AN ANALYSIS OF ELLIPTIC CURVES VIA THE BSD CONJECTURE

RYAN TAMURA

Abstract. This paper aims to provide a self-contained exposition on the geometric, group-theoretic, and analytic properties of elliptic curves. We begin with an exposition of the basic algebraic properties of elliptic curve, such as the group law and isogenies. We then transition to an analysis of elliptic curves over finite and global fields. In particular, we'll provide proofs of the Mordell-Weil theorem over the rational numbers and the Weil conjectures for elliptic curves. Afterwards, we'll transition to an analysis of the associated L-Dirichlet series of an elliptic curve in order to understand the modularity theorem. We'll conclude with an exposition of relatively recent results on the Birch and Swinnerton-Dyer and Hasse-Weil conjectures.

Contents

1. Introduction

Elliptic curves have been at the forefront of numerous breakthroughs in arithmetic geometry and analytic number theory. For example, Wiles' remarkable proof that semistable elliptic curves over the rational numbers were modular yielded Fermat's Last theorem, thereby resolving one the central problems of number theory. In addition elliptic curves have numerous important conjectures which relate their algebraic and analytic properties such as the Birch and Swinnerton-Dyer and Hasse-Weil conjectures.

This paper presumes knowledge of the fundamentals of algebraic geometry. In the latter sections dealing with the analytic properties of elliptic curves, the reader

should have prior knowledge of some elementary analytic number theory and Fourier analysis, in particular, the analytic properties of the Riemann zeta function. Beyond these requirements, the paper will be self-contained.

2. Preliminaries

In this section, we'll cover the necessary perquisites in order to understand the algebraic properties of elliptic curves. We will first discuss some terminology associated with morphisms between curves, such as separablilty and ramification indices. We will then transition to a discussion about divisors and Kahler-Differentials of curves, which allow us to the define the genus of a curve based on the Riemann-Roch theorem.

For some of the more lengthy proofs, the reader should consult [3]. Throughout this section, we presume K is a perfect field and $\overline{K}$ its algebraic closure.

Definition 2.1 (Curve)**.** A curve, denoted by C, is a projective variety which is of dimension one. We say a curve C is defined over K if its homogeneous ideal $I(C)$ can be generated by polynomials with coefficients in K. If it is the case C is defined over K, we'll denote this by C/K.

Definition 2.2. Suppose C is a curve. Its set of $K-$rational of points, denoted by $C(K)$, is defined to be the set of all points $P \in C$, such there exists homogeneous coordinates $x_0, \cdots, x_n \in K$, such that $P = [x_0, \cdots, x_n]$.

Example 2.3. Consider $\mathbb{P}^1(\overline{\mathbb{Q}})$. We observe that the set $\mathbb{P}^1(\mathbb{Q}) = [x, y]$ has homogeneous coordinates $x, y \in \mathbb{Q}$. By the equivalence relation on projective space we can make x, y be integers by clearing their denominators.

Definition 2.4. Suppose $C_1 \subset \mathbb{P}^m$ and $C_2 \subset \mathbb{P}^n$ are curves. A morphism $\phi : C_1 \to C_2$ is a map of the form

$$\phi = [\phi_0, \cdots, \phi_n], \tag{2.5}$$

which satisfies the following properties.

(i) The $\phi_i \in k[x_0, \cdots, x_m]$ are homogeneous polynomials of the same degree not all in $I(C_1)$.
(ii) For $f \in I(C_2)$, $f(\phi_0, \cdots, \phi_m) \in I(C_1)$.

Recall that a morphism $\phi : C_1/K \to C_2/K$ induces a pullback map

$$\phi^* : \overline{K}(C_2) \to \overline{K}(C_1),\ \phi^*(f) = f(\phi). \tag{2.6}$$

Note that the pullback is injective since it's a homomorphism of fields.

Definition 2.7. A morphism of curves $\phi : C_1 \to C_2$ is said to be separable, inseparable, or purely inseparable if the corresponding field extension $\overline{K}(C_1)/\phi^*(\overline{K}(C_2))$ has the corresponding property.

Definition 2.8. Let $\phi : C_1 \to C_2$ be a morphism of curves. Its degree, denoted by $\deg(\phi)$, is the degree of the field extension $\overline{K}(C_1)/\overline{K}(C_2)$. Similarly, the quantities $\deg_s(\phi)$ and $\deg_i(\phi)$ denote the separable and inseparable degrees of the extension.

Let C is a curve defined over a field K with characteristic $p > 0$ and $I(C)$ its homogeneous ideal. If q is a pth power and $f \in K[x_1, \cdots, x_n]$, we set f^q to be the polynomial obtained from f by raising its coefficients to the q power. We can

define a new curve, which we denote by C^q whose homogeneous ideal $I(C^q)$ has the generating set $\{f^q | f \in I(C)\}$.

Definition 2.9. The qth-power Frobenius map $\phi : C \to C^q$ is defined to be

$$\phi([x_0, \cdots, x_n]) = [x_0^q, \cdots, x_n^q] \tag{2.10}$$

Proposition 2.11. *Suppose that K is a perfect field with characteristic p and q a pth power. The qth power Frobenius map is purely inseparable.*

Proof. It suffices to show that $\phi^*(K(C^q)) = (K(C))^q$. From definition, we have

$$\phi^*(K(C^q)) = \{\frac{f(x_0^q, \cdots, x_n^q)}{g(x_0^q, \cdots, x_n^q)} | f, g \in K[C]\}$$

with f, g being homogeneous polynomials of same degree. Observe that $(K(C))^q$ consists of quotients of polynomials f^q/g^q with f and g being homogeneous with same degree. Since every element of K is a qth power we obtain that $K[x_0^q, \cdots, x_n^q] = K[x_0, \cdots, x_n]^q$, which implies that two subfields are the same. □

Proposition 2.12. *Let $\phi : C \to C^q$ denote the qth-power Frobenius map. Then* $\deg(\phi) = q$.

Proof. See [6], Chapter II, Proposition 2.11. □

Lemma 2.13. *Suppose $\phi : C_1 \to C_2$ is a morphism of curves whose degree is one. Then ϕ is an isomorphism.*

Proof. See [6], Chapter II, Corollary 2.4.1 □

Definition 2.14. Suppose $\phi : C_1 \to C_2$ is a morphism of curves. The ramification index of ϕ at $P \in C_1$, denoted by $e_{\phi(P)}$, is the quantity $\mathrm{ord}_p(\phi^*(t_{\phi(P)}))$ with $t_{\phi(P)}$ being a uniformizer of C_2 at $\phi(P)$. We say ϕ is unramified if $e_\phi(p) = 1$ for all $P \in C_1$.

Proposition 2.15. *Suppose that $\phi : C_1 \to C_2$ is a morphism of smooth curves.*

(a) For every $Q \in C_2$, $\deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\varphi(P)$.
(b) For all but finitely many $Q \in C_2$, satisfy $|\phi^{-1}(Q)| = \deg_s(\phi)$.
(c) Let $\varphi : C_2 \to C_3$ be another morphism of smooth curves. Then for any $P \in C_1$

$$e_{\varphi \circ \phi}(P) = e_\phi(P) e_\varphi(\phi(P)).$$

Proof. (a) See [3], Chapter II, Proposition 6.7.
(b) See [3], Chapter II, Proposition 6.8.
(c) Let $t_{\phi(P)}$ and $t_{\varphi\phi}(P)$ be uniformizers at the indicated points. From the definition of the ramification index and that the pullback switches the order of composition, we have

$$\mathrm{ord}_{\phi(P)} \phi^* t_{\phi(P)}^{e_{\varphi(\phi(P))}} = \mathrm{ord}_P((\varphi\phi)^* t_{\varphi\phi P}),$$

which is the desired result. □

We can construct a free abelian group which is generated by the points of a curve. This group is known as the divisor group of C.

Definition 2.16. The divisor group, denoted by $\mathrm{Div}(C)$ of a curve C, is the free abelian group generated by points of C. Concretely, a divisor D is a formal sum

$$D = \sum_{P \in C} n_p P \tag{2.17}$$

where $n_p \in \mathbb{Z}$ is zero for all but finitely many points $P \in C$.

Example 2.18. Let $f \in \overline{K}(C)$. We define its associated divisor

$$\mathrm{div}(f) = \sum_{P} \mathrm{ord}_P(f) P \tag{2.19}$$

with $\mathrm{ord}_p(f)$ being its order of vanishing at P. It is the clear that the set of divisors of the form (2.19) is a subgroup of $\mathrm{Div}(C)$.

Definition 2.20. A divisor D is said to be principal if there exists a $f \in \overline{K}(C)$ such that $D = \mathrm{div}(f)$. The Picard group, denoted by $\mathrm{Pic}(C)$, is the quotient group of $\mathrm{Div}(C)$ by its subgroup of principal divisors. We say that D and D' are linearly equivalent, denoted by $D \sim D'$, if $D - D' = \mathrm{div}(f)$ with $f \in K(C)^*$.

Definition 2.21. Let $D = \sum_{P \in C} n_p P$ be a divisor of C. The degree of D, denoted by $\deg(D)$, is the sum $\sum_{P \in C} n_p$.

We will need the following result concerning the degree of principals divisors.

Proposition 2.22. *Suppose that C is a smooth curve. Then*

(a) $\mathrm{div}(f) = 0$ *iff* $f \in K^*$.
(b) $\deg(\mathrm{div(f)}) = 0$.

Proof. (a) For the forward direction, note that if $\mathrm{div}(f) = 0$, then f has no poles or zeroes. This implies that the induced morphism $f : C \to \mathbb{P}^1$ is not surjective since f is regular for all $P \in C$. Since morphisms between curves are either constant or surjective, we have that f is a constant. The reverse direction follows from definition.
(b) See [3], Chapter II, Corollary 6.10. □

Definition 2.23. The degree zero part of $\mathrm{Div}(C)$, denoted by $\mathrm{Div}^0(C)$, is the subgroup of divisors with degree 0. The degree zero part of the Picard group, denoted by $\mathrm{Pic}^0(C)$, is the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors.

Suppose $\phi : C_1 \to C_2$ is a morphism of curves. We have two induced maps of divisor groups

$$\phi^*_{\mathrm{Div}} : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1),\ \phi^*_{\mathrm{Div}}((Q)) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) \tag{2.24}$$

$$\phi_{\mathrm{Div}*} : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2),\ \phi_{\mathrm{Div}*}((P)) = (\phi(P)) \tag{2.25}$$

which are extended $\mathbb{Z}-$linearly.

Proposition 2.26. *Let $\phi : C_1 \to C_2$ be a morphism of curves, $P \in C_1$, and $Q \in C_2$. Then*

(a) $\deg(\phi^*_{\mathrm{Div}}(D)) = \deg(\phi)(\deg(D))$
(b) $\phi^*_{\mathrm{Div}}(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$
(c) $\deg(\phi_{\mathrm{Div}*}(D)) = \deg(D)$

(d) $\phi_{\mathrm{Div}*}(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$

Proof. See [6], Chapter 2, Proposition 3.6. □

We now introduce the $\overline{K}(C)$ vector space of space differentials of a curve. These differentials allow us to define the genus of a curve.

Definition 2.27. Let C be a curve. The space of (mereomorphic) differentials of C, denoted by Ω_C, is the $\overline{K}(C)$ vector space generated by symbols dx subject to the three relations:

(1) $d(a) = 0$ for all $a \in \overline{K}$.
(2) $d(x+y) = dx + dy$ for all $x, y \in \overline{K}(C)$.
(3) $d(xy) = xdy + ydx$ for all $x, y \in \overline{K}(C)$.

Suppose that $\phi : C_1 \to C_2$ is a morphism of curves. The morphism induces a map of between spaces of differentials, defined by

$$\phi_\omega^* : \Omega_{C_2} \to \Omega_{C_1},\ \phi_\omega^*(\sum_i f_i dx_i) = \sum_i \phi^*(f_i) d(\phi^*(x_i)), \tag{2.28}$$

where $\phi^* : \overline{K}(C_2) \to \overline{K}(C_1)$ is the pullback on function fields.

Proposition 2.29. *Let C be a curve.*

(a) Ω_C is a one dimensional $\overline{K}(C)$-vector space.
(b) Let $x \in \overline{K}(C)$. We have dx is a $\overline{K}(C)$-basis iff $\overline{K}(C)/\overline{K}(x)$ is a finite separable extension.
(c) Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is separable iff

$$\phi_\omega^* : \Omega_{C_2} \to \Omega_{C_1}$$

is injective.

Proof. See [6], Chapter 2, Proposition 4.2. □

Proposition 2.30. *Suppose that C is a smooth curve and t is a uniformizer for a point P of C.*

(a) Suppose $\omega \in \Omega_C$. Then there exists a unique $f \in \overline{K}(C)$, such that $\omega = f dt$. We denote the unique differential associated to f by ω/dt.
(b) Suppose $f \in \overline{K}(C)$ is regular at P. Then df/dt is regular.
(c) Suppose $\omega \in \Omega_C$ is a nonzero differential. Then the quantity

$$\mathrm{ord}_P(\omega/dt)$$

is independent of choice of uniformizer. The value $\mathrm{ord}_P(\omega)$ is called the order of ω at P.

Proof. (a) This follows from (2.29a), (2.29b), and that $\overline{K}(C)/\overline{K}(t)$ is a finite separable extension.
(b) See [3], comment following IV.2.1.
(c) Suppose that t' is another uniformizer at P. Then from (a), we can write uniquely $\omega = f dt' = f\frac{dt'}{dt} dt$. From (b) and that $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$, we obtain the result. □

We can associate a divisor with a differential by employing its order at points of C. This allows us to define the canonical divisor of a curve.

Definition 2.31. Let $\omega \in \Omega_C$ be a differential of C. Its associated $\mathrm{div}(\omega)$ is

$$\mathrm{div}(\omega) = \sum_P \mathrm{ord}_p(\omega)P \tag{2.32}$$

Definition 2.33. The canonical divisor class of C is the class of any $\mathrm{div}(\omega)$ in $\mathrm{Pic}(C)$ with $\omega \neq 0$. Any divisor in the canonical divisor class is called a canonical divisor, which we denote by K_C.

Example 2.34. Let $C = \mathbb{P}^1$ and t be a coordinate function. We observe that we have the uniformizer $\frac{1}{t}$, which yields by (2.30a)

$$dt = -t^2 d(\frac{1}{t}).$$

From this, at the point of infinity ∞ we have $\mathrm{ord}_\infty(dt) = -2$.

We define a partial order on $\mathrm{Div}(C)$ in the following manner.

Definition 2.35. Let D, D' be divisors of C. We say D is positive if $n_p \geq 0$ for all $P \in C$. We say $D \geq D'$ if $D - D'$ is a positive divisor.

Remark 2.36. Note that $f \in \overline{K}(C)$ has a zero of order at most n at P iff $\mathrm{div}(f) \geq nP$. In a similar fashion, f has a pole of order at most n at P iff $\mathrm{div}(f) \geq -nP$.

Definition 2.37. Suppose D is a divisor of C. We can associate to D the $\overline{K}$-vector space of functions $\mathcal{L}(C) := \{f \in \overline{K}(C)^*\} \cup \{0\}$. We denote its dimension by $\ell(D)$.

Remark 2.38. It's clear from definition that $\mathcal{L}(C)$ is a $\overline{K}-$vector space.

Proposition 2.39. *Suppose $D \in \mathrm{Div}(C)$. Then*

(a) If $\deg(D) < 0$, then $\ell(D) = 0$
(b) $l(D)$ is finite.
(c) If D and D' have the same class in $\mathrm{Pic}(C)$, then $\ell(D) = \ell(D')$.

Proof. (a) Suppose that $\mathcal{L}(C)$ has a non-zero element f. Observe by (2.22b), we have

$$0 = \deg(\mathrm{div}(f)) \geq \deg(-D) = -\deg(D),$$

which contradicts our assumption.
(b) [3], Chapter 2, Theorem 5.19.
(c) From the assumption, we have $D = D' + g$ with $g \in \mathcal{K}(C)^*$. Thus, we can define the isomorphism $\varphi : \mathcal{L}(D) \to \mathcal{L}(D'),\ f \mapsto fg$.

□

Theorem 2.40. *Let C be a smooth curve and K_C be a canonical divisor of C. Then we have the following equality*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1 \tag{2.41}$$

with g being the genus of the curve C.

There are several easy and useful results which relate the canonical divisor with the genus of a curve.

Corollary 2.42. *We have the following three equalities:*

(a) $\ell(K_C) = g$.
(b) $\deg(K_C) = 2g - 2$.
(c) If $\deg(D) > 2g - 2$, then $\ell(D) = \deg(D) - g + 1$.

Proof. (a) Employ (2.40) with $D = 0$ and note that $\ell(0) = 1$.
(b) Use part (a) and substitute $D = K_C$.
(c) From part (b), we obtain $\deg(K_C - D) < 0$. Observe from (2.39.a), we have $\ell(K_C - D) = 0$, thus by (2.40) we have our result. □

Remark 2.43. The genus may be viewed as the standard topological invariant when curves are viewed as compact Riemann surfaces. In the case when we are dealing with elliptic curves, the genus equaling one corresponds with the interpretation that elliptic curves are complex torii.

3. Elliptic Curves, the Group Law, and Isogenies

This section is an introduction to elliptic curves and their fundamental algebraic properties. Throughout this section, K will denote a perfect field.

Definition 3.1. An elliptic curve E is a smooth genus one curve with a single base point (point at infinity), denoted by $O = [0, 1, 0]$.

There is a more concrete definition which connects elliptic curves to solution sets of non-singular Weierstrass equations.

Definition 3.2. A Weierstrass (homogeneous) equation is a cubic equation of the form

$$f(x, y) = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.3}$$

with $a_1, \cdots, a_6 \in \overline{K}$.

Remark 3.4. Since E is a projective sub-variety of $\mathbb{P}^2(\overline{K})$, the reader should have mind that (3.3) is of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4x + a_6,\ a_1, \cdots, a_6 \in \overline{K}.$$

This presentation shows that $O = [0, 1, 0] \in E$.

Proposition 3.5. *Let E/K be an elliptic curve. There exists functions $x, y \in K(E)$, such that the map*

$$\phi : E \to \mathbb{P}^2, \phi = [x, y, 1]$$

is an isomorphism of E/K onto a curve whose homogeneous ideal is generated by the smooth Weierstrass equation

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in K$ and $\phi(O) = [0, 1, 0]$. The functions x and y are called Weierstrass coordinate functions.

Proof. See [6], Chapter 3, Proposition 3.1. □

Remark 3.6. It should be noted that if we consider isomorphism classes of elliptic curves that the Weierstrass equation is not unique. However, a Weierstrass equation is unique up to linear change of variables. For instance, if K is a field of characteristic 0, then a Weierstrass equation of an isomorphism class of elliptic curves can take the form

$$E : y^2 = x^3 + Ax + B,\ A, B \in \overline{K}.$$

We will employ the following useful coefficients of elliptic curves

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6,\ b_8 = \frac{b_2b_6 - b_4^2}{4}. \tag{3.7}$$

Using these coefficients, we define the discriminant Δ and $j-$invariant of an elliptic curve as follows:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{3.8}$$

$$j(E) = \frac{(b_2^2 - 24b_4)^3}{\Delta}. \tag{3.9}$$

Remark 3.10. Remarkably, two elliptic curves have the same $j-$invariant iff they are isomorphic as abelian varieties.

We can construct a group law on the set of points of an elliptic curve which has a simple geometric interpretation.

Definition 3.11. Let E be an elliptic curve and $P, Q \in E$. Let L be the through P and Q (tangent line if $P = Q$) and R be the third point of intersection of E and L. Let L' be the vertical line (line connecting R and O). Then L' intersects a third point, which we denote by $P + Q$.

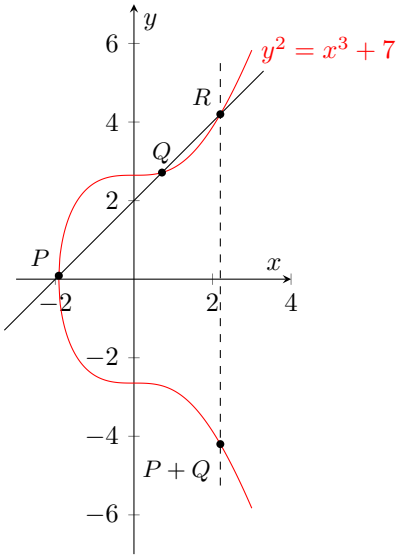

Figure 1: An illustration of the group law on the elliptic curve $y^2 = x^3 + 7$.

Proposition 3.12. *The composition law gives an abelian group structure on E.*

Proof. The only property not immediately obvious from the geometric interpretation is associativity. We'll prove that this operation is associative later in (3.18*c*). Note that the identity element with respect to the composition law is O. □

Example 3.13. Let $E/\mathbb{Q}$ be the elliptic curve $E : y^2 = x^3 + 1$, $P_1 = (-1, 0)$ and $P_2 = (1, 0)$ be integral points on E. We have that

$$P_1 + P_2 = (-2, 3),\ 2P_2 = (0, -1).$$

Now that we know that ellliptic curves are abelian groups, we will employ isogenies, which are morphisms of abelian varieties. We will present the less restrictive definition, which only requires invariance with respect to the point at infinity.

Definition 3.14. Suppose E_1 and E_2 are elliptic curves. An isogeny $\phi : E_1 \to E_2$ is a morphism satisfying $\phi(O) = O$. We say two elliptic curves E_1 and E_2 are isogenous if there exists a non-trivial isogeny $\phi : E_1 \to E_2$. We denote the space of isogenies from E_1 to E_2 by $\mathrm{Hom}(E_1, E_2)$.

Just like we did with curves, we say an isogeny $\phi : E_1 \to E_2$ is separable or inseparable if it has that property when viewed as a morphism of curves. We will again let $\deg(\phi)$ denote the degree of the field extension $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$. Similarly, we denote $\deg_s(\phi)$ and $\deg_i(\phi)$ to mean the separable and inseparable degree of the aforementioned extension of fields. We follow standard convention and let $\deg[0] = 0$ to ensure the multiplicativity of degrees:

$$\deg(\varphi \circ \phi) = \deg(\varphi)\deg(\phi) \text{ for all chains of isogenies } E_1 \xrightarrow{\phi} E_2 \xrightarrow{\varphi} E_3$$

Example 3.15. Suppose that K has characteristic $p > 0$ and let E/K have the Weierstrass equation

$$f(x, y) = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in K.$$

We observe that to verify that E^q is an elliptic curve, it suffices to show that f^q remains non-singular. By employing that the qth-power map is a field homomorphism, one may do a tedious calculation

$$j(E^q) = (j(E))^q \text{ and } \Delta(E^q) = (\Delta)^q.$$

Thus E^q remains an elliptic curve since the discriminant is non-zero (see [6], Chapter III, Proposition 1.4a). It's clear that the qth-power Frobenius map $\varphi((x, y)) = (x^q, y^q)$ preserves the point at infinity. Thus φ is an isogeny from E to E^q. We note that if $K = \mathbb{F}_q$, that $f^q = f$, thus $\varphi : E \to E$. It's also clear from definition that the fixed points of φ is $E(\mathbb{F}_q)$.

Remarkably, isogenies are automatically algebraic group homomorphisms.

Theorem 3.16. *Suppose $\phi : E_1 \to E_2$ is an isogeny. Then for all $P, P' \in E_1$,*

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

We require two lemmas which allow us to construct maps between E and $\mathrm{Pic}^0(E)$.

Lemma 3.17. *Suppose E is an elliptic curve and $P, Q \in E$. Then $(P) \sim (Q)$ iff $P = Q$.*

Proof. By definition, there exists an $f \in K(C)^*$, such that $\mathrm{div}(f) = (P) - (Q)$. This implies that $f \in \mathcal{L}(Q)$, but by (2.42c) we obtain $\dim \mathcal{L}(Q) = 1$, which implies $f = c \in \overline{K}^*$. Since $\mathrm{div}(c) = 0$, we have our result. The reverse direction is clear. □

Lemma 3.18. *Suppose E is an elliptic curve. Then following statements hold:*

- *(a) There exists a surjective map $\sigma : \mathrm{Div}^0(C) \to E$ which sends D to the unique point P, such that $D \sim (P) - (O)$.*
- *(b) Let $D_1, D_2 \in \mathrm{Div}^0(E)$. Then $\sigma(D_1) = \sigma(D_2)$ iff $D_1 \sim D_2$. Thus, σ induces a bijection of sets $\sigma : \mathrm{Pic}^0(E) \simeq E$.*
- *(c) The map $\kappa : E \to \mathrm{Pic}^0(E),\ \kappa(P) = [(P) - (O)]$ is the inverse σ and is also a group homomorphism.*

Proof. (a) By corollary 2.42*c*, we obtain that $\ell(D+(O)) = 1$. Suppose $f \in \overline{K}(E)$ is a basis element of $\mathcal{L}(D+(O))$. By definition and (2.22*b*), we have $\operatorname{div}(f) \geq -D-(O)$ and $\deg(\operatorname{div}(f)) = 0$, thus

$$\deg(\operatorname{div}(f) + (D + (O))) = 1$$

which implies there exists a $P \in E$, such that $\operatorname{div}(f) = (P) - (O) - D$.

For uniqueness, observe that since $\sim$ is an equivalence relation, that for any P' which satisfies this property, we have

$$(P) \sim D + (O) \sim (P').$$

and by (3.17) yields uniqueness. For surjectivity, observe that $D = (P) - (O)$ is a preimage of (P).
(b) Let $P = \sigma(D)$ and $P' = \sigma(D')$. Then from the definition of σ, we obtain $(P) - (P') \sim D - D'$. If $P = P'$, then $D \sim D'$. For the other direction, if $D \sim D'$, observe that we have $(P) - (P') = \operatorname{div}(f)$ which by (3.18) yields the result.
(c) From part (a), it's clear that κ is the inverse of the induced map of σ, thus we focus on proving that it is a group homomorphism. Let $L : \alpha x + \beta y + \gamma z = 0$ be the line which connects P, Q and R. Let $L' : \alpha' x + \beta' y + \gamma' z = 0$ be the vertical line connecting R and O. We observe that since the line $Z = 0$ intersects E at O with multiplicity three, we have

$$\operatorname{div}(\mathrm{L/Z}) = (P) + (Q) + (R) - 3(O)$$
$$\operatorname{div}(\mathrm{L'/Z}) = (R) + (P + Q) - 2(O).$$

Thus, subtracting the second equation by the first, we obtain

$$\operatorname{div}(f'/f) = (P + Q) - (P) - (Q) + (O),$$

thus by definition of κ, we have $\kappa(P + Q) - \kappa(P) - \kappa(Q) = 0$ which yields the result. □

(3.16). We note that the map ϕ^*_{Div} preserves principal divisors and divisors of zero degree by (2.26*a*) and (2.26*b*). From (3.18), we have the group isomorphism

$$\kappa_i : E_i \to \operatorname{Pic}^0(E_i),\ P \mapsto [(P) - (O)].$$

Observe that we have commutative diagram by definition of κ_i and that $\phi(O) = O$

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \operatorname{Pic}^0(E) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_{\mathrm{Div}*}} \\ E_2 & \xrightarrow{\kappa_2} & \operatorname{Pic}^0(E_2). \end{array}$$

Since the κ_i are group isomorphisms and $\phi_{\mathrm{Div}*}$ is a group homomorphism, we have ϕ is a group homomorphism as desired.

□

There is a useful corollary of (3.17) and (3.18) in determining when a zero degree divisor is principal.

Corollary 3.19. *Suppose E is an elliptic curve and $D = \sum_P n_p(P) \in \operatorname{Div}(E)$. Then D is a principal divisor iff $D \in \operatorname{Div}^0(C)$ and $\sum_{P \in E}[n_P]P = O$.*

Proof. Note that a principal divisor D has degree 0. Since σ is a bijection, we have $D \sim O$ iff $\sigma(D) = O$. Note that

$$\sigma(D) = \sigma(\sum_{P\in E}[n_P]P) = \sigma(\sum_{P\in E} n_p(P) - \sum_{P\in E} n_P(O)) = \sum_{P\in E}[n_p]P,$$

which yields the result.

□

One useful invariant of elliptic curves is the invariant differential ω. This differential gives a useful criteria of when a map is separable, which will be employed for the proof of the Hasse-Weil Bound.

Definition 3.20. Let E be an elliptic curve whose Weierstrass equation is given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. The invariant differential of E, denoted by ω_E, is the differential of the form

$$\omega_E = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4}. \tag{3.21}$$

Since the proof of the following theorem is quite technical and not much related to our latter results, we omit the proof.

Theorem 3.22. *Suppose E and E' are elliptic curves and ω is an invariant differential of E. If $\phi, \varphi : E' \to E$ are isogenies, then*

$$(\phi + \varphi)^*(\omega) = \phi^*(\omega) + \varphi^*(\omega)$$

with addition on the left-hand side being point-wise addition in $\mathrm{Hom}(E_1, E_2)$ *and on the right-hand side being addition in Ω_E.*

Proof. See [6], Chapter III, Theorem 5.2. □

There are several nifty corollaries of (3.22) which will allow us to employ the inseparablity of the qth-power Frobenius morphism. We will first need the $m-$multiplication isogeny to construct separable maps.

Definition 3.23. Let E/K be an elliptic curve and $m \in \mathbb{Z}$. The $m-$multiplication isogeny, denoted by $[m] : E \to E$, is defined if $m > 0$ as

$$[m]P = P + \cdots + P = mP \tag{3.24}$$

for $P \in E$. If $m < 0$, then

$$[m]P = [-m](-P) = (-P) + \cdots + (-P). \tag{3.25}$$

The kernel of this map, denoted by, $E[m] = \{P \in E |\ [m]P = O\}$ is the $m-$torsion points of E.

Remark 3.26. Note from (2.29c) that we clearly have $[m]$ is a separable map if $m \neq 0$.

Corollary 3.27. *For any invariant differential ω of E, we have*

$$[m]^*\omega = m\omega.$$

Proof. It is immediate for $m = 0, 1$ that we have the result, thus we proceed to the inductive step. Observe from (3.22), that we have

$$[m+1]^*\omega = [m]^*\omega + \omega = (m+1)\omega,$$

which gives the result. The case when m is negative uses the same approach.

□

We can employ (3.22) and (3.27) to construct a family of separable maps from the qth-power Frobenius morphism.

Corollary 3.28. *Suppose $E/\mathbb{F}_q$ with $\mathbb{F}_q$ a field of characteristic p. Let ϕ be the $qth-$power Frobenius morphism and $m, n \in \mathbb{Z}$. Then the map*

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

is separable iff $p \nmid m$.

Proof. Let ω be an invariant differential of E. It suffices to check by 2.29c that $[m + n\phi]^*\omega \neq 0$ iff $p \nmid m$. Observe by (2.11), (2.29c), (3.22), (3.27), that we have

$$[m + n\phi]^*\omega = [m]^*(\omega) = m\omega.$$

Note that $m\omega = 0$ iff $p|m$, which yields the result. □

We will employ a strengthen form of (2.15) in the case when $\phi : E_1 \to E_2$ is an isogeny. We'll also need to use the translation map $\tau_R : E \to E,\ \tau(P) = P + R$.

Proposition 3.29. *Suppose $\phi : E_1 \to E_2$ is a non-zero isogeny.*

(a) For every $Q \in E_2$, $|\phi^{-1}(Q)| = \deg_s(\phi)$. In addition, for any $P \in E_1$, we have $\deg_i(\phi) = e_\phi(P)$.
(b) Suppose that ϕ is separable. Then ϕ is unramified and $|\ker \phi| = \deg(\phi)$.

Proof. (a) Note that from (2.15b), that for all but finitely many $Q \in E_2$, we have $|\phi^{-1}(Q)| = \deg_s(\phi)$. Note for any Q, Q', we have there exists an $P \in E_1$, such that $\phi(P) = Q' - Q$ due to the surjectivity of ϕ. Since ϕ is a group homomorphism, we have the one-to-one correspondence of fibres

$$\phi : \phi^{-1}(Q) \simeq \phi^{-1}(Q'),\ P \mapsto P + R. \tag{3.30}$$

Since there are only finitely many Q' where $\deg_s(\phi) \neq |\phi^{-1}(Q')|$, applying (2.15$b$) gives the first part of (3.29a).

For the second part of (a), suppose $P, P' \in E_1$ with $P, P' \in \phi^{-1}(Q)$ and $R = P' - P$. We observe that $\phi \circ \tau_R = \phi$. Using (2.15c) and the definition of τ_R, we have

$$e_\phi(P) = e_{\phi\circ\tau_R}(P)e_\phi(\tau_R(P))e_{\tau_R}(P) = e_\phi(P'),$$

thus ϕ has the same ramification index for any $P \in \phi^{-1}(Q)$. We have by the first part of (a),

$$\deg(\phi) = |\phi^{-1}(Q)|e_\phi(P) = \deg_s(\phi)e_\phi(P) = \deg_s(\phi)\deg_i(\phi),$$

which yields the second part.

(b). Since ϕ is separable, we have for all $Q \in C_2$, that $|\phi^{-1}(Q)| = \deg(\phi)$. Observe from (2.15$a$), we have $|\phi^{-1}(Q)| = \deg(\phi)$ for all $Q \in C_2$ iff $\sum_{P\in\phi^{-1}(Q)} e_\phi(P) = |\phi^{-1}(Q)|$. Since by definition, we have $e_\phi(P) \geq 1$, we must have that $e_\phi(P) = 1$, which yields the result. To obtain the equality $|\ker \phi| = \deg(\phi)$ substitute O for P. □

3.1. **The Dual Isogeny and Weil Pairing.** We can define an involution on $\mathrm{Hom}(E_1, E_2)$ which provides a new isogeny $\hat{\phi} : E_2 \to E_1$ with especially nice properties.

Definition 3.31. Suppose $\phi : E_1 \to E_2$ is an isogeny with degree m. The dual isogeny, denoted by $\hat{\phi} : E_2 \to E_1$, is the unique isogeny, such that $\hat{\phi} \circ \phi = [m]$.

The existence of the dual isogeny is rather unelightening, thus we'll only prove the uniqueness and a concrete form. Let $\psi : \mathrm{Div}(E) \to E$ be defined as

$$\psi : \mathrm{Pic}(E) \to E : \ \psi(\sum_{P \in E} n_p(P)) = \sum_{P \in E} [n_P]P. \tag{3.32}$$

Proposition 3.33. *Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree m. Then*

(a) The dual isogeny $\hat{\phi}$ is unique.
(b) The dual isogeny when viewed as a group homomorphism takes the form

$$\hat{\phi} = \psi \circ \phi^*_{\mathrm{Div}} \circ \kappa_2.$$

Proof. (a) Suppose there exists a $\hat{\phi}'$ with the same property. Then

$$(\hat{\phi}' - \hat{\phi}) \circ \phi = 0,$$

which implies that $\hat{\phi}' = \hat{\phi}$ since ϕ is an epimorphism.
(b) By uniqueness, it suffices to check that the map $\hat{\phi}$ suffices the defining property of the dual isogeny. Suppose $Q \in E_2$, we then have

$$\begin{aligned}
\psi \circ \phi^*_{\mathrm{Div}} \circ \kappa_2(Q) &= \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T \in \phi^{-1}(O)} [e_\phi(T)]T \\
&= [\deg_i(\phi)] \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(O)} T \right) \\
&= [\deg_i(\phi)] \left(\sum_{T \in \phi^{-1}(O)} P + T - \sum_{T \in \phi^{-1}(O)} T \right) \\
&= [\deg_i(\phi)] \circ [|\phi^{-1}(Q)|]P = [\deg(\phi)]P
\end{aligned}$$

□

Proposition 3.34. *Let $\phi : E_1 \to E_2$ be an isogeny and $m = \deg(\phi)$. Then the following properties hold*

(a) $\phi \circ \hat{\phi} = [m]$ on E_2.
(b) Suppose $\varphi : E_2 \to E_3$ is another isogeny, then $\widehat{\varphi \circ \phi} = \hat{\phi} \circ \hat{\varphi}$.
(c) Let $\tau : E_1 \to E_2$ be another isogeny, then $\widehat{\phi + \tau} = \hat{\phi} + \hat{\tau}$.
(d) For all $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.
(e) $\deg(\hat{\phi}) = \deg(\phi)$.

Proof. (a) Observe that we have $(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi$. Since ϕ is surjective we obtain the result.
(b) Suppose $n = \deg(\varphi)$. We observe that

$$(\hat{\phi} \circ \hat{\varphi}) \circ (\varphi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [nm].$$

From the uniqueness statement of (3.34a), we have the result $\hat{\phi} \circ \hat{\varphi} = \widehat{\varphi \circ \phi}$.
(c) See [6], Chapter III, Theorem 6.2c.
(d) For $m = 0, 1$ the result is clear, thus we proceed to the inductive step. We observe from (c), that

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]} = [m] + [1] = [m+1].$$

For the case when m is negative, one can use the same argument outlined above.

For the second part of (d), suppose $d = \deg[m]$. We observe by definition of the dual isogeny, we have

$$\widehat{[m]} \circ [m] = [m] \circ [m] = [m^2],$$

which yields the result.
(e) Suppose $m = \deg(\phi)$. From parts (a) and (d), we have

$$m^2 = \deg[m] = \deg(\phi \circ \hat{\phi}) = (\deg(\phi))(\deg(\hat{\phi})) = m \deg(\hat{\phi}),$$

which yields the result.

□

Corollary 3.35. *Suppose E is an elliptic curve and m is an integer.*

(a) Suppose $\mathrm{char}(K) \nmid m$. *Then* $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(b) If the characteristic of K divides m, the one of the following is true:

$$E[p^e] = \{0\} \text{ for all } e \geq 0$$
$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z} \text{ for all } e \geq 0$$

Proof. (a) We note by (3.34d), we have $\deg[m] = m^2$, thus we have that $|E[m]| = \deg[m] = m^2$ by (3.29b) and $[m]$ being separable by assumption. Observe that for $d|m$, we have $|E[d]| = d^2$, thus by the fundamental of finitely generated groups, we have $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
(b) Suppose ϕ is the pth-power Frobenius morphism. We note by applying (2.11), (3.29a), and the definition of the dual isogeny, we obtain the chain of equalities

$$|E[p^e]| = (\deg_s(\hat{\phi} \circ \phi))^e = (\deg_s \hat{\phi})^e.$$

From (2.12) and (3.34e), we have $\deg(\hat{\phi}) = p$, thus either $\hat{\phi}$ is separable or purely inseparable. For the former case, we have the first possibility. One then employs writing $E[p^e]$ as a product of cyclic groups to obtain the decomposition. Otherwise, $|E[p^e]| = 1$, which yields the second case.

□

3.2. **Preparation for Elliptic Curves over Finite Fields.** This subsection will introduce the preparatory results to prove the Hasse-Weil bound and Weil conjectures. We'll start by proving an important fact that the degree map is a quadratic form on the abelian group of isogenies of an elliptic curve. This allows us to prove the Hasse-Weil bound via an easy application of the Cauchy-Schwarz inequality. In the latter part, we'll analyze the the representation of the Galois group $G(\overline{K}/K)$ on the ℓ-adic Tate module $T_\ell(E)$. This representation will pave way to an easy proof of the Weil conjectures for elliptic curves.

Definition 3.36. Suppose A is an abelian group. A quadratic form $d : A \to \mathbb{Z}$ is a function which has the two properties:

(i) $d(-\alpha) = d(\alpha)$
(ii) The pairing $B : A \times A \to \mathbb{Z}$ defined by

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

is bilinear.

A quadratic form is said to be positive definite, if in addition in satisfying the two properties above, it also satisfies:

(iii) $d(\alpha) \geq 0$ for all $\alpha \in A$.
(iv) $d(\alpha) = 0$ iff $\alpha = 0$.

Proposition 3.37. *Suppose that E_1 and E_2 are ellptic curves. Then the degree map*

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

is a positive definite quadratic form.

Proof. All properties except (3.36*ii*) are obvious from definitions. We need to verify that

$$B(\varphi, \phi) = \deg(\varphi + \phi) - \deg(\varphi) - \deg(\phi)$$

is a bilinear map. We obtain from the definition of the dual isogeny, the equality

$$B(\varphi, \phi) = \widehat{\varphi + \phi} \circ (\varphi + \phi) - \hat{\varphi} \circ \varphi - \hat{\phi} \circ \phi = \hat{\varphi} \circ \phi + \hat{\phi} \circ \varphi.$$

From the above equation and $\widehat{\phi + \phi'} = \hat{\phi} + \hat{\phi}'$, we obtain the desired result. □

Suppose $m \geq 2$ and the characteristic of K does not divide m. Then by (3.35a), we have $E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Recall that $G(\overline{K}/K)$ acts on E by

$$\sigma(P) = [\sigma(x_0), \sigma(x_1), \sigma(x_2)]. \tag{3.38}$$

We note that $E[m]$ is invariant under the action of the absolute Galois group $G(\overline{K}/K)$, since for any $\sigma \in G(\overline{K}/K)$, we have

$$[m](\sigma(P)) = \sigma([m]P) = \sigma(O) = O.$$

Thus, we have a representation $G(\overline{K}/K) \to \mathrm{Aut}(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z})$.

Suppose that $\ell \in \mathbb{Z}$ is a prime. We note that we have the inversely directed family of abelian groups $(\{E[\ell^n]\}, \{f_i^j\})$ with $f_i^j(m_j) = [\ell^{j-i}]m_j$.

Definition 3.39. Suppose $\ell \in \mathbb{Z}$ is a prime. We define the $\ell-$adic Tate module of E, denoted by $T_\ell(E)$, as the inverse limit

$$T_\ell(E) = \varprojlim_n E[\ell^n]. \tag{3.40}$$

We will also need the same construction for mth-roots of unity.

Definition 3.41. Let $\mu_{\ell^n} \subset \overline{K}$ denote the group of ℓ^nth roots of unity. We have the inversely directed system of abelian groups $(\{\mu_{\ell^n}\}, \{f_i^j\})$ with $f_i^j(m_j) = (m_j)^{\ell^{j-i}}$. The Tate module of K is the inverse limit of abelian groups

$$T_\ell(\mu) = \varprojlim_n \mu_{\ell^n}. \tag{3.42}$$

Remark 3.43. Concretely we may view $T_\ell(E) \subset \prod_n E[\ell^n]$ with $(x_0, x_1, \cdots,) \in T_\ell(E)$ if $x_{i-1} = f_{i-1}^i(x_i)$ for all $i \geq 1$.

Let $(a_1, a_2, \cdots) \in \mathbb{Z}_\ell$ and $(m_1, m_2, \cdots) \in T_\ell(E)$. Note that $E[\ell^n]$ has a $\mathbb{Z}/\ell^n\mathbb{Z}$-module structure defined by scalar multiplication. Thus, we can define a $\mathbb{Z}_\ell-$module structure on $T_\ell(E)$ by

$$(a_1, a_2, \cdots) \cdot (m_1, m_2, \cdots) = ([a_1]m_1, [a_2]m_2, \cdots).$$

Proposition 3.44. *Let $\mathbb{Z}_\ell$ denote the $\ell-$adic integers. The $\ell-$adic Tate module has the following properties as a $\mathbb{Z}_\ell$-module:*

(a) If $\ell \neq \mathrm{char}(K)$, then $T_\ell(E) = \mathbb{Z}_\ell \times \mathbb{Z}_\ell$.
(b) If $\ell = \mathrm{char}(K)$, then $T_\ell(E) = \{0\}$ or $T_\ell(E) = \mathbb{Z}_\ell$

Proof. The proof for both statements follows immediately (3.35a), (3.35b), and that inverse limits preserve direct products. □

We note that since $E[\ell^n]$ is invariant under the group action of $G(\overline{K}/K)$ for any n, we have a representation of $G(\overline{K}/K)$ on $T_\ell(E)$.

Definition 3.45. The $\ell-$adic representation of $G(\overline{K}/K)$ is the homomorphism $\rho : G(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E))$ defined by

$$\sigma(m_1, m_2, \cdots) = (\sigma(m_1), \sigma(m_2), \cdots). \tag{3.46}$$

Remark 3.47. We verify that this group action is well defined with the respect to the compatibility condition. We note that $f_{i-1}^i(\sigma m_i)) = [l](\sigma(m_i)) = \sigma([l]m_i) = \sigma(m_{i-1})$ which is the desired result.

We will employ the $\ell-$adic Tate module in studying isogenies. We note an isogeny $\phi : E_1 \to E_2$ induces maps

$$\phi : E_1[\ell^n] \to E_2[\ell^n],$$

since ϕ is a group homomorphism. Thus ϕ induces a $\mathbb{Z}_\ell-$linear map

$$\phi_\ell : T_\ell(E_1) \to T_\ell(E_2),\ \phi_\ell((m_1, m_2, \cdots)) = (\phi(m_1), \phi(m_2), \cdots). \tag{3.48}$$

In the case where $\ell \neq \mathrm{char}(K)$, we have $T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Thus with respect to some basis, ϕ_ℓ may be represented by a 2×2 matrix with coefficients in $\mathbb{Z}_\ell$. We will analyze $\det(\phi_\ell)$ and $\mathrm{tr}(\mathrm{tr}_\ell)$ by constructing a bilinear, non-degenerate, and alternating form on $T_\ell(E)$.

Suppose $P \in E[m]$. We note that $m(P) - m(O) = \mathrm{div}(f)$ for some $f \in \overline{K}(E)$ by (3.17). Let $P' \in E$ be a point where $[m]P' = P$. Since $[m]$ is unramified due to being separable, we have

$$[m]^*_{\mathrm{Div}}(Q) = \sum_{P \in [m]^{-1}(Q)} P,$$

thus

$$[m]^*_{\mathrm{Div}}(P) - [m]^*_{\mathrm{Div}}(O) = \sum_{R \in E[m]} ((P' + R) - (R)).$$

By (3.17), there exists a $g \in \overline{K}(E)$, such that $\mathrm{div}(g) = [m]^*_{\mathrm{Div}}(P) - [m]^*_{\mathrm{Div}}(O)$ since $|E[m]| = m^2$. We observe that

$$\mathrm{div}(g^m) = \sum_{R \in E[m]} (m(T' + R) - m(R)) = \mathrm{div}(f \circ [m]),$$

since f vanishes and has a pole at P and O respectively. Thus, we can assume by re-scaling that $g = f \circ [m]$. We observe for any $Q \in E[m]$, that

$$g(X+Q)^m = f([m]X + [m]Q) = f([m]X) = g(X)^m.$$

Thus as a function of X, we have $\left(\frac{g(x+Q)}{g(X)}\right)^m = 1$, which implies $g(X+Q)/g(X)$ takes values in μ_m which are the mth roots of unity. This implies that the morphisim $E \to \mathbb{P}^1,\ X \mapsto \frac{g(X+Q)}{g(X)}$ is constant.

Definition 3.49. Suppose E is an elliptic curve and $P, Q \in E$. The Weil e_m-pairing is defined by

$$e_m : E[m] \times E[m] \to \mu_m,\ e_m(Q,P) = \frac{g(X+Q)}{g(X)} \tag{3.50}$$

with g being the polynomial derived from $m(P) - m(O)$ and $X \in E$ being any value where $g(X+Q)$ and $g(X)$ are both well-defined and non-zero.

Proposition 3.51. *The Weil e_m-pairing has the following properties:*

(a) It is bilinear:

$$e_m(Q_1+Q_2,P) = e_m(Q_1,T)e_m(Q_2,P),$$
$$e_m(Q,P_1+P_2) = e_m(Q,P_1)e_m(Q,P_2)$$

(b) It is alternating: $e_m(P,P) = 1$. In particular $e_m(Q,P) = e_m(P,Q)^{-1}$.

(c) It is non-degenerate: If $e_m(Q,P) = 1$ for all $S \in E[m]$, then $P = O$.

(d) For any $Q \in E[mm']$ and $P \in E[m]$, we have the compatibility relation

$$e_{mm'}(Q,P) = e_m([m']Q,P).$$

Proof. See [6], Chapter 3, Proposition 8.1. □

Proposition 3.52. *Suppose $\phi : E_1 \to E_2$ is an isogeny of elliptic curves. Then for all torsion points $P \in E_1[m]$ and $Q \in E_2[m]$,*

$$e_m(P, \hat{\phi}(Q)) = e_m(\phi(P), Q).$$

Proof. We observe from definition that $e_m(\phi(P),Q) = \frac{g(X+\phi(P))}{g(X)}$with $g^m(X) = f \circ [m](X)$. We will now construct the associated f and g for $\hat{\phi}(Q)$. From (3.33*b*), there exists a $h \in \overline{K}(E_1)$, such that

$$\phi^*_{\mathrm{Div}}((Q)) - \phi^*_{\mathrm{Div}}((O)) = \mathrm{div}(h) - (O) + (\hat{\phi}(Q)).$$

We obtain

$$\mathrm{div}\left(\frac{f\circ\phi}{h^m}\right) = \phi^*_{\mathrm{Div}}(\mathrm{div}(f)) - m\mathrm{div}(h) = m(\hat{\phi}(Q)) - m(O)$$

from $\mathrm{div}(f) = m(Q) - m(O)$. We also obtain by the defining property of g,

$$\left(\frac{g\circ\phi}{h\circ[m]}\right)^m = \frac{f\circ[m]\circ\phi}{(h\circ[m])^m} = \left(\frac{f\circ\phi}{h^m}\right)\circ[m].$$

From these two equations we have

$$e_m(P,\hat{\phi}(Q)) = \frac{g(\phi(X)+\phi(P))}{g(\phi(X))} \cdot \frac{h([m]X)}{h([m]X+[m]P)} = e_m(\phi(P),Q)$$

□

Suppose that $\ell \neq \text{char}(K)$. The Weil e_m-pairing induces an $\ell-$adic Weil pairing

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

which is defined component-wise. One may verify that $e_{\ell^{n+1}}(P,Q)^\ell = e_{\ell^n}([\ell]P, [\ell]Q)$ for any $P, Q \in E[\ell^{n+1}]$ by using the bilinearity and compatiblity of Weil e_m-pairing.

We note that since e is defined component-wise by bilinear, non-degerate, and alternate pairings, that we have the following result.

Proposition 3.53. *The $\ell-$adic Weil pairing is bilinear, non-degenerate, and alternating pairing. In addition, if $\phi : E_1 \to E_2$ is an isogeny, then $e(\phi(P), Q) = e(P, \hat{\phi}(Q))$.*

Recall that if $\ell \neq \text{char}(K)$, that $T_\ell(E)$ is a rank two Z_ℓ-module. So for any endomorphism τ, we can represent it as a 2×2 matrix with coefficients in $\mathbb{Z}_\ell$.

Proposition 3.54. *Let ϕ be an endoisogeny of E and $\phi_\ell : T_\ell(E) \to T_\ell(E)$ the induced $Z_\ell-$linear map. Then $\det(\phi_\ell) = \deg(\phi)$ and $\text{tr}(\phi_\ell) = 1+\deg(\phi)-\deg(1-\phi)$.*

Proof. Let $\{v_1, v_2\}$ be a basis for ϕ_ℓ and let

$$\phi_\ell(v_1) = av_1 + bv_2,\ \phi_\ell(v_2) = cv_1 + dv_2.$$

Thus, with respect to this basis we have

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

Employing the properties of the Weil pairing and dual isogeny, we have

$$\begin{aligned} e(v_1, v_2)^{\deg(\phi)} &= e([\deg(\phi)]v_1, v_2) \\ &= e(\hat{\phi}_\ell \phi_\ell(v_1), v_2) \\ &= e(\phi_\ell(v_1), \phi_\ell(v_2)) \\ &= e(av_1 + bv_2, cv_1 + dv_2) \\ &= e(v_1, v_2)^{\det \phi}. \end{aligned}$$

Since e is a non-degenerate form and the v_1, v_2 are a basis, we have $\deg(\phi) = \det(\phi_\ell)$. The trace formula follows from

$$\text{tr}(A) = 1 + \det(A) - \det(1 - A).$$

with A being a $n \times n$ matrix. □

4. Elliptic Curves over Finite Fields

This section will discuss the properties of elliptic curves of finite fields. We'll first go over the Hasse bound on the number of F_p-rational points of elliptic curves. We conclude with a proof of the Weil conjectures for elliptic curves, which allows us to define the $L-$ series associated with an elliptic curve as a product of local zeta functions. Throughout this section we will let $\mathbb{F}_p$ denote the finite field with p elements and $\mathbb{F}_q$ a finite extension with $q = p^r$.

4.1. **The Hasse-Weil Bound.** Suppose that $E/\mathbb{F}_q$ is an elliptic curves defined over some finite field. We will provide an upper bound on the size of $E(\mathbb{F}_q)$ which by definition is set of ordered pairs $(x, y) \in \mathbb{F}_q^2$, which satisfy

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Artin conjectured that $|E(\mathbb{F}_q)|$ was roughly equivalent to $q + 1$ based on heuristic evidence of the solvability of quadratic equations in finite fields. This conjecture was proven by Hasse in the 1930s, who was able to come up with an explicit error bound. Weil was also able to generalize this bound for curves over finite fields.

Theorem 4.1 (Hasse)**.** *Suppose $E/\mathbb{F}^q$ is an elliptic curve defined over a finite field. Then*

$$||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}. \tag{4.2}$$

In order to prove this theorem, we only require a generalization of the Cauchy-Schwarz inequality for abelian groups.

Lemma 4.3 (Schwarz)**.** *Suppose that A is abelian group equipped with a positive definite quadratic form d and $\psi, \phi \in A$, then*

$$|B(\psi, -\phi)| \leq 2\sqrt{d(\psi)d(\phi)} \tag{4.4}$$

Proof. Since d is a positive definite quadratic form, we have for $m, n \in \mathbb{Z}$

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

with the equality obtained from $d(a\phi) = a^2d(\phi)$ for any $a \in \mathbb{Z}$. Taking $m = -B(\psi, -\phi)$ and $n = 2d(\psi)$ yields

$$0 \leq d(\psi)(4d(\psi)d(\phi) - B(\psi, -\varphi)^2),$$

which gives the result. □

We can now proceed to the proof of the Hasse-Weil bound.

(4.1). Let ϕ denote the qth-power Frobenius map. We will first prove the easy observation that $P \in E(\mathbb{F}_q)$ iff $P \in \ker(1 - \phi)$. The first direction is clear, thus we focus on the second. From the classification of finite fields, we have that $\alpha \in \mathbb{F}_q$ iff it satisfies the polynomial $f(x) = x^q - x$, hence we obtain the other direction. Thus, we obtain the chain of equalities

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

with the second equality following from (3.29*b*). By (4.3), we obtain

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

which is the desired result. □

4.2. **The Weil Conjectures for Elliptic Curves.** From (4.1), we know that $E(\mathbb{F}_{q^n})$ is a finite group for $n \geq 1$. Thus, we are able to construct a generating function whose nth coefficient is the cardinality of $E(\mathbb{F}_{q^n})$.

Definition 4.5. The local zeta function of a projective variety $V/\mathbb{F}_q$ is the generating function

$$Z(V/\mathbb{F}_q) = \exp\left(\sum_{n=1}^{\infty} |V(\mathbb{F}_{q^n})| \frac{T^n}{n}\right) \tag{4.6}$$

Example 4.7. We will show that $Z(\mathbb{P}^N/\mathbb{F}_q;T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^NT)}$. We note that $[x_0,\cdots,x_N] \in \mathbb{P}^N(\mathbb{F}_{q^n})$ iff it has homogeneous coordinates contained $\mathbb{F}_{q^n}$. Observe that $|\mathbb{F}_{q^n}^N| = q^{n(N+1)} - 1$, thus $|\mathbb{P}(\mathbb{F}_{q^n})| = \frac{q^{n(N+1)}-1}{q^n-1} = \sum_{i=0}^N q^{ni}$. Thus,

$$\log Z(\mathbb{P}^N/\mathbb{F}_q;T) = \sum_{i=1}^{\infty}\left(\sum_{i=0}^N q^{ni}\right)\frac{T^n}{n} = \sum_{i=0}^N -\log(1-q^iT),$$

which yields

$$Z(\mathbb{P}^N/\mathbb{F}_q;T) = \frac{1}{(1-T)\cdots(1-q^NT)}.$$

Remarkably, Andre Weil was able to develop a series of ambitious conjectures on the algebraic and analytic properties of the zeta function. Specifically, he conjectured that $Z(V/\mathbb{F}_q;T)$ was rational, satisfied a functional equation, and had roots which lied on the critical line, thus giving an analog of the Riemann hypothesis for finite fields. The rationality and functional equation conjectures were resolved by Dwork (60) and Grothendieck (65) respectively. The more difficult portion of the conjectures: the analog of the Riemann Hypothesis was resolved by Deligne (74) by employing powerful techniques from algebraic geometry and $l-$adic cohomology.

Luckily in the case of elliptic curves, we only require the usage of the $l-$adic representation and basic properties of $T_\ell(E)$. The proof of this special case of the Weil conjectures will give us motivation in defining the global zeta function.

Theorem 4.8. *Suppose $E/\mathbb{F}_q$ is an elliptic curve. Then there exists an $a \in \mathbb{Z}$ such that*

(a) Rationality

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

Moreover, $(1-aT+qT^2) = (1-\alpha T)(1-\beta T)$ with $|\alpha| = |\beta| = \sqrt{q}$ and α,β complex conjugates.

(b) The zeta function exhibits a functional equation

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

(c) Riemann Hypothesis
We have $1-at+qT^2 = (1-\alpha T)(1-\beta T)$ with $|\alpha| = |\beta| = \sqrt{q}$.

We require only a simple lemma involving the qth-power Frobenius map

Lemma 4.9. *Let $E/\mathbb{F}_q$ be an elliptic curve, ϕ be the $qth-$power Frobenius map, and $a = q+1-|E(\mathbb{F}_q)|$. Suppose $\alpha,\beta \in \mathbb{C}$ are roots of $T^2-aT+qT^2$. Then α and β are complex conjugates satisfying $|\alpha| = |\beta| = \sqrt{q}$. In addition*

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

Proof. We note from (3.29*b*) and (3.54) that $|E(\mathbb{F}_q)| = \deg(1-\phi)$ and $\det(\phi_\ell) = \deg(\phi) = q$ and $\mathrm{tr}(\phi_\ell) = 1+\deg(\phi)-\deg(1-\phi) = 1+q-|E(\mathbb{F}_q)| = a$. Thus the characteristic polynomial of ϕ_ℓ is $P(T) = T^2 - at + q$.

We have the factorization $P(T) = (T-\alpha)(T-\beta)$ with $\alpha, \beta \in \mathbb{C}$. We observe for $\frac{m}{n} \in \mathbb{Q}$ and that $\det(\gamma A) = \gamma^2 \det(A)$ yields the equation

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

Since the polynomial $T^2 - aT + q \in \mathbb{Z}[T]$ is continuous, we have it is non-negative for all $T \in \mathbb{R}$. Thus, it either has complex roots (which implies they are conjugate) or a double root. Regardless, we have

$$\alpha\beta = \deg(\phi) = q,$$

which yields $|\alpha| = |\beta| = \sqrt{q}$. One may repeat for each integer $n \geq 1$, the q^nth-power Frobenius endomorphism satisfies $|E(\mathbb{F}_{q^n})| = \deg(1 - \phi^n)$. Putting the matrix of ϕ_ℓ into Jordan normal form with α, β on the diagonal, we find

$$\phi_\ell^n = \begin{pmatrix} \alpha & 1 \\ 0 & \beta \end{pmatrix}^n = \begin{pmatrix} \alpha^n & \gamma \\ 0 & \beta^n \end{pmatrix}$$

with γ a linear combination of α and 1. This yields the characteristic equation $(T - \alpha^n)(T - \beta^n)$ for ϕ_ℓ^n. We obtain $|E(\mathbb{F}_{q^n})| = \deg(1 - \phi^n) = \det(1 - \phi_\ell^n) = 1 - \alpha^n - \beta^n + q^n$ with the second equality obtained from (3.54).

□

(4.8). (a) Observe by taking the logarithm on both sides, we obtain

$$\begin{aligned} \log Z(E/\mathbb{F}_q; T) &= \sum_{n=1}^{\infty} \frac{|E(\mathbb{F}_{q^n})|T^n}{n} \\ &= \sum_{n=1}^{\infty} \frac{(1 - \alpha^n - \beta^n + q^n)T^n}{n} \\ &= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT) \end{aligned}$$

with the second equality obtained from (4.9). The final equality yields the rationality of $Z(E/\mathbb{F}_q; T)$ by taking the exponential on both sides. The factorization of $(1 - at + qT^2)$ was shown by (4.9).
(b) We observe that we have

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

(c) This was already proven in (4.9). □

Remark 4.10. The third part of the Weil conjectures is known as the Riemann hypothesis for finite fields. To see its connection with the infamous conjecture involving the Riemann zeta function, we substitute $T = q^{-s}$, which yields

$$\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q; q^{-s}) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}.$$

Note that (4.8*b*) yields $\zeta_{E/\mathbb{F}_q}(1-s) = \zeta_{E/\mathbb{F}_q}(s)$ which is the ordinary functional equation of the normalized Riemann zeta function. Moreover, note that if $\zeta_{E/\mathbb{F}_q}(s) = 0$, then $|q^s| = \sqrt{q}$, which implies $\mathrm{Re}(s) = \frac{1}{2}$.

We just need one more concept before we proceed with the global properties of elliptic curves.

Definition 4.11. Suppose $E/\mathbb{Q}$ is an elliptic curve with Weierstrass equation

$$E : y^2 = x^3 + Ax + B,\ A, B \in \mathbb{Q}.$$

With suitable change of variables $x \mapsto \frac{x}{c^2}$ and $y \mapsto \frac{y}{c^3}$ with $c \in \mathbb{Q}$, we can assume that $a, b \in \mathbb{Z}$ and $|\Delta|$ is minimal with respect to the set of Weierstrass equations of E. A Weierstrass equation E is a minimal Weierstrass equation if satisfies the two aforementioned properties.

Since a minimal Weierstrass equation E has integer coefficients, we can obtain a reduced Weierstrass equation $\tilde{E}$ whose coefficients are reduced modulo p,

$$\tilde{E} : y^2 = x^3 + \bar{A}x + \bar{B},\ \bar{A}, \bar{B} \in \mathbb{F}_p.$$

We note that the reduced Weierstrass equation may be singular, which leads to our final definition.

Definition 4.12. Suppose $E/\mathbb{Q}$ is an elliptic curve with

$$E : y^2 = x^3 + Ax + B,\ A, B \in \mathbb{Z}$$

is a minimal Weierstrass equation and p a prime.

(a) $E/\mathbb{Q}$ has a good reduction if $\tilde{E}$ is non-singular. Then the projective variety defined by $\tilde{E}$ is an elliptic curve.
(b) $E/\mathbb{Q}$ has semistable (multiplicative) reduction if $\tilde{E}$ has a node.
(c) $E/\mathbb{Q}$ has additive reduction if $\tilde{E}$. has a cusp.

Example 4.13. Suppose $p \geq 5$ is a prime. Then the elliptic curve

$$E : y^2 = x^3 + px^2 + 1$$

has good reduction for any p.

Remark 4.14. We use the term semistable reduction since we can consider $E/\mathbb{Q}$ over some number field K where we can change the minimal equation of E to remove the singular point.

Definition 4.15. An elliptic curve $E/\mathbb{Q}$ is semistable if it does not have additive reduction over any prime p.

5. L Dirichlet Series and modular Forms

We briefly cover the theory of modular forms and L functions. We'll start by defining congruence subgroups and modular forms, which are holomorphic functions with certain transformation properties. This section will also include discussion of Hasse's theorem which states that the $L-$Dirichlet series associated with a cusp form has an analytic continuation onto the entire complex plane.

Throughout this section, we will have $\mathbb{H}$ be the upper-half plane and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ be the two generators of $SL_2(\mathbb{Z})$.

Definition 5.1. A principal congruence subgroup $\Gamma(N)$ of $SL_2(\mathbb{Z})$ consists of elements of the form

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) | \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\}.$$

A subgroup $\Gamma \subset SL_2(\mathbb{Z})$ is called a congruence subgroup if it contains a principal congruence subgroup $\Gamma(N)$. The smallest integer N, where $\Gamma \supset \Gamma(N)$ is called the level of Γ.

We will specify two important congruence subgroups of Γ for convenience.

Definition 5.2. The Hecke congruence subgroup of level N is

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma |\ c \equiv 0 \pmod{N}\}.$$

We also define

$$\Gamma_1(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} |\ a, d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N}\}.$$

Recall that have the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}. \tag{5.3}$$

Definition 5.4. A k-weight weak modular form of Γ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that

$$f(\gamma\tau) = (c\tau + d)^k f(\tau)$$

for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Example 5.5. The Eisenstein series $G_k(\tau)$ is a weak-modular form of weight k for $SL_2(\mathbb{Z})$ if $k \geq 3$. Recall that $G_k(\tau)$ is defined as

$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2/(0,0)} \frac{1}{(m + n\tau)^k}. \tag{5.6}$$

Since we restrict G_k on $\mathbb{H}$, the above series converges absolutely to a holomorphic function, thus we simply need to verify the transformation property for the two generators of $SL_2(\mathbb{Z})$. Note that

$$G_k(S\tau) = G_k(\frac{-1}{\tau}) = \sum_{(m,n)\in\mathbb{Z}^2/(0,0)} \frac{1}{(m - \frac{n}{\tau})^k} = \sum_{(m,n)\in\mathbb{Z}^2/(0,0)} \frac{\tau^k}{(m\tau - n)^k} = \tau^k G(\tau),$$

$$G_k(T\tau) = G_k(\tau + 1) = \sum_{(m,n)\in\mathbb{Z}^2/(0,0)} \frac{1}{(m + (n+1)\tau)^k} = G(\tau).$$

Recall that we have the extended upper half plane $\mathbb{H}* = \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$. The points $\mathbb{Q} \cup \{i\infty\}$ are called the cusps of the extended upper half-plane. Since Γ is a congruence subgroup, there exists a matrix $\alpha = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$ for some $N \in \mathbb{Z}$. If f is a $k-$weight weak modular form, then $f(\alpha\tau) = f(\tau + N) = f(\tau)$. Thus f is periodic for some integer N. This implies that we have a Fourier series

$$f(\tau) = f^*(q^{\frac{1}{N}}) = \sum_{n=n_0}^{\infty} a_n q^{\frac{n}{N}} \tag{5.7}$$

with $q = e^{2\pi i\tau}$. Since we can view $q : \mathbb{H} \to \mathbb{D}$, we have that $f^* : \mathbb{D} \to \mathbb{H}$. Thus, we can consider whether $f(\tau)$ is holomorphic at the cusp $i\infty$.

We note that for any $\gamma \in \Gamma$, that $f(\gamma\tau)$ is invariant under α since

$$f(\alpha(\gamma\tau)) = (c\tau + d)^k f(\alpha\tau) = (c\tau + d)^k f(\tau + N) = f(\gamma\tau),$$

thus $f(\gamma\tau)$ also has Fourier expansion. Hence, we can consider when f is holomorphic at a cusp $r \in \mathbb{Q}$.

Definition 5.8. Suppose $f : \mathbb{H} \to \mathbb{C}$ is a modular form for some congruence subgroup Γ. We say f is holomorphic at $i\infty$ if f^* is holomorphic at 0. If r is a cusp not equal to $i\infty$, we choose $\gamma \in \Gamma$ such that $\lim_{\mathrm{Im}\tau\to\infty} \gamma(\tau) = r$. We will say f is holomorphic at r if $f \circ \gamma$ is holomorphic at ∞.

Definition 5.9. A modular form of a congruence subgroup Γ is a weak modular form f which is holomorphic at the cusps. In addition, if the Fourier series expansion has coefficients with only positive index, we say f is a k-weight cusp form. We will let $M_k(\Gamma)$ and $S_k(\Gamma)$ be the set of $k-$weight modular and cusp forms respectively of Γ.

We now introduce the concept of a Dirichlet series.

Definition 5.10. Suppose $\{a_n\}$ is a sequence of complex numbers. A Dirichlet series associated with a sequence $\{a_n\}$ is the series

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \tag{5.11}$$

A Dirichlet series defines a holomorphic function on the right half-plane $\mathrm{Re}(s) > 1 + \frac{\sigma}{2}$ provided the a_n satisfy the growth condition $|a_n| = O(n^\sigma)$.

Example 5.12. The most famous example of a Dirichlet series is the Riemann zeta-function

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

We can construct a Dirchlet series of a modular form by taking the coefficients of Fourier series expansion.

Definition 5.13. Suppose that $f \in M_k(\Gamma)$ with Fourier series expansion. The associated Dirichlet series, denoted by $L_f(s)$, is

$$L_f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{5.14}$$

where the a_n are the Fourier coefficients of f.

Remarkably if $f \in S_k(\Gamma)$, its associated Dirichlet series $L_f(s)$ has an analytic continuation onto $\mathbb{C}$.

Definition 5.15. Let $\mathbb{R}_+^*$ be the group of positive real numbers under multplication and $f : \mathbb{R}_+^* \to \mathbb{C}$ be a continuous function. The Mellin transform, denoted by $L(f, s)$, is the improper integer

$$L(f, s) = \int_0^\infty (f(y) - f(\infty))\, y^{s-1} dy, \tag{5.16}$$

provided $f(\infty) = \lim_{y\to\infty} f(y)$ and the integral exists.

The Mellin transform will allow us to construct analytic continuations of k-weight cusp forms of $\Gamma_1(N)$.

Theorem 5.17 (Hecke)**.** *Suppose $f \in S_k(\Gamma_1(N))$, then its Mellin transform $\Lambda_N(s)$ extends to an entire function which satisfies the functional equation*

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

Consequently $L_f(s)$ has an analytic continuation on $\mathbb{C}$.

Proof. See [2], Chapter 5, Theorem 5.10.2. □

We now define the global zeta function of an elliptic curve, which can be viewed as an Eulerian product of numerators of the local zeta functions. We will let $\tilde{E}_p$ denote the projective variety associated with the reduced Weierstrass equation modulo p where p denotes a prime number.

Definition 5.18. The L-function of an elliptic curve $E/\mathbb{Q}$ is the Eulerian product

$$L_E(s) = \prod_p \left(1 - a_p p^{-s} + \chi(p) p p^{-2s}\right)^{-1} \tag{5.19}$$

with $a_p = p + 1 - |\tilde{E}(\mathbb{F}_p)|$ and $\chi(p) = \begin{cases} 0 & E \text{ has bad reduction mod } p \\ 1 & E \text{ has good reduction mod } p \end{cases}$.

Remark 5.20. We can show in the case where $E/\mathbb{Q}$ has bad reduction that $a_p \in \{-1, 0, 1\}$ by considering if the Weierstrass equation E has multiplicative or additive reduction.

We can construct a holomorphic function $f_E(\tau)$ from the L-function of an elliptic curve.

Definition 5.21. Suppose $E/\mathbb{Q}$ is an elliptic curve with L-function

$$L_E(s) = \prod_p \left(1 - a_p p^{-s} + \chi(p) p p^{-2s}\right)^{-1} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

The holomorphic function associated with $L_E(s)$, denoted by $f_E(\tau) : \mathbb{H} \to \mathbb{C}$ is defined by

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n q^n, \ q = e^{2\pi i \tau}. \tag{5.22}$$

We just need two more definitions to give a concrete statement of the modularity theorem.

Definition 5.23. Suppose $E/\mathbb{Q}$ is an elliptic curve. A global minimial Weierstrass equation is an integral Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

whose discriminant $\Delta_{\min}$ divides the discriminant of any integral Weierstrass equation for E.

Definition 5.24. Suppose $E/\mathbb{Q}$ is an elliptic curve with minimal discriminant $\Delta_{\min}(E)$. The conductor, denoted by N_E, is the product of prime divisors of $\Delta_{\min}(E)$.

6. Birch and Swinnerton-Dyer Conjecture and the Modularity Theorem

The proof of the modularity theorem was one of the crowning achievements of number theory in the past century. It is also deeply connected with important conjectures connecting the algebraic and analytic properties of elliptic curves, in particular the Birch and Swinnerton-Dyer conjecture (BSD). This short section will introduce the modularity theorem and one of its consequences: the Hasse-Weil conjecture. We'll then conclude with the BSD conjecture.

Definition 6.1. An elliptic curve $E/\mathbb{Q}$ is modular if $f_E(\tau)$ is a modular form.

Remark 6.2. One can show via analyzing the multiplicative properties of the coefficients a_p that if $f_E(\tau)$ is a modular then $f_E \in S_2(\Gamma_0(N_E))$.

Theorem 6.3 (Modularity)**.** *Every $E/\mathbb{Q}$ elliptic curve is modular.*

Remark 6.4. Remarkably, one needs to only prove the semistable case to show that Fermat's last theorem is true. The proof of this special case was due to Wiles and Taylor [7]. The proof of the entire modularity theorem was done by Breuil, Conrad, Diamond, and Taylor [1] by improving the techniques employed for the semistable case.

By (5.17) and (6.3), we have that the $L-$function of an elliptic curve $E/\mathbb{Q}$ has an analytic continuation onto the entire complex plane. This will ensure that the statement of the Birch and Swinnerton-Dyer conjecture (BSD) conjecture is well-defined.

Corollary 6.5. *Suppose $L_E(s)$ is the $L-$function of an elliptic curve $E/\mathbb{Q}$. Then $L_E(s)$ has a holomorphic analytic continuation on $\mathbb{C}$ whose completed $L-$function*

$$\tilde{L}_E(s) = N_E^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L_E(s)$$

satisfies the functional equation

$$\tilde{L}_E(s) = w_E\tilde{L}_E(2-s),\ w_E = \pm 1.$$

By (6.5) it makes sense to consider the order of vanishing of $L_E(s)$ at $s = 1$. This leads to the statement of BSD conjecture. We present the weaker but still important version for simplicity.

Conjecture 6.6. *Suppose $E/\mathbb{Q}$ is an elliptic curve of rank r. Then r is equal to the order of vanishing of $L_E(s)$ at $s = 1$.*

This important conjecture is well understood for elliptic curves of rank zero and one due to the results of Gross-Zagier and Kolyvagin.

Theorem 6.7 (Gross, Zagier)**.** *If E is a modular elliptic curve has zero of order one at $s = 1$. Then $E(\mathbb{Q})$ has rank at least one.*

Theorem 6.8 (Kolyvagin)**.** *If $L_E(s)$ does not vanish at $s = 1$, then E has rank zero. In addition if $L_E(s)$ has a zero of order at $s = 1$, then E has rank one.*

For elliptic curves of higher rank, we have little knowledge in approaching the Birch and Swinnerton-Dyer conjecture. In fact, we still have little understanding

on even the number of elliptic curves of high rank.

We conclude this paper with a groundbreaking result due to Bhargava and Shankar who were able to bound the average rank of elliptic curves defined over the rationals.

Theorem 6.9 (Bhargava, Shankar)**.** *A positive proportion of elliptic curves satisfy the BSD conjecture.*

Acknowledgments

I am deeply indebted to my mentor Wei Yao for introducing me to this beautiful subject and for her constant advice and input in this project. Without her support and patience, this project would've been impossible. I am also deeply indebted to Professor May's ability in organizing the wonderful Chicago REU in these trying times.

References

[1] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over q: Wild 3-adic exercises. *Journal of the American Mathematical Society*, pages 843–939, 2001.
[2] Fred Diamond and Jerry Michael Shurman. *A First Course in Modular Forms*, volume 228. Springer, 2005.
[3] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.
[4] James S Milne. *Elliptic Curves*. World Scientific, 2006.
[5] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.
[6] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer, 2009.
[7] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain hecke algebras. *Annals of Mathematics*, pages 553–572, 1995.