S. Alberts

Quadratic points on modular curves

Master thesis

Supervisor: Dr. P.J. Bruin

Date: November 24, 2017

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction **3**

1 Modular and hyperelliptic curves **5**
1.1 The definition of modular curves 5
1.2 The Tate normal form of elliptic curves 7
1.3 A few low level examples of modular curves 9
1.3.1 The universal elliptic curve for $X_1(4)$ 9
1.3.2 The universal elliptic curve for $X_1(5)$ 10
1.4 Mumford representations 10
1.5 A classification of points on genus 2 hyperelliptic curves 12

2 Counting points of the Jacobian **16**
2.1 Reduction modulo primes 16
2.2 Selmer groups 16
2.2.1 Galois cohomology 17
2.2.2 Restriction 18
2.2.3 The definition of Selmer groups 19

3 Points on $X_1(13)$ **20**
3.1 A hyperelliptic equation for $X_1(13)$ 20
3.2 Classifying points on $X_1(13)$ over quadratic extensions of $\mathbb{Q}(\zeta_{13})^+$ 21

4 An equation for $X_1(16)$ **23**
4.1 The universal elliptic curve for $X_1(8)$ 23
4.2 A hyperelliptic equation for $X_1(16)$ 24
4.3 The universal elliptic curve for $X_1(16)$ 25

5 The Jacobian of $X_1(16)$ **27**
5.1 Counting the points of $J_1(16)(K)$ 27
5.2 Classifying points on $X_1(16)$ over quadratic extensions of $\mathbb{Q}(\zeta_{16})^+$ 28

A Lists of elliptic curves with torsion points **30**
A.1 List of elliptic curves with a point of order 13 30
A.2 List of elliptic curves with a point of order 16 32

B Codes **34**
B.1 Magma code for listing the points of $X_1(13)$ 34
B.2 Magma code for listing the points of $X_1(16)$ 36

Introduction

For many years, people have been interested in the possible torsion structures of elliptic curves over a given base field K. For $K = \mathbb{Q}$, Mazur gave a complete list of possible torsion structures of elliptic curves in the article [Mazu] from 1977.

Theorem (Mazur)**.**
If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups: $\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $m \in \{1, \ldots, 10\} \cup \{12\}$ and $n \in \{2, 4, 6, 8\}$.

The proof of this theorem uses modular curves. We will be using modular curves to study 13- and 16-torsion points of elliptic curves over number fields.

Modular curves are curves that parametrize pairs of an elliptic curve, together with some torsion structure. This torsion structure can be a finite subgroup, a point or something else. What torsion structure it is depends on the modular curve. Over the complex numbers, modular curves can be obtained by taking quotients of the upper half plane by congruence subgroups. We consider the curves $Y_1(N)$ for $N \geq 4$. The points of these curves correspond in a natural way to pairs of an elliptic curve together with a point of order N, up to isomorphism.

The article [KaNe] started to list the quadratic points of the curve $X_1(13)$ over $\mathbb{Q}(\zeta_{13})^+$. Using the results of [KaNe] about the Jacobian of $X_1(13)$, we will finish this list. After this, we use many of the same techniques that we used for $X_1(13)$ to list all quadratic points of $X_1(16)$ over $\mathbb{Q}(\zeta_{16})^+$. It will also be explained which elliptic curves correspond to all these quadratic points.

The curves $X_1(13)$ and $X_1(16)$ are hyperelliptic curves of genus 2. Therefore, the first chapter will contain some general theory about modular and hyperelliptic curves. We will discuss the basic definitions and properties of modular curves. After this, we will move on to hyperelliptic curves and their Jacobians. Chapter 1 will finish by proving a theorem about how to classify all quadratic points of hyperelliptic curves of genus 2. To find all quadratic points of $X_1(13)$ and $X_1(16)$, we need to use the points of their Jacobians. Chapter 2 will cover two methods of bounding the torsion subgroup of the Jacobian of any abelian variety. These methods involve reduction modulo primes and Selmer groups.

Chapter 3 starts by deriving a hyperelliptic equation for $X_1(13)$. Then the theory from chapter 1 will be used to list the points of $X_1(13)$ defined over quadratic extensions of $\mathbb{Q}(\zeta_{13})^+$. This builds on the article [KaNe]. In chapter 4 we will move on to $X_1(16)$. A hyperelliptic equation will be derived for $X_1(16)$. In chapter 5 we will bound the torsion subgroup of the Jacobian of $X_1(16)$. Then the same techniques as in chapter 3 will be used to list the points of $X_1(16)$ defined over quadratic extensions of $\mathbb{Q}(\zeta_{16})^+$.

This thesis is aimed at master level students who have taken an introductory course in algebraic geometry and elliptic curves. We will not assume any knowledge in scheme theory. This is why we will skip some constructions and precise

definitions that involve schemes. Instead, we will state and use the relevant properties for us.

1 Modular and hyperelliptic curves

In this chapter we give an introduction to modular curves and hyperelliptic curves. We will give the basic definitions and results about modular curves. Then we will discuss the Tate normal form of elliptic curves and give some examples of modular curves. After this we move on to hyperelliptic curves. We state the general definition of hyperelliptic curves and their Jacobian variety. We discuss the Mumford representation of points of the Jacobian. We finish this chapter by showing how these Mumford representations can be used to make a classification of all points of the hyperelliptic curve.

1.1 The definition of modular curves

We start this chapter by giving an introduction to modular curves. The algebraic definition is rather involved. The precise construction is not necessary for our purposes. Therefore, we give the analytic construction of modular curves. This construction only covers modular curves over the complex numbers. In [DiSh] one can read how to define modular curves over arbitrary base fields. First we need the definition of a congruence subgroup.

Definition 1.1 (Congruence subgroup)**.**

1. A **principal congruence subgroup** is a group of the form

$$\Gamma(N) := \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

   for some positive integer N.

2. A **congruence subgroup** is a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ that contains a principal congruence subgroup $\Gamma(N)$. The smallest such N is called the **level** of Γ.

Examples 1.2.

The most important examples of congruence subgroups for our purposes are $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$. Those last two groups are defined by

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N \right\},$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a, d \equiv 1 \bmod N, c \equiv 0 \bmod N \right\}.$$

There is an action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane

$$\mathbb{H} := \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}.$$

This action is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

Therefore, every congruence subgroup acts on $\mathbb{H}$ as well.

Given a congruence subgroup Γ, we can consider the quotient space $Y(\Gamma) := \Gamma\backslash\mathbb{H}$. It is a non-trivial fact that this space has the structure of a Riemann surface. By adding finitely many points to $Y(\Gamma)$, one can obtain a compact Riemann surface denoted by $X(\Gamma)$. The space $X(\Gamma)$ can also be obtained as a quotient space. This is done by extending the upper half plane to $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. This $\mathbb{H}^*$ can be given a topology, which we shall not describe here. Any congruence subgroup Γ is still acting on $\mathbb{H}^*$. We can obtain $X(\Gamma)$ as the quotient space $\Gamma\backslash\mathbb{H}^*$. Although $\mathbb{H}^*$ does not have the structure of a Riemann surface, the quotient space does. For details on the topological and complex structure on these spaces $Y(\Gamma)$ and $X(\Gamma)$, see chapter 2 of [DiSh].

Definition 1.3 (Complex modular curve)**.**

A **complex modular curve** is either:

1. a quotient $Y(\Gamma) := \Gamma\backslash\mathbb{H}$, where Γ is a congruence subgroup;
2. the compactification $X(\Gamma)$ of $Y(\Gamma)$ described above;

where Γ is a congruence subgroup.

Examples 1.4. We denote

$$Y(N) := Y(\Gamma(N)),\ Y_0(N) := Y(\Gamma_0(N)),\ Y_1(N) := Y(\Gamma_1(N)).$$

The compactifications of these curves are denoted by $X(N), X_0(N), X_1(N)$.

Definition 1.5 (Cusps)**.**

Let Γ be a congruence subgroup. The points in $X(\Gamma) - Y(\Gamma)$ are called the **cusps** of $X(\Gamma)$.

The main reason of interest for these curves is their *moduli interpretation*: the points of these curves can be used to classify elliptic curves together with certain torsion data. These curves all have equivalents over arbitrary base fields, as summarized in the following theorem.

Theorem & Definition 1.6.

Let $N \geq 1$ be an integer. There exist algebraic curves $Y(N), Y_0(N)$ and $Y_1(N)$ over $\mathbb{Q}$, such that for all fields K with $\mathrm{char}(K) = 0$ we have:

- If $N \geq 3$, there is a natural one-to-one correspondence between K-points of $Y(N)$ and isomorphism classes of pairs $(E, (P, Q))$, where E is an elliptic curve over K and (P, Q) is a $\mathbb{Z}/N\mathbb{Z}$-basis for the N-torsion of $E(K)$.

- If K is algebraically closed, there is a natural one-to-one correspondence between points of $Y_0(N)$ and isomorphism classes of pairs (E, C), where E is an elliptic curve over K and C is a cyclic subgroup of order N of $E(K)$.

- If $N \geq 4$, there is a natural one-to-one correspondence between points of $Y_1(N)$ and isomorphism classes of pairs (E, P), where E is an elliptic curve over K and P is a point of $E(K)$ of order 13.

By adding finitely many points to these curves, we can obtain smooth projective curves, which are denoted by $X(N)$, $X_0(N)$ and $X_1(N)$ respectively. For $K = \mathbb{C}$, the curves $Y_1(N)$, $Y_0(N)$, $X_1(N)$ and $X_0(N)$ are as defined in Examples 1.4.

As we mentioned before, constructing these modular curves is too involved to include here. Instead, we will just use the existence and moduli interpretation of these curves. The precise definition of the curves and their compactifications is covered in great detail in the book [DiSh].

We will be interested in the curves $X_1(N)$. Given a non-cuspidal point of this curve, we need to be able to calculate the corresponding elliptic curve.

Theorem & Definition 1.7 (Universal elliptic curve)**.**

Let $N \geq 4$ be an integer. There is a family of curves, naturally parametrized by the points of $X_1(N)$, such that every non-cuspidal point of $X_1(N)$ corresponds to an elliptic curve with $(0, 0)$ of order N. This family is called the **universal elliptic curve** for $X_1(N)$.

Concretely, the universal elliptic curve will be given by an equation of the form

$$y^2 + cxy + by = x^3 + bx^2.$$

In this equation, b and c will be rational functions on $X_1(N)$. The equation defines a smooth curve whenever Q is a non-cuspidal point of $X_1(N)$.

Remark 1.8.

For a precise definition of the modular curves $X(N), X_0(N)$ and $X_1(N)$, as well as the universal elliptic curve, we would need to go into what natural means. However, this involves scheme theory. Because we do not want to assume scheme theory as a prerequisite, we will not go into the precise definition here. In our applications, we will have concrete examples of modular curves and explicit correspondences between points and elliptic curves.

1.2 The Tate normal form of elliptic curves

We will now discuss the Tate normal form of an elliptic curve, which we can then use to give some concrete examples of modular curves.

Definition 1.9 (Tate normal form)**.**

Let K be a field, E and elliptic curve over K and $P \in E(K)$ a point that is not of order 1, 2 or 3. The **Tate normal form** of the pair (E, P) is a model for E given by an equation

$$y^2 + cxy + by = x^3 + bx^2,$$

where b, c are in K and $P = (0, 0)$.

One way to derive an equation for $X_1(N)$ is to look at a possible relation between b, c that can be obtained from the fact that P is of order N. We will do this later for $N = 4$ and $N = 5$. Before that, we need to discuss how to find the Tate normal form of such a pair.

We let (E, P) be a pair as in the above definition. Let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

be a Weierstrass equation for E. We can always translate our curve, so we can assume that $P = (0, 0)$. This gives that $a_6 = 0$.

Next, we know that P is not of order 2. This gives that the tangent line to E through P is not vertical. This tangent line is given by the linear parts of the equation for E, so this line is given by $a_3y = a_4x$. Thus we find that $a_3 \neq 0$. We can therefore make the change of variables given by

$$y := y' + \frac{a_4}{a_3}x.$$

Now the tangent line at 0 is given by $y' = 0$.

Substituting this, we get a model for E of the form

$$E : y^2 + b_1xy + b_3y = x^3 + b_2x^2,$$

with $P = (0, 0)$ of order N and $b_3 \neq 0$.

Now we use that P is not a 3-torsion point. This means that $P + P + P \neq 0$. Therefore, the third point on the tangent line on E in $(0, 0)$ is different from $(0, 0)$. This line is given by $y = 0$, giving that $x^3 + b_2x^2$ has a root different from 0; hence $b_2 \neq 0$.

We make another change of variables, by

$$y := \left(\frac{b_3}{b_2}\right)^3 y',\ x := \left(\frac{b_3}{b_2}\right)^2 x'.$$

Substituting this in the equation and dividing by $\left(\frac{b_3}{b_2}\right)^6$, we find the equation

$$y^2 + \frac{b_1b_2}{b_3}xy + \frac{b_2^3}{b_3^2}y = x^3 + \frac{b_2^3}{b_3^2}x^2.$$

By writing $c = \frac{b_1b_2}{b_3}$ and $b = \frac{b_2^3}{b_3^2}$, we see that this is the desired form. In summary, we have found the following algorithm.

Algorithm 1.10 (Derivation of the Tate normal form)**.** Let E be an elliptic curve given by a Weierstrass equation

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6. \tag{1.2}$$

Let $P = (x_0, y_0)$ be a point of order $N \geq 4$.

1: Substitute

$$x = x' + x_0, y = y' + y_0$$

into equation (1.2). To simplify the notation, we omit the primes. We obtain the following equation for E:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x. \tag{1.3}$$

2: Substitute

$$y = y' + \frac{a_4}{a_3}x$$

into equation (1.3). We obtain the following equation for E:

$$y^2 + b_1xy + b_3y = x^3 + b_2x^2. \tag{1.4}$$

3: Substitute

$$y = \left(\frac{b_3}{b_2}\right)y',\ x = \left(\frac{b_3}{b_2}\right)x'$$

into equation (1.4).

4: Divide the equation obtained in step 3 by $\left(\frac{b_3}{b_2}\right)^6$.

Remark 1.11. The Tate normal form is the unique Weierstrass equation with the conditions that $P = (0, 0)$, the tangent line at P is horizontal and $a_2 = a_3$. This is because the only admissible coordinate changes on elliptic curves are given by

$$x = u^2x' + r,\ y = u^3y' + su^2x + t,$$

where $u \in K^\times$ and $r, s, t \in K$. There is no non-trivial coordinate change that respects the above conditions on the Tate normal form.

1.3 A few low level examples of modular curves

We want to give some examples of modular curves. We will derive the universal elliptic curve for $X_1(4)$ and $X_1(5)$.

1.3.1 The universal elliptic curve for $X_1(4)$

We let $N = 4$. Let (E, P) be a pair of an elliptic curve E and a point P of order 4, given in Tate normal form. So we have $P = (0, 0)$ and E is given by an equation of the form

$$y^2 + cxy + by = x^3 + bx^2.$$

First we compute $-2 \cdot P$, which is the third intersection point of the tangent line at P with E. This line is horizontal, and we find that $-2 \cdot P = (-b, 0)$. Because this point is of order 2, the tangent line here is vertical. We translate $(-b, 0)$ to 0, by substituting $x = x' - b$. We find

$$y^2 + c(x' - b)y + by = (x' - b)^3 + b(x' - b)^2.$$

The linear part of this equation gives an equation for the tangent line. We get

$$-cby + by = 3b^2x' - 2b^2x'.$$

This line is vertical precisely if $c = 1$. Therefore, we find that E is given by

$$y^2 + xy + by = x^3 + bx^2 \tag{1.5}$$

with $b \neq 0$. This is the equation for the universal elliptic curve for $X_1(4)$. The discriminant of this equation is $-16b^5 + b^4$. So if $b = \frac{1}{16}$, the resulting curve is not smooth. Therefore, $\frac{1}{16}$ is a cusp of $X_1(4)$. We find that

$$Y_1(4)(K) = \left\{ b \in K^\times \;\middle|\; b \neq \frac{1}{16} \right\},$$

and $X_1(4)$ is the projective line over K. The three cusps of $X_1(4)$ are 0, $\frac{1}{16}$ and the point at infinity.

1.3.2 The universal elliptic curve for $X_1(5)$

We now take $N = 5$ and as before our pair (E, P) is in Tate normal form, so E is given by

$$y^2 + cxy + by = x^3 + bx^2. \tag{1.6}$$

The tangent line at $-2P = (-b, 0)$ is given by

$$y = \frac{b}{1-c}(x + b).$$

We know that $c \neq 1$, because then P would be of order 4, so we are not dividing by 0. Substituting this into equation (1.6) gives us a degree 3 equation for the x-coordinate of $4P = -2 \cdot -2P$. Solving this equation gives us the x-coordinate $\frac{b^2+bc-b}{c^2-2c+1}$ for $4P$. Now using that $4P = -P = (0, -b)$, we find that

$$\frac{-b^2 + bc - b}{c^2 - 2c + 1} = 0.$$

This gives $b(-b + c - 1) = 0$. Because $b \neq 0$, we find that $c = 1 + b$. So the universal elliptic curve for $X_1(5)$ becomes

$$E : y^2 + (1 + b)xy + by = x^3 + bx^2.$$

We see that $X_1(5)$ is the projective line.

These are relatively simple, in both cases the resulting curve is a line. In chapters 3 and 4, more complicated modular curves will be described.

1.4 Mumford representations

In section 1.3 we chose to discuss $X_1(4)$ and $X_1(5)$ because they are relatively simple to describe. The result of this is that we have found a line twice. Later on in this thesis we will be looking at more complicated examples, which turn out to be hyperelliptic curves. Therefore, we need to discuss hyperelliptic curves.

Definition 1.12 (Hyperelliptic curve)**.** A **hyperelliptic curve** over a field K is a smooth projective curve of genus at least 2, that admits a double cover to the projective line.

Any hyperelliptic curve X can be given by an equation of the form $y^2+h(x)y = f(x)$, and if $\text{char}(K) \neq 2$ this can be rewritten into the form $y^2 = f(x)$. These equations are called **hyperelliptic equations** for X.

In a regular projective plane, hyperelliptic equations do not describe a smooth curve. Therefore, hyperelliptic curves are embedded in the weighted projective space $\mathbb{P}(1 : g + 1 : 1)$, where g is the genus of X.

When E is an elliptic curve over K, we know that its set of K-points is an abelian group. This group structure is useful when trying to find points. When X is a hyperelliptic curve, we do not have a group structure on $X(K)$. That is why we need the Jacobian variety of X. Whenever $X(K)$ is non-empty, the K-points of the abelian variety J form a group isomorphic to the Picard group of X.

Definition 1.13 (Picard group)**.** Let X be a curve over a field K. The Picard group of X is the group $\text{Pic}^0(X)$ of K-rational divisors of X of degree 0, modulo principal divisors.

Theorem & Definition 1.14 (Jacobian variety)**.**

Let X be a hyperelliptic curve over a field K with $X(K) \neq \varnothing$. There is an abelian variety $J(X)$, for which its group of K-points is naturally isomorphic to the Picard group of X. This variety $J(X)$ is called the **Jacobian variety** of X.

Remark 1.15.

As with the definition of modular curves, there is a notion of naturality in the definition of the Jacobian. This naturality involves scheme theory and therefore we will not explain what it means here.

The construction of the Jacobian is too complicated to describe here. For this we refer to [MiJV]. As we did with modular curves, we will just use the existence and properties of Jacobian varieties.

The reason we need Jacobian varieties is because we can use their points to extract points of the original curve. We will run the involved calculations in Magma. For this we need the following definition.

Definition 1.16 (Mumford representation)**.**

Let X be a hyperelliptic curve over a field K, given by

$$y^2 + h(x)y = f(x).$$

Let g be the genus of X. Let $J(X)$ be the Jacobian of X. The **Mumford representation** of a point in $J(X)(K)$ is a triple $(a(x), b(x), d)$, where:

- $a(x)$ and $b(x)$ are polynomials over K;
- $a(x)$ is monic of degree at most g;
- $b(x)$ has degree at most $g + 1$;
- $a(x)$ divides $b(x)^2 + h(x)b(x) - f(x)$;
- d is a positive integer with $\deg(a(x)) \leq d \leq g + 1$, such that

$$\deg(b(x)^2 + h(x)b(x) - f(x)) \leq 2g + 2 - d + \deg(a(x)).$$

Every non-zero K-point of $J(X)$ has a unique Mumford representation, see theorem 4.145 of [CoFr]. In algorithm 1.17 we will explain how to find a divisor class corresponding to a K-point of $J(X)$ in Mumford representation. Magma lists points of $J(X)$ in Mumford representation. From these Mumford representations we can extract points of X. A K-point of $J(X)$ is an element of the Picard group of X, so it is an equivalence class of a degree 0 divisor. A representative of this equivalence class is a sum of points of X. We will now describe an algorithm to find such a representative from a Mumford representation.

There are some technicalities which make this more complicated when g is odd and X has no K-rational points at infinity. This is irrelevant for our purposes, so we will assume that g is even and X has at least one K-rational point at infinity. The following algorithm can also be found in [Magm].

Algorithm 1.17 (Recovering divisors from Mumford representations)**.**

Let X be a hyperelliptic curve over a field K. Assume that its genus g is even and X has at least one K-rational point at infinity. Let $J(X)$ be the Jacobian of X. Let $(a(x), b(x), d)$ be the Mumford representation of a non-zero K-point of $J(X)$.

1: Homogenize the polynomial $a(x)$ to a polynomial $A(x, z)$ of degree d. Homogenize the polynomial $b(x)$ to a polynomial $B(x, z)$ of degree $g + 1$.

2: Solve the equations $A(x, 1) = 0$ and $A(x, 0) = 0$ over an algebraic closure of K.

3: For a solution α of $A(x, 1) = 0$, we put $P_\alpha := (\alpha, b(\alpha))$. For a solution β of $A(x, 0)$ we put $P_\beta := (\beta : B(\beta, 0) : 0)$ in the weighted projective space $\mathbb{P}(1 : g + 1 : 1)$.

4: Let D be the divisor of degree d obtained by summing all the points P_α and P_β.

5.1: If X has precisely one K-rational point ∞ at infinity, then $D - d\infty$ is a representative for the triple $(a(x), b(x), d)$.

5.2: If X has more than one K-rational point at infinity, then let ∞_1, ∞_2 be two distinct points at infinity. In this case, d is always even. Then $D - d/2(\infty_1 + \infty_2)$ is a representative for the triple $(a(x), b(x), d)$.

1.5 A classification of points on genus 2 hyperelliptic curves

We finish this chapter by describing a way to classify all points of hyperelliptic curves of genus 2, defined over quadratic extensions of the base field. Let K be a field and X a hyperelliptic curve of genus 2.

Before we can give a proof of our classification theorem, we need a lemma. We consider the variety $\mathrm{Sym}^2 X = (X \times X)/S_2$, where S_2 is the symmetric group permuting the coordinates. This is an alternative description of degree 2 divisors of X. However, with this description we can also view it as a geometric object.

The hyperelliptic map $X \to \mathbb{P}^1$ gives a degree 2 divisor D_∞ which consists of the points that map to $\infty \in \mathbb{P}^1$. If these two points happen to coincide, then this means that D_∞ equals twice this single point. We obtain a map

$$\begin{array}{rccc} \varphi: & \mathrm{Sym}^2 X & \to & J, \\ & D & \mapsto & [D - D_\infty]. \end{array} \tag{1.7}$$

To show how to classify quadratic points of hyperelliptic curves, we need the following lemma.

Lemma 1.18.

Consider the map φ defined in (1.7).

1. Outside of $0 \in J(K)$, the map φ is bijective. That is, for all $0 \neq Q \in J(K)$, the inverse image $\varphi^{-1}(Q)$ consists of a single divisor D_Q.

2. The inverse image $\varphi^{-1}(0)$ is a line. That is,

$$\varphi^{-1}(0) = \{x^{-1}(a) : a \in \mathbb{P}^1(K)\},$$

where $x : X \to \mathbb{P}^1$ is the hyperelliptic map obtained from the equation $y^2 = f(x)$.

Proof.

1. Let $0 \neq Q \in J(K)$. Choose any divisor F_Q of degree 0 which is a representative for Q. We are trying to find a divisor $D_Q \in (\mathrm{Sym}^2 X)(K)$ which satisfies $[D_Q - D_\infty] = [F_Q]$, in other words D_Q has to be linearly equivalent to $F_Q + D_\infty$. We use the Riemann-Roch theorem and Serre duality to find this. We consider the 1-form $\omega = y^{-1}dx$. This has simple zeroes at the infinite points and no poles. Therefore we can take $\mathrm{div}(\omega) = D_\infty$ as a canonical divisor. Riemann-Roch and Serre then give that

$$\dim_K H^0(X, \mathcal{O}_X(F)) - \dim_K H^0(X, \mathcal{O}_X(D_\infty - F)) = 1 - 2 + \deg(F),$$

for all divisors F. Applied to $F = F_Q + D_\infty$ we obtain

$$\dim_K H^0(X, \mathcal{O}_X(F_Q + D_\infty)) - \dim_K H^0(X, \mathcal{O}_X(-F_Q)) = 1.$$

Therefore the space $H^0(X, \mathcal{O}_X(F_Q + D_\infty)$ is non-trivial. We prove that it is one-dimensional. Because $Q \neq 0$, we know that there is no rational function f with $\mathrm{div}(f) - F_Q = 0$. However, because the degree of F_Q is 0, this in fact means that there can not be any f with $\mathrm{div}(f) - F_Q \geq 0$ either. For every point P with $v_P(f) - F_Q(P) > 0$, we would need a P' with $v_{P'}(f) - F_Q(P') < 0$. Therefore, the space $H^0(X, \mathcal{O}_X(-F_Q))$ is trivial. Hence $H^0(X, \mathcal{O}_X(F_Q + D_\infty))$ is one-dimensional.

So there exists a rational function f_Q on X such that $\mathrm{div}(f_Q) + F_Q + D_\infty$ is effective. We can take $D_Q := \mathrm{div}(f_Q) + F_Q + D_\infty$. Any other rational function g satisfying $\mathrm{div}(g) + F_q + D_\infty \geq 0$ lies in the same one-dimensional space as f_Q and is therefore a scalar multiple. Thus, the divisor D_Q is unique.

2. First note that all the points $x^{-1}(a)$ are indeed mapped to 0, as we can look at the rational function $x-a$ on X. This function has zeroes whenever $x = a$ and poles when x is at infinity, so indeed $\mathrm{div}(x-a) = x^{-1}(a) - D_\infty$.

   Suppose now that D_1, D_2 are two distinct degree 2 divisors on X, with $\varphi(D_1) = \varphi(D_2)$. This means that D_1 and D_2 are linearly equivalent. Hyperelliptic maps are unique up to automorphism of $\mathbb{P}^1$. For a proof of this, see [Hart], page 158 and 342. We get a rational function $f : X \to \mathbb{P}^1$ with $\mathrm{div}(f) = D_1 - D_2$. Because the degrees of D_1, D_2 are equal to 2, this map must be a 2-cover. This means that f is the hyperelliptic map x, composed with some automorphism of $\mathbb{P}^1$. Given that $D_1 = f^{-1}(0), D_2 = f^{-1}(\infty)$, the automorphism gives that there are $a, b \in \mathbb{P}^1(K)$ with $D_1 = x^{-1}(a), D_2 = x^{-1}(b)$. This gives that φ is injective outside of $\{x^{-1}(a) : a \in \mathbb{P}^1(K)\}$. Moreover, this means that no point outside of this set is mapped to 0.

□

With this lemma we can formulate and prove the following theorem.

Theorem 1.19 (Classification of points of hyperelliptic curves of genus 2)**.**

Let X be a hyperelliptic curve of genus 2 over a field K of characteristic different from 2. Let X be given by the equation $y^2 = f(x)$. Let J be the Jacobian of X. Then we have the following points that are defined over quadratic extensions of K:

1. For every $a \in K$, we have the points $(a, \pm\sqrt{f(a)})$.

2. Let $Q \in J(K)$ be non-zero. Let $(a(x), b(x), d)$ be its Mumford representation. Then for α a root of $a(x)$, we have the point $(\alpha, b(\alpha))$.

3. Let $Q \in J(K)$ be non-zero. Let $(a(x), b(x), d)$ be its Mumford representation. Let $A(x, z)$ be the degree 2 homogeneous polynomial of a. For a root β of $A(x, 0) = 0$, we have the point $(\beta : b(\beta) : 0)$.

Moreover, the points we listed here are all the points of X that are defined over quadratic extensions of K.

Proof. It is clear that all points listed above are indeed defined over quadratic extensions of K, from the definition of Mumford representations. We have to show that these are all points.

Let L be a quadratic extension of K. Let $P \in X(L)$. The non-trivial K-automorphism σ of L acts on $X(L)$, so we get a point ${}^\sigma P$. This gives a degree 2 divisor $D = P + {}^\sigma P$ which is defined over K, and so it is a point of $(\mathrm{Sym}^2 X)(K)$. Lemma 1.18 gives that we have two cases. If $\varphi(D) = 0$, then D is of the form $x^{-1}(a)$ for some $a \in \mathbb{P}^1(K)$. This means that $D = (a, \sqrt{f(a)}) + (a, -\sqrt{f(a)})$ and thus $P = (a, \pm\sqrt{f(a)})$ is of the first form.

Otherwise D is mapped to a non-zero point of $J(K)$, then we know from algorithm 1.17 that P is of the second or third form.

□

Definition 1.20 (Exceptional points)**.** Let K be a field with $\mathrm{char}(K) \neq 2$. Let X be a hyperelliptic curve over K of genus 2, with equation $y^2 = f(x)$. An **exceptional point** of X is a point of X that is defined over a quadratic extension of K and not of the form $(x, \sqrt{f(x)})$.

In later chapters, we will be listing the exceptional points of various modular curves. Theorem 1.19 tells that all exceptional points are obtained from K-rational points of the Jacobian.

2 Counting points of the Jacobian

Theorem 1.19 tells how to find all points on hyperelliptic curves of genus 2 defined over quadratic extensions of the base field, using the points of the Jacobian. Because there is always a family of points parametrized by the base field K, the number of such points will be infinite unless K is finite. However, in some cases it is possible to make a finite list of all exceptional points of hyperelliptic curves. This is only possible when the group of K-points of the Jacobian is finite and when we can explicitly compute all its points. In this section we will provide two methods of bounding the number of torsion points of the Jacobian. When we are dealing with finite Jacobians in later chapters, these methods will be useful to find all its points.

2.1 Reduction modulo primes

In this section, we shall consider a number field K with ring of integers $\mathcal{O}$ and a hyperelliptic curve X over K. We let J be the Jacobian of X. Let X be given by an equation $y^2 = f(x)$, with $f \in \mathcal{O}[x]$. Let $\mathfrak{p}$ be a non-zero prime of K. Let $k(\mathfrak{p})$ be the residue field of K at $\mathfrak{p}$.

Theorem 2.1. Let Δ be the discriminant of f. Suppose $\mathfrak{p} \nmid 2\Delta$. Then:

1. The curve $\overline{X}$ given by $y^2 = f(x) \bmod \mathfrak{p}$ is a hyperelliptic curve over $k(\mathfrak{p})$;
2. If $\overline{J}$ is the Jacobian of $\overline{X}$, then there is a reduction map $J(K) \to \overline{J}(k(\mathfrak{p}))$;
3. Let e be the ramification index of $\mathfrak{p}$. Let p be the prime number lying under $\mathfrak{p}$. Then if $e < p - 1$, then the reduction map $J(K) \to \overline{J}(k(\mathfrak{p}))$ is injective on the torsion subgroup of $J(K)$.

Remark 2.2. The precise definition of the reduction map is too technical to include here. This theorem is a specific case of reduction modulo primes. In general, if A is an abelian variety over a field K, there is a notion of good reduction at a prime $\mathfrak{p}$ of K. At these primes, there is a reduction map from the K-points of A to the $k(\mathfrak{p})$-points of the reduction of A modulo $\mathfrak{p}$. When the hypothesis from part 3 of theorem 2.1 is satisfied, this reduction map is injective on the torsion subgroup of $A(K)$. However, to define good reduction at primes in general, we would need to assume scheme theory. For our purposes, the version stated here is sufficient. In the appendix of [Katz] a proof of the more general version of theorem 2.1 is given.

2.2 Selmer groups

Sometimes reducing modulo primes will not give a sufficient upper bound for the torsion of an abelian variety. Before we can define the Selmer groups, we need to define the Galois cohomology groups. Then we define a restriction map on these Galois cohomology groups. With this map, we will define the Selmer groups, which are certain subgroups of Galois cohomology groups. The construction of the Selmer groups will tell how they can be used to bound the number of points of an abelian variety. We will not go into proofs on this matter, because they

are not relevant for our purposes. We refer to the article [Poon] for details and proofs.

2.2.1 Galois cohomology

Let K be a number field with algebraic closure $\overline{K}$. We write $G := \mathrm{Gal}(\overline{K}/K)$. To define Galois cohomology, we need the definition of G-modules.

Definition 2.3 (G-module)**.**

A **left G-module** is an abelian group A together with a left G-action that distributes over the group structure on A and is continuous. That means, if A is equipped with the discrete topology, the map $G \times A \to A$ is continuous.

Given a G-module A, we can look at its subgroup of G-invariants A^G. Taking the G-invariants of a G-module defines a left-exact functor from the category of G-modules to the category of abelian groups. So if

$$0 \to A \to B \to C \to 0 \tag{2.1}$$

is a short exact sequence of G-modules, the sequence

$$0 \to A^G \to B^G \to C^G \tag{2.2}$$

is still exact, but the last map is in general not surjective.

Definition 2.4 (Galois cohomology groups)**.**

Let M be a G-module. For $i \geq 0$, we define $\mathcal{C}^i(M)$ to be the group of continuous G-equivariant functions from G^{i+1} to M, where the G-action on G^{i+1} is the coordinate-wise multiplication in G and the topology on M is discrete. Together with this, we define coboundary operators $d : \mathcal{C}^i(M) \to \mathcal{C}^{i+1}(M)$. Given $f \in \mathcal{C}^i(M)$, and $(g_0, \ldots, g_{i+1}) \in G^{i+2}$ we put

$$\begin{aligned}(df)(g_0, \ldots, g_{i+1}) := g_0 \cdot f(g_1, \ldots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j f(g_0, \ldots, g_j g_{j+1}, \ldots, g_{i+1}) \\ + (-1)^{i+1} f(g_0, \ldots, g_i).\end{aligned} \tag{2.3}$$

These groups and operators define a cochain complex $\mathcal{C}^\bullet(M)$. The **ith Galois cohomology group of** M is defined to be the ith cohomology group of $\mathcal{C}^\bullet(M)$.

Galois cohomology is functorial in M. We have $H^0(G, M) \cong M^G$. The higher degree Galois cohomology groups are a way of measuring the non-exactness of sequence (2.2). For every short exact sequence

$$0 \to A \to B \to C \to 0,$$

of G-modules, we get a long exact sequence

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to \cdots$$

in Galois cohomology groups. This is obtained by considering the induced short exact sequence

$$0 \to \mathcal{C}^\bullet(A) \to \mathcal{C}^\bullet(B) \to \mathcal{C}^\bullet(C) \to 0$$

of chain complexes and taking the long exact sequence in cohomology of this short exact sequence.

2.2.2 Restriction

To define Selmer groups, we need to define a restriction map on the Galois cohomology groups.

Throughout section 2.2.2, we let K be a number field.

Definition 2.5 (Place)**.**

A **place** of K is an equivalence class of absolute values on K, where two absolute values are equivalent if one is a power of the other.

Definition 2.6 (Non-Archimedean places)**.**

Let v be a place of K. Let $|\cdot|_v$ an absolute value representing v. Then v is called **non-Archimedean** or **finite** if it satisfies the strong triangle inequality

$$|x+y|_v \leq \max\{|x|_v, |y|_v\}$$

for all $x, y \in K$.

If a place v is not non-Archimedean, it is called **Archimedean** or **infinite**.

Non-Archimedean places correspond to prime ideals of K. Given a prime ideal $\mathfrak{p}$ of K and $x \in K^\times$, we can define $\mathrm{ord}_\mathfrak{p}(x)$ to be the largest integer n for which $x \in \mathfrak{p}^n$. The corresponding absolute value is given by $|x|_\mathfrak{p} := c^{\mathrm{ord}_\mathfrak{p}(x)}$, where $c \in (0,1)$.

Archimedean places are obtained from embeddings of K into $\mathbb{C}$. Each pair of complex conjugate embeddings gives an absolute value on K, by restricting the absolute value on $\mathbb{C}$.

At any place v of K we can take the completion K_v. If v corresponds to the prime ideal $\mathfrak{p}$, lying over the prime number p, then K_v will be a finite extension of $\mathbb{Q}_p$. At Archimedean places, the completion will be isomorphic to $\mathbb{R}$ or $\mathbb{C}$.

We choose an algebraic closure $\overline{K}$ of K. For any place v, we choose an algebraic closure $\overline{K_v}$ of K_v. We also choose an embedding $\overline{K} \hookrightarrow \overline{K_v}$. This embedding induces a restriction map

$$\mathrm{res}_v : \mathrm{Gal}(\overline{K_v}/K_v) \to \mathrm{Gal}(\overline{K}/K),$$

which is injective. This follows from corollary 7.62[1] of [MiAN]. We write G for $\mathrm{Gal}(\overline{K}/K)$ and G_v for $\mathrm{Gal}(\overline{K_v}/K_v)$. Let M be any G-module. The restrictions res_v induce maps

$$H^i(G, M) \to H^i(G_v, M).$$

Combining all these maps, we get the map

$$\mathrm{Res} : H^i(G, M) \to \prod_{v \text{ a place}} H^i(G_v, M), \tag{2.4}$$

which is given by restricting on each coordinate.

[1]The corollary is stated for finite extensions of $\mathbb{Q}_p$, but the proof can be generalized to finite extensions of K_v for any number field K.

2.2.3 The definition of Selmer groups

Let K be a number field with algebraic closure $\overline{K}$. Let A be an abelian variety over K. Let $n \geq 2$ be an integer. Let $A[n]$ denote the n-torsion subgroup of $A(\overline{K})$ and $G := \mathrm{Gal}(\overline{K}/K)$. We get the short exact sequence of G-modules

$$0 \to A[n] \to A(\overline{K}) \xrightarrow{\cdot n} A(\overline{K}) \to 0, \tag{2.5}$$

of which we can take the long exact sequence in cohomology. Because $H^0(G, -)$ takes G-invariants, the sequence starts with $A[n]$, $A(K)$ and $A(K)$. We get the following sequence:

$$0 \to A[n] \to A(K) \xrightarrow{\cdot n} A(K) \to H^1(G, A[n]) \to H^1(G, A) \xrightarrow{\cdot n} H^1(G, A) \to \cdots.$$

Note that we abbreviate the notation a bit. For every place v of K, we fix a algebraic closure $\overline{K_v}$ of K_v. We also choose embeddings $\overline{K} \hookrightarrow \overline{K_v}$ for all v. We include the map Res from (2.4) in this picture, to get the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(K)/n & \longrightarrow & H^1(G, A[n]) & \longrightarrow & H^1(G, A)[m] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{Res}} & \overset{\phi}{\searrow} & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \longrightarrow & \prod_v A(K_v)/n & \longrightarrow & \prod_v H^1(G_v, A[n]) & \longrightarrow & \prod_v H^1(G_v, A) & \longrightarrow & 0.
\end{array} \tag{2.6}$$

In this diagram, all products range over all places v of K, and G_v denotes the Galois group $\mathrm{Gal}(\overline{K_v}/K_v)$. The bottom sequence is obtained by starting with sequence (2.5), but with K_v instead of K. This diagram is commutative with exact rows.

Definition 2.7 (Selmer groups)**.**

Let ϕ be the map $H^1(G, A[n]) \to \prod_v H^1(G_v, A)$ from diagram (2.6). The **n-th Selmer group of** A is the kernel of ϕ. It is denoted by $\mathrm{Sel}_n(A)$.

Because the diagram is commutative with exact rows, we see that $A(K)/nA(K)$ is mapped into $\mathrm{Sel}_n(A)$. This means that the Selmer group can be used to bound the size of $A(K)/nA(K)$.

3 Points on $X_1(13)$

Until now, we discussed some general theory about modular and hyperelliptic curves. This chapter is an extension of the article [KaNe], where $X_1(13)$ is studied. The article gives an equation for $X_1(13)$ and calculates the points of the Jacobian. In this chapter, we will be using the universal elliptic curve for $X_1(13)$ to derive another equation. Then we will use the work of [KaNe] and theorem 1.19 to make a list of all exceptional points of $X_1(13)$. The calculations for making this list will be run in Magma.

3.1 A hyperelliptic equation for $X_1(13)$

In this section we will be deriving an equation for $X_1(13)$. The curve $X_1(13)$ is a hyperelliptic curve of genus 2. The article [KaNe] already gave an equation for $X_1(13)$, but we want to link an equation to the universal elliptic curve for $X_1(13)$. That is why we will now derive another equation for $X_1(13)$.

We start with the universal elliptic curve for $X_1(13)$. This universal elliptic curve is given by

$$y^2 + cxy + by = x^3 + bx^2 \tag{3.1}$$

where b and c depend on the points of $X_1(13)$. We make the coordinate change given by

$$b = t(t-1)s,\ c = 1 + (t-1)s. \tag{3.2}$$

These equations give a one-to-one correspondence between s and t, unless $c = 1$ or $c = 1 + b$. In section 1.3 we found that these equations describe $X_1(4)$ and $X_1(5)$, so for $X_1(13)$ we can make this coordinate change. In these new coordinates, the universal elliptic curve is given by

$$y^2 + (1 + (t-1)s)xy + t(t-1)sy = x^3 + t(t-1)sx^2. \tag{3.3}$$

To derive an equation for $X_1(13)$ from this universal elliptic curve, we run some calculations in Magma. We want to determine what it means for $(0,0)$ to be of order 13. So we want to know when $13 \cdot (0,0)$ is the point at infinity. We enter the elliptic curve given by equation (3.3) into Magma. Then we can compute $13 \cdot (0,0)$. This is the point at infinity precisely if the numerators of the x- and y-coordinate vanish. These numerators, p_x and p_y, are two polynomials in s and t. They turn out to be powers of the same irreducible polynomial ϕ_{13}. Specifically, we have $p_x = \phi_{13}^2$ and $p_y = \phi_{13}^3$. Hence we find $\phi_{13} = p_y/p_x$. We get

$$\phi_{13} = t^3 - (s^4 + 5s^3 + 9s^2 + 4s + 2)t^2 + (s^3 + 6s^2 + 3s + 1)t + s^3. \tag{3.4}$$

This is an equation for $X_1(13)$, but it is singular. To get a hyperelliptic equation for $X_1(13)$, we make a few changes of variables.

First we write

$$s = s_1 - 1, \quad t = s_1 t_1 + 1.$$

We substitute this into equation (3.4) and divide the new equation by s_1^3. We get

$$t_1^3 + (-s_1^3 - s_1^2 + 3)t_1^2 + (-2s_1^2 - s_1 + 3)t_1 + (-s_1 + 1). \tag{3.5}$$

We substitute

$$t_1 = \frac{s_1}{t_2} - 1$$

into equation (3.5) and multiply the new equation by $\frac{t_2^3}{s_1^2}$. We get

$$-t_2 s_1^3 + (2t_2^2 - t_2)s_1^2 + (-t_2^3 + 1)s_1 + (t_2^3 - t_2^2). \tag{3.6}$$

We write

$$s_1 = s_2 + t_2.$$

Substituting this in equation (3.6) gives

$$(-s_2^2 - 2s_2 - 1)t_2^2 + (-s_2^3 - s_2^2 + 1)t_2 + s_2. \tag{3.7}$$

We write $q := (-s_2^2 - 2s_2 - 1)$ and we multiply (3.7) by q. This gives

$$(qt_2)^2 + (-s_2^3 - s_2^2 + 1)qt_2 + qs_2. \tag{3.8}$$

We put $v := qt_2$ and $u := s_2$. Our hyperelliptic equation for $X_1(13)$ is

$$v^2 + (-u^3 - u^2 + 1)v - (u^3 + 2u^2 + u) = 0. \tag{3.9}$$

For the purpose of computing points in Magma, we rewrite (3.9) into an equation of the form $y^2 = f(x)$. By completing the square, we get

$$(2v + (-u^3 - u^2 + 1))^2 - (-u^3 - u^2 + 1)^2 - 4(u^3 + 2u^2 + u) = 0. \tag{3.10}$$

We write $x = u, y = 2v + (-u^3 - u^2 + 1)$, to obtain the equation

$$y^2 = f(x) = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1. \tag{3.11}$$

In the next section, we list points of $X_1(13)$ in these (x, y)-coordinates. In our Magma code in appendix B.1 we convert the (x, y)-coordinates back to the (s, t)-coordinates from (3.3).

3.2 Classifying points on $X_1(13)$ over quadratic extensions of $\mathbb{Q}(\zeta_{13})^+$

In this section we give a classification of all the pairs of elliptic curves and points of order 13, defined over quadratic extensions of $K = \mathbb{Q}(\zeta_{13})^+$. This section is a continuation of the article [KaNe]. In the article a primitive element for K is given. This primitive element a satisfies

$$a^6 - a^5 - 5a^4 + 4a^3 + 6a^2 - 3a - 1.$$

Our model of $X_1(13)$ is different from the one used in the [KaNe]. We use the equation

$$y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1$$

that we derived in section 3.1.

The article [KaNe] shows that $X_1(13)(K)$ only contains cusps. There are precisely 12 of them. It is also shown that $J_1(13)$ contains precisely 361 points defined over K. The article finishes by listing some of the exceptional points of $X_1(13)$, which is a list we will complete.

In theorem 1.19 we formulated a way to classify all the exceptional points of $X_1(13)$. Therefore, we need to find all the points on $J_1(13)$. Then we will extract the quadratic points of $X_1(13)$ from the K-points of $J_1(13)$. We do some computations in Magma to find a $\mathbb{Z}/19\mathbb{Z}$-basis for $J_1(13)(K)$. We consider the points $\infty_1 = (1:0:0)$, $P = (0,1)$ and

$$Q = (a^5 - 4a^3 - a^2 + 3a, 6a^5 + 6a^4 - 31a^3 - 19a^2 + 21a + 5)$$

of $X_1(13)(K)$. From these points we get two points $P - \infty_1, Q - \infty_1$ of $J_1(13)(K)$. A calculation in Magma gives that these two points span a group of 361 elements, which is the whole group $J_1(13)(K)$.

We can now compute all points of $J_1(13)(K)$ in Magma by taking $\mathbb{Z}/19\mathbb{Z}$-linear combinations of $P - \infty_1$ and $Q - \infty_1$. Magma will list these points in Mumford representation. As discussed in section 1.4, these Mumford representations will give back points of $X_1(13)$ defined over quadratic extensions of K. These extension fields are quadratic, because the genus of $X_1(13)$ is 2.

This computation produces a list of all elliptic curves together with a point of order 13, up to isomorphism. We run the computation in Magma. The code for this process is included in appendix B.1. The result is a list of 288 elliptic curves with the point $(0,0)$ of order 13.

A list of 288 curves is too big to include in this thesis. Therefore we refine the list. Given curves in our list, we check whether they are defined over $\mathbb{Q}$-isomorphic fields. If this is the case, we check whether the curves themselves are isomorphic after a coordinate change. Any two curves that turn out to be isomorphic, will not be listed twice. This refinement results in a list of 8 elliptic curves with $(0,0)$ as a point of order 13. This list is included at the end of this thesis, in appendix A.1. The code in appendix B.1 produces both the full list of 288 curves and the refined list of 8 curves.

4 An equation for $X_1(16)$

In the previous chapter we have applied the theory from chapter 1 to list points of $X_1(13)$, making use of theorem 1.19. In this chapter we will make a start to do the same for $X_1(16)$.

Like $X_1(13)$, the curve $X_1(16)$ is hyperelliptic of genus 2. Therefore, we can use theorem 1.19 again. However, our research on $X_1(13)$ was a continuation of [KaNe]. For $X_1(16)$ we do all the research ourselves.

In this chapter we will use two-division on the universal elliptic curve for $X_1(4)$ we derived in section 1.3.1 to find the universal elliptic curve for $X_1(8)$. This will then be used to derive an equation for $X_1(16)$. We will relate this equation to the universal elliptic curve for $X_1(16)$.

4.1 The universal elliptic curve for $X_1(8)$

In this first section we will find the universal elliptic curve for $X_1(8)$. For this we use the universal elliptic curve for $X_1(4)$. In section 1.3.1 we found that the universal elliptic curve for this curve is given by

$$y^2 + xy + by = x^3 + bx^2, \tag{4.1}$$

where b is non-zero and $(0,0)$ is a point of order 4. For any pair (E,Q) with Q of order 8, we know that $(E,2Q)$ can be written in the form of (4.1). Therefore if we find all possible two-division points of $(0,0)$ on the universal elliptic curve for $X_1(4)$, we will find all possible points of order 8.

Definition 4.1 (Two-division polynomial)**.**

Let E be an elliptic curve over a field K and P a point of E. The two-division polynomial of (E,P) is the monic polynomial $f \in K[t]$ with the possible x-coordinates of two-division points as its roots. That is, $f(\alpha) = 0$ if and only if there is a point $Q \in E(\overline{K})$ with α as its x-coordinate and $2Q = P$. Here $\overline{K}$ is an algebraic closure of K.

The computation for a two-division polynomial is done in Sage[2]. Write E for the universal elliptic curve given by (4.1). The two-division polynomial for $(E,(0,0))$ is

$$t^4 - bt^2 - 2b^2t - b^3.$$

Hence the equation we get for $X_1(8)$ is

$$t^4 - bt^2 - 2b^2t - b^3 = 0. \tag{4.2}$$

We will now write b as a function of a new parameter r. We write $t = br$. Substituting this in (4.2) gives

$$b^4r^4 - b^3r^2 - 2b^3r - b^3 = 0. \tag{4.3}$$

[2]Magma can list the two-division points defined over the given base field. However, to our knowledge, it can not produce the two-division polynomial of arbitrary points.

We divide this equation by b^3. We can now solve the equation for b. We get

$$b = \frac{r^2 + 2r + 1}{r^4}. \tag{4.4}$$

Thus, we find that $X_1(8)$ is parametrized by the single variable r, so it is the projective line.

Substituting (4.4) expression into (4.1), we get the curve given by

$$y^2 + xy + \frac{r^2 + 2r + 1}{r^4}y = x^3 + \frac{r^2 + 2r + 1}{r^4}x^2. \tag{4.5}$$

This curve has a point Q of order 8, with x-coordinate $br = \frac{r^2+2r+1}{r^3}$. There are two points with that x-coordinate, but only one of the points satisfies $2Q = (0, 0)$. We can compute which point this is by computing the two possible y-coordinates. Then we get two points Q_1 and Q_2. Precisely one of these points satisfies $2Q_i = (0, 0)$. We then have $Q = Q_i$. We find that

$$Q = \left(\frac{r^2 + 2r + 1}{r^3}, \frac{r^3 + 3r^2 + 3r + 1}{r^5}\right)$$

is a point of order 8.

To get the universal elliptic curve for $X_1(8)$ we have to rewrite the pair (E, Q) into its Tate normal form. We follow the algorithm 1.10 from section 1.2. We find that the universal elliptic curve for $X_1(8)$ is given by

$$y^2 + \frac{r^2 + 4r + 2}{r^2 + 3r + 2}xy + \frac{r}{r^2 + 4r + 4}y = x^3 + \frac{r}{r^2 + 4r + 4}x^2. \tag{4.6}$$

4.2 A hyperelliptic equation for $X_1(16)$

In this section we will derive an equation for the universal elliptic curve for $X_1(16)$. We will use the same techniques as in our derivation for the universal elliptic curve for $X_1(8)$. Write E for the universal elliptic curve for $X_1(8)$, so E is given by

$$E : y^2 + \frac{r^2 + 4r + 2}{r^2 + 3r + 2}xy + \frac{r}{r^2 + 4r + 4}y = x^3 + \frac{r}{r^2 + 4r + 4}x^2. \tag{4.7}$$

We compute the two-division polynomial of $(E, (0, 0))$. We let Sage run the computation. This polynomial is

$$s^4 - \frac{r(r^2 + 4r + 2)}{(r + 1)(r + 2)^3}s^2 - \frac{2r^2}{(r + 2)^4}s - \frac{r^3}{(r + 2)^6}. \tag{4.8}$$

We change this into a polynomial equation in two variables by multiplying by all the numerators. This gives the equation

$$(r+1)(r+2)^6s^4 - r(r^2+4r+2)(r+2)^3s^2 - 2r^2(r+1)(r+2)^2s - r^3(r+1) = 0. \tag{4.9}$$

This is a singular equation for $X_1(16)$. We can find a hyperelliptic equation by removing the singularities. We compute this equation and the coordinate change in Magma. Denote C for the curve given by equation (4.9). The Magma command `IsHyperelliptic(C)` gives a hyperelliptic equation for $X_1(16)$, namely

$$v^2 + (u^3 + u^2 + u + 1)v = -u^4 - u^3 - u^2 - u. \tag{4.10}$$

The `IsHyperelliptic` function only gives a coordinate change from (r, s) to (u, v). It does not give a coordinate change from (u, v) to (r, s). Therefore, we use the function `IsIsomorphic`. Let C^{proj} be the projective closure of C. Denote its coordinates by R, S, T.

The function `IsIsomorphic` applied to $(X_1(16), C^{\text{proj}})$ gives the coordinate change from $X_1(16)$ to C^{proj}. We let

$$\begin{array}{rcrcl} u & \mapsto & R(u,v,w) & = & -u^6w - u^4w^3 + u^2w^5 + w^7, \\ v & \mapsto & S(u,v,w) & = & u^7 + u^4v - u^3vw - u^3w^4, \\ w & \mapsto & T(u,v,w) & = & u^6w + 2u^4w^3 + u^2w^5. \end{array}$$

Then the coordinate change from $X_1(16)$ to C^{proj} is given by

$$(u : v : w) \mapsto (R(u, v, w) : S(u, v, w) : T(u, v, w)).$$

Here $X_1(16)$ is identified with its closure in the $(1, 3, 1)$-weighted projective space.

We can restrict to affine coordinates: the infinite points of C^{proj} don't give rise to two-division points of $(0, 0)$. This is because the roots of equation 4.8 are the x-coordinates of all possible two-division points. All other points of C^{proj} will therefore describe infinite points of E. The only infinite point of an elliptic curve is not of order 16. So we can ignore those u, v, w with $T(u, v, w) = 0$. Therefore, for the relevant points we have $r = R/T$ and $s = S/T$. Moreover, the infinite points of $X_1(16)$ in $(u : v : w)$-coordinates are all $\mathbb{Q}$-rational. Mazur's theorem, stated in the introduction of this thesis, implies that the $\mathbb{Q}$-rational points of $X_1(16)$ are cusps.

Because we don't need to consider infinite points, we can restrict to the points with $w = 1$. We can express r and s in terms of u and v. We get

$$\begin{aligned} r &= \frac{-u^6 - u^4 + u^2 + 1}{u^2(u^2+1)^2}, \\ s &= \frac{u^7 + u^4v - u^3v - u^3}{u^2(u^2+1)^2}. \end{aligned} \tag{4.11}$$

4.3 The universal elliptic curve for $X_1(16)$

We finish this chapter by finding the universal elliptic curve for $X_1(16)$. In the last section we found a hyperelliptic equation for $X_1(16)$, given by

$$v^2 + (u^3 + u^2 + u + 1)v = -u^4 - u^3 - u^2 - u. \tag{4.12}$$

To link this equation to the universal elliptic curve for $X_1(16)$, we need to consider the universal elliptic curve for $X_1(8)$. This curve E is given by

$$y^2 + \frac{r^2+4r+2}{r^2+3r+2}xy + \frac{r}{r^2+4r+4}y = x^3 + \frac{r}{r^2+4r+4}x^2. \tag{4.13}$$

We expressed r in (u,v)-coordinates. It is given by

$$r = \frac{-u^6-u^4+u^2+1}{u^2(u^2+1)^2}.$$

We have a two-division point Q of $(0,0)$ on E with

$$s = \frac{u^7+u^4v-u^3v-u^3}{u^2(u^2+1)^2}$$

as its x-coordinate. The pair (E,Q) is a pair of an elliptic curve together with a point of order 16. To find the universal elliptic curve for $X_1(16)$, we have to write this pair in its Tate normal form. To do this, we need to find the corresponding y-coordinate. There are two possible y-coordinates. These give two points Q_1 and Q_2 with x-coordinate s. One of these satisfies $2Q_i = (0,0)$. We get $Q = Q_i$, which gives

$$Q = \left(s, \frac{-u^2(u^2-1)}{(u^2+1)^3}v - \frac{u^2(u^2-1)}{(u^2+1)^2}\right)$$

is a two-division point of $(0,0)$. Hence Q is of order 16.

By running algorithm 1.10, we obtain the universal elliptic curve for $X_1(16)$. It is given by

$$y^2 + c(u,v)xy + b(u,v)y = x^3 + b(u,v)x^2, \tag{4.14}$$

where

$$\begin{aligned} b(u,v) &= \frac{u^4+u^3+u^2+u-1}{u^8(u^2+2u-1)}v + \frac{u^6+2u^5+3u^4+2u^3+u^2-1}{u^7(u^2+2u-1)}, \\ c(u,v) &= \frac{u^4+2u-1}{u^5(u-1)(u^2+2u-1)}v + \frac{u^7+u^6-3u^5+3u^4+u^3+u^2+u-1}{u^4(u-1)(u^2+2u-1)}, \end{aligned} \tag{4.15}$$

and $(0,0)$ is the point of order 16.

5 The Jacobian of $X_1(16)$

In chapter 3, the Jacobian of $X_1(13)$ is used to find all exceptional points of $X_1(13)$. We will do this again for $X_1(16)$, working over the field $K = \mathbb{Q}(\zeta_{16})^+$. We need to find the number of points of the Jacobian of $X_1(16)$ defined over this field. After this, Magma will compute all these points. Then we will finish our research and produce a list of elliptic curves defined over quadratic extensions of our base field, together with a point of order 16.

5.1 Counting the points of $J_1(16)(K)$

Our work here is inspired by the work in [KaNe]. It is based on the theory we discussed in chapter 2.

Let J be the Jacobian of $X_1(16)$. The Magma function `RankBound` gives an upper bound for the rank of the J over K. This bound is 0, which means that the number of K-points of J is finite. So we only need to compute the number of torsion points of $J(K)$.

We use Magma to compute a number of points of $X_1(16)$ defined over K. The infinite points of $X_1(16)$ are $(1:0:0)$ and $(1:-1:0)$. The finite points we found are

$$\begin{array}{cc} (-1,0), & (1,-2), \\ (0,-1), & (0,0), \\ (-a^2+4a-3, 2a^2-8a+6), & (a^2-4a+1, -2a^2+8a-2), \\ (a^2-4a+3, -2a^3+8a^2-6a-2), & (a^2-4a+3, 2a^3-16a^2+38a-26), \\ (-a^2+4a-1, 4a^3-20a^2+18a-2), & (-a^2+4a-1, -4a^3+28a^2-50a+6). \end{array} \tag{5.1}$$

Here a is a primitive element of K, which is an element satisfying

$$a^4 - 8a^3 + 20a^2 - 16a + 2 = 0. \tag{5.2}$$

These elements are written in (u,v)-coordinates. We substitute these coordinates in the equation for the universal elliptic curve, which is given by equations (4.14) and (4.15). Using Magma, we can now verify that the curve described by the resulting equation is singular for all of the points listed in (5.1). Therefore all of these points are cusps.

By taking $\mathbb{Z}$-linear combinations of these cusps we can create 200 K-points of J. We denote

$$\begin{array}{cc} \infty_1 := (1:0:0), & P := (-1,0), \\ Q := (a^2-4a+3, -2a^3+8a^2-6a-2), & R := (-a^2+4a-3, 2a^2-8a+6). \end{array} \tag{5.3}$$

Then all 200 K-points of J we can make are in the set

$$J_{\text{points}} := \{i \cdot (P - \infty_1) + j \cdot (Q - \infty_1) + k \cdot (R - \infty_1) : 1 \leq i, j, k \leq 10\}. \tag{5.4}$$

Theorem 5.1.

The points of $J(K)$ contained in the set J_{points} defined by (5.4) are all points of $J(K)$.

Proof. Our model of $X_1(16)$ has discriminant -2^9, which means that J has good reduction at all primes apart from the ones above 2. Moreover, the discriminant of K is also a power of 2, which means that there is no ramification at any of those primes. As a result, the hypothesis of theorem 2.1 is automatically satisfied for all these primes.

The prime number 17 splits completely in K. Therefore, the residue class field at primes above 17 is $\mathbb{F}_{17}$. Magma gives that the order of $\overline{J}(\mathbb{F}_{17})$ is 400. So the number of points of $J(K)$ is either 200 or 400.

To finish the proof, we need to use the Selmer groups. In section 2.2.3 we found that $J(K)/nJ(K)$ injects into the group $\mathrm{Sel}_n(J)$ for any positive integer n. Magma tells us that the group structure of $\overline{J}(\mathbb{F}_{17})$ is $(\mathbb{Z}/2\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z})^2$. Therefore the group structure $J(K)$ is $(\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/5\mathbb{Z})^2$ or $(\mathbb{Z}/2\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z})^2$. Consequently, the group structure of $J(K)/2J(K)$ is either $(\mathbb{Z}/2\mathbb{Z})^3$ or $(\mathbb{Z}/2\mathbb{Z})^4$. The 2-Selmer group $\mathrm{Sel}_2(J)$ can be computed in Magma. We find that this is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. Because $J(K)/2J(K)$ is isomorphic to a subgroup of $\mathrm{Sel}_2(J)$, this implies that it must be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$. We conclude that $J(K)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3 \oplus (\mathbb{Z}/5\mathbb{Z})^2$ and thus has precisely 200 elements.

□

5.2 Classifying points on $X_1(16)$ over quadratic extensions of $\mathbb{Q}(\zeta_{16})^+$

In this last section we finish listing the exceptional points of $X_1(16)$. This is almost identical to the work done in section 3.2. We define the field $K = \mathbb{Q}(\zeta_{16})^+$ by using the primitive element a defined by

$$a^4 - 8a^3 + 20a^2 - 16a + 2 = 0. \tag{5.5}$$

We enter the curve $X_1(16)$ into Magma by using equation (4.12). After this, we enter the points ∞_1, P, Q, R defined by equation (5.3).

We use these points to create the set J_{points} defined in equation (5.4). As proved in theorem 5.1, these are all the points of the Jacobian of $X_1(16)$ defined over K. Algorithm 1.17 is then used to recover the points of $X_1(16)$ from these $J_1(16)$-points. Finally the formulae from equation 4.15 are used to convert the non-cuspidal points to elliptic curves. The code for this computation can be found in appendix B.2.

The result is a list of 128 elliptic curves defined over quadratic extensions of K, together with $(0, 0)$ as a point of order 16, as well as one new cuspidal point. A list of 128 curves is too long to include in this thesis. We refine the list by checking if two curves defined over $\mathbb{Q}$-isomorphic fields are isomorphic after a coordinate change. If this is the case, we don't list them twice. This gives a list of 9 elliptic curves with a point of order 16, which is included in appendix A.2. The code from appendix B.2 produces both the full list of 128 curves and the refined list of 9 curves.

Remark 5.2. The refinement looks at the orbits of the different curves under the action of the group $\mathrm{Gal}(K/\mathbb{Q}) \times ((\mathbb{Z}/16\mathbb{Z})^\times/\{\pm 1\})$ and takes just one representative from each of these orbits. If the orbits were of equal length, we would

find a total of $8 = 128/16$ curves in the refined list. However, an investigation in Magma yields that there are two orbits of length 8 and seven orbits of length 16. The representative curves from the orbit of length 8 are defined over quadratic extensions of the quadratic subfield of K, which is why they are invariant under the action of a non-trivial subgroup of $\mathrm{Gal}(K/\mathbb{Q})$.

A Lists of elliptic curves with torsion points

A.1 List of elliptic curves with a point of order 13

In section 3.2 we discussed how to list all isomorphism classes of pairs of an elliptic curve with a point of order 13, defined over quadratic extensions of $K = \mathbb{Q}(\zeta_{13})^+$. This list consists of 288 pairs, most of which have quite complicated equations. The refinement we ran compressed this list to 8. We list them as follows: a is the generator for K over $\mathbb{Q}$ as mentioned in [KaNe] and 3.2, and our pairs will be in Tate normal form. Thus, the curves shall be given by an equation of the form

$$y^2 + cxy + by = x^3 + bx^2,$$

and the point of order 13 will be the point $(0, 0)$. This curve shall be defined over the quadratic extension L of K. In the table below we give a defining polynomial for $L = K(u)$, and then list the values of b, c.

Minimal polynomial of u	**Value of** b	**Value of** c
$x^2 + (-a^5 + 5a^3 - 6a)x$ $-a^4 + a^3 + 4a^2 - 2a - 4$	$(6355a^5 - 1840a^4$ $-33102a^3 + 1943a^2$ $+39541a + 8967)u$ $+(5869a^5 - 1701a^4$ $-30567a^3 + 1797a^2$ $+36512a + 8280)$	$(37a^5 - 10a^4$ $-194a^3 + 10a^2$ $+232a + 53)u + 1$
$x^2 + (3a^5 - 2a^4 - 15a^3$ $+9a^2 + 16a - 9)x$ $-a^3 + a^2 + 3a - 2$	$(1881a^5 - 4354a^4$ $-4627a^3 + 14211a^2$ $-4059a - 1853)u$ $+1671a^5 - 3338a^4$ $-4449a^3 + 10755a^2$ $-2739a - 1335$	$(9a^5 - 32a^4 - 12a^3$ $+99a^2 - 34a - 14)u$ $+14a^5 - 23a^4 - 37a^3$ $+64a^2 - 12a - 6$
$x^2 + (a^4 - 2a^3 - 2a^2$ $+2a + 3)x + a^4 - a^3$ $-3a^2 + a + 3$	$(-38325666a^5 + 106197055a^4$ $+3562684a^3 - 159611891a^2$ $+52704627a + 21641771)u$ $-20319726a^5 + 56304183a^4$ $+1888871a^3 - 84623977a^2$ $+27943268a + 11474166$	$(-1224a^5 + 3357a^4$ $+185a^3 - 5043a^2$ $+1577a + 663)u$ $-667a^5 + 1785a^4$ $+192a^3 - 2679a^2$ $+724a + 327$
$x^2 + (a^5 - 2a^4 - 4a^3$ $+7a^2 + 2a - 1)x - a^5$ $+2a^4 + 2a^3 - 6a^2 + 3a$	$(935219a^5 - 1997752a^4$ $-2406392a^3 + 6474863a^2$ $-1744961a - 823164)u$ $-1094129a^5 + 2337201a^4$ $+2815281a^3 - 7575038a^2$ $+2041453a + 963031$	$(328a^5 - 702a^4$ $-842a^3 + 2273a^2$ $-614a - 288)u$ $-383a^5 + 818a^4$ $+986a^3 - 2653a^2$ $+717a + 337$

Minimal polynomial of u	**Value of b**	**Value of c**
$x^2 + (-a^5 + 6a^3 - 8a)x - 4a^5 + a^4 + 21a^3 - a^2 - 25a - 5$	$(470596a^5 - 136856a^4 - 2450016a^3 + 144839a^2 + 2926220a + 663533)u + 1212608a^5 - 352618a^4 - 6313113a^3 + 373120a^2 + 7540245a + 1709796$	$(256a^5 - 73a^4 - 1332a^3 + 69a^2 + 1589a + 377)u + 664a^5 - 192a^4 - 3457a^3 + 198a^2 + 4129a + 946$
$x^2 + (-a^4 + a^3 + 4a^2 - 3a - 2)x + a^5 - a^4 - 4a^3 + 3a^2 + 3a$	$(-7a^5 + 9a^4 + 33a^3 - 37a^2 - 33a + 29)u - 4a^5 + 3a^4 + 16a^3 - 13a^2 - 13a + 10$	$(-a^5 + 2a^4 + 3a^3 - 5a^2 - 3a + 3)u - a^4 + a^3 + a^2 - a + 2$
$x^2 + (-a^5 - a^4 + 3a^3 + 3a^2 - 1)x - a^4 + 3a^2 - 1$	$(7353641a^5 + 6926275a^4 - 23318187a^3 - 15866643a^2 + 13310676a + 3786860)u + 2888976a^5 + 2721078a^4 - 9160860a^3 - 6233419a^2 + 5229275a + 1487718$	$(681a^5 + 646a^4 - 2163a^3 - 1477a^2 + 1236a + 352)u + 270a^5 + 247a^4 - 850a^3 - 570a^2 + 482a + 138$
$x^2 + (2a^5 - 2a^4 - 10a^3 + 7a^2 + 12a - 3)x + 2a^5 - 3a^4 - 10a^3 + 12a^2 + 12a - 8$	$1/13((-11600107a^5 + 14396626a^4 + 54529775a^3 - 59546108a^2 - 55245487a + 48118479)u - 17101529a^5 + 21224264a^4 + 80391009a^3 - 87786250a^2 - 81446202a + 70939084)$	$1/13((-4639a^5 + 5762a^4 + 21797a^3 - 23817a^2 - 22081a + 19240)u - 6831a^5 + 8480a^4 + 32109a^3 - 35071a^2 - 32531a + 28353)$

A.2 List of elliptic curves with a point of order 16

In section 5.2 we discussed how to list all isomorphism classes of pairs of an elliptic curve with a point of order 16, defined over quadratic extension of $K = \mathbb{Q}(\zeta_{16})^+$. This resulted in 128 pairs. After the refinement we ran, this number is reduced to 9 pairs. We let a be the generator of K over $\mathbb{Q}$ defined by equation (5.2), and we list the curves in Tate normal form, given by

$$y^2 + cxy + by = x^3 + bx^2,$$

with $(0, 0)$ as the point of order 16. The base field is the field $L = K(u)$, and we shall list the minimal polynomial for u, and then the values of b and c.

Minimal polynomial of u	**Value of b**	**Value of c**
$x^2 + (-a^3 + 6a^2 - 9a + 3)x - a^2 + 5a - 4$	$1/4\big((12a^3 - 81a^2 + 139a - 19)u + (-5a^3 + 34a^2 - 59a + 9)\big)$	$1/4\big((5a^3 - 34a^2 + 60a - 12)u + (-a^3 + 6a^2 - 6a - 4)\big)$
$x^2 + 1/2(-3a^3 + 16a^2 - 16a)x + 1/2(-3a^3 + 16a^2 - 18a + 2)$	$1/2\big((-348717a^3 + 2736647a^2 - 6557711a + 4581122)u + (417281a^3 - 3274722a^2 + 7847078a - 5481853)\big)$	$(-698a^3 + 5478a^2 - 13128a + 9173)u + 1/2(1671a^3 - 13114a^2 + 31424a - 21948)$
$x^2 + 1/2(a^2 - 2a)x + 1/2(2a^3 - 11a^2 + 14a - 4)$	$1/2\big((3111a^3 - 21047a^2 + 36234a - 5038)u + (-1531a^3 + 10358a^2 - 17833a + 2481)\big)$	$(105a^3 - 710a^2 + 1221a - 168)u + 1/2(-67a^3 + 454a^2 - 784a + 114)$
$x^2 + (-a^3 + 7a^2 - 12a + 3)x - a^3 + 6a^2 - 10a + 2$	$1/2\big((656a^3 - 3424a^2 + 3573a - 425)u + (1683a^3 - 8800a^2 + 9250a - 1180)\big)$	$1/2(-27a^3 + 140a^2 - 144a + 16)u - 36a^3 + 189a^2 - 204a + 31$
$x^2 + 1/2(3a^3 - 19a^2 + 30a - 4)x + 1/2(a^3 - 7a^2 + 12a)$	$1/2\big((-2508a^3 + 10443a^2 - 10136a + 1310)u + (-2016a^3 + 8358a^2 - 8115a + 1049)\big)$	$(32a^3 - 131a^2 + 125a - 16)u + 1/2(57a^3 - 236a^2 + 220a - 26)$
$x^2 + (a^2 - 4a + 4)x - a^2 + 4a - 1$	$1/4\big((-2928299a^3 + 12159003a^2 - 11781066a + 1522080)u + (-10341301a^3 + 42939573a^2 - 41604886a + 5375232)\big)$	$(1181a^3 - 4904a^2 + 4752a - 614)u + 1/2(8341a^3 - 34634a^2 + 33558a - 4334)$

Minimal polynomial of u	**Value of b**	**Value of c**
$x^2 - x - a^2 + 4a - 2$	$1/8(3a^2 - 12a + 16)u$ $+1/4(-4a^2 + 16a - 15)$	$u/2 + 1/2(-a^2 + 4a - 2)$
$x^2 + 1/2(-a^3 + 6a^2$ $-8a + 2)x + 1/2(-a^3$ $+4a^2 - 2a)$	$1/2\left((328005a^3 - 2574104a^2\right.$ $+6168215a - 4309024)u$ $+206560a^3 - 1621033a^2$ $+ 3884412a - 2713593)$	$(-818a^3 + 6419a^2$ $-15381a + 10745)u$ $+1/2(-1031a^3 + 8088a^2$ $-19376a + 13536)$
$x^2 + (-a^2 + 3a$ $+3)x - a^3 + 6a^2$ $-9a + 2$	$1/2\left((5948a^3 - 46676a^2\right.$ $+111846a - 78137)u$ $+18992a^3 - 149052a^2$ $+ 357191a - 249558)$	$1/2(83a^3 - 646a^2$ $+1540a - 1074)u$ $+130a^3 - 1020a^2$ $+2446a - 1712$

B Codes

B.1 Magma code for listing the points of $X_1(13)$

This code is to create the set of points on the Jacobian of $X_1(13)$ defined over $K = \mathbb{Q}(\zeta_{13})^+$, in Mumford representation. After that, we convert these back to points of $X_1(13)$ defined over quadratic extensions of K. Finally we convert them to give a list of elliptic curves with $(0, 0)$ as a point of order 13. After running this code, `EC` will consists of the full list of 288 pairs of curves with $(0, 0)$ as a point of order 13, and `ECref` consists of the refined list we included in this thesis.

```
Q := RationalField();
R<t> := PolynomialRing(Q);
g := t^6 - t^5 - 5*t^4 + 4*t^3 + 6*t^2 -3*t - 1;
K<a> := NumberField(g);
A<x> := PolynomialRing(K);
f := x^6 + 2*x^5 + x^4 + 2*x^3 + 6*x^2 + 4*x + 1;
X := HyperellipticCurve(f);
J := Jacobian(X);
Xpoints := Points(X: Bound := 5);

P := Xpoints[3];
Q := Xpoints[12];
infty1 := Xpoints[1];
//P-infty1,Q-infty1 form a Z/19Z-basis for J

Jpoints := [i*(P-infty1) + j*(Q-infty1) : i in [1..19],
j in [1..19]];
//Creation of all the points of the Jacobian

j := 0; //Counter of curves
k := 0; //Counter of refined curves
l := 0; //Counter of loops
EC := [ ]; //Set of curves
Fields := [ ]; //Set of fields
ECref := [ ]; //Refined set of curves
Fieldsref := [ ]; //Refined set of fields

for n in [1..361] do
    l := l+1;
    h := Jpoints[n];
    if (Degree(h[1]) eq 2) and (IsIrreducible(h[1])) then
    //Only these points of Jpoints give new points
        L<u> := NumberField(h[1]);
        y := Evaluate(h[2],u);
        v := 1/2*(y - (-u^3 - u^2+1));
        t2 := v/(-u^2-2*u-1);
        s1 := t2+u;
```

```
        s := s1-1;
        t1 := s1/t2 -1;
        t := t1*s1 + 1;
        Y := [1+t*s-s, t*(t-1)*s, t*(t-1)*s, 0, 0];
        E:= EllipticCurve(Y);
        //Conversion from coordinates to elliptic curves

        j := j+1;
        EC[j] := E;
        Fields[j] := L;//Count and add curve and field

        B := true;
        //Parameter to check if we have found a new curve
        for m in [1..k] do //The refinement
            L1 := AbsoluteField(L);
            L2 := AbsoluteField(Fieldsref[m]);
            //to get all iso's we have to convert these
            //to fields over Q
            if (IsIsomorphic(L1,L2)) then
                //Are the fields iso?
                Ell1 := ChangeRing(E, L2);
                Ell2 := ChangeRing(ECref[m],L2);
                //Convert E to an elliptic curve over new field
                for sigma in Automorphisms(L2) do
                    Z := [sigma(c) : c in aInvariants(Ell1)];
                    Ell := EllipticCurve(Z);
                    if (IsIsomorphic(Ell,Ell2)) then
                    //Are the curves iso?
                        B := false;
                        //Parameter sets to False
                    end if;
                end for;
            end if;
        end for;
        if B then
        //If parameter is still True, add curve to the list
            k := k+1;
            ECref[k] := E;
            Fieldsref[k] := L;
        end if;
    end if;
    "Number of loops:", l;
    "Number of curves:", k;//To keep track of the process
    " ";
end for;
```

B.2 Magma code for listing the points of $X_1(16)$

This code is to create the set of points on the Jacobian of $X_1(16)$ defined over $K = \mathbb{Q}(\zeta_{16})^+$, in Mumford representation. After that, we convert these back to points of $X_1(16)$ defined over quadratic extensions of K. Finally we convert them to give a list of elliptic curves with $(0,0)$ as a point of order 16. After running this code, `EC` will consists of the full list of 128 pairs of curves with $(0,0)$ as a point of order 16, and `ECref` consists of the refined list we included in this thesis.

```
Q := RationalField();
R<t> := PolynomialRing(Q);
g := t^4-8*t^3+20*t^2-16*t+2;
K<a> := NumberField(g);
A<x> := PolynomialRing(K);
f := - x^4 - x^3 - x^2 - x;
h := x^3 + x^2 + x + 1;
X := HyperellipticCurve(f,h);
J := Jacobian(X);
Xpoints := Points(X: Bound := 5);

P := Xpoints[3];
Q := Xpoints[9];
R := Xpoints[5];
infty1 := Xpoints[1];
//P-infty1,Q-infty1,R-infty1 span J
Jpoints := [i*(P-infty1) + j*(Q-infty1) + k*(R-infty1)
: i in [1..10], j in [1..10], k in [1..10]];

j := 0; //Counter of curves
k := 0; //Counter of refined curves
n := 0; //Counter of cusps
l := 0; //Counter of loops
EC := [ ]; //Set of curves
Fields := [ ]; //Set of fields
ECref := [ ]; //Refined set of curves
Fieldsref := [ ]; //Refined set of fields
Cusps := [ ]; //Set of cusps

for i in [1..200] do
    l := l+1;
    h := Jpoints[i];
    if (Degree(h[1]) eq 2) and (IsIrreducible(h[1])) then
    //Only these points of Jpoints give new points
        L<u> := NumberField(h[1]);
        v := Evaluate(h[2],u);
        c1d := u^4 + 2*u - 1;
        //first component of c, denominator
        c1n := u^8 + u^7 - 3*u^6 + u^5;
        //first component of c, numerator
```

```
c1 := c1d/c1n;
//first component of c
c2d := u^7 + u^6 - 3*u^5 + 3*u^4 + u^3 + u^2 + u - 1;
//etc
c2n := u^7 + u^6 - 3*u^5 + u^4;
c2 := c2d/c2n;
c := c1*v + c2;

b1d := u^4 + u^3 + u^2 + u - 1;
b1n := u^10 + 2*u^9 -u^8;
b1 := b1d/b1n;
b2d := u^6 + 2*u^5 + 3*u^4 + 2*u^3 + u^2 - 1;
b2n := u^9 + 2*u^8 - u^7;
b2 := b2d/b2n;
b := b1*v+b2;

B<x,y> := PolynomialRing(L,2);
Aff := AffineSpace(B);
F := y^2 + c*x*y + b*y - x^3 - b*x^2;
//This data is to check if the curve is smooth
if not IsSingular(Curve(Aff,F)) then
//If it is, we can proceed as before
    E := EllipticCurve([c,b,b,0,0]);
    j := j+1;
    EC[j] := E;
    Fields[j] := L; //count and add curve and field
    B := true;
    //Parameter to check if we have found a new curve
    for m in [1..k] do //The refinement
        L1 := AbsoluteField(L);
        L2 := AbsoluteField(Fieldsref[m]);
        if (IsIsomorphic(L1,L2)) then
        //Are the fields iso?
            Ell1 := ChangeRing(E, L2);
            Ell2 := ChangeRing(ECref[m],L2);
            //Converse to a curve over new field
            for sigma in Automorphisms(L2) do
                Z := [sigma(c) : c in aInvariants(Ell1)];
                Ell := EllipticCurve(Z);
                if (IsIsomorphic(Ell,Ell2)) then
                //Are the curves iso?
                    B := false;
                    //Parameter sets to False
                end if;
            end for;
        end if;
    end for;
    if B then
    //If parameter is still True, add curve to the list
        k := k+1;
```

```
                ECref[k] := E;
                Fieldsref[k] := L;
            end if;
        else //Add to cusps if curve wasn't smooth
            n := n+1;
            Cusps[l] := [u,v];
        end if;
    end if;
    "Number of loops:", l;
    "Number of curves:", k;//To keep track of the process
    " ";
end for;
```

References

[CoFr] Henri Cohen and Gerhard Frey, *Handbook of Elliptic & Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2006.

[DiSh] Fred Diamond and Jerry Shurman, *A First Course in Modular Forms*, Springer, 2005.

[Hart] Robin Hartshorne, *Algebraic Geometry*, Springer, 1977.

[KaNe] S. Kamienny and B. Newman, *Points of order 13 on elliptic curves*, preprint, 2016, arXiv:1608.08672v3.

[Katz] Nicholas M. Katz, *Galois Properties of Points on Abelian Varieties*, Inventiones mathematicae, volume 62 (1981), pages 481–502.

[Magm] N. Bruin, B. Creutz, S. Donnelly, M. Harrison, D. Kohel, P. van Wamelen, *Magma Handbook: Points on the Jacobian*, 2017, `http://magma.maths.usyd.edu.au/magma/handbook/text/1499`.

[Mazu] Barry Mazur, *Modular curves and the Eisenstein ideal,* Publications mathématiques de l'I.H.É.S., tome 47 (1977), pages 33–186.

[MiAN] J.S. Milne, *Algebraic Number Theory*, course notes, 2017, `http://www.jmilne.org/math/CourseNotes/ANT.pdf`.

[MiJV] J.S. Milne, *Jacobian varieties*. Pages 167–212 in: Gary Cornell, Joseph H. Silverman, *Arithmetic Geometry*, Springer, 1986.

[Poon] Bjorn Poonen, *The Selmer group, the Shafarevich-Tate group, and the weak Mordell-Weil theorem*, course notes, 2002, `http://math.univ-lyon1.fr/~roblot/ihp/weakmw.pdf`.

Index

G-module, 15
$X(N)$, 5
$X_0(N)$, 5
$X_1(13)$, 18
$X_1(4)$, 8
$X_1(5)$, 8
$X_1(8)$, 21
$X_1(N)$, 5, 8, 18, 21
$Y(N)$, 5
$Y_0(N)$, 5
$Y_1(N)$, 5
$\Gamma(N)$, 4
$\Gamma_0(N)$, 4
$\Gamma_1(N)$, 4
$\mathbb{H}$, 4
$\mathrm{Pic}^0(X)$, 9
$\mathrm{Sel}_n(A)$, 17

Archimedean, 16

Congruence subgroup, 4
Cusps, 5

Exceptional points, 12, 13

Galois cohomology, 15

Hyperelliptic curve, 9
Hyperelliptic equation, 9
    for $X_1(13)$, 18, 19
    for $X_1(16)$, 22, 23

Jacobian variety, 9

Modular curve, 5
Mumford representation, 10

Non-Archimedean, 16

Picard group, 9
Place, 16

Selmer group, 17

Tate normal form, 6, 7
Two-division polynomial, 21

Universal elliptic curve, 6
    for $X_1(13)$, 18
    for $X_1(16)$, 23, 24
    for $X_1(4)$, 8
    for $X_1(5)$, 8
    for $X_1(8)$, 21, 22