University of Alberta

Heegner Points, Hilbert's Twelfth Problem, and the Birch and Swinnerton-Dyer Conjecture

by

Jordan Kostiuk

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements for the degree of

Master of Science

in

Mathematics

Department of Mathematics and Statistical Sciences

Fall 2013

Edmonton, Alberta

Abstract

Heegner points on modular curves play a key role in the solution of Hilbert's twelfth problem for quadratic imaginary fields, as well as the proof of the Birch and Swinnerton-Dyer conjecture for the case $\mathrm{ord}_{s=1} L(E,s) \leq 1$. The relationship between Heegner points and Hilbert's twelfth is classically described by the j-function; we supply evidence that suggests that this relationship is one that transcends the j-function and should be able to be recast in terms of other suitable modular functions. The proof of the Birch and Swinnerton-Dyer conjecture for the case $\mathrm{ord}_{s=1} L(E,s) \leq 1$ is examined and made concrete by using sage to illustrate, very explicitly, the role played by the Heegner points. Both of these results suggest a deep connection between geometry and arithmetic that we hope to see in other contexts.

Contents

Introduction

Two of the most intriguing conjectures in number theory are Hilbert's twelfth problem and the Birch and Swinnerton-Dyer conjecture. The former asks whether or not it is possible to explicitly construct abelian extensions of number fields, using special values of analytic functions say, while the former postulates that their is a deep connection between the arithmetic properties of an elliptic E, and the analytic properties of its L-function.

While little is known about Hilbert's twelfth in a general setting, it is known to hold for $\mathbf{Q}$, as well as for quadratic imaginary extensions of $\mathbf{Q}$. The solution over $\mathbf{Q}$ is the contents of the Kronecker-Weber theorem, which states that every abelian extension of $\mathbf{Q}$ is contained in some cyclotomic extension $\mathbf{Q}(\zeta)$. Alternatively, we may think of generating abelian extensions of $\mathbf{Q}$ by adjoining special values of the analytic function $e^{2\pi iz}$, namely, the values at rational arguments. For quadratic imaginary fields K, we are able to generate (most of) its abelian extensions by evaluating modular functions at special points in the upper-half plane. The first two sections of this thesis are devoted to developing and illustrating enough of the general theory to explain this result in detail.

Once we describe the basic preliminary theory, we introduce a very interesting set of points, the Heegner points, lying on the modular curves $X_0(N)$. We will see that the solution to Hilbert's twelfth problem for quadratic imaginary fields can be recast as a statement about Heegner points and certain modular functions. The value in this is the following: the classical solution to Hilbert's twelfth problem is a statement about Heegner points on $X_0(1)$ and the modular function j. On the other hand, the Heegner points are available to us on all of the curves $X_0(N)$. Some of these curves admit an analogue of the j-function, and we are then able to give convincing evidence that the same statements that hold for Heegner points on $X_0(1)$ and j hold for their counterparts.

The remaining section of the thesis is devoted to describing some important theorems involving Heegner points that have allowed us to make progress on the Birch and Swinnerton-Dyer conjecture. To do this, we will first describe how we can obtain points on an elliptic curve from the Heegner points on the modular curves $X_0(N)$. Theorems of Gross, Zagier, and Kolyvagin, then tell us that these points enjoy many nice properties that will allow for a proof of a version of the Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbf{Q}$ whose L-functions vanish at $s = 1$ to an order of 0 or 1.

Throughout the thesis, emphasis will be placed on making the theory discussed as explicit as possible. This will be accomplished by performing computations using the algebra experimentation software, sage. We will see that sage can be used as an illustrative tool, demonstrating some of the known theory, as well as a tool for experimentation. This gives a concreteness to the subject that was not readily available a few decades ago. In turn, this helps with the exposition of known material, as well as the discovery of new results.

1. Modular Form Theory

1.1. **Basic Definitions.** In this section, we recall some of the general theory of modular forms. For an easy to understand introduction to the subject, the reader is referred to [5].

Consider the group $\mathrm{SL}_2(\mathbf{Z})$ of integer matrices with determinant 1. This group acts on the complex upper half-plane, $\mathcal{H}$, by Möbius transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

Note that we have $\mathrm{im}(\gamma\tau) = |c\tau + d|^{-2}\mathrm{im}(\tau)$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, from which we see that $\gamma\tau \in \mathcal{H}$ whenever $\tau \in \mathcal{H}$. It is easy to check that $\gamma_1(\gamma_2(\tau)) = (\gamma_1\gamma_2)(\tau)$, and so we do indeed have an action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathcal{H}$.

We now define certain subgroups of $\mathrm{SL}_2(\mathbf{Z})$ that play a key role in the theory, especially where arithmetic is concerned.

Definition 1.1.1. The principal congruence subgroup of level N is denoted by $\Gamma(N)$ and is defined to be the kernel of the reduction map

$$\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}).$$

A congruence subgroup of level N is a subgroup of $\mathrm{SL}_2(\mathbf{Z})$ that contains $\Gamma(N)$ with finite index. Of particular importance are the subgroups $\Gamma_0(N)$, defined as

$$\Gamma_0(N) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \colon c \equiv 0 \bmod N\}$$

All of these groups, being subgroups of the group $\mathrm{SL}_2(\mathbf{Z})$, are discrete subgroups that act on the upper half-plane. The orbit space for such a subgroup, $\Gamma\backslash\mathcal{H}$, can be given a complex structure that makes the resulting object a non-compact Riemann surface, which is denoted by $Y(\Gamma)$. If $\Gamma = \Gamma(N)$, resp. $\Gamma_0(N)$, the curve is typically denoted $Y(N)$, resp. $Y_0(N)$. The theory of compact Riemann surfaces is easier to work with, so we compactify our Riemann surface by adding finitely many points, called cusps, to be defined below.

The extended upper-half plane is denoted by $\mathcal{H}^*$ and is the union of the usual upper half-plane $\mathcal{H}$ with the rational numbers in the real-axis and a point at infinity. That is, $\mathcal{H}^* = \mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$. The action of $\mathrm{SL}_2(\mathbf{Z})$ extends naturally to the extended upper half-plane, by setting

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (x \colon y) := (ax + by \colon cx + dy)$$

Note that if x, y are co-prime, then we can find integers a, b such that $ax + by = 1$. In this case, the matrix $\gamma = \left(\begin{smallmatrix} a & y \\ -b & x \end{smallmatrix}\right)$ satisfies

$$\gamma(0 \colon 1) = (y \colon x)$$

It follows that we can send the point ∞ to any other point. That is, the action of $\mathrm{SL}_2(\mathbf{Z})$ on the set $\mathbf{P}^1(\mathbf{Q})$ is transitive. Therefore, if we take Γ to be a congruence subgroup, then the set of orbits under Γ of $\mathbf{P}^1(\mathbf{Q})$ will be finite.

Just as before, the orbit space $\Gamma\backslash\mathcal{H}^*$ can be made into a Riemann surface, but this time the resulting object is compact. These curves will be denoted by $X(\Gamma)$ and, just like above, we will often write $X(N)$ and $X_0(N)$ in the case where Γ is either $\Gamma(N)$ or $\Gamma_0(N)$ respectively. Note that $Y(\Gamma) \subseteq X(\Gamma)$ and that the set-difference is the set of orbits of $\mathbf{P}^1(\mathbf{Q})$. This finite set of points is called the set of cusps for $X(\Gamma)$.

We can now define the notion of a modular form:

Definition 1.1.2. We define the weight k-operator on the set of functions $\mathcal{H} \to \mathbf{C}$ via the formula

$$(f[\gamma]_k)(\tau) := (c\tau + d)^{-k} f(\gamma(\tau)),$$

where (c, d) is the bottom row of γ. A modular form of weight k for a congruence subgroup Γ is then a function that is holomorphic on $\mathcal{H}$, satisfies $f[\gamma]_k = f$ for $\gamma \in \Gamma$ and is holomorphic at the cusps. This means the following: first, Γ contains $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ for some minimal positive h. It follows that f has a fourier expansion in the variable $q^{\frac{1}{h}}$ where $q = e^{2\pi i\tau}$. We say f is holomorphic at ∞ if this fourier expansion is holomorphic at 0, as a function of q. If we take another cusp c, we can write it as $c = \alpha(\infty)$ for some $\alpha \in \mathrm{SL}_2(\mathbf{Z})$. The function $f[\alpha]_k$ is then holomorphic in $\mathcal{H}$ and invariant under $\alpha^{-1}\Gamma\alpha$, another congruence subgroup. We say that f is holomorphic at c if $f[\alpha]_k$ is holomorphic at ∞.

The modular forms which vanish at ∞ are referred to as cusp forms. The space of all modular forms of weight k for Γ is denoted by $M_k(\Gamma)$ and the space of all cusp forms is denoted by $S_k(\Gamma)$.

Of particular importance is the space $S_2(\Gamma)$, the space of weight 2 cusp-forms. In this case, if we assign to the modular form f, the differential form on $X(\Gamma)$, $\omega_f := 2\pi i f(\tau)d\tau$, we obtain an identification with the space of weight 2 cusp-forms and the space of holomorphic differentials on the compact Riemann surface $X(\Gamma)$. In particular, the Riemann-Roch theorem then tells us that this space is finite dimensional, and in fact has dimension equal to the genus of the curve $X(\Gamma)$.

Because the emphasis of this paper is on concreteness, we will not say anything in more generality than is necessary. Thus, in what follows, we will often restrict to modular forms of weight 2 for the subgroups $\Gamma_0(N)$. Most of the general theory will be illustrated below in this case and the interested reader is, again, referred to [5] for a more proper introduction.

1.2. **Hecke Operators.** Let $M_2(N)$ denote the space of modular forms for $\Gamma_0(N)$ and let $S_2(N)$ denote the space of cusp-forms sitting inside. As mentioned above, has dimension equal to the genus of the curve $X_0(N)$. We wish to find a suitable basis for this space with which to work and, for this reason, we define the notion of a Hecke operator:

Definition 1.2.1. We define the p-th Hecke operator on $S_2(N)$ as

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

We define the n-th Hecke operator by imposing that the formal identity

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

holds.

In particular, if $p \nmid N$, then the following identity holds:

$$T_{p^r} = T_p T_{p^{r-1}} - p T_{p^{r-2}}$$

The action of these operators on the fourier coefficients is given by

$$T_p(f) = \begin{cases} \sum_{p|n} a_n q^{n/p} + p \sum a_n q^{pn} & \text{if } p \nmid N \\ \sum_{p|n} a_n q^{n/p} & \text{if } p|N \end{cases}$$

One checks easily that the Hecke-operators T_p and T_ℓ commute for primes p and ℓ and so we see that in fact,all the Hecke operators commute with each other. One also checks that these operators take cusp forms of weight k and level N to forms of the same type, so we do indeed have operators on the space $S_2(N)$.

It is apparent by the above formula that $a_1(T_p f) = a_p(f)$, where $a_n(f)$ is the n-th fourier coefficient. In the case that f is an eigenvector, say $T_p = \lambda f$, if follows that $a_1(f)\lambda = a_p(f)$. Therefore, if we assume that f is normalized to satisfy $a_1(f) = 1$, the eigenvalue of the p-th Hecke operator corresponding to f is simply the p-th coefficient $a_p(f)$. Because of this nice description of the eigenvalues of a Hecke operator in terms of the fourier coefficients of the corresponding normalized eigenform, together with the fact that we have a family of commuting linear operators on the space $S_2(N)$, one might hope that, by linear algebra, we can find a basis for $S_2(N)$ consisting of simultaneous eigenvectors for all of the Hecke operators. This is indeed almost the case.

Let $\mathbf{T}$ denote the commutative sub-algebra of $\mathrm{End}(S_2(N))$ generated by all of the Hecke operators and let let $\mathbf{T}^0$ denote the sub-algebra of $\mathbf{T}$ generated by the Hecke operators indexed by numbers that are co-prime to the level N. These are in fact finitely generated subalgebras with $\mathbf{T}$ having rank g. These sub-algebras give us a nice decomposition of our space $S_2(N)$, as described below. But first, let us mention that $S_2(N)$ comes equipped with an inner-product, called the Peterson product. The details of this product are not important to us at the moment. What is important are the following facts.

First, the operators in $\mathbf{T}^0$ are self-adjoint with respect to this inner-product. Therefore, linear algebra gives us for free that $S_2(N)$ decomposes as an orthogonal sum of eigenspaces

$$S_2(N) = \bigoplus S^0_\lambda,$$

where the sum is over all homomorphisms $\lambda\colon \mathbf{T}^0 \to \mathbf{C}$ and S^0_λ is the λ-eigenspace. That is, $f \in S^0_\lambda$ iff $T_n f = \lambda(T_n) f$ for all n co-prime to N. These eigenspaces need not be

one dimensional. However, the eigenspaces corresponding to the larger algebra are one-dimensional. Indeed, if f is an eigenfunction, then $a_n(f) = a_1(f)\lambda(T_n)$, so it is unique up to a scalar multiple.

We are not lucky enough to always have a decomposition of $S_2(N)$ into one-dimensional eigenspaces. What we do have is a canonical sub-space that does have such a decomposition. To be precise, a cusp-form $f \in S_2(N)$ is called an old-form if it is a linear combination of cusp-forms of the form $g(d'\tau)$ where d' is a divisor of d, which is in turn a divisor of N and $g \in S_2(N/d)$. The space of new-forms is defined to be the orthogonal complement to this space. Then, we have the following decomposition of the space of cusp-forms

$$S_2(N) = S_2(N)_{old} \bigoplus_{\lambda} \mathbf{C} f_\lambda,$$

where $f_\lambda = \sum \lambda(T_n) q^n$. That is, the new space has a decomposition into the sum the one-dimensional eigenspaces. Note that since many of our examples will take place at the prime level, we should note that since the prime p has no non-trivial divisors, we don't have an old subspace to worry about. In this case, $S_2(p)$ has a decomposition into one-dimensional eigenspaces. One last property to note about the Hecke operators which has arithmetic importance, is the fact that the eigenvalues will always be algebraic integers.

We also remark that since the newforms are eigenfunctions for all of the hecke operators, our earlier observations tell us that the fourier coefficients are given by the formula $a_n(f) = a_1(T_n(f))$. Because the Hecke operators obey certain identities, the same will be true of the coefficients of a newform. For example, we have the identity $a_n a_m = a_{nm}$ whenever n and m are co-prime. We also know that, for $p \nmid N$, we have $a_{p^r} = a_p a_{p^{r-1}} - p a_{p^{r-2}}$

Sage has spaces of modular forms and Hecke operators already built in and ready to go for us:

First, we are able to construct the spaces of modular forms and cusp-forms we are working with.

```
sage: M=ModularForms(11,2)

sage: M

Modular Forms space of dimension 2 for Congruence Subgroup Gamma0(11) of weight
2 over Rational Field

sage: M.basis()

[q - 2*q^2 - q^3 + 2*q^4 + q^5 + O(q^6),

1 + 12/5*q + 36/5*q^2 + 48/5*q^3 + 84/5*q^4 + 72/5*q^5 + O(q^6)]
```

```
sage: C=CuspForms(11,2)

sage: C

Cuspidal subspace of dimension 1 of Modular Forms space of dimension 2 for Congruence
Subgroup Gamma0(11) of weight 2 over Rational Field

sage: C.basis()
```

$[q - 2*q^2 - q^3 + 2*q^4 + q^5 + O(q^6)]$

```
sage: C.newforms()
```

$[q - 2*q^2 - q^3 + 2*q^4 + q^5 + O(q^6)]$

Since the space of modular forms at this level was 2-dimensional, we expected that the cuspidal space would be one-dimensional. We can also construct the Hecke operators and have a look at their characteristic polynomials. In this case, since the cuspidal space is one-dimensional, we expect linear polynomials of course. Note though that the coefficients are integers.

```
sage: T7=C.hecke_operator(7)

sage: T7.domain()

Cuspidal subspace of dimension 1 of Modular Forms space of dimension 2 for Congruence
Subgroup Gamma0(11) of weight 2 over Rational Field

sage: T7.charpoly()
```

$x + 2$

```
sage: g=C.basis()[0]

sage: T7(g)
```

$-2*q + 4*q^2 + 2*q^3 - 4*q^4 - 2*q^5 + O(q^6)$

If we now switch the level to 23, we find that the cuspidal space is 2-dimensional, so the theory discussed above becomes a little more relevant.

```
sage: C23=CuspForms(23,2)

sage: C23
```

```
Cuspidal subspace of dimension 2 of Modular Forms space of dimension 3 for Congruence
Subgroup Gamma0(23) of weight 2 over Rational Field
```

```
sage: C23.basis()
```

$[q - q^3 - q^4 + O(q^6), q^2 - 2*q^3 - q^4 + 2*q^5 + O(q^6)]$

Note that the basis sage gives us is not the basis of newforms that we know we are entitled to. Sage can give us this basis if we ask for the newforms. Since the coefficients of the newforms at this level are not all integers, we must specify a name for the elements adjoined to $\mathbf{Q}$ to obtain the coefficients.

```
sage: C23.newforms("a")
```

$[q + a0*q^2 + (-2*a0 - 1)*q^3 + (-a0 - 1)*q^4 + 2*a0*q^5 + O(q^6)]$

```
sage: f=C23.newforms("a")[0]
```

```
sage: a=f.coefficients([2])[0]
```

```
sage: a.parent()
```

Number Field in a0 with defining polynomial $x^2 + x - 1$

Note that although it looks like Sage has given us a single newform, we are to interpret this as being two newforms, one for each choice of embedding of $a0$ into $\mathbf{C}$, and there are two choices. We can verify that the hecke operator T_2 indeed has characteristic polynomial as claimed

```
sage: T2=C23.hecke_operator(2)
```

```
sage: T2.charpoly()
```

$x^2 + x - 1$

More than this, if we ask Sage to compute the 6-th fourier coefficient of f, we can construct the number field given above and verify that the coefficients satisfy the relations that we expect of them.

```
sage: K.<a>=NumberField(x^2 + x - 1)
```

```
sage: f.coefficients(9)
```

$[1, a, -2*a - 1, -a - 1, 2*a, a - 2, 2*a + 2, -2*a - 1, 2]$

Now we will check that the coefficients satisfy $a_2a_3 = a_6$, $a_4 = a_2^2 - 2$, $a_8 = a_2a_4 - 2a_2$, $a_9 = a_3^2 - 3$.

```
sage:  a*(-2*a-1), a^2-2, a*(-a-1)-2*a, (-2*a-1)^2-3
```

```
(a - 2, -a - 1, -2*a - 1, 2)
```

Lastly, let us compute the first 10 characteristic polynomials for the Hecke operators and verify that they do indeed have integer coefficients:

```
sage:  print [C23.hecke_operator(i).charpoly() for i in range(1,11)]
```

```
[x^2 - 2*x + 1, x^2 + x - 1, x^2 - 5, x^2 + x - 1, x^2 + 2*x - 4,
x^2 + 5*x + 5, x^2 - 2*x - 4, x^2 - 5, x^2 - 4*x + 4, x^2 - 6*x + 4]
```

1.3. **Modular Curves as Moduli Spaces.** One of the reasons that we study the quotients of $\mathcal{H}$ by certain subgroups of $\mathrm{SL}_2(\mathbf{Z})$ is by interpreting these spaces as moduli spaces for elliptic curves. First, let us begin by considering the quotient of $\mathcal{H}$ by the full modular group, $\mathrm{SL}_2(\mathbf{Z})$.

Recall that an elliptic curve over the complex numbers is a compact Riemann surface of genus one. Equivalent, it is a smooth cubic curve in $\mathbf{P}^2(\mathbf{C})$, and we may always assume the equation for this curve is given by the Weierstrass normal form

$$y^2 = 4x^3 - g_2x - g_3,$$

for some constants $g_2, g_3 \in \mathbf{C}$.

Yet another description of an elliptic curve is as a complex torus. This goes as follows: let $\Lambda \subseteq \mathbf{C}$ be a $\mathbf{Z}$-lattice. That is, a free rank 2 abelian group sitting inside $\mathbf{C}$. Let $\wp_\Lambda(z)$ denote the Weierstrass $\wp$ function given by

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

This a doubly-periodic meromorphic function with poles of order 2 at each lattice point and no poles anywhere else. It's derivative is given by

$$\wp'_\Lambda(z) = -\frac{1}{z^3} - \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{(z-\lambda)^3}$$

One finds that the Laurent expansion of the $\wp$-function is given by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2(n+1)}(\Lambda) z^{2n},$$

where, for $n \geq 3$, we define

$$G_n(\Lambda) := \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{\lambda^n}.$$

The G_n are called the Eisenstein series of weight n.

From this, one easily shows by a direct computation that $\wp$ satisfies the following differential equation

$$(\wp'_\Lambda(z))^2 = 4\wp_\Lambda(z)^3 - G_4\wp_\Lambda(z) - G_6$$

The cubic on the right hand side is in fact non-singular. That is, the discriminant $\Delta(\Lambda) := G_4(\Lambda)^3 - 27G_6(\Lambda)^2$ is non-zero. It follows that the map $z \mapsto (\wp(z), \wp'(z))$ gives a map from $\mathbf{C}/\Lambda$ to the elliptic curve defined by the equation

$$y^2 = 4x^3 - g_2x - g_3,$$

where $g_2 = G_4$ and $g_3 = G_6$. This map is actually an analytic group-isomorphism. The inverse map is given by considering path integrals of the canonical invariant differential on the elliptic curve. For more details, the interested reader is referred to [1][Ch. VI].

The take-home message is that elliptic curves are the same as quotients of $\mathbf{C}$ by a lattice. How much freedom do have in our choice of lattice? That is, when will Λ and Λ' give us the same elliptic curve? Well, it is not too hard to see using covering-space theory that $\mathbf{C}/\Lambda$ will be isomorphic to $\mathbf{C}/\Lambda'$ precisely when the lattices are homothetic. That is, when $\Lambda = \alpha\Lambda'$ for some $\alpha \in \mathbf{C}^\times$. This means that we should consider lattices only up to homothety. Choosing an oriented basis ω_1, ω_2 for our lattice, we may assume that $\frac{\omega_2}{\omega_1}$ lies in $\mathcal{H}$ and thus assume that our lattice is of the form $\Lambda_\tau := \mathbf{Z} \oplus \tau\mathbf{Z}$ for some $\tau \in \mathcal{H}$. Choosing such normalized lattices isn't quite good enough however, because Λ_τ could very well be equal to Λ'_τ for some $\tau' \in \mathcal{H}$. In fact, this will happen precisely when we can write $\tau' = \frac{a\tau+b}{c\tau+d}$ for some $a, b, c, d \in \mathbf{Z}$ satisfying $ad - bdc = 1$. That is, $\Lambda_\tau = \Lambda'_\tau$ exactly when

$$\tau' = \gamma\tau, \ \gamma \in \mathrm{SL}_2(\mathbf{Z}).$$

These observations combine to give us the following fact:

Proposition 1.3.1. *Let S denote the set of all elliptic curves, up to isomorphism. There is a bijection between $\mathrm{SL}_2(\mathbf{Z})/\mathcal{H}$ and S give by the mapping*

$$\tau \mapsto \mathbf{C}/\Lambda_\tau$$

In this way, we may view this quotient of the upper half-plane as a moduli space. As mentioned earlier, our main focus is actually on the subgroup $\Gamma_0(N)$. Can we similarly interpret this quotient as a moduli space? The answer is yes, once we endow the elliptic curves we are considering with more structure. To be precise, let $S_0(N)$ denote the set of pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of order N, where we consider two pairs (E, C) and (E', C') equivalent if there is an isomorphism between E and E' that takes C onto C'. What kind of canonical representative should we work with? Well, we should first of all assume that E is of the form $\mathbf{C}/\Lambda_\tau$ for some $\tau \in \mathcal{H}$. Our cyclic subgroup is then generated by some point $Q = \frac{c\tau+d}{N}$ for some integers c, d. In fact,

$\gcd(c,d,N)=1$ since Q must be a point of order N. But then we can find $a,b,k\in\mathbf{Z}$ such that $ad-bc-kN=1$, and so the matrix $\gamma=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ reduces into $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$. Since we can change the entries of γ modulo N without affecting Q, and since $\mathrm{SL}_2(\mathbf{Z})$ surjects onto $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$, we may assume $\gamma\in\mathrm{SL}_2(\mathbf{Z})$. Now let $\tau'=\gamma\tau$ and $m=c\tau+d$. Then, one checks that $m\Lambda_{\tau'}=\Lambda_\tau$ and that $m/N=Q$, from which it follows that our pair is isomorphic to a pair of the form $(\mathbf{C}/\Lambda_\tau,\langle 1/N\rangle)$. Lastly, with some work, one can show that two such normalized pairs $(\mathbf{C}/\Lambda_\tau,\langle 1/N\rangle)$ and $(\mathbf{C}/\Lambda'_\tau,\langle 1/N\rangle)$ will be isomorphic precisely when τ and τ' lie in the same $\Gamma_0(N)$-orbit. This shows

Proposition 1.3.2. *There is bijection between the quotient $\Gamma_0(N)\backslash\mathcal{H}$ and $S_0(N)$.*

There is one more way in which to view this moduli space that is sometimes useful to consider. Recall that an isogeny between elliptic curves is a non-constant algebraic map (so finite-to-one). Such maps are necessarily surjective. We list some important facts about isogenies which can be found in [1][Ch. III].

- An isogeny is completely determined by its kernel. That is, if we have isogenies $\phi_1\colon E\to E_1$, and $\phi_2\colon E\to E_2$, with $\ker\phi_1=\ker\phi_2$, then there is an isomorphism $E_1\to E_2$.
- Given a finite subgroup of E, there is an elliptic E' and an isogeny $E\to E'$ with kernel equal to our given subgroup.

Using these notions, we may view the moduli space $S_0(N)$ as the set of diagrams $(\phi\colon E\to E')$ where ϕ is an isogeny with cyclic kernel of order N and where we take the elliptic curves up to isomorphism. In this description, the pair $(\mathbf{C}/\Lambda_\tau,\langle 1/N\rangle)$ corresponds to the pair $(\mathbf{C}/\Lambda_\tau\to\mathbf{C}/\frac{1}{N}\mathbf{Z}+\tau\mathbf{Z})$, (map induced by identity on $\mathbf{C}$) which is the same as $(\mathbf{C}/\Lambda_\tau,\mathbf{C}/\Lambda_{N\tau})$.

1.4. **Some Important Modular Functions.** We will now discuss some important modular forms that play a key role in the theory of elliptic curves. Recall the Weierstrass $\wp$-function discussed above. Its Laurent expansion was given in terms of the Eisenstien series

$$G_n(\Lambda):=\sum_{\lambda\in\Lambda-\{0\}}\frac{1}{\lambda^n}.$$

If we normalize our lattice to Λ_τ, we may then consider the function

$$G_n(\tau):=\sum_{(a,b)\in\mathbf{Z}^2-\{0\}}\frac{1}{(a+b\tau)^n},$$

as a function on $\mathcal{H}$. Clearly, $G_n(\tau)$ is invariant under $\tau\mapsto\tau+1$ and we check that

$$G_n(\frac{-1}{\tau})=\sum\frac{1}{(a-\frac{b}{\tau})^n}=\tau^n\sum\frac{1}{(a\tau-b)^n}=\tau^nG_n(\tau),$$

from which it follows that $G_n(\tau)$ is actually a modular form of weight n for $\mathrm{SL}_2(\mathbf{Z})$ (the transformations $\tau\mapsto\tau+1$ and $\tau\mapsto-\frac{1}{\tau}$ generate $\mathrm{SL}_2(\mathbf{Z})$). Here we must assume that that $n>2$ to ensure that we have absolute convergence of the series above. The Eisenstein series generate the space of all modular forms in the following sense: the space of all modular forms

is a graded $\mathbf{C}$-algebra where the k-th graded pieces is the space of modular forms of weight k. This space is isomorphic to $\mathbf{C}[G_4, G_6]$. For the details, see [5][Ch.III]

Another important modular form that is found in the theory is given by the modular discriminant Δ. Recall that the discriminant of the cubic equation coming from the $\wp$-function was, up to a multiple of 2^8, given by

$$\Delta(\Lambda) = G_4(\Lambda)^3 - 27G_6(\Lambda)^2.$$

Normalizing our lattice to one of the form Λ_τ, and using the fact that we know G_4 and G_6 are modular forms, we see at once that $\Delta(\tau) := \Delta(\Lambda_\tau)$ is a modular form of weight 12. In fact, one can show that Δ is a cusp form. Even more importantly, we interpret $\Delta(\tau)$ as the discriminant of the elliptic curve with lattice Λ_τ, so that Δ is non-vanishing on $\mathcal{H}$.

With these modular forms at our disposal, we now define one of the most important modular functions with which we will work. Consider the function

$$j(\tau) := 1728\frac{G_4(\tau)^3}{\Delta(\tau)}.$$

Since we know that G_4 is a modular form of weight 4 and Δ is a modular form of weight 12, this function is a modular form of weight 0; that is, a well-defined $\mathbf{C}$-valued function on the quotient $\mathrm{SL}_2(\mathbf{Z})\backslash\mathcal{H}$, or a modular function. In fact, since Δ is a cusp-form, j will have a pole at ∞ and no other poles since Δ is holomorphic everywhere and non-vanishing on $\mathcal{H}$. Moreover, one can show easily that $G_4(\omega) = 0$ where $\omega = e^{\frac{2\pi i}{3}}$. With a little more work, it is possible to show that these zeroes and poles are in fact simple. From this, we conclude that j gives us a non-constant degree one map from $\mathrm{SL}_2(\mathbf{Z})\backslash\mathcal{H} \to \mathbf{P}^1(\mathbf{C})$, which must then be an isomorphism.

There are two important reasons for studying the j-function; the first being its applications to the theory of elliptic curves. We just saw that the j-function gives us a bijective map to the Riemann-sphere. In particular, we have a bijective map $\mathrm{SL}_2(\mathbf{Z})\backslash\mathcal{H}^* \to \mathbf{C}$. On the other-hand, the quotient on the left describes the moduli space for elliptic curves up to isomorphism. It follows that if we define the j-invariant of an elliptic curve $\mathbf{C}/\Lambda_\tau$ to be $j(\tau)$, then this j-invariant is enough to describe an elliptic curve up to isomorphism. Moreover, there exists an elliptic curve with a given j-invariant. The second reason for studying the j-function is the fact that *all* modular functions for $\mathrm{SL}_2(\mathbf{Z})$ are generated by it. That is, the set of meromorphic functions on $\mathrm{SL}_2(\mathbf{Z})/\mathcal{H}$ is isomorphic to $\mathbf{C}(j)$. Moreover, we can actually use this function to generate all the modular functions for $\Gamma_0(N)$. Since j is a modular function for $\mathrm{SL}_2(\mathbf{Z})$, one can check easily that $j_N(\tau) := j(N\tau)$ is a modular function for $\Gamma_0(N)$. It is then a fact that the space of meromorphic functions on $X_0(N)$ is isomorphic to $\mathbf{C}(j, j_N)$ [5][Ch.III].

Being such important functions, sage can compute the the q-expansions of all the functions discussed above.

```
sage:  j_invariant_qexp(5)
```

$$\mathtt{q^{-}1 + 744 + 196884 * q + 21493760 * q^2 + 864299970 * q^3 + 20245856256 * q^4 + O(q^5)}$$

```
sage: delta_qexp(5)
```

$$q - 24*q^2 + 252*q^3 - 1472*q^4 + O(q^5)$$

```
sage: eisenstein_series_qexp(4,5,normalization="constant")
```

$$1 + 240*q + 2160*q^2 + 6720*q^3 + 17520*q^4 + O(q^5)$$

```
sage: eisenstein_series_qexp(6,5,normalization="constant")
```

$$1 - 504*q - 16632*q^2 - 122976*q^3 - 532728*q^4 + O(q^5)$$

Note that sage returns the Eisenstein series suitably normalized; here, we were returned the series scaled so that the constant term is equal to 1.

With the basics of modular forms discussed, we now move onto the theory of elliptic curves with complex multiplication.

2. Complex Multiplication And Algebraic j-Values

2.1. **Basic Theory of Complex Multiplication.** It is well known that for an elliptic curve E over a number field (or more generally, a field of characteristic zero), the endomorphism ring is either isomorphic to $\mathbf{Z}$ or an order $\mathcal{O}$ in a quadratic imaginary field K. Recall that an order $\mathcal{O}$ in a number field F is a subring of $\mathcal{O}_F$ that is a free $\mathbf{Z}$-module of the same rank as $\mathcal{O}_F$. When $F = K$ is a quadratic field, there is a simple way of describing these subrings by their conductor. Namely, if we write $\mathcal{O}_K = \mathbf{Z}[\tau]$ for some $\tau \in K$, then every order of K is of the form $\mathbf{Z}[c\tau]$ for some integer $c \in \mathbf{Z}$ called the conductor of $\mathcal{O}$. We will often write $\mathcal{O}_c$ to denote the order of conductor c.

Elliptic curves with the larger endomorphism rings are said to have complex multiplication by $\mathcal{O}$, or by K if it is understood that $\mathcal{O}$ is the ring of integers of K, the maximal order. In the case that E is given to us a quotient of $\mathbf{C}$ by the lattice $\Lambda = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2$, this amounts to saying that $\frac{\omega_2}{\omega_1} \in K$ for some quadratic imaginary field K. Indeed, it is well-known that the endomorphism ring of $\mathbf{C}/\Lambda$ is given to us by

$$\mathrm{End}(\mathbf{C}/\Lambda) = \{\alpha \in \mathbf{C} \colon \alpha\Lambda \subseteq \Lambda\}$$

Now, by modifying by a homothety, we may assume that $\omega_1 = 1$, and that $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$ for some τ. If $\alpha \in \mathrm{End}(\mathbf{C}/\Lambda)$, then we see that we may pick integers a, b, c, d such that

$$\alpha = a + b\tau,\ \alpha\tau = c + d\tau.$$

It follows that $\tau = \frac{\alpha - a}{b}$, which we substitute into the second equation to find

$$\alpha\frac{\alpha - a}{b} = c + d\frac{\alpha - a}{b},$$

from which we find, after simplifying,

$$\alpha^2 - (a+d)\alpha + ad - bc = 0,$$

whence α is integral over $\mathbf{Z}$. If $\mathrm{End}(\mathbf{C}/\Lambda)$ is strictly larger than $\mathbf{Z}$, then we can find such an α that is not integer, so that α must in fact generate a quadratic extension of $\mathbf{Q}$. Since α clearly generates the same extension as τ, this is equivalent to the fact that $\mathbf{Q}(\tau)$ is quadratic imaginary as desired. Note that this field must be imaginary because $\tau \notin \mathbf{R}$.

We now consider two basic examples of elliptic curves that possess complex-multiplication.

Example 2.1.1. Let $E = \mathbf{C}/\mathbf{Z}[i]$. Then, clearly $\{\alpha \in \mathbf{C} \colon \alpha\mathbf{Z}[i] = \mathbf{Z}[i]\} = \mathbf{Z}[i]$, so E has complex multiplication by $\mathbf{Z}[i]$. In fact, we note that $i\mathbf{Z}[i] = \mathbf{Z}[i]$, from which it follows that

$$G_6(\mathbf{Z}[i]) = G_6(i\mathbf{Z}[i]) = i^6 G_6(\mathbf{Z}[i]) = -G_6(\mathbf{Z}[i]);$$

that is, $G_6(\mathbf{Z}[i]) = 0$. It follows that this curve is given by the equation

$$y^2 = 4x^3 - G_4(\mathbf{Z}[i])x,$$

from which we find that the j-invariant of this curve is equal to 1728.

Example 2.1.2. Completely analogously, let $\rho = e^{\frac{2\pi i}{6}}$. Then $C/\mathbf{Z}[\rho]$ has complex multiplication by $\mathbf{Z}[\rho]$. Since $\rho\mathbf{Z}[\rho] = \mathbf{Z}[\rho]$, we find that

$$G_4(\mathbf{Z}[\rho]) = \rho^4 G_4(\mathbf{Z}[\rho]),$$

from which it follows that $G_4(\rho) = 0$ and that this elliptic curve is given by the equation $y^2 = 4x^3 - G_6(\mathbf{Z}[\rho])$, and this curve has j-invariant 0.

These two elliptic curves are isomorphic to $y^2 = x^3 - x$ and $y^2 = x^3 + 1$ respectively, so that they have models over $\mathbf{Q}$. Later on, we will explain how to find all elliptic curves that are defined over $\mathbf{Q}$ possessing complex multiplication.

Before giving the above example, we saw that every elliptic curve that possesses complex multiplication is isomorphic to $\mathbf{C}/\Lambda_\tau$ where $\tau \in K$ for some quadratic imaginary field. That is, $\Lambda_\tau \subseteq K$, and if we let $\mathcal{O} \subseteq K$ be the order by which E has complex multiplication, we see that Λ_τ is in fact an $\mathcal{O}$-submodule of K such that there is some $\lambda \in K^\times$ such that $\lambda\Lambda \subseteq \mathcal{O}$. It can in fact be shown [3][Ch. V] that Λ is invertible under multiplication of such submodules, so that Λ in fact lies in the group of invertible fractional $\mathcal{O}$-ideals of K. Conversely, if we start with such a module $\mathcal{O}$, and view $K \subseteq \mathbf{C}$, then $\mathbf{C}/\Lambda$ will have complex multiplication by $\mathcal{O}$. That is, we can construct an elliptic curve that has complex multiplication by $\mathcal{O}$ as soon as we are given $\mathcal{O}$.

By working with elliptic curves over $\mathbf{C}$, it is clear what it means for $\alpha \in K$ to be an endomorphism of $\mathbf{C}/\Lambda$; it is is simply the map induced by multiplication by α on $\mathbf{C}$. On the other hand, it is not so clear what we mean by "multiplication by α" if we do not use this lattice description. Alternatively, there may be more than one way to view the order $\mathcal{O}$ as isomorphic to $\mathrm{End}(E)$, so we now wish to describe a natural way to pin this down. To this end, let E be an elliptic curve defined over some subfield of $\mathbf{C}$. Let $f \colon \mathbf{C}/\Lambda \to E$ be the Weierstrass parameterization of E. Then, we define $[\alpha] \in \mathrm{End}(E)$ to be the map that fits

into the following commutative diagram:

$$\begin{array}{ccc} \mathbf{C}/\Lambda & \xrightarrow{\alpha} & \mathbf{C}/\Lambda \\ \downarrow f & & \downarrow f \\ E & \xrightarrow{[\alpha]} & E \end{array}$$

This map is uniquely determined by the property that $[\alpha]^*\omega = \alpha\omega$, where ω is the canonical invariant differential on E. When we are working with an elliptic curve over a number field, this is what we have in mind when we are identifying $\mathcal{O}$ with $\mathrm{End}(E)$.

Let us now fix a quadratic imaginary field K and an order $\mathcal{O}$ sitting inside it. We will now describe the set $Ell(\mathcal{O})$, the set consisting of $\mathbf{C}$-isomorphism classes of elliptic curves that have complex multiplication by $\mathcal{O}$. Since we just saw that all such elliptic curves are isomorphic to $\mathbf{C}/\mathfrak{a}$ for some fractional ideal $\mathfrak{a}$, and we know that $\mathbf{C}/\Lambda_1 \cong \mathbf{C}/\Lambda_2$ iff there is some $\lambda \in \mathbf{C}$ such that $\Lambda_1 = \lambda\Lambda_2$, we conclude that there is a bijection between $Ell(\mathcal{O})$ and the group of fractional-ideals modulo multiplication by $K^\times$. That is, $Ell(\mathcal{O})$ is in bijection with the Picard group of $\mathcal{O}$, which is denoted by $\mathrm{Pic}(\mathcal{O})$.

More than just being in bijection with the Picard group, $Ell(\mathcal{O})$ actually admits an action by this group. Indeed, let $\mathbf{C}/\mathfrak{a}$ be an element in $Ell(\mathcal{O})$ and let $\mathfrak{b} \in \mathrm{Pic}(\mathcal{O})$. Then, $\mathfrak{b}^{-1}\mathfrak{a}$ is another fractional $\mathcal{O}$-ideal and $\mathbf{C}/\mathfrak{b}^{-1}\mathfrak{a}$ depends only on the equivalence class of $\mathfrak{b} \in \mathrm{Pic}(\mathcal{O})$. We thus define

$$[\mathfrak{b}] * [\mathbf{C}/\mathfrak{a}] := [\mathbf{C}/\mathfrak{b}^{-1}\mathfrak{a}]$$

This clearly defines an action on $Ell(\mathcal{O})$ and we will see a little later why the inverse is used here. More than just being some action however, this action is actually a simply transitive one. Indeed, consider $\mathbf{C}/\mathfrak{a}$ and $\mathbf{C}/\mathfrak{b}$. Then $\mathfrak{a}\mathfrak{b}^{-1}$ sends $\mathbf{C}/\mathfrak{a}$ to $\mathbf{C}/\mathfrak{b}$. More, if $[\mathfrak{c}] * [\mathbf{C}/\mathfrak{a}] = [\mathbf{C}/\mathfrak{b}]$, then $\mathfrak{c}^{-1}\mathfrak{a}$ is homothetic to $\mathfrak{b}$, whence $[\mathfrak{c}] = [\mathfrak{a}][\mathfrak{b}]^{-1}$, from which simple transitivity follows.

While it didn't take much work to construct the bijection given above, there is a very interesting corollary to be had.

Proposition 2.1.3. *Let E be an elliptic with complex multiplication. Then $j(E)$ is algebraic. Equivalently, suppose that τ is a quadratic surd lying in the upper-half plane. Then $j(\tau)$ is algebraic where j is the modular function defined earlier.*

Proof. Let $\sigma\colon \mathbf{C} \to \mathbf{C}$ be an automorphism. Note that $j(E^\sigma) = j(E)^\sigma$ and that $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$. That is, E^σ also has complex multiplication by $\mathcal{O}$. But then E^σ must belong to the finite set of all such curves and thus, the values $j(E)^\sigma$ as σ runs through all automorphisms must also belong to a finite set. That is, $j(E)$ is algebraic.

In fact, $j(E)$ is an algebraic integer, a fact that will be touched upon a little later. $\square$

The fact that $j(\tau)$ takes on algebraic values when τ is a quadratic imaginary surd cannot be overstated. The j function is defined as a rational function of Eisenstein series, functions that clearly cannot be expected to preserve any amount of algebraicity. More than this, the degree 2 case is unique! If $\tau \in \mathcal{H}$ is algebraic of degree at least 3, then we know that $j(\tau)$ must be transcendental [7][Theorem 17]. We can actually say a lot more about the algebraic properties of $j(\tau)$.

2.2. **Extensions Generated by j.** If E is an elliptic curve with complex multiplication, then $j(E)$ is more than just some random algebraic number, as we will now see. Let G_K denote the absolute Galois group of K. Since $j(E)$ is algebraic, E is defined over $\overline{\mathbf{Q}}$, so it makes sense to let G_K act on the set $Ell(\mathcal{O})$ by sending setting E^σ to be the elliptic curve obtained by letting σ act on the coefficients of E. Since E^σ will also have complex multiplication by $\mathcal{O}$, this action is well-defined. We now fix some $E \in Ell(\mathcal{O})$. Since the action of $\mathrm{Pic}(\mathcal{O})$ is simply transitive, there is a uniquely defined $\eta_K(\sigma) \in \mathrm{Pic}(\mathcal{O})$ such that

$$E^\sigma = \eta_K(\sigma) * E.$$

This defines a homomorphism from G_K to $\mathrm{Pic}(\mathcal{O})$ that is, in fact, independent of the base curve E that we fixed upfront. Indeed, first we note that the action of G_K on $Ell(\mathcal{O})$ commutes with the action of $\mathrm{Pic}(\mathcal{O})$ on this set. The best way to see this is by noting that we have

$$[\mathfrak{a}] * [E] = [E/E[\mathfrak{a}]],$$

where $E[\mathfrak{a}]$ is the $\mathfrak{a}$-torsion. Then,

$$([\mathfrak{a}] * [E])^\sigma = [(E/E[\mathfrak{a}])^\sigma] = [E^\sigma/E^\sigma[\mathfrak{a}^\sigma]] = [\mathfrak{a}^\sigma] * E^\sigma = [\mathfrak{a}] * E^\sigma,$$

where we observe that σ fixes K, and hence fixes $\mathfrak{a}$.

Next, suppose that $E_1 = \mathfrak{a} * E$ is another choice of base curve and let $\eta_1 \colon G_K \to \mathrm{Pic}(\mathcal{O})$ be the associated homomorphism. Then on one hand, we have

$$[E_1^\sigma] = \eta_1(\sigma) * [E_1],$$

while on the other hand,

$$[E_1^\sigma] = [(\mathfrak{a} * E)^\sigma] = [\mathfrak{a} * \eta_K(\sigma) * E] = [\eta_K(\sigma) * E_1],$$

since $\mathrm{Pic}(\mathcal{O})$ is abelian. It follows that $\eta_K(\sigma) = \eta_1(\sigma)$, whence the result.

So, now we have a homomorphism $\eta_K \colon G_K \to \mathrm{Pic}(\mathcal{O})$. Let $H := \overline{K}^{\ker \eta}$, so that H is an abelian extension of K with Galois group isomorphic to a sub-group of $\mathrm{Pic}(\mathcal{O})$. In fact, η is a surjection, as we will see shortly, so that the Galois group of H/K is in fact isomorphic to $\mathrm{Pic}(\mathcal{O})$. This is not just some random isomorphism, but one that the reader might be familiar with in the context of class field theory.

Theorem 2.2.1. *Let c be the conductor of $\mathcal{O}$. Then H as defined above is the ring class field of conductor c. That is, H_c is unramified outside of the primes dividing c and its Galois group over K is identified with $\mathrm{Pic}(\mathcal{O})$ via the Artin map. In fact, $\eta_K(\sigma_\mathfrak{p}) = [\mathfrak{p}]$ for all primes not dividing c, where $\sigma_\mathfrak{p}$ denotes the Frobenius automorphism at $\mathfrak{p}$.*

In particular, if $\mathcal{O}$ is the maximal order, then H is the Hilbert class field of K and we have

$$\eta_K((\mathfrak{a}, H/K)) = [\mathfrak{a}]$$

Proof. Following [4][Ch.III] , it suffices to show that for almost all primes $\mathfrak{p}$ that do not divide c, we have

$$\eta_K(\sigma_\mathfrak{p}) = [\mathfrak{p}]$$

Let Σ denote the set of primes in K which satisfy the following conditions

- $\mathfrak{p}$ is unramified in H/K;
- E has good reduction at all primes in H above $\mathfrak{p}$;
- The prime $\mathfrak{p}$ does not divide the norm of $j(E_i) - j(E_k)$ for all $i \neq k$ where E_i are the finitely many elliptic curves with complex multiplication by $\mathcal{O}$;
- If p is the prime of $\mathbf{Z}$ lying under $\mathfrak{p}$, then p ramifies or splits in $K/\mathbf{Q}$.

This set of primes has Dirichlet density one, and so $\mathrm{Gal}(H/K)$ is generated by the frobenius elements attached to such primes, so we will prove that $\eta_K(\sigma_\mathfrak{p}) = [\mathfrak{p}]$ for $\mathfrak{p} \in \Sigma$. To this end, fix a prime $\mathfrak{p}'$ lying above $\mathfrak{p}$ and let $\overline{E}$ denote the reduction of E at $\mathfrak{p}'$. Note that $\overline{E^{\sigma_\mathfrak{p}}} = \overline{E}^{(p)}$, the curve obtained by applying the p-th power frobenius morphism to $\overline{E}$.

On the other hand, consider the map $E \to E/E[\mathfrak{p}]$. One can show without much work that $E[\mathfrak{p}]$ is a free $\mathcal{O}/\mathfrak{p}$-module of rank one, and so the map has degree equal to $p = N_\mathbf{Q}^K(\mathfrak{p})$. On the other hand, I claim that the induced map $\overline{E} \to \overline{E}/\overline{E}[\mathfrak{p}]$ is purely inseparable of degree p. Quite generally, one can show that the induced map will always have the same degree, so we show that the map is inseparable.

To this end, we choose some ideal $\mathfrak{a}$, co-prime to $\mathfrak{p}$ such that $\mathfrak{a}\mathfrak{p}$ is principal, say equal to (α). Pick a minimal Weierstrass model for E and let ω be the invariant differential so that $\overline{\omega}$ is the invariant differential on the reduced curve. If we consider the composite upstairs

$$E \to E/E[\mathfrak{p}] \to E/E[\mathfrak{a}\mathfrak{p}] = E/E[(\alpha)] \cong E,$$

then the pull-back of the differential ω is simply $\alpha\omega$. Therefore, the effect of the pull-back on $\overline{\omega}$ is sending it to $\overline{\alpha\omega}$. But since $(\alpha) = \mathfrak{p}\mathfrak{a}$, we see that $\overline{\alpha} = 0$, so that the pull-back of this differential is zero under this map. It follows that the induced map of the composite above is inseparable. But the map $E/E[\mathfrak{p}] \to E/E[\mathfrak{a}\mathfrak{p}]$ has degree prime to p and the isomorphism has degree one. It follows that the map $\overline{E} \to \overline{E}/\overline{E}[\mathfrak{p}]$ must be inseparable. Since this map has degree p, it follows that $\overline{E}/\overline{E}[\mathfrak{p}]$ must be isomorphic to $\overline{E}^{(p)}$ by [1][Ch.III].

That is, modulo $\mathfrak{p}'$, we find that $\overline{E^{\sigma_\mathfrak{p}}} = \overline{E}/\overline{E}[\mathfrak{p}]$. But we know that the j-invariants of the curves in $Ell(\mathcal{O})$ are all distinct mod $\mathfrak{p}$! It follows that we must actually have

$$E^{\sigma_\mathfrak{p}} \cong [\mathfrak{p}] * E,$$

from which the result now follows. □

Note that

$$\begin{aligned}\ker \eta_K &= \{\sigma \in G_K \colon \eta_K(\sigma) * E = E\} \\ &= \{\sigma \in G_K \colon j(E)^\sigma = j(E)\}\end{aligned}$$

from which it follows that $H^{\ker \eta_K} = K(j(E))$. Ironing out the rest of the details, we obtain the following more complete theorem that can be found in [3][Ch. V].

Theorem 2.2.2. *Let $\mathcal{O}$ be an order in K and let $\mathfrak{a}$ be a fractional ideal. Then the following hold:*

(i) $\mathrm{Gal}(K(j(\mathfrak{a}))/K)$ *is isomorphic to* $Pic(\mathcal{O})$ *through the correspondence* $\sigma \mapsto \mathfrak{b}$ *such that* $j(\mathfrak{a})^\sigma = j(\mathfrak{b}^{-1}\mathfrak{a})$.
(ii) $[K(j(\mathfrak{a})) \colon K] = [\mathbf{Q}(j(\mathfrak{a})) \colon \mathbf{Q}]$.
(iii) If $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *are representatives for* $\mathrm{Pic}(\mathcal{O})$*, then* $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_n)$ *form a complete set of conjugates of* $j(\mathfrak{a})$ *over* $\mathbf{Q}$*, and over* K.

2.3. **Numerical Examples.** Let us now illustrate the above theory with some examples that sage can help us with.

Example 2.3.1. It is well-known that there are only finitely quadratic imaginary fields with class number one, namely the quadratic imaginary fields whose discriminant D belongs to $\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$. From this, it immediately follows from Theorem 2.2.2 that there are only finitely many elliptic curves defined over $\mathbf{Q}$ that possess complex multiplication by K for some quadratic imaginary field K. With just a little more work, we will show that there are, in fact, only finitely many elliptic curves over $\mathbf{Q}$ that possess complex multiplication (by an arbitrary order) and, using sage, we will easily exhibit models for all of these curves after computing their j-invariants.

To begin, let us fix a quadratic imaginary field K with maximal order $\mathcal{O}_K$. It is of importance in this example, as well as later on in the paper, that we have an adequate description of $\mathrm{Pic}(\mathcal{O})$ where $\mathcal{O}$ is another order in K. For this, we have a natural exact sequence whose description is spelled out in [6][Ch.II].

$$1 \longrightarrow \mathcal{O}_c^\times \longrightarrow \mathcal{O}_K^\times \longrightarrow \frac{(\mathcal{O}_K/c)^\times}{(\mathcal{O}_c/c)^\times} \longrightarrow \mathrm{Pic}(\mathcal{O}_c) \longrightarrow \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 1$$

From this, we obtain the short exact sequence

$$1 \longrightarrow \frac{(\mathcal{O}_K/c)^\times}{\mathcal{O}_K^\times(\mathbf{Z}/c\mathbf{Z})^\times} \longrightarrow \mathrm{Pic}(\mathcal{O}_c) \longrightarrow \mathrm{Pic}(\mathcal{O}) \longrightarrow 1$$

In particular, $\mathrm{Pic}(\mathcal{O}_c)$ is trivial if and only if both $\mathrm{Pic}(\mathcal{O})$ and

$$A_c := \frac{(\mathcal{O}_K/c)^\times}{\mathcal{O}_K^\times(\mathbf{Z}/c\mathbf{Z})^\times}$$

are trivial.

So, by Theorem 2.2.2, it follows that the elliptic curves defined over $\mathbf{Q}$ possessing complex multiplication are the curves corresponding the orders in quadratic imaginary fields whose discriminant is one of those listed above and such that A_c is trivial. We now work this out in detail.

We begin by observing that we have natural surjections from A_c to A_p whenever $p|c$. It follows that if A_c is trivial, then so must all of the A_p. In the case where $\mathcal{O}_K^\times = \{\pm 1\}$, the chinese remainder theorem actually tells us the more powerful fact that A_c is isomorphic the product of all the $A_{p_p^{v}(c)}$ for $p|c$. No matter what the unit group looks like, we do have the following description of A_p:

$$A_p \cong \begin{cases} \mathbf{F}_{p^2}^\times / \mathcal{O}_K^\times \mathbf{F}_p^\times & \text{if } p \text{ is inert in } K \\ (\mathbf{Z}/p^2\mathbf{Z})^\times / \mathcal{O}_K^\times \mathbf{F}_p^\times & \text{if } p \text{ is ramified in } K \\ \mathbf{F}_p^\times \times \mathbf{F}_p^\times / \mathcal{O}_K^\times \mathbf{F}_p^\times & \text{if } p \text{ splits in } K \end{cases}$$

First, we deal with the two exceptional cases where $D \in \{-3, -4\}$; these cases correspond to when K has unit group larger than $\{\pm 1\}$.

The Case $D = -4$. This corresponds to $K = \mathbf{Q}(i)$ and $\mathcal{O}_K = \mathbf{Z}[i]$. In this case, we know that $\mathcal{O}_K = \langle i \rangle$. The only prime that ramifies in this extension is 2. In this case, by our description above, we find that A_2 is trivial. Next, we note that $i \in \mathbf{F}_p^\times$ if and only if p splits in K. Therefore, if p is inert, we find

$$|A_p| = |\mathbf{F}_{p^2}^\times / \langle i \rangle \mathbf{F}_p^\times| = \frac{p^2 - 1}{2(p-1)} > 1,$$

so A_p is non-trivial. Similarly, if p is split, we find

$$|A_p| = |\mathbf{F}_p^\times \times \mathbf{F}_p^\times / \mathbf{F}_p^\times| = p - 1 > 1,$$

so A_p is non-trivial in this case as well. It follows that A_c is trivial only if c is a power of 2.

Let us now consider the group A_4. It is easy to verify that there are 8 units in $\mathcal{O}_K/4$, so we find that $|A_4| = \frac{\varphi(2^4)}{2 \cdot \varphi(2^2)} = \frac{8}{2 \cdot 2} = 2$. But then we see that A_{2^n} is non-trivial for all $n \geq 2$.

In conclusion, the only orders in $K = \mathbf{Q}(i)$ that have trivial picard group are the maximal one and the one of conductor 2.

The Case $D = -3$. This corresponds to $K = \mathbf{Q}(\omega)$ where ω is a third root of unit. Here, we have $\mathcal{O}_K^\times = \langle \omega \rangle$. The ramified prime is 3 and $\omega \notin \mathbf{F}_3^\times$, so we find that

$$|A_3| = \frac{\varphi(3^2)}{3 \cdot \varphi(3)} = \frac{6}{6} = 1,$$

so A_3 is trivial.

As before, if p is unramified, then $\omega \in \mathbf{F}_p^\times$ if and only if p is split in K. It follows that if p is inert, then

$$|A_p| = \frac{p^2-1}{3(p-1)},$$

which is always greater than 1 unless $p = 2$ (note that 2 is indeed inert).

Similarly, if p is split,

$$|A_p| = p - 1 > 1,$$

so that we conclude that A_p is trivial only if $p = 2, 3$. One can check by hand that all of the groups A_4, A_6, A_9 are non-trivial, so our conclusion is that the only orders in $K = \mathbf{Q}(\omega)$ that have trivial picard group are the maximal order and the orders of conductor 2 and 3.

The Case $D \in \{-7, -8, -11, -19, -43, -67, -163\}$. This time, the unit group is just $\{\pm 1\}$ which contributes nothing to the group A_p. Note also that A_c is the product of $A_{p^{v_p(c)}}$ for $p|c$ so there is a little less checking to do; namely, we just need to know when A_{p^n} vanishes.

This time we know that

$$A_p \cong \begin{cases} \mathbf{F}_{p^2}^\times/\mathbf{F}_p^\times & \text{if } p \text{ is inert in } K \\ (\mathbf{Z}/p^2\mathbf{Z})^\times/\mathbf{F}_p^\times & \text{if } p \text{ is ramified in } K \\ \mathbf{F}_p^\times \times \mathbf{F}_p^\times/\mathbf{F}_p^\times & \text{if } p \text{ splits in } K \end{cases}$$

from which it follows that the only way this group is trivial is when $p = 2$ and p splits in K. A quick calculation with Legendre symbols shows that this only happens when $D = -7$. In this case, one checks that A_4 is non-trivial and so we conclude that the only orders in $\mathbf{Q}(\sqrt{D})$ that have trivial picard group are the maximal orders and the order of conductor 2 when $D = -7$.

So, we have just shown that there are finitely many elliptic curves that are defined over $\mathbf{Q}$ that possess complex multiplication by some order of a quadratic imaginary field. Let us now find models for these elliptic curves and calculate their j-invariants.

To compute the j-invariants, we just choose τ such that $\mathcal{O} = \mathbf{Z}[\tau]$ and compute to some high precision $j(\tau)$ using sage. Since we know that $j(\tau)$ must be an integer by Theorem 2.2.2, it is easy to obtain the exact value.

We have already seen that the j-invariants corresponding to $\mathbf{Z}[i]$ and $\mathbf{Z}[\omega]$ are 1728 and 0 respectively. The following sage script will compute the q-expansion of the j-function to twenty terms, and compute $j(\tau)$ to a high precision. Then, to neaten things up, it will find the nearest integer and factor it for us.

```
sage:  def j(tau):
```

$$\texttt{A} = \texttt{j\_invariant\_qexp}(20).\texttt{truncate}(20).\texttt{subs}(\texttt{q} = \texttt{e}^{(}2 * \texttt{pi} * \texttt{I} * \texttt{tau})).\texttt{n}(200)$$

```
    B = A.real_part().nearby_rational(max_denominator = 1)+
    A.imag_part().nearby_rational(max_denominator = 1)
    returnB.factor()
```

Let us first find the j-invariant associated to the order in $\mathbf{Q}(i)$:

```
sage:  j(I)
```

$2^6 * 3^3$

```
sage:  j(2*I)
```

$2^3 * 3^3 * 11^3$

Now let us find the invariants associated to the orders in $\mathbf{Q}(\omega)$:

```
sage:  j((1+sqrt(-3))/2)
```

0

```
sage:  j(2*(1+sqrt(-3))/2)
```

$2^4 * 3^3 * 5^3$

```
sage:  j(3*(1+sqrt(-3))/2)
```

$-1 * 2^{15} * 3 * 5^3$

Next, let us work with $\mathbf{Q}(\sqrt{-7})$:

```
sage:  j((1+sqrt(-7))/2)
```

$-1 * 3^3 * 5^3$

```
sage:  j(2*(1+sqrt(-7))/2)
```

$3^3 * 5^3 * 17^3$

Above were all the fields that admitted more than one elliptic curve with complex multiplication. The other j-invariants can be found in table 1 below.

Now that we have the j-invariants associated to the elliptic curves, sage can give us a model over $\mathbf{Q}$ for each curve. We will ask it to give us a Weierstrass model:

```
sage:  def E(j):
    return EllipticCurve(j = j).integral_short_weierstrass_model()
sage : E(2^6 * 3^3)
Elliptic Curve defined by y^2 = x^3 - x  over Rational Field
sage : E(2^3 * 3^3 * 11^3)
Elliptic Curve defined by y^2 = x^3 - 11 * x - 14 over Rational Field
sage : E(0)
Elliptic Curve defined by y^2 = x^3 + 16  over Rational Field
sage : E(2^4 * 3^3 * 5^3)
Elliptic Curve defined by y^2 = x^3 - 15 * x + 22  over Rational Field
sage : E(-2^15 * 3 * 5^3)
Elliptic Curve defined by y^2 = x^3 - 480 * x + 4048  over Rational Field
sage : E(-1 * 3^3 * 5^3)
Elliptic Curve defined by y^2 = x^3 - 35 * x - 98  over Rational Field
sage : E(3^3 * 5^3 * 17^3)
Elliptic Curve defined by y^2 = x^3 - 595 * x - 5586  over Rational Field
```

Lastly, sage can double check for us that these elliptic curves do indeed have complex multiplication. Let us verify this for the elliptic curve coming from the order of conductor 2 in $\mathbf{Q}(\sqrt{-7})$:

```
sage : E = EllipticCurve(j = 3^3 * 5^3 * 17^3)
sage : E.has_cm()
True
sage : E.cm_discriminant()
-28
```

This last calculation tells that E, defined as above, has complex multiplication by the order of discriminant -28, which is the same as the order of conductor 2 in $\mathbf{Q}(\sqrt{-7})$, as we expected. We now give a table that summarizes the results of all of these calculations.

TABLE 1. Elliptic Curves over $\mathbf{Q}$ with Complex Multiplication

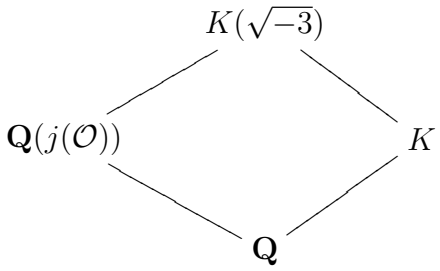
Discriminant of K	Conductor of $\mathcal{O}$	j-invariant of $\mathbf{C}/\mathcal{O}$	Weierstrass Equation
-3	1	0	$y^2 = x^3 + 16$
	2	$2^4 \cdot 3^3 \cdot 5^3$	$y^2 = x^3 - 15x + 22$
	3	$-2^{15} \cdot 3 \cdot 5^3$	$y^2 = x^3 - 480x + 4048$
-4	1	$2^6 3^3$	$y^2 = x^3 - x$
	2	$2^3 3^3 11^3$	$y^2 = x^3 - 11x - 14$
-7	1	$-3^3 5^3$	$y^2 = x^3 - 35x - 98$
	2	$3^3 5^3 17^3$	$y^2 = x^3 - 595x - 5586$
-11	1	-2^{15}	$y^2 = x^3 - 9504x + 365904$
-19	1	$-2^{15} 3^3$	$y^2 = x^3 - 608x + 5776$
-43	1	$-2^{18} 3^3 5^3$	$y^2 = x^3 - 13760x + 621264$
-67	1	$-2^{15} 3^3 5^3 11^3$	$y^2 = x^3 - 117920x + 15585808$
-163	1	$-2^{18} 3^3 5^3 23^3 29^3$	$y^2 = x^3 - 34790720x + 78984748304$

Example 2.3.2. As a second example of the general theory, let's verify numerically that we can use special j-values to generate Hilbert Class-fields.

First, let's take a quadratic example. Let $K = \mathbf{Q}(\sqrt{-5})$. Then, sage can tell us everything we need to about the Hilbert class field.

```
sage : K. < a >= NumberField(x^2 + 15)

sage : K.class_group()

Class group of order 2 with structure C2 of Number Field in a with defining
polynomial x^2 + 15

sage : K.class_group().gens()

[Fractionalidealclass(2, 1/2 * a + 1/2)]

sage : K.hilbert_class_field_defining_polynomial()

x^2 - x + 1
```

So, we know that the Hilbert Class field as a quadratic extension of K and is in fact equal to $K(\sqrt{-3})$. On the other hand, we know that $j(\mathcal{O}_K)$ generates an extension of $\mathbf{Q}$ that sits in the lattice of fields as



Next, note how complex conjugation acts on $j(\mathcal{O})$:

$$\overline{j(\mathcal{O})} = j(\overline{\mathcal{O}}) = j(\mathcal{O}),$$

from which it follows that $\mathbf{Q}(j(\mathcal{O})$ must, in fact, be a real subfield. It follows that in fact $j(\mathcal{O}) \in \mathbf{Q}(\sqrt{5})$. Note that $K(\sqrt{5}) = K(\sqrt{-3})$. We now compute $j(\mathcal{O})$ and its conjugate as an element of H explicitly.

We begin by writing

$$\begin{aligned} j(\mathcal{O}) &= A + B\sqrt{5} \\ j(\mathfrak{a}) &= A - B\sqrt{5} \end{aligned}$$

where $\mathfrak{a}$ is the non-trivial class in $\mathrm{Pic}(\mathcal{O})$, and $A, B \in \mathbf{Q}$. This allows us to easily solve for A and B, namely

$$\begin{aligned} A &= \frac{j(\mathcal{O}) + j(\mathfrak{a})}{2} \\ B &= \frac{j(\mathcal{O}) - j(\mathfrak{a})}{2\sqrt{5}} \end{aligned}$$

We can now compute A and B to a high precision in sage. Note that since these are algebraic integers, we have

$$j(\mathcal{O}) = (A - B) + 2B\frac{1+\sqrt{5}}{2},$$

with $A - B$ and $2B$ integers.

We now compute:

$\mathtt{sage} : \mathtt{A} = (\mathtt{j}(1/2 * (1 + \mathtt{sqrt}(-15))) + \mathtt{j}(1/4 * (1 + \mathtt{sqrt}(-15))))/2$

$\mathtt{sage} : \mathtt{B} = (\mathtt{j}(1/2 * (1 + \mathtt{sqrt}(-15))) - \mathtt{j}(1/4 * (1 + \mathtt{sqrt}(-15))))/(2 * \mathtt{sqrt}(5).\mathtt{n}(100))$

$\mathtt{sage} : \mathtt{A} - \mathtt{B}$

$-52515.000000000000000000000000 - 1.736595329765758697307189495 1\mathtt{e} - 32 * \mathtt{I}$

$\mathtt{sage} : 2 * \mathtt{B}$

$-85995.000000000000000000000000 + 1.073274938499570844749933861 8\mathtt{e} - 32 * \mathtt{I}$

and since we know that the above numbers must be integers, we conclude that

$$j(\mathcal{O}) = -52515 - 85995\frac{1+\sqrt{5}}{2}.$$

In particular, we can see at once that $K(j(\mathcal{O})) = H$.

Note that the significance of Theorem 2.2.2 is not that we can compute Hilbert class fields by using modular forms in practice, but that the class fields of quadratic imaginary fields are generated in a natural way by the values of a single modular function. It is a statement about the elegance and simplicity of the theory behind the situation, not a computational tool.

For a more complicated example, let us now work out the above example when K has class-group of order 3, namely $K = (\mathbf{Q}(\sqrt{-23})$.

$\mathtt{sage} : \mathtt{K}. < \mathtt{a} >= \mathtt{NumberField}(\mathtt{x}^2 + 23)$

```
sage : K.class_group()

Class group of order 3 with structure C3 of Number Field in a with defining
polynomial x^2 + 23
```

Here, we expect a cubic extension. Since the ring of integers is generated by $\alpha = \frac{1+\sqrt{-23}}{2}$, we compute $j(\alpha)$, and then see if it satifies a polynomial of degree 3:

```
sage:  a=j((1+sqrt(-23))/2)

sage:  p=a.algdep(3)

sage:  p

x^3 + 3491750 * x^2 - 5151296875 * x + 12771880859375
```

We then compute the relative extension and check that it is unramified:

```
sage:  R.<t>=K[]

sage:  L.<b>=K.extension(p.subs(x=t))

sage:  L.relative_discriminant()

Fraction Ideal (1)
```

So, we have again generated the Hilbert class-field, as predicted by theorem 2.2.2.

Having covered the basics of complex multiplication, we will introduce a very special collection of points on $X_0(N)$ in the next section.

3. Heegner Points

3.1. **Heegner Points on $X_0(N)$.** In this section, we describe a special class of points on the modular curve $X_0(N)$ called Heegner points. We will use the definitions and notations found in Gross' article [8]. Recall that the non-cuspidal points of $X_0(N)$ can be identified by pairs of elliptic curves connected by an isogeny with cyclic kernel.

Definition 3.1.1. A *Heegner point* on $X_0(N)$ is a point of the form $(\varphi\colon E_1 \to E_2)$ where E_1 and E_2 both have complex multiplication by the same order $\mathcal{O}$ in a quadratic imaginary field K. If c denotes the conductor of the order $\mathcal{O}$, we say that $(\varphi\colon E_1 \to E_2)$ is a Heegner point of conductor c for K.

For what follows, let the quadratic imaginary field K be fixed. Given a Heegner point $(\varphi\colon E_1 \to E_2)$, with order $\mathcal{O} \subseteq K$, we may assume, by the previous section, that $E_1 = \mathbf{C}/\mathfrak{a}$,

$E_2 = \mathbf{C}/\mathfrak{b}$ for fractional ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ and that φ is induced by the identity on $\mathbf{C}$; i.e., that $\mathfrak{a} \subseteq \mathfrak{b}$. In this case, $\mathfrak{n} := \mathfrak{a}\mathfrak{b}^{-1}$ is an ideal in $\mathcal{O}$ and $\ker \varphi = \mathfrak{b}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{n}$. That is, $\mathfrak{n}$ is an ideal of $\mathcal{O}$ with cyclic quotient of order N.

Conversely, suppose we are given an order $\mathcal{O}$, a fractional ideal $\mathfrak{a}$ and an ideal $\mathfrak{n}$ such that $\mathcal{O}/\mathfrak{n}$ is cyclic of order N. Then $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{n}^{-1}$, so that the identity map on $\mathbf{C}$ induces an isogeny $\varphi\colon \mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1}$ with kernel given by

$$\ker \varphi = \mathfrak{a}\mathfrak{n}^{-1}/\mathfrak{a} \cong \mathcal{O}/\mathfrak{n},$$

which is cyclic of order $\mathfrak{n}$. In this way, we have constructed a Heegner point for $\mathcal{O}$. Note that this construction depends only on the class of $\mathfrak{a}$ in the Picard group of $\mathcal{O}$.

The upshot is that a Heegner point is completely determined by giving an order $\mathcal{O}$ in a quadratic imaginary field K, a class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ and an ideal $\mathfrak{n} \subseteq \mathcal{O}$ having cyclic quotient of order N. We denote the Heegner point on $X_0(N)$ associated to this set of data by

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]).$$

Yet another description of Heenger points is given by their coordinates in the upper-half plane. If we start with the Heegner point $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ we may assume, after picking oriented bases for $\mathfrak{n}$ and $\mathfrak{a}$ in a suitable way, that

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\varphi\colon \mathbf{C}/\Lambda_\tau \to \mathbf{C}/\Lambda_{N\tau}),$$

so that the Heegner point corresponds to the orbit of $\tau \in \mathcal{H}$.

We can be a little more precise about what from τ takes. Let $D = c^2 D_K$ be the discriminant of the order $\mathcal{O}$ (here, c is the conductor of $\mathcal{O}$ and D_K the discriminant of K). Then, since $\mathbf{C}/\Lambda_\tau$ has complex multiplication by $\mathcal{O}$, τ must be a root of an equation of the form $A\tau^2 + B\tau + C = 0$ with $A, B, C \in \mathbf{Z}$, $A > 0$, $\gcd(A, B, C) = 1$, such that $N|A$ and $D = B^2 - 4AC$. Indeed, since $\mathbf{C}/\Lambda_\tau$ has complex multiplication by $\mathcal{O}$, we know that $\sqrt{D} \in \Lambda_\tau$. That is,

$$\sqrt{D} = x + y\tau,$$

with $x, y \in \mathbf{Z}$. If we square both sides and re-arrange, we find that

$$y^2\tau^2 + 2xy\tau + x^2 - D.$$

Letting $y^2 = A, 2xy = B, x^2 - D = C$, we find that τ satisfies

$$A\tau^2 + B\tau + C = 0,$$

and that

$$B^2 - 4AC = 4x^2y^2 - 4y^2(x^2 - D) = D.$$

It is only left to check that $\gcd(A, B, C) = 1$ and $N|A$. First, if p were a prime that divided all of A, B, and C, then τ would be the root of the quadratic equation

$$\frac{A}{p}\tau^2 + \frac{B}{p}\tau + \frac{C}{p},$$

which has discriminant $\frac{D}{p^2}$. But such a τ would correspond to the elliptic curve $\mathbf{C}/\Lambda_\tau$ which would have complex multiplication by an order that contains the order of discriminant $\frac{D}{p^2}$, so that this elliptic curve cannot have complex multiplication by $\mathcal{O}$. It follows that $\gcd(A, B, C) = 1$.

Finally, since $\mathbf{C}/\Lambda_{N\tau}$ must have the same order of complex multiplications, we find that $N\tau$ satisfies an equation of the from $A'(N\tau)^2 + B'(N\tau) + C' = 0$, with $\gcd(A', B', C') = 1$ and $\gcd(A', B', C') = 1$. That is,

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

On the other hand, the equation for τ tells us that

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

from which it follows that

$$\frac{N}{2A} = \frac{1}{2A'},$$

after taking imaginary parts; that is, $N|A$.

With this description, we can recover $\mathfrak{a}$ (up to homothety) by multiplying Λ_τ by $2A$. Doing the same for $\Lambda_{N\tau}$, and dividing by N we obtain $\mathfrak{a}\mathfrak{n}^{-1}$ (up to homothety), finding that

$$\mathfrak{a} = 2A\mathbf{Z} + (-B + \sqrt{D})\mathbf{Z}, \text{ and } \mathfrak{a}\mathfrak{n}^{-1} = 2A'\mathbf{Z} + (-B + \sqrt{D})\mathbf{Z},$$

from which it is obvious that their quotient is isomorphic to $\mathbf{Z}/N\mathbf{Z}$ since $A = NA'$.

From now on, we will only consider the Heegner points for which the conductor c of our order $\mathcal{O}$ is prime to N. One reason for this assumption is that the ideal $N\mathcal{O}$ will factor in the same manner in which (N) factors in $\mathcal{O}_K$. That is, if $(N) = \prod \mathfrak{p}_i^{r_i}$, then

$$N\mathcal{O} = \prod(\mathfrak{p}_i^{r_i} \cap \mathcal{O}) = \prod(\mathfrak{p}_i \cap \mathcal{O})^{r_i}$$

is the prime factorization in $\mathcal{O}$.

The curve $X_0(N)$ has a planar model given by n-th modular polynomial. More precisely, the function field of $X_0(N)$ is generated by the functions $j(\tau)$ and $j(N\tau)$ and these functions satisfy a polynomial relation [2][Ch.II]. This polynomial defines an algebraic model of $X_0(N)$ that is defined over $\mathbf{Q}$ and the so it makes sense to ask whether points on $X_0(N)$ are algebraic. It turns out that the theory of complex multiplication tells us that the Heegner points are such points. Indeed, in the planar model for $X_0(N)$, which is defined over $\mathbf{Q}$, we find that the Heegner point $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ corresponds to the point $(j(\mathfrak{a}), j(\mathfrak{a}\mathfrak{n}^{-1}))$. By the theory described in the previous section, this point is an H_c-rational point where, as usual, H_c is the ring-class field to K of conductor c. Moreover, we know exactly how the Galois group

$\mathrm{Gal}(H_c/K) \cong \mathrm{Pic}(\mathcal{O})$ acts on these points; if $\sigma \in \mathrm{Gal}(H_c/K)$ corresponds to $\mathfrak{b} \in \mathrm{Pic}(\mathcal{O})$, then

$$(j(\mathfrak{a}), j(\mathfrak{a}\mathfrak{n}^{-1}))^\sigma = (j(\mathfrak{b}^{-1}\mathfrak{a}, j(\mathfrak{b}^{-1}\mathfrak{a}\mathfrak{n}^{-1})),$$

or in our other notation,

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^\sigma = (\mathcal{O}, \mathfrak{n}, [\mathfrak{b}^{-1}\mathfrak{a}]).$$

The Hecke operators defined in section 2 actually come from natural correspondences on $X_0(N)$. More precisely, there is a notion of Hecke operators T_ℓ on the divisor group of $X_0(N)$. In the case where $\ell \nmid N$, we have the following description. Let

$$x = (\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2)$$

be a point on $X_0(N)$, where $\Lambda_1 \subseteq \Lambda_2$, so that $\Lambda_2/\Lambda_1 \cong \mathbf{Z}/N\mathbf{Z}$. Observe that if $\Lambda \subseteq \Lambda_1$ has index ℓ, then Λ has index $N\ell$ in Λ_2, and since $\ell \nmid N$, we conclude that $\Lambda_2/\Lambda \cong \mathbf{Z}/N\ell\mathbf{Z}$. It follows that we can find a unique Λ' such that $\Lambda \subseteq \Lambda' \subseteq \Lambda_2$ and Λ'/Λ is isomorphic to $\mathbf{Z}/N\mathbf{Z}$. That is, the map $\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$ is a cyclic N-isogeny. The Hecke operator then takes the following form

$$x \mapsto \sum_{\Lambda_1/\Lambda = \mathbf{Z}/\ell\mathbf{Z}} (\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'),$$

where, again, the sum is a divisor. This definition needs to modified slightly for $\ell | N$.

It is thus natural to ask how the Hecke operators T_ℓ act on divisors supported on Heegner points. For $\ell \nmid N$, we have

$$T_\ell(\mathcal{O}, \mathfrak{n}, [\mathfrak{b}]) = \sum (\mathcal{O}_\mathfrak{b}, \mathfrak{n}_\mathfrak{b}, [\mathfrak{b}]),$$

where the sum is over the $(\ell + 1)$ sub-lattices $\mathfrak{b} \subseteq \mathfrak{a}$ of index ℓ, with $\mathcal{O}_\mathfrak{b} = \mathrm{End}(\mathbf{C}/\mathfrak{b})$, and $\mathfrak{n}_\mathfrak{b} = \mathcal{O}_\mathfrak{b} \cap \mathfrak{n}\mathcal{O}_K$. Note that $\mathfrak{b}$ does admit complex multiplication; if $b \in \mathfrak{b}$, and $\alpha \in \mathcal{O}$, then $\ell\alpha b \in \mathfrak{b}$ since $\mathfrak{b}$ has index ℓ in $\mathfrak{a}$.

The curve $X_0(N)$ is always equipped with the Fricke involution, w_N which sends the pair $(\varphi\colon E_1 \to E_2)$ to the dual isogeny, which goes in the opposite direction. It interchanges the cusps 0 and ∞. It's effect on Heegner points is given by

$$w_N(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}\mathfrak{n}^{-1}]),$$

where $\mathfrak{n}^\tau$ is the complex conjugate of $\mathfrak{n}$.

Even more generally, the curve $X_0(N)$ comes equipped with involutions w_d for all divisors d of N such that $\gcd(d, N/d) = 1$. These are defined as follows. Let $(\varphi\colon E_1 \to E_2)$ be our point in $X_0(N)$ and let D_1 and D_2 denote the subgroups of $\ker\varphi$ and $\ker\hat{\varphi}$ of order d. Then,

$$w_d(\varphi\colon E_1 \to E_2) := (E/D \to E/\ker\varphi \cong E' \to E'/D).$$

We often write w_p for the involution $w_{p^{v_p(N)}}$. One checks that these involutions form a group isomorphic to $(\mathbf{Z}/2\mathbf{Z})^s$, where s is the number of distinct prime divisors of N and that $w_N = \prod_{p|N} w_p$.

The action of the involutions w_p can be described as follows: let $N = p^k m$ with $p \nmid m$. Then, if $\mathfrak{p}$ is the *unique* factor of $\mathfrak{n}$ that divides $\mathcal{O}$, then $\mathfrak{n} = \mathfrak{p}^k\mathfrak{m}$ for some ideal $\mathfrak{p} \nmid \mathfrak{m}$. Let $\mathfrak{n}'$ be the ideal of $\mathcal{O}$ given by $(\mathfrak{p}^\tau)^k\mathfrak{m}$, where τ is given by complex conjugation. Then, $\mathfrak{n}'$ has quotient cyclic of order N and we find

$$w_p(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \mathfrak{n}', [\mathfrak{a}\mathfrak{p}^{-k}])$$

Lastly, $X_0(N)$ is also equipped with an action of complex conjugation τ. Its action on the Heegner points is given by

$$(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^\tau = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}^{-1}])$$

Note the connection between this action and the action of w_N; if $\sigma \in \mathrm{Gal}(H/K)$ denotes the element corresponding to $\mathfrak{n}$, we have

$$w_N(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = ((\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^\tau)^\sigma$$

3.2. **Field Extensions Generated by Heegner Points.** We saw in section 2 that we could use the j function to generate very special field extensions of quadratic imaginary fields. We can reformulate the results we discussed in terms of Heegner points as follows. First, let us observe that a Heegner point for $X_0(1)$ is just a single elliptic curve that has complex multiplication. Indeed, by our definition of a Heegner point, we need a pair of elliptic curves E_1 and E_2, both with the same order of complex multiplications, admitting a cyclic isgoeny of degree one. But such an isogeny must be an isomorphism, whence our observation. Sticking to notation that is similar to what we used above, we will denote by $(\mathcal{O}, [\mathfrak{a}])$ the Heegner point corresponding to the order $\mathcal{O}$ inside of a quadratic imaginary field K and $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$. The theory of complex multiplication then tells us exactly how the automorphisms of $\mathbf{C}$ act on these Heegner points: complex conjugation will take the point $(\mathcal{O}, [\mathfrak{a}])$ to $(\mathcal{O}, [\mathfrak{a}]^{-1})$, and the Galois group G_K acts on the points by $(\mathcal{O}, [\mathfrak{b}])^\sigma = (\mathcal{O}, [\mathfrak{a}\mathfrak{b}^{-1}])$, if σ corresponds to $\mathfrak{b}$ under the Artin map. We now think of j as a map from $X_0(1) \to \mathbf{P}^1(\mathbf{C})$ and, on the Heegner points, we may write $j(\mathcal{O}, [\mathfrak{a}]) := j(\mathfrak{a})$. The observation that the j-function respects the action of the automorphisms of $\mathbf{C}$ was enough to guarantee that the j function takes these Heegner points to algebraic values and, after a finer analysis of this action, we concluded that the corresponding j-values generated ring class fields, and were permuted in the same fashion as the Heegner points on $X_0(1)$ were.

Cast in this language, it seems natural to ask whether or not we can generalize this story to other modular curves. That is, we have a notion of Heegner point on all of the curves $X_0(N)$, and the theory of complex multiplication gives us a complete description of how automorphisms of $\mathbf{C}$ act on these points — is there a way to use these points to generate special field extensions like we did for the curve $X_0(1)$? A good place to start with such a question would be whenever $X_0(N)$ has genus zero. In this case, $X_0(N)$ admits a *hauptmodul*: a function $h\colon X_0(N) \to \mathbf{P}^1(\mathbf{C})$ that gives an isomorphism of $X_0(N)$ with the Riemann sphere. If we can find such a hauptmodul that respects the action of the automorphisms of $\mathbf{C}$, then we would, in principle, be in a position to "replace" j by h and prove similar results for the values that h takes at the Heegner points.

It is well known that $X_0(N)$ has genus zero only for

$$N \in \{2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\},$$

and a paper of Maier, [16], contains a table that has a normalized hauptmodul for each $X_0(N)$ for N as above. These hauptmoduln are given as η-products; that is, functions of the form

$$\kappa \prod_{\delta|N} \eta(\delta\tau)^{r_\delta},$$

where η is the usual Dedekind η-function, δ are divisors of N, $r_\delta \in \mathbf{Z}$, and $\kappa \in \mathbf{Z}$. For the details of why these are actually hauptmoduln, we refer the reader to Maier's paper, [16]. What is important for us is that sage knows how to compute η-products, so we can simply see what happens when we evaluate the hauptmoduln at the Heegner points.

Let us start by programming in the hauptmodul t_2 for $X_0(2)$:

```
sage:  def t2(n):

         return 2^12 * EtaProduct(2, 2 : 24, 1 : -24).qexp(n).truncate(n)

sage:  t2(10)

10747904 * q^4 + 1228800 * q^3 + 98304 * q^2 + 4096 * q
```

Notice that, like j, the q-expansion for this hauptmodul has rational coefficients. Now, let's evaluate this function at a Heegner point and see what happens:

```
sage:  P=heegner_point(2,-23)

sage:  tau=P.tau()

sage:  z=t2(500).subs(q=exp(2*pi*I*tau)).n(400)

sage:  z

-0.02813445276637...  -2.1911045152...*I
```

Let us now compute the class number of the field in question in order to predict what kind of value we have.

```
sage:  K.<a>=NumberField(-23)

sage:  K.class_number()

3
```

If we simply expect to have the same algebraicity result that we had for j, we would expect our computed value to be algebraic of degree 3 over $\mathbf{Q}$.

```
sage:  z.algdep(3)
```

$$4855660743104803566636772654545040434966176223698120902398 0 * x^3$$

$$-5121363479060539741072672972416958973706077412076418278632 4 * x^2$$

$$+2301202704118280488336239906396380103496929610566435798129 71 * x$$

$$-2590334930416640628854393885061092779480828565607755776756 69$$

This doesn't seem to be anything useful, but let us see if z is algebraic of degree $2 \cdot 3 = 6$ over $\mathbf{Q}$:

```
sage:  z.algdep(6)
```

$$x^6 + 166 * x^5 + 3503765 * x^4 + 412493295 * x^3$$

$$+14351421440 * x^2 + 2785017856 * x + 68719476736$$

This looks a little better and, in fact, we should have expected this. If we look at how the automorphisms of $\mathbf{C}$ affected the Heegner points of level 1, we see that the complex conjugation doesn't affect the orbit of a Heegner point. That is, for a Heegner point P of level 1, we have $\{gP\}_{g\in \mathrm{Pic}(\mathcal{O})}$ is the same set as $\{gP\}_{g\in \mathrm{Pic}(\mathcal{O})\rtimes\langle conj\rangle}$. But, if we look at heegner points of a different level, then these orbits are different. Indeed, as long as our Heegner point $P = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ satisfies the Heegner hypothesis, (conductor prime to N and every $p|N$ splits in K), then complex conjugation acts non-trivially on $\mathfrak{n}$. Therefore, when we let the automorphisms of $\mathbf{C}$ act on P, we actually obtain $2 \cdot h_{\mathcal{O}}$ points: the points of the form $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ for $\mathfrak{a} \in \mathrm{Pic}(\mathcal{O})$, together with the points $(\mathcal{O}, \overline{\mathfrak{n}}, [\mathfrak{a}])$ for $\mathfrak{a} \in \mathrm{Pic}(\mathcal{O})$.

We can verify in sage that the roots of this degree 6 polynomial are the t_2 values of the Galois orbit of the heegner point P and the Galois orbit of its conjugate, which is Galois-equivalent to the point obtained from P by acting with w_2:

```
sage:  T=[P.tau() for P in P.galois_orbit_over_K()]

sage:  T1=[P.atkin_lehner_act().tau() for P in P.galois_orbit_over_K()]

sage:  Z=[t2(500).subs(q=exp(2*pi*I*tau)).n(400) for tau in T]

sage:  Z1=[t2(500).subs(q=exp(2*pi*I*tau)).n(400) for tau in T1]

sage:  A=[z.algdep(6) for z in Z]
```

```
sage:  B=[z.algdep(6) for z in Z1]

sage:  A[0]==A[1]==A[2]==B[0]==B[1]==B[2]

true

sage:  Z

[-0.0281344...  -2.1911045...*I, -58.972451...  + 24.8646323...*I, -23.999413...
- 1869.068664...*I]

sage:  Z1

[-23.99941...  + 1869.06866...*I, -58.97245...  - 24.86463...*I, -0.028134...
+ 2.191104...*I]
```

Note these numbers are all distinct, and that the three numbers in $Z1$ are the complex conjugates of the numbers appearing in Z, which is what we hoped for.

Lastly, we verify that these values generate the class fields that we would expect of them. Before doing so, observe that our ideas would lead us to believe that this polynomial found above should split into two cubic polynomials over K. This is indeed the case, as we will see below, so we then pick a factor and see what kind of field extension is generated.

```
sage:  R.<t>=K[]

sage:  p=z.algdep(6).subs(x=t).factor()

sage:  p
```

$$(t^3 + (-385 * a + 83) * t^2 + (-45815/2 * a + 87701/2) * t - 45045/2 * a - 477713/2)*$$

$$(t^3 + (385 * a + 83) * t^2 + (45815/2 * a + 87701/2) * t + 45045/2 * a - 477713/2)$$

```
sage:  f=p[1][0]

sage:  L=K.extension(f)

sage:  L.relative_discriminant()

Fraction Ideal (1)
```

So, we see that we do generate the Hilbert class-field, as we had hoped. It is not hard to automate this process in sage, so that we can verify directly that the t_2-values of heegner points generate class-fields. We have found that we either always generate class-fields in this manner, or we obtain a computer error. When we get errors, the class groups tend to be

quite large, which explains why the computer errors would occur: the larger the degree of the number fields we are working with, the more difficult the computations become.

Performing similar calculations with the other hauptmoduln for $X_0(N)$ of genus zero produces the exact same results as we encountered above. Because these class-fields are so special, this provides very convincing evidence that these hauptmoduln are able to play the role of j for the curves $X_0(N)$ and the Heegner points. While a completely worked out proof of this is not yet known, Cox, McKay and Stevenhagen, [17] have shown that these observations hold for certain Heegner points that fail the Heegner hypothesis (that is, Heegner points where $\mathfrak{n}$ is stable under conjugation). In this setting, they show that taking values at these points with a hauptmodul having rational coefficients will give algebraic values that generate the corresponding class fields.

Having discussed the relationship between the theory of Heegner points and Hilbert's twelfth problem, we will now discuss the relationship to the Birch and Swinnerton-Dyer conjecture. The first step in this direction is to explain how we go about obtaining Heegner points on elliptic curves.

3.3. **Heegner Points on Elliptic Curves.** In this section, we will explain how to obtain points on an elliptic curve from the Heegner points discussed above. In order to do this, we will need to describe the modular parameterization.

Recall that the Jacobian of a curve X is defined as the quotient $\Omega^1_{hol}(X)^*/H_1(X, \mathbf{Z})$, where Ω^1_{hol} is the space of holomorphic differentials on X. Note that $H_1(X, \mathbf{Z})$ embeds as a lattice in this space by sending a cycle c to the functional $\omega \mapsto \int_c \omega$. The dual space itself if isomorphic to $\mathbf{C}^g$, so that the quotient is, complex-analytically, a g-dimensional complex torus. Abel's theorem then tells us that the Jacobian, as defined above, is isomorphic to the degree-0 part of the Picard group, $\mathrm{Pic}^0(X)$, which is the group of degree-zero divisors modulo the principal divisors. This isomorphism is given by the following map:

$$\sum_x n_x x \mapsto \sum_x n_x \int_{x_0}^x$$

If we assume that the genus of X is positive, then the map $X \to \mathrm{Pic}^0(X)$ defined by

$$P \mapsto (P) - (x_0),$$

defines an embedding of X into the Picard group. In this way, our curve can be embedded into its Jacobian.

Specializing now to the case of interest, namely, $X = X_0(N)$, we will let $J_0(N)$ denote the Jacobian of $X_0(N)$. We will identify $X_0(N)$ lying inside of its Jacobian via the map

$$P \mapsto (P) - (\infty)$$

Since we've already remarked earlier that the space of holomorphic differentials on $X_0(N)$ is naturally identified with the space of holomorphic weight 2 cusp forms, we can also think

of the Jacobian as the quotient

$$S_2(N)^*/H_1(X_0(N), \mathbf{Z}).$$

The point is that, on $S_2(N)$, we have at our disposal the Hecke operators. These operators induce endomorphisms of the dual space $S_2(N)^*$ and so we can think of the Hecke operators as lying inside $\mathrm{End}(J_0(N))$. We call the commutative sub-algebra generated by the Hecke operators the Hecke algebra, and we denote this object by $\mathbf{T}$. We will now describe how we can construct certain Abelian varieties as quotients of the Jacobian.

Let $f \in S_2(N)$ be a normalized newform. Then, we have a natural map $\lambda_f \colon \mathbf{T} \to \mathbf{C}$ which is defined by

$$T_n(f) = \lambda_f(T_n) f$$

We let $I_f := \ker \lambda_f$. Since we remarked earlier that the coefficients of such a new form lie in some algebraic extension of $\mathbf{Q}$, this gives an injection

$$\mathbf{T}/I_f \to K_f,$$

where K_f is the field generated by the coefficients of f. In fact, the rank of $\mathbf{T}/I_f$ is equal to the degree $[K_f \colon \mathbf{Q}]$.

Now, we can consider the quotient $A_f := J_0(N)/I_f J_0(N)$. This is an abelian variety and it turns out that its dimension is equal to the degree of K_f over $\mathbf{Q}$ [5][Ch. VI].

In particular, if f has integer coefficients, then the abelian variety constructed in this way will be an elliptic curve. The following theorem of Wiles', the so-called modularity theorem, will now give us the modular parameterization of an elliptic curve defined of $\mathbf{Q}$.

Theorem 3.3.1. *Let E be an elliptic curve defined over $\mathbf{Q}$ with conductor N. For a prime p, define numbers a_p as follows*

$$a_p := \begin{cases} p + 1 - |E(\mathbf{F}_p)| & \text{if } p \nmid N \\ 0 & \text{if } E \text{ has additive reduction at } p \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \end{cases}$$

We extend the definition to a_n for all n by demanding that the following identity holds:

$$\sum a_n n^{-s} = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \mid N} \frac{1}{1 - a_p p^{-s}}$$

Then, $f := \sum a_n q$ is a (normalized) weight 2 newform for $\Gamma_0(N)$.

What does this get us? Well, if we start with an elliptic curve E defined over $\mathbf{Q}$, we obtain an associated newform f. Proceeding as above, we obtain an elliptic curve E_f as a quotient of the Jacobian $J_0(N)$. It turns out that the a_p's associated to this elliptic curve are the same a_p's coming from f, so that by Falting's Isogeny theorem, it follows that the curve

E_f is isogenous (via a rational isogeny in fact) to our original curve E. In this manner, we obtain a map

$$X_0(N) \to J_0(N) \to E_f \to E.$$

The map $\Phi_N \colon X_0(N) \to E$ is called the modular parameterization and the curve E_f is called the strong Weil curve attached to E, or to f.

It is important to note that the maps $X_0(N) \to J_0(N)$ and the projection $J_0(N) \to E_f$ are algebraic maps, so that the modular parameterization Φ_N can be used to construct algebraic points on E_f (and thus on E) in the following manner. Let P be a Heegner point corresponding to the quadratic imaginary field K and the conductor of order c, so that P is an H_c-rational point of $X_0(N)$; then, $\Phi_N(P) \in E(H_c)$.

It is useful to note that we can describe the map Φ_N complex-analytically, as follows. The pullback of the Néron differential ω on E_f takes the form

$$c \cdot \omega_f,$$

where ω_f is the holomorphic differential associated to f and $c \in \mathbf{Q}$. The number is called the Manin constant of E.

Now let $\Phi_w \colon \mathbf{C}/\Lambda_{E_f} \to E_f(\mathbf{C})$ be the Weierstrass uniformization discussed earlier. Then, if we view $X_0(N)$ as $\mathcal{H}^*/\Gamma_0(N)$, the point $\Phi_N(\tau)$ corresponds to

$$\int_{\Phi_N(\infty)}^{\Phi_N(\tau)} \omega = c \cdot \int_{\infty}^{\tau} \omega_f,$$

using the properties of pull-backs.

It follows that we can compute the modular parameterization by computing $c \int_{\infty}^{\tau} \omega_f$, followed by the Weierstrass map. We can compute the integral as

$$\begin{aligned} c \cdot \int_{\infty}^{\tau} \omega_f &= c \cdot 2\pi i \int_{\infty}^{\tau} f(z)\, dz \\ &= = c \int_0^{e^{2\pi i \tau}} \frac{f(q)}{q}\, dq \\ &= c \cdot \int_0^{e^{2\pi i \tau}} \sum_{n=1}^{\infty} a_n q^{n-1}\, dq \\ &= c \cdot \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau} \end{aligned}$$

That is, we have

$$\Phi_N(\tau) = \Phi_w \left(c \cdot \sum \frac{a_n}{n} e^{2\pi i n \tau} \right)$$

The advantage to this description of the map is that it lends itself more easily to direct computation using sage. Below, we demonstrate how to use the modular parametrization in sage. The command itself is very straightforward:

```
sage:  E=EllipticCurve(j=0)

sage:  E

Elliptic Curve defined by y^2 + y = x^3 over Rational Field

sage:  Phi=E.modular_parametrization()

sage:  Phi(I,800)
```

This command will evaluate the modular parameterization at the point $i \in \mathcal{H}$, up to the high precision that we told it to compute. It is necessary to compute to such a high precision to ensure that the resulting point indeed lies on the elliptic curve that we expect it. Rather than show the really large numbers, we will simply give names to the coordinates and verify that they satisfy the equation for the elliptic curve with which we are working:

```
sage:  a,b=Phi(I,800)[0],Phi(I,800)[1]

sage:  b^2 + b - a^3

0.000000000000000000000000000000000000000000000000000000000000000000000000
```

As described above, the modular parameterization is actually a map to the Weil curve of E, or the optimal curve. We can compute the manin consant of E in sage and we see that E is not optimal:

```
sage:  E.manin_constant()

3
```

Sage can then compute the optimal curve associated to E:

```
sage:  F=E.optimal_curve()

sage:  F

 Elliptic Cruve defined by y^2 + y = x^3 - 7 over Rational Field
```

Next, sage can compute the minimal isogeny from F to E. This ends up having degree 3:

```
sage:  Alpha=F.isogeny(None,E,3)

sage:  Alpha

Isogeny of degree 3 from Elliptic Curve defined by y^2 + y = x^3 - 7 over Rational
Field to Elliptic Curve defined by y^2 + y = x^3 over Rational Field
```

Sage can give us this map in terms of rational maps, so we can then compute the composition of the modular parameterization to F and this isogeny. We will see that this is the same as the modular paramaterization to E:

```
sage:Alpha.rational_maps()
```

$((x^3 - 27)/x^2, (x^3 * y + 54 * y + 27)/x^3)$

```
sage:  P=F.modular_parametrization()(I,800)

sage:  a1,b1=P[0],P[1]

sage:  Q=((a1^3 - 27)/a1^2, (a1^3 * b1 + 54 * b1 + 27)/a1^3)

sage:  Q[0]

286751.31500409572741576690162787484849890947388903358 71

sage:  a

286751.31500409572741576690162787484849890947388903358 71

sage:  Q[1]

-1.53552937395446706947450592504792685038080742239129851

sage:  b

-1.53552937395446706947450592504792685038080742239129851
```

So, we see that the modular parametrization is built into sage and works the way we would expect it to.

Now that we have fully explained how to get Heegner points on elliptic curves, we move on to the next section, which explains some of the deep theorems relating the Heegner points to the Birch and Swinnerton-Dyer conjecture.

4. The Theorems of Gross, Zagier, and Kolyvagin

4.1. **The L-functions Associated to Modular Forms and Elliptic Curves.** In this section we define and describe the basic properties of L-functions, which are holomorphic functions associated to modular forms and elliptic curves that, conjecturally, have deep arithmetic connections with the corresponding objects.

Definition 4.1.1. Let $f \in S_2(N)$ be a newform. We define the L-series attached to f by setting

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

if $f = \sum_{n=1}^{\infty} a_n q^n$.

This series converges in the half plane $\Re(s) > \frac{3}{2}$ and enjoys the following three properties:

(1) **Euler Product** The L-series can be written as the following infinite product:

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

This follows from the fact that f is an eigenform and that the Hecke operators satisfy the same relation.

(2) **Integral Representation** If we set $\Lambda(f,s) := (2\pi)^{-s}\Gamma(s)N^{\frac{s}{2}}L(f,s)$, then we have

$$\Lambda(f,s) = N^{\frac{s}{2}} \int_0^{\infty} f(it)t^{s-1}\, dt$$

Indeed, we compute

$$\begin{aligned}
\Lambda(f,s) &= N^{\frac{s}{2}} \sum_{n=1}^{\infty} a_n \cdot (2\pi n)^{-s} \int_0^{\infty} e^{-t}t^{s-1}dt \\
&= N^{\frac{s}{2}} \sum_{n=1}^{\infty} \int_0^{\infty} a_n \cdot (2\pi n)^{-s} e^{-t}t^{s-1}\, dt \\
&= N^{\frac{s}{2}} \sum_{n=1}^{\infty} \int_0^{\infty} a_n e^{-2\pi n t}t^{s-1}\, dt \text{ (substitute } t = 2\pi n t') \\
&= N^{\frac{s}{2}} \int_0^{\infty} \sum_{n=1}^{\infty} a_n e^{-2\pi n t}t^{s-1}\, dt \\
&= N^{\frac{s}{2}} \int_0^{\infty} f(it)t^{s-1}\, dt
\end{aligned}$$

(3) **Functional Equation** The function $\Lambda(f,s)$ should obey a functional equation relating its arguments at s and $2-s$. More precisely, let w_N be the operator on $S_2(N)$ defined by $w_N(f)(\tau) := \frac{1}{N\tau^2} f(\frac{-1}{N\tau})$. It is easy to check that w_N is an involution and, via a direction calculation, one can see easily that this operator commutes with the Hecke operators. It follows that if f is a newform, $w_N(f) = \epsilon f$, with $\epsilon \in \{\pm 1\}$. Then, the functional equation for $\Lambda(f,s)$ is

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

Indeed, by making a change of variable, we see that

$$\Lambda(f,s) = \int_0^{\infty} f\left(\frac{it}{\sqrt{N}}\right) t^{s-1}\, dt$$

We now split this as the sum

$$\Lambda(f,s) = \int_0^1 f\left(\frac{it}{\sqrt{N}}\right) t^{s-1}\, dt + \int_1^\infty f\left(\frac{it}{\sqrt{N}}\right) t^{s-1}\, dt$$

We now observe that

$$w_N(f)\left(\frac{i}{\sqrt{N}t}\right) = t^2 f\left(\frac{it}{\sqrt{N}}\right),$$

which allows us re-write the first summand,after making the change of variable $t \mapsto 1/t$,

$$-\int_1^\infty w_N(f)\left(\frac{i}{\sqrt{N}t}\right) t^{s-3}\, dt,$$

and so we see that $\Lambda(f,s)$ can be written as

$$(*) \qquad \Lambda(f,s) = \int_1^\infty \left\{ f\left(\frac{it}{\sqrt{N}}\right) t^{s-1} - w_N(f)\left(\frac{it}{\sqrt{N}}\right) t^{s-3} \right\} dt,$$

from which it follows upon making the substitution $s \mapsto 2-s$ that

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

where ϵ is defined as above.

Note that $(*)$ also gives the analytic continuation for $\Lambda(E,s)$; since f is a modular form, $f(it)$ converges to 0 very quickly, so the integral above converges for s in compact subsets of $\mathbf{C}$, from which it follows that $(*)$ defines a holomorphic function on all of $\mathbf{C}$.

Next, let us associate an L-function to an elliptic curve E, defined over $\mathbf{Q}$.

Definition 4.1.2. Let E be an elliptic curve with conductor N. For p a prime number, define numbers a_p as follows (these are the same a_p's defined in the statement of Theorem 3.3.1).

$$a_p := \begin{cases} p+1-|E(\mathbf{F}_p)| & \text{if } p \nmid N \\ 0 & \text{if } E \text{ has additive reduction at } p \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p \end{cases}$$

We define the L-function of E as the infinite product

$$L(E,s) := \prod_{p \nmid N} \frac{1}{1-a_p p^{-s}+p^{1-2s}} \cdot \prod_{p|N} \frac{1}{1-a_p p^{-s}}$$

It can be checked without much difficulty that this product converges whenever $\Re(s) > \frac{3}{2}$.

We would like to say that $L(E,s)$ enjoys the same three properties that were shown to hold for the L-functions associated to newforms of level N. Since we've defined the function $L(E,s)$ as an Euler product, we have the first property for free. As for the integral representation and a functional equation, it is not at all clear where to even begin with these. This is one of the amazing consequences of Theorem 3.3.1; it tells us that the L-function

defined as above corresponds to the modular form $f = \sum a_n q^n$, and in this way, we have the desired properties for the L-functions of elliptic curves defined over $\mathbf{Q}$.

If we want to work over number fields other than $\mathbf{Q}$, then there is still a definition of L-function, though most of its desired properties are still conjectural.

Definition 4.1.3. Let K be a number field and E an elliptic curve over K. For each finite place v of K, we define *local L-series* as follows: if v is a place of good reduction, let $a_v := |v| + 1 - |E(\mathbf{F}_{|v|})|$, where $|v|$ is the norm of v from K to $\mathbf{Q}$, and put

$$L_v(E/K, s) := \frac{1}{1 - a_v|v|^{-s} + |v|^{1-2s}}.$$

If v is a place of bad reduction, we define $L_v(E/K, s)$ via the following prescription:

$$L_v(E/K, s) := \begin{cases} 1 - |v|^{-s} & \text{if } E \text{ has split multiplicative reduction at } v \\ 1 + |v|^{-s} & \text{if } E \text{ has non-split multiplicative reduction at } v \\ 1 & \text{if } E \text{ has additive reduction at } v \end{cases}$$

We then define the L-function of E/K to be the infinite product

$$L(E/K, s) := \prod_v L_v(E/K, s)$$

Again, it can be shown that this series converges for $\Re(s) < \frac{3}{2}$. It is conjectured that it can be analytically continued to the entire complex plane and satisfies a functional equation relating its values at s and $2 - s$. Unfortunately, there is no modularity theorem for elliptic curves defined over number fields, so it is very unclear where to even start with proving such things.

One last kind of L-function that we will discuss here are the L-functions attached to ℓ-adic representations of Galois groups. This will allow us to view the L-functions of an elliptic curve in a new light as well as to obtain some useful factorizations, which will be important in subsequent sections.

Definition 4.1.4. Fix a number field K. An ℓ-adic Galois representation of K is a continuous group homomorphism

$$\rho\colon G_K \to \mathrm{GL}_n(\overline{\mathbf{Q}}_\ell),$$

for some n, where G_K is the absolute Galois group of K and $\overline{\mathbf{Q}}_\ell$ is an algebraic closure of $\mathbf{Q}_\ell$.

There are three types of representations that we will consider here. First, we have the Artin representations. These are complex representations that factor through a finite quotient, so they are representations

$$\rho\colon \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbf{C})$$

for some number field L. It is well known that any such representation is isomorphic to one with coefficients in $\mathbf{Q}(\zeta_{[L\colon K]})$, so we may assume that ρ has algebraic coefficients. If we fix

an embedding $\overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_\ell$, we obtain an ℓ-adic representation which we denote by ρ_ℓ. Now let $V = \overline{\mathbf{Q}}_\ell$ with G_K action via ρ. If v is a finite place of K such that $v \nmid \ell$, we define the local L-series attached to ρ_ℓ as

$$L_v(\rho_\ell, s) := \frac{1}{\det\left(1 - |v|^{-s}\rho_\ell(\sigma_v)|V^{I_v}\right)}$$

Note that as long as ℓ is not divisible by v, this local series is independent of ℓ; this is because ρ_ℓ comes from an Artin representation. It therefore makes sense to define the local L-series for ρ as

$$L_v(\rho, s) := L_v(\rho_\ell, s),$$

for any ℓ not divisible by v. From here, we can define the global L-series attached to ρ as

$$L(\rho, s) := \prod_v L_v(\rho, s),$$

the product being over all the finite places of K.

The second type of representations we will consider are the ones attached to an elliptic curve.

Definition 4.1.5. Let E be an elliptic curve defined over the number field K. Then, the Galois group G_K acts on the groups $E[\ell^n]$ in a compatible way such that we have an action of G_K on the direct limit. Since $E[\ell^n] \cong \mathbf{Z}/\ell\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}$, this gives a representation

$$\rho_\ell \colon G_K \to \mathrm{GL}_2(\mathbf{Z}_\ell) \subseteq \mathrm{GL}_2(\overline{\mathbf{Q}}_\ell).$$

We denote that direct limit of the $E[\ell^n]$'s as $T_\ell(E)$, and call this the ℓ-adic Tate module.

Since we don't have a global representation to discuss here, we will attach an L-function to the family of representations given by the ρ_ℓ above.

Definition 4.1.6. If v is a finite place of K, we define the local L-series attached to the family of representations $F := \{\rho_\ell\}_\ell$ to be

$$L_v(F, s) := \frac{1}{\det\left(1 - |v|^{-s}\rho_\ell(\sigma_v)|T_\ell(E)^{I_v}\right)}$$

where $v \nmid \ell$.

We define the L-series of F to be

$$L(F, s) := \prod_v L_v(F, s)$$

Unlike the case for Artin representations, it is not clear that the above definition is well-defined; why are the local series independent of our choice of ℓ? For this, we appeal to [1][Ch.V] which says that, for a place of good reduction, we have

$$\det(\rho_\ell(\sigma_v)) = |v|, \quad tr(\rho_\ell(\sigma_v)) = a_v,$$

where the a_v are the ones defined above. So, not only does this mean that our definition is well-defined (it works for places of bad reduction, but this requires a little more work

that won't add to the understanding), but that the L-function attached to this family of representations is none other than $L(E/K, s)$!

The last kind of L-function that we will discuss arises by combining the two types above.

Definition 4.1.7. Let E be an elliptic defined over the number field K and let χ be an Artin representation for K. Then, for each ℓ, let V_ℓ be the representation obtained by tensoring the ℓ-adic representation ρ_ℓ on E with χ_ℓ. V_ℓ is called the *twist* of ρ_ℓ by χ. As usual, if we fix a place v of K, we define the local L-series for the family $F_\chi := \{V_\ell\}_\ell$, via

$$L_v(F_\chi, s) := \frac{1}{\det\left(1 - |v|^{-s}\rho_\ell \otimes \chi(\sigma_v)|V^{I_v}\right)},$$

for any ℓ not divisible by v and we define the global L-series via

$$L(F_\chi, s) := \prod_v L_v(F_\chi, s).$$

It is true, but beyond the scope of this paper to show, that the above definition is well-defined. The L-function defined above is called the L-function of E twisted by χ and will henceforth be denoted by

$$L(E/K, \chi, s)$$

It is conjectured that the Artin L-functions have analytic extensions to the whole complex plane whenever ρ is non-trivial and irreducible, and that the Artin L-functions obey a functional equation relating the values at s to the values at $1-s$. These conjectures are known to hold for one-dimensional characters. The twisted L-functions are also conjectured to extend to an analytic function and obey a functional equation similar to the ones we've seen. In the following sections, we will be interested in the case where K is a quadratic imaginary field and χ is a character of $\mathrm{Gal}(H_c/K)$ for some conductor c. In this case, we have the following theorem which follows from extensions of Rankin's method by Jacquet [10].

Theorem 4.1.8. *Let K be a quadratic imaginary field and $\chi\colon \mathrm{Gal}(H_c/K) \to \mathbf{C}$. Let*

$$\Lambda(E/K, \chi, s) := A^{\frac{s}{2}}(2\pi)^{-2s}\Gamma(s)^2 L(E/K, \chi, s),$$

where $A = \frac{N^2 D_K^2}{\gcd(N, D_K)}$. Then $L(E/K, \chi, s)$ extends to an analytic function and obeys the following functional equation

$$\Lambda(E/K, \chi, x) = sign(E, K)\Lambda(E/K, \chi, 2 - s),$$

where the sign depends only on E and K, not on the character χ.

In particular, it makes sense to talk about $L(E/K, s)$, $L(E, s)$ and $L(E, \chi, s)$ whenever χ is a quadratic Dirichlet character, K is the associated quadratic field and E is an elliptic curve defined over $\mathbf{Q}$.

Artin [13] was able to show that the L-functions defined by him behaved well with respect to the constructions in representation theory. Namely, he showed that the L-functions obeyed the following two properties that will be of interest to us.

- **Multiplicativity** Suppose that χ and ψ are two representations of G_K. Then we have
$$L(\chi \oplus \psi, s) = L(\chi, s)L(\psi, s)$$
- **Induction** Suppose we have a tower of extensions $K \subseteq M \subseteq L$ with L/K Galois. If ρ is a representation of $\mathrm{Gal}(L/M)$, we can induce up to get the representation $\mathrm{Ind}\rho$ of $\mathrm{Gal}(L/K)$. We have
$$L(\mathrm{Ind}\rho, s) = L(\rho, s)$$

Note that these two properties give us a useful factorization of $\zeta_L(s) = L(\mathbf{1}_L, s)$ whenever L/K is Galois. If we induce $\mathbf{1}_L$ to $\mathrm{Gal}(L/K)$, we obtain the regular representation. On the other hand, it is well known that this regular representation is isomorphic to
$$\bigoplus_{\chi} \dim(\chi)\chi,$$
where the sum is over all irreducible representations of $\mathrm{Gal}(L/K)$. Combining these facts, we obtain
$$\zeta_L(s) = \prod_{\chi} L(\chi, s)^{\dim(\chi)}$$

Next, we have that the same properties hold for the L-functions of elliptic curves and their twists. In particular, we have the following factorization of of $L(E/L, s)$ whenever E is an elliptic curve defined over $K \subseteq L$
$$L(E/L, s) = \prod_{\chi} L(E/K, \chi, s)^{\dim(\chi)}$$

4.2. **The Gross-Zagier Formula and Kolyvagin's Theorem.** For this section, we fix an elliptic curve $E/\mathbf{Q}$ of conductor N and a quadratic imaginary field K such that all the primes dividing N split completely in K; this condition is referred to as the Heegner hypothesis. Next, we fix a Heegner point x of conductor 1 and let $P \in E(H)$ be its image under the modular parameterization, where H is the Hilbert class field of K. Letting P_K denote the trace of this point to K,
$$P_K := \mathrm{Tr}_K^H P = \sum_{\sigma \in \mathrm{Gal}(H/K)} P^\sigma$$
we obtain a point in $E(K)$. In fact, the point P_K is independent of the Heegner point with with we started, up to a sign.

To see this, factor N as $\prod_i (\mathfrak{p}_i \mathfrak{p}_i^\tau)^{r_i}$, where the sum is over all the primes p_i dividing N and $\mathfrak{p}_i\mathfrak{p}_i^\tau = p_i$, and let $x = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$, and $y = (\mathcal{O}, \mathfrak{n}', [\mathfrak{b}])$ denote two Heegner points. Then, we can write
$$\mathfrak{n} = \prod_i \mathfrak{q}_i^{r_i},$$
where q_i is equal to either $\mathfrak{p}_i$, or its conjugate. Similarly,
$$\mathfrak{n}' = \prod_i \mathfrak{c}_i^{r_i},$$

where $\mathfrak{c}_i$ is equal to either $\mathfrak{p}_i$, or its conjugate. It follows from the description of the action of w_p on the Heegner points described in section 3.1, that for a suitable product w of these involutions, we have

$$w(x) = y^\sigma,$$

for some $\sigma \in \mathrm{Gal}(H/K)$. For example, if $\mathfrak{n}' = \mathfrak{n}^\tau$, then

$$w(x) = (\mathcal{O}, \mathfrak{n}^\tau, [\mathfrak{a}\mathfrak{n}^{-1}]) = y^\sigma,$$

where σ corresponds to $\mathfrak{b}\mathfrak{n}\mathfrak{a}^{-1}$. Since $w(x)$ maps to $\pm P$ under the modular parameterization, taking trace on both sides yields the claim.

The upshot is, we have now obtained a point $P_K \in E(K)$ that is canonical, up to a sign. The following result of Benedict Gross and Donald Zagier tells us that this point "knows" about the L function $L(E/K, s)$ defined above.

Theorem 4.2.1 (Gross-Zagier Formula)**.** *Let E be an elliptic curve over $\mathbf{Q}$ and K an imaginary field satisfying the Heegner hypothesis with discriminant E and u_K the order of $\mathcal{O}^\times/\{\pm 1\}$. Let ω denote the invariant differential of E and c the Manin constant of E and P_K the point constructed above. Then*

$$L'(E/K, 1) = \frac{||\omega||^2 h(P_K)}{c^2 u_K^2 \sqrt{|D|}},$$

where

$$||\omega||^2 := \int_{E(\mathbf{C})} |\omega \wedge \overline{\omega}|,$$

and $h(P_K)$ is the canonical height of P_K over K.

All we will say about the canonical height h_K is that it is a map $h_K \colon E(K) \to [0, \infty[$ that gives rise a bilinear pairing defined by $h_K(P+Q) - h_K(P) - h_K(Q)$. The map is constructed in such a way that $h_K(P) = 0$ if and only P is a torsion point. So, the theorem is saying that the point P_K has infinite order if and only if the derivative of the L-function is non-zero. Assuming that the point P_K above is not torsion, we may obviously deduce that the group $E(K)$ has rank at least 1. The next theorem of Kolyvagin tells us the much more surprising fact that $E(K)$ has rank *exactly* one.

Theorem 4.2.2 (Kolyvagin)**.** *With the set-up as above, assume that P_K is a point of infinite order. Equivalently, $L'(E/K, 1) \neq 0$. Then, the following are true:*

(1) P_K generates a subgroup of finite-index in $E(K)$, so that the rank of the group $E(K)$ is equal to one.
(2) The Shafarevich-Tate group, $Ш(E/K)$ is finite.

4.3. **The Birch and Swinnerton-Dyer Conjecture.** In this section, we will recall the definition of the Shafarevich-Tate group that appears in Kolyvagin's theorem and describe a fascinating conjecture of Birch and Swinnerton-Dyer about that relates the arithmetic of an elliptic curve with analytic properties of its L-function. Then, in the sections following, we

will explain how the two results mentioned above help us shed some light on this conjecture for elliptic curves defined over $\mathbf{Q}$.

Let K be a number field and E and elliptic over K. The Mordell-Weil theorem tells us that the group $E(K)$ is a finitely generated abelian group, but the proof does not give us an effective algorithm for computing this group. In fact, as of writing this paper, there is no known effective algorithm (one which is guaranteed to finish in a finite amount of time) to compute this group. As we will see below, the reason why it is so difficult to compute this group is the Shafarevich-Tate group.

Let us first remark that the computation of the group $E(K)$ can be reduced to the problem of computing the group $E(K)/mE(K)$ for some $m \geq 2$. We can start by trying to compute this group using the obvious short exact sequence of G_K modules

$$0 \longrightarrow E[m] \longrightarrow E \xrightarrow{m} E \longrightarrow 0$$

Now, if we take G_K-cohomology, we obtain the following long exact sequence

$$0 \longrightarrow E(K)[m] \longrightarrow E(K) \xrightarrow{m} E(K) \longrightarrow H^1(G_K, E[m]) \longrightarrow H^1(G_K, E) \xrightarrow{m} H^1(G_K, E)$$

from which we obtain the short exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow H^1(G_K, E[m]) \longrightarrow H^1(G_K, E)[m] \longrightarrow 0$$

Our ultimate goal is therefore to compute the image of $E(K)/mE(K)$ in the cohomology group $H^1(G_K, E[m])$, or equally as well, to compute the kernel of the map $H^1(G_K, E[m]) \to H^1(G_K, E)[m]$. To do this, we note that the above can be carried out for E/K_v where K_v is the completion of K at the place v. If we do this for every place v, we obtain the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/mE(K) & \longrightarrow & H^1(G_K, E[m]) & \longrightarrow & H^1(G_K, E)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/mE(K_v) & \longrightarrow & \prod_v H^1(G_{K_v}, E[m]) & \longrightarrow & \prod_v H^1(G_{K_v}, E)[m] & \longrightarrow & 0 \end{array}$$

Definition 4.3.1. The m-Selmer group of E/K is denoted by $S^{(m)}(E/K)$ and is defined as

$$S^{(m)}(E/K) := \ker \left\{ H^1(G_K, E[m]) \to \prod_v H^1(G_{K_v}, E)[m] \right\}.$$

The Shafarevich-Tate group of E/K is denoted by $Ш(E/K)$ and defined as

$$Ш(E/K) := \ker \left\{ H^1(G_K, E) \to \prod_v H^1(G_K, E) \right\}.$$

Straight from the definition of these two groups, we see that $E(K)/mE(K)$ fits into an exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow S^{(m)}(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0$$

The point is that the Selmer groups are effectively computable, in theory [1][Ch.X]. So, if we wish to compute the group $E(K)/mE(K)$, it would suffice to find some m such that $Ш(E/K)[m] = 0$. This would certainly be the case if $Ш(E/K)$ were a finite group. While it is conjectured that this is case, it is not known to hold all the time; in this sense, the group $Ш(E/K)$ is what keeps us from an effective algorithm to compute the group $E(K)$.

For simplicity, we will now suppose that E is an elliptic curve defined over $\mathbf{Q}$. We define the following arithmetic quantities associated to $E/\mathbf{Q}$:

- We define the regulator of E as follows. Suppose that $E(\mathbf{Q})$ has rank r and let $\{P_1, \ldots, P_r\}$ be a basis for $E(\mathbf{Q})/E(\mathbf{Q})_{tors}$. The regulator of $E/\mathbf{Q}$ is defined as
$$R(E/\mathbf{Q}) := \det(\langle P_i, P_j \rangle)_{ij},$$
where $\langle -, - \rangle$ is the Néron-Tate pairing.
- We define $\Omega := \left| \int_{E(\mathbf{R})} \omega \right|$; this is the real-period associated to E or twice the real period depending on whether or not E is connected.
- Let $E_0(\mathbf{Q}_p)$ denote those points of $E(\mathbf{Q}_p)$ whose reduction mod p is a nonsingular point on the reduced curve. Let $c_p := |E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)|$. Then, the c_p are finite [1][Ch.VII]. and in fact, equal to 1 for all $p \nmid N$, where N is the conductor of E.

Now that all the ingredients have been defined, we are ready to state the conjecture of Birch and Swinnerton-Dyer

Theorem 4.3.2 (Conjecture)**.** *Let $E/\mathbf{Q}$ be an elliptic curve. Then,* $\operatorname{ord}_{s=1} L(E, s) = \operatorname{rank}(E(\mathbf{Q}))$*, and the first non-zero coefficient of the Taylor series expansion for $L(E, s)$ about $s = 1$ is given by*

$$\frac{\Omega \cdot |Ш(E/\mathbf{Q})| \cdot R(E/\mathbf{Q}) \cdot \prod_p c_p}{|E(\mathbf{Q})_{tors}|^2}$$

As mysterious as this conjecture is, the theorems of Gross-Zagier and Kolyvgain already give a hint as to why the analytic and algebraic ranks of an elliptic curve might be connected. In fact, piecing the two results together will give us the Gross-Zagier-Kolyvagin theorem which proves the rank portion of the Birch and Swinnerton-Dyer conjecture for elliptic curves with analytic rank at most 1. The precise formula for the first non-zero coefficient of the L-function could be thought of in analogy with the analytic class-number formula for ζ-functions of number fields.

4.4. **Two Key Examples.** Before discussing the theorem of Gross-Zagier-Kolyvagin in more detail, let us examine two examples in detail. We will take two elliptic curves over $\mathbf{Q}$ whose L-functions vanish to an order of 0 or 1 and show that they satisfy the conclusion of Birch

and Swinnerton-Dyer. With the examples suitably discussed, we will be able to see how one goes about proving such a beautiful theorem.

To aid with some computations, we will use the following fact about the L-functions that we will be dealing with. Let K be a quadratic field, with discriminant D and let $E/\mathbf{Q}$ be an elliptic curve. We will let E_D denote the quadratic twist of E by K; if E has a weierstrass equation of the form $y^2 = f(x)$, then E_D is given by $Dy^2 = f(x)$. Also, let $\chi\colon \mathrm{Gal}(K/\mathbf{Q}) \to \mathbf{C}^\times$ denote the non-trivial character. Then, we have the following factorizations of $L(E/K, s)$:

$$L(E/K, s) = L(E, s)L(E, \chi, s) = L(E, s)L(E_D, s)$$

Indeed, the first equality was discussed above and the second can be seen as follows. We need to show an equality of Euler product

$$\prod_{\mathfrak{p}|p} L_{\mathfrak{p}}(E/K, s) = L_p(E, s)L_p(E_D, s)$$

for all primes p. We will prove that this holds for all $p \nmid ND$, and omit the details for the other p. There are two case to consider: either p splits in K, or p is inert in K. If p splits in K and $\mathfrak{p}$ is a prime lying above p, then the residue field of K at $\mathfrak{p}$ is the residue field of $\mathbf{Q}$ at p, from which it is clear that $a_p = a_{\mathfrak{p}}$ for the two primes above p. On the other hand, since p is split, then p is a square mod D, from which it follows that the curves $\tilde{E}$ and $\tilde{E_D}$ are isomorphic over $\mathbf{F}_p$ where $\tilde{}$ denotes reduction mod p. It follows that $a_p(E) = a_p(E_D)$, from which the desired equality of Euler products holds.

Now assume that p is inert and consider the Euler product term $L_p(E/K, s)$. In this case, let $\sigma_p \in G_{\mathbf{Q}}$ denote a Frobenius at p. Then σ^2 restricts to a Frobenius at p in K, from which it follows that

$$L_p(E/K, s) = \frac{1}{\det\left(1 - \rho(\sigma_p^2)p^{-2s}\right)}$$

Now, the Euler factor at p for $L(E, s)$ can be written as $(1 - \lambda_1 p^{-s})(1 - \lambda_2 p^{-s})$ where λ_1, λ_2 are the eigenvalues of $\rho(\sigma_p)$ acting on the Tate-module. Similarly, the Euler factor p for $L(E/K, s)$ can written in the same form, but we know the eigenvalues must be λ_1^2, λ_2^2. Since $\lambda_1\lambda_2 = p$ and $\lambda_1 + \lambda_2 = a_p(E)$, it follows that the Euler factor $L_p(E/K, s)$ is given by

$$L_p(E/K, s) = \frac{1}{1 - (a_p(E)^2 - 2p)p^{-2s} + p^{2(1-s)}}$$

One the other hand, consider the reductions mod p, $\tilde{E}$ and $\tilde{E_D}$. If we fix $x \in \mathbf{F}_p$, we see that either x corresponds to a single point on both curves, or x corresponds to two points on exactly one of the curves. It follows that we have the relation

$$|E_1(\mathbf{F}_p)| + |E_2(\mathbf{F}_p)| = 2(p + 1),$$

from which it follows that $a_p(E) = -a_p(E_D)$. Multiplying the two Euler product terms $L_p(E, s)L_p(E_D, s)$ then yields the desired equality.

Let us now examine two elliptic curves and try to prove the Birch and Swinnerton-Dyer conjecture for these curves. We will satisfy ourselves by only proving the rank portion of the conjecture.

Example 4.4.1 (An Elliptic Curve with $\mathrm{ord}_{s=1} L(E,s) = 0$). Consider the elliptic curve $E/\mathbf{Q}$ given by the equation

$$E\colon y^2 = x^3 + 1$$

In Sage, we can compute the L-series of E and evaluate it at $s = 1$, along with its derivatives:

```
sage:  E=EllipticCurve(QQ,[0,1])

sage:  E

Elliptic Curve defined by y^2 = x^3 + 1 over Rational Field

sage:  L=E.lseries()

sage:  L(1)

0.701091052662727
```

From this, we see that $\mathrm{ord}_{s=1} L(E,s) = 0$ and so, if we expect the Birch and Swinnerton-Dyer conjecture to be true, we should expect that $E(\mathbf{Q})$ is a torsion group.

To see why this is the case, we want to use the results of Gross-Zagier and Kolyvagin. In order to do so, we need to find a suitable quadratic field K with which to work. More precisely, we would like to find a quadratic field K that satisfies the Heegner hypothesis with respect to E and also satisfies $\mathrm{ord}_{s=1} L(E/K,s) = 1$. In this case, the theory predicts that we are entitled to a point $P_K \in E(K)$ that generates a finite-index subgroup of $E(K)$. We then wish to analyze this point and see what it has to say about $E(\mathbf{Q})$.

Sage can tell us which quadratic fields K satisfy the Heegner hypothesis with respect to the conductor N:

```
sage:  E.conductor()

36

sage : E.heegner_discriminants(50)

[−23, −47]
```

This command returns to us all the discriminants that satisfy the Heegner hypothesis up to -50. We can check that this is indeed the case by factoring the ideals (2) and (3) in $K = \mathbf{Q}(\sqrt{-23})$.

```
sage:  K=QuadraticField(-23)

sage:  I=K.ideal(2)

sage:  I.factor()

(Fractional ideal (2, 1/2 * a - 1/2)) * (Fractional ideal (2, 1/2 * a + 1/2))

sage:  J=K.ideal(3)

sage:  J.factor()

(Fractional ideal (3, 1/2 * a - 1/2)) * (Fractional ideal (3, 1/2 * a + 1/2))
```

Now we hope to find a quadratic field K, in the list above, such that $L(E/K, s)$ vanishes at $s = 1$ to order 1. We check using Sage that the field $K = \mathbf{Q}(\sqrt{-23})$ as above works for these purposes.

```
sage:  E2 = E.quadratic_twist(-23)

sage:  L2=E2.lseries()

sage:  L2.at1()

0

sage:  L2.deriv_at1()

(5.93874740885491, 0.0801774443659141)
```

The last number is an approximation of the error involved in computing the derivative; we see it is small enough that we can be sure that the derivative does not vanish. Therefore, the L-function $L(E_{-23}, s)$ has a zero of order 1 at $s = 1$, so that by our factorization of the L-function $L(E/K, s)$, we know that $L(E/K, s)$ has a zero at $s = 1$ of order 1 as well. So, if we construct the corresponding Heegner point $P_K \in E(K)$, we expect it to have infinite order. Since we expect $E(\mathbf{Q})$ to be a torsion group, we also expect to find that $P_K \notin E(\mathbf{Q})$ as well.

```
sage:  P = E.heegner_point(-23).point_exact()

sage:  P

(a : 2/15 * a^5 + 1/5 * a^4 + 2/5 * a^3 - 1/5 * a^2 - 4/15 * a + 13/15 : 1)
```

Sage can tell us exactly where a lies and give us the minimal polynomial over $\mathbf{Q}$.

```
sage:  P[0].parent()

Number Field in a with defining polynomial x^6 + x^5 + 6*x^4 - 3*x^3 + 10*x^2 + 8
```

We can check that this polynomial is reducible in $K[X]$, and in fact splits into two cubic factors:

```
sage:  x=PolynomialRing(K,"x").gen()

sage : f = x^6 + x^5 + 6*x^4 - 3*x^3 + 10*x^2 + 8

sage : f.is_irreducible()

False

sage:  f.factor()

(x^3 + (-1/2*alpha + 1/2)*x^2 - 1/2*alpha - 3/2)*

(x^3 + (1/2*alpha + 1/2)*x^2 + 1/2*alpha - 3/2)
```

Picking the factor g of which a is a root, we can define, in Sage, the relative extension H/K where H is a root g. This will be a cubic extension of K and since the class group of K has order 3 (as we'll see), this means that the field H constructed is indeed the Hilbert class-field.

```
sage : g = x^3 + (-1/2*alpha + 1/2)*x^2 - 1/2*alpha - 3/2

sage:  g.subs(x=a)

0

sage:  H.<a>=K.extension(g)

sage : K.class_group().order()

3
```

Now, we can factor g is $H[X]$ to find the conjugates of a over K

```
sage:  y=PolynomialRing(H,"y").gen()

sage : (y^3 + (-1/2*alpha + 1/2)*y^2 - 1/2*alpha - 3/2).factor()

(y - a)*(y + (-1/12*alpha - 1/12)*a^2 + (-1/6*alpha - 1/6)*a - 1/3*alpha - 1/3)*
```

(y + (1/12 * alpha + 1/12) * a^2 + (1/6 * alpha + 7/6) * a - 1/6 * alpha + 5/6)

From this, we see that the conjugates of a over K are

$$a, \frac{\alpha+1}{12}a^2 + \frac{\alpha+1}{6}a + \frac{\alpha+1}{3}, \ -\frac{\alpha+1}{12}a^2 - \frac{\alpha+7}{6} + \frac{\alpha-5}{6}$$

With this data, we can construct the elliptic curve over H and compute the trace

```
sage : b = -((-1/12 * alpha - 1/12) * a^2 + (-1/6 * alpha - 1/6) * a - 1/3 * alpha - 1/3)
```

```
sage : c = -((1/12 * alpha + 1/12) * a^2 + (1/6 * alpha + 7/6) * a - 1/6 * alpha + 5/6)
```

```
sage : S = [a, b, c]
```

```
sage:  EH=EllipticCurve(H,[0,1])
```

```
sage:  T=[EH(i, 2/15 * i^5 + 1/5 * i^4 + 2/5 * i^3 - 1/5 * i^2 - 4/15 * i + 13/15) for i in
S]
```

```
sage:  PK=sum(Q for Q in T)
```

```
sage:  PK
```

```
(-1/8*alpha + 5/8 :  -1/16*alpha + 13/16 :  1)
```

We see immediately that P_K does indeed lie in $E(K)$, and we can check that P_K has infinite order.

```
sage : PK.has_finite_order()
```

```
False
```

From this point P_K, we can construct a point on $E(\mathbf{Q})$ be taking the trace from K to $\mathbf{Q}$. However, we see that this construction leads to a torsion point:

```
sage:  PKconj=EK(-1/8 * alpha.conjugate() + 5/8, -1/16 * alpha.conjugate() + 13/16)
```

```
sage : Q = PK + PKconj
```

```
sage:  Q
```

```
(-1 : 0 : 1)
```

This allows us to conclude that $E(\mathbf{Q})$ is a torsion group. Indeed, what we saw above was that $P_K + P_K^\tau$ is torsion. Now suppose E had a rational point Q of infinite order. Since $E(\mathbf{Q}) \subseteq E(K)$ and $E(K)$ has rank 1, it follows that there are integers n, m such that the

following equation holds

$$nQ = mP_K \bmod E(K)_{tors}$$

Since τ acts trivially on the left-hand side, we find that

$$\begin{aligned} mP_K &= mP_K^\tau \\ &= -mP_K \bmod E(K)_{tors}, \end{aligned}$$

from which it follows that $2mP_K$ is torsion, which cannot possibly be the case. It follows that $E(\mathbf{Q})$ is a torsion group, so that the rank portion of the Birch and Swinnerton- Dyer conjecture holds for this curve.

Example 4.4.2 (An Elliptic Curve with $\mathrm{ord}_{s=1} L(E,s) = 1$). Next, let us take an elliptic curve with analytic rank 1. We see that the elliptic curve defined by

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

is such a curve.

```
sage: E=EllipticCurve([3,0])

sage: E

Elliptic Curve defined by y^2 = x^3 + 3*x over Rational Field

sage: L=E.lseries()

sage: L(1)

0.000000000000000

sage : L.deriv_at1()

(1.41211481653694, 0.00824491199346881)
```

Our goal this time is to prove that the algebraic rank of $E/\mathbf{Q}$ is equal to one. Once again, we wish to use the theorems of Gross-Zagier and Kolyvagin, so our strategy will be to examine what happens if we pick a suitable quadratic imaginary field K; that is, one that satisfies the Heegner hypothesis with respect to E and such that $\mathrm{ord}_{s=1} L(E/K,s) = 1$.

```
sage: E.conductor().factor()

2^5 * 3^2

sage : E.heegner_discriminants(50)
```

$[-23, -47]$

Since the primes dividing the conductor are the same as in the earlier example, we expected this same list. We will see if the field $K = \mathbf{Q}(\sqrt{-47})$ will work for our purposes

```
sage : E2 = E.quadratic_twist(−47)

sage:  L2=E2.lseries()

sage:  L2(1)

3.28789517160128
```

We see that the twisted L-function $L(E_{-47}, s)$ is non-zero at $s = 1$ so that, with $K = \mathbf{Q}(\sqrt{-47})$, we have $\mathrm{ord}_{s=1} L(E/K, s) = 1$. Once again, it follows that if we construct the heegner point P_K, we obtain a point of infinite order that generates a finite-index subgroup of $E(K)$. Let us verify this:

```
sage : P = E.heegner_point(−47)

sage : P.point_exact()

(a : a^4 − 4 ∗ a^3 + 5 ∗ a^2 − 4 ∗ a : 1)

sage : P.point_exact()[0].parent()

Number Field in a with defining polynomial x^5 − 4 ∗ x^4 + 7 ∗ x^3 − 8 ∗ x^2 + 4 ∗ x − 1
```

We construct the field K and the field H. We verify first that the field extension of K by the above polynomial is indeed the Hilbert class-field.

```
sage:  K.<alpha>=QuadraticField(-47)

sage : K.class_group().order()

5

sage:  H.<a>=K.extension(x^5 − 4 ∗ x^4 + 7 ∗ x^3 − 8 ∗ x^2 + 4 ∗ x − 1)
```

Since $a \in H$, it follows that H as constructed above is the Hilbert class-field of K. Unlike in the above example, the minimal polynomial for a is irreducible over K. This allows us to find the conjugates of a a little more easily this time.

```
sage : conj1 = a.galois_conjugates(H)

sage : a.galois_conjugates(H)
```

$[(-8/47 * \texttt{alpha} - 1) * \texttt{a}^4 + (55/94 * \texttt{alpha} + 7/2) * \texttt{a}^3 + (-37/47 * \texttt{alpha} - 5) * \texttt{a}^2$

$+(69/94 * \texttt{alpha} + 9/2) * \texttt{a} - 6/47 * \texttt{alpha},$

$(-3/47 * \texttt{alpha} + 1) * \texttt{a}^4 + (21/94 * \texttt{alpha} - 7/2) * \texttt{a}^3 + (-16/47 * \texttt{alpha} + 5) * \texttt{a}^2$

$+(11/47 * \texttt{alpha} - 5) * \texttt{a} + 2,$

$\texttt{a},$

$(3/47 * \texttt{alpha} + 1) * \texttt{a}^4 + (-21/94 * \texttt{alpha} - 7/2) * \texttt{a}^3 + (16/47 * \texttt{alpha} + 5) * \texttt{a}^2$

$+(-11/47 * \texttt{alpha} - 5) * \texttt{a} + 2,$

$(8/47 * \texttt{alpha} - 1) * \texttt{a}^4 + (-55/94 * \texttt{alpha} + 7/2) * \texttt{a}^3 + (37/47 * \texttt{alpha} - 5) * \texttt{a}^2$

$+(-69/94 * \texttt{alpha} + 9/2) * \texttt{a} + 6/47 * \texttt{alpha}]$

With the conjugates in our hands, we now construct the curve over the field H and compute the trace exactly as we did previously.

```
sage:  EH=EllipticCurve(H,[3,0])
```

```
sage:  T = [EH(i, i^4 - 4*i^3 + 5*i^2 - 4*i) for i in conj1]
```

```
sage:  Q=sum(b for b in T)
```

```
sage:  Q
```

$(1/4 : -7/8 : 1)$

So, we find that P_K is a rational point! Now we verify that P_K has infinite order

```
sage:  Q.height()
```

```
2.00472956818871
```

It follows that P_K is a point of infinite order, as expected, so that $E(\mathbf{Q})$ has algebraic rank at least one. Since we know $E(K)$ has rank one, it follows that $E(\mathbf{Q})$ has rank 1, which verifies the rank portion of the Birch and Swinnerton-Dyer conjecture for this elliptic curve.

Note that in both examples above, we were able to prove that the rank of $E(\mathbf{Q})$ was 0 or 1 by examining the point P_K; in the first example $P_K \notin E(\mathbf{Q})$, while for the second example, $P_K \in E(\mathbf{Q})$. P_K was guaranteed to be a point of infinite order by Kolyvagin's theorem and the fact that P_K did or did not belong to $E(\mathbf{Q})$ was a direct consequence of whether the analytic rank was 0 or 1. That is, the above examples show us that the algebraic ranks were

what they were *because* the analytic ranks were what they were; there is much more going on here than simply computing the analytic rank and algebraic rank separately and seeing that they are, in fact, the same. What we observed above will allows us to explain most of the proof of the Gross-Zagier-Kolyvagin theorem.

4.5. **The Gross-Zagier-Kolyvagin Theorem.** With the two examples above under our belt, we set out to see why the following theorem is true

Theorem 4.5.1. *[Gross-Zagier-Kolyvagin] Let $E/\mathbf{Q}$ be an Elliptic curve over $\mathbf{Q}$. If*

$$\mathrm{ord}_{s=1} L(E,s) \leq 1,$$

then $\mathrm{rank}(E(\mathbf{Q})) = \mathrm{ord}_{s=1} L(E,s)$ *and* $Ш(E/\mathbf{Q})$ *is finite.*

Before sketching the proof of this theorem, we need two lemmas. The first one describes how complex conjugations act on the Heegner points and generalizes the observations we made in the examples above. The second gives a description of the sign appearing in the functional equation for $L(E/K,s)$, where K is a quadratic field satisfying the Heegner hypothesis.

Lemma 4.5.2. *Let x_n be a Heegner point of conductor n on $X_0(N)$ and y_n its image under the modular parameterization. If τ denotes a complex conjugation in* $\mathrm{Gal}(H_n/\mathbf{Q})$*, we have*

$$y_n^\tau = -sign(E/\mathbf{Q}) y_n^\sigma + T,$$

for some $\sigma \in \mathrm{Gal}(H_n/K)$ and $T \in E(H_n)_{tors}$.

Proof. We observed at the end of section 3.1 that if w_N denotes the Fricke involution, we have

$$x_n^\tau = w_N(x_n^\sigma),$$

for some $\sigma \in \mathrm{Gal}(H_n/K)$. Since the cusp ∞ is rational, it follows that

$$(x_n - \infty)^\tau = w_N(x_n - \infty)^\sigma + (w_N(\infty) - \infty) = w_N(x_n - \infty)^\sigma + (0 - \infty),$$

using the fact that w_N interchanges 0 and ∞. Next, we note that $(0-\infty)$ is torsion in the Jacobian of $X_0(N)$ (consider the divisor of $\frac{\Delta(\tau)}{\Delta(N\tau)}$), and that $w_N(x_n - \infty)$ is mapped to $-sign(E/\mathbf{Q})y_n$ under the modular parameterization, whence the result.

The following theorem allows to give a description of the sign appearing in the functional function for $L(E/K,s)$ when K satisfies the Heegner hypothesis. It is a consequence of work by Jaquet and Rohrlich [10] [11].

Theorem 4.5.3. *Suppose $E/\mathbf{Q}$ is an elliptic curve and K is a quadratic field. Then*

$$sign(E/K) = (-1)^{|S_{E,K}|},$$

where $S_{E,K}$ is the set of places of K which are archimedean or at which E has split-multiplicative reduction.

In the case that K is a quadratic imaginary field satisfying the Heegner hypothesis, then $S_{E,K}$ has an odd number of places. Indeed, there is a single archimedean place and, since the

primes dividing N are split in K, the places λ at which E has split-multiplicative reduction come in pairs, whence the result. It follows that, if K satisfies the Heegner hypothesis, we have $sign(E/K) = -1$.

We now have everything we need to describe the proof of the Gross-Zagier-Kolyvagin theorem.

Sketch of Proof of Theorem 4.5.1. Suppose that $E/\mathbf{Q}$ is an elliptic curve and suppose

$$\mathrm{ord}_{s=1} L(E, s) \leq 1.$$

It follows that the sign that appears in its functional equation, $sign(E/\mathbf{Q})$, is sufficient to determine this order; if $sign(E/\mathbf{Q}) = -1$, then $L(E, s)$ must vanish at $s = 1$, from which it follows that $\mathrm{ord}_{s=1} L(E, s) = 1$. On the other hand, if $sign(E/\mathbf{Q}) = 1$, then the order of vanishing at $s = 1$ must be even, from which we see that $\mathrm{ord}_{s=1} L(E, s) = 0$.

We want to use the results of Gross-Zagier and Kolyvagin, so we need to find a suitable quadratic imaginary field K to proceed. That is, we seek a quadratic imaginary field K that satisfies the Heegner hypothesis with respect to E and such that $\mathrm{ord}_{s=1} L(E/K, s) = 1$. If we first assume that $sign(E/\mathbf{Q}) = -1$, then a result of [12] tells us that there infinitely many quadratic Dirichlet characters χ that satisfy the following three conditions:

- $\chi(\ell) = 1$ for all $\ell \nmid N$;
- $\chi(-1) = -1$;
- $L(E, \chi, 1) \neq 0$

The first two properties tell us that the corresponding quadratic field K is imaginary, and satisfies the Heegner Hypothesis. The last property tells us that $\mathrm{ord}_{s=1} L(E, \chi, s) = 0$, so that $\mathrm{ord}_{s=1} L(E/K, s) = 1$ since $L(E/K, s) = L(E, s)L(E, \chi, s)$.

On the other hand, if $sign(E/\mathbf{Q}) = 1$, there are analytic results of [14] and [15] that insure that we can find a quadratic Dirichlet character χ satisfying the first two properties above, together with the property that $L'(E, \chi, 1) \neq 0$. Note that if χ satisfies the first two properties, then $L(E, \chi, 1) = 0$ since $L(E/K, s) = L(E, s)L(E, \chi, s)$, together with the fact that $L(E/K, s)$ vanishes to an odd order and $\mathrm{ord}_{s=1} L(E, s) = 0$. It follows that $\mathrm{ord}_{s=1} L(E, K) = 1$ if K is the associated quadratic field.

So, regardless of the sign, we can find a suitable quadratic character χ such that the field K corresponding to χ satisfies the Heegner hypothesis with respect to E and $\mathrm{ord}_{s=1} L(E/K, s) = 1$. Now let $P_K \in E(K)$ be the trace of the Heegner point $(\mathcal{O}, \mathfrak{n}, [1])$, as defined earlier above. Since $L'(E/K, 1) \neq 0$, the Gross-Zagier formula tells us that P_K is not torsion. Next, Kolyvagin's theorem tells us that the algebraic rank of $E(K)$ is exacty 1 and that the group $Ш(E/K)$ is finite.

To finish the proof, we observe that, by lemma 4.5.2, $P_K \in E(\mathbf{Q}) \bmod E(H)_{tors}$ if and only if $sign(E/\mathbf{Q}) = -1$. If $sign(E/\mathbf{Q}) = -1$, then after replacing P_K by $P_K + T$ for some $T \in E(H)_{tors}$, we have produced a point of infinite order in $E(\mathbf{Q})$, so that the algebraic rank

is equal to 1, as predicted by the Birch and Swinnerton-Dyer conjecture. On the other hand, if $sign(E/\mathbf{Q}) = 1$, then $E(\mathbf{Q})$ has no point of infinite order. Indeed, suppose that $Q \in E(\mathbf{Q})$ were a point of infinite order. Then, we see that

$$mQ = nP_K + T$$

for some integers m, n and $T \in E(K)_{tors}$. Letting complex conjugation act, and using lemma 4.5.2, we find that

$$nP_K + T = -nP_K + T^\tau,$$

from which it follows that

$$2nP_K = T^\tau - T,$$

so that P_K is a point of finite order, contradicting the Gross-Zagier formula. It follows that $E(\mathbf{Q})$ is a torsion group, which agrees with the Birch and Swinnerton-Dyer conjecture once more.

Lastly, it is not hard to see that the finiteness of $Ш(E/K)$ readily implies the finiteness of $Ш(E/\mathbf{Q})$, which completes (the sketch of) the proof of the Gross-Zagier-Kolyvagin Theorem.

5. Conclusion

We have seen the role played by Heegner points in arithmetic in two fascinating ways: the first being their connection to Hilbert's twelfth problem, and the second being their use in proving a portion of the Birch and Swinnerton-Dyer conjecture.

Evidence was given to support the claim that the relationship between the Heegner points and the class-fields they generate is one that transcends the particular choice of modular function used to express it. While the classical theory uses the j-function and Heegner points on $X_0(1)$, our evidence suggests that this relationship can be found in the modular curves $X_0(N)$ and their hauptmoduln when $X_0(N)$ has genus zero, and we suspect that such a relationship should exist even when $X_0(N)$ has positive genus.

As far as being able to extend the results discussed in this thesis, Darmon has proposed a conjectural construction that can be found in [4] of so-called Stark-Heegner points on Shimura curves that, if true, would provide points on elliptic curves over totally real fields that would play a similar role as Heegner points in the quadratic imaginary case. It is hoped that this might shed light on the Birch and Swinnerton-Dyer conjecture for such curves, as well as Hilbert's twelfth problem for totally real fields.

References

[1] Joseph Silverman *The Arithmetic of Elliptic Curves* Graduate Texts in Mathematics Springer-Verlag, 1984

[2] Joseph Silverman *Advanced Topics in the Arithmetic of Elliptic Curves* Graduate Texts in Mathematics Springer-Verlag, 1994

[3] Goro Shimura *Introduction to the Arithmetic Theory of Automorphic Functions* Princeton University Press, 1971

[4] Henri Darmon *Rational Points on Modular Elliptic Curves* Regional Conference Series in Mathematics AMS, 2004
[5] Fred Diamond and Jerry Shurman *A First Course in Modular Forms* Graduate Texts in Mathematics Springer-Verlag, 2005
[6] Jürgen Neukirch *Algebraic Number Theory* A Series of Comprehensive Studies in Mathematics Springer-Verlag, 1999
[7] Theodor Schneider *Introduction aux Nombres Transcendents* Grund. der Math. Wiss 81, Springer Verlag, 1957.
[8] Benedict Gross *Heegner Points on $X_0(N)$* Modular Forms (Durham, 1983), pg. 87-105 Horwood, Chichester, 1984
[9] Benedict Gross , Donald Zagier *Heegner Points and Derivatives of L-series* Invent. math, 84 no. 2, 225-320, 1986
[10] Hervé Jacquet *Automorphic Forms on* GL(2) Part II. Lecture Notes in Mathematics 278 Springer-Verlag, 1972
[11] David Rohrlich *Galois Theory, Elliptic Curves, and Root Numbers* Compositio Math. 100 no. 3, 311-349, 1996
[12] J. L. Waldspurger *Sur les valeurs de certaines fonctions L autotrophes en leur centre de symétrie* Compositio Math. 54, no. 2, 173-242, 1985
[13] Emile Artin *Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren* Abh. Math. Sem. University of Hamburg no. 8, 292-306, 1930
[14] Maruti Murty, Vijaya Murty *Mean Values of Derivatives of Modular L-series* Annals of Math 133, no. 3, 447-475
[15] Daniel Bump, Solomon Friedberg, Jeffrey Hoffstein *Eisentein Series on the Metaplectic Group and Nonvanishing Theorems for Automorphic L-function and their Derivatives* Annals of Math. 131, no. 1, 53-127, 1990
[16] Robert Maier *On Rationally Paramaterized Modular Equations* J. Ramanujan Math. Soc. 24 (2009), 1-73
[17] David Cox, John McKay, and Peter Stevenhagen *Principal Moduli and Class Fields* Bull. London Math. Soc. 36 (2004) 3-12