Heegner Points and the Shimura Correspondence: Finding rational points on elliptic curves of rank 1

Haakma, E.

Heegner Points and the Shimura Correspondence

Finding rational points on elliptic curves of rank 1

Emiel Haakma

Universiteit Leiden

A thesis presented for the degree of
Master of Mathematics.

Supervised by dr. J.B. Vonk.
Mathematical Institute
Leiden University
The Netherlands
May 5th, 2021

Preface

This paper will discuss Heegner Points, which is a class of rational points on elliptic curves of rank 1. The first chapter will discuss the major motivation behind defining this class, namely the Birch and Swinnerton-Dyer conjecture. Heegner Points have been used to prove specific cases of this conjecture, so we will discuss it in depth, going over every step to make sure each symbol within it makes sense. Then, in the second chapter, we will define Heegner Points. For this, we will first need to discuss several terms from class field theory. In addition, we discuss a few results that show that Heegner Points are indeed as useful as we claim. And finally, in the third chapter, we will consider Shimura Correspondence, as Heegner Points prove useful for computation of specific cases of this correspondence.

As this paper works extensively with elliptic curves and modular forms, it is important that the reader has experience in these subjects. In addition, some experience in Galois theory and class field theory is useful. While certain definitions, such as those of modularity and L-functions, will be given here, overall it is expected that the reader is familiar with most. To grow familiar with these subjects, textbooks such as [SVM] are useful.

Throughout this paper, we will focus on one specific example of an elliptic curve. This curve is defined as

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

It has conductor 89 and algebraic rank 1, and its simple equation and prime conductor allow us to simplify many of our calculations. We hope to clarify the theory by applying it to this specific example.

Contents

1 Birch and Swinnerton-Dyer Conjecture

It was the early 1960s when mathematicians Bryan Birch and Peter Swinnerton-Dyer were using numerical methods to calculate $\#E(\mathbb{F}_p)$, i.e. the number of points of E over the finite field $\mathbb{F}_p$, for different elliptic curves E with known algebraic ranks and various prime numbers p. Over time, the two began to notice a pattern, and in 1965 they conjectured in [BSD] that

$$\prod_{p \leq P} \frac{\#E(\mathbb{F}_p)}{p} \sim C(\log P)^g$$

as $P \to \infty$, where g is the rank of the elliptic curve E and C is some constant.
They noticed quickly that the expression on the left-hand side of this equation converges to the value of the L-function of the elliptic curve at $s = 1$, and this soon led them to the most well-known statement of the Birch and Swinnerton-Dyer Conjecture:

Conjecture 1 (Weak Birch and Swinnerton-Dyer)**.**
The analytic rank of $L(E, s)$ at $s = 1$ is equal to the algebraic rank of E.

As the right-hand side of the equation was analyzed further by people such as John Tate Jr., Igor Shafarevich, John Cassels, and Andrew Wiles, a stronger version of the conjecture was stated in [TAT65]:

Conjecture 2 (Strong Birch and Swinnerton-Dyer)**.**

$$\frac{L^{(r)}(E, s)}{r!} = \frac{\#Ш_{E/\mathbb{Q}} R_\infty \omega_\infty \prod_{p|2N} \omega_p}{E(\mathbb{Q})^{tors}} \tag{1}$$

In the above notation, the left-hand side is the first non-zero coefficient in the Taylor series expansion of the L-function around $s = 1$, while the right-hand side contains a variety of constants that depend only on the elliptic curve. In the rest of this chapter, we will discuss this statement and what exactly it means: in section 1.1, we will discuss the L-function and the modularity of elliptic curves, in section 1.2 we will discuss the various curve constants to understand the right-hand side of the conjecture, and in section 1.3 we will discuss special cases of the BSD Conjecture that have been proven and which options we have to potentially reach a full proof.

1.1 L-functions and Modularity

1.1.1 Definition of L-functions

To begin, let us quickly go through the definition of the L-function of an elliptic curve. First, define

$$a_p := p + 1 - \#E(\mathbb{F}_p)$$

$$L_p(s) := \begin{cases} (1 - a_p p^{-s} + p \cdot p^{-2s})^{-1} & \text{if } E \text{ has good reduction modulo } p \\ (1 - p^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction modulo } p \\ (1 + p^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction modulo } p \\ 1 & \text{if } E \text{ has additive reduction modulo } p \end{cases}$$

for prime numbers p.
Then, we have

$$L(E, s) = \prod_{p \text{ prime}} L_p(s)$$

For the elliptic curve $E : y^2 + xy + y = x^3 + x^2 - x$ defined in the preface, this gives us the following L-function:

$$L(E,s) = \prod_{\substack{p \text{ prime} \\ p \neq 89}} \frac{1}{1 + \frac{a_p}{p^s} + \frac{p}{p^{2s}}} \cdot \frac{1}{1 + \frac{1}{89^s}}$$

Now, we can multiply the L-function out to get a Dirichlet series, i.e. of the form $L(E,s) = \sum_{n \geq 1} \frac{a_n}{n^s}$. We can calculate the values of these a_n and see that, as our notation suggests, $a_p = p + 1 - \#E(\mathbb{F}_p)$ for p a prime where E has good reduction. If we go through the calculations for our E, the following table lists the first few a_n:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_n	1	-6	-8	34	-12	48	-19	-192	61	72	-25	-272	-25	114	96

Using the Hasse-Weil bound, which states that $|a_p| \leq 2\sqrt{p}$ in the case of elliptic curves, we can see that $a_n = \mathcal{O}(p^{1/2})$. Thus, we get that $L(E,s)$ converges for all s with $\mathrm{Re}(s) > \frac{3}{2}$. However, the BSD conjecture talks about the value of the L function at $s = 1$. We must thus find an analytic continuation: to do so, let us discuss modularity of elliptic curves.

There is a very well known theorem, known as the modularity theorem:

Theorem 1 (Modularity)**.**
For any elliptic curve E with conductor N, there is an $f \in S_2(\Gamma_0(N))$ such that $L(E,s) = L(f,s)$.

This theorem was formerly known as the Taniyama-Shimura-Weil conjecture and its proof was done over many years through cooperation between many mathematicians, such as Andrew Wiles, Christophe Breuil, and Fred Diamond, and it goes beyond the scope of this paper. If the reader does desire a full proof, it can be found in [WIL95] and [TW], with further exploration in [BCDT].
However, while we will not prove the Modularity Theorem in general, we can prove it holds for our specific curve E.

1.1.2 Modularity of E

Recall that we have defined E as the elliptic curve defined by the equation $y^2 + xy + y = x^3 + x^2 - x$ and that it has conductor 89. We can apply the transformation $y_1 = 2y + x + 1$ to find the equivalent equation $y_1^2 = 4x^3 + 5x^2 - 2x + 1$.
We consider the group Γ, which is generated by $\Gamma_0(89)$ and

$$w_{89} = \begin{pmatrix} 0 & \frac{-1}{\sqrt{89}} \\ \sqrt{89} & 0 \end{pmatrix}$$

We claim there is an isomorphism $\mathbb{H}/\Gamma \cup \{\infty\} \cong E(\mathbb{C})$, where $\mathbb{H}$ is the complex upper half plane. More specifically, we will find an isomorphism

$$\phi : \mathbb{H}/\Gamma \cup \{\infty\} \to E(\mathbb{C})$$

with $\phi^*(\frac{dx}{y_1}) = 2\pi i f(t)dt$, where f is the unique, normalized cusp form of weight 2 with integer coefficients in the q-expansion. We can calculate

$$f = q - q^2 - q^3 - q^4 - q^5 + q^6 - 4q^7 + 3q^8 - 2q^9 + \mathcal{O}(q^{10})$$

Now, we will define ϕ via two holomorphic, Γ-invariant functions ξ and η, such that for all $\tau \in \mathbb{H}/\Gamma$, $\phi(\tau) = (\xi(\tau), \eta(\tau)) \in E(\mathbb{C})$. Using the curve equation for E as well as the requirement $\phi^*(\frac{dx}{y_1}) = 2\pi i f(t)dt$ with $y_1 = 2y + x + 1$, we see that the following equalities hold:

$$\eta(\tau)^2 + \xi(\tau)\eta(\tau) + \eta(\tau) = \xi(\tau)^3 + \xi(\tau)^2 - \xi(\tau)$$
$$\frac{\xi'(\tau)}{2\eta(\tau) + \xi(\tau) + 1} = 2\pi i f(\tau)$$

Using these two equations, we can think about the orders of the poles of ξ and η at ∞. First of all, from the curve equation, we see that η^2 and ξ^3 must have a pole of same order at ∞. In addition, since f is a cusp form and thus does not have a pole at ∞, we must also have that ξ' and η have the same order pole at ∞. The order of the pole of ξ' is one higher than the one of ξ, so η has a pole of order one higher than ξ. This now gives us that ξ and η must have poles of 2 and 3 respectively at ∞. In other words, their first non-zero coefficients in the Fourier expansion are at q^{-2} and q^{-3} respectively. Using this information, and assuming ξ and η exist as we need them, we can recursively determine their first few Fourier coefficients:

$$\xi = q^{-2} + q^{-1} + 1 + 2q + 3q^2 + 3q^3 + 5q^4 + 6q^5 + 8q^6 + 10q^7 + \mathcal{O}(q^8)$$
$$\eta = -q^{-3} - 2q^{-2} - 3q^{-1} - 5 - 7q - 10q^2 - 15q^3 - 20q^4 - 28q^5 - 38q^6 - 52q^7 + \mathcal{O}(q^8)$$

Let us now continue to assume ξ and η exist as we need them. Then, as they are both Γ-invariant and f is a cusp form of weight 2, we can define $f_4 = f^2\xi$ and $f_6 = f^3\eta$ as modular forms of weight 2; they are holomorphic at infinity, since the constant term is the lowest-order term in the q-expansion of both. Then we also have $\xi = \frac{f_4}{f^2}$ and $\eta = \frac{f_6}{f^3}$, which means we can substitute this into the equations we have for ξ and η, giving us

$$f_6^2 + f_4 f_6 f + f_6 f^3 = f_4^3 + f_4^2 f^2 + f_4 f^4$$
$$f(2f_6 + f f_4 + f^3) = 2f_4 f' - f f_4'$$

after some rewriting. But now we can turn it around: if we were to find f_4 and f_6 that satisfy the above equations, we can divide them by powers of f to find our ξ and η. But these equations are simply equalities of modular forms of weight 12, which we can solve by simply checking finitely many coefficients and computing bases for $M_4(\Gamma)$ and $M_6(\Gamma)$, as these vector spaces are known to be finitely dimensional. Thus, we find our ξ and η, and we have proven the modularity of E, as it is now isomorphic to an elliptic curve we know is modular.

1.1.3 Analytic Continuation of L(E, s)

With the proof of the modularity of E, our next goal will be to find an analytic continuation for the L-function of E. Writing f for the modular form associated to E once again, we have $L(E,s) = L(f,s) = \sum_{n\geq 1} b_n n^{-s}$ where the b_n are the coefficients of the q-expansion of f. We will now define

$$\Lambda(E,s) := \frac{\sqrt{89}^s \Gamma(s)}{(2\pi)^s} L(E,s)$$

At first glance, this definition will seem strange, but we do it because it has an easily discoverable integral representation, using the q-expansion of f:

$$\begin{aligned}
\int_0^\infty f\left(\frac{it}{\sqrt{89}}\right) t^s \frac{dt}{t} &= \int_0^\infty \sum_{n\geq 1} b_n e^{2n\pi i \frac{it}{\sqrt{89}}} t^s \frac{dt}{t} \\
&= \sum_{n\geq 1} b_n \int_0^\infty e^{-\frac{2\pi nt}{\sqrt{89}}} t^s \frac{dt}{t} \\
&= \left(\frac{\sqrt{89}}{2\pi}\right)^s \sum_{n\geq 1} b_n n^{-s} \int_0^\infty e^{-v} v^s \frac{dv}{v} \\
&= \left(\frac{\sqrt{89}}{2\pi}\right)^s \cdot L(f,s) \cdot \Gamma(s) \\
&= \Lambda(E,s)
\end{aligned}$$

where we write $v = \frac{2\pi nt}{\sqrt{89}}$. We will now use this expression to prove that $\Lambda(E,s)$, and thus $L(E,s)$, has an analytic continuation to all of $\mathbb{C}$. To do so, we must take a closer look at the expression $f(\frac{it}{\sqrt{89}})$ in the

integral representation of $\Lambda(E,s)$. Recall that f is a cusp form of weight 2 over Γ, where Γ contains w_{89}. Thus, for all $\tau \in \mathbb{H}$, we have

$$\begin{aligned} f(w_{89}\tau) &= (\sqrt{89}\tau)^2 \cdot f(\tau) \\ &= 89\tau^2 \cdot f(\tau) \end{aligned}$$

and $w_{89}\tau = -\frac{1}{89\tau} = -\frac{1}{89}\tau^{-1}$. Thus, we can rewrite:

$$f\left(\frac{it^{-1}}{\sqrt{89}}\right) = f\left(-\frac{1}{89}\cdot\frac{\sqrt{89}}{it}\right) = f\left(w_{89}\frac{it}{\sqrt{89}}\right) = 89\cdot\left(\frac{it}{\sqrt{89}}\right)^2 \cdot f\left(\frac{it}{\sqrt{89}}\right) = -t^2 \cdot f\left(\frac{it}{\sqrt{89}}\right)$$

Using this equality, we can rewrite the integral to find out analytic continuation:

$$\begin{aligned} \Lambda(E,s) &= \int_0^\infty f\left(\frac{it}{\sqrt{89}}\right) t^s \frac{dt}{t} \\ &= \int_0^1 f\left(\frac{it}{\sqrt{89}}\right) t^s \frac{dt}{t} + \int_1^\infty f\left(\frac{it}{\sqrt{89}}\right) t^s \frac{dt}{t} \\ &= \int_\infty^1 f\left(\frac{it^{-1}}{\sqrt{89}}\right) t^{-s} \frac{-t^{-2}dt}{t^{-1}} + \int_1^\infty f\left(\frac{it}{\sqrt{89}}\right) t^s \frac{dt}{t} \\ &= -\int_1^\infty -t^2 \cdot f\left(\frac{it}{\sqrt{89}}\right) t^{-s} \frac{dt}{-t} + \int_1^\infty f\left(\frac{it}{\sqrt{89}}\right) t^s \frac{dt}{t} \\ &= -\int_1^\infty f\left(\frac{it}{\sqrt{89}}\right) t^{2-s} \frac{dt}{t} + \int_1^\infty f\left(\frac{it}{\sqrt{89}}\right) t^s \frac{dt}{t} \\ &= \int_1^\infty f\left(\frac{it}{\sqrt{89}}\right) (t^s - t^{2-s}) \frac{dt}{t} \end{aligned}$$

This final result is an analytic function on all of $\mathbb{C}$, so we have found an analytic continuation. In addition to that, we can now set up a functional equation, as we can easily read from this final description that $\Lambda(E,s) = -\Lambda(E,2-s)$. But then, in particular. $\Lambda(E,1) = -\Lambda(E,1)$, so $\Lambda(E,1) = 0$, which immediately implies $L(E,1) = 0$. Thus, we have proven that $L(E,s)$ has a zero at $s = 1$.
Finally, to conclude this subsection, let us prove $L'(E,1) \neq 0$. For this, we once again consider $\Lambda(E,s)$, and specifically its derivative at $s = 1$, which we can find since we have proven it is analytic. In fact, the integrand of its integral representation is analytic, so we can switch order of derivation and integration to find

$$\Lambda'(E,s) = \int_1^\infty \frac{i}{\sqrt{89}} \cdot f'\left(\frac{it}{\sqrt{89}}\right)(t^s - t^{2-s}) + f\left(\frac{it}{\sqrt{89}}\right) \cdot \log(t) \cdot (t^s + t^{2-s}) \frac{dt}{t}$$

Clearly, the first term of the integrand vanishes at $s = 1$, so we have

$$\Lambda'(E,1) = 2\int_1^\infty f\left(\frac{it}{\sqrt{89}}\right) \log(t) dt \approx 0.46731... \neq 0$$

Finally, note that $\Lambda'(E,1) = \frac{\sqrt{89}\Gamma(1)}{2\pi} L'(E,1)$; after all, if we use the product rule, all other terms vanish at $s = 1$, since we have proven that $L(E,1) = 0$. Thus, $L'(E,1) \neq 0$. Thus, we can conclude that the analytic rank of $L(E,s)$ at $s = 1$ is equal to 1. This is equal to the algebraic rank of E, as predicted by the Weak BSD Conjecture. In fact, since $\Gamma(1) = 1$, we can now calculate the left-hand side of (1):

$$L'(E,1) = \frac{2\pi}{\sqrt{89}} \Lambda'(E,1) \approx 0.62247...$$

In the next section, we will prove that this is indeed equal to the right-hand side.

1.2 Curve Constants

In this section, we will take a close look at the right-hand side of the strong BSD Conjecture. It contains a variety of curve-dependent constants, and we will define them and calculate them for our curve E.

1.2.1 The Tate-Shafarevich group

To begin, let us consider the symbol $\#Ш_{E/\mathbb{Q}}$. This is the order of the Tate-Shafarevich group, and is the most difficult to calculate. First, we will define the Tate-Shafarevich group:

$$Ш_{E/\mathbb{Q}} := \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E_{\mathbb{Q}_p})\right)$$

Here, $G_K := \mathrm{Gal}(\overline{K}/K)$ for all fields K, p runs over all primes as well as infinity, while $\mathbb{Q}_p$ are the places of $\mathbb{Q}$. Finally, the groups $H^1(G_{\mathbb{Q}}, E)$ are the Galois cohomology groups. Note that we restrict our definitions to $\mathbb{Q}$, but it can be extended for elliptic curves defined over any number field.
This definition is hard to work with, which is reflected in our lack of knowledge on this group. As a matter of fact, we are currently unsure whether the group is even finite:

Conjecture 3 (Tate-Shafarevich Conjecture)**.**
For all elliptic curves over $\mathbb{Q}$, the Tate-Shafarevich group is finite.

It should be clear that the strong BSD conjecture implies the Tate-Shafarevich Conjecture, and in [WIL06], Wiles expresses his hope that proving the BSD Conjecture would be a route to prove the finiteness of $Ш_{E/\mathbb{Q}}$ as well.
In 1987, mathematician Karl Rubin proved the Tate-Shafarevich Conjecture for elliptic curves of rank at most 1. His proof uses the theory of complex multiplication, which will not be discussed extensively in this paper, so we instead refer to [RUB, Theorem A].
With this, we can say that at least in the case of our $E : y^2 + xy + y = x^3 + x^2 - x$, we know the Tate-Shafarevich group is finite. In fact, it can be shown to be trivial in this case, giving us $\#Ш_{E/\mathbb{Q}} = 1$. The proof of this will be skipped.

1.2.2 The Regulator and the Torsion Group

We combine the regulator R_∞ and the torsion group order $\#E(\mathbb{Q})^{\mathrm{tors}}$, as together, they describe the Mordell-Weil group $E(\mathbb{Q})$. This group is defined as follows:

$$E(\mathbb{Q}) := \{P \in E(\mathbb{C}) : P \text{ is defined over } \mathbb{Q}\}$$

At first glance, the definition is simple, but discussing the Mordell-Weil group is one of the biggest subjects in elliptic curves right now. There is no general algorithm to determine what this group looks like, meaning it often has to be determined in specific cases. However, thanks to Mordell, we do have the following theorem:

Theorem 2 (Mordell)**.**
For all elliptic curves, the Mordell-Weil group is finitely generated.

The proof of this theorem will not be discussed here, but it can be found in [SVM, chapter VIII].
A direct corollary of this is that the Mordell-Weil group consists of a torsion subgroup $E(\mathbb{Q})^{\mathrm{tors}}$ and a finitely generated subgroup with elements of infinite order. In fact, it is isomorphic to $E(\mathbb{Q})^{\mathrm{tors}} \times \mathbb{Z}^r$, where r is the algebraic rank of the elliptic curve. We will discuss these two subgroups separately.
Let us first recall the definition of the torsion group:

$$E(\mathbb{Q})^{\mathrm{tors}} := \{P \in E(\mathbb{Q}) \mid \exists n \in \mathbb{Z} : nP = \mathcal{O}\}$$

where $\mathcal{O}$ is the point at infinity of E. There are a variety of ways of exploring the torsion group, but one of the most efficient ways is discussed in in [SVM, Chapter VIII.7]. Specifically, we can use the following lemma, which is Corollary 7.2 in [SVM]:

Lemma 1.
Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation $y^2 = x^3 + Ax + B$ for $A, B \in \mathbb{Z}$. Suppose that $P \in E(\mathbb{Q})$ is a non-zero torsion point. Then

(i) Both coordinates of P are integers.

(ii) $2P = \mathcal{O}$ or the y-coördinate of P divides $4A^3 + 27B^2$.

Using the transformation described in [SVM, Chapter III.1], we see that our elliptic curve can be defined with the equation $y^2 = x^3 - 1323x + 28134$ as well as the lemma, we see that there are no points on E that satisfy both conditions, meaning there are no non-trivial torsion points. Thus, we get

$$\#E(\mathbb{Q})^{\text{tors}} = 1$$

Before we get to defining the regulator R_∞, let us quickly review heights of points on elliptic curves. The Weil height of a rational number $\frac{a}{b} \in \mathbb{Q}$ is defined as

$$h\left(\frac{a}{b}\right) = \log(\max\{|a|, |b|\})$$

Now, we can define the canonical height of a point $P \in E(\mathbb{Q})$ as

$$\hat{h}(P) = \lim_{n\to\infty} n^{-2} h(x(nP))$$

This gives a function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ that induces a positive definite quadratic form on $E(K) \otimes \mathbb{R}$. We can also define the height pairing as follows:

$$\langle P, Q\rangle = \frac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q))$$

We will not go into detail on where these definitions come from, as most textbooks on elliptic curves extensively discuss heights. Instead, we will now move to the definition of the regulator. Let r be the algebraic rank of the elliptic curve and $P_1, ..., P_r$ be generators of $E(\mathbb{Q})/E(\mathbb{Q})^{\text{tors}}$. Then the regulator of E is defined as:

$$R_\infty = |\det\left(\langle P_i, P_j\rangle_{1\leq i,j\leq r}\right)|$$

Calculating this value is an easy exercise once the generators of the Mordell-Weil group are known. This is, however, a problem, as we have discussed before. Luckily, we can at least look at certain special cases: if $r = 0$, then we immediately see that $R_\infty = 1$, while if $r = 1$, then the regulator is equal to the canonical height of a generator. This is the case we are in with our chosen elliptic curve. We find that $P = (0 : 0 : 1)$ generates the group $E(\mathbb{Q})/E(\mathbb{Q})^{\text{tors}}$, and we can numerically calculate

$$R_\infty = \hat{h}(0 : 0 : 1) = 0.11210...$$

1.2.3 The Real Period

We know that for all elliptic curves E, there is an isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where Λ is a lattice. We now define the real period as the least positive real element of Λ, multiplied by the number of components of $E(\mathbb{R})$. In other words, it is equal to

$$\omega_\infty := \min(\Lambda \cup \mathbb{R}_{\geq 0}) \cdot n_{\mathbb{R}}$$

where $n_{\mathbb{R}}$ is the number of components of $E(\mathbb{R})$.
It is known that when we define an elliptic curve with a Weierstrass equation, Λ is equal to the period lattice of $\frac{dx}{2y+a_1x+a_3}$. In our case, this differential is

$$\frac{dx}{y_1} = \frac{dx}{\sqrt{4x^3 + 5x^2 - 2x + 1}}$$

In addition, we have that in our case, $n_{\mathbb{R}} = 1$ (which can be intuitively confirmed with a simple sketch). Now, to calculate ω_∞, we must simply calculate the integral

$$\omega_\infty = \int_{E(\mathbb{R})} \frac{dx}{\sqrt{4x^3 + 5x^2 - 2x + 1}}$$

To do so, we must first see what $E(\mathbb{R})$ looks like. Note that, with our description $E : y_1^2 = 4x^3 + 5x^2 - 2x + 1$, we get that every point on $E(\mathbb{R})$ must have an x-coördinate satisfying $4x^3 + 5x^2 - 2x + 1 \geq 0$, and that every such x-coördinate defines two points on $E(\mathbb{R})$. Thus, we now want to find when $4x^3 + 5x^2 - 2x + 1 \geq 0$. We first see that the polynomial has a root at $\alpha = -1.64603...$, and $4x^3 + 5x^2 - 2x + 1 \geq 0$ whenever $x \geq \alpha$. Thus, the integral from before reduces to

$$\omega_\infty = \int_{E(\mathbb{R})} \frac{dx}{\sqrt{4x^3 + 5x^2 - 2x + 1}} = \int_\alpha^\infty \frac{dx}{\sqrt{4x^3 + 5x^2 - 2x + 1}} \approx 5.55262...$$

which we calculate numerically.

1.2.4 The Tamagawa Product

For any elliptic curve, we will define a Tamagawa number ω_p for every prime number p:

$$\omega_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$$

where $E^0(\mathbb{Q}_p)$ is the subgroup of $E(\mathbb{Q}_p)$ containing those points whose reduction modulo p is smooth. We see that if E has smooth reduction at p, then $\omega_p = 1$. The Tamagawa Product is the product of all of these ω_p. We know this is finite, as E has good reduction at all but finitely many primes, meaning that the Tamagawa product reduces to the finite product $\prod_{p|2N} \omega_p$, where N is the conductor of the elliptic curve. To calculate these last, finitely many values in general, John Tate gives an algorithm in [TAT06, Chapter III]. In our case, however, we can use a different method. Our goal will be to prove that $\omega_{89} = 1$, as all others are already 1 immediately. We will consider the description $E : y_1 = 4x^3 + 5x^2 - 2x + 1$ and we will show it contains no points that reduce to a singular point modulo 89. First of all, we see that reducing the curve equation modulo 89 gives

$$E : y_1^2 = 4(x + 9)(x + 74)^2 \bmod 89$$

We will now make the substitution $z = x + 74$ to get the isomorphic curve

$$E' : y_1^2 = 4z^2(z + 24) \bmod 89$$

With this equation, we see immediately that it has a single singular point at $(0, 0)$. Thus, we know that there $[E(\mathbb{Q}_{89}) : E^0(\mathbb{Q}_{89})] = 1$ if and only if there is no point on E' that reduces to $(0, 0)$ modulo 89. To check that, let us look at the equation for E' over $\mathbb{Q}$, which we find by again doing the substitution $z = x + 74$:

$$\begin{aligned} E : y_1^2 &= 4(z - 74)^4 + 5(z - 74)^2 - 2x + 1 \\ &= 4z^2(z + 24) + 89(-11z^2 + 730z - 17903) \end{aligned}$$

Now, by way of contradiction, assume there is a point $(y_1, z) \in E'$ that reduces to $(0, 0)$ modulo 89. Then 89 divides y_1, so y_1^2, which is the left-hand side of the curve equation, is divisible by 89^2. However, z is also divisible by 89, so all terms except $89 \cdot -17903$ of the right-hand side are also divisible by 89^2. But this last one is not, so the right-hand side is not divisible by 89^2, which is a contradiction. Thus, no such (y_1, z) exists, which then gives us that $\omega_{89} = 1$. With this proof, we can conclude

$$\prod_{p|2N} \omega_p = 1$$

1.2.5 Validating the BSD Conjecture

Finally, we can take a look at the strong BSD Conjecture for our $E : y^2 + xy + y = x^3 + x^2 - x$. In section 1.1, we have already proven the weak BSD Conjecture and showed that the left-hand side of the strong BSD Conjecture is equal to 0.62247.... With the values we have calculated in this section, we now get

$$\frac{\#Ш_{E/\mathbb{Q}} R_\infty \omega_\infty \prod_{p|2N} \omega_p}{E(\mathbb{Q})^{\text{tors}}} = \frac{1 \cdot 0.11210... \cdot 5.55262... \cdot 1}{1} \approx 0.62247...$$

While this is, of course, nowhere near a real proof, it is compelling evidence for the conjecture. In the next section, we will look at the BSD Conjecture from a more general angle, as we discuss what proofs have already been reached and what options we have for the future.

1.3 Proving the BSD Conjecture

Over time, many mathematicians have put in effort to prove the BSD Conjecture, and a variety of important results have already been found. In this section, we will briefly discuss the most important of these works, namely the results found by Gross, Zagier, and Kolyvagin. Their proofs will go beyond the scope of this paper, but discussing them is important to get a feel for the problems that we may encounter in the search for a full proof.

The main result that was found was that the BSD Conjecture holds for elliptic curves of rank 0 and 1. For rank 0, it was worked on by a variety of mathematicians, and the most important results were proven by Coates and Wiles in [CW], as well as Kolyvagin in [KOL]. In this paper, however, we will focus on rank 1 elliptic curves. In this case, there were several problems encountered by Gross, Zagier, and Kolyvagin. The most severe of these was the construction of rational points to determine the Mordell-Weil group and the regulator. There were no simple methods at the time for computing this, and it effectively prevented them from continuing.
However, there was one solution. Bryan Birch had defined a collection of points known as Heegner Points. These were rational points that could be calculated relatively easily, which was already quite useful. And then, in 1986, the Gross-Zagier Theorem was proven, which related the heights of these Heegner Points to the derivative of the L-function at $s = 1$:

Theorem 3 (Gross-Zagier)**.**
Let E be an elliptic curve of conductor N and let d be a positive integer such that $-d$ is a fundamental discriminant and a square modulo N. Define the twisted L-function

$$L(E, d, s) := \sum_{n=1}^{\infty} \left(\frac{-d}{n}\right) \frac{a(n)}{n^s}$$

where the $a(n)$ are the Dirichlet coefficients of $L(E, s)$. Then let P_d be the Heegner Point on E associated to d. Then

$$\hat{h}(P_d) = \frac{\sqrt{d}}{8\pi^2 ||f||^2} L'(E, 1) L(E, d, 1)$$

where

$$||f||^2 = \int_{\mathbb{H}/\Gamma_0(N)} |f(u + iv)|^2 du dv$$

is the norm of f coming from the Petersoon inner product.

For discussion of the twisted L-functions and a proof of this theorem, we can refer to [GZ, Chapter I.6] and [ZAG, Chapter V].

To understand exactly why this is useful, we consider [SVM, Theorem 9.3d]:

Proposition 1.
Let E/K be an elliptic curve and $P \in E(K)$. Then $\hat{h}(P) \geq 0$ and

$$\hat{h}(P) = 0 \Leftrightarrow P \in E(K)^{tors}$$

Now, we can pick a $d > 0$ such that $-d$ is a fundamental discriminant and $L(E, d, 1) \neq 0$. Then, if $L'(E, 1) \neq 0$, we see that $\hat{h}(P_d) \neq 0$ so P_d is not a torsion point by proposition 1. Thus, E has algebraic rank at least 1, which is a beautiful result in the context of the BSD Conjecture.

So now, it should be clear that Heegner Points are quite useful. In the next chapter, we will be defining these Heegner Points and exploring them further.

2 Heegner Points

Before we can get to defining and discussing Heegner Points themselves, we will first need some important background. Specifically, we will have to discuss class groups, as they hold important relationships to the Heegner Points and we will need them in several proofs.

2.1 Class Groups

2.1.1 Orders and The Ideal Class Group

First, let us consider a quadratic number field K, which we can write uniquely as $K = \mathbb{Q}(\sqrt{N})$ with N a square-free integer. In [COX, Chapter VII.A], it is proven that we can write the ring of integers of K as

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]$$

where we use the discriminant d_K, which is defined as

$$d_K = \begin{cases} N & N \equiv 1 \bmod 4 \\ 4N & N \not\equiv 1 \bmod 4 \end{cases}$$

Now, we can also consider $\mathcal{O}_K$ differently, namely as a *maximal order* of K. To understand this definition, we will need to understand what an *order* of K is: it is a subring of K that contains 1, is a finitely generated $\mathbb{Z}$-module, and contains a $\mathbb{Q}$-basis for K. This definition is unfortunately rather abstract, but we can use a few results from [COX, Chapter VII] to describe them more intuitively. First of all, note that we can show that, as suggested by the name 'maximal order', every order of K is a subring of $\mathcal{O}_K$. In addition, one can show that every order is a free $\mathbb{Z}$-module of rank 2. This then leads us to the following proposition:

Proposition 2.
Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then $c = [\mathcal{O}_K : \mathcal{O}]$ is finite and, writing $w_K = \frac{d_K + \sqrt{d_K}}{2}$, we have

$$\mathcal{O} = [1, cw_K]$$

where $[a, b]$ denotes the free $\mathbb{Z}$-module of rank 2 generated by a and b.

The c in this proposition is called the *conductor* of $\mathcal{O}$. In addition to this constant, we will also need the *discriminant* $d_\mathcal{O}$ of $\mathcal{O}$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ be the non-identity element. We can write $\mathcal{O} = [\alpha, \beta]$, as we know it is a $\mathbb{Z}$-module of rank 2. Then we define

$$\begin{aligned} d_\mathcal{O} &:= \left(\det \begin{pmatrix} \alpha & \beta \\ \sigma(\alpha) & \sigma(\beta) \end{pmatrix}\right)^2 \\ &= c^2 d_K \end{aligned}$$

where we use proposition 1 for the equality.

Next, recall the definition of a fractional ideal, specifically in the context of an order $\mathcal{O}$ of a quadratic field K. It is a subset of K that is a non-zero, finitely generated $\mathcal{O}$-module. In other words, it is a subgroup of (the additive group) K that is closed under multiplication with $\mathcal{O}$, distributive, and associative and has a finite $\mathcal{O}$-basis. With this definition, we can now give the following proposition:

Proposition 3.
Let $\mathcal{O}$ be an order of a quadratic field K and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}$. Then the following are equivalent:

(a) $\{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}$

(b) There is a fractional ideal $\mathfrak{b}$ *of* $\mathcal{O}$ *such that* $\mathfrak{a}\mathfrak{b} = \mathcal{O}$

If a fractional ideal satisfies (a), we call it *proper*, while if it satisfies (b), we call it *invertible*. Thus, the proposition states that a fractional ideal is proper if and only if it is invertible. In [COX], it is proposition 7.4, and a proof is given there. The proof uses two important lemmas, which we will also state here:

Lemma 2.
Let $\mathcal{O}$ *be an order of a quadratic field* K *and* $\mathfrak{a}$ *a non-zero fractional ideal. Then* $\mathfrak{a}$ *is a free* $\mathbb{Z}$*-module of rank 2.*

Lemma 3.
Let τ *be an algebraic element over* $\mathbb{Q}$ *with minimal polynomial* $f(x) = ax^2 + bx + c$ *where* a*,* b*, and* c *are relatively prime integers. Consider the quadratic field* $\mathbb{Q}(\tau)$*. Then* $[1, \tau]$ *is a proper fractional ideal of the order* $[1, a\tau]$ *of* $\mathbb{Q}(\tau)$*.*

Now we are ready to define the *ideal class group* of $\mathcal{O}$. First, consider the following sets for an order $\mathcal{O}$ of a quadratic field K:

$$I(\mathcal{O}) := \{\mathfrak{a} : \mathfrak{a} \text{ is a proper fractional ideal of } \mathcal{O}\}$$
$$P(\mathcal{O}) := \{\mathfrak{a} \lhd \mathcal{O} : \mathfrak{a} \text{ is a principal ideal of } \mathcal{O}\}$$

One can show that $I(\mathcal{O})$ is a group under multiplication and that $P(\mathcal{O})$ is a subgroup of it, which then immediately leads us to the definition

$$C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$$

which we call the ideal class group of $\mathcal{O}$. The following is a well-known result from algebraic number theory:

Theorem 4.
For all orders $\mathcal{O}$ *of imaginary quadratic fields* K*,* $C(\mathcal{O})$ *is finite.*

A proof of a more general form of this statement can be found in [STE, theorem 5.4], but expects more background than we want to go over in this paper, such as canonical volumes and the Minkowski bound.
The order of the ideal class group is called the *class number* of $\mathcal{O}$. It is denoted $h(\mathcal{O})$ or $h(d)$, where d is the discriminant of $\mathcal{O}$.

In the rest of this section, we will define different groups to use the finiteness of $C(\mathcal{O})$ to define Heegner Points.

2.1.2 Form Class Group

In this section, we prove the first of two important results. To do so, we must first define the *form class group*. Consider a quadratic form in two variables $f(x, y) = ax^2 + bxy + cy^2$ where the coefficients are coprime, as well as $\mathrm{SL}_2(\mathbb{Z})$, the group of two-dimensional matrices with integer entries and determinant equal to 1. Let $\mathrm{SL}_2(\mathbb{Z})$ act on quadratic forms as follows:

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} f(x, y) = f(px + qy, rx + sy)$$

It is not difficult to show that this is indeed a group action. If we now define the discriminant of a form as usual, $D(f) = b^2 - 4ac$, we can find the following with a simple calculation:

$$D\left(\begin{pmatrix} p & q \\ r & s \end{pmatrix} f\right) = (ps - qr)^2 D(f)$$

Importantly, we see that $ps - qr$ is the discriminant of the matrix, which is equal to 1 by definition of $\mathrm{SL}_2(\mathbb{Z})$. Thus, we see that the group action leaves the discriminant invariant. Now define $F(d)$ as the set of quadratic

forms of discriminant d, relatively prime integer coefficients and $a > 0$. We can let $\mathrm{SL}_2(\mathbb{Z})$ act on $F(d)$, which leads us to the following definition:

$$C(d) := F(d)/\mathrm{SL}_2(\mathbb{Z})$$

which is known as the *form class group*. Note that we call it a group, though we have yet to define a group operation on it. For this, we could use Dirichlet composition, which is discussed in [COX, Chapter III]. However, instead, we will reach a group structure via the next theorem.

The notation $C(d)$ should immediately suggest a relationship between $C(d)$ and $C(\mathcal{O}_K)$, and this is indeed true. The following theorem is one of the core results of this section.

Theorem 5.
Let $d < 0$ be an integer with $d \equiv 0 \bmod 4$ or $d \equiv 1 \bmod 4$. Let $\mathcal{O}$ be the order of discriminant d in an imaginary quadratic field K. Define a map $\psi : C(d) \to C(\mathcal{O})$ as follows:

$$\begin{array}{rcl} \psi : C(d) & \longrightarrow & C(\mathcal{O}) \\ ax^2 + bxy + cy^2 & \longmapsto & [a, \frac{1}{2}(-b + \sqrt{d})] \end{array}$$

Then ψ is a bijection.

Proof. First of all, we most show ψ is a well-defined map. To do so, we first show that $\mathfrak{a}_f$ is indeed a proper fractional ideal of $\mathcal{O}$. It is clearly a fractional ideal, so we only have to show it is proper. Let us consider $f(x, 1) = ax^2 + bx + c$. This is a quadratic polynomial of degree 2 with negative discriminant d, and thus irreducible over $\mathbb{Q}$. Its zeroes are $\frac{1}{2a}(-b \pm \sqrt{d})$. If we write $\tau = \frac{1}{2a}(-b + \sqrt{d})$, then $f(x, 1)$ is the minimal polynomial of τ. In addition, we can write

$$\mathfrak{a}_f = [a, \tfrac{1}{2}(-b + \sqrt{d})] = [a, a\tau] = a[1, \tau]$$

Now, by lemma 2, $[1, \tau]$ is a proper fractional ideal of $[1, a\tau]$, and thus so is $a[1, \tau]$. We must now show that $[1, a\tau] = \mathcal{O}$, and to do so, let c be the conductor of $\mathcal{O}$ and use $d = c^2 d_K$ to get

$$\begin{aligned} a\tau &= \frac{1}{2}(-b + \sqrt{d}) \\ &= \frac{1}{2}(-b - cd_K + cd_K + c\sqrt{d_K}) \\ &= -\frac{1}{2}(b + cd_K) + \frac{c}{2}(d_K + \sqrt{d_K}) \\ &= -\frac{1}{2}(b + cd_K) + cw_K \end{aligned}$$

with w_K as in proposition 1. Now, since $d = b^2 - 4ac$, d has the same parity as b. In addition, $d = cd_K$, so d is odd if and only if both c and d_K are odd, meaning d has the same parity as cd_K. Thus, b and cd_K have the same parity, so $-\frac{1}{2}(b + cd_K) \in \mathbb{Z}$. But then we have $[1, a\tau] = [1, -\frac{1}{2}(b + cd_K) + cw_K] = [1, cw_K] = \mathcal{O}$ by proposition 1. Thus we have shown that $\mathfrak{a}_f = a[1, \tau]$ is a proper fractional ideal of $\mathcal{O} = [1, a\tau]$.

Next, we must show that ψ is well-defined on the classes. Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be two quadratic forms such that $f \sim g$. In other words, there is a matrix

$$\gamma := \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that $f = \gamma g$, so $f(x, y) = \gamma g(x, y) = g(px + qy, rx + sy)$. Let τ be as before, i.e. the unique root of $f(x, 1)$ with positive imaginary part. Then

$$\begin{aligned} 0 = f(\tau, 1) &= g(p\tau + q, r\tau + s) \\ &= (r\tau + s)^2 g\left(\frac{p\tau + q}{r\tau + s}, 1\right) \end{aligned}$$

Thus, $g\left(\frac{p\tau+q}{r\tau+s}, 1\right) = 0$. And we can show that

$$\mathrm{Im}\left(\frac{p\tau+q}{r\tau+s}\right) = \det\begin{pmatrix} p & q \\ r & s \end{pmatrix} \left|(r\tau+s)^{-2}\right| \mathrm{Im}(\tau)$$

so the imaginary part of $\frac{p\tau+q}{r\tau+s}$ is positive if and only if that of τ is, so we have shown that $\frac{p\tau+q}{r\tau+s}$ is the unique root of $g(x,1)$ with positive imaginary part. We will write $\tau' = \frac{p\tau+q}{r\tau+s}$. Now, under the map we have defined, we see that f is mapped to $a[1,\tau]$ and g is mapped to $a'[1,\tau']$. Consider the principal fractional ideal $(r\tau+s)$ of $\mathcal{O}$. Then we have

$$\begin{aligned}(r\tau+s)[1,\tau'] &= [r\tau+s, (r\tau+s)\tau'] \\ &= [r\tau+s, p\tau+q]\end{aligned}$$

We claim this last expression is equal to $[1,\tau]$. Clearly $[r\tau+s, p\tau+q] \subset [1,\tau]$. In addition, we see $p(r\tau+s) - r(p\tau+q) = 1$, since $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, so $1 \in [r\tau+s, p\tau+q]$. In addition, by the same logic, $-q(r\tau+s) + s(p\tau+q) = \tau$, so $\tau \in [r\tau+s, p\tau+q]$. Thus, indeed $[r\tau+s, p\tau+q] = [1,\tau]$. But then we have found a principal ideal $(r\tau+s)$ such that $[1,\tau] = (r\tau+s)[1,\tau']$. But then also

$$a[1,\tau] = a(r\tau+s)[1,\tau'] = \left(\frac{a(r\tau+s)}{a'}\right) a'[1,\tau']$$

so we have $a[1,\tau] \sim a'[1,\tau']$ by definition of the ideal class group.

Thus, we have confirmed ψ is well-defined. We must now show it is bijective. We will do injectivity first. Take $f(x,y) = ax^2+bxy+cy^2$ and $g(x,y) = a'x^2+b'xy+c'y^2$ with roots τ and τ' respectively, both with positive imaginary part, and assume they have the same image under our map. Thus, $a[1,\tau] \sim a'[1,\tau']$. This is equivalent to $[1,\tau] \sim [1,\tau']$. In other words, there exists a principal fractional ideal (λ) of $\mathcal{O}$ such that $[1,\tau] = (\lambda)[1,\tau'] = [\lambda, \lambda\tau']$. Thus, by definition, there exist integers p, q, r and s such that

$$\lambda\tau' = p\tau + q\lambda = r\tau + s$$

where, using that this is an equivalence relation, we can see that $\gamma := \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. We now immediately get $\tau' = \frac{p\tau+q}{r\tau+s}$, and now the formula we gave earlier for the imaginary part of this expression shows that $\det\gamma = 1$, so $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. But then $f(x,1)$ and $g(px+q, rx+s)$ have the same root with positive imaginary part, which implies they are equal (as their coefficients can be directly calculated found from the real and imaginary parts of the root $\tau = \frac{1}{2a}(-b+\sqrt{d})$ as well as the discriminant $d = b^2-4ac$). This shows that $f \sim g$, so we have proven injectivity.

Finally, we will show surjectivity. Let $\mathfrak{a}$ be a proper fractional ideal of $\mathcal{O}$. By Lemma 1, we can write $\mathcal{O} = [\alpha, \beta]$ for some $\alpha, \beta \in K$. Without loss of generality, we may assume $\tau = \frac{\beta}{\alpha}$ has positive imaginary part, as we can take negatives or swap α and β if needed. Let ax^2+bx+c be the minimal polynomial of τ and consider $f(x,y) = ax^2+bxy+cy^2$, where we can assume that a, b, and c are coprime integers. Then we can show that $f(x,y)$ has discriminant d, and we clearly have that $f(\tau,1) = 0$, so f maps to $a[1,\tau]$. It is obvious that $a[1,\tau] \sim \alpha[1,\tau] = \mathfrak{a}$, which gives us the surjectivity we need. Thus, we have that ψ is a bijection.

□

In particular, we have managed to show that $|C(d)| = |C(\mathcal{O})| = h(d) < \infty$. In addition, we can now let the form class group inherit the group structure of $C(\mathcal{O})$. In the next section, we will build on this to find a similar result for different classes of quadratic forms.

2.1.3 Class Group of level N

Let N be a positive integer and d a negative integer. Also let ρ be an integer modulo $2N$ such that $\rho^2 \equiv d \bmod 4N$. With $F(d)$ as in the previous section, we define

$$F_{N,\rho}(d) := \{ax^2 + bxy + cy^2 \in F(d) : a \equiv 0 \bmod N, b \equiv \rho \bmod 2N\}$$

Now, we would like to let $\mathrm{SL}_2(\mathbb{Z})$ act on this set the same way it acts on $F(d)$. However, this action is not well-defined, as it does not in general take elements of $F_{N,\rho}(d)$ to other elements of $F_{N,\rho}(d)$. Thus, we instead consider the Hecke congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level N:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : r \equiv 0 \bmod N \right\}$$

A simple calculation will show that $\Gamma_0(N)$ acts on $F_{N,\rho}(d)$, as we see that for $ax^2 + bxy + cy^2 \in F_{N,\rho}(d)$, a matrix in $\Gamma_0(N)$ sends a to $ap^2 + bpr + cr^2 \equiv 0 \bmod N$ (since $a \equiv r \equiv 0 \bmod N$) and b to $2apq + b(ps + qr) + 2crs \equiv b(1 + 2qr) \equiv b \bmod N$ (since $ps - qr = 1$). This now leads us to define a *class group of level N*:

$$C_{N,\rho}(d) := F_{N,\rho}(d)/\Gamma_0(N)$$

This set will prove to be very important to us, but for now, we will focus on proving an important result for it:

Theorem 6.
Let $d < 0$ be an integer, N be prime and ρ be an integer modulo $2N$ with $\rho^2 \equiv d \bmod 4N$. Define the map $\chi : C_{N,\rho}(d) \to C(d)$ as sending a class in $C_{N,\rho}(d)$ to the class of its elements in $C(d)$. Then χ is a bijection.

Proof. To understand χ a little more, we will first show exactly what the map does. If we have $f(x, y) = ax^2 + bxy + cy^2$ with integer, coprime coefficients and $a \equiv 0 \bmod N$ and $b \equiv \rho \bmod 2N$, then we can simply map the class of f in $C_{N,\rho}(d)$ to its own class in $C(d)$. This immediately gives a well-defined map $C_{N,\rho}(d) \to C(d)$. We must now show it is a bijection.

We will begin by showing it is injective, as this is easier. Assume we have $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ such that they are in $F_{N,\rho}(d)$ and in the same class in $C(d)$. First, note that we have $b \equiv \rho \bmod 2N \equiv b' \bmod 2N$. Thus, we get that $b \equiv b' \bmod 2N$.
We also know there is a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $g(x, y) = \gamma f(x, y)$. Our goal is to show that $\gamma \in \Gamma_0(N)$. We can rewrite the relation between g and f as follows:

$$\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \Rightarrow \begin{cases} a' &= ap^2 + bpr + cr^2 \\ b' &= 2apq + b(ps + qr) + 2crs \\ c' &= aq^2 + bqs + cs^2 \end{cases}$$

Now we consider the first equation modulo N, using that both a' and a are divisible by N. This gives

$$r(bp + cr) \equiv 0 \bmod N$$

We will also consider the second equation modulo $2N$, where we use that $b \equiv b' \bmod 2N$ and $ps - qr = 1$. This gives

$$\begin{aligned} b &\equiv b(ps + qr) + 2crs \bmod 2N \\ b(1 - ps) &\equiv bqr + 2crs \bmod 2N \\ -bqr &\equiv bqr + 2crs \bmod 2N \\ 0 &\equiv 2r(bq + cs) \bmod 2N \\ 0 &\equiv r(bq + cs) \bmod N \end{aligned}$$

Because N is prime, there are no zero divisors modulo N. Thus, these two results together give that either $r \equiv 0 \bmod N$ or $bp+cr \equiv bq+cs \equiv 0 \bmod N$. However, since $ps-qr=1$ and b and c can't both be divisible by N (as otherwise, a, b, and c would all be divisible by 89 and thus not be coprime), we can conclude that the latter is impossible. This thus gives us $r \equiv 0 \bmod N$ and $\gamma \in \Gamma_0(89)$. Thus, f and g are in the same class in $C_{N,\rho}(d)$ and we have shown injectivity.

Next, we will show surjectivity. For this, take $f(x,y) = ax^2+bxy+cy^2$ in $F(d)$. We must show it is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to some quadratic form in $F_{N,\rho}(d)$. In other words, we must find a matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that the expression $a' = ap^2+bpr+cr^2$ is divisible by N, and $b' = 2apq+b(ps+qr)+2crs \equiv \rho \bmod 2N$. We can show such a matrix exists if

$$\begin{pmatrix} a & \frac{1}{2}(b-\rho) \\ \frac{1}{2}(b+\rho) & c \end{pmatrix} \begin{pmatrix} p \\ r \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \bmod N$$

This matrix equation is solvable in coprime integers p and r, because $\gcd(a,b,c)=1$ and the determinant of the matrix in this equation is $ac-\frac{1}{4}(b^2-\rho^2) = -\frac{1}{4}d+\frac{1}{4}\rho^2 \equiv 0 \bmod N$. And then, since we find p and r coprime, we can find integers q and s such that $ps-rq=1$, which gives us $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. This concludes the proof. □

With this, we have one more thing to define in this section. Assume N is prime and let

$$w_N = \begin{pmatrix} 0 & \frac{-1}{\sqrt{N}} \\ \sqrt{N} & 0 \end{pmatrix}$$

We call this matrix the *Atkin-Lehner involution*. Let $f = ax^2+bxy+cy^2 \in F_{N,\rho}(d)$. Then we can calculate that $w_N f = cNx^2 - bxy + \frac{a}{N}y^2$, where w_N 'acts' on f as matrices have been. From this description, we see something notable: $w_N f \in F_{N,-\rho}(d)$. This now lets us realize that w_N can act on the set $F_{N,\rho}(d) \cup F_{N,-\rho}(d)$. Since N is prime, ρ and $-\rho$ are actually the only valid choices for this parameter. Thus, we can define

$$F_N(d) := F_{N,\rho} \cup F_{N,-\rho} = \{ax^2+bxy+cy^2 \in F(d) : a \equiv 0 \bmod N\}$$

In addition, we know both $\Gamma_0(N)$ and w_N act on this set, so if we let $\Gamma := \langle \Gamma_0(N), w_N \rangle$, then Γ acts on $F_N(d)$. This now gives us another class group of level N:

$$C_N(d) := F_N(d)/\Gamma$$

Now one may see the following result coming

Proposition 4.
Let $d<0$ be an integer and N be prime. Choose ρ an integer modulo $2N$ such that $\rho^2 \equiv d \bmod 4N$. Then the map $\nu : C_{N,\rho}(d) \to C_N(d)$ defined by sending a class in $C_{N,\rho}(d)$ to the class of its elements in $C_N(d)$ is a bijection.

Proof. It should be immediately clear that ν is well-defined, since two elements being $\Gamma_0(N)$-equivalent certainly implies that they are Γ-equivalent. Thus, we must only show that is is injective and surjective. We will begin with surjectivity.

Let $f = ax^2+bxy+cy^2 \in F_N(d)$. Our goal is to show that f is Γ-equivalent to some $g \in F_{N,\rho}(d)$, and this is easily seen. We know that $b^2-4ac=d$, so $b^2 \equiv d \bmod 4N$. Thus, $b \equiv \pm\rho \bmod 2N$. If $b \equiv \rho \bmod 2N$, then $f \in F_{N,\rho}(d)$ and we are done. If $b \equiv -\rho \bmod 2N$, we see that $w_N f \in F_{N,\rho}(d)$, and since $w_N \in \Gamma$, we are also done in this case. Thus, indeed, ν is surjective.

Next, we must show ν is injective. For this, we will need the following two facts:

- $w_N^2 = -I \in \Gamma_0(N)$
- For all $\gamma \in \Gamma_0(N)$, we have $w_N \gamma w_N \in \Gamma_0(N)$

Both of these can be shown with simple matrix multiplication. Now assume we have $f, f' \in F_{N,\rho}(d)$ such that they map to the same class in $C_N(d)$. In other words, they are Γ-equivalent. Then there exists a matrix $\gamma \in \Gamma$ such that $\gamma f = f'$. We know that γ, like all matrices in Γ, is a product of matrices in $\Gamma_0(N)$ and w_N. However, $\Gamma_0(N)$ maps forms from $F_{N,\rho}(d)$ to other forms in $F_{N,\rho}(d)$, and similarly for $F_{N,-\rho}(d)$. Meanwhile, w_N maps forms from $F_{N,\rho}(d)$ to forms in $F_{N,-\rho}(d)$ and vice versa. Thus, since f and f' are both in $F_{N,\rho}(d)$, the product that makes up γ must contain an even number of w_N factors. But, by the facts that we have mentioned, all products that contain an even number of w_N factors are in fact elements of $\Gamma_0(N)$. But then f and f' are $\Gamma_0(N)$-equivalent and thus ν is injective. □

With this proposition, we are ready to finally define Heegner Points.

2.2 Definition and rationality of Heegner Points

2.2.1 Definition

Let E be an elliptic curve of prime conductor N. Consider some integer $d > 0$ and $\mathcal{O}$ the order of an imaginary quadratic field K of discriminant $-d$, and let $\mathfrak{a}$ represent some class in $C(\mathcal{O})$. Also recall the definition of $\phi = (\xi, \eta)$ as defined in section 1.1.2, and note that we can assume that $\mathfrak{a}$ is of the form $a[1, \tau_\mathfrak{a}]$ for some integer a and complex number τ with positive imaginary part, as we showed in the surjectivity proof of theorem 5. Then the *Heegner Point on E associated to $\mathfrak{a}$* is defined as

$$P_\mathfrak{a} := \phi(\tau_\mathfrak{a})$$

Next, we aim to define the *Heegner Point on E associated to d.* For this, we will need two extra terms. First, we define u to be half the number of units in $\mathcal{O}$; we know that $u = 3$ if $d = 3$, $u = 2$ if $d = 4$, and $u = 1$ in all other cases. Then define $P_d^0 \in E(\mathbb{C})$ as follows:

$$uP_d^0 := \sum_{\mathfrak{a} \in C(\mathcal{O})} P_\mathfrak{a}$$

We know this is well-defined, as by theorem 4, $C(\mathcal{O})$ is finite, meaning this is simply a finite sum. With this, we define the *Heegner Point on E associated to d* as

$$P_d := \begin{cases} P_d^0 & d \text{ is a fundamental discriminant} \\ \sum_{e^2 | d} P_{d/e^2}^0 & \text{otherwise} \end{cases}$$

Our goal for the rest of this section is to prove that these Heegner Points are rational for all $d > 0$. To do so, we will first have to briefly discuss ring class fields.

We will begin by defining them. Let d be a positive integer and $\mathcal{O}$ an the order of discriminant $-d$ in an imaginary quadratic field K. The *ring class field of discriminant $-d$* is a field extension H_d of $\mathbb{Q}(\sqrt{-d}) = K$ that satisfies the following:

1. H_d/K is Galois and abelian, and $\mathrm{Gal}(H_d/K) \cong C(\mathcal{O})$;
2. If $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ that does not divide $c\mathcal{O}_K$, where c is the conductor of $\mathcal{O}$, then $\mathfrak{p}$ is unramified in H_d/K;
3. If $\mathfrak{p} = (\alpha)$ is a prime in $\mathcal{O}$ that does not divide $c\mathcal{O}$, then $\mathfrak{p}$ splits completely in $\mathcal{O}_{H_d}$.

One can show that for each d, there is exactly one such extension that satisfies all 3 of these conditions.

Now, before we move on, let us cover an example of such a ring class field. This example is also done by Cox in [COX, Proposition 9.5] and we refer to him for details. Here, we will instead use a more concise approach. Consider the order $[1, \sqrt{-27}] = [1, 3\sqrt{-3}]$ of $K = \mathbb{Q}(\sqrt{-3})$. We see that $d_K = -3$ and that $c = [\mathcal{O}_K : \mathcal{O}] = 6$, so in this case $-d = 36 \cdot -3 = -108$. Thus, we can use this order to calculate the ring class field H_{108}. Now, first of all, we must have that $\mathrm{Gal}(H_{108}/K) \cong C(\mathcal{O})$. We can calculate that $C(\mathcal{O}) = C_3$, which then gives us $[H_{108} : K] = 3$ and thus $[H_{108} : \mathbb{Q}] = 6$. In fact, we find that $\mathrm{Gal}(H_{108}/\mathbb{Q}) = C_3 \rtimes C_2 = S_3$. Finally, note that since $\mathcal{O}$ has conductor 6, we need all ramified primes in $\mathcal{O}_K$ to divide $6\mathcal{O}_K$.

Now, first of all, we realize that K contains a primitive 3rd root of unity, namely $-\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, so Kummer theory implies that every extension of K of degree 3 is of the form $K(\sqrt[3]{\alpha})$ for some $\alpha \in K$. Thus, we write $H_d = K(\sqrt[3]{\alpha})$. Next, we know that all ramified primes in H_d/K must divide $6\mathcal{O}_K$, which limits us to $\alpha = 2^i 3^j$ with $0 \leq i, j \leq 2$. With this, we have considered the first two conditions in the definition of the ring class field, so we must look at the last. The primes in $\mathcal{O}$ that don't divide $6\mathcal{O}$ are of the form $x^2 + 27y^2$ with x and y integers. Now, we can simply check them one by one and find that the only α that makes all of these primes split completely is $\sqrt[3]{2}$. Thus, we get $H_d = K(\sqrt[3]{2})$.

In the next section, we will discuss the relevance of ring class fields to Heegner Points.

2.2.2 Shimura's Reciprocity Law

Now that we know what a ring class field is, we will move to an important result in algebraic number theory. It is called *Shimura's Reciprocity Law*, and is a more general statement than we will give here. It can be found in more detail in [LAN, chapter XI]. Its proof is complicated and goes far beyond the scope of this paper, so instead, we will give the most important statements we can derive from it:

Theorem 7 (Shimura's Reciprocity Law)**.**
Let $d > 0$ be an integer and E be an elliptic curve of conductor N. Let $\mathfrak{a} \in C(\mathcal{O})$ be chosen arbitrarily. Then the following holds:

(i) $P_{\mathfrak{a}} \in E(H_d)$

(ii) Since $Gal(H_d/K) \cong C(\mathcal{O})$, we know that $C(\mathcal{O})$ acts on the points of $E(H_d)$. With this action, we have for all $\mathfrak{b} \in C(\mathcal{O})$

$$P_{\mathfrak{a}}^{\mathfrak{b}} = P_{\mathfrak{b}^{-1}\mathfrak{a}}$$

(iii) $P_{\mathfrak{a}^{-1}} = \overline{P_{\mathfrak{a}}}$*, where $\overline{P_{\mathfrak{a}}}$ is defined as $P_{\mathfrak{a}}^{\sigma}$, with σ being the action of complex conjugation.*

These statements make computing Heegner Points easier and, more importantly, we can use them to find a very powerful and crucial corollary:

Corollary 1.
Let $d > 0$ be an integer and E be an elliptic curve of conductor N. Then $P_d \in E(\mathbb{Q})$.

Proof. We will first assume $-d$ is a fundamental discriminant. Then Shimura's Reciprocity Law (i) gives us that $P_d = \sum_{\mathfrak{a} \in C(\mathcal{O})} P_{\mathfrak{a}} \in E(H_d)$. Thus our goal will be to show that P_d is fixed by the Galois group $\mathrm{Gal}(H_d/\mathbb{Q})$. To do this, first consider the group $\mathrm{Gal}(H_d/\mathbb{Q}(\sqrt{-d})) \cong C(\mathcal{O})$. By Shimura's Reciprocity Law (ii), we see that for $\mathfrak{b} \in C(\mathcal{O})$, we have

$$\begin{aligned} P_d^{\mathfrak{b}} &= \sum_{\mathfrak{a} \in C(\mathcal{O})} P_{\mathfrak{a}}^{\mathfrak{b}} = \sum_{\mathfrak{a} \in C(\mathcal{O})} P_{\mathfrak{b}^{-1}\mathfrak{a}} \\ &= \sum_{\mathfrak{b}^{-1}\mathfrak{a} \in C(\mathcal{O})} P_{\mathfrak{b}^{-1}\mathfrak{a}} = P_d \end{aligned}$$

so indeed, $\mathrm{Gal}(H_d/\mathbb{Q}(\sqrt{-d}))$ fixes P_d. Thus, $P_d \in E(\mathbb{Q}(\sqrt{-d}))$.
Next, consider the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d})/\mathbb{Q}) = C_2$. Its only non-trivial element is complex conjugation

σ, and thanks to Shimura's Reciprocity Law (iii), we easily see

$$\begin{aligned}\sigma P_d &= \sum_{\mathfrak{a}\in C(\mathcal{O})} \overline{P_{\mathfrak{a}}} = \sum_{\mathfrak{a}\in C(\mathcal{O})} P_{\mathfrak{a}^{-1}} \\ &= \sum_{\mathfrak{a}^{-1}\in C(\mathcal{O})} P_{\mathfrak{a}^{-1}} = P_d\end{aligned}$$

where we use that P_d does not depend on the choice of ρ in the final part. Thus, we get that P_d is also fixed by $\mathrm{Gal}(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$ and thus $P_d \in \mathbb{Q}$ as required.

Finally, if d is not a fundamental discriminant, then the above proof applies to each of the P^0_{d/e^2}, so P_d is a sum of rational points and thus rational itself. □

With this, we have shown that indeed, these Heegner points are rational, giving us the ability to construct many rational points for any elliptic curve. In the next section, we will go over an algorithm for actually computing these.

2.3 Computing Heegner Points

In this section, we once again return to our elliptic curve

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

of conductor 89 as defined in the preface, and we will go through the process used to compute its first 200 Heegner Points. We will do this step-by-step to clarify the thought process fully.

2.3.1 Roots of C(d)

To start, we will assume that $-d$ is a fundamental discriminant. Then, we have that

$$P_d = P^0_d = \sum_{\mathfrak{a}\in C(\mathcal{O}_K)} P_{\mathfrak{a}}$$

where $K = \sqrt{-89}$, which makes the calculation simpler. Our first goal will be to simply compute each of the $P_{\mathfrak{a}}$, which we will do by calculating the $\tau_{\mathfrak{a}}$ first. We know that these $\tau_{\mathfrak{a}}$ are actually equal to the τ_f, i.e. the roots with positive imaginary part of forms $f \in C_N(-d)$. As we have seen in the previous section, we only have to consider the set of τ_f divided out by the standard action of $\Gamma = \langle \Gamma_0(89), w_{89}\rangle$ on them. Let $\mathcal{D}'_\Gamma$ be the fundamental domain of Γ: then we know that every class of the upper half plane under the action of $\mathrm{SL}_2(\mathbb{Z})$ has a unique representative in $\mathcal{D}_\Gamma$. Since we know that all of the τ_f are only mapped to elements of the form $\tau_{f'}$ for $f' \sim f$, we can restrict our search to finding the τ_f that lie in $\mathcal{D}_\Gamma$.

Now, we know that

$$\mathcal{D}_\Gamma = \bigcup_{\gamma\in R} \gamma\mathcal{D}$$

where R is a set of coset representatives of $\Gamma\backslash\mathrm{SL}_2(\mathbb{Z})$ and $\mathcal{D}$ is the fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$. It is now easy to see that for all $f \in C_{89}(-d)$, we have $\tau_f = \gamma\tau_g$ with $\gamma \in R$ and $g \in C(-d)$. Thus, our goal will be to find these τ_g.

Now, recall the definition of the fundamental domain $\mathcal{D}$ of $\mathrm{SL}_2(\mathbb{Z})$:

$$\mathcal{D} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0, -1/2 \le \mathrm{Re}(z) \le 1/2 \text{ and } |z| \ge 1\}$$

We know that each class of the upper half plane under the action of $\mathrm{SL}_2(\mathbb{Z})$ has a unique representative in $\mathcal{D}$, unless this representative is on the border, in which case there are 2. To avoid the exception, we will not consider any z with $\mathrm{Re}(z) = \frac{1}{2}$ or $|z| = 1$ and $\mathrm{Re}(z) > 0$. Then, we know that $\tau_g \in \mathcal{D}$ for all $g \in C(-d)$.

Write $g(x, y) = ax^2 + bxy + cy^2$. We know that then, $\tau_g = \frac{1}{2a}(-b + \sqrt{-d})$ and $-d = b^2 - 4ac$. We can now rewrite the condition $\tau_g \in \mathcal{D}$ as follows, using that $\mathrm{Re}(\tau_g) = \frac{-b}{2a}$ and $\mathrm{Im}(\tau_g) = \frac{\sqrt{-d}}{2a}$:

$$\begin{aligned} -\frac{1}{2} \leq -\frac{b}{2a} &\leq \frac{1}{2} \\ \left|\frac{b}{2a}\right| &\leq \frac{1}{2} \\ |b| &\leq a \end{aligned}$$

Where we use that $a > 0$. Next, we get

$$\begin{aligned} |\tau_g| &\geq 1 \\ \left|\frac{-b^2 - d}{4a^2}\right| &\geq 1 \\ \frac{c}{a} &\geq 1 \\ c &\geq a \end{aligned}$$

Here, we use that $-d = b^2 - 4ac$. Thus, we get from this that $c \geq a \geq |b|$, which immediately gives $ac \geq b^2$. Using this, we can keep rewriting to get

$$\begin{aligned} -d = b^2 - 4ac \leq b^2 - 4b^2 &= -3b^2 \\ |b| &\leq \sqrt{\frac{d}{3}} \end{aligned}$$

Next, we have that $a > 0$ is an integer, so $ac \geq c$. Thus

$$\begin{aligned} -d = b^2 - 4ac &\leq b^2 - 4c \\ c &\leq \frac{d + b^2}{4} \end{aligned}$$

And finally, with $a \leq c$, we now get a finite set of integers to investigate. After all, all we now have to do is find all sets of integers that satisfy $|b| \leq \sqrt{\frac{d}{3}}$, $c \leq \frac{d+b^2}{4}$, $a \leq c$ and $-d = b^2 - 4ac$. We can easily let a computer program do this for us, and this gives us all τ_g that we need.

However, we need to be careful here: this still includes all τ_g that are on the border we set to include. Thus, we now remove τ_g from the list if $\mathrm{Re}(\tau_g) = \frac{1}{2}$, or $|\tau_g| = 1$ and $\mathrm{Re}(\tau_g) > 0$. This way, we ensure we are not counting double anywhere.

Next, we must find the τ_f, which as said before are all of the form $\gamma\tau_g$ with $\gamma \in R$. Computing the γ is not difficult, so we simply calculate all (finitely many) $\gamma\tau_g$ and check which satisfy $a' \equiv 0 \bmod 89$. This will give us all τ_f, and we can check that this is true by seeing that the amount we find is exactly equal to the class number $h(-d)$: this must be true by theorems 5 and 6.

Let us consider an example. Let $d = 55$. We know that -55 is a fundamental discriminant, as we used in our process, so we can let our program first search for the triples a, b, and c. We expect it to find exactly 4 of them, as we have $h(-55) = 4$. And indeed, we get the following, written out as forms:

- $2x^2 + xy + 7y^2$

- $2x^2 - xy + 7y^2$
- $x^2 + xy + 14y^2$
- $4x^2 + 3xy + 4y^2$

Now, we let each of the coset representatives of $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$ act on the roots of these forms and keep only those that belong to a form with $a \equiv 0 \bmod 89$; note that we don't use the coset representatives of $\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. The reason for this that these are more complicated to calculate than the ones we use, and we will later show a way around this. This gives us the following list:

- $5785x^2 + 215xy + 2y^2$
- $12727x^2 + 319xy + 2y^2$
- $178x^2 + 37xy + 2y^2$
- $2492x^2 + 141xy + 2y^2$
- $356x^2 + 37xy + y^2$
- $4984x^2 + 141xy + y^2$
- $89x^2 + 37xy + 4y^2$
- $1246x^2 + 141xy + 4y^2$

Now, we see we find 8 forms, where we may have expected 4. This is a direct result of the coset representatives we chose to use, as these are the representatives of both $C_{89,\rho}(-55)$ and $C_{89,-\rho}(-55)$. We could now pick a ρ, where are choices are 37 mod 178 and 141 mod 178, and only keep those where $b \equiv \rho \bmod 178$, but this is impractical. In order to find our choices for ρ when N gets large, we'd have to take modular square roots, and this is difficult. As such, we use a different method to solve this problem, which we will get to later.

Now that we have our list of τ_f, it may appear the next step is easy: simply calculate each of the $P_f = \phi(\tau_f)$ and add them together. However, it is here that we run into a problem. After all, we have defined ϕ numerically, meaning that the operation $\phi(\tau_f)$ inevitably introduces rounding errors into our program. In addition, adding points on an elliptic curve together is a difficult process that amplifies these errors significantly, which can lead to major errors, such as the found coordinates only being correct to 3 decimals. While we can increase the precision of ϕ almost arbitrarily, it is impractical to make it so precise that we get reliable results. Instead, we use the *Lenstra-Lenstra-Lovász lattice basis reduction algorithm*, or *LLL algorithm* for short, to determine exactly which points on the elliptic curve we have found.

2.3.2 LLL Algorithm

We will not be going through the process of the LLL algorithm itself in this section. For those interested, there are a variety of resources available that explain it in detail, including [LLL], which is the original paper by Arjen Lenstra, Hendrik Lenstra and László Lovász describing the algorithm. In addition, it is also implemented into a variety of programs, such as SageMath, PARI/GP, and Maple. Instead, we will be going over what the algorithm's input and output are and how we can use it for our purposes.

Say we have a lattice $L \subset \mathbb{R}^n$ with basis $B = \{b_1, ..., b_k\}$. The LLL algorithm outputs a basis $B' := \{b'_1, ..., b'_k\}$ of L that is *LLL-reduced*. To define this, let $B^* := \{b^*_1, ..., b^*_k\}$ be the basis of L gotten by letting B' go through the Gram-Schmidt process, and let

$$\mu_{i,j} = \frac{\langle b'_i, b^*_j \rangle}{\langle b^*_j, b^*_j \rangle} \text{ for } 1 \leq j < i \leq k$$

Then B' is LLL-reduced if there exists a real number $\frac{1}{4} < \delta \leq 1$ such that

- For all $1 \leq j < i \leq k$, we have $|\mu_{i,j}| \leq \frac{1}{2}$

- For all $1 < j \leq k$, we have $\delta||b_{j-1}^*||^2 \leq ||b_j^*||^2 + \mu_{j,j-1}||b_{j-1}^*||^2$

where $||\cdot||$ is the norm on L.
Intuitively, this definition means that the basis is 'nearly orthogonal' and, importantly for our purposes, 'short', so the inner product of the basis vector is small, and so is the norm of the vector.

So the next question we have is how we use this to determine our P_f exactly. We know from what we have shown before [may have to be added here] that there exist polynomials $h_x(x)$ and $h_y(x)$ such that every x-coordinate of the P_f is a root of $h_x(x)$ and every y-coordinate is a root of $h_y(x)$, and in fact that all their roots appear as a coordinate at least once. We also see that the degree of $h_x(x)$ and $h_y(x)$ is less than or equal to the class number $h(-d)$, which is also the amount of P_f.

Our goal will be to find these $h_x(x)$ and $h_y(y)$. In other words, given rounded calculated value $x(P_f)$, we aim to find a polynomial $h_x(x)$ such that $x(P_f)$ is 'almost' a root of $h_x(x)$. To this end, consider the lattice of $\mathbb{Z}^{h(-d)}$ generated by $[1, 0, 0, ..., 0, 10^\ell x(P_f)^{h(-d)}], [0, 1, 0, ..., 0, 10^\ell x(P_f)^{h(-d)-1}], ..., [0, 0, 0, ..., 1, 10^\ell]$ where ℓ is an exponent that depends on the precision of $x(P_f)$. Then the LLL algorithm will output a basis of this lattice consisting of LLL-reduced vectors. We can look at the first vector of this basis. It must be a linear combination of the generators, so it is of the form $[a_1, a_2, ..., a_{h(-d)-1}, 10^\ell h'(x(P_f))]$ where the a_i are integers and h' is the polynomial of degree $h(-d)$ with coefficients a_i. However, we know this vector is 'short', so its entries must each be small. But since $h'(x(P_f))$ is being multiplied by the large factor 10^ℓ, so in order for this multiplication to be small, $h'(x(P_f))$ must be close to zero. Thus, $x(P_f)$ must be close to a root of h', and we set $h_x = h'$. We can find h_y in an entirely analogous way.

So we have now found the polynomials which the coordinates of our exact P_f are roots of. Consider the number field L generated by the zeroes of h_x and h_y. Clearly, we have $P_f \in E(L)$, and they are exact. Thus, in this number field, we can add each of the P_f together to finally get our P_d^0 as an element of $E(L)$. However, we are not quite done. After all, since we did not choose ρ yet, we have actually calculated $2P_d^0$. Now, if our goal were to simply construct a rational point, this would suffice too, as it is a multiple of a rational point. However, if we wanted to specifically calculate the Heegner Point, we need an extra step.

We can define P_0 as the generator of the Mordell-Weil group of E. In our case, it is $P_0 := (0 : 0 : 1)$. We know that P_d^0 is a rational point, so $P_d^0 = b_d P_0$ for some integer b_d. We can check every multiple of P_0 until we find an integer a_d such that $2P_d^0 = a_d P_0$. Then we get $b_d = \frac{1}{2}a_d$ and $P_d^0 = b_d P_0$, which we can calculate. That way, we get P_d^0 and since $-d$ is fundamental, this is equal to P_d.

Let us return to our example. Letting ϕ act on the list of forms we found, we get irrational numbers that we can let the LLL algorithm act on. Using this, we see that each of the x-coordinates of the $\phi(\tau_f)$ are roots of the polynomial $x^4 + x^3 - 2x - 1$, while each of the y-coordinates are roots of $x^4 + x^3 - 5x^2 + 3x + 9$. All we have to do now is add up the P_f over the splitting field of these polynomials, and they add up to $(-1 : -1 : 1) \in E(\mathbb{Q})$. Thus, we know that $2P_{55} = (-1 : -1 : 1)$ and we see that $(-1 : -1 : 1) = 2P_0$. Thus, $P_{55} = P_0 = (0 : 0 : 1)$.

Finally, we can consider the case where $-d$ is not fundamental. However, now this is simple: all we have to do is go through the previous process for each d/e^2 for e such that $e^2|d$. Afterwards, we can add these together, as they are all exact values, thus giving us any Heegner Point we wish to calculate.

2.3.3 Tables of Examples

Now that we have gone over the process, there is but one thing left to do: put it into action. To start, we will see the results for the elliptic curves we have been taking a close look at throughout this paper:

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

Note that for many values of d, we find that $F_{89}(-d)$ is empty, in which case we very quickly get $P_d^0 = \mathcal{O}$, where $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity on E. As there are many of such d, we have left them out of the table for the purpose of remaining concise. This now gives us the following results for $1 \leq d \leq 200$: We

d	4	8	11	16	20	32	39	40	47	55
P_d	$(0,0)$	$(0,0)$	$(0,-1)$	$(0,-1)$	$(0,0)$	$(0,-1)$	$(0,-1)$	$(0,-1)$	$(0,-1)$	$(0,0)$
d	64	67	68	79	80	87	88	99	100	107
P_d	$(0,-1)$	$(2,-5)$	$(0,0)$	$(-1,-1)$	$(0,-1)$	$(0,0)$	$(-1,-1)$	$(-1,-1)$	$(-1,1)$	$(-1,1)$
d	111	123	128	131	136	156	160	168	176	179
P_d	$(-1,1)$	$(0,0)$	$(0,-1)$	$(0,-1)$	$(0,-1)$	$(-1,1)$	$(0,0)$	$(\frac{3}{4},\frac{1}{8})$	$(-1,-1)$	$(-1,1)$
d	180	183	187	188	195	196	199			
P_d	$(-1,1)$	$(2,2)$	$(0,-1)$	$(-1,-1)$	$(2,-5)$	$(2,2)$	$(0,-1)$			

Table 1: Heegner Points on $E : y^2 + xy + y = x^3 + x^2 - x$

see that, as expected, the Heegner Point is rational for all values of d we check.

The process we used for this curve is not specific and is easily generalized. As such, we can use an extremely similar program to find a similar table for the commonly used curve $E : y^2 + y = x^3 - x$ of conductor 37:

d	3	4	7	11	12	16	27	28	36
P_d	$(0,-1)$	$(0,-1)$	$(0,0)$	$(0,-1)$	$(0,0)$	$(1,0)$	$(-1,-1)$	$(-1,0)$	$(1,0)$
d	40	44	47	63	64	67	71	75	83
P_d	$(1,-1)$	$(0,0)$	$(0,0)$	$(1,-1)$	$(1,-1)$	$(6,-15)$	$(0,-1)$	$(0,0)$	$(0,0)$
d	84	99	100	108	111	112	115	120	123
P_d	$(0,0)$	$(2,-3)$	$(-1,-1)$	$(-1,0)$	$(0,-1)$	$(2,-3)$	$(6,14)$	$(1,0)$	$(-1,0)$
d	127	132	136	144	147	148	151	152	155
P_d	$(0,-1)$	$(-1,0)$	$(2,2)$	$(2,2)$	$(1,0)$	$(6,14)$	$(1,0)$	$(1,0)$	$(1,-1)$
d	159	160	164	175	188	192	195		
P_d	$(0,-1)$	$(2,-3)$	$(0,0)$	$(0,-1)$	$(-1,0)$	$(1,-1)$	$(1,-1)$		

Table 2: Heegner Points on $E : y^2 + y = x^3 - x$

Thus, with this program we will be able to generate such tables for any elliptic curve of rank 1, and it would be a relatively simple task to extend it to different ranks as well.

Now that we are able to compute Heegner Points and have seen their rationality, our next purpose will be to highlight one important application for them. In the next chapter, we will do just that.

3 Shimura Correspondence

In 1973, Shimura ([SHI]) related spaces of modular forms of weight $2k$ to those of modular forms of weight $k + \frac{1}{2}$. In this section, we will discuss this result in the case of $k = 1$ and the relationship it has to Heegner Points.

3.1 Modular Forms of Half-Integral Weight

Before we get to the theorem of Shimura Correspondence, we will have to discuss modular forms of half-integral weight. It is assumed the reader is familiar with these, but we will discuss their definition again here. First, we consider the function $\theta : \mathbb{H} \to \mathbb{C}$, where $\mathbb{H}$ is the complex upper half plane, defined as follows:

$$\theta(z) = \sum_{n \in \mathbb{Z}} \exp\big(2\pi i n^2 z\big) = \sum_{n \in \mathbb{Z}} q^{n^2}$$

with $q = \exp(2\pi i z)$. We know that θ satisfies the following transformation formulas:

$$\theta(z+1) = \theta(z)$$
$$\theta\left(\frac{z}{4z+1}\right) = \sqrt{4z+1}\theta(z)$$

where $\sqrt{4z+1}$ is taken to have positive real part.
From this, it is easy to see that θ^2 is a modular form of weight 1 for $\Gamma_1(4)$. Then, in some sense, θ is a modular form of 'weight $\frac{1}{2}$'. In fact, θ is considered the prototypical modular form of weight $\frac{1}{2}$, and we can use it to build a rigorous definition. For now, let us define another important term. Let $N > 0$ be an integer divisible by 4 and $\gamma \in \Gamma_0(N)$, as well as $z \in \mathbb{H}$. Then

$$j(\gamma, z) := \frac{\theta(\gamma z)}{\theta(z)}$$

With what we have seen before, this should be at least somewhat natural. After all, we now have $j(\gamma, z)^2 = rz + s$, where $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma_1(4)$.

Now that we have this definition, we can move to the full definition of modular forms of half-integral weight. Let $N > 0$ be an integer that is divisible by 4, k an odd integer, and $f : \mathbb{H} \to \mathbb{C}$ a holomorphic function that is holomorphic at the cusps of $\Gamma_0(N)$. Finally, let χ be a character modulo N, Then f is a *modular form of weight $\frac{k}{2}$, level N, and character χ* if

$$f(\gamma z) = \chi(s) j(\gamma, z)^k f(z)$$

for all $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma_0(N)$ and $z \in \mathbb{H}$.

This definition should seem somewhat familiar, as it is quite similar to the one for modular forms of integer weight. Nonetheless, there are quite a few important differences. For example, we always work with congruence subgroups $\Gamma_0(N)$ where N is divisible by 4. This follows directly from our motivation; this came from the θ-function, the square of which is a modular form of $\Gamma_1(4)$, so our definition of $j(\gamma, z)$ doesn't make sense for congruence groups of levels not divisible by 4. Importantly, spaces of half-integral weight modular forms are more difficult to calculate than those of integral weight modular forms. Regardless of this difficulty however, working with modular forms of half-integral weight is still important, as Shimura Correspondence shows.

3.2 Shimura Correspondence

Before we get to the theorem, we will need to discuss another definition. Once again, let $N > 0$ be an integer and consider the Atkin-Lehner involution

$$w_N = \begin{pmatrix} 0 & \frac{-1}{\sqrt{N}} \\ \sqrt{N} & 0 \end{pmatrix}$$

As expected, we can let w_N act on the upper half plane as follows: for $z \in \mathbb{H}$, we have

$$w_N z = \frac{-1}{Nz} \tag{2}$$

Now let $\epsilon \in \{\pm 1\}$ and define the subspace

$$S_2^{\epsilon}(\Gamma_0(N)) := \{f \in S_2(\Gamma_0(N)) \mid \forall z \in \mathbb{H} : f(w_N z) = \epsilon N z^2 f(z)\}$$

Intuitively, this means that $S_2^{+}(\Gamma_0(N))$ is the subspace of $S_2(\Gamma_0(N))$ consisting of those cusp forms that are also cusp forms of weight 2 for w_N.

Next, we also define the space $S_{3/2}^{\epsilon}(N)$. Let $S_{3/2}(N)$ be the space of cusp forms of weight $3/2$, level $4N$, and trivial character, which are defined naturally from what we discussed in the last section. Consider $g = \sum_{d>0} c_d q^d \in S_{3/2}(N)$. Then we say $g \in S_{3/2}^{\epsilon}(N)$ if and only if $c_d = 0$ whenever $-d \equiv 2, 3 \bmod 4$ or $(\frac{-d}{N}) = -\epsilon$.

Now, at first glance, there doesn't appear to be much relation between $S_2^{\epsilon}(\Gamma_0(N))$ and $S_{3/2}^{\epsilon}(N)$. After all, they contain entirely different functions that are cusp forms of different weights. And yet, Shimura found a close, intricate relationship between the two:

Theorem 8 (Shimura Correspondence)**.**
Let N be prime and $\epsilon \in \{\pm 1\}$. Then for every $f = \sum_{n>0} a_n q^n \in S_2^{\epsilon}(\Gamma_0(N))$, there is a $g = \sum_{d>0} c_d q^d \in S_{3/2}^{\epsilon}(N)$ such that for all $n \in \mathbb{Z}_{>0}$ and fundamental discriminants $-d$, we have

$$a_n c_d = \sum_{r|n, r>0} \left(\frac{-d}{r}\right) c_{\frac{n^2}{r^2} d}$$

This g is unique up to multiplication by a constant. We also have $\dim S_2^{\epsilon}(\Gamma_0(N)) = \dim S_{3/2}^{\epsilon}(N)$

The proof of this theorem goes beyond the scope of this paper and can instead be found in Shimura's original paper [SHI, Section 3].

Now, there are a few important notes about this theorem. First of all, we see that as expected, a form g corresponding to a form f is only defined up to multiplication with a constant; after all, multiplying each coefficient c_d with a constant would end up doing the same on both sides of the equality, thus ensuring it still holds. Secondly, and more importantly, we see that while Shimura's statement gives an easy way to calculate the coefficients a_d given the coefficients c_d, it is not possible to go in the other direction. In some sense, the coefficients of modular forms of weight $\frac{3}{2}$ hold more 'information' and those of modular forms of weight 2.

As an example of this, recall our brief discussion on the Tate-Shafarevich group in 1.2.1. At the time, we mentioned that it is a largely unknown factor and that it is often difficult to work with. However, we do have a bit more information. Let $E : y^2 = h(x)$ be an elliptic curve, where h is a cubic polynomial. Then for $d \neq 0$ not a square in $\mathbb{Q}$, we consider the *quadratic twist of E at d* as

$$E_d : dy^2 = h(x)$$

Then Waldspurger showed in [WAL] that if the BSD Conjecture holds, we have for all d and some constant k that $\#Ш_{E_d/\mathbb{Q}} = kc_d^2$, where the c_d are the coefficients of the Shimura correspondent of the elliptic curve associated to E.

This result alone should show that these values c_d are very useful. For a while, however, they were difficult to compute. However, the result by Gross, Kohnen and Zagier ([GKZ, Theorem B] and [ZAG, Theorem 4]) changed this in certain cases, and we will discuss it in the next section.

3.3 Index of Heegner Points

Let $N > 0$ be a prime number. Our goal will be to take some cusp form $f = \sum_{n>0} a_n q^n \in S_2^\epsilon(\Gamma_0(N))$ and find the $g = \sum_{d>0} c_d q^d \in S_{3/2}^\epsilon(N)$ such that f and g are associated by Shimura correspondence. Unfortunately, we cannot do so for any arbitrary f, so we will have to place some additional requirements on this f. Specifically, we will assume that there exists an elliptic curve E of rank one and conductor N such that $L(E, s) = L(f, s)$.

Now consider $d > 0$ an integer and P_d the Heegner Point on E associated to d. We have seen in chapter 2 that we can compute P_d. In addition, we can compute P_0, the generator of the Mordell-Weil group $E(\mathbb{Q})/E(\mathbb{Q})^{\text{tors}}$. Then, we can define the *index of the Heegner Point* as b_d, where b_d is an integer such that $P_d = b_d P_0$. We note a few facts about b_d. Specifically, if $-d$ is not the discriminant of any orders of imaginary quadratic fields, then we can conclude that the same is true for all $-(d/e^2)$ (with $e^2|d$), and thus, we conclude that P_d is equal to an empty sum. Thus, we would get $P_d = (0 : 1 : 0) \in E$, which immediately gives $b_d = 0$. So when is $-d$ not such a discriminant? Well, we know by theorem 5, that if it is, then it is also a discriminant of some quadratic form. In other words, it is of the form $-d = b^2 - 4ac$ for integers a, b and c with $N|a$. In particular, we see that $-d$ is a square modulo 4 and modulo N, as it is equivalent to b^2. Thus, if we have that $-d \equiv 2, 3 \bmod 4$ or $(\frac{-d}{N}) = -1$, we immediately know $b_d = 0$.

This fact may seem familiar. If we now assume that $\epsilon = 1$, then we see that for c_d, we also have that $c_d = 0$ if $-d \equiv 2, 3 \bmod 4$ or $(\frac{-d}{N}) = -1$. This realization might already be enough to suggest a link between the values of b_d and c_d, but Zagier realized there was likely more. When he, Gross and Buhler computed tables for the b_d and c_d and found they matched up exactly, it led them to a conjecture, which was proven in [GKZ].

Theorem 9.
Let $N > 0$ be a prime number and $f \in S_2^+(\Gamma_0(N))$ be associated to an elliptic curve E of rank 1 and conductor N. Let $g = \sum_{d>0} c_d q^d \in S_{3/2}^+(N)$ be such that f and g are associated by Shimura correspondence. Let b_d be the index of the Heegner Point on E associated to d. Then, for all d and some constant k, $b_d = kc_d$.

This was a rather amazing result, as it was a way for us to calculate the c_d by simply computing Heegner Points, we have shown is possible. This then gave us the ability to, for any form f that corresponded to an elliptic curve of rank 1 and prime conductor, calculate the form g given by Shimura correspondence.

We will not be going over the full proof of the statement here; a general version can be found in [GKZ, Theorem B]. Here, we can discuss briefly the specific case of $\dim(S_{3/2}^+(N)) = 1$, which Zagier discusses in [ZAG]. The key ingredient of the proof is to show that

$$\sum_{d>0} b_d q^d$$

is the q-expansion of a modular form in $S_{3/2}^+$, which uses the deep work of Hirzebruch-Zagier about modular curves on modular surfaces ([HZ]).

To conclude this chapter, we will use the next section to show a few examples.

3.4 Examples

Let us do begin with the example we have used throughout this paper. Consider the modular form

$$f = q - q^2 - q^3 - q^4 - q^5 + q^6 - 4q^7 + 3q^8 - 2q^9 + \mathcal{O}(q^{10})$$

which is associated to $E : y^2 + xy + y = x^3 + x^2 - x$. Then, using Theorem 9 and Table 1, we easily find the following table: Thus, we can conclude that the Shimura corresponding form of weight $\frac{3}{2}$ should be

d	4	8	11	16	20	32	39	40	47	55
c_d	1	1	-1	-1	1	-1	-1	-1	-1	1
d	64	67	68	79	80	87	88	99	100	107
c_d	-1	3	1	2	-1	1	2	2	2	-2
d	111	123	128	131	136	156	160	168	176	179
c_d	-2	1	-1	-1	-1	-2	1	4	2	-2
d	180	183	187	188	195	196	199			
c_d	-2	-3	-1	2	3	-3	-1			

Table 3: Indices of Heegner Points on $E : y^2 + xy + y = x^3 + x^2 - x$

$$g = q^4 + q^8 - q^{11} - q^{16} + q^{20} - q^{32} - q^{39} - q^{40} - q^{47} + \mathcal{O}(q^{55})$$

And indeed, if we use the formula given in Shimura Correspondence, we find that f and g indeed satisfy it, so the correspondence holds.

Similarly, we can see other examples, such as

$$f = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + \mathcal{O}(q^{10}) \in S_2^+(\Gamma_0(37))$$

This form is associated to the elliptic curve $E : y^2 + y = x^3 - x$, which we have already considered in Table 2. Using this, we can conclude that

$$g = -q^3 - q^4 - q^{11} + q^{12} + 2q^{16} + 3q^{27} - 3q^{28} + 2q^{36} - 2q^{40} + q^{44} + q^{47} + \mathcal{O}(q^{63})$$

The following is a short table of modular forms, their associated elliptic curves, and then their calculated Shimura corresponding forms.

f	E	g
$q - 2q^2 - 2q^3 + 2q^4 - 4q^5 + \mathcal{O}(q^6)$	$y^2 + y = x^3 + x^2$	$q^3 + q^7 - q^8 - q^{12} + 2q^{19} - q^{20} + \mathcal{O}(q^{27})$
$q - q^2 - 3q^3 - q^4 + \mathcal{O}(q^6)$	$y^2 + xy + y = x^3 - x^2$	$-q^4 - q^7 + q^{11} + q^{15} + q^{16} - q^{24} + \mathcal{O}(q^{28})$
$q - q^2 - 2q^3 - q^4 - 3q^5 + \mathcal{O}(q^6)$	$y^2 + xy = x^3 - 2x + 1$	$q^3 - q^4 - q^{15} + q^{16} + q^{19} + q^{20} + \mathcal{O}(q^{27})$
$q - q^2 - q^3 - q^4 - 2q^5 + \mathcal{O}(q^6)$	$y^2 + xy + y = x^3 + x^2 + x$	$-q^8 + q^{15} + q^{19} - q^{24} + \mathcal{O}(q^{32})$
$q - 2q^3 - 2q^4 - q^5 + \mathcal{O}(q^7)$	$y^2 + y = x^3 + x^2 - x - 1$	$-q^4 - q^{19} + q^{20} + q^{23} + \mathcal{O}(q^{31})$

Table 4: Modular Forms and Shimura Correspondence

References

[SVM] J. H. Silverman. *The Arithmetic of Elliptic Curves.* (2000)

[GZ] B. Gross and D. Zagier. *Heegner points and derivatives of L-series.* Inventiones Mathematicae. Volume 84. (1986)

[COX] D. A. Cox. *Primes Of The Form $x^2 + xy^2$.* (1989)

[STE] P. Stevenhagen. *Number Rings.* (2019)

[BSD] B.J. Birch and H.P.F. Swinnerton-Dyer. *Notes on elliptic curves. II..* Journal für die reine und angewandte Mathematik. Volume 1965, Issue 218. (1963)

[WIL06] A. Wiles. *The Birch and Swinnerton-Dyer conjecture.* The Millenium Prize Problems. (2006)

[TAT65] J. Tate *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog* Séminaire N. Bourbaki. Expose 306. (1964-1966)

[AWL] A. Weil. *Numbers of solutions of equations in finite fields.* Bulletin of the American Mathematical Society. Volume 5, Number 5. (1949)

[WIL95] A. Wiles. *Modular elliptic curves and Fermat's Last Theorem.* Annals of Mathematics. Second Series, Volume 141, Number 3. (1995)

[TW] R. Taylor and A. Wiles. *Ring-theoretic properties of certain Hecke algebras.* Annals of Mathematics. Second series, Volume 141, Number 3. (1995)

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor. *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises.* Journal of the American Mathematical Society. Volume 14, Number 4. (2001)

[RUB] K. Rubin. *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication.* Inventiones Mathematicae. Volume 89. (1987)

[TAT06] J. Tate. *Algorithm for determining the type of a singular fiber in an elliptic pencil.* Modular Functions of One Variable IV. (2006)

[ZAG] D. Zagier *Modular Points, Modular Curves, Modular Surfaces and Modular Forms.* Arbeitstagung. (1984)

[CW] J. Coates and A. Wiles *On the Conjecture of Birch and Swinnerton-Dyer* Inventiones Mathematicae. Volume 39. (1977)

[KOL] V.A. Kolyvagin *Finiteness of and for a Subclass of Weil Curves* Mathematics of the USSR-Izvestiya. Volume 32, Number 3. (1989)

[LLL] A.K. Lenstra, H.W. Lenstra and L. Lovász. *Factoring Polynomials with Rational Coefficients.* Mathematische Annalen. Volume 261. (1982)

[LAN] S. Lang. *Graduate Texts in Mathematics.* (1987)

[SHI] G. Shimura. *On Modular Forms of Half Integral Weight.* Annals of Mathematics. Second Series, Volume 97, Number 3. (1973)

[KOH] W. Kohnen. *Fourier Coefficients of Modular Forms of Half-Integral Weight.* Mathematische Annalen. Volume 271. (1985)

[HZ] F. Hirzebruch and D. Zagier. *Intersection Numbers of Curves on Hilbert Modular Surfaces and Modular Forms of Nebentypus.* Inventiones Mathematicae. Vol. 36. (1976)

[GKZ] B. Gross, W. Kohnen and D. Zagier *Heegner points and derivatives ofL-series. II.* Mathematische Annalen. Vol. 278. (1987)

[WAL] J.-L. Waldspurger *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*. (1981)