L-functions of Rational Elliptic Curves

by

Kwan Sheng Ong

Supervisor: Alex Ghitza

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science
(Mathematics)

at the
University of Melbourne
2024

L-functions of Rational Elliptic Curves

Kwan Sheng Ong

Abstract

In this thesis, we investigate and present the correspondence between L-functions associated with rational elliptic curves and L-functions of modular forms, whose relationship was crucial to the proof of Fermat's Last Theorem. We start with the general theory of elliptic curves over local and global fields and present the construction of the L-function associated to a rational elliptic curve. Then we introduce modular forms and discuss the theory of L-functions associated with cusp forms. We end with a survey on Birch Swinnerton-Dyer conjecture and present some promising progress on said conjecture.

Dedication

To mum and dad.

Acknowledgements

First and foremost, I want to thank my supervisor Alex Ghitza for supervising this master project. Thank you for your guidance and patience, even when I seemed to be going in circles at times. Next, I would like to thank my family for their endless support, and my dad's well-timed suppers when I am exhausted from my studies. Thank you to my GOATED brother who always carry me in the games. (Requested by my brother, Kwan Ping Ong) I would like to thank Anthony Wu, Joel Griffin, Tianqi Feng, Albert Tran, Steven Nguyen, Moshe Uhrig. I would also like to thank these amazing groups of people for the fun times, their kindness, and, most importantly, all the help they gave me (and all those tricky assignments **we** tackled together):

Number Theory Crew: (Sasha) Alexander Stratov, Bowan Hafey, Chengjing Zhang, Chenyan Wu, Kevin Fergusson, Qizheng Han, Miles Koumouris, Riley Moriss.

G90 + Math Crew: Adam Monteleone, Amit Ben Harim, Ben Gaudin, Brandon Xie, Davood Nejaty, Fei Peng, Grace Yuan, Haris Rao, Jake Brown, (J1) Jeremy Lorenzo, (J2) Jeremy Lvovsky, Joel Maldonado, Jonah Nelson, Julianne Cai, Oliver Li, Peter Karapalidis, Quan Nguyen, Rodney Dharma, Sean Malton, Tyler Franke, Wei Sun, (Jerry) Yanchao Yang, Yuhan Gai, Yuhan Liao, Zin Li, etc.

Physics/PUBG/Mahjong Crew: Abdul Basit, Arash Moghaddamtabrizi, Bryan Junjie Tah, Junhao Zhan, Sam Junsheng He.

Contents

Chapter 1

Introduction

The story of elliptic curves started in ancient Greece, in Diophantus of Alexandria's *Arithmetica*. Like many of the problems worked on by Diophantus, this involved solving for integer and rational solutions to polynomial equations, in particular, an equation of the form

$$y^2 = ax^3 + bx^2 + cx + d,$$

where the cubic on the right hand side has no repeated roots. The problem Diophantus recorded can be stated as: "To divide a given number into two numbers such that their product is a cube minus its side." [Hea85, Book IV, Problem 24] Let a be Diophantus' given number, then we would like to find x and y such that

$$y(a - y) = x^3 - x.$$

By a (linear) change of variables $Y = y - a/2,\ X = -x$, we get the equation

$$Y^2 = X^3 - X + \left(\frac{a}{2}\right)^2.$$

This equation will later become known as one that defines an elliptic curve.

Fast forward to the 1600s, when Pierre de Fermat famously scribbled on the tiny margins of his translated copy of *Arithmetica* his famous last conjecture: if the integer n is greater than 2, then the equation

$$a^n + b^n = c^n$$

has no integer solutions with $abc \neq 0$. Unbeknownst to Fermat, his mysterious "truly marvelous proof" will ignite one of the longest pursuits in mathematics history spanning more than 350 years, engaging countless mathematicians. The problem

was finally solved by Andrew Wiles and Richard Taylor in 1994, whose proof relied heavily on the theory of elliptic curves among other mathematical tools. [Wil95] Central to their work was the question:

Are all (semistable) elliptic curves defined over the rationals modular?

Let us rewind to the start of 1900s, when modern theory of elliptic curves first begun with a question posed by Bernhard Riemann:

Is the group of rational points of an elliptic curve finitely generated?

This question was answered in the 1920s by Louis Mordell, who proved what is now known as Mordell's theorem. Building on Mordell's work, André Weil later provided a new proof and extended the results to higher-dimensional analogues of elliptic curves known as abelian varieties over number fields, and this generalisation became known as Mordell-Weil theorem. [Wei29] The 1930s saw further signficant advancements with Helmut Hasse's series of papers focusing on elliptic curves over finite fields. In his paper, Hasse showed two significant results, the first being the Hasse bound, which gives a sharp estimate for the number of points on an elliptic curve over a finite field. The second is the analogue of the Riemann hypothesis for elliptic curves. Hasse's insights not only significantly deepened the understanding of the behavior of elliptic curves in arithmetic contexts, but also established a foundational link between the geometry of elliptic curves and algebraic structures in number theory.

Weil later generalised these ideas to smooth algebraic varieties in what became known as the Weil Conjectures, a set of deep conjectures about zeta functions of algebraic varieties over finite fields. [Wei49] Weil's successful attempt for curves showed promise for more general algebraic varieties, but it was out of reach at the time. This would later spark two decades of development in étale cohomology by Alexander Grothendieck and his collaborators, as they worked toward solving the Weil Conjectures. These early 20th-century developments, particularly Mordell's and Weil's results, firmly established elliptic curves as central objects of study in number theory and algebraic geometry, laying the groundwork for later applications in areas such as cryptography, coding theory, and the eventual proof of Fermat's Last Theorem.

In more recent times, elliptic curves have been discovered to have increasingly important and sometimes surprising applications, particularly in the field of cryptography. In 1985, both Neal Koblitz and Victor Miller independently proposed using elliptic curves for cryptographic purposes, marking the beginning of elliptic curve

cryptography (ECC). [Kob87; Mil86] The primary advantage of ECC lies in the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), which is thought to be much harder to break than traditional methods like factoring large composite numbers used in RSA encryption. Specifically, for the same level of security, elliptic curve cryptography can use significantly smaller key sizes, making it more efficient. For example, a 256-bit key in ECC provides comparable security to a 3072-bit key in RSA, offering substantial benefits in terms of computational efficiency, memory usage, and transmission bandwidth. This makes ECC especially appealing for use in environments where resources are limited. As a result, elliptic curves have become a crucial part of modern cryptographic systems.

Thus, from ancient Greece to modern cryptography, elliptic curves continue to reveal their profound influence across mathematics and technology.

1.0.1 Structure of Thesis

This thesis is organised as follows. **Chapter 2** sets the stage by discussing various types of L-functions, from the classical Riemann zeta function to the general Dirichlet L-function. In **Chapter 3**, we delve into elliptic curves and their associated structures, including isogenies and Tate modules, offering insights into their algebraic properties. **Chapter 4** focuses on elliptic curves over finite fields, introducing Hasse's bound and Weil's conjectures in the setting of elliptic curves. We also define the L-function associated to a rational elliptic curve. **Chapter 5** addresses the theory of modular forms and Hecke operators, which leads to the statement of the modularity theorem. Finally, **Chapter 6** provides a detailed exploration of the Birch and Swinnerton-Dyer conjecture, reviewing both classical results and recent developments in the study of the rank of elliptic curves and the behaviour of their L-functions.

Chapter 2

Some Examples of L-functions

The theory of L-functions originates from the Riemann zeta function, defined as:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$

It was Leonhard Euler who first noticed that properties of primes could be studied analytically. He noticed, for a real number $s > 1$, one can factorise $\zeta(s)$ into the infinite product

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

This insight connects prime numbers to the analytic properties of the zeta function. Many are familiar with Euclid's proof of the infinitude of primes. Here, we present a different proof by Euler that leverages the properties of the series above.

Theorem 2.0.1. *There are infinitely many primes.*

Proof. For a prime p, we have $1/p < 1$, thus the ratio $1/(1 - 1/p)$ can be expanded into the geometric series

$$\frac{1}{1 - 1/p} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots .$$

By Fundamental Theorem of Arithmetic, for finite products we get

$$\prod_{p}^{N} \frac{1}{1 - 1/p} = \sum_{n \in N_p} \frac{1}{n}$$

where the left hand side runs over all primes left than or equal to N and $N_p = \{n \in$

$\mathbb{N} \mid n = p_1 p_2 \cdots p_r,\ p_i \leq N,\ \forall i\}$. Therefore, as we limit N to ∞, we get

$$\prod_p \frac{1}{1-1/p} = \sum_{n\in\mathbb{N}} \frac{1}{n}.$$

Since the harmonic series on the right hand side diverges, the left hand side cannot be a product of finitely many terms. And thus, there are infinitely many terms in the product, which means there are infinitely many primes. □

This is one of the first signs that show arithmetic objects such as the prime numbers can be studied analytically through functions such as the Riemann zeta function. In 1837, to study the primes in arithmetic progressions, Johann Peter Dirichlet introduced the Dirichlet L-functions, which he in turn used to prove his eponymous theorem.

Theorem 2.0.2 (Dirichlet's theorem)**.** *For all coprime integers a and m, there are infinitely many primes $p \equiv a \bmod m$.*

To define a Dirichlet L-series, we start with a Dirichlet character.

Definition 2.0.3. *A complex-valued arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ is a **Dirichlet character of modulus** m if for all integers a, b, we have:*

i. χ *is completely multiplicative, i.e.* $\chi(ab) = \chi(a)\chi(b)$.

ii. $\chi(a) \begin{cases} = 0, & \text{if } \gcd(a,m) > 1, \\ \neq 0, & \text{if } \gcd(a,m) = 1. \end{cases}$

iii. χ *is periodic with period m, i.e.* $\chi(a+m) = \chi(a)$.

Definition 2.0.4. *A **Dirichlet L-series** is a function of the form*

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

where χ is a Dirichlet character and s is a complex variable with $Re(s) > 1$.

Remark. *If χ_0 is the trivial character, i.e. it sends everything to 1, we recover the Riemann zeta function $L(s,\chi_0) = \zeta(s)$.*

Remark. *Note that the L-series, which is an infinite series representation (for example the Dirichlet series for the Riemann zeta function), is distinguished from the L-function, which is the function in the complex plane that is its analytic continuation.*

Over time, the theory of L-functions was extended to various other contexts. For example, the L-function of an elliptic curve is given by:

Example 2.0.5 (L-function of elliptic curves)**.** *The L-function of elliptic curve is*

$$L(s, E) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

where the coefficients a_p are related to the number of points on the elliptic curve over finite fields (as we will define in Section 4.4).

This is one of many modern examples of how L-functions are used to study arithmetic objects. The development of L-functions, beginning with the Riemann zeta function, laid the foundation for some of the most important results in number theory, including the Prime Number Theorem:

Theorem 2.0.6 (Prime Number Theorem)**.** *Let $\pi(x)$ be the prime-counting function, i.e. it equals to the number of primes less than or equal to x. Then we have*

$$\pi(x) \sim \frac{x}{\log(x)}.$$

This result, proved using properties of the Riemann zeta function, reveals the deep connection between primes and the behavior of analytic functions.

Chapter 3

Elliptic Curves and Tate Modules

This chapter will largely follow [Sil09, Chapter III]. At the heart of number theory, elliptic curves frequently emerge. This is because they possess a unique duality, originating as analytic objects while also exhibiting rich algebraic properties. In this chapter we will showcase some of their algebraic qualities.

3.1 Elliptic Curves

Definition 3.1.1 (Elliptic Curves)**.** *An **elliptic curve** E is a curve C in the projective plane $\mathbb{P}^2$ given by a Weierstrass equation*

$$C : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

*We denote the point $[0, 1, 0]$ by O. This is called the prescribed point of the elliptic curve E. The elliptic curve E is **defined over** K, written E/K, if the coefficients $a_1, \ldots, a_6$ are in K.*

Remark. *Some might have seen elliptic curves defined as a nonsingular curve of genus one with a prescribed point O. This is an equivalent definition as the set of curves defined by Definition 3.1.1 maps surjectively onto the set of nonsingular curves of genus one with a prescribed point [Sil09, Chapter III, §3, Proposition 3.1].*

Remark. *If $Z = 0$, from the Weierstrass equation above, we can see $X^3 = 0$ which gives $X = 0$. Since in projective space, at least one of the coordinates is nonzero, it means $Y \neq 0$. WLOG assume $Y = 1$. This means $O = [0, 1, 0]$ is the only point on an elliptic curve E with $Z = 0$. So often in literature, one replaces X, Y, Z with*

$$x = \frac{X}{Z} \qquad \text{and} \qquad y = \frac{Y}{Z},$$

and works in the affine plane $\mathbb{A}^2$ while calling the point O the point at infinity. Some also denote the prescribed point/point at infinity with ∞.

Let $L \subseteq \mathbb{P}^2$ be a line. Since the equation of an elliptic curve E is degree 3, by Bézout's theorem, $L \cap E$ taken with multiplicities consists of exactly three points. This allow us to define a group law on the points of the elliptic curve E. We define the composition law as follows:

1. Let $P, Q \in E$ and L be the line through P and Q. If $P = Q$, then let L be the tangent line to E at P.
2. Then let R denote the third point of intersection of L with E.
3. Let L' be another line that goes through the points R and $O = [0, 1, 0]$.
4. Then L' intersects E at three points, R, O, and a third point. Denote this third point by $P + Q$, the "sum" of the points P and Q.

Proposition 3.1.2. *The composition law has the following properties:*

(a) If a line L intersects E at the (not necessarily distinct) points P, Q, R, then $(P + Q) + R = O$.

(b) (Identity) $P + O = P$ for all $P \in E$.

(c) (Commutativity) $P + Q = Q + P$ for all $P, Q \in E$.

(d) (Additive Inverse) Let $P \in E$. There is a point of E, denoted by $-P$, satisfying $P + (-P) = O$.

(e) (Associativity) Let $P, Q, R \in E$. Then $(P + Q) + R = P + (Q + R)$.

So the points of E form an abelian group with group operation $+$.

(f) If E is defined over a field K, then

$$E(K) = \{(x, y) \in K^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

is a subgroup of E with group operation $+$.

3.2 Isogeny

Every elliptic curve has a prescribed point O, so it is useful to look at morphisms between varieties that respect the prescribed points when we look at maps between elliptic curves.

Definition 3.2.1. *Let E_1 and E_2 be elliptic curves. An **isogeny** from E_1 to E_2 is a map of curves $\phi : E_1 \to E_2$ satisfying $\phi(O) = O$. Two elliptic curves E_1 and E_2 are **isogenous** if there is a nonconstant isogeny from E_1 to E_2.*

The zero isogeny $[0]$ is defined as follows, $[0](P) = O$ for all $P \in E_1$. By [Sil09, Chapter II, §2, Theorem 2.4(a)], a nonconstant map $\phi : C_1 \to C_2$ of curves defined over K will induce a map of function fields $\phi^* : K(C_2) \to K(C_1)$ such that $K(C_1)$ is a finite extension of $\phi^*(K(C_2))$. So ϕ is called a *finite* map of curves if it is nonconstant. So except for the zero isogeny, every other isogeny is a finite map of curves. Thus we get the injection of function fields

$$\phi^* : \bar{K}(E_2) \to \bar{K}(E_1),$$

which allows us to define the degree of an isogeny.

Definition 3.2.2. *The degree of an isogeny $\phi : E_1 \to E_2$ is defined as the degree of the finite extension $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$, with $\deg_s(\phi)$ and $\deg_i(\phi)$ denoting the separable and inseparable degrees of the extension respectively.*

The theorem below shows an isogeny ϕ actually commutes with the group operation on the points of an elliptic curve, in other words, every isogeny is a group homomorphism on the points of elliptic curves.

Theorem 3.2.3. *Let $\phi : E_1 \to E_2$ be an isogeny. Then*

$$\phi(P + Q) = \phi(P) + \phi(Q) \quad \textit{for all } P, Q \in E_1.$$

Proof. [Sil09, Chapter III, §4, Theorem 4.8] □

Because the points of E_2 form an abelian group, we can define addition between between isogenies with pointwise addition

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

So the isogenies from E_1 to E_2 form an abelian group

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\}$$

with identity [0], the zero isogeny.

Example 3.2.4. *[Was08, Section 12.2, Example 12.3]*
Let $E_1 : y_1^2 = x_1^3 + ax_1^2 + bx_1$ be an elliptic curve over some field of characteristic not 2. We require $b \neq 0$ and $a^2 - 4b \neq 0$ in order to have E_1 nonsingular. Then $(0,0)$ is a point of order 2. Let E_2 be the elliptic curve $y_2^2 = x_2^3 - 2ax_2^2 + (a^2 - 4b)x_2$. Define $\alpha : E_1 \to E_2$ as follows:

$$(x_1, y_1) \mapsto \left(\frac{y_1^2}{x_1^2}, \frac{y_1(x_1^2 - b)}{x_1^2} \right).$$

α is clearly a nonconstant map of curves. If we look at the first coordinate and substitute y_1^2 with $x_1^3 + ax_1^2 + bx_1$, we get the rational function

$$r(x) = \frac{x^3 + ax_2 + bx}{x^2} = \frac{x^2 + ax + b}{x},$$

which gives us $\deg(\alpha) = 2$ and α is separable. As we will later see in Theorem 3.2.7, this means there are two points in the kernel $\alpha^{-1}(O_2)$. Note the kernel is the inverse image of the point at infinity O_2 because it is the identity element in the group formed by the points of E_2. From $r(x) = x + a + (b/x)$, we see that the two points must be $(0,0)$ and O_1, since all of the other points have finite images.

Example 3.2.5 (Multiplication-by-m isogeny $[m]$)**.** *For each $m \in \mathbb{Z}$, we can define the **multiplication-by-m isogeny** as follows:*

$$[m] : E \to E, \quad [m](P) = \begin{cases} \underbrace{P + P + \cdots + P}_{m \text{ terms}}, & \text{if } m > 0, \\ O, & \text{if } m = 0, \\ [-m](-P) = \underbrace{-P - P - \cdots - P}_{m \text{ terms}}, & \text{if } m < 0. \end{cases}$$

The map defined above is clearly an isogeny since $[m](O) = O$.

We can now define the torsion subgroups of an elliptic curve E.

Definition 3.2.6. *Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \geq 1$. The **m-torsion subgroup of** E is the set of points of E of order m,*

$$E[m] = \{P \in E(\bar{K}) \mid [m]P = O\}.$$

The torsion subgroup of E is the set of points of finite order,

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

If E is defined over K, then $E_{tors}(K)$ denotes the points of finite order in $E(K)$.

Next, let $Q \in E$ be a point in E. Then we define the translation-by-Q map in the following way:

$$\tau_Q : E \to E, \qquad \tau_Q(P) = P + Q, \quad \forall\ P \in E.$$

We then have the following theorem on the Galois theory of elliptic function fields.

Theorem 3.2.7. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny.*

(a) For every $Q \in E_2$, we have

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

Furthermore, for every $P \in E_1$,

$$e_\phi(P) = \deg_i(\phi).$$

(b) The map

$$\ker(\phi) \to \text{Aut}(\bar{K}(E_1)/\phi^*(\bar{k}(E_2))), \tag{3.1}$$
$$T \mapsto \tau_T^*, \tag{3.2}$$

is an isomorphism.

(c) Suppose that ϕ is separable. Then ϕ is unramified,

$$\#\ker(\phi) = \deg(\phi),$$

and $\bar{K}(E_1)$ is a Galois extension of $\phi^*(\bar{K}(E_2))$.

This theorem tells us that an elliptic curve isogenous to the elliptic curve E_1 is uniquely determined by the kernel of the isogeny from E_1 to it.

Corollary 3.2.7.1. *Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be nonconstant isogenies,*

and assume that ϕ is separable. If $\ker(\phi) \subseteq \ker(\psi)$, then there is a unique isogeny

$$\lambda : E_2 \to E_3$$

satisfying $\psi = \lambda \circ \phi$.

Therefore, if $\ker(\phi) = \ker(\psi)$, then E_2 is isomorphic to E_3.

Remark. *Isogenies are important in the study of elliptic curves. For example, for elliptic curves defined over finite fields $\mathbb{F}_q$, elliptic curves E_1, E_2 are isogenous over $\mathbb{F}_q$ if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$. Similarly, for elliptic curves over $\mathbb{Q}$, they are isogenous if and only if their L-series [which we define in Chapter 4.4] are equal. This theorem arose from Falting's proof of Mordell's conjecture that an algebraic curve of genus 2 has finitely many rational points. [Was08, Section 12.5]*

3.3 Dual Isogeny

Being isogenous is actually an equivalence relation because of the existence of a "reverse" isogeny we call the dual isogeny. The following theorem gives the existence and uniqueness of the dual isogeny.

Theorem 3.3.1. *Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree m. Then there exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1 \quad \textit{satisfying} \quad \hat{\phi} \circ \phi = [m].$$

We call $\hat{\phi}$ from above the **dual isogeny** to ϕ.

Example 3.3.2. *Let E_1 be an elliptic curve given by $y_1^2 = x_1^3 + ax_1^2 + bx_1$ with $b \neq 0$ and $a^2 - 4b \neq 0$ so it is nonsingular. From Example 3.2.4, we know there is an isogeny $\alpha : E_1 \to E_2$ to the elliptic curve E_2 given by $y_2^2 = x_2^3 - 2ax_2^2 + (a^2 - 4b)x_2$. Its dual isogeny $\hat{\alpha} : E_2 \to E_1$ is defined as follows*

$$(x_2, y_2) \mapsto \left(\frac{1}{4}(x_2 + \frac{-2ax_2 + a^2 - 4b}{x_2}), \frac{1}{8}(y_2 - \frac{(a^2 - 4b)y_2}{x_2^2}).\right)$$

Composing $\hat{\alpha} \circ \alpha$, we get

$$x_1 \mapsto \frac{y_1^2}{x_1^2} \mapsto \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)^2 - a - 2x_1,$$

which is the formula for the x-coordinate of $2(x_1, y_1)$. [Sil09, Chapter III, §2, Group Law Algorithm 2.3] A similar calculation for the y-coordinate tells us $\hat{\alpha} \circ \alpha = [2]$, which verifies $\hat{\alpha}$ is the unique dual isogeny of α. For more detailed calculations, look at [Was08, Section 12.3, Example 12.4].

The following theorem lists the properties of the dual isogeny.

Theorem 3.3.3. *Let $\phi : E_1 \to E_2$ be an isogeny.*

(a) Let $m = \deg(\phi)$. Then

$$\hat{\phi} \circ \phi = [m] \quad \text{on } E_1 \quad \text{and} \quad \phi \circ \hat{\phi} = [m] \quad \text{on } E_2.$$

(b) Let $\lambda : E_2 \to E_3$ be another isogeny. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then

$$\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}.$$

(d) For all $m \in \mathbb{Z}$, we have

$$\hat{[m]} = [m] \quad \text{and} \quad \deg[m] = m^2.$$

(e) $\deg(\hat{\phi}) = \deg(\phi)$.

(f) $\hat{\hat{\phi}} = \phi$.

Corollary 3.3.3.1. *Let E_1 and E_2 be elliptic curves. Then the degree map*

$$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

Corollary 3.3.3.2. *Let E be an elliptic curve and let $m \in \mathbb{Z}$ be nonzero.*

(a) If $m \neq 0$ in K, i.e. $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) \nmid m$, then

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(b) If $\mathrm{char}(K) = p > 0$*, then one of the following is true:*

i. $E[p^e] = \{O\}$ *for all* $e = 1, 2, 3, \ldots$.

ii. $E[p^e] \cong \frac{\mathbb{Z}}{p^e\mathbb{Z}}$ *for all* $e = 1, 2, 3, \ldots$.

3.4 Tate Modules

As noted in Corollary 3.3.3.2, the group of m-order torsion points has a natural $\mathbb{Z}/m\mathbb{Z}$-module structure. Since the Galois group $G_{\bar{K}/K}$ acts on the torsion subgroups for an elliptic curve E/K, it is often useful to investigate the Galois representations related to these torsion subgroups. As we will soon find out, it will be useful to package together the torsion subgroups for all prime powers of a fixed prime as they are, in a sense, a nested sequence of subgroups.

Definition 3.4.1 (Tate Modules of an Elliptic Curve)**.** *Let* E *be an elliptic curve and let* $\ell \in \mathbb{Z}$ *be a prime that is not equal to* $\mathrm{char}(K) = p \geq 0$*. The* ℓ*-adic Tate Module of* E *is the* $\mathbb{Z}_\ell$*-module*

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

with the inverse limit being taken with respect to the natural maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

From Corollary 3.3.3.2, the Tate module $T_\ell(E)$, as a $\mathbb{Z}_\ell$-module, has the following structure:

- If $\ell \neq \mathrm{char}(K)$, then $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$.
- If $p = \mathrm{char}(K) > 0$, then $T_p(E) \cong \{0\}$ or $\mathbb{Z}_p$.

This also illustrates another advantage of the Tate module. We can now work in the p-adic field $\mathbb{Q}_\ell$, which has characteristic 0, instead of the ring $\mathbb{Z}/\ell^n\mathbb{Z}$.

Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then ϕ induces a map $\phi : E_1[\ell^n] \to E_2[\ell^n]$ since it is a group homomorphism by Theorem 3.2.3. Thus it induces a $\mathbb{Z}_\ell$-linear map $\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$ on the Tate modules. This gives us a natural homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

If $E_1 = E_2 = E$, we then get the homomorphism of rings

$$\mathrm{End}(E) \to \mathrm{End}(T_\ell(E)).$$

Back to the homomorphism from isogenies to linear maps between Tate modules, tensoring with $\mathbb{Z}_\ell$ we get a homomorphism of $\mathbb{Z}_\ell$ modules

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)). \tag{3.3}$$

If $\ell \neq \mathrm{char}(K)$, the map (3.3) is injective. This means isogenies between elliptic curves are entirely characterised by their induced map on the Tate modules, and the latter is linear whereas the former often is not! (Check Example 3.2.4) This gives us the following corollary:

Corollary 3.4.1.1. *Let E_1 and E_2 be elliptic curves. Then $\mathrm{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most 4.*

It has been shown (3.3) is an isomorphism in following two situations:

1. K is a finite field. [Tat66]
2. K is a number field. [Fal83; Fal86]

3.5 Weil Pairing

For an abelian variety A, the Weil pairing is a pairing between the m-torsion elements of A and its dual abelian variety $\hat{A}$ [Sil10]

$$A[m] \times \hat{A}[m] \to \mu_m.$$

Since elliptic curves are self-dual, we get a pairing of the form

$$E[m] \times E[m] \to \mu_m.$$

We will directly invoke the proposition below to get the existence of the Weil pairing, in particular the induced Weil pairing on the Tate modules, for more details on the explicit construction of the Weil pairing, look at [Sil09, Chapter III §8] or [Sil10].

Proposition 3.5.1. *Let μ denote the roots of unity. Then there exists a pairing*

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

with the following properties:

(a) It is bilinear:

$$e(S_1 + S_2, T) = e(S_1, T)e(S_2, T),$$
$$e(S, T_1 + T_2) = e(S, T_1)e(S, T_2).$$

(b) It is alternating:

$$e(S, T) = e(T, S)^{-1} \qquad \text{and} \qquad e(T, T) = 1.$$

(c) It is nondegenerate: If $e(S, T) = 1$ for all $S \in T_\ell(E)$, then $T = O$.

(d) It is Galois invariant:

$$e(S, T)^\sigma = e(S^\sigma, T^\sigma) \qquad \text{for all } \sigma \in G_{\bar{K}/K}.$$

(e) Furthermore, if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and its dual $\hat{\phi}$ are adjoints for the pairing, i.e. $e(\phi S, T) = e(S, \hat{\phi}T)$.

We will now use it to prove the following proposition that allows us to compute the degree of an isogeny using the determinant and trace of the induced map on Tate modules ϕ_ℓ. This proposition is later applied to count the number of K-rational points of an elliptic curve defined over a finite field K.

Proposition 3.5.2. *Let $\phi \in \mathrm{End}(E)$, let $\ell \neq \mathrm{char}(k)$ and let $\phi_\ell : T_\ell(E) \to T_\ell(E)$ be the map that ϕ induces on the Tate module of E. Then*

$$\det(\phi_\ell) = \deg(\phi) \qquad \text{and} \qquad \mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi).$$

In particular, $\det(\phi_\ell)$ and $\mathrm{tr}(\phi_\ell)$ are in $\mathbb{Z}$ and are independent of ℓ.

Proof. Let $\{v_1, v_2\}$ be a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$. Write $\phi_\ell(v_1) = av_1 + bv_2$ and $\phi_\ell(v_2) = cv_1 + dv_2$. So the matrix of ϕ_ℓ relative this basis is

$$\phi_\ell = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Using the properties of Weil pairing from Proposition 3.5.1, we have

$$\begin{aligned}
e(v_1, v_2)^{\deg(\phi)} &= e([\deg \phi]v_1, v_2) && \text{(bilinearity of } e\text{)} \\
&= e(\hat{\phi}_\ell \phi_\ell v_1, v_2) && \text{(Theorem 3.3.1)} \\
&= e(\phi_\ell v_1, \phi_\ell v_2) && \text{(Proposition 3.5.1, Theorem 3.3.3 } (f)\text{)} \\
&= e(av_1 + bv_2, cv_1 + dv_2) \\
&= e(av_1, cv_1)e(bv_2, cv_1)e(av_1, dv_2)e(bv_2, dv_2) \\
&= e(v_1, v_1)^{ac} e(v_1, v_2)^{-bc} e(v_1, v_2)^{ad} e(v_2, v_2)^{bd} \\
&= e(v_1, v_2)^{ad-bc} && \text{(since } e \text{ is bilinear and alternating)} \\
&= e(v_1, v_2)^{\det \phi_\ell}.
\end{aligned}$$

Since e is nondegenerate, we can conclude that $\deg(\phi) = \det(\phi_\ell)$. For any 2×2 matrix, we have

$$\operatorname{tr}(A) = a + d = q + (ad - bc) - ((1 - a)(1 - d) - bc) = 1 + \det(A) - \det(1 - A).$$

Thus we get the desired proposition. □

The independence of ℓ shows that both $\det(\phi_\ell)$ and $\operatorname{tr}(\phi_\ell)$ are intrinsic values of the elliptic curve E and are not simply introduced by the linearisation to $T_\ell(E)$, which requires a choice of a prime ℓ.

Chapter 4

Elliptic Curves over Finite Fields

It is often useful to study equations over finite fields because it is easier to find solutions and often provides intriguing insights into solutions in other infinite fields such as $\mathbb{Q}$ and $\mathbb{C}$. This statement will come in the form of Weil Conjectures in a bit.

4.1 Frobenius Morphism

Let K be a field of characteristic $p > 0$, and let $q = p^r$ for some $r \geq 1$.

Let E/K be an elliptic curve given by a Weierstrass equation. Then $E^{(q)}/K$ is defined by raising the coefficients of the equation for E to the q^{th}-power. Since $E^{(q)}$ is the zero locus of a Weierstrass equation, if the equation is nonsingular, then it will be an elliptic curve. It can be shown that the discriminant of $E^{(q)}$ satisfies $\Delta(E^{(q)}) = \Delta(E)^q$, thus $E^{(q)}$ is also an elliptic curve.

The **Frobenius morphism** ϕ_q is defined by

$$\phi_q : E \to E^{(q)}, \quad (x, y) \mapsto (x^q, y^q).$$

The following theorem specifies the conditions for separability of the map $m + n\phi$, which is needed later to show Hasse's bound.

Theorem 4.1.1. *Let $E/\mathbb{F}_q$ be an elliptic curve. Let $\phi : E \to E$ be the q^{th}-power Frobenius morphism and let $m, n \in \mathbb{Z}$. Then the map*

$$m + n\phi : E \to E$$

is separable if and only if $p \nmid m$. In particular, the map $1 - \phi$ is separable.

Proof. [Sil09, Chapter III, §5, Corollary 5.5] □

Previously in Example 3.3.2 we gave an example of the dual isogeny to a separable isogeny. Here is an example for an inseparable isogeny, in particular the Frobenius morphism ϕ_q. Let $E/\mathbb{F}_q$ be an elliptic curve. Let $a = q + 1 - \#E(\mathbb{F}_q)$, then we have $\phi_q^2 - a\phi_q + q = 0$. [Was08, Section 4.2, Theorem 4.10] Therefore, if we let $\hat{\phi}_q = a - \phi$, then we have

$$\hat{\phi}_q \circ \phi_q = (a - \phi_q) \circ \phi_q = a\phi_q - \phi_q^2 = q = \deg(\phi_q).$$

4.2 Hasse's Bound

In this section, we show Hasse's bound on the number of points on an elliptic curve $E/\mathbb{F}_q$. For a rough bound, we can first look at the Weierstrass equation for E

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

where we have set $Z = 1$ without loss of generality. For each value of X, the equation will yield at most two values of Y since it is a quadratic, so a rough upper bound is

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

The $+1$ comes from the prescribed point $O = [0, 1, 0]$. However, because there are q^2 distinct monic quadratic polynomials with coefficients in $\mathbb{F}_q$ and roughly $q^2/2$, i.e. half of them are reducible in $\mathbb{F}_q$, we expect the bound to be around q instead of $2q$. We will first prove Cauchy-Schwarz for a positive quadratic form.

Lemma 4.2.1 (Cauchy-Schwarz)**.** *Let A be an abelian group, and let*

$$d : A \longrightarrow \mathbb{Z}$$

be a positive definite quadratic form. Then we have the inequality

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)} \qquad \text{for all } \psi, \phi \in A.$$

Proof. If $\psi = 0$, then the inequality is trivially satisfied. Let $\phi, \psi \in A$ where $\psi \neq 0$, and define the following bilinear form

$$L(\psi, \phi) = d(\psi - \phi) - d(\phi) - d(\psi)$$

associated to the quadratic form d. Since d is a positive quadratic form, by A.1.1

we have for all $m, n \in \mathbb{Z}$,

$$mnL(\psi, \phi) = L(m\psi, n\phi) = d(m\psi - n\phi) - d(m\psi) - d(n\phi)$$

and thus

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi).$$

Now, we pick

$$m = -L(\psi, \phi) \qquad \text{and} \qquad n = 2d(\psi),$$

which gives us

$$0 \leq d(\psi)(4d(\psi)d(\phi) - L(\psi, \phi)^2).$$

This gives us the desired inequality because $\psi \neq 0$. □

We now proceed to show Hasse's bound.

Theorem 4.2.2 (Hasse's Bound)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Proof. We first choose a Weierstrass equation for E with coefficients in $\mathbb{F}_q$. Let $\phi : E \to E$, $(x, y) \mapsto (x^q, y^q)$ be the q^{th}-power Frobenius morphism. Since the Galois group $G_{\bar{\mathbb{F}}_q/\mathbb{F}_q}$ is (topologically) generated by the q^{th}-power map on $\bar{\mathbb{F}}_q$, we see that for any point $P \in E(\bar{\mathbb{F}}_q)$, we have

$$P \in E(\mathbb{F}_q) \text{ if and only if } \phi(P) = P,$$

in other words, P has coordinates in $\mathbb{F}_q$ if and only if it is fixed by the Galois group $G_{\bar{\mathbb{F}}_q/\mathbb{F}_q}$ which is generated by the Frobenius element ϕ. Thus we have $E(\mathbb{F}_q) = \ker(1 - \phi)$. By Theorem 4.1.1, $1 - \phi$ is separable, and thus by Theorem 3.2.7(c) we have

$$\#E(\mathbb{F}_q) = \ker(1 - \phi) = \deg_s(1 - \phi) = \deg(1 - \phi).$$

Since the degree map on $\mathrm{End}(E)$ is a positive quadratic form by Theorem 3.3.3.1, noting $\deg(\phi) = q$, Lemma 4.2.1 gives us the desired result

$$|\deg(1 - \phi) - \deg(\phi) - \deg(1)| \leq 2\sqrt{\deg(\phi)\deg(1)}$$
$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

□

Example 4.2.3. *Let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 = x^3 + 3$. We are going to calculate the points on $E(\mathbb{F}_7)$. Naturally, we have the prescribed point O. Calculations will show the rest are*

$$\{(1,2),(1,5),(2,2),(2,5),(3,3),(3,4),(4,2),(4,5),(5,3),(5,4),(6,3),(6,4)\}.$$

Therefore, $\#E(\mathbb{F}_7) = 13$. Applying Hasse's bound (Theorem 4.2.2), we get

$$|\#E(\mathbb{F}_7) - 7 - 1| = 5 \leq 2\sqrt{7} \approx 5.2915.$$

This is one example of where the Hasse bound is sharp.

4.3 Weil Conjectures

Having a sequence of integers $\{\#V(\mathbb{F}_{q^n})\}$, it is often useful to collect them into a generating series. The zeta function of a variety $V/\mathbb{F}_q$ is defined as follows:

Definition 4.3.1. *The zeta function of $V/\mathbb{F}_q$ is the power series*

$$Z(V/\mathbb{F}_q; T) \coloneqq \exp\left(\sum_{n=1}^{\infty} (\#V(\mathbb{F}_{q^n}))\frac{T^n}{n}\right),$$

where $\#V(\mathbb{F}_{q^n})$

For any power series $F(T) \in \mathbb{Q}[[T]]$ with no constant term, the power series $\exp(F(T))$ is defined to be the series $\sum_{k\geq 0} \frac{F(T)^k}{k!}$. From the definition, we can see we can recover the information on $\#V(\mathbb{F}_{q^n})$ from $Z(V/\mathbb{F}_q; T)$.

Below, we have a theorem that gives one part of the Weil Conjectures.

Theorem 4.3.2. *Let $E/\mathbb{F}_q$ be an elliptic curve and $\phi : E \to E$ be the q^{th}-power Frobenius endomorphism. Let $a = q + 1 - \#E(\mathbb{F}_q)$, and then let $\alpha, \beta \in \mathbb{C}$ be the roots of the polynomial $T^2 - aT + q$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$, and for every $n \geq 1$, we have*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

Proof. From the proof of Theorem 4.2.2, we see that $\#E(\mathbb{F}_q) = \deg(1 - \phi)$. We

then use Proposition 3.5.2 to compute the following:

$$\begin{aligned}\det(\phi_\ell) &= \deg(\phi) = q \\ \operatorname{tr}(\phi_\ell) &= 1 + \deg(\phi) - \deg(1-\phi) = 1 + q - \#E(\mathbb{F}_q) = a\end{aligned}$$

Hence the characteristic polynomial of ϕ_ℓ is

$$\det(T - \phi_\ell) = T^2 - tr(\phi_\ell)T + \det(\phi_\ell) = T^2 - aT + q = (T-\alpha)(T-\beta)$$

where the last equality comes from factoring over $\mathbb{C}$ since the coefficients a and q are both in $\mathbb{Z}$. For every rational number $m/n \in \mathbb{Q}$, we have

$$\det\left(\frac{m}{n} - \phi_\ell\right) = \frac{\det(m - n\phi_\ell)}{n^2} = \frac{\deg(m - n\phi)}{n^2} \geq 0.$$

Because $\det(T - \phi_\ell) \geq 0$ for all rationals $\mathbb{Q}$, we have the quadratic polynomial $\det(T - \phi_\ell) = T^2 - aT + q \in \mathbb{Z}[T]$ is nonnegative for all $T \in \mathbb{R} = \overline{\mathbb{Q}}$. Thus the polynomial either has complex conjugate roots, or it has a double root. In either case, we have $|\alpha| = |\beta|$. Then from $\alpha\beta = \det(\phi_\ell) = \deg(\phi) = q$, we have $|\alpha||\beta| = q$ and so $|\alpha| = |\beta| = \sqrt{q}$ as above. Similarly, for each integer $n \geq 1$, the $(q^n)^{th}$-power Frobenius endomorphism satisfies $\#E(\mathbb{F}_{q^n}) = \ker(1 - \phi^n) = \deg(1 - \phi^n)$ because ϕ^n fixes only $\mathbb{F}_{q^n}$, i.e. it fixes only points with coordinates in $\mathbb{F}_{q^n}$. By putting ϕ_ℓ in Jordan normal form, we can see the characteristic polynomial of ϕ_ℓ^n will be given by $\det(T - \phi_\ell^n) = (T - \alpha^n)(T - \beta^n)$. Therefore, we have

$$\begin{aligned}\#E(\mathbb{F}_{q^n}) &= \deg(1 - \phi^n) \\ &= \det(1 - \phi_\ell^n) && \text{from Proposition 3.5.2} \\ &= 1 - \alpha^n - \beta^n + q^n\end{aligned}$$

□

Since α, β are the roots of $1 - aT + qT^2$, the integer a determines what they can be. So the formula $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$ from Theorem 4.3.2 directly implies the number of $\mathbb{F}_q$-points in E fixes the number of $\mathbb{F}_{q^n}$-points for all n. This is a special property of elliptic curves defined over finite fields.

Remark. *Another way to see this is to look at the sequence*

$$a_n = q^n + 1 - \#E(\mathbb{F}_{q^n}), \qquad n \geq 1.$$

By convention let $a_0 = 2$, then we have the recurrence relation

$$a_{n+2} = a_1 a_{n+1} - q a_n \qquad \text{for all } n \geq 0.$$

To show this, let ϕ_ℓ be the map the Frobenius morphism induces on the Tate module $T_\ell(E)$ of E. By Proposition 3.5.2, we have

$$\mathrm{tr}(\phi_\ell^n) = 1 + \deg(\phi^n) - \deg(1 - \phi^n) = 1 + q^n - \#E(\mathbb{F}_{q^n}) = a_n.$$

Since ϕ_ℓ is a 2×2 matrix (if we fix a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$), let λ_1, λ_2 denote the two (possibly identical) eigenvalues of ϕ_ℓ. Then because the trace is the sum of eigenvalues, we have

$$\begin{aligned} a_1 a_{n+1} - q a_n &= \mathrm{tr}(\phi_\ell)\mathrm{tr}(\phi_\ell^{n+1}) - q\,\mathrm{tr}(\phi_\ell^n) \\ &= (\lambda_1 + \lambda_2)(\lambda_1^{n+1} + \lambda_2^{n+1}) - q(\lambda_1^n + \lambda_2^n) \\ &= \lambda_1^{n+2} + \lambda_2^{n+2} + \lambda_1\lambda_2^{n+1} + \lambda_1^{n+1}\lambda_2 - q(\lambda_1 + \lambda_2) \\ &= \lambda_1^{n+2} + \lambda_2^{n+2} + (\lambda_1\lambda_2 - q)(\lambda_1 + \lambda_2) \\ &= \mathrm{tr}(\phi_\ell^{n+2}) + (\det(\phi_\ell) - q)(\lambda_1 + \lambda_2) \\ &= a_{n+2} \end{aligned}$$

because $\det(\phi_\ell) = q$, giving us the desired recurrence relation. This recurrence relation also indicates all the subsequent a_n's are fixed by a_1, which we can obtained from the number of points in $E(\mathbb{F}_q)$.

Theorem 4.3.3 (Weil Conjectures for $E/\mathbb{F}_q$)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve.*

Then there is an $a \in \mathbb{Z}$ such that

$$Z(E/\mathbb{F}_q; T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}.$$

Furthermore,

$$Z(E/\mathbb{F}_q; 1/(qT)) = Z(E/\mathbb{F}_q; T)$$

and

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$

with $|\alpha| = |\beta| = \sqrt{q}$.

Proof. By definition of zeta function, we have

$$\begin{aligned}
\log(Z(E/\mathbb{F}_q;T)) &= \sum_{n=1}^{\infty}(\#E(\mathbb{F}_{q^n}))\frac{T^n}{n} \\
&= \sum_{n=1}^{\infty}\frac{(1-\alpha^n-\beta^n+q^n)T^n}{n} \qquad \text{by Theorem 4.3.2} \\
&= -\log(1-T)+\log(1-\alpha T) \\
&\quad +\log(1-\beta T)-\log(1-qT).
\end{aligned}$$

The last line follows from the Taylor series of $\log(1+x)$. Therefore we have

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1-aT+qT^2}{(1-T)(1-qT)}.$$

The functional equational above is satisfied as follows:

$$\begin{aligned}
Z(E/\mathbb{F}_q;1/(qT)) &= \frac{1-a(1/(qT))+q(1/(qT)^2)}{(1-(1/(qT)))(1-q(1/(qT)))} \\
&= \frac{1-a(1/(qT))+q(1/(qT)^2)}{(1-(1/(qT)))(1-(1/(T)))} \\
&= \frac{T^2-a(1/q)T+(1/q)}{(T-(1/q))(T-1)} \\
&= \frac{qT^2-aT+1}{(qT-1)(T-1)} \\
&= \frac{qT^2-aT+1}{(1-qT)(1-T)} \\
&= Z(E/\mathbb{F}_q;T).
\end{aligned}$$

The last assertion of the theorem also comes directly from Theorem 4.3.2. □

Remark. *Note that the numerator of $Z(E/\mathbb{F}_q;T)$, $1-aT+qT^2$, is a polynomial of degree 2. This is precisely double of the genus of a torus, which every elliptic curve is isomorphic to over $\mathbb{C}$. [Sil09, Chapter VI, §5, Corollary 5.1.1] This is not just a mere coincidence. In fact, the degree of the polynomial in the numerator is the first Betti number of the torus, which, for a closed orientable surface, is double of its genus. This is also part of the more general Weil Conjectures for projective algebraic varieties.*

The remark above illustrates why the Weil Conjectures are so interesting. There are seemingly deep connections between the physical (or geometrical) properties of

a curve, which in our case is the topology of the complex points on a variety V, and the number theoretic properties, the number points of variety V over finite fields.

4.4 L-function

Let K be a local field, complete with respect to a discrete valuation v. Let R be the ring of integers of K. Let $\mathcal{M}$ be the unique maximal ideal of R and $k = R/\mathcal{M}$ be the residue field of R.

There are many possible Weierstrass equations for an elliptic curve E. We want to choose one such that the reduction properties over maximal ideal $\mathcal{M}$ is as good as possible. The idea is to minimize the "zeroness" of the discriminant with respect to the maximal ideal we are reducing by, i.e. we want to minimize the discriminant with respect to the given valuation v. We call such an equation a minimal Weierstrass equation for E at v.

Definition 4.4.1. *Let E/K be an elliptic curve and v be the valuation. A Weierstrass equation for E is called* ***minimal (Weierstrass) equation for E at v*** *if $v(\Delta)$ is minimized subject to a restriction on the coefficients $a_1, a_2, a_3, a_4, a_6 \in R$.*

In the case of $E/\mathbb{Q}$ and reduction over p, we want to pick a Weierstrass equation such that the cubic has the largest obtainable number of distinct roots mod p and the power of p in the discriminant Δ is as small as possible for each p. The existence of a minimal Weierstrass equation is guaranteed by the discreteness of the valuation v.

Proposition 4.4.2. *Every elliptic curve E/K has a minimal Weierstrass equation.*

Here we define the good and bad reduction of an elliptic curve.

Definition 4.4.3. *Let E/K be an elliptic curve, and let $\tilde{E}$ be the reduction modulo $\mathcal{M}$ of a minimal Weierstrass equation for E. Then*

- *E has* ***good (or stable)*** *reduction if $\tilde{E}$ is nonsingular.*
- *E has* ***multiplicative (semistable)*** *reduction if $\tilde{E}$ has a node.*
- *E has* ***additive (or unstable)*** *reduction if $\tilde{E}$ has a cusp.*

For multiplicative reduction, it is called split if the slopes of the tangent lines at the node of $\tilde{E}$ are in k, non-split otherwise.

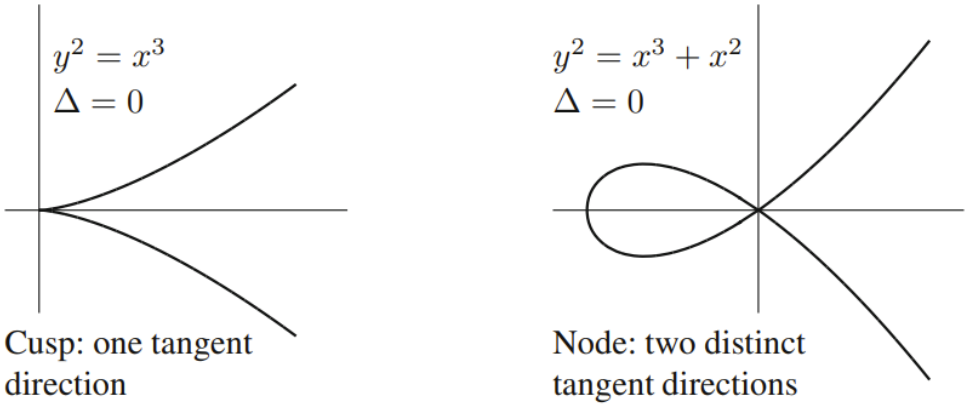

Figure 4.1: Two singular curves. [Sil09, Chapter III, §1, Figure 3.2]

Remark. *Cusp means there is one tangent direction at the singular point and node means there are two distinct tangent direction at the singular point, as shown in Figure 4.1.*

Example 4.4.4. *[Was08, Section 14.2, Example 14.1]*
Suppose we start with the Weierstrass equation

$$y^2 = x^3 - 270000x + 128250000.$$

The discriminant of this cubic is $-2^8 3^{12} 5^{12} 11$*, so* E *has good reduction everywhere except possibly at* $2, 3, 5, 11$*. Let us apply the change of variables* $x = 25x_1, y = 125y_1$*, which transforms the equation into*

$$y_1^2 = x_1^3 - 432x_1 + 8208.$$

The discriminant of this new cubic is $-2^8 3^{12} 11$*, so this indicates* E *also has good reduction at* 5*. Now, a second change of variables* $x_1 = 9x_2 - 12, y_1 = 27y_2$ *will change the equation to*

$$y_2^2 = x_2^3 - 4x_2^2 + 16.$$

The discriminant of this cubic is $-2^8 11$*, thus* E *has good reduction at* 3*. A final change of variables* $x_2 = 4x_3, y_2 = 8y_3 + 4$ *will change the equation of* E *to*

$$y_3^2 + y_3 = x_3^3 - x_3^2.$$

This is nonsingular at 2 *since the partial derivative with respect to* y

$$2y + 1 \equiv 1 \not\equiv 0 \mod 2$$

is nonzero. Therefore, E *has good reduction at* 2*. If we look at the discriminant of the cubic, it is* -11*. Since any change of variables can be shown to change the discriminant by a square, the last equation is actually a minimal Weierstrass equation for* E *at all of the finite places (look at the discriminant), and thus is the minimal Weierstrass equation. Looking at the situation at* 11 *a bit more closely, we see the polynomial in* x_2 *factors as*

$$x_2^3 - 4x_2^2 + 16 \equiv (x_2 + 1)^2(x_2 + 5) \mod 11.$$

Because of the 2 *in the exponent of* $(x + 1)$*, we know the singular point is going to be at* $x = -1$*, and hence* $y = 0$*, and it is going to be a node. To find the tangents at the singular point, look at the line given by* $y = mx + c$*. For it to past through the curve at the point* $(-1, 0)$*, we need to have* $c = m$*. Substituting* $y = mx + m$ *into the equation* $y^2 = x^3 - 4x^2 + 5$*, we get*

$$m^2x^2 + 2m^2x + m^2 = x^3 - 4x^2 + 5 \tag{4.1}$$

$$\implies x^3 + (-m^2 - 4)x^2 - 2m^2x + 5 - m^2 = 0. \tag{4.2}$$

To be a tangent line to the elliptic curve at $(-1, 0)$*, it needs to intersect the curve to order* 3*, in other words the polynomial 4.2 needs to have a zero of order* 3 *at* $x = -1$*, i.e.*

$$x^3 + (-m^2 - 4)x^2 - 2m^2x + 5 - m^2 \equiv (x + 1)^3 \mod 11.$$

Expanding the right hand side and matching the coefficients give us $m^2 \equiv 4 \mod 11$*. So the slopes of the tangents at* $(-1, 0)$ *are* ± 2 *which is in* $\mathbb{F}_{11}$*. Therefore,* E *has split multiplicative reduction at* 11*.*

Definition 4.4.5.

$$L_p(T) = \begin{cases} 1 - a_pT + pT^2, & \text{if } E \text{ has good reduction at } p, \\ 1 - T, & \text{if } E \text{ has split multiplication reduction at } p, \\ 1 + T, & \text{if } E \text{ has non-split multiplication reduction at } p, \\ 1, & \text{if } E \text{ has additive reduction at } p, \end{cases}$$

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

Definition 4.4.6 (L-function of an Elliptic Curve E over $\mathbb{Q}$)**.**

$$L(s,E) = \prod_p \frac{1}{L_p(p^{-s})}$$

where the product is over all primes p.

Remark. *It can also be defined through combining all of the numerators of the zeta function for E for all prime p, i.e.*

$$L(s,E) = \prod_p \frac{1}{\text{num}(Z(E/\mathbb{F}_q; p^{-s}))}$$

We can expand the L-function into a Dirichlet series

$$\sum_{n=1} \frac{b_n}{n^s}.$$

To find b_n, we look closer at the product in Definition 4.4.6

$$\begin{aligned}\prod_p \frac{1}{L_p(p^{-s})} &= \prod_{p \text{ good}} \frac{1}{1 - a_p p^{-s} + p^{-2s+1}} \times \prod_{p \text{ additive}} 1 \\ &\quad \times \prod_{p \text{ split multiplicative}} \frac{1}{1-p^{-s}} \times \prod_{p \text{ non-split multiplicative}} \frac{1}{1+p^{-s}} \\ &= \prod_{p \text{ good}} \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})} \times \prod_{p \text{ additive}} 1 \\ &\quad \times \prod_{p \text{ split multiplicative}} \frac{1}{1-p^{-s}} \times \prod_{p \text{ non-split multiplicative}} \frac{1}{1+p^{-s}}\end{aligned}$$

because $1 - a_p T + qT^2 = (1-\alpha_p T)(1-\beta_p T)$ by Theorem 4.3.3 for all p. Each linear factor in the denominator can be expanded as a geometric series

$$\frac{1}{1-\gamma p^{-s}} = \sum_{k=0}^{\infty} (\gamma p^{-s})^k,$$

thus we have

$$\sum_{n=1}^{\infty} \frac{b_n}{n^s} = \prod_{p \text{ good}} (1 + \alpha_p p^{-s} + \alpha_p^2 p^{-2s} + \cdots)(1 + \beta_p p^{-s} + \beta_p^2 p^{-2s} + \cdots) \tag{4.3}$$
$$\times \prod_{p \text{ additive}} 1 \times \prod_{p \text{ split multiplicative}} (1 + p^{-s} + p^{-2s} + \cdots)$$
$$\times \prod_{p \text{ non-split multiplicative}} (1 - p^{-s} + p^{-2s} - \cdots)$$

So finding b_n boils down to finding how many ways we can form $1/n^s$. First, we observe for $m, n \in \mathbb{Z}_{\geq 1}$ such that $\gcd(m, n) = 1$, none of the primes in m will contribute to $1/n^s$ and vice versa. Therefore, the number of ways to form $1/(mn)^s$ is equal to the product of the ways to form $1/n^s$ and $1/m^s$. In other words,

$$b_{mn} = b_m b_n \qquad \text{if } \gcd(m, n) = 1,$$

i.e. the sequence $\{b_n\}$ is multiplicative. So it suffices to describe b_1 and b_{p^r} for all primes p and $r \in \mathbb{Z}_{\geq 1}$.

It is clear that $b_1 = 1$ from (4.3). For each prime p, the number b_{p^r} can be determined entirely from the corresponding Euler factor

$$\frac{1}{L_p(p^{-s})} = \sum_{r=0}^{\infty} \frac{b_{p^r}}{(p^r)^s}.$$

1. If p is a prime of additive reduction, then $b_{p^r} = 0$ for all $r \in \mathbb{Z}_{\geq 1}$.

2. If p is a prime of split multiplicative reduction, then $b_{p^r} = 1$ for all $r \in \mathbb{Z}_{\geq 1}$.

3. If p is a prime of non-split multiplicative reduction, then $b_{p^r} = (-1)^r$ for all $r \in \mathbb{Z}_{\geq 1}$.

4. If p is a prime of good reduction, then $b_1 = 1, b_p = a_p$, and the rest follows from the following recurrence relation

$$b_{p^r} = b_p b_{p^{r-1}} - p b_{p^{r-2}} \qquad \text{for } r \geq 2.$$

To see this, let

$$\sum_{r=0}^{\infty} \frac{b_{p^r}}{(p^r)^s} = (1 + \frac{\alpha_p}{p^s} + \frac{\alpha_p^2}{p^{2s}} + \cdots)(1 + \frac{\beta_p}{p^s} + \frac{\beta_p^2}{p^{2s}} + \cdots) \tag{4.4}$$

where $1 - a_pT + qT^2 = (1 - \alpha_pT)(1 - \beta_pT)$. With $\alpha_p\beta_p = p$ and $\alpha_p + \beta_p = a_p$, we can expand the RHS of (4.4) to get

$$\begin{aligned} b_p &= \alpha_p + \beta_p = a_p \\ b_{p^2} &= \alpha_p^2 + \alpha_p\beta_p + \beta_p^2 = (\alpha_p + \beta_p)^2 - \alpha_p\beta_p = a_p^2 - p \\ b_{p^3} &= \alpha_p^3 + \alpha_p^2\beta_p + \alpha_p\beta_p^2 + \beta_p^3 = (\alpha_p + \beta_p)^3 - 2\alpha_p\beta_p(\alpha_p + \beta_p) = a_p^3 - 2pa_p \\ &\vdots \end{aligned}$$

We observe that

$$b_{p^r} = \sum_{m=0}^{r} \alpha_p^{r-m}\beta_p^m.$$

With the identity

$$\sum_{m=0}^{r} \alpha_p^{r-m}\beta_p^m = (\alpha_p + \beta_p)\sum_{m=0}^{r-1} \alpha_p^{r-1-m}\beta_p^m - \alpha_p\beta_p\sum_{m=0}^{r-2} \alpha_p^{r-2-m}\beta_p^m,$$

we have the recursion pattern

$$b_{p^r} = b_p b_{p^{r-1}} - pb_{p^{r-2}} \qquad \text{for } r \geq 2,$$

with $b_1 = 1$ and $b_p = a_p$.

Remark. *Note the recursion pattern can also be deduced from looking at the behaviour of the coefficient of a Hecke eigenform. Refer to Chapter 5 for more details, in particular Subsection 5.2.3 and Theorem 5.4.2.*

To show convergence of the Euler product/Dirichlet series in a half plne, we first state the following proposition:

Proposition 4.4.7. *[Hus10, Chapter 11, §6, Corollary 6.5]*
A quadratic Euler product

$$\prod_p \frac{1}{1 - a_pp^{-s} + p^{c-2s}}$$

converges for $\mathrm{Re}(s) > 1 + c/2$ *when* $|a_p| \leq 2p^{c/2}$ *for each* p.

With Proposition 4.4.7, convergence of the L-function $L(s, E)$ in the half plane $\mathrm{Re}(s) > 3/2$ follows directly from Hasse's bound [Theorem 4.2.2].

Example 4.4.8. *Going back to the elliptic curve $E/\mathbb{Q}$ in Example 4.4.4 given by the Weierstrass equation*

$$y^2 + y = x^3 - x^2.$$

We have established that it has good reduction everywhere except at $p = 11$, where it has split multiplicative reduction. So its L-function looks like

$$L(s, E) = \prod_{p \neq 11} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \times \frac{1}{1 - (11)^{-s}}.$$

When expanded, it will have the form

$$L(s, E) = \frac{1}{1^s} - \frac{2}{2^s} - \frac{1}{3^s} + \frac{2}{4^s} + \frac{1}{5^s} + \frac{2}{6^s} - \frac{2}{7^s} - \frac{2}{9^s} - \frac{2}{10^s} + \frac{1}{11^s} + \cdots$$

To preface the next section on modular forms, we state the following fact. The following complex-valued function on the upper half plane $\mathcal{H}$

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots$$

where $q = e^{2\pi i \tau/11}, \tau \in \mathcal{H}$, is a modular form. In fact, it is a cusp form. Notice how the first few coefficients of the modular form and the L-function from Example 4.4.8 are matching up. Further calculations to higher precision will still match up. In fact, they will always match up. Several more examples of these pairings of elliptic curves and modular forms will give us the following questions: Can we always create a modular form from the L-function of an elliptic curve? And conversely, does every modular form have a corresponding elliptic curve such that the coefficients of the modular form "matches" with the coefficients of the L-function?

Chapter 5

Application of Modularity

Notation: $\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$

5.1 Modular Forms

5.1.1 Congruence subgroups

We begin with the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. Let

$$\Gamma(N) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N \right\}$$

denote the principal congruence subgroup of level N.

Definition 5.1.1. *A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a **congruence subgroup** if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{Z}^+$. We call such a subgroup Γ a congruence subgroup of level N if N is minimal such that $\Gamma(N) \subseteq \Gamma$.*

Remark. *Since*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} (1 - \frac{1}{p^2}),$$

this gives us many subgroups of finite index. Note, not all subgroups of finite index are congruence subgroups, this is known as the congruence subgroup problem.

Here are some important examples of congruence subgroups.

Example 5.1.2.

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \bmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N \right\}$$

For these congruence subgroups, we have the following inclusion,

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

5.1.2 Modular Forms

The group $\mathrm{GL}_2^+(\mathbb{R})$ acts on the upper half plane $\mathcal{H}$ in the following way, for each $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2^+(\mathbb{R})$ and $\tau \in \mathcal{H}$, we have

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

Definition 5.1.3. *Let $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ and k be an integer. We define the* ***weight-k operator*** *$[\gamma_k]$ on functions $f : \mathcal{H} \to \mathbb{C}$ as follows:*

$$(f[\gamma]_k)(\tau) = (\det(\gamma))^{k/2}(c\tau + d)^{-k} f(\gamma(\tau)), \quad \forall \tau \in \mathcal{H}.$$

Remark. *Since $(c\tau + d)$ is never zero or infinity on $\mathcal{H}$, if f is meromorphic, then $f[\gamma]_k$ is also meromorphic and has the same zeros and poles as f.*

Definition 5.1.4. *A meromorphic function f on $\mathcal{H}$ is* ***weakly modular of weight k with respect to*** *Γ if*

$$f(\tau) = (c\tau + d)^{-k} f(\gamma(\tau)) = (f[\gamma]_k)(\tau), \quad \forall \tau \in \mathcal{H}, \gamma \in \Gamma.$$

In other words, it is weight-k invariant under the congruence subgroup Γ. Do note $\det(\gamma) = 1$ for all $\gamma \in \Gamma$.

Definition 5.1.5. *Let k be an integer and Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A function $f : \mathcal{H} \to \mathbb{C}$ is a* ***modular form of weight k with respect to*** *Γ if f satisfies all of these properties:*

- *f is holomorphic on $\mathcal{H}$.*
- *f is weight-k invariant under Γ.*
- *$f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.*

It is common to call f a modular form of level N when Γ is a congruence subgroup of level N.

Remark (Holomorphic at ∞)**.** *Since $\Gamma(N)$ contains the translation matrix*

$$\begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} : \tau \mapsto \tau + N,$$

every meromorphic function $f : \mathcal{H} \to \mathbb{C}$ that is weight-k invariant with respect to Γ is $N\mathbb{Z}$-periodic. Let $D = \{q \in \mathbb{C} \mid |q| < 1\}$ be the open complex unit disk, and let $D' = D - \{0\}$ be the punctured disk. Then

$$\mathcal{H} \to D', \quad \tau \mapsto e^{2\pi i \tau / N}$$

is an $N\mathbb{Z}$-periodic map. So the function g corresponding to f, defined as follows

$$g : D' \to \mathbb{C}, \quad g(q) = f(N \log(q)/(2\pi i))$$

is well defined even though the logarithm is determined only up to $2\pi i\mathbb{Z}$.

Since f is holomorphic on the upper half plane, the composition g is then holomorphic on the punctured disk since the logarithm can be defined holomorphically about each point, and so g has a Laurent expansion $g(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ for $q \in D'$. The relation $|q| = e^{-2\pi \mathrm{Im}(\tau)}$ shows that $q \to 0$ as $\mathrm{Im}(\tau) \to \infty$. So we define f to be ***holomorphic at*** *∞ if the corresponding g extends holomorphically to the puncture point $q = 0$, or equivalently, the Laurent series sums over non-negative integers $n \in \mathbb{N}$. From this, we also get that a modular form f of weight k with respect to a congruence subgroup Γ of level N has a Fourier expansion at ∞*

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i \tau / N}, a_n(f) \in \mathbb{C}.$$

Usually we omit the f and simplify $a_n(f)$ to a_n.

Example 5.1.6 (Eisenstein series)**.** *The Eisenstein series G_{2k} is given by*

$$G_{2k}(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

where $\sigma_l(n) = \sum_{0<d|n} d^l$ is the sum of the l-th powers of the positive divisors of n, and $q = e^{2\pi i \tau}$. It is a family of modular forms of even weight $2k$ with respect to the modular group $\mathrm{SL}_2(\mathbb{Z})$.

Definition 5.1.7. *A cusp form of weight k with respect to Γ is a modular form of weight k with respect to Γ whose Fourier expansion at any cusp has leading coefficient*

$a_0 = 0$, *i.e.*

$$f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i \tau / N}.$$

Example 5.1.8 (Modular discriminant)**.** *The modular discriminant form Δ is defined as follows*

$$\Delta(\tau) = -16(4(-15G_4(\tau))^3 + 27(-35G_6(\tau))^2).$$

This is a modular form of weight 12 for $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$, therefore it is of level 1. $\Delta(\tau)$ has a simple zero at ∞ and no other zeros. The q-expansion of Δ is

$$q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 + \cdots$$

[LMFDB, Modular Form 1.12.a.a]. Evidently from the q-expansion, the modular discriminant Δ is a cusp form.

The set of modular forms of weight k with respect to Γ is denoted $\mathcal{M}_k(\Gamma)$ and the subset of cusp forms of weight k with respect to Γ is denoted with $\mathcal{S}_k(\Gamma)$. They are both finite-dimensional $\mathbb{C}$-vector spaces, with $\mathcal{S}_k(\Gamma)$ forming a $\mathbb{C}$-linear subspace of $\mathcal{M}_k(\Gamma)$. [Zag08, Chapter 1, §3, Proposition 3]

Definition 5.1.9. *A modular form is said to be* ***normalised*** *if the first nonzero coefficient of its q-expansion is equal to* 1*.*

Proposition 5.1.10. *Let $k \geq 2$ and let Γ be a congruence subgroup. Let Γ' be another congruence subgroup contained in Γ. Then any modular form f of weight k for Γ is also a modular form of the same weight for Γ'. Therefore, $\mathcal{M}_k(\Gamma)$ is a $\mathbb{C}$-linear subspace of $\mathcal{M}_k(\Gamma')$ and $\mathcal{S}_k(\Gamma) \subseteq \mathcal{S}_k(\Gamma')$.*

Let $N \geq 1$ and M be a positive divisor of N. Then $\Gamma(N) \leq \Gamma(M)$. So Proposition 5.1.10 implies the $M_k(\Gamma(M)) \subseteq M_k(\Gamma(N))$. Also, suppose that $N = MM'$, where $1 < M, M' < N$ so that M and M' are proper divisors of N, and $g(\tau) \in M_k(\Gamma(M))$. Then, we can show that $f(\tau) \coloneqq g(M'\tau) \in M_k(\Gamma(N))$. To see this, let $\gamma \in \Gamma(N)$. Then by definition,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod N.$$

Since M is a proper divisor of N, it implies

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mod M,$$

i.e. $\gamma \in \Gamma(M)$. So, we have

$$\begin{aligned} f[\gamma]_k(\tau) &= (c\tau + d)^{-k} f(\gamma(\tau)) \\ &= (c\tau + d)^{-k} g(M'\gamma(\tau)) \\ &= (c\tau + d)^{-k} g\left(\frac{a(M'\tau) + M'b}{c\tau + d}\right) \\ &= (\frac{c}{M'}(M'\tau)\tau + d)^{-k} g\left(\frac{a(M'\tau) + M'b}{\frac{c}{M'}(M'\tau)\tau + d}\right) \\ &= \left(g \begin{bmatrix} a & M'b \\ c/M' & d \end{bmatrix}_k\right)(M'\tau) \\ &= g(M'\tau) = f(\tau) \end{aligned}$$

because $\left[\begin{smallmatrix} a & M'b \\ c/M' & d \end{smallmatrix}\right] \in \Gamma(M)$ and $g \in \mathcal{M}_k(\Gamma(M))$, thus weight-$k$ invariant under $\Gamma(M)$.

Definition 5.1.11. *Let $N, k \geq 1$ be integers. A modular form of weight k for $\Gamma(N)$ is said to be an **old form** if:*

(a) There are some positive divisor M of N such that $f(z)$ is a modular form in the space $M_k(\Gamma(M))$; or,

(b) $N = MM'$ and $f(z) = g(M'z)$, for some $g \in M_k(\Gamma(M))$; or,

(c) $f(z)$ is a $\mathbb{C}$-linear combination of forms of (a) and (b).

The $\mathbb{C}$-linear subspace spanned by the set of all old forms of $M_k(\Gamma(N))$ is usually denoted by $M_k^{old}(\Gamma(N))$. We also define $S_k^{old}(\Gamma(N)) \coloneqq M_k^{old}(\Gamma(N)) \cap S_k(\Gamma(N))$ to be the space of all old cusp forms.

5.1.3 Petersson Inner Product

Let Γ be a congruence subgroup and $\mathcal{D}$ be a fundamental domain of Γ. Let D^* denote a fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$, then $\mathcal{D}$ is the union of (almost disjoint) translates of D^*:

$$\mathcal{D} = \bigcup_j \alpha_j D^*$$

where $\{\alpha_j\}$ is a set of coset representatives for $(\pm 1 \cdot \Gamma)\backslash \mathrm{SL}_2(\mathbb{Z})$.

Let $X(\Gamma) = \Gamma\backslash\mathcal{H}$. Let $\phi : \mathcal{H} \to \mathbb{C}$ be a function on the upper half plane. If ϕ is Γ-invariant, we may then define the integral of ϕ on $X(\Gamma)$ as:

$$\begin{aligned}\int_{X(\Gamma)} \phi(\tau)d\mu(\tau) &= \sum_j \int_{\alpha_j D^*} \phi(\tau)d\mu(\tau) = \sum_j \int_{D^*} \phi(\alpha_j(\tau))d\mu(\alpha_j(\tau)) \\ &= \sum_j \int_{D^*} \phi(\alpha_j(\tau))d\mu(\tau).\end{aligned}$$

Since ϕ is Γ-invariant, the last term in the above equality shows that the definition is independent of the choice of coset representatives. So we may calculate the covolume of Γ as follows:

$$\text{covol}(\Gamma) = \int_{X(\Gamma)} d\mu(\tau) = [\text{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]\text{covol}(\text{SL}_2(\mathbb{Z})) = \frac{\pi}{3}[\text{PSL}_2(\mathbb{Z}) : \overline{\Gamma}].$$

Let $f, g \in \mathcal{S}_k(\Gamma)$ be two cusp forms for Γ of weight k, and set $\phi(\tau) = f(\tau)\overline{g(\tau)}\text{Im}(\tau)^k$. We then have the following lemma:

Lemma 5.1.12. *The function ϕ is Γ-invariant, and for all $\alpha \in \text{SL}_2(\mathbb{Z})$, the translate $\phi(\alpha(\tau))$ is bounded on D^*.*

Proof. For $\gamma \in \Gamma$, we have

$$\begin{aligned}\phi(\gamma(\tau)) &= f(\gamma(\tau))\overline{g(\gamma(\tau))}\text{Im}(\gamma(\tau))^k \\ &= (c\tau + d)^k f(\tau)\overline{(c\tau + d)^k g(\tau)}|cz + d|^{-2k}\text{Im}(\tau)^k \\ &= \phi(\tau).\end{aligned}$$

For $\alpha \in \text{SL}_2(\mathbb{Z})$, we have

$$\begin{aligned}\phi(\alpha(\tau)) &= f(\gamma(\tau))\overline{g(\gamma(\tau))}\text{Im}(\gamma(\tau))^k \\ &= f[\alpha]_k\overline{g[\alpha]_k}\text{Im}(\tau)^k \\ &= O(q)\overline{O(q)}y^k = O(|q|^2 y^k),\end{aligned}$$

where $y = \text{Im}(\tau)$ and q comes from the q expansions of f and g. So this approaches 0 as y approaches infinity, because $q = e^{2\pi i\tau/k} = e^{2\pi i(x+iy)/k}$. This gives the boundedness in the lemma. □

This lemma allows us to define an inner product on the spaces of cusp forms:

Definition 5.1.13. *The **Petersson inner product** of f and g is:*

$$\langle f, g\rangle_\Gamma = \frac{1}{\text{covol}(\Gamma)} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)}\text{Im}(\tau)^k d\mu(\tau).$$

Remark. *The reason to divide by* $\text{covol}(\Gamma)$ *is that if we have two congruence subgroups such that* $\Gamma \subseteq \Gamma'$*, then*

$$\langle f, g\rangle_\Gamma = \langle f, g\rangle_{\Gamma'}.$$

Remark. *For the above integral to converge, it is enough to just have one of f or g be a cusp form. Therefore it is well-defined to extend it to an inner product between a modular form and a cusp form. So we can still define the orthogonal complement of $\mathcal{S}_k(\Gamma)$ in the space of modular forms $\mathcal{M}_k(\Gamma)$:*

$$\mathcal{E}_k(\Gamma) = \{f \in \mathcal{M}_k(\Gamma) \mid \langle f, g\rangle_k = 0 \ \ \forall g \in \mathcal{S}_k(\Gamma)\},$$

this is called the Eisenstein space of $\mathcal{M}_k(\Gamma)$. As the name suggests, this is the space of Eisenstein series. In other words, the space of modular forms can be broken down into a direct sum of cusp forms and Eisenstein series.

Here we define the orthogonal complement of the old forms $\mathcal{S}_k^{old}(\Gamma(N))$ in the space $\mathcal{S}_k(\Gamma(N))$:

Definition 5.1.14. *Let $N, k \geq 1$. Let $S_k^{old}(\Gamma(N))$ be the subspace of $S_k(\Gamma(N))$ of old forms. We define a new subspace of **new forms**, denoted $S_k^{new}(\Gamma(N))$ as the orthogonal complement of $S_k^{old}(\Gamma(N))$ in $S_k(\Gamma(N))$ with respect to the Petersson inner product, i.e.*

$$\begin{aligned} S_k^{new}(\Gamma(N)) &\coloneqq S_k^{old}(\Gamma(N))^\perp \\ &= \{f(z) \in S_k(\Gamma(N)) \mid \langle f(z), g(z)\rangle = 0 \text{ for all } g \in S_k^{old}(\Gamma(N))\} \end{aligned}$$

5.2 Hecke Operators

5.2.1 W_N operators

Define the operator W_N on $\mathcal{M}_k(\Gamma_1(N))$ as follows:

$$\begin{aligned} W_N : M_k(\Gamma_1(N)) &\to M_k(\Gamma_1(N)), \\ f &\mapsto i^k N^{1-k/2} f[\left[\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right]]_k = i^k N^{-k/2} \tau^{-k} f(-1/(N\tau)). \end{aligned}$$

Proposition 5.2.1. *[Loz11, Chapter 4, §4, Proposition 4.4.2] Let $N, k \geq 1$ and let $f(\tau) \in \mathcal{S}_k(\Gamma_0(N))$. Then*

- *$W_N(f)$ is also a modular form in $\mathcal{S}_k(\Gamma_0(N))$;*
- *W_N is $\mathbb{C}$-linear; and*
- *The square of W_N is the identity, i.e. $W_N(W_N(f)) = f$.*

We will use the operator W_N to decompose the space $\mathcal{S}_k(\Gamma_0(N))$ in later subsections.

5.2.2 Diamond operators $\langle\delta\rangle$

Let $\delta \in \mathbb{Z}$ be fixed. Let $M = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_0(N)$ such that $d \equiv \delta \bmod N$.

The **diamond operator** $\langle\delta\rangle$ is a linear map

$$\langle\delta\rangle : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N)), \tag{5.1}$$

$$(\langle\delta\rangle f)(z) = (cz + d)^{-k} f(Mz). \tag{5.2}$$

The definition of $\langle\delta\rangle$ does not depend on the choice of M, thus $\langle\delta\rangle$ is determined by the value $\delta \bmod N$. In other words, there are N distinct diamond operators, one for each value $0, 1, \ldots, N-1$. Note that $\langle 1\rangle f = f$ because we can pick $M = \mathrm{id}$.

Here are some properties of the diamond operator $\langle\delta\rangle$.

Proposition 5.2.2. *Let $N, k \geq 1$ be fixed integers and let $\delta, \delta' \in \mathbb{Z}$ be integers with $(\delta\delta', N) = 1$. Then*

$$\langle\delta'\rangle(\langle\delta\rangle f) = \langle\delta\rangle(\langle\delta'\rangle f) = \langle\delta'\delta\rangle f.$$

In particular, $\langle\delta\rangle^{\phi(N)} = \langle 1\rangle = \mathrm{id}$ and the eigenvalues of $\langle\delta\rangle$ must be roots of unity of order dividing $\phi(N)$, where ϕ is the Euler phi function. Proposition 5.2.2 also shows the diamond operators with $\gcd(\delta, N) = 1$ form a group under multiplication.

Let $\mu_{\phi(N)}$ be the set of all roots of unity of order dividing $\phi(N)$. Then for each $\delta \in \mathbb{Z}$ and every $\xi \in \mu_{\phi(N)}$, there is an eigenspace of $M_k(\Gamma_1(N))$ formed by eigenvectors of $\langle\delta\rangle$ with eigenvalues ξ. There is also another decomposition of $M_k(\Gamma_1(N))$ with respect to the diamond operator $\langle\delta\rangle$.

Proposition 5.2.3. *Let $N, k \geq 1$ be fixed integers. For every group homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, i.e. a character, we define the subspace:*

$$M_k(N, \chi) = \{f \in M_k(\Gamma_1(N)) \mid \langle\delta\rangle f = \chi(\delta) f \text{ for all } \delta \in (\mathbb{Z}/N\mathbb{Z})^\times\}.$$

Then we have $M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(N, \chi)$*, where the direct sum is over all possible characters* χ *of* $(\mathbb{Z}/N\mathbb{Z})^\times$*.*

Remark. *If* χ_0 *is the trivial character, i.e.* $\chi_0(\delta) = 1$ *for all* $(\delta, N) = 1$*, then* $M_k(N, \chi_0) = M_k(\Gamma_0(N))$*.*

5.2.3 T_n operators

Let $f(\tau) \in M_k(N, \chi)$ and suppose that $f(\tau)$ has the q-expansion $f(\tau) = \sum_{n\geq 0} a_n q^n$ where $q = e^{2\pi i \tau}$. Let $p \geq 2$ be a prime.

We define the operator T_p as follows:

$$T_p(f)(\tau) = \frac{1}{p}\sum_{j=0}^{p-1} f(\frac{\tau + j}{p}) + \chi(p)p^{k-1}f(p\tau)$$

where $\chi(p) = 0$ if $N \equiv 0 \bmod p$. Equivalently, we can define $T_p(f)$ to be

$$T_p(f)(\tau) = \sum_{n\geq 0} b_n q^n$$

with $b_n = a_{pn} + \chi(p)p^{k-1}a_{n/p}$ where $a_{n/p} = 0$ if $n \not\equiv 0 \bmod p$. Then we define the general T_n operators for $n \geq 1$ as follows:

- If $n = p^r$ where $r \geq 1$ and $p \mid N$, then:

  $$T_{p^r} = (T_p)^r,$$

  where the product means T_p composed with itself r times.

- If $n = p^r$ and $p \nmid N$, then T_{p^r} can be calculated with the recurrence relation:

  $$T_p \cdot T_{p^r} = T_{p^{r+1}} + p^{k-1}\langle p\rangle T_{p^{r-1}}.$$

- If $(n, m) = 1$, then:

  $$T_{nm}(f) = (T_n \cdot T_m)(f) = (T_m \cdot T_n)(f) = T_m(T_n(f)).$$

There are numerous equivalent ways to define the Hecke operators. It can either be defined as above, or as a function on lattices, or as a double coset operator.

Each Hecke operator T_n defines a linear map

$$T_n : M_k(N, \chi) \to M_k(N, \chi).$$

What might be surprising is there are modular forms that are eigenvectors for all of the Hecke operators.

Definition 5.2.4. *Let $f \in M_k(N, \chi) \subseteq M_k(\Gamma_1(N))$. We say f is an **eigenform** if f is an eigenvector for all Hecke operators $T_n, n \geq 1$, i.e. there exists $\lambda_n \in \mathbb{C}$ such that*

$$T_n(f) = \lambda_n f \quad \forall n \geq 1.$$

Theorem 5.2.5. *Let $k \geq 1$ and suppose that f is an eigenform in the space $M_k(N, \chi) \subseteq M_k(\Gamma_1(N))$, with $T_n(f) = \lambda_n f$ for all $n \geq 1$. Suppose further that f has a q-expansion of the form $f(\tau) = \sum_{n \geq 0} a_n q^n$, then:*

1. *$a_1 \neq 0$ and $a_n = \lambda_n a_1$ for all $n \geq 1$, and*
2. *if $a_0 \neq 0$ [i.e. not a cusp form], then the eigenvalues are given by the formula*

$$\lambda_n = \sum_{d|n} \chi(d) d^{k-1}.$$

Definition 5.2.6. *An eigenform $f \in M_k(N, \chi) \subseteq M_k(\Gamma_1(N))$ is said to be **normalised** if $a_1 = 1$.*

Proposition 5.2.7. *Let $f \in \mathcal{M}_k(N, \chi)$ be a modular form with Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$. Then f is a normalised eigenform if and only if its Fourier coefficients satisfy:*

i. $a_1(f) = 1$.

ii. $a_{p^r}(f) = a_p(f) a_{p^{r-1}}(f) - \chi(p) p^{k-1} a_{p^{r-2}}(f)$ *for all primes p and $r \geq 2$.*

iii. $a_{mn}(f) = a_m(f) a_n(f)$ *when $(m, n) = 1$.*

Proof. [DS05, Chapter 5, §8, Proposition 5.8.5] □

Theorem 5.2.8. *[Loz11, Chapter 4, §4, Theorem 4.4.15] The spaces of modular forms $S_k^{new}(\Gamma_1(N))$ and $S_k^{old}(\Gamma_1(N))$ are stable under W_N, the diamond operators, and T_n for all $n \geq 1$.*

Furthermore, the space $S_k^{new}(\Gamma_1(N))$ has orthonormal basis that consists of new normalised eigenforms for the Hecke operators W_N and T_n, for all $n \geq 1$.

Definition 5.2.9. *A normalised eigenform f that is one of the elements of an orthonormal basis of the space $S_k^{new}(\Gamma_1(N))$ is called a* ***newform****, not to be confused with the* new forms *defined in Definition 5.1.14.*

5.3 L-function of a Cusp Form

Each cusp form $f \in \mathcal{S}_k(\Gamma_1(N))$ has an associated Dirichlet series, its L-function. Let f have the Fourier expansion $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$ where $q = e^{2\pi i \tau}$, and $s \in \mathbb{C}$ be a complex variable. Then we define the associated L-function to be the formal sum

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

Theorem 5.3.1. *Let $f \in \mathcal{S}_k(N, \chi)$ be a cusp form with Fourier expansion $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$. Then f is a normalised eigenform if and only if $L(s, f)$ has an Euler product expansion*

$$L(s, f) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}$$

where the product is taken over all primes p.

Proof. By Proposition 5.2.7, it is equivalent to showing the Fourier coefficients of f satisfy the three conditions if and only if its corresponding L-function $L(s, f)$ has an Euler product expansion. We start by showing conditions (i) and (ii) in Proposition 5.2.7 is equivalent to

$$\sum_{r=0}^{\infty} a_{p^r} p^{-rs} = \frac{1}{1 - a_p p^{-s} + \chi(p) p^{k-1-2s}} \tag{5.3}$$

for prime p. Fix a prime p, then multiplying condition (ii) in Proposition 5.2.7 by

p^{-rs} and summing over $r \geq 2$, we get

$$\begin{aligned}
& a_{p^r}(f) = a_p(f)a_{p^{r-1}}(f) - \chi(p)p^{k-1}a_{p^{r-2}}(f) && , \ \forall r \geq 2 \\
\iff \quad & a_{p^r}(f)p^{-rs} = a_p(f)a_{p^{r-1}}(f)p^{-rs} - \chi(p)p^{k-1}a_{p^{r-2}}(f)p^{-rs} && , \ \forall r \geq 2 \\
\iff \quad & \sum_{r\geq 2} a_{p^r}(f)p^{-rs} = \sum_{r\geq 2}(a_p(f)a_{p^{r-1}}(f)p^{-rs} - \chi(p)p^{k-1}a_{p^{r-2}}(f)p^{-rs}) \\
\iff \quad & \sum_{r\geq 2} a_{p^r}(f)p^{-rs} = \sum_{r\geq 1} a_p(f)a_{p^r}(f)p^{-(r+1)s} - \sum_{r\geq 0}\chi(p)p^{k-1}a_{p^r}(f)p^{-(r+2)s} \\
\iff \quad & a_1 + a_p p^{-s} - a_p a_1 p^{-s} = \sum_{r=0}^{\infty} a_{p^r}p^{-rs}\cdot(1 - a_p p^{-s} + \chi(p)p^{k-1-2s})
\end{aligned}$$

which gives us

$$\sum_{r=0}^{\infty} a_{p^r}p^{-rs}\cdot(1 - a_p p^{-s} + \chi(p)p^{k-1-2s}) = a_1 + (1-a_1)a_p p^{-s}. \tag{5.4}$$

If also condition (i) in Proposition (5.2.7), i.e. $a_1(f) = 1$, holds, then the equality becomes

$$\sum_{r=0}^{\infty} a_{p^r}p^{-rs}\cdot(1 - a_p p^{-s} + \chi(p)p^{k-1-2s}) = 1 + (1-1)a_p p^{-s} = 1,$$

i.e. (5.3) holds. Conversely, suppose (5.3) holds. The let $s \to +\infty$. We then see LHS $= a_1$, thus $a_1 = 1$. This also implies (5.4), which implies condition (ii) if we go back up the ladder of equivalent statements above. This gives us the desired equivalence. Note that the Fundamental Theorem of Arithmetic implies that for a function g of prime powers, we have

$$\prod_p \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1}^{\infty}\prod_{p^r||n} g(p^r), \tag{5.5}$$

where $p^r||n$ means that p^r is the highest power of p that divides n, assuming g is small enough for formal rearrangements. Now, if (5.4) holds along with condition (iii), then we can compute

$$
\begin{aligned}
L(s,f) &= \sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} \left(\prod_{p^r || n} a_{p^r} \right) n^{-s} && \text{by condition } (iii), \\
&= \sum_{n=1}^{\infty} \prod_{p^r || n} a_{p^r} (p^r)^{-s} && \text{prime factorisation of } n, \\
&= \prod_{p} \sum_{r=0}^{\infty} a_{p^r} p^{-rs} && \text{by (5.5)}, \\
&= \prod_{p} (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1} && \text{by (5.4)},
\end{aligned}
$$

giving the Euler product expansion. Conversely, suppose we were given the Euler product expansion. Then we can compute using geometric series formula and 5.5

$$
\begin{aligned}
L(s,f) &= \prod_{p} (1 - a_p p^{-s} + \chi(p) p^{1-k-2s})^{-1} = \prod_{p} (1 - p^{-s}(a_p + \chi(p) p^{1-k-s}))^{-1} \\
&= \prod_{p} \sum_{r=0}^{\infty} b_{p,r} (p^{-s})^r \qquad \text{for some } \{b_{p,r}\}, \\
&= \sum_{n=1}^{\infty} \prod_{p^r || n} b_{p,r} p^{-rs} \\
&= \sum_{n=1}^{\infty} \left(\prod_{p^r || n} b_{p,r} \right) n^{-s}.
\end{aligned}
$$

By matching the coefficients of n^{-s}, we have $a_n = \prod_{p^r || n} b_{p,r}$. This gives condition (iii) by Fundamental Theorem of Arithmetic and shows $b_{p,r} = a_{p^r}$. This in turn implies

$$
\sum_{r=0}^{\infty} a_{p^r} p^{-rs} = \frac{1}{1 - a_p p^{-s} + \chi(p) p^{k-1-2s}}.
$$

□

5.3.1 Convergence of L-function of a Cusp Form in a Half-plane

Convergence of $L(s,f)$ in a half-plane can be shown by estimating the coefficients a_n.

Proposition 5.3.2. *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a cusp form. Then the associated L-function $L(s, f)$ converges absolutely for all s with $\mathrm{Re}(s) > k/2 + 1$.*

Proof. Let $g(q) = \sum_{n=1}^{\infty}$ be the Fourier expansion of f, which is a holomorphic function on the open unit disk $\{q \mid |q| < 1\}$. By Cauchy's Formula, we have

$$\begin{aligned} a_n &= \frac{1}{2\pi i}\int_{|q|=r} g(q)q^{-n}\frac{dq}{q} && \text{for any } r \in (0,1), \\ &= \int_{x=0}^{1} f(x+iy)e^{-2\pi i n(x+iy)}dx && \text{for any constant } y > 0, \text{ where } q = e^{2\pi i(x+iy)}, \\ &= e^{2\pi}\int_{x=0}^{1} f(x+i/n)e^{-2\pi i n x}dx && \text{letting } y = 1/n. \end{aligned}$$

Since f is a cusp form, the value $\mathrm{Im}(\tau)^{k/2}|f(\tau)|$ is bounded on the upper half plane $\mathcal{H}$, and so bounding the last integral with this inequality gives $|a_n| \leq Cn^{k/2}$. Since $|a_n n^{-s}| = O(n^{k/2-\mathrm{Re}(s)})$, the result follows because the Riemann zeta function converges absolutely for $\mathrm{Re}(s) > 1$. □

5.3.2 $\mathcal{S}_k(\Gamma_1(N))^{\pm}$ Spaces

Recall the definition of the operator W_N on $\mathcal{S}_k(\Gamma_1(N))$ as follows:

$$\begin{aligned} W_N : S_k(\Gamma_1(N)) &\to S_k(\Gamma_1(N)), \\ f &\mapsto i^k N^{1-k/2} f[\left[\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right]]_k = i^k N^{-k/2}\tau^{-k} f(-1/(N\tau)). \end{aligned}$$

This operator is an involution i.e. $W_N^2 = \mathrm{id}$ (Proposition 5.2.1) and it is self-adjoint

$$\langle W_N f_1, f_2\rangle = \langle f_1, W_N f_2\rangle \quad \forall f_1, f_2 \in \mathcal{S}_k(\Gamma_1(N))$$

where $\langle \cdot, \cdot \rangle$ is the Petersson inner product. Since it is an involution, it will only have ± 1 as eigenvalues. Let $\mathcal{S}_k(\Gamma_1(N))^+$ and $\mathcal{S}_k(\Gamma_1(N))^-$ denote the eigenspaces

$$\mathcal{S}_k(\Gamma_1(N))^{\pm} = \{f \in \mathcal{S}_k(\Gamma_1(N)) \mid W_N f = \pm f\}.$$

Then we get an orthogonal decomposition of $\mathcal{S}_k(\Gamma_1(N))$,

$$\mathcal{S}_k(\Gamma_1(N)) = \mathcal{S}_k(\Gamma_1(N))^+ \oplus \mathcal{S}_k(\Gamma_1(N))^-.$$

5.3.3 Analytic Continuation of L-function of a Cusp Form

Let $f(\tau) = \sum_{n=1}^{\infty} a_n q^n \in \mathcal{S}_k(\Gamma_1(N))$ be a cusp form of weight k. Its associated L-function is $L(s, f) = \sum_{n=1}^{\infty} a_n n^{-s}$ and it is convergent for $\mathrm{Re}(s) > k/2 + 1$.

The Mellin transform of a function h is

$$g(s) = \int_{t=0}^{\infty} h(it) t^s \frac{dt}{t}$$

for values of s such that the integral converges absolutely.

Proposition 5.3.3. *The Mellin transform of f is*

$$g(s) = (2\pi)^{-s}\Gamma(s)L(s, f), \quad \mathrm{Re}(s) > k/2 + 1.$$

Let $\Lambda_N(s) = N^{s/2} g(s)$. This function satisfies the following functional equation.

Theorem 5.3.4. *Suppose $f \in \mathcal{S}_k(\Gamma_1(N))^{\pm}$. Then the Mellin transform $\Lambda_n(s)$ extends to an entire function satisfying the functional equation*

$$\Lambda_N(s) = \pm\Lambda_N(k - s).$$

Consequently, $L(s, f)$ has an analytic continuation to the full s-plane.

So the L-function attached to a cuspidal Hecke eigenform has an Euler product and an analytic continuation to $\mathbb{C}$.

5.4 Modularity Theorem

Define the value f_p as follows:

$$f_p = \begin{cases} 0, & \text{if } E \text{ has good reduction at } p, \\ 1, & \text{if } E \text{ has multiplicative reduction at } p, \\ 2, & \text{if } E \text{ has additive reduction at } p, \text{ and } p \neq 2, 3, \\ 2 + \delta_p, & \text{if } E \text{ has additive reduction at } p = 2, 3. \end{cases}$$

where δ_p is a technical invariant that described whether there is wild ramification in the action of the inertia group at p of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the Tate module $T_p(E)$.

Definition 5.4.1. *The **conductor** $N_{E/\mathbb{Q}}$ of $E/\mathbb{Q}$ is defined to be*

$$N_{E/\mathbb{Q}} = \prod_p p^{f_p}$$

where the product is over all the primes and the exponents f_p are defined as above.

Theorem 5.4.2 (Modularity Theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then for some newform $f \in S_2(\Gamma_0(N_E))$, we have*

$$L(s, f) = L(s, E).$$

Chapter 6

Birch and Swinnerton-Dyer Conjecture

The first step to the Birch and Swinnerton-Dyer conjecture is the Mordell-Weil theorem. Although it is proven in general for abelian varieties over a number field, here we will restrict to the case of elliptic curves over the rationals $\mathbb{Q}$.

6.1 Mordell-Weil Theorem over $\mathbb{Q}$

Theorem 6.1.1 (Weak Mordell-Weil)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Let $m \geq 2$ be an integer, then*

$$E(\mathbb{Q})/mE(\mathbb{Q})$$

is a finite group.

First, the following lemma allows us to assume $E[m] \subseteq E(\mathbb{Q})$.

Lemma 6.1.2. *[Sil09, Chapter 8, §1, Lemma 1.1.1] Let L/K be a finite Galois extension and $m \geq 2$ be an integer. If $E(L)/m(L)$ is finite, then $E(K)/mE(K)$ is also finite.*

Next, we define the Kummer Pairing.

Definition 6.1.3 (Kummer Pairing)**.** *The Kummer pairing is defined as follows:*

$$\begin{aligned} \kappa : E(K) \times G_{\bar{K}/K} &\to E[m] \\ (P, \sigma) &\mapsto Q^\sigma - Q \end{aligned}$$

where $Q \in E(\bar{K})$ is any point satisfying $[m]Q = P$.

The Kummer Pairing induces a perfect bilinear pairing:

$$\frac{E(K)}{mE(K)} \times G_{L/K} \to E[m]$$

where $L = K([m]^{-1}E(K))$. Since $E[m]$ is finite, the finiteness of $E(K)/mE(K)$ depends on the finiteness of $G_{L/K}$, in other words the finiteness of the extension L/K. [Sil09, Chapter 8.1, Proposition 1.6]

It can be shown that the extension L/K is abelian of exponent m and is unramified outside of a certain finite set of absolute values on K. [Sil09, Chapter 8.1, Proposition 1.5] Then by Kummer theory of fields, we can show L/K is a finite extension as desired. This gives us Weak Mordell-Weil theorem. To prove $E(\mathbb{Q})$ is finitely generated, we need to employ the theory of heights. We start with the following theorem:

Theorem 6.1.4 (Descent Theorem)**.** *Let A be an abelian group. Suppose that there exists a (height) function*

$$h : A \longrightarrow \mathbb{R}$$

with the following three properties:

i. Let $Q \in A$. There is a constant C_1, depending on A and Q, such that

$$h(P + Q) \leq 2h(P) + C_1 \qquad \text{for all } P \in A.$$

ii. There are an integer $m \geq 2$ and a constant C_2, depending on A, such that

$$h(mP) \geq m^2 h(P) - C_2 \qquad \text{for all } P \in A.$$

iii. For every constant C_3, the set

$$\{P \in A : h(P) \leq C_3\}$$

is finite.

Suppose further that for the integer m in (ii), the quotient group A/mA is finite. Then A is finitely generated.

Proof. Since the quotient group A/mA is finite, we can pick a finite set of coset representatives $\{Q_1, \ldots, Q_r\} \in A$. Then for any $P \in A$, properties i and ii give allow us to show the difference between P and an appropriate linear combination of

$Q_1, \ldots, Q_r$ is a multiple of a point whose height is smaller than a constant that is *independent of* P. Notice this collection is finite by property *iii*. So $\{Q_1, \ldots, Q_r\}$ and a finite collection of points finitely generate all of A. □

So we need to find a suitable height function:

Definition 6.1.5. *Let $t \in \mathbb{Q}$, then $t = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$. Then define height of t to be*

$$H(t) = \max\{|p|, |q|\}.$$

Then we define the logarithmic height on $E(\mathbb{Q})$ to be

$$h_x(P) = \begin{cases} \log(H(x(P))) & , P \neq O, \\ 0 & , P = O, \end{cases}$$

where O is the point at infinity of E and $x(P)$ is the "x-coordinate" of P with respect to a Weierstrass equation.

With the height function h_x in Definition 6.1.5, by Theorem 6.1.1 and Theorem 6.1.4, we have

Theorem 6.1.6 (Mordell-Weil)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated.*

In other words, the Mordell-Weil theorem says that the **Mordell-Weil group** $E(\mathbb{Q})$ of an elliptic curve can be written in the form

$$E(\mathbb{Q}) \cong E_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^r,$$

where the r is called the **algebraic rank** of the elliptic curve.

The following theorem gives a characterisation of the possible torsion subgroups:

Theorem 6.1.7 (Mazur)**.** *[Maz77; Maz78] Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one fo the following fifteen groups:*

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z} \qquad & \text{with } 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} \ & \text{with } 1 \leq N \leq 4. \end{aligned}$$

Further, each of these groups occurs as $E_{\text{tors}}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

Eventhough the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ is well understood and relatively easy to compute [Sil09, Chapter VIII §7], we still do not know a general way to determine the rank of an elliptic curve. In fact, quite a lot is not known about this algebraic rank, for example:

Conjecture 6.1.8. *[Sil09, Chapter VIII, §10, Conjecture 10.1] There exists elliptic curves $E/\mathbb{Q}$ of arbitrarily large rank.*

One key piece of evidence is that the analogous statement for elliptic curves over function fields $\mathbb{F}_p(T)$ is true. [TS67] However, it is known that the rank of a "randomly chosen" elliptic curve defined over $\mathbb{Q}$ will tend to be relatively small, in fact the average rank is bounded by 7/6 [BS15].

6.2 Birch and Swinnerton-Dyer Conjecture

We can associate another important numerical to an elliptic curve E, known as its analytic rank.

Definition 6.2.1. *Let $L(s, E)$ be the L-function associated to an elliptic curve E. Then the **analytic rank** of the elliptic curve E is the order of vanishing of $L(s, E)$ at the central point $s = 1$.*

Around late 1950s, Bryan John Birch and Peter Swinnerton-Dyer began a series of computations on the EDSAC, the first practical general purpose electric computer at the time. They calculated the zeta functions of certain elliptic curves and observed coincidences that led them to the following conjecture outlined in their second paper, "Notes on elliptic curves II". [SB65]

Conjecture 6.2.2 (Birch and Swinnerton-Dyer)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $L(s, E)$ has a zero at $s = 1$ of order equal to the rank of $E(\mathbb{Q})$, in other words the analytic rank of E is equal to the algebraic rank of E.*

So the Birch and Swinnerton-Dyer Conjecture asserts that the rank of an elliptic curve $E/\mathbb{Q}$ can determined by its reductions at the primes p.

6.2.1 A Heuristic from Koblitz

To build intuition for the conjecture, consider the following heuristic by Koblitz. [Kob05, Chapter II, §6] We start by pretending the Euler product $L(s, E)$ converges

at $s = 1$. Therefore we have

$$L(1,E) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}\bigg|_{s=1} = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p - a_p + 1}$$
$$= \prod_p \frac{p}{\#E(\mathbb{F}_p)}$$

By Hasse's bound (Theorem 4.2.2), we know the number $\#E(\mathbb{F}_p)$ stays close p, with deviations bounded by $2\sqrt{p}$. If the distance is evenly distributed across p, we have $\#E(\mathbb{F}_p) \approx p \pm \sqrt{p}$. Then one would expect the infinite product of $p/\#E(\mathbb{F}_p)$ to converge to a nonzero limit [Kob05, Chapter II, §6, Problem 1], so the analytic rank is zero. If the algebraic rank is at least one (i.e. there are infinitely many rational points), then one would expect reducing modulo p will result in a large contribution to $\#E(\mathbb{F}_p)$, so the number of $\mathbb{F}_q$ points will lean towards the higher side of the bound, making it approximately $p + \sqrt{p}$. Therefore,

$$L(1,E) \approx \prod_p \frac{p}{p + \sqrt{p}} = \prod_p \frac{1}{1 + p^{-1/2}} = 0,$$

in other words the analytic rank is also at least one.

6.2.2 Congruent Number Problem

"The congruent number problem, the written history of which can be traced back at least a millennium, is the oldest unsolved major problem in number theory, and perhaps in the whole of mathematics." — John H. Coates.

The congruent number problem asks the question: When is an integer n the area of a right triangle with rational side lengths? In 1983, Jerrold Tunnell gave the following resolution [Tun83]:

Theorem 6.2.3 (Tunnell). *[Con08] Let n be a squarefree integer. Let*

$$f(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 2y^2 + 8z^2 = n\},$$
$$g(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 2y^2 + 32z^2 = n\},$$
$$h(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 4y^2 + 8z^2 = n/2\},$$
$$k(n) = \#\{(x,y,z) \in \mathbb{Z}^3 \mid x^2 + 4y^2 + 32z^2 = n/2\}.$$

For odd n, if n is congruent then $f(n) = 2g(n)$. For even n, if n is congruent then $h(n) = 2k(n)$. Moreover, if the weak Birch and Swinnerton-Dyer conjecture

is true for the curve $y^2 = x^3 - n^2x$ then the converse of both implications is true: $f(n) = 2g(n)$ implies n is congruent when n is odd and $k(n) = 2k(n)$ implies n is congruent when n is even.

Therefore, if weak Birch and Swinnerton-Dyer conjecture (Conjecture 6.2.2) holds true, it will resolve one of the oldest — if not the oldest — problem in Diophantine Geometry.

6.2.3 Key Developments Supporting the Conjecture

The first breakthrough for the Birch and Swinnerton-Dyer conjecture came in 1977 from John Coates and his student Andrew Wiles.

Theorem 6.2.4 (Coates and Wiles)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication. If E has infinitely many $\mathbb{Q}$-points, then $L(E, 1) = 0$.*

Remark. *The original proof [CW77] required the additional assumption that the quadratic imaginary field of complex multiplication to have class number 1, but it turned out not to be necessary.*

This result was a step forward in connecting the algebraic and analytic ranks, at least for the curves with complex multiplication.

Benedict Gross and Don Zagier made a breakthrough for modular elliptic curves with their famous result on Heegner points [GZ86]. This allowed them to deduce:

Theorem 6.2.5 (Gross and Zagier)**.** *[GZ86] Let E be a modular elliptic curved defined over the rational numbers. If $L_E(s)$ has a simple zero at $s = 1$, then it has a rational point of infinite order.*

This result provided strong evidence that the behaviour of $L(s, E)$ is indeed connected to the algebraic rank of the elliptic curve.

In 1983, Ralph Greenberg was able to make progress on a partial converse [Gre83]:

Theorem 6.2.6 (Greenberg)**.** *Let E be an elliptic curve $E/\mathbb{Q}$ with complex multiplication by the ring of integers of an imaginary quadratic field K. If $L(s, E)$ has an odd order zero at $s = 1$, then either $E(\mathbb{Q})$ has rank greater than or equal to 1, or the p-primary subgroup of the Tate-Shafarevich group $Ш(E, \mathbb{Q})$ is infinite for all primes p where E has good, ordinary reduction (except possibly $p = 2$ or 3).*

The Tate-Shafarevich group, introduced by Serge Lang, John Tate, and Igor Shafarevich, plays a key role in the stronger form of the Birch and Swinnerton-Dyer Conjecture. It is known for being both mysterious and extremely difficult to compute.

In 1989, Kolyvagin developed a new tool known as Euler systems. He was able to use them to make advancements in the converse direction:

Theorem 6.2.7 (Kolyvagin)**.** *[Kol89] Let $E/\mathbb{Q}$ be a modular elliptic curve. If $L(1, E) \neq 0$, then E has algebraic rank 0, i.e. the Mordell-Weil group $E(\mathbb{Q})$ is finite. If $L(1, E)$ is a first-order zero, then E has algebraic rank 1.*

Together with earlier work from others, Kolyvagin was able to confirm the conjecture holds for elliptic curves of rank 0 and rank 1.

The next leap came with Andrew Wiles' momentus proof of Fermat's Last Theorem. [Wil95] In his paper, Wiles was able to established the modularity of semistable elliptic curves:

Theorem 6.2.8. *[Wil95] All semistable elliptic curves over $\mathbb{Q}$ are modular.*

Remark. *Semistable means elliptic curves that only have bad reduction of multiplicative type, i.e. the conductor (Definition 5.4.1) is square-free.*

This was further extended by Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor.

Theorem 6.2.9. *[Bre+01] All elliptic curves defined over $\mathbb{Q}$ are modular.*

This result solidified the connection between elliptic curves and modular forms, a cornerstone of Wiles' strategy in his proof of Fermat's Last Theorem.

Recent work by mathematicians such as Manjul Bhargava and Arul Shankar has deepened our understanding of the distribution of ranks of elliptic curves.

Theorem 6.2.10. *When all elliptic curves over $\mathbb{Q}$ are ordered by height, their average rank is at most $7/6$.*

In combination with result from Tim Dokchister and Vladimir Dokchister [DD10], Bhargava and Shankar were able to get:

Theorem 6.2.11. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have algebraic rank 0.*

Combining with work from Christopher Skinner and Eric Urban [SU14] on the Iwasawa Main Conjectures for GL_2 gives:

Theorem 6.2.12. *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have analytic rank* 0*, i.e. a positive proportion of them satisfy* $L(1, E) \neq 0$.

Combining these results with Kolyvagin's theorem, we find that a positive proportion of elliptic curves $E/\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer Conjecture. Thus, while the conjecture remains open in its full generality, substantial progress has been made in certain cases, bringing us closer to fully understanding the deep connection between the analytic and algebraic properties of elliptic curves.

Appendix A

Appendix

A.1 Quadratic Form

Definition A.1.1. *Let A be an abelian group. A function $d : A \to \mathbb{R}$ is a* ***quadratic form*** *if it satisfies:*

i. $d(\alpha) = d(-\alpha)$ *for all* $\alpha \in A$.

ii. The pairing $A \times A \to \mathbb{R},\ (\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$ *is bilinear.*

The quadratic form is ***positive definite*** *if it further satisfies:*

iii. $d(\alpha) \geq 0$ *for all* $\alpha \in A$.

iv. $d(\alpha) = 0$ *if and only if* $\alpha = 0$.

Lemma A.1.2. *Let A be an abelian group. If $d : A \to \mathbb{R}$ is a quadratic form, then it satisfies*

$$d(n\alpha) = n^2 d(\alpha) \qquad \forall \alpha \in A, n \in \mathbb{Z}.$$

Proof. Since $d(\alpha) = d(-\alpha)$, we only need to show it for $n \in \mathbb{N}$. We proceed by induction. Let

$$L(\alpha, \beta) = d(\alpha + \beta) - d(\alpha) - d(\beta)$$

denote the associated bilinear form to the quadratic form d. We first show $d(0) = 0$. For this we look at

$$L(0, 0) = -L(-0, 0) = -L(0, 0) \implies L(0, 0) = 0.$$

Thus $d(0) = 2d(0)$ which means $d(0) = 0$. For the base case, we have the following

$$L(\alpha, \alpha) = d(2\alpha) - d(\alpha) - d(\alpha) = d(2\alpha) - 2d(\alpha) \tag{A.1}$$
$$= -L(\alpha, -\alpha) \tag{A.2}$$
$$= -(d(0) - d(\alpha) - d(\alpha)) = 2d(\alpha) \tag{A.3}$$

which gives $d(2\alpha) = 4d(\alpha)$. Assume the lemma be true for $0, 1, \ldots, n$, then look at

$$L(n\alpha, \alpha) = d((n+1)\alpha) - d(n\alpha) - d(\alpha) = d((n+1)\alpha) - n^2 d(\alpha) - d(\alpha) \tag{A.4}$$
$$= nL(\alpha, \alpha) \tag{A.5}$$
$$= n(d(2\alpha) - 2d(\alpha)) = n(2d(\alpha)). \tag{A.6}$$

We thus have $d((n+1)\alpha) = (n^2 + 2n + 1)d(\alpha) = (n+1)^2 d(\alpha)$, which completes the induction. □

A.2 Surface Integrals

This section follows Section 4.4 of [Mas15].

Let $V \subseteq \mathbb{C}$. A 2-form on V is an expression of the form $\omega = f(z, \bar{z})dz \wedge d\bar{z}$. Note that

$$dz \wedge d\bar{z} = (dx + idy) \wedge (dx - idy) = -2idx \wedge dy.$$

The integral of ω on V is:

$$\int_V \omega = \int_V f(z, \bar{z})dz \wedge d\bar{z} = \iint -2if(x + iy, x - iy)dxdy.$$

Consider now, for $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2^+(\mathbb{R})$, the map $z \mapsto \alpha.z = \frac{az+b}{cz+d}$. Then we have

$$\mathrm{Im}(\alpha.z) = \frac{\det(\alpha)}{|cz + d|^2}\mathrm{Im}(z).$$

We also have

$$d(\alpha.z) = \frac{\det(\alpha)}{(cz+d)^2}dz \qquad \text{and} \qquad \overline{d(\alpha.z)} = \frac{\det(\alpha)}{\overline{(cz+d)^2}}d\bar{z},$$

which gives

$$d(\alpha.z) \wedge \overline{d(\alpha.z)} = \frac{(\det(\alpha))^2}{|cz + d|^4}dz \wedge d\bar{z}.$$

Therefore the 2-form $(dz \wedge d\bar{z})/(\mathrm{Im}(z)^2)$ is invariant under the action of $\mathrm{GL}_2^+(\mathbb{R})$.

Define

$$d\mu(z) = \frac{dx \wedge dy}{y^2} = \frac{-1}{2i}\frac{dz \wedge d\bar{z}}{\mathrm{Im}(z)^2},$$

then we define the **covolume** of $\mathrm{SL}_2(\mathbb{Z})$ to be

$$\mathrm{covol}(\mathrm{SL}_2(\mathbb{Z})) = \int_{D^*} d\mu(z)$$

where D^* is the fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$.

Lemma A.2.1. $\mathrm{covol}(\mathrm{SL}_2(\mathbb{Z})) = \frac{\pi}{3}$.

Corollary A.2.1.1. *If ϕ is a bounded function on D^*, then $\int_{D^*} \phi(z) d\mu(z)$ is a well-defined complex number.*

Bibliography

[Hea85] T. L. Heath. *Diophantos of Alexandria: a study in the history of Greek algebra*. eng. OCLC: 893976069. Cambridge: Cambridge University Press, 1885. ISBN: 978-1-139-60006-4.

[Wei29] A. Weil. "L'arithmétique sur les courbes algébriques". en. In: *Acta Mathematica* 52.0 (1929), pp. 281–315. DOI: 10.1007/BF02592688. URL: http://projecteuclid.org/euclid.acta/1485887804.

[Wei49] A. Weil. "Numbers of solutions of equations in finite fields". In: *Bulletin of the American Mathematical Society* 55.5 (1949), pp. 497–508.

[SB63] P. Swinnerton-Dyer and B.J. Birch. "Notes on elliptic curves. I." In: *Journal für die reine und angewandte Mathematik* 212 (1963), pp. 7–25. URL: http://eudml.org/doc/150565.

[SB65] P. Swinnerton-Dyer and B.J. Birch. "Notes on elliptic curves. II." In: *Journal für die reine und angewandte Mathematik* 218 (1965), pp. 79–108. URL: http://eudml.org/doc/150676.

[Tat66] J. Tate. "Endomorphisms of Abelian Varieties over Finite Fields." In: *Inventiones mathematicae* 2 (1966), pp. 134–144. URL: http://eudml.org/doc/141848.

[TS67] J. Tate and I. R. Shafarevich. "The rank of elliptic curves". In: *Doklady Akademii Nauk*. Vol. 175. 4. Russian Academy of Sciences. 1967, pp. 770–773.

[CW77] J. Coates and A. Wiles. "On the conjecture of Birch and Swinnerton-Dyer". In: *Inventiones mathematicae* 39.3 (Oct. 1977), pp. 223–251. DOI: 10.1007/BF01402975. URL: https://doi.org/10.1007/BF01402975.

[Maz77] B. Mazur. "Modular curves and the Eisenstein ideal". en. In: *Publications Mathématiques de l'IHÉS* 47 (1977), pp. 33–186. URL: http://www.numdam.org/item/PMIHES_1977__47__33_0/.

[Maz78] B. Mazur. "Rational isogenies of prime degree". In: *Inventiones mathematicae* 44.2 (June 1978). With an appendix by Goldfeld, D., pp. 129–162. DOI: 10.1007/BF01390348. URL: https://doi.org/10.1007/BF01390348.

[Fal83] G. Faltings. “Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.” ger. In: *Inventiones mathematicae* 73 (1983), pp. 349–366. URL: http://eudml.org/doc/143051.

[Gre83] R. Greenberg. “On the Birch and Swinnerton-Dyer Conjecture.” In: *Inventiones mathematicae* 72 (1983), pp. 241–266. URL: http://eudml.org/doc/143019.

[Tun83] J.B. Tunnell. “A Classical Diophantine Problem and Modular Forms of Weight 3/2.” In: *Inventiones mathematicae* 72 (1983), pp. 323–334. URL: http://eudml.org/doc/143024.

[Fal86] G. Faltings. “Finiteness Theorems for Abelian Varieties over Number Fields”. In: *Arithmetic Geometry*. Ed. by G. Cornell and J. H. Silverman. New York, NY: Springer New York, 1986, pp. 9–26. DOI: 10.1007/978-1-4613-8655-1_2. URL: https://doi.org/10.1007/978-1-4613-8655-1_2.

[GZ86] B. H. Gross and D. B. Zagier. “Heegner points and derivatives of L-series”. In: *Inventiones mathematicae* 84.2 (June 1986), pp. 225–320. DOI: 10.1007/BF01388809. URL: https://doi.org/10.1007/BF01388809.

[Mil86] V. S. Miller. “Use of Elliptic Curves in Cryptography”. en. In: *Advances in Cryptology — CRYPTO ’85 Proceedings*. Ed. by Hugh C. Williams. Vol. 218. Series Title: Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 1986, pp. 417–426. DOI: 10.1007/3-540-39799-X_31. URL: http://link.springer.com/10.1007/3-540-39799-X_31.

[Kob87] N. Koblitz. “Elliptic curve cryptosystems”. en. In: *Mathematics of Computation* 48.177 (1987), pp. 203–209. DOI: 10.1090/S0025-5718-1987-0866109-5. URL: https://www.ams.org/mcom/1987-48-177/S0025-5718-1987-0866109-5/.

[Kol89] V A Kolyvagin. “Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves”. In: *Mathematics of the USSR-Izvestiya* 32.3 (June 1989), pp. 523–541. DOI: 10.1070/IM1989v032n03ABEH000779. URL: https://iopscience.iop.org/article/10.1070/IM1989v032n03ABEH000779.

[Wil95] A. Wiles. “Modular Elliptic Curves and Fermat’s Last Theorem”. In: *The Annals of Mathematics* 141.3 (May 1995), pp. 443–551. DOI: 10.2307/2118559. URL: https://www.jstor.org/stable/2118559?origin=crossref.

[Bro00] E. Brown. “Three Fermat Trails to Elliptic Curves”. en. In: *The College Mathematics Journal* 31.3 (May 2000), pp. 162–172. DOI: 10.1080/07468342.2000.11974137. URL: https://www.tandfonline.com/doi/full/10.1080/07468342.2000.11974137.

[Bre+01] C. Breuil et al. "On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises". en. In: *Journal of the American Mathematical Society* 14.4 (May 2001), pp. 843–939. DOI: 10.1090/S0894-0347-01-00370-8. URL: https://www.ams.org/jams/2001-14-04/S0894-0347-01-00370-8/.

[BM02] E. Brown and B. T. Myers. "Elliptic Curves from Mordell to Diophantus and Back". en. In: *The American Mathematical Monthly* 109.7 (Aug. 2002), pp. 639–649. DOI: 10.1080/00029890.2002.11919894. URL: https://www.tandfonline.com/doi/full/10.1080/00029890.2002.11919894.

[DS05] F. Diamond and J. M. Shurman. *A first course in modular forms*. eng. Graduate texts in mathematics 228. New York: Springer, 2005. ISBN: 978-0-387-27226-9.

[Kob05] N. Koblitz. *Introduction to elliptic curves and modular forms*. eng. Second Edition. OCLC: 1042904421. New York: Springer, 2005. ISBN: 978-1-4612-6942-7.

[Con08] K. Conrad. "The congruent number problem". In: *The Harvard College Mathematics Review* 2.2 (2008), pp. 58–74.

[Was08] L. C. Washington. *Elliptic curves: number theory and cryptography*. 2nd ed. Discrete mathematics and its applications. OCLC: ocn192045762. Boca Raton, FL: Chapman & Hall/CRC, 2008. ISBN: 978-1-4200-7146-7.

[Zag08] D. Zagier. "Elliptic Modular Forms and Their Applications". In: *The 1-2-3 of modular forms: lectures at a summer school in Nordfjordeid, Norway*. Ed. by J. H. Bruinier. Universitext. OCLC: ocn173239471. Berlin: Springer, 2008. ISBN: 978-3-540-74117-6.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. eng. 2nd ed. Graduate texts in mathematics 106. New York, NY: Springer, 2009. ISBN: 978-0-387-09494-6.

[DD10] T. Dokchitser and V. Dokchitser. "On the Birch-Swinnerton-Dyer quotients modulo squares". en. In: *Annals of Mathematics* 172.1 (June 2010), pp. 567–596. DOI: 10.4007/annals.2010.172.567. URL: http://annals.math.princeton.edu/2010/172-1/p11.

[Hus10] D. Husemöller. *Elliptic curves*. eng. 2nd ed. OCLC: 981373675. New York: Springer Science+Business Media, 2010. ISBN: 978-1-4419-3025-5.

[Sil10] J. H. Silverman. "A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties". eng. In: *Pairing-based cryptography - Pairing 2010: 4th international conference, Yamanaka Hot Spring, Japan, December 13-15, 2010 ; proceedings*. Ed. by Marc Joye, Atsuko Miyaji, and Akira Otsuka. Lecture notes in computer science 6487. Meeting Name: Pairing Conference. Berlin Heidelberg: Springer, 2010, pp. 377–396. ISBN: 978-3-642-17454-4.

[Loz11] Á. Lozano-Robledo. *Elliptic curves, modular forms, and their L-functions*. eng. Student mathematical library. IAS/Park City mathematical subseries volume 58. Providence, R.I: American Mathematical Society, 2011. ISBN: 978-0-8218-5242-2.

[AG12] A. Ash and R. Gross. *Elliptic tales: curves, counting, and number theory*. OCLC: ocn761850914. Princeton: Princeton University Press, 2012. ISBN: 978-0-691-15119-9.

[SU14] C. Skinner and E. Urban. "The Iwasawa Main Conjectures for GL2". en. In: *Inventiones mathematicae* 195.1 (Jan. 2014), pp. 1–277. DOI: 10.1007/s00222-013-0448-1. URL: http://link.springer.com/10.1007/s00222-013-0448-1.

[BS15] M. Bhargava and A. Shankar. "Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0". en. In: *Annals of Mathematics* (Mar. 2015), pp. 587–621. ISSN: 0003-486X. DOI: 10.4007/annals.2015.181.2.4. URL: https://annals.math.princeton.edu/2015/181-2/p04.

[Mas15] M. Masdue. *Modular Forms (MA4H9)*. 2015. URL: https://mdave16.github.io/notes/Modular%20Forms%20-%20Marc%20Masdeu.pdf.

[LMFDB] The LMFDB Collaboration. *The L-functions and modular forms database*. https://www.lmfdb.org. [Online; accessed 26 September 2024]. 2024.