Heegner Point Constructions for Modular Elliptic Curves

Erik Holum
New College
University of Oxford

A thesis submitted for the degree of
MSc in Mathematics and
Foundations of Computer Science

2011

Acknowledgements

I would first like to thank my dissertation supervisor, Dr. Alan Lauder, for his tremendous support and generous giving of time. I would also like to acknowledge my advisors in the mathematical institute, Professor Michael Collins and Professor Roger Heath-Brown for their constant guidance throughout my time at Oxford. I am extremely grateful to my parents, without whom I would not have had the chance to write this paper nor study in England, and who patiently edited many drafts despite their limited mathematical knowledge. I would like to thank my friends who have supported and entertained me while I wrestled with this challenging project. Finally, I honor the University of Oxford for providing me with the extraordinary opportunity to read for this degree.

Abstract

Let $E/\mathbb{Q}$ be an elliptic curve in minimal Weierstrass form

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

Finding rational points on $E(\mathbb{Q})$ has been a long standing problem, and currently there are several methods. The brute force method of looping over the value a/d^2 for $d = 1, 2, 3, ...$ and $a = \pm 1, \pm 2, \pm 3, ...$ is disappointingly slow, and other algorithms have been developed to speed up the process. In this paper, we examine one such algorithm which uses the modular parameterization of $E/\mathbb{Q}$ and so called Heegner points to construct a rational point on a curve of analytic (and hence algebraic) rank 1.

The aim of this paper is precisely to describe each step in the process as well as enough of the under-lying mathematics for someone with limited experience working with modular curves to be able to understand the majority of the computation. We first present background on elliptic functions, complex lattices, and isomorphism classes of elliptic curves, then continue with a brief overview of modular forms and the modularity theorem for elliptic curves, and then define Heegner points in both an abstract and concrete manner. We then discuss the process of constructing a rational point on $E/\mathbb{Q}$, as well as provide several examples ranging in height complexity from less than 1 to over 1000.

Contents

Chapter 1

Introduction

Elliptic curves today are one of the most prominently studied objects in mathematics. Yet despite the efforts of a great deal tremendous research, for the most part they remain shrouded in mystery. The Mordell-Weil theorem, proved in 1922, combined with the work of Mazur, exactly describes the structure of points on an elliptic curve E defined over the rationals as

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r,$$

where T is the torsion subgroup of E and r is called the rank of the elliptic curve. Despite the simple group structure and the decades of research, very little is currently known about the rank of elliptic curves. It is conjectured that there exist curves of arbitrarily high rank, but to this day the largest rank computed is merely 18. The Birch−Swinnerton-Dyer conjecture concerning the L-series and the rank of elliptic curves was deemed important and difficult enough to merit a $1,000,000 prize offered by the Clay Maths Institute for the first correct proof.

Currently, very special cases of the BSD conjecture have been proven. One recent step showed the conjecture to be true for curves of analytic rank 1. Recall the analytic rank is defined to be the order of vanishing of $L(E, s)$ at $s = 1$. The proof (by Kolyvagin, building on work by Gross and Zagier) involved a method of constructing rational points using the recently proved modularity theorem and so called Heegner points on the modular curve $X_0(N)$.

In this paper, we will focus on this method of construction, paying particular attention to the computational aspects of Heegner points and modular curves. Our goal is to give sufficient mathematical background to be able precisely to describe an algorithm to find a non-torsion rational point on an elliptic curve of analytic rank 1. The first three chapters discuss the relevant mathematical structures and ideas used

in the algorithm. The final chapter discusses practical issues in the computation, then presents several examples.

We implement the algorithm using SAGE, with extremely limited usage of built in classes so as to optimize the code for our purposes. Specifically, all aspects of the algorithm were implemented by the author excluding methods for continued fractions, the Weierstrass-$\wp$-function, and some basic operations on elliptic curves (we use the SAGE Cremona database to find the curves used in our examples).

Chapter 2

Complex Elliptic Curves

In this section we discuss the relationship between classes of elliptic curves and lattices, $\Lambda \subset \mathbb{C}$. Specifically, we show that every elliptic curve is analytically isomorphic to a torus $\mathbb{C}/\Lambda$ for some lattice Λ.

2.1 Elliptic Functions

Fix $w_1, w_2 \in \mathbb{C}$ such that w_1, w_2 are linearly independent over $\mathbb{R}$. Let Λ be the lattice generated by w_1 and w_2, so

$$\Lambda = \{mw_1 + nw_2 : m, n \in \mathbb{Z}\}.$$

Definition 2.1.1. *Given $w_1, w_2 \in \mathbb{C}$ as above, an elliptic function $f : \mathbb{C}/\Lambda$ is a meromorphic function such that for all $z \in \mathbb{C}$, we have*

$$f(w_1 + z) = f(z) = f(w_2 + z).$$

Here, w_1 and w_2 are called the periods of f.

The lattice Λ is called the *period lattice* attached to f. It is clear that every element in $\mathbb{C}$ is equivalent modulo $\mathbb{Z}w_1 + \mathbb{Z}w_2$ to some point in the parallelogram

$$\Pi = \{xw_1 + zw_2 : 0 \leq x, z < 1\}.$$

Such a set Π is called the *fundamental domain* for $\mathbb{C}/\Lambda$.

Definition 2.1.2. *The order of an elliptic function f is defined to be the number of poles in the fundamental parallelogram. Or, equivalently, the number of zeros of f.*

It is not clear from the definition that there exist any nonconstant elliptic functions. Additionally, it is not hard to show that any holomorphic elliptic function is constant and any elliptic function with no zeroes is constant [17, Page 161]. The following lemma will be important in the construction of a nonconstant elliptic function.

Lemma 2.1.3. *Let $s \in \mathbb{R}$ with $s > 2$. Then the sum*

$$\sum_{w \in \Lambda - \{0\}} \frac{1}{|w|^s}$$

converges.

Proof. See [10, Page 154]. □

2.2 The Weierstrass $\wp$-Function

For our purposes the most important non-constant elliptic function is the Weierstrass $\wp$-function.

Definition 2.2.1. *Let $\Lambda \subset \mathbb{C}$ be a lattice with generators w_1, w_2. Then the Weierstrass $\wp$-function relative Λ is given by*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w \in \Lambda - \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Let $k \geq 1$ be an integer. Then we also define the Eisenstein series of weight $2k$ relative Λ by

$$G_{2k}(\Lambda) = \sum_{w \in \Lambda - \{0\}} \frac{1}{w^{2k}}.$$

It follows from Lemma 2.1.3 that $\wp$ is convergent for all $z \in \mathbb{C}$ and that G_{2k} is convergent for all Λ. We will drop the Λ when the relative lattice is clear from the context.

Proposition 2.2.2. *The function, $\wp(z)$ is an even elliptic function with periods w_1, w_2 and poles at the points of Λ, the order of $\wp(z)$ is 2, and $\wp'(z)$ can be computed term by term.*

Proof. See [10, Section VI.3] for the full proof. As computing this function will be relevant to the construction of Heegner points, we make some brief remarks on the

term-by-term computation. Specifically, direct computation gives the derivative of $\wp$ as

$$\begin{aligned}\wp'(z) &= \frac{d}{dz}\wp(z) \\ &= -2\sum_{w\in\Lambda-\{0\}}\frac{1}{(z-w)^3}.\end{aligned}$$

It is a fact that $\wp'$ is again an elliptic function with poles of order 3 at $z=0$. Thus, mapping a point from $\mathbb{C}/\Lambda$ to $\mathbb{C}$ using $\wp'$ can be done to a certain precision by computing a finite number of terms of the above sum. □

Using the Weierstrass function, we can construct a map from the quotient space $\mathbb{C}/\Lambda$ onto an elliptic curve, $E(\mathbb{C})$. Define the constants g_2, g_3 by

$$g_2 = 60G_4,$$

$$g_3 = 140G_6.$$

Again, since $G_m(\Lambda)$ is convergent, we have $g_2, g_3 \in \mathbb{C}$.

Proposition 2.2.3. *For any $\Lambda \subset \mathbb{C}$ and any $z \in \mathbb{C}/\Lambda$, the Weierstrass $\wp$-function satisfies the differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 + g_2\wp(z) + g_3.$$

Proof. See [23, Page 436]. □

Assuming w_2/w_1 is in the upper half plane (if not, we can swap w_1 and w_2), then specific formulae for g_2 and g_3 are given in [6, Proposition 7.4.1] as

$$g_2 = \frac{4}{3}\left(\frac{\pi}{w_2}\right)^4\left(1+240\sum_{n\geq 1}\frac{n^3}{e^{2\pi i n w_1/w_2}-1}\right) \tag{2.2.1a}$$

$$g_3 = \frac{8}{27}\left(\frac{\pi}{w_2}\right)^6\left(1-504\sum_{n\geq 1}\frac{n^5}{e^{2\pi i n w_1/w_2}-1}\right). \tag{2.2.1b}$$

Proposition 2.2.4. *Fix a lattice $\Lambda \subset \mathbb{C}$. Let $E(\mathbb{C})$ be the complex cubic curve given in affine form by*

$$y^2 = 4x^3 + g_2x + g_3.$$

Then $E(\mathbb{C})$ is an elliptic curve. Moreover, the map $\Phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ defined by

$$\Phi(z) = \begin{cases} (\wp(z), \wp'(z), 1) & \text{if } z \notin \Lambda \\ (0,1,0) & \text{if } z \in \Lambda. \end{cases} \tag{2.2.2}$$

is an isomorphism.

Proof. See [17, Page 170]. □

Proposition 2.2.4 shows that tori, $\mathbb{C}/\Lambda$, in the complex plane can be considered as elliptic curves, $E(\mathbb{C})$, related by the mapping Φ.

2.3 Inverting the Map Φ

We now turn our attention to the converse problem. Given any elliptic curve, $E(\mathbb{C})$, we are able to find a lattice, Λ, such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. We have the following theorem from uniformization theory.

Theorem 2.3.1 (Uniformization Theorem)**.** *Let $A, B \in \mathbb{C}$ such that $4A^2 - 27B^2 \neq 0$. Then there exists a lattice $\Lambda \subset \mathbb{C}$ such that $60G_4(\Lambda) = A$ and $140G_6(\Lambda) = B$.*

Proof. See [12, Section 4.2] or [11, Proposisiont VII.5] for example. □

From here, we can show that for any elliptic curve E there exists a lattice Λ with $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. Ideally, however, we would like to be able to be given an elliptic curve in general Weierstrass form, and be able to derive explicit formulae for computing w_1, w_2, and Φ^{-1}, as computationally it will provide us with more information. We first recall the definition of the arithmetic-geometric mean (AGM) of two numbers.

Definition 2.3.2. *Let x, y be positive real numbers. Then the arithmetic-geometric mean of a and b, denoted $M(a, b)$, is defined as the common limit of the two sequences (x_n) and (y_n). Where $x_1 = \frac{1}{2}(a + b)$, $y_1 = \sqrt{ab}$, and*

$$x_{n+1} = \frac{1}{2}(x_n + y_n),$$
$$y_{n+1} = \sqrt{x_n y_n}.$$

The AGM also exists when we fix a and b as arbitrary complex numbers. In order for this to make sense, we must make the geometric mean of two numbers unambiguous by choosing which square roots to use in the definition of (y_n). In this way, $M(a, b)$ can take on an infinite number of possibilities depending on the choices of square roots. Moreover, the infinite set

$$L = \{z \in \mathbb{C} \text{ such that } z = \frac{\pi}{M(a,b)}, \text{ for some choice of square roots}\} \cup \{0\} \quad (2.3.1)$$

forms a lattice in $\mathbb{C}$. The link between the AGM and elliptic curves is given in the following proposition.

Theorem 2.3.3. *Let $E(\mathbb{C})$ be an elliptic curve given in affine form by*

$$y^2 = 4x^3 + g_2x + g_3, \tag{2.3.2}$$

and let e_1, e_2, e_3 be the three complex roots of E. Then the set of all possible determinations of

$$\frac{\pi}{M(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})}$$

together with 0 forms a lattice L such that $E(\mathbb{C}) \cong \mathbb{C}/L$.

Proof. See [10, Section VI.9]. □

As any elliptic curve can be written via a change of variables in the form of (2.3.2), it follows that every elliptic curve is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ. Additionally, if ω_1, ω_2 is a basis for a lattice Λ, then Λ is homothetic to the lattice generated by $\{1, \tau\}$, where $\tau = \omega_2/\omega_1$. We can thus write any elliptic curve in terms of a lattice

$$\Lambda_\tau = \{a + b\tau : a, b \in \mathbb{Z}\}.$$

2.4 Isomorphism Classes of Elliptic Curves

By considering elliptic curves as complex lattices we are able easily to determine the isomorphism class of any curve.

Proposition 2.4.1. *Let $E(\mathbb{C}) = \mathbb{C}/\Lambda_\tau$ and $E'(\mathbb{C}) = \mathbb{C}/\Lambda_{\tau'}$ be two elliptic curves. Then $E(\mathbb{C}) \cong E'(\mathbb{C})$ if and only if there exists some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_\tau = \Lambda_{\tau'}$.*

Proof. See [17, Page 171]. □

Given two lattices it is not immediately obvious how to determine if such an α exists. The modular j-invariant is a powerful tool in classifying these lattices.

Definition 2.4.2. *Let $\Lambda \subset \mathbb{C}$ be a lattice. Then the modular j-invariant of Λ is defined to be*

$$j(\Lambda) = 1728\frac{g_2(\Lambda)}{\Delta(\Lambda)}.$$

Where $\Delta(\Lambda)$ is the discriminant of the curve $\mathbb{C}/\Lambda$,

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^3.$$

We will sometimes write $j(\tau)$ for $j(\Lambda_\tau)$ for any $\tau \in \mathbb{C}^\times$. Moreover, for any $\alpha \in \mathbb{C}^\times$, we have $j(\tau) = j(\alpha\tau)$. How to classify lattices using the j-invariant is described by the following proposition.

Proposition 2.4.3. *Two lattices Λ_τ and $\Lambda_{\tau'}$ represent isomorphic elliptic curves defined over $\mathbb{C}$ if and only if*

$$j(\tau) = j(\tau').$$

Proof. See [15, Page 36] □

We summarize the results of this chapter in the following theorem.

Theorem 2.4.4. *The category of elliptic curves over $\mathbb{C}$ with isogenies between them is equivalent to the category of lattices $\Lambda \subset \mathbb{C}$ with maps between them (the maps defined by multiplying lattices by an $\alpha \in \mathbb{C}$). The functor between the two categories is exactly described by the maps and isomorphims defined in this section.*

As the set of all isogenies from an elliptic curve to itself forms a ring, so does the set of maps from a lattice to itself. Given an elliptic curve $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, we define the endomorphism ring of E to be the set

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}.$$

We shall discuss an important application of this ring when we consider the theory of complex multiplication later on.

Chapter 3

The Modularity Theorem

In the previous section we defined an analytic isomorphism between elliptic curves and lattices, Λ. By considering properties of these lattices we are able to determine many results about the curves they represent. Of primary importance for our discussion is the famous modularity theorem for elliptic curves. Namely, that for any elliptic curve $E/\mathbb{Q}$ there exists a surjective morphism $X_0(N) \to E$ defined over $\mathbb{Q}$ - where $X_0(N)$ is the classical modular curve. Wiles is credited with the proof of this beautiful theorem, and he certainly provided the most important details. Ultimately, many people played important roles in its development. It was originally conjectured by Taniyama [20], and made more precise by Shimura [13, 12]. Wiles, together with Taylor, proved the result for semistable curves in [24] and [21], which was enough to prove Fermat's last theorem. The full theorem for all Elliptic curves over $\mathbb{Q}$ was not proved until 2001 by Breuil, Conrad, Harris, and Taylor in [5]. In this section we will discuss the relevant ideas and structures to the construction of Heegner points on Elliptic curves, and develop a small part of the background to the proof of the modularity theorem.

3.1 Modular Forms

This section will define modular forms only for $SL_2(\mathbb{Z})$ and the congruence subgroup $\Gamma_0(N)$. For a more complete description we direct the reader to William Stein's book [18].

Fix the following notations:

$$\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\},$$
$$\Lambda_\tau = \{a + b\tau : a, b \in \mathbb{Z}\} \text{ for } \tau \in \mathcal{H}.$$

It is clear that any lattice $\Lambda \subset \mathbb{C}$ is homothetic to some Λ_τ for some $\tau \in \mathcal{H}$. We wish to be able to determine easily when two lattices Λ_τ and $\Lambda_{\tau'}$ are equivalent. To do this, we note that the set $SL_2(\mathbb{Z})$ acts on $\mathcal{H}$ by fractional linear transformations, defined for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $\tau \in \mathcal{H}$ as

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

We note that, excluding $\pm I$, there are no nontrivial actions, thus the set

$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$$

acts faithfully on $\mathcal{H}$. We prove some additional details about this action.

Proposition 3.1.1. *The region*

$$F = \{z \in \mathcal{H} : |z| \geq 1 \text{ and } |\Re(z)| \leq \frac{1}{2}\}$$

is a fundamental domain for $\mathcal{H}/SL_2(\mathbb{Z})$.

Proof. See [17, Page 430]. □

It follows that every lattice $\Lambda \subset \mathbb{C}$ is in fact homothetic to a lattice Λ_τ for some $\tau \in F$ (more on this below). Moreover, given a lattice with two bases $\Lambda = \{\omega_1, \omega_2\}$ and $\Lambda = \{\omega_1', \omega_2'\}$, we can relate them by

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}$$

for some $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$. By possibly switching the values of ω_1 and ω_2, we can assume that $\Im(\omega_2/\omega_1) > 0$. Set $\tau = \omega_2/\omega_1$, then we have

$$\Lambda = \omega_1 \Lambda_\tau.$$

Computing with $\{\omega_1', \omega_2'\}$, we find

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} a\tau + b \\ c\tau + d \end{pmatrix}.$$

So we can associate a τ and τ' by

$$\tau' = \frac{a\tau + b}{c\tau + d}.$$

This is exactly the group action described above. Additionally, we also find the group $SL_2(\mathbb{Z})$ to have a very clearly defined structure.

Lemma 3.1.2. *The group $SL_2(\mathbb{Z})$ is generated by the elements*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Proof. See [10, Page 228]. □

Note that the elements S and T induce the functions $z \mapsto -1/z$ and $z \mapsto z+1$, respectively. We are now in a position to define modular forms.

Definition 3.1.3. *Fix an integer k. A meromorphic function f on $\mathcal{H}$ that satisfies*

$$f(\gamma\tau) = (c\tau + d)^k f(\tau) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

is called an unrestricted modular function of weight k.

Let $q = e^{2\pi i\tau}$. Then by using its Fourier expansion and the fact that $f(z) = f(z+1)$, we define the q-expansion of f about ∞ to be

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

(See [10, Page 224]). We say that a modular function f is a modular form if its q-expansion above has $a_n = 0$ for $n < 0$. If we have the additional condition that $a_0 = 0$, then we call f a cusp form.

Corollary 3.1.4. *Suppose f is a meromorphic function on $\mathcal{H}$ such that, for all $\tau \in \mathcal{H}$*

$$f(\tau + 1) = f(\tau),$$
$$f(-1/\tau) = (-\tau)^k f(\tau),$$

and the q-expansion of f at infinity has no negative terms. Then f is a modular form.

Proof. Follows from Lemma 3.1.2. □

Proposition 3.1.5. *If k is an odd number, then any modular function of weight k is zero.*

Proof. We note that for $\alpha = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, we have $\alpha\tau = \tau$ for all $\tau \in \mathcal{H}$. Let k be an odd integer, then if f is a modular form of weight k we have

$$f(\tau) = f(\alpha\tau) = (-1)^k f(\tau) = -f(\tau).$$

It follows that f is zero. □

After working with modular forms, it soon becomes clear that we must also consider functions that are modular only on some subgroups of $SL_2(\mathbb{Z})$. While there are several important subgroups that provide a rich description of the structure of modular forms, we will focus solely on one. Fix an integer $N > 1$, then of primary importance for us is the subgroup $\Gamma_0(N) \subset SL_2(\mathbb{Z})$, defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

In other words, $\Gamma_0(N)$ is the set of matrices which are upper triangular modulo N. Again, $\Gamma_0(N)$ acts on $\mathcal{H}$ by the same action, so we may consider the quotient space $\mathcal{H}/\Gamma_0(N)$. For our purposes it will be useful to compactify the space in the usual way by adjoining additional points. Let $\mathcal{H}^*$ be obtained by adjoining $\mathbb{P}^1(\mathbb{Q})$ (where $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$) to $\mathcal{H}$, so

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

In the next section we will describe precisely how to topologize $\mathcal{H}^*$, and then will show that $\mathcal{H}^*/\Gamma_0(N)$ is a Hausdorff, compact space. For now, let us merely extend our action onto $\mathcal{H}^*$ by including the rule

$$\gamma\infty = \frac{a}{c} = \lim_{\tau \to \infty} \gamma\tau.$$

Of central importance to modular functions will be the set of *cusps* for $\Gamma_0(N)$. Let $C(\Gamma_0(N))$ be the set of $\Gamma_0(N)$ orbits of $\mathbb{P}^1(\mathbb{Q})$. From [18, Lemma 1.12] we have that $C(\Gamma_0(N))$ is a finite set. The definition of a modular function on $\Gamma_0(N)$ is as follows.

Definition 3.1.6. *Fix an integer k. A meromorphic function f on $\mathcal{H}$ that satisfies the following:*

- $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ *for all* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$,
- f *is meromorphic at all cusps in* $C(\Gamma_0(N))$,

is called a modular function of weight k on $\Gamma_0(N)$.

A modular function f on $\Gamma_0(N)$ is called a modular form if it is holomorphic on $\mathcal{H}$ and on all points in $C(\Gamma_0(N))$. If f is a modular form that vanishes at all points in $C(\Gamma_0(N))$, then f is called a cusp form. We let $S_2(N)$ be the set of all cusp forms of weight two on $\Gamma_0(N)$. Let $f \in S_2(N)$, then f satisfies $f|\gamma = f$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, where

$$(f|\gamma)(z) = (cz + d)^{-2} f(\gamma z). \tag{3.1.1}$$

Since $(cz+d)^{-2} = \frac{d}{dz}(\gamma z)$, it follows that

$$f(\gamma z)d(\gamma z) = f(z)dz.$$

Additionally, since f vanishes at its cusps, it has a Fourier expansion about ∞, given by

$$f(z) = \sum_{n=1}^{\infty} a_n q^n.$$

In the coming sections we will be interested in associating to each elliptic curve a special kind of cusp form $f \in S_2(N)$ (which will have all integer coefficients) called a newform. These newforms play an important part in the proof of the existence of a modular parameterization for rational elliptic curves.

3.2 The Modular Curve $X_0(N)$

Now let $\mathcal{H}^*$ and $\Gamma_0(N)$, together with the action of $\Gamma_0(N)$ on $\mathcal{H}^*$, be defined as above. We endow $\mathcal{H}^*$ with a topology by the following rules:

1. Any open disc completely contained in $\mathcal{H}$ is open.
2. For $x \in \mathbb{Q}$, an open set around x is of the form $D \cup \{x\}$ where D is an open disc in $\mathcal{H}$ with radius $r > 0$, centered at $x + ir$.
3. For any $r > 0$, the set $\{z \in \mathcal{H} : \Im(z) > r\}$ is open and centered at ∞.

It is easy to see that $\mathcal{H}^*$ is Hausdorff. We define the curve $X_0(N)$ to be the algebraic curve whose complex points are identified with the quotient space $\mathcal{H}^*/\Gamma_0(N)$. E.g.

$$X_0(N) := \mathcal{H}^*/\Gamma_0(N).$$

Proposition 3.2.1. *$X_0(N)$ is a compact, Hausdorff space that is also a Riemann surface.*

Proof. See [10, Pages 311 and 333]. □

As it is difficult to write down explicit expressions for points on $X_0(N)$, we first define an easy way to present points on $X_0(N)$. Specifically as two elliptic curves with an isogeny between them. We require the following proposition.

Proposition 3.2.2. *Let E be an elliptic curve, $N \geq 1$ an integer, $C \subseteq E$ be a cyclic subgroup of order N. Then there exists a unique elliptic curve E' and isogeny $\phi : E \to E'$ such that $\ker(\phi) = C$.*

Proof. See [17, Page 74]. □

Let $\gamma \in \Gamma_0(N)$, $\tau \in \mathcal{H}/\Gamma_0(N)$, and let E_{Λ_τ} be the associated elliptic curve with cyclic subgroup

$$C = \left\{ \frac{1}{N}, \frac{2}{N}, ..., \frac{N-1}{N} \right\} \subset \mathbb{C}/\Lambda_\tau = E(\mathbb{C}).$$

One can easily check that C remains invariant under the action of γ. It follows from Proposition 3.2.2 that the point $\tau \in \mathcal{H}$ corresponds exactly to a unique triple $(E_{\Lambda_\tau}, E', \phi)$, where $\phi : E_{\Lambda_\tau}$ is the unique isogeny with $\ker(\phi)$ cyclic of order N. We can think of points of $X_0(N)$ as covering pairs of elliptic curves with an isogeny between them (in some texts points are written (E, C), where E is an elliptic curve and C is a cyclic subgroup or order N). Note that two points (E, E', ϕ) and $(\hat{E}, \hat{E}', \hat{\phi})$ on $X_0(N)$ are equivalent if and only if there exists isomorphism ψ, ψ' such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi'} \\ \hat{E} & \xrightarrow{\hat{\phi}} & \hat{E}' \end{array}$$

Additionally, the modular j-invariant parameterizes $X_0(N)$. As elliptic curves can be defined over arbitrary fields (such as $\mathbb{Q}(\sqrt{d})$ or $\mathbb{C}$, so can $X_0(N)$. The j-invariant makes the complex description of $X_0(N)$ very clear. As the map

$$\tau \mapsto (j(\tau), j(N\tau))$$

identifies $X_0(N)(\mathbb{C})$ with an algebraic curve in $\mathbb{C}^2$. This parameterization will be further utilized in our discussion of complex multiplication.

This is a very brief description of the modular curve, for a more detailed construction we would direct the reader to [12, Chapter 1].

3.3 Modular Elliptic Curves

Let $E(\mathbb{Q})$ be an elliptic curve. We recall that a modular parameterization of an elliptic curve is a finite $\mathbb{Q}$-rational morphism

$$\varphi : X_0(N) \to E.$$

If such a morphism exists, then we say that E is a modular elliptic curve. This section will provide an extremely superficial look at the development of the proof of

the modularity theorem, focusing on aspects relevant to Heegner points. We begin with a brief discussion of Hecke operators for modular functions, then define and state several facts about the L-series attached to cusp forms. Finally, we state the Eichler-Shimura theorem and the modularity theorem.

3.3.1 Hecke Operators

Hecke operators are a powerful tool in the study of vector spaces of modular forms. As we barely scratch the surface, we would suggest the reader refer to [7, Chapter 2] and [13, Chapter VII] for a more complete overview of Hecke operators related to modular forms.

In the simplest context, for a fixed integer n and lattice $\Lambda \subset \mathbb{C}$ with basis $\{w_1, w_2\}$, a Hecke operator is a function T of the form

$$T_N(\Lambda) = \sum_{\substack{\Lambda' \subset \Lambda \\ [\Lambda : \Lambda'] = n}} (\Lambda').$$

It is shown in [15, Section I.9] how Hecke operators on lattices act on modular forms over $SL_2(\mathbb{Z})$. However, for our purposes we only consider Hecke operators for cusp forms of weight two the group $\Gamma_0(N)$ (recall we called this space $S_2(N)$). Let $\Omega(X_0(N))$ denote the vector space of holomorphic differentials on $X_0(N)$. Then the map from $S_2(N)$ to $\Omega(X_0(N))$ which associates the form f by

$$f \longmapsto w_f = 2\pi i f(\tau) d\tau$$

identifies $S_2(N)$ with $\Omega(X_0(N))$. It follows from the Riemann-Roch theorem that $S_2(N)$ is a finite-dimensional vector space with dimension equal to that of $X_0(N)(\mathbb{C})$.

In order to fully define the Eichler-Shimura relationship between elliptic curves and modular forms, we must define the notion of Hecke operators on $\Gamma_0(N)$. More specifically, on cusp forms $f \in S_2(N)$.

Definition 3.3.1. *Fix a cusp form $f \in S_2(N)$, and a prime $p|N$. Then the p^{th} Hecke operator T_p on f is defined by*

$$T_p(f) = \begin{cases} \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) + pf(p\tau) & \text{if } p|N, \\ \frac{1}{p} \sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right) & \text{otherwise.} \end{cases}$$

We extend the definition to a generic $n \in \mathbb{N}$ by equating the coefficient of n^{-s} in the formal Dirichlet series

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p|N} \frac{1}{1 - T_p(p)^{-s}} \prod_{p \nmid N} \frac{1}{1 - T(p)^{-s} + p^{1-2s}}.$$

Proposition 3.3.2. *Let $\mathbb{T}$ be the commutative algebra generated over $\mathbb{Z}$ by the Hecke operators $\{T_n\}$. Then $\mathbb{T}$ is a commutative subalgebra of $End_{\mathbb{C}}(S_2(N))$ and is a finitely generated $\mathbb{Z}$-module with rank equal to the genus of $X_0(N)$.*

Proof. See [7, Page 15]. □

Denote the set of cusp forms in $S_2(N)$ with integer coefficients by $S_2(N, \mathbb{Z})$. It follows from $\mathbb{T}$ being a finitely generated $\mathbb{Z}$-module that $S_2(N)$ has a basis consisting only of modular forms in $S_2(N, \mathbb{Z})$ [7, Page 16]. Moreover, for each $f \in S_2(N, \mathbb{Z})$, there exists a $\mathbb{Z}$-algebra homomorphism $\lambda : \mathbb{T} \to \mathbb{Z}$ such that for each Hecke operator T_n we have [18, Page 162]

$$T_n(f) = \lambda(T_n)(f).$$

We discuss an application of this operator in the next section.

Remark 3.3.3. *The space $S_2(N)$ actually has an orthogonal decomposition arising from a subspace $S_2^{new}(N)$ of so-called newforms that decomposes as a direct sum of one-dimensional eigenspaces under the action of $\mathbb{T}$ (a result of Atkin-Lehner theory). It is not crucial to our discussion, but it is in fact these newforms that are used in the Eichler-Shimura construction and the modularity theorem. For a succinct summary of newforms, we would direct the reader to [10, Page 283].*

3.3.2 The Eichler-Shimura Construction and the Modularity Theorem

Let f be a newform of level N. Then we define the L-series of f to be

$$L(f, s) = \sum_{n=1}^{\infty} a_n n^{-s},$$

where $a_n = \lambda(T_n)$. Fix a newform

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n,$$

with $a_1 = 1$ and $a_n \in \mathbb{Z}$ for all n. We state several important properties of these L-functions (as appear in [7, Section 2.4]), taking note the similarities to the L-function of an elliptic curve.

Proposition 3.3.4. *The L-series attached to f has an Euler product factorization*

$$L(f,s) = \prod_{p|N} \frac{1}{1-c(p)p^{-s}} \prod_{p\nmid N} \frac{1}{1-c(p)p^{-s}+p^{1-2s}}.$$

Proof. See [10, Page 282]. □

Proposition 3.3.5. *$L(f,s)$ has the integral representation*

$$L(f,s) = (2\pi)^s \Gamma(s)^{-1} \int_1^\infty (t^{s-1} + (-1)^k t^{2k-s-1}) f(it) dt,$$

where $\Gamma(s)$ is the usual Γ function defined by $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$.

Proof. See [15, Page 84]. □

Proposition 3.3.6. *The function*

$$\Lambda(f,s) = N^{s/2}(s\pi)^{-s}\Gamma(s)L(f,s)$$

satisfies the functional equation

$$\Lambda(f,s) = -\Lambda(w_N(f), 2-s) = -\epsilon\Lambda(f, 2-s).$$

Proof. See [10, Page 270]. □

The fact that the L-series of cusp forms and the L-series of elliptic curves have extremely similar properties suggests a relationship between them. The strength of this relationship is demonstrated by the following theorem.

Theorem 3.3.7 (Eichler-Shimura Theorem)**.** *Let $f \in S_2(N,\mathbb{Z})$ be a normalized newform, together with a Fourier expansion $a_n(f)$ such that each $a_i \in \mathbb{Z}$. Then there exists an elliptic curve E_f over $\mathbb{Q}$ such that*

$$L(E_f, s) = L(f, s).$$

Proof. Knapp [10, Chapter XI] provides an excellent overview of the Eichler-Shimura construction. We provide some of the basic proof ideas (all of which appear in the reference.)

We let W_N be the Atkin-Lehner involution on $\mathcal{H}$ given by

$$W_N(\tau) = -\frac{1}{N\tau}.$$

Then W_N normalizes $\Gamma_0(N)$. We let λ be the $\mathbb{Z}$-algebra homomorphism associated with f, so f must also be an eigenform for W_N. Let ϵ be the eigenvalue for W_N (so $\epsilon \in \{\pm 1\}$), then we have

$$W_N(f) = \epsilon f.$$

We let $I_f \subseteq \mathbb{T}$ be the ideal generated by $\ker(\lambda)$.

Now let

$$J_0(N) = \Omega(X_0(N))/H_1(X_0(N), \mathbb{Z})$$

be the Jacobian of $X_0(N)$, where $H_1(X_0(N), \mathbb{Z})$ is the first homology with coefficients in $\mathbb{Z}$. And let $A : X_0(N) \to J_0(N)$ be the Abel-Jacobi map defined by

$$P \mapsto \left(z \mapsto \int_{i\infty}^{P} z \right).$$

We note that since $S_2(N)$ can be identified with $\Omega(X_0(N))$ using the map $f \mapsto w_f = 2\pi i f(\tau) d\tau$, we can write the Jacobian $J_0(N)$ in terms of $S_2(N)$ as

$$J_0(N) \cong S_2(N)/H_1(X_0(N), \mathbb{Z}).$$

In this way, the Hecke operators in $\mathbb{T}$ define endomorphisms of $J_0(N)$ over $\mathbb{Q}$. Thus we may consider the image $I_f(J_0(N)) \subseteq J_0(N)$, as well as the quotient

$$J_0(N)/I_f(J_0(N)).$$

As it turns out, this object is an elliptic curve (see [10, Chapter XI, Sections 10 and 11]), which we denote E_f. Let Q be the quotient map from $J_0(N)$ to $J_0(N)/I_f(J_0(N))$, then we can define the map $\varphi : X_0(N) \to E_f$, as

$$\varphi(z) = A(Q(z)).$$

Showing that the L-series of E_f and f coincide is not an easy task, and we leave it at the reader's discretion to view in [13]. □

It was conjectured after the proof of the Eichler-Shimura theorem that this construction worked in both directions. As said before, the path to prove the following theorem was long and had many contributors.

Theorem 3.3.8 (The Modularity Theorem)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ in minimal Weierstrass form of conductor N. Then there is a surjective map of non-constant morphisms (the modular parameterization)*

$$\varphi : X_0(N) \to E$$

where E can be viewed in terms of a lattice $\mathbb{C}/\Lambda$ with normalized generators w_1, w_2 as defined previously, and N is the smallest such integer for which the parameterization exists.

Proof. The proof can be understood from the references listed in the beginning of this Chapter. We simply note that to any elliptic curve $E/\mathbb{Q}$ we can associate a newform $f \in S_2(N, \mathbb{Z})$ so that the L-series coincide. Then, using f, we construct the map φ from $X_0(N)$ to $E(\mathbb{C})$, noting the image of z is in the quotient $\mathbb{C}/\Lambda$,

$$z \longmapsto 2\pi i \int_{i\infty}^{z} f(z) = \sum_{n=0}^{\infty} \left(\frac{a_n}{n}\right) e^{2\pi i n \tau}.$$

We can then map the point $\varphi(\tau)$ to the associated point on $E(\mathbb{C})$ using the function Φ defined in Section 2.2. It is these two facts that will be relevant to our construction. □

Knowing that each elliptic curve is modular and having a clear formula to describe the parameterization is a powerful tool in understanding the structure of a particular curve. In the next section, we consider special points on $X_0(N)$ and their images under this map.

Chapter 4

Heegner Points

The evolution of the theory of Heegner points is described by Bryan Birch in [4]. Kurt Heegner in [9], who had been working with imaginary quadratic fields and the congruence number problem, developed somewhat mystical techniques for constructing rational points on very specific elliptic curves using the fact that these curves were modular. Birch, Gross, and Zagier were interested in a generalization of this technique to apply to any elliptic curve defined over certain class fields. While this was before the proof of the modularity theorem, they realized that one could find points on $X_0(N)$, and then use the modular parameterization to map these points onto elliptic curves. For more information, we would direct the reader to [1, 2, 5].

Given an elliptic curve E, defined over the rationals, of analytic rank 1 and conductor N, we will explicitly define a Heegner point on $X_0(N) = \mathcal{H}^*/\Gamma_0(N)$ that can be used construct a non-trivial point of infinite order on $E(\mathbb{Q})$, so the algebraic rank of E is at least 1. We first define the points from an abstract perspective, then give a more concrete approach which lends itself to specific calculation of these types of points.

4.1 Complex Multiplication

Let K be an imaginary quadratic extension of $\mathbb{Q}$ with discriminant $D < 0$. So we may write $K = \mathbb{Q}(\omega)$ where

$$\omega = \begin{cases} \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \\ \frac{\sqrt{D}}{2} & \text{otherwise.} \end{cases}$$

Let $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$ be the ring of integers of K, then an order of K, $\mathcal{O} \subseteq \mathcal{O}_K$, is a subring of K of the form

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}c\omega$$

where c is any integer greater than zero. Note that every order is uniquely determined by c, which we will call the conductor of $\mathcal{O}$.

Let E be an elliptic curve with $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Recall the endomorphism ring attached to E is defined by

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}.$$

From [17, Page 102], we have that $\mathrm{End}(E)$ is either isomorphic to $\mathbb{Z}$ or to some order in an imaginary quadratic extension K of $\mathbb{Q}$.

Definition 4.1.1. *If an elliptic curve E has $End(E) \cong \mathcal{O} \supset \mathbb{Z}$ (properly contains $\mathbb{Z}$) for some order in an imaginary quadratic field, then we say E has complex multiplication. More specifically, given an order $\mathcal{O}$, we say that E has complex multiplication by $\mathcal{O}$ if $End(E) \cong \mathcal{O}$.*

Let's examine complex multiplication using the map $\Phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$. To start, let $h : E(\mathbb{C}) \to E(\mathbb{C})$ be an isogeny, and consider the function $(\Phi^{-1} \circ h \circ \Phi)$. It follows from [10, Lemma 6.18] that $(\Phi^{-1} \circ h \circ \Phi)(z) = az$ for some $a \in \mathbb{C}$. Note that the only non-trivial, well-defined isogenies have $a \in \mathbb{C}, a \notin \mathbb{R}$. Let w_1, w_2 be the generators for the lattice Λ. Then we have an easy method for determining whether an elliptic curve has complex multiplication.

Proposition 4.1.2. *An elliptic curve E has complex multiplication if and only if w_2/w_1 lies in an imaginary quadratic extension $\mathbb{Q}$. In which case $End(E)$ will be isomorphic to some order, $\mathcal{O} \subseteq \mathbb{Q}(w_2/w_1)$.*

Proof. See [17, Page 176]. □

4.2 Definition of Heegner Points

We recall that points on the curve $X_0(N) = \mathcal{H}^*/\Gamma_0(N)$ correspond to triples (E, E', ϕ) of elliptic curves with isogenies between them. Fix $N > 1$, and let $P = (E, E', \phi) \in X_0(N)$. Then we can choose $\tau \in \mathcal{H}$ such that $E \cong \mathbb{C}/\Lambda_\tau$ and

$$E' \cong \frac{1}{N}\mathbb{Z} + \mathbb{Z}\tau.$$

Then supposing E has complex multiplication by an order $\mathcal{O} \subset \mathbb{Q}(\sqrt{D})$, from the proposition above we must have $\mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{D})$. We define Heegner points using complex multiplication.

Definition 4.2.1. *Fix an imaginary quadratic number field K. Let $(E, E', \phi) \in X_0(N)$ such that*

$$End(E) \cong End(E') \cong \mathcal{O}$$

for some order $\mathcal{O} \subset K$ with $\mathcal{O} = \mathbb{Z} + \mathbb{Z}c\omega$ of discriminant $D < 0$. Then we call (E, E', ϕ) a Heegner point of level N, discriminant D, and conductor c on $X_0(N)$. Let $\mathcal{HP}_N(D, c)$ denote the set of Heegner points of level N, discriminant D, and conductor c.

We will mostly leave out the conductor of a Heegner point, as it is not crucial to our discussion. The principles for larger conductors are essentially the same. For the remainder of the paper we set $c = 1$ and write $\mathcal{HP}_N(D)$ for the set of Heegner points with conductor 1. We will show in the next section that $\mathcal{HP}_N(D)$ is a finite set with easily calculable size. We begin by asking exactly which orders $\mathcal{O}$ of imaginary quadratic rings K could possibly satisfy the above condition for an elliptic curve E; moreover, we would like to understand the images of these points on $E(\mathbb{C})$. Fix an integer N, choose $K = \mathbb{Q}(\sqrt{D})$ a binary quadratic field with fundamental discriminant $D < 0$, and let $\mathcal{O}_K$ be the ring of integers of K. We first note that a Heegner point on $X_0(N)$ is of the form

$$\phi : \mathbb{C}/I \to \mathbb{C}/I(n^{-1})$$

where $[I] \in Cl(D)$ and n is a primitive ideal of $\mathcal{O}_K$ of norm N such that $\mathcal{O}_K/n\mathcal{O}_K \cong \mathbb{Z}/N\mathbb{Z}$, and ϕ is the natural isomorphism between them [4]. Thus, a Heegner point can be determined by a triple

$$(\mathcal{O}_K, n, [I]).$$

We note that by ranging over different ideal classes in $Cl(D)$ we obtain precisely $h(D)$ Heegner points of level N and discriminant D related to the primitive ideal n (where $h(D)$ is the class number of D). For such an ideal n to exist, we must have all primes p dividing N splitting in $K/\mathbb{Q}$, otherwise $\mathcal{HP}_N(D)$ will be empty. We refer to this condition as the *Heegner hypothesis* or the *Heegner condition*.

In the coming sections, we provide an alternative method by describing Heegner points in a more computationally friendly manner.

4.3 Computing Heegner Points

We begin by recalling that ideal classes in $Cl(D)$ can be represented by primitive binary quadratic forms. Gauss showed that for every value of D, there are only finitely many binary quadratic forms of discriminant D, and the number of these forms is

exactly the class number $h(D)$. Given a negative discriminant D, he additionally described an algorithm to find binary quadratic forms representing each ideal class in $Cl(D)$ (see [6, Chapter 5] for example). With this in mind, we let $\tau \in \mathcal{H}$ be a quadratic surd with associated integral primitive quadratic form $f_\tau = (A, B, C)$, so $A^2\tau + B\tau + C = 0$, $A > 0$, and $\gcd(A, B, C) = 1$. Define the discriminant of τ by $D = \Delta(\tau) = B^2 - 4AC < 0$. Then we can write τ in terms of A, B, C as

$$\tau = \frac{-B + \sqrt{D}}{2A}.$$

Proposition 4.3.1. *If τ is a quadratic surd in in $\mathcal{H}$ with discriminant $D < 0$, then $j(\tau)$ is an algebraic number defined over $K(D)$.*

Proof. See [7, Page 30]. □

Then if τ has discriminant D, $N\tau$ will typically have discriminant N^2D, and thus $j(N\tau) \in K(N^2D)$. We continue with an alternative presentation of a Heegner point to that given previously. In some texts this is given as the definition of a Heegner point, in others it is a lemma following from Definition 4.2.1. It is this representation that is most useful to algorithmically finding representatives for Heegner points.

Lemma 4.3.2. *Let D and N be integers that satisfy the Heegner hypothesis (all primes p dividing N are split in $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Let $\tau \in \mathcal{H}$ be a quadratic surd with $f_\tau = (A, B, C)$ and $\Delta(\tau) = D$. Then τ is a Heegner point of level N and discriminant D (up to modulo $\Gamma_0(N)$) if and only if $\Delta(\tau) = \Delta(N\tau) = D$.*

Proof. From the proposition above, we have both $j(\tau)$ and $j(N\tau)$ are defined over the same quadratic field $K = \mathbb{Q}(\sqrt{D})$. Moreover, by Gauss we have that both τ and $N\tau$ represent the same ideals in K. Let n be the relevant primitive ideal with respect to N in $\mathcal{O}_K$, and let $[I]$ be the ideal class corresponding to the binary quadratic forms represented by τ and $N\tau$. Then the Heegner point is $(\mathcal{O}_K, n, [I])$. See [19, Chapter 3] for further details. □

We will now prove several facts about Heegner points and their images under the map $\varphi : X_0(N) \to E(\mathbb{C})$, using this alternative representation of Heegner points. For the remainder of this section, fix an elliptic curve E over the rationals with conductor N. We have the following simple formula to determine if any $\tau \in \mathcal{H}/\Gamma_0(N)$ is a Heegner point via the following proposition.

Proposition 4.3.3. *Let τ, f_τ be as above, then τ is a Heegner point if and only if $N|A$ and $\gcd(A/N, B, CN) = 1$.*

Proof. We have

$$\tau = \frac{-B + \sqrt{D}}{2A} \quad \text{and} \quad N\tau = \frac{-NB + N\sqrt{D}}{2A},$$

and we wish to show that there exist B', A' such that

$$N\tau = \frac{-B' + \sqrt{D}}{2A'}.$$

We rewrite and equate real parts and imaginary parts to obtain $A = NA'$ and $B = B'$, which implies that N divides A. Also, since

$$\frac{A}{N}(N\tau)^2 + B(N\tau) + (CN) = 0,$$

the rest follows. The other direction is similar. □

We again note that $\mathcal{HP}_N(D)$ will be non-empty only when all prime factors p of N are either split or ramified in $\mathbb{Q}(\sqrt{D})$. To be more precise, we have the following proposition to describe the number of Heegner points in $\mathcal{HP}_N(D)$.

Proposition 4.3.4. *Let*

$$\mathcal{S}(D, N) = \left\{ \sqrt{D (mod\ 4N)} (mod\ 2N) \right\}.$$

Then the set $\mathcal{HP}_N(D)$ is in bijection with the set

$$\mathcal{S}(D, N) \times Cl(\mathbb{Q}(\sqrt{D})).$$

Proof. Given a Heegner point $\tau \in \mathcal{HP}_N(D)$ with

$$\tau = \frac{-B + \sqrt{D}}{2A},$$

let $f_\tau = (A, B, C)$ and in one direction we have

$$\tau \longmapsto (B \mod 2N, [f_\tau]).$$

For the other direction, fix $(\beta, [f]) \in \mathcal{S}(D, N) \times Cl(\mathbb{Q}(\sqrt{D}))$. Then we can find an $(A, B, C) \in [f]$ such that N divides A and $B \equiv \beta \pmod{2N}$. We send

$$(\beta, [f]) \longmapsto \frac{-B + \sqrt{D}}{2A}.$$

□

Our goal is to prove that we can use Heegner points, or at least their images on C/Λ, to construct a rational point on an elliptic curve. The first step is given in the following proposition.

Proposition 4.3.5. *Let τ be a Heegner point of discriminant D on $\mathcal{H}/\Gamma_0(N)$, and let H be the maximal unramified abelian extension of $Q(\sqrt{D})$ (ie. the Hilbert class field of $\mathbb{Q}(\sqrt{D})$). Then $\varphi(\tau) \in E(H)$.*

Proof. See [7, Page 33]. This can be shown using the theorem of complex multiplication of Shimura [13],[14]. □

From this, we can prove the following.

Theorem 4.3.6. *Let $E(\mathbb{Q})$ be an elliptic curve of conductor N, and let $\mathcal{HP}_N(D, \beta)$ be the set of all Heegner points $\tau \in \mathcal{HP}_N(D)$ such that $f_\tau = (A, B, C)$ has $B \equiv \beta \pmod{2N}$. Then define the complex point z_β as*

$$z_\beta = \varphi\left(\sum_{\tau \in \mathcal{HP}_N(D,\beta)} \tau\right) = \sum_{\tau \in \mathcal{HP}_N(D,\beta)} \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau}.$$

Let $P_\beta = \Phi(z_\beta)$ under usual mapping $\mathbb{C}/\Lambda \to E(\mathbb{C})$. Then $P_\beta \in E(\mathbb{Q})$.

Proof. See [2] or [22, Theorem 2.8]. □

Chapter 5

Algorithm and Examples

From the last section we see that given an elliptic curve $E/\mathbb{Q}$ of analytic rank 1, we can use Heegner points to construct points on $E(\mathbb{Q})$. A major issue with our algorithm is that we have no guarantee that the point P_β will be non-torsion, much less non-trivial. In this section, we discuss the practical issues of using Heegner points on $X_0(N)$ to construct rational points on an elliptic curve. We then demonstrate the process described on several different curves. Mark Watkins has implemented a highly efficient algorithm for constructing Heegner points on elliptic curves using *Magma*. For simplicity and understanding, we implement our algorithm in *SAGE*, and skip many of the optimization steps taken by Watkins in [22].

5.1 Algorithm for the Construction of a Rational Point

Based on the information in the preceeding sections, given an elliptic curve $E/\mathbb{Q}$ of conductor N, analytic rank 1, and whose associated newform f has an odd functional equation, we have a potential algorithm for the construction of a rational point on E.

1. Pick a fundamental discriminant $D < 0$ that satisfies the Heegner hypothesis.
2. Choose a $\beta \in \mathcal{S}(D, N)$, and compute the τ_i representatives for the Heegner points in $\mathcal{HP}_N(D, \beta)$ using Gauss's method in [6, Section 5.9].
3. Compute the sum
$$P_\beta = \sum_{\tau \in \mathcal{HP}_N(D,\beta)} \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau}$$
to sufficient precision on $\mathbb{C}/\Lambda$.

4. Using the function $\Phi : \mathbb{C}/\Lambda \to E$, map the value z_β to the point P_β on E and try to recognize the value as a rational number.

As said above, there is no guarantee that the point P_β will have infinite order. However, in the mid 1980s, Gross and Zagier proved a remarkable theorem precisely describing the canoical height of a Heegner point in terms of L-series.

Theorem 5.1.1 (Gross-Zagier Theorem)**.** *Let $D < -3$ be a fundamental discriminant that is also a square modulo $4N$, and $\gcd(D, 2N) = 1$, then*

$$\hat{h}(P_N(D)) = \frac{\sqrt{|D|}}{4Vol(E)} L'(E,1)L(E_D,1) \left(\frac{w(D)}{2}\right)^2 2^{\omega(gcd(D,N))} \tag{5.1.1}$$

where $\hat{h}$ be the canonical height function on the elliptic curve $E(\mathbb{Q})$, E_D is the quadratic twist of E by D, $Vol(E)$ is the volume of the fundamental parallelogram, Π, $w(D) = |\mathbb{Q}(\sqrt{D})^*|$, and $\omega(n)$ is the number of distinct prime factors of n.

Proof. See [8]. □

Then as a point $P \in E(\mathbb{Q})$ is torsion if and only if $\hat{h}(P) = 0$, we have a relatively simple method for predicting what height our Heegner point should have. We amend the algorithm described above to include the step

- Before computing $\mathcal{HP}_N(D, \beta)$, compute the expected height of the Heegner point. If it is zero, choose a different fundamental discriminant and start again.

In addition to being able to anticipate the height of a Heegner point, we can predict, using the Birch−Swinnerton-Dyer conjecture, what height a generator should have, and obtain a value for the index of a Heegner point in the Mordell-Weil group. Namely, we write $P_\beta = lG + T$, where $l \in \mathbb{N}$, G is a generator, and T is a torsion point (see [22, Conjecture 3.2]). Then we use BSD [3] to replace $L'(E, 1)$. We obtain

$$l^2 = \frac{\Omega_{re}}{4Vol(E)} \left(\prod_{p|N\infty} c_p(\#\text{Ш})\right) \frac{\sqrt{|D|}}{\#E(\mathbb{Q})^2_{tors}} L(E_D,1) \left(\frac{w(D)}{2}\right)^2 2^{\omega(gcd(D,N))}, \tag{5.1.2}$$

where Ω_{re} and Ω_{im} represent the real and imaginary portions of a normalized basis for a lattice Λ with $E \cong \mathbb{C}/\Lambda$. We further amend our algorithm to include the possibility that we do not get a generator (and thus potentially have a largely inflated height), we can then use the information to find a generator (modulo torsion) for the elliptic curve as follows (credit this step to [22]):

- After computing z_β, let $m = \gcd(l, \exp(E(\mathbb{Q})_{tors}))$, then rather than only checking if H_β is close to a rational point, we do it for several different values $\bar{z} \in \mathbb{C}/\Lambda$, ranging over possible values for the generator. Let u run over the range $1, .., lm$. Then if $\Delta(E) > 0$, check to see if the points

$$\Phi(\bar{z}_\beta) = \Phi\left(\frac{m\Re(z) + u\Omega_{re}}{ml}\right)$$

and

$$\Phi(\bar{z}_\beta) = \Phi\left(\frac{m\Re(z) + u\Omega_{re}}{ml} + \frac{\Omega_{im}}{2}\right)$$

are close to rational points on E. Otherwise, if $\Delta(E) < 0$, we let $o = \Im(z)/\Im(\Omega_{im})$ and check if the points

$$\Phi(\bar{z}_\beta) = \Phi\left(\frac{m\Re(z) + u\Omega_{re}}{ml} + \frac{o\Omega_{re}}{2}\right)$$

are close to rational points on E.

5.2 Computational Issues

An important question is to what level of accuracy must we do our computations in order to be sure we will be able to recognize the final points as rational numbers. The use of continued fractions says that if we expect a point with numerator and denominator of H digits, then we will need about $2H$ digits of precision to guarantee we can recognize it at as rational number. The first step is to be able to compute the height to a sufficient accuracy to be able to confidently describe the value $\hat{h}(P)$. We have the following to bound the error in computing $L'(E, 1)$.

Proposition 5.2.1 ([16], Proposition 4.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with a functional equation of odd sign. Then for $m \geq 100$, we have*

$$\left| L'(E,1) - 2\sum_{n=1}^{m} \frac{a_n}{n} E_1\left(\frac{2\pi n}{\sqrt{N}}\right) \right| \leq \frac{\sqrt{N}}{\pi m^{3/2 - 1/\log\log m}(e^{2\pi m/\sqrt{N}} - 1)},$$

where

$$E_1(x) = \int_x^\infty \frac{e^{-t}}{t} dt.$$

As we will be dealing (for the purposes of this paper), with points with generally small height, the above proposition convinces us that the height computation will be rapidly convergent as we do not need many points of accuracy. As we are more

interested in an approximation than the actual value. We wish to know how many terms of the L-series we must compute to ensure we have enough accuracy to reconstruct the image of the point z_β on $E(\mathbb{Q})$. We have the following error bound for the computation to with 10^{-d}.

Proposition 5.2.2 ([7], Proposition 1.1)**.** *For any $\tau \in \mathcal{H}$, the sum can be computed to within 10^{-d} using M terms of the L-series. Where*

$$M = \frac{\log 10^{-d}}{-2\pi\Im(\tau)}.$$

In other words

$$\left| \left(\sum_{n=1}^{\infty} \frac{a_n}{n} a^n \right) - \left(\sum_{n=1}^{M} \frac{a_n}{n} a^n \right) \right| \leq 10^{-d}.$$

5.3 Examples

We present three sample computations, the first on simple curves with small height to demonstrate the process, we then compute a Heegner point of larger height. When computing heights of points P, we use the notation $x+$ to mean $\hat{h}(P) \geq x$.

5.3.1 The Curve $E : y^2 + y = x^3 - x$

We present a step by step computation of a Heegner point on the curve $[0, 0, 1, -1, 0]$ of conductor 37. We compute the first several possible discriminants to be

$$D = -4, -7, -11, -40, -47, -67, -71, -83, -84, -95, ...$$

Using the Gross-Zagier formula, we have the height of the Heegner point on the curve as $\hat{P}_\beta \approx 0.205...$, then, combining with the Birch-Swinnerton−Dyer conjecture we have the index as $l = 4$. We can expect a generator to have height $\approx 0.0511....$ We choose $D = -40$, for which the number $h(D) = 2$, and compute the relevant τ representatives as binary forms. We have $\beta \in \{16, 58\}$, choosing $\beta = 16$ we have

(A, B, C)	τ	$\approx \varphi(\tau)$
$(37, 16, 2)$	$\frac{\sqrt{-40}-16}{74}$	$0.567136607830584 - 0.5721826548836951i$
$(74, 16, 1)$	$\frac{\sqrt{-40}-16}{148}$	$0.567136607830584 + 0.5721826548836951i$

Summing the values in the last column gives

$$z_{16} \approx 1.134273215661168281021611290 5...$$

Which under the weierstrass $\wp$-function gives $x(P_{16}) = 1$. Thus, a Heegner point of discriminant -40 associated to E is given by

$$P_{16} = (1, -1, 1).$$

We of course note that a naive point search would have yielded this point, however the example is a simple demonstration of how the construction works.

5.3.2 The Curve $E : y^2 + xy + y = x^3 - 362x + 2615$

We next consider a curve with slightly larger conductor, and larger generator, the curve $[1, 0, 1, -362, 2615]$ of conductor 120687. We choose $D = -383$ for which the class number is $h(D) = 17$, and $\beta = 16559$. Using the Gross-Zagier formula we compute the height of the Heegner point to be $\hat{h}(P_{16559}) = 135.7534+$, and combined with the BSD conjecture, we get $l^2 = 6$. Thus we can expect the height of a generator to be $\approx 3.77+$. By the formulae above, we need 19 digits of accuracy to guarantee we can reconstruct the point. We compute using $\approx 300,000$ terms of the L-series, the points

(A, B, C)	τ	$\approx \varphi(\tau)$
$(120687, 16559, 568)$	$\frac{\sqrt{-383}-16559}{241374}$	$0.26508 - 0.50747i$
$(241374, 16559, 284)$	$\frac{\sqrt{-383}-16559}{482748}$	$2.2320 + 1.7208i$
$(241374, 257933, 68907)$	$\frac{\sqrt{-383}-257933}{482748}$	$-2.6162 - 0.75971i$
$(362061, 257933, 45938)$	$\frac{\sqrt{-383}-257933}{724122}$	$-1.1695 - 0.79339i$
$(482748, 16559, 142)$	$\frac{\sqrt{-383}-16559}{965496}$	$2.7122 + 1.7673i$
$(482748, 740681, 284107)$	$\frac{\sqrt{-383}-740681}{965496}$	$-1.1768 + 0.76975i$
$(724122, 257933, 22969)$	$\frac{\sqrt{-383}-257933}{1448244}$	$-2.6157 - 1.4293i$
$(724122, 982055, 332966)$	$\frac{\sqrt{-383}-982055}{1448244}$	$1.6474 + 0.11133i$
$(844809, 1223429, 442934)$	$\frac{\sqrt{-383}-1223429}{1689618}$	$-3.2257 - 1.1638i$
$(965496, 16559, 71)$	$\frac{\sqrt{-383}-16559}{1930992}$	$0.85187 + 1.8400i$
$(965496, 1706177, 753768)$	$\frac{\sqrt{-383}-1706177}{1930992}$	$1.6393 + 3.1599i$
$(1086183, 1706177, 670016)$	$\frac{\sqrt{-383}-1706177}{2172366}$	$-1.8627 + 0.89410i$
$(1448244, 1706177, 502512)$	$\frac{\sqrt{-383}-1706177}{2896488}$	$-1.0722 - 0.039521i$
$(1689618, 1223429, 221467)$	$\frac{\sqrt{-383}-1223429}{3379236}$	$-2.8211 - 2.3519i$
$(1930992, 1947551, 491063)$	$\frac{\sqrt{-383}-1947551}{3861984}$	$0.053184 - 0.58565i$
$(2051679, 2188925, 583838)$	$\frac{\sqrt{-383}-2188925}{4103358}$	$-1.2826 - 2.1691i$
$(3861984, 5809535, 2184803)$	$\frac{\sqrt{-383}-5809535}{7723968}$	$-0.71193 - 1.1009i$

Again, we sum the values in the last column to obtain

$$z_{16559} \approx -9.062773485354465964287119 8... - 0.54744493234053133982509759...i$$

for which the associated point on the curve is

(272102349952560490569588857348997982142836423870936241800081/23719803251449217039203879701728255083093757587426409640000, −347846021501465403966847189167974399347780583229849859648987375084929568240434704677106293653142586306364103111822826114820627371570273018415832850716784927077990972186312000000, 1)

Ranging over u, we obtain the relevant point

$$\bar{z}_{16559} \approx 1.21449691341147726718101677171508954359916116665510...$$

Which mapping to the curve E using Φ and reconstructing using continued fractions gives the point (a generator)

$$P_{16559} = (47, 276, 1).$$

5.3.3 A Larger Example

In this section, we compute a generator for the curve

$$E : y^2 + xy = x^3 - x^2 - 36502495762x - 2684284892271276$$

of conductor $N = 169862$. We choose $D = -327$ for which $h(D) = 12$. The Heegner point will have height $\approx 53875.2354+$, with index $l = 12$. Thus, we can expect the height of a generator to be $\approx 374.1336+$

(A, B, C)	τ	$\approx \varphi(\tau)$
$(169862, 2019, 6)$	$\frac{\sqrt{-327}-2019}{339724}$	$0.970181534584... + 0.406208134780...i$
$(339724, 2019, 3)$	$\frac{\sqrt{-327}-2019}{679448}$	$0.849773113022... - 1.48265683802...i$
$(509586, 2019, 2)$	$\frac{\sqrt{-327}-2019}{1019172}$	$0.849773113023... + 1.48265683803...i$
$(679448, 681467, 170873)$	$\frac{\sqrt{-327}-681467}{1358896}$	$-1.09610353086... + 0.434878106545...i$
$(1019172, 2019, 1)$	$\frac{\sqrt{-327}-2019}{2038344}$	$0.970181534228... - 0.406208134590...i$
$(1189034, 1700639, 608093)$	$\frac{\sqrt{-327}-1700639}{2378068}$	$2.72107335869... + 0.940911270411...i$
$(1358896, 2040363, 765894)$	$\frac{\sqrt{-327}-2040363}{2717792}$	$0.602123038432... + 0.687526987751...i$
$(1868482, 3399259, 1546036)$	$\frac{\sqrt{-327}-3399259}{3736964}$	$0.404037632964... + 1.44424276131...i$
$(2038344, 2040363, 510596)$	$\frac{\sqrt{-327}-2040363}{4076688}$	$-1.11162239378... + 0.424870695321...i$
$(2378068, 4078707, 1748883)$	$\frac{\sqrt{-327}-4078707}{4756136}$	$-0.309688979078... + 0.196557136776...i$
$(3567102, 4078707, 1165922)$	$\frac{\sqrt{-327}-4078707}{7134204}$	$-1.64937813999... + 1.14796507415...i$

Summing the last column gives

$$z_{2019} \approx 1.51530061234467421072689 + 6.53036974554911187723558...i$$

Which under Φ maps to the point (given as an approximation as the actual height of the point is more than 50,000)

$$\Phi(z_{2019}) \approx (224420.76106432775576446..., -20767447.521321148901535..., 1)$$

Ranging over u, we obtain the relevant point

$$\bar{z}_{2019} \approx 0.00160833384531783394267873506580427684144895118679603 3...$$

Which using Φ and continued fractions gives the numerator of the x-coordinate of the generator as

240054507144997007130114738055349271937302280494307429461295927475132
098062593060368553213237943056588684360058918855245626373349819540388 4
247586894501016717396831

and denominator

587816173710576592312252140523912865842173625028142055203331783133133 10
507808004995120899224023193398285606884710833710673722165248359430854 9
5483585006716961.

5.3.4 An Even Larger Example

In this section, we compute a generator for the curve

$$E : y^2 + xy = x^3 - x^2 - 36502495762x - 2684284892271276$$

of conductor $N = 137935$. Using the Gross-Zagier theorem we compute the height to be $\approx 801916.7242...+$. Using the BSD, we have the Heegner index as $l = 24$. We conclude a generator has height $\approx 1392.2165+$. We choose $D = -1531$ for which $h(D) = 11$, and $\beta = 15313$. We compute the points with approximately 700 digits of accuracy, requiring 1.7 million terms of the L-series.

(A, B, C)	τ	$\approx \varphi(\tau)$
$(137935, 15313, 425)$	$\frac{\sqrt{-1531}-15313}{275870}$	$2.5240523... - 0.80324413...i$
$(689675, 15313, 85)$	$\frac{\sqrt{-1531}-15313}{1379350}$	$1.0906444... + 1.3449735...i$
$(965545, 1118793, 324091)$	$\frac{\sqrt{-1531}-1118793}{1931090}$	$1.1152957... + 1.2461843...i$
$(1517285, 567053, 52981)$	$\frac{\sqrt{-1531}-567053}{3034570}$	$-4.4162473... - 0.49225933...i$
$(1517285, 1946403, 624221)$	$\frac{\sqrt{-1531}-1946403}{3034570}$	$0.28553233... + 3.1838307...i$
$(1793155, 291183, 11821)$	$\frac{\sqrt{-1531}-291183}{3586310}$	$2.3013780... - 3.6751200...i$
$(1793155, 1946403, 528187)$	$\frac{\sqrt{-1531}-1946403}{3586310}$	$1.0039738... - 2.1025912...i$
$(2344895, 15313, 25)$	$\frac{\sqrt{-1531}-15313}{4689790}$	$1.7303887... + 2.4623977...i$
$(2344895, 2774013, 820415)$	$\frac{\sqrt{-1531}-2774013}{4689790}$	$-1.0292041... + 0.18691389...i$
$(8138165, 8567283, 2254757)$	$\frac{\sqrt{-1531}-8567283}{16276330}$	$0.94786611... - 0.062477747...i$
$(10896865, 842923, 16301)$	$\frac{\sqrt{-1531}-842923}{21793730}$	$3.5690822... - 3.8393057...i$

Summing the number in the last column gives us

$$z_{15313} = 9.122729003720080215832543... - 2.550652302665054658941520 4...i$$

which maps the the point on the curve (as a decimal approximation as $\hat{h}(\Phi(z_{15313})) > 800,000!$)

$$(7897488.40710718011799693319..., -22065108231.4885475723339747..., 1).$$

Ranging over u, we obtain the relevant point

$$\bar{z}_{15313} = 0.00216493469614259853994544411592625108230863582766152054709 67...$$

which we map to $E(\mathbb{Q})$ by the map Φ and reconstruct using continued fractions. We obtain the x-coordinate of the generator with numerator

926732779916808207853907239936293284403077981388267042294515784199515485024347441090498377489975500630043239183351325324555319173463009575582514563893463026447343079363571234866290588589093582551362843392922157791697531090761590572546904022030611514134046815181221970260153996013143927777512480932728400021115238046789688927937723666428374399736863129092864620821699949482654263659184625787305817119345001824991364060196849718323569920675272099597907720725127822512950697987452162632576182006093265291760364313103946949420952723303531552450723405298078632271568630468855467466722868343438542987603143264614 1

and denominator

187206254480810022395006081856056994282369451768882476896558085096146465791779125968746896394501536834547126961018199932102614318214006727325785414164145898567506966543556159966280793780756097059378748093069274196419137237900142332844921488735770230487885197854728703241537527567537507910860246949153150085609879713257789968012151313669022229882992311810140461770635464559397191313722600374237096602130759635105943407762039058590034038075331990908476403368211356983649543584998914089444436467984319815408384590921997677318504245993733977905342944473340838427103004564519167427929508265670990789764964.

Bibliography

[1] B. J. Birch. Elliptic curves and modular functions. In *Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69)*, pages 27–32. Academic Press, London, 1970.

[2] B. J. Birch. Heegner points of elliptic curves. In *Symposia Mathematica, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973)*, pages 441–445. Academic Press, London, 1975.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[4] Bryan Birch. Heegner points: the beginnings. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 1–10. Cambridge Univ. Press, Cambridge, 2004.

[5] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[6] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[7] Henri Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[8] B. Gross, W. Kohnen, and D. Zagier. Heegner points and derivatives of L-series. II. *Math. Ann.*, 278(1-4):497–562, 1987.

[9] Kurt Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[10] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[11] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[12] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[13] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Number 46 in Princeton Math. Series. Princeton Univ. Press, Princeton, NJ, 1998.

[14] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[15] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[16] Joseph H. Silverman. Computing rational points on rank 1 elliptic curves via L-series and canonical heights. *Math. Comp.*, 68(226):835–858, 1999.

[17] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[18] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[19] Nelson Stephens. Computation of rational points on elliptic curves using Heegner points. In *Number theory and applications (Banff, AB, 1988)*, volume 265 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 205–214. Kluwer Acad. Publ., Dordrecht, 1989.

[20] Yutaka Taniyama. Jacobian varieties and number fields. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, pages 31–45, Tokyo, 1956. Science Council of Japan.

[21] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[22] Mark Watkins. Some remarks on heegner point computations. 0:1–11, 2005.

[23] E. T. Whittaker and G. N. Watson. *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions: with an account of the principal transcendental functions.* Fourth edition. Reprinted. Cambridge University Press, New York, 1962.

[24] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.