HEEGNER POINTS AND THE CLASS NUMBER OF IMAGINARY QUADRATIC FIELDS

by

DEANNA LYNN VERONES

B.Sc., Simon Fraser University, 1996

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

THE FACULTY OF GRADUATE STUDIES

Mathematics

We accept this thesis as conforming
to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

August 1999

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Mathematics
The University of British Columbia
Vancouver, Canada

Date Sept 2 1999

Abstract

Gauss' class number problem is that of finding an upper bound for $|D|$ with given class number $h(D)$ where D is a negative fundamental discriminant. A theorem of Goldfeld reduces the class number problem to finding an elliptic curve defined over $\mathbb{Q}$ with rank $r \geq 3$ which satisfies the Birch and Swinnerton-Dyer conjecture. A theorem of Gross and Zagier gives a method of predicting when a Heegner point yields rational point of infinite order on an elliptic curve. In some cases their theorem allows us to say for certain whether the derivative of the L-series of an elliptic curve vanishes. Applying their theorem to a particular elliptic curve with rank $r = 3$, Gross and Zagier were able to show that their curve satisfied the Birch and Swinnerton-Dyer conjecture, thus solving the class number problem. This thesis examines closely the theory of Heegner points including computational results varifying the Gross-Zagier theorem.

Table of Contents

Acknowledgements

I would like to thank everyone who has supported me in my studies. I would like to thank my supervisor Dr. David Boyd for his encouragement and guidance in particular throughout my work on this thesis and in general in my pursuit of knowledge in number theory. I would also like to thank my second reader Dr. Vinayak Vatsal who has been extremely helpful to me in my work on this thesis.

I would like to again thank Dr. Boyd along with the Department of Mathematics at the University of British Columbia for financial support throughout my Master's degree.

I would like to thank my friends in and outside of UBC along with the faculty and office staff who have always been friendly and helpful.

Finally, I would like to thank my parents Joan and Oreste and my fiancé Mark for their love and encouragement.

Chapter 1
Introduction

*The story was told that the young Dirichlet had as a constant companion all his travels, like a devout man with his prayer book, an old, worn copy of the Disquisitiones Arithmeticae of Gauss.....*Tietze

The class number problem dates back to the work of Karl Friedrich Gauss, *Disquisitiones Arithmeticae.* According to Goldfeld [17], it may go back to Fermat. Gauss' class number problem poses the question, given a number h, how many discriminants D exist with class number equal to h? Gauss conjectured that for negative discriminants, this number is finite. His conjecture was proved in the 1930s by a combination of theorems by Hecke and Heilbronn [20]. Unfortunately, their theorems did not provide an effective formula for computing an upper bound for discriminants with a given class number.

The history of Gauss' class number problem is vast and interesting. Many famous mathematicians worked on this problem including Dirichlet with his class number formula, Hecke, Heilbronn, Siegel, Birch, Baker and Stark to name a few. More recently, in the 1980s, Goldfeld, Gross and Zagier were able to solve the general problem of finding an upper bound for the absolute value of a negative discriminant given a class number using the theory of elliptic curves.

In the 1960s, Birch examined a proof of the class number equal to one problem by Kurt Heegner published in 1952. Along with Stephens, he discovered a method to produce rational points on elliptic curves and, in 1981-82, conjectured the conditions in which these points are of finite or infinite order. Almost immediately, Gross and Zagier verified the conjectures of Birch and Stephens. With a suitable point on an elliptic curve provided by the Heegner point method, the theorem of Gross and Zagier

combined with a theorem of Goldfeld solves the class number problem.

The purpose of this thesis is to investigate the theory and computation of Heegner points and their connection to the class number problem.

This thesis is organized as follows. The next chapter describes the history of the class number problem in detail, from the work of Lagrange to Heegner's proof of the class number one problem in 1952. Chapter 3 is an overview of the theory of elliptic curves including complex multiplication, L-series and the canonical height function. Chapter 4 provides some necessary information on modular curves and the conjecture of Shimura and Taniyama which links elliptic curves to modular curves. Chapter 5 introduces us to the theory of Heegner points and describes how we can use these points to produce rational points on elliptic curves. The important theorem of Gross and Zagier will be stated in terms of rational points on elliptic curves. Also included will be some computations of points on elliptic curves using Heegner points. Finally, Chapter 6 is intended to tie the theory of Heegner points to the class number problem via the theorems of Goldfeld, Gross and Zagier.

Chapter 2
The Class Number Problem

Gauss' class number problem arises from the theory of binary quadratic forms. The purpose of this chapter is to describe the history of the problem from Lagrange's work to the result of Heegner.

Let $f = ax^2 + bxy + cy^2 = (a, b, c)$ be a binary quadratic form with a, b and c integers and discriminant $D = b^2 - 4ac$.

Definition 2.1 *The form $f = ax^2 + bxy + cy^2$ is said to* represent the integer m *if there exist integers x and y such that $m = ax^2 + bxy + cy^2$.*

Definition 2.2 *Two forms, $f = ax^2 + bxy + cy^2$ and $F = Ax'^2 + Bx'y' + Cy'^2$ are said to be* equivalent, *$(a, b, c) \sim (A, B, C)$, if F can be obtained from f by a linear transformation*

$$x = \alpha x' + \beta y'$$

$$y = \gamma x' + \delta y'$$

where $\alpha\delta - \beta\gamma = 1$.

It can be easily shown that equivalent forms represent the same set of integers and have the same discriminant. It can also be shown that equivalence of forms is an equivalence relation [6].

Definition 2.3 *The* class number, *denoted $h(D)$, is the number of inequivalent forms with discriminant D.*

A binary quadratic form $ax^2+bxy+cy^2$ with negative discriminant is called a definite form. It is easy to see that a and c must have the same sign.

Definition 2.4 *A* positive definite form *is a form with negative discriminant where both a and c are positive.*

In the 1770s, Lagrange [24] developed a general theory of binary quadratic forms $ax^2+bxy+cy^2$. He showed that every positive definite form is equivalent to a certain canonically chosen reduced form as follows.

Definition 2.5 *A form with negative discriminant is said to be* reduced *if it satisfies*

$$-a < b \leq a \leq c \text{ or } 0 \leq b \leq a = c.$$

The idea of equivalence is closely connected to the modular group

$$\Gamma = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) : ad - bc = 1 \right\}.$$

The group Γ acts on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ by

$$z \mapsto \frac{az+b}{cz+d}.$$

Definition 2.6 *For any group G of one-to-one transformations of a set X to itself, a* fundamental domain *R (if one exists) is a subset of X such that any point in X can be mapped by some transformation in G to some point in R, and no two points in the interior of R can be mapped to each other by any transformation in G.*

An example of a fundamental domain of Γ (see Figure 2.1) is

$$R = \{z : \operatorname{Im} z \geq 0, |z| \geq 1, |\operatorname{Re} z| \leq 1/2\}.$$

Given two equivalent forms $f = (a,b,c) \sim (A,B,C) = F$ with discriminant $D = b^2 - 4ac = B^2 - 4AC < 0$, we can associate two complex numbers in $\mathbb{Q}(\sqrt{D})$

$$\omega = (-b + \sqrt{D})/2a,$$

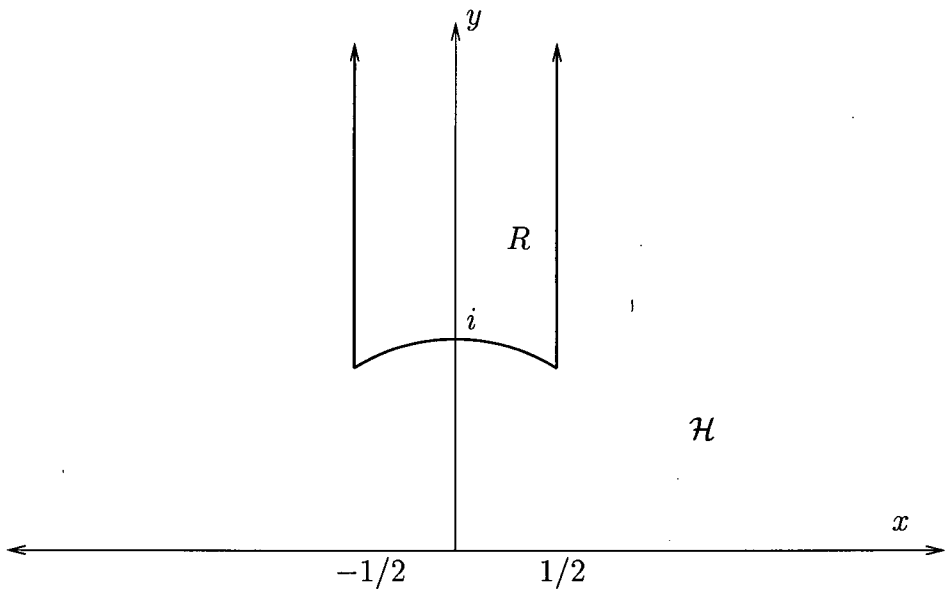

Figure 2.1: The Fundamental Region R

$$\omega' = (-B + \sqrt{D})/2A$$

lying in the upper half plane $\mathcal{H}$. We say that ω is equivalent to ω' in the sense that

$$\omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta},$$

where $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is the same transformation that takes f to F. A form is reduced if its associated complex number ω lies in the fundamental domain R of the modular group Γ. This leads to a modern interpretation of the class number which will proceed the following definition.

Definition 2.7 *D is a* fundamental, or field, discriminant *if D is of the form $b^2 - 4ac$, with a, b and c relatively prime integers.*

So D is a fundamental discriminant if and only if $D \equiv 1 (\text{mod } 4)$ and D is squarefree, or $D/4 \equiv 1,\ 2 (\text{mod } 4)$ and $D/4$ is squarefree.

Given a field K, the ring of integers of K, denoted $\mathcal{O}(K)$, is the set of elements of K which satisfy a monic polynomial equation over $\mathbb{Z}$.

If $K = \mathbb{Q}(\sqrt{D})$ then $\mathcal{O}(K) = \mathcal{O}_D = \mathbb{Z}[\frac{1}{2}(D + \sqrt{D})]$.

To each binary quadratic form $ax^2 + bxy + cy^2$ of negative discriminant D we can associate an ideal

$$[a, (-b + \sqrt{D})/2] \tag{2.1}$$

in the ring of integers $\mathcal{O}_D$.

Definition 2.8 *Two ideals $\mathcal{A}$ and $\mathcal{B}$ are said to be* equivalent, *$\mathcal{A} \sim \mathcal{B}$, if there exist principal ideals (λ_1) and (λ_2) such that $\mathcal{A}(\lambda_1) = \mathcal{B}(\lambda_2)$.*

It can be shown that equivalent ideals of type (2.1) correspond to equivalent forms [10].

The equivalence classes of ideals of $\mathbb{Q}(\sqrt{D})$ are called ideal classes. They form a group and $h(D)$ is equal to the order of this group. In particular, when $h(D) = 1$, every ideal in $\mathbb{Q}(\sqrt{D})$ is principal and the integers of $\mathbb{Q}(\sqrt{D})$ have unique factorization.

Gauss expanded the ideas of Lagrange in his book of 1801, *Disquisitiones Arithmeticae* [14]. It is important to note that Gauss only considered forms of the type $ax^2 + 2bxy + cy^2$ with even middle coefficient and defined the discriminant, often called the determinant, as $d = b^2 - ac$. Many of Gauss' results apply to general binary quadratic forms.

Gauss proved that the class number $h(D)$ is finite for any discriminant D. He did this by defining a composition of binary quadratic forms of discriminant D and proving that the classes of binary quadratic forms form a finite group although the notion of "group" had not yet been formally defined.

This result can also be proved by noticing that if $f = (a, b, c)$ is a reduced form of discriminant D, then $4b^2 \leq 4ac = b^2 - D$. This implies that $3b^2 \leq -D$ which then implies that $|b| \leq \sqrt{-D/3}$. Thus there are only finitely many candidates for reduced forms since the set of possible b's is finite and each such b determines a finite set of factorings of $b^2 - D$ into $4ac$.

Another important result of Gauss, which uses the genus theory of forms (see [6]), is that $2^{t-1}|h(D)$, where t is the number of distinct prime factors of D. If $h(D) = 1$ then this implies that $-D$ must be prime or a power of 2 equal to 4 or 8.

Gauss also conjectured:

Conjecture 2.1 (Gauss) *The number of negative discriminants $D < 0$ which have a given class number h is finite.*

From the tables of Gauss, it was known that $h(-p) = 1$ for the following 9 values of p:

$$3, 4, 7, 8, 11, 19, 43, 67, 163.$$

It is interesting to note that in 1911, Dickson [12] showed that if any further negative fundamental discriminants existed with class number one then they must be at least as small as -1500000.

Gauss' conjecture, which was proved in 1934 by a combination of theorems by Hecke and Heilbronn [20], leads to the modern form of Gauss' class number problem as stated by Goldfeld [17]:

> *Find an effective algorithm for determining all negative discriminants with given class number h.*

Let χ be a Dirichlet character modulo m. The Dirichlet L-series can be defined by

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

This series converges for all $\mathrm{Re}\, s > 1$. For nonprincipal characters, this series converges on the entire complex plane.

Dirichlet also studied the class number problem for binary quadratic forms and, like Gauss, considered only forms with an even middle term.

In 1839, Dirichlet proved that $\sum_Q \zeta_Q(s) = \zeta(s) L(s, \chi)$ where the sum is over a set of inequivalent forms of discriminant D and

$$\zeta_Q(s) = \sum_{m,n=-\infty}^{\infty}{}' (am^2 + bmn + cn^2)^{-s},$$

where $\sum'$ indicates that the sum is over all $(m, n) \neq (0, 0)$, $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the Riemann zeta function and χ is the real nonprincipal Dirichlet character modulo D.

Dirichlet used this result to prove his **Class Number Formula**:

$$L(1,\chi) = \frac{2\pi h(D)}{\omega\sqrt{|D|}} \text{ where } \omega = \begin{cases} 2 & D < -4 \\ 4 & D = -4 \\ 6 & D = -3 \end{cases},$$

D is a fundamental discriminant and χ mod D is the real nonprincipal Dirichlet character; thus proving that $L(1,\chi)$ is nonzero which is a key to proving his theorem on the infinitude of primes in arithmetic progression.

In 1918, Landau [25] published the following theorem which was first stated in a lecture given by Hecke:

Theorem 2.1 *Let D be a negative discriminant and let χ be the odd, real, primitive character modulo D.*
If $L(s,\chi) \neq 0$ for s real and $1 > s \geq 1 - c/\log|D|$, then

$$h(D) > c_1\sqrt{|D|}/\log|D|,$$

where $c, c_1 > 0$ are fixed absolute constants.

The generalized Riemann hypothesis states that the only nontrivial zeros of $L(s,\chi)$ are on the line $\mathrm{Re}s = 1/2$. This implies, by Hecke's theorem, that $h(D) > c_1\sqrt{|D|}/\log|D|$ and this in turn implies Gauss' conjecture that the number of negative discriminants D with a given class number is finite.

The classical Riemann hypothesis states that the only nontrivial zeros of the Riemann zeta function $\zeta(s)$ are on the line $\mathrm{Re}\, s = 1/2$.

In 1933, Deuring [11] proved the theorem:

Theorem 2.2 *If the classical Riemann hypothesis is false, then $h(D) \geq 2$ for $-D$ sufficiently large.*

In the same year, Lehmer [26] improved Dickson's bound for a tenth discriminant $-p$ with $h(-p) = 1$, to -5×10^9.

In 1934, Mordell [28] proved that if the classical Riemann hypothesis is false, then

$$h(D) \to \infty \text{ as } D \to -\infty,$$

thus proving that if the classical Riemann hypothesis is false then Gauss' conjecture is true.

This result was quickly improved upon by Heilbronn [20] who proved, in 1934 also, that if the generalized Riemann hypothesis is false then

$$h(D) \to \infty \text{ as } D \to -\infty.$$

Specifically, Heilbronn proves, "If there is, to modulus m, at least one real character, χ, principal or not, so that $L(\rho, \chi) = 0$ for at least one ρ in the half-plane $\sigma > 1/2$ then

$$h(D) \to \infty \text{ as } D \to -\infty."$$

Here, $\sigma = \text{Re}\, \rho$.

When combined with Hecke's theorem, this leads simply to

$$h(D) \to \infty \text{ as } D \to -\infty,$$

proving Gauss' conjecture and ensuring a finite number of discriminants with a given class number.

Unfortunately, the constants in the proof were not effective, since if the generalized Riemann hypothesis were false, all constants would depend on a real zero β of $L(s, \chi)$ such that $1/2 < \beta < 1$. β is called Siegel's zero [17].

Shortly after, also in 1934, Heilbronn and Linfoot [21] proved that there are at most ten negative fundamental discriminants D for which $h(D) = 1$:

$$D = -3, -4, -7, -8, -11, -19, -43, -67, -163, ?$$

The existence of the tenth discriminant depends on Siegel's zero. If the tenth discriminant did exist, the generalized Riemann hypothesis would be false.

In 1935, Siegel [30] proved:

Theorem 2.3 (Siegel) *For every $\epsilon > 0$, there exists a constant $c > 0$ (not effective) such that $h(D) > c|D|^{1/2-\epsilon}$.*

In 1951, Tatazawa [34] improved upon Siegel's theorem by showing that it is true, with an effectively computable constant $c > 0$ for all $D < 0$, except for at most one exceptional discriminant D, this discriminant's existence depending on the existence of Siegel's zero.

In 1952, Heegner [19] published a proof of the class number one problem (ie. that there is no tenth fundamental discriminant). He reduced the problem to the solution of a system of Diophantine equations. Unfortunately, his proof was discounted due to a supposed gap traceable to a result of Weber. Deuring [11] and Birch [4] each filled the gap in 1968, as did Stark [32] in 1969.

Birch's examination of Heegner's proof led him to develop the theory of Heegner points, ultimately leading to a solution of Gauss' class number problem. In the next chapter, we review some theory of elliptic curves.

Chapter 3
Elliptic Curves

3.1 Introduction

A significant connection between elliptic curves and the class number problem is due to a theorem of Goldfeld's [16] which will be stated in the concluding chapter. We begin by giving the formal definition of an elliptic curve.

Definition 3.1.1 *An* elliptic curve *is a pair (E, O) where E is a smooth projective curve of genus 1 and O is a (base) point of E.*

Every elliptic curve can be embedded as a smooth cubic curve in the projective plane $\mathbb{P}^2$ given by an equation of the form

$$ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

or, simply, as

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.1}$$

Equation 3.1 is called a (long) Weierstrass equation for E. The point O is the point $[0, 1, 0]$ at infinity. If E is defined over a field K, then the a_i's can be chosen to be in K.

Definition 3.1.2 *An* admissible change of variables over K *in a Weierstrass equation is one of the form*

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

where u, r, s and t are elements of K and u is nonzero.

Note that an admissible change of variables fixes the point at infinity and the group law to be described below.

Definition 3.1.3 *Two elliptic curves defined over a field K that are related by an admissible change of variables over K are said to be* isomorphic.

If the characteristic of K, $\text{char}(K) \neq 2, 3$, then E has a Weierstrass equation of the form

$$E : y^2 = x^3 + Ax + B. \tag{3.2}$$

This is done by making the change of variables

$$Y = y + \frac{1}{2}a_1 x + \frac{1}{2}a_3,$$

$$X = x + \frac{4a_2 + a_1^2}{12}.$$

Equation 3.2 is called a short Weierstrass equation for E.

Assuming E is nonsingular (the cubic in x in the right hand side of Equation 3.2 has 3 distinct roots), the discriminant of E is defined by

$$\Delta(E) = \Delta = -16(4A^3 + 27B^2) \neq 0.$$

I will now briefly discuss the group law (see Figure 3.1). Given 2 points, P_1, P_2 on E, construct the line P_1P_2. This line will intersect E at a 3rd point (possibly the point at infinity), Q. The group law is defined such that $P_1 + P_2 + Q = O$ or, $P_1 + P_2 = -Q$, where $-Q$ is defined to be the reflection of Q about the x-axis. ($-(x, y) = (x, -y)$.) This construction makes $E(K)$, the points (x, y) on E with $x, y \in K$, including the point O at infinity, into an abelian group with O the identity element. The only nonobvious group law is the associativity law.

This gives the set of points $E(\mathbb{Q})$ a very important structure. Mordell proved (see [31]) that $E(\mathbb{Q})$ is a finitely generated abelian group. Weil improved this result to a more general theorem.

Theorem 3.1.1 (Mordell,Weil) *Let K be a number field. Then $E(K)$ is a finitely generated abelian group. In other words, $E(K) \cong \mathbb{Z}^r \oplus E(K)_{tors}$, where r is called the rank of $E(K)$ and $E(K)_{tors}$ is finite abelian.*

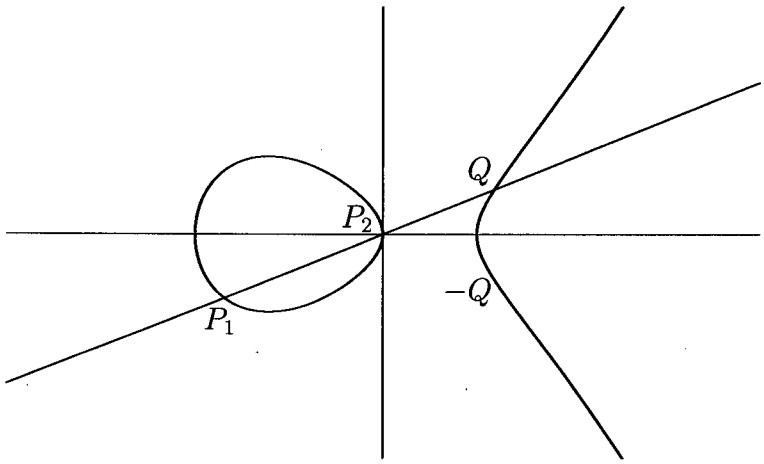

Figure 3.1: The Group Law

3.2 Elliptic Curves over $\mathbb{C}$ and Elliptic Functions

Given two complex numbers ω_1 and ω_2 with $\mathrm{Im}(\omega_1/\omega_2) > 0$, let $\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ be a lattice.

Definition 3.2.1 *An* elliptic function *is a Λ-periodic meromorphic function $f(z)$.*

In other words, $f(z)$ is holomorphic except for possibly countably many poles and $f(z+\omega) = f(z)$ for $z \in \mathbb{C}, \omega \in \Lambda$. The collection of all elliptic functions for Λ forms a field, denoted $\mathbb{C}(\Lambda)$.

Definition 3.2.2 *The* Weierstrass $\wp$-function

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

is an elliptic function with a double pole at each point of Λ and no other poles.

Note that $\wp(z)$ converges uniformly and absolutely on compact subsets of $\mathbb{C} - \Lambda$. This can be proved using the Weierstrass M-test.

We will need to also consider the function,

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3} \in \mathbb{C}(\Lambda).$$

Definition 3.2.3 *Two lattices Λ_1 and Λ_2 are* homothetic *if there exists a complex number τ such that*

$$\Lambda_1 = \tau\Lambda_2.$$

Theorem 3.2.1 *a) $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$= the set of rational functions over $\mathbb{C}$ in $\wp(z), \wp'(z)$.*

b) The functions $\wp(z)$ and $\wp'(z)$ satisfy the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

where $g_2(\Lambda) = 60G_4(\Lambda)$, $g_3(\Lambda) = 140G_6(\Lambda)$ and

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^{2k}}.$$

(Note: $G_{2k}(\Lambda)$ are absolutely convergent for all integers $k \geq 2$ and $G_{2k}(\lambda L) = \lambda^{-2k}G_{2k}(\Lambda)$ for any $\lambda \in \mathbb{C}^\times$.)

Also, the discriminant $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$ of the cubic polynomial is non-zero, so

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

defines an elliptic curve over $\mathbb{C}$.

(c) The map

$$\begin{array}{rccc} \phi_\Lambda : & \mathbb{C}/\Lambda & \to & E_\Lambda(\mathbb{C}) \\ & z & \mapsto & (\wp(z), \wp'(z)) \end{array}$$

is a complex analytic isomorphism of complex Lie groups.

(d) Conversely, given any elliptic curve E defined over $\mathbb{C}$, there exists a lattice Λ such that $E_\Lambda \cong E$. (Λ is unique up to homothety.)

In fact,

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\sum_{k=1}^{\infty} \frac{(k+1)}{\omega^{k+2}} z^k \right) \\ &= \frac{1}{z^2} + \sum_{k=1}^{\infty} (k+1) G_{k+2} z^k \\ &= \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \cdots\end{aligned}$$

Further,

$$\wp'(z) = \frac{-2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \cdots$$

It can also be shown [23]

$$G_k \in \mathbb{Q}[G_4, G_6].$$

In particular, if E is defined over $\mathbb{Q}$ given in short Weierstrass form

$$E : y^2 = 4x^3 - 60G_4 x - 140G_6,$$

then $G_k \in \mathbb{Q}$ for all k. We will use this result in Chapter 5.

The isomorphism described in (c) implies that

$$(\wp(z_1 + z_2), \wp'(z_1 + z_2)) = (\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)),$$

where the addition on the right hand side is addition of points on the elliptic curve according to the group law.

We can now define the j-invariant of an elliptic curve $E = E_\Lambda$.

Definition 3.2.4

$$j(E) = 1728 \frac{{g_2}^3}{{g_2}^3 - 27{g_3}^2}$$

Theorem 3.2.2 *The function $j(E)$ characterizes the isomorphism class of E over $\mathbb{C}$. More precisely, E is isomorphic to E' if and only if $j(E) = j(E')$.*

3.3 Complex Multiplication

We have our bijection from $\mathbb{C}/\Lambda$ to the elliptic curve E_Λ. Clearly, $n\Lambda \subset \Lambda$ for any integer n.

Definition 3.3.1 *We say* E has, or admits, complex multiplication *if there exists a complex number* $\beta \in \mathbb{C} - \mathbb{Z}$ *such that* $\beta\Lambda \subset \Lambda$.

Let $\Lambda = [\omega_1, \omega_2]$ be the lattice generated by ω_1 and ω_2. Then $\beta\Lambda \subset \Lambda$ if and only if $\beta \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = M \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ where $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$ is a matrix with integer entries. β is an eigenvalue of M and so a root of the characteristic polynomial of M, a quadratic monic polynomial with integer coefficients. Hence, β lies in a quadratic extension of $\mathbb{Q}$. In fact, all the β's lie in the same quadratic extension:

Write $\beta\omega_2 = t\omega_1 + u\omega_2$ with t and u integers as above. Then $\beta = t(\omega_1/\omega_2) + u$ which implies that $\beta, \omega_1/\omega_2 \in \mathbb{Q}(\sqrt{-D}) = K$, where D is a positive integer.

If E_Λ has complex multiplication, then the set $\{\beta \in \mathbb{C} : \beta\Lambda \subset \Lambda\}$ is a subring of $\mathcal{O}_K$ for some complex quadratic field $K = \mathbb{Q}(\sqrt{-D})$.

Another way to characterize complex multiplication is as follows. Suppose points on E are given by $(\wp(z), \wp'(z))$. Recall that addition on E corresponds to addition in $\mathbb{C}$:

$$(\wp(z_1), \wp'(z_1)) + (\wp(z_2), \wp'(z_2)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2))$$

Therefore, multiplication by m is

$$[m]P = [m](\wp(z), \wp'(z)) = (\wp(mz), \wp'(mz))$$

for any integer m.

In particular, $\wp(2z) = 2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2$.

In general, $\wp(mz) = \dfrac{\text{polynomial in } \wp(z) \text{ of degree } m^2}{\text{polynomial in } \wp(z) \text{ of degree } m^2 - 1}$.

An elliptic curve E has complex multiplication by a non-integer $\beta \in \mathbb{C}$ if and only if $\wp(\beta z) = f(\wp(z))/g(\wp(z))$, where f and g are polynomial functions over $\mathbb{C}$. Further, the degrees of f and g are $|\beta|^2$ and $|\beta|^2 - 1$, respectively.

Examples

1) $E : y^2 = x^3 + x$ has complex multiplication.

This can be seen in two ways:

a) If $(x, y) \in E$ then $(-x, iy) \in E$.
b) E is isomorphic to $\mathbb{C}/\Lambda$, where $\Lambda = [i, 1]$.
Clearly, $i\Lambda \subset \Lambda$. In fact, $i\Lambda = \Lambda$.

2) $E : y^2 = x^3 + 1$ has complex multiplication.

a) If $(x, y) \in E$ then $(\rho x, y) \in E$.
b) E is isomorphic to $\mathbb{C}/\Lambda$, where $\Lambda = [\rho, 1]$.
It is not difficult to show $\rho\Lambda = \Lambda$.

Definition 3.3.2 *A non-constant morphism, $\phi : E_1 \to E_2$ between elliptic curves which satisfies $\phi(O) = O$ is called an* isogeny.

An isogeny is always a group homomorphism.

Definition 3.3.3 *The* endomorphism ring of E, denoted $\mathrm{End}(E)$, *is the set of isogenies from E to itself.*

Notice that $\mathrm{End}(E)$ is a ring where $(\phi+\psi)(P) = \phi(P)+\psi(P)$ and $\phi\psi(P) = \phi(\psi(P))$.

Example If m is an integer then the multiplication by m map, $[m] : E \to E$, is in $\mathrm{End}(E)$.

Theorem 3.3.1 *Let E be an elliptic curve defined over a field K. Then there are three possibilities:*

$$End(E) = \begin{cases} \mathbb{Z} \\ \textit{an order in a quadratic imaginary field} \\ \textit{a maximal order in a quaternion algebra} \end{cases}$$

The third case can only occur if the characteristic of K is nonzero [22].

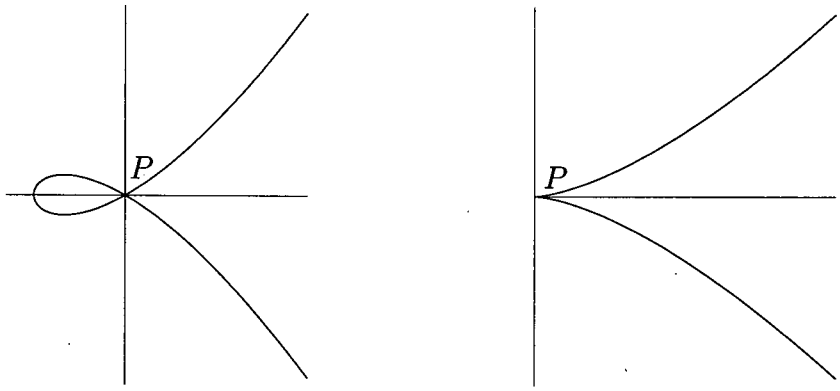

Figure 3.2: Two distinct tangent directions at P on the left; One distinct tangent direction at P on the right.

If E has complex multiplication then the endomorphism ring of E is strictly larger than $\mathbb{Z}$. This is another way to define complex multiplication.

3.4 L-Series of Elliptic Curves

Given an elliptic curve E defined over $\mathbb{Q}$ in long Weierstrass form, we can make the substitution as in Definition 3.1.2 with rational numbers u, r, s, t yielding an elliptic curve E' isomorphic to E with $\Delta(E') = u^{-12}\Delta(E)$. Then there exists a substitution that makes Δ minimal subject to $a_i \in \mathbb{Z}$. This curve is called the global minimal model.

We can reduce an elliptic curve E modulo a prime p by reducing the coefficients of the Weierstrass equation of E modulo p. Denote this elliptic curve by E_p.

Definition 3.4.1 *E has* good reduction modulo p *if p does not divide $\Delta(E)$. (ie. $\Delta(E_p) \neq 0$.)*

In this case, E_p is an elliptic curve over $\mathbb{F}_p$, where $\mathbb{F}_p$ is the finite field with p elements.

Otherwise, we say E has bad reduction modulo p. In the case of bad reduction, there is a singular point P on E_p. We distinguish two types of bad reduction by the nature of the singularity. (See Figure 3.2)

1) If there are two distinct tangent directions at P over $\overline{\mathbb{F}}_p$ we say that P is a node and that E has *multiplicative reduction mod p.*

2) If there is a single tangent direction at P over $\overline{\mathbb{F}}_p$ we say that P is a cusp and that E has *additive reduction mod p.*

Definition 3.4.2 *The* conductor N *of* E *is defined by*

$$N = \prod_{p|\Delta(E)} p^{e_p}$$

where $e_p = \begin{cases} 1 & \text{if } E \text{ has multiplicative reduction modulo } p. \\ \geq 2 & \text{if } E \text{ has additive reduction modulo } p \text{ (See [7]).} \end{cases}$

We now define the L-series of E:

Definition 3.4.3

$$L(E/\mathbb{Q}, s) = L_E(s) = \prod_{p|N}(1 - a_p p^{-s})^{-1} \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where $a_p = \begin{cases} p + 1 - N_p & \text{if } p \nmid N \\ \pm 1 \text{ or } 0 & \text{if } p|N \end{cases}$ *and* $N_p = |E_p(\mathbb{F}_p)|$.

Theorem 3.4.1 (Hasse) $|a_p| \leq 2\sqrt{p}$

Theorem 3.4.1 is known as the Riemann hypothesis for elliptic curves over finite fields. It implies that the Euler product for $L_E(s)$ converges absolutely for Re $s > 3/2$. Therefore, for Re $s > 3/2$, we may write $L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s}$.

For certain elliptic curves, $L_E(s)$ has an analytic continuation to the entire complex plane as we will discuss in Chapter 4.

3.5 Heights

The canonical height function will not be used until Chapter 5, but it is convenient to introduce it at this point.

Let E be an elliptic curve defined over $\mathbb{Q}$ and suppose that $P = (x, y)$ is a point in $E(\mathbb{Q})$ such that $x = p/q$ where p and q are relatively prime integers.

Definition 3.5.1 *The* naive height of P *is defined by*

$$h(P) = \begin{cases} \log \max(|p|, |q|) & \text{if } P \neq O \\ 0 & \text{if } P = O \end{cases}$$

Definition 3.5.2 *The* canonical height of P *is given by*

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}.$$

Theorem 3.5.1 *1.* $\hat{h}(P) - h(P)$ *is bounded*

2. $\hat{h}(2P) = 4\hat{h}(P)$

Further, $\hat{h}(P) \geq 0$ *with equality if and only if* P *has finite order.*

Also, the set $\{P \in E(\mathbb{Q}) : \hat{h}(P) < C\}$ *is finite for any real number* C.

We will also need the definition of the regulator of an elliptic curve over $\mathbb{Q}$ which is related to the canonical height. First, we need to define the Néron-Tate pairing.

Definition 3.5.3 *The* Néron-Tate pairing on $E/\mathbb{Q}$ *is the bilinear form*

$$\langle , \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$$

defined by $\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$.

The regulator of an elliptic curve E defined over $\mathbb{Q}$ may be defined in terms of the Néron-Tate pairing.

Definition 3.5.4 *The* elliptic regulator of an elliptic curve E defined over $\mathbb{Q}$, denoted $R_{E/\mathbb{Q}}$, *is given by*

$$R_{E/\mathbb{Q}} = \det \langle P_i, P_j \rangle$$

where $P_1, .., P_r$ *are generators of the nontorsion part of* $E(\mathbb{Q})$ *and* $1 \leq i, j \leq r$.

If the rank $r = 0$, *we set* $R_{E/\mathbb{Q}} = 1$.

Note that the regulator is independent of the choice of generators for $E(\mathbb{Q})$.

Chapter 4
Modular Curves

4.1 Modular Forms

In order to describe modular curves and their relationship to elliptic curves, we must first explore briefly the theory of modular forms.

Recall that $\Gamma = SL_2(\mathbb{Z})$ is the modular group,

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}) : ad - bc = 1 \right\}$$

and that Γ acts on the upper half plane $\mathcal{H} = \{z \in C : \text{Im } z > 0\}$ by

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

Definition 4.1.1 *Let $f(z)$ be a meromorphic function on the upper half plane $\mathcal{H}$ and let k be an integer. Suppose that $f(\gamma z) = (cz + d)^k f(z)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in Γ. Further, suppose that $f(z)$ is "meromorphic at infinity". This means that the Fourier series*

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n, \text{ where } q = e^{2\pi i z},$$

has at most finitely many nonzero a_n with $n < 0$. Then $f(z)$ is called a modular function of weight k for Γ.

We also have the following definition:

Definition 4.1.2 *If a modular function of weight k $f(z)$ is holomorphic on $\mathcal{H}$ and at infinity (ie. $a_n = 0$ for all $n < 0$), then $f(z)$ is called a* modular form of weight k for Γ. *If a modular form $f(z)$ vanishes at infinity, which occurs when $a_0 = 0$, then $f(z)$ is called a* cusp form of weight k for Γ.

Notice if the weight k is zero, then the modular function $f(z)$ is invariant under Γ.

Examples

1) Let k be an integer greater than 1. For $z \in \mathcal{H}$ we define

$$G_{2k}(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^{2k}},$$

where the sum is over pairs of integers. If the lattice $\Lambda_z = [1, z]$ is generated by 1 and z then this is the definition of $G_{2k}(z) = G_{2k}(\Lambda_z)$ from the previous chapter. $G_{2k}(z)$ is a modular form of weight k. As in the previous chapter, we let $g_2(z) = 60G_4(z)$ and $g_3(z) = 140G_6(z)$.

2) The discriminant

$$\Delta(z) = g_2(z)^3 - 27g_3(z)^2$$

is a cusp form of weight 12 for Γ.

3) The j-invariant

$$j(z) = \frac{1728g_2(z)^3}{\Delta(z)}$$

is a modular form of weight 0 for Γ.

It can be shown that

$$j(\omega) = \frac{\{1 + 240\sum_{n=1}^{\infty}\sigma_3(n)e^{2\pi in\omega}\}^3}{e^{2\pi i\omega}\prod_{n=1}^{\infty}(1-e^{2\pi in\omega})^{24}},$$

where $\sigma_3(n) = \sum_{d|n} d^3$.

Theorem 4.1.1 *The modular functions of weight 0 for Γ are precisely the rational functions of j [6].*

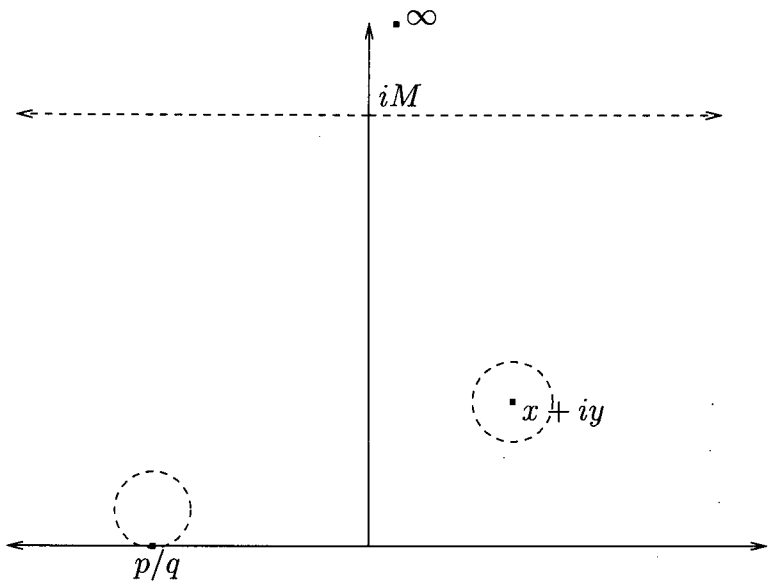

Figure 4.1: Open Sets in $\mathcal{H}^*$

4.2 The Modular Curve $X_0(N)$

As usual, we let $\mathcal{H}$ denote the upper half plane and let

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

Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}'(\mathbb{Q})$ be the completion of $\mathcal{H}$, where $\mathbb{P}'(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

We topologize $\mathcal{H}^*$ as follows: A basic open set about a point of $\mathcal{H}$ is an open disc wholly within $\mathcal{H}$, and a basic open set about ∞ is $\{\tau : \text{Im}\, \tau > M\}$ for each positive real number M. If $x = p/q \in \mathbb{P}'(\mathbb{Q})$ is rational, a basic open set about x is of the form $D \cup \{x\}$, where D is an open disc in $\mathcal{H}$ of positive radius r and center $x + ir$. The resulting topology on $\mathcal{H}^*$ is Hausdorff, $\mathcal{H}$ is an open subset and Γ acts continuously. (See Figure 4.1)

$X_0(N) = \mathcal{H}^*/\Gamma_0(N)$ is a compact Hausdorff space. It can be shown that $X_0(N)$ is a Riemann surface and this Riemann surface can be realized as the set of complex points of a projective curve defined over $\mathbb{Q}$ [22].

As usual, $j(z)$ is the modular invariant and we let $j_N(z) = j(Nz)$. The meromorphic

functions on $\mathcal{H}$ invariant by $\Gamma_0(N)$ are rational functions of j and j_N. There is an equation, called the modular equation, given by $F_N(j, j_N) = 0$, connecting j and j_N with $F_N(u, v) \in \mathbb{Z}[u, v]$. This makes the curve

$$Z_0(N) : \ F_N(u, v) = 0$$

into an irreducible plane model for $X_0(N)$.

Let θ be the mapping:

$$\theta : X_0(N) \to Z_0(N)$$
$$z \mapsto (j(z), j(Nz)).$$

By a point on $X_0(N)$ we will mean either a point $z \in \mathcal{H}^*/\Gamma_0(N)$ or its image $(j(z), j(Nz)) \in Z_0(N)$.

4.3 Weil Curves and the Shimura-Taniyama Conjecture

Some modular curves are elliptic curves themselves. For example, $X_0(11)$ has genus one and can be defined as an elliptic curve over $\mathbb{Q}$. Unfortunately, there are only finitely many modular curves $X_0(N)$ of any given genus. However, it often happens that there is a map

$$\phi : X_0(N) \to E,$$

defined over $\mathbb{Q}$, from $X_0(N)$ onto an elliptic curve E also defined over $\mathbb{Q}$. In this case, we say that E is a modular elliptic curve or a Weil curve. To avoid confusion between "modular elliptic curves" and "modular curves", the term "Weil curve" will henceforth be used. We also may say that E has a modular parametrization of level N or that E is parametrized by modular functions.

For Weil curves, $L_E(s)$ has an analytic continuation to the entire complex plane given by the functional equation:

$$\left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L_E(s) = \pm \left(\frac{\sqrt{N}}{2\pi}\right)^{2-s} \Gamma(2-s) L_E(2-s). \tag{4.1}$$

One reason why the analytic continuation of the L-series $L_E(s)$ is so important is due to a famous conjecture of Birch and Swinnerton-Dyer [3]:

Conjecture 4.3.1 (Birch,Swinnerton-Dyer) *Rank*$(E(\mathbb{Q})) = r$ *if and only if*

$$L_E(s) = c_E(s-1)^r + \text{ higher order terms},$$

where c_E *can also be explicitly conjectured as*

$$c_E = \frac{S \cdot \Omega(f) \cdot R \cdot \prod c_p}{|T|^2}.$$

R *is the regulator of* $E/\mathbb{Q}$, $|T|$ *is the order of the torsion subgroup* $E(\mathbb{Q})_{tors}$ *and* $\Omega(f)$ *is a certain integer multiple of the least real period of* E, *to be specified later. The local indices* c_p, *sometimes called the Tamagawa numbers, are certain positive integers with* $c_p > 1$ *only if* $p|N$ *(see [31]). Further,* S *is conjectured to be the order of a group associated to the elliptic curve* E *called the Tate-Shafaravich group.*

So the behaviour of $L_E(s)$ at $s = 1$ may contain a lot of information about the elliptic curve E.

Recall that the L-series for E may be given by the product

$$L_E(s) = \prod_{p|N}(1 - a_p p^{-s})^{-1} \prod_{p \nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1}$$

or by the series $\sum_{n=1}^{\infty} a_n n^{-s}$.

Let $f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n$, where $q = e^{2\pi i \tau}$.

The following theorem connects elliptic curves to cusp forms of weight 2. For the purpose of this thesis, it is unnecessary to go into detail on the subject of newforms, a special class of cusp forms. For a detailed explanation, see [22].

Theorem 4.3.1 *Let* f *be a modular cusp form of weight* 2 *for the group* $\Gamma_0(N)$. *In other words,* f *is an analytic function on the upper half plane* $\mathcal{H}$, *such that for* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, $z \in \mathcal{H}$,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z).$$

Assume further that f *is a normalized newform and that* f *has rational Fourier coefficients. Then there exists an elliptic curve* E *defined over* $\mathbb{Q}$ *such that* $f = f_E$.

Notice that if $f(z)$ is a modular form of weight 2 for $\Gamma_0(N)$ then the differential form $f(z)dz$ is invariant under $\Gamma_0(N)$. In the case described by the above theorem, E is a Weil curve by a theory due to Eichler and Shimura (for a good source see [22]).

Corollary 4.3.1 *Let E be a Weil curve and let $f = \sum_{n=1}^{\infty} a_n q^n$ be the corresponding cusp form. Then $L_E(s)$ satisfies the functional equation 4.1. In addition we have*

$$f\left(\frac{-1}{N\tau}\right) = -\epsilon N\tau^2 f(\tau)$$

where ϵ is the sign in the functional equation for $L_E(s)$.

We may now state the famous conjecture due to Shimura and Taniyama (and occasionally credited also to Weil).

Conjecture 4.3.2 (Shimura,Taniyama) *Let E be an elliptic curve defined over $\mathbb{Q}$, let $L_E(s)$ be its L-series and let $f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n$ be the inverse Mellin transform of $(2\pi)^{-s}\Gamma(s)L_E(s)$.*

Then f is a cusp form of weight 2 on $\Gamma_0(N)$.

Furthermore, there exists a map ϕ from $X_0(N)$ to E, defined over $\mathbb{Q}$, such that the inverse image by ϕ of the differential $dx/(2y+a_1x+a_3)$ is the differential $c(2\pi i)f(\tau)d\tau = cf(\tau)dq/q$, where c is some constant.

More simply, the Shimura-Taniyama conjecture states that every elliptic curve is a Weil curve.

There is a great deal of evidence to support the Shimura-Taniyama conjecture. In particular, it is known to be true for all elliptic curves with complex multiplication, for all curves with square-free conductor, and for all curves with conductor N such that 27 does not divide N [8]. In fact, it would appear that the conjecture has recently been proven by Breuil, Conrad, Diamond and Taylor, although the proof is as yet unpublished.

Given an isogeny class of elliptic curves defined over $\mathbb{Q}$, there exists an elliptic curve E in the isogeny class called a "strong Weil curve" together with a map ϕ from $X_0(N)$ to E characterized as follows.

Given a map ϕ' from $X_0(N)$ to E', where E' is in the same isogeny class as E, there is an isogeny F from E to E' such that $\phi' = F \circ \phi$.

The map ϕ is called a strong Weil parametrization of E and the constant c above, called Manin's constant, is conjectured to be always equal to ± 1 when ϕ is a strong Weil parametrization of E.

In the case where E is a strong Weil curve, there is a simple map [33]

$$u : X_0(N) \to \mathbb{C}/\Lambda \cong E(\mathbb{C})$$

$$\omega \mapsto u(\omega)$$

given by

$$u(\omega) = -2\pi i \int_{\omega}^{i\infty} f(\tau) d\tau = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i \omega n}.$$

This is a rapidly converging series and $F \circ u = \phi$, where F is the isomorphism,

$$F : \mathbb{C}/\Lambda \to E(\mathbb{C}).$$

We will use this rapidly converging series in our calculations of points on elliptic curves.

Note that the map u is independent of the choice of the representative ω on $X_0(N)$ since $f(\tau)d\tau$ is invariant under $\Gamma_0(N)$.

If E is not a strong Weil curve, then E is isogenous to a strong Weil curve and the points obtained by $u(\omega)$ will give us points on that strong Weil curve.

Chapter 5
Heegner Points

5.1 Introduction

Given an elliptic curve E defined over $\mathbb{Q}$, as usual let $E(\mathbb{Q})$ denote the set of rational points on E, including the point at infinity. As we know, a theorem of Mordell states that $E(\mathbb{Q})$ is a finitely generated abelian group.

Much is known about the torsion subgroup. For example, a torsion point can have order at most 12. However, less is known about the rank r. One would like an algorithm to construct rational points on E of infinite order, if they exist. In some cases, this is what Heegner points can do for us.

The purpose of this chapter is to develop the theory of Heegner points and to describe an algorithm that can be used to find a rational point on an elliptic curve and to predict in which circumstances this point should turn out to be of infinite order.

First, let us briefly review some class field theory which will prove very important in our construction.

5.2 Class Field Theory

Class field theory is the study of abelian extensions of number fields. Suppose ω is an imaginary quadratic number. Then ω satisfies an equation

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

where A, B and C are relatively prime integers. Denote the discriminant of ω as $\Delta(\omega) = B^2 - 4AC$ and let K be the quadratic extension $\mathbb{Q}(\omega)$.

In general, the Hilbert class field of a given field F is defined to be the maximal unramified abelian extension of F. For quadratic fields, $K_1 = K(j(\omega)) = \mathbb{Q}(\omega, j(\omega))$ is the Hilbert class field of $\mathbb{Q}(\omega)$ [31].

The following theorem (see [31]) will be useful in our construction of rational points on elliptic curves.

Theorem 5.2.1 *1. The Hilbert class field is unique.*

2. $[K_1 : K] = [K(j(\omega)) : \mathbb{Q}] = h(\Delta)$ *=the class number of* Δ.

3. K_1 *depends only on* Δ*, rather than on* ω.

5.3 The Heegner Point Construction

As in the previous section, we will let $\omega \in \mathcal{H}$ be a complex quadratic number with discriminant $\Delta = \Delta(\omega)$.

There are several equivalent ways of defining a Heegner point of $X_0(N)$. We will use the following definition:

Definition 5.3.1 ω *is a* Heegner point of $X_0(N)$ *if it satisfies*

$$A\omega^2 + B\omega + C = 0$$

where A, B *and* C *are relatively prime integers and* $A \equiv 0 (\text{mod } N)$.

So ω satisfies

$$NA'\omega^2 + B\omega + C = 0 \tag{5.1}$$

and $\Delta(\omega) = B^2 - 4NA'C$.

Multiplying 5.1 by N:

$$N^2A'\omega^2 + BN\omega + CN = 0,$$

yielding

$$A'(N\omega)^2 + B(N\omega) + CN = 0.$$

Further, A', B amd CN are relatively prime integers and $\Delta(N\omega) = B^2 - 4NA'C = \Delta(\omega)$.

Theorem 5.3.1 *A complex quadratic number ω is a Heegner point of $X_0(N)$ if and only if $\Delta(\omega) = \Delta(N\omega)$.*

We may also interpret any point τ of $X_0(N)$ as a pair of elliptic curves, $E = \mathbb{C}/\mathbb{Z}\oplus\tau\mathbb{Z}$, $E' = \mathbb{C}/\mathbb{Z} \oplus N\tau\mathbb{Z}$, together with the $N-$isogeny $E \to E'$. Then a Heegner point ω corresponds to a pair of $N-$isogenous elliptic curves, each with the same complex multiplication. This can be seen by noticing that $\Delta(\omega) = \Delta(N\omega)$ and ω and $N\omega$ lie in the same quadratic field.

Recall from the Chapter 4 that the image of ω on $X_0(N)$ may be represented on the plane model as

$$(j(\omega), j_N(\omega)) \in Z_0(N).$$

For $z \in \mathcal{H}$, $j(1/\overline{z}) = j(-\overline{z}) = \overline{j(z)}$. So for ω a Heegner point, it is easy to show that

$$\overline{j(\omega)} = j(1/\overline{\omega}) = j(N\omega) = j_N(\omega).$$

Given an elliptic curve E defined over $\mathbb{Q}$ of conductor N, we will assume that E is a Weil curve so that there is a rational map

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

If ω is a Heegner point then $\phi(\omega) \in E(\mathbb{Q}(j(\omega), j_N(\omega)))$.

Now, the Hilbert class field $K_1 = \mathbb{Q}(\omega, j(\omega)) = \mathbb{Q}(\omega, j_N(\omega))$, since the Hilbert class field of K depends only on $\Delta(\omega) = \Delta(N\omega)$.

Therefore, $\mathbb{Q}(j(\omega), j_N(\omega)) \subset \mathbb{Q}(\omega, j(\omega)) = K_1$ and we have $\phi(\omega) \in K_1$.

This is very convenient since K_1 is Galois over $K = \mathbb{Q}(\omega)$. Now let the discriminant of ω, $\Delta(\omega) = D$ and the class number $h = h(D)$. In order to obtain a complete set of K_1/K conjugates, we must find h Heegner points $\omega_1, ..., \omega_h$, each satisfying $A_i\omega_i^2 + B_i\omega + C_i = 0$ with $B_i^2 - 4A_iC_i = D \equiv r^2 (\text{mod } 4N)$, $A_i \equiv 0 (\text{mod } N)$, $B_i \equiv r (\text{mod } 2N)$. Then if we take the sum

$$P = \phi(\omega_1) + \cdots + \phi(\omega_h),$$

we will obtain a point in $E(K)$.

The question becomes, how can we extract a point in $E(\mathbb{Q})$ from the point U?

Let us now assume that E is a strong Weil curve. Recall that this means that there exists a cusp form of weight 2 for $\Gamma_0(N)$ given by $f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau}$, such that

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

Moreover, in the case where E is a strong Weil curve, recall the simple map,

$$u : X_0(N) \to \mathbb{C}/\Lambda \cong E(\mathbb{C}),$$

where

$$u(\omega) = -2\pi i \int_{\omega}^{i\infty} f(\tau) d\tau = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \omega},$$

and $F \circ u = \phi$, where F is the isomorphism

$$F : \mathbb{C}/\Lambda \to E(\mathbb{C}).$$

Let ϵ be the sign in the functional equation for $L_E(s)$ so that we also have the functional equation for $f(\tau)$:

$$f\left(-\frac{1}{N\tau}\right) = -\epsilon N \tau^2 f(\tau),$$

where $f(\tau)$ is as above.

Theorem 5.3.2 *If ω is a Heegner point,*

$$\overline{u(\omega)} = \epsilon(L(f,1) - u(\omega)).$$

Proof

$$\begin{aligned}
u(\omega) &= -2\pi i \int_{\omega}^{i\infty} f(\tau)d\tau \\
&= -2\pi i \int_{\frac{-1}{N\omega}}^{\frac{-1}{Ni\infty}} f\left(\frac{-1}{N\tau}\right)\frac{1}{N\tau^2}d\tau \text{ making the change of variables } \tau \mapsto \frac{-1}{N\tau} \\
&= -2\pi i \int_{-\overline{\omega}}^{0} -\epsilon f(\tau)d\tau \text{ since for } \omega \text{ a Heegner point, } \overline{\omega} = \frac{1}{N\omega} \\
&= -2\pi i \int_{0}^{-\overline{\omega}} \epsilon f(\tau)d\tau \\
&= -2\pi i \int_{0}^{i\infty} \epsilon f(\tau)d\tau - \left(-2\pi i \int_{-\overline{\omega}}^{i\infty} \epsilon f(\tau)d\tau\right) \\
&= \epsilon L(f,1) - \epsilon u(-\overline{\omega}) \\
&= \epsilon(L(f,1) - u(-\overline{\omega}))
\end{aligned}$$

Now, $u(\omega) = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n\omega}$.

Therefore,

$$\begin{aligned}
\overline{u(-\overline{\omega})} &= \sum_{n=1}^{\infty} \frac{a_n}{n} e^{\overline{2\pi i(-\overline{\omega}n)}} \\
&= \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i\omega n} \\
&= u(\omega),
\end{aligned}$$

and $u(\omega) = \epsilon(L(f,1) - \overline{u(\omega)})$. □

Since we are assuming E is a modular curve,

$$L(f,1) = L_E(1) = \Omega(f) \cdot K,$$

where K is a rational number and

$$\Omega(f) = \begin{cases} \Omega_0(E) & \text{if the real locus of } E \text{ has one component} \\ 2\Omega_0(E) & \text{if the real locus of } E \text{ has two components} \end{cases}$$

and $\Omega_0(E)$ is the least positive real period of E [9]. (Recall the value $\Omega(f)$ in the Birch, Swinnerton-Dyer conjecture.) We take the sum

$$U = u(\omega_1) + \cdots + u(\omega_h)$$

yielding a point

$$(x, y) \in E(K).$$

Ultimately, we would like a point in $E(\mathbb{Q})$. A theorem by Gross and Zagier to be discussed in the next section will then predict when this point will be of infinite order.

We have two cases depending on the sign in the functional equation for $L_E(s)$.

Case 1: $\epsilon = -1$

Then $L_E(1) = 0$ by the functional equation for E. In fact, the zero must be of odd order. Therefore, $U = \overline{U} \in \mathbb{R}$ and $\wp(U) \in \mathbb{R}$, $\wp'(U) \in \mathbb{R}$.

Hence the point $(x, y) \in E(K) \cap E(\mathbb{R}) = E(\mathbb{Q})$.

Case 2: $\epsilon = +1$

We have $\overline{U} = h(D)L(f, 1) - U$ by Theorem 5.3.2 and

$$L_E(1) = L(f, 1) = \Omega(f) \cdot K$$

which is equal to a *rational* multiple of the least positive real period of E. So if we pick a discriminant D such that $h(D)L(f, 1)$ is equal to an *integer* multiple of the least positive real period of E then we will have $\overline{U} = h(D)L(f, 1) - U \equiv -U$ modulo Λ. In this case, U mod Λ will be pure imaginary and we will have

$\wp(U) \in \mathbb{R}$ and $\wp'(U) = -2U^{-3} + 6G_4U + 20G_6U^3 + 42G_8U^5 + ...$ is pure imaginary.

Therefore, $\wp(U) \in \mathbb{Q}$ and $\wp'(U) = \sqrt{D}B$ for some $B \in \mathbb{Q}$.

So, $(\wp(U), \wp'(U)/\sqrt{D}) \in E^D(\mathbb{Q})$, where

$$E^D : Dy^2 = 4x^3 + ax + b$$

is the short Weierstrass form of a twist of the elliptic curve E.

In the case where the rank r of E is zero, the Birch and Swinnerton-Dyer conjecture predicts that

$$L(f, 1) = \frac{S \cdot \Omega(f) \cdot \prod c_p}{|T|^2}.$$

In this case we may take D such that $h(D) \prod c_p$ is an integer multiple of $|T|^2$.

5.4 The Theorem of Gross and Zagier

In 1982, Birch and Stephens published a conjecture about the height of the rational point arising from the Heegner construction:

Conjecture 5.1 *If E is an elliptic curve over $\mathbb{Q}$ which is parametrized by modular functions, ie. E is a Weil curve, and K is a complex quadratic field such that the Mordell-Weil group $E(K)$ of K-rational points of E has odd rank, then the "canonical" K-rational point of E which is given by Heegner's construction has Tate height measured by $L'_{E/K}(1)$.*

Birch and Stephens go on to state [5]:

> *Unhappily, it is a consequence of this conjecture that the Heegner point turns out to be trivial whenever the rank is more than one.*

Recall that a point on an elliptic curve is trivial whenever it has canonical height equal to zero, or, equivalently, whenever it is a torsion point.

Soon after, also in 1983, Gross and Zagier [18] proved this conjecture.

Let E be the elliptic curve $y^2 = 4x^3 + ax + b$ defined over $\mathbb{Q}$. Let E^D be the twist $Dy^2 = 4x^3 + ax + b$, where $D < 0$ is the discriminant of an imaginary quadratic field. Assume also that D and N are relatively prime, where N is the conductor of E and that $D \equiv \beta^2 (\text{mod } 4N)$ for some β. Let ϵ be the sign of the functional equation of $L_E(s)$. Then if we let Ω_E and Ω_{E^D} denote the least positive real periods of the elliptic curves E and E^D, respectively, there are two cases:

Case 1: $\epsilon = -1$

Then there exists a point $P_D \in E(\mathbb{Q})$ such that

$$L_{E^D}(1)L'_E(1) = c\Omega_{E^D}\Omega_E\hat{h}(P_D)$$

where c is a nonzero rational number and $\hat{h}$ is the height function on $E(\mathbb{Q})$.

Case 2: $\epsilon = +1$

Then there exists a point $P_D \in E^D(\mathbb{Q})$ such that

$$L_E(1)L'_{E^D}(1) = c\Omega_{E^D}\Omega_E\hat{h}_{E^D}(P_D)$$

where c is as above and $\hat{h}_{E^D}$ is the height function on $E^D(\mathbb{Q})$.

In both cases, the point P_D is the point given in the construction described in section 5.3. Recall that in Case 2, we must take D such that $h(D)L(f,1)$ is an integer multiple of the least positive real period of E.

5.5 Heegner Point Computations

In this section, a basic step-by-step approach to computing Heegner points will be given, as well as several sample calculations. Note that all calculations were performed with the aid of the Pari-GP calculator.

Given a strong Weil curve E defined over $\mathbb{Q}$ of rank r and conductor N, the Heegner point computation can be performed as follows:

Step 1: Compute $\epsilon =$ the sign in the functional equation for $L_E(s)$.

Step 2: Find a fundamental discriminant $D < 0$ such that $(N, D) = 1$, $D \equiv \beta^2 (\text{mod } 4N)$. If $\epsilon = +1$, restrict D further so that $h(D)\prod c_p/|T|^2 =$ an integer.

Step 3: Find $h = h(D)$ Heegner points $\omega_1, ..., \omega_h$ such that $\omega_i = (B_i + \sqrt{D})/2A_i$, $A_i \equiv 0 (\text{mod } N)$, $B_i \equiv \beta (\text{mod } 4N)$, representing the distinct classes of the ideal class group.

Step 4: Compute $U = u(\omega_1) + \cdots + u(\omega_h)$ where $u(z) = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n z}$.

Step 5: Convert U mod Λ to $P = (x, y)$.
If $\epsilon = -1$, try to recognize $x, y \in \mathbb{Q}$.
If $\epsilon = +1$, try to recognize $x, y/\sqrt{D} \in \mathbb{Q}$.

Step 6: If $\epsilon = -1$, compute $\Omega_E\Omega_{E^D}\hat{h}_E(P)$ and compare with $L_{E^D}(1)L'_E(1) = c\Omega_E\Omega_{E^D}\hat{h}_E(P)$.

If $\epsilon = +1$, compute $\Omega_E \Omega_{E^D} \hat{h}_{E^D}(P_D)$ where $P_D = (x, y/\sqrt{D})$ and compare with $L'_{E^D}(1)L_E(1) = c\Omega_E \Omega_{E^D} \hat{h}_{E^D}(P_D)$.

Example

E is the strong Weil curve given by

$$E : y^2 = x^3 - x + 1/4.$$

The conductor $N = 37$, the torsion group is trivial, the rank $r = 1$.

1. $\epsilon = -1$.
2. Choose $D = -3$ with $h(D) = 1$.
3. $\omega_1 = (-21 + \sqrt{-3})/2 \cdot 37$.
4. $U \cong 0.2046805... - 1.22569469...i$
5. $P = (-1, 1/2)$ on E,
6.

$$\Omega_E \Omega_{E^D} \hat{h}_{E^D}(P_D) \cong 0.974440434816...$$

$$L_{E^D}(1)L'_E(1) \cong 0.86616927199...$$

So we have

$$L'_{E^D}(1)L_E(1) = \frac{8}{9}\Omega_E \Omega_{E^D} \hat{h}_(P).$$

We can compare this result to the Birch and Swinnerton-Dyer conjecture which would predict that

$$L'_{E^D}(1)L_E(1) = \frac{4\Omega_E \Omega_{E^D} S_E S_{E^D} \prod c_p \langle Q, Q \rangle}{(|T_E| \cdot |T_{E^D}|)^2} \tag{5.2}$$

where S_E, S_{E^D} are the orders of the Tate-Shafaravich groups of E and E^D, respectively, $\prod c_p$ is the product of the Tamagawa numbers of E and E^D, Q is a generator of E and $|T_E|, |T_{E^D}|$ are the respective orders of the torsions subgroups of E and E^D.

One can check that E^D is the strong Weil curve of conductor $N = 333$ given by $E^D : y^2 = x^3 - 9x - \frac{27}{4}$.

Now, $\langle Q, Q \rangle = 2\hat{h}(Q)$, $S_E = 1$, $S_{E^D} = 1$, $\prod c_p = 1$, $|T_E| = 1$, and $|T_{E^D}| = 1$ so equation 5.2 becomes

$$L'_{E^D}(1)L_E(1) = 8\Omega_E \Omega_{E^D} \langle Q, Q \rangle$$

Thus, assuming the Birch and Swinnerton-Dyer conjecture, the height of the point given by our construction $\hat{h}(P)$ is $9\hat{h}(Q)$ where Q is a generator of the curve $E(\mathbb{Q})$. In fact, $P = (-1, 0) = -3(0, 1/2)$ where the point $(0, 1/2)$ is a generator of $E(\mathbb{Q})$.

Sample Heegner Point Computations

Case 1: $\epsilon = -1$

1a) $N = 83$, $D = -19$, $h(D) = 1$
$E : y^2 = x^3 + \frac{47}{48}x - \frac{199}{864}$
$\omega = (-75 + \sqrt{-19})/2 \cdot 83$
$U \cong -1.28268224...$
$P = (5/12, 1/2)$ on E.
$L'_E(1)L_{E^D}(1) = 4\Omega_E\Omega_{E^D}\hat{h}(P) \neq 0$

b) $N = 83$, $D = -43$, $h(D) = 1$
$E : y^2 = x^3 + \frac{47}{48}x - \frac{199}{864}$
$\omega = (149 + \sqrt{-43})/2 \cdot 83$
$U \cong 0.809104417526...$
$P = (17/12, -2)$ on E.
$L'_E(1)L_{E^D}(1) = 4\Omega_E\Omega_{E^D}\hat{h}(P) \neq 0$

Case 2: $\epsilon = +1$

1. $N = 19$, $D = -31$, $h(D) = 3$
$E : y^2 = x^3 - \frac{28}{3}x - \frac{1261}{108}$
$\omega_1 = (49 + \sqrt{-31})/2 \cdot 76$, $\omega_2 = (-103 + \sqrt{-31})/2 \cdot 133$, $\omega_3 = (-103 + \sqrt{-31})/2 \cdot 190$
$U \cong -2.03963... - 1.581922...i$
$P = (-14/3, -3\sqrt{-31}/2)$ on $E \to P_D = (-14/3, -3/2)$ on E^D.
$L'_{E^D}(1)L_E(1) = 4\Omega_E\Omega_{E^D}\hat{h}_{E^D}(P_D) \neq 0$

2. $N = 37$, $D = -139$, $h(D) - 3$
$E = E_0 : y^2 = x^3 - \frac{70}{3}x - \frac{4537}{108}$
$\omega_1 = (71 + \sqrt{-139})/2 \cdot 37$, $\omega_2 = (219 + \sqrt{-139})/2 \cdot 185$, $\omega_3 = (-225 + \sqrt{-139})/2 \cdot 259$
$U \cong -1.08852159... - 1.76761067...i$
$P = O$ on $E \to P_D = O$ on E^D.
$L'_{E^D}(1)L_E(1) = 0$

3. $N = 53$, $D = -55$, $h(D) = 4$
$E : y^2 = x^3 + x - 10$
$\omega_1 = (293 + \sqrt{-55})/2 \cdot 364$, $\omega_2 = (85 + \sqrt{-55})/2 \cdot 52$,
$\omega_3 = (-539 + \sqrt{-55})/2 \cdot 572$, $\omega_4 = (-331 + \sqrt{-55})/2 \cdot 884$
$U \cong -0.502573...i$
$P = (-42/11, 136\sqrt{-55}/121)$ on $E \to P_D = (-42/11, 136/121)$ on E^D.
$L'_{E^D}(1)L_E(1) = 4\Omega_E\Omega_{E^D}\hat{h}_{E^D}(P_D) \neq 0$

4. $N = 100$, $D = -39$, $h(D) = 4$
$E : y^2 = x^3 - x^2 - 33x + 62$
$\omega_1 = (-69 + \sqrt{-39})/2 \cdot 100$, $\omega_2 = (-69 + \sqrt{-39})/2 \cdot 200$,
$\omega_3 = (1131 + \sqrt{-39})/2 \cdot 1300$, $\omega_4 = (1131 + \sqrt{-39})/2 \cdot 600$
$U \cong -0.6315494811... - 0.915366...i$
$P = (329066/69277, 33523812\sqrt{-39}/65743873)$ on E
$\to P_D = (329066/69277, 33523812/65743873)$ on E^D.
$L'_{E^D}(1)L_E(1) = 8\Omega_E\Omega_{E^D}\hat{h}_{E^D}(P_D) \neq 0$

5. $N = 115$, $D = -11$, $h(D) = 1$
$E : y^2 = x^3 + 7x - \frac{43}{4}$
$\omega = (37 + \sqrt{-11})/2 \cdot 115$
$U \cong 1.34013549...i$
$P = (1, \sqrt{-11}/2)$ on $E \to P_D = (1, 1/2)$ on E^D.
$L'_{E^D}(1)L_E(1) = 4\Omega_E\Omega_{E^D}\hat{h}_{E^D}(P_D) \neq 0$

Using the Pari-GP calculator, it was often necessary to convert a given strong Weil curve to its global reduced form. In particular, this was needed to compute values of L-series and heights of points.

Chapter 6

Elliptic Curves and the Class Number Problem

The purpose of this concluding chapter is to continue the story of the class number problem from where it was left off in Chapter 2. Due to a result of Goldfeld's and the Gross-Zagier theorem, there is a connection between the construction of rational points on elliptic curves via the Heegner point construction and Gauss' class number problem.

In 1975, Goldfeld [15] proved:

Theorem 6.1 *If $h(D) < \epsilon\sqrt{|D|}/\log|D|$ with $\epsilon > 0$ sufficiently small, then there exists a real number $\beta < 1$ such that, for χ the real, odd, primitive character modulo D, then $L(\beta, \chi) = 0$. Further, β is given asymptotically as $D \to -\infty$ by*

$$1 - \beta \sim \frac{6}{\pi^2} L(1, \chi) \sum_{Q} \frac{1}{a}.$$

So β is Siegel's zero and this theorem clearly contradicts the generalized Riemann hypothesis.

In 1976, Goldfeld [16] also proved the following theorem which links the Birch and Swinnerton-Dyer conjecture to the class number problem.

Theorem 6.2 (Goldfeld) *Let $E : y^2 = 4x^3 + ax + b$ be an elliptic curve defined over $\mathbb{Q}$ with conductor N and L-function $L_E(s)$.*

Let $r = rank(E(\mathbb{Q}))$. Fix $D < 0$ a fundamental discriminant and $\mathbb{Q}(\sqrt{D})$ an imaginary quadratic field. Let χ modulo D be the real, odd, primitive Dirichlet character associated to $\mathbb{Q}(\sqrt{D})$.

Choose $\mu = 1, 2$ so that $\chi(-N) = (-1)^{r-\mu}$. If $L_E(s) \sim c_1(s-1)^r$ as $s \to 1$ then, for D and N relatively prime,

$$h(D) > \frac{c(\log|D|)^{r-\mu-1}}{r^{4r}N^{13}\exp(21\sqrt{r\log\log|D|})},$$

where c is an absolute constant independent of E.

This theorem would effectively solve the class number problem if an appropriate elliptic curve of rank $r \geq 3$ could be found. Gross and Zagier were able to find an appropriate curve by the Heegner point construction.

For a special example, $E_0 : y^2 = x^3 + 10x^2 - 20x + 8$, which is a strong Weil curve with conductor $N = 37$, $\epsilon = +1$ and choosing discriminant $D = -139$, Gross and Zagier showed that the point $P_{139} \in E_0^D(\mathbb{Q})$ is trivial. Therefore, $L'_{E_0^D}(1) = 0$ and $L_{E_0^D}(s) \sim c_1(s-1)^m$ as $s \to 1$ where $m > 1$ is the order of vanishing of $L_{E_0^D}(1)$. It can be shown that the sign in the functional equation for E_0^D is negative, so the order of vanishing must be odd. Therefore $m \geq 3$ and it can be shown numerically that $m < 4$. Therefore the so-called *analytic rank* of E_0^D is 3. It is known that the rank of E_0^D is also 3. This is Example 2 on page 37.

Therefore, the curve E_0^D satisfies the conditions in Goldfeld's theorem. Combined with Goldfeld's theorem, this gives:

Theorem 6.3 (Goldfeld,Gross,Zagier) *For every $\epsilon > 0$ there exists an effectively computable constant $c > 0$ such that $h(D) > c(\log|D|)^{1-\epsilon}$.*

Oesterlé [29] computed the constant in Goldfeld's theorem for a special elliptic curve and obtained the result:

$$h(D) > \frac{1}{7000}(\log|D|)\prod_{\substack{p|D \\ p\neq D}}\left(1 - \frac{[2\sqrt{p}]}{p+1}\right).$$

Of course, the Goldfeld, Gross and Zagier theorem along with Oesterlé's constant provides very large upper bounds for $|D|$. Other methods have had to be used as well to find all discriminants with class number equal to h. This problem has now been solved (see [1], [2], [27], [35]) for

$$h(D) = 1, 2, 3, 4, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23.$$

Bibliography

[1] S. Arno, *The imaginary quadratic fields of class number 4*, Acta Arith. **60** (1992), 321-334.

[2] S. Arno, M.L. Robinson and F.S. Wheeler, *Imaginary quadratic fields with small odd class number*, Acta Arith. **83** (1998), 295-330.

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

[4] B.J. Birch, *Diophantine analysis and modular functions*, Algebraic Geometry, (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press (1969), 35-42.

[5] B.J. Birch and N.M. Stephens, *Heegner's construction of points on the curve* $y^2 = x^3 - 1728e^3$, Seminar on number theory, Paris 1981-1982, 1-19, Birkhäuser, 1983.

[6] D.A. Buell, *Binary quadratic forms - Classical theory and modern computations*, Springer-Verlag New York Inc., 1989.

[7] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, Springer-Verlag, New York Inc., 1993.

[8] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc., **12** (1999), 521-567.

[9] J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, U.K., 1997.

[10] H. Davenport, *Multiplicative number theory*, Springer-Verlag New York Inc., 1980.

[11] M. Deuring, *Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins*, Math. Z. **37** (1933), 405-415.

[12] L.E. Dickson, *On the negative discriminants for which there is a single class of positive primitive binary quadratic forms*, Bull. Amer. Math. Soc. (2) **17** (1911), 534-537.

[13] L. Dirichlet, *Recherches sur diverse applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. **19** (1839).

[14] C.F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[15] D. Goldfeld, *An asymptotic formula relating the Siegel zero and the class number of quadratic fields*, Ann. Scuola Norm. Sup. Pisa (4) **2** (1975), 611-615.

[16] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa (4) **3** (1976), 623-663.

[17] D. Goldfeld, *Gauss' class number problem for imaginary quadratic fields*, Bull. of the Amer. Math. Soc., (1) **13** (1985), 23-74.

[18] B. Gross and D. Zagier, *Points de Heegner et derivées de fonctions L*, C. R. Acad. Sci. Paris **297** (1983), 85-87.

[19] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. **56** (1952), 227-253.

[20] H. Heilbronn, *On the class number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. (2) **5** (1934), 150-160.

[21] H. Heilbronn and E.H. Linfoot, *On the imaginary quadratic corpora of class number one*, Quart. J. Math. Oxford Ser. (2) **5** (1934), 293-301.

[22] A.W. Knapp, *Elliptic curves*, Princeton University Press, Princeton, N.J., 1992.

[23] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York Inc., 1984.

[24] J.L. Lagrange, *Recherches d'arithmétique*, Nouv. Mém. Acad. Berlin (1773), 265-312; Oeuvres, III, 693-758.

[25] E. Landau, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Göttinger Nachr. (1918), 285-295.

[26] D.H. Lehmer, *On imaginary quadratic fields whose class number is unity*, Bull. American Math. Soc. (2) **39**, (1933), 360.

[27] H. Montgomery and P. Weinberger, *Notes on small class numbers*, Acta Arith. **24** (1974), 529-542.

[28] L.J. Mordell, *On the Riemann hypothesis and imaginary quadratic fields with a given class number*, J. London Math. Soc. **9** (1934), 289-298.

[29] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Séminaire Nicolas Bourbaki, 1983-1984, Exp. 631.

[30] C.L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*, Acta. Arith. **1** (1935), 83-86.

[31] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate texts in mathematics 106, Springer-Verlag, New York, 1986.

[32] H.M. Stark, *On the "gap" in a theorem of Heegner*, J. Number Theory **1** (1969), 16-27.

[33] N. Stephens, *Computation of rational points on elliptic curves using Heegner points*, Number theory and applications (Banff, AB, 1988), 205-214.

[34] T. Tatazawa, *On a theorem of Siegel*, Japan J. Math. **21** (1951), 163-178.

[35] C. Wagner, *Class number 5, 6, and 7*, Math. Comp. (214) **65** (1996), 785-800.