Torsion points on elliptic curves over Q

Vorm, David van der

W.D. van der Vorm

Torsion points on elliptic curves over $\mathbb{Q}$

Master thesis

March 8, 2024

Thesis supervisor: Prof. dr. J.B. Vonk

Leiden University
Mathematical Institute

Contents

1 Introduction

Finding the rational points on an elliptic curve is an example of solving a Diophantine equation. This is one of the oldest problems in mathematics, dating back to ancient Greece, in which one attempts to find integer or rational solutions of polynomials in n variables. Since an elliptic curve E is not only a geometric object (a curve) but also an arithmetic object (an abelian group), we can use the arithmetic of elliptic curve to determine $E(K)$, the points of E that are defined over a number field K. An important early result is the following theorem that was proven for $K = \mathbf{Q}$ by Mordell and generalised to number fields by Weil.

Theorem 1.1 (Mordell-Weil [Mor22], [Wei28])**.** *Let K be a number field and E/K be an elliptic curve. Then the group $E(K)$ is finitely generated.*

In Appendix A, we prove that for any integer $n \geq 2$, the quotient

$$E(K)/nE(K)$$

is finite. This is referred to as the *weak Mordell-Weil Theorem*, and implies Theorem 1.1 after an argument with heights.

Every finitely generated abelian group G is isomorphic to $F \times \mathbf{Z}^r$ for some non-negative integer r and finite group F. The integer r is called the rank of G, and F is called the torsion subgroup of G. Hence the study of the arithmetic of elliptic curves splits into two different areas: determining the rank $r(E(K))$ and determining the torsion subgroup $E_{\text{tors}}(K)$ over a certain number field K. In this thesis, we consider torsion subgroups over $K = \mathbf{Q}$.

1.1 Rational torsion

Both the rank and torsion of elliptic curves are extensively studied. Much is still unknown about the rank, for instance whether it is uniformly bounded. However, the torsion structure over $\mathbf{Q}$ is completely classified, due to Mazur's theorem from 1977.

Theorem 1.2 (Mazur [Maz77a], Theorem 1.8)**.** *Let $E/\mathbf{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbf{Q})$ is isomorphic to one of the following 15 groups:*

$$\mathbf{Z}/n\mathbf{Z} \text{ with } 1 \leq n \leq 10 \text{ or } n = 12,$$

$$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2n\mathbf{Z} \text{ with } 1 \leq n \leq 4.$$

It was long known that these 15 subgroups can occur [Lev08], but the hard part was showing that other groups could not occur, in particular $\mathbf{Z}/n\mathbf{Z}$ where n is a prime bigger than 7.

The case of 13-torsion was settled by Mazur and Tate [MT73], and was the stepping stone to proving Theorem 1.2. We follow Mazur's approach to this problem by studying the *modular curve* $X_1(n)$. This is the compactification of $Y_1(n)$, which is the moduli space of elliptic curves with a point of order n up to isomorphism. Unlike Mazur and Tate, we compute explicit equations for $X_1(n)$, by computing the n-division polynomial from the coordinates of a point on an elliptic curve in Tate normal form. The curve $X_1(n)$ is in some sense easier to study than $Y_1(n)$, but one has to account for the cusps $X_1(n)\backslash Y_1(n)$, that do not correspond to elliptic curves with a point of order n.

The genus of the curve $X_1(n)$ gives information about the possible structure of the set of rational points on the curve. If it has genus 0 and contains a rational point, then it is isomorphic to $\mathbb{P}^1$ and it has infinitely many rational points. If it has genus 1, then it is an elliptic curve and there may be finitely many or infinitely many K-rational points on $X_1(n)$, in accordance with Theorem 1.1. Lastly, we know since Faltings' proof of the Mordell conjecture [Mor22] that a curve of genus at least 2 contains only finitely many rational points [Fal83]. This distinguishes three possible cases, where as usual the complexity of the matter increases with the genus.

1.2 Contribution

The goal of this thesis is to give an overview of the methods of determining $X_1(n)(\mathbf{Q})$ for different genera. We investigate the curves $X_1(n)$ for $n \in \{11, 12, 13\}$, and we will see that the three genera 0, 1 and 2 occur here. However, the methods of finding rational points on the curves differ significantly, which can be attributed to the different genera.

In Chapter 2, we show how to compute equations for the modular curves $X_1(n)$, and find smooth models for $n \in \{11, 12, 13\}$. For $n = 12$, we determine a parametrisation of the set of elliptic curves with a point of order 12 up to isomorphism. In Chapter 3, we continue with the study of the elliptic curve $X_1(11)$. We develop the method of irreducible 2-descent based on theory that is included in appendix A. We apply the 2-descent to find that $X_1(11)(\mathbf{Q})$ only contains cusps, and conclude that there are no elliptic curves over $\mathbf{Q}$ with a point of order 11. In Chapter 4, we consider the curve $X_1(13)$ of genus 2. We discuss aspects of the proof of Mazur and Tate that the rank of the Jacobian of $X_1(13)$ is zero, and hence that the only rational points on $X_1(13)$ are cusps. Furthermore, we highlight more recent methods that prove the same statement. A theorem of Kolyvagin-Logachev [KL90] and Kato [Kat04] shows that the Jacobian has rank zero, and then a theorem by Stoll [Sto06] about the method of Chabauty gives a quick proof that $X_1(13)(\mathbf{Q})$ only contains cusps.

2 The modular curve $X_1(n)$

The goal of this chapter is to find equations for $X_1(n)$. For $n \in \{11, 12, 13\}$, we desingularise the equations and find smooth models. We prove the following theorem.

Theorem 2.1. *There are infinitely many elliptic curves over* $\mathbf{Q}$ *with a rational* 12*-torsion point.*

In §2.1, we define the elliptic curve Tate normal form and explain how to use this to define a singular curve C_n with the same function field as $X_1(n)$. The resolution of singular points of algebraic varieties in general is a rich subject. For our purpose of desingularising the curves C_n, it is not necessary to know a lot of theory. We will see that it suffices to perform a few blow-ups, and that the procedure is in fact very similar for different n. In §2.2, we find the smooth curves that are birationally equivalent to C_n for $n \in \{11, 12, 13\}$, and they serve as models for $X_1(n)$. In agreement with Mazur's theorem, the case of 12-torsion proves to be the easiest and is worked out in §2.2.2. We study the curves $X_1(11)$ in Chapter 3 and $X_1(13)$ in Chapter 4.

2.1 Tate normal form

If $n \geq 4$, then an elliptic curve with a point P of order n can be written in a Weierstrass form with 2 parameters called the *Tate normal form*. From the addition formula, one can find a necessary and sufficient condition on u, v for P to have order n. We use this to define a not necessarily smooth curve C_n that parametrises pairs (E, P) where $P \in E$ has order n. From here, $X_1(n)$ can be obtained by resolving a finite number of singularities. We refer to [Sil09, Chapter III] for the necessary addition, doubling and substitution formulas.

Proposition 2.2. *Let* $n \in \mathbf{N}_{\geq 4}$*,* K *be a number field and* E/K *an elliptic curve with a point* P *of order* n*. Then there are* $u, v \in K$ *such that* E *is isomorphic over* K *to the curve*

$$E_{u,v} : y^2 + uxy + vy = x^3 + vx^2$$

and P *is mapped to the point* $(0, 0)$ *under this isomorphism.*

Proof. The translation of P to $(0, 0)$ allows one to write E in the form

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

Since P does not have order 2, we know that $P \neq -P = (0, -a_3)$ so $a_3 \neq 0$. Hence we can make the substitution $x \mapsto x'$ and $y \mapsto y' + \frac{a_4}{a_3}x'$ to find the isomorphic curve

$$y^2 + \left(a_1 + \frac{2a_4}{a_3}\right)xy + a_3y = x^3 + \left(a_2 - \frac{a_4a_1}{a_3} - \frac{a_4^2}{a_3^2}\right)x^2.$$

Let b_1, b_2, b_3 denote these coefficients, i.e.

$$\begin{aligned} b_1 &= \left(a_1 + 2\tfrac{a_4}{a_3}\right) \\ b_2 &= \left(a_2 - \tfrac{a_4 a_1}{a_3} - \tfrac{a_4^2}{a_3^2}\right) \\ b_3 &= a_3. \end{aligned}$$

The point P is still at $(0,0)$, so $2P = (-b_2, b_2 b_1 - b_3)$ and $-P = (0, -b_3)$. Since P does not have order 3, these points are not equal, and $b_2 \neq 0$. Hence $t = b_3/b_2$ is well-defined and nonzero. We can make the substitution $x \mapsto t^2 x'$ and $y \mapsto t^3 y'$ and divide by t^6 to obtain the isomorphic curve

$$y^2 + t^{-1} b_1 xy + t^{-3} b_3 y = x^3 + t^{-2} b_2 x^2.$$

Let $u = t^{-1} b_1$ and $v = t^{-2} b_2 = t^{-3} b_3$. We finally have

$$E_{u,v} : y^2 + uxy + vy = x^3 + vx^2.$$

□

The discriminant $\Delta_{u,v}$ of $E_{u,v}$ factors over $\mathbf{Q}(u,v)$ as

$$\Delta_{u,v} = -v^3 \cdot (u^4 - u^3 + 8u^2 v - 36uv + 16v^2 + 27v).$$

If $E_{u,v}$ is an elliptic curve, then $nP = 0$ if and only if the denominator of $y(nP)$ is zero. This denominator is the third power of the *n-division polynomial* ψ_n [Eng99]. One can compute the division polynomials from the elliptic divisibity sequence as in [Sil09, Exercise 3.7], but for our purpose it is easy enough to compute the coordinates of nP in Sage.

For $n \in \mathbf{N}_{\geq 4}$, let F_n be ψ_n with all factors in common with $\Delta_{u,v}$ or F_m for $m < n$ removed. Define

$$C_n : F_n(P) = 0.$$

Now smooth points on C_n correspond canonically to isomorphism classes of elliptic curves with a point of order n. Hence the unique smooth curve, up to isomorphism, that is birationally equivalent to C_n, is a smooth model for $X_1(n)$. We denote this model by $X_1(n)$ for convenience. A cusp of $X_1(n)$ is a point that is mapped under this birational equivalence to zero or pole of $\Delta_{u,v}$. Equivalently, the cusps of $X_1(n)$ are exactly the points that do not correspond to an elliptic curve with a point of order n. Since F_n does not have factors in common with $\Delta_{u,v}$, there are finitely many cusps on $X_1(n)$.

Definition 2.3. The curve $Y_1(n)$ is the open subcurve of $X_1(n)$ of non-cuspidal points.

We then have a bijection

$$\begin{array}{rcl} \{(E,P) : E \text{ an elliptic curve}, P \in E[n]\} / \cong & \xrightarrow{\sim} & Y_1(n) \\ (E_{u,v}, (0,0)) & \longmapsto & (u:v:1). \end{array}$$

Two pairs $(E,P), (E',P')$ are isomorphic if and only if there is an isomorphism $\varphi : E \to E'$ of elliptic curves with $\varphi(P) = P'$. Under the bijection above, elliptic curves defined over a field K correspond precisely to the points of $Y_1(n)$ defined over K. So for any number field K we get a bijection

$$\begin{array}{rcl} \{(E,P) : E \text{ an elliptic curve over } K, P \in E(K)[n]\} / \{\pm 1\} & \xrightarrow{\sim} & Y_1(n)(K) \\ (E_{u,v}, (0,0)) & \longmapsto & (u:v:1). \end{array}$$

This reduces the question of finding all elliptic curves over K with a point of order n, to finding all K-rational points on the curve $Y_1(n)$. In practice, we determine $X_1(n)(K)$ and check which points are cusps.

2.2 Smooth equations for $X_1(n)$

In this section, we describe how to desingularise C_n to find an explicit equation for $X_1(n)$. In the second part, we compute equations for $X_1(n)$ for $n \in \{11, 12, 13\}$.

The curve C_n is smooth for $n \leq 6$, but it is singular at $(1,0)$ for $7 \leq n \leq 13$, and presumably for all $n \geq 7$. It turns out that resolving the singularity of C_7 is the first step in resolving the singularity of C_n for $n > 7$. To show this, we rewrite C_7 to $X_1(7)$ step by step, and use this C_7-substitution to desingularise C_{12} for illustration.

The curve C_7 is

$$C_7 : u^3 - 3u^2 - uv + v^2 + 3u + v - 1 = 0$$

with a node at $(1,0)$ and no other singularities (see Figure 1). The birational equivalence $u \mapsto b+1$ and $v \mapsto b(a+1)$ gives the curve

$$C_7' : a^2 + a + b = 0$$

which is a smooth equation. It is isomorphic to a line by $a \mapsto c$ and $b \mapsto (d-1)c$, which gives

$$C_7'' : c + d = 0.$$

The full substitution is $u = (d-1)c + 1$ and $v = (c+1)(d-1)c$.

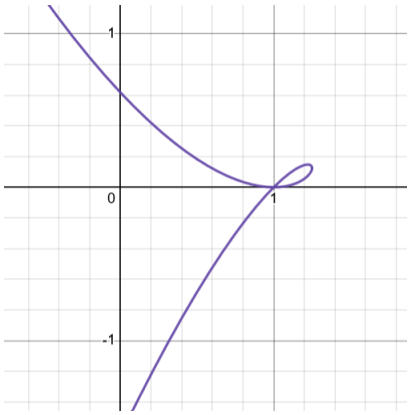

Figure 1: $C_7(\mathbb{R})$ around $(1,0)$

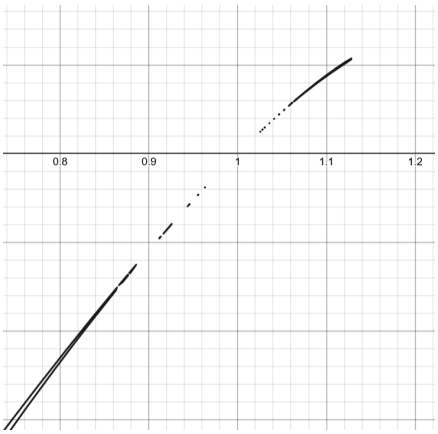

Figure 2: $C_{12}(\mathbb{R})$ around $(1,0)$

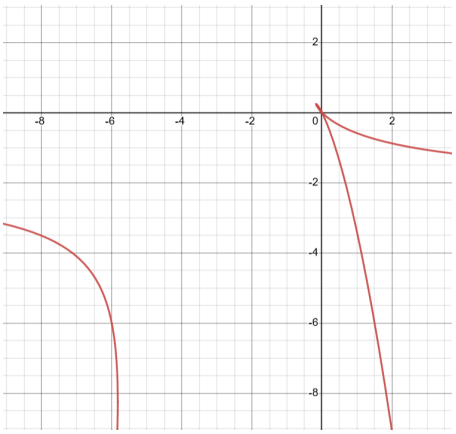

Figure 3: $C'_{12}(\mathbb{R})$ around $(0,0)$

Now consider

$$C_{12} : u^6 - 6u^5 - u^4v + u^2v^3 + 16u^4 - u^3v + 10u^2v^2 - 11uv^3 + 3v^4$$

$$-24u^3 + 9u^2v - 20uv^2 + 10v^3 + 21u^2 - 11uv + 10v^2 - 10u + 4v + 2 = 0.$$

Indeed, the point $(1,0)$ is a nodal singularity (see Figure 2; the plot is of poor quality, but one can check that both partial derivatives vanish at $(1,0)$). With the C_7-substitution $u = (d-1)c + 1$ and $v = (c+1)(d-1)c$, we find the birationally equivalent curve

$$C'_{12} : c^2d + 2c^2 + 3cd + d^2.$$

This equation is singular at $(0,0)$ (see Figure 3), but has degree 3 instead of 6, which is evidence that the C_7-substitution was a useful step. Resolving the singularity $(0,0)$ with $c = g/h$ and

$d = g$, we obtain the smooth curve

$$C''_{12} : h^2 + g + 3h + 2 = 0$$

of genus 0. We continue with the analysis of C_{12} in §2.2.2.

In the following sections, we only give the full substitutions that desingularise C_n immediately. The method is the same as above: use the C_7-substitution and keep blowing up singularities until one finds a non-singular equation.

2.2.1 Equation for $X_1(11)$

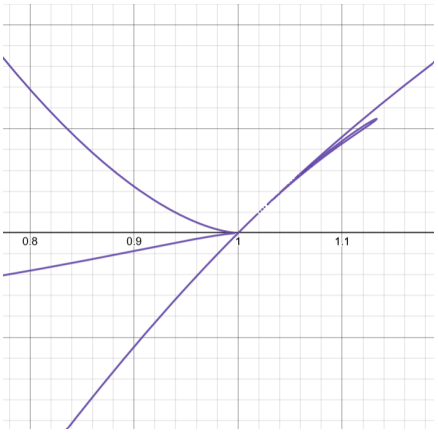

Figure 4: $C_{11}(\mathbb{R})$ around $(1, 0)$

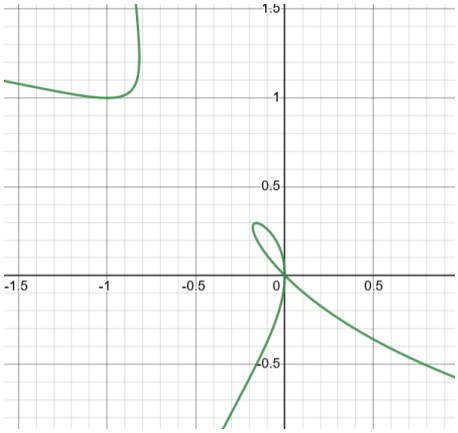

Figure 5: $C'_{11}(\mathbb{R})$ around $(0, 0)$

The curve C_{11} is defined as

$$C_{11} : u^7v - 10u^6v + 3u^5v^2 - u^6 + 45u^5v - 24u^4v^2 + 4u^3v^3 + 6u^5 - 110u^4v$$

$$+65u^3v^2 - 9u^2v^3 - 3uv^4 + v^5 - 15u^4 + 155u^3v - 81u^2v^2 + 6uv^3 + 3v^4 + 20u^3$$

$$-126u^2v + 48uv^2 - v^3 - 15u^2 + 55uv - 11v^2 + 6u - 10v - 1 = 0$$

The only singular point is $(1, 0)$ (see Figure 4). The C_7-substitution gives the birational equivalence with the curve

$$C'_{11} : cd^3 + d^3 + c^2 + cd$$

with a node at $(0, 0)$ (see Figure 5). The substitution $c \mapsto y^2/x^3$ and $d \mapsto y/x$ gives the birational equivalence with the curve

$$C''_{11} : y^2 + y = x^3 - x^2.$$

This is an elliptic curve with discriminant -11, and indeed the common model for $X_1(11)$ [LMF23, Elliptic Curve 11.a3]. We study $X_1(11)$ in Chapter 3. The full substitution is

$$\begin{aligned} u &= x^{-4} \cdot \left(x^4 + xy^2 + y^3\right) \\ v &= -x^{-7} \cdot (x+y) \cdot y^2 \cdot \left(-x^3 + y^2\right). \end{aligned}$$

In the variables x, y, the discriminant of $E_{u,v}$ equals

$$\Delta_{u(x,y),v(x,y)} = x^{-37} \cdot (x+y)^4 \cdot y^{11} \cdot (-x^3 + y^2)^3 \cdot F(x,y)$$

where $F(x,y)$ is an irreducible polynomial of degree 8.

2.2.2 Parametrisation of $X_1(12)$

We already found that the substitution

$$\begin{aligned} u &= h^{-1} \cdot (g^2 - g + h) \\ v &= h^{-2} \cdot g \cdot (g-1) \cdot (g+h) \end{aligned}$$

gives the non-singular curve

$$C''_{12} : h^2 + g + 3h + 2 = 0.$$

Since $g = -(h+1)(h+2)$ on C''_{12}, we can write

$$\begin{aligned} u(h) &= h^{-1} \cdot (h^4 + 6h^3 + 14h^2 + 16h + 6) \\ v(h) &= -h^{-2} \cdot (h+1) \cdot (h+2) \cdot (h^2 + 2h + 2) \cdot (h^2 + 3h + 3). \end{aligned}$$

In the variable h, the discriminant of $E_{u,v}$ equals

$$\Delta_{u(h),v(h)} = h^{-10} \cdot (h+2)^6 \cdot (h+1)^{12} \cdot (h^2 + 6h + 6) \cdot (h^2 + 2h + 2)^3 \cdot (h^2 + 3h + 3)^4.$$

We get an isomorphism of curves

$$\mathbb{P}^1 \to X_1(12) : (h:1) \longmapsto \left(E_{u(h),v(h)}, (0,0)\right)$$

which means that $X_1(12)$ is a curve of genus 0. The curve $E_{u(h),v(h)}$ is the universal elliptic curve with a point of order 12. The rational cusps of $X_1(12)$ are the images of points $(h:1)$ where the discriminant is zero or undefined: these are $(0:1), (-1:1), (-2:1), (1:0)$. In particular, the map

$$\begin{aligned} \mathbf{Q} \backslash \{0, -1, -2\} &\longrightarrow Y_1(12)(\mathbf{Q}) \\ h &\longmapsto \left(E_{u(h),v(h)}, (0,0)\right) \end{aligned}$$

is a bijection. This proves Theorem 2.1.

Similarly, one can find for all $4 \leq n \leq 10$ that $X_1(n)$ is a curve of genus 0 with a rational point. One can always make a parametrisation $\mathbb{P}^1 \to X_1(n)$ for those n, and this is done in for example [Wie23]. This proves that all the subgroups $\mathbf{Z}/n\mathbf{Z}$ for those n occur infinitely many times, as stated by Levi in [Lev08].

2.2.3 Equation for $X_1(13)$

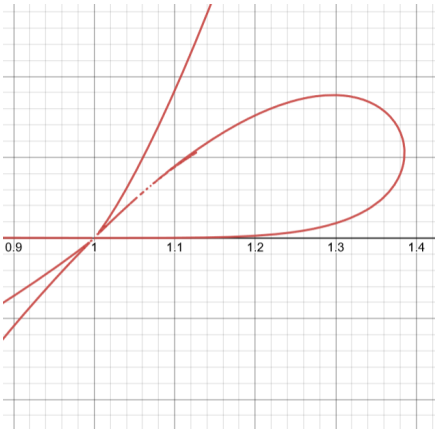

Figure 6: $C_{13}(\mathbb{R})$ around $(1,0)$

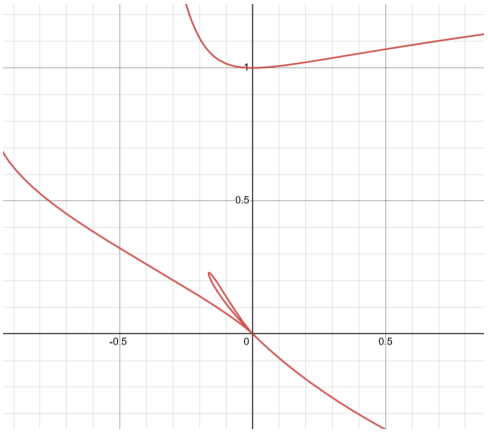

Figure 7: $C'_{13}(\mathbb{R})$ around $(0,0)$

The curve C_{13} is

$$-u^9v^2 - u^{10} + 15u^8v^2 - 5u^7v^3 + 10u^9 + 6u^8v - 105u^7v^2 + 59u^6v^3 - 9u^5v^4 - 45u^8 - 51u^7v$$
$$+412u^6v^2 - 270u^5v^3 + 60u^4v^4 - 4u^3v^5 + 120u^7 + 190u^6v - 987u^5v^2 + 655u^4v^3 - 170u^3v^4$$
$$+27u^2v^5 - 6uv^6 + v^7 - 210u^6 - 405u^5v + 1506u^4v^2 - 925u^3v^3 + 240u^2v^4 - 42uv^5 + 6v^6$$
$$+252u^5 + 540u^4v - 1475u^3v^2 + 765u^2v^3 - 165uv^4 + 19v^5 - 210u^4 - 461u^3v + 900u^2v^2$$
$$-344uv^3 + 44v^4 + 120u^3 + 246u^2v - 312uv^2 + 65v^3 - 45u^2 - 75uv + 47v^2 + 10u + 10v - 1 = 0.$$

The only singular point is $(1,0)$ (see Figure 6). The C_7-substitution gives the birational equivalence with the curve

$$C'_{13} : c^2d^4 + c^2d^3 + 2cd^4 + cd^3 + d^4 - c^3 - 3c^2d - 3cd^2 - d^3 = 0$$

with a singularity at $(0,0)$ (see Figure 7). Blowing up this singularity leaves a node at $(0,0)$, which can also be blown up to find the smooth curve

$$C''_{13} : e^3f - 2e^2f^2 + ef^3 - e^3 + ef^2 + e^2 - f = 0.$$

Rewriting this to the form $y^2 = f(x)$, we obtain

$$C_{13}''' : y^2 = x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1.$$

This is an equation of a hyperelliptic curve of genus 2, and will be our model for $X_1(13)$. It is studied in Chapter 4. The full substitution is

$$\begin{aligned} u &= 2^{-1} \cdot (x+1)^{-2} \cdot (-x^3 - x^2 + y + 1)^{-1} \\ &\quad \cdot \big(x^7 + 4x^6 + x^5 + 2x^4 y - 10x^4 + 4x^3 y - 12x^3 + 2x^2 y + xy^2 - 4x^2 + 4xy + 3x + 2y + 2\big) \\ v &= 2^{-1} \cdot (x+1)^{-1} \cdot x \cdot (-x^3 - x^2 + y + 1)^{-2} \cdot (x^3 + x^2 + y + 1) \\ &\quad \cdot (x^3 + x^2 - 2x + y - 1) \cdot (x^3 + 3x^2 + 2x + y + 1). \end{aligned}$$

In the variables x, y, the discriminant of $E_{u,v}$ equals

$$\Delta_{u(x,y),v(x,y)} = -2^{-7} \cdot (x+1)^{-11} \cdot x^5 \cdot F(x,y)$$

where $F(x,y)$ is a polynomial of degree 83 with irreducible factors of degree 3 and 11.

3 The elliptic curve $X_1(11)$

In this section, we prove the following theorem.

Theorem 3.1. *There are no elliptic curves over* $\mathbf{Q}$ *with a rational point of order 11.*

This is a special case of Mazur's theorem 1.2. The approach is the same as that of Mazur in [Maz77a] and [Maz77b] (in the latter he calls it an 'extremely intriguing technique'): we prove that all rational points on $X_1(11)$ are cusps. In §2.2.1, we showed that $X_1(11)$ is an elliptic curve with the equation

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

or in the form that we will use:

$$y^2 = x^3 - x^2 + \frac{1}{4}.$$

The standard method of descent by 2-isogeny, as described in for example [Sil09], requires the existence of a rational 2-torsion point. However, the curve $X_1(11)$ does not have a rational point of order 2. Therefore we need to extend the method to the case of irreducible 2-torsion. Developing irreducible 2-descent is done in §3.1. We apply this method to $X_1(11)$ in §3.2. Finally, we show that all the rational points of $X_1(11)$ are cusps in §3.3.

3.1 Irreducible 2-descent

We develop the method of irreducible 2-descent based on [Sil09, exercise 10.9]. This is not treated in the main texts of Silverman [Sil09] or Milne [Mil06]. A more computation-heavy version is described in the book [Cre97], but the author leaves part of the proof to a previous paper of his; his focus lies on implementability in computer algorithms. Also Cassels provides an irreducible 2-descent for $K = \mathbf{Q}$ in his book [Cas91]. We provide both an explicit proof of the method, and a cohomological interpretation in Remark 3.7 that is not present in any of the mentioned works.

Consider an elliptic curve $E : y^2 = f(x)$ over a number field K, such that $E(K)[2] = 0$. Fix a $T \in E(\bar{K})[2]$ and define $L = K(T) = K[X]/f(X)$. Let e_2 denote the Weil pairing on $E[2]$ ([Sil09, Section III.8]). For $P \in E(K)$, let $Q_P \in E(\bar{K})$ be a point such that $2Q_P = P$. We define the following maps:

$$\begin{aligned}
&\varphi_1 : E(K) \longrightarrow H^1(K, E[2]) : && P \longmapsto [\sigma \mapsto Q_P^\sigma - Q_P] \\
&\varphi_2 : H^1(K, E[2]) \longrightarrow H^1(L, E[2]) : && \xi \longmapsto \xi|_{G_L} \\
&\varphi_3 : H^1(L, E[2]) \longrightarrow H^1(L, \mu_2) : && \xi \longmapsto [\sigma \mapsto e_2(\xi(\sigma), T)] \\
&\varphi_4 : L^*/(L^*)^2 \xrightarrow{\sim} H^1(L, \mu_2) : && b \longmapsto [\sigma \mapsto \sqrt{b}^\sigma / \sqrt{b}]
\end{aligned}$$

Here φ_1 is the boundary map of the long exact sequence of cohomology corresponding to the multiplication-by-2 map on $E(K)$; the map φ_2 is the restriction map; the map φ_4 is the Kummer map.

Definition 3.1. The *descent map for E/K and T* is

$$\varphi_{E,T} = \varphi_4^{-1} \circ \varphi_3 \circ \varphi_2 \circ \varphi_1 : E(K) \to L^*/(L^*)^2.$$

It is easy to compute $\varphi_{E,T}(P)$ in terms of the coordinates of $P \in E(K)$.

Lemma 3.2. *Let $P \in E(K)$. Then we have $\varphi_{E,T}(P) \equiv x(P) - x(T) \mod (L^*)^2$.*

Proof. Let $f_T \in L(E)$ such that $\operatorname{div}(f_T) = 2(T) - 2(O)$ and $f_T \circ [2] = g_T^2$ for some $g_T \in L(E)^*$. It is proven on [Sil09, page 313] that $f_T(P) = x(P) - x(T) \in L^*/(L^*)^2$. It is clear that the composition $\varphi_3 \circ \varphi_2 \circ \varphi_1$ maps P to the cocycle class $[\sigma \mapsto e_2(Q_P^\sigma - Q_P, T)]$. It is left to show that this is equal to $\varphi_4(f_T(P))$.

With the definition of the Weil pairing and [Sil09, Proposition III.8.1(d)] we have that

$$e_2(Q_P^\sigma - Q_P, T) = g_T(Q_P^\sigma)/g_T(Q_P) = g_T(Q_P)^\sigma / g_T(Q_P).$$

Since $f_T(P) = g_T(Q_P)^2$, we have

$$\varphi_4(f_T(P)) = [\sigma \mapsto \sqrt{f_T(P)}^\sigma / \sqrt{f_T(P)}] = [\sigma \mapsto g_T(Q_P)^\sigma / g_T(Q_P)].$$

□

We now investigate the image of the descent map $\varphi_{E,T}$.

Definition 3.3. Let $K \subset L$ be a finite extension of number fields, and let $S \subset M_L$ be a finite subset of places containing at least the archimedean places. Define

$$L(K,S) \coloneqq \left\{ a \in L^*/(L^*)^2 : N_{L/K}(a) \in (K^*)^2, \forall v \in M_L \backslash S : \operatorname{ord}_v(a) \equiv 0 \mod 2 \right\}.$$

By Lemma A.14, we know that $L(K,S)$ is finite.

Lemma 3.4. *Let $S \subset M_L$ be the set of archimedean places, places dividing 2 and places where E has bad reduction. Then the image of $\varphi_{E,T}$ is contained in $L(K,S)$.*

Proof. First we show that for any $P \in E(K)$ and $v \in M_L \backslash S$ we have $\operatorname{ord}_v(\varphi_{E,T}(P)) \equiv 0 \mod 2$. Let $P \in E(K)$ and $v \in M_L \backslash S$, and Q satisfy $2Q = P$. We have that

$$\operatorname{ord}_v(\varphi_{E,T}(P)) \equiv \operatorname{ord}_v(f_T(P)) \equiv \operatorname{ord}_v(g_T(Q)^2) \mod 2.$$

Suppose that v is unramified in $L(g_T(Q))$. Then for all places v' of $L(g_T(Q))$ extending v, we have

$$\mathrm{ord}_v(g_T(Q)^2) = \mathrm{ord}_{v'}(g_T(Q)^2) = 2 \cdot \mathrm{ord}_{v'}(g_T(Q)) \equiv 0 \mod 2.$$

So it suffices to show that v is unramified in $L(g_T(Q))$, and we will do this by showing that v is unramified in the field $L(Q)$, which contains $L(g_T(Q))$.

Let $v' \in M_{L(Q)}$ extend $v \in M_L$, and let $l'_{v'}/l_v$ be the corresponding extension of residue fields. Let $I_{v'/v} \subset G_{\bar{L}/L}$ be the inertia group for v'/v. We will show that $Q^\sigma - Q = O$, which means that $I_{v'/v}$ acts trivially on Q, hence on $L(Q)$, so that $L(Q)$ is unramified at v.

E has good reduction at v by assumption, so it has good reduction at v'. Hence we have a reduction map $E(L(Q)) \to \tilde{E}(l'_{v'})$, and since $v \nmid 2$ we have an injection

$$g : E(L(Q))[2] \hookrightarrow \tilde{E}(l'_{v'}).$$

Let $\sigma \in I_{v'/v}$. Then $Q^\sigma - Q \in E(L(Q))[2]$. Also, σ acts trivially on $\tilde{E}(l'_{v'})$, so

$$\widetilde{Q^\sigma - Q} = \widetilde{Q^\sigma} - \tilde{Q} = \tilde{Q} - \tilde{Q} = \tilde{O}$$

hence $Q^\sigma - Q = O$.

Secondly, we show that for every $P \in E(K)$, we have

$$N_{L/K}(\varphi_{E,T}(P)) \in (K^*)^2.$$

Since $\varphi_{E,T}(P) = c^2 \cdot (x(P) - x(T))$ for some $c \in L^*$, it suffices to show that $N_{L/K}(x(P) - x(T)) \in (K^*)^2$. Let $A = \{\sigma : L \to \bar{K} \mid \forall x \in K : \sigma(x) = x\}$. Since E is in short Weierstrass form $y^2 = f(x)$, we have

$$N_{L/K}(x(P) - x(T)) = \prod_{\sigma \in A} \sigma(x(P) - x(T))$$

$$= \prod_{\sigma \in A} (x(P) - \sigma(x(T))) = f(x(P)) = y(P)^2 \in (K^*)^2.$$

□

Lastly, we show that the kernel of $\varphi_{E,T}$ is $2E(K)$, so that we get an injection $\psi_{E,T}$ from $E(K)/2E(K)$ into a finite group, which we will also refer to as a descent map. The following lemma is based on [Cas91, Lemma 15.2].

Lemma 3.5. *The kernel of $\varphi_{E,T}$ is equal to $2E(K)$.*

Proof. Let $P \in E(K)$ be such that $x(P) - x(T) \in (L^*)^2$. Write $x = x(P)$ and $\theta = x(T)$. We will show that $P \in 2E(K)$ by constructing a point $R \in E(K)$ such that $-2R = P$.

There are $p_0, p_1, p_2 \in K$ such that

$$x - \theta = (p_2\theta^2 + p_1\theta + p_0)^2 \in (L^*)^2$$

with $p_2 \neq 0$, or otherwise θ would satisfy a quadratic polynomial over K.

We can find four values $r_0, r_1, s_0, s_1 \in K$ not all zero such that

$$(s_1\theta + s_0)(p_2\theta^2 + p_1\theta + p_0) = r_1\theta + r_0$$

since the quadratic coefficient on the left-hand side is $s_0p_2 + s_1p_1$. Since $p_2 \neq 0$, we cannot have both $s_1 = 0$ and $s_0 \neq 0$. Neither $s_0 = s_1 = 0$ is possible, hence $s_1 \neq 0$, and multiplying all r_i and s_i with the same appropriate scalar, we can assume that $s_1 = -1$. We will now show that the point $R = (s_0, r_1s_0 + r_0)$ lies on $E(K)$ and satisfies $-2R = P$.

Squaring the previous equation gives

$$(s_0 - \theta)^2(x - \theta) - (r_1\theta + r_0)^2 = 0.$$

In this equation, we can substitute all θ with the variable X, modulo a K-scalar multiple of $f_\theta^K(X) = f(X)$. Hence there exists an $a \in K$ such that

$$(r_1X + r_0)^2 - (s_0 - X)^2(x - X) = a \cdot f(X).$$

Since the coefficient of X^3 on the left side is equal to 1, we have $a = 1$.

This means that the line $Y = r_1X + r_0$ intersects our elliptic curve $Y^2 = f(X)$ exactly in the points where $(s_0 - X)^2(x - X) = 0$, which is twice in the point $R \in E(K)$ and once in the point P. Hence $P = -2R \in 2E(K)$. □

We summarise the previous statements in the following theorem.

Theorem 3.6. *Let K be a number field and E/K be an elliptic curve with no 2-torsion over K. Let $T \in E(\bar{K})[2]\backslash\{O\}$, and $L = K(T)$. Then there is an injective homomorphism*

$$\psi_{E,T} : E(K)/2E(K) \hookrightarrow L(K, S)$$

given by

$$P \mapsto x(P) - x(T) \mod (L^*)^2.$$

Remark 3.7. For the reader who thinks that the maps φ_i and the composition $\varphi_{E,T}$ are somewhat ad hoc, we provide a more cohomological perspective that we did not find in other literature. Let P_1, P_2, P_3 be the nontrivial 2-torsion points of E, and let $T = P_1$ and $L = K(P_1) = K(T)$. We construct an exact sequence of G_K-modules

$$0 \to E[2] \to \mathrm{Ind}_L^K(\mu_2) \to \mu_2 \to 0$$

as follows. There is a group homomorphism

$$\psi : E[2] \to \mathbf{F}_2^3 : P \mapsto (e_2(P, P_i))_{i=1,2,3}.$$

By the properties of the Weil pairing, the image consists of the triples with product equal to 1, hence the map $\mathbf{F}_2^3 \to \mu_2 : (a_1, a_2, a_3) \mapsto a_1 \cdot a_2 \cdot a_3$ makes the above sequence of groups exact.

To make this a map of G_K-modules, we define the following permutation action on $\mathbf{F}_2^3$. Let $\sigma(i)$ be defined as $P_{\sigma(i)} = P_i^{\sigma^{-1}}$. Then

$$\sigma\left((a_i)_{i\in\{1,2,3\}}\right) = (a_{\sigma(i)})_{i\in\{1,2,3\}}.$$

We show that this makes $\mathbf{F}_2^3$ isomorphic to $\mathrm{Ind}_L^K(\mu_2)$ as G_K-modules. Recall that

$$\mathrm{Ind}_L^K(\mu_2) = \{f : G_K \to \mu_2 : \forall g \in G_K, h \in G_L, \text{ we have } f(gh) = hf(g)\}.$$

If we equip μ_2 with the trivial G_L-action, then we have $h(f(g)) = f(g)$ for all $g \in G_K, h \in G_L$. This means that all maps $f \in \mathrm{Ind}_L^K(\mu_2)$ are constant on the G_L-cosets of G_K. For $i \in \{1, 2, 3\}$, let $\sigma_i \in G_K$ be such that $\sigma_i(P_i) = P_1$. Then the following map is an isomorphism of G_K-modules:

$$\mathrm{Ind}_L^K(\mu_2) \to \mathbf{F}_2^3 : f \mapsto (f(\sigma_i))_{i\in\{1,2,3\}}.$$

This means that the sequence

$$0 \to E[2] \to \mathrm{Ind}_L^K(\mu_2) \to \mu_2 \to 0$$

is indeed a short exact sequence of G_K-modules. Hence it induces a long exact sequence. We can simplify that sequence with Shapiro's lemma [NSW08, Proposition 1.6.4], which implies that $H^i(K, \mathrm{Ind}_L^K(M)) = H^i(L, M)$ for all $i \geq 0$. Hence the long exact sequence is

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(K, E[2]) & \longrightarrow & H^0(L, \mu_2) & \longrightarrow & H^0(K, \mu_2) \\ & & & & & \swarrow & \\ & & H^1(K, E[2]) & \longrightarrow & H^1(L, \mu_2) & \longrightarrow & H^1(K, \mu_2). \end{array}$$

Applying Kummer theory, we know that in the commutative diagram

$$\begin{array}{ccccccc} E(K)/2E(K) & \hookrightarrow & H^1(K,E[2]) & \longrightarrow & H^1(L,\mu_2) & \longrightarrow & H^1(K,\mu_2) \\ & \searrow & & & \uparrow\wr & & \uparrow\wr \\ & & & & L^*/(L^*)^2 & \longrightarrow & K^*/(K^*)^2 \end{array}$$

the row is exact at $H^1(L,\mu_2)$. We observe that the dotted arrow is precisely the map $\psi_{E,T}$, and that the map $L^*/(L^*)^2 \to K^*/(K^*)^2$ is the norm map. This shows that the map

$$\psi_{E,T} : E(K)/2E(K) \to L^*/(L^*)^2 : P \mapsto x(P) - x(T)$$

is well-defined and injective and that it lands in the subgroup of elements with square norm in K. If we assume Lemma 3.4, then it proves Theorem 3.6 in a different way.

3.2 Rational points on $X_1(11)$

We are now ready to apply the 2-descent to the elliptic curve $E = X_1(11)$. In this section, we show that $E(\mathbf{Q})/2E(\mathbf{Q}) = 0$.

The Weierstrass equation that we use for $X_1(11)$ is

$$E : y^2 = x^3 - x^2 + \frac{1}{4}.$$

The polynomial on the right-hand side is irreducible over $\mathbf{Q}$, so $E(\mathbf{Q})[2] = \{O\}$. Let $T = (\beta, 0)$ be a nontrivial 2-torsion point. Let $f = x^3 - 2x^2 + 2 \in \mathbf{Q}[x]$, such that $f(2\beta) = 0$. Let $\alpha = 2\beta$, and $L = \mathbf{Q}(\alpha) = \mathbf{Q}(T)$. Writing a point $P \in E(\mathbf{Q})$ as $(x/t^2, y/t^3)$ with $x, y, t \in \mathbf{Z}$ and $\gcd(x,t) = \gcd(y,t) = 1$, the descent map as in Theorem 3.6 is

$$\psi_{E,T} : E(\mathbf{Q})/2E(\mathbf{Q}) \hookrightarrow L^*/(L^*)^2$$

$$(x/t^2, y/t^3) \longmapsto [x/t^2 - \beta] = [4x - 2t^2\alpha].$$

We now want to construct the set $S \subset M_L$ of archimedean places, places dividing 2 and places where E has bad reduction, and then determine the subgroup $L(\mathbf{Q}, S) \subset L^*/(L^*)^2$. We state some easily verifiable facts about the number field L in Table 1.

Let $\mathfrak{p}_2 = (\alpha)$, $\mathfrak{p}_{11} = (\alpha - 3)$ and $\mathfrak{q}_{11} = (\alpha^2 - 3)$, so that $(2) = \mathfrak{p}_2^3$ and $(11) = \mathfrak{p}_{11} \cdot \mathfrak{q}_{11}^2$ in $\mathcal{O}_L$. Then $S = \{\infty_r, \infty_c, \mathfrak{p}_2, \mathfrak{p}_{11}, \mathfrak{q}_{11}\}$. Since $\mathcal{O}_L$ is a unique factorisation domain, the generators of

$$\left\{a \in L^*/(L^*)^2 : \forall v \in M_L \backslash S : \mathrm{ord}_v(a) \equiv 0 \mod 2\right\} = L(L,S)$$

Generating polynomial	$x^3 - 2x^2 + 2$
Discriminant	-44
Signature	(1,1)
Unit group	$\langle -1, \alpha - 1 \rangle$
Class number	1
Factorisation of $2\mathcal{O}_L$	$(\alpha)^3$
Factorisation of $11\mathcal{O}_L$	$(\alpha - 3) \cdot (\alpha^2 - 3)^2$

Table 1: Properties of the number field $\mathbf{Q}[X]/(x^3 - 2x + 2)$

are the generators of the primes in S, so

$$L(L, S) = \langle -1, \alpha - 1, \alpha, \alpha - 3, \alpha^2 - 3 \rangle \subset L^*/(L^*)^2.$$

We are left with the question of which of the elements of this subgroup have norm in $(\mathbf{Q}^*)^2$. Hence we compute the norms of the generators in Table 2. It is clear from table 2 that the

Element	Norm
-1	-1
$\alpha - 1$	-1
α	-2
$\alpha - 3$	-11
$\alpha^2 - 3$	-11

Table 2: Norms of the generators of the ideals in S

elements with square norm are generated by $-1 \cdot (\alpha - 1)$ and $(\alpha - 3)(\alpha^2 - 3)$. So we have

$$L(\mathbf{Q}, S) = \langle 1 - \alpha, -\alpha^2 - 3\alpha + 7 \rangle.$$

Hence we have an injection

$$\varphi_{E,T} : E(\mathbf{Q})/2E(\mathbf{Q}) \hookrightarrow \langle 1 - \alpha, -\alpha^2 - 3\alpha + 7 \rangle \subset L^*/(L^*)^2 :$$

$$(x/t^2, y/t^3) \mapsto [4x - 2t^2\alpha].$$

Clearly the zero class in $E(\mathbf{Q})/2E(\mathbf{Q})$ contains O, which is mapped to $1 \in L^*/(L^*)^2$. We want to show that there are no other classes in the image by showing for every $x \in \mathbf{Q}$ that $4x - 2t^2\alpha \notin L(\mathbf{Q}, S) \backslash \{1\}$. This will be done by finding for all three $\delta \in L(\mathbf{Q}, S) \backslash \{1\}$ local obstructions to the equation

$$4x - 2t^2\alpha = \delta \cdot (X + Y\alpha + Z\alpha^2)^2.$$

We express the right-hand side of these equations as

$$Q_0^\delta(X,Y,Z) + Q_1^\delta(X,Y,Z)\cdot\alpha + Q_2^\delta(X,Y,Z)\cdot\alpha^2$$

which translates the equation to the system of equations

$$\begin{aligned} Q_0^\delta(X,Y,Z) &= 4x \\ Q_1^\delta(X,Y,Z) &= -2t^2 \\ Q_2^\delta(X,Y,Z) &= 0. \end{aligned}$$

Our method will be to find either a local obstruction to Q_2^δ or a point on Q_2^δ. In the latter case, we parametrise the curve Q_2^δ as $(f(X,Y,Z), g(X,Y,Z), h(X,Y,Z))$ and substitute it in Q_1^δ to find a local obstruction for that equation. This way, we do not have to deal with the variable x. We use Sage [The23] to determine the conics Q_i^δ, and to parametrise and substitute Q_2^δ.

We will repeatedly use the following fact.

Lemma 3.8. *Let K be a non-archimedean local field with discrete valuation ν. Let $a_1, ..., a_n \in K$. If there is a k such that for all j, we have $\nu(a_k) < \nu(a_j)$, then*

$$\nu\left(\sum_{i=1}^{n} a_i\right) = \min_{1\le i\le n} \nu(a_i) = \nu(a_k).$$

In this case, we call a_k *uniquely minimal for ν among $a_1, ..., a_n$.*

The following proposition proves that $E(\mathbf{Q})/2E(\mathbf{Q}) = 0$.

Proposition 3.9. *The image of*

$$\varphi_{E,T} : E(\mathbf{Q})/2E(\mathbf{Q}) \hookrightarrow \langle 1-\alpha, -\alpha^2 - 3\alpha + 7\rangle \subset L^*/(L^*)^2$$

is trivial. Therefore

$$E(\mathbf{Q})/2E(\mathbf{Q}) = 0.$$

Proof. We show that the three nontrivial elements of the codomain are not in the image.

Let us start with $\delta_1 = 1-\alpha$. We have

$$Q_2^{\delta_1}(X,Y,Z) = -2XY - Y^2 - 2XZ - 4YZ - 2Z^2$$

which has a global solution $(1,0,0)$. Parametrising and substituting this in $Q_1^{\delta_1}$, we get an equation that is isomorphic to

$$-2t^2 = -5w^4 - 12w^3 - 4w^2 + 8w + 4.$$

Clearly the 2-adic valuation $\mathrm{ord}_2(-2t^2)$ of the left-hand side is odd.
It is easily verified that, depending on $\mathrm{ord}_2(w)$, either $-5w^4$ or 4 is uniquely minimal for ord_2 among the terms of the right-hand side. Also $\mathrm{ord}_2(-5w^4), \mathrm{ord}_2(4) \in 2\mathbf{Z}$ so $\mathrm{ord}_2(-5w^4 - 12w^3 - 4w^2 + 8w + 4) \in 2\mathbf{Z}$, but $\mathrm{ord}_2(-2t^2) \notin 2\mathbf{Z}$.
We conclude that the equations

$$Q_1^{\delta_1}(X, Y, Z) = -2t^2$$
$$Q_2^{\delta_1}(X, Y, Z) = 0$$

do not have a mutual nontrivial rational solution $(X, Y, Z, t) \in \mathbf{Q}^4$, hence $1 - \alpha$ is not in the image of $\varphi_{E,T}$.

Let us continue with $\delta_2 = (1 - \alpha)(-\alpha^2 - 3\alpha + 7) = 4\alpha^2 - 10\alpha + 5$. We have

$$Q_2^{\delta_2}(X, Y, Z) = 4X^2 - 4XY + Y^2 + 2XZ - 12YZ - 8Z^2$$

which has a global solution $(1, 2, 0)$. Parametrising and substituting this in $Q_1^{\delta_2}$, we get the equation that is isomorphic to

$$11t^2 = g(w)$$

for $g(w) = w^4 - 2w^3 + 44w^2 - 160w + 108$. Then

$$g(w - 5) = w^4 - 22w^3 + 220w^2 - 1210w + 2783.$$

It is easily verified that, depending on $\mathrm{ord}_{11}(w)$, either w^4 or $2783 = 11^2 \cdot 23$ is uniquely minimal for ord_{11} among the terms of $g(w - 5)$. Also $\mathrm{ord}_{11}(w^4), \mathrm{ord}_{11}(2783) \in 2\mathbf{Z}$ so $\mathrm{ord}_{11}(g(w - 5)), \mathrm{ord}_{11}(g(w) \in 2\mathbf{Z}$ for any w, but $\mathrm{ord}_{11}(11t^2) \notin 2\mathbf{Z}$.
We conclude that the equations

$$Q_1^{\delta_2}(X, Y, Z) = -2t^2$$
$$Q_2^{\delta_2}(X, Y, Z) = 0$$

do not have a mutual nontrivial rational solution $(X, Y, Z, t) \in \mathbf{Q}^4$, hence $4\alpha^2 - 10\alpha + 5$ is not in the image of $\varphi_{E,T}$.

Let us finish with $\delta_3 = -\alpha^2 - 3\alpha + 7$. We find that $Q_2^{\delta_3}(X, Y, Z) = 0$ diagonalises to

$$-2w^2 + 44v^2 + 11z^2 = 0.$$

We will show that this conic has no nontrivial solutions in $\mathbf{Q}_{11}$.
Suppose that $w, v, z \in \mathbf{Q}_{11}^*$ are such that $-2w^2 + 44v^2 + 11z^2 = 0$. Then $\mathrm{ord}_{11}(44v^2 + 11z^2) = \mathrm{ord}_{11}(2w^2) \in 2\mathbf{Z}$. Hence $\mathrm{ord}_{11}(44v^2) = \mathrm{ord}_{11}(11z^2)$ and $\mathrm{ord}_{11}(v) = \mathrm{ord}_{11}(z)$. Without loss of

generality, we can assume that $\mathrm{ord}_{11}(v) = \mathrm{ord}_{11}(z) = 0$. Then there is a $k \in \mathbf{Z}$ such that we can assume that $\mathrm{ord}_{11}(w) = 0$ and

$$-2 \cdot 11^{2k-1} w^2 + 4v^2 + z^2 = 0.$$

Since $\mathrm{ord}_{11}(4v^2 + z^2) \geq 0$ and $\mathrm{ord}_{11}(4v^2 + z^2) \neq 0$, we know that $k > 0$. Hence we have that

$$-4v^2 \equiv z^2 \mod 11.$$

But -4 is not a square modulo 11, which gives a contradiction.

We conclude that the equation

$$Q_2^{\delta_3}(X, Y, Z) = 0$$

does not have a nontrivial rational solution $(X, Y, Z, t) \in \mathbf{Q}^4$, hence $\alpha^2 - 3\alpha - 7$ is not in the image of $\varphi_{E,T}$.

□

3.3 Elliptic curves with rational 11-torsion

We have shown that $E(\mathbf{Q})/2E(\mathbf{Q}) = 0$, but that only implies that the rank of E is zero and that there is no rational 2-torsion. To find other torsion points, we reduce E modulo 2, where E has good reduction, and use the fact that the non-2-primary part of $E(\mathbf{Q})_{tors}$ injects into $\tilde{E}(\mathbf{F}_2)$.

The discriminant of $E : y^2 + y = x^3 - x^2$ equals $\Delta(E) = -11$, so E has good reduction at 2. For all $\tilde{x}, \tilde{y} \in \mathbf{F}_2$, we have $\tilde{y}^2 + \tilde{y} = \tilde{x}^3 - \tilde{x}^2 = 0$. Hence all the 4 affine points in $\mathbb{P}^2(\mathbf{F}_2)$ lie on the curve $\tilde{E}(\mathbf{F}_2)$, in addition to the point at infinity. Note that the Hasse upper bound for the number of points of an elliptic curve over $\mathbf{F}_p$ is equal to $p + 1 + 2\sqrt{p}$ [Sil09, Theorem V.1.1]. For $p = 2$, the largest integer below $3 + 2\sqrt{2}$ is 5. So this elliptic curve contains the maximum number of points over $\mathbf{F}_2$, namely $|\tilde{E}(\mathbf{F}_2)| = 5$.

Now we know that $\#E(\mathbf{Q}) \mid 5$. Since $(0, 0) \in E(\mathbf{Q})$, we have that $\#E(\mathbf{Q}) = 5$. The points in $\tilde{E}(\mathbf{F}_2)$ have easy lifts to $E(\mathbf{Q})$, so we list all the points of $E(\mathbf{Q})$.

We return to the substitutions we made in §2.2.1 to find the curve E. Recall that the discriminant of $E_{u(x,y),v(x,y)}$ is

$$\Delta_{u(x,y),v(x,y)} = x^{-37} \cdot (x + y)^4 \cdot y^{11} \cdot (-x^3 + y^2)^3 \cdot F(x, y)$$

where $F(x, y)$ is an irreducible polynomial of degree 8. With this substitution, all points of $E(\mathbf{Q})$ give an undefined or zero discriminant. Hence all the points are cusps. We conclude that the 5 rational points on

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

Point	Order
$(0:1:0)$	1
$(0:0:1)$	5
$(0:-1:1)$	5
$(1:0:1)$	5
$(1:-1:1)$	5

Table 3: The points of $E(\mathbf{Q})$

do not correspond to a pair of an elliptic curve with a rational point of order 11, and that $Y_1(11)(\mathbf{Q}) = \emptyset$. This completes the proof of Theorem 3.1.

Theorem 3.1. *There are no elliptic curves over* $\mathbf{Q}$ *with a rational point of order 11.*

4 The curve $X_1(13)$ and the Jacobian

In section 2.2.3, we determined that $X_1(13)$ has genus 2. This means that neither the methods from $X_1(12)$ with genus 0 and $X_1(11)$ with genus 1 can directly be applied to $X_1(13)$ to find its rational points. Falting's theorem [Fal83] states that a curve of genus 2 or higher has finitely many rational points. However, the proof of the theorem is not constructive, and it does not help us find the rational points.

In 1973, Mazur and Tate [MT73] attacked this problem with the help of Ogg, by embedding $X_1(13)$ into its Jacobian $J_1(13)$. Ogg [Ogg73] had found a rational point of order 19 on $J_1(13)$, and Mazur and Tate conjectured that this made $J_1(13)$ 'not entitled to have any other points'. They proved themselves correct by using a 19-descent on the Jacobian to show that it has rank 0 over $\mathbf{Q}$, which was the key to proving the following theorem.

Theorem 4.1. *There are no elliptic curves over* $\mathbf{Q}$ *with a rational point of order* 13.

This section is intended to give an overview of some methods that can be used to prove this theorem. The main goal is to illustrate some of the ideas of the proof of Mazur and Tate. Going in-depth requires more machinery, for example in the $fppf$-cohomology, than we are willing to develop. The secondary goal is to discuss how one can prove the same statement using newer techniques, that were not available to Ogg, Mazur and Tate in the 70's.

In section 4.1, we discuss the set of cusps $X_1(n)$ as well as their rationality and show that $X_1(13)$ contains 6 rational cusps. Then we show that a slight improvement of the theorem of Chabauty-Coleman by Stoll [Sto06] shows that, conditional on the fact that $J_1(13)$ has rank 0, there are exactly 6 rational points on $X_1(13)$. In section 4.2, we give part of the argument of Mazur and Tate to show that the rank of $J_1(13)$ is 0. Then we show that a theorem of Kolyvagin-Logachev [KL90] and Kato [Kat04], which proves a special case of the conjecture of Birch and Swinnerton-Dyer, proves the same statement.

Throughout this chapter, we denote $X = X_1(13)$ and $J = J_1(13)$.

4.1 Rank-conditional proof

We prove the following proposition in two ways.

Proposition 4.2. *If the rank of* J *is* 0*, then there are no elliptic curves over* $\mathbf{Q}$ *with a rational point of order* 13.

First, we describe the classical modular construction of $X_1(n)$ in section 4.1.1. Then we illustrate how Ogg used this to find the rational point of order 19 on $J(\mathbf{Q})$ in section 4.1.2, and give the first proof of the proposition. Lastly, we show in section 4.1.3 that a theorem of Stoll gives an effective bound on $|X_1(n)|$ that also proves the proposition.

4.1.1 Cusps on $X_1(n)$

The following section is adapted from [Ogg73]. More extensive theory can be found in for example [Ste82]. Most of the statements below hold for any integer $n \geq 2$, but for us it is enough to assume that n is prime.

Let $\mathrm{PSL}(2, \mathbf{Z})$ be the full modular group, that is, the group of 2×2 integer-valued matrices with determinant 1 modulo the subgroup $\{\pm 1\}$. Define the following subgroups of $\mathrm{PSL}(2, \mathbf{Z})$:

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod n \right\}$$

and

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod n \right\}.$$

Then $\mathrm{PSL}(2, \mathbf{Z})$ and its subgroups act on the upper half plane of $\mathbb{C}$. Then $Y(n)$ and $Y_1(n)$ are the quotients of the upper half plane under the action of $\Gamma(n)$ and $\Gamma_1(n)$ respectively, and $X(n)$ and $X_1(n)$ are the compactifications. Then $Y_1(n)$ parametrises elliptic curves with a point of order n. The complement $X_1(n) \backslash Y_1(n)$ is exactly the set of cusps of $X_1(n)$.

The cusps of $X(n)$ are pairs $\pm(x, y)$ with $x, y \in \mathbf{Z}/n\mathbf{Z}$ coprime, and the cusps of $X_1(n)$ can be regarded as orbits under $G_1(n) = \Gamma_1(n)/\Gamma(n)$. We have

$$G_1(n) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbf{Z}/n\mathbf{Z} \right\}$$

so a cusp of $X_1(n)$ is an orbit $\pm(x + by, y)$.

This allows us to count the number of cusps of $X_1(n)$ for any n by counting the orbits, but it is simpler for n prime, which is the case for $n = 13$. Any nonzero $y \in \mathbf{Z}/n\mathbf{Z}$ is a unit, so $\pm(x, y), \pm(x', y)$ are in the same orbit for any $x, x' \in \mathbf{Z}/n\mathbf{Z}$ and $y \in (\mathbf{Z}/n\mathbf{Z})^*$. In particular, we can represent the orbits by $\pm(0, y)$. This gives $(n-1)/2$ orbits for $y \neq 0$. On the other hand, if $y = 0$, then clearly there are again $(n-1)/2$ orbits $\pm(x, 0)$.

As for rationality, all the cusps are defined over $\mathbf{Q}(\zeta_n)$. The Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q})$, which is naturally isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$, acts on the cusps of $X_1(n)$ by $\pm(x,y)^\sigma = \pm(\sigma x, y)$, i.e. multiplication on the first coordinate. Hence the $(n-1)/2$ cusps $\pm(0,y)$ are fixed by this action, which means that they are defined over $\mathbf{Q}$. The $(n-1)/2$ cusps $\pm(x,0)$ are conjugate under this action, and they are defined over $\mathbf{Q}(\zeta_n)^+$.

Remark 4.3. For $n = 11$, this result is in agreement with what we found in Chapter 3: the curve $X_1(11)$ contains 5 rational cusps. One can find the non-rational cusps that are predicted above by analysing the irreducible factor $F(x,y)$ of degree 8 of the discriminant $\Delta_{u,v}$ defined in section 2.2.1. The non-rational cusps of $X_1(11)$ are exactly the points on the curve that also lie on $F(x,y)$, and they can be found by computing the resultant of $F(x,y)$ and the defining equation of $X_1(11)$. The splitting field of the resultant is $\mathbf{Q}(\zeta_{11})^+$.

4.1.2 Classical approach

We state the two main results of Ogg [Ogg73]: that $J_{\mathrm{tors}}(\mathbf{Q}) \cong \mathbf{Z}/19\mathbf{Z}$ and that $X(\mathbf{Q}) \cap J_{\mathrm{tors}}(\mathbf{Q})$ only contains cusps.

We now know that for $n = 13$, the modular curve $X_1(13) = X$ contains 12 cusps in total, 6 of which are rational and 6 of which are defined over $\mathbf{Q}(\zeta_{13})^+$. Ogg then uses Eisenstein series to find linear relations on the images of the cusps in J, and deduces from them that the cusps generate a rational group of order 19 in J. He finds that the Jacobian contains 19 points over the fields $\mathbf{F}_2$ and $\mathbf{F}_3$ where it has good reduction, which proves the following lemma.

Lemma 4.4. *The torsion subgroup of $J(\mathbf{Q})$ is isomorphic to $\mathbf{Z}/19\mathbf{Z}$, and generated by the difference of any two rational cusps.*

The last part is the following lemma.

Lemma 4.5. *The intersection $X(\mathbf{Q}) \cap J_{\mathrm{tors}}(\mathbf{Q})$ only contains the 6 cusps.*

Proof. We know that all the cusps are contained in the intersection, which is true in general by the Manin-Drinfeld Theorem [Man72, Dri73] and in this case by Lemma 4.4. It is left to prove that there are no other points. To do this, we show that a non-cuspidal rational point of X maps to a non-torsion point in J.

Suppose that $x \in X(\mathbf{Q})$ is not a cusp. Then x corresponds to a pair (E,P) where E is an elliptic curve over $\mathbf{Q}$ and P a point of order 13. Then we know that E has bad reduction modulo 3, because otherwise there would be a point $\bar{P} \in \tilde{E}(\mathbf{F}_3)$ of order 13, which contradicts the Hasse-Weil bound.

Suppose that E has potential good reduction at 3. Recall that $E_0(\mathbf{Q}_3)$ is the set of points on $E(\mathbf{Q}_3)$ that reduce to non-singular points on $\mathbf{F}_3$. Then the quotient $E(\mathbf{Q}_3)/E_0(\mathbf{Q}_3)$ has order at most 4 [Sil09, Theorem VII.6.1], and cannot contain a point of order 13. Then $E(\mathbf{Q}_3)$ does not contain a point of order 13, which is a contradiction. Hence E has (potential) multiplicative reduction at 3.

Hence modulo 3, we have that $x \equiv y$ where y is a rational cusp. Without loss of generality, for example by applying a diamond operator that we can define in §4.2.1, we can assume that $y = \infty$. Since $x \equiv \infty \mod 3$, we have that $(x) - (\infty)$ is contained in the kernel of reduction mod 3. This is isomorphic to $\mathbf{Z}_3^2$ as formal groups, hence torsion-free. Hence the image of x in J has infinite order. □

This proves Proposition 4.2.

4.1.3 Modern approach

We use an improvement of the theorem of Chabauty-Coleman [Col85], namely a special case of Corollary 6.7 of [Sto06].

Lemma 4.6 ([Sto06], Corollary 6.7)**.** *Let C be a curve of genus g over $\mathbf{Q}$. Let p be prime of good reduction, and suppose that $r(J(C)) < g$ and $p > 2r(J(C)) + 2$. Then*

$$|C(\mathbf{Q})| \leq |C(\mathbf{F}_p)| + 2r(J(C)).$$

If we assume that $r(J) = 0$, then we have that $|X(\mathbf{Q})| \leq |X(\mathbf{F}_p)|$ for $p > 2$ of good reduction. For $p = 3$, we can iterate over $\mathbb{P}^2(\mathbf{F}_3)$ using the equation from section 2.2.3 to find that

$$X(\mathbf{F}_3) = \{(0,1), (0,-1), (1,1), (1,-1), (1:1:0), (1:-1:0)\}$$

which contains 6 points. Hence $|X(\mathbf{Q})| \leq 6$. We also find that all the points over $\mathbf{F}_3$ lift easily to points over $\mathbf{Q}$, so that

$$X(\mathbf{Q}) = \{(0,1), (0,-1), (1,1), (1,-1), (1:1:0), (1:-1:0)\}.$$

Hence $X(\mathbf{Q})$ contains 6 points, all of which are cusps. This proves Proposition 4.2.

4.2 Rank of the Jacobian

In this section we show that J has rank 0. For elliptic curves, the main way to show such statements is by 2-descent, as we did for $X_1(11)$. However, descent is in general a complex method

that is only well studied for curves of genus 1 and the prime 2. Some authors have developed or even used methods for higher descent on elliptic curves [Fis00, Sta05, Cre10, Gro19]. On the Jacobian of a hyperelliptic curve of genus 2, which is an abelian surface, descent is significantly harder than on elliptic curves.

Long before Magma or Sage came around, Ogg, Mazur and Tate had to avoid using equations for X and J or direct computations at all. However, the existence of a rational 19-torsion point on J prompted the idea of a 19-descent. The beauty of the argument of [MT73] is exactly in the absence of these computations. We show some of the ideas in section 4.2.1.

In section 4.2.2, we state a case of a theorem of Kolyvagin-Logachev and Kato, that proves the conjecture for modular abelian varieties over $\mathbf{Q}$ and rank 0. This gives another proof of the fact that $X(\mathbf{Q})$ is finite.

4.2.1 Introduction to 19-descent

The full 19-descent by Mazur and Tate is beyond the scope of this thesis. This section aims to introduce the ideas of the article. We study the 19-torsion subgroup of J, which is an important prerequisite for the 19-descent. This already shows some differences with the 2-descent we did in Chapter 3.

In order to apply a 19-descent, it is important to understand the 19-torsion $V = J[19]$. We describe V by describing the action of the twisted dihedral group Δ on the rational line in V.

The group $(\mathbf{Z}/13\mathbf{Z})^*$ acts on X by $m(E,P) = (E,mP)$. Since $(E,P) \cong (E,-P)$, this action is actually an action of $\Gamma := (\mathbf{Z}/13\mathbf{Z})^*/\{\pm 1\}$ and it is faithful. If $m \in \mathbf{Z}$ is coprime to 13, we write γ_m for the image of m in Γ. Note that γ_2 is a generator of Γ. These operators are called the *diamond operators*.
We extend the group Γ with a coset $\Gamma' = \{\tau_\zeta : \zeta \in \mu_{13}, \tau_\zeta = \tau_{\zeta^{-1}}\}$ with the relations

$$\begin{aligned} \tau_\zeta^2 &= 1 \\ \gamma_m \tau_\zeta &= \tau_{\zeta^m} \\ \tau_\zeta \gamma_m \tau_\zeta &= (\gamma_m)^{-1}. \end{aligned}$$

Now $\Delta = \Gamma \cup \Gamma'$ is a dihedral group of order 12 with a $G_{\mathbf{Q}}$-action, where elements of Γ' act on Γ as inversion. Mazur and Tate call this the twisted dihedral group. The elements of Γ' act on X as follows. If $\zeta \in \mu_{13}$ and $(E,P) \in X$, then there is a $Q \in E[13]$, unique up to multiples of

P, such that $e_{13}(P,Q) = \zeta$. Then $\tau_\zeta(E,P) = (E/\langle P\rangle, \bar{Q})$. Mazur and Tate leave the verification that this defines an action of Δ to the reader, so we verify it.

Lemma 4.7. *The above action is indeed a group action of Δ on X.*

Proof. It is clear that $1(E,P) = \gamma_1(E,P) = (E,P)$ and that

$$\gamma_l(\gamma_m(E,P)) = (E, lmP) = (\gamma_l\gamma_m)(E,P)$$

so that it defines a group action of Γ on X. Now we only need to check that the action satisfies the three relations on Δ from above.

We have

$$\tau_\zeta^2(E,P) = \tau_\zeta(E/\langle P\rangle, \bar{Q}) = (E/\langle P,Q\rangle, \bar{R})$$

where $R \in (E/\langle P\rangle)[13]$ is such that $e_{13}(\bar{Q},R) = \zeta$. Then the map

$$E \longrightarrow E/\langle P,Q\rangle$$

is the multiplication-by-13 map on E, because it has kernel $E[13] = \langle P,Q\rangle$. Since the Weil-pairing is isogeny-invariant, we have for a $\tilde{R}$ mapping to R under $E \to E/\langle P\rangle$ that $e_{13}(Q,\bar{R}) = e_{13}(\bar{Q},R) = \zeta = e_{13}(Q,P)^{-1}$. By the non-degeneracy of the Weil pairing, we have $\bar{R} = -P$.

Secondly, since $e_{13}(P,mQ) = e_{13}(P,Q)^m = \zeta^m$ we have that

$$(\gamma_m\tau_\zeta)(E,P) = \gamma_m(E/\langle P\rangle, \bar{Q}) = (E/\langle P\rangle, m\cdot\bar{Q}) = (E/\langle P\rangle, \overline{mQ}) = \tau_{\zeta^m}(E,P).$$

Thirdly, since $e_{13}(\bar{Q},R) = e_{13}(m\bar{Q}, m^{-1}R)$ and $(\gamma_m)^{-1} = \gamma_{m^{-1}}$ we have that

$$(\tau_\zeta\gamma_m\tau_\zeta)(E,P) = (\tau_\zeta\gamma_m)(E/\langle P\rangle,\bar{Q}) = \tau_\zeta(E/\langle P\rangle, m\bar{Q})$$

$$= (E/\langle P,Q\rangle, m^{-1}\bar{R}) \cong (E, m^{-1}P) = (\gamma_m)^{-1}(E,P).$$

□

The Jacobian J is simple over $\mathbf{Q}$, because if it was a product of two elliptic curves, then one of those would have a rational point of order 19 over $\mathbf{F}_2$, which is not possible due to the Hasse bound. The action of γ_2 on J has order 6, which means that its characteristic polynomial is a power of $\Phi_6(x) = x^2 - x + 1$. Hence the principal ideal domain $R = \mathbf{Z}[x]/\Phi_6 = \mathbf{Z}[\zeta_3]$ acts on J as endomorphisms over $\mathbf{Q}$. An important observation is that the rational prime 19 splits in R, i.e. we can write $19 = \pi\cdot\bar{\pi}$ where $\pi,\bar{\pi}$ are primes in R. This is the starting point for decomposing the vector space V.

Lemma 4.8. *Let $V_\pi = \ker(\pi \in \mathrm{End}(J))$ and $V_{\bar{\pi}} = \ker(\bar{\pi} \in \mathrm{End}(J))$. Then*

$$V = V_\pi \oplus V_{\bar{\pi}}.$$

Proof. Since $\pi, \bar{\pi}$ are coprime, there are $\alpha, \beta \in R$ such that $1 = \alpha\pi + \beta\bar{\pi}$ for $\alpha, \beta \in R$. Hence for $x \in V$ we have that $x = \alpha\pi x + \beta\bar{\pi}x$. Since $19x = 0$, we have that $\alpha\pi x \in V_{\bar{\pi}}$ and $\beta\bar{\pi}x \in V_{\pi}$, so that $V = V_{\pi} + V_{\bar{\pi}}$.
Now suppose that $x \in V_{\pi} \cap V_{\bar{\pi}}$. Then $x \in \ker(\gcd(\pi, \bar{\pi})) = \ker(1) = 0$. Hence $V_{\pi} \cap V_{\bar{\pi}} = 0$ and $V = V_{\pi} \oplus V_{\bar{\pi}}$.

□

The subspaces $V_{\pi}, V_{\bar{\pi}}$ are stable under $G_{\mathbf{Q}}$ and Γ, because γ_2 commutes with these groups. However, conjugation with any τ_{ζ} gives a non-trivial automorphism of R, hence permutes π and $\bar{\pi}$.

Let $V(1) \subset V$ be the 1-dimensional rational torsion subgroup. Since it is stable under γ_2, we can without loss of generality assume that $V(1) \subset V_{\bar{\pi}}$. Choose a surjective map $G_{\mathbf{Q}} \to \Gamma$, and write γ_{α} for the image of $\alpha \in G_{\mathbf{Q}}$. Let $V(\gamma) = \{v \in V : \forall \alpha \in G_{\mathbf{Q}}, v^{\alpha} = \gamma_{\alpha} v\}$. Then any τ_{ζ} permutes $V(1)$ and $V(\gamma)$, so the latter is a 1-dimensional subspace of V_{π}, and it is stable under the action of $G_{\mathbf{Q}}$ and Γ.

Let $V(\chi)$ be the Galois module μ_{19}. Now Mazur and Tate use Cartier duality of V_{π} and $V_{\bar{\pi}}$ to prove that the following sequence of $G_{\mathbf{Q}}$-modules is exact:

$$0 \longrightarrow V(\gamma) \longrightarrow V_{\pi} \longrightarrow V(\chi) \longrightarrow 0.$$

The crux is that $V_{\bar{\pi}}$ and V_{π} are self-orthogonal with respect to the Weil-pairing, because $e_{19}(\gamma_2 u, \gamma_2 v) = e_{19}(u, v)$, and $V_{\pi}, V_{\bar{\pi}}$ are eigen-spaces with eigenvalues the two primitive sixth roots of unity in $\mathbf{F}_{19}$, which do not have square equal to 1. Also, $V(\gamma)$ and $V(\chi)$ are not isomorphic because the $G_{\mathbf{Q}}$-action factors through $\mathbf{Q}(\zeta_{13})^{+}$ and $\mathbf{Q}(\zeta_{19})$ respectively.

This is a fairly precise description of the Galois module $V \subset J$, which makes the π-descent of Mazur and Tate possible. However, it would be too much to ask to need only Galois cohomology on J to get a good enough upper bound of the rank of J. In the case of a curve of genus 1 and prime 2, this can be solved by eliminating the elements of the Selmer group by using explicit equations for conics, as we did in §3.2. For the abelian surface J, this would be much harder. That is why Mazur and Tate use the finer $fppf$-cohomology to improve the upper bound on the rank, and they manage to show that it is in fact trivial.

4.2.2 Non-vanishing of L-function

When Mazur and Tate published their paper in 1973, the conjecture of Birch and Swinnerton-Dyer was completely open. It was already verified by Ogg [Ogg73] that the conjecture predicts

that the rank of J is 0. Since then, only special cases of the conjecture have been proven, mostly for varieties of small rank (0 or 1) or genus (elliptic curves). For our case, we use a result due to Kolyvagin-Logachev and Kato.

Theorem 4.9 (Kolyvagin-Logachev, Kato [KL90], [Kat04])**.** *Let A be a modular abelian surface over $\mathbf{Q}$. Let $L(A/\mathbf{Q}, s)$ be the L-series over A. If $L(A/\mathbf{Q}, s)$ does not vanish at $s = 1$, then $A(\mathbf{Q})$ is finite.*

From LMFDB [LMF24], we find that the special value $L(J, 1)$ is approximately 0.09, hence not equal to 0. It follows that $J_1(13)(\mathbf{Q})$ is finite. This proves Theorem 4.1.

A Weak Mordell-Weil Theorem

In this appendix, we prove that for any number field K and integer $n \geq 2$ the weak Mordell-Weil group $E(K)/nE(K)$ injects into the Selmer group $S^{(n)}(E/K)$, and that the latter is finite. This is done in many textbooks, such as [Sil09] and [Mil06], and for $K = \mathbf{Q}$ in [Cas91]. We follow a combination of the treatments of [Sil09] and [Mil06].

A.1 Galois cohomology

Let K be a number field, and $\bar{K}$ be an algebraic closure of K. Let $G_K = \mathrm{Gal}(\bar{K}/K)$. Then G_K is a profinite group, and we equip it with the induced profinite topology.

Definition A.1. A G_K-module is an abelian group M with the discrete topology, together with a continuous action of G_K on M. A G_K-module homomorphism is a group homomorphism of G_K-modules $\varphi : M \to N$ that commutes with the action of G_K.

We define the 0^{th} and 1^{st} cohomology groups of a G_K-module, because that is all the cohomology that we need for our purpose.

Definition A.2. Let K be a number field and M a G_K-module. The 0^{th} cohomology group of M is

$$H^0(G_K, M) \coloneqq M^{G_K}.$$

For the first cohomology group, we need to define cocycles and coboundaries.

Definition A.3. Let K be a number field and M a G_K-module. A continuous 1-cocycle from G_K to M is a continuous map $\xi : G_K \to M$ such that for all $\sigma, \tau \in G_K$ we have

$$\xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau).$$

We denote the Abelian group of continuous 1-cocycles from G_K to M by $Z^1_{cont}(G_K, M)$. From now on, we mean continuous 1-cocycle when we say cocyle.

Definition A.4. Let K be a number field and M a G_K-module. A 1-coboundary from G_K to M is a map $\xi : G_K \to M$ such that there is an $m \in M$ such that for all $\sigma \in G_K$ we have

$$\xi(\sigma) = m^\sigma - m.$$

We denote the Abelian group of coboundaries from G_K to M by $B^1(G_K, M)$. From now on, we mean 1-coboundary when we say coboundary. Since $m^{\sigma\tau} - m = (m^{\sigma\tau} - m^\sigma) + (m^\sigma - m) = (m^\sigma - m)^\tau + (m^\tau - m)$, all coboundaries are cocycles. Continuity follows from the fact that the map $\sigma \to m^\sigma$ is continuous: it is exactly the G_K-action on M.

Definition A.5. Let K be a number field and M a G_K-module. The first cohomology group of M is

$$H^1(G_K, M) \coloneqq Z^1_{cont}(G_K, M)/B^1(G_K, M).$$

Let

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

be an exact sequence of G_K-modules. Taking G_K-invariants is left exact but not right exact. That is, the sequence

$$0 \longrightarrow H^0(G_K, M) \longrightarrow H^0(G_K, N) \longrightarrow H^0(G_K, P)$$

is exact but the map on the right need not be surjective. The first cohomology groups measure the non-surjectivity of that map.

Lemma A.6. *Let*

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

be an exact sequence of G_K-modules. Then there is an exact sequence of cohomology groups

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(G_K, M) & \longrightarrow & H^0(G_K, N) & \longrightarrow & H^0(G_K, P) \\ & & & & & \overset{\delta}{\swarrow} & \\ & & H^1(G_K, M) & \longrightarrow & H^1(G_K, N) & \longrightarrow & H^1(G_K, P). \end{array}$$

Proof. The boundary map δ is defined as follows. Let $p \in H^0(G_K, P) \subset P$. Then there is an inverse image $n_p \in N$ of p. For any $\sigma \in G_K$, the value $n_p^\sigma - n_p$ maps to 0 in P, so it lies in the image of M. Hence the map $\xi : G_K \to M : \sigma \mapsto n_p^\sigma - n_p$ is well-defined. Then ξ is a 1-cocycle from G_K to M, and we define $\delta(p)$ to be the class of ξ.

Furthermore, we have $[\delta(p)] = [0]$ if and only if $\sigma : n_p^\sigma - n_p$ is a coboundary, if and only if $n_p \in H^0(G_K, N)$, so the diagram is exact at $H^0(G_K, P)$. Similarly, a cocycle class $[\xi]$ maps to zero in $H^1(G_K, N)$ if and only if $\xi : G_K \to N$ is a coboundary, if and only if there is a $n \in N$ such that $\xi(\sigma) = n^\sigma - n$ for all σ, if and only if $\xi = \delta(p)$ for a $p \in P$, which proves exactness at $H^1(G_K, M)$. □

Let L/K be a finite Galois extension. Since G_L is a finite index normal subgroup of G_K, a G_K-module M is naturally a G_L-module. This gives a *restriction map*

$$\mathrm{res} : H^1(G_K, M) \to H^1(G_L, M).$$

Since L/K is finite, the quotient group $G_{L/K} = G_K/G_L$ is finite. The submodule M^{G_L} is naturally a $G_{L/K}$-module, so any cocycle $\xi : G_{L/K} \to M^{G_L}$ extends to a cocycle $G_K \to M$ via

$$G_K \to G_{L/K} \to M^{G_L} \subset M$$

This is the *inflation map*

$$\inf : H^1(G_{L/K}, M^{G_L}) \to H^1(G_K, M)$$

Lemma A.7 (Inflation-restriction sequence)**.** *Let L/K be a finite Galois extension, and M be a G_K-module. Then the following sequence is exact.*

$$0 \to H^1(G_{L/K}, M) \xrightarrow{\inf} H^1(G_K, M) \xrightarrow{\text{res}} H^1(G_L, M)$$

From now, we will often write $H^i(K, M)$ for $H^i(G_K, M)$ to shorten notation.

A.2 Selmer group

The exact sequence of G_K-modules

$$0 \to E[n](\bar{K}) \to E(\bar{K}) \xrightarrow{n} E(\bar{K}) \to 0$$

induces by Lemma A.6 an exact cohomology sequence

$$0 \to E[n](K) \to E(K) \xrightarrow{n} E(K) \to H^1(K, E[n]) \to H^1(K, E) \xrightarrow{n} H^1(K, E)$$

which induces the exact Kummer sequence

$$0 \to E(K)/nE(K) \to H^1(K, E[n]) \to H^1(K, E)[n] \to 0.$$

We want to show that the group $E(K)/nE(K)$ is finite, so it would suffice if the group in the middle $H^1(K, E[n])$ is finite. Unfortunately, this need not be true. For example, if all the n-torsion is defined over K, then Kummer theory tells us that $H^1(K, E[2]) \cong H^1(K, \mu_2^2) \cong (K^*/(K^*)^2)^2$. What we want is an exact sequence as above, with $E(K)/nE(K)$ on the left, but a finite group in the middle. The Selmer group will be this group in the middle.

For any place $\nu \in M_K$, we can view E as elliptic curve over K_ν, which gives us the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K_\nu)/nE(K_\nu) & \longrightarrow & H^1(K_\nu, E[n]) & \longrightarrow & H^1(K_\nu, E)[n] & \longrightarrow & 0.
\end{array}$$

The map $H^1(K, E[n]) \to H^1(K_\nu, E[n])$ comes from the action of G_{K_ν} on $\bar{K}$, which defines a homomorphism $G_{K_\nu} \to G_K$. By composition, we can extend a cocycle $G_K \to E[n]$ to a cocyle $G_{K_\nu} \to G_K \to E[n]$.

Taking the product over all places of K gives

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & H^1(K, E[n]) & \longrightarrow & H^1(K, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{\nu \in M_K} E(K_\nu)/nE(K_\nu) & \longrightarrow & \prod_{\nu \in M_K} H^1(K_\nu, E[n]) & \longrightarrow & \prod_{\nu \in M_K} H^1(K_\nu, E)[n] & \longrightarrow & 0. \end{array}$$

This diagram induces the definitions of the Selmer group and Tate-Shafarevich group.

Definition A.8. Let E/K be an elliptic curve, and let $n \in \mathbf{N}_{\geq 2}$, and let $[n] : E \to E$ be the multiplication-by-n map on E. The Selmer group corresponding to $[n]$ is

$$S^{(n)}(E/K) = \ker \left(H^1(K, E[n]) \to \prod_{\nu \in M_K} H^1(K_\nu, E) \right).$$

In other words, the Selmer group is the subgroup of cocycle classes of $\gamma : G_K \to E[n]$ such that for all primes ν, the image $\gamma_\nu : G_{K_\nu} \to E[n]$ comes from a point in $E(K_\nu)/nE(K_\nu)$.

Definition A.9. Let E/K be an elliptic curve, and let $n \in \mathbf{N}_{\geq 2}$, and let $[n] : E \to E$ be the multiplication-by-n map on E. The Tate-Shafarevich group corresponding to $[n]$ is

$$Ш(E/K) = \ker \left(H^1(K, E) \to \prod_{\nu \in M_K} H^1(K_\nu, E) \right).$$

The Selmer and Tate-Shafarevich group fit in an exact sequence as desired.

Corollary A.10. *Let E/K be an elliptic curve, and let $n \in \mathbf{N}_{\geq 2}$, and let $[n] : E \to E$ be the multiplication-by-n map on E. There is an exact sequence of G_K-modules*

$$0 \to E(K)/nE(K) \to S^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

Proof. Apply the kernel-cokernel lemma to the sequence

$$H^1(K, E[n]) \to H^1(K, E)[n] \to \prod_{v \in M_K} H^1(K_v, E)[n].$$

□

We will prove the Selmer group to be finite, which implies the Weak Mordell-Weil Theorem. It is unknown whether the Tate-Shafarevich group is always finite. It is however known that the order of a finite Tate-Shafarevich group is always a square [Sil09, Theorem 4.14].

It is easiest to prove the finiteness of the Selmer group $S^{(n)}(E/K)$ when $\mu_n \subset K^*$ and $E(K)[n] = E(\bar{K})[n]$. Hence we will extend to a finite Galois extension L/K where this is satisfied. The following lemma proves that the finiteness of $S^{(n)}(E/L)$ implies the finiteness of $S^{(n)}(E/K)$.

Lemma A.11. *Let K be a number field, $L \supset K$ be a finite Galois extension, and E be an elliptic curve over K. If $S^{(n)}(E/L)$ is finite, then $S^{(n)}(E/K)$ is finite.*

Proof. We will show that $\ker\left(S^{(n)}(E/K) \to S^{(n)}(E/L)\right)$ is finite. The Selmer groups are subgroups of the respective first cohomology groups, so it suffices to show that the kernel of the map $H^1(K, E[n]) \to H^1(L, E[n])$ is finite. By Lemma A.7, the kernel is precisely equal to $H^1(\mathrm{Gal}(L/K), E[n](L))$. Since both $\mathrm{Gal}(L/K)$ and $E[n](L)$ are finite, the number of cocycles $\mathrm{Gal}(L/K) \to E[n](L)$ is finite, and it follows that $\ker(S^{(n)}(E/K) \to S^{(n)}(E/L))$ is finite. □

From now on, we may assume that our number field K contains μ_n, and that all n-torsion of E is defined over K.

We will use without proof the following lemma. The proof uses at the core that multiplication by n is an isomorphism on $E_1(K_\nu)$ for a local field K_ν.

Lemma A.12. *Let E be an elliptic curve over K with discriminant Δ, and let $S \subset M_K$ be the set of places dividing $2n\Delta$. For any $\gamma \in S^{(n)}(E/K)$ and any $\nu \notin S$, there exists a finite unramified extension L of K_ν such that γ maps to zero in $H^1(L, E[n])$.*

Proof. [Mil06, Lemma 3.6]. □

The proof of the finiteness of the Selmer group elegantly uses both finiteness results of algebraic number theory: the class group C of an algebraic number field K is finite, and the unit group U is finitely generated. In fact, we even use a stronger statement for S-unit groups.

Lemma A.13. *Let K be a number field and $S \subset M_K$ be finite. Let U_S and C_S be defined by the exactness of*

$$0 \to U_S \to K^* \to \bigoplus_{\nu \in M_K \setminus S} \mathbf{Z} \to C_S \to 0.$$

Then U_S is finitely generated and C_S is finite.

Proof. It follows from the kernel-cokernel sequence of $L^* \to \bigoplus_{\nu \in M_K} \mathbf{Z} \to \bigoplus_{\nu \in M_K \setminus S} \mathbf{Z}$. □

The next lemma is an important step towards proving the finiteness of the Selmer group.

Lemma A.14. *Let K be a number field, and S be a finite subset of M_K. Let*

$$N = \{a \in K^*/(K^*)^n : \forall v \in M_K \backslash S : \mathrm{ord}_p(a) \equiv 0 \mod n\}.$$

Then N is finite.

Proof. The set N is precisely the kernel of the map

$$K^*/(K^*)^n \to \bigoplus_{v \in M_K \backslash S} \mathbf{Z}/n\mathbf{Z} : a \mapsto (\mathrm{ord}_v(a))_{v \in M_K \backslash S}.$$

Consider the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^* & \xrightarrow{n} & K^* & \longrightarrow & K^*/(K^*)^n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_{v \in M_K \backslash S} \mathbf{Z} & \xrightarrow{n} & \bigoplus_{v \in M_K \backslash S} \mathbf{Z} & \longrightarrow & \bigoplus_{v \in M_K \backslash S} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & 0. \end{array}$$

The vertical maps map a to the order of a at the given places. Adding the kernels and cokernels of these maps, we get the following diagram.

$$\begin{array}{ccccccccc} & & U_S & & U_S & & N & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K^* & \xrightarrow{n} & K^* & \longrightarrow & K^*/(K^*)^n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_{v \in M_K \backslash S} \mathbf{Z} & \xrightarrow{n} & \bigoplus_{v \in M_K \backslash S} \mathbf{Z} & \longrightarrow & \bigoplus_{v \in M_K \backslash S} \mathbf{Z}/n\mathbf{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & C_S & & C_S & & & & \end{array}$$

Applying the Snake Lemma, one gets an exact sequence

$$0 \longrightarrow U_S \xrightarrow{n} U_S \longrightarrow N \longrightarrow C_S \xrightarrow{n} C_S$$

hence

$$0 \longrightarrow U_S/(U_S)^n \longrightarrow N \longrightarrow (C_S)[n].$$

Since U_S is finitely generated and C_S is finite, all groups in this sequence are finite. □

We are now ready to prove the main goal of this section.

Theorem A.15. *Let K be a number field, and E an elliptic curve over K, and $n \geq 2$ an integer. Then the Selmer group $S^{(n)}(E/K)$ is finite, and hence $E(K)/nE(K)$ is finite.*

Proof. By Lemma A.11, we can assume that all n-torsion is defined over K. Let $S \subset M_K$ be the set of archimedean places, places dividing n, and primes where E has bad reduction.
Let $\gamma_0 \in S^{(n)}(E/K)$. For each prime $\nu \in M_K \backslash S$, there exists by Lemma A.12 a finite unramified extension $K_\nu(\alpha_\nu)$ of K_ν such that the image of γ_0 under the map $H^1(K, E[n]) \to H^1(K_\nu(\alpha_\nu), E[n])$, which can be written as

$$l : (K^*/(K^*)^n)^2 \to (K_\nu(\alpha_\nu)^*/(K_\nu(\alpha_\nu)^*)^n)^2$$

is zero. Consider the map

$$(K_\nu(\alpha_\nu)^*/(K_\nu(\alpha_\nu)*)^n)^2 \to (\mathbf{Z}/n\mathbf{Z} : (b_1, b_2) \mapsto (\mathrm{ord}_\nu(b_1), \mathrm{ord}_\nu(b_2)).$$

Since $K_\nu \subset K_\nu(\alpha_\nu)$ is unramified, we have for the natural inclusion $i : K \hookrightarrow K_\nu(\alpha_\nu)$ and $a \in K^*$ that $\mathrm{ord}_\nu(a) = \mathrm{ord}_\nu(i(a))$. Since $\nu \nmid n$, this means that for $b \in K^*/(K^*)^n$ that $\mathrm{ord}_\nu(b) \equiv \mathrm{ord}_\nu(l(b)) \mod n$. Hence the composition $(K^*/(K^*)^n)^2 \to (K(\alpha_\nu)^*/(K(\alpha_\nu)^*)^n)^2 \to (\mathbf{Z}/n\mathbf{Z})^2$ is the natural map $(\mathrm{ord}_\nu, \mathrm{ord}_\nu) : (K^*/(K^*)^n)^2 \to (\mathbf{Z}/n\mathbf{Z})^2$. However, we do know now that γ_0 is in the kernel of this map. We also know that this composition does not depend on the choice of γ_0, so in fact, all elements of the Selmer group are in the kernel.

Therefore we get a map

$$(K^*/(K^*)^n)^2 \to \prod_{\nu \in M_K \backslash S} (K_\nu(\alpha_\nu)^*/(K_\nu(\alpha_\nu)^*)^n)^2 \to \prod_{\nu \in M_K \backslash S} (\mathbf{Z}/n\mathbf{Z})^2 .$$

By Lemma A.14, the kernel of this map is finite. But we also know that $S^{(n)}(E/K)$ is contained in the kernel. Hence $S^{(n)}(E/K)$ is finite. □

References

[Cas91] Ian Cassels. *LMSST: 24 Lectures on Elliptic Curves.* London Mathematical Society Student Texts. Cambridge University Press, 1991.

[Col85] Robert Coleman. Effective Chabauty. *Duke Math. J.*, 52:765–770, 1985.

[Cre97] John Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1997.

[Cre10] Brendan Creutz. *Explicit Second p-descent on Elliptic Curves.* PhD thesis, International University Bremen, 2010.

[Dri73] Vladimir Drinfeld. Two theorems on modular curves. *Akademija Nauk SSSR. Funkcionalnyi Analiz i ego Priloženija*, 7(2):83–84, 1973.

[Eng99] Andreas Enge. *Elliptic curves and their applications to cryptography — an introduction.* Kluwer, 1999.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones Mathematicae*, 73(3):349–366, 1983.

[Fis00] Tom Fisher. *On 5 and 7 descents for elliptic curves.* PhD thesis, University of Cambridge, 2000.

[Gro19] Steven Groen. Descent by 3-isogeny on elliptic curves. Master's thesis, University of Groningen, 2019.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[KL90] Victor Kolyvagin and Dmitry Logachev. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Leningrad Math. J.*, 1(5):1229–1253, 1990.

[Lev08] Beppo Levi. Saggio per una teoria aritmetica delle forme cubiche ternarie. *Atti della Reale Acc. Sci. di Torino*, 1906-1908.

[LMF23] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2023. [Online; accessed 30 November 2023].

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database, home page of the L-function $L(A, s)$ for genus 2 curve 169.a.169.1.

https://www.lmfdb.org/L/4/13e2/1.1/c1e2/0/0, 2024. [Online; accessed 5 January 2024].

[Man72] Yuri Manin. Parabolic points and zeta functions of modular curves. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 36(1):19–66, 1972.

[Maz77a] Barry Mazur. Modular curves and the Eisenstein ideal. *Publications mathématiques de l'I.H.É.S.*, 47:33–186, 1977.

[Maz77b] Barry Mazur. Rational points on modular curves. *Modular Functions of one Variable V. Lecture Notes in Mathematics*, 601:107–148, 1977.

[Mil06] James Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[Mor22] Louis Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21:179–192, 1922.

[MT73] Barry Mazur and John Tate. Points of order 13 on elliptic curves. *Inventiones mathematicae*, 22:41–50, 1973.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. Springer, 2008.

[Ogg73] Andrew Ogg. Rational points on certain elliptic modular curves. *Proc. Symp. Pure Math*, 24:221–231, 1973.

[Sil09] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[Sta05] Sebastian Stamminger. *Explicit 8-descent on elliptic curves*. PhD thesis, International University Bremen, 2005.

[Ste82] Glenn Stevens. *Arithmetic on Modular Curves*, volume 20 of *Progress in Mathematics*. Birkhäuser, 1982.

[Sto06] Michael Stoll. Independence of rational points on twists of a given curve. *Compos. Math.*, 142:1201–1214, 2006.

[The23] The Sage Developers. *SageMath, the Sage Mathematics Software System*, 2023. https://www.sagemath.org.

[Wei28] André Weil. *L'arithmetique sur les coubres algebriques*. PhD thesis, University of Uppsala, 1928.

[Wie23] Laurens Wiersema. Elliptic curves with q-rational points of order n. Bachelor thesis, University of Groningen, 2023.