An essay on Iwasawa Theory, The Eichler-Selberg Trace Formula and Shimura's Algebraicity Theorem

Sachin Kumar
Faculty of Mathematics, University of Waterloo

July 2024

Abstract

In this essay, I will give a detailed overview on classical Iwasawa theory, The Eichler-Selberg Trace Formula, Shimura's Algebraicity Theorem (about special values of L-functions) and proof of Weil conjectures for Elliptic curves over Finite fields (i.e., $E/\mathbb{F}_p$). I will provide intuition on some important topics in this field and how it is being used in developing theories arithmetic geometry and algebraic number theory. I would like mention that, Ch1-5 are on Iwasawa theory (which is recommended to be read in the same order), but Ch6-8 are independent chapters, i.e., those chapters can be read individually without the prior knowledge of other sections.

Contents

1 Iwasawa Theory

In this section, we summarize Iwasawa's Theorem about growth of class numbers in infinite towers of number fields. This is a very beautiful theorem that uses tools from algebraic number theory and commutative algebra. Personally, it is the theorem that got me interested in this subject.

In number theory, we often study arithmetic objects over a single number field. For example, we might ask the following questions:

QUESTION 1.1. For a given number field K.

(a) What is the class group of K?
(b) Given an elliptic curve E/K, what is the rank of the Mordell-Weil group of E over K?

These questions are often very deep and hard to answer. Iwasawa theory is based on the counter intuitive insight that even though answering these questions over a single number field is hard, answering them over a ***infinite tower*** of number fields is often easier.

$$\{\text{arithmetic objects over a number field}\} \longleftrightarrow$$
$$\{\text{arithmetic objects over an infinite tower of number fields}\}$$

For example, instead of asking: "what is the class group of this number field?", Iwasawa theory would ask, given an infinite tower of number fields $K_1 \subset K_2 \subset K_3 \subset \cdots$. How does the class group of K_n grow as n goes to ∞? Or given an elliptic curve E/K_1, how does the rank of the group $E(K_n)$ grow as n goes to ∞? The fundamental insight of Iwasawa theory is that these growth questions are often easier to answer than their counterparts over single number fields.

The first proof of concept of this philosophy was given by Iwasawa in the following now famous theorem. For an integer $m \geq 1$, let $\mathbb{Q}(\zeta_m)$ denote the m^{th} cyclotomic field.

THEOREM 1.2 (IWASAWA). *Let p be a prime. Consider the tower of cyclotomic fields*

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \mathbb{Q}(\zeta_{p^3}) \subset \mathbb{Q}(\zeta_{p^4}) \subset \cdots$$

Let p^{e_n} be the exact power of p dividing the class number of $\mathbb{Q}(\zeta_{p^n})$. Then there exists integers $\mu, \lambda, \nu \geq 0$ such that $e_n = \mu p^n + \lambda n + \nu$, for all $n \geq 0$.

Why is this theorem so interesting? Well, nobody knows how to compute class groups. The class groups of cyclotomic fields, especially, are basically impossible to calculate by naive methods once the fields get large. So the fact that you can say anything about them is quite amazing. Most people could not calculate the class group of even a single cyclotomic field. Iwasawa arranged them in an infinite tower and calculated their class number in one shot.

Before we proceed, it's worth pointing out what Iwasawa's theorem doesn't tell us. First, the theorem doesn't tell us anything about the group structure of the class groups. It only tells us about the class numbers. Furthermore, it also doesn't tell us the size of the entire class group, only the power of p dividing the class number. Lastly, it doesn't tell us what the integers μ, λ, ν are explicitly; it is a purely abstract result. Even given these caveats, however, Iwasawa's theorem is pretty amazing.

EXAMPLE 1.3. Consider $p = 5$, so we have the number fields

$$\mathbb{Q}(\zeta_5) \subset \mathbb{Q}(\zeta_{5^2}) \subset \mathbb{Q}(\zeta_{5^3}) \subset \mathbb{Q}(\zeta_{5^4}) \subset \cdots$$

It turns out that $\mu = \lambda = \nu = 0$ in Iwasawa's formula. So if 5^{e_n} is the power of 5 dividing the class number of $\mathbb{Q}(\zeta_{5^n})$, we have $e_n = 0$ for all n. In other words, 5 is coprime to the class number of $\mathbb{Q}(\zeta_{5^n})$ for all n.

EXAMPLE 1.4. Now consider $p = 37$, so we have the number fields

$$\mathbb{Q}(\zeta_{37}) \subset \mathbb{Q}(\zeta_{37^2}) \subset \mathbb{Q}(\zeta_{37^3}) \subset \mathbb{Q}(\zeta_{37^4}) \subset \cdots$$

It turns out that $\mu = 0$ and $\lambda = \nu = 1$ in Iwasawa's formula. So if 27^{e_n} is the power of 37 dividing the class number of $\mathbb{Q}(\zeta_{37^n})$, then $e_n = n + 1$ for all $n \geq 0$. That is, the power of 37 dividing the class number of $\mathbb{Q}(\zeta_{37^n})$ grows linearly.

a. *Proof of Iwasawa's Theorem*

The proof of Iwasawa's theorem is incredibly beautiful and it sets up a general strategy for proving growth theorems in infinite towers. In this section, I'll sketch the strategy of the proof, without giving all the details. The full proof is given in Chapter 13 of Lawrence Washington's book "Introduction to Cyclotomic Fields". I highly recommend that you read this chapter because it's beautifully written and it was what first made me fall in love with Iwasawa theory.

The Setup

So the setup is that we have a tower of number fields

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \mathbb{Q}(\zeta_{p^3}) \subset \mathbb{Q}(\zeta_{p^4}) \subset \cdots$$

Let X_n denote the p-Sylow subgroup of the class group $\mathrm{Cl}(\mathbb{Q}(\zeta_{p^n}))$. There is a norm map $N : \mathbb{Q}(\zeta_{p^{n+1}}) \to \mathbb{Q}(\zeta_{p^n})$ and this induces a norm map on the class groups $X_{n+1} \to X_n$ for all n. So, we get the following infinite sequence:

$$\cdots \to X_{n+3} \to X_{n+2} \to X_{n+1} \to X_n \to \cdots$$

where the arrows are the norm maps. Put

$$X_\infty = \varprojlim X_n$$

where the inverse limit is taken with respect to the norm maps. An element of X_∞ is an infinite sequence $(x_1, x_2, x_3, \dots)$ where $x_n \in X_n$ and the norm of x_n is equal to x_{n+1}.

Commutative Algebra

Iwasawa's insight is that even though each X_n is very mysterious, the a priori more complex object X_∞ is actually easier to study. In fact, we can study X_∞ using tools from commutative algebra. To do this, first note that X_n is a $\mathbb{Z}_p$-module because it is p-primary abelian group. Furthermore, X_n has an action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$. Therefore, X_n is a module over the group ring $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})]$.

Taking inverse limits, this means that $X_\infty = \varprojlim X_n$ is a module over the inverse limit of group rings: $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})]$. The first inverse limit is taken with respect to the norm maps on class groups. The second inverse limit is taken with respect to the quotient maps on the Galois groups.

So X_∞ is module over the mysterious ring $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})]$. We will then study the X_∞ using general commutative algebra results about modules over the ring $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})]$. To do this, we will use the following important remark.

Remark 1.5. There is an isomorphism of $\mathbb{Z}_p$-modules: $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})] \cong \mathbb{Z}_p[\![T]\!]$, where $\mathbb{Z}_p[\![T]\!]$ is the ring of formal power series in T with coefficients in $\mathbb{Z}_p$.

From now on, the only fact we will remember is this: X_∞ is a $\mathbb{Z}_p[\![T]\!]$-module. Our main input will be the below structure theorem from commutative algebra.

Structure Theorem

Put $\Lambda = \mathbb{Z}_p[\![T]\!]$. We'll now give a structure theorem for finitely-generated Λ-modules that is reminiscent of the structure theorem of finitely generated modules over a PID. There are two things that we need to state the theorem:

(a) A polynomial $f \in \Lambda$ is distinguished if when you reduce it mod p, only the highest degree term remains.
(b) If M_1 and M_2 are Λ-modules, then a pseudo-isomorphism is a map $M_1 \to M_2$ with finite kernel and cokernel. If there is such a pseudo-isomorphism, then we write $M_1 \sim M_2$.

Theorem 1.6 (Structure Theorem for Λ-modules by Iwasawa-Serre). *Let M be a finitely-generated torsion Λ-module. Then there is a pseudo-isomorphism*

$$M \sim \bigoplus_{i=1}^{n} \frac{\Lambda}{p^{e_i}} \oplus \bigoplus_{j=1}^{m} \frac{\Lambda}{f_j}$$

where the f_j are distinguished polynomials.

One can show that X_∞ is indeed finitely-generated and torsion, so the structure theorem gives us a pseudo-isomorphism:

$$X_\infty \sim \bigoplus_{i=1}^{n} \frac{\Lambda}{p^{e_i}} \oplus \bigoplus_{j=1}^{m} \frac{\Lambda}{f_j}$$

where the f_j are distinguished polynomials.

Going from $X_\infty \to X_n$

We now have an abstract result about X_∞. How do we extract information about the structure of X_n? Our key will be the following fact:

Proposition 1.7. *There is an isomorphism of Λ-modules: $X_\infty/((1+T)^{p^n}-1) \cong X_n$.*

This proposition is hugely important because it allows us to recover $X_n \to X_\infty$. It tells us that to calculate $|X_n|$, it is enough to calculate $|X_\infty/((1+T)^{p^n}-1)|$ for all n. We will do this using the structure theorem. Given that we have a pseudo-isomorphism:

$$X_\infty \sim \bigoplus_{i=1}^{n} \frac{\Lambda}{p^{e_i}} \oplus \bigoplus_{j=1}^{m} \frac{\Lambda}{f_j}$$

let's compute the right-hand side of the above equation modulo $(1+T)^{p^n}-1$.

(a) First, we have

$$\left| \left(\bigoplus_{i=1}^{n} \frac{\Lambda}{p^{e_i}} \right) / ((1+T)^{p^n}-1) \right| = p^{(\sum_{i=1}^{n} e_i) p^n}$$

(b) Next, we have

$$\left|\left(\bigoplus_{j=1}^{m}\frac{\Lambda}{f_j}\right)/((1+T)^{p^n}-1)\right| = p^{(\sum_{j=1}^{m} f_j)n}$$

One can show that the "pseudo-isomorphism" gives us a factor of p^ν for some constant ν. So in total, we get that

$$|X_n| = |X_\infty/((1+T)^{p^n}-1)| = p^{(\sum_{i=1}^{n} e_i)p^n+(\sum_{j=1}^{m} f_j)^{n+\nu}}$$

Putting $\mu = \sum_{i=1}^{n} e_i$ and $\lambda = \sum_{j=1}^{m} f_j$, we get $|X_n| = p^{\mu p^n+\lambda n+\nu}$ for all $n \geq 0$. This proves Iwasawa's theorem.

2 p-adic L-functions

In this section, we introduce p-adic L-functions, which are a key ingredient in the analytic side of Iwasawa theory. Specifically, it talks about the Kubota-Leopoldt p-adic L-function and its interpolation properties.

Many problems in modern number theory revolve around the following theme: relate arithmetic objects to special values of L-functions

$$\{\text{arithmetic objects}\} \longleftrightarrow \{\text{complex } L\text{-functions}\}$$

For example, on the left side, we might want to study the class group of a number field and on the right side, we might want to study values of Dirichlet L-functions. The bridge linking them is the class number formula.

As an another example, on the left side, we might want to study the rank of an elliptic curve and on the right side, we might want to study the Hasse Weil L-function of that elliptic curve. The bridge linking them is the Birch and Swinnerton-Dyer formula.

The problem with proving these theorems is that the left side is arithmetic, while the right side is analytic. So they are very "far" and it is hard to relate them. A crucial tool in relating them is to use an intermediary object called a "***p-adic L-function***".

$$\{\text{arithmetic objects}\} \longleftrightarrow \{p\text{-adic } L\text{-functions}\} \longleftrightarrow \{\text{complex } L\text{-functions}\}$$

This p-adic L-function (whatever it is) should straddle the worlds of arithmetic and analysis. On one hand, it should know "analytic" information from the complex function. On the other hand, it should also be "algebraic" in nature, which would make it easier to relate to arithmetic objects than the purely complex L-functions.

This approach has been immensely successful in proving, for example, big results in the direction of the Birch and Swinnerton Dyer Conjecture. The breakthrough results of Kato and Skinner-Urban about BSD rely critically on the notion of p-adic L-functions. And it's almost certain that p-adic L-functions will play a huge role in proving "arithmetic-analytic" theorems in the future.

In this section, I'll explain the simplest example of a p-adic L-function, the Kubota-Leopoldt p-adic L-function, to illustrate the basic ideas behind it. I'll also give a hint about its relation to arithmetic, which is the so-called ***Iwasawa main conjecture***.

a. *Congruences between zeta values*

The Kubota-Leopoldt p-adic L-function (whatever it is) "p-adically interpolates" special values of the Riemann zeta function. Consider the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. The fundamental observation, first observed by Kummer, is that the values of $\zeta(s)$ at negative integers satisfy interesting congruences.

EXAMPLE 2.1. In both these examples, we set $p = 5$. Set $s_1 = -1$ and $s_2 = -21$. We have the congruence $-1 \equiv -21 \pmod 5$. We can calculate $\zeta_5(s_1) = \frac{1}{3}$ and $\zeta_5(s_2) = \frac{9260535240173320423}{69}$, and it turns out that $\zeta_5(-1) \equiv \zeta_5(-21) \pmod{5^2}$.

As another example, put $s_1 = -1$ and $s_2 = -101$. Then $-1 \equiv -101 \pmod{5^2}$. And we can calculate that $\zeta(-1) \equiv \zeta(-101) \pmod{5^3}$. These can be phrased as a rigorous theorem.

THEOREM 2.2 (KUMMER). *Let p be a prime and let $\zeta_p(s) = (1 - p^{-s})\zeta(s)$ be the Riemann zeta function with the Euler factor at p removed. Define the set*

$$S = \{s \in \mathbb{Z}_{<0} : s \equiv -1 \pmod{p-1}\}$$

Then for any $s_1, s_2 \in S$, we have

$$s_1 \equiv s_2 \pmod{p^n} \Rightarrow \zeta_p(s_1) \equiv \zeta_p(s_2) \pmod{p^{n+1}}$$

We can phrase this in a more suggestive way: the function $\zeta_p(s)$ is p-adically continuous on the set $S \subset \mathbb{Z}$.

b. *The connection to p-adic L-functions*

Here is a very simple observation: the set S defined above is dense in $\mathbb{Z}_p$. So we have a continuous function $\zeta_p : S \to \mathbb{Z}_p$ defined on a dense subset S of $\mathbb{Z}_p$. So we can ask: can we extend ζ_p to a continuous function to all of $\mathbb{Z}_p$? That is, can we define a continuous function $\mathbb{Z}_p \to \mathbb{Z}_p$ whose restriction to S agrees with ζ_p?

It turns out that the answer is yes! And furthermore, not only does such an extension exist, it is also unique. This was proven by Kubota and Leopoldt.

THEOREM 2.3 (KUBOTA-LEOPOLDT). *There is a unique continuous function $\zeta_p : \mathbb{Z}_p \to \mathbb{Z}_p$ which extends the function ζ_p defines on S defined earlier. That is, for any $s \in S$, we have $\zeta_p(s) = (1 - p^{-s})\zeta(s)$.*

DEFINITION 2.4. The function $\zeta_p : \mathbb{Z}_p \to \mathbb{Z}_p$ in the above theorem is called the p-adic Riemann zeta function, or the Kubota-Leopoldt p-adic zeta function.

c. *Analogy*

What we have just done is a p-adic analogue of the process of analytic continuation for complex L-functions. In the complex story, we define an L-function on a right half of the complex plane, and we show that we can extend it via analytic continuation to the entire complex plane. We then show that this extension is unique.

In our case, we define a p-adically continuous function ζ_p on a set S, and then we "analytically continue" ζ_p to all of $\mathbb{Z}_p$. We then show that this extension is unique. We call this function the Kubota-Leopoldt p-adic L-function.

d. *The General Definition of the Kubota-Leopoldt p-adic zeta function*

You might have noticed that when we wrote down Kummer's Theorem about congruences of the zeta function, we defined the set S as

$$S = \{s \in \mathbb{Z}_{<0} : s \equiv -1 \pmod{p-1}\}$$

But why -1 in particular in the above definition? There is nothing special about -1 here; we could define for any $i = -1, -3, -5, \ldots$, the set

$$S_i = \{s \in \mathbb{Z}_{<0} : s \equiv i \pmod{p-1}\}$$

Note that what we originally called S is just S_i in the case where $i = -1$. For the sets S_i, we have an analogous form of Kummer's theorem.

THEOREM 2.5 (KUMMER). *Let p be a prime and let $\zeta_p(s) = (1 - p^{-s})\zeta(s)$ be the Riemann zeta function with the Euler factor at p removed. Then for any $i = -1, -3, -5, \ldots$, the function $\zeta_p : S_i \to \mathbb{Z}_p$ is p-adically continuous on S_i.*

And just like before, S_i is dense subset of $\mathbb{Z}_p$, and we can extend ζ_p to a continuous function on all of $\mathbb{Z}_p$.

THEOREM 2.6 (KUBOTA-LEOPOLDT). *There is a unique continuous function $\zeta_p^{(i)} : \mathbb{Z}_p \to \mathbb{Z}_p$ which extends the function ζ_p defined on S_i defined earlier.*

This function $\zeta_p^{(i)}$ is called the ***i^{th} branch of the Kubota-Leopoldt zeta function***. The zeta function ζ_p we defined in the previous section was the branch corresponding to $i = -1$.

e. *Why do we do this?*

So who cares about p-adic zeta functions? A priori, they are just numerical curiosities. It turns out, however, that p-adic zeta functions encode very deep arithmetic information: they "know" about the class groups of cyclotomic fields. This is the content of a very deep theorem called the ***Iwasawa Main Conjecture***.

$$\{p\text{-adic zeta function}\} \xleftrightarrow{\text{Iwasawa Main Conjecture}} \{\text{class groups of cyclotomic fields}\}$$

The left side is analytic; it is constructed by p-adically interpolating special values of the Riemann zeta function. The right side is algebraic; it is group that measures the failure of unique factorization in a number ring. The Iwasawa main conjecture (whatever it is) gives a profound connection between the analytic and algebraic sides of number theory.

It turns out that $\zeta_p^{(i)}$, the i^{th} branch of the Kubota-Leopoldt p-adic zeta function, encodes information about the χ^i-th eigenspaces of the class groups of cyclotomic fields, where χ is the cyclotomic character. (This is why we need all the branches of the p-adic L-function in the first place.)

I won't say more now, because this connection is discussed in more detail and properly motivate and state the main conjecture in 3.

3 The Iwasawa Main Conjecture

In this section, we draw the link between the algebraic side of Iwasawa theory and the analytic side of Iwasawa theory. These two worlds are connected via the so-called "Iwasawa main conjecture".

The Iwasawa main conjecture is a deep connection between two objects: class groups of cyclotomic fields and special values of the Reimann zeta function. The former object is algebraic: it is a class group of a number field. The latter is analytic: it is the value of a complex function at certain special points. The main conjecture, therefore (whatever it is), spells out an interesting connection between an algebraic and an analytic object.

a. *Kummer's Theorem*

The first indication that such a connection might exist is a theorem of Kummer.

THEOREM 3.1 (KUMMER). *Let p be a prime number. Then p divides the class number of $\mathbb{Q}(\zeta_p)$ if and only if p divides the numerator of $\zeta(r)$ for some integer $r = -1, -3, -5, \ldots$.*

EXAMPLE 3.2. As an example, set $p = 691$. Then 691 divides the numerator of $\zeta(-11) = \frac{691}{32760}$. So Kummer's theorem tells us that 691 divides the class number of $\mathbb{Q}(\zeta_{691})$. This is already quite interesting because calculating class numbers by hand is basically impossible. This theorem says that the Riemann zeta function can be used to obtain this information in a different way.

But what is the meaning of -11 in $\zeta(-11)$? It turns out that -11 encodes the Galois action on the class group of $\mathbb{Q}(\zeta_{691})$. Precisely, the class group $\mathrm{Cl}(\mathbb{Q}(\zeta_{691}))$ has a natural action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{691})/\mathbb{Q})$. And this Galois group acts on $\mathrm{Cl}(\mathbb{Q}(\zeta_{691}))$ via χ^{-11}, where χ is the cyclotomic character. In other words, we have an inclusion of Galois modules

$$\mathrm{Cl}(\mathbb{Q}(\zeta_{691})) \supset (\mathbb{Z}/691\mathbb{Z})(-11)$$

where the (-11) means that Galois acts via χ^{-11}.

b. *Herbrand-Ribet Theorem*

This example actually holds in general, and this was proved by Herbrand and Ribet.

THEOREM 3.3 (HERBRAND-RIBET). *Let p be a prime number and let $r = -1, -3, -5, \ldots$. Then $\mathrm{Cl}(\mathbb{Q}(\zeta_p)) \supset (\mathbb{Z}/p\mathbb{Z})(-r)$ if and only if $p \mid \zeta(r)$.*

The slogan here is:

$$\text{zeta value} = \text{class group with Galois action}$$

It actually turns out that much more is true. To see that, I'll rephrase the Herbrand-Ribet Theorem above as follows. Let $\mathrm{Cl}^{(r)}(\mathbb{Q}(\zeta_p))$ be the χ^r-eigenspace of $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ (i.e., it is the subgroup of $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ where Galois acts via χ^r). Then Herbrand-Ribet equivalently says:

THEOREM 3.4. *Let p be a prime number and let $r = -1, -3, -5, \ldots$. Then*

$$ord_p(\#\,\mathrm{Cl}^{(r)}(\mathbb{Q}(\zeta_p))) > 0$$

if and only if $ord_p(\zeta(-r)) > 0$.

In truth, however, it turns out that the ord_p of both sides are in fact equal. That is, one can show that

$$\mathrm{ord}_p(\#\,\mathrm{Cl}^{(r)}(\mathbb{Q}(\zeta_p))) = \mathrm{ord}_p(\zeta(-r))$$

This however is much harder to prove, and requires the full strength of the Iwasawa main conjecture. In that sense, the Iwasawa main conjecture (whatever it is) is a strengthening of the Herbrand-Ribet Theorem.

c. *The Iwasawa Main Conjecture*

To state the Iwasawa main conjecture, we have to do something which is a signature of Iwasawa theory: we have to state the formulate Herbrand-Ribet theorem in infinite towers. On the algebraic side, instead of looking at just one class group, look at class groups in an infinite tower of cyclotomic fields. On the analytic side, instead of looking at just one zeta value, we will look at infinitely many zeta values are p-adically interpolate them into a p-adic L-function.

THE ALGEBRAIC SIDE

For Herbrand-Ribet, we considered the group $\mathrm{Cl}^{(r)}(\mathbb{Q}(\zeta_p))$, which is the χ^r eigenspace of the class group of $\mathbb{Q}(\zeta_p)$. Now we will do everything in $\mathbb{Z}_p$-extensions.

Consider the $\mathbb{Z}_p$-extensions $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)$ with layers given by:

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \mathbb{Q}(\zeta_{p^3}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty})$$

The for every $n \geq 0$, consider we can consider the χ^r-eigenspace $\mathrm{Cl}^{(r)}(\mathbb{Q}(\zeta_{p^n}))$. The central object of study will be the inverse limit of these groups:

$$X_\infty^{(r)} = \varprojlim_n \mathrm{Cl}^{(r)}(\mathbb{Q}(\zeta_{p^n}))$$

Then $X_\infty^{(r)}$ is a module over $\Lambda = \mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p))]\!]$. And $X_\infty^{(r)}$ is also finitely generated and torsion as a Λ-module. There is a non-canonical isomorphism $\Lambda \cong \mathbb{Z}_p[\![T]\!]$. So by the structure theorem for finitely generated torsion Λ-modules, we have a pseudoisomorphism:

$$X_\infty^{(r)} \sim \bigoplus_{i=1}^{n} \frac{\Lambda}{p^{e_i}} \oplus \bigoplus_{j=1}^{m} \frac{\Lambda}{f_j}$$

where the $f_j \in \mathbb{Z}_p[\![T]\!]$ are distinguished polynomials (i.e., a polynomial $f \in \mathbb{Z}_p[\![T]\!]$ is distinguished if when you reduce it mod p, only the highest degree term remains).

The two quantities of interest:

(a) Define the μ-invariant to be $\mu = e_1 + \cdots + e_n$.
(b) Define the λ-invariant to be $\lambda = \deg f_1 + \cdots + \deg f_m$.

Then we have Iwasawa's growth formula: there is an integer $\nu \geq 0$ such that

$$|\operatorname{Cl}^{(r)}(\mathbb{Q}(\zeta_{p^n}))| = p^{\mu p^n + \lambda n + \nu}$$

for all $n \geq 0$. So the quantities μ and λ in the structure theorem have a concrete meaning in terms of class numbers of the intermediate layers of the tower.

We can wrap up μ and λ in a quantity called the ***characteristic ideal***.

DEFINITION 3.5. The characteristic ideal of $X_\infty^{(r)}$ is defined as:

$$\operatorname{char} X_\infty^{(r)} = (p^{e_1 + \cdots + e_n} f_1 \cdots f_m) \subset \mathbb{Z}_p[\![T]\!]$$

That is, you take all the "denominators" in the structure theorem, multiply them together. The ideal generated by that element in $\mathbb{Z}_p[\![T]\!]$ is the characteristic ideal. Note that we can recover μ and λ from the characteristic ideal.

THE ANALYTIC SIDE

On the algebraic side, we looked at infinitely many number fields and "strung together" their class groups by taking an inverse limit. On the analytic side we will look at infinitely many zeta values and we will string them together by p-adically interpolating them. Doing this will create a p-adic L-function, which is the main object of the analytic side of the main conjecture.

We discussed p-adic L-function in detail in section 2. I'd definitely recommend reading that section first before coming here. For here, I'll just recall the main theorem from that section, which proves the existence and uniqueness of the p-adic Riemann zeta function.

THEOREM 3.6 (KUBOTA-LEOPOLDT). *Let p be a prime, and let $r = -1, -3, -5, \ldots$ be a negative odd integer. There exists a unique p-adically continuous function $\zeta_p^{(r)} : \mathbb{Z}_p \to \mathbb{Z}_p$ with the following interpolation property: Define the set $S_r = \{n \in \mathbb{Z}_{<0} : n \equiv r \pmod{p-1}\}$. Then for all $s \in S_r$, we have*

$$\zeta_p(s) = (1 - p^{-s})\zeta(s)$$

*This function is called the **(r^{th} branch of the) Kubota-Leopoldt p-adic zeta function**. The set S_r consists of the "points of interpolation" of $\zeta_p^{(r)}$. At these points, the function $\zeta_p^{(r)}$ coincides with the Riemann zeta function with the Euler factor at p removed.*

If any of this feels unfamiliar, check out section 2 where I explained this theorem much more slowly.

The Iwasawa main conjecture relates the module $X_\infty^{(r)}$ to the p-adic L-function $\zeta_p^{(r)}$:

$$X_\infty^{(r)} \xleftrightarrow{\text{Iwasawa Main Conjecture}} \zeta_p^{(r)}$$

The problem is that these two objects live in different worlds: the module $X_\infty^{(r)}$ is an object from commutative algebra whereas $\zeta_p^{(r)}$ is a p-adic analytic function. So it's not even clear how to state a precise conjecture relating them. It was Iwasawa who realized that $\zeta_p^{(r)}$ can be expressed as a power series in $\mathbb{Z}_p[\![T]\!]$, which will allow us to view it as an object in commutative algebra.

THEOREM 3.7 (IWASAWA). *Let p be a prime and let $r = -1, -3, -5, \ldots$ be an odd negative integer. Then there is a unique power series $\zeta(T) \in \mathbb{Z}_p[\![T]\!]$ satisfying*

$$G_r((1+p)^s - 1) = \zeta_p^{(r)}(s)$$

for all $s \in \mathbb{Z}_p$.

By abuse of notation, we also call $G_r(T)$ the (r^{th} branch of the) Kubota-Leopoldt p-adic zeta function. We will no longer think of the p-adic zeta function as a literal function $\mathbb{Z}_p \to \mathbb{Z}_p$, but we will view it as a power series in $\mathbb{Z}_p[\![T]\!]$.

THE MAIN CONJECTURE

On the algebraic side, we have the characteristic ideal $\text{char}(X_\infty^{(r)})$. On the analytic side, we have the p-adic zeta function $G_i(T)$. We can look at the ideal $(G_i(T)) \subset \mathbb{Z}_p[\![T]\!]$ generated by this p-adic zeta function. The main conjecture asserts that these two ideals are equal.

CONJECTURE 3.8 (IWASAWA MAIN CONJECTURE). *Let p be a prime and let $r = -1, -3, -5, \ldots$ be a negative odd integer. Then:*

$$char(X_\infty^{(r)}) = (G_r(T))$$

When I first saw this, I understood basically nothing. So I want to take it apart a bit to understand it better. First, I found it helpful to phrase this in terms of power series instead of ideals. We had a pseudo-isomorphism:

$$X_\infty^{(r)} \sim \bigoplus_{i=1}^{n} \frac{\Lambda}{p^{e_i}} \oplus \bigoplus_{j=1}^{m} \frac{\Lambda}{f_j}$$

Also, by the Weierstrass preparation theorem, we can factor $G_r(T)$ as

$$G_r(T) = p^k u(T) f(T)$$

where $u(T)$ is a unit and $f(T)$ is a distinguished polynomial.

CONJECTURE 3.9 (POWER SERIES FORMULATION OF IMC). *We have*

$$p^{e_1+\cdots+e_n} f_1 \cdots f_m \sim G_r(T)$$

where $\sim$ indicates equality upto a unit in $\mathbb{Z}_p[\![T]\!]$. In particular, $e_1 + \cdots + e_n = k$ and $f_1 \cdots f_m \sim f$.

This might seem kind of opaque (I definitely thought so at first), but it has a very concrete consequence about μ and λ-invariants. To see it, let's remember Iwasawa's growth formula: there is an integer $\nu \geq 0$ such that

$$|\operatorname{Cl}^{(r)}(\mathbb{Q}(\zeta_{p^n}))| = p^{\mu p^n + \lambda n + \nu}$$

for all $n \geq 0$. The main Iwasawa conjecture then implies that:

(a) The quantity μ in the above formula is the power of p dividing $G_r(T)$.
(b) And the quantity λ in the above formula is the degree of the of p dividing $G_r(T)$.

So we can read off μ and λ right from the p-adic zeta function. This is really weird! The p-adic zeta-function interpolates special values of the Riemann zeta function. Why on earth should we be able to read off μ and λ-invariants for class groups from these zeta functions?

d. *The Main Conjecture is now a theorem!*

Regardless of how mysterious the statement is, Mazur and Wiles were actually able to prove the main conjecture in a brilliant 1984 Inventiones paper.

THEOREM 3.10 (MAZUR-WILES). *The Iwasawa Main Conjecture is true.*

4 Kato's Euler System

In this section, we describe the construction of Kato's Euler system, which was used to prove one direction of the Iwasawa main conjecture for modular forms. Kato's Euler System is a technical tool that was used to prove many deep results in the direction of the BSD conjecture. It was developed in Kato's 2004 Asterisque Paper. This paper is a 100+ page tour de force and would easily take several years to study fully. The purpose of this section is to give a high level overview of the main ideas of the paper.

a. *What is an Euler System?*

Many problems in modern number theory revolve around the following theme: relate Galois cohomology classes to special values of L-functions

$$\{\text{Galois cohomology}\} \longleftrightarrow \{\text{special values of } L\text{-functions}\}$$

EXAMPLE 4.1. For example, suppose you have an elliptic curve $E/\mathbb{Q}$. On the left side of the diagram, you might want to study the Selmer group of E over $\mathbb{Q}$. This is a group defined using Galois cohomology that essentially controls the arithmetic of E. On the right side, you might want to study the Hasse-Weil L-function $L(E,s)$. Relating these two objects would give deep results in the direction of BSD.

An Euler System, simply put, is an object that links these two worlds. It is a technical tool that allows you to link Galois cohomology groups to special values of L-functions.

$$\{\text{Galois cohomology}\} \overset{\text{Euler Systems}}{\longleftrightarrow} \{\text{special values of } L\text{-functions}\}$$

Kato developed an Euler system and used it to prove the following amazing result (among many other results):

THEOREM 4.2 (KATO). *Let $E/\mathbb{Q}$ be an elliptic curve, and let $L(E,s)$ be the Hasse-Weil L-function of E. If $E(\mathbb{Q})$ is infinite, then $L(E,1)=0$.*

In other words, "positive algebraic rank implies positive analytic rank." In the rest of the section, I will describe what Kato's Euler system is.

b. *Kato's Euler System*

Setup

For us, E will be an elliptic curve over $\mathbb{Q}$ and p will be a prime of good reduction. We will $T_pE = \varprojlim_n E[p^n]$ for the tate module of E. So, T_pE is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, i.e., $T_pE \cong \mathbb{Z}_p \times \mathbb{Z}_p$, as an abelian group and it has an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Now define

$$V_pE = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

Then V_pE is a two-dimensional $\mathbb{Q}_p$-vector space with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ inherited from the first factor T_pE of the tensor product. (We write V_pE because the V stands for Vector space).

Kato's Euler System - the bottom layer

Kato considers the Galois cohomology group $H^1(\mathbb{Q}, V_pE)$. With this group, Kato does two things.

(a) First, Kato defines a class $z^{\mathrm{Kato}} \in H^1(\mathbb{Q}, V_pE)$ called the ***Kato class***.

(b) Second, Kato defines a very mysterious map called the dual exponential map:

$$\exp^* : H^1(\mathbb{Q}_p, V_pE) \to \mathbb{Q}_p\omega_E$$

which is defined using p-adic Hodge theory. We will not define explicitly and treat like a black box. Here ω_E is the invariant differential on E.

Now let $\mathrm{res}_p : H^1(\mathbb{Q}, V_pE) \to H^1(\mathbb{Q}_p, V_pE)$ denote the restriction map. Kato showed that

$$\exp^*(\mathrm{res}_p(z^{\mathrm{Kato}})) = \frac{L_{\{p\}}(E,1)}{\Omega_E}\omega_E$$

The function $L_{\{p\}}(E,s)$ is the L-function $L(E,s)$ with the p^{th} Euler Factor removed. And Ω_E is the real Neron period of E. This identity is called the ***explicit reciprocity law***.

Kato's Euler System - the other layers

Kato realized that this class z^{Kato} is not alone, but is just the first class in an entire infinite collection of classes that interpolate L-values in different ways.

For each prime power p^m, consider the cohomology group $H^1(\mathbb{Q}(\zeta_{p^m}), V_pE)$. Kato defined a class $z^{\mathrm{Kato}} \in H^1(\mathbb{Q}(\zeta_{p^m}), V_pE)$. Kato also defined a dual exponential map using p-adic Hodge theory:

$$\exp^* : H^1(\mathbb{Q}(\zeta_{p^m}), V_pE) \to \mathbb{Q}_p(\zeta_{p^m})\omega_E$$

The explicit reciprocity law here says: for any Dirichlet character $\chi : (\mathbb{Z}/p^m)^\times \to \mathbb{C}^\times$ of conductor p^m, we have

$$\exp^*\left(\sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p)} \mathrm{res}_p(z^{\mathrm{Kato}}_{p^m})^\sigma\right) = \frac{L_{\{p\}}(E,\chi,1}{\Omega_E^{\pm}}\omega_E$$

Here $\mathrm{res}_p : H^1(\mathbb{Q}(\zeta_p), V_pE) \to H^1(\mathbb{Q}_p(\zeta_p), V_pE)$ denotes the restriction map. The periods Ω_E^+ and Ω_E^- are the real and imaginary periods of E, respectively.

KATO'S EULER SYSTEM - THE WHOLE THING

The collection of classes $\{z_{p^m}^{\text{Kato}}\}_{m\geq 1}$ called ***Kato's Euler System***. The class $z_{p^m}^{\text{Kato}}$ is the p^m***-th layer*** of Kato's Euler System.

Ok, this is a bit of a lie. Kato actually defined classes z_m^{Kato} for every integer $m \geq 1$, not just prime powers p^m. But we only need the layers which are prime powers, so that's not a problem for us.

c. *Construction of Kato's Euler System*

In this section, I'll describe the construction of the ***bottom class*** of Kato's Euler system, the element $z^{\text{Kato}} = z_{p^0}^{\text{Kato}} \in H^1(\mathbb{Q}, V_pE)$.

MODULARITY

Since every elliptic curve over $\mathbb{Q}$ is modular, there exists a modular parametrization $X_0(N) \to E$, where N is the conductor of E. Compose this with the natural surjection $X_1(N) \to X_0(N)$, to get a map

$$X_1(N) \to E$$

This induces a map on the Jacobians: $J_1(N) \to E$. This is turn induces a map on their Tate modules: $T_p(J_1(N)) \to T_pE$. Tensoring with $\mathbb{Q}_p$, we get a Galois equivariant:

$$V_p(J_1(N)) \to V_pE$$

This induces a map on Galois cohomology, so we get a map which I'll call (a):

$$H^1(\mathbb{Q}, V_p(J_0(N))) \xrightarrow{(a)} H^1(\mathbb{Q}, V_pE)$$

ÉTALE COHOMOLOGY

There is an isomorphism of $G_{\mathbb{Q}}$-modules:

$$H^1_{\text{et}}(\overline{Y_1(N)}, \mathbb{Q}_p(Q)) \xrightarrow{\sim} V_p(J_1(N))$$

where H^1_{et} denotes the etale cohomology group and $\overline{Y_1(N)}$ is the base-change of $Y_1(N)$ to $\overline{\mathbb{Q}}$. This induces a map on Galois cohomology which we denote (b):

$$H^1(\mathbb{Q}, H^1_{\text{et}}(\overline{Y_1(N)}, \mathbb{Q}_p(1))) \xrightarrow{(b)} H^1(\mathbb{Q}, V_p(J_1(N)))$$

A SPECTRAL SEQUENCE

The next step is to use a spectral sequence to get a map from $H^2 \to H^1(\mathbb{Q}, H^1(\cdots))$. Precisely, consider the spectral sequence

$$E_2^{i,j} = H^i(\mathbb{Q}, H^j_{\text{et}}(\overline{Y_1(N)}, -)) \Rightarrow H^{i+j}(Y_1(N), -)$$

And use a fact from étale cohomology: $H^i_{\text{et}}(C, -) = 0$ for $i \geq 2$ whenever C is an affine curve over an algebraically closed field. Combining these two facts (I do not know spectral sequences, so have not (and don't know how to) verify this fact. Kato says that you get this map, so I'm taking it for granted), I am told that one obtains a map:

$$H^2(Y_1(N), \mathbb{Q}_p(1)) \xrightarrow{(c)} H^1(\mathbb{Q}, H^1_{\text{et}}(\overline{Y_1(N)}, \mathbb{Q}_p(1)))$$

Crucially, in the domain of the map (c), we consider the curve $Y_1(N)$ over $\mathbb{Q}$, whereas in the target, we consider $Y_1(N)$ base-changed to the algebraic closure $\overline{\mathbb{Q}}$. So the group $H^2(Y_1(N), \mathbb{Q}_p(1))$ does not have a Galois action. The benefit, therefore, of working over $\mathbb{Q}$ is that we can use tools from geometry (namely, the Kummer map) to produce classes in $H^2(Y_1(N), \mathbb{Q}_p(1))$.

Then we are going to apply a Tate twist to get a map (d):

$$H^2(Y_1(N), \mathbb{Q}_p(2)) \xleftarrow{(d)} H^2(Y_1(N), \mathbb{Q}_p(1))$$

Cup Product

There is a cup-product map in étale cohomology:

$$H^1(Y_1(N), \mathbb{Q}_p(1)) \times H^1(Y_1(N), \mathbb{Q}_p(1)) \xrightarrow{(e)} H^2(Y_1(N), \mathbb{Q}_p(2))$$

A useful mnemonic: when you apply the cup product, you add the twists (so $\mathbb{Q}_p(1)$ and $\mathbb{Q}_p(1)$ becomes $\mathbb{Q}_p(2)$) and add the degrees (so $H^1 \times H^1$ becomes H^2).

The Kummer Map

The Kummer Map is a map $\kappa : \mathcal{O}(Y_1(N))^\times \to H^1(Y_1(N), \mathbb{Q}_p(1))$. Applying the map $\kappa \times \kappa$, we obtain a map (f):

$$(\mathcal{O}(Y_1(N))^\times)^2 \xrightarrow{(f)} H^2(Y_1(N), \mathbb{Q}_p(1))^2$$

Putting it all together

Composing the maps (a) through (f), we have

$$\begin{aligned}(\mathcal{O}(Y_1(N))^\times)^2 &\xrightarrow{(f)} H^2(Y_1(N), \mathbb{Q}_p(1))^2 \\ &\xrightarrow{(e)} H^2(Y_1(N), \mathbb{Q}_p(2)) \\ &\xrightarrow{(d)} H^2(Y_1(N), \mathbb{Q}_p(1)) \\ &\xrightarrow{(c)} H^1(\mathbb{Q}, H^1_{\text{et}}(\overline{Y_1(N)}, \mathbb{Q}_p(1))) \\ &\xrightarrow{(b)} H^1(\mathbb{Q}, V_p(J_1(N))) \\ &\xrightarrow{(a)} H^1(\mathbb{Q}, V_pE)\end{aligned}$$

This is confusing! To recap, the maps are given as follows:

- (a) is induced by the map $V_p(J_1(N)) \to V_p(E)$,
- (b) is induced by the isomorphism $H^1_{\text{et}}(\overline{Y_1(N)}, \mathbb{Q}_p(1)) \cong V_p(J_1(N))$,
- (c) comes from a certain spectral sequence,
- (d) is a twist,
- (e) is the cup-product map in étale cohomology, and
- (f) is the (square of the) Kummer map.

To produce an element of $H^1(\mathbb{Q}, V_pE)$, Kato defines an explicit element of $(\mathcal{O}(Y_1(N))^\times)^2$ and lets z^{Kato} be its image under the maps (a) through (f).

Kato-Seigel Units

Elements of $\mathcal{O}(Y_1(N))^\times$ are called ***modular units***, and we can write some of them down using nothing but classical 19th century elliptic function theory.

Definition 4.3. Let $N \geq 1$ and $0 \geq a, b < n$ be integers. For each pair $\left(\frac{a}{M}, \frac{b}{M}\right) \in \mathbb{Q}^2 \setminus (0,0)$, define the function $g_{\frac{a}{M},\frac{b}{M}} : \mathbb{H} \to \mathbb{C}$ as follows:

$$g_{\frac{a}{M},\frac{b}{M}}(z) = q^w \prod_{n=0}^{\infty} \left(1 - q^{n+a/N}\zeta_N^b\right) \prod_{n=1}^{\infty} (1 - q^{n-a/N}\zeta_N^{-b})$$

where $q = e^{2\pi iz}$ and $w = \frac{1}{12} - \frac{a}{N} + \frac{a^2}{2N^2}$.

This is well-defined (independent of the choice of common denominator N). We would like to say that it is modular of level N, but this is not quite true. Acting on it by an element of $\Gamma(N)$ multiplies it by a root of unity so it defines an element of $\mathcal{O}(Y(N)) \otimes_{\mathbb{Z}} \mathbb{Q}$. We can kill the denominator by making a very simple modification:

Definition 4.4. Let $c > 1$ be an integer coprime to $6N$. Put

$${}_cg_{\frac{a}{N},\frac{b}{N}} = \frac{\left(g_{\frac{a}{N},\frac{b}{N}}\right)^{c^2}}{g_{\frac{ca}{N},\frac{cb}{N}}}$$

Then ${}_cg_{\frac{a}{N},\frac{b}{N}}$ is $\Gamma(N)$-invariant so it belongs to $\mathcal{O}(Y(N)_{\mathbb{C}})^\times$.

However, we can do better: it actually descends to the number field $\mathbb{Q}(\zeta_N)$. Since the affine curve $Y(N)$ is defined over $\mathbb{Q}(\zeta_N)$, we have:

Proposition 4.5. *The units ${}_cg_{\frac{a}{N},\frac{b}{N}}$ belong to $\mathcal{O}(Y(N))^\times$.*

Definition of z^{Kato} (Wrong version)

I say "wrong version" because this is morally correct and conveys the overall idea, but is technically false. The basic idea is that Kato picks parameters M, N appropriately and gets a pair of modular units ${}_cg_{\frac{1}{M},0}, {}_dg_{0,\frac{1}{N}}$ in $(\mathcal{O}(Y_1(N))^\times)^2$. Then Kato lets z^{Kato} be its image under the maps (a) through (f).

DEFINITION OF z^{KATO} (CORRECT VERSION)

The full details here are very overwhelming (at least I found them so). From this point onwards, I'm skipping over a bunch of technical details to get the main point across. If you'd like technical details, then I'd suggest looking Sections 2 and 5 of Kato's paper as a reference.

Kato fixes two integers $c, d > 1$ such that $\gcd(cd, 6N) = 1$. He considers a pair of Seigel units $({}_c g_{\frac{1}{M},0}, {}_d g_{0,\frac{1}{N}})$ where M, N are chosen appropriately. After doing this, Kato obtains an element which he denotes ${}_{c,d}z_{M,N} = ({}_c g_{\frac{1}{M},0}, {}_d g_{0,\frac{1}{N}})$. This element ${}_{c,d}z_{M,N}$ belongs to $(\mathcal{O}(Y(M,N))^\times)^2$, where $Y(M,N)$ is a certain "two-level" modular curve and M, N are parameters to be chosen later.

Then for any matrix $\xi \in \mathrm{SL}_2(\mathbb{Z})$, Kato "twists" this pair by ξ and applies a norm map down to $Y_1(N)$ to get an element which Kato denotes by

$$ {}_{c,d}z_{1,N,m}(k = 2, r = 1, r' = 1, \xi, S = \text{ prime}(Np)) \in (\mathcal{O}(Y_1(N))^\times)^2$$

(See page 153 of Kato's paper for the precise definition).

The image of the above element ${}_{c,d}z_{1,N,m}(2, 1, 1, \xi, S)$ under the maps (a) through (f) is denoted (see Sections 8.9, 8.11 of Kato's paper)

$$ {}_{c,d}z(f, \xi) = {}_{c,d}z^{(p)}_{m=1}(f, r = 1, r' = 1, \xi, S = \text{ prime}(pN))$$

Then in 13.9 of Kato's paper, the zeta element z^{Kato} (denoted $z^{(p)}_\gamma$ in Kato's paper for some auxiliary parameter γ) is defined as quotients of elements of the form ${}_{c,d}z(f, \xi)$ by certain elements $\mu(c, d)$. It is this element $z^{(p)}_\gamma$ which is related to L-values.

This is clearly very technical. And to be fully honest, I don't intuitively understand a lot of the motivation behind Kato's constructions. But hopefully this gives at least a vague idea about how Kato's Euler System is constructed.

5 The Main Conjecture for Elliptic Curves

In this section, we draw the link between the algebraic side of Iwasawa theory and the analytic side of Iwasawa theory for elliptic curves. These two worlds are connected via the so-called "Iwasawa main conjecture".

The Iwasawa Main Conjecture (IMC) is a deep conjecture that connects the Selmer group of an elliptic curve (an algebraic object) to its p-adic L-function (an analytic object). We will first summarize the objects on the algebraic side of the main conjecture, then summarize the objects on the analytic side, and then state the Iwasawa main conjecture which bridges these two worlds.

a. *The algebraic side*

In this section, p will denote an odd prime and $E/\mathbb{Q}$ will be an elliptic curve with good ordinary reduction at p. Let $\mathbb{Q}^{\text{cyc}}$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

For any algebraic extension $K/\mathbb{Q}$, the Selmer group of E over K is a certain subgroup of $H^1(G_K, E(\overline{\mathbb{Q}})_{\text{tors}})$, where $G_K = \text{Gal}(\overline{K}/K)$. The Selmer group fits into the fundamental exact sequence

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \to \text{Sel}(E/K) \to \text{Sha}(E/K) \to 0$$

where $\text{Sha}(E/K)$ denotes the Tate-Shafarevich group of E over K. Let $K = \mathbb{Q}^{\text{cyc}}$. Then we can consider the Selmer group $\text{Sel}(E/\mathbb{Q}^{\text{cyc}})$, and this has an action of $\Gamma = \text{Gal}(\mathbb{Q}^{\text{cyc}}/\mathbb{Q})$. Its p-primary subgroup $\text{Sel}(E/\mathbb{Q}^{\text{cyc}})_p$ can be regarded as a Λ-module, where $\Lambda = \mathbb{Z}_p[\![T]\!]$. This ring Λ is called the ***Iwasawa algebra***. It is now known from the deep work of Kato that the Pontryagin dual $X(E/\mathbb{Q}^{\text{cyc}}) = \text{Sel}(E, \mathbb{Q}^{\text{cyc}})_p^\vee$ is a finitely generated ***torsion*** Λ-module. Therefore the structure theorem of finitely generated Λ-modules says that one has a pseudo-isomorphism

$$X(E/\mathbb{Q}^{\text{cyc}}) \sim \left(\bigoplus_{i=1}^{n} \frac{\Lambda}{(f_i(T)^{a_i})} \right) \oplus \left(\bigoplus_{j=1}^{m} \frac{\Lambda}{p^{\mu_j}} \right)$$

where the $f_i(T)$'s are irreducible distinguished polynomials (A polynomial $f(T)$ is distinguished if when you reduce f modulo p, only the highest degree term remains.) One can then define the algebraic Iwasawa invariants by

$$\lambda_E^{\text{alg}} = \sum_{i=1}^{n} a_i \deg(f_i(T)) \quad \text{and} \quad \mu_p^{\text{alg}}(E) = \sum_{j=1}^{m} \mu_j$$

DEFINITION 5.1. The ***characteristic ideal*** of $X(E/\mathbb{Q}^{\text{cyc}})$ is the ideal of Λ generated by $p^\mu f_1(T)^{a_1} \cdots f_n(T)^{a_n}$.

b. *The Analytic Side*

For an elliptic curve $E/\mathbb{Q}$ with good ordinary reduction at a prime p and χ an even Dirichlet character, denote by $L(E, \chi, s)$ the Hasse-Weil L-function of E twisted by χ. Let Ω_E be the Neron period of E. It is known by the work of Shimura that $L(E, \chi, 1)/\Omega_E$, a priori a transcendental number, is in fact an algebraic number.

Mazur and Swinnerton-Dyer have attached to E a p-adic L-function $\mathcal{L}_p(E, T) \in \Lambda \otimes \mathbb{Q}_p$ satisfying the following interpolation properties. If we write $a_p = (p+1) - \#E(\mathbb{F}_p)$, consider the Hecke polynomial $X^2 - a_p X + p$. Let $\alpha \in \mathbb{Z}_p^\times$ denote this unique p-adic root of the Hecke polynomial. Then,

$$\mathcal{L}_p(E, 0) = \left(1 - \frac{1}{\alpha}\right)^2 \cdot \frac{L(E, 1)}{\Omega_E^+}$$

Let χ be an even Dirichlet character of conductor p^n and p-power order. Then,

$$\mathcal{L}_p(E, \chi(1+p) - 1) = \frac{1}{\alpha^{n+1}} \cdot \frac{p^{n+1}}{g(\chi^{-1})} \frac{L(E, \chi^{-1}, 1)}{\Omega_E}$$

where $g(\chi)$ denotes the Gauss sum.

Using the Weierstrass preparation theorem, we can define the analytic invariants $\mu_p^{\text{an}}(E)$ and μ_p^{an} be writing:

$$\mathcal{L}_p(E, T) = p^{\mu_p^{\text{an}}(E)} \cdot u(T) \cdot f(T)$$

where $f(T)$ is a distinguished polynomial of degree μ_p^{an} and $u(T)$ is a unit in Λ. It is known that if E has good ordinary reduction at an odd prime p, and that $E[p]$ is irreducible as a Galois module, then $\mu_p^{\text{an}}(E) \geq 0$. In other words, $\mathcal{L}_p(E, T) \in \Lambda$.

c. *The Main Conjecture*

The Iwasawa main conjecture relates the Selmer group on the algebraic side to the p-adic L-function on the analytic side. Precisely, suppose that $E/\mathbb{Q}$ is an elliptic curve with good ordinary reduction at an odd prime p, and that $E[p]$ is irreducible as a Galois module. Then on the algebraic side, we can look at the characteristic ideal of the p-primary Selmer group $X(E/\mathbb{Q}^{\text{cyc}})$; this is an ideal in Λ. On the analytic side, we can attach to E a p-adic L-function $\mathcal{L}_p(E,T) \in \Lambda$.

CONJECTURE 5.2 (THE MAIN CONJECTURE). *The characteristic ideal of the p-primary Selmer group $X(E/\mathbb{Q}^{cyc})$ is generated by the p-adic L-function $\mathcal{L}_p(E,T)$. In particular, we have $\mu_E^{alg} = \mu_E^{an}$ and $\lambda_E^{alg} = \lambda_E^{an}$.*

PROGRESS ON THE MAIN CONJECTURE

In a magnum opus paper, Kato proved one divisibility of the Main conjecture under mild technical conditions:

THEOREM 5.3 (KATO). *If $p \geq 5$ and the mod p Galois representation of E is surjective, then the characteristic ideal of $X(E/\mathbb{Q}^{cyc})$ divides the ideal generated by $\mathcal{L}_p(E,T)$. In particular, $\mu_E^{alg} \leq \mu_E^{an}$ and $\lambda_E^{alg} \leq \lambda_E^{an}$.*

In another beautiful paper, using completely different techniques, Skinner-Urban proved the other divisibility of the main conjecture under mild technical conditions:

THEOREM 5.4. *Let N denote the conductor of E. Assume:*

(a) *We have $p \geq 5$.*
(b) *The mod p Galois representation $\overline{\rho}_{E,p}$ of E is surjective.*
(c) *There exists a prime $q \neq p$ such that q strictly divides N and $\overline{\rho}_{E,p}$ is ramified at p.*

Then the ideal generated by $\mathcal{L}_p(E,T)$ divides the characteristic ideal of $X(E/\mathbb{Q}^{cyc})$.

Combining this with Kato's Theorem, we conclude that the main conjecture is true for E.

6 The Eichler-Selberg Trace Formula and Class Numbers

This independent section describes a paper of Kuniaki Horie, which uses the Eichler-Selberg Trace Formula to prove an interesting result about class numbers of imaginary quadratic fields.

In a beautiful 1987 Inventiones paper, Kuniaki Horie proved the following theorem about class numbers of imaginary quadratic fields:

THEOREM 6.1 (HORIE). *Let p be a fixed prime number. There exist infinitely many imaginary quadratic fields K such that p is non-split K and p does not divide the class number of K.*

This theorem has consequences for Iwasawa theory. If K is a number field, then let K^{cyc}/K denote the cyclotomic $\mathbb{Z}_p$-extension of K. Let μ_K and λ_K denote the Iwasawa μ and λ-invariants of K^{cyc}/K. Iwasawa proved that if K has a unique prime lying over p and p does not divide the class number of K, then $\mu_K = 0$. Therefore, Horie's theorem proves:

COROLLARY 6.2. *Let p be a fixed prime number. There exist infinitely many imaginary quadratic fields K with $\mu_K = 0$ and $\lambda_K = 0$.*

The fact that $\mu_K = 0$ is already known by the Ferrero-Washington theorem since K is an abelian extension of $\mathbb{Q}$. So the new content of Horie's theorem is that $\lambda_K = 0$ for infinitely many K.

a. *The Trace Formula*

To prove this theorem, Horie uses Galois representations attached to modular forms, along with the Eichler-Selberg trace formula. I'll take this time to explain in detail what the Eichler-Selberg trace formula says.

Let $N \geq 1$ be an integer. Let $S_2(\Gamma_0(N))$ denote the space of weight 2 cuspforms for the congruence group $\Gamma_0(N)$. Every cuspform $f \in S_2(\Gamma_0(N))$ has a q-expansion $f = \sum_{n=1}^{\infty} a_n q^n$.

For every integer $m \geq 1$, there is a linear operator $T_m : S_2(\Gamma_0(N)) \to S_2(\Gamma_0(N))$. For $\gcd(m, N) = 1$, the operator T_m is defined on q-expansion as follows:

$$T_m : \sum_{n=1}^{\infty} a_n q^n \longmapsto \sum_{n=1}^{\infty} \left(\sum_{d \mid \gcd(m,n)} d a_{mn/d^2} \right) q^n$$

The Eichler-Selberg trace formula gives a closed form expression for the trace of the linear operator T_m in terms of class numbers of imaginary quadratic fields.

THEOREM 6.3 (EICHLER-SELBERG TRACE FORMULA (N PRIME)). *Suppose that N is a prime number. For any prime number q not dividing the level N, we have*

$$\operatorname{Tr}(T_q) = q - 1 - \sum_{a,b} \frac{h((a^2 - 4q)/b^2)}{w(a^2 - 4q)/b^2)} \mu(a, b, q)$$

where:

- *a runs through all integers such that $a^2 < 4q$.*
- *b runs through integers $b \geq 1$ such that b^2 divides $a^2 - 4q$ and $\frac{a^2-4q}{b^2} \equiv 0, 1 \pmod 4$.*
- *$h\left(\frac{a^2-4q}{b^2}\right)$ is the class number of the order with discriminant $\frac{a^2-4q}{b^2}$.*
- *$w\left(\frac{a^2-4q}{b^2}\right)$ is the number of roots of unity of the order with discriminant $\frac{a^2-4q}{b^2}$.*
- *$\mu(a, b, q) = \frac{\psi(N)}{\psi(N/N_b)} \sum_c 1$, where $\psi(N) = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$, $N_b = \gcd(N, b)$, and c runs through all elements of $(\mathbb{Z}/N\mathbb{Z})^*$ which lift to solutions of $c^2 - ac + q \equiv 0 \pmod{NN_b}$.*

The slogan of the trace formula is:

$$\text{Trace of } T_q = \text{weighted sum of class numbers of imaginary quadratic fields}$$

There is also a version of the trace formula for the case $N = 1$, which we state here:

THEOREM 6.4 (EICHLER-SELBERG TRACE FORMULA ($N = 1$)). *For any prime number q, the trace of T_q on $S_2(\mathrm{SL}_2(\mathbb{Z}))$ is given as:*

$$\mathrm{Tr}(T_q) = -q + \sum_{a,b} \frac{h((a^2-4q)/b^2)}{w((a^2-4q)/b^2)}$$

where as before:

- *a runs through all integers such that $a^2 < 4q$.*
- *b runs through integers $b > 1$ such that b^2 divides $a^2 - 4q$ and $\frac{a^2-4q}{b^2} \equiv 0, 1 \pmod 4$.*
- *$h\left(\frac{a^2-4q}{b^2}\right)$ is the class number of the order with discriminant $\frac{a^2-4q}{b^2}$.*
- *$w\left(\frac{a^2-4q}{b^2}\right)$ is the number of roots of unity of the order with discriminant $\frac{a^2-4q}{b^2}$.*

A good reference for the trace formula is the book Traces of Hecke Operators by Knightly and Li. The end of the book contains a full statement of the trace formula. This book contains a formula for the trace of T_n for arbitrary n, arbitrary level N, and any weight k.

EXAMPLE 6.5 ($N = 1$). Let $N = 1$, the space $S_2(\Gamma_0(1)) = S_2(\mathrm{SL}_2(\mathbb{Z}))$ is zero. So for all primes q, we have $\mathrm{Tr}(T_q) = 0$. Rearranging the trace formula, we obtain the following non-trivial relations between class numbers for all primes q:

$$q = \sum_{a,b} \frac{h((a^2-4q)/b^2)}{w((a^2-4q)/b^2)}$$

Suppose $q = 2$. Then the pairs of (a, b) are:

$$(a, b) = (-2, 1), (-1, 1), (0, 1), (1, 1), (2, 1)$$

Therefore, the trace formula becomes:

$$\begin{aligned} 2 &= 2\frac{h(-4)}{w(-4)} + 2\frac{h(-7)}{w(-7)} + \frac{h(-8)}{w(-8)} \\ &= \frac{h(-4)}{2} + h(-7) + \frac{h(-8)}{2} \\ &= \frac{1}{2} + 1 + \frac{1}{2} \end{aligned}$$

For an example with non-trivial class numbers, put $q = 7$. The trace formula gives:

$$\begin{aligned} 7 &= 6\frac{h(-3)}{w(-3)} + 2\frac{h(-12)}{w(-12)} + 2\frac{h(-19)}{w(-19)} + 2\frac{h(-24)}{w(-24)} + 2\frac{h(-27)}{w(-27)} + \frac{h(-28)}{w(-28)} + \frac{h(-7)}{w(-7)} \\ &= h(-3) + h(-12) + h(-19) + h(-24) + h(-27) + \frac{h(-28)}{2} + \frac{h(-7)}{2} \\ &= 1 + 1 + 1 + 1 + 2 + \frac{1}{2} + \frac{1}{2} \end{aligned}$$

where in the last line, we used the fact that $h(-27) = 2$ and $h(d) = 1$ for all the other values of d above.

EXAMPLE 6.6. The space $S_2(\Gamma_0(11))$ is one-dimensional, spanned by the newform $f = q - 2q^2 - q^3 + 2q^4 + q^5 + \cdots$. Writing $f = \sum a_n q^n$, it follows that for all q coprime to 11, i.e., $\gcd(q, 11) = 1$, we have $\mathrm{Tr}(T_q) = a_q(f)$. Let us verify this using the trace formula.

If $q = 3$, then the trace formula reads:

$$\begin{aligned}\mathrm{Tr}(T_3) &= 3 - 1 - 4\frac{h(-8)}{w(-8)} - 2\frac{h(-11)}{w(-11)} \\ &= 3 - 1 - 2h(-8) - h(-11) \\ &= -1 \\ &= a_3(f)\end{aligned}$$

where we used the facts that $h(-8) = h(-11) = 1$.

If $q = 5$, the trace formula reads.

$$\begin{aligned}\mathrm{Tr}(T_5) &= 5 - 1 - 2\frac{h(-11)}{w(-11)} - 4\frac{h(-19)}{w(-19)} \\ &= 5 - 1 - h(-11) - 2h(-19) \\ &= 1 \\ &= a_5(f)\end{aligned}$$

where we used the facts that $h(-11) = h(-19) = 1$.

HORIE'S PROOF

Fix a prime $p \geq 5$ for the rest of this section. Horie uses two trace formula: the trace formula for $\Gamma_0(p)$

$$\mathrm{Tr}(T_q) = q - 1 - \sum_{a,b} \frac{h((a^2 - 4q)/b^2)}{w((a^2 - 4q)/b^2)} \mu(a, b, q)$$

and the trace formula for $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$ (see example 6.5):

$$q = \sum_{a,b} \frac{h((a^2 - 4q)/b^2)}{w((a^2 - 4q)/b^2)}$$

Here q is a prime (different from p) which will be chosen later. Substituting the second equation into this first equation, we get:

$$\mathrm{Tr}(T_q) + q + 1 = \sum_{a,b} \frac{h((a^2 - 4q)/b^2)}{w((a^2 - 4q)/b^2)} \left(1 - \left\{\frac{(a^2 - 4q)/b^2}{p}\right\}\right) \tag{1}$$

Now we will prove the easier result that there is ***one*** imaginary quadratic field K such that p does not divide the class group of K and p is non-split in K. Suppose that we can find a prime q such that the LHS of (1) is nonzero modulo p. Then there would exist (a, b) such that

$$\frac{h((a^2 - 4q)/b^2)}{w((a^2 - 4q)/b^2)} \left(1 - \left\{\frac{(a^2 - 4q)/b^2}{p}\right\}\right) \not\equiv 0 \pmod{p}$$

This implies that $p \nmid h((a^2-4q)/b^2)$. It also implies that $\left\{\frac{(a^2-4q)/b^2}{p}\right\} \neq -1$, which means that p is non-split in $\mathbb{Q}\left(\sqrt{\frac{a^2-4q}{b^2}}\right)$.

So it suffices to prove the following:

LEMMA 6.7. *There exists a prime ℓ different from p such that* $\mathrm{Tr}(T_\ell) + \ell + 1 \not\equiv 0 \pmod{p}$.

PROOF. Let ℓ be the least positive quadratic non-residue modulo p. Then ℓ is a prime number and $\ell < \frac{p}{2}$ (Why?)

The trace formula for $q = \ell$ give us:

$$\mathrm{Tr}(T_\ell) + \ell + 1 = \sum_{a,b} \frac{h((a^2-4\ell)/b^2)}{w((a^2-4\ell)/b^2)} \left(1 - \left\{\frac{(a^2-4\ell)/b^2}{p}\right\}\right) \tag{2}$$

Therefore, we can write

$$\mathrm{Tr}(T_\ell) + \ell + 1 \geq \left(1 - \left(\frac{-\ell}{p}\right)\right) \frac{h(-4\ell)}{w(-4\ell)} + \left(1 - \left(\frac{1-\ell}{p}\right)\right) \frac{h(4-4\ell)}{w(4-4\ell)} \tag{3}$$

Since ℓ is a non square mod p, we have $\left(\frac{\ell}{p}\right) = -1$ and $\left(\frac{1-\ell}{p}\right) = 1$. Therefore, the RHS of the above inequality is always positive, so that $\mathrm{Tr}(T_\ell) + \ell + 1 > 0$. On the other hand, the trace formula and the identity $\ell < \frac{p}{2}$ shows that $\mathrm{Tr}(T_\ell) + \ell + 1 < p$. Since $\mathrm{Tr}(T_\ell) \in \mathbb{Z}$, we obtain

$$\mathrm{Tr}(T_\ell) + \ell + 1 \not\equiv 0 \pmod{p} \tag{4}$$

which completes the proof of the Lemma. □

THE PROOF IN GENERAL

We'll now use the above Lemma along with the Chebotarev Density Theorem to prove the theorem in general.

Let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$. If $X_0(N)$ has genus g, then $J_0(N)$ is an abelian variety over $\mathbb{Q}$ of dimension g. Let $J_0(N)[p]$ denote the p-torsion of $J_0(N)$; this is a $\mathbb{F}_p$-vector space of dimension $2g$ with a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This gives rise to the following Galois representation:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{2g}(\mathbb{F}_p)$$

By the Eichler-Shimura relations, we know that "traces of Frobenius equal traces of Hecke"; i.e: for all primes q away from Np, we have

$$\mathrm{Tr}(\rho(\mathrm{Frob}_q)) = \mathrm{Tr}(T_q)$$

where the right side denotes the trace of T_q on $S_2(\Gamma_0(N))$.

b. *Chebotarev Density Theorem*

Fix a large prime r. We will find an imaginary quadratic field with discriminant $> r$ satisfying the conditions of the theorem. By the Chebotarev Density Theorem, there exists a positive proportion of primes q such that:

- $\mathrm{Frob}_q \equiv \mathrm{Frob}_\ell \pmod{p}$, where ℓ is the prime from lemma 6.7,
- q is inert in $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}\sqrt{\left(\frac{-1}{v}\right)v}$ for every odd prime $v \leq r$ different from p.

The first point implies that

$$\mathrm{Tr}(T_\ell) \equiv \mathrm{Tr}(T_q) \pmod{p} \tag{5}$$

Furthermore, by the Weil Pairing, the field $\mathbb{Q}(J_0(N)[p])$ contains the cyclotomic field $\mathbb{Q}(\zeta_p)$. Therefore, the congruence $\mathrm{Frob}_q \equiv \mathrm{Frob}_\ell \pmod{p}$ implies that

$$q \equiv \ell \pmod{p} \tag{6}$$

The lemma shows that $\mathrm{Tr}(T_\ell) + \ell + 1 \not\equiv 0 \pmod{p}$. Combining this with the above two points gives:

$$\mathrm{Tr}(T_q) + q + 1 \not\equiv 0 \pmod{p}$$

Hence, by the trace formula, there exists (a, b) such that

$$\frac{h((a^2-4q)/b^2)}{w((a^2-4q)/b^2)} \not\equiv 0 \pmod{p} \quad \text{and} \quad \left\{\frac{(a^2-4q)/b^2}{p}\right\} \neq 1$$

Now put $k = \mathbb{Q}(\sqrt{(a^2-4q)/b^2})$. Let f_k be the conductor of k. We will show that $f_k > r$.

First, note that q is not inert in k. To see this, write $-f_k u^2 - (a^2-4q)/b^2$ for some $0 < u \in \mathbb{Z}$. Then $4q$ is the norm of $a + bu\sqrt{-f_k}$ for $k/\mathbb{Q}$ and hence q is not inert in k. Since $\left\{\frac{(a^2-4q)/b^2}{p}\right\} \neq 1$, the field k is not equal to $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, or $\mathbb{Q}(\sqrt{v\,*})$ for every prime $v \leq r$ different from p. It follows that $r < f_k$, as desired.

Now we will show that the class number of k is not divisible by p. This follows from the following relation:

$$\frac{h((a^2-4q)/b^2)}{w((a^2-4q)/b^2)} = \frac{h(-f_k)}{w(-f_k)} u \prod_{v|u} \left(1 - \left(\frac{-f_k}{v}\right) v^{-1}\right)$$

with the product on the right taken over the prime divisors v of u. Since, $w(-f_k) \mid 12$ and we have assumed $p \geq 5$, it follows from this that $h(-f_k)$ is not divisible by p.

In conclusion, we obtain an imaginary quadratic field k such that p is non-split in k, the class number of k is prime to p, and $f_k > r$. Since r is an arbitrary prime number, we have proved our Theorem.

7 Shimura's Algebraicity Theorem

In a beautiful 1976 paper, Shimura proved that one can normalize critical L-values of modular forms to make them algebraic. This independent explains Shimura's theorem and sketches a proof.

Let f be a newform of weight 2 and level $\Gamma_0(N)$. We can attach to f, its Hasse-Weil L-series

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

The L-series converges for $\Re(s) > \frac{3}{2}$. It has analytic continuation to all $s \in \mathbb{C}$ and satisfies a functional equation.

THEOREM 7.1 (SHIMURA). *Let $f \in S_2(\Gamma_0(N))$ be an eigenform. Let χ and ψ be primitive Dirichlet characters of opposite sign: i.e $\chi\psi(-1) = -1$. Put*

$$C(f,\chi,\psi) := \frac{L(f,\chi,1)L(f,\psi,1)}{\pi^2\langle f,f\rangle_N} \cdot \frac{Ga(\overline{\chi\psi})}{i}$$

(a) *The value $C(f,\chi,\psi)$, a priori a transcendental number, is in fact an algebraic number. Furthermore, $C(f,\chi,\psi)$ belongs to the number field $K_\chi K_\psi$. (Here K_χ and K_ψ are the number fields containing the values of χ and ψ, respectively).*

(b) *For any automorphism $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, we have*

$$C(f,\chi,\psi)^\sigma = C(f^\sigma,\chi^\sigma,\psi^\sigma)$$

This is quite a surprising theorem, because it shows that the ratio of two transcendental quantities is actually algebraic, and it behaves nicely under the action of Galois. I would highly recommend reading Shimura's original paper. This is Theorem 4 in Shimura's paper (the proof is very clearly written and packed with a lot of insight).

a. *The Rankin-Selberg Method*

The proof of Shimura's theorem uses a technique known as the Rankin-Selberg method. To introduce this method, we need some definitions:

THEOREM 7.2. *Let $N \geq 1$ be an integer and let ω be the Dirichlet character mod N. Define for $\tau \in \mathbb{H}$ (the upper half plane) and $s \in \mathbb{C}$,*

$$G_\omega(\tau,s) = \frac{N}{-4\pi i \cdot Ga(\omega)} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{\omega(n)}{(mN\tau+n)\cdot|mN\tau+n|^{2s}}$$

For fixed $\tau \in \mathbb{H}$, the function $G_\omega(\tau,s)$ is analytic in s for $\Re(s)$ sufficiently large. For fixed $\tau \in \mathbb{H}$, the function $G_\omega(\tau,s)$ has an analytic continuation to all $s \in \mathbb{C}$ and is holomorphic at $s = 0$.

Put $G_\omega(\tau) := G_\omega(\tau,0)$.

REMARK 7.3. Here are some facts:

(a) The function $G_\omega(\tau)$ belongs to $\mathcal{E}_1(\Gamma_0(N), \omega)$, the space of weight 1 Eisenstein series for $\Gamma_0(N)$ with nebentype ω. It is also an eigenform.
(b) If ω is a primitive character, then $G_\omega(\tau)$ has the q-expansion

$$G_\omega(\tau) = \frac{L(0,\omega)}{2} + \sum_{n=1}^{\infty}\left(\sum_{d|n}\omega(d)\right)$$

DEFINITION 7.4. Let $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$ and $g = \sum_{n=1}^{\infty} b_n q^n \in M_1(\Gamma_0(N), \omega)$ be a cuspform and a modular form, respectively. Define the ***Rankin-Selberg convolution*** L***-function*** of f and g as follows:

$$L(s, f \times g) := L(2s-1, \omega)\left(\sum_{n=1}^{\infty}\frac{a_n b_n}{n^s}\right)$$

Suppose that f and g are eigenforms with Galois representations ρ_f and ρ_g. Then $L(s, f \times g)$ is the L-function attached to the tensor product representation $\rho_f \otimes \rho_g$. The main theorem is:

THEOREM 7.5. *The L-series $L(s, f \times g)$ has meromorphic continuation to all $s \in \mathbb{C}$. It is holomorphic at $s = 1$ and satisfies:*

$$\langle f, g \cdot G_\omega \rangle_N = L(1, f \times g)\frac{Ga(\overline{\omega})}{8\pi^2 i}$$

b. *Determining the form g*

We now need to determine the form g. To do that, we'll introduce another definition.

DEFINITION 7.6. Let χ and ψ be Dirichlet characters mod N such that $\chi\psi(-1) = -1$. There is an Eisenstein series

$$G_{\chi,\psi} = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{E}_1(\Gamma_0(N))$$

where for $n \geq 1$, we have

$$a_n = \sum_{d|n}\chi(d)\psi(n/d)$$

and

$$a_0 = \begin{cases} 0 & \text{if } \chi, \psi \text{ non-trivial} \\ \frac{L(0,\chi\psi)}{2} & \text{else} \end{cases}$$

Here $G_{\chi,\psi}$ is the Eisenstein series whose associated Galois representation is $\chi \oplus \psi$. This is a more-or-less standard fact about Eisenstein series; for a proof, see for example Miyake's book Modular Forms (Theorem 4.7.1).

We need one last proposition:

PROPOSITION 7.7. *Let $f \in S_2(\Gamma_0(N))$ be an eigenform. Let χ and ψ be Dirichlet characters mod N such that $\chi\psi(-1) = -1$. Then for all $s \in \mathbb{C}$, we have*

$$L(s, f \times G_{\chi,\psi}) = L(f, \chi, s)L(f, \psi, s)$$

The proof of this is Lemma 1 in Shimura's paper, and it is proved by computing the Euler products of the L-functions on both sides. Alternatively, the LHS has Galois representation $\rho_f \otimes (\chi \oplus \psi)$ and the RHS has Galois representation $(\rho_f \otimes \chi) \oplus (\rho_f \otimes \psi)$. These two Galois representations are equal.

Combining this Proposition with the above Theorem, we obtain:

THEOREM 7.8. *Let $f \in S_2(\Gamma_0(N))$ be an eigenform. Let χ and ψ be primitive Dirichlet characters of opposite sign: i.e., $\chi\psi(-1) = -1$. Then*

$$\frac{\langle f, G_{\chi,\psi} \cdot G_{\overline{\chi\psi}}\rangle_N}{\langle f, f\rangle_N} = \frac{L(f, \chi, 1)L(f, \psi, 1)}{\langle f, f\rangle_N} \cdot \frac{Ga(\overline{\chi\psi})}{8\pi^2 i}$$

In other words, suppose that $f_1, \ldots, f_n$ form a basis of eigenforms for $S_2(\Gamma_0(N))$. We can decompose $G_{\chi,\psi} \cdot G_{\overline{\chi\psi}}$ in terms of the eigenforms f_j as follows:

$$G_{\chi,\psi} \cdot G_{\overline{\chi\psi}} = E + \sum_{j=1}^{n} \left(\frac{L(f, \chi, 1)L(f, \psi, 1)}{\langle f, f\rangle_N} \cdot \frac{Ga(\overline{\chi\psi})}{8\pi^2 i} \right) f_j$$

where $E \in \mathcal{E}_2(\Gamma_0(N))$ is an Eisenstein series.

The following Lemma (Lemma 4 in Shimura's paper) essentially completes the proof of the algebraicity theorem:

LEMMA 7.9. *Let $f \in S_2(\Gamma_0(N))$ be an eigenform and let $h \in M_2(\Gamma_0(N))$ be a modular form. Suppose that both f and h have algebraic Fourier coefficients in number fields K_f and K_h respectively. Then:*

(a) *The value $\frac{\langle f,h\rangle}{\langle f,f\rangle}$ belongs to $K_f K_h$.*
(b) *For every automorphism σ of $\mathbb{C}$, we have*

$$\left(\frac{\langle f, h\rangle}{\langle f, f\rangle}\right)^{\sigma} = \frac{\langle f^{\sigma}, h^{\sigma}\rangle}{\langle f^{\sigma}, f^{\sigma}\rangle}$$

PROOF. For simplicity, we prove this when N is prime. It is well-known from the theory of newforms that $S_2(\Gamma_0(N))$ has a basis of newforms $\{f_1, \ldots, f_n\}$ where

(a) The f_i are pairwise orthogonal, i.e., $\langle f_i, f_j\rangle = 0$ for $i \neq j$.
(b) If $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ is an automorphism, then the f_i are permutated under σ.

Put $f = f_1$. Write $h = E + a_1 f_1 + \cdots + a_n f_n$, where $E \in \mathcal{E}_2(\Gamma_0(N))$ is an Eisenstein series. Then $\frac{\langle f,h\rangle}{\langle f,f\rangle} = a_1$. Applying σ to both sides of the above equation, we get $h^{\sigma} = E^{\sigma} + a_1^{\sigma} f_1^{\sigma} + \cdots + a_n^{\sigma} f_n^{\sigma}$. This implies that $\frac{\langle f^{\sigma},h^{\sigma}\rangle}{\langle f^{\sigma},f^{\sigma}\rangle} = a_1^{\sigma}$. This proves the second claim of the Lemma.

It remains to prove the first claim. The second claim implies that $\frac{\langle f,h\rangle}{\langle f,f\rangle}$ is invariant under the action of $\mathrm{Gal}(\mathbb{C}/K_f K_h)$. It follows from Galois theory that $\frac{\langle f,h\rangle}{\langle f,f\rangle}$ must actually belong to $K_f K_h$, proving the first claim. This completes the proof of the Lemma, at least when N is prime. □

PROOF OF SHIMURA'S THEOREM

We are ready to prove Shimura's Theorem. Our "Key Theorem" said the following:

Let $f_2 \in S_2(\Gamma_0(N))$ be an eigenform. Let χ and ψ be primitive Dirichlet characters of opposite sign: i.e $\chi\psi(-1) = -1$. Then

$$\frac{\langle f, G_{\chi,\psi} \cdot G_{\overline{\chi\psi}} \rangle_N}{\langle f, f \rangle_N} = \frac{L(f,\chi,1)L(f,\psi,1)}{\langle f, f \rangle_N} \cdot \frac{\mathrm{Ga}(\overline{\chi\psi})}{8\pi^2 i}$$

Now f has Fourier coefficients in K_f and $G_{\chi,\psi} \cdot G_{\overline{\chi\psi}}$ has Fourier coefficients in $K_\chi K_\psi$. (Here K_χ and K_ψ are the number fields containing the values of χ and ψ respectively). The Lemma above says, therefore, that the LHS of the above identity lives in $K_f K_\chi K_\psi$ and transforms functorially under Galois. This proves Shimura's theorem.

c. *Examples*

The beauty of Shimura's proof is that it allows us to calculate algebraic L-values in a fairly effective way. We demonstrate this in two examples.

EXAMPLE 1

Let $p = 11$ and let $\chi(n) = \left(\frac{-11}{n}\right)$ be the unique quadratic character of conductor 11. The character χ is odd.

The Eisenstein series $G_{1,\chi}$ is the unique normalized eigenform in the space $\mathcal{E}_1(\Gamma_0(11), \chi)$. Using Sage, we compute:

$$G_{1,\chi} = \frac{1}{2} + q + 2q^3 + q^4 + 2q^5 + 3q^9 + q^11 + 2q^{12} + 4q^{15} + q^{16} + O(q^{20})$$

The Eisenstein series $G_{1,\overline{\chi}}$ belongs to the space $\mathcal{E}_1(\Gamma_0(11), \overline{\chi})$. Since χ is a quadratic character, we have $\chi = \overline{\chi}$ so in fact $G_{1,\overline{\chi}} = G_{1,\chi}$. Therefore,

$$(G_{1,\chi})^2 = \frac{1}{4} + q + q^2 + 2q^3 + 5q^4 + 4q^5 + O(q^6)$$

This forms $(G_{1,\chi})^2$ belongs to $M_2(\Gamma_0(11))$. The space $M_2(\Gamma_0(11))$ is spanned by an Eisenstein series and a cuspidal newform whose q-expansions are:

$$E = \frac{5}{12} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + O(q^6)$$
$$f = q - 2q^2 - q^3 + 2q^4 + q^5 + O(q^6)$$

By examining these q-expansions, we find that

$$G_{1,\chi} \cdot G_{1,\chi} = \frac{3}{5}E + \frac{2}{5}f$$

Therefore,

$$\frac{L(f,1)L(f,\chi,1)}{\langle f, f \rangle_N} \cdot \frac{\mathrm{Ga}(\chi)}{8\pi^2 i} = \frac{\langle f, G_{1,\chi} \cdot G_{\overline{\chi}} \rangle_N}{\langle f, f \rangle_N} = \frac{2}{5}$$

EXAMPLE 2

Let $p = 37$. Let χ be the unique Dirichlet character of conductor 37 such that $\chi(2) = \zeta_{36}$. Then χ is odd. Note that χ is not a quadratic character so our theorem does not say anything about it. But we include this example because it shows a modular form with analytic rank 1.

The Eisenstein series $G_{1,\chi}$ is the unique eigenform (normalized so that $a_1 = 1$) in the space $\mathcal{E}_1(\Gamma_0(37), \chi)$. Using Sage, we calculate the q-expansion as:

$$\begin{aligned} G_{1,\chi} =& \frac{6}{37}\zeta_{36}^{11} + \frac{3}{37}\zeta_{36}^{10} - \frac{17}{37}\zeta_{36}^{9} - \frac{27}{37}\zeta_{36}^{8} + \frac{5}{37}\zeta_{36}^{7} - \frac{16}{37}\zeta_{36}^{6} - \frac{14}{37}\zeta_{36}^{5} - \frac{7}{37}\zeta_{36}^{4} + \\ & \frac{15}{37}\zeta_{36}^{3} + \frac{26}{37}\zeta_{36}^{2} + \frac{13}{37}\zeta_{36} + \frac{25}{37} + q + (\zeta_{36}+1)q^2 + (-\zeta_{36}^{8}+1)q^3 + \\ & (\zeta_{36}^{2} + \zeta_{36} + 1)q^4 + (-\zeta_{36}^{5}+1)q^5 + \cdots \end{aligned}$$

The Eisenstein series $G_{\overline{\chi}}$ belongs to the space $\mathcal{E}_1(\Gamma_0(37), \overline{\chi})$. Using Sage again, we calculate the q-expansion as,

$$\begin{aligned} G_{\overline{\chi}} =& -\frac{18}{37}\zeta_{36}^{11} + \frac{1}{37}\zeta_{36}^{10} + \frac{2}{37}\zeta_{36}^{9} + \frac{4}{37}\zeta_{36}^{8} + \frac{8}{37}\zeta_{36}^{7} + \frac{16}{37}\zeta_{36}^{6} + \frac{13}{37}\zeta_{36}^{5} + \frac{26}{37}\zeta_{36}^{4} + \\ & \frac{15}{37}\zeta_{36}^{3} - \frac{7}{37}\zeta_{36}^{2} - \frac{14}{37}\zeta_{36} + \frac{9}{37} + q + (-\zeta_{36}^{11} + \zeta_{36}^{5} + 1)q^2 + (\zeta_{36}^{10}+1)q^3 + \\ & (-\zeta_{36}^{11} - \zeta_{36}^{10} + \zeta_{36}^{5} + \zeta_{36}^{4} + 1)q^4 + (\zeta_{36}^{7} - \zeta_{36} + 1)q^5 + \cdots \end{aligned}$$

The product of these two forms is $G_{1,\chi} \cdot G_{\overline{\chi}}$, which belongs to $M_2(\Gamma_0(11))$. The space $M_2(\Gamma_0(11))$ is spanned by an Eisenstein series E and two cuspidal newforms f and g whose q-expansions are:

$$\begin{aligned} E &= \frac{3}{2} + q + 3q^2 + 4q^3 + 7q^4 + 6q^5 + \cdots \\ f &= q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + \cdots \\ g &= q + q^3 - 2q^4 + \cdots \end{aligned}$$

By examining these q-expansions, we find that

$$\begin{aligned} & G_{1,\chi} \cdot G_{\overline{\chi}} \\ &= \left(-\frac{12}{37}\zeta_{36}^{11} + \frac{4}{37}\zeta_{36}^{10} - \frac{8}{111}\zeta_{36}^{9} - \frac{32}{111}\zeta_{36}^{8} + \frac{2}{111}\zeta_{36}^{7} + \frac{34}{111}\zeta_{36}^{5} + \frac{20}{111}\zeta_{36}^{4} + \frac{16}{111}\zeta_{36}^{3} + \frac{20}{111}\zeta_{36}^{2} + \frac{34}{111}\zeta_{36} + \frac{34}{37}\right)E \\ &+ 0 \cdot f + \left(-\frac{1}{3}\zeta_{36}^{9} - \frac{1}{3}\zeta_{36}^{8} + \frac{1}{3}\zeta_{36}^{7} - \frac{1}{3}\zeta_{36}^{5} + \frac{1}{3}\zeta_{36}^{4} + \frac{2}{3}\zeta_{36}^{3} + \frac{1}{3}\zeta_{36}^{2} - \frac{1}{3}\zeta_{36}\right)g \end{aligned}$$

Therefore,

$$\frac{L(f,1)L(f,\chi,1)}{\langle f, f\rangle_{37}} \cdot \frac{\mathrm{Ga}(\overline{\chi})}{8\pi^2 i} = \frac{\langle f, G_{1,\chi} \cdot G_{\overline{\chi}}\rangle_{37}}{\langle f, f\rangle_{37}} = 0$$

So, $L(f,1)L(f,\chi,1) = 0$. The newform f corresponds via modularity to the elliptic curve $E =$ `37.a1` with Weierstrauss equation $E : y^2 + y = x^3 + x$. This curve E has Mordell-Weil rank 1. Under Birch and Swinnerton-Dyer conjecture (BSD), this implies that $L(f,1) = 0$. This is consistent with our calculation that $L(f,1)L(f,\chi,1) = 0$.

Furthermore, we have

$$\frac{L(g,1)L(g,\chi,1)}{\langle g, g\rangle_{37}} \cdot \frac{\mathrm{Ga}(\overline{\chi})}{8\pi^2 i} = \frac{\langle g, G_{1,\chi} \cdot G_{\overline{\chi}}\rangle_{37}}{\langle g, g\rangle_{37}} = -\frac{1}{3}\zeta_{36}^{9} - \frac{1}{3}\zeta_{36}^{8} + \frac{1}{3}\zeta_{36}^{7} - \frac{1}{3}\zeta_{36}^{5} + \frac{1}{3}\zeta_{36}^{4} + \frac{2}{3}\zeta_{36}^{3} + \frac{1}{3}\zeta_{36}^{2} - \frac{1}{3}\zeta_{36}$$

8 Weil Conjectures for Elliptic curves over $\mathbb{F}_p$

a. *Introduction*

Let p be an odd prime. Consider the elliptic curve $E/\mathbb{F}_p$ given by

$$E/\mathbb{F}_p : y^2 = x^3 - x$$

The most basic question we can ask about E is: What is the size of $E(\mathbb{F}_p)$? In Figure 1 below, we have plotted $|E(\mathbb{F}_p)|$ as a function of p: we can see that the plot roughly follows the red line $|E(\mathbb{F}_p)| = p + 1$. We might guess that,

$$|E(\mathbb{F}_p)| \approx p + 1$$

But this estimate is not meaningful unless we have a handle on the error $|E(\mathbb{F}_p)| - (p + 1)$. In Figure 2, we plot this error as a function of p and we notice that the points are sandwiched between two red lines with equations $2\sqrt{p}$ and $-2\sqrt{p}$. This could lead us to guess that

$$-2\sqrt{p} \leq |E(\mathbb{F}_p)| - (p + 1) \leq 2\sqrt{p}$$

This theorem actually holds true for all elliptic curves over $\mathbb{F}_p$.

THEOREM 8.1 (HASSE-WEIL BOUND). *Let $E/\mathbb{F}_p$ be an elliptic curve. Then*

$$|E(\mathbb{F}_p)| = p + 1 + a_p$$

where $|a_p| \leq 2\sqrt{p}$.

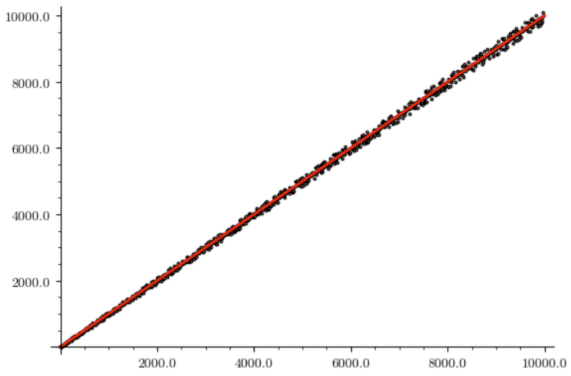

Figure 1: Plot of $|E(\mathbf{F}_p)|$ vs. p

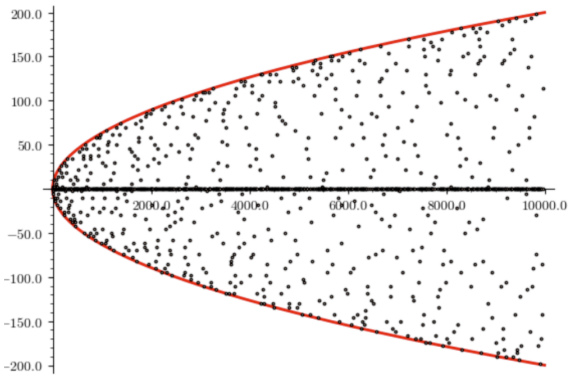

Figure 2: Plot of $|E(\mathbf{F}_p)| - (p + 1)$ vs. p

There is something curious about this theorem. Namely, the number of solutions to an equation mod p seems to be a purely number-theoretic problem, but it is stated for elliptic curves, which have a ***group*** structure. Is that assumption necessary? Shouldn't the number of solutions to a polynomial mod p only have to do with the polynomial itself, and not whether the underlying curve has a group structure?

The answer is yes: theorems like the above actually do hold for general curves that are not groups, indeed more generally for varieties of any dimension, over $\mathbb{F}_p$. The difficulty, of course, lies in the fact that these are much harder to prove because the proofs cannot rely on the extra structure given by elliptic curves. These theorems are spelled out in a set of conjectures called the ***Weil Conjectures***. These conjectures can be thought of as distilling the true nature of the Hasse-Weil bound, generalizing the it in such a manner that its inessential features are stripped away.

As an illustration, the Weil conjectures imply the following generalization of the Hasse- Weil bound, which crucially, does not assume any group structure on the curve.

THEOREM 8.2. *Let C be a smooth curve over $\mathbb{F}_p$. Let g denote the genus of C. Then*

$$|C(\mathbb{F}_p)| = p + 1 + a_p$$

where $|a_p| \leq 2g\sqrt{p}$.

In this paper, we will state the Weil conjectures for smooth curves over $\mathbb{F}_p$ and then prove them in the special case of elliptic curves.

b. *The ζ-function*

Unlike the Hasse-Weil bound, the Weil Conjectures are not phrased explicitly in terms of $|C(\mathbb{F}_p)|$. Rather, they are phrased in terms of the so-called ***ζ-function of a curve*** C, a function which encodes a lot of information about $|C(\mathbb{F}_{p^n})|$ for all n. We will first present the definition of the ζ-function, and then indicate the motivation for the definition.

DEFINITION 8.3. Let C be a smooth curve over $\mathbb{F}_p$. The ζ-function of C is defined as

$$\zeta_{C/\mathbb{F}_p}(s) = \exp\left(\sum_{n=1}^{\infty} |C(\mathbb{F}_{p^n})| \frac{(p^{-s})^n}{n}\right)$$

If we expand out the exponential in the definition of $\zeta_{C/\mathbb{F}_p}$, we get that $\zeta_{C/\mathbb{F}_p}(s) \in \mathbb{Q}[\![p^{-s}]\!]$, i.e., ζ is a power series with rational coefficients in the variable p^{-s}. The Weil Conjectures are phrased completely in terms of this ζ-function; they give detailed information about its roots and in doing so, it gives us bounds for $|C(\mathbb{F}_{p^n})|$ for various n. But this raises two questions:

(a) Why do we want to wrap up the various values $|C(\mathbb{F}_{p^n})|$ in this function? What is the use of this?
(b) Why does the ζ-function have this particular form; i.e: why is the exponential there?

Here are some answers:

(a) The general philosophy is that ζ functions allow us to use ***analysis*** to study algebraic objects. If we can prove complex analytic facts about this ζ-function (e.g: it has zeroes at these points, poles at those points with these residues, etc), we can translate that information back into the realm of algebra to solve our original problem. This approach is essential to proving the Weil Conjectures for higher dimensional varieties.
(b) Here the answer is simpler: if we put exp in front, the ζ-function turns out to be a ***rational function*** of p^{-s}. This makes it much easier to deal with that the otherwise complicated infinite series. (We see this in the examples.)

EXAMPLES

(a) If $C = \mathbb{P}^1$, then $|\mathbb{P}^1(\mathbb{F}_p)| = p + 1$. More generally, $|\mathbb{P}^1(\mathbb{F}_{p^n})| = p^n + 1$. This gives us,

$$\zeta_{\mathbb{P}^1}(s) = \exp\left(\sum_{n=1}^{\infty}(p^n + 1)\frac{(p^{-s})^n}{n}\right)$$

In the following, we will write $T = p^{-s}$ and $\zeta(T)$ instead of $\zeta(s)$ to make the notation easier. We know that $\zeta_{\mathbb{P}^1}(T)$ is a power-series in the variable T with $\mathbb{Q}$-coefficients. As a concrete case, we will show that if $p = 5$, then the power series of $\zeta(T)$ is:

$$\zeta_{\mathbb{P}^1/\mathbb{F}_5}(T) = 1 + 6T + 31T^2 + 156T^3 + 781T^4 + \cdots$$

Here is how to derive this series. Instead of working with ζ directly, the standard trick is to work with $\log\zeta$ to get rid of the exponential. We then get

$$\log\zeta_{\mathbb{P}^1}(T) = \sum_{n=1}^{\infty}(p^n + 1)\frac{T^n}{n} = -\log(1 - pT) - \log(1 - T)$$

where in the last equality, we used the power-series $-\log(1 - X) = \sum_{n=1}^{\infty}\frac{X^n}{n}$. Simplifying this via the logarithm rules, we get

$$\zeta_{\mathbb{P}^1}(T) = \frac{1}{(1 - pT)(1 - T)}$$

so as promised, $\zeta(T)$ is a ***rational function*** of T. This motivates why ζ was defined the way it was; the exponential function allows us to use logarithms in this argument, which lead to the function being rational. To write this rational function as an element of $\mathbb{Q}[\![T]\!]$, use the geometric series

$$\frac{1}{(1 - z)} = 1 + z + z^2 + \cdots$$

and multiply the two resulting power series. For example, if $p = 5$, we get:

$$\begin{aligned}\zeta_{\mathbb{P}^1/\mathbb{F}_5}(T) &= (1 + 5T + 25T^2 + 125T^3 + \cdots)(1 + T + T^2 + T^3 + \cdots)\\ &= 1 + 6T + 31T^2 + 156T^3 + 781T^4 + \cdots\end{aligned}$$

which gives us the power series from the start.

(b) We will later prove that for any elliptic curve $E/\mathbb{F}_p$, the ζ-function is of the form:

$$\zeta_{E/\mathbb{F}_p}(T) = \frac{1 + (|E(\mathbb{F}_p)| - (p + 1))T + pT^2}{(1 - T)(1 - pT)}$$

As an example, the curve $E/\mathbb{F}_p : y^2 = x^3 - x$ is an elliptic curve over $\mathbb{F}_p$ for all odd primes. Take $p = 5$, then Sage tells us that $|E(\mathbb{F}_5)| = 8$. To get a power series, use the geometric series $\frac{1}{(1-z)} = 1 + z + z^2 + \cdots$, and multiply the two resulting power series. Then the ζ-function for $E/\mathbb{F}_5$ is:

$$\zeta_{E/\mathbb{F}_5}(T) = \frac{1 + 2T + 5T^2}{(1 - T)(1 - 5T)} = 1 + 8T + 48T^2 + 248T^3 + 1248T^4 + \cdots$$

If $p = 13$, then $|E(\mathbb{F}_{13})| = 8$, so the ζ-function for $E/\mathbb{F}_{13}$ is:

$$\zeta_{E/\mathbb{F}_{13}}(T) = \frac{1 - 6T + 13T^2}{(1-T)(1-13T)} = 1 + 8T + 112T^2 + 1464T^3 + 19040T^4 + \cdots$$

We have plotted $\zeta_{E/\mathbb{F}_5}$ (Figure 3) and $\zeta_{E/\mathbb{F}_{13}}$ (Figure 4) as a function of s (recall that $T = p^{-s}$). Observe that all the zeroes fall on a ***line (called the critical line)***; this line is $\Re(s) = \frac{1}{2}$.

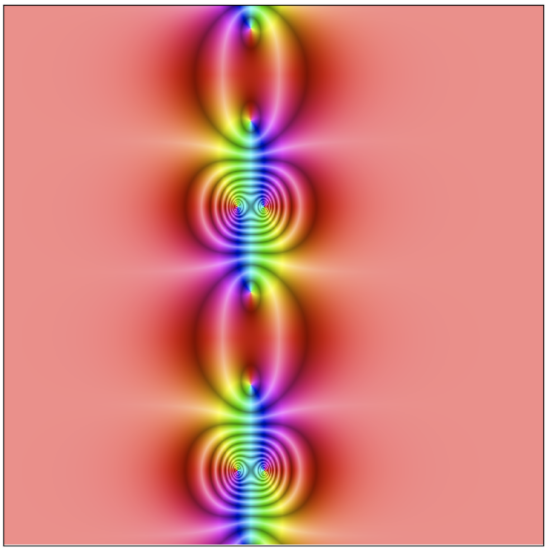

Figure 3: Plot of $\zeta_{E/\mathbf{F}_p}(s)$ for $p = 5$

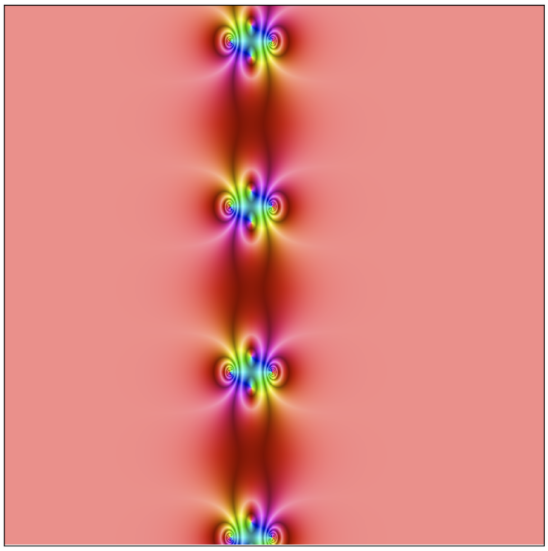

Figure 4: Plot of $\zeta_{E/\mathbf{F}_p}(s)$ for $p = 13$

c. *Statement of the Weil Conjectures*

THEOREM 8.4 (WEIL CONJECTURES FOR CURVES). *Let C be a smooth curve over $\mathbb{F}_p$. Let g denote the genus of C. Let $\zeta_{C/\mathbb{F}_p}(s)$ be the ζ-function of C.*

(a) *The ζ-function of C is a rational function of p^{-s}. Furthermore, we can write*

$$\zeta_{C/\mathbb{F}_p}(p^{-s}) = \frac{F(p^{-s})}{(1-p^{-s})(1-p\cdot p^{-s})}$$

where $F \in \mathbb{Q}[p^{-s}]$ is a polynomial of degree $2g$.

(b) *The ζ-function of C satisfies the so-called functional equation:*

$$\zeta_{C/\mathbb{F}_p}(s) = \zeta_{C/\mathbb{F}_p}(1-s)$$

(c) *The zeroes of $\zeta_{C/\mathbb{F}_p}(s)$ lie on the critical line $\Re(s) = \frac{1}{2}$.*

To appreciate the importance of these statements, it helps to compare this with the situation for the ordinary Riemann zeta function $\zeta(s) = \sum \frac{1}{n^s}$. The ordinary Riemann ζ-function is ***not*** rational; it is a complicated infinite series, and that is the source of great trouble in analytic number theory. So the fact that $\zeta_{C/\mathbb{F}_p}$ is a rational function is quite remarkable. This is a general phenomenon: many problems in number theory have cousins in the world of algebraic curves, which are simpler to state and solve because we can make use of algebraic geometry.

d. *Proof of Weil Conjectures for Elliptic Curves*

We will now prove the Weil Conjectures for elliptic curves over $\mathbb{F}_p$. The proof has a different flavour from the rest of the paper because it relies in an essential way on the ***group structure*** of elliptic curves. We begin with a proposition.

PROPOSITION 8.5. *Let E be an elliptic curve over $\mathbb{F}_p$.*

(a) *For every n, we have:*

$$|E(\mathbb{F}_{p^n})| = p^n + 1 - \alpha^n - \beta^n$$

where $\alpha, \beta \in \mathbb{C}$ are the complex roots of the polynomial $T^2 + (|E(\mathbb{F}_p)| - (p+1))T + p$.

(b) *Furthermore, the roots α, β are complex conjugates of each other, and they satisfy*

$$|\alpha| = |\beta| = \sqrt{p}$$

*These complex numbers α and β are called the **eigenvalues of Frobenius** (for reasons that will become clear).*

PROOF. Let E be an elliptic curve over $\mathbb{F}_p$.

(a) Here is the overall structure of the proof. We will first use the Frobenius map to reinterpret $|E(\mathbb{F}_{p^n})|$ in the language of algebraic geometry. Then we will use the Tate Module $T_\ell E$ to convert this algebraic geometry problem into a simpler one about linear algebra.
Carrying out the first step is simple. To do this, let Frob $: E \to E$ denote the p-power Frobenius map given by $(x, y) \mapsto (x^p, y^p)$. Then $x \in E(\mathbb{F}_{p^n})$ if and only if x is fixed by Frob^n, which is true if and only if $x \in Ker(\text{Frob}^n - \text{id})$. Since Frob^n $-$id is an isogeny, we conclude that

$$|E(\mathbb{F}_{p^n})| = |Ker(\text{Frob}^n - \text{id})| = \deg(\text{Frob}^n - \text{id})$$

So we have reduced the problem of finding $|E(\mathbb{F}_{p^n})|$ to the problem of finding the degree of the map Frob^n $-$id. To find the degree, note that ℓ is a prime different from p, we have an injection $\text{End}(E) \hookrightarrow \text{End}(T_\ell E)$. This is useful because of the following claim.
Claim (Proved in [1]). Given a map $\phi \in \text{End}(E)$, let $\phi_\ell \in \text{End}(T_\ell E)$ be its image. Then

$$\begin{aligned} \det \phi_\ell &= \deg \phi \\ \text{Tr}\, \phi_\ell &= 1 + \deg \phi + \deg(1 - \phi) \end{aligned}$$

This fact tells us that we can find deg(Frob^n $-$id) by finding the determinant of the linear map $(\text{Frob}^n - \text{id})_\ell \in \text{End}(T_\ell E)$. We do this using linear algebra. Write Frob^n $-$id instead of $(\text{Frob}^n - \text{id})_\ell$ for convenience. We will find the determinant of this map using the following claim.
Claim. If A is a 2×2 matrix, then $\det(A - 1) = \det(A) - \text{Tr}(A) + 1$.
This fact, combined with the multiplicativity of det, means that

$$\det(\text{Frob}^n - 1) = \det(\text{Frob})^n - \text{Tr}(\text{Frob}^n) + 1 \tag{7}$$

We know that $\det(\text{Frob}) = \deg(\text{Frob}) = p$, so we have half the formula. To find $\text{Tr}(\text{Frob}^n)$, we use the fact that $\text{Tr}(\text{Frob}^n)$ is the sum of the eigenvalues of Frob^n (counted with multiplicity). But the eigenvalues of Frob^n are the eigenvalues of Frob (counted with multiplicity) raised to the n^{th} power, so we have that $\text{Tr}(\text{Frob}^n) = \alpha^n + \beta^n$, where $\alpha, \beta \in \mathbb{C}$ are the eigenvalues of Frob. Combining this with (7), we get

$$\det(\text{Frob}^n - 1) = p^n + 1 - \alpha^n - \beta^n$$

Since $|E(\mathbb{F}_{p^n})| = \det(\text{Frob}^n - 1)$, this completes the proof of (a).

(b) Apply the quadratic formula to the characteristic polynomial of Frob, which is $T^2 + (|E(\mathbb{F}_p)| - (1+p))T + p$. Noting that the discriminant

$$\Delta = (|E(\mathbb{F}_p)| - (1+p))^2 - 4p = -3p - |E(\mathbb{F}_p)| + 1 < 0$$

is negative, it follows that the roots of the characteristic polynomial are complex conjugates. Since $\alpha\beta = p$ (look at the characteristic polynomial), it follows that $|\alpha| = |\beta| = \sqrt{p}$.

This completes the proof of the proposition. □

Now we can prove the Weil Conjectures for elliptic curves.

PROOF. Plugging in our expression for $|E(\mathbb{F}_{p^n})|$ into the ζ-function for E, we get:

$$\begin{aligned}
\log \zeta_{E/\mathbb{F}_p}(T) &= \sum_{n=1}^{\infty} |E(\mathbb{F}_{p^n})| \frac{T^n}{n} \\
&= \sum_{n=1}^{\infty} (p^n + 1 - \alpha^n - \beta^n) \frac{T^n}{n} \\
&= -\log(1 - pT) - \log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T)
\end{aligned}$$

where in the last equality, we used the power-series for $-\log(1 - X)$ from before. This means that

$$\zeta_{E/\mathbb{F}_p}(T) = \frac{1 + (|E(\mathbb{F}_p)| - (p+1))T + pT^2}{(1 - T)(1 - pT)}$$

which shows that ζ is a rational function of T. This proves part (a) of the Weil Conjectures.

The part (b), i.e., the functional equation, is a calculation with the rational function for ζ obtained above.

Now we prove part (c) of the Weil Conjectures. Using the quadratic formula, note that the zeroes of $\zeta_{E/\mathbb{F}_p}(s)$ are precisely the zeroes of the polynomial,

$$(p^{-s})^2 + (|E(\mathbb{F}_p)| - (1+p))p^{-s} + p$$

divided by p. So the roots of $\zeta_{E/\mathbb{F}_p}$ are $\frac{\alpha}{p}$ and $\frac{\beta}{p}$ with norm $\frac{1}{\sqrt{p}}$, where α and β are the eigenvalues of Frob. Therefore, if s is a zero of $\zeta_{E/\mathbb{F}_p}$, then $|p^{-s}| = p^{-\frac{1}{2}}$, so $\Re(s) = \frac{1}{2}$, as desired. This completes the proof of the Weil Conjectures for elliptic curves. □

Now we illustrate how information about the ζ-function gives us what we were originally after: bounds on $|E(\mathbb{F}_{p^n})|$ for all values of n.

COROLLARY 8.6 (GENERALIZED HASSE-WEIL BOUND). *Let $E/\mathbb{F}_p$ be an elliptic curve. Then for all n, we have*

$$|E(\mathbb{F}_{p^n})| = p^n + 1 + a_p$$

where $|a_p| \leq 2\sqrt{p^n}$.

PROOF. We can write $\zeta_{E/\mathbb{F}_p}$ as follows:

$$\zeta_{E/\mathbb{F}_p}(T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-pT)}$$

where α and β are as in the Proposition. Taking logarithms, and expanding in power series, we get:

$$\begin{aligned}\log \zeta_{E/\mathbb{F}_p}(T) &= \log(1-\alpha T) + (1-\beta T) - \log(1-T) - \log(1-pT) \\ &= \sum_{n=1}^{\infty} (-\alpha^n - \beta^n + p^n + 1)\frac{T^n}{n}\end{aligned}$$

Matching coefficients, we get that

$$|E(\mathbb{F}_{p^n})| = -\alpha^n - \beta^n + p^n + 1$$

The Riemann Hypothesis implies that $|\alpha| = |\beta| = \sqrt{p}$, so we have

$$|E(\mathbb{F}_{p^n})| - (p^n + 1) \leq |\alpha^n| + |\beta^n| = 2\sqrt{p^n}$$

completing the proof. □

9 References

[1] Joseph Silverman. ***The Arithmetic of Elliptic Curves***. Springer-Verlag, New York, 2009.

[2] Dino Lorenzini. ***Invitation to Arithmetic Geometry***. American Mathematical Society, Providence, 1996.

[3] Brian Osserman. ***A Concise Account of the Weil Conjectures and Etale Cohomology***.

[4] Lawrence C. Washington. ***Introduction to Cyclotomic Fields***. Springer GTM, New York, 1997.