.$$

From this we get that $C(\mathbb{F}_5)$ is a cyclic group of order 7.
Now we will show how the addition formulas work. Let $P = (0, 2) = (x_1, y_1) \in C(\mathbb{F}_5)$. If we want to see what element in $C(\mathbb{F}_5)$ is equal to $2P = P + P = (x_3, y_3)$, we follow the instructions from the previous chapter. By doing this, we find that $\lambda = \frac{2}{4} = 2 \cdot 4^{-1} = 2 \cdot 4 = 8 \equiv 3 \bmod 5$ and $\mu = y_1 - \lambda x_1 = 2 - 0 = 2$. Using this, we get that $x_3 = \lambda^2 - 2x_1 = 9 \equiv 4 \bmod 5$ and $y_3 = -\lambda x_3 - \mu = -12 - 2 = -14 \equiv 1 \bmod 5$, hence $2P = (4, 1)$. By applying the rules from the previous chapter again and again, we find that

$$3P = (2, 1), \quad 4P = (2, -1), \quad 5P = (4, -1), \quad 6P = (0, -2) \quad \text{and} \quad 7P = \mathcal{O}.$$

In the example it is clear that $C(\mathbb{F}_5)$ only has finitely many points for our curve C. In fact, for all elliptic curves C and all primes p we have that $C(\mathbb{F}_p)$ is a finite group. This is the case because x and y

only have a finite number of possibilities. Because $C(\mathbb{F}_p)$ is a finite group, it can always be finitely generated.

One might ask how many points $C(\mathbb{F}_p)$ has, and if there is a formula to determine the number of points in it. Sadly, such a formula does not exist, but the Hasse-Weil theorem gives a good approximation for this number. This theorem is stated as follows.

Theorem 4.1.2. *(Hasse-Weil Theorem)[12, Theorem 4.1] Let C be an elliptic curve defined over $\mathbb{F}_p$. Then*

$$p + 1 - 2\sqrt{p} \leq \#C(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}.$$

4.2 p-adic numbers

In this section we will introduce the p-adic numbers $\mathbb{Q}_p$ for primes p. To do this, we will mostly take a look at [4, Section 2].

Before we can introduce the p-adic numbers, we first have to introduce a certain valuation. Recall that a valuation on a field K is a map $|\ | : K \to \mathbb{R}$ which satisfies the following three properties [4, Definition 2.1]:

1. $|x| \geq 0$ for all $x \in K$, with $|x| = 0 \Leftrightarrow x = 0$.
2. $|xy| = |x| \cdot |y|$ for all $x, y \in K$.
3. $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

We will now define the specific valuation which is needed for the definition of the p-adic numbers.

Definition 4.2.1. Let p be a prime and take $x \in \mathbb{Q}$. Note that we can write x as $x = p^r \frac{a}{b}$, such that $p \nmid a$, $p \nmid b$. Then the *p-adic valuation* of x is denoted by $|x|_p$ and is given by: $|x|_p = |p^r \frac{a}{b}|_p = p^{-r}$ if x is non-zero and $|0|_p$ is defined to be 0. We define the *p-adic distance* between two elements x and y of $\mathbb{Q}$ to be $d_p(x, y) = |x - y|_p$, where d_p is a metric.

To check whether this is indeed a valuation, we must check the three properties. The first property is easily seen, because $p^{-r} > 0$ for all primes p and all integers r, and since $p^{-r} \neq 0$ we get that $|x|_p = 0$ if and only if $x = 0$. To check if the second property holds, we take $x = p^r \frac{a}{b}, y = p^s \frac{c}{d}$ for prime p and integers a, b, c, d such that p does not divide any of them. Then

$$|xy|_p = |p^{r+s} \frac{ac}{bd}|_p = p^{-(r+s)} = p^{-r} \cdot p^{-s} = |x|_p \cdot |y|_p.$$

For the third property, we will say without loss of generality that $r \leq s$. Then it follows that

$$|x + y|_p = |\frac{p^r ad + p^s bc}{bd}|_p = |p^r \frac{p^t f}{bd}|_p = p^{-(r+t)} \leq p^{-r} \leq p^{-r} + p^{-s} = |x|_p + |y|_p,$$

for some $t \geq 0$ and $f \in \mathbb{Z}$.

For example, we have for $x = 2^3 3^{-8} 5^{-1}$ that $|x|_2 = 2^{-3}$, $|x|_3 = 3^8$, $|x|_5 = 5$ and $|x|_p = 1$ for primes $p \geq 7$.

Now that we defined the p-adic valuation, we can define the set of p-adic numbers.

Definition 4.2.2. The set of *p-adic numbers*, denoted by $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ for the metric $d_p(x, y)$, and is the smallest field containing $\mathbb{Q}$ which is complete with respect to $|\ |_p$.

We say that any two elements $a, b \in \mathbb{Q}_p$ are congruent modulo p^n, denoted by $a \equiv b (\bmod p^n)$, if and only if $|a-b|_p \leq p^{-n}$.

Note that any element $x \in \mathbb{Q}_p$ can be written as follows:

$$x = \sum_{n=N}^{\infty} a_n p^n, \text{ where } N \in \mathbb{Z}, a_N \neq 0 \text{ and each } a_n \in \{0, \ldots, p-1\}.$$

From this we get that $|x|_p = p^{-N}$. Note that if $N \geq 0$, then it follows that $|x|_p \leq 1$. The set $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ is a subring of $\mathbb{Q}_p$, called *the ring of p-adic integers*. [2, Page 6]

4.3 Reduction Modulo p

In this section we are going to introduce the reduction modulo p map. We will mostly be looking at [4, Section 3], [11, Section VII.1 and VII.2] and [12, Appendix A.5] to do this.

Before we introduce the reduction modulo p map, we first have to introduce normalized coordinate triples.

Definition 4.3.1. A homogeneous coordinate triple $[a, b, c] \in \mathbb{P}^2(\mathbb{Q}_p)$ is said to be *normalized* if the largest p-adic valuation of a, b, c is 1. This gives us that a, b and c are in $\mathbb{Z}_p$ and at least one of the coordinates can be written as $\sum_{n=0}^{\infty} a_n p^n$ where $a_0 \neq 0$ and $a_n \in \{0, \ldots, p-1\}$ for all n.

It is possible for any point $P = [a, b, c]$ in $\mathbb{P}^2(\mathbb{Q}_p)$ to be represented by a normalized coordinate triple. This can be done by dividing a, b and c with the value with the greatest p-adic valuation. Note that P does not change if we do this.

We will now introduce the reduction mod p map, for any fixed prime p. To do this, we first let $\tilde{a} \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote the residue modulo p for any p-adic integer $a \in \mathbb{Z}_p$. Note for any normalized coordinate triple $[a, b, c]$ that a, b and c are not all divisible by p. So, for each normalized coordinate triple $[a, b, c]$ for a point $P \in \mathbb{P}^2(\mathbb{Q}_p)$, we let $[\tilde{a}, \tilde{b}, \tilde{c}]$ define a point $\tilde{P} \in \mathbb{P}^2(\mathbb{F}_p)$. This point $\tilde{P}$ is not determined by the choice of coordinates of P, because the different choices of homogeneous coordinate triples of P are related by multiplication with elements with p-adic valuation 1. This gives us a well-defined map

$$\mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p),$$

where $P \mapsto \tilde{P}$. This map is called the *reduction mod p map*, which we will denote by red_p [4, Definition 3.1].

Definition 4.3.2. Let $C : F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3) = 0$ denote a projective elliptic curve over $\mathbb{Q}_p$. So $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}_p$. We call F *normalized* if $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}_p$.

Note that, since the coefficients of Y^2Z and X^3 are equal to ± 1, we get that the largest p-adic valuation of the coefficients of a normalized F is one if $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}_p$.

It is also possible to normalize any polynomial equation for an elliptic curve over $\mathbb{Q}_p$ [11, Proposition 1.3.a]. This can be done by the substitution $(X, Y, Z) \mapsto (u^{-2}X, u^{-3}Y, Z)$ for some specific non-zero $u \in \mathbb{Q}_p$. This will lead to the following equation:

$$F(X, Y, Z) = u^{-6}Y^2Z + u^{-5}a_1XYZ + a_3u^{-3}YZ^2 - (u^{-6}X^3 + u^{-4}a_2X^2Z + u^{-2}a_4XZ^2 + a_6Z^3) = 0.$$

By multiplying both sides with u^6, we get the next equation:

$$F(X, Y, Z) = Y^2Z + ua_1XYZ + a_3u^3YZ^2 - (X^3 + u^2a_2X^2Z + u^4a_4XZ^2 + u^6a_6Z^3) = 0.$$

So if we pick u in such a way that $u^i a_i \in \mathbb{Z}_p$, then we have a normalized polynomial F.

Now let F be a normalized polynomial and let $\tilde{F}$ denote the polynomial that is obtained by reducing the coefficients of F modulo p. Then $\tilde{F}$ is non-zero and defines a curve $\tilde{C}$ over $\mathbb{F}_p$. Since $x \to \tilde{x}$ is a homomorphism, we get for any normalized coordinate triples $[a, b, c]$ with $F(a, b, c) = 0$, that $\tilde{F}(\tilde{a}, \tilde{b}, \tilde{c}) = 0$. Hence if P is a $\mathbb{Q}_p$-rational point on C, then $\tilde{P}$ is a point on $\tilde{C}$. This gives that the reduction mod p maps $C(\mathbb{Q}_p)$ to $\tilde{C}(\mathbb{F}_p)$.

The reduction mod p map respects the group law on elliptic curves. To find this, one first has to look at the reduction of the intersection of two curves and the intersection of the reduction of two curves.
If we have two curves C_1 and C_2, then it follows that

$$\widetilde{(C_1(\mathbb{Q}_p) \cap C_2(\mathbb{Q}_p))} \subset \tilde{C}_1(\mathbb{F}_p) \cap \tilde{C}_2(\mathbb{F}_p).$$

One might say that we can apply Bezout's theorem (Theorem 2.3.1) to find that $\widetilde{(C_1 \cap C_2)} = \tilde{C}_1 \cap \tilde{C}_2$ since the reduced curves have the same degree as the original curves. But this is not the case, since we do not have that the ground field is algebraically closed. Nonetheless everything works out if the intersection points over $\overline{\mathbb{Q}_p}$ are $\mathbb{Q}_p$- rational. To prove that the reduction map respects the group law, we only need to discuss the case where one of the curves is an elliptic curve and the other a line.

Theorem 4.3.1. *[12, Proposition A.5] Let C be a projective elliptic curve over $\mathbb{Q}_p$ and L be a projective line over $\mathbb{Q}_p$, where L is not a component of C. Suppose that all intersection points over $\overline{\mathbb{Q}_p}$ are $\mathbb{Q}_p$-rational. Let $C \cap L = \{P_1, P_2, P_3\}$, where P_i is repeated in the list as many times as its multiplicity. If $\tilde{L}$ is not a component of $\tilde{C}$, then $\tilde{C} \cap \tilde{L} = \{\tilde{P}_1, \tilde{P}_2, \tilde{P}_3\}$ with the correct multiplicity.*

Theorem 4.3.1 can be applied to show that the reduction mod p map respects the group law on elliptic curves, which will be proven in the next theorem.

Theorem 4.3.2. *[12, Corollary A.7] Let C be a projective elliptic curve over $\mathbb{Q}_p$ and let $\mathcal{O} = [0, 1, 0]$ be the origin for the group law on C. Suppose that $\tilde{C}$ is non-singular and take $\tilde{\mathcal{O}} = \mathcal{O}$ as the origin for the group law on $\tilde{C}$. Then the reduction mod p map $P \mapsto \tilde{P}$ is a group homomorphism for $C(\mathbb{Q}_p) \to \tilde{C}(\mathbb{F}_p)$.*

Proof. Let $P, Q \in C(\mathbb{Q}_p)$ and let $R = P + Q$. Then there are projective lines L_1 and L_2 over $\mathbb{Q}_p$ and a $\mathbb{Q}_p$-rational point $S = P * Q \in C(\mathbb{Q}_p)$ such that

$$C \cap L_1 = \{P, Q, S\} \quad \text{and} \quad C \cap L_2 = \{S, \mathcal{O}, R\}.$$

If we now apply Theorem 4.3.1, then we get that

$$\tilde{C} \cap \tilde{L}_1 = \{\tilde{P}, \tilde{Q}, \tilde{S}\} \quad \text{and} \quad \tilde{C} \cap \tilde{L}_2 = \{\tilde{S}, \tilde{\mathcal{O}}, \tilde{R}\}.$$

From this one can conclude that $\tilde{P} + \tilde{Q} = \tilde{R}$, so the reduction mod p map $P \mapsto \tilde{P}$ is a group homomorphism $C(\mathbb{Q}_p) \to \tilde{C}(\mathbb{F}_p)$. □

As for later purpose we want to know which affine points P of a projective elliptic curve over $\mathbb{Q}_p$ reduce to the point at infinity. The next theorem will tell us this.

Theorem 4.3.3. *[13, Proposition 3.1.4] Let $C : F(X, Y, Z) = 0$ be a projective elliptic curve over $\mathbb{Q}_p$ where F is normalized. Let $P = (a, b, 1) \in C$ with $a, b \in \mathbb{Q}_p$. Then $\tilde{P} = \tilde{\mathcal{O}}$ if and only if a and b are not both in $\mathbb{Z}_p$.*

A proof of this theorem can be found on page 23 of [13]. We will denote the set with all points of the curve that reduce to the point at infinity by $C_1(\mathbb{Q}_p)$. This set is a subgroup, because it is the kernel of the reduction map, which is an homomorphism. Note that for a point $P = (a, b, 1) \in C_1(\mathbb{Q}_p)$ we also have that $|a|_p < |b|_p$.

4.4 Logarithm map

In this section we are going to introduce the logarithm map, which maps $C(\mathbb{Q}_p)$ to $\mathbb{Q}_p$. To do this, we first define a homomorphism $g : C_1(\mathbb{Q}_p) \to \mathbb{Q}_p$ as follows. If $Q = (x, y)$ is an affine point in $C_1(\mathbb{Q}_p)$ we define $g(Q)$ to be the formal logarithm from page 127 of [11] evaluated at $-\frac{x}{y}$, which is given by

$$g(Q) = -\frac{x}{y} + \frac{c_1}{2}(-\frac{x}{y})^2 + \frac{c_2}{3}(-\frac{x}{y})^3 + \ldots \in \mathbb{Q}_p, \tag{4.1}$$

for some $c_i \in \mathbb{Z}_p$; we also set $g(\mathcal{O}) = 0$. Note, since we are working in $C_1(\mathbb{Q}_p)$, we get that $Q = (x, y)$ can be represented by $(p^r\frac{a}{b}, p^s\frac{c}{d}, 1)$, where $x = p^r\frac{a}{b}, y = p^s\frac{c}{d}$, p does not divide the coefficients a, b, c and d, $s < r$ and $s < 0$. From this we get that $|-\frac{x}{y}|_p = |-p^{(r-s)}\frac{ad}{bc}|_p = p^{-(r-s)} < 1$, which tells us that $(-\frac{x}{y})^n \to 0$ in $\mathbb{Q}_p$ as $n \to \infty$. Then [4, Theorem 2.12] tells us that $\sum_{n=1}^{\infty}(-\frac{x}{y})^n$ is convergent in $\mathbb{Q}_p$. Since each $c_i \in \mathbb{Z}_p$, we get that $g(Q)$ converges at $-\frac{x}{y}$ if $\frac{c_{n-1}}{n}(-\frac{x}{y})^n$ tends to 0 p-adically as n tends to infinity. To show this, we first have to note that

$$|\frac{c_{n-1}}{n}(-\frac{x}{y})^n|_p \leq \frac{p^{-n}}{|n|_p}. \tag{4.2}$$

If we write n as $p^{ord_p(n)} \cdot m$, where $p \not| m$, then we get that the right hand side of (4.2) can be written as $p^{-n+ord_p(n)}$. Since n goes faster to infinity than $ord_p(n)$, it follows that the right hand side of (4.2) goes to zero, which also gives us that $\frac{c_{n-1}}{n}(-\frac{x}{y})^n$ goes to zero p-adically, hence $g(Q)$ coverges at $-\frac{x}{y}$. Note that, since $c_i \in \mathbb{Z}_p$, $|-(\frac{x}{y})|_p < 1$ and $n > ord_p(n)$, we get that it follows that $g(Q) \in p\mathbb{Z}_p$.
The fact that g is a homomorphism follows from page 132 of [11, Theorem 6.4(a)].

It is also possible to extend g to $C(\mathbb{Q}_p) \to \mathbb{Q}_p$. This is done as follows. If $Q \notin C_1(\mathbb{Q}_p)$, then we let n be a non-zero integer such that $nQ \in C_1(\mathbb{Q}_p)$. Then we define $g(Q) := g(nQ)/n$. Note that such an n always exists, because if we pick $n = \#C(\mathbb{F}_p)$, then $red(nQ) = n \cdot red(Q) = \mathcal{O}$.

The new map g is also a homomorphism, which we will show now. Let $Q_1, Q_2 \in C(\mathbb{Q}_p)$ and let n, m be non-zero integers such that $nQ_1, mQ_2 \in C_1(\mathbb{Q}_p)$. Then it also follows that $nmQ_1, nmQ_2 \in C_1(\mathbb{Q}_p)$. From this we get that

$$\begin{aligned} g(Q_1) + g(Q_2) &= \frac{g(nQ_1)}{n} + \frac{g(mQ_2)}{m} \\ &= \frac{m \cdot g(nQ_1) + n \cdot g(mQ_2)}{nm} \\ &= \frac{g(mnQ_1) + g(nmQ_2)}{nm} \\ &= \frac{g(nm(Q_1 + Q_2))}{nm} \\ &= g(Q_1 + Q_2). \end{aligned}$$

Now that we have defined the homomorphism g, we can define a logarithm map from $C(\mathbb{Q}_p)$ to $\mathbb{Q}_p$. This logarithm map is defined as follows

$$\log_{P,p}(z) = \log_P(z) = \frac{g(z)}{g(P)}.$$

Note that since g is a homomorphism it follows that if $z = aP$ for some $a \in \mathbb{Z}$, then $\log_{P,p}(z) = \frac{g(aP)}{g(P)} = \frac{ag(P)}{g(P)} = a$.

So all we need to know now is how to compute g on $C_1(\mathbb{Q}_p)$. In fact, we need a bit less: we need $\frac{g(z)}{g(P)}$ mod p. Note that for any $Q \in C(\mathbb{Q}_p)$ there exists a non-zero $n \in \mathbb{Z}$ such that $nQ \in C_1(\mathbb{Q}_p)$. Recall that, for any $nQ \in C_1(\mathbb{Q}_p)$ it follows that $g(nQ) \in p\mathbb{Z}_p$, so we get that $g(Q) \in p\mathbb{Z}_p$, provided that p does not divide n. From this it follows in general that $g(z)$ and $g(P)$ will be 0 mod p, so we need to know at least

$g(z)$ and $g(P)$ modulo p^2 to hope to know $\frac{g(z)}{g(P)}$. But by the way that we defined the map g it is clear that if $Q \in C_1(\mathbb{Q}_p)$ for an odd p, then $g(Q) = -\frac{x(Q)}{y(Q)} \mod p^2$. Now let $n \in \mathbb{Z}$ such that $nz, nP \in C_1(\mathbb{Q}_p)$. If we have that $|\frac{x(nP)}{y(nP)}|_p = p^{-1}$, then

$$\log_{P,p}(z) \equiv \frac{\frac{x(nz)}{y(nz)}}{\frac{x(nP)}{y(nP)}} \mod p.$$

Note that if $\frac{g(z)}{g(P)} \notin \mathbb{Z}_p$, then there does not exist an $a \in \mathbb{Z}$ such that $z = aP$.

Chapter 5

Sieving p-adic points on elliptic curves

In this chapter we discuss some possible extension of and some limitations of Appendix A of [1]. To do this it is useful to first explain what is happening in the Appendix.

5.1 Sieving with pseudo-amicable primes

Let C denote an elliptic curve of rank 1 over $\mathbb{Q}$ and suppose that we have a subset $\mathcal{A}$ of $C_0(\mathbb{Z})$. Then the goal is to prove that $\mathcal{A} = C_0(\mathbb{Z})$. To do this, [1] first assumes that $C(\mathbb{Q})$ is torsion-free. Then, by Mordell's theorem (Theorem 3.4.1) it follows that $C(\mathbb{Q}) \cong \mathbb{Z}$, which gives us that $C(\mathbb{Q})$ can be generated by a single point of the curve. Let us fix a choice of generator P. Then it follows that if $R \in C(\mathbb{Q})$, then there is an $n \in \mathbb{Z}$ such that $R = nP$. If $R = (x, y)$ is an integral point, then $x, y \in \mathbb{Z}_p$ for any prime p, so by Theorem 4.3.3 we get that the reduction modulo p of R is not the point at infinity of $C(\mathbb{F}_p)$. Since $C(\mathbb{Q})$ is a subgroup of $C(\mathbb{Q}_p)$ and the reduction map $red : C(\mathbb{Q}_p) \to C(\mathbb{F}_p)$ is a homomorphism, we have

$$red(R) = red(nP) = n \cdot red(P).$$

We will now try to prove that $\mathcal{A} = C_0(\mathbb{Z})$ by using quadratic Chabauty for several primes. Quadratic Chabauty is a method that produces, for all primes p of good reduction, finitely many finite subsets of $C(\mathbb{Q}_p)$, denoted by $R_{1,p} \dots, R_{k,p}$ with the property that if z is an integral point, then there exists an n where $1 \leq n \leq k$ such that for every prime p, $z \in R_{n,p}$. Here $k \in \mathbb{Z}$ is dependent on C, but independent of p, and we also have that n is independent of p. We try to prove that for any n, there is no point in $C_0(\mathbb{Z}) - \mathcal{A}$ such that it is in all $R_{n,p}$ for all primes p.

We will use quadratic Chabauty on primes with certain conditions. A prime p is called a *prime of good reduction* for C if the reduction of C modulo p gives a non-singular curve over $\mathbb{F}_p$. We call a pair of distinct primes (p_1, p_2) *amicable* if

$$p_2 = \#C(\mathbb{F}_{p_1}) \quad \text{and} \quad p_1 = \#C(\mathbb{F}_{p_2}),$$

and two distinct primes (p_1, p_2) are called *pseudo-amicable* if

$$p_2 \mid \#C(\mathbb{F}_{p_1}) \quad \text{and} \quad p_1 \mid \#C(\mathbb{F}_{p_2}).$$

Method 1: Suppose that p_1 and p_2 are odd primes of good reduction for C such that $p_1 | ord(red_{p_2}(P))$ and $p_2 | ord(red_{p_1}(P))$. Then it follows that (p_1, p_2) is pseudo-amicable. Now quadratic Chabauty is applied to C for p_1 and p_2.

Step 1.1: Suppose that $z \in R_{n,p_1}$ for some n. Since we are trying to reach a contradiction, we assume that z is also an element of $C_0(\mathbb{Z})$. Then z is also in $C(\mathbb{Q})$, so $z = aP$ for some $a \in \mathbb{Z}$. We do not know a, but we can compute $A := a \bmod p_2$ from the reduction map $C(\mathbb{Q}_{p_1}) \to C(\mathbb{F}_{p_1})$ and $B := a \bmod p_1$ from the logarithm map. It might be a little bit hard to see how we get A, so we will include some details about it. We get this A by first reducing modulo p_1. This will give $a \cdot red_{p_1}(P) = red_{p_1}(aP) = red_{p_1}(z)$, where a is

known modulo $ord(red_{p_1}(P))$. Since $p_2 | ord(red_{p_1}(P))$, we can also compute $A := a \bmod p_2$. Note that if P does not reduce to a generator of $C(\mathbb{F}_{p_1})$, then it might be possible that such an A does not exist.

Step 1.2: Since we assumed that $z \in C_0(\mathbb{Z})$, it follows that $z \in R_{n,p_2}$. So there must be a $z_2 \in R_{n,p_2}$ such that $\log_{P,p_2}(z_2) = A \bmod p_2$ and $red_{p_2}(z_2) = (l \cdot p_1 + B) \cdot red_{p_2}(P)$ for some $l \in \{0, \ldots, (ord(red_{p_2}(P))/p_1) - 1\}$. If such a z_2 does not exist, then we know that z is not a point of $C_0(\mathbb{Z})$.

Example 5.1.1. Let C be the elliptic curve given by

$$y^2 = x^3 - 8x + 4.$$

According to [8] the rank of C is 1 and the torsion is trivial over $\mathbb{Q}$. We also have that $P = (0, 2)$ is a generator of $C(\mathbb{Q})$.

If we compute aP for $a \in \{-10, -9 \ldots, 9, 10\}$, we find a set of integral points $\mathcal{A} = \{(0, \pm 2), (-3, \pm 1), (4, \pm 6)\}$. We will now show that $\mathcal{A} = C_0(\mathbb{Z})$ by using **Method 1** for the pseudo-amicable pair $(p_1, p_2) = (7, 5)$, where $p_1 = ord(red_{p_2}(P))$ and $2 \cdot p_2 = ord(red_{p_1}(P))$.

If we apply quadratic Chabauty for p_1, we find a set of 10 points in $C(\mathbb{Q}_7)$ divided over two subsets, which could be integral points that are not in $\mathcal{A}$. We call these points $z_1(i)$, where $1 \leq i \leq 10$, where $z_1(1)$ is given by

$$(2 \cdot 7 + O(7^2), 5 + 3 \cdot 7 + O(7^2)).$$

Each of these points belongs to one of the two subsets, which have an index $n(i)$. For $z_1(1)$, we have that $n(1) = 1$.

We will now compute A and B from **Step 1.1** for $z_1(1)$. To compute A, we use the reduction mod p_1 map, which gives us that $red_7(z_1(1)) = (0, 5)$. We find that $(0, 5)$ is equal to $4P$ in $C(\mathbb{F}_7)$. From this it follows that $A = 4$, i.e. a is congruent to 4 mod 5.
We will now compute B by using the logarithm map. To do this we first have to note that $5P = \left(4 \cdot 7^{-2} + O(7^{-1}), 7^{-3} + O(7^{-2})\right) \in C_1(\mathbb{Q}_7)$, and that $5z_1(1) = (2 \cdot 7^{-2} + O(7^{-1}), 7^{-3} + O(7^{-2})) \in C_1(\mathbb{Q}_7)$, so we get that $\log_{P,7}(z_1(1)) = 4 + O(7) \equiv 4 \bmod 7$. From this it follows that $B = 4$, i.e. a is congruent to 4 mod 7. Hence we obtain for $z_1(1)$ that $(a \bmod 5, a \bmod 7, n(1))$ is given by $(4, 4, 1)$.

If we apply **Step 1.1** for all 10 points $z_1(i)$, we find the following possibilities for $(a \bmod 5, a \bmod 7, n(i))$:

$$(4, 4, 1), (1, 3, 1).$$

If we apply quadratic Chabauty for p_2, we find a set of 6 points in $C(\mathbb{Q}_5)$ divided over two subsets, which could be integral points that are not in $\mathcal{A}$. We call these points $z_2(i)$, where $1 \leq i \leq 6$, where $z_2(3)$ is given by

$$(2 + 4 \cdot 5 + O(5^2), 4 + 4 \cdot 5 + O(5^2)).$$

Each of these points also has an index $n(i)$. In particular, $n(3) = 1$.

We will now compute A and B from **Step 1.2** for $z_2(3)$, and check whether they have the same properties as the result of **Step 1.1**. To compute B, we use the reduction modulo p_2 map, which gives us that $red_5(z_2(3)) = (2, 4)$. We find that $(2, 4)$ is equal to $4P$ in $C(\mathbb{F}_5)$. From this it follows that $B = 4$, i.e. a is congruent to 4 mod 7.

Since we now have that a is congruent to 4 mod 7, we get that $z_2(3)$ is a potential integral point that is not in $\mathcal{A}$ if we get that $A = 4$ from the logarithm map. To check whether this is true we first have to note that $7P = (4 \cdot 5^{-2} + O(5^{-1}), 2 \cdot 5^{-3} + O(5^{-2})) \in C_1(\mathbb{Q}_5)$, and that $7z_2(3) = (5^{-2} + O(5^{-1}), 4 \cdot 5^{-3} + O(5^{-2})) \in C_1(\mathbb{Q}_5)$, so we get that $\log_{P,5}(z_2(3)) = 2 + O(5) \equiv 2 \bmod 5$. This gives us that $A = 2 \neq 4$, so we get that $z_2(3)$ is not an integral point of C. In fact, if we apply **Step 1.2** for all 6 points $z_2(i)$, we find that there is no point

such that it has the same possibilities for $(a \bmod 5, a \bmod 7, n(i))$ as the ones after **Step 1.1**, so none of the points $z_1(i)$ are integral points. Hence we have shown that $(0, \pm 2), (-3, \pm 1), (4, \pm 6)$ are the only integral points on C. A code for this can be found in Appendix A.1. However all the computations could be done by hand using the formulas in the previous chapters.

More generally, we call a sequence of primes $\overline{p} = (p_1, p_2, \ldots, p_l)$ an *aliquot cycle* of length l for C if $p_{i+1} = \#C(\mathbb{F}_{p_i})$, where i is taken modulo l. A sequence of primes is called a *pseudo-aliquot cycle* if $p_{i+1} \mid \#C(\mathbb{F}_{p_i})$.

Method 2: Suppose that we have a sequence of primes $\overline{p} = (p_1, \ldots p_l)$, such that $p_{i+1} | ord(red_{p_i}(P))$. Then it follows that $\overline{p}$ is pseudo-aliquot. We will now again apply quadratic Chabauty to C for the primes $p_1 \ldots p_l$.

Step 2.1: Suppose that $z \in R_{n,p_1}$ for some n. Also assume that $z \in C_0(\mathbb{Z})$. Then z is also in $C(\mathbb{Q})$, which gives that $z = aP$ for some $a \in \mathbb{Z}$. Here a is not known, but we can compute $A_1 := a \bmod p_1$ from the logarithm and $A_2 := a \bmod p_2$ from the reduction map $C(\mathbb{Q}_{p_1}) \to C(\mathbb{F}_{p_1})$.

Step 2.2: Since we assumed that $z \in C_0(\mathbb{Z})$, it also follows that $z \in R_{n,p_2}$. So there must be a $z_2 \in R_{n,p_2}$ such that $\log_{P,p_2}(z_2) = A_2 \bmod p_2$. If this is the case, then we can also find an A_3 such that $A_3 := a \bmod p_3$ from the reduction map $C(\mathbb{Q}_{p_2}) \to C(\mathbb{F}_{p_2})$. Then, since $z \in C_0(\mathbb{Z})$ it also follows that $z \in R_{n,p_3}$, where we can repeat step 2.2 until $l - 1$.

Step 2.l: Since we assumed that $z \in C_0(\mathbb{Z})$, it also follows that $z \in R_{n,p_l}$. So there must be a $z_l \in R_{n,p_l}$ such that $\log_{P,p_l}(z_l) = A_l \bmod p_l$ and $red_{p_l}(z_l) = (k \cdot p_1 + A_1) \cdot red_{p_l}(P)$, for some $k \in \{0, \ldots, (ord(red_{p_l}(P))/p_1) - 1\}$. We will call the collection of the points z_i a *lift* of $\overline{p}$. If no such lift exists, then we have that z is not in $C_0(\mathbb{Z})$. If this holds for all elements in the union over n of R_{n,p_1}, then we get that $\mathcal{A} = C_0(\mathbb{Z})$.

5.2 Extra condition

It might be possible that not all points in $C(\mathbb{Q}_{p_1})$ are eliminated after using **Method 1**, i.e. there exists a $z \in C(\mathbb{Q}_{p_1})$ which is not eliminated. If this is the case, we check if there is an odd prime p_3 of good reduction such that $p_1 \cdot p_2 \mid ord(red_{p_3}(P))$, which might be useful to eliminate the remaining points in **Method 3**.

Method 3: Suppose that p_1, p_2 and p_3 are odd primes of good reduction for C such that $p_1 | ord(red_{p_2}(P))$, $p_2 | ord(red_{p_1}(P))$ and $p_1 \cdot p_2 \mid ord(red_{p_3}(P))$ and suppose that **Method 1** does not eliminate all potential integral points in $C(\mathbb{Q}_{p_1})$ that are not in $\mathcal{A}$. Then we first apply quadratic Chabauty to C for the prime p_3.

Step 3.1: Since we assumed that there is a point z such that $z \in C_0(\mathbb{Z}) - \mathcal{A}$, it follows that $z \in R_{n,p_3}$, where n is the same as the one of the point that survived **Method 1**, and that $z \in C(\mathbb{Q})$. So there must be a $z_3 \in R_{n,p_3}$ such that $z_3 = aP$ for some $a \in \mathbb{Z}$. This a is unknown, but we are able to compute $M := a \bmod p_1 \cdot p_2$ from the reduction map $C(\mathbb{Q}_{p_3}) \to C(\mathbb{F}_{p_3})$. From this we are also able to compute $A' := a \bmod p_2$ and $B' := a \bmod p_1$. Recall that we already have that $A = a \bmod p_2$ and $B = a \bmod p_1$ from **Method 1**. So for z to be an integral point, we need that $A' = A$ and $B' = B$. If there does not exist a $z_3 \in R_{n,p_3}$ which satisfies this, we can conclude that z is not an integral point of $C_0(\mathbb{Z})$.

Example 5.2.1. Let C be the elliptic curve given by

$$y^2 + xy + y = x^3 + x^2 - 21x - 45.$$

According to [9] the rank of C is 1 and the torsion is trivial over $\mathbb{Q}$. We also have that $P = (-3, 2)$ is a generator of $C(\mathbb{Q})$.

If we compute aP for $a \in \{-10, -9, \ldots, 9, 10\}$, we find a set of integral points $\mathcal{A} = \{(-3, 2), (-3, 0), (5, 0), (5, -6)\}$. We now want to show that $\mathcal{A} = C_0(\mathbb{Z})$ by using **Method 3** for the three primes $p_1 = 5, p_2 = 7$ and $p_3 = 31$, where $2 \cdot p_1 = ord(red_{p_2}(P))$, $p_2 = ord(red_{p_1}(P))$ and $p_1 \cdot p_2 = ord(red_{p_3}(P))$. But before we do this, we

first show that **Method 1** fails for the primes p_1 and p_2.

If we use quadratic Chabauty for p_1, we find a set of 8 points in $C(\mathbb{Q}_5)$ which could be integral points that are not in $\mathcal{A}$. We call these points $z_1(i)$, where $1 \leq i \leq 8$, where $z_1(1)$ is given by

$$(2 \cdot 5 + O(5^2), 4 \cdot 5 + O(5^2)).$$

In Example 5.1.1, we saw that the potential integral points were divided over two subsets and that each of these points had an index $n(i)$. In this example, we have that all potential integral points are in one subset, so for each point we have that $n(i) = 1$.

We will now compute A and B from **Step 1.1** for $z_1(1)$. To compute A, we use the reduction mod p_1 map, which gives us that $red_5(z_1(1)) = (0, 0)$. We find that $(0, 0)$ is equal to $2P$ in $C(\mathbb{F}_5)$. From this it follows that $A = 2$, i.e. a is congruent to 2 mod 7.
We will now compute B by using the logarithm map. To do this, we first have to note that $7P = (4 \cdot 5^{-2} + O(5^{-1}), 3 \cdot 5^{-3} + O(5^{-2})) \in C_1(\mathbb{Q}_5)$, and that $7z_1(1) = (5^{-2} + O(5^{-1}), 4 \cdot 5^{-3} + O(5^{-2})) \in C_1(\mathbb{Q}_5)$, so we get that $\log_{P,5}(z_1(1)) = 3 + O(5) \equiv 3 \bmod 5$. From this it follows that $B = 3$, i.e. a is congruent to 3 mod 5. Hence we obtain for $z_1(1)$ that $(a \bmod 5, a \bmod 7, n(i)) = (3, 2, 1)$.

If we apply **Step 1.1** for all 8 points $z_1(i)$, we find the following possibilities for $(a \bmod 5, a \bmod 7, n(i))$:

$$(3, 2, 1), (2, 5, 1), (0, 6, 1), (0, 1, 1), (3, 4, 1), (0, 4, 1), (2, 3, 1), (0, 3, 1). \tag{5.1}$$

If we apply quadratic Chabauty for p_2, we find a set of 14 points in $C(\mathbb{Q}_7)$ which could be integral points that are not in $\mathcal{A}$. We call these points $z_2(i)$, where $1 \leq i \leq 14$, where $z_2(1)$ is given by

$$(6 + 5 \cdot 7 + O(7^2), 2 + 7 + O(7^2)).$$

We will now compute A and B from **Step 1.2** for $z_2(1)$, and check whether they have the same properties as the result of **Step 1.1**. To compute B, we use the reduction modulo p_2 map, which gives us that $red_7(z_2(1)) = (6, 2)$. We find that $(6, 2)$ is equal to $3P$ in $C(\mathbb{F}_7)$. From this we get that $B = 3$, i.e. a is congruent to 3 mod 5.

Since we now have that a is congruent to 3 mod 5, we get that $z_2(1)$ is a potential integral point that is not in $\mathcal{A}$ if we get that $A = 2$ or $A = 4$ from the logarithm map. To check whether this is true we first have to note that $10P = (2 \cdot 7^{-2} + O(7^{-1}), 7^{-3} + O(7^{-2})) \in C_1(\mathbb{Q}_7)$, and that $10z_2(1) = (4 \cdot 7^{-2} + O(7^{-1}), 7^{-3} + O(7^{-2}))$, so we get that $\log_{P,7}(z_2(1)) = 2 + O(7) \equiv 2 \bmod 7$. This gives us that $A = 2$, so we get that $z_2(1)$ is a potential integral point that is not in $\mathcal{A}$.

If we apply **Step 1.2** for all 14 points $z_2(i)$, we find that the following possibilities for $(a \bmod 5, a \bmod 7, n(i))$ from (5.1) survive **Step 1.2**:

$$(3, 2, 1), (2, 5, 1), (0, 4, 1), (0, 3, 1). \tag{5.2}$$

This tells us indeed that **Method 1** does not eliminate all possible integral points in $R_{1,5}$, so we will now use **Method 3** to eliminate the remaining points in $R_{1,5}$. To do this, we first use quadratic Chabauty for p_3, which gives us a set of 20 points in $C(\mathbb{Q}_{31})$ which could be integral points that are not in $\mathcal{A}$. We call these points $z_3(i)$, where $1 \leq i \leq 20$, where $z_3(1)$ is given by

$$(28 + 8 \cdot 31 + O(31^2), 2 + 22 \cdot 31 + O(31^2)).$$

We will now compute A' and B' from **Step 3.1** for $z_3(1)$, but before we can do that, we have to compute M for $z_3(1)$. To compute M, we use the reduction modulo p_3 map, which gives us that $red_{31}(z_3(1)) = (28, 2)$, which is equal to P in $C(\mathbb{F}_{31})$. This gives us that $M = 1$, i.e. a is congruent to 1 mod 35. From this it also follows that a is congruent to 1 mod 5 and 1 mod 7, i.e. $A' = B' = 1$. But since $(1, 1, 1)$ is not in (5.2), it follows that $z_3(1)$ is not an integral point on C. In fact, if we apply **Step 3.1** for all 20 points $z_3(i)$, we find that there is no point such that it has the same possibilities for $(a \bmod 5, a \bmod 7, n(i))$ as in (5.2), so none of the points $z_1(i)$ are integral points. Hence we have shown that indeed $(-3, 2), (-3, 0), (5, 0), (5, -6)$ are the only integral points on C. A code for this can be found in Appendix A.2. However all the computations could again be done by hand using the formulas in the previous chapters.

5.3 Torsion free

In the beginning of this chapter we assumed that $C(\mathbb{Q})$ was torsion-free. So one might ask themselves if it is possible to apply this method to a curve which is not torsion-free. The following proposition shows that this is not the case.

Proposition 5.3.1. Let $C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^2 + a_6$ be an elliptic curve of rank 1 over $\mathbb{Q}$. Let $p_1, \dots p_l$ be a pseudo-aliquot cycle of arbitrary length l, where p_i are odd primes of good reduction, for all $i \in \{1 \dots, l\}$. Then the $C(\mathbb{Q})$ is torsion-free.

We are going to prove this proposition by contradiction. To do this, we will need two important theorems. The first theorem tells us how large the torsion subgroup might be, whereas the second theorem gives a relationship between $\#T(\mathbb{Q})$ and $\#\tilde{C}(\mathbb{F}_p)$. The theorems are stated as follows.

Theorem 5.3.2. *(Mazur's Theorem) [11, Theorem VIII.7.5] Let C be an elliptic curve over $\mathbb{Q}$. Then the torsion subgroup T of $C(\mathbb{Q})$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z} \text{ with } 1 \leq n \leq 10 \text{ or } n = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ with } 1 \leq n \leq 4.$$

Theorem 5.3.3. *[7, Theorem5.1.2] Let C be an elliptic curve over the rational numbers $\mathbb{Q}$ and let $T(\mathbb{Q})$ denote the group of rational torsion points on C. Then the reduction homomorphism $red_p|T(\mathbb{Q}) : T(\mathbb{Q}) \to \tilde{C}(\mathbb{F}_p)$ is injective for any odd prime p of good reduction.*

From Theorem 5.3.3 it follows that $\#T(\mathbb{Q}) = \#im(red_p(T(\mathbb{Q})))$. From the fact that red_p is a homomorphism it follows from the first isomorphism theorem that $im(red_p(T(\mathbb{Q})))$ is a subgroup of $\tilde{C}(\mathbb{F}_p)$. From this it follows that $\#im(red_p(T(\mathbb{Q})))|\#\tilde{C}(\mathbb{F}_p)$. Combining this with the fact that $\#T(\mathbb{Q}) = \#im(red_p(T(\mathbb{Q})))$, we get that $\#T(\mathbb{Q})|\#\tilde{C}(\mathbb{F}_p)$, which is an important property to prove Proposition 5.3.1.

Proof of Proposition 5.3.1. Let $C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. We want to reach a contradiction, so we first assume that the torsion subgroup T is non-trivial. Then $\#T = t \neq 1$. From Theorem 5.3.3, we now get that $t \mid \#C(\mathbb{F}_{p_i})$ for $i \in \{1, \dots, l\}$. Now assume that the primes $p_1, \dots p_l$ form a pseudo-aliquot cycle, so $p_1, \dots p_l$ are primes of good reduction such that $p_{i+1} \mid \#C(\mathbb{F}_{p_i})$ and $p_1 \mid \#C(\mathbb{F}_{p_l})$. Without loss of generality, we can assume that $p_2 = \max\{p_1, \dots, p_l\}$. Then, because all our primes are primes not equal to 2, we get that $p_2 \geq p_i + 2$ for all $i \in \{1, 3, 4, 5, \dots, l-1, l\}$.

We can now distinguish between two cases, namely the case where $p_2 \nmid t$ and the one where $p_2 \mid t$.

Case 1 $p_2 \nmid t$**:**

Since $t \mid \#C(\mathbb{F}_{p_1})$ and $p_2 \mid \#C(\mathbb{F}_{p_1})$, we get that

$$\#C(\mathbb{F}_{p_1}) = t \cdot p_2 \cdot m \geq t(p_1 + 2), \tag{5.3}$$

for some $m \in \mathbb{Z}_{>0}$. By the Hasse-Weil theorem (Theorem 4.1.2) we also have the inequality

$$\#C(\mathbb{F}_{p_1}) \leq p_1 + 1 + 2\sqrt{p_1}. \tag{5.4}$$

If we combine equation (5.3) and (5.4), we get that

$$t(p_1 + 2) \leq \#C(\mathbb{F}_{p_1}) \leq p_1 + 1 + 2\sqrt{p_1}.$$

If we leave only the square root on the right hand side, we get

$$(t-1)p_1 + 2t - 1 \leq 2\sqrt{p_1}.$$

Since both sides are greater than zero, we are allowed to square both sides. By doing this, and bringing the right hand side to the left, we get

$$(t-1)^2p_1^2 + (2(t-1)(2t-1)-4)p_1 + (2t-1)^2 \leq 0. \tag{5.5}$$

The discriminant D of this equation, is $D = -32t^2 + 48t$, which is equal to 0 for $t = 0$ and for $t = \frac{3}{2}$, larger than zero for $0 < t < \frac{3}{2}$ and smaller than zero otherwise. Since we assumed that $t \neq 1$ and that $t \in \mathbb{Z}_{>0}$, we get that the discriminant is negative. This gives us that there is no intersection point for p_1 with the x-axis, so the left hand side is always positive or always negative as a function of p_1 for a fixed value of t. We can prove which one it is by substituting a value for p_1. If we take for example $p_1 = 3$, then the left hand side of (5.5) becomes

$$25t^2 - 40t + 4,$$

which is positive for all $t \in \mathbb{Z}$ where $t \neq 1$. This gives us that the left hand side of (5.5) is positive, which is a contradiction. This gives us that the case where $p_2 \nmid t$ is not possible.

Case2 $p_2 \mid t$**:**

Since $p_2 = \max\{p_1, \ldots, p_l\}$ and $p_2 \mid t$, it follows from Theorem (5.3.2) we get that t is either $5, 7$ or 10 with p_2 equal to 5 or 7. So if we have a pseudo-aliquot cycle with more than three primes, we get that $p_2 > 7$, which makes it impossible for p_2 to divide t. Now take a look at the case where $p_2 = 7$. If we have three primes, we get that $p_3 | \#C(\mathbb{F}_{p_2})$, and in the case where we have two primes, we get that $p_1 | \#C(\mathbb{F}_{p_2})$. In either case, we denote by p_i the prime that divides $\#C(\mathbb{F}_{p_2})$. Since p_i is a prime smaller than p_2, we get that $p_i \nmid t$, otherwise we would contradict Theorem (5.3.2). Now recall that $t \mid \#C(\mathbb{F}_{p_2})$ and $p_i \mid \#C(\mathbb{F}_{p_2})$. Thus, $\#C(\mathbb{F}_{p_2}) = p_i \cdot t \cdot m = p_i \cdot p_2 \cdot n \geq p_i \cdot p_2$ for some $m, n \in \mathbb{Z}_{>0}$. By the Hasse-Weil theorem (Theorem 4.1.2), we have $\#C(\mathbb{F}_{p_2}) \leq p_2 + 1 + 2\sqrt{p_2}$. If we combine both equations, we get that

$$p_i \cdot p_2 \leq p_2 + 1 + 2\sqrt{p_2}.$$

Dividing both sides of the equation by p_2 gives

$$p_i \leq \frac{p_2 + 1 + 2\sqrt{p_2}}{p_2}.$$

Since $p_i \geq 3$, we get the following:

$$3 \leq \frac{p_2 + 1 + 2\sqrt{p_2}}{p_2} = \frac{7 + 1 + 2\sqrt{7}}{7} \approx 1.8987.$$

This inequality is incorrect, so $p_2 \neq 7$.

The only case left is the one where $p_2 = 5$. In this case, the length of the cycle must be 2 and we must have $p_1 = 3$. Using the same reasoning as before, we get that

$$p_1 \leq \frac{p_2 + 1 + 2\sqrt{p_2}}{p_2}.$$

By substituting p_1 and p_2, we get

$$3 \leq \frac{5 + 1 + 2\sqrt{5}}{5} \approx 2.0944,$$

which is incorrect, so $p_2 \neq 5$. This gives us that $p_2 \mid t$ is not possible.
So now we have found that both cases $p_2 \nmid t$ and $p_2 \mid t$ are not possible, which gives us that the torsion subgroup T must be trivial for this method to work.

□

Appendix A

Appendix

A.1 Code for Method 1

In this section of the appendix, a code for **Method 1** is given for the elliptic curve that is defined by $y^2 = x^3 - 8 \cdot x + 4$ for primes $p_1 = 7$ and $p_2 = 5$. This code also works for other curves and other primes, provided that $p_1 | ord(red_{p_2}(P))$ and that $p_2 | ord(red_{p_1}(P))$, where P is a generator for the elliptic curve over $\mathbb{Q}$. The code is stated as follows:

```
load("./quadratic_chabauty_elliptic.sage") #this is a slightly modified version of https://github.com/bianchifrancesca/quadratic_chabauty/blob/master/quadratic_chabauty_elliptic.sage in such a way that all inverses of each potential integral point in C(Q_p) are also given.
E = EllipticCurve([-8,4])
p1 = 7
n = 20 #this is the precision of the computation (we can compute with p-adic numbers only modulo a certain power of p)
p2 = 5
P = E.gens()[0]
E
print "the generator is ", P
print "the rank of the curve is", E.rank()
G = E.torsion_subgroup(); G
Ep1 = E.change_ring(GF(p1)) #the reduction of E modulo p1
Ep2 = E.change_ring(GF(p2))
ord_P_p1 = Ep1(P).order()
ord_P_p2 = Ep2(P).order()
print "order of reduction of p1 is ", ord_P_p1
print "order of reduction of p2 is ", ord_P_p2
E.Np(p1)
E.Np(p2)
ap1,bp1,cp1 = quadratic_chabauty_rank_1(E,p1,n)
ap2,bp2,cp2 = quadratic_chabauty_rank_1(E,p2,n) #first define ap1,bp1,cp1,ap2,bp2 and cp2, where api is the set of known integral points, bpi is the number of points in C(Q_pi) that we want to show do not correspond to integral points and cpi is the set of potential integral points of C(Q_pi)

def nonelistmaker(n): #a list with only Nones
    listofnones = [None] * n
    return listofnones
z=nonelistmaker(bp1)
gz=nonelistmaker(bp1)
log_P_z=nonelistmaker(bp1)
a_mod_ord_P_p1 = nonelistmaker(bp1)

# Now we are going compute Log_P(z) for a point z in E(Q_p1) (to find a mod p1)

gz=nonelistmaker(bp1)
gP1=((E.Np(p1)*P)[0])/((E.Np(p1)*P)[1])
m1= E.Np(p1)
```

```
for i in range(bp1):
    z[i]=cp1[i][0]
    gz[i]=((m1*(z[i]))[0])/((m1*(z[i]))[1])
    log_P_z[i] = gz[i]/gP1
    log_P_z[i]=ZZ(log_P_z[i]%p1)
print "If z[i]=aP, then a is congruent to %s mod %s" %(log_P_z,p1)

# Now we will show how to compute a such that a*red(P) = red(z), where red is reduction
    modulo p1. Here a will be known modulo the order of red(P)

for i in range(bp1):
    for n in range(ord_P_p1):
        if n*Ep1(P) == Ep1(z[i]):
            a_mod_ord_P_p1[i]=n
print "For each i, a is congruent to %s modulo %s, where None means not possible" %(
    a_mod_ord_P_p1, ord_P_p1)

#Last step
ans = nonelistmaker(bp1)
gy = None
gP2=((E.Np(p2)*P)[0])/((E.Np(p2)*P)[1])
m2=E.Np(p2)
for y in cp2:
    for i in range(bp1):
        if a_mod_ord_P_p1[i] != None:
            if y[1] == cp1[i][1]:
                gy = ((m2*(y[0]))[0])/((m2*(y[0]))[1])
                log_P_y = gy/gP2
                for k in range(ord_P_p2/p1):
                    if ZZ(log_P_y %p2) == a_mod_ord_P_p1[i]%p2: #need a mod p2 to be ZZ(
    Log_P_y %p2) for the point to correspond to z2
                        if (k*p1+log_P_z[i])*Ep2(P) == Ep2(y[0]): #need a mod p1 to be
    Log_P_z[i] for the point to correspond to z2
                            ans[i] = y
if ans ==nonelistmaker(bp1):
        print "No point in cp1 can correspond to an integral point"
else:
    print "There is a point in E(Q_p2) which could correspond to a point in E(Q_p1), namely"
    , y
```

The outcome of the code is given as follows:

```
Elliptic Curve defined by y^2 = x^3 - 8*x + 4 over Rational Field
the generator is  (0 : 2 : 1)
the rank of the curve is 1
Torsion Subgroup isomorphic to Trivial group associated to the Elliptic Curve defined by y^2
     = x^3 - 8*x + 4 over Rational Field
order of reduction of p1 is  5
order of reduction of p2 is  7
10
7
W_for_sieving: [((2, 0),), ((2, -4/3),)]
W_for_sieving: [((2, 0),), ((2, -4/3),)]
If z[i]=aP, then a is congruent to [4, 3, 6, 2, 1, 5, 2, 5, 5, 2] mod 7
For each i, a is congruent to [4, 1, None, None, None, None, None, None, None, None] modulo
    5, where None means not possible
No point in cp1 can correspond to an integral point
```

In the outcome, 'W_for_sieving' gives information about the numbers of subsets that quadratic Chabauty gives.

A.2 Code for Method 3

In this section of the appendix, a code for **Method 3** is given for the elliptic curve that is defined by $y^2 + x \cdot y + y = x^3 + x^2 - 21 \cdot x - 45$ for primes $p_1 = 5, p_2 = 7$ and $p_3 = 31$. This code also works for other curves and other primes, provided that $p_1 | ord(red_{p_2}(P))$, that $p_2 | ord(red_{p_1}(P))$ and that $p_1 \cdot p_2 | ord(red_{p_3}(P))$ where P is a generator for the elliptic curve over $\mathbb{Q}$. The code is stated as follows:

```
E = EllipticCurve([1,1,1,-21,-45])
p1 = 5
p2 = 7
p3 = 31
load("./quadratic_chabauty_elliptic.sage") #this is a slightly modified version of https://github.com/bianchifrancesca/quadratic_chabauty/blob/master/quadratic_chabauty_elliptic.sage in such a way that all inverses of each potential integral point in C(Q_p) are also given.
Ep1 = E.change_ring(GF(p1)) #the reduction of E modulo p1
Ep2 = E.change_ring(GF(p2))
Ep3 = E.change_ring(GF(p3))
P = E.gens()[0]
ord_P_p1 = Ep1(P).order()
ord_P_p2 = Ep2(P).order()
ord_P_p3 = Ep3(P).order()
E
print "The generator of E(Q) is", P
print "the rank of the curve is", E.rank()
G = E.torsion_subgroup(); G
print "order of reduction of p1 is ", ord_P_p1
print "order of reduction of p2 is ", ord_P_p2
print "order of reduction of p3 is ", ord_P_p3

E.Np(p1)
E.Np(p2)
E.Np(p3)
n = 30 #this is the precision of the computation (we can compute with p-adic numbers only modulo a certain power of p)
ap1,bp1,cp1 = quadratic_chabauty_rank_1(E,p1,n)
ap2,bp2,cp2 = quadratic_chabauty_rank_1(E,p2,n)
ap3,bp3,cp3 = quadratic_chabauty_rank_1(E,p3,n) #first define api,bpi and cpi where api is the set of known integral points, bpi is the number of points in C(Q_pi) that we want to show do not correspond to integral points and cpi is the set of potential integral points of C(Q_pi)

def nonelistmaker(n): #a list with only Nones
    listofnones = [None] * n
    return listofnones
z=nonelistmaker(bp1)
gz=nonelistmaker(bp1)
log_P_z=nonelistmaker(bp1)
a_mod_ord_P_p1 = nonelistmaker(bp1)

# Now we are going compute Log_P(z) for a point z in E(Q_p1) (to find a mod p1 )

gz=nonelistmaker(bp1)
gP1=((E.Np(p1)*P)[0])/((E.Np(p1)*P)[1])
m1= E.Np(p1)
for i in range(bp1):
    z[i]=cp1[i][0]
    gz[i]=((m1*(z[i]))[0])/((m1*(z[i]))[1])
    log_P_z[i] = gz[i]/gP1
    log_P_z[i]=ZZ(log_P_z[i]%p1)
print "If z[i]=aP, then a is congruent to %s mod %s" %(log_P_z,p1)

# Now we will show how to compute a such that a*red(P) = red(z), where red is reduction modulo p1. Here a will be known modulo the order of red(P)

for i in range(bp1):
    for n in range(ord_P_p1):
```

```
        if n*Ep1(P) == Ep1(z[i]):
            a_mod_ord_P_p1[i]=n
print "For each i, a is congruent to %s modulo %s, where None means not possible" %(
    a_mod_ord_P_p1, ord_P_p1)

#Last step
ans1 = nonelistmaker(bp1)
gy = None
gP2=((E.Np(p2)*P)[0])/((E.Np(p2)*P)[1])
m2=E.Np(p2)
for y in cp2:
    for i in range(bp1):
        if a_mod_ord_P_p1[i] != None:
            if y[1] == cp1[i][1]:
                gy = ((m2*(y[0]))[0])/((m2*(y[0]))[1])
                log_P_y = gy/gP2
                for k in range(ord_P_p2/p1):
                    if ZZ(log_P_y %p2) == a_mod_ord_P_p1[i]%p2: #need a mod p2 to be ZZ(
    Log_P_y %p2) for the point to correspond to z2
                        if (k*p1+log_P_z[i])*Ep2(P) == Ep2(y[0]): #need a mod p1 to be
    Log_P_z[i] for the point to correspond to z2
                            ans1[i] = y
if ans1 ==nonelistmaker(bp1):
        print "No point in cp1 can correspond to an integral point"
else:
    print "There is a point in E(Q_p2) which could correspond to a point in E(Q_p1), namely"
    , ans1

#Continue if there is a point

a_mod_ord_P_p3=nonelistmaker(bp3)
a_mod_ord_P_p3_to_p1=nonelistmaker(bp3)
a_mod_ord_P_p3_to_p2=nonelistmaker(bp3)
ans_p3=nonelistmaker(bp3)
#for x in cp3:
for i in range (bp3):
    for n in range (ord_P_p3):
        if n*Ep3(P) == Ep3(cp3[i][0]):
            a_mod_ord_P_p3[i] = n #compute a such that a*red(P) = red(z), where red is
    reduction modulo 13. Here a will be known modulo the order of red(P)
            a_mod_ord_P_p3_to_p1[i] = a_mod_ord_P_p3[i] % p1 # a mod p1 from a mod ord p3
            a_mod_ord_P_p3_to_p2[i] = a_mod_ord_P_p3[i] % p2 # a mod p2 from a mod ord p3
    for j in range (bp1):
        if cp3[i][1]==cp1[j][1]:
            if ans1[j] != None:
                if a_mod_ord_P_p3_to_p1[i] == log_P_z[j]: # to check if both methods get
    same a mod p1
                    if a_mod_ord_P_p3_to_p2[i] == a_mod_ord_P_p1[j]%p2: # to check if both
    methods give a mod p2
                        ans_p3[i] = cp3[i]
if ans_p3 == nonelistmaker(bp3):
    print "No point in cp1 can correspond to an integral point"
else:
    print "There is a point in E(Q_p3) which could correspond to a point in E(Q_p1) and E(
    Q_p2), namely", ans_p3
```

The outcome of the code is given as follows:

```
Elliptic Curve defined by y^2 + x*y + y = x^3 + x^2 - 21*x - 45 over Rational Field
The generator of E(Q) is (-3 : 2 : 1)
the rank of the curve is 1
Torsion Subgroup isomorphic to Trivial group associated to the Elliptic Curve defined by y^2
     + x*y + y = x^3 + x^2 - 21*x - 45 over Rational Field
order of reduction of p1 is  7
order of reduction of p2 is  10
order of reduction of p3 is  35
7
10
35
```

```
W_for_sieving: [((2, -2/3),)]
W_for_sieving: [((2, -2/3),)]
W_for_sieving: [((2, -2/3),)]
If z[i]=aP, then a is congruent to [3, 2, 0, 0, 3, 0, 2, 0] mod 5
For each i, a is congruent to [2, 5, 6, 1, 4, 4, 3, 3] modulo 7, where None means not
    possible
There is a point in E(Q_p2) which could correspond to a point in E(Q_p1), namely [((6 + 5*7
    + 6*7^3 + 2*7^5 + 7^6 + 6*7^7 + 2*7^8 + 6*7^9 + 6*7^10 + 5*7^12 + 2*7^13 + 6*7^14 +
    5*7^15 + 7^16 + 4*7^17 + 2*7^18 + O(7^19) : 2 + 7 + 5*7^2 + 5*7^3 + 6*7^4 + 2*7^5 + 7^6
    + 6*7^7 + 4*7^8 + 3*7^9 + 2*7^10 + 2*7^11 + 3*7^12 + 2*7^13 + 3*7^14 + 2*7^15 + 3*7^16 +
     7^17 + 2*7^18 + O(7^19) : 1 + O(7^30)), ((2, -2/3),)), ((6 + 5*7 + 6*7^3 + 2*7^5 + 7^6
    + 6*7^7 + 2*7^8 + 6*7^9 + 6*7^10 + 5*7^12 + 2*7^13 + 6*7^14 + 5*7^15 + 7^16 + 4*7^17 +
    2*7^18 + O(7^19) : 5 + 6*7 + 2*7^3 + 6*7^4 + 7^5 + 4*7^6 + 7^7 + 6*7^8 + 3*7^9 + 4*7^10
    + 3*7^11 + 5*7^12 + 7^13 + 4*7^14 + 5*7^15 + 7^16 + 7^17 + 2*7^18 + O(7^19) : 1 + O
    (7^30)), ((2, -2/3),)), None, None, None, ((1 + 5*7 + 7^2 + 7^3 + 7^5 + 3*7^6 + 4*7^7 +
    7^8 + 6*7^9 + 7^10 + 4*7^11 + 4*7^12 + 4*7^13 + 6*7^14 + 3*7^17 + 5*7^18 + 3*7^19 + O
    (7^20) : 6 + 5*7 + 4*7^2 + 2*7^3 + 5*7^4 + 2*7^5 + 7^6 + 2*7^7 + 3*7^8 + 2*7^9 + 5*7^10
    + 5*7^11 + 6*7^12 + 7^13 + 4*7^14 + 2*7^15 + 7^16 + 3*7^17 + 7^18 + O(7^19) : 1 + O
    (7^30)), ((2, -2/3),)), None, ((1 + 5*7 + 7^2 + 7^3 + 7^5 + 3*7^6 + 4*7^7 + 7^8 + 6*7^9
    + 7^10 + 4*7^11 + 4*7^12 + 4*7^13 + 6*7^14 + 3*7^17 + 5*7^18 + 3*7^19 + O(7^20) : 6 +
    2*7 + 3*7^3 + 7^4 + 3*7^5 + 2*7^6 + 2*7^8 + 5*7^9 + 6*7^10 + 3*7^11 + 2*7^12 + 3*7^14 +
    3*7^15 + 5*7^16 + O(7^19) : 1 + O(7^30)), ((2, -2/3),))]
No point in cp1 can correspond to an integral point
```

Bibliography

[1] Balakrishnan, J., Besser, A., and Müller, J. (2017). Computing integral points on hyperelliptic curves using quadratic Chabauty. Mathematics of Computation, 86(305), 1403-1434.

[2] Evertse, J. H. (2011). p-Adic Numbers. Lecture notes, Leiden University.

[3] Flynn, V. Elliptic Curves. HT 2019/20: Preliminary Reading, available at University of Oxford {https://courses.maths.ox.ac.uk/node/view_material/47117}

[4] Flynn, V. Elliptic Curves. HT 2019/20, available at University of Oxford {https://courses.maths.ox.ac.uk/node/view_material/47116}

[5] Gica, A. (2006) Rational Points on Elliptic Curves. Aailable on http://www.imar.ro/~sergium/ens/Rational.pdf

[6] How to Transform a Cubic (With a Rational Point) into Weierstrass Normal Form. Available on https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/Matsuura-projective_transformation.pdf

[7] Husemöller, D. (1987). Elliptic curves, volume 111 of. Graduate Texts in Mathematics, 99.

[8] LMFDB, https://www.lmfdb.org/EllipticCurve/Q/404/b/1

[9] LMFDB, https://www.lmfdb.org/EllipticCurve/Q/906/e/1

[10] Milne, J. S. (1996). Elliptic curves. Available on http://www.jmilne.org/math/CourseNotes/math679.html.

[11] Silverman, J. H. (2009). The arithmetic of elliptic curves (Vol. 106). Springer Science & Business Media.

[12] Silverman, J. H., and Tate, J. T. (1992). Rational points on elliptic curves (Vol. 9). New York: Springer-Verlag. Silverman,

[13] Winter, R. (2011). Elliptic curves over $\mathbb{Q}_p$. Universiteit Leiden.