Iwasawa Theory of Elliptic Curves with Complex Multiplication

Anna Seigal

2nd May 2014

Contents

1 Introduction

1.1 Elliptic Curves with Complex Multiplication

Let F be a number field: that is, $F/\mathbb{Q}$ some finite extension. An elliptic curve E/K is one of the simplest non-trivial examples of an abelian variety. It is a smooth genus 1 algebraic variety upon which we also have an abelian group structure. It can be considered to be the projective closure of a curve of the form

$$y^2 = f(x)$$

where f is some cubic polynomial with no quadratic term in x. We obtain the closure by adjoining at point at infinity, denoted O_E. In fact, we can show that any curve defined over a field F with $\mathrm{char}(F) \neq 2, 3$ can be put into this form, not just those defined over a number field.

An endomorphism of an elliptic curve is a morphism of varieties which maps the curve to itself, and the point at infinity to itself. The set $\mathrm{End}_F(E)$ denotes those endomorphisms which are defined over F, that is, they are expressible as ratios of polynomials whose coefficients lie in the field F.

The additive abelian group action is denoted by $(P, Q) \mapsto P \oplus Q$. It admits the "multiplication by n" homomorphism

$$[n] : P \mapsto \underbrace{P \oplus \cdots \oplus P}_{n \text{ times}}$$

Since we never have $mP = nP$ for all $P \in E(\overline{F})$ and $m \neq n$, this shows that we can always inject $\mathbb{Z}$ into the group $\mathrm{End}_F(E)$.

Definition: An elliptic curve E/F has *complex multiplication* if

$$\mathrm{End}_F(E) \neq \mathbb{Z}$$

This means we have endomorphisms of E, defined over F, that are not "multiplication by n" maps, for some $n \in \mathbb{Z}$. Since F is a number field, this implies that

$$\mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$$

where K is some imaginary quadratic field. We briefly remark here the importance of F being an extension of the field $\mathbb{Q}$. If F were a field with positive characteristic, we would trivially have additional endomorphisms since the coefficients of the curve would all satisfy $x^q = x$ for some q.

If we consider $E/\mathbb{C}$, we have the isomorphism

$$E(\mathbb{C}) \approxeq \mathbb{C}/L$$

for some lattice L. Complex multiplication arises when we have maps on L that are not $[n]$ for some $n \in \mathbb{Z}$, that is, extra symmetries (rotations) of the lattice L.

More generally we use the term "complex multiplication" as applied to other objects to refer to the case where we have more than the usual number of endomorphisms. It allows us to develop a far richer theory than we otherwise could.

We will only study elliptic curves with complex multiplication, and this property will underlie the majority of our analyses. In the case of elliptic curves without complex multiplication we can sometimes still show the analytic continuation and functional equation of the complex L-function but, at present, it is not known how to do so via the method we will use.

An example of the necessity for the curve to have complex multiplication is shown in Section 2.2. Here we find the commutants of the Tate module (defined in Section 2.2.1). If the curve has no complex multiplication then all the endomorphisms trivially commute and this analysis gives no additional information.

We are able to generate abelian extensions of our ground field, corresponding to adjoining the points of α-torsion for some $\alpha \in \mathrm{End}_F(E)$. These are crucial to our later analyses. In Chapter 3 we will use the complex multiplication property to construct the p-adic L-functions and in Chapter 4 we relate these functions to the arithmetic properties of the curve.

1.2 Motivating Examples

1.2.1 The Congruent Number Problem

The *congruent number problem* is widely held to be the main motivating example of the study of the arithmetic properties of elliptic curves. It asks when an integer is

expressible as the area of a right-angled triangle with rational sides. Since a great deal of work goes into this theory, it is worth thinking about whether this question is natural, important and interesting, and I will pause for a moment here to discuss the congruent number problem and its long-standing mathematical interest.

The congruent number problem is thought to date back thousands of years, and very early written references have been found, including an anonymous manuscript written in Arabic which pre-dates the year 972[1]. It is thought to first have entered western thought via the Sicilian court of Frederic II in the early 13th Century[2].

Examples of congruent numbers were found and documented for many hundreds of years before the first known instance of theory that moved beyond just finding an example. This was the claim

"1 is not congruent"

It was proven by Fermat in the 17th century using his famous method of infinite descent.

The main conjecture associated to the study of congruent numbers is the claim:

$$D = 5, 6, 7 \mod 8 \quad \Longrightarrow \quad D \text{ congruent}$$

It is clear from written sources that this pattern has long been observed. We are now importantly able to explain why the above implication *should* hold. It has also been shown recently that for every k, there are infitely many square-free D in each of the above congruence classes such that the above implication holds[3]. At the time of writing, a complete proof of the above conjecture remains out of reach and is a very important open problem in number theory.

The congruent number problem is related to elliptic curves $E_D/\mathbb{Q}$ as follows: the condition "D is congruent" is equivalent to the existence of a $(x, y) \in E_D(\mathbb{Q})$, with $y \neq 0$, where

$$E_D : y^2 = x^3 - D^2 x$$

The transformation sending $(x, y) \mapsto (-x, iy)$ is an endomorphism of E_D, and is not of the form $[n]$ for some $n \in \mathbb{Z}$. Hence E_D has complex multiplication. We can show that the torsion group of E_D exactly consists of the 2-torsion:

$$\{(0, 0), (D, 0), (-D, 0), O_E\}$$

Hence, D being congruent is equivalent to the positivity of the rank of $E(\mathbb{Q})$. This connection to the rank of the elliptic curve links our question about right-angled triangles to the Birch and Swinnerton-Dyer Conjecture.

[1] L.E. Dickson, *History of the Theory of Numbers: Diophantine Analysis* Volume 2, 1971
[2] N. Schappacher, *Diophantus of Alexandria: A Text and its History*, 2005
[3] Y. Tian, *Congruent Numbers and Heegner Points*, 2012

1.2.2 Introduction to our Main Example

I will focus on a different elliptic curve, which also has great importance within this field of study. The curve has minimal Weierstrass equation given by

$$y^2 + xy = x^3 - x^2 - 2x - 1$$

and it has complex multiplication by $\mathbb{Z}\left[\frac{(1+\sqrt{-7})}{2}\right]$. We note that

$$-7 = 1 \mod 4 \quad \Longrightarrow \quad (1+\sqrt{-7})/2 \in \mathcal{O}_K$$

and hence it has complex multiplication by the full ring of integers in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-7})$.

Note that $K = \mathbb{Q}(\sqrt{-7})$ has class number 1, and the only roots of unity in K are $\{\pm 1\}$: roots of unity are algebraic integers, so $\mu \in K$ implies $\mu = a + b(1+\sqrt{-7})/2$ for some $a, b \in \mathbb{Z}$.

$$\left| a + b\frac{(1+\sqrt{-7})}{2} \right| = 1 \quad \Rightarrow \quad (a + b/2)^2 + 7b^2/4 = 1 \quad \Rightarrow \quad b = 0$$

since both squared terms are positive, and $7/4 > 1$. Evaluating the complex L-function of E at $s = 1$ show that E has rank 0.

We know additional information about the elliptic curve E by considering its corresponding modular curve, $X_0(49)$. We have a non-constant rational map defined over $\mathbb{Q}$:

$$X_0(49) \to E$$

which sends the cusp of $X_0(49)$ at infinity, denoted by $[\infty]$, to the point at infinity on E. The other equivalence class of cusps on $X_0(49)$ is sent via this map to the other torsion point on E defined over $\mathbb{Q}$: the point $(2, -1)$. We often refer to the elliptic curve E by is corresponding modular curve $X_0(49)$.

The "strong version" of the Birch and Swinnerton-Dyer conjecture is known to be true for $X_0(49)$, i.e. the p-part of the conjecture is known to be true for all p. In Section 1.4.2 we will see the statement of the Birch and Swinnerton-Dyer conjecture (or BSD conjecture, for short) and perform a calculation which shows the "strong version" of the conjecture to hold for our curve.

The theory that is developed over the course of this essay tells us about the p-adic L-functions, and later the p-part of the BSD conjecture, where p is an odd prime which splits in the quadratic field K.

This accessibility of the full BSD for our curve is on account of its behaviour at the prime 2. This prime is not covered, in general, by the methods involving p-adic L-functions that we will use. However much more can be said in the case of this particular curve on account of the fact that it has potentially ordinary reduction at 2. In Section 1.4.2, we will define the family of curves obtained by taking certain quadratic twists of this curve, which allows us to construct an infinite family of

related elliptic curves with complex multiplication. We will then see that the "strong version" of the BSD conjecture is known for this entire family. This makes the family of curves very special.

1.3 Set-up and Strategy

Take E/F an elliptic curve. As above, E has complex multiplication and

$$\mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q} = K$$

which implies that $\mathrm{End}_F(E)$ is an order in $\mathcal{O}_K$, the ring of integers of K. At times, we will restrict to the case $\mathrm{End}_F(E) = \mathcal{O}_K$, the full ring of integers. Any curve whose ring of endomorphisms, R, is an order in $\mathcal{O}_K$ is isogenous over K to a curve whose ring of integers is all of $\mathcal{O}_K$. So, relative to our sphere of consideration, this assumption does not result in a loss of generality.

In Chapter 2, I will outline how to construct the Grossencharacter associated to our elliptic curve E, and demonstrate how this is used to show the analytic continuation and functional equation of the complex L-function of the curve. We express the complex L-function as the product of two Hecke L-functions, that of the Grossencharacter and that of its complex conjugate Grossencharacter.

Whilst the theory works, with almost identical proofs, for the case E/F an elliptic curve defined over a general number field F, I will restrict (for computational ease) to the case where E is defined over K, and E also has complex multiplication by an order in the field K (E is described as having "complex multiplication by K").

Consider the faithful action of $\mathrm{End}_F(E)$ on the ring of differentials $\Omega_{F/E}$:

$$fdg \mapsto (\phi^* f) d(\phi^* g)$$

We obtain an embedding $K \hookrightarrow F$. When we assume that, in fact, $F = K$, we get that the Hilbert Class Field is also K. These assumptions imply that $h_K = 1$, where h_K is the size of the ideal class group $\mathrm{Cl}(K)$, which we can see by considering the degree of the endomorphism as a well-ordering on K.

In Chapter 2, we will also see that we can adjoin the α-torsion points on E to a field K, to generate an abelian Galois extension. In the spirit of Iwasawa theory, these field extensions are useful because we will eventually consider the infinite tower of fields generated by α^n-torsion points, for all n. We observe here the similarity in the construction to the cyclotomic infinite tower:

$$E_{p^n}, \text{ the } p^n\text{-torsion points} \qquad \Longleftrightarrow \qquad \mu_{p^n}, \text{ the } p^n\text{th roots of unity}$$

In brief, the way that our theory develops in Chapter 2, is via the key observation that our Frobenius endomorphism (on the reduced curve at a place v) has a *unique* lift to an endomorphism of the original curve, up to tensoring by some element of $\mathbb{Q}$. This uniqueness carries over to the key property required in constructing the

Grossencharacter: we require a unique generating element of the prime v. In the case where $F = K$, this generating element will simply be the lifting of our Frobenius map. In the case where F is some finite extension of K, things are complicated only by the need to consider the norm $N_{F/K}$ of elements in F.

Despite all we can show about the complex L-function of our elliptic curve, we are unable to link its properties to the arithmetic properties of the curve without a consideration of the corresponding p-adic scenario.

In Chapter 3, I will construct the $\mathfrak{p}$-adic L-function where p is some prime in $\mathbb{Q}$ which satisfies:

1. The prime $p > 3$, and p splits in K as $\mathfrak{p}\mathfrak{p}^*$, with $\mathfrak{p} \neq \mathfrak{p}^*$
2. The curve E has good, ordinary reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$, i.e. the reduced curve obtained at these primes is non-singular, and the p^r torsion groups are non-trivial

Here I will mostly follow the approach taken in the "Iwasawa Theory of Elliptic Curves with Complex Multiplication" notes from Lent Term 2010, Cambridge. The notes represent the backbone for how I came to understand the topic, and in my remarks and proofs I will aim to remain true to this process. The proofs I will give of the main results along the way, together with the elaborations and explanations, are my own.

In the cyclotomic case, we show that the field obtained by adjoining all the p-power roots of unity is related to the p-adic analogue of the Riemann-Zeta function. Similarly here we show that the field obtained by adjoining the $\mathfrak{p}$-power torsion points on E to K is related to the $\mathfrak{p}$-adic analogue of the complex L-function: the $\mathfrak{p}$-adic L-function.

The method for this chapter, roughly, is as follows: our group of interest is

$$G = \mathrm{Gal}(K(E_{\mathfrak{p}^\infty})/K)$$

the Galois group of the infinite tower of fields extension of K we obtain by adjoining the $\mathfrak{p}^n$-torsion points on E, for all n. We show a correspondence between p-adic measures of our group, and a certain formal power series ring. A surprisingly hard stage is to identify a canonical element of the power series ring that we can associate to our measures. We seek a measure with certain properties and, from this, obtain a primitive pseudo-measure. The power series associated to the measure will be our $\mathfrak{p}$-adic L-function.

In Chapter 4 we see how the $\mathfrak{p}$-adic L-function relates to the main conjecture of Iwasawa theory for elliptic curves with complex multiplication. We will focus here on the one-variable main conjecture and continue to restrict to the simplest set-up of fields: that with E/K our curve, and $\mathrm{End}_K(E) \otimes \mathbb{Q} = K$.

We will construct the statement of the main conjecture. This requires the introduction of a few more concepts, most importantly a structure theorem for a type of torsion module and defining, from this, the characteristic ideal. We then define the

groups of global, elliptic and local units which we use in our first stage of proving the main conjecture. I will give a brief mention of the next stage of proving the main conjecture, using the evaluation of our Euler function in at particular points of the curve, but I will not go into detail on this.

We will then discuss how these results relate to the arithmetic of the elliptic curve via the BSD conjecture. We will see that the $\mathfrak{p}$-adic L-functions are used to describe the $\mathfrak{p}$-parts of the $Ш_{E/K}$ group, and hence to give a full description of the $\mathfrak{p}$-part of the BSD conjecture. We note that, for the primes that are not of the above form, our methods do not tell us about the prime part of $Ш_{E/K}$ for that prime.

1.4 Knowns and Unknowns in the Main Conjectures of Iwasawa Theory

This essay discusses the theory underlying the one-variable main conjecture of Iwasawa theory for elliptic curves with complex multiplication. To place this conjecture in a wider context, and appreciate the limitations of our current knowledge about the Iwasawa theory of elliptic curves, I briefly discuss the following in Section 1.4.1:

1. How our one-variable main conjecture relates to the other Iwasawa conjectures about elliptic curves
2. Which parts of the conjectures have been proven for different curves and at different primes

In Section 1.4.2, we discuss the knowns and unknowns in relation to the BSD conjecture. That which is known for elliptic curves with complex multiplication is largely proven via the methods of Iwasawa theory.

The main conjectures of Iwasawa theory for elliptic curves with complex multiplication are, equivalently, the conjectures for Iwasawa theory for an imaginary quadratic field. I have already mentioned the first example of Iwasawa theory: the main conjecture for cyclotomic fields. This was originally stated, and almost proven, by Iwasawa himself.

Iwasawa theory main conjectures have now been postulated, and proven, over many different types of field, including further examples of p-adic Lie extensions of number fields. They are characterised by an association between formulae concerning the arithmetic properties of stuctures (such as elliptic curves, in our case, or elements of the category of motives, more generally) and the evaluation of their corresponding L-functions. For example, an appropriate version of the main conjecture has been proven for all totally real fields[4].

[4] A. Wiles, *The Iwasawa Conjecture for Totally Real Fields*, Annals of Mathematics, 1990

1.4.1 Iwasawa Theory of Elliptic Curves

In very broad terms, the one-variable main conjecture of Iwasawa theory says that the $\mathfrak{p}$-adic L-function, which we will later construct, generates the charactestic ideal for a certain module over the Iwasawa algebra given in terms of the field

$$K_\infty = K(E_{\mathfrak{p}^\infty})$$

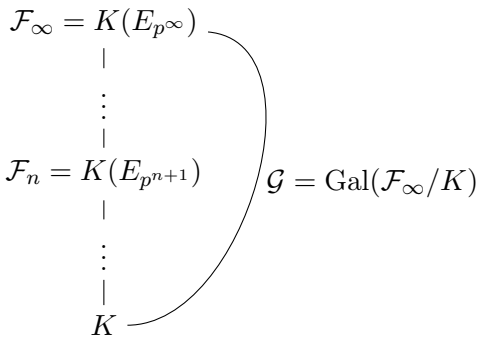
This conjecture is completely proven for elliptic curves with complex multiplication when $p = \mathfrak{p}\mathfrak{p}^*$ is the prime factorisation of p in K with p a prime of good, ordinary reduction.

We also have an analogous two-variable main conjecture which is also completely proven in the case where p is a prime of good, ordinary reduction. It is the direct sibling of the main conjecture for cyclotomic fields. It can be proven in much the same way, and differs from the one-variable main conjecture in that we discuss the group

$$\mathcal{G} = \mathrm{Gal}(\mathcal{F}_\infty/K)$$

where $\mathcal{F}_\infty$ is the two-variable analogue of F_∞: it is the field we obtain by adjoining the p^n torsion points on E, for all n, as opposed to just the $\mathfrak{p}^n$ torsion points. That is, we adjoin the $\mathfrak{p}^*$-power torsion, too, where $\mathfrak{p}\mathfrak{p}^* = p$.

The following diagram shows the set-up of fields and groups that we have for the two-variable main conjecture:



As we see at the start of Chapter 3 this is very similar to the field set-up we have for the one-variable case.

The main conjectures of Iwasawa theory remain unproven in the case where our prime is potentially supersingular, i.e. not of the above form. The reason we are unable to do the analysis for this case is that we cannot carry out the majority of the $\mathfrak{p}$-adic theory for such primes. In some of these cases even a suitable exact statement of the main conjecture remains unknown.

1.4.2 The Birch and Swinnerton-Dyer Conjecture

The main conjectures of Iwasawa theory for elliptic curves tell us about the p-part of $Ш_{E/K}$ predicted by the Birch and Swinnerton-Dyer Conjecture. The "weak version" of the BSD conjecture says that if we let

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

then this rank is the same as the arithmetic rank of the curve E/K, i.e. the rank of the group $E(K)$. The arithmetic rank is denoted by g.

The "strong version" of the BSD conjecture says that, for an elliptic curve E defined over $\mathbb{Q}$, we have

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_\infty \mathrm{Reg}(E) |Ш_{E/\mathbb{Q}}| \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}$$

We note that the left hand side is simply the coefficient of $(s-1)^r$ in the Taylor series expansion for $L(E, s)$ expanded around the points $s = 1$. There is *overwhelming* computational evidence for this conjecture.

The constant Ω_∞, which we define again later, is the period of the invariant differencial ω on E, c_p are the Tamagawa factors for all p, and $\mathrm{Reg}(E)$ is called the regulator of E. It is defined in terms of generators for the the non-torsion part of $E(\mathbb{Q})$.

For a general field F, the Tate-Shafarevich group, $Ш_{E/F}$ is defined by

$$Ш_{E/F} = \ker \left(H^1(F, E) \to \prod_{v \in \Sigma_F} H^1(F_v, E) \right)$$

where Σ_F are the places of F, F_v the completion of F at a plave v, and H^1 the first cohomology group. The group is a measure of our failure to compute the ranks of elliptic curves. It is conjectured to have finite size. If proven, this would not only tell us the ranks of elliptic curves but would also yield an effective algorithm for finding the rank. Proving finiteness of the group in general is still a long way away.

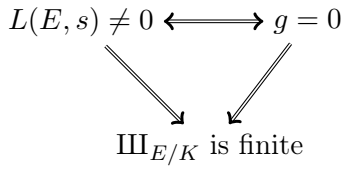
We are interested in the p-part of the group, that is, the subgroup of maximal p-power order: the main conjectures of Iwasawa theory can be used to show that the p-part of $Ш_{E/K}$ has finite size.

The range of values of p for which the methods can be applied depends upon the value of r, defined above. We know the most in the case $r = 0$, we know something in the case $r = 1$, and very little is known for $r \geq 2$.

The Case $r = 0$:

In this case, the "weak version" of the BSD conjecture says that $L(E, s)$ does not vanish at $s = 1$. The "strong version" gives a formula for the evaluation of $L(E, s)$ at $s = 1$. In particular, if the "strong version" of the BSD conjecture could be

shown to hold, this would tell us that the group $Ш_{E/K}$ is always finite. Here are the implications that should hold:



Using our methods, we can prove results that come close to the BSD conjecture for rank 0 elliptic curves.

Let μ_K denote the roots of unity in the field K over which E has complex multiplication. Let $Ш_{E/K}(\mathfrak{p})$ denote the $\mathfrak{p}$-part of $Ш_{E/K}$. We can show that the top equivalence's implication from right to left holds, provided we can find some $\mathfrak{p}$ such that $\mathfrak{p} \nmid |\mu_K|$ and $Ш_{E/K}(\mathfrak{p})$ is finite. This implication holds on account of our results from Iwasawa theory (it requires hard work).

In fact, the following implication holds which is stronger than the implication from left to right in the above diagram:

$$L(E,1) \neq 0 \implies g = 0 \text{ and } Ш_{E/K} \text{ is finite}$$

Furthermore, when $L(E,s) \neq 0$, if, for some prime $\mathfrak{p} \nmid |\mu_K|$, we can show that $Ш_{E/K}(\mathfrak{p})$ is finite, it follows that the order of $Ш_{E/K}(\mathfrak{p})$ is what it should be from the "strong version" of the BSD conjecture.

Piecing all this information together, the BSD conjecture hinges on the existence of a prime $\mathfrak{p} \in K$ for which the $\mathfrak{p}$-part of $Ш_{E/K}$ is finite, and further analysis of those primes dividing $|\mu_K|$. Unless the cube roots of unity lie in K, i.e. $K = \mathbb{Q}(\sqrt{-3})$, we need only remove the primes above 2, and the BSD conjecture holds for all the other primes. For the primes above $p = 2$, though, we often encounter difficulty. Our main example is one of the least troublesome at the prime $p = 2$.

In fact, in the case $L(E,1) \neq 0$, something can also be said in the case where $E/\mathbb{Q}$ does not have complex multiplication, although a very different method of proof is taken to our Iwasawa theory approach. We know[5] that the order of $Ш_{E/\mathbb{Q}}(p)$ is as predicted by the BSD conjecture, for all but finitely many good ordinary primes p.

Example: The BSD Conjecture for our Main Example

Recall that the rank of

$$y^2 + xy = x^3 - x^2 - 2x - 1$$

is 0, and that we showed that the only roots of unity in K are $\{\pm 1\}$, hence

$$|\mu_K| = 2$$

[5]Theorem 33; J. Coates, *Lecture Notes On the Birch-Swinnerton-Dyer Conjecture*, Notices of the International Congress of Chinese Mathematicians, November 2013

We aim to show that the full "strong version" of the BSD conjecture holds for our curve.

A calculation shows that there exists some p for which the p-part of $Ш_{E/\mathbb{Q}}$ *is finite. To show that the full BSD conjecture holds, it remains to look at the place* $p = 2$*. This is much more easily examined for our curve than for most other curves because the prime* 2 *splits in* $K = \mathbb{Q}(\sqrt{-7})$ *as*

$$(2) = \left(\frac{1}{2} + \frac{\sqrt{-7}}{2}\right)\left(\frac{1}{2} - \frac{\sqrt{-7}}{2}\right)$$

and E *has good ordinary reduction at 2.*

The invariant differencial of our curve is

$$\omega = \frac{dx}{2y + x}$$

and we can show that the period of this differential (see later) is

$$\Omega_\infty = \frac{\Gamma(4/7)\Gamma(2/7)\Gamma(1/7)}{2\pi\sqrt{7}}$$

From this, we see that

$$L(E, 1)/\Omega_\infty = 1/2$$

and we deduce that the order of Ш *is predicted to be*

$$Ш_{E/\mathbb{Q}} = \frac{1}{2}\frac{|E(\mathbb{Q})_{tors}|^2}{Reg(E)\prod c_p} = \frac{1}{2} \times \frac{4}{2} = 1$$

We can confirm that this is true.

Example: The BSD Conjecture for a Family of Quadratic Twists of our Main Example

For a general elliptic curve, E, the quadratic twist of $E : y^2 = f(x)$ by $R \in \mathbb{Z}_{>0}$ is given by the equation

$$E^{(R)} : Ry^2 = f(x)$$

The two curves $E^{(R)}$ and E are isomorphic over the field $\mathbb{Q}(\sqrt{R})$. To give an explicit eqation for the quadratic twists of our main example curve, we use the substitutions $y' = y + x/2$ and $x' = x - 1/4$ and make use of the fact that we can multiply through the coordinates a_i by q^i, for some prime q, leaving the elliptic curve unchanged. These allow us to show that the equation

$$E : y^2 + xy = x^3 - x^2 - 2x - 1$$

is equivalent to the equation

$$E : y'^2 = x'^3 - 35x' - 98$$

and hence the quadratic twist of E by $R \in \mathbb{Z}_{>0}$ is given by

$$E^{(R)} : Ry^2 = x^3 - 35x - 98$$

We are able to construct an infinite family of elliptic curves with complex multiplication related to our original curve E. We can then show that, for all members of this family, the full BSD conjecture is known!

Our family of curves are the quadratic twists $E^{(R)}$ where R has particular properties. We require that $R = q_1...q_n$ where, for all i,

$$q_i = 1 \bmod 4 \quad \text{and} \quad q_i \text{ is inert in } \mathbb{Q}(\sqrt{-7})$$

The Case $r = 1$:

For $r = 1$, similarly to the case $r = 0$, the following diagram of equivalences is predicted to hold by the BSD conjecture:

$$\begin{array}{ccc} \text{ord}_{s=1}(L(E,s)) = 1 & \Longleftrightarrow & g = 1 \\ & \searrow \quad \swarrow & \\ & Ш_{E/K} \text{ is finite} & \end{array}$$

Just as before, a stronger version of the left-right implication of the top equivalence holds, and we can actually show that $L(E, s)$ having a simple pole at $s = 1$ implies that $g = 1$ and also $Ш_{E/K}$ is finite. Once again, this is an equivalence and we get the far weaker version of the right-left implication contingent upon the finiteness of $Ш_{E/K}$.

We obtain the same proven results as for the case $r = 0$ but we must make the sacrifice of having to restrict our set of primes for which the full BSD conjecture holds. Here, the primes we consider are those that are good and ordinary. That is, they split in the field K and the reduced curves are non-singular. The BSD conjecture rests upon the existence of a single good, ordinary prime $\mathfrak{p}$ (with $\mathfrak{p} \nmid |\mu_K|$) such that $Ш_{E/K}(\mathfrak{p})$ is finite.

We find a prime $\mathfrak{p}$ such that this holds from our Iwasawa theory arguments. Once it has been obtained, we can show that the "strong version" of the $\mathfrak{p}$-part of the BSD conjecture also holds, i.e. we get the predicted formula for the order of $Ш_{E/K}(\mathfrak{p})$ for good ordinary primes not dividing $|\mu_K|$.

Example: The BSD Conjecture for the Congruent Number Problem

Recall that the congruent number problem requires us to show whether the rank of E_D is positive (we do not wish to find the rank). The above results show that if D is congruent then the complex L-function for our corresponding curve

$$E_D : y^2 = x^3 - D^2x$$

has a zero at $s = 1$ of some order, i.e. vanishes at $s = 1$. Furthermore, if we can find some prime p such that $Ш_{E_D/\mathbb{Q}}(p)$ is finite, then we can show the converse implication: the vanishing of the L-function implies the congruence of D.

When the L-function vanishes at $s = 1$, Rubin has further shown that, if $E(K)$ is finite, then we must have the (seemingly unlikely) scenario that $Ш_{E/K}(\mathfrak{p})$ is infinite for all primes $\mathfrak{p} \nmid |\mu_K|$. We see this again in Section 4.3.

The case $r \geq 2$:

When $\text{ord}_{s=1}(L(E, s)) \geq 2$, we have to restrict the range of scenarios that we can consider even further than for the $r = 1$ case. For example, when $r = 0$ or 1 it is known that the order of vanishing of the $\mathfrak{p}$-adic L-function at $s = 1$ is equal to that of the complex L-function, but this is not known when $r \geq 2$, so we cannot use our same methods from Iwasawa theory to show that the corresponding $\mathfrak{p}$-part of $Ш_{E/K}$ is finite.

However, we can compare the order of vanishing of the $\mathfrak{p}$-adic L-function with the arithmetic rank, g, of the elliptic curve. We can show that the order of vanishing of the $\mathfrak{p}$-adic L-function at $s = 1$ is greater than or equal to g (and in fact we can show that it exceeds the sum of g and the $\mathbb{Z}_p$-corank of $Ш_{E/K}(\mathfrak{p})$).

In the case where the order of vanishing of the $\mathfrak{p}$-adic L-function is equal to g, we can find the order of $Ш_{E/K}(\mathfrak{p})$. This is obtained by looking at the leading term of the Taylor series expansion of the $\mathfrak{p}$-adic L-function at $s = 1$. However, we cannot prove that $Ш_{E/K}(\mathfrak{p})$ is of the form predicted by the "strong version" of the BSD conjecture.

2 The Grossencharacter and the Complex L-function

In this chapter we construct the Grossencharacter, $\psi_{E/K}$, associated to the elliptic curve E. We will then show how it relates to the complex L-function of E via the equation

$$L(E/K, s) = L(\psi_{E/K}, s)L(\psi^*_{E/K}, s)$$

where $\psi^*_{E/K}$ is the complex conjugate Grossencharacter of $\psi_{E/K}$. We will then show how it is used to prove the analytic continuation and functional equation of the complex L-function.

Take an elliptic curve E/K with complex multiplication. We assume that

$$\text{End}_K(E) \otimes \mathbb{Q} = K$$

is an imaginary quadratic field, with $R := \text{End}_K(E)$ some order in K. Recall that the theory works in much the same way for E/F with $F \neq K$, and we make this restriction solely for more simplified calculations. The case $F = K$ includes that of our two main examples since they can both be defined over $\mathbb{Q}$.

Consider the reduction of E at some place v. Our reduced curve $\tilde{E_v}$ is defined over the residue field k_v. Recall that E has good reduction at v if the resulting reduced curve is non-singular.

Example: Good and Bad Reduction

Consider our cure $E : y^2 + xy = x^3 - x^2 - 2x - 1$, $K = \mathbb{Q}(\sqrt{-7})$. *It has discriminant* $\Delta = -7^3$. *The only prime in* $\mathbb{Q}$ *where* E *has bad reduction is* 7, *at which it has additive reduction. We wish to find the primes of bad reduction in* $\mathbb{Q}(\sqrt{-7})$. *Any such prime divides the discriminant.*

The prime factorisation of 7 *in* $\mathbb{Q}(\sqrt{-7})$ *is:*

$$7 = -(\sqrt{-7})^2$$

so $(\sqrt{-7})$ *is the only prime that may be of bad reduction. Changing integral models for* $E/\mathbb{Q}$ *changes the exponent of* $\mathfrak{p}$ *in the dicriminant by* $\mathfrak{p}^{12a}$ *for some* $a \in \mathbb{Z}$. *So,* $(\sqrt{-7})|\Delta$ *for all integral models of* E, *hence it is a prime of bad reduction.*

2.1 The L-function

The complex L-function of E/F is:

$$L(E/F, s) = \prod_{v \in \Sigma_F, v \text{ good}} (1 - a_v (Nv)^{-s} + (Nv)^{1-2s})^{-1}$$

where Σ_F denotes the places of F, $Nv := \#k_v$ is as defined above, and a_v satisfies

$$\#(\tilde{E}_v(k_v)) = Nv + 1 - a_v$$

The L-function's factor at a place v tells us about the reduced curve $\tilde{E}_v$. The L-function is of great interest: its properties are linked conjecturally to arithmetic properties of E, such as the rank, and the Tate-Shafarevich group $Ш_{E/F}$ as detailed in Section 1.4.

2.2 The l-adic representation associated to E

We define the Galois representation:

$$\rho_l : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E))$$

where $T_l(E)$ is the Tate module of E, defined below, and l is some prime number with $l \neq \mathrm{char}(K)$. This gives an action of $\mathrm{Gal}(\overline{K}/K)$ on $T_l(E)$ which we will show is abelian. Later on, we use this to study the abelian extension $K(E[l])/K$.

2.2.1 The Tate Module

Recall that our elliptic curve E is an abelian group. We define the m-torsion group

$$E[m] = \{P \in E(\overline{K}) : mP = 0\}$$

Consider the collection of groups given by $E[l^n]$ for all n. We have the "multiplication by l" map:

$$[l] : E[l^{n+1}] \to E[l^n]$$

which, considered to map from $E[l^{n+1}]$ for all n, give a collection of maps. These groups and maps together give us an inverse system. The Tate module is the inverse limit of the above inverse system. That is, the inverse limit of the groups $E[l^n]$ with respect to the "multiplication by l" maps. It is denoted by

$$T_l(E) = \lim_{\leftarrow n} E[l^n]$$

2.2.2 Defining the Galois Action on the Tate Module

Lemma: *The Galois group Gal$(\overline{K}/K)$ acts on the group $E[l^n]$, for all n, and commutes with the multiplication by l map.*

Proof: The latter claim follows directly from the fact that σ is a homomorphism. Consider some $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and some $P \in E[l^n]$. Using the fact that σ is a homomorphism, we have

$$[l^n](\sigma(P)) = \sigma([l^n]P) = \sigma(0) = \sigma$$

Hence $\sigma(P) \in E[l^n]$. $\square$

This shows that $\sigma \in \mathrm{Gal}(\overline{K}/K)$ acts on $T_l(E)$, and we have the desired map,

$$\rho_l : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E))$$

For all curves E, and for all m with $\mathrm{char}(K) \nmid m$, $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

Note: Over $\mathbb{C}$, this may readily be illustrated. Consider the lattice, L, such that $E(\mathbb{C}) \cong \mathbb{C}/L$. The m-torsion points in $\mathbb{C}/L$ are the images of the points $P \in \frac{1}{m}L$ under the projection $\mathbb{C} \to \mathbb{C}/L$. In each lattice direction, these points have a $(\mathbb{Z}/m\mathbb{Z})$ group structure, hence we obtain the group $(\mathbb{Z}/m\mathbb{Z})^2$ overall.

Using this expression for the group structure of $E[m]$, for $\mathrm{char}(K) \neq l$:

$$T_l(E) \cong \lim_{\leftarrow} (\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}) = \mathbb{Z}_l \times \mathbb{Z}_l$$

When $\mathrm{char}(K)|l$, either $E[l^n] = 0$ or $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z}$, depending only on l and not on n. I will not go into detail on this case.

2.2.3 The Galois Action on the Tate Module is Abelian

We consider the actions of $\mathrm{Gal}(\overline{K}/K)$ and $\mathrm{End}_K(E)$ on the module $T_l(E)$. The ring $\mathrm{End}_K(E)$ acts on the Tate module (i.e. maps each $E[l^n]$ to itself) with the same proof as that for $\mathrm{Gal}(\overline{K}/K)$.

Claim: *The map sending $\phi \in End_K(E)$ to $\phi_l \in Aut(T_l(E))$ is injective.*

Proof: If $\phi_l = 0$ then, for all n, $\phi(P) = 0$ for all $P \in E[l^n]$. Hence, $\phi = [l^n] \circ \psi$ for some $\psi \in \mathrm{End}_K(E)$. If this factorisation of the map ϕ exists for all n, it means $\phi \equiv 0$. So we can think of $\mathrm{End}_K(E)$ as *embedding* into $\mathrm{Aut}(T_l(E))$.

Lemma: *The following equation holds for all $f \in End_K(E)$, $\sigma \in Gal(\overline{K}/K)$:*

$$f \circ \sigma = \sigma \circ f$$

Proof: Since $f : E \to E$ is expressible over K it can be written as $f = (\frac{f_1}{f_2}, \frac{f_3}{f_4})$ where, if $P = (x, y) \in E$, $f_k(x, y) = \sum_{i,j} a_{ij}^{(k)} x^i y^j$ where the $a_{ij}^{(k)} \in K$.

$$\sigma(f_k(x,y)) = \sigma\left(\sum_{i,j} a_{ij}^{(k)} x^i y^j\right) = \sum_{i,j} a_{ij}^{(k)} \sigma(x)^i \sigma(y)^j = f_k(\sigma(x,y))$$

The middle equality holds because $\sigma|_K = \mathrm{id}_K$ and it is a homomorphism. Since this holds for all $(x, y) \in T_l(E)$, σ commutes with each of the f_k, $k = 1, ..., 4$, and hence commutes with f. $\square$

For brevity, we write $R = \mathrm{End}_K(E)$. The above shows that $\rho_l(\mathrm{Gal}(\overline{K}/K) \subset \mathrm{GL}_2(\mathbb{Z}_l)$ lies in the commutant of R.

We will show that the commutant of the image of R in $\mathrm{Aut}(T_l(E))$ is abelian. We can then deduce that the the action of $\mathrm{Gal}(\overline{K}/K)$ on $T_l(E)$ is abelian, by combining this result with our inclusion of $\rho_l(\mathrm{Gal}(\overline{K}/K)$ into the commutant of R.

We define $V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, and $K_l := K \otimes_{\mathbb{Q}} \mathbb{Q}_l$. Since $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$, we have:

$$V_l(E) \cong \mathbb{Q}_l \times \mathbb{Q}_l \quad \text{and} \quad \mathrm{Aut}(V_l(E)) = \mathrm{GL}_2(\mathbb{Q}_l)$$

Since K_l is a vector space over $\mathbb{Q}_l$ of dimension 2, $K_l \cong V_l(E) \cong \mathbb{Q}_l \times \mathbb{Q}_l$ and we may consider the embedding:

$$K_l \to \mathrm{Aut}(V_l(E))$$

$$(x_1, x_2) \mapsto \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}$$

where the $x_i \in \mathbb{Q}_l$.

The elements of $\mathrm{Aut}(V_l(E))$ which commute with R certainly commute with K_l (since K_l is obtained from R by taking the field of fractions and tensoring over $\mathbb{Q}_l$,

and neither of these operations affects the commutativity). Clearly the converse is true, because $R \subset K_l$. The commutant of K_l in $\mathrm{Aut}(V_l(E))$ is the set of matrices such that, for all $x_i \in \mathbb{Q}_l$:

$$\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix} = 0$$

Solving the above equation, it follows immediately that $b = c = 0$. So, the commutant of K_l is the set of diagonal matrices in $\mathrm{GL}_2(V_l(E))$, i.e. the elements of K_l under our embedding map. It is clear that this subgroup of matrices is abelian.

We now wish to consider matrices whose elements lie in the ring $\mathbb{Z}_l$ as opposed to the field $\mathbb{Q}_l$. Consider some element $g \in \mathrm{Aut}(T_l(E)) = \mathrm{GL}_2(\mathbb{Z}_l)$ which commutes with all of R. Then $g \in \mathrm{Aut}(V_l(E))$ and it commutes with all of K_l. So g is a diagonal matrix in $\mathrm{GL}_2(\mathbb{Z}_l)$. Since the subgroup of diagonal matrices is abelian, we are done.

2.3 The Frobenius Map

2.3.1 The Pre-Image of the Frobenius Map

Consider some place v at which E has good reduction. Our reduced curve is $\tilde{E}_v$ defined over k_v. Since $x^{Nv} = x$ for all $x \in k_v$, the map $\phi_v : \tilde{E}_v \to \tilde{E}_v$:

$$\phi_v : (x, y) \mapsto (x^{Nv}, y^{Nv})$$

is in $\mathrm{End}_{k_v}(\tilde{E}_v)$. We call it the Frobenius of $\tilde{E}_v$ at v.

Consider the injective map

$$i_v : \mathrm{End}_K(E) \otimes \mathbb{Q} \to \mathrm{End}_{k_v}(\tilde{E}_v) \otimes \mathbb{Q}$$

which maps an endomoprhism to its action on the reduced curve. We want to show that the Frobenius map has a pre-image in $\mathrm{End}_K(E) \otimes \mathbb{Q} = K$ under i_v.

Note: The Frobenius map commutes with all other elements of of $End_{k_v}(\tilde{E}_v)$ by the same proof as that of Lemma 2.3 (since $\phi_v|_{k_v} = id$).

We study the commutant of $i_v(K)$ in $\mathrm{Aut}(T_l(E))$ with the following changes to our original set-up:

1. Consider the reduced ring of endomorphisms, $\mathrm{End}_{k_v}(\tilde{E}_v)$, and the Tate module of the reduced curve $T_l(\tilde{E}_v)$
2. Replace K by $i_v(K)$, the copy of K inside $\mathrm{End}_{k_v}(\tilde{E}_v) \otimes \mathbb{Q}$
3. We identify $\phi \in K$ with its action on $T_l(\tilde{E}_v)$, first by reduction at the place v, then by applying the map

$$j_v : \mathrm{End}_{k_v}(\tilde{E}_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to \mathrm{Aut}(V_l(\tilde{E}_v))$$

The commutator of $i_v(K)_l$ in $\mathrm{Aut}(V_l(\tilde{E}_v))$ is $i_v(K)_l$. The proof of this is unchanged from our earlier result, save for the changes of notation above.

Since the Frobenius map ϕ_v commutes with all of $\mathrm{End}_{k_v}(\tilde{E}_v)$, we have

$$\phi_v \in i_v(K)_l \cap \mathrm{End}_{k_v}(\tilde{E}_v)$$

It remains to show that $\phi_v \in i_v(K)$. The above implies, in particular, that every element of $i_v(K)$ lies in the commutant of $i_v(K)$ in $\mathrm{End}_{k_v}(\tilde{E}_v)$. But, in fact, the commutant of $i_v(K)$ cannot be larger than this, since the index of $\mathbb{Q}$ in its commutator cannot decrease under the embedding map j_v, and the index of $\mathbb{Q}_l$ in $i_v(K)_l$ is 2.

So, there exists some $\pi_v \in \mathrm{End}_K(E) \otimes \mathbb{Q}$ with $i_v(\pi_v) = \phi_v$.

2.3.2 The Generating Element for the Prime Ideal v

Assume that E/K is an elliptic curve with complex multiplication by some order in K. Take v a prime of good reduction with residue field k_v and $p_v = \mathrm{char}(k_v)$. Assume that $p_v \nmid [\mathcal{O}_K : \mathrm{End}_K(E)]$.

We will show that $(\pi_v) = v$, where (π_v) is the fractional ideal generated by π_v. That is, π_v is a generating element for the prime ideal v.

Step 1: The prime ideal v divides (π_v)

It suffices to show that $\tilde{\pi}_v = 0$, where $\tilde{}$ denotes reduction mod v.

For a general curve E/F with $\mathrm{End}_F(E) \otimes \mathbb{Q} = K$, we have the action of $\mathrm{End}_K(E)$ on the space of holomorphic differentials on E/F, denoted $\Omega_{E/F}$. It is equal to $F\omega$, a one-dimensional vector space over F, where ω is the invariant differential on E. This gives us an embedding $K \hookrightarrow F$. We map each $\phi \in K$ to f where $\phi^*\omega = f\omega$. Here we consider $F = K$, hence $\phi^*\omega = \phi\omega$ for all $\phi \in K$.

Now,

$$\phi_v^*(dx) = d(x^{Nv}) = Nvx^{Nv-1}dx = 0$$

since $\mathrm{char}(k_v)|Nv$. This implies that $\phi_v^* = 0$ on k_v. Take m coprime to p_v such that $m\pi_v$ is in $\mathrm{End}_K(E)$ (possible since $\pi_v \in \mathrm{End}_K(E) \otimes \mathbb{Q}$). Consider the reduction of $(m\pi_v)^*\omega = m\pi_v\omega$ at v. We get

$$(m\tilde{\pi}_v)^*\tilde{\omega} = m\phi_v^*\tilde{\omega} = 0$$

since $\phi_v^*\tilde{\omega} = 0^*\tilde{\omega} = 0$.

Hence $m\tilde{\pi}_v\tilde{\omega} = 0$, therefore $\tilde{\pi}_v = 0$, since m is a unit in k_v. It follows that $v|(\pi_v)$ and this concludes Step 1.

Step 2: We have equality of norms $N_{K/Q}(\pi_v) = Nv = |N_{K/\mathbb{Q}}v|$

Recall that for some endomorphism $\phi \in \mathrm{End}_K(E) \otimes \mathbb{Q}$, i.e. $\phi \in K$, ϕ_l is the map induced by ϕ on the Tate module $T_l(E)$ by considering the action of ϕ on the groups $E[l^n]$.

We have the result[6] $\det(\phi_l) = \deg(\phi)$. The determinant of ϕ_l is $N_{K/\mathbb{Q}}(\phi)$. We have an isomorphism between the modules $V_l(E)$ and $V_l(\tilde{E}_v)$ which we obtain by "reducing at v". See Section 2.4.1 for an explanation of why reduction mod v is injective on $E[l^n]$. Step 2 follows from seeing that the determinant of the image of ϕ_l under this map is Nv.

Step 3: We deduce that $v = (\pi_v)$

The ideal (π_v) is only divisible by primes of K above p_v, since $\mathfrak{p}|(\pi_v)$ implies that $\mathfrak{p}|N_{K/\mathbb{Q}}(\pi_v)$ and $N_{K/\mathbb{Q}}(\pi_v) = |N_{K/\mathbb{Q}}(v)| = p_v^m$ for some $m \in \mathbb{N}$, since v is a prime in K above p_v.

Since p_v has at most two distinct prime factors in K, $(\pi_v) = v^i v^{*j}$ is the prime ideal factorisation of (π_v) where $p_v = vv^*$ is that of p_v and we do not rule out the possibility that $v^* = v$. Step 1 implies that $i > 0$.

By multiplicativity of the norm, $N_{K/\mathbb{Q}}(\pi_v) = (N_{K/\mathbb{Q}}v)^i (N_{K/\mathbb{Q}}v^*)^j$, where $N_{K/\mathbb{Q}}v$ and $N_{K/\mathbb{Q}}v^*$ are both powers of p_v. Now

$$N_{K/\mathbb{Q}}(\pi_v) = Nv = |N_{K/\mathbb{Q}}v|$$

implies that $(N_{K/\mathbb{Q}}v)^{i-1}(N_{K/\mathbb{Q}}v^*)^j = 1$. Hence $i = 1$ and $j = 0$. This concludes the claim that $(\pi_v) = v$.

2.4 The Grossencharacter using Ideals

The Grossencharacter is useful because it allows us to construct an L-function for which we know the analytic continuation and functional equation.

We have E/K with complex multiplication by K. Here, we assume

$$\mathrm{End}_K(E) = \mathcal{O}_K$$

This is solely for simplicity, the results are unchanged without this assumption provided that we replace S by

$$S \cup \{v : v \nmid [\mathcal{O}_K : \mathrm{End}_K(E)]\}$$

We will write $\psi_E = \psi_{E/K}$, since the field K is fixed. Our map ψ_E is defined on primes v by:

$$\psi_E(v) = \pi_v$$

[6] III.9 Prop 8.6; J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2009

where π_v is the lifting of the Frobenius map ϕ_v, defined above, and $(\pi_v) = v$ from Section 2.3.2. We extend it by multiplicativity to all ideals of K (recall that, in our case, K is a principal ideal domain). So, for each ideal in K, we choose a generating element, i.e.

$$(\psi_E((\alpha))) = (\alpha)$$

For a general map ϕ to be a Grossencharacter, we require the existence of an integral ideal $\mathfrak{g} \subset \mathcal{O}_K$ such that ϕ is a group homomorphism from the group of fractional ideals of K which are coprime to $\mathfrak{g}$, to $\mathbb{C}^\times$. Furthermore, on those principal fractional ideals (α) such that $\mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(\mathfrak{g})$, we require it to be a continuous homomorphism.

We show that ψ_E satisfies this condition for a suitable choice of $\mathfrak{g}$ first by considering it as a map into $K^\times$, and then using the obvious embedding $K^\times \hookrightarrow \mathbb{C}^\times$.

Claim: *There exists some $\mathfrak{g}$ an integral ideal of K, with no $v \in S$ coprime to $\mathfrak{g}$, such that for all $\alpha \in K^\times$ with $ord_v(\alpha - 1) \geq ord_v(\mathfrak{g})$,*

$$\psi_E((\alpha)) = \alpha$$

Since $(\psi_E((\alpha))) = (\alpha)$, we have $\psi_E((\alpha)) = u_\alpha \alpha$. We must find some $\mathfrak{g}$ such that, for the α specified in the claim, $u_\alpha = 1$.

The above claim shows that ψ_E is a Grossencharater, since this map factors as $\alpha \mapsto (\alpha) \mapsto \alpha$, and is hence a continuous homomorphism because the identity map is a continuous homomorphism.

See Section 2.4.2 for a proof of the above claim. The proof uses an application of Artin's Reciprocity Law to the abelian field extension $K(E_l)/K$, obtained by adjoining the coordinates of the l-torion points on E to K, where l is some rational prime coprime to S.

2.4.1 The Frobenius Element

For notational brevity we denote $E[m]$ by E_m. For l some prime, we write E_{l^∞} for the group of points that are l^n-torsion for some n. The field extension $K(E_m)/K$ is that obtained by adjoining the coordinates of the points in E_m.

Claim: *The field extension $K(E_l)/K$ is abelian.*

Proof: Section 2.2.3 says that $\rho_l(\mathrm{Gal}(\overline{K}/K))$ is abelian. This implies that $K(E_{l^\infty})/K$ is abelian. Since $K(E_l) \subset K(E_{l^\infty})$, we deduce that $K(E_l)/K$ is abelian. $\square$

Example: The field extensions for our Main Example

We give the two fields $\mathbb{Q}(E_2)$ and $\mathbb{Q}(E_4)$, and their corresponding Galois groups, where E is our main example curve:

$$y^2 + xy = x^3 - x^2 - 2x - 1$$

and we adjoin the coordinates of the points to $\mathbb{Q}$, because E is defined over $\mathbb{Q}$. We then show that these extensions are both abelian. We obtain

$$\mathbb{Q}(E_2) = \mathbb{Q}(\sqrt{-7}) = K \qquad \textit{and} \qquad \mathbb{Q}(E_4) = \mathbb{Q}(i, \sqrt[4]{-7}) = K(i, \sqrt[4]{-7})$$

We get corresponding Galois groups

$$Gal(\mathbb{Q}(E_2)/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \qquad \textit{and} \qquad Gal(\mathbb{Q}(E_4)/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$$

and observe that these two groups are both abelian.

Take v to be some prime of K unramified in $K(E_l)/K$. Recall that the *Frobenius element* of v is the Frobenius automorphism

$$\sigma_v := (v, K(E_l)/K) : x \mapsto x^{Nv} \quad \text{for all } x \in \mathcal{O}_{K(E_l)}/w\mathcal{O}_{K(E_l)}$$

where w is some prime of $K(E_l)$ above v, and is the identity map on $\mathcal{O}_K/v\mathcal{O}_K$. The fact that $\mathrm{Gal}(K(E_l)/K)$ is abelian means that its conjugacy classes are singleton elements. We may therefore think of σ_v as an element of $\mathrm{Gal}(K(E_l)/K)$.

Claim: *If $v \notin S' = S \cup \{w : w|l\}$, then indeed $K(E_l)/K$ is unramified at v*

Proof: Assume we have some $P \in E_l$ with $\tilde{P} = 0$ under reduction mod v. Then $P \in E_{p_v}$ where p_v is the prime in $\mathbb{Q}$ below $v \in K$. But $v \nmid l$ implies that $(l, p_v) = 1$. So, $up_v + tl = 1$ for some $u, t \in \mathbb{Z}$. Hence

$$P = (up_v + tl)(P) = u(p_v P) + t(lP) = u(0) + t(0) = 0$$

So reduction mod v is injective on E_l. Therefore, $K(E_l)/K$ is unramified at v. $\square$

For a general ideal $\mathfrak{a}$ coprime to S', we may define the *Artin Symbol*

$$\sigma_{\mathfrak{a}} = ((K(E_l)/K), \mathfrak{a})$$

to be the product of the maps σ_v, where v are the primes of K dividing $\mathfrak{a}$, counted with multiplicity.

Claim: *We have the equality $\psi_E(\mathfrak{a}) = \sigma_{\mathfrak{a}}$ as maps on E_l*

Proof: First we note that, as we saw earlier, both $\psi_E(\mathfrak{a})$ and $\sigma_{\mathfrak{a}}$ act on E_l, since they are endomorphisms of the curve, and this is true for all $\mathfrak{a}$. By multiplicativity, it suffices to prove that $\psi_E(v)(P) = \sigma_v(P)$ for all $P \in E_l$. Now,

$$\psi_E(v)(P) = \pi_v(P) \quad \Rightarrow \quad \widetilde{\psi_E(v)(P)} = \tilde{\pi}_v(\tilde{P}) = \phi_v(\tilde{P})$$

by definition of π_v as the lifting of the Frobenius map. Also, by definition,

$$\widetilde{\sigma_v(P)} = \phi_v(\tilde{P})$$

Hence

$$\widetilde{\sigma_v(P)} = \widetilde{\psi_E(v)(P)}$$

So, by the injectivity of reduction mod v on the points $P \in E_l$, we conclude that the claim holds. $\square$

2.4.2 Applying Artin's Reciprocity Law

Artin's Reciprocity Law says that there exists some $\mathfrak{g} \subset \mathcal{O}_K$ such that $\sigma_{(\alpha)} = 1$ when $\mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(\mathfrak{g})$ for all $v \in S'$. We can assume that $\mathfrak{g}$ is divisible by all primes in S' since this makes it easier for our conditions to be satisfied.

We use the equality of the maps $\sigma_{(\alpha)}$ and $\psi_E((\alpha))$ on E_l, for a particular choice of l, to show that $u_\alpha = 1$ for these α. We pick l coprime to the number of units (roots of unity) in K. Since $\psi_E((\alpha))(P) = \sigma_\alpha(P) = P$ for all $P \in E_l$, we have $(\psi_E((\alpha)) - 1)(P) = 0$ for all $P \in E_l$. As we saw before, this means that $\psi_E((\alpha)) - 1 = [l] \circ f$ for some $f \in \mathrm{End}_K(E)$. Hence

$$\psi_E((\alpha)) - 1 = 0 \mod l$$

Since $\psi_E((\alpha)) = u_\alpha \alpha$, we have $u_\alpha \alpha = 1 \bmod l$. All primes dividing l lie in S', hence divide $\mathfrak{g}$, so $\mathrm{ord}_v(\alpha - 1) = \mathrm{ord}_v(\mathfrak{g})$ for all $v \in S'$ implies that $\alpha = 1 \bmod l$. So $u_\alpha = 1 \bmod l$ and our choice of l ensure that this forces $u_\alpha = 1$.

This concludes the proof that ψ_E is a Grossencharacter on $K^\times$.

2.5 Expressing the L-function as a Product of Hecke L-functions

We define the L-function of ψ_E to be:

$$L(\psi_E, s) = \prod_{v \text{ unramified}} \left(1 - \frac{\psi_E(v)}{(Nv)^s}\right)^{-1}$$

where we define below what it means for ψ_E to be unramified at v. We aim to give an outline for why $L(E/K, s) = L(\psi_E, s)L(\psi_E^*, s)$, where ψ_E^* is defined by

$$\psi_E^*(x) = \overline{\psi_E(x)}$$

We re-cast our earlier construction of the Grossencharacter in terms of ideles. The idele group of K is:

$$I_K = \{(x_v)_v \in \prod_{v \in \Sigma_K} K_v^* : |x_v| = 1 \text{ for all but finitely many } v\}$$

Considering things in terms of ideles tidies our notation because they are efficient at recording and comparing information simaltaneously about behaviour at the different places v (for example, the order of vanishing of some element at v).

We have a unique continuous map on I_K which agrees with ψ_E on $K^\times$ (or rather, the image of the elements of $K^\times$ in I_K). We "normalise this map at ∞" to ensure that it is identically 1 upon $K^\times$, and compose with an embedding of the target space into $\mathbb{C}^\times$. This yields our Grossencharacter, once again denoted ψ_E.

Define the L-function of ψ_E as above where $v \in \Sigma_K$ is said to be *unramified* if

$$\psi_E(u) = 1 \text{ for all } u \in \mathcal{O}_{K_v} \text{ with } u \text{ a unit}$$

In fact, using Class Field Theory and the Néron-Ogg-Shafarevich Criterion we show that the map ψ_E is unramified at v just when E has good reduction at v. So encouragingly the product formulae for the complex L-function, and that for the two Hecke L-functions, are taken over the same places $v \in \Sigma_K$.

It remains to show that we have agreement of the L-functions at all unramified places v, that is

$$(1 - (\pi_v + \overline{\pi}_v)(Nv)^{-s} + (Nv)^{1-2s}) = \left(1 - \frac{\psi_E(v)}{(Nv)^s}\right)\left(1 - \frac{\psi_E^*(v)}{(Nv)^s}\right)$$

Just as in Section 2.3.2, we have

$$\pi_v \overline{\pi_v} = N_{K/\mathbb{Q}}(\pi_v) = Nv$$

and we can very similarly prove the trace formula

$$\pi_v + \overline{\pi_v} = \mathrm{Tr}_{K/\mathbb{Q}}(\pi_v) = Nv + 1 - \#(\tilde{E}_v(k_v))$$

These formulae allow us to show the agreement of the required factors of the L-functions at each unramified place v.

2.6 The Analytic Continuation of the Complex L-function

By the results of Section 2.5, to show the analytic continuation of $L(E/K, s)$ it suffices to show the analytic continuation of $L(\psi_E, s)$. From this, the analytic continuation of ψ_E^* follows directly. We give an outline for showing analytic continuation using Eisenstein-Kronecker Series.

Given some Hecke character χ, define the *conductor* of χ as follows: it is the largest ideal $\mathfrak{f}$ such that χ acts trivially upon $1 + \mathfrak{f}\mathcal{O}_K$.

Define the character ψ_E^n by

$$\psi_E^n(v) = (\psi_E(v))^n$$

and denote the conductor of ψ_E^n by $\mathfrak{f}_n$, where $\mathfrak{f} := \mathfrak{f}_1$. Since K has class number 1, $\mathfrak{f} = (f)$ for some $f \in \mathcal{O}_K$.

Note that $\mathfrak{f} \subset \mathfrak{f}_n$ for all n, since $\psi_E(1+x) = 1 \implies \psi_E(1+x)^n = 1$. However,

$$(\psi_E(1+x))^n = 1 \quad \not\Rightarrow \psi_E(1+x) = 1$$

so we may have $\mathfrak{f}_n$ a proper divisor of $\mathfrak{f}$.

Define the L-function $L_{\mathfrak{f}}(\psi_E^n, s)$ by taking a product over those v coprime to $\mathfrak{f}$. Note that we are missing those factors from $L(\psi_E^n, s)$ corresponding to places v coprime to $\mathfrak{f}_n$ which are not coprime to $\mathfrak{f}$. This makes $L_{\mathfrak{f}}$ imprimitive.

Our next stage is to consider the following function used by Kronecker:

$$H_k(z, s, L) = \sum_{w \in L \setminus \{-z\}} \frac{(\overline{z} + \overline{w})^k}{|z + w|^{2s}}$$

where L is some lattice in $\mathbb{C}$, and we state the result that $\Gamma(s)H_k(z,s,L)$ has holomorphic continuation and functional equation. Take L to be the period lattice of E. Using our expression for $L_{\mathfrak{f}}$, we get a formula for $L(\psi_E^n, s)$ as a sum of H_n functions. When $n \geq 3$, H_n converges and we conclude that we have analytic continuation.

It remains to show analytic continuation in the important cases $n = 1, 2$, for which $H_n(z, n, L)$ does not converge. For this, we introduce the functions $\mathcal{E}_n^*(z, L)$, for $n = 1$ and 2, expressed in terms of lattice invariants, the ζ-function and the Weierstrass $\mathcal{P}$-function. For more details on this, see the $\mathfrak{p}$-adic theory in Chapter 3.

The functional equation of the L-function relates its value at s to that at $2 - s$. It is most simply stated in terms of the function $\Lambda(E, s)$ which is defined by

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

where $c(E)$ denotes the conductor of E. The functional equation of the L-function may then be written as

$$\Lambda(E, s) = w_E\Lambda(E, 2 - s)$$

where w_E is some constant which takes the value 1 or -1.

In Chapter 3, we will study the interpolation property which relates our complex L-function to the $\mathfrak{p}$-adic L-function. The constants which relate the two L-functions in the interpolation property arise naturally from the above functional equation.

2.7 Special Values of the L-function

We require the special values

$$L_{\mathfrak{f}}(\psi_E^n, n)$$

to prove the existence of the p-adic L-functions in Chapter 3. For this, we make use of the analytic continuation and functional equation of H_k defined in Section 2.6.

Note that

$$\left(1 - \frac{\psi_E(v)}{(Nv)}^n\right)^{-1} \neq 0 \qquad \text{for } n \geq 1$$

For $n \geq 3$, the Euler product for $L_{\mathfrak{f}}(\psi_E^n, s)$ converges absolutely, so

$$L_{\mathfrak{f}}(\psi_E^n, n) = \prod_v \left(1 - \frac{\psi_E(v)}{(Nv)}^n\right)^{-1}$$

Hence we conclude that $L_{\mathfrak{f}}(\psi_E^n, n) \neq 0$, since none of the factors are 0.

We obtain an expression for $L_{\mathfrak{f}}(\psi_E^n, n)$, when $n \geq 3$, in terms of the field extension $K(E_f)/K$ (where $(f) = \mathfrak{f}$) and the value $\Omega_\infty \in L$ which is the period of the invariant differential, i.e. Ω_∞ satisfies the equation

$$\Omega_\infty \mathcal{O}_K = L$$

In particular, we now have the result

$$\Omega_\infty^{-n} L_\mathfrak{f}(\psi_E^n, n) \in K$$

It is much harder to show that the same results holds for $n = 1, 2$, because we do not have the convergence of $H_n(z, n, L)$. We require the introduction of the rational function

$$r_\lambda(P) = \prod_{V \in E_\lambda^*/\pm 1} (x(P) - x(V))^{-1}$$

where E_λ^* is the set of non-zero λ-torsion points, and $\lambda \in \mathcal{O}_K$ is not divisible by 2 or 3. We will see more of this function in Section 3.6.1. We also make use of the Weierstrass $\mathcal{P}$-function, and a function θ chosen such that

$$\frac{\theta^2(z, L)^{N\lambda}}{\theta^2(z, \lambda^{-1}L)}$$

is an elliptic function with respect to the lattice L (i.e. is meromorphic and periodic with respect to L).

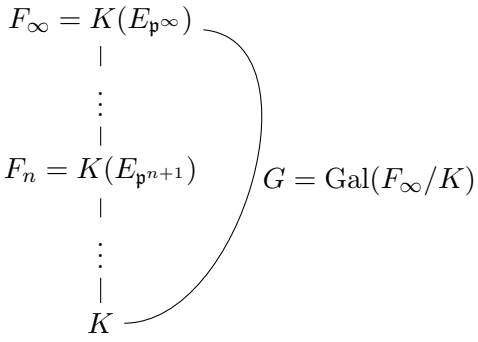
3 Construction of the p-adic L-functions

Take p some prime, with $p > 2$ and $p = \mathfrak{p}\mathfrak{p}^*$ the prime factorisation of p in K, with $\mathfrak{p} \neq \mathfrak{p}^*$ and E having good reduction at $\mathfrak{p}$ (so $\mathfrak{p}$ does not divide the conductor of E). Recall that we write

$$E_{\mathfrak{p}^\infty} = \{P \in E(\overline{K}) : \mathfrak{p}^n P = 0 \text{ for some } n\}$$

where K having class number 1 means that $\mathfrak{p}^n$ is a principal ideal, say $\mathfrak{p}^n = (\alpha_n)$ where α_n is the canonical generating element. The map $\mathfrak{p}^n$ acts on $P \in E$ via the endomorphism α_n and we say that $\mathfrak{p}^n P = 0$ if $\alpha_n P = 0$.

We have the following set-up:



Note the comparison with the diagram of the fields and groups for the two-variable main conjecture in Section 1.4.1.

We seek a p-adic measure on G: a way of integrating functions from G to a p-adic target space. The main example of such a function that we are interested in is the character which gives the action of G on $E_{\mathfrak{p}^\infty}$. It is defined below in Section 3.1.

The construction of the p-adic L-functions echoes that of the p-adic analogue of the Riemann-Zeta function in the case of cyclotomic fields. In both cases, we relate the p-adic version to the non p-adic one via its evaluation at particular "special" integers. In the cyclotomic case, we evaluate at the even integers. In the case of the main conjecture for imaginary quadratic fields, our "special" integers are those congruent to $1 \mod p-1$.

In Chapter 4, we define the characteristic ideal of the module. The main conjecture gives a relationship between the characteristic ideal and the p-adic L-function. We use this relationship to prove results about the arithmetic properties of our elliptic curve.

3.1 A p-adic character

We wish to define the character $\chi_{\mathfrak{p}}$ of the representation obtained from the action of G on $E_{\mathfrak{p}^\infty}$.

1. **Define the action of G on $E_{\mathfrak{p}^\infty}$. We denote the representation by $\rho_{\mathfrak{p}}$**

   The group G acts on $E_{\mathfrak{p}^n}$ for all n since $g \in G$, $P \in E_{\mathfrak{p}^n}$ implies that

   $$\mathfrak{p}^n(g(P)) = g(\mathfrak{p}^n P) = g(0) = 0$$

   where the first inequality holds because $g|_K = \mathrm{id}|_K$ so g commutes with all automorphisms defined over K. So G acts on $\mathrm{Aut}_{\mathcal{O}_{\mathfrak{p}}}(E_{\mathfrak{p}^\infty})$, i.e. we have a map:

   $$\rho_{\mathfrak{p}} : G \hookrightarrow \mathrm{Aut}_{\mathcal{O}_{\mathfrak{p}}}(E_{\mathfrak{p}^\infty})$$

2. **Define the embedding, $i_{\mathfrak{p}} : K \hookrightarrow \mathbb{Q}_p$, and define $\mathcal{O}_{\mathfrak{p}} := i_{\mathfrak{p}}(\mathcal{O}_K)$**

   The field K is imaginary quadratic, say $K = \mathbb{Q}(\sqrt{-d})$ for d some positive integer. Let $\alpha = \sqrt{-d}$; $g = X^2 + d$ is its minimal polynomial. Since $p > 2$, and $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ or 2, the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ is coprime to p, and we may use Dedekind's Criterion:

   $$(p) = \mathfrak{p}\mathfrak{p}^* \text{ in } K \quad \Leftrightarrow \quad \overline{g} = \phi\phi^*$$

   where $\overline{g} = g \mod p$. We get two roots of $g \mod p$: denote by $v, v^* \in \mathbb{F}_p$ the roots of ϕ, ϕ^* respectively. Since $\phi(v) = 1 \neq 0$, we apply Hensel's Lemma to show there exists $u \in \mathbb{Q}_p$ such that $\phi(u) = 0$.

   Claim: *We have an embedding $i_p : K \hookrightarrow \mathbb{Q}_p$*

   Proof: Each element of K may be written in the form $a + b\alpha$ where $a, b \in \mathbb{Q}$. Define i_p by

   $$i_{\mathfrak{p}}(a + b\alpha) = a + bu$$

where $u \in \mathbb{Q}_p$ is as above. This maps all of K into $\mathbb{Q}_p$ since $a + bu \in \mathbb{Q}_p$ for all $a, b \in \mathbb{Q}$, and is an embedding since $u \notin \mathbb{Q}$, so we have no linear combination $a + bu = 0$. $\square$

Consider the image of $\mathcal{O}_K$ under this map. It is a subgroup of $\mathbb{Q}_p$ and, since $i_\mathfrak{p}|_\mathbb{Q} = \mathrm{id}|_\mathbb{Q}$, algebraic integers in K are mapped to algebraic integers in $\mathbb{Q}_p$, i.e. $\mathcal{O}_\mathfrak{p} := i_\mathfrak{p}(\mathcal{O}_K) \subset \mathbb{Z}_p$. Since $\mathcal{O}_p \subset \mathbb{Z}_p$, we have

$$\mathcal{O}_\mathfrak{p}^\times \subset \mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p$$

3. **Show that $\rho_\mathfrak{p}$ is 1-dimensional over $\mathcal{O}_\mathfrak{p}$**

   Claim: *The group* $Aut_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty}) \approxeq \mathcal{O}_\mathfrak{p}^\times \approxeq \mathbb{Z}_p^\times$

   Take some $\alpha \in \mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty})$. It maps $E_{\mathfrak{p}^n}$ to itself for all n, since it is a homomorphism and is the identity map on 0. The multiplication by p^n map, $[p^n]$, has degree p^{2n} and factors as conjugate maps

   $$[p^n] = [p]^n = \mathfrak{p}^n \mathfrak{p}^{*n}$$

   So, $\mathfrak{p}^n$ has degree p^n, and $\#E_{\mathfrak{p}^n} = p^n$. We have $p^{n-1}(p-1)$ principal $\mathfrak{p}^n$-torsion points, and mapping one to the other commutes with action by an element of $\mathcal{O}_\mathfrak{p}$. If α maps a principal $\mathfrak{p}^n$-torsion point to a non-principal $\mathfrak{p}^n$-torsion points, then $E_\mathfrak{p} \subset \ker(\alpha)$. This contradicts α being an automorphism.

   Hence, $\mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^n}) = \mathrm{Aut}(\mathbb{F}_{p^n}) = (\mathbb{Z}/p^n\mathbb{Z})^\times$. Taking the inverse limit, we see that $\mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty}) = \mathbb{Z}_p^\times$.

   So $\mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty})$ is 1-dimensional, hence our automorphisms act by multiplication by an element of $\mathcal{O}_\mathfrak{p}$. Clearly $\mathcal{O}_\mathfrak{p}^\times \subset \mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty})$, and 0 is not an automorphism, so $\mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty}) = \mathcal{O}_\mathfrak{p}^\times$.

4. **Define the character $\chi_\mathfrak{p}$**

   Take $x \in \mathcal{O}_\mathfrak{p}$ and $g \in G$. The 1-dimensionality of $\rho_\mathfrak{p}$ means $\sigma(x)$ is multiplication of x by some element in $\mathcal{O}_\mathfrak{p}$. Let $\chi_\mathfrak{p}$ denote the character of the representation: σ acts on x by multiplication by $\chi(\sigma) \in \mathcal{O}_\mathfrak{p}$. So we have

   $$\chi_\mathfrak{p} : G \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(E_{\mathfrak{p}^\infty}) = \mathcal{O}_\mathfrak{p}^\times = \mathbb{Z}_p^\times$$

From now on, we will refer to the group G interchangeably as G and $\mathbb{Z}_p^\times$ where we implicitly make use of the isomorphism above. Note that we can decompose elements of $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p$ and we do so as follows:

First we show that the only roots of unity in $\mathbb{Z}_p^\times$ are μ_{p-1}. The following equation holds in $\mathbb{F}_p$:

$$T^{p-1} - 1 = (T-1)...(T-(p-1)) \mod p$$

The derivative of $T^{p-1} - 1$ is non-zero at every $T \neq 0$. Hensel's lemma can therefore be applied to show that $\mathbb{Z}_p$ contains all the $(p-1)$th roots of unity, which all clearly

lie in $\mathbb{Z}_p^\times$. There are no further roots of unity, since these would satisfy an equation mod p in the residue field $\mathbb{F}_p$.

Consider the value of $x \in \mathbb{Z}_p^\times$ mod p. It must be a unit in $\mathbb{F}_p$. Once again, by lifting to $\mathbb{Z}_p$ we see that $x = u(1 + py)$ where y is some element of $\mathbb{Z}_p$ and u is a root of unity in $\mathbb{Z}_p^\times$. Hence

$$\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$$

The ring $\mathcal{I}$ is defined as follows: consider the maximal unramified field extension of $\mathbb{Q}_p$ which we denote by $\mathbb{Q}^{\mathrm{nr}}$:

$$\mathbb{Q}^{\mathrm{nr}} = \mathbb{Q}_p \left(\bigcup_{(n,p)=1} \mu_n \right)$$

Consider its completion with respect to the p-adic metric, and then take $\mathcal{I}$ to be those elements whose p-adic valuation is positive, i.e. the ring of integers.

We now have a map from G to a p-adic space. The remainder of Chapter 3 will be spent outlining a construction for a pseudo-measure on G, obtained by taking the primitive branch of a measure on G, which satisfies certain properties involving the evaluation of our original L-function at particular integers. This is our analogue of the p-adic Riemann-Zeta function as applied to a general L-function.

3.2 The Iwasawa Algebra

The Iwasawa algebra is the main definition that we make use of in our construction. It is defined to be

$$\Lambda_{\mathcal{I}}(G) = \varprojlim_U \mathcal{I}[G/U]$$

where we take the inverse limit over open subgroups of G.

Claim: *The group G/U is finite*

Proof: I will prove the claim in the special case $G = \mathbb{Z}_p$ or $G = \mathbb{Z}_p^\times$. These are the groups whose Iwasawa Algebras we will make use of.

Elements of G are of the form

$$x = \pm \sum_{i=0}^{\infty} a_i p^i \qquad a_i \in \{0, ..., p-1\}$$

Since $U \neq \emptyset$, we can take some $y \in U$. The openness of U implies that there is some $N_y \in \mathbb{N}$ such that, if the first N_y terms of the above expression for y vanish, i.e. if

$$y' - y = \pm \sum_{i=Ny+1}^{\infty} a_i p^i$$

then $y' \in U$. Consider the finite set

$$Z = \left\{ z \in G : z = y + \sum_{i=0}^{Ny} b_i p^i \text{ for some } b_i \in \{0, ..., p-1\} \right\}$$

Then $\#Z \leq (p-1)^{Ny}$ and, in particular, Z is finite. We aim to show that, for all $x' \in G$, there exists some $z \in Z$ such that $z - x \in U$.

Take x such that $x = \sum_{i=0}^{\infty} a_i p^i$. Let $z = y + \sum_{i=0}^{Ny} a_i p^i$. Then

$$(z - x) - y = \sum_{i=Ny+1}^{\infty} (-a_i) p^i$$

So we see that $x - z$ is of the form of y', above. From this, we deduce that

$$G/U \subset \{z + U : z \in Z\}$$

and hence G/U is finite. $\square$

The group $\mathcal{I}[G/U]$ is defined to be the ring of elements that are a sum $\sum k_i x_i$, where $x_i \in G/U$, $k_i \in \mathcal{I}$.

Claim: *The Iwasawa algebra $\Lambda_{\mathcal{I}}(G)$ is an $\mathcal{I}$-algebra*

Proof: Each projective component $\mathcal{I}[G/U]$ is an $\mathcal{I}$-algebra: it is a ring by definition we can map $\mathcal{I} \to \mathcal{I}[G/U]$ by taking $\mu \mapsto \mu x$ for some $x \in G/U$. $\square$

Later (in Section 3.5) we see that $\Lambda_{\mathcal{I}}(\mathbb{Z}_p) \cong \mathcal{I}[[W]]$, the ring of formal power series in W with coefficients in $\mathcal{I}$. We are interested in $\Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times)$, which is more difficult to get a handle on. We will also define the set of $\mathcal{I}$-valued measures on G and show (in Section 3.4) that the Iwasawa algebra of G is isomorphic to this set.

3.3 Some p-adic Measure Theory

Denote the set of continuous functions $G \to \mathbb{C}_p$ by $C(G, \mathbb{C}_p)$.

We will use both $\mathcal{I}$-valued measures and $\mathcal{I}$-valued pseudo-measures. An $\mathcal{I}$-valued measure is defined as follows:

An $\mathcal{I}$-valued measure on G is a continuous map, L, which assigns a p-adic value (in $\mathcal{I}$) to $f \in C(G, \mathbb{C}_p)$. An example of a p-adic function on G is our character $\chi_{\mathfrak{p}} : G \to \mathbb{Z}_p^\times \subset \mathbb{Q}_p$ defined in Section 3.1. Then L assigns a p-adic size to it that lies in $\mathcal{I}$. We require that

$$|L(f)|_p \leq ||f|| \quad \text{for all } f \in C(G, \mathbb{C}_p)$$

The functional, L, is of the form

$$L(f) = \int_G f d\mu$$

where μ is some element of $\Lambda_{\mathcal{I}}(G)$. We will also refer to the measure L by μ.

A pseudo-measure is a generalisation of a measure which allows μ to take certain values in $\mathrm{Frac}(\Lambda_{\mathcal{I}}(G))$ whose denominators are non-trivial. We may apply our pseudo-measure to non-trivial multiplicative homomorphisms $f : G \to \mathbb{C}_p^\times$, but not to all continuous functions. This is a sacrifice we are willing to make! We require that $(g-1)\mu \in \Lambda_I(G)$ for all $g \in G$, and define:

$$\int_G f d\mu = \frac{\int_G f d((g-1)\mu)}{f(g)-1}$$

where g is some element of G such that $f(g) \neq 1$, and $(g-1)\mu \in \Lambda_{\mathcal{I}}(G)$ means that the numerator takes the form of a p-adic measure. Since f is non-trivial, there exists some $g \in G$ with $f(g) \neq 1$.

Claim: *The definition above is well defined: subject to choosing some g such that $f(g) \neq 1$, the expression above is independent of g*

Proof: The map $f : G \to \mathbb{C}_p^\times$ is a homomorphism. It induces a map on $\Lambda_{\mathcal{I}}(G)$. $\square$

We now return to our measures; we denote the set of all $\mathcal{I}$-valued measures by $M_{\mathcal{I}}(G)$. We prove a couple of preliminary results about the group of measures $M_{\mathcal{I}}(G)$ and about the structure of a p-adic continuous function on G. These allow us to work towards one of our main results which relates the Iwasawa algebra, $\Lambda_{\mathcal{I}}(G)$, to the group $M_{\mathcal{I}}(G)$.

Claim: *The set $M_{\mathcal{I}}(G)$ is an $\mathcal{I}$-module*

Proof: Consider a set of functions which span $C(G, \mathbb{C}_p)$ over $\mathcal{I}$

$$< f_i : i \in I >= C(G, \mathbb{C}_p)$$

Consider those measures L_i associated to each f_i such that L_i is 1 on $< f_i >$ and 0 elsewhere. Then all other modules are expressible as a sum of some L_i with coefficients in $\mathcal{I}$. $\square$

Every function $f \in C(G, \mathbb{C}_p)$ is a limit of locally constant functions.

Claim: *A locally constant element of $C(G, \mathbb{C}_p)$ factors through G/U for some open $U \leq G$.*

Proof: A locally constant function is one that is contant upon an open set around each point. Say our function is constant on the open ball around x of radius ϵ_x, denoted $B_x(\epsilon_x)$ for all $x \in G$. From the compactness of G, we can take

$$\min\{\epsilon_x : x \in G\} > 0$$

It is then clear that f factors through G/U where $U = B_y(\epsilon)$ for some $y \in G$. $\square$

Big Claim: *We have an isomorphism $c : \Lambda_{\mathcal{I}}(G) \to M_{\mathcal{I}}(G)$, i.e. elements of the Iwasawa algebra correspond to measures on G.*

I will give a proof which aims to highlight why this correspondence is a natural one, sacrificing brevity for added motivation.

Step 1: Construct the map from $\Lambda_{\mathcal{I}}(G) \to M_{\mathcal{I}}(G)$

Given some $\mu \in \Lambda_{\mathcal{I}}(G)$, we seek a corresponding measure, denoted $c(\mu)$. To get a p-adic value of a function $f \in C(G, \mathbb{C}_p)$, the most direct way is to evaluate it at some $g \in G$.

We start off by taking a simple example of some $\mu \in \Lambda_{\mathcal{I}}(G)$: take μ whose projections $\Lambda_{\mathcal{I}}(G) \to \mathcal{I}[G/U]$ are given by $\overline{g}$, the image of g in G/U, for all U. We aim to construct c such that

$$c(\mu)(f) = f(g)$$

for this $g \in G$. To do so, we make use of the above claim which shows that f is the limit of functions which factor through G/U for some open U. Assume that f itself actually factors through G/U. Then, for this U,

$$f(\overline{g}) = f(g)$$

If f is not itself locally constant, we can take the limit of such functions.

Now extend by linearity (with coefficients in $\mathcal{I}$) to all μ, not just those of the above form. General μ have projections of the form

$$\sum_{x \in G/U} a_x x \qquad \text{for some } a_x \in \mathcal{I}$$

We require that the coefficients obtained in our projections be independent of U. By definition of the inverse limit, the projections of μ in $\mathcal{I}[G/U]$ are all compatible (in the precise sense given by the inverse limit). In particular, the coefficients are independent of U. For all U_i such that f factors through G/U_i, the coefficients are the same.

To show that we have $c(\mu) \in M_{\mathcal{I}}(G)$, we require that all the conditions satisfied for an $\mathcal{I}$-valued measure hold. These conditions are all clear, except for showing that $|c(\mu)(f)|_p \leq ||f||$ for all f. This follows from the fact that our coefficients a_x lie in the ring of integers, i.e. have p-adic valuation $|a_x|_p \leq 1$. We now make use of the strong triangle inequality to see that

$$|c(\mu)(f)|_p \leq \max_{\substack{U \subset G \text{ open} \\ x \in G/U}} |f(x)|_p \leq ||f||$$

This concludes the first step.

Step 2: Construct the inverse map

Take some $L \in M_{\mathcal{I}}(G)$. We wish to construct a corresponding element $\mu \in \Lambda_{\mathcal{I}}(G)$. This requires the construction of compatible elements of $\mathcal{I}[G/U]$ for all U open subgroups of G.

Our set $M_{\mathcal{I}}(G)$ is spanned by those measures which simply evaluate some $f \in C(G, \mathbb{C}_p)$ at a particular point of G. In general, we assess how similar our measure L is to one which "evaluates at x" by evaluating L at a function

$$f_{x,U} = \begin{cases} 1 & \text{for } x \in U \\ 0 & \text{for } x \in G \backslash U \end{cases}$$

where U is some small open neighbourhood of x.

Taking the inverse limit of $L(f_{x,U})$ as U varies across all open subsets of G, we get the behaviour of L "at x". So, $L(f_{x,U})$ is the natural coefficient that $\overline{x}$ should have in $\mathcal{I}[G/U]$, where $\overline{x}$ is the image of x in G/U. These coefficients are compatible in the sense of the inverse limit. So, we define μ to have projections onto $\mathcal{I}[G/U]$ equal to:

$$\sum_{x \in G/U} L(f_{x,U})x$$

we conclude the proof of the existence of the inverse map.

These maps are mutually inverse since, for $L = c(\mu)$,

$$L(f_{x,U}) = c(\mu)(f_{x,U}) = a_x$$

where a_x is the coefficient of x in the projection of μ onto $\mathcal{I}[G/U]$. For the converse, it suffices to see that (as explained above) the action of L on the functions $f \in C(G, \mathbb{C}_p)$ is characterised by its action upon those functions of the form $f_{x,U}$, i.e.

$$\sum_{x \in G/U} L(f_{x,U}) f(x) = L(f)$$

This concludes the construction of our isomorphism. $\square$

3.4 Finding a Canonical Element of the Iwasawa Algebra

We want to construct the Iwasawa algebra of our main Galois group

$$G = \mathrm{Gal}(F_\infty / K)$$

Since $G \approxeq \mathbb{Z}_p^\times$, we wish to construct the $\mathcal{I}$-algebra $\Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times)$. We will do so by considering $\Lambda_{\mathcal{I}}(\mathbb{Z}_p)$, which is much easier to study, and then we will characterise $\Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times)$ as a subgroup of it. In fact, we show that $\Lambda_{\mathcal{I}}(\mathbb{Z}_p)$ is isomorphic to $\mathcal{I}[[W]]$. Then we consider $\Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times)$ as a subset of $\Lambda_{\mathcal{I}}(\mathbb{Z}_p)$ and find the subset of $\mathcal{I}[[W]]$ corresponding to $\Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times)$.

3.4.1 From an Iwasawa Algebra to Formal Power Series

Our first step is to show that we have an isomorphism:

$$\Lambda_{\mathcal{I}}(\mathbb{Z}_p) \xrightarrow{\sim} \mathcal{I}[[W]]$$

where, once again, $\mathcal{I}[[W]]$ denotes the ring of formal power series in W whose coefficients lie in $\mathcal{I}$. We use Mahler's theorem which characterises elements of $C(G, \mathbb{C}_p)$ when $G = \mathbb{Z}_p$.

Consider the functions $f_n : \mathbb{Z}_p \to \mathbb{C}_p$, with $f_n(x) = \binom{x}{n}$. Mahler's theorem says that any element of $C(\mathbb{Z}_p, \mathbb{C}_p)$ can be written as a linear combination of f_n with coefficients in $\mathbb{C}_p$. This can be proven using generating functions.

Claim: *We have an isomorphism from* $\Lambda_{\mathcal{I}}(\mathbb{Z}_p) \to \mathcal{I}[[W]]$

Proof: Consider the measure $c(\mu)$ associated to $\mu \in \Lambda_{\mathcal{I}}(G)$ under the ismorphism "c" from Section 3.4. By Mahler's theorem, the measure $c(\mu)$ on $C(\mathbb{Z}_p, \mathbb{C}_p)$ is determined by $c(\mu)(\binom{x}{n})$. So, it is natural to think of these as the nth coefficients of $c(\mu)$. Furthermore, $c(\mu)(\binom{x}{n})$ lie in $\mathcal{I}$ because $\binom{n}{x}$ lies in the ring of integers of $\mathbb{C}_p$. So, the map

$$\mu \mapsto \sum_{n=0}^{\infty} c(\mu)\left(\binom{x}{n}\right) W^n$$

is a map from $\Lambda_{\mathcal{I}}(G) \to \mathcal{I}[[W]]$.

Conversely, given some elements $c_n \in \mathcal{I}$, we wish to construct a measure $c(\mu) \in M_{\mathcal{I}}(\mathbb{Z}_p)$. This follows directly: for some function $f \in C(\mathbb{Z}_p, \mathbb{C}_p)$, $f = \sum a_n \binom{x}{n}$, we let

$$c(\mu)(f) = \sum a_n c_n$$

This concludes the existence of our isomorphism. $\square$

3.4.2 From our Iwasawa Algebra to Formal Power Series

We will now refer to a measure $L = c(\mu)$ by its corresponding element, μ, of the Iwasawa algebra. Given some measure, $\mu \in \Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times)$, we define the associated measure $\iota(\mu) \in \Lambda_{\mathcal{I}}(\mathbb{Z}_p)$ by:

$$\iota(\mu)(f) = \mu(f|_{\mathbb{Z}_p^\times})$$

where f is some element of $C(\mathbb{Z}_p, \mathbb{C}_p)$. To show that

$$\iota : \Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times) \to \Lambda_{\mathcal{I}}(\mathbb{Z}_p)$$

is an injective map, we use the property that the zero-measure $0 \in \Lambda_{\mathcal{I}}(\mathbb{Z}_p)$ is the only one which satisfies $0(f) = 0$ for all $f \in C(\mathbb{Z}_p, \mathbb{C}_p)$ and we require that

$$\mu(f|_{\mathbb{Z}_p^\times}) = 0 \text{ for all } f \implies \mu = 0$$

That is, we must prove that in order to show that the evaluation of the measure is 0 at all continuous functions on $\mathbb{Z}_p^\times$, it suffices to consider those which are restrictions of continuous functions on $\mathbb{Z}_p$. In fact, we will show that all continuous functions on $\mathbb{Z}_p^\times$ arise as the restrictions of continous functions on $\mathbb{Z}_p$.

This follows from the fact that $\mathbb{Z}_p^\times$ is both open and closed in $\mathbb{Z}_p$: $\mathbb{Z}_p^\times = \mathbb{Z}_p \backslash p\mathbb{Z}_p$ and $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : v_p(x) \geq 1\} = \{x \in \mathbb{Z}_p : v_p(x) > 0\}$. Since valuation is a continuous property which admits a metric, this shows $p\mathbb{Z}_p$ to be both open and closed in $\mathbb{Z}_p$, from which it follows that its complement in $\mathbb{Z}_p$ is also both open and closed.

So, we can extend a continuous function on $\mathbb{Z}_p^\times$ to one on $\mathbb{Z}_p$ by setting it to be 0 on $\mathbb{Z}_p \backslash \mathbb{Z}_p^\times = p\mathbb{Z}_p$.

We have therefore embedded $\Lambda_{\mathcal{I}}(G) = \Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times) \hookrightarrow \Lambda_{\mathcal{I}}(\mathbb{Z}_p)$. We seek to characterise those elements of $\Lambda_{\mathcal{I}}(\mathbb{Z}_p)$ which come from something in $\Lambda_{\mathcal{I}}(G)$.

For some $\eta \in \Lambda_{\mathcal{I}}(\mathbb{Z}_p)$, $f \in C(\mathbb{Z}_p, \mathbb{C}_p)$, we have

$$\eta(f) = \eta(f|_{\mathbb{Z}_p^\times}) + \eta(f|_{p\mathbb{Z}_p})$$

by linearity of a measure. If $\eta = \iota(\mu)$ for some $\mu \in \Lambda_{\mathcal{I}}(G)$, then

$$\eta(f) = \iota(\mu)(f) = \mu(f|_{\mathbb{Z}_p^\times})$$

We wish to relate this to a more tangible condition involving the power series ring, $\mathcal{I}[[W]]$, and thus to find the subset of $\mathcal{I}[[W]]$ that corresponds to elements of $\Lambda_{\mathcal{I}}(G)$. Let g also denote the image of $\mu \in \Lambda_{\mathcal{I}}(\mathbb{Z}_p)$ under the isomorphism taking it to the ring of formal power series $\mathcal{I}[[W]]$.

Claim: *The elements of μ coming from $\Lambda_{\mathcal{I}}(\mathbb{Z}_p^\times)$ are those whose images in $\mathcal{I}[[W]]$ satisfy:*

$$\sum_{\zeta \in \mu_p} g(\zeta(1+W) - 1) = 0$$

The proof uses the usual open sets $x + p^n\mathbb{Z}_p$, as x and n vary, and is elementary, save for an application of the Weierstrass Preparation Theorem. This says that, given some $f \in \mathcal{I}[[W]]$ whose nth coefficient is a unit, we can express f as the product of an n-degree polynomial, and an element of $\mathcal{I}[[W]]^\times$.

3.5 The Existence of our Pseudo-Measure

We now follow a recipe to find some particular $g \in \mathcal{I}[[W]]$ which satisfies the above equation. This is the canonical element of the Iwasawa algebra $\Lambda_{\mathcal{I}}(G)$ whose properties underlie the main conjectures of Iwasawa theory.

3.5.1 The Canonical Rational Function

Recall that in Section 2.7 we introduced the following function to find special values of the L-function of the Grossencharacter ψ_E^n in the cases $n = 1, 2$:

$$r_\lambda(P) = \prod_{V \in E_\lambda^*/\pm 1} (x(P) - x(V))^{-1}$$

where $\lambda \in \mathcal{O}_K$ is some endomorphism not divisible by 2 or 3. Recall that the invariance of this function under action by an element of $\mathrm{Gal}(K(E_\lambda)/K)$ means, by Galois theory, that $r_\lambda(P) \in K(E)$, i.e. it is some rational function on E with coefficients in K.

Our general aim is to define a related function, denoted $\mathcal{R}_\lambda(P)$, and to consider its expansion in terms of power series. We will obtain a function with very nearly the property that we require of g, above.

Step 1: The Normalising Constant $c_E(\lambda)$

Consider $r_\lambda(\alpha(P))$ where r_λ is the function above and $\alpha \in \mathcal{O}_K$ is some non-zero endomorphism coprime to λ. We begin by comparing the two functions:

$$r_\lambda(\alpha(P)) \qquad \text{and} \qquad \prod_{U \in E_\alpha} r_\lambda(P \oplus U)$$

Now, $r_\lambda(\alpha(P))$ has a pole of order 1 whenever P is such that $\alpha(P) = \pm V$ for some $V \in E_\lambda^*/\pm 1$. Given some $R \in E$ such that $\alpha(\pm R) = \pm V$, for fixed $V \in E_\lambda^*/\pm 1$, the other R' with $\alpha(R') = \pm V$ are given by $\pm R \oplus U$ where $U \in E_\alpha$.

The function $r_\lambda(P \oplus U)$ has a pole whenever $P \oplus U = \pm V$ where $V \in E_\lambda^*/\pm 1$. This implies that

$$\alpha(P \oplus U) = \pm\alpha(V) \implies \alpha(P) \oplus \alpha(U) = \alpha(P) \oplus O_E = \alpha(P) = \pm\alpha(V)$$

Since $(\alpha, \lambda) = 1$, applying α permutes the elements of $E_\lambda^*/\pm$. Taking the product over all $U \in E_\alpha$, we see that there are poles of $\prod_{U \in E_\alpha} r_\lambda(P \oplus U)$ just when there are poles of $r_\lambda(\alpha(P))$.

There are visibly no roots of these two equations, so they can only differ by a constant.

In fact, we can show that the constant is $c_E(\lambda)^{N\alpha - 1}$ where c_E depends only on the elliptic curve, E, and we can further express c_E as a function

$$c_E : \mathcal{O}_K \to K(E)$$

$$\lambda \mapsto \frac{\Delta(E)^{N\lambda - 1}}{\lambda^{12}}$$

We define a new function $R_\lambda(P) = c_E(\lambda) r_\lambda(P)$. This is one step away from our final rational function.

Step 2: Defining the Rational Function $\mathcal{R}_\lambda$

Recall that Ω_∞ is the element of our period lattice such that $L = \Omega_\infty \mathcal{O}_K$. Clearly, this equation remains true when we multiply Ω_∞ by a root of unity but, apart from this flexibility, Ω_∞ is unique. Recall also that we have an isomorphism

$$\mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C})$$

We obtain a primitive f-torsion point on E by taking the image of $\frac{\Omega_\infty}{f}$ under this map. Denote it by Q. Applying elements of the Galois group $\mathrm{Gal}(K(E_\mathfrak{f})/K)$ to Q, and recalling that $(f) = \mathfrak{f}$, we obtain the other primitive f-torsion points on E. We define

$$\mathcal{R}_\lambda(P) = \prod_{\tau \in \mathrm{Gal}(K(E_\mathfrak{f})/K)} R_\lambda(P \oplus Q^\tau)$$

It is clear that taking the product over all $\tau \in \mathrm{Gal}(K(E_\mathfrak{f})/K)$ means this function is invariant under the action of this group, thus once again by Galois theory we see that it is in $K(E)$.

In fact, we will see that $\mathcal{R}_\lambda$ is an Euler function on E, defined over K (see definition below) which will later be of great use to us. An Euler function, ρ, satisfies the following properties:

1. There exists some finite set of primes S, containing the primes of bad reduction on E, such that the function ρ has no zeroes or poles in

$$W_S = \bigcup_{(\alpha, S)=1} E_\alpha$$

2. For each $Q \in W_S$, the power series expansion of $\rho(P \oplus Q)$ in t has $\mathfrak{a}$-integral coefficients for every $\mathfrak{a}$ a prime of K with $(\mathfrak{a}, S) = 1$ and $\mathfrak{a}$ coprime to the order of the point Q under the group action on E

3. For every prime $\mathfrak{a}$ with $(\mathfrak{a}, S) = 1$, we have

$$\prod_{Q \in E_\mathfrak{a}} \rho(P \oplus Q) = \rho(\psi_E(\mathfrak{a})(P))$$

Step 3: A Key Property of $\mathcal{R}_\lambda$

We aim to show that $\mathcal{R}_\lambda$ satisfies the following property involving the Grossencharacter ψ_E:

$$\mathcal{R}_\lambda(\psi_E(\mathfrak{a})(P)) = \prod_{V \in E_\mathfrak{a}} \mathcal{R}_\lambda(P \oplus V)$$

That is, we aim to show that is satisfies condition three, above, required of an Euler function.

This follows in much the same way as the comparison of the functions $r_\lambda(\alpha(P))$ and $\prod_{U \in E_\alpha} r_\lambda(P \oplus U)$ that we did, above. Take α such that $(\alpha) = \mathfrak{a}$. The proof relies on

the fact that applying α to the primitive f-torsion points Q^τ, $\tau \in \mathrm{Gal}(K(E_\mathfrak{f})/K)$, permutes them.

This follows from the coprimality of α and λ. So,

$$R_\lambda(\alpha(P) \oplus Q) = R_\lambda(\alpha(P \oplus Q'))$$

where Q' is some other f-torsion point and from our earlier result, and our good choice of normaliser $c_E(\lambda)$, we get

$$R_\lambda(\alpha(P) \oplus Q) = R_\lambda(\alpha(P \oplus Q')) = \prod_{V \in E_\mathfrak{a}} R_\lambda(P \oplus Q' \oplus V)$$

And hence we have shown that

$$\mathcal{R}_\lambda(\alpha(P)) = \prod_{\tau \in \mathrm{Gal}(K(E_\mathfrak{f})/K)} \left(\prod_{v \in E_\mathfrak{a}} R_\lambda(P \oplus Q^\tau \oplus V) \right) = \prod_{v \in E_\mathfrak{a}} \mathcal{R}_\lambda(P \oplus V)$$

In fact, $\mathcal{R}_\lambda$ satisfies all the conditions required to be an Euler function if we take S to be the primes of bad reduction and the primes dividing 2λ.

From the "key property" result, we are motivated to define

$$\Phi_\lambda(P) = \frac{\mathcal{R}_\lambda(P)^p}{\mathcal{R}_\lambda(\psi_E(\mathfrak{p})(P))} = \prod_{V \in E_\mathfrak{p}} \left(\frac{\mathcal{R}_\lambda(P)}{\mathcal{R}_\lambda(P \oplus V)} \right)$$

where $\mathfrak{p}$ is the prime of good reduction in $\mathcal{O}_K$ whose character $\chi_\mathfrak{p} : G \xrightarrow{\sim} \mathbb{Z}_p^\times$ we are still chasing after.

We see immediately that

$$\prod_{V \in E_\mathfrak{p}} \Phi_\lambda(P) = \prod_{V \in E_\mathfrak{p}} \prod_{V' \in E_\mathfrak{p}} \left(\frac{\mathcal{R}_\lambda(P \oplus V)}{\mathcal{R}_\lambda(P \oplus V \oplus V')} \right) = 1$$

since every factor of this product appears exactly once in both the denominator and the numerator.

Eventually, we will show that the power series expansion of $\Phi_\lambda(P)$ in terms of the formal group local parameter $t = -\frac{x}{y}$ is very closely related to something that is nearly the g we are looking for.

3.5.2 The Formal Group of E at $\mathfrak{p}$

The formal group of E at $\mathfrak{p}$ is denoted by $\hat{E}_\mathfrak{p}$. It is a formal group of height 1 defined over $\mathcal{O}_\mathfrak{p}$, which we may actuall show to be a Lubin-Tate group over $\mathcal{O}_\mathfrak{p}$.

A formal group is defined by a group law F which is a power series in two variables, X and Y. We have

$$F = X + Y + \text{ higher order terms}$$

Furthermore, F is symmetric in X and Y, and satisfies $F(X, F(Y, Z)) = F(F(X, Y), Z)$ and $F(X, 0) = X$ (hence XY divides the higher order terms above).

An endomorphism $\hat{E}_{\mathfrak{p}} \to \hat{E}_{\mathfrak{p}}$ defined over R is given by a power series $f \in R[[T]]$ which satisfies

$$F(f(X), f(Y)) = f(F(X, Y))$$

All formal groups are isomorphic over their fields of fractions. We are interested in those that are isomorphic as defined over certain rings of integers (in our case, the ring $\mathcal{I}$). Here, it is clear why we define our measures and algebras in terms of the ring $\mathcal{I}$ as opposed to the perhaps more obvious choice of the ring of integers $\mathbb{Z}_p$. We want to show that we have an isomorphism, defined over $\mathcal{I}$, from our formal group of E at $\mathfrak{p}$ to the formal multiplicative group $\hat{\mathbb{G}}_m$. We will see that such an isomorphism exists over $\mathcal{I}$ but we note that it does not exist over the smaller ring $\mathbb{Z}_p$.

The formal multiplicative group $\hat{\mathbb{G}}_m$ has group operation given by

$$F(X, Y) = X \oplus_{\hat{\mathbb{G}}_m} Y = X + Y + XY$$

The local parameter for $\hat{E}_{\mathfrak{p}}$ is $t = -\frac{x}{y}$. The set of points which belong to our formal group $\hat{E}_{\mathfrak{p}}$ are those which can be specified in terms of our parameter.

We have a one-to-one correspondence between the endomorphisms, α, of E and associated formal endomorphisms $[\alpha]$, which are formal power series in t that begin $[\alpha]t = \alpha t + ...$ Note the potential for confusion, here, with the "multiplication by n" map which is denoted by $[n]$, also with square brackets.

3.5.3 The power series expansion of $\Phi_\lambda(P)$

Using the definitions of the functions R_λ and $\mathcal{R}_\lambda$ and of the constant $c_E(\lambda)$, and considering the formal group structure of E at $\mathfrak{p}$, we may show that the power series expansion of $\mathcal{R}_\lambda(P)$ in terms of the local parameter $t = -\frac{x}{y}$ is a unit in $\mathcal{O}_{\mathfrak{p}}[[t]]$.

We first show that our power series lies in $\mathcal{O}_{\mathfrak{p}}[[t]]$, that is, the negative powers of t all eventually cancel out. It then remains to show that the constant term of the power series is a unit, since this is all that is required for a formal power series to be invertible.

We seek the power series expansion of $\Phi_\lambda(P)$, and we aim to show that it lies in

$$1 + \psi_E(\mathfrak{p})\mathcal{O}_{\mathfrak{p}}[[t]] = 1 + \mathfrak{p}$$

The function $\Phi_\lambda(P)$ is defined as a fraction of functions of $\mathcal{R}_\lambda$. Denote the power series expansion of $\mathcal{R}_\lambda(P)$ by:

$$A_\lambda(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathcal{O}_{\mathfrak{p}}[[t]] \qquad a_0 \in \mathcal{O}_{\mathfrak{p}}^\times$$

It is obvious that the power series expansion for $\mathcal{R}_\lambda(P)^p$ is given by $A_\lambda(t)^p$, so it remains to find the power series expansion for $\mathcal{R}_\lambda(\psi_E(\mathfrak{p})P) = \mathcal{R}_\lambda(\pi_\mathfrak{p} P)$.

This is given by a composition of the power series expansion for $\pi_\mathfrak{p}$, as an element of the endomorphism ring of the formal group of E at $\mathfrak{p}$, with the power series $A_\lambda(t)$. We consider the formal endomorphism $[\pi_\mathfrak{p}]$ associated to the endomorphism $\pi_p \in \mathcal{O}_K$. We know that

$$[\pi_\mathfrak{p}](t) = \pi_\mathfrak{p} t + ...$$

We consider the reduction of $[\pi_\mathfrak{p}](t)$ mod $\mathfrak{p}$, i.e. its image in the residue power series ring $\mathbb{F}_p[[t]]$. Just as in the non-formal endomorphism case, we have that it gives an endomorphism of the reduced curve. By associating our regular ring of endomorphisms to the reduced curve $\tilde{E}_\mathfrak{p}$, we see that this map is the formal endomorphism corresponding to the Frobenius map. The "power series" expansion of the Frobenius map is known for the coordinates x and y. Since it has a very simple form, this yields an expression for it in terms of $t = -\frac{x}{y}$. We deduce

$$\widetilde{[\pi_\mathfrak{p}](t)} = \widetilde{[\pi_\mathfrak{p}]\left(-\frac{x}{y}\right)} = -\frac{x^p}{y^p} = \left(-\frac{x}{y}\right)^p = t^p$$

where we use the fact that p is odd and recall that we insisted upon $p > 2$.

We now evaluate

$$A_\lambda([\pi_\mathfrak{p}]t) = \sum_{n=0}^{\infty} a_n([\pi_\mathfrak{p}]t)^n = \sum_{n=0}^{\infty} a_n t^{pn} \mod \mathfrak{p}$$

We also have

$$A_\lambda(t)^p = \sum_{n=0}^{\infty} a_n^p t^{np} = A_\lambda([\pi_\mathfrak{p}]t) \mod \mathfrak{p}$$

since $a_n^{p-1} = 1 \mod \mathfrak{p}$. So

$$\frac{g(t)^p}{g([\pi_\mathfrak{p}](t))} = \frac{\sum_{n=0}^{\infty} a_n t^{np}}{\sum_{n=0}^{\infty} a_n t^{np}} \mod \mathfrak{p} = 1 \mod \mathfrak{p}$$

and, since $\mathfrak{p} = \psi_E(\mathfrak{p})\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$ and $1 \in \mathcal{O}_\mathfrak{p}$, the power series expansion of $\Phi_\lambda(P)$ lies in $\mathcal{O}_\mathfrak{p}[[t]]$. We denote it by $B_\lambda(t)$.

We define $C_\lambda(t) = \frac{1}{p}\log B_\lambda(t)$. This power series almost satisfies the conditions required of our element $g(W) \in \mathcal{I}[[W]]$. We get

$$\sum_{R \in E_\mathfrak{p}} C_\lambda(t \oplus t_R) = 0$$

3.5.4 Using the Formal Group to Construct a Measure

Recall that we seek some $g(W) \in \mathcal{I}[[W]]$ such that

$$\sum_{\zeta \in \mu_p} g(\zeta(1+W) - 1) = 0$$

Consider

$$(\zeta - 1) \oplus_{\hat{\mathbb{G}}_m} W = (\zeta + 1) + W + (\zeta + 1)W = \zeta(1 + W) - 1$$

This is of the form of the summand argument above. From Tate-Lubin theory, we can show that the formal group of E at $\mathfrak{p}$, $\hat{E}_{\mathfrak{p}}$, is ismorphic over $\mathcal{I}$ to $\hat{\mathbb{G}}_m$. This is promising, because the relation we have on C_λ, above, now differs from what we want only by a change in the group operation. The elements of $E_{\mathfrak{p}}$ exactly correspond to the pth roots of unity in the multiplicative group. So, if we can get an isomorphism between the two groups whose coefficients lie in $\mathcal{I}$, then we can construct an element of $\mathcal{I}[[W]]$ satisfying out claim.

We denote the isomorphism from $\hat{G} \to \hat{E}_{\mathfrak{p}}$ by δ and we call its linear coefficient $\Omega_{\mathfrak{p}}$. This is an important constant which we will also see later on. Our local parameter in $\hat{E}_{\mathfrak{p}}$ is expressible in terms of the local parameter in $\hat{\mathbb{G}}_m$ by $t = \delta(W)$.

The final definition of this section is

$$g(W) = C_\lambda(\delta(W))$$

As explained above, g satisfies the condition required to be the canonical generating power series of our Iwasawa algebra $\Lambda_{\mathcal{I}}(G)$.

3.6 The Canonical Element gives a Measure

The power series $g(W) \in \mathcal{I}[[W]]$ corresponds to some element of the Iwasawa algebra, since we have an isomorphism from $\Lambda_{\mathcal{I}}(\mathbb{Z}_p) \to \mathcal{I}[[W]]$, and the properties of g mean that it comes from an element of $\Lambda_{\mathcal{I}}(G)$. We denote the corresponding measure by μ_λ. Our recipe for constructing g means that $g(W) \in \mathcal{I}[[W]]$ is canonical. Hence the measure μ_λ corresponding to it under our isomorphism is also canonical. It depends only on the choice of λ.

Recall that

$$\mu_\lambda(f) = \int_G f d\mu_\lambda$$

Using the properties of our g, and the exponential map which goes from $\hat{\mathbb{G}}_a \to \hat{\mathbb{G}}_m$, we obtain an expression for

$$\mu_\lambda(\chi_{\mathfrak{p}}^n) = \int_G \chi_{\mathfrak{p}}^n d\mu_\lambda$$

in terms of the evaluation of the imprimitive L-function at n, $L_{\mathfrak{f}}(\psi_E^n, n)$.

This is almost what we want: we normalise our measure μ_λ to simplify our expression. This is fairly straightforward. The hard part is dealing with the potential case that our imprimitive L-function is missing factors (corresponding to those places where the conductor $\mathfrak{f}_n$ is a proper factor of $\mathfrak{f}$). We seek an expression for our measure in terms of the *primitive* L-function.

3.6.1 Normalising the Measure

Recall that we have a function relating our measure to the L-function, $L_{\mathfrak{f}}$:

$$\int_G \chi_{\mathfrak{p}}^n d\mu_\lambda = F(n, \Omega_{\mathfrak{p}}, \Omega_\infty, f, \lambda, \mathfrak{p}, \psi_E(\mathfrak{p})) \times L_{\mathfrak{f}}(\overline{\psi}_E^n, n)$$

where F is some function in the variables shown. We want to make the function F as simple as possible. In the end, we will show that we can choose a measure such that F is

$$(n-1)!\left(\frac{\Omega_p}{\Omega_\infty}\right)^n \left(1 - \frac{\psi_E(\mathfrak{p})^n}{N\mathfrak{p}}\right)$$

This is done by constructing some other measure η_λ such that the measure of G with respect to η_λ equals all the other terms in the expression for F. We then use the multiplicativity of the meaures to construct the normalised measure

$$\mu'_\lambda = \frac{\mu_\lambda}{\eta_\lambda}$$

Constructing this measure η_λ requires imposing additional restraints on λ:

So far, we require $\lambda \in \mathcal{O}_K$ to be coprime to 2 and 3. In order that we can normalise our measure, we further require that:

1. The element λ is not a unit in $\mathcal{O}_K$.
2. Let $\mathfrak{f}$, as before, be the conductor of ψ_E. Then $\lambda = 1 \mod 2\mathfrak{f}$.
3. If p is our prime in $\mathbb{Q}$ which splits in K as $p = \mathfrak{p}\mathfrak{p}^*$ with $\mathfrak{p} \neq \mathfrak{p}^*$, then the congruences $\lambda = 1 \mod \mathfrak{p}$ and $\lambda = 2 \mod \mathfrak{p}^*$ hold.

The conductor $\mathfrak{f}$ and the primes $\mathfrak{p}$ and $\mathfrak{p}^*$ are coprime since $\mathfrak{p}$ and $\mathfrak{p}^*$ are both places of good reduction on E, and only primes of bad reduction divide the conductor. Furthermore, $(\mathfrak{p}, \mathfrak{p}^*) = 1$. This means we can apply the Chinese remainder theorem. We obtain a family of solutions to our numbered congruence relations which is unique up to mod $2\mathfrak{f}p$.

3.6.2 Obtaining Primitive L-values

Recall, firstly, that the L-function $L_{\mathfrak{f}}$ differs from the primitive L-function for ψ_E^n because it is missing those factors at places coprime to the conductor, $\mathfrak{f}_n$, of ψ_E^n but dividing the conductor, $\mathfrak{f}$, of ψ_E.

Since we have an embedding of $\mathcal{O}_K \hookrightarrow \mathbb{Z}_p$, $\mu_K \subset \mu_{p-1}$.

Claim: *If $n = m \mod p-1$, then their conductors will be the same.*

Proof: Let $m = n + r(p-1)$, where r is some integer, so the argument is entirely reversible. Say $\mathfrak{a}$ is some ideal such that

$$\psi_E^{n+r(p-1)}(\mathfrak{a}) = \psi_E(\mathfrak{a})^{n+r(p-1)} = 1$$

Then $\psi_E(\mathfrak{a})$ is a root of unity in K, hence $\psi_E(\mathfrak{a})^{p-1} = 1$. We deduce that $\psi_E^n(\mathfrak{a}) = 1$. $\square$

So, we index the conductors $\mathfrak{f}_n$ by the congruence class of n mod $p-1$.

Recall also that we had the decomposition of

$$\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p) \cong \mu_{p-1} \times \mathbb{Z}_p \cong G$$

where, for the penultimate isomorphism, we consider the map

$$1 + px \mapsto x$$

Let Δ and Γ be the subgroups of G corresponding to μ_{p-1} and $\mathbb{Z}_p$, respectively, under the final isomorphism.

We think of the $(p-1)$ copies of Γ living inside G (each corresponding to an element of μ_{p-1}) to be the $(p-1)$ "branches" of the group G. The isomorphism

$$G \xrightarrow{\sim} \underbrace{\Gamma \times \cdots \times \Gamma}_{p-1 \text{ copies}}$$

induces an isomorphim of the Iwasawa algebras

$$\Lambda_{\mathcal{I}}(G) \xrightarrow{\sim} \underbrace{\Lambda_{\mathcal{I}}(\Gamma) \times \cdots \times \Lambda_{\mathcal{I}}(\Gamma)}_{p-1 \text{ copies}}$$

This is useful because $\Gamma \cong \mathbb{Z}_p$ so we know that $\Lambda_{\mathcal{I}}(\Gamma)$ is isomorphic to $\mathcal{I}[[G]]$. We will use these branches to allow us to find an expression for $\int_G \chi_{\mathfrak{p}}^n d\mu$ in terms of the primitive L-functions, as opposed to the imprimitive ones.

We can map our measure $\mu := \mu'_\lambda$ into these copies of $\Lambda_{\mathcal{I}}(\Gamma)$, and we denote the element of the ith copy of $\Lambda_{\mathcal{I}}(\Gamma)$ by μ_i.

The main property which makes these branches a workable way of defining our p-adic L-function is that they satisfy

$$\int_G \chi_{\mathfrak{p}}^n d\mu = \int_\Gamma \chi_{\mathfrak{p}}^n d\mu_i \quad \text{where } n = i \mod p-1$$

Let $\chi_{\mathfrak{p}}(g) \in \mathbb{Z}_p^\times$ be expressible, according to our decomposition, as the product of a root of unity and an element of $1 + p\mathbb{Z}_p$. Then the root of unity decomposition of $\chi_{\mathfrak{p}}^n(g)$ is ζ_{p-1}^i where ζ is chosen to be some canonical primitive root of unity such

that multiples of ζ^i correspond to the ith copy of Γ (note that the "$p-1$"th copy corresponds to $\zeta^{p-1}=1$).

To finally show the existence of the p-adic L-function as constructed via this method, we aim to show that the element $\mu_1 \in \Lambda_{\mathcal{I}}(\Gamma)$, satisfies the equation:

$$\Omega_{\mathfrak{p}}^{-n}\int_G \chi_{\mathfrak{p}}^n d\mu_1 = (n-1)!\Omega_\infty^{-n} L(\overline{\psi}_E^n, n)\left(1-\frac{\psi_E^n(\mathfrak{p})}{N\mathfrak{p}}\right) \quad \text{for all } n=1 \mod p-1$$

Taking branches of the measure makes the changes required of the conductor to ensure that our L-function is primitive. We note that it is not hard to show the uniqueness of such a measure via the use of the Weierstrass Preparation Theorem.

The pseudo-measure on G whose branches are given by the μ_i is denoted by $L_{\mathfrak{p},E}$. It is through this pseudo-measure that the $\mathfrak{p}$-adic L-functions are used in the statement of the main conjecture.

This formulation of the $\mathfrak{p}$-adic L-function is equivalent to the existence of a power series, denoted $H_{\mathfrak{p}}(T) \in \mathcal{I}[[T]]$, with

$$H_{\mathfrak{p}}((1+p)^n-1) = L_{\mu,1}(n) := \int_G \chi_{\mathfrak{p}}^n d\mu_i$$

The first equality follows by considering the isomorphism from Γ to $1+p\mathbb{Z}_p$ and using the fact that this map takes a topological generator of Γ, i.e. one that generates a dense subset of Γ, to one of $1+p\mathbb{Z}_p$ and that $1+p$ is a generator of $1+p\mathbb{Z}_p$.

4 The Main Conjecture

4.1 Formulation of the Main Conjecture

To define the main conjecture of Iwasawa theory for elliptic curves with complex multiplication, we consider the following set-up:

As before, we make the assumption that E is defined over K and $\mathrm{End}_K(E)\otimes\mathbb{Q} = K$. We further assume that $\mathrm{End}_K(E) = \mathcal{O}_K$. We take some prime $p>3$ which splits in K as $p=\mathfrak{p}\mathfrak{p}^*$ with $\mathfrak{p}\neq\mathfrak{p}^*$ and where E has good reduction at $\mathfrak{p}$ and $\mathfrak{p}^*$.

Recall that $K_\infty = K(E_{\mathfrak{p}^\infty})$ is the field extension of K obtained by adjoining the $\mathfrak{p}^n$-torsion for all n. Recall also that $\mathfrak{p}$ is totally ramified in each of the intermediate field extensions

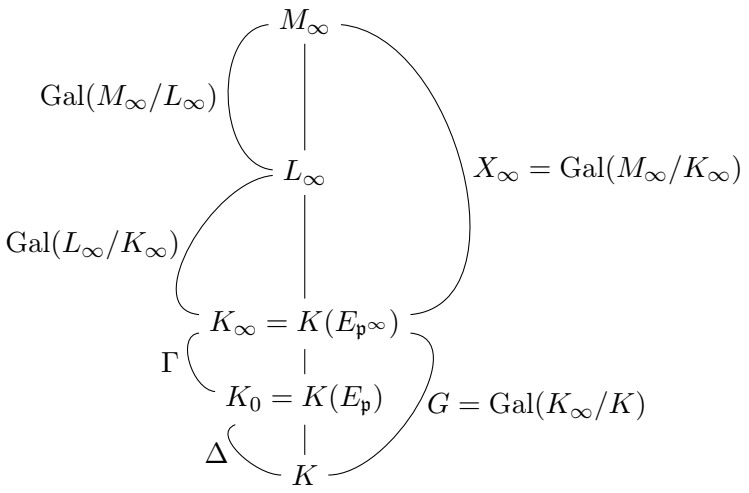
$$K_n = K(E_{\mathfrak{p}^{n+1}})$$

and we denote the unique prime above $\mathfrak{p}$ in K_n by $\mathfrak{p}_n$. All the finite field extensions, and the infinite extension F_∞ in our tower, are unramified outside of the primes above $\mathfrak{p}$. Recall that

$$\mathbb{Z}_p^\times \cong G = \mathrm{Gal}(K_\infty/K) = \Delta\times\Gamma$$

where $\Delta \approxeq \mu_{p-1}$ and $\Gamma \approxeq 1 + p\mathbb{Z}_p \approxeq Z_p$ and they are the Galois groups of the field extensions shown in the diagram below.

The first field extension of K_∞ that we consider is the maximal everywhere unramified extension of K_∞. This is denoted by L_∞. Our second field extension of interest is the maximal extension of K_∞ unramified outside of those primes above $\mathfrak{p}$, this is denoted by M_∞. Our set-up may be summarised by the following diagram:



In Section 3.2, we defined the Iwasawa algebra with coefficients in $\mathcal{I}$. We now use the analogous module which has coefficients in $\mathbb{Z}_p$ instead of $\mathcal{I}$. Just as we denoted our previous Iwasawa algebra by $\Lambda_\mathcal{I}(G)$, we denote this one by

$$\Lambda_{\mathbb{Z}_p}(G) = \varprojlim_U \mathbb{Z}_p[G/U]$$

where we take the limit over $U \subset G$ open subgroups. To simplify the notation, we write $\Lambda(G)$ for $\Lambda_{\mathbb{Z}_p}(G)$.

A $\Lambda(G)$-torsion module is a module Y over $\Lambda(G)$ such that for all $y \in Y$ there is some $\lambda_y \in \Lambda(G)$ (which is not a divisor of 0 in $\Lambda(G)$) with

$$\lambda_y y = 0$$

When G is an abelian group, we have a global annihilator for the group. That is, some $\lambda \in \Lambda(G)$ such that $\lambda y = 0$ for all $y \in Y$. In the non-abelian case such a global annihilator cannot necessarily be found.

We have the following structure theorem for finitely generated $\Lambda(G)$-torsion modules: The sequence

$$0 \to Y \to \bigoplus_{i=1}^{n} \frac{\Lambda(G)}{f_i \Lambda(G)} \to D \to 0$$

is exact, for f_i elements of $\Lambda(G)$ (not divisors of 0) and D some finite $\Lambda(G)$-module.

From this we may define the characteristic ideal of a $\Lambda(G)$-module. This is denoted by $\mathrm{ch}_G(Y)$ and is defined by

$$\mathrm{ch}_G(Y) = f_1 \cdots f_r \Lambda(G)$$

where the f_i are those appearing in the exact sequence above. The characteristic ideal is well-defined because the exact sequence giving the structure theorem, above, is unique up to units in each of the f_i and up to re-ordering of the factors $\frac{\Lambda(G)}{f_i \Lambda(G)}$.

Our main conjecture is a result about the group $X_\infty = \mathrm{Gal}(M_\infty/K_\infty)$. It can be shown, see Section 4.2, that this is a $\Lambda(G)$-torsion module. We choose some $f \in \Lambda(G)$ which generates its characteristic ideal:

$$\mathrm{ch}_G(X_\infty) = \mathrm{ch}_G(\mathrm{Gal}(M_\infty/K_\infty)) = (f)$$

Recall that $L_{\mathfrak{p},E}$ is the pseudo-measure on G given by our construction of the $\mathfrak{p}$-adic L-functions.

There is one final definition that we must make before stating the main conjecture. This is the notion of an augmentation ideal. We will wish to consider the augmentation ideal of $\Lambda_{\mathcal{I}}(G)$. The augmentation ideal is that generated by the set

$$\{\mu - 1 : \mu \in \Lambda_{\mathcal{I}}(G)\}$$

we denote the augmentation ideal of $\Lambda_{\mathcal{I}}(G)$ by $I(G)$.

The One-Variable Main Conjecture of Iwasawa Theory of Elliptic Curves with Complex Multiplication:

$$f\Lambda_{\mathcal{I}}(G) = L_{\mathfrak{p},E} I(G)$$

where f, as above, is a generating element for $\mathrm{ch}_G(X_\infty)$ and $X_\infty = \mathrm{Gal}(M_\infty/K_\infty)$. So, the main conjecture says that the characteristic ideal can be generated by a $\mathfrak{p}$-adic L-function of E.

The consequences of the main conjecture include a proven connection between the L-function and the arithmetic properties of the curve E via the BSD conjecture. These are introduced in Section 1.4. We discuss this connection further in Section 4.3.

4.2 On the Proof of the Main Conjecture

4.2.1 The Useful Unit Groups

The proof of the main conjecture requires that we define the following groups of units lying inside K_n:

- The group of (global) units of K_n is $\mathcal{E}_n$

- The group of (local) units of the completion of K_n at $\mathfrak{p}_n$, which are congruent to 1 modulo $\mathfrak{p}_n$, is U_n
- The group of elliptic units of K_n (defined below) is C_n
- The closure of $\mathcal{E}_n \cap U_n$ in U_n is $\overline{\mathcal{E}}_n$, taken with respect to the $\mathfrak{p}_n$-adic topology
- The closure of $C_n \cap U_n$ in U_n is $\overline{C}_n$, also taken with respect to the $\mathfrak{p}_n$-adic topology

Given any one of the above groups of units, we consider the collection of groups of units obtained by indexing by n and the associated collection of maps obtained via inclusion. We take the inverse limit of this inverse system and denote it by a subscript "∞". For example

$$C_\infty = \varprojlim_n C_n$$

and we similarly construct $\mathcal{E}_\infty$, U_∞, $\overline{\mathcal{E}}_\infty$ and $\overline{C}_\infty$.

The elliptic units are a special class of units of the abelian extensions K_n. We construct them using primitive division points on E, which we obtain as before via the identification of our elliptic curve with the quotient $\mathbb{C}/L$ where L is a lattice such that

$$\Phi : E/\mathbb{C} \xrightarrow{\sim} \mathbb{C}/L$$

Note that our E is defined over an imaginary quadratic field, K, which we know can be embedded into $\mathbb{C}$ (since $K \subset \mathbb{C}$), so for these purposes we can think of the elliptic curve as being defined over $\mathbb{C}$. Consider some ideal $\mathfrak{a} \subset \mathcal{O}_K$. For every prime $l|\mathfrak{a}$, satisfying particular congruency conditions, we can consider an element x_l of our lattice which has order exactly l. This may be found by taking an element of $L \backslash lL$ and dividing it by l. We then consider a point, call it τ, which has order exactly $\mathfrak{p}^m$ for some m. We consider the point in E corresponding to the element

$$\tau + \sum_l x_l$$

where we take the sum over those $l|\mathfrak{a}$ which satisfy the required congruency conditions. Our elliptic units are obtained by considering those functions which send ideals $\mathfrak{a}$ to such a point as above.

In our case, the elliptic units are the subgroup of the units generated by applying the functions $\mathcal{R}_\lambda$ and Φ_λ to primitive $\mathfrak{p}^n$-torsion points on E for all n. The other variables range over suitable sets specified in terms of E and its conductor $\mathfrak{f}$.

Along the way to proving the main conjecture, we prove the "analytic class number formula" which gives us insight into the important invariants of a number field. For F some extension of K, with the p-part of $\mathrm{Gal}(F/K)$ cyclic and all primes of K not dividing p having ramification degree prime to p, we have a simple formula relating the p-part of the ideal class group of F to the p-part of the quotient of the global units in F by the elliptic units.

Note that $\overline{U}_\infty$ and $\overline{C}_\infty$ are both modules over the Iwasawa algebra $\Lambda(G)$. These groups of units allow us to study certain key exact sequences, from which we may deduce the proof of the main conjecture.

4.2.2 Restating the Main Conjecture using Exact Sequences

Let $\mu_{p^\infty}(K_\infty)$ denote the p-power roots of unity which lie in K_∞. Let f be some element of $\Lambda(G)$ which satisfies

$$f\Lambda_{\mathcal{I}}(G) = L_{\mathfrak{p},E}I(G)$$

(where we note that the main conjecture is the statement that we can choose such an f satisfying the above equation to also generate the characteristic ideal of X_∞). Then we have the following exact sequence:

$$0 \to U_\infty/\overline{C_\infty} \to \Lambda(G)/f\Lambda(G) \to \mu_{p^\infty}(K_\infty) \to 0$$

Global class field theory applied to the above exact sequence gives us the even more useful exact sequence

$$0 \to \overline{E}_\infty/\overline{C}_\infty \to U_\infty/\overline{C}_\infty \to \mathrm{Gal}(M_\infty/K_\infty) \to \mathrm{Gal}(L_\infty/K_\infty) \to 0$$

We may then readily prove that the two groups $\mathrm{Gal}(L_\infty/K_\infty)$ and $\mathrm{Gal}(M_\infty/L_\infty)$ are $\Lambda(G)$-torsion modules, as defined above. The former proof is mostly elementary and procedes via an application of Nakayama's Lemma. The latter is much more involved and requires the involvement of class field theory.

So for the two groups, $\mathrm{Gal}(M_\infty/L_\infty)$ and $\mathrm{Gal}(L_\infty/K_\infty)$, we have the above structure theorem and can define their characteristic ideals.

Aim: *Prove that the main conjecture is equivalent to the statement*

$$\mathrm{ch}_G(\overline{E}_\infty/\overline{C}_\infty) = \mathrm{ch}_G(\mathrm{Gal}(L_\infty/K_\infty))$$

We prove this using the multiplicativity of the characteristic ideal function "ch_G" which goes from $\Lambda(G)$-torsion modules to elements of $\Lambda(G)$. We then use an important fact, see below.

Claim: *If* $0 \to X_1 \to X_2 \to X_3 \to 0$ *is an exact sequence, then*

$$\mathrm{ch}_G(X_2) = \mathrm{ch}_G(X_1)\mathrm{ch}_G(X_3)$$

Proof: We say that two modules X and Y are pseudo-isomorphic if there is a map $\phi : X \to Y$ such that $\ker(\phi)$ and $\mathrm{coker}(\phi)$ are both finite.

Say we have the following exact sequences (for $j = 1, 2, 3$) coming from the structure theorem for the $\Lambda(G)$-torsion modules:

$$0 \to X_j \to \bigoplus_{i=1}^{n_j} \frac{\Lambda(G)}{f_i^{(j)}\Lambda(G)} \to D_j \to 0$$

The finiteness of D_j implies that each X_j is pseudo-isomorphic to the corresponding middle term of the above exact sequence. Recall that G is isomorphic to the product of $p-1$ copies of Γ, where $\Gamma \cong \mathbb{Z}_p$. We have a corresponding isomorphism of Iwasawa algebras

$$\Lambda(G) \xrightarrow{\sim} \underbrace{\Lambda(\Gamma) \times \cdots \times \Lambda(\Gamma)}_{p-1 \text{ copies}}$$

Using this decomposition, we consider the module $X_j^{(k)}$ which is pseudo-isomorphic to

$$\bigoplus_{i=1}^{n} \frac{\Lambda(\Gamma)}{f_{i,k}^{(j)}\Lambda(\Gamma)}$$

where $\Lambda(\Gamma)$ is the kth copy of $\Lambda(\Gamma)$ inside $\Lambda(G)$, and the $f_{i,k}^{(j)}$ are the non-zero divisors obtained by projecting $\Lambda(G)/f_i^{(j)}\Lambda(G)$ to the kth copy of $\Lambda(G)$ and we note that we may have $f_{i,k}^{(j)} = 1$.

We have exact sequences

$$0 \to X_1^{(k)} \to X_2^{(k)} \to X_3^{(k)} \to 0$$

for all k where the $X_i^{(k)}$ are $\Lambda(\Gamma)$-torsion modules. The multiplicativity of the characteristic ideals on exact sequences for these $\Lambda(\Gamma)$-torsion modules can be shown by the theory of pseudo-isomophisms over local torsion modules[7]. The multiplicativity of the characteristic ideals for our original exact sequence can then be found by piecing these exact sequences together. $\square$

Fact:

$$(f) = \mathrm{ch}_G(U_\infty/\overline{C}_\infty) \quad \Longrightarrow \quad f\Lambda_{\mathcal{I}}(G) = L_{\mathfrak{p},E}I(G)$$

This means that the property required of the group X_∞ in order to prove the main conjecture is possessed by the group $U_\infty/\overline{C}_\infty$. So, to prove the main conjecture, it suffices to show that the characteristic ideals of these two groups are the same.

From our exact sequences, and via the multiplicativity of the characteristic ideal function "ch_G", we have

$$\mathrm{ch}_G(\overline{E}_\infty/\overline{C}_\infty)\mathrm{ch}_G(X_\infty) = \mathrm{ch}_G(U_\infty/\overline{C}_\infty)\mathrm{ch}_G(\mathrm{Gal}(L_\infty/K_\infty))$$

from which it immediately follows that

$$\mathrm{ch}_G(U_\infty/\overline{C}_\infty) = \mathrm{ch}_G(X_\infty) \quad \Longleftrightarrow \quad \mathrm{ch}_G(\overline{E}_\infty/\overline{C}_\infty) = \mathrm{ch}_G(\mathrm{Gal}(L_\infty/K_\infty))$$

[7]Chapter VII; N. Bourbaki, *Commutative Algebra*, 1972

The proof progresses using Kolyvagin's systems of units. Recall the two functions

$$\mathcal{R}_\lambda(P) = \prod_{\tau \in \mathrm{Gal}(K(E_\mathfrak{f})/K)} R_\lambda(P \oplus Q^\tau)$$

and

$$\Phi_\lambda(P) = \frac{\mathcal{R}_\lambda(P)^p}{\mathcal{R}_\lambda(\psi_E(\mathfrak{p})(P))}$$

Our proof of the main conjecture procedes by evaluating these functions at carefully chosen points of finite order.

We first make use of these to determine the size of the eigenspaces of the p-part of the ideal class group of an abelian field extension F/K with $p \nmid [F : K]$. From this, we then progress to consider fields F where F/K is a finite extension of any degree.

4.3 Connections to the Birch and Swinnerton-Dyer Conjecture

As ever, we have the following set-up: E an elliptic curve with complex multiplication defined over K with

$$\mathrm{End}_K(E) = \mathcal{O}_K$$

The period of the invariant differential on E is denoted by Ω_∞ and satisfies $\Omega_\infty \mathcal{O}_K = L$ where L is the period lattice. The roots of unity in the field K are denoted by μ_K, and $|\mu_K||6$. The Grossencharacter associated to the curve E/K is denoted by ψ_E and its complex conjugate Grossencharacter by ψ_E^*.

As before, the order of vanishing of $L(E, s)$ at $s = 1$ is denoted by r, and the arithmetic rank of $E(K)$ is denoted by g. Also, $X_\infty = \mathrm{Gal}(M_\infty/K_\infty)$ for M_∞ the extension of K_∞ defined above.

We study the $\mathfrak{p}$-part of the group $Ш_{E/K}$, denoted by $Ш_{E/K}(\mathfrak{p})$, i.e. the part of the group of maximal $\mathfrak{p}$-power order. As described in Section 1.4.2, we can use the results of our methods from Iwasawa theory to show that $Ш_{E/K}(\mathfrak{p})$ is finite for particular primes $\mathfrak{p}$, provided that

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

The strictness of the restrictions that we must place on the prime $\mathfrak{p}$ depend on whether $r = 0$ or $r = 1$.

For $\phi \in \mathrm{End}_K(E)$, the ϕ-Selmer group is

$$S^{(\phi)}(E/K) = \ker\left(H^1(K, E[\phi]) \to \prod_{v \in \Sigma_K} H^1(K_v, E) \right)$$

We give an important result which yields a proof of the "weak version" of the BSD conjecture in the case $r = 0$ and a partial proof of the "strong version" of the BSD conjecture at the $\mathfrak{p}$-part for all $\mathfrak{p} \nmid |\mu_K|$:

Claim: *If $r = 0$, then $g = 0$ and, for all primes $\mathfrak{p} \in K$ with $\mathfrak{p} \nmid |\mu_K|$, we have*

$$Ш_{E/K}(\mathfrak{p}) = N\mathfrak{p}^{m(\mathfrak{p})} \qquad \text{where} \qquad m(\mathfrak{p}) = \text{ord}_{\mathfrak{p}}\left(|E(K)|\frac{L(\psi_K^*)}{\Omega_\infty}\right)$$

where, as before, $N\mathfrak{p} = \#(\mathcal{O}_K/\mathfrak{p})$ is the norm of $\mathfrak{p}$.

We have a corresponding result for $r \neq 0$:

Claim: *If $r \geq 1$, then $g \geq 1$ provided that $Ш_{E/K}(\mathfrak{p})$ is finite for some prime $\mathfrak{p}$ of K with $\mathfrak{p} \nmid |\mu_K|$.*

The proofs of these results procede via a consideration of the Galois cohomology of $Ш_{E/K}(\mathfrak{p})$ and a group S obtained by taking the direct limit of the Selmer groups of E relative to powers of $\mathfrak{p}$. We then prove a relationship between the Selmer group and the module X_∞ defined above. We require the structure theorem of $\Lambda(G)$-torsion modules and the groups of units that we met in Section 4.2.1.

We split into the case where E has good reduction at $\mathfrak{p}$, and that where E has bad reduction at $\mathfrak{p}$. The case of good reduction follows via the use of Wiles' reciprocity law. For the case of bad reduction, we get back to the case of good reduction by replacing our elliptic curve by a suitable choice of its quadratic twists.

For the second claim, above, we conclude with the ultimatum which says that either $E(K)$ is infinite, which implies that the rank of $E(K)$ is non-zero, or the groups $Ш_{E/K}(\mathfrak{p})$ are infinite for all $\mathfrak{p} \nmid |\mu_K|$.

4.4 The Weak Parity Theorem

Before concluding this essay, I will pause for a moment to consider a result which links the BSD conjecture to the L-function of the elliptic curve in a way that is different to that we have previously seen.

The Strong Parity Conjecture states that

$$r = g \mod 2$$

where we recall that $r = \text{ord}_{s=1}(L(E, s))$ and g is the arithmetic rank of $E(K)$ for our elliptic curve E.

A proof of this conjecture remains, at present, far out of reach. The finiteness of the group $Ш_{E/K}$ implies that this conjecture holds for elliptic curves E defined over number fields and in fact the finiteness of $Ш_{E/K}$ and the strong parity conjecture are almost equivalent conjectures.

We define the integer t_p such that

$$Ш_{E/K}(p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_p} \oplus T$$

where T is some finite group. The Weak Parity Theorem says that

$$r = t_p + g \mod 2$$

for all primes p. It was proven by V. Dokchitser and T. Dokchitser in 2010[8], and is currently the closest known result to the Strong Parity Conjecture.

4.5 Concluding Thoughts

Throughout writing this essay my impression of Iwasawa theory and the BSD conjecture has oscillated drastically. One the one hand, it is surprising how elusive and unknown the theoretical results remain: there is a wealth of computational evidence and, on the theoretical side, there are results which appear as close to a conclusion as the ultimatum we finished upon in Section 4.3. On the other hand, the theory appears so intricate at times that I think it is a wonder we know anything at all.

What has remained consistent is that this is a fascinating area of mathematics and I feel very grateful for the opportunity to embark upon studying it. I would like to thank Prof. John Coates for his time and clear responses to my questions, and for the excellent sets of lecture notes (1-4 in References, below) whose clarity greatly helped to engage and sustain my interest. I would also like to thank Toby Gee and Sarah Zerbes for our helpful conversation about Tate modules.

[8]V. Dokchitser, T. Dokchitser, *On the Birch-Swinnerton-Dyer Quotients Modulo Squares*, Annals of Mathematics Vol 172, 2010

References

[1] Lecture notes: *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Beijing, China, March 2007

[2] Lecture notes: *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Cambridge, UK, Lent Term 2010

[3] Lecture notes: *"cm2"*, place and date unknown

[4] Lecture notes: *An Introduction to Elliptic Curves with Complex Multiplication and their Iwasawa Theory*, Postech, South Korea, date unknown

[5] Talk: K. Tsoi, *From Cyclotomic Fields to the BSD Conjecture*, Cambridge, UK, March 2014

[6] J. Coates, Y. Li, Y. Tian, S. Zhai, *Quadratic Twists of Elliptic Curves*, `http://arxiv.org/abs/1312.3884`, December 2013

[7] J. Coates, *Lecture Notes On the Birch-Swinnerton-Dyer Conjecture*, Notices of the International Congress of Chinese Mathematicians, November 2013

[8] J. Coates, *Elliptic Curves with Complex Multiplication and Iwasawa Theory*, Presidential addres to the London Mathematical Society, November 1990

[9] K. Rubin, *The "Main Conjectures" of Iwasawa Theory for Imaginary Quadratic Fields*, Inventiones Mathematicae, 1990

[10] J. Coates, R. Sujatha, *Cyclotomic Fields and Zeta Values*, April 2006

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2009

[12] E. De Shalit, *The Iwasawa Theory of Elliptic Curves with Complex Multiplication*, 1987

[13] J. W. S. Cassels, A. Froelich, *Algebraic Number Theory*, 1967

[14] K. Rubin, *The One-Variable Main Conjecture for Elliptic Curves with Complex Multiplication* in *L-functions and Arithmetic*, London Mathematical Society Lecture Note Series, 1991