University College London

Master's Project

Verifying some consequences of the Birch Swinnerton-Dyer Conjecture

Felipe Jacob

supervised by
Dr Richard Hill UCL

March 7, 2017

Contents

1 Introduction **2**

2 Elliptic Curve Invariants and the BSD Conjecture **3**
2.1 Basic definitions and the group law 3
2.2 Local Zeta Functions 6
2.3 The Hasse-Weil L-function 11
2.4 The Regulator 12
2.5 The Real Period and Sha 13
2.6 Tamagawa Numbers 14
2.7 The BSD Conjecture and Tunnell's Theorem 15

3 Modular Forms **17**
3.1 Lattices and Modular points 17
3.2 Modular Functions 19
3.3 Forms of Half-integral Weight 24
3.4 The Shimura Correspondence and Tunnell's Theorem 29

4 Galois Cohomology **31**
4.1 Group Cohmology 31
4.2 Galois Cohomology 33
4.3 Applications to Elliptic Curves 35
4.4 The Selmer and Tate-Shafarevich Groups 37

5 Calculations **39**
5.1 Introduction 39
5.2 Coefficients of Theta Series 39
5.3 Selmer Group 42
5.3.1 l-adic case 44
5.3.2 p-adic case 45
5.3.3 2-adic case 50
5.4 Tamagawa Numbers 54

6 Conclusion **62**

Bibliography **66**

Chapter 1

Introduction

In this project we will investigate some of the deep techniques employed in working out the rank of an elliptic curve. In particular, we will consider the problem of finding the rank of the curves given by

$$E_n(\mathbb{Q}) : y^2 = x^3 - n^2 x,$$

where n is odd and squarefree.

To do this we will pursue two different chains of ideas:

1. The famous Birch Swinnerton Dyer conjecture relates many invariants of an elliptic curve to a complex analytic object called the Hasse-Weil L-function. We intend to provide a self-contained explanation of all the quantities that occur in the BSD conjecture, and how they relate to the arithmetic properties of the curve. Once the theoretical ground is laid, we will calculate all these invariants for the curves E_n. This will require a variety of methods, ranging from p-adic numbers to Galois Cohomology.

2. The theory of modular forms provides techniques to deal with L-functions at a Fourier analytic level. In particular, Tunnell's theorem takes advantage of the fact that $L(E_n, s)$ are given by twists of $L(E_1, s)$ by a quadratic character to give very concise way of describing the critical values $L(E_n, 1)$. We intend to give an overview of the chain of results that imply Tunnell's theorem.

Finally, we will see that Tunnell's theorem, together with the Birch Swinnerton-Dyer conjecture, predicts that

$$a_n^2 = \#\text{Sha}(E_n) \cdot R_{E_n} \cdot 4^{\omega(n)} \cdot 0^r \tag{1.0.0.1}$$

where the a_n are certain integers associated to the Hasse-Weil L-function $L(E_n, s)$, r is the rank of E_n, $\text{Sha}(E_n)$ is the Tate-Shafarevich group, R_{E_n} is the Regulator and $\omega(n)$ is the number of prime factors of n. All these quantities will be defined in due time.

The calculations in this project will allow us to prove (see 6.0.0.4):

Theorem. *Let n be odd and squarefree. If $\text{Sha}(E_n)$ is finite, we have*

$$a_n^2 \equiv \#\text{Sha}(E_n) \cdot R_{E_n} \cdot 4^{\omega(n)} \cdot 0^r \mod 16.$$

Furthermore, if $n \equiv 3\,(8)$, this holds modulo 32.

In the (unlikely) possibility that $\text{Sha}(E_n)$ is infinite, we also formulate and prove weaker statements. Namely, we can interpret the existence of 2-torsion in $\text{Sha}(E_n)$ as saying that Equation 1.0.0.1 holds modulo 8.

Chapter 2

Elliptic Curve Invariants and the BSD Conjecture

One of the major topics in modern number theory is the study of rational solutions to cubic equations in two variables, called elliptic curves. In this project we will investigate the relationships between the arithmetic invariants of such equations and certain analytic functions. Such relationships give rise to many conjectures with powerful implications, a few of which we will discuss. We will first define the objects of interest and their invariants, and then continue with the main calculations.

2.1 Basic definitions and the group law

Definition 2.1.0.1. If K is a field, we say an **elliptic curve** over K is a smooth cubic projective curve E defined over K with at least one rational point $\mathcal{O} \in E(K)$ that we call the **point at infinity**.

With the help of algebraic geometry, we know that such curves can be put into particularly simple forms.

Proposition 2.1.0.2. *If E is an elliptic curve over K, then it is birationally equivalent to the projective completion of the curve*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1.0.1}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$. Furthermore, when $char(K) \neq 2$ (such as when K is a number field) , the affine variety also can be written as the locus of

$$E : y^2 = x^3 + ax^2 + bx + c \tag{2.1.0.2}$$

with $a, b, c \in K$. This equivalence also takes the rational point $\mathcal{O}$ to $(0 : 1 : 0)$. Conversely, an equation of the form 2.1.0.2 is an elliptic curve if

$$\Delta(E) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0,$$

i.e. if the RHS cubic has no repeated roots.

Proof. [See Sil16, Chapter III, pages 42-43]. □

Henceforth we will only consider elliptic curves $E(K)$ given by the affine model in Equation 2.1.0.2. The point $\mathcal{O}$ will always correspond to the point $(0:1:0)$ in the projective completion of $\mathbb{A}^2(K)$. We will usually take $K = \mathbb{Q}$, unless otherwise specified.

In this project we will be particularly interested in the following family of elliptic curves

Definition 2.1.0.3. The family of **quadratic twists of the curve** $E_1 : y^2 = x^3 - x$ is the family of curves

$$E_n : y^2 = x^3 - n^2 x \tag{2.1.0.3}$$

where n is a positive integer.

We will only be interested in the case where n is odd and squarefree. Such curves have a long history going back to Fermat, and are notorious for their appearance in the problem of finding right triangles with rational sides and a given area. See [Kob93] for a lot more on this story.

Elliptic curves are of particular interest primarily because, besides being a variety, they also form an abelian group. To build the group, we take the affine model in Equation 2.1.0.2 and define a geometric way to combine two points of E. This will turn out to behave like a group law.

Given two distinct points $P_1, P_2 \in E(K)$, let $P_1 * P_2$ be the third point which intersects both E and the projective line between P_1 and P_2. If $P_1 = P_2 \in E(K)$, let $P_1 * P_2$ be the other point of $E(K)$ which meets the line tangent to $E(K)$ at P_1.

In both cases the operation $*$ is well defined, since finding the coordinates of $P_1 * P_2$ amounts to solving a cubic equation with coefficients in K and 2 known roots. Finally, we set

$$P_1 + P_2 = (x_3, -y_3) \text{ where } (x_3, y_3) = P_1 * P_2.$$

The verification that the operation $+$ is indeed a group law involves either extensive case checking or some complex analysis, which we will not go into, but see [Gra11, pp. 129-137] for a sketch.

A few explicit formulas for the addition law that we will use throughout the project are given in the next proposition.

Proposition 2.1.0.4. *If $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E$ with neither being the point at infinity, and $P_1 \neq P_2$, let*

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

Then we have

$$P_1 + P_2 = (x_3, -y_3)$$

where

$$\begin{aligned} x_3 &= \lambda^2 - a - x_1 - x_2 \\ y_3 &= \lambda x_3 + (y_1 - \lambda x_1). \end{aligned} \tag{2.1.0.4}$$

If instead $P_1 = P_2$, let

$$\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}.$$

We similarly have

$$P_1 + P_2 = (x_3, -y_3)$$

where

$$\begin{aligned} x_3 &= \lambda^2 - a - 2x_1 \\ y_3 &= \lambda x_3 + (y_1 - \lambda x_1). \end{aligned} \tag{2.1.0.5}$$

Proof. [See Kob93, Chapter 1.7, page 34]. □

The following results about $E(\mathbb{Q})$ were discussed in the course MATH3705, and their proofs can be found in [ST90], chapters II and III for the case where Equation 2.1.0.2 has at least 1 rational root.

Theorem 2.1.0.5 (Mordell-Weil Theorem)**.** *The group $E(\mathbb{Q})$ is a finitely generated abelian group.*

Proof. [See ST90, Chapter III, pages 63-88]. Also see the discussion in section 4.3. □

By the classification theorem of finitely generated abelian groups, covered in MATH3201, we can write

$$E(\mathbb{Q}) = \mathrm{Tors}(E(\mathbb{Q})) \times \mathbb{Z}^r \tag{2.1.0.6}$$

for some natural number r. The subgroup $\mathrm{Tors}(E(\mathbb{Q}))$ is the (finite) set of points of finite order in $E(\mathbb{Q})$, called the **torsion points of** $E(\mathbb{Q})$.

Definition 2.1.0.6. The number r occuring in Equation 2.1.0.6 is called the **rank of** $E(\mathbb{Q})$. Finding r for an arbitrary E is one of the main problems in the theory of Elliptic Curves.

Theorem 2.1.0.7 (Nagell-Lutz Theorem)**.** *Let*

$$E : y^2 = f(x) = x^3 + ax + b$$

be an elliptic curve over $\mathbb{Q}$, and let $\Delta = -4a^3 - 27b^2$ be the polynomial discriminant of $f(x)$. If $P = (x, y)$ is a point of finite order, then either $y = 0$, in which case P has order 2, or we must have $y^2 \mid \Delta$.

Proof. [See ST90, Chapter II, pages 49-56]. □

For the curves E_n, it turns out that the only torsion points are the obvious ones of order 2.

Proposition 2.1.0.8. *The curve $E_n(\mathbb{Q})$ has 4 torsion points, and*

$$E_n(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}.$$

Proof. [See Kob93, Chapter I-9, pages 44-45]. □

2.2 Local Zeta Functions

One of the most powerful tools in all of discrete mathematics is the passing from sequences of combinatorial magnitudes $\{a_n\}$ to a formal power series

$$f(z) = \sum_{n=0}^{\infty} a_n z^n$$

called the **generating function** of $\{a_n\}$. This formal power series encapsulates the whole sequence into a single object. By letting $z \in \mathbb{C}$, we can hope the resulting analytic properties of f as a holomorphic function can be translated back to information about the coefficients a_n.

One of the main advantages to this approach is that multiplication of different generating functions acts in a combinatorially meaningful way on the coefficients of their product via a convolution

$$\sum_{n=0}^{\infty} a_n z^n \cdot \sum_{n=0}^{\infty} b_n z^n = \sum_{n=0}^{\infty} \left(\sum_{s+t=n} a_s b_t \right) z^n.$$

We can use this fact to construct more complicated series from simpler ones, and use this construction to simplify our analysis.

In number theory, the generating function of choice usually takes a different form called the **Dirichlet series of** $\{a_n\}$

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \ s \in \mathbb{C}.$$

This is useful to us since the convolution now takes a multiplicative form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \cdot \sum_{n=1}^{\infty} \frac{b_n}{n^s} = \sum_{n=1}^{\infty} \left(\sum_{s \cdot t=n} a_s b_t \right) n^{-s}$$

which translates better the combination of sequences that appear in number theory. What we have is a situation in which all objects of size n are obtained by stitching together s objects of size t, where s and t are some divisors of n. For a few neat elementary applications of this principle, see [Wil06, Section 2.6, pages 59-68].

Example 2.2.0.1. The **Riemann Zeta Function** is the Dirichlet series of $\{1\}_{n=1}^{\infty}$ given by

$$\zeta(s) = \sum_{n=1} \frac{1}{n^s},$$

and takes a prominent role in analytic number theory. As a consequence of uniqueness of factorization in $\mathbb{Z}$, we can also write

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - p^{-s}\right)^{-1}.$$

This is called the **Euler product** of ζ.

Example 2.2.0.2. Let $d_k(n)$ be the number of ordered ways of writing n as a product of k factors. Then we can write

$$d_k(n) = \sum_{a_1 a_2 \cdots a_k = n} 1.$$

Using the convolution formula, we get that

$$\sum_{n=1}^{\infty} \frac{d_k(n)}{n^s} = \zeta^k(s),$$

so analytic information about ζ can be used to study the growth of $d_k(n)$.

We can generalise generating functions further by changing the denominator of the Dirichlet series.

Example 2.2.0.3. Let $K : \mathbb{Q}$ be a number field and let $\mathcal{O}_K$ be the ring of algebraic integers of K. The **Dedekind-Zeta function of** K is a series given by

$$\zeta(K, s) = \sum_{I \lhd \mathcal{O}_K} \frac{1}{||I||^s}$$

where the sum ranges over all nonzero ideals of $\mathcal{O}_K$. Since $\mathcal{O}_K$ is a Dedekind domain, it has the property of unique factorization of ideals, so we can also write the Euler product

$$\prod_P \left(1 - ||P||^{-s}\right)^{-1}.$$

Here P ranges over the maximal ideals of $\mathcal{O}_K$.

The importance of this example is that now the convolution is no longer multiplicative in $\mathbb{Z}$, but in the ideals I of $\mathcal{O}_K$. This allows us to consider arithmetic sequences that combine multiplicatively on larger number fields.

Example 2.2.0.4. Let $K = \mathbb{Q}(\sqrt{-2})$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-2}]$. Later we will find a simple formula for the coefficient of n^{-s} of $\zeta(K, s)$ when n is odd and squarefree.

We can also define a function $d_k(K, n)$ which counts the number of ways of writing an ideal of norm n as a product of k ideals in $\mathcal{O}_k$, i.e. the number of k-tuples $P_1, \ldots, P_k$ such that $||P_1 \cdots P_k||_{\mathcal{O}_K} = n$. From the convolution rule for number fields, we get

$$\sum_{I \lhd \mathcal{O}_K} = \frac{d_k(K, ||I||)}{||I||^s} = \zeta^k(K, s).$$

Thus, we can try to understand factorization of ideals in $\mathcal{O}_K$ from the analytic properties of $\zeta^k(\mathbb{Z}[\sqrt{-2}], s)$.

The zeta functions we are going to be most interested in will help us capture the behaviour of an elliptic curve $E(K)$ locally, i.e. when $K = \mathbb{F}_p$.

Let p be an odd prime and $\mathbb{F}_p$ be the unique field of p elements. We say that a polynomial $f \in \mathbb{F}_p[x, y]$ is **absolutely irreducible** if it is irredubicle in the algebraic closure $\overline{\mathbb{F}}_p[x, y]$.

Proposition 2.2.0.5. *Let $f \in \mathbb{F}_p[x,y]$ be absolutely irreducible, and assume the variety $V_f(\overline{\mathbb{F}}_p)$ is nonsingular. Then the coordinate ring*

$$C_f = \frac{\mathbb{F}_q[x,y]}{(f)}$$

is a Dedekind domain with finite quotients. In particular, it has the property of unique factorization of ideals.

Proof. [See Lor96, Corollary 2.7, page 229]. □

Inspired by our previous examples, we can define a zeta function for V_f. Let

$$\zeta(V_f, \mathbb{F}_p, s) = \sum_{I \lhd C_f} \frac{1}{||I||^s}$$

where the sum is over all ideals of C_f. Here the norm $||I||$ is defined to be the number of elements in C_f/I. Since C_f has unique factorization of ideals, we also get a Euler product

$$\zeta(V_f, \mathbb{F}_p, s) = \prod_{M \in \mathrm{Max}(C_f)} \left(1 - ||M||^{-s}\right)^{-1}$$

where $\mathrm{Max}(C_f)$ is the set of maximal ideals of C_f. If we let

$$b_k = \#\{M \in \mathrm{Max}(C_f)\,;\, |C_f/M : \mathbb{F}_p| = k\},$$

then by definition $||M|| = |C_f/M| = p^k$, so we get

$$\zeta(V_f, \mathbb{F}_p, s) = \prod_{n=1}^{\infty} (1 - q^{-sn})^{-b_n}.$$

Now let $z = p^{-s}$ and let $Z(z) = \zeta(V_f, \mathbb{F}_p, s)$. Taking logarithms we ge

$$\begin{aligned}
\log(Z(z)) &= -\sum_{n=1}^{\infty} b_n \log(1 - z^d) \\
&= \sum_{n=1}^{\infty} \left(\sum_{k=1}^{\infty} \frac{z^{nk}}{k} \right) \\
&= \sum_{n=1}^{\infty} \big(\sum_{k|n} k b_k \big) \frac{z^n}{n}.
\end{aligned}$$

Proposition 2.2.0.6. *We have*

$$\sum_{k|n} k b_k = \#V_f(\mathbb{F}_{p^r})$$

where $\#V_f(\mathbb{F}_{p^n})$ is the number of roots of f in the unique field of p^n elements.

Proof. [See Lor96, Proposition VII-3.5, page 232]. □

The above remarks motivate the following definition:

Definition 2.2.0.7. Let V be a variety over $\mathbb{F}_p$. The **local zeta function of V at p** is the formal power series

$$Z(V,p,z) = \exp\left(\sum_{r=1}^{\infty} \#V(\mathbb{F}_{p^r})\frac{z^r}{r}\right) \tag{2.2.0.1}$$

where $\#V(\mathbb{F}_{p^r})$ is the number of points of V in the (unique) field of p^r elements.

Example 2.2.0.8 (Point)**.** If $V = (x_0 : y_0 : z_0)$ is a point, then $\#V(\mathbb{F}_{p^r}) = 1$, so

$$\begin{aligned} Z(V,p,z) &= \exp\left(\sum_{r=1}^{\infty} \frac{z^r}{r}\right) \\ &= \exp(-\log(1-z)) \\ &= \frac{1}{1-z}. \end{aligned}$$

Example 2.2.0.9 (Affine Space)**.** If $V = \mathbb{A}^n$ is the affine n-space , $\#\mathbb{A}^n(\mathbb{F}_{p^r}) = p^{rn}$, so

$$\begin{aligned} Z(\mathbb{A}^n) &= \exp\left(\sum_{r=1}^{\infty} \frac{(pz)^r}{r}\right) \\ &= \exp(-\log(1-p^n z)) \\ &= \frac{1}{1-p^n z} \end{aligned}$$

Example 2.2.0.10 (Projective Space)**.** If $V = \mathbb{P}^n$ is the projective n-space, then $\#\mathbb{P}^n(\mathbb{F}_{p^r}) = 1 + p^r + \cdots + p^{nr}$. So

$$\begin{aligned} Z(\mathbb{P}^n) &= \exp\left(\sum_{r=1}^{\infty}\sum_{s=0}^{n}\left(\frac{z^r}{r}\right)\right) \\ &= -\sum_{s=0}^{n} \log(1-p^n z) \\ &= \frac{1}{(1-z)(1-pz)\cdots(1-p^n z)} \end{aligned}$$

We note, in tandem with our philosophy of generating functions and convolutions, the expression

$$Z(\mathbb{P}^n) = Z(\mathbb{A}^0) \times Z(\mathbb{A}^1) \times \cdots \times Z(\mathbb{A}^n)$$

beautifully mimics the geometric construction of $\mathbb{P}^n$ from a point, attaching one cell of each dimension.

Turning to the curves in our family E_n, we will show later (see 5.4.0.1) that E_n is nonsingular at p if and only if $p \nmid 2n$. This will affect the form of its local zeta function.

At the primes where it has bad reduction, $Z(E_n, p, z)$ is identical to the zeta function of a projective line:

Proposition 2.2.0.11. *If $p \mid 2n$, then*

$$Z(E_n, p, z) = \frac{1}{(1-z)(1-pz)}.$$

Proof. There are two cases to consider.

- If $p = 2$, the affine equation takes the form

  $$E_2 : y^2 = x^3 + x,$$

  with the single point at infinity $(0 : 1 : 0)$.

  But in $\mathbb{F}_{2^r}$, the map $x \mapsto x^2$ is injective since

  $$x^2 = y^2 \implies x^2 - y^2 = (x-y)^2 = 0 \implies x = y,$$

  where the middle equality follows from characteristic 2. Since $\mathbb{F}_{2^r}$ is finite, the squaring map must also be surjective, so all elements have unique square roots. Thus,

  $$\#E_n(\mathbb{F}_{2^k}) = 1 + \#\mathbb{F}_{2^k} = 1 + 2^k,$$

  and

  $$\begin{aligned} Z(E_n, 2, z) &= \exp\left(\sum_{r=1}^{\infty}(1+2^r)\frac{z^r}{r}\right) \\ &= \exp\left(\sum_{r=1}^{\infty}\frac{z^r}{r}\right)\exp\left(\sum_{r=1}^{\infty}\frac{(2z)^r}{r}\right) \\ &= \frac{1}{(1-z)(1-2z)}. \end{aligned}$$

- If $p \mid n$, the equation of the curve becomes

  $$E_p : y^2 = x^3,$$

  again with a single point at infinity $(0 : 1 : 0)$.

  Since p is odd, each element in $\mathbb{F}_{p^r}$ has either 0 or 2 square roots. Let χ be the quadratic character in $\mathbb{F}_{p^r}$. Then

  $$\begin{aligned} \#E_n(\mathbb{F}_{p^r}) &= 1 + \sum_{x\in\mathbb{F}_{p^r}}\big(1+\chi(x^3)\big) = 1 + p^r + \sum_{x\in\mathbb{F}_{p^r}}\chi(x) \\ &= 1 + p^r. \end{aligned}$$

  The last sum is 0 since there are as many quadratic residues as quadratic non-residues in $\mathbb{F}_{p^r}$. Thus, again we get

  $$\begin{aligned} Z(E_n, p, z) &= \exp\left(\sum_{r=1}^{\infty}(1+p^r)\frac{z^r}{r}\right) \\ &= \frac{1}{(1-z)(1-pz)}. \end{aligned}$$

□

For the primes where E_n has good reduction, Equation 2.2.0.1 takes the form of a quadratic rational function in z:

Proposition 2.2.0.12. *If $p \nmid 2n$, then*

$$Z(E_n, p, z) = \frac{1 - 2a_p z + pz^2}{(1-z)(1-pz)}$$

where $a_p = \Re(\alpha)$, and α is the complex number $i\sqrt{p}$ if $p \equiv 3\,(4)$ or an element of $\mathbb{Z}[i]$ of norm p congruent to $(\frac{n}{p})$ modulo $2+2i$ if $p \equiv 1\,(4)$.

Proof. [See Kob93, Chater II-2, pages 59-61]. □

2.3 The Hasse-Weil L-function

The last step in this chain of generalisations is to let the prime p vary. Following the philosophy of convolutions, it is natural to consider the product

$$\prod_p Z(V, p, z_p),$$

over all primes numbers, which incorporates information about the variety V in all possible finite fields. Making the change of variables $z_p = p^{-s}$, we arrive at the next definition.

Definition 2.3.0.1. The **Hasse-Weil L-function of** V is the function

$$L(V, s) = \prod_p Z(V, p, p^{-s})$$

where the product is over all prime numbers p.

Example 2.3.0.2. If V is a point, we saw that

$$Z(V, p, z) = \frac{1}{1-z},$$

so

$$L(V, s) = \prod_p Z(V, p, p^{-s}) = \prod_p \frac{1}{1-p^{-s}} = \zeta(s)$$

is the familiar Riemann-Zeta function.

Example 2.3.0.3. If $V = \mathbb{P}^n$ is the projective n-space, we saw that

$$Z(\mathbb{P}^n, p, z) = \frac{1}{(1-z)(1-pz)\cdots(1-p^n z)},$$

so

$$\begin{aligned} L(\mathbb{P}^n, s) &= \prod_p \frac{1}{(1-p^{-s})(1-p^{1-s})\cdots(1-p^{n-s})} \\ &= \zeta(s)\zeta(1-s)\cdots\zeta(n-s). \end{aligned}$$

For the elliptic curves E_n, the local zeta function at p may take two possible forms depending on wether $\Delta(E_n)$ is a multiple of p. Putting both results together gives

$$\begin{aligned}\prod_p Z(E_n, p, p^{-s}) &= \prod_{p\nmid 2n} \frac{1 - 2a_p p^{-s} + p^{2-s}}{(1-p^{-s})(1-p^{1-s})} \cdot \prod_{p|2n} \frac{1}{(1-p^{-s})(1-p^{1-s})} \\ &= \zeta(s)\zeta(s-1) \prod_{p\nmid 2n} (1 - 2a_p p^{-s} + p^{2-s})\end{aligned}$$

where we spotted the Euler product of the Riemann-Zeta function in the denominators. The a_p are the real numbers obtained on Proposition 2.2.0.12.

Taking the reciprocal and clearing off the Riemann-Zeta factors, we arrive at the next definition.

Definition 2.3.0.4. The **Hasse-Weil L-function** of E_n is written

$$L(E_n, s) = \frac{\zeta(s)\zeta(s-1)}{\prod_{p\nmid 2n} Z(E, p, p^{-s})} = \prod_{p\nmid 2n} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}. \tag{2.3.0.1}$$

It is this function that will play the main role in the statement of the Birch Swinnerton-Dyer conjecture. The usefulness of considering L-functions comes not so much in analyzing a single curve, but in understanding the behaviour of certain families of curves which have similar L-functions.

In the case of our family E_n, let

$$L(E_1, s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s}$$

be the Dirichlet series corresponding to $L(E_1, s)$. Then, it turns out ([See Kob93, Pages 80-81]) that $L(E_n, s)$ has the related Dirichlet series

$$L(E_n, s) = \sum_{m=1}^{\infty} \chi_n(m) \frac{a_m}{m^s}.$$

where $\chi_n(m)$ is the Jacobi symbol $\left(\frac{n}{m}\right)$ with the exception that we let $\chi_n(2) = 0$.

Thus, the series for $L(E_n, s)$ is what is called a **twist of $L(E_1, s)$ by the character** χ_n. This justifies we calling the curves E_n the family of quadratic twists of E_1.

2.4 The Regulator

Going back to considering elliptic curves, the next invariant measures the rate of growth of the complexity of points as we take higher and higher multiples of a fixed point. We first need a few definitions.

Definition 2.4.0.1. Let $P = (\frac{a}{b}, y) \in E(\mathbb{Q}), (a, b) = 1$. The **height of** P is defined to be the number

$$H(P) = \max\{|a|, |b|\}.$$

It turns out that taking an integer multiple of a point of E has an exponential effect on its height, so we prefer to work with the logarithmic height $h(P) = \log(H(P))$. To better yet capture the now almost linear behaviour of $h(P)$, we define

Definition 2.4.0.2 (Neron-Tate height)**.** Let $P \in E(\mathbb{Q})$. Then the **Neron-Tate height of** P is defined to be

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

It turns out that the Neron-Tate height enables us to define an inner product on $E(\mathbb{Q})$.

Definition 2.4.0.3 (Neron-Tate pairing)**.** Let $P, Q \in E(\mathbb{Q})$. Then the pairing

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

is an inner product on $E(\mathbb{Q})$ called the **Neron-Tate pairing**.

We will use the Neron-Tate pairing to define an invariant that plays a role similar to that of the determinant of a linear map in measuring the size of the image of the unit cube.

Definition 2.4.0.4 (Regulator)**.** Let $P_1, \dots P_r$ be a basis for $\frac{E(\mathbb{Q})}{\mathrm{Tors}(E)}$. Then the **regulator of** $E(\mathbb{Q})$ is the number

$$R_E = \det(\langle P_i, P_j\rangle)_{1\le i,j\le r}.$$

The importance of the regulator is justified by the following proposition

Proposition 2.4.0.5. *Let r be the rank of $E(\mathbb{Q})$.*
If $r = 0$ then $\#E(\mathbb{Q}) = \#\mathrm{Tors}(E)$.
If $r \ge 1$ then, as $x \to \infty$,

$$\#\{P \in E(\mathbb{Q}) \mid \hat{h}(P) \le x\} \approx \frac{\#\mathrm{Tors}(E)}{R_E^{1/2}} B_r x^{r/2}$$

where B_r is the volume of the r-dimensional unit ball.

Proof. [See Gra11, Chapter 13.7, page 127]. □

Remark 2.4.0.6. To check that all definitions given in this section behave precisely as stated, see [Gra11, Chapter 13.7-8, pages 123-127].

2.5 The Real Period and Sha

Before we are ready to state the main conjecture, we need to define a few other invariants of E.

Definition 2.5.0.1 (Real Period)**.** The **real period of** E is defined to be the real number

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y}.$$

For the family E_n of quadratic twists of E_1, it turns out that

$$\Omega_{E_n} = \frac{1}{\sqrt{n}}\,\Omega_{E_1} = \frac{2}{\sqrt{n}}\int_1^\infty \frac{dx}{\sqrt{x^3-x}}.$$

The last integral cannot be evaluated in terms of elementary functions, but its value is a real number $\beta \approx 2.622$.

The next invariant that will appear in the BSD conjecture is the **Tate Shafarevich group** $\text{Sha}(E)$, which will be defined in 4.4.0.3. It is an abelian group which intuitively measures the hardness of working out the rank of $E(\mathbb{Q})$ by local methods, and is conjectured to be finite.

2.6 Tamagawa Numbers

Note that the local zeta function of E gives us essentially no information to Equation 2.3.0.1 at the primes where the curve is singular. The arithmetic data at those primes enters the BSD conjecture by means of the Tamagawa Numbers. Let

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c$$

be an elliptic curve $\mathbb{Q}$ with coefficients $a, b, c \in \mathbb{Z}$.

If p is not a factor of $\Delta(E)$, the discriminant of the cubic polynomial $f(x)$, then the reduction $\tilde{E} : y^2 \equiv x^3 + ax^2 + bx + c\,(p)$ is also an elliptic curve over $\mathbb{F}_p$. The group $E(\mathbb{F}_p)$ turns out to be closely related to $E(\mathbb{Q})$.

Proposition 2.6.0.1 (Reduction Modulo p)**.** *If p is not a factor of $\Delta(E)$, the reduction map*

$$E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p)$$

is a group homomorphism.

Proof. [See ST90, Chapter IV, pages 121-123]. □

If p is a factor of ΔE then $\tilde{E}(\mathbb{F}_p)$ has no natural group law, but

$$\tilde{E}(\mathbb{F}_p)_{ns} := \{P \in \tilde{E}(\mathbb{F}_p) \mid P \text{ is nonsingular}\}$$

is still a group with addition of points defined in the same way as for $E(\mathbb{F}_p)$.

Looking at E in the completion $\mathbb{Q}_p$, we still have a map

$$E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p)$$

. If we let $E(\mathbb{Q}_p)_0$ be the preimage of $\tilde{E}(\mathbb{F}_p)_{ns}$ we get a group homomorphism

$$E(\mathbb{Q}_p)_0 \to \tilde{E}(\mathbb{F}_p)_{ns}.$$

Definition 2.6.0.2. The **Tamagawa Number of E at p** is the number of cosets

$$c_p = \left|\frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0}\right|.$$

If $p \nmid \Delta(E)$ then $c_p = 1$.

In section 5.4, we will compute the Tamagawa numbers at all primes for the family of quadratic twists E_n.

2.7 The BSD Conjecture and Tunnell's Theorem

During the 1960s, Bryan Birch and Peter Swinnerton-Dyer formulated, based on numerical evidence, an influential conjecture relating the Hasse-Weil L-function to the arithmetic invariants of E.

Conjecture 2.7.0.1 (Birch Swinnerton-Dyer Conjecture)**.** *The Hasse-Weil L-function $L(E,s)$ can be written as*

$$L(E,s) = C(s-1)^r + O((s-1)^{r+1})$$

where

$$C = \frac{\#\mathrm{Sha}(E)\,\Omega_E R_E}{\#Tors(E(\mathbb{Q}))^2}\prod_p c_p \tag{2.7.0.1}$$

In particular, setting $s=0$, it predicts the value of

$$0^r \cdot \frac{\#\mathrm{Sha}(E)\,\Omega_E R_E}{\#\mathrm{Tors}(E(\mathbb{Q}))^2}\prod_p c_p.$$

In this project we will show that the predicted value for $L(E_n,1)$ is correct modulo 16.

The BSD conjecture is particularly powerful to gather information about parametrised families of elliptic curves. We can then form a parametric family of L-functions and hope that, by analysing how they change as we range through the family, we can recover useful arithmetic information about the original curves.

This can be seen quite clearly for the E_n, since even though it is very difficult to tackle all of them together artihmetically, their L-functions are just twists of $L(E_1,s)$ by a quadratic character. This idea culminates in the following remarkable result, proven using the machinery of modular forms, which shows that the critical value $L(E_n,1)$ takes a particularly simple form.

Theorem 2.7.0.2 (Tunnell's Theorem)**.**

$$L(E_n,1) = \begin{cases} \frac{\beta}{4\sqrt{n}}a_n^2 & \text{if } n \text{ is odd} \\ \frac{\beta}{2\sqrt{n}}a_{n/2}'^2 & \text{if } n \text{ is even} \end{cases} \tag{2.7.0.2}$$

where the a_i, a_i' are coefficients of the fourier expansions of the functions f, f' given by

$$f(z) = \sum_{m=-\infty}^{\infty} a_m q^m = (\Theta(z)-\Theta(4z))\left(\Theta(32z)-\frac{1}{2}\Theta(8z)\right)\Theta(2z) \tag{2.7.0.3}$$

and

$$f'(z) = \sum_{m=-\infty}^{\infty} a_m' q^m = (\Theta(z)-\Theta(4z))\left(\Theta(32z)-\frac{1}{2}\Theta(8z)\right)\Theta(4z) \tag{2.7.0.4}$$

with $q = e^{2\pi i z}$.

Here $\Theta(z)$ is the theta-function given by

$$\Theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2} \text{ where } q = e^{2\pi iz}$$

and

$$\beta = \int_1^{\infty} \frac{dx}{\sqrt{x^3 - x}}.$$

Proof. [See Tun83, pages 325-328]. □

In this project we will take advantage of the fact that the coefficients of $L(E_n, 1)$ are given by relatively simple arithmetic functions, and use that to verify the BSD conjecture modulo 16 for the family E_n.

To do this we will first compute all the invariants of E_n, and then find a simple form for the coefficients of f and f' modulo a high enough power of 2. This will enable us to predict the rank of E_n and, in some cases, the size of $\text{Sha}(E_n)$..

Chapter 3

Modular Forms

Our goal in this section is to sketch the chain of results from the theory of modular forms that make it possible to write the critical values $L(E_n, 1)$ of the Hasse-Weil L-function in terms of Theta functions.

3.1 Lattices and Modular points

Definition 3.1.0.1. A **lattice** L in the complex plane is an additive subgroup of the form

$$L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2, \;\; \omega_1, \omega_2 \in \mathbb{C}$$

where ω_1 and ω_2 are not in the same line through the origin. A base $\langle \omega_1, \omega_2 \rangle$ is said to be oriented if ω_1/ω_2 is in the upper half plane $\mathbb{H}$.

From now on, we will write $\Gamma := SL(2, \mathbb{Z})$. A lattice L will also be called a **modular point for** Γ. Lattices have the following basic properties:

Proposition 3.1.0.2 (Properties of Lattices)**.** *Let $L = \langle \omega_1, \omega_2 \rangle, L' = \langle \omega_1', \omega_2' \rangle$ be lattices. We have:*

(i) *$L = L'$ as a subgroup of $\mathbb{C}$ if and only if there exists a matrix $M \in \Gamma$ such that $(\omega_1', \omega_2') = M(\omega_1, \omega_2)$ as vectors in $\mathbb{C}^2$.*

(ii) *$\mathbb{C}/L$ and $\mathbb{C}/L'$ are analytically isomorphic as additive groups if and only if L and L' are homothetic, i.e. $L' = \alpha L$ for some $\alpha \in \mathbb{C}$.*

(iii) *$\mathbb{C}/L$ is analytically isomorphic to $\mathbb{C}/\langle \tau, 1 \rangle$ where $\tau = \omega_1/\omega_2$.*

(iv) *Let $\tau, \tau' \in \mathbb{H} = \{z \in \mathbb{C} \,|\, \Im(z) > 0\}$. Then $\mathbb{C}/\langle \tau, 1 \rangle \simeq \mathbb{C}/\langle \tau', 1 \rangle$ if and only if there exists is a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ such that*

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

When this is true we will write $\tau' = M\tau$.

Proof. The algebraic bits are standard calculations. For the results on analytic isomorphisms, see [Loz78, Appendix B.6, pages 168-169]. □

Our motivation for introducing lattices comes from the following facts:

Proposition 3.1.0.3 (Uniformization Theorem)**.** *Let $L = \langle \omega_1, \omega_2 \rangle$ be a lattice. Then*

(i) $\mathbb{C}/L$ is analytically isomorphic as an additive group to an elliptic curve in $\mathbb{P}^2(\mathbb{C})$.

(ii) Every elliptic curve over $\mathbb{C}$ is obtained in this way.

Proof. [See Gra11, Pages 131-134 and 136-137]. □

Corollary 3.1.0.4. *The isomorphism classes of elliptic curves over $\mathbb{C}$ are in one-to-one correspondence to $\mathbb{H}/\Gamma$ under the action of Proposition 3.1.0.2 (iv).*

Thus, the set $\mathbb{H}/\Gamma$ can be considered as a moduli space for elliptic curve over $\mathbb{C}$.

Definition 3.1.0.5. It turns out to be useful to consider moduli spaces for elliptic curves with some extra structure. We define:

(i) A "**modular point for** Γ" s a lattice L.

(ii) A "**modular point for** $\Gamma_1(N)$" s a pair (L, t) where L is a lattice and $t \in \mathbb{C}/L$ is a point of exact order N.

(iii) A "**modular point for** $\Gamma_0(N)$" s a pair (L, S) where L is a lattice and $S < \mathbb{C}/L$ is a subgroup of order N.

(iv) A "**modular point for** $\Gamma(N)$" s a pair $(L, \{t_1, t_2\})$ where $t_1, t_2 \in \mathbb{C}/L$ are a basis for the points of order N.

From the Uniformization Theorem, we know these correspond to elliptic curves over $\mathbb{C}$ with some extra N-torsion data. As it turns out, on each case we can find moduli spaces for equivalence classes of modular points as a quotients $\mathbb{H}/\Gamma'$, where Γ' are certain subgroups of Γ. This will justify the choice of notation for each Γ'.

Definition 3.1.0.6. We define the following subgroups of Γ.

$$\Gamma_1(N) = \left\{ M \in \Gamma; M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

$$\Gamma_0(N) = \left\{ M \in \Gamma; M \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$$

$$\Gamma(N) = \left\{ M \in \Gamma; M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

where $*$ denotes that there are no congruence conditions on that slot.

It turns out that these groups are the right candidates to form moduli spaces of more general modular points.

Proposition 3.1.0.7. *For each $\Gamma' = \Gamma_1(N), \Gamma_0(N), \Gamma(N)$, the equivalence classes of isomorphic modular points for Γ' are precisely given by $\mathbb{H}/\Gamma'$ under the action of Proposition 3.1.0.2 (iv).*

If $\Gamma' < \Gamma$ contains $\Gamma(N)$ for some N, it is called a **congruence subgroup of level** N.

We also define a family of operators that act on modular points from $\Gamma_1(N)$. Let $\mathcal{L} = \oplus \mathbb{Q}(L,t)$ be the $\mathbb{Q}$-vector space of linear combinations of modular points (L,t) for $\Gamma_1(N)$. Here the sum is over all lattices L with a tagged point t of order N.

Definition 3.1.0.8 (Hecke Operators)**.** The **Hecke operator** T_n is the linear map $T_n : \mathcal{L} \to \mathcal{L}$ acting on each basis vector $e_{L,t}$ by

$$T_n((L,t)) = \frac{1}{n}\sum_{L'}(L',t).$$

The summation is over all lattices L' containing L such that

(i) L'/L is a subgroup of $\mathbb{C}/L$ of order n

(ii) t also has order N in L'.

We note that the sum is finite. This is because by condition (i), any lattice L' corresponds corresponds to a subgroup of order n in $\frac{1}{n}L/L' \simeq (\mathbb{Z}/n\mathbb{Z})^2$.

3.2 Modular Functions

In this section we will define certain spaces of functions, called modular forms, which transform nicely with respect to the groups in the previous section. These functions will turn out to be highly symmetrical. This symmetry, in turn, conveniently forces them to live in certain finite dimensional vector spaces. Thus, whenever we encounter a function which transforms similarly to a known modular form, we can hope to find it in the corresponding vector space as a linear combination of previously known modular forms.

Our ultimate goal, and the main result of Tunnell's Theorem, is to find a modular form which transforms similarly to the L-functions $L(E_n, s)$. This will enable us to write the critical values $L(E_n, 1)$ in terms of a explicitly describable function.

In order for this program to work, we will need to define increasingly more complicated transformation rules. It will turn out that the odd coefficients of $L(E_n, s)$ will be related to a special function living in the space $S_{3/2}(\tilde{\Gamma}_0(128))$. In the next sections we build up the vocabulary required to state the main results that make this possible.

Definition 3.2.0.1. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called **weakily modular of weight** k if for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and $z \in \mathbb{H}$,

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

Furthermore,

(i) If f has a Fourier series

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q^n,$$

where $q = e^{2\pi i z}$, with at most finitely many nonzero a_n for $n < 0$, then f is called a **modular function of weight** k.

(ii) If $a_n = 0$ for all $n < 0$, f is called a **modular form of weight** k. The space of such functions is written $M_k(\Gamma)$.

(iii) If we further have $a_0 = 0$, f is called a **cusp form of weight** k. The space of such functions is written $S_k(\Gamma)$.

Remark 3.2.0.2. If $f \in S_k(\Gamma)$ and we further have $a_1 = 1$, we say f is **normalized**. It is clear that for any cusp form $f = \sum a_n q^n$, $a_1^{-1} f$ is a normalized cusp form.

Substituting $M = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ we see that there are no nonzero modular functions of weight k if k is odd. As we mentioned in the introduction to this section, the spaces of modular / cusp forms are particularly useful because they are also finite dimensional vector spaces over $\mathbb{C}$.

Proposition 3.2.0.3. *Let k be an even positive integer. Then*

$$\dim M_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1, & \text{if } k \not\equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor, & \text{if } k \equiv 2 \mod 12 \end{cases}$$

$$\dim S_k(\Gamma) = \begin{cases} \lfloor \frac{k}{12} \rfloor, & \text{if } k \not\equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor - 1, & \text{if } k \not\equiv 2 \mod 12 \end{cases}$$

Proof. The proof comes by looking at the possible residues of f using a contour integral along a fundamental domain of $\mathbb{H}/\Gamma$. [See Kob93, Propositions 8-9, Pages 115-118]. □

Example 3.2.0.4 (Eisenstein Series)**.** Let k be an even integer greater than 2 and set

$$E_k(z) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n)=1}} \frac{1}{(mz+n)^k}.$$

Then $E_k \in M_k(\Gamma)$. It is easy to see that E_k transforms correctly under Γ, and computing its Fourier expansion one can see that it is indeed a modular form.

Example 3.2.0.5 (Discriminant Form)**.** Let $\Delta : \mathbb{H} \to \mathbb{C}$ be the **discriminant form** is defined by

$$\Delta(z) = \frac{(2\pi)^{12}}{1728} \left(E_4(z)^3 - E_6(z)^2 \right).$$

One can show that $\Delta(z) \in S_{12}(\Gamma)$, so it is a nonzero cusp form of the lowest possible weight. Under our interpretation of $\mathbb{H}/\Gamma$ as a moduli space, $\Delta(z)$ turns out to be the familiar discriminant for the elliptic curves associated to the modular point given by z. If the curve $y^2 = x^3 + ax + b$ comes from the equivalence class of a lattice $\langle z, 1 \rangle$, we have

$$\Delta(z) = -16(4a^3 + 27b^2).$$

This provides a very indirect proof that isomorphic elliptic curves have the same discriminant.

We now generalize our definitions to congruence subgroups. To do this, we introduce the following notation: for $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $f : \mathbb{H} \to \mathbb{C}$, write

$$f(z)|[M]_k = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right)$$

Definition 3.2.0.6. Let Γ' be one of the congruence subgroups of Γ. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called **weakily modular of weight** k **for** Γ' if for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma'$ and $z \in \mathbb{H}$,

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

Since Γ' is a congruence subgroup, it contains $\Gamma(N)$ for some $N \geq 1$. In particular,

$$f\left(\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) z\right) = f(z+N) = f(z),$$

so f is N periodic. Let

$$f(z) = \sum_{n \in \mathbb{Z}} a_n (q_N)^n$$

where $q_N = e^{2\pi i z/N}$ be a Fourier expansion for f.

(i) If for each $M \in \Gamma'$, the function $f(z)|[M]_k$ has a fourier expansion with finitely many nonzero negative terms, then f is called a **modular function of weight** k **for** Γ'.

(ii) If furthermore all negative terms in the Fourier expansions of each $f(z)|[M]_k$ are 0, then f is called a **modular form of weight** k **for** Γ'. We also say f **is holomorphic at the cusps**. The space of such functions is written $M_k(\Gamma')$.

(iii) If the coefficient a_0 in all Fourier expansions from the previous items are also 0, then f is called a **cusp form of weight** k **for** Γ'. We also say f **vanishes at the cusps**. The space of such functions is written $S_k(\Gamma')$.

If f is a form for a congruence subgroup $\Gamma(N)$, we can choose N to be the least possible. In other words, we can choose the least N such that f is N-periodic along the real axis. We then say is f a **form of level** N.

Definition 3.2.0.7. If $f \in M_k(\Gamma(N))$ but f is also in $M_k(\Gamma(M))$ for some positive divisor M of N, we say f is a **old form of** $M_k(\Gamma(N))$. The space of old forms is written $M_k^{\text{old}}(\Gamma(N))$. We can define the space $S_k^{\text{old}}(\Gamma(N))$ of old cusp forms in the same way.

In order to get more interesting modular forms, it will be necessary to consider one further generalisation. Let $f \in M_k(\Gamma_1(N))$ and let χ be a Dirichlet character modulo N. we define

$$M_k(N,\chi) = \{f \in M_k(\Gamma_1(N)) \mid f(z)|[\gamma]_k = \chi(d)f(z), \text{ for all } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)\}$$

Example 3.2.0.8. Let

$$\Theta^2(z) = \left(\sum_{n \in \mathbb{Z}} q^{n^2}\right)^2.$$

Then $\Theta^2 \in M_1(4,\chi)$ where $\chi(d) = (-1)^{(d-1)/2}$. This is obtained in [Kob93, Proposition 30] by carefully consdering how Θ^2 transforms under a set of generators for $\Gamma_1(4,\chi)$. [Kob93, Proposition 28] further shows that $M_1(4,\chi) = M_1(\Gamma_1(4))$, so in this case we recover a familiar congruence subgroup.

As we noted before, there is a one-to-one correspondence between the points $z \in \mathbb{H}$ and lattices homothetic to $\langle z, 1\rangle$. Extending this analogy to functions, let $f \in M_k(\Gamma_1(N))$. We can define a complex valued function F on the set of all modular points (L, t) for $\Gamma_1(N)$ by

$$F(L, t) = f(z),$$

where z is a point in $\mathbb{H}$ such that $(\langle z, 1\rangle, \frac{1}{N})$ is a modular point homothetic to (L, t). This pairing turns out to be one-to-one between function $f \in M_k(\Gamma_1(N))$ and complex-valued functions on modular points for $\Gamma_1(N)$ such that

$$F(\lambda L, \lambda t) = \lambda^{-k} F(L, t).$$

This extends the other types modular points in the obvious manner, and provides further motivation for the defintion of modular forms of weight k and level N. The details are covered in [Kob93, Section III-5, Pages 153-155].

We now use the reverse correspondence to define Hecke operators T_n on congruence subgroups.

Definition 3.2.0.9. The **Hecke operator** $T_n : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$ by

$$T_n f(z) = F(T_n(L, t)) := \frac{1}{n} \sum_{L'} F((L', t))$$

where F, L and t are defined in the remarks above, and the T_n acts on modular points as defined on Definition 3.1.0.8.

The next proposition gives an effectively computable well to work out the T_n.

Proposition 3.2.0.10. *The operator T_n satisfies the following additional properties:*

(i) *T_n preserves cusp forms, so we can consider the linear map $T_n : S_k(\Gamma_1) \to S_k(\Gamma_1)$.*

(ii) *T_n also preserves the spaces $M_k(N, \chi)$ and $S_k(N, \chi)$.*

(iii) *We have*

$$T_n(f)(z) = n^{k-1} \sum_{\gamma} f(z)|[\gamma]_k$$

where the sum is over all elments in the left quotient $\frac{M}{\Gamma}$, where M is the set of all 2x2 matrices with determinant n.

(iv) *Let m, n be positive integers, then*

$$T_n \cdot T_m = \sum_{d|(m,n)} d^{k-1} \cdot T_{nm/d^2}.$$

Proof. [Kil15, Section 4.1.2, Pages 61-64]. □

Proposition 3.2.0.10(iv) gives us a way to recursively work out T_n from knowing T_p for all primes p diving n.

The linear operators T_n turn out to have eigenvectors when we restrict them to the cusp forms $S_k(N, \chi)$.

Definition 3.2.0.11. Let $f \in S_k(N, \chi)$. We say f **is an eigenform** if for each $n \geq 1$ there exists some $\lambda_n \in \mathbb{C}$ such that

$$T_n f = \lambda_n f.$$

This means that f is an eigenvector with eigenvalue λ_n for all the operators T_n.

Most important examples of modular forms turn out to be eigenforms. When this is true a lot can be concluded about its Fourier coefficients.

Keeping with the theme of doing simple linear algebra in the spaces of modular forms, last tool from of this section gives us an inner product for spaces of cusp forms.

Definition 3.2.0.12. Let Γ'', Γ' be congruence subgroups with $\Gamma'' \subset \Gamma'$. Let f, g be modular forms for Γ'' with at least one of them a cusp form. Then the **Peterson inner product of** f **and** g is define by

$$\langle f, g \rangle = \frac{1}{[\overline{\Gamma'} : \overline{\Gamma''}]} \int f(x+iy)\overline{g(x+iy)} y^k \frac{dxdy}{y^2}$$

where $\overline{\Gamma'} = \Gamma'/\{\pm \mathrm{Id}\}$ and the integral is over a fundamental domain for $\overline{\Gamma''}$.

The proof that the integral converges for all f, g can be found in [Kob93, Chapter III-5, page 170]. Once we know that, it is clear from the definition that $\langle \cdot \rangle$ defines a Hermitian inner product.

The Peterson inner product interacts well with the previous definitions. For instance, if χ is a Dirichlet character modulo N and c_n is either square root of $\bar{\chi}(n)$, then the operator $c_n T_n$ is Hermitian on $S_k(N, \chi)$. That is

$$\langle c_n T_n f, g \rangle = \langle f, c_n T_n g \rangle$$

for every $f, g \in S_k(N, \chi)$.

Definition 3.2.0.13. The orthogonal complement of $S_k^{\mathrm{old}}(\Gamma(N))$ under the Peterson inner product is called the space of **new forms of level** N, and written

$$S_k^{\mathrm{new}}(\Gamma(N)) = S_k^{\mathrm{old}}(\Gamma(N))^{\perp}.$$

Since everything is finite dimensional, we have

$$S_k(\Gamma(N)) = S_k^{\mathrm{new}}(\Gamma(N)) \oplus S_k^{\mathrm{old}}(\Gamma(N)).$$

We can also define new forms for other congruence subgroups, for instance by letting

$$S_k^{\mathrm{new}}(\Gamma_1(N)) = S_k(\Gamma_1(N)) \cap S_k^{\mathrm{new}}(\Gamma(N)).$$

The next definition will take a prominent role later in the description of the Shimura correspondence.

Definition 3.2.0.14. A normalized form $f \in S_k^{\mathrm{new}}(\Gamma_1)$ that is also an eigenform for all Hecke operators T_n is called a **newform**.

Proposition 3.2.0.15. *There exists an orthonormal basis of newforms for* $S_k^{\text{new}}(\Gamma_1(N))$.

Proof. [See Lan76, Theorem 3.1, Pages 125-137]. □

For a Dirichlet series $L(E,s) = \sum \frac{a_n}{n^s}$, we let $f_{E(z)}$ be a function on $\mathbb{H}$ with Fourier expansion $f_{E(z)} = \sum a_n q^n$. Conversely, if f is a modular form $f(z) = \sum b_n q^n$ we form its associated L-series by $L_f(s) = \sum \frac{b_n}{n^s}$.

The motivation for all definitions so far comes from the following result:

Proposition 3.2.0.16. *Let* $L(E_n, s)$ *be the Hasse-Weil L-function for the curve* $y^2 = x^3 - n^2 x$. *Then we have*

(i) $f_{E_1} \in M_2(\Gamma_0(32))$

(ii) $f_{E_n} \in M_2(\Gamma_0(32n^2))$.

Proof. See [Kob93, Pages 140-143] for a sketch. This is derived from a theorem of Weil, which says that something similar holds for all functions which satisfy a certain functional equation and a certain decay condition on its coefficients. □

Having found functions intimately related to $L(E_n, s)$ sitting into some congruence subgroups, Tunnell took advantage of some deep properties of the spaces $M_k(\Gamma_0(N))$ to find a way to paremetrise all of the critical values $L(E_n, 1)$ by the coefficients of a single form.

This is done using a theorem of Waldspurger, which in our case states the following:

Let $g := f_{E_1} \in M_2(\Gamma_0(32))$, and let $L_g(\chi_n, s) = L(E_n, s)$ be the analytic continuation of the twist by χ_n of the L-series corresponding to g. Then there exists a form $f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$ such that the critical values of $L_g(\chi_n, 1) = L(E_n, 1)$ satisfy

$$L_g(\chi_n, 1) = \lambda(n) a_n^2,$$

where $\lambda(n)$ can be effectively described.

It turns out that f lives in the space $S_{3/2}(\tilde{\Gamma}_0(128))$ of half-integral weight modular forms. We describe the construction of this space in the next section. After that, we will describe the main tool used in Waldspurger's theorem to find the form f, called the Shimura Correspondence.

3.3 Forms of Half-integral Weight

The desire of inventing a theory for forms of half-integral weight comes from considering objects which transform in a way that is reminscent but more general than classical forms.

Example 3.3.0.1. Let $\Theta(z) = \sum q^{n^2}$, with $q = e^{2\pi i z}$ as usual, be the Theta function. As we noted in 3.2.0.8, we have $\Theta^2 \in M_1(4, \chi)$. A classical calculation, carried out in [Kob93, Chapter III-4, Pages 148-149], shows that

$$\Theta(\gamma z) = \left(\frac{c}{d}\right) \varepsilon_d \sqrt{cz + d}\, \Theta(z),$$

where $\left(\frac{c}{d}\right)$ is the Jacobi symbol and

$$\varepsilon_d = \begin{cases} 1 & \text{if } d \equiv 1 \mod 4 \\ -i & \text{if } d \equiv 3 \mod 4. \end{cases}$$

and the square root branch is taken so that the argument lies in $(-\pi/2, \pi/2]$ This is, up to multiplication by a complex unit, very similar to what the transformation rule for a form of weight $1/2$ should look like. In general, one can write similar transformation rules for Θ^k with k odd.

The main obstruction to a theory of forms of half-integral weight is dealing with the choice of branch for the square root. In order to explain Tunnell's result, we will only need to work in the congruence subgroups $\Gamma_0(4N)$. Recall that they consist of integer matrices of the form $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $c \equiv 0\,(4N)$ and $ad - bc = 1$.

In order to get the right definition we will need to generalize classical forms in three directions

1. We will need to consider more general transformation rules, which not only scale correctly but also make the signs work out.

2. We will need to consider matrices living in a larger group, where the square root function doesn't have branches.

3. Once the first 2 steps are carried out, we will need to be careful in defining the appropriate holomorphicity conditions to get forms and cusp forms.

Definition 3.3.0.2. To carry out the first generalization, we take the transformation rule for the Theta function as a model and define the **automorphy factor**. For $\gamma \in \Gamma_0(4)$, let

$$j(\gamma, z) = \frac{\Theta(\gamma z)}{\Theta(z)} = \left(\frac{c}{d}\right) \varepsilon_d \sqrt{cz + d}.$$

Similar to the case for classical forms, we would want weight $k/2$ forms to satisfy

$$f(z)|[\gamma]_{k/2} := j(\gamma, z)^{-k} f(\gamma z) = f(z).$$

On the other hand, working with square roots branches in $\Gamma_0(4)$ forces us to define an operator $[\gamma]_{k/2}$ at a 4-sheeted cover of $GL_2^+(\mathbb{Q})$.

Definition 3.3.0.3. We define the **metaplectic cover of** $GL_2^+(\mathbb{Q})$ by

$$G = \{(\alpha, \phi)\}$$

where $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2^+(\mathbb{Q})$ and $\phi : \mathbb{H} \to \mathbb{C}$ is a holomorphic function such that

$$\phi(z)^4 = \frac{cz + d}{\sqrt{\det \alpha}}$$

The product in G is defined to be

$$(\alpha, \phi(z))(\beta, \psi(z)) = (\alpha\beta, \phi(\beta z)\psi(z)).$$

[Kob93, Pages 179-180] shows that G is indeed a group and a quadruple cover of $GL_2^+(\mathbb{Q})$. For $\xi = (\alpha, \phi) \in G$, we define the operator $[\xi]_{k/2}$ by

$$f(z)|[\xi]_{k/2} = f(\alpha z)\phi(z)^{-k}.$$

Finally, to get the right transformation rules, note that we can lift subgroups of $\Gamma_0(4)$ to subgroups of G:

Let Γ' be a subgroup of $\Gamma_0(4)$ of finite index. We define

$$\tilde{\Gamma} = \{(\gamma, j(\gamma, z)) \,|\, \gamma \in \Gamma'\}$$

and call $\tilde{\Gamma}'$ the lift of Γ'. For some $\gamma \in \Gamma_0(4)$, we write lift of γ to G by writing

$$\tilde{\gamma} = (\gamma, j(\gamma, z)) \in G.$$

Definition 3.3.0.4. Let k be an odd integer, and let $\Gamma' \leq \Gamma_0(4)$ have finite index. Let $f : \mathbb{H} \to \mathbb{C}$ be a holomorphic function. We say f **is weakily modular of weight** $k/2$ **for** Γ' if

$$f|[\tilde{\gamma}]_{k/2}(z) = f(z), \forall \tilde{\gamma} \in \tilde{\Gamma}'.$$

In the classical case, we defined holomorphicity at the cusps by considering the Fourier expansions of every $f|[\gamma]$ for γ ranging over the congruence subgroup under consideration. There is an analogous but more complicated way to "move" a modular form of half-integral weight by elements of G and get equivalent holomorphicity conditions.

For each weakily modular f of weight $k/2$, and $\tilde{\gamma} \in \tilde{\Gamma}'$, [Kob93, page 180-182] shows that there exists a least integer h and $t \in \{\pm 1, \pm i\}$ such that

$$g = f|[\gamma]_{k/2}$$

and

$$g(z) = g(z)|\left[\left(\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right), t\right)\right]_{k/2} = t^{-k} g(z + h)$$

If we write $t^k = e^{2\pi i r}$, for $r \in \{0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}\}$, then $e^{-2\pi i r z/h}$ is h periodic. Thus we can write a Fourier expansion

$$g(z) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i z(n+r)/h}.$$

If for all $\tilde{\gamma} \in \tilde{\Gamma}'$, the corresponding g has $a_n = 0$ for all $n < 0$, we say f is **holomorphic at the cusps of** Γ'. If we further have $a_0 = 0$, we say f **vanishes at the cusps of** Γ'.

Definition 3.3.0.5. Let $k \in \mathbb{Z}$, $\Gamma' < \Gamma_0(4)$ have finite index and let f be a weakily modular form of weight $k/2$.

1. If f is holomorphic at every cusp of Γ', we say f is a **modular form of weight** $k/2$. The space of such functions is written $M_{k/2}(\tilde{\Gamma})$.

2. If f also vanishes at every cusp, we say f is a **cusp form of weight** $k/2$. The space of such functions is written $S_{k/2}(\tilde{\Gamma}')$.

Example 3.3.0.6 (Eisenstein Series of Half-Integer Weight)**.** Let $k \geq 5$ be an odd integer, and set

$$E_{k/2}(z) = \sum_{\substack{4|m,n>0 \\ (m,n)=1}} \left(\frac{m}{n}\right) \varepsilon_n^k \frac{1}{(mz+n)^{k/2}}.$$

Then [Kob93, Page 186] shows that $E_{k/2} \in M_{k/2}(\tilde{\Gamma}_0(4))$.

As with integral weight forms, there is a theory showing finitely dimensionality and computing the dimensions of spaces for each weight. Half-integral weight forms also admit Hecke operators.

Since we lose the analogies from modular points in the $k/2$ case, it becomes harder to define T_n geometrically. The definition we will give here uses the alternative double coset approach, which could also have been employed in defining T_n for classical forms. This algebraic apparatus gives rise to the theory of Hecke modules, which can be used to generalize the concepts from this section even further. We begin giving an alternative expression for the T_n for classical forms.

Proposition 3.3.0.7. *Let n be positive integers, and let Δ^n be the set of 2x2 matrices with integers entries and determinant n. Recall that Γ is the full modular group $SL_2(\mathbb{Z})$. We have:*

(i) For any $\alpha \in \Delta^n$, there are only finitely many disjoint double cosets $\Gamma\alpha\Gamma$ in Δ^n. A complete set of double coset representatives is given by $\alpha = \left(\begin{smallmatrix} a & 0 \\ 0 & ab \end{smallmatrix}\right)$ where a, b run through all positive integers such that $n = ab^2$. In particular, if n is squarefree, we have $\Delta^n = \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right) \Gamma$, and if $n = p^2$ is the square of a prime, $\Delta^{p^2} = \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p^2 \end{smallmatrix}\right) \Gamma \amalg p\Gamma$.

(ii) For any double coset $\Gamma\alpha\Gamma \subset \Delta^n$ with $\alpha \in \Delta^n$, we have $\Gamma\alpha\Gamma = \Gamma\gamma_1 \amalg \cdots \amalg \Gamma\gamma_k$, so the double coset splits as a finite disjoint union of single cosets.

Proof. [See Kob93, Chapter IV-3, Pags 202-203]. □

These special properties of Δ^n allow us to give an alternative definition for the operators T_n, as an average not over modular points, but over coset representatives.

Definition 3.3.0.8 (Alternative definition of classical Hecke operator)**.** Let k, n be positive integers with k even. For $f \in M_k(\Gamma)$, set

$$f|[\Gamma\alpha\Gamma]_k = \sum_j f|[\alpha\gamma_j]_k$$

where the sum is over all right cosets $\Gamma\alpha\gamma_j \subset \Gamma\alpha\Gamma$. Then

$$T_n f = n^{(k/2)-1} \sum f|[\Gamma\alpha\Gamma]_k,$$

where the sum is over all double cosets of Γ in Δ^n. [Kob93, Chapter III-5, Page 167] shows that the sum is well defined, and that this expression agrees with how we defined the T_n in 3.2.0.9.

We can now generalize this construction to forms of half-integral weight. Recall that G is the quadruple cover of $GL_2^+(\mathbb{Q})$ given by

$$G = \left\{ (\alpha, \phi(z)) \,|\, \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2^+(\mathbb{Q}) \text{ and } \phi(z)^4 = \frac{cz+d}{\sqrt{\det \alpha}} \right\}$$

and

$$\tilde{\Gamma}_0(4) = \{(\alpha, j(\alpha, z)) \,|\, \alpha \in \Gamma_0(4)\}$$

where $j(\alpha, z)$ is the automorphy factor defined in 3.3.0.2.

In order to make an equivalent construction of the double coset operator for subgroups of G, we let

$$\xi_n = \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right), \sqrt[4]{n} \right)$$

and consider the double cosets of the form $\tilde{\Gamma}_1(N)\xi_n\tilde{\Gamma}_1(N)$. The following proposition generalizes the double coset decomposition in Proposition 3.3.0.7 to $\tilde{\Gamma}_1(N)$.

Proposition 3.3.0.9. *For any positive integer n, the double coset $\tilde{\Gamma}_1(N)\xi_n\tilde{\Gamma}_1(N)$ splits as the disjoint union of finitely many right cosets*

$$\tilde{\Gamma}_1(N)\xi_n\tilde{\Gamma}_1(N) = \tilde{\Gamma}_1(N)\xi_n\tilde{\gamma_1} \amalg \cdots \amalg \tilde{\Gamma}_1(N)\xi_n\tilde{\gamma_k}$$

where $\tilde{\gamma_i} = (\gamma_i, 1)$ for some $\gamma_i \in \Gamma_1(N)$.

Proof. [See Kob93, Chapter IV-3, Pages 203-204]. □

For $f \in M_{k/2}(\tilde{\Gamma}_1(N))$, we can then define an analogous double coset action by

$$f|[\tilde{\Gamma}_1(N)\xi_n\tilde{\Gamma}_1(N)]_{k/2} = \sum_j f|[\xi_n\tilde{\gamma}_j]_{k/2},$$

where the sum is over the coset representatives from Proposition 3.3.0.9.

The main difference in the theory for Hecke operators of forms of half-integral weight comes from the fact that if $(n, N) = 1$ and n is not a perfect square, then

$$f|[\tilde{\Gamma}_1(N)\xi_n\tilde{\Gamma}_1(N)] = 0.$$

This means that when searching for eigenforms for the generalizations of the T_n, it is not helpful to consider n that are not perfect squares, since then the only eigenform for T_n would be 0. We thus restrict our definition of T_n for the case where $n = p^2$ is the square of a prime.

Definition 3.3.0.10. Let p be a prime number, and $f \in M_{k/2}(\tilde{\Gamma}_1(N))$. The **Hecke operator** T_{p^2} is defined by

$$\begin{aligned} T_{p^2}f &= p^{(k/2)-2} f|[\tilde{\Gamma}_1(N)\xi_{p^2}\tilde{\Gamma}_1(N)]_{k/2} \\ &= p^{(k/2)-2} \sum_j f(z)|[\xi_{p^2}\tilde{\gamma}_j]_{k/2} \end{aligned}$$

where

$$\xi_{p^2} = \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & p^2 \end{smallmatrix}\right), \sqrt{p} \right)$$

and the sum is over the coset representatives from Proposition 3.3.0.9. If for every prime p there exists some $\lambda_p \in \mathbb{C}$ such that $T_{p^2}f = \lambda_p f$, we call f an **eigenform for the** T_{p^2}.

In the next section we will see that certain cusp forms which are also eigenforms for all T_{p^2} actually correspond to classical forms in a surprising fashion.

3.4 The Shimura Correspondence and Tunnell's Theorem

Theorem 3.4.0.1 (Shimura Correspondence)**.** *Let $k \geq 3$ be an odd integer, $\lambda = \frac{k-1}{2}$, N a multiple of 4 and χ a Dirichlet character modulo N. Let $f(z) = \sum a_n q^n \in S_{k/2}(\Gamma_0\tilde{(}N))$ be an eigenform for T_{p^2} with eigenvalue λ_p for all primes p. Define a function g with Dirichlet L-function and Euler product*

$$g_L(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s} = \prod_p \frac{1}{1 - \lambda_p p^{-s} + \chi(p)^2 p^{k-2-2s}}.$$

*Then $g \in M_{k-1}(N/2, \chi^2)$. If $k \geq 5$, then g is a cusp form. We call g the **Shumura lift** of f, and write*

$$g = \mathrm{Shim}(f).$$

Kohnen improved on this result for a specific case where $N = 4$, which is precisely the one useful for Tunnell's theorem. Let

$$S^+_{k/2} = \{f = \sum a_n q^n \in S_{k/2}(\tilde{\Gamma}_0(4)) \,|\, a_n = 0 \text{ if } (-1)^\lambda \equiv 2 \text{ or } 3 \mod 4\}.$$

Theorem 3.4.0.2. *The Shimura map actually gives an isomorphism*

$$S^+_{k/2}(\tilde{\Gamma}_0(4)) \to S_{k-1}(\Gamma).$$

Based on these ideas, Waldspurger proved a result which uses the Shimura correspondence to parametrise the critical values of L functions coming from modular forms. The general result is very complicated. The following specialization is given in Tunnell's paper [Tun83, Page 328].

Theorem 3.4.0.3 (Waldspurger's Theorem)**.** *Let $g \in M_{k-1}(N, \chi^2)$ be a newform such that $g = \mathrm{Shim}(f)$, for $f \in M_{k/2}(\tilde{\Gamma}_0(M))$. Assume $16 \mid N$. Then there exists a function $A(t)$ from squarefree integers to $\mathbb{C}$ such that*

$$A(t)^2 \varepsilon(\chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, 1/2) = 2(2\pi)^{(1-k)/2}\Gamma\left(\frac{k-1}{2}\right) L\left(g\,\chi^{-1}\chi_{-1}^{(k-1)/2}\chi_t, \frac{k-1}{2}\right).$$

Futhermore, for each positive integer N, there exists a finite set of explicitly described functions $c(n)$, specified by 11 equations, such that the sums

$$\sum_{n \text{ squarefree}} A(n)c(n)q^n,$$

span the preimages of ϕ of level N and character χ under the Shimura map.

Recall that if $L(s) = \sum \frac{a_n}{n^s}$ is a Dirichlet series, we can form a new function with Fourier expansion $f_L(z) = \sum a_n q^n$, where $q = e^{2\pi i z}$. When L is the Hasse-Weil L-function, we saw in Proposition 3.2.0.16 that

$$f_{E_n} \in M_2(\Gamma_0(32n^2)).$$

We will be interested in the case where $k = 3$, so that the Shimura map takes forms of weight $3/2$ to forms of weight 2, where $f_{L(E_1)}$ lives. In this setting, Tunnell saw that Waldspurger's theorem simplifies considerably. First, he computes all preimages of $f_{L(E_1)}$ under the Shimura map. It turns out to be necessary to work at level 128, but by finding a basis for $S_{3/2}(\tilde{\Gamma}_0(N), \chi)$ he manages to write the preimages of $f_{L(E,1)}$ under the Shimura map in terms of theta functions.

By observing carefully what Waldspurger's theorem says for the form f_L, Tunnell noted that there are only 4 options for the $c(n)$, and by carefully comparing coefficients he was able to arrive at his result:

Theorem 3.4.0.4 (Tunnell's Theorem)**.** *Let*

$$f_1(z) = (\Theta(z) - \Theta(4z))(\Theta(32z) - \frac{1}{2}\Theta(8z)) \in S_1(\Gamma_0(128)).$$

Then

$$f_1(z)\Theta(2z), f_1(z)\Theta(8z) \in S_{3/2}(\tilde{\Gamma}_0(128))$$

and

$$f_1(z)\Theta(4z), f_1(z)\Theta(16z) \in S_{3/2}(\tilde{\Gamma}_0(128), \chi_2)$$

are a maximal set of linearly independent eigenforms for all of the T_{p^2}, whose image under the Shimura lift is the modular form $f_{L(E_1)}$.

Let n be a squarefree odd positve integer. Then Waldspurger's theorem implies:

$$L(E_n, 1) = \frac{\beta}{4\sqrt{n}} a_n^2$$

and

$$L(E_{2n}, 1) = \frac{\beta}{2\sqrt{2n}} b_n^2$$

where $\beta = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}}$.

Proof. [See Tun83, Theorem 3, Page 328-329]. □

Chapter 4

Galois Cohomology

4.1 Group Cohmology

We begin by recalling some concepts from algebra. Let G be a finite group. We define the **group ring** $\mathbb{Z}[G]$ to be the ring of formal sums

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} x_i g \,|\, x_i \in \mathbb{Z} \right\}$$

with identity $1 \cdot e_G$ and addition and multiplication defined by

$$\left(\sum_{g \in G} x_g g \right) + \left(\sum_{g \in G} y_g g \right) = \sum_{g \in G} (x_g + y_g) g$$

and

$$\left(\sum_{g \in G} x_g g \right) \cdot \left(\sum_{h \in G} y_h h \right) = \sum_{g,h \in G} (x_g y_h) gh$$

We say an abelian group A is a **G-module** if it is a module for the ring $\mathbb{Z}[G]$.

If A and B are R-modules for a ring R, recall that $\mathrm{Hom}_R(A, B)$ is the group of module homomorphisms from A to B. Recall that an exact sequence

$$E : 0 \to B \to E \to A \to 0$$

of module homomorphism is called an **extension of A by B**. If we have two extensions

$$E_1 : 0 \to B \xrightarrow{f} E \xrightarrow{g} A \to 0$$

$$E_2 : 0 \to B \xrightarrow{f'} E' \xrightarrow{g'} A \to 0$$

we can form the **Baer sum of E_1 and E_2** by

$$E_1 + E_2 : 0 \to B \to Y \to A \to 0$$

where

$$Y = \frac{\{(e, e') \in E \oplus E' \,|\, g(e) = g'(e')\}}{\{(f(b), 0) - (0, f'(b)) \,|\, b \in B\}}$$

The set of extensions of A by B is called $\mathrm{Ext}^1_R(A, B)$. We saw in MATH3201 that this is an abelian group with addition given by the Baer sum.

Definition 4.1.0.1. The **zeroth and first cohomology groups of** A are defined by

$$H^0(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

and

$$H^1(G, A) = \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

where $\mathbb{Z}$ is considered the trivial G-module where $gx = x$ for every $x \in \mathbb{Z}, g \in G$.

We can also give alternative definitions for the cohomology groups in terms of cycles and boundaries. Let $\phi : \mathbb{Z} \to A$ be a module homomorphism. Then

$$\begin{aligned}\phi(1) &= \phi(g \cdot 1) \quad \forall g \in G \\ &= g \cdot \phi(1),\end{aligned}$$

so $\phi(1) \in A^G = \{x \in A \,|\, gx = x, \forall g \in G\}$, the set of elements of A at which G acts trivially. But ϕ is completely determined by the image of 1, so we can set

$$H^0(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) = A^G.$$

In order to recover H^1, note that we have a surjective homomorphism $\phi : \mathbb{Z}[G] \to \mathbb{Z}$ given by

$$\sum_{g \in G} x_g g \mapsto \sum_{g \in G} x_g,$$

which gives a presentation

$$0 \to \ker(\phi) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

of the G-module $\mathbb{Z}$.

Using this presentation we may write $H^1(G, A)$ as

$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)}$$

where

$$Z^1(G, A) = \{\phi : G \to A \,|\, \phi(gh) = \phi(g) + g\phi(h)\}$$

$$B^1(G, A) = \{\delta \in Z^1 \,|\, \exists a \in A \text{ such that } \delta(g) = ga - a, \forall g \in G\}$$

The following proposition shows that H^1 measures, is some sense, the lack of exactness of the functor of G-modules to abelian groups given by $A \mapsto A^G$.

Proposition 4.1.0.2. *For any short exact sequence of G-modules*

$$0 \to A \to B \to C \to 0$$

we can form the long exact sequence

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C)$$

Proof. [See Sil16, Appendix B, Pages 416-417]. □

4.2 Galois Cohomology

We will now transport the machinery of group cohomology to the setting of field extensions. All throughout this section, we will assume K is a perfect field. We recall this means that every extension of K is separable. We also let $L : K$ be a finite degree Galois extension with Galois group $G_{L:K}$. A **Galois module** A is a module over $G_{L:K}$.

Example 4.2.0.1. We can consider the Galois modules $A = L \simeq K[G]$, or $A = L^\times$ where $L^\times$ is the multiplicative group of L.

Example 4.2.0.2. If E is an elliptic curve over K then $A = E(L)$ is a Galois module. Recall the addition formulas (Equation 2.1.0.4) for an elliptic curve given by

$$E : y^2 = x^3 + ax^2 + bx + c, \text{ with } a, b \in K.$$

Let $P_1, P_2 \in E(L)$. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, we have $P_1 + P_2 = (x_3, -y_3)$, where

$$x_3 = \lambda^2 - a - x_1 - x_2$$

and $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. The y coordinate is then given by

$$y_3^2 = x_3^3 + ax_3 + b.$$

Thus, both coordinates of $P_1 + P_2$ are given by polynomials with coefficients in K. For any $\sigma \in G_{L:K}$, we then have

$$x(\sigma(P_1 + P_2)) = \sigma(x_3) = x(\sigma(P_1) + \sigma(P_2)),$$

and an identical expression holds for the y-coordinate.

Thus, $\sigma(P_1 + P_2) = \sigma(P_1) + \sigma(P_2), \forall \sigma \in G_{L:K}$, so $E(L)$ is indeed a Galois module.

Definition 4.2.0.3. The **zeroth and first Galois cohomology groups** are written

$$H^0(L : K, A) = H^0(G_{L:K}, A) = A^{G_{L:K}}$$
$$H^1(L : K, A) = H^1(G_{L:K}, A)$$

The following result gives an important terminating condition for the long exact sequences:

Theorem 4.2.0.4 (Hilbert's Theorem 90)**.** *For any finite Galois extension $L : K$, we have*

$$H^1(L : K, L^\times) = 0$$

where $L^\times$ is the multiplicative group of L.

Proof. [See Ser79, Chapter X, page 150] □

Unpacking the definitions, we see that if $\phi : G_{L:K} \to L^\times$ is a map satisfying

$$\phi(gh) = \phi(g) \cdot g(\phi(h)),$$

then there exists some $\lambda \in L^\times$ such that

$$\phi(g) = \frac{g(\lambda)}{\lambda}, \text{ for all } g \in G_{L:K}.$$

In what follows we will let $L = \bar{K}$, the algebraic closure of K and let $G_K = G_{\bar{K}:K}$ be the absolute Galois group of K. This extension is usually infinite, so it will be necessary to make amendmends to the previous defintions.

Definition 4.2.0.5. A G_K-module A is called a **continuous G_K-module** if for all $g \in G_K$ and $a \in A$, there exists a finite Galois extension $L : K$ such that $g(a)$ depends only on the image of g in L. In other words, $g(a)$ is determined by the coset of g modulo $G_{\bar{K}:L}$.

The definition of continious Galois module guarantees that, at least locally, we can still work with finite extensions.

Example 4.2.0.6. $\bar{K}$ and $\bar{K}^\times$ are continuous G_K-modules.

To see this in the first case, note that for $\alpha \in \bar{K}$, by definition α is algebraic over K, so $K(\alpha) : K$ is finite, with degree equal to the degree of the minimal polynomial of α over K. But then, for any $\alpha \in K$ and $g \in G_K$, the number $g(\alpha)$ is a conjugate of α, and hence also lies in $K(\alpha)$. Thus, the value of $g(\alpha)$ depends only on the image of g in L, as wanted.

To form cohomology groups for continuous Galois modules, set

$$H^1_{\text{cts}}(K, A) = \frac{Z^1_{\text{cts}}(K, A)}{B^1(K, A)}$$

where

$$Z^1_{\text{cts}}(K, A) = \left\{ \begin{array}{l} \phi : G_K \to A \,|\, \phi \in Z^1(G_K, A) \text{ and there exists a finite extension } L : K \\ \text{ such that } \phi(g) \text{ depends only on } g \text{ modulo } G_{\bar{K}:L} \end{array} \right\}.$$

Remark 4.2.0.7. Because A is continuous, it follows that $B^1 \subset Z^1_{\text{cts}}$, so the quotient is well defined.

Lemma 4.2.0.8. *$E(\bar{K})$ is a continuous G_K-module. If $K = \mathbb{Q}$, we have*

$$H^0(\mathbb{Q}, E(\bar{\mathbb{Q}})) = E(\bar{\mathbb{Q}})^{G_{\bar{\mathbb{Q}}:\mathbb{Q}}} = E(\mathbb{Q}).$$

Proof. For $P = (x, y) \in E(\bar{K})$, let L be the field generated by the coordinates of P. Then $P \in E(L)$ and L is finite. This is because x, y are algebraic over K.

But then $g(P) = P, \forall g \in G_{\bar{K}:L}$, so the value of $g(P)$ for some $g \in G_K$ is entirely determined by g modulo $G_{\bar{K}:L}$, as wanted. □

We also have an extension of Hilbert's Theorem 90 to the continuous setting:

Theorem 4.2.0.9. *Let K be a perfect field. We have*

$$H^1_{\text{cts}}(\bar{K} : K, \bar{K}^\times) = 0.$$

Proof. The idea of the proof is to take advantage of the finiteness conditions afforded by continuity, and reduce the problem to the finite extension case. We will show that $Z^1_{\text{cts}}(\bar{K} : K, \bar{K}^\times) = B^1(\bar{K} : K, \bar{K}^\times)$.

Let $\phi : G_K \to \bar{K}^\times$ with $\phi \in Z^1_{\text{cts}}$. By continuity, there exists a finite extension $L : K$ such that for $g \in G_K$, the value of $\phi(g)$ depends only on the restriction of g to L. Thus, we have a map

$$\phi : G_{L:K} \to \bar{K}^\times,$$

and $G_{L:K}$ is finite. Now let $L_1 : L$ be the field extension generated by the images of ϕ in $\bar{K}^\times$. This is a finite extension by construction. Finally, let $L_2 : K$ be the normal closure of $L_2 : K$, which is a Galois extension, since we are assuming K is a perfect field.

Putting everything together, note we can consider ϕ as a map

$$\phi : G_{L_2:K} \to L_2^\times$$

by construction, so $\phi \in Z^1(L_2 : K, L_2^\times)$. But by Hilbert's Theorem 90, $H^2(L_2 : K, L_2^\times) = 0$, so we must have $\phi \in B^1(L_2 : K, L_2^\times)$.

By the definition of B^1, this means that we can write for all $g \in G_K$,

$$\phi(g) = \frac{g(\lambda)}{\lambda},$$

for some $\lambda \in L_2^\times \subset \bar{K}^\times$. Thus, $\phi \in B^1(\bar{K} : K, \bar{K}^\times)$, and we have $H^1(\bar{K} : K, \bar{K}^\times = 0)$.

□

Similarly to the group case, if we have a short exact sequence of continuous G_K-modules

$$0 \to A \to B \to C \to 0$$

we can form a long exact sequence of Galois cohomology groups

$$0 \to A^{G_K} \to B^{G_K} \to C^{G_K} \to H^1(K, A) \to H^1(K, B) \to H^1(K, C).$$

It will be this sequence that will allow us to tackle the calculation of the rank of the elliptic curves E_n explicitly.

Remark 4.2.0.10. From now on we will write $H^1(\mathbb{Q}, E)$ for the group $H^1(\mathbb{Q}, E(\bar{\mathbb{Q}}))$.

4.3 Applications to Elliptic Curves

A crucial step in the proof of the Mordell-Weil theorem is the study of the size of the quotient $E(\mathbb{Q})/2E(\mathbb{Q})$. In curves with at least one 2-torsion point, this can be done with the help of an isogeny.

Remark 4.3.0.1. From now on, for any morphism $\phi : A \to B$, we will write

$$\ker(\phi) = A[\phi].$$

Let

$$E : y^2 = x^3 + ax^2 + bx$$

be an elliptic curve over $\mathbb{Q}$. We know E has the rational points $\mathcal{O}$ and $T = (0, 0)$. By the Nagell-Lutz theorem, we know that T has order 2 in $E(\mathbb{Q})$. This is the most general case we have to consider, since if E has a 2-torsion point, we can translate it to the origin to get a birationally equivalent curve which contains the point $(0, 0)$.

We also consider the curve

$$\bar{E} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. Repeating this process yields the curve

$$\bar{\bar{E}} : y^2 = x^3 + 4ax^2 + 16bx$$

which is birationally equivalent to E by the transformation $y \mapsto 8y, x \mapsto 4x$.

Proposition 4.3.0.2. *Let $E, \bar{E}$ be as above. The maps $\phi : E \to \bar{E}$ and $\psi : \bar{E} \to E$ defined by*

$$\phi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}), & \text{if } P \neq \mathcal{O}, T \\ \bar{\mathcal{O}}, & \text{if } P = \mathcal{O} \text{ or } P = T \end{cases}$$

and

$$\psi(P) = \begin{cases} (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}), & \text{if } P \neq \bar{\mathcal{O}}, \bar{T} \\ \bar{\mathcal{O}}, & \text{if } \bar{P} = \bar{\mathcal{O}} \text{ or } \bar{P} = \bar{T} \end{cases}$$

are elliptic curve isogenies, $Ker(\phi) = \{\mathcal{O}, T\}$ and

$$\psi \circ \phi(P) = 2P, \text{ for all points } P \in E.$$

Proof. [See ST90, Chapter 4, page 79]. □

Lemma 4.3.0.3. *If $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ and $\bar{E}(\mathbb{Q})/\phi(E(\mathbb{Q}))$ are finite, then so is $E(\mathbb{Q})/2E(\mathbb{Q})$. In fact, the rank r of E satisfies*

$$2^r = \frac{\#E/\psi(\bar{E}) \cdot \#\bar{E}/\phi(E)}{4}$$

where all curves are understood to be over $\mathbb{Q}$.

Proof. [See ST90, Chapter 4, page 83]. □

We are thus led to consider the quotient $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ (the other one can be treated identically).

By the proposition, we have a short exact sequence of $G_{\mathbb{Q}}$-modules

$$0 \to \{\mathcal{O}, T\} \to \bar{E}(\bar{\mathbb{Q}}) \xrightarrow{\psi} E(\bar{\mathbb{Q}}) \to 0,$$

and $\{\mathcal{O}, T\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Taking Galois cohomology we get the long exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \bar{E}(\mathbb{Q}) \xrightarrow{\psi} E(\mathbb{Q}) \to H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \to H^1(\mathbb{Q}, \bar{E}) \xrightarrow{H^1(\psi)} H^1(\mathbb{Q}, E)$$

This in turn gives us the short exact sequence

$$0 \to \frac{E(\mathbb{Q})}{\psi(\bar{E}(\mathbb{Q}))} \to H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \to H^1(\mathbb{Q}, \bar{E}(\mathbb{Q}))[\psi] \to 0. \tag{4.3.0.1}$$

To get the order of $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ we need to investigate the group $H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$.

Proposition 4.3.0.4. *Let K be a perfect field. There exists a canonical isomorphism*

$$H^1(K, \mathbb{Z}/2\mathbb{Z}) \simeq K^\times/(K^\times)^2$$

Proof. Consider the exact sequence of Galois modules

$$0 \to \mu_2 \to \bar{K}^\times \xrightarrow{2} \bar{K}^\times \to 0$$

where μ_2 is the multiplicative group $\{1, -1\}$.

Taking cohomology gives the long exact sequence

$$0 \to \mu_2 \to K^\times \xrightarrow{2} K^\times \to H^1(K, \mathbb{Z}/2\mathbb{Z}) \to H^1(K, \bar{K}^\times)$$

and $H^1(K, \bar{K}^\times) \simeq 0$ by Hilbert's Theorem 90. Thus,

$$H^1(K, \mathbb{Z}/2\mathbb{Z}) \simeq K^\times/(K^\times)^2.$$ □

Remark 4.3.0.5. If the characteristic of K is 2, the group μ_2 is trivial, so we actually have $\bar{K}^\times \simeq (\bar{K}^\times)^2$, and thus $H^1(K, \mathbb{Z}/2\mathbb{Z}) = 0$.

Applying the result to Equation 4.3.0.1, we have $H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, giving the short exact sequence

$$0 \to \frac{E(\mathbb{Q})}{\psi(\bar{E}(\mathbb{Q}))} \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to H^1(\mathbb{Q}, \bar{E}(\mathbb{Q}))[\psi] \to 0,$$

which shows that $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ is a subgroup of $\mathbb{Q}/(\mathbb{Q}^\times)^2$.

4.4 The Selmer and Tate-Shafarevich Groups

In the effort to understand $E(\mathbb{Q})/2E(\mathbb{Q})$, we were led to consider the quotient $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$. Our application of Galois cohomology showed that this group is a subgroup of the multiplicative group of rationals modulo squares $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This opens the possibility of employing local methods to study $E(\mathbb{Q})/2E(\mathbb{Q})$.

Definition 4.4.0.1. A **place** ν is either a prime number p or ∞. $\mathbb{Q}_\nu$ then is either the field of p-adic numbers if $\nu = p$ or $\mathbb{R}$ if $\nu = \infty$.

We have a natural inclusion

$$\mathbb{Q} \hookrightarrow \prod_\nu \mathbb{Q}_\nu$$

given by

$$x \mapsto (x, x, \dots),$$

since $\mathbb{Q} \hookrightarrow \mathbb{Q}_\nu$ canonically for each ν. This gives rise to the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q})) & \longrightarrow & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 & \longrightarrow & H^1(\mathbb{Q}, \bar{E})[\psi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_\nu E(\mathbb{Q}_\nu)/\psi(\bar{E}(\mathbb{Q}_\nu)) & \longrightarrow & \prod_\nu (\mathbb{Q}_\nu^\times/(\mathbb{Q}_\nu)^\times)^2 & \longrightarrow & \prod_\nu H^1(\mathbb{Q}_\nu, \bar{E})[\psi] & \longrightarrow & 0
\end{array}$$

This diagram gives an interface for studying $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ via local methods. It turns out that we can split the information required to work out the size of $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ in two parts, given by the following important definitions.

Definition 4.4.0.2 (Selmer Group)**.** The **Selmer group** of the elliptic curve E is defined

$$\mathrm{Sel}_\psi(E) = \mathrm{Ker}\left((\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to \prod_\nu H^1(\mathbb{Q}_\nu, \bar{E})[\psi]\right)$$

We can also make an analogous construction for $\mathrm{Sel}_\phi(E)$ by considering the ϕ isogeny. This group is important in rank calculations primarily because it is effectively computable. To understand $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ fully, we also need

Definition 4.4.0.3 (Tate-Shafarevich Group)**.** The **Tate-Shafarevich group** of the elliptic curve E is defined

$$\text{Sha}(E) = \text{Ker}\left(H^1(\mathbb{Q}, \bar{E}) \to \prod_{\nu} H^1(\mathbb{Q}_\nu, \bar{E})\right)$$

Note that the isogeny $\psi : \bar{E} \to E$ gives rise to maps $H^1(\mathbb{Q}, \bar{E}) \to H^1(\mathbb{Q}, E)$ and $H^1(\mathbb{Q}_\nu, \bar{E}) \to H^1(\mathbb{Q}_\nu, E)$. It therefore restricts to a map $\text{Sha}(\bar{E}) \to \text{Sha}(E)$. We will write $\text{Sha}(E)[\psi]$ for the kernel of this map, and call it the **subgroup of ψ-torsion of** $\text{Sha}(E)$.

Putting both groups together, we get the short exact sequence

$$0 \to \frac{E(\mathbb{Q})}{\psi(\bar{E}(\mathbb{Q}))} \to \text{Sel}_\psi(E) \to \text{Sha}(E)[\psi] \to 0$$

If $\text{Sha}(E)[\psi] \simeq 0$, we get $\text{Sel}_\psi(E) \simeq E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$. By playing the same game with the isogeneous curve $\bar{E}$, if $\text{Sha}(E)[\phi] \simeq 0$, we also know $\bar{E}(\mathbb{Q})/\phi(E(\mathbb{Q}))$ and can use 4.3.0.3 to compute the rank of E.

For curves with a 2-torsion point, the map

$$\alpha : E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q})) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

has been explicitly computed in [ST90, Page 91] and is given by

$$(x, y) \mapsto x \mod (\mathbb{Q}^\times)^2.$$

Furthermore, [ST90, Pages 85-87] also shows that the image of α is contained in the subgroup G of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ given by

$$G = \langle -1, p_1, \ldots, p_k \rangle,$$

where $p_1, \ldots, p_n$ are the distinct prime factors of $\Delta(E)$.

In fact, Sel_ψ is also contained in G, and contains the image of α. Thus, we know that Sel_ψ is finite, and as a consequence, we see that $E(\mathbb{Q})/\psi(\bar{E}(\mathbb{Q}))$ is also finite. If we let

$$\bar{\alpha} : \bar{E}(\mathbb{Q})/\phi(E(\mathbb{Q})) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

be the map obtained by working with ϕ instead of ψ, we get an alternative formula for the rank r of E given by

$$2^r = \frac{\#\text{Im}(\alpha) \cdot \#\text{Im}(\bar{\alpha})}{4}$$

Considering the Selmer groups, we can give a computable upper bound for the rank of E from the following equation:

$$2^{s_r} = \frac{\#\text{Sel}_\phi(E) \cdot \#\text{Sel}_\psi(E)}{4}.$$

The positive integer s_r defined by this formula is called the **Selmer rank of** E, and we have $s_r \geq r$.

Chapter 5

Calculations

5.1 Introduction

From Tunnell's theorem we know that $L(E_n, 1)$ has a particularly simple form in terms of Theta functions. In this section we will show that they can be used to predict the existence of 2-torsion in $\text{Sha}(E_n)$. We will also compute the arithmetic invariants of E described in Chapter 2 and show that our predictions can be verified at least modulo 16.

5.2 Coefficients of Theta Series

We recall Tunnel's theorem leads us to consider the function given by the Fourier expansion given in Equation 2.7.0.3:

$$f(z) = \sum_{m=-\infty}^{\infty} a_m q^m = (\Theta(z) - \Theta(4z)) \left(\Theta(32z) - \frac{1}{2}\Theta(8z) \right) \Theta(2z).$$

We are only interested in the coefficients for n odd. In this case we can ignore terms in the product of Equation 2.7.0.3 where all arguments of Θ are even. Thus, it is enough to consider the n-th coefficient of

$$\Theta(z) \left(\Theta(32z) - \frac{1}{2}\Theta(8z) \right) \Theta(2z) = \sum_{x,y,z \in \mathbb{Z}} q^{2x^2+y^2+32z^2} - \frac{1}{2} \sum_{x,y,z \in \mathbb{Z}} q^{2x^2+y^2+8z^2}.$$

Here we will compute the coefficients a_m and give a very simple expression for their residues modulo 4. This will enable us to match our previous calculations to what the BSD conjecture predicts. To put it differently, set

$$A_n = \#\{(x, y, z) \,|\, n = 2x^2 + y^2 + 32z^2\}$$
$$B_n = \#\{(x, y, z) \,|\, n = 2x^2 + y^2 + 8z^2\}.$$

Then, the n-th coefficient of f will be

$$a_n = A_n - \frac{1}{2}B_n.$$

Note that whenever we have a solution to either equation in A_n or B_n, if none of the variables is 0, then there are in fact 8 distinct solutions given by $(\pm x, \pm y, \pm z)$. In this case, they together make no contribution to A_n or B_n modulo 8.

Similarly, if only one of the variables is 0, say z, then each choice from $(\pm x, \pm y)$ gives a distinct solution, so they make no contribution to A_n modulo 4.

Lemma 5.2.0.1. *If n is an odd squarefree integer, and $n > 1$, then A_n is congruent to 0 modulo 4.*

Proof. As we saw above, solutions with less than two variables equal to 0 make no contribution to A_n modulo 4. We're left to consider solutions when either 2 or 3 of variables are are 0.

But clearly there are none. By assumption n is odd, squarefree and positive, so it can't be equal to $0, 2x^2, y^2$, or $32z^2$ for any $x, y, z \in \mathbb{Z}$. □

If remains to compute $\frac{1}{2}B_n$ modulo 4. The factor of $\frac{1}{2}$ requires us to consider B_n modulo 8. An identical argument shows that there are no solutions with two or three variables equal to 0, so we're left to consider solutions where only one of x, y, z is 0. We define the quatities

$$\begin{aligned} P_n &= \#\{(x,y) \,|\, n = x^2 + 2y^2\} \\ Q_n &= \#\{(x,y) \,|\, n = x^2 + 8y^2\} \\ R_n &= \#\{(x,y) \,|\, n = 2x^2 + 8y^2\}. \end{aligned}$$

so that

$$B_n \equiv P_n + Q_n + R_n \mod 8.$$

Clearly $R_n = 0$ since n is odd. We will now use some algebraic number theory to compute P_n and Q_n.

Theorem 5.2.0.2. *Let $n = p_1 \cdots p_k$ where the p_i are the distinct prime factors of n. We have the formulae*

(i) $P_n = 2 \times \prod_{p_i | n} \left(1 + \left(\frac{-2}{p_i}\right)\right)$

(ii) $Q_n = \begin{cases} P_n & \text{if } n \equiv 1 \mod 8 \\ 0 & \text{otherwise.} \end{cases}$

Proof. (i) In algebraic number theory parlance, working out P_n is equivalent to counting the number of elements in $\mathbb{Z}[\sqrt{-2}]$ with norm n. Since $\mathbb{Z}[\sqrt{-2}]$ is a PID, we have unique factorization of elements. Thus, for $\alpha \in \mathbb{Z}[\sqrt{-2}]$,

$$N(\alpha) = n$$

if and only if

$$\alpha = \pi_1 \cdots \pi_k$$

where the π_i are distinct irreducibles and $N(\pi_i) = p_i$. Since $\mathbb{Z}[\sqrt{-2}]$ has 2 units, by Dirichlet's unit theorem we have

$$P_n = 2 \prod_{p_i | n} \alpha_i$$

where α_i is the number of prime ideals in $\mathbb{Z}[\sqrt{-2}]$ with norm p_i.

Again since $\mathbb{Z}[\sqrt{-2}]$ is a PID, we can pass from properties of prime ideals to properties of irreducible elments. Applying the result in [Mar77, Page 74, Theorem 25] for each p_i, there are 2 cases to consider.

- If $\left(\frac{-2}{p_i}\right) = -1$, p_i is already irreducible in $\mathbb{Z}[\sqrt{-2}]$, and $N(p_i) = p_i^2$. Thus, there are no elements of norm p_i, and hence none of norm n.

- If $\left(\frac{-2}{p_i}\right) = 1$, p_i splits, so we can write $p_i = \pi_i\bar{\pi}_i$ for some irreducible $\pi_i \in \mathbb{Z}[\sqrt{-2}]$ with $N(\pi_i) = p_i$. In this case there are 2 ideals of norm p_i generated by π_i and $\bar{\pi}_i$ respectively. Thus, we can write

$$\alpha_i = \left(1 + \left(\frac{-2}{p_i}\right)\right),$$

  which gives our formula for P_n.

(ii) For the second formula, note that each $x, y \in \mathbb{Z}$ satisfying

$$x^2 + 8y^2 = x^2 + 2 \cdot (2y)^2 = n$$

corresponds to an element $x + y\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ with norm n and y even. There are three possibilities.

- If $n \equiv 5, 7\,(8)$, n must have at least one prime factor $p_i \mid n$ with $p_i \not\equiv 1, 3\,(8)$. But then $\left(\frac{-2}{p_i}\right) = -1$, so by the formula for P_n, there are no elements in $\mathbb{Z}[\sqrt{-2}]$ with norm n, and Q_n is also 0.

- If $n \equiv 1\,(8)$, assume there exists an element $x + y\sqrt{-2}$ of norm n in $\mathbb{Z}[\sqrt{-2}]$. Note that

$$n = x^2 + 2y^2 \equiv x^2 \mod 2,$$

  so x must be odd. Suppose y is also odd. Checking the squares of all odd numbers modulo 8, we see that $y^2 \equiv 1\,(8)$, so

$$n = x^2 + 2y^2 \equiv 3 \mod 8,$$

  a contradiction. Thus y must be even, and each solution contributing to P_n also contributes to Q_n, so $P_n = Q_n$.

- If $n \equiv 3\,(8)$ and y is even,

$$n = x^2 + 2y^2 \equiv 1 \mod 8,$$

  a contradiction. Thus, y must be odd, and solutions contributing to P_n make no contribution to Q_n, so $Q_n = 0$.

Putting everything together gives the desired formula.

□

We are now ready to find an expression for a_n modulo 4.

Theorem 5.2.0.3. *If $n = p$ is prime, the coefficient a_p of $f(z)$ in Equation 2.7.0.3 satisfies*

$$a_p \equiv \begin{cases} 0 \mod 4 \text{ if } p \equiv 1, 5, 7 \mod 8 \\ 2 \mod 4 \text{ if } p \equiv 3 \mod 8. \end{cases}$$

If n has at least 2 prime factors, we have

$$a_n \equiv 0 \mod 4.$$

Proof. Recall that

$$\begin{aligned} a_n &= A_n - \frac{1}{2}B_n \\ &\equiv -\frac{1}{2}(P_n + Q_n) \mod 4. \end{aligned}$$

Note that $\left(1 + \left(\frac{-2}{p}\right)\right)$ is always even, so if n has two or more prime factors, clearly $P_n \equiv Q_n \equiv 0\,(8)$. In this case we have

$$a_n \equiv 0 \mod 4.$$

If $n = p$ is an odd prime, theorem 5.2.0.2 gives

$$P_p = 2 \cdot \left(1 + \left(\frac{-2}{p}\right)\right)$$

- If $p \equiv 1\,(8), Q_p = P_p = 2 \cdot 2 = 4$.
- If $p \equiv 3\,(8), P_p = 4$ but $Q_p = 0$.
- If $p \equiv 5, 7\,(8), P_p = Q_p = 0$.

Thus, $-\frac{1}{2}(P_p + Q_p) = 0$ unless $p \equiv 3\,(8)$, in which case it equals -2. This gives the result. □

5.3 Selmer Group

Now we proceed in the other direction, and examine the expected rank of the curve by studying its arithmetic invariants. We'll first compute the Selmer group of E_p and $\bar{E}_p$. Recall that in this case, the Selmer group is a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. It won't be necessary to calculate the Selmer rank of E_n for composite n. This is because, as last section showed, in this case we don't have any information about the coefficients of the theta series associated with E_n besides knowing that it is a multiple of 4.

Proposition 5.3.0.1. $\mathrm{Sel}(E_p)$ *is a subgroup of the multiplicative group $\{\pm 1, \pm p\}$, and $d_1 \in \mathrm{Sel}$ if and only if the equation*

$$N^2 = d_1 M^4 - \frac{p^2}{d_1} e^4 \tag{5.3.0.1}$$

has a solution in $\mathbb{Q}_p$ for all p and has a solution in $\mathbb{R}$. Similarly, $\mathrm{Sel}(\bar{E}_p)$ *is a subgroup of the multiplicative group $\{\pm 1, \pm 2, \pm p, \pm 2p\}$, consisting of elements d_1 at which*

$$N^2 = d_1 M^4 + \frac{4p^2}{d_1} e^4 \tag{5.3.0.2}$$

has a real and p-adic solution for all prime numbers.

We will compute Sel by looking at the equation modulo different primes. To do this we first state some general results. The first tells us how to get a solution in the infinite field $\mathbb{Q}_p$ from a solution in a finite field.

Proposition 5.3.0.2 (Hensel's Lemma)**.** *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_m], x = (x_i) \in (\mathbb{Z}_p)^m, n, k \in \mathbb{Z}$ and j an integer such that $0 \leq j \leq m$. Suppose that $2k < n$ and that*

$$f(x) \equiv 0\,(p^n) \text{ and } \nu_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

Then there exists a zero y of f in $(\mathbb{Z}_p)^m$ which is congruent to x modulo p^{n-k}.

Proof. [See Ser96, Chapter 2-2, page 14]. □

The next result gives a bound on the number of solutions in $\mathbb{Z}_p$ for an equation where all variables can be isolated.

Proposition 5.3.0.3. *Let $a_1, \ldots, a_r \in \mathbb{F}_p^\times$ and assume $l_1, \ldots, l_r$ all divide $p-1$. The number of solutions N_p to the equation*

$$a_1 x_1^{l_1} + \cdots a_r x_r^{l_r} \equiv 0\,(p)$$

satisfies

$$|N_p - p^{r-1}| \leq M(p-1)p^{(r/2)-1} \tag{5.3.0.3}$$

where M is the number of r-tuples of Dirichlet characters $\chi_1, \ldots, \chi_r$ where $\chi_i^{l_i} = \varepsilon, \chi_i \neq \varepsilon$ for $i = 1, \ldots, r$ and $\chi_1 \chi_2 \cdots \chi_r = \varepsilon$.

Proof. [See IR90, Chapter 8-7, page 103]. □

The following proposition will be useful to show existence of solutions to polynomials of low enough degree.

Proposition 5.3.0.4 (Chevalley Warning Theorem)**.** *Let $f \in \mathbb{F}_p[X_1, \ldots, X_n]$ be a homogeneous polynomial in n variables such that* $\deg(f) \leq n$*. Then f has a nontrivial 0.*

Proof. [See Ser96, Chapter 1, page 5] □

To compute the Selmer groups, we will have to consider three kinds of primes: 2, p, and any odd prime $l \neq p$.

5.3.1 l-adic case

Let l be an odd prime not equal to p. In order to work out if equation Equations 5.3.0.1 and 5.3.0.2 have solutions in $\mathbb{Q}_l$, we will first show they always have a nontrivial solution in $\mathbb{Z}/l\mathbb{Z}$, and then lift this solution to $\mathbb{Q}_l$ using Hensel's lemma. In the l-adic case, will be simpler to show that every equation of the form

$$N^2 = aM^4 + be^4 \tag{5.3.1.1}$$

with $a, b \in \mathbb{Z}_l^\times$ has a nontrivial solution in $\mathbb{Q}_l$. This is sufficient, since all possible coefficients appearing in Equations 5.3.0.1 and 5.3.0.2 are units in $\mathbb{Z}_l$, as they are always divisors of $4p^2$.

Lemma 5.3.1.1. *Equation 5.3.1.1 always has a nontrivial solution in $\mathbb{F}_l$.*

Proof. We are looking at the number of solutions to

$$N^2 - aM^4 - be^4 \equiv 0\,(l)$$

where a and b are units in $\mathbb{Z}_l$. Thus, we may apply all results from the previous section. Let N_l be the number of solutions to Equation 5.3.1.1 is $\mathbb{F}_l$. There are two cases to consider.

- If $l \equiv 3\,(4)$, the values taken by x^4 modulo l are the same as those taken by x^2, so N_l is also the number of solutions to

  $$N^2 - aM^2 - be^2 \equiv 0\,(l).$$

  But here $\deg(f) = 2$ and there are 3 variables. Thus, by the Chevalley Warning theorem, there exists a nontrivial solution in $\mathbb{F}_l$.

- If $l \equiv 1\,(4)$, there are three nontrivial Dirichlet characters modulo l of order dividing 4. The primitive quartic characters $\chi^{\pm 1}$ and the quadratic character χ^2 where $\chi^2(n) = (\frac{n}{p})$.

  Thus, M is the number of tuples χ^2, χ^a, χ^b with $a, b = \pm 1, 2$ where $\chi^2\chi^a\chi^b = \varepsilon$. There are only two options, given by $a = b = 1$ and $a = b = -1$, so $M = 2$. Substituting this into the bound in proposition 5.3.0.3 we get

  $$|N_l - l^{r-1}| \leq 2(l-1)l^{(3/2)-1}.$$

  This implies that if $|N_l - l^2| \leq l^2 - 2$, Equation 5.3.2.1 will have a nontrivial solution in $\mathbb{F}_l$. But

  $$2(l-1)l^{1/2} \leq l^2 - 2$$

  is satisfied for all $l \geq 3$.

□

Theorem 5.3.1.2 (Existence of l-adic Solutions)**.** *For $a, b \not\equiv 0\,(l)$, there is always a triple $x, y, z \in \mathbb{Q}_l^\times$ such that $x^2 = ay^4 + bz^4$.*

Proof. Let $f(x, y, z) = x^2 - ay^4 - bz^4$. We know from Lemma 5.3.1.1 that f has a nontrivial root (X, Y, Z) in $\mathbb{F}_l$. Wihtout loss of generaility, we may assume that $X \not\equiv 0\,(l)$ (see Lemma 5.3.2.2 for a more complicated, but essentially identical argument of why).

Since l is odd and the variables are isolated, none of the partial derivatives increase the l-adic valuation of f. For instance, $\nu_l\left(\frac{\partial f}{\partial x}\right) = \nu_l(2X) = 0$ and $f(X, Y, Z) \equiv 0\,(l)$, so $\nu_l(f(X, Y, Z)) \geq 1$. Thus, Hensel's lemma applies and we get a solution $\tilde{X}, \tilde{Y}, \tilde{Z} \in \mathbb{Q}_l$. □

5.3.2 p-adic case

Now there are only finitely many equations to check. We will proceed case by case. Remember we are trying to find solutions in $\mathbb{Q}_p$ to the equations

$$N^2 = d_1 M^4 - \frac{p^2}{d_1} e^4 \tag{5.3.2.1}$$

and

$$N^2 = d_1 M^4 + \frac{4p^2}{d_1} e^4 \tag{5.3.2.2}$$

corresponding to the curves E_p and $\bar{E}_p$.

Theorem 5.3.2.1 (Existence of p-adic solutions)**.** *The equations 5.3.2.1 have a nontrivial solution in $\mathbb{Q}_p$. In fact, they have solutions in $\mathbb{Q}$.*

Proof. This is easy since we can spot rational solutions in all cases.

- If $d_1 = -1$, we have the rational solution $(p, 0, 1)$.
- If $d_1 = p$, we have the rational solution $(0, 1, 1)$.
- If $d_1 = -p$, we have the rational solution $(0, 1, 1)$.

□

To work on the isogeneous curve, we need three aditional technical lemmas, that will help us streamline our computations.

Lemma 5.3.2.2. *Let $a, b \in \mathbb{Z}_p$. Then the equation*

$$N^2 = aM^4 + be^4 \tag{5.3.2.3}$$

has a nontrivial solution in $\mathbb{Q}_p$ if and only if it has a solution with $N, M, e \in \mathbb{Z}_p$. Furthermore, we may assume one of the variables N, M, e is a unit.

Proof. First suppose we have a solution and write

$$N = p^{-a}x,\ M = p^{-b}y,\ e = p^{-c}z$$

where $x, y, z \in \mathbb{Z}_p$ and $a, b, c \in \mathbb{N}$. We have

$$p^{-2a}x^2 = ap^{-4b}y^4 + bp^{-4c}z^4.$$

Multiplying by $p^{4(a+b+c)}$ gives

$$p^{2a+4b+4c}x^2 = ap^{4a+4c}y^4 + bp^{4a+4b}z^4,$$

so we get a new solution $(p^{a+2b+2c}x, p^{a+c}y, p^{a+b}z)$ to Equation 5.3.2.3 with all variables in $\mathbb{Z}_p$.

Now suppose $N, M, e \in \mathbb{Z}_p$. If all of them are divisible by p, writing $N = pN', M = pM', e = pe'$ for N', M', e' still in $\mathbb{Z}_p$ gives

$$p^2 N'^2 = ap^4 M'^4 + bp^4 e'^4,$$

so $N \equiv 0\,(p)$ and we in fact have $N' = pN'', N'' \in \mathbb{Z}_p$. But then,

$$p^4 N''^2 = ap^4 M'^4 + bp^4 e'^4.$$

Dividing through by p^4 we see that (N'', M', e') is a new solution to Equation 5.3.2.3 where each variable has strictly smaller valuation. Thus, we may assume one of N, M, e is a unit. □

Lemma 5.3.2.3. *Let $a, b \in \mathbb{Z}_p^\times$. Then the equation*

$$N^2 = aM^4 + bp^2 e^4 \tag{5.3.2.4}$$

has a nontrivial solution in $\mathbb{Q}_p$ if and only if either $\left(\frac{a}{p}\right) = 1$ or $\left(\frac{b}{p}\right) = 1$.

Proof. Suppose we have a solution. From 5.3.2.2, we may assume $N, M, e \in \mathbb{Z}_p$, with one of the variables a unit. There are 2 cases to consider.

- If neither N nor M is 0 modulo p, we get

  $$N^2 \equiv aM^4 \mod p^2$$

  or

  $$a \equiv \left(\frac{N}{M^2}\right)^2 \mod p,$$

  and we must have $\left(\frac{a}{p}\right) = 1$ as wanted.

- If one of N or M is 0 modulo p, Equation 5.3.2.4 clearly shows the other must also be, so we can write $N = pN'$, $M = pM'$. We get

  $$p^2 N^2 = ap^4 M^4 + bp^2 e^4$$

  or

  $$N'^2 = ap^2 M'^4 + be^4.$$

  This is just Equation 5.3.2.4 with the variables reversed. From the previous lemma, we may assume that e is a unit, so the previous case shows that we must have $\left(\frac{b}{p}\right) = 1$.

This concludes the only if direction of our theorem.

Conversely, if $\left(\frac{a}{p}\right) = 1$, by applying Hensel's lemma to the polynomial $X^2 - a$ we see that a has a square root in $\mathbb{Q}_p$. Thus, we have a solution to Equation 5.3.2.4 given by

$$(\sqrt{a}, 1, 0)$$

If $\left(\frac{b}{1}\right) = 1$ we similarly have the solution

$$(p\sqrt{b}, 0, 1).$$

□

Lemma 5.3.2.4. *Let $a, b \in \mathbb{Z}_p^\times$. Then the equation*

$$N^2 = apM^4 + bpe^4 \tag{5.3.2.5}$$

has a nontrivial solution in $\mathbb{Q}_p$ if and only if $\frac{-a}{b}$ is a 4th power in $\mathbb{F}_p$.

Proof. This is similar to the previous lemma. If we have a solution, lemma 5.3.2.2 shows that we may assume $N, M, e \in \mathbb{Z}_p$ with one of them a unit. Clearly $p|N^2$ and hence N, so we may write $N = pN'$, giving

$$p^2N'^2 = apM^4 + bpe^4$$

or

$$pN'^2 = aM^4 + be^4.$$

If M is divisble by p, clearly e must also be. But this contradicts lemma 5.3.2.2, so we may assume M and e are both units. Thus, we must have

$$aM^4 + be^4 \equiv 0 \mod p$$

or

$$\frac{-a}{b} \equiv \left(\frac{e}{M}\right)^4 \mod p$$

as wanted.

Conversely, if $\frac{-a}{b}$ is a 4th power in $\mathbb{F}_p$, we may lift it to $\mathbb{Q}_p$ using Hensel's lemma on $X^4 + \frac{a}{b}$, giving the solution

$$\left(0, 1, \left(\frac{-a}{b}\right)^{1/4}\right)$$

to Equation 5.3.2.5. □

We are now ready to work with the homogeneous spaces of $\bar{E}$ in $\mathbb{Q}_p$.

Theorem 5.3.2.5 (Existence of p-adic solutions, isogeneous curve)**.** *The equations 5.3.2.2 have a nontrivial solution in $\mathbb{Q}_p$ subject to the following conditions:*

d_1	*condition*
1	✓
2	$p \equiv 1, 7\,(8)$
p	$p \equiv 1\,(4)$
$2p$	$p \equiv 1\,(8)$
-1	$p \equiv 1\,(4)$
-2	$p \equiv 1, 3\,(8)$
$-p$	$p \equiv 1\,(4)$
$-2p$	$p \equiv 1\,(8)$

For instance, if $d_1 = 2p$, 5.3.2.2 has a nontrivial solution in $\mathbb{Q}_p$ if and only if $p \equiv 1\,(8)$.

Proof. Proceeding case by case:

- If $d_1 = 2$, we're trying to solve

$$N^2 = 2M^4 + 2p^2.$$

We may apply lemma 5.3.2.3, so we have a nontrivial solution iff $\left(\frac{2}{p}\right) = 1$.

In other words, we must have

$$p \equiv 1 \text{ or } 7 \mod 8.$$

- If $d_1 = p$, we're trying to solve

$$N^2 = pM^4 + 4pe^4.$$

This is of the same form as Equation 5.3.2.5, so we have a nontrivial solution iff -4 is a 4th power in $\mathbb{F}_p$.

First note that if $p \equiv 3\,(4)$, the values taken by x^4 are the same as those taken by x^2, so the condition is equivalent to -4 being a square. But $\left(\frac{-4}{p}\right) = \left(\frac{-1}{p}\right) = -1$ since $p \equiv 3\,(4)$, a contradiction.

If $p \equiv 1\,(4)$, we need to solve

$$x^4 = -4,$$

or equivalently,

$$x^2 = \pm 2\sqrt{-1}.$$

There are 2 cases to consider:

If $p \equiv 1\,(8)$, $\left(\frac{2}{p}\right) = 1$. Furthermore, [Con, page 4, Theorem 3.1] shows that $\mathbb{Q}_p$ contains a primitive 8th root of unit ζ_8. But then, since $(\zeta_8^4)^2 - 1 = 0$ in the field $\mathbb{Q}_p$, by primitivity we must have $\zeta_8^4 = -1$. Thus we may take

$$-4 = (\zeta_8\sqrt{2})^4.$$

If $p \equiv 5\,(8)$, $\left(\frac{2}{p}\right) = -1$ and there are no primitive 8th roots of 1. In particular, there are no 4th roots of -1, and thus

$$\left(\frac{2\sqrt{-1}}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{\sqrt{-1}}{p}\right) = (-1) \cdot (-1) = 1.$$

In this case we can take

$$-4 = \left(\sqrt{2\sqrt{-1}}\right)^4.$$

Thus, we have a nontrivial solution iff

$$p \equiv 1 \mod 4.$$

- If $d_1 = 2p$, we're trying to solve

$$N^2 = 2pM^4 + 2pe^4.$$

Again we can apply lemma 5.3.2.4, so we have a nontrivial solution iff $\frac{-2}{2} = -1$ is a 4th power. By the reasoning in the previous case, this is true iff

$$p \equiv 1 \mod 8.$$

- If $d_1 = -1$, we're trying to solve

$$N^2 = -M^4 - 4p^2e^4.$$

This is of the same form as Equation 5.3.2.4, so we have a nontrivial solution iff either $\left(\frac{-1}{p}\right)$ or $\left(\frac{-4}{p}\right)$ is equal to 1.

In other words, we must have

$$p \equiv 1 \mod 4.$$

- If $d_1 = -2$, we're trying to solve

$$N^2 = -2M^4 - 2p^2e^4,$$

Applying lemma 5.3.2.3, a similar argument shows we must have $\left(\frac{-2}{p}\right) = 1$, or equivalently,

$$p \equiv 1, 3 \mod 8.$$

- If $d_1 = -p$, we're trying to solve

$$N^2 = -pM^4 + -4pe^4.$$

Applying lemma 5.3.2.4, we again have a nontrivial solution iff -4 is a 4th power. We saw before that we must then have

$$p \equiv 1 \mod 4.$$

- If $d_2 = -2p$, we're trying to solve

$$N^2 = -2pM^4 + -2pe^4.$$

Again applying lemma 5.3.2.4, we have a nontrivial solution iff -1 is a 4th power. This is the case iff

$$p \equiv 1 \mod 8.$$

□

5.3.3 2-adic case

Finally, we consider the 2-adic solutions.

Note that we didn't make use of p being odd in the proof of lemma 5.3.2.2, so we also have:

Lemma 5.3.3.1. *Let $a, b \in \mathbb{Z}_2$. Then the equation*

$$N^2 = aM^4 + be^4$$

has a nontrival solution in $\mathbb{Q}_2$ if and only if it has a solution with $N, M, e \in \mathbb{Z}_2$. Furthermore, we may assume one of the variables N, M, e is a 2-adic unit.

Remember that Equation 5.3.2.1 has rational solutions. Since $\mathbb{Q} \hookrightarrow \mathbb{Q}_2$, we only need to consider the isogeneous curve.

Theorem 5.3.3.2. *The equations 5.3.2.2 have a nontrivial solution in $\mathbb{Q}_2$ subject to the following conditions:*

d_1	*condition*
1	✓
2	$p \equiv 1, 7\,(8)$
p	$p \equiv 1\,(4)$
$2p$	$p \equiv 1\,(8)$
-1	✗
-2	✗
$-p$	$p \equiv 3\,(4)$
$-2p$	$p \equiv 7\,(8)$

Proof. We're trying to find a root for

$$f(N, M, e) = N^2 - d_1 M^2 - \frac{4p^2}{d_1} e^4$$

in $\mathbb{Q}_2$, where d_1 ranges over all divisors of $4p^2$. We begin with a few preliminary remarks that will help to simplify our calculations.

Checking all possible cases we see that

$$x^4 \equiv \begin{cases} 1 & \mod 16 \text{ if } x \text{ is even} \\ 0 & \mod 16 \text{ if } x \text{ if odd} \end{cases}.$$

Thus, M^4 and e^4 may only take the values 0 or 1 modulo 16. Also note that the values taken by N^2 modulo 16 are among 0, 1, 4 and 9.

We now treat each possibility for d_1 separately.

- If $d_1 = 2$, we're trying to solve

$$N^2 = 2M^4 + 2p^2 e^4$$

in $\mathbb{Q}_2$. Since the RHS is even, we will need to work modulo 32. Writing

$$N^2 \equiv 2M^4 + 2p^2 e^4\,(32)$$

we see that N is even. Let $N = 2N'$, so we have

$$2N'^2 \equiv M^4 + p^2e^4 \,(16).$$

Since p is odd, there are 2 possibilities.

If $p^2 \equiv 9\,(16)$, we see that the equation

$$2N'^2 \equiv M^4 + 9e^4 \,(16)$$

has no solutions by checking each possibility $M^4, e^4 = 0, 1$ and $N'^2 = 0, 1, 4, 9$. Thus, our original equation has no solutions modulo 32.

If $p^2 \equiv 1\,(16)$, the equation

$$2N^2 \equiv M^4 + e^4 \,(16)$$

has the solution $(1, 1, 1)$, so the original equation has a solution modulo 32 given by $(2, 1, 1)$.

In order to apply Hensel's lemma in the variable N, note that $\frac{\partial f}{\partial N} = 2N = 4$, so we need to work modulo $4^2 \cdot 2 = 32$ as we already have.

Thus, we have a nontrivial solution in $\mathbb{Q}_2$ if and only if $p^2 \equiv 1\,(16)$, or equivalently,

$$p \equiv 1, 7 \mod 8.$$

- If $d_1 = p$, we're trying to solve

$$N^2 = pM^4 + 4pe^4$$

in $\mathbb{Q}_2$. Here it is sufficient to work modulo 16. We must have one of

$$0, 1, 4, 9 \equiv \begin{cases} p \\ 4p \\ 5p \end{cases} \mod 16.$$

Thus, we will have a solution modulo 16 iff

$$p \equiv 1, 9\,(16)$$

or

$$4p \equiv 4\,(16) \implies p \equiv 1\,(4)$$

or

$$5p \equiv 1, 9\,(16) \implies p \equiv 5, 13\,(16).$$

The second possibility brings nothing new, so we can work with only the first and the third. In any case we have a solution modulo 16 with N and M odd.

To apply Hensel's lemma, note that $\frac{\partial f}{\partial N} = 2N$. Since N is odd, we only need to work modulo $2^2 \cdot 2 = 8$. Thus, in each case the solution lifts, and we must have

$$p \equiv 1 \mod 4.$$

- If $d_1 = 2p$, we're trying to solve

$$N^2 = 2pM^4 + 2pe^4$$

in $\mathbb{Q}_2$. Again we must work modulo 32. By the same reasoning as the case $d_1 = 2$, we can instead solve

$$2N'^2 \equiv pM^4 + pe^4 \,(16),$$

where $N = 2N'$. Since p is odd, our only hope for a solution is if $2p \equiv 2\,(16)$, or $p \equiv 1\,(8)$. In this case, a solution mod 32 is $(2, 1, 1)$.

To apply Hensel's lemma, note that $\frac{\partial f}{\partial N} = 2N = 4$, so we were justified in working mod 32 in the first place. Thus, we must have

$$p \equiv 1 \mod 8.$$

- If $d_1 = -1$, we're trying to solve

$$N^2 = -M^4 - 4p^2e^4$$

in $\mathbb{Q}_2$. Working modulo 16, we must have one of

$$0, 1, 4, 9 \equiv \begin{cases} -1 \\ -4p^2 \\ -1 - 4p^2 \end{cases} \mod 16.$$

The first option never has a solution.

The second takes the values

$$-4p^2 \equiv -4 \cdot 1, 4 \cdot 9 \equiv 12\,(16),$$

so neither it nor the third possibility give any solutions.

Thus, in this case there are no solutions modulo 16, and hence in $\mathbb{Q}_2$.

- If $d_1 = -2$, we're trying to solve

$$N^2 = -2M^4 - 2p^2e^4$$

in $\mathbb{Q}_2$. Again we must have one of

$$0, 1, 4, 9 \equiv \begin{cases} -2 \\ -2p^2 \\ -2 - 2p^2 \end{cases} \mod 16.$$

The first option never has a solution

The second takes the values

$$-2p^2 \equiv -2 \cdot 1, -2 \cdot 9 \equiv 14\,(16),$$

so neither it nor the third option have any solutions.

Thus, in this case there are no 2-adic solutions.

- If $d_1 = -p$, we're trying to solve

$$N^2 = -pM^4 + -4pe^4$$

in $\mathbb{Q}_2$. Emulating the case $d_1 = p$, we can work modulo 16. We must have one of

$$0, 1, 4, 9 \equiv \begin{cases} -p \\ -4p \\ -5p \end{cases} \mod 16.$$

We will have a nontrivial solution modulo 16 iff

$$-p \equiv 1, 9\,(16) \implies p \equiv 7, 15\,(16)$$

or

$$-4p \equiv 4\,(16) \implies p \equiv -1\,(4)$$

or

$$-5p \equiv 1, 9\,(16) \implies p \equiv 3, 11\,(16).$$

The second possibility brings nothing new, so again we can assume N and M are odd. To apply Hensel's lemma, note that $\frac{\partial f}{\partial N} = 2N$, so we may lift a root modulo $2^2 \cdot 2 = 16$. Thus, in each case the solution lifts, and we must have

$$p \equiv 3 \mod 4.$$

- If $d_1 = -2p$, we're trying to solve

$$N^2 = -2pM^4 + -2pe^4$$

in $\mathbb{Q}_2$. We must work modulo 32. Again we may set $N = 2N'$ and solve

$$2N'^2 = -pM^4 - pe^4\,(16).$$

This time our only hope is if $-2p \equiv 2\,(16)$, or $p \equiv -1\,(8)$. In this case a solution mod 32 is $(2, 1, 1)$.

To apply Hensel's lemma, note that $\frac{\partial f}{\partial N} = 2N = 4$, so we were justified in working mod 32. Thus, we must have

$$p \equiv 7 \mod 8.$$

□

We can now put everything together to work out the Selmer rank of E_p.

d_1	l-adic	p-adic	2-adic	$\mathbb{R}$	Sel
1	✓	✓	✓	✓	✓
2	✓	$p \equiv 1, 7\,(8)$	$p \equiv 1, 7\,(8)$	✓	$p \equiv 1, 7\,(8)$
p	✓	$p \equiv 1\,(4)$	$p \equiv 1\,(4)$	✓	$p \equiv 1\,(4)$
$2p$	✓	$p \equiv 1\,(8)$	$p \equiv 1\,(8)$	✓	$p \equiv 1\,(8)$
-1	✓	$p \equiv 1\,(4)$	✗	✗	✗
-2	✓	$p \equiv 1, 3\,(8)$	✗	✗	✗
$-p$	✓	$p \equiv 1\,(4)$	$p \equiv 3\,(4)$	✗	✗
$-2p$	✓	$p \equiv 1\,(8)$	$p \equiv 7\,(8)$	✗	✗

Theorem 5.3.3.3 (Selmer rank of E_p)**.** *The Selmer rank r of E satisfies*

$$r = \begin{cases} 0 \text{ if } p \equiv 3 \mod 8 \\ 1 \text{ if } p \equiv 5, 7 \mod 8 \\ 2 \text{ if } p \equiv 1 \mod 8. \end{cases}$$

Proof. Let s_r be the Selmer rank, then

$$2^{s_r} = \frac{\#\mathrm{Sel}_\phi(E) \cdot \#\mathrm{Sel}_\psi(\bar{E})}{4} = \#\mathrm{Sel}_\psi(\bar{E}) = \begin{cases} 1 & \text{if } p \equiv 3 \mod 8 \\ 2 & \text{if } p \equiv 5, 7 \mod 8 \\ 4 & \text{if } p \equiv 1 \mod 8 \end{cases}$$

Comparing exponents of 2 gives the result. □

5.4 Tamagawa Numbers

The final step of our calculations is to work out the Tamagawa numbers of the curves E_n. Recall that

$$c_p = \left| \frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0} \right|$$

where $E(\mathbb{Q}_p)_0$ is the preimage of the nonsingular points of the reduced curve modulo p of the map

$$E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p).$$

We begin with a straightforward lemma.

Lemma 5.4.0.1. *The curve*

$$\tilde{E}(\mathbb{F}_p) : y^2 \equiv x^3 - n^2 x \mod p$$

is nonsingular unless $p \mid 2n$.

If $p = 2$ the only singular point is $(1, 0)$.

If $p \mid n$ the only singuar point is $(0, 0)$.

Proof. Since $\mathcal{O}$ may could also turn out to be singular, we consider the projective completion

$$f(x, y, z) = y^2 z - x^3 + n^2 x z^2.$$

A point is singular if and only if all partial derivatives vanish. We have

$$\begin{aligned} \frac{\partial f}{\partial x} &= -3x^2 + n^2 z^2 \\ \frac{\partial f}{\partial y} &= 2yz \\ \frac{\partial f}{\partial z} &= y^2 + n^2 x \end{aligned}$$

There are 3 cases to consider.

- If $p = 2$, working in $\mathbb{F}_2$ we get

$$\frac{\partial f}{\partial x} = x^2 + z^2 = (x-z)^2, \quad \frac{\partial f}{\partial y} = 0, \quad \frac{\partial f}{\partial z} = y^2.$$

  Thus, we must have $x = z$ and $y = 0$. Since x, y, z can't be 0 simultaneously, the only candidate is the point $(1:0:1)$, which is in fact in the curve, and descends to the point $(1,0)$ in the affine model.

- If $p \mid n$, working in $\mathbb{F}_p$ we get

$$\frac{\partial f}{\partial x} = -3x^2, \quad \frac{\partial f}{\partial y} = 2yz, \quad \frac{\partial f}{\partial z} = y^2.$$

  If $y = 0$, we have $f(x,y,z) = -x^3 = 0$, so $x = 0$. Thus, only $(0:0:1)$ is singular, and it descends to the point $(0,0) \in \tilde{E}(\mathbb{F}_p)$.

- If $p \nmid 2n$, the equations for the partial derivatives require us to have either $y = 0$ or $z = 0$.

  If $z = 0$, we must have $-x^3 = 0$, so $y = 1$. But then $\frac{\partial f}{\partial z} \neq 0$.

  If $y = 0$, $\frac{\partial f}{\partial z} = n^2 x = 0$, so $x = 0$, and $\frac{\partial f}{\partial x} = n^2 z^2 = 0$ and $z = 0$, a contradiction.

  Thus, there are no singular points on $\bar{E_n}(\mathbb{F}_p)$ if $p \nmid n$. □

As an easy application, we have

Corollary 5.4.0.2. *If $p \not| 2n$, the Tamagawa number $c_p = 1$.*

Proof. In this case, all points are nonsingular, so $E(\mathbb{Q}_p)_0 = E(\mathbb{Q}_p)$, and

$$c_p = |\{1\}| = 1$$

as wanted. □

It now remains to consider the Tamagawa number at the primes where E_n has bad reduction. We first consider the case where $p \mid n$. To do this we will give an explict parametrization for the map

$$\psi : E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p)$$

Working in $\mathbb{Q}_p$, if $x \equiv 0\,(p)$ then

$$y^2 = x^3 - p^2 b^2 x \equiv 0 \mod p^2,$$

where we write $n = pb$ with $p \not| b$, since n is squarefree. Thus, $y \equiv 0\,(p)$ and (x,y) reduces to the singular point.

If $x \notin p\mathbb{Z}_p$, we can write $x = p^{-n}u$ for some $u \in \mathbb{Z}_p^\times$ and $n \geq 0$. Then,

$$y^2 = p^{-3n}u^3 - p^{2-n}b^2 u,$$

so n must be even. Writing $n = 2m$ we get

$$p^{6m}y^2 = u^3 - p^{2+2m}b^2 u.$$

We can't have $p^{6m}y^2 \equiv 0\,(p)$ since then $u \equiv 0\,(p)$, a contradiction. Thus we can write $y = p^{-3m}v$ for some $v \in \mathbb{Z}_p^\times$. We arrive at the equation

$$v^2 = u^3 - p^{2+2m}b^2u, \text{ with } u, v \in \mathbb{Z}_p^\times,$$

giving

$$v^2 \equiv b^2u^3 \mod p.$$

For this to have a solution, we must have $\left(\frac{u}{p}\right) = 1$, so x is the reciprocal of a square in $\mathbb{Z}_p$.

Setting

$$x = \frac{1}{r^2},\ r \in \mathbb{Z}_p$$

we get

$$y^2 = \frac{1}{r^6} - n^2r^2 = \frac{1 - n^2r^4}{r^6}.$$

We can thus parametrise the points in $E(\mathbb{Q}_p)_0$ by the map

$$P : \mathbb{Z}_p \to E(\mathbb{Q}_p)_0$$

mapping

$$\begin{aligned} r &\mapsto \left(\frac{1}{r^2}, \frac{\sqrt{1 - n^2r^4}}{r^3}\right), \text{ if } r \neq 0 \\ 0 &\mapsto \mathcal{O}. \end{aligned} \tag{5.4.0.1}$$

Note that the series $\sqrt{1 - n^2r^4}$ converges p-adically for all $r \in \mathbb{Z}_p$ since $n \equiv 0\,(p)$. As we're letting r range over $\mathbb{Z}_p$ the choice of square root doesn't matter, since we may just replace r with $-r$ and get the other one.

We are now ready to investigate the quotient group $\left|\frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0}\right|$.

Theorem 5.4.0.3. *If $p \nmid n$ for n odd and squarefree, the torsion points $\mathcal{O}, (0,0), (n,0), (-n,0)$ are a complete set of representatives for $\frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0}$.*

Proof. From Equation 5.4.0.1 we have, for $r \in \mathbb{Z}_p$, $P(r) = (\frac{1}{r^2}, \frac{\sqrt{1-n^2r^4}}{r^3}) = (x, y)$.

Step 1: We will compute

$$S := P(r) + Q$$

for each torsion point Q using the addition formulas from Equation 2.1.0.4.

If $Q = \mathcal{O}$: $P(r) + \mathcal{O} = P(r)$.

Now suppose the line between $P(r)$ and Q is given by

$$y = \lambda x + \nu.$$

- If $Q = \mathcal{O}$: $S = P(r) + \mathcal{O} = P(r)$, and

$$x(S) = \frac{1}{r^2}.$$

Since $r \in \mathbb{Z}_p$, we have in particular

$$x(S) \not\equiv 0 \mod p.$$

- If $Q = (0, 0)$: We have $\lambda = \frac{y}{x}$, so

$$\begin{aligned} x(S) = \lambda^2 - x - 0 &= \frac{\frac{1-n^2r^4}{r^6}}{\frac{1}{r^4}} - \frac{1}{r^2} \\ &= -n^2r^2 = -p^2b^2r^2. \end{aligned}$$

  In particular,

$$x(S) \equiv 0 \mod p^2.$$

- If $Q = (n, 0)$: We have $\lambda = \frac{y}{x-n} = \frac{\frac{\sqrt{1-n^2r^4}}{r^3}}{\frac{1-nr^2}{r^2}}$, so

$$\begin{aligned} x(S) = \lambda^2 - x - n &= \frac{\frac{1-n^2r^4}{r^6}}{\frac{(1-nr^2)^2}{r^4}} - \frac{1}{r^2} - n \\ &= \frac{1-n^2r^4}{r^2(1-nr^2)^2} - \frac{1+nr^2}{r^2} \\ &= -n + \frac{2n}{1-nr^2} \end{aligned}$$

  But considering the p-adic power series for the quotient, we have

$$\frac{1}{1-nr^2} = 1 - nr^2 + O(n^2) \equiv 1 - nr^2 \,(p^2),$$

  and

$$-n + \frac{2n}{1-nr^2} \equiv -n + 2n - 2n^2r^2 \equiv n \,(p^2).$$

  Thus, in this case we have

$$x(S) \equiv pb \mod p^2.$$

- If $Q = (-n, 0)$: We have $\lambda = \frac{y}{x+n}$, so

$$\begin{aligned} x(S) = \lambda^2 - x + n &= \frac{\frac{1-n^2r^4}{r^6}}{\frac{(1+nr^2)^2}{r^4}} - \frac{1}{r^2} + p \\ &= n - \frac{2n}{1+nr^2} \end{aligned}$$

  A similar calculation shows that

$$x(S) \equiv -pb \mod p^2.$$

As a consequence, the 4 cosets are distinct, since the x coordinates of $P(r) + Q$ for each Q are all incongruent modulo p^2.

Step 2: We now show that indeed those are all the possibilities for x modulo p^2.

Note that if $x \not\equiv 0 \,(p)$, then also $y \not\equiv 0 \,(p)$, so $(x, y) \neq (0, 0)$ in $\tilde{E}(\mathbb{F}_p)$ and thus (x, y) is the preimage of a nonsingular point, and belongs to the trivial coset $E(\mathbb{Q}_p)_0$.

Otherwise, if $x \equiv 0 \,(p)$,

$$y^2 = x^3 - p^2b^2x \equiv 0 \,(p^3)$$

so

$$y \equiv 0\,(p^2)$$

and

$$x^3 - p^2b^2x \equiv 0\,(p^4).$$

Letting $x = pa$ we get

$$p^3a^3 - p^3b^2a \equiv 0\,(p^4)$$

so finally

$$a^3 - b^2a \equiv 0\,(p).$$

Since $\mathbb{F}_p$ is a field, we have unique factorization and thus must have $a \equiv 0, \pm b\,(p)$, so

$$x \equiv 0, bp, -bp \mod p^2$$

as wanted.

Step 3: The next step is to show that indeed those cosets span all of $\frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0}$. To do this we need to show that for each possible residue $x \equiv 0, bp, -bp\,(p^2)$ we can solve for r to find a preimage in $\mathbb{Z}_p$.

Let $S = (x, y)$. Again we proceed in cases.

- If $x \equiv 0\,(p^2)$, we can write $x = p^2t$ for some $t \in \mathbb{Z}_p$. We want to show that S is a member of the coset $P(r) + (0, 0)$, i.e. that we can solve

  $$x = -p^2b^2r^2$$

  for some $r \in \mathbb{Z}_p$. From the equation of the curve we have

  $$\begin{aligned} y^2 &= x^3 - (pb)^2x \\ &= x(x + pb)(x - pb) \\ x &= \frac{y^2}{(x + pb)(x - pb)} \\ &= \frac{-y^2}{p^2(1 + tpb)(1 - tpb)} \end{aligned}$$

  where in the last line we substituted our hypothesis $x = p^2t$. But $1 + tpb$ and $1 - tpb$ are squares in $\mathbb{Z}_p$, since they are congruent to 1 modulo p, $\left(\frac{1}{p}\right) = 1$, and we can lift them noting that $\nu_p(1 \pm tpb) = 0$. Thus,

  $$\sqrt{-x} = \frac{y}{p\sqrt{1 + tpb}\sqrt{1 - tpb}}, \in \mathbb{Q}_p,$$

  and is in fact in $\mathbb{Z}_p$ since x also is. Finally, we have the solution

  $$r = \frac{\sqrt{-x}}{pb},$$

  so indeed $S \in P(r) + (0, 0)$.

- If $x \equiv pb\,(p^2)$, we want to show that $S \in P(r) + (n, 0)$. Writing $x = pb + tp^2$ for some $t \in \mathbb{Z}_p$, we want to find $r \in \mathbb{Z}_p$ such that

$$x = -n + \frac{n}{1 - nr^2}$$

or equivalently

$$r^2 = \frac{1}{n} \cdot \frac{x - n}{x + n}.$$

Again using the equation of the curve,

$$\begin{aligned} r^2 &= \frac{1}{n} \cdot \frac{x(x-n)^2}{x(x+n)(x-n)} \\ &= \frac{(x-n)^2 x}{ny^2}. \end{aligned}$$

But $x = pb + p^2 t$, so

$$r^2 = \left(\frac{x - n}{y}\right)^2 (1 + pb^{-1}t).$$

A similar argument to the above case shows that $1 + pb^{-1}t$ is a square in $\mathbb{Z}_p$ enabling us to solve for $r \in \mathbb{Z}_p$. Thus, we have $S \in P(r) + (n, 0)$.

- If $x \equiv -pb\,(p^2)$, we want to show that $S \in P(r) + (-n, 0)$. After writing $x = -pb + tp^2$, an entirely analogous computation to the previous case using the corresponding formulas gives

$$r^2 = \left(\frac{x + n}{y}\right)^2 (1 - pb^{-1}t).$$

Again we know $1 - pb^{-1}t$ is a square in $\mathbb{Z}_p$, and can solve for r. Thus, we have $S \in P(r) + (-n, 0)$.

Since, as we noted, the cosets are distinct, this finishes the proof of the theorem. □

As an immediate consequence, we have:

Theorem 5.4.0.4. *Let n be a odd squarefree integer. If $p \nmid 2n$, the Tamagawa number c_p of E_n is 4.*

It remains to compute the Tamagawa number of E_n at 2. Modulo 2, the equation of the curve reduces to

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

Checking manually, we get that

$$\tilde{E}(\mathbb{F}_2) = \{\mathcal{O}, (0, 0), (1, 0)\},$$

where we remember that $(1, 0)$ is the singular point (see 5.4.0.1).

We will consider the reduction modulo 2 map

$$\pi : E(\mathbb{Q}_2) \to \tilde{E}(\mathbb{F}_2).$$

Recall that

$$c_2 = \left| \frac{E(\mathbb{Q}_2)}{E(\mathbb{Q}_2)_0} \right|,$$

where

$$E(\mathbb{Q}_2)_0 = \pi^{-1}(\tilde{E}(\mathbb{F}_2)_{ns}) = \{P \in E(\mathbb{Q}_2) \,|\, \pi(P) = \mathcal{O} \text{ or } \pi(P) = (0,0)\}.$$

Theorem 5.4.0.5. *Let n be an odd squarefree integer. Then the Tamagawa number c_2 of E_n is 2.*

Proof. The preimages of $\mathcal{O}$ and $(0,0)$ are nonsingular, and hence are in the trivial coset. To prove our claim, we will show that the preimages of the singular point $(1,0)$ lie in a single different coset $\overline{(1,0)}$.

In other words, if $P, Q \in \pi^{-1}(1,0)$, we want to show that

$$P = Q + R, \text{ for some } R \in E(\mathbb{Q}_2)_0$$

or equivalently,

$$P - Q \in E(\mathbb{Q}_2)_0.$$

It turns out that choosing $Q = (n,0)$ does the job. Note that $Q = -Q$, so me may show that $P + Q \in E(\mathbb{Q}_2)_0$.

Let $P = (x,y)$ and $(u,v) = P + (n,0)$. In order to get a contradiction, assume $(u,v) \notin E(\mathbb{Q}_2)_0$ so $\pi(u,v) = (1,0)$. Writing $(u,v) = (u : v : 1)$ in projective coordinates for a moment, we have

$$\pi(u : v : 1) = (1 : 0 : 1)$$

so there exists some $a \in \mathbb{Z}$ so that

$$2^a u \in \mathbb{Z}_2^\times, \;\; 2^a v \in 2\mathbb{Z}_2, \;\; 2^a 1 \in \mathbb{Z}_2^\times.$$

The last condition forces $a = 0$, so $2^a u = u$ is a unit. The same argument also shows that x must be a unit.

Back to affine coordinates, let λ be the gradient of the line through $(x,y), (n,0)$ and (u,v).

From the addition formulas, we have

$$u = \lambda^2 - x - n,$$

so

$$\lambda^2 = u + x + n \equiv 1 + 1 + 1 \equiv 1 \,(2),$$

and we see that λ is a 2-adic unit.

By definition,

$$\lambda = \frac{y}{x - n},$$

and plugging into the equation of the curve gives

$$(\lambda(x-n))^2 = y^2 = x^3 - nx = x(x+n)(x-n).$$

Simpliflying, we get

$$\lambda^2 = \frac{x(x+n)}{x-n}.$$

Here x and λ are units, so $\frac{x+n}{x-n}$ must also belong to $\mathbb{Z}_2^\times$. To get a contradiction, we will show $x+n$ and $x-n$ have different valuations.

If $\nu_2(x+n) = a$, writing $x+n = 2^a k, k \in \mathbb{Z}_2^\times$, we get

$$x - n = 2^a k - 2n = 2(2^{a-1}k - n).$$

But $\nu_2(2^{a-1}k - n) \neq a-1$ since n is odd, so

$$\nu_2(x+n) \neq \nu_2(x-n),$$

as wanted.

Thus, u is not a unit, and $\pi(P + (n,0)) \neq (1,0)$, which concludes our proof. □

Corollary 5.4.0.6. *Let n be odd and square free. Then*

$$\prod_p c_p(E_n) = 2 \cdot 4^{\omega(n)},$$

where $\omega(n)$ is the number of distinct prime factors of n.

Chapter 6

Conclusion

Having worked out all the main computable invariants for the family E_n, we now match our calculations with what is predicted by the BSD conjecture.

Recall Tunnell's theorem (Equation 2.7.0.2), which in our case states that if n is odd and squarefree then

$$L(E_n, 1) = \frac{\beta}{4\sqrt{n}} a_n^2,$$

where $\beta = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}}$ and the integers a_n are the coefficients of the theta series described in Equation 2.7.0.2.

We know that the size of the torsion group of E_n is

$$\#\mathrm{Tors}(E_n) = 4,$$

(see Proposition 2.1.0.8). The real period of E_n is given by

$$\Omega_{E_n} = \frac{2\beta}{\sqrt{n}}$$

(see Definition 2.5.0.1) and the Tamagawa numbers of E_n are

$$\begin{aligned} c_2(E_n) &= 2 \\ c_p(E_n) &= 4 \text{ if } p \mid n \\ c_l(E_n) &= 1 \text{ if } l \neq p. \end{aligned}$$

(see Theorems 5.4.0.4 and 5.4.0.5).

Substituting the data into the BSD conjecture (Equation 2.7.0.1), we get the prediction

$$L(E_n, s) = C(s-1)^r + O((s-1)^{r+1})$$

where

$$\begin{aligned} C &= \frac{\#\mathrm{Sha}(E_n) R_{E_n} \Omega_{E_n}}{\#\mathrm{Tors}(E_n)^2} \prod_p c_p \\ &= \frac{\#\mathrm{Sha}(E_n) R_{E_n} \beta}{4} \cdot 4^{\omega(a)}. \end{aligned}$$

Putting both expressions for $L(E_n, 1)$ together, the Birch Swinnerton-Dyer conjecture predicts that

$$a_n^2 = \#\mathrm{Sha}(E_n) \cdot R_{E_n} \cdot 4^{\omega(n)} \cdot 0^r. \tag{6.0.0.1}$$

where $\omega(n)$ is the number of prime factors of n.

If n has at least 2 prime factors, we computed (see Theorem 5.2.0.3)

$$a_n \equiv 0 \mod 4,$$

so Equation 6.0.0.1 predicts that

$$0 \equiv 0 \mod 16,$$

which is true, but a bit uninsteresting.

If $n = p$ is an odd prime, we have found (see Theorem 5.2.0.3)

$$a_p \equiv \begin{cases} 0 \mod 4 & \text{if } p \equiv 1, 5, 7 \mod 8 \\ 2 \mod 4 & \text{if } p \equiv 3 \mod 8 \end{cases}$$

so that

$$a_p^2 \equiv \begin{cases} 0 \mod 16 & \text{if } p \equiv 1, 5, 7 \mod 8 \\ 4 \mod 32 & \text{if } p \equiv 3 \mod 8, \end{cases}$$

since the squares of all numbers congruent to 2 modulo 4 are congruent to 4 modulo 32.

We also found (see Theorem 5.3.3.3) that the Selmer rank s_r of E_p satisfies

$$s_r = \begin{cases} 0 \text{ if } p \equiv 3 \mod 8 \\ 1 \text{ if } p \equiv 5, 7 \mod 8 \\ 2 \text{ if } p \equiv 1 \mod 8. \end{cases}$$

In order to achieve the strongest possible results, we will need to refer to one last tool, which gives some structure to the Tate-Shafarevich group.

Proposition 6.0.0.1. *Let $E(\mathbb{Q})$ be an elliptic curve. There exists an alternating bilinear pairing*

$$\langle \cdot \rangle : \text{Sha}(E) \times \text{Sha}(E) \to \mathbb{Q}/\mathbb{Z}.$$

The kernel of $\langle \cdot \rangle$ is given by

$$K = \{x \in \text{Sha}(E) \mid \text{ for all positive integers } n, \exists y \in \text{Sha}(E) \text{ such that } x = ny\}.$$

In particular, if $\text{Sha}(E)$ is finite, then its order is a perfect square.

Proof. [See Cas62]. □

Conjecture 6.0.0.2. *We have $K = 0$, where K is the set of divisible elmeents of $\text{Sha}(E)$, defined in the previous proposition.*

This conjecture is known to be true when the rank is 0, which will be enough for our purposes.

The calculations in this project have allowed us to formulate and prove the following two predictions.

Theorem 6.0.0.3. *If $p \not\equiv 3\,(8)$, Equation 6.0.0.1 is valid modulo 8. If Conjecture 6.0.0.2 is true, then it also holds modulo 16.*

Proof. If $p \not\equiv 3\,(8)$, the coefficient a_p is 0 modulo 4. Thus, the BSD conjecture predicts that

$$4 \cdot \#\text{Sha}(E_p) \cdot R_{E_p} \cdot 0^r \equiv 0 \mod 16. \tag{6.0.0.2}$$

- We will first show that Equation 6.0.0.2 is true modulo 8. This is equivalent to showing that

  $$\#\text{Sha}(E_p) \cdot R_{E_p} \cdot 0^r \equiv 0 \mod 2.$$

  If the rank is nonzero, this is trivially satisfied, since the left hand side is then precisely 0. If $r = 0$, $R_{E_p} = 1$, so we expect

  $$\#\text{Sha}(E_p) \equiv 0 \mod 2.$$

  If $\text{Sha}(E_p)$ is infinite, we will take this statement to mean that $\text{Sha}(E_p)$ contains a point of 2-torsion.

  For the case where $p \not\equiv 3\,(8)$ and the rank is 0, no equations from 5.3.2.2 besides the trivial one (with $d_1 = 1$) have rational solutions. Thus, we have

  $$\#\text{Sha}(\bar{E}_p)[\psi] = \#\text{Sel}(\bar{E}_p)[\psi] = \begin{cases} 2 & \text{if } p \equiv 5, 7 \mod 8 \\ 4 & \text{if } p \equiv 1 \mod 8. \end{cases}$$

  and

  $$\#\text{Sha}(E_p)[\phi] = \#\text{Sha}(E_p)[\phi] = 1$$

  Recall that the construction of the ϕ and ψ isogenies gives us a sequence of homomorphisms

  $$\text{Sha}(E_p) \xrightarrow{\phi} \text{Sha}(\bar{E}_p) \xrightarrow{\psi} \text{Sha}(E_p)$$

  with $\psi \circ \phi(P) = 2P$. Since $\text{Sha}(E_p)[\phi] = 0$, we must have $\text{Sha}(E_p)[2] = \text{Sha}(\bar{E}_p)[\psi]$, so

  $$\#\text{Sha}(E_p)[2] = 2 \text{ or } 4 > 0.$$

  Thus, $\text{Sha}(E_p)$ contains an element of 2-torsion, as wanted.

- In order to prove Equation 6.0.0.2, we must have

  $$\#\text{Sha}(E_p) \equiv 0 \mod 4.$$

  We will show that, assuming Conjecture 6.0.0.2, that $\text{Sha}(E_p)$ has in fact at least 4 elements of 2-torsion.

  Let $x \in \text{Sha}(E_p)$ be the element of 2-torsion found above. Assuming the conjecture, we can find some $y \in \text{Sha}(E_p)$ such that $\langle x, y \rangle \neq 0$ (since the kernel of $\langle \cdot \rangle$ is then equal to 0). But then

  $$2\langle x, y \rangle = \langle 2x, y \rangle = \langle 0, y \rangle = 0,$$

  so $\langle x, y \rangle = \frac{1}{2}$.

Suppose y has order n in $\text{Sha}(E_p)$. Then

$$0 = \langle x, ny \rangle = n\langle x, y \rangle = \frac{n}{2},$$

so $\frac{n}{2} \in \mathbb{Z}$, and n is even. Write $n = 2^a k$ for k odd, and let $z = ky$. Then

$$\langle x, z \rangle = \frac{k}{2} \equiv \frac{1}{2},$$

so in particular $z \neq x$. But z has order 2^a, so it is contained in the 2-Sylow subgroup of $\text{Sha}(E_p)$, and thus $\#\text{Sha}(E_p)$ is a multiple of 4, as wanted.

□

Theorem 6.0.0.4. *If $p \equiv 3\,(8)$, the BSD conjecture predicts that the rank of E_p is 0, and this is indeed true. If furthermore $\text{Sha}(E_p)$ is finite, then Equation 6.0.0.1 holds modulo 32.*

Proof. If $p \equiv 3\,(8)$, we have $a_p^2 \equiv 4\,(32)$, so the BSD conjecture predicts that

$$\#\text{Sha}(E_p) \cdot R_{E_p} \cdot 0^r \equiv 4 \mod 32.$$

In particular, the right hand side is not 0, so we must have $r = 0$. This agrees with the calculations of the Selmer rank, where we've seen that in this case $s_r = 0$, and we always have $s_r \geq r$. In this case, the regulator $R_{E_p} = 1$, so the prediction is equivalent to

$$\#\text{Sha}(E_p) \equiv 1 \mod 8.$$

In this case we have $\text{Sha}(E_p)[\phi] = \text{Sha}(\bar{E}_p)[\psi] = 0$, so $\text{Sha}(E_p)[2] = 0$. By Sylow's theorem, this means that in Sha is finite, it must have odd order. But then the Cassels pairing is perfect, so the order of $\text{Sha}(E_p)$ is a square, and hence congruent to 1 modulo 8. This finishes the proof. □

The takeaway is that if we assume $\text{Sha}(E_n)$ is finite, we have proved that Equation 6.0.0.1 holds either modulo 16 if $n \not\equiv 3\,(8)$, or modulo 32 if $n \equiv 3\,(8)$. If $\text{Sha}(E_n)$ is *not* finite, we can still interpret our result as saying that Equation 6.0.0.1 holds modulo 8 for all n.

Bibliography

[Cas62] John William Scott Cassels. "Arithmetic on curves of genus 1. III. The Tate-Shafarevich and Selmer groups". In: *Proceedings of the London Mathematical Society* (1962).

[Con] Keith Conrad. *Hensel's Lemma*. URL: `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf`.

[Gra11] Andrew Granville. *Rational and Integral Points on Curves*. 2011. URL: `http://www.dms.umontreal.ca/~andrew/Courses/RationalPtsOnCurves.pdf`.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, 1990.

[Kil15] L. J. P. Kilford. *Modular Forms: a classical and computational introduction*. Imperial College Press, 2015.

[Kob93] Neal Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer, 1993.

[Lan76] Serge Lang. *Introduction to Modular Forms*. Springer, 1976.

[Lor96] Dino Lorenzini. *An Invitation to Arithmetic Geometry*. American Mathematical Society, 1996.

[Loz78] Alvaro Lozano-Robledo. *Elliptic Curves, Modular Forms, and Their L-Functions*. American Mathematical Society, 1978.

[Mar77] Daniel Marcus. *Number Fields*. Springer, 1977.

[Ser02] Jean-Pierre Serre. *Galois Cohomology*. Springer, 2002.

[Ser79] Jean-Pierre Serre. *Local Fields*. Springer, 1979.

[Ser96] Jean-Pierre Serre. *A Course in Arithmetic*. Springer, 1996.

[Sil16] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2016.

[ST90] Joseph Silverman and John Tate. *Rational Points on Elliptic Curves*. Springer, 1990.

[Tun83] J.B. Tunnell. "A Classical Diophantine Problem and Modular Forms of Weight 3/2". In: *Inventiones Mathematicae* 72 (1983), pp. 323, 334.

[Wil06] Herbert S. Wilf. *Generatingfunctionology*. CRC Press, 2006.