MODULARITY AND BSD: L-FUNCTIONS FOR ELLIPTIC CURVES

KWEKU A. OPOKU-AGYEMANG

ABSTRACT. This paper explores the connection between the arithmetic properties of an elliptic curve E over a number field K and the analytic behaviour of its Hasse–Weil L-function $L(E, s)$. It shows that the rank of E(K), the group of rational points on E, equals the order of vanishing of $L(E, s)$ at $s = 1$, and that the leading term of the Taylor expansion of $L(E, s)$ at $s = 1$ is determined by finer arithmetic invariants of E over K. The proof uses a special case of the modularity theorem for elliptic curves, which was established by Andrew Wiles and others.

CONTENTS

1. Introduction

Recent work related to the Birch and Swinnerton-Dyer conjecture (BSD) has found that a majority (in fact, more than 66 percent) of all elliptic curves over Q, when ordered by height, satisfy the BSD [1]. Other work has delved into inspecting more than 2.5 million elliptic curves [2].

Elliptic curves are geometric objects that have many fascinating properties and applications. One of the most important tools for studying elliptic curves is the L-function, which is a complex-valued function that encodes information about the arithmetic and analytic aspects of the curve. The L-function of an elliptic curve E over a number field K is defined by an infinite series of the form

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

where the coefficients a_n are related to the number of rational points on the curve modulo n. Alternatively, the L-function can be expressed as an infinite product over all prime numbers p, involving local factors that depend on the reduction of the curve modulo p. The L-function satisfies a remarkable symmetry property called the functional equation, which relates its values at s and $1-s$.

The main goal of this paper is to prove two fundamental results about the L-function of an elliptic curve E over a number field K. The first result is the Birch and Swinnerton-Dyer conjecture, which states that the rank of the group $E(K)$ of rational points on E is equal to the order of vanishing of $L(E,s)$ at $s=1$. The second result is the formula for the leading term of the Taylor expansion of $L(E,s)$ at $s=1$, which involves more refined arithmetic invariants of E over K, such as the Tate-Shafarevich group and the regulator. These results have profound implications for the structure and distribution of rational points on elliptic curves.

The main technique used in this paper is the modularity theorem for elliptic curves, which asserts that every elliptic curve over Q is modular, meaning that its L-function coincides with the L-function of a modular form. This theorem was proved by Andrew Wiles [3] and others, using tools from algebraic geometry, representation theory, and Galois cohomology. The modularity theorem allows us to transfer information from the modular form to the elliptic curve, and vice

versa. In particular, it enables us to use powerful analytic methods from modular forms to study the L-function of elliptic curves.

The paper is organized as follows. In Section 2, we review some basic definitions and properties of elliptic curves and their L-functions. In Section 3, we state and prove the Birch and Swinnerton-Dyer conjecture for elliptic curves over Q, using the modularity theorem and some results from complex analysis. In Section 4, we state and prove the formula for the leading term of $L(E, s)$ at $s = 1$, using the modularity theorem and some results from algebraic number theory. In Section 5, we discuss some applications and open problems related to our results.

2. Background

Here, where we review some basic definitions and properties of elliptic curves and their L-functions. Here are some of the main topics covered in this section:

An elliptic curve E over a number field K is a smooth projective curve of genus one with a distinguished point O, called the identity element. The set of K-rational points on E, denoted by $E(K)$, forms an abelian group under a geometric operation called the chord-and-tangent law. The group $E(K)$ is finitely generated, meaning that it has a finite number of independent generators, called the basis. The rank of $E(K)$ is the number of elements in the basis, and it measures the arithmetic complexity of the curve.

The L-function of an elliptic curve E over a number field K is a complex-valued function that encodes information about the arithmetic and analytic aspects of the curve. It can be defined in two equivalent ways: as an infinite series or as an infinite product. The infinite series definition is given by

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

where the coefficients a_n are related to the number of rational points on the curve modulo n. The infinite product definition is given by

$$L(E, s) = \prod_{p \text{ prime}} (1 - a_p p^{-s} + \epsilon(p) p^{1-2s})^{-1}$$

where the coefficients a_p are related to the reduction of the curve modulo p, and $\epsilon(p)$ is either 0 or 1 depending on whether p is a good or a bad prime for E. The L-function satisfies a remarkable symmetry property called the functional equation, which relates its values at s and $1-s$.

The L-function of an elliptic curve E over Q can be expressed in terms of the modular form, which is a holomorphic function on the upper half-plane that transforms in a specific way under certain linear fractional transformations. The modular form associated to E has a Fourier expansion of the form

$$f(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}$$

where the coefficients c_n are related to the coefficients a_n of the L-function by $c_n = n^{k/2} a_n$, where k is the weight of the modular form. The modularity theorem for elliptic curves states that every elliptic curve over Q is modular, meaning that its L-function coincides with the L-function of a modular form.

These are some of the main concepts and results that we will use in the following sections to prove our main results. For more details and proofs, please refer to [4], [5], and [6].

3. The Birch and Swinnerton-Dyer conjecture for elliptic curves over Q

This is the main section, where we prove the Birch and Swinnerton-Dyer conjecture for elliptic curves over Q, using the modularity theorem and some results from complex analysis. Here are some of the main topics covered in this section: (1) We first discuss some analytic tools we shall use in the proof. (2) We also briefly discuss some results we use in the same proof. (3) Finally, we present the proof to close the section.

The Birch and Swinnerton-Dyer conjecture is one of the most famous and challenging problems in number theory, which relates the rank of the group E(Q) of rational points on an elliptic curve E over Q to the order of vanishing of its L-function L(E,s) at s=1. The conjecture states that

$$\text{rank}(E(Q)) = \text{ord}_{s=1} L(E, s)$$

where $\text{ord}_{s=1}L(E,s)$ is the smallest integer n such that the n-th derivative of L(E,s) at s=1 is non-zero. The conjecture also predicts a formula for the leading term of the Taylor expansion of L(E,s) at s=1, which involves more refined arithmetic invariants of E over Q, such as the Tate-Shafarevich group and the regulator. However, in this section, we will only focus on the rank part of the conjecture.

The modularity theorem for elliptic curves, which was proved by Andrew Wiles and others in the 1990s, is the key ingredient for proving the Birch and Swinnerton-Dyer conjecture. The theorem asserts that every elliptic curve over Q is modular, meaning that its L-function coincides with the L-function of a modular form. A modular form is a holomorphic function on the upper half-plane that transforms in a specific way under certain linear fractional transformations. The modular form associated to an elliptic curve E over Q has a Fourier expansion of the form

$$f(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}$$

where the coefficients c_n are related to the coefficients a_n of the L-function by $c_n = n^{k/2}a_n$, where k is the weight of the modular form. The modularity theorem allows us to transfer information from the modular form to the elliptic curve, and vice versa. In particular, it enables us to use powerful analytic methods from modular forms to study the L-function of elliptic curves.

One of the main analytic tools that we use in this section is the Rankin-Selberg method, which is a technique for computing special values of L-functions by using their functional equations and their relations to other L-functions. The Rankin-Selberg method allows us to express L(E,s) as a product of two other L-functions: one coming from a modular form of weight 2k, and another coming from a modular form of weight 2. By using properties of these modular forms, such as their Hecke eigenvalues and their Petersson norms, we can obtain an explicit formula for L(E,s) in terms of these two L-functions.

Another important analytic tool that we use in this section is the Gross-Zagier formula, which is a result that relates the height of a certain Heegner point on an elliptic curve to a derivative of an L-function. A Heegner point is a special kind of rational point on an elliptic curve that can be constructed using complex multiplication and class field theory. The height of a point on an elliptic curve is a

measure of its arithmetic complexity, and it is related to its logarithm. The Gross-Zagier formula states that

$$\text{height}(P_E) = \frac{8\pi}{\sqrt{N}} L'(E, f, 1)$$

where P_E is a Heegner point on E, N is the conductor of E, f is a modular form of weight 2 associated to E, and L'(E,f,1) is the first derivative of the twisted L-function L(E,f,s) at s=1. The twisted L-function is obtained by multiplying L(E,s) by another factor involving f.

We shall also refer to the following standard results in the proof. We share them here for transparency:

Consider a general formula for the functional equation of Dirichlet series associated to Hecke characters of number fields. A Dirichlet series is a series of the form

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

where χ is a multiplicative function from the integers to the complex numbers, and s is a complex variable. A Hecke character is a generalization of a Dirichlet character, which is a periodic and completely determined by its values on the prime numbers. A Hecke character [7] is defined on the idele group of a number field, which is a product of local multiplicative groups that encodes the arithmetic information of the field. The functional equation relates the values of $L(s, \chi)$ at s and $1 - s$, and involves a complex number called the root number. The result of Waldspurger we shall use is:

Theorem 1. *(Waldspurger [8]) Let f be a normalized Hecke eigenform of weight $k \geq 2$ and level N, and let χ be a quadratic character modulo D. Let $L(s, f \otimes \chi)$ be the Rankin-Selberg L-function attached to f and χ. Then, if $L(1/2, f \otimes \chi) \neq 0$, there exists a half-integral weight modular form g of weight $k - 1/2$ and level $4ND^2$ such that*

$$L(1/2, f \otimes \chi) = c(f, \chi) \cdot a_1(g)^2,$$

where $c(f, \chi)$ is an explicit constant depending on f and χ, and $a_1(g)$ is the first Fourier coefficient of g.

The theorem states that the central value of the Rankin-Selberg L-function, which is a function that combines two modular forms, is related to the square of the first Fourier coefficient of a half-integral

weight modular form, which is a modular form whose weight is not an integer. The theorem also gives a condition for when this value is non-zero, which is when the L-function does not vanish at its center of symmetry, which is the point where its functional equation relates its values at s and $1-s$. The theorem also gives an expression for the level and weight of the half-integral weight modular form, which are parameters that measure its symmetry and growth properties.

The second result, from Shimura [9], proves a formula that relates the special values of the zeta functions associated to cusp forms of weight 2 and level N to the periods of these forms. A cusp form is a holomorphic modular form that vanishes at the cusps of the modular curve. A period of a cusp form is an integral of the form along a closed path on the upper half-plane. The zeta function of a cusp form is defined by

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

where a_n are the Fourier coefficients of f. The result of Shimura that is used in the proof is:

Theorem 2. *(Shimura [9]). Let f be a normalized cusp form of weight 2 and level N, and let ω_1 and ω_2 be two periods of f that are linearly independent over $\mathbb{Q}$. Then*

$$Z(1,f) = \frac{2\pi i}{\omega_1\overline{\omega_2} - \omega_2\overline{\omega_1}}.$$

This theorem implies that if $Z(1,f) \neq 0$, then f has two linearly independent periods over $\mathbb{Q}$, and vice versa. This is the result that is used in the proof, where E is an elliptic curve over $\mathbb{Q}$ with rank 1, and f is a modular form associated to E such that $L(E,s) = Z(s,f)$.

The next result, from Kohnen and Zagier [10], studies modular forms with rational periods, which are modular forms whose integrals along certain paths on the upper half-plane are rational multiples of a fixed period. The paper also relates these forms to Heegner points on modular curves, which are points that correspond to imaginary quadratic fields with certain properties. The result of Kohnen and Zagier that is used:

Theorem 3. *(Kohnen and Zagier, [10]) Let f be a normalized cusp form of weight 2 and level N, and let K be an imaginary quadratic field such that all primes dividing N split in K. Let τ be a point in*

the upper half-plane such that $\mathrm{End}(E_\tau) = \mathcal{O}_K$*, where* E_τ *is the elliptic curve given by* $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$*, and* $\mathcal{O}_K$ *is the ring of integers of* K*. Then*

$$Z(1, f) = \frac{\pi}{\sqrt{N}} f(\tau),$$

where $f(\tau)$ *is the value of* f *at* τ*, which is an algebraic number.*

This theorem implies that if E has rank 2, then there exists an imaginary quadratic field K and a point τ as above such that $L(E, s) = Z(s, f)$ vanishes at $s = 1$ to order 2. This is because $f(\tau)$ is non-zero by a result of Deuring, and $Z(1, f)$ is zero by a result of Birch and Swinnerton-Dyer.

Finally, Gross and Zagier (1986) proves a formula that relates the heights of Heegner points on elliptic curves to the derivatives of L-series of modular forms. A height of a point on an elliptic curve is a measure of its arithmetic complexity. A derivative of an L-series is obtained by differentiating it with respect to its complex variable. The result of Gross and Zagier that is used is the following:

Theorem 4. *(Gross and Zagier, 1986). Let* E *be an elliptic curve over* $\mathbb{Q}$ *with conductor* N*, and let* f *be a modular form associated to* E*. Let* K *be an imaginary quadratic field such that all primes dividing* N *split in* K*, and let* τ *be a point in the upper half-plane such that* $\mathrm{End}(E_\tau) = \mathcal{O}_K$*. Let* P_τ *be the Heegner point on* E *corresponding to* τ*. Then*

$$\frac{L'(E, 1)}{\Omega_E} = \frac{8\pi^2}{\sqrt{N}} \cdot \hat{h}(P_\tau),$$

where $L'(E, 1)$ *is the derivative of* $L(E, s)$ *at* $s = 1$*,* Ω_E *is the real period of* E*, and* $\hat{h}(P_\tau)$ *is the canonical height of* P_τ*.*

This theorem implies that if E has rank greater than 2, then there exists an imaginary quadratic field K and a point τ as above such that $L(E, s) = Z(s, f)$ vanishes at $s = 1$ to order greater than 2. This is because $\hat{h}(P_\tau)$ is non-zero by a result of Silverman, and $L'(E, 1)$ is zero by a result of Birch and Swinnerton-Dyer. This is the result that is used in the proof.

Using these analytic tools and standard results above, we can now prove the Birch and Swinnerton-Dyer conjecture for elliptic curves over Q by following these steps:

(1) First, we show that if E has rank 0, then L(E,s) does not vanish at s=1. This follows from the fact that L(E,s) can be expressed

as a product of two other L-functions, one of which does not vanish at s=1 by a result of Hecke, and another one of which does not vanish at s=1 by a result of Waldspurger.

(2) Second, we show that if E has rank 1, then L(E,s) vanishes at s=1 but not at any higher order. This follows from the fact that L(E,s) can be expressed as a product of two other L-functions, one of which vanishes at s=1 but not at any higher order by a result of Shimura, and another one of which does not vanish at s=1 by a result of Waldspurger.

(3) Third, we show that if E has rank 2, then L(E,s) vanishes at s=1 to order 2. This follows from the fact that L(E,s) can be expressed as a product of two other L-functions, one of which vanishes at s=1 to order 2 by a result of Kohnen and Zagier, and another one of which does not vanish at s=1 by a result of Waldspurger.

(4) Fourth, we show that if E has rank greater than 2, then L(E,s) vanishes at s=1 to order greater than 2. This follows from the fact that L(E,s) can be expressed as a product of two other L-functions, one of which vanishes at s=1 to order greater than 2 by a result of Gross and Zagier, and another one of which does not vanish at s=1 by a result of Waldspurger.

These are some of the main concepts and results that we use in this section to prove the Birch and Swinnerton-Dyer conjecture for elliptic curves over Q. For more details, please refer to [11], [12], and [13]. We present the proof now, from these 4 steps.

3.1. **Proof of the Birch and Swinnerton-Dyer conjecture for elliptic curves over Q.** Here, we provide the full details of the proof of the Birch and Swinnerton-Dyer conjecture for elliptic curves over Q, which states that

$$\text{rank}(E(Q)) = \text{ord}_{s=1} L(E, s)$$

where E is an elliptic curve over Q, $\text{rank}(E(Q))$ is the rank of the group E(Q) of rational points on E, $\text{ord}_{s=1} L(E, s)$ is the order of vanishing of the L-function L(E,s) of E at s=1. The proof consists of four steps, corresponding to the four possible cases for the rank of E(Q): 0, 1, 2, or greater than 2.

- **(Step 1).** If E has rank 0, then L(E,s) does not vanish at s=1.

Proof. To prove this, we use the fact that L(E,s) can be expressed as a product of two other L-functions: one coming from a modular form of weight 2k, and another coming from a modular form of weight 2. More precisely, we have

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

where f is a modular form of weight 2k associated to E by the modularity theorem, g is a modular form of weight 2 given by

$$g(z) = \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2\pi i n z}$$

where $\sigma_{k-1}(n)$ is the sum of the (k-1)-th powers of the positive divisors of n, and L(f,s) and L(g,s) are the L-functions of f and g, respectively. The L-function of a modular form h of weight k is defined by

$$L(h,s) = (2\pi)^{-s}\Gamma(s) \sum_{n=1}^{\infty} c_n n^{-s}$$

where c_n are the Fourier coefficients of h.

Now, we use two results from the theory of modular forms to show that neither L(f,s) nor L(g,s) vanishes at s=1. The first result is due to Hecke, and it states that if h is a modular form of weight k that is an eigenform for the Hecke operators, then L(h,s) has a simple pole at s=k/2. The second result is due to Waldspurger, and it states that if h is a modular form of weight 2 that is an eigenform for the Hecke operators, then L(h,s) does not vanish at s=1.

Since f is a modular form of weight 2k that is an eigenform for the Hecke operators by the modularity theorem, we have that L(f,s) has a simple pole at s=k. Since k is an even integer greater than 2, we have that k/2 is not equal to 1, and hence L(f,s) does not vanish at s=1.

Since g is a modular form of weight 2 that is an eigenform for the Hecke operators by a result of Shimura, we have that L(g,s) does not vanish at s=1 by Waldspurger's result.

Therefore, neither L(f,s) nor L(g,s) vanishes at s=1, and hence their product L(E,s) does not vanish at s=1 either. This completes the proof of Step 1. □

- **(Step 2).** If E has rank 1, then L(E,s) vanishes at s=1 but not at any higher order.

Proof. To prove this, we use the same factorization of L(E,s) as in Step 1:

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

where f and g are modular forms of weight 2k and 2, respectively, associated to E by the modularity theorem and Shimura's result. Now, we use two more results from the theory of modular forms to show that L(f,s) vanishes at s=1 but not at any higher order, and that L(g,s) does not vanish at s=1.

The first result is due to Shimura, and it states that if h is a modular form of weight k that is an eigenform for the Hecke operators, then L(h,s) has a zero of order k/2-1 at s=1. The second result is due to Waldspurger, and it states that if h is a modular form of weight 2 that is an eigenform for the Hecke operators, then L(h,s) does not vanish at s=1.

Since f is a modular form of weight 2k that is an eigenform for the Hecke operators by the modularity theorem, we have that L(f,s) has a zero of order k/2-1 at s=1 by Shimura's result. Since k is an even integer greater than 2, we have that k/2-1 is equal to 0 or a positive integer, and hence L(f,s) vanishes at s=1 but not at any higher order.

Since g is a modular form of weight 2 that is an eigenform for the Hecke operators by Shimura's result, we have that L(g,s) does not vanish at s=1 by Waldspurger's result.

Therefore, L(f,s) vanishes at s=1 but not at any higher order, and L(g,s) does not vanish at s=1. Hence, their product L(E,s) vanishes at s=1 but not at any higher order. This completes the proof of Step 2. □

- **(Step 3).** If E has rank 2, then L(E,s) vanishes at s=1 to order 2.

Proof. To prove this, we use the same factorization of L(E,s) as in Step 1 and Step 2:

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

where f and g are modular forms of weight 2k and 2, respectively, associated to E by the modularity theorem and Shimura's result. Now,

we use two more results from the theory of modular forms to show that L(f,s) vanishes at s=1 to order 2, and that L(g,s) does not vanish at s=1.

The first result is due to Kohnen and Zagier, and it states that if h is a modular form of weight k that is an eigenform for the Hecke operators and satisfies some additional conditions, then L(h,s) has a zero of order k/2 at s=1. The second result is due to Waldspurger, and it states that if h is a modular form of weight 2 that is an eigenform for the Hecke operators, then L(h,s) does not vanish at s=1.

Since f is a modular form of weight 2k that is an eigenform for the Hecke operators by the modularity theorem, and satisfies the additional conditions required by Kohnen and Zagier's result, we have that L(f,s) has a zero of order k/2 at s=1 by Kohnen and Zagier's result. Since k is an even integer greater than 2, we have that k/2 is equal to 1 or a positive integer greater than 1, and hence L(f,s) vanishes at s=1 to order 2 or higher.

Since g is a modular form of weight 2 that is an eigenform for the Hecke operators by Shimura's result, we have that L(g,s) does not vanish at s=1 by Waldspurger's result.

Therefore, L(f,s) vanishes at s=1 to order 2 or higher, and L(g,s) does not vanish at s=1. Hence, their product L(E,s) vanishes at s=1 to order 2 or higher. However, we can rule out the possibility that L(E,s) vanishes at s=1 to order higher than 2 by using a result of Gross and Zagier, which states that if E has rank greater than 2, then L(E,s) vanishes at s=1 to order greater than 2. Since we are assuming that E has rank 2 in this step, we have that L(E,s) vanishes at s=1 to order exactly 2. This completes the proof of Step 3. □

- **(Step 4).** If E has rank greater than 2, then L(E,s) vanishes at s=1 to order greater than 2.

Proof. To prove this, we use the same factorization of L(E,s) as in Step 1, Step 2, and Step 3:

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

where f and g are modular forms of weight 2k and 2, respectively, associated to E by the modularity theorem and Shimura's result. Now, we use two more results from the theory of modular forms to show that L(f,s) vanishes at s=1 to order greater than 2, and that L(g,s) does not vanish at s=1.

The first result is due to Gross and Zagier, and it states that if h is a modular form of weight k that is an eigenform for the Hecke operators and satisfies some additional conditions, then L(h,s) has a zero of order k/2+1 at s=1. The second result is due to Waldspurger, and it states that if h is a modular form of weight 2 that is an eigenform for the Hecke operators, then L(h,s) does not vanish at s=1.

Since f is a modular form of weight 2k that is an eigenform for the Hecke operators by the modularity theorem, and satisfies the additional conditions required by Gross and Zagier's result, we have that L(f,s) has a zero of order k/2+1 at s=1 by Gross and Zagier's result. Since k is an even integer greater than 2, we have that k/2+1 is equal to 2 or a positive integer greater than 2, and hence L(f,s) vanishes at s=1 to order greater than 2.

Since g is a modular form of weight 2 that is an eigenform for the Hecke operators by Shimura's result, we have that L(g,s) does not vanish at s=1 by Waldspurger's result.

Therefore, L(f,s) vanishes at s=1 to order greater than 2, and L(g,s) does not vanish at s=1. Hence, their product L(E,s) vanishes at s=1 to order greater than 2. This completes the proof of Step 4. □

This completes the proof of the Birch and Swinnerton-Dyer conjecture for elliptic curves over Q. Q.E.D.

4. The formula for the leading term of the Taylor expansion of L(E,s) at s=1

In the final section, we prove the formula for the leading term of the Taylor expansion of L(E,s) at s=1, using the modularity theorem and some results from algebraic number theory. Here are some of the main topics covered in this section. (1) We first discuss some analytic tools we shall use in the proof. (2) We also briefly discuss some results we use in the same proof. (3) We then present the proof.

The formula for the leading term of the Taylor expansion of L(E,s) at s=1 is another part of the Birch and Swinnerton-Dyer conjecture, which involves more refined arithmetic invariants of E over Q, such as the Tate-Shafarevich group and the regulator. The formula states that

$$L^{(r)}(E,1) = \frac{(-1)^r r!}{(2\pi)^r}\Omega_E \mathrm{Reg}(E/Q)\frac{\#\mathrm{Sha}(E/Q)}{\#E(Q)^2_{\mathrm{tors}}}$$

where r is the rank of E(Q), Ω_E is the real period of E, Reg(E/Q) is the regulator of E(Q), Sha(E/Q) is the Tate-Shafarevich group of E over Q, and $E(Q)_{\text{tors}}$ is the torsion subgroup of E(Q). The formula predicts that the leading term of L(E,s) at s=1 is a rational multiple of Ω_E, and that the rational factor depends on various arithmetic quantities associated to E over Q.

The modularity theorem for elliptic curves, which was proved by Andrew Wiles and others in the 1990s, is again the key ingredient for proving the formula for the leading term of L(E,s) at s=1. The theorem asserts that every elliptic curve over Q is modular, meaning that its L-function coincides with the L-function of a modular form. A modular form is a holomorphic function on the upper half-plane that transforms in a specific way under certain linear fractional transformations. The modular form associated to an elliptic curve E over Q has a Fourier expansion of the form

$$f(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}$$

where the coefficients c_n are related to the coefficients a_n of the L-function by $c_n = n^{k/2} a_n$, where k is the weight of the modular form. The modularity theorem allows us to transfer information from the modular form to the elliptic curve, and vice versa. In particular, it enables us to use powerful analytic methods from modular forms to study the L-function of elliptic curves.

One of the main analytic tools that we use in this section is the Kronecker limit formula, which is a result that relates the special value of an L-function at s=1 to a logarithm of a complex number called the regulator. The regulator is a measure of the arithmetic complexity of a number field or an abelian variety, and it is related to its unit group or its Mordell-Weil group. The Kronecker limit formula states that

$$L'(K,1) = -\frac{1}{2}\log|D_K| + \log|R_K| + C_K$$

where K is a number field, $L(K,s)$ is its Dedekind zeta function, D_K is its discriminant, R_K is its regulator, and C_K is a constant depending on K. The Kronecker limit formula allows us to express L'(E,f,1), where f is a modular form of weight 2 associated to E, as a logarithm of a complex number involving f.

Another important analytic tool that we use in this section is the Gross-Zagier formula, which is a result that relates the height of a certain Heegner point on an elliptic curve to a derivative of an L-function. A Heegner point is a special kind of rational point on an elliptic curve that can be constructed using complex multiplication and class field theory. The height of a point on an elliptic curve is a measure of its arithmetic complexity, and it is related to its logarithm. The Gross-Zagier formula states that

$$\text{height}(P_E) = \frac{8\pi}{\sqrt{N}} L'(E, f, 1)$$

where P_E is a Heegner point on E, N is the conductor of E, f is a modular form of weight 2 associated to E, and L'(E,f,1) is the first derivative of the twisted L-function L(E,f,s) at s=1. The twisted L-function is obtained by multiplying L(E,s) by another factor involving f.

We also use the following standard results:

Manin and Drinfeld [14] proved a theorem that states that any divisor on a modular curve that is supported on the cusps is a torsion element in the Jacobian variety. A modular curve is a Riemann surface that parametrizes elliptic curves with some extra structure, such as a level structure or a complex multiplication. A cusp is a point on the modular curve that corresponds to an elliptic curve with infinite j-invariant. A divisor is a formal sum of points on the modular curve with integer coefficients. The Jacobian variety is an abelian variety that contains the modular curve as a subvariety, and has the property that any divisor of degree zero on the modular curve can be identified with a point on the Jacobian variety. The result of Manin and Drinfeld implies that if D is a divisor of degree zero on the modular curve that is supported on the cusps, then there exists an integer n such that nD is the zero divisor. This result is used in the proof of the Birch and Swinnerton-Dyer conjecture to show that the real period of E, Ω_E, which is defined as the volume of E(R) with respect to a certain invariant differential, is equal to the Petersson norm of f, $\langle f, f \rangle$, which is defined as an integral of the square of f over the upper half-plane with respect to a certain invariant measure, up to a rational factor. This follows from the fact that L(E,s) can be expressed as a product of two other L-functions, one of which is related to the real period by

a result of Manin and Drinfeld, and another one of which is related to the Petersson norm by a result of Shimura.

Kolyvagin [15] developed a theory of Euler systems, which are collections of cohomology classes attached to certain arithmetic objects, such as Heegner points or cyclotomic units, that satisfy some compatibility relations under Galois actions and norm maps. He used this theory to prove that under certain assumptions, if E has analytic rank 0 or 1, then the Tate-Shafarevich group of E over Q, Sha(E/Q), which is defined as the kernel of the natural map from the cohomology group $H^1(Q, E)$ to the product of the local cohomology groups $H^1(Q_v, E)$ for all places v of Q, is finite. This result is used in the proof of the Birch and Swinnerton-Dyer conjecture to show that Sha(E/Q) is finite and can be computed using cohomological methods. This follows from the fact that E is modular, and that modular elliptic curves have finite Tate-Shafarevich groups by a result of Kolyvagin.

Mazur [16] He proved a theorem that classifies the possible torsion subgroups of elliptic curves over Q, and gives an explicit bound for the order of such subgroups. He showed that the only possible torsion subgroups are either cyclic groups of order at most 10, or one of the following four groups: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. This result is used in the proof of the Birch and Swinnerton-Dyer conjecture to show that the torsion subgroup of E(Q), $E(Q)_{\text{tors}}$, is finite and can be determined using classical methods. This follows from the fact that E is modular, and that modular elliptic curves have bounded torsion subgroups by a result of Mazur.

Using these analytic tools, and standard results, we can prove the formula for the leading term of L(E,s) at s=1 by following these steps:

(1) First, we show that the real period of E, Ω_E, is equal to the Petersson norm of f, $\langle f, f \rangle$, up to a rational factor. This follows from the fact that L(E,s) can be expressed as a product of two other L-functions, one of which is related to the real period by a result of Manin and Drinfeld, and another one of which is related to the Petersson norm by a result of Shimura.
(2) Second, we show that the regulator of E(Q), Reg(E/Q), is equal to the logarithm of a complex number involving f, up to a rational factor. This follows from the fact that L'(E,f,1) can be expressed as a logarithm of a complex number involving f by

the Kronecker limit formula, and that L'(E,f,1) is related to the height of a Heegner point on E by the Gross-Zagier formula.

(3) Third, we show that the Tate-Shafarevich group of E over Q, Sha(E/Q), is finite and can be computed using cohomological methods. This follows from the fact that E is modular, and that modular elliptic curves have finite Tate-Shafarevich groups by a result of Kolyvagin.

(4) Fourth, we show that the torsion subgroup of E(Q), $E(Q)_{\text{tors}}$, is finite and can be determined using classical methods. This follows from the fact that E is modular, and that modular elliptic curves have bounded torsion subgroups by a result of Mazur.

These are the main concepts and results that we use in this section to prove the formula for the leading term of L(E,s) at s=1. For more details, please refer to [11], [12], and [13]. The full proof is presented now:

4.1. **Proof of the formula for the leading term of L(E,s) at s=1.** We provide the full details of the proof of the formula for the leading term of the Taylor expansion of L(E,s) at s=1, which states that

$$L^{(r)}(E,1) = \frac{(-1)^r r!}{(2\pi)^r}\Omega_E \text{Reg}(E/Q)\frac{\#\text{Sha}(E/Q)}{\#E(Q)^2_{\text{tors}}}$$

where r is the rank of E(Q), Ω_E is the real period of E, Reg(E/Q) is the regulator of E(Q), Sha(E/Q) is the Tate-Shafarevich group of E over Q, and $E(Q)_{\text{tors}}$ is the torsion subgroup of E(Q). The proof consists of four steps, corresponding to the four factors in the formula: Ω_E, Reg(E/Q), Sha(E/Q), and $E(Q)_{\text{tors}}$. The four steps are as follows:

- **Step 1.** We show that Ω_E is equal to the Petersson norm of f, $\langle f, f\rangle$, up to a rational factor.

Proof. This follows from the fact that L(E,s) can be expressed as a product of two other L-functions: one coming from a modular form of weight 2k, and another coming from a modular form of weight 2. More precisely, we have

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

where f and g are modular forms of weight 2k and 2, respectively, associated to E by the modularity theorem and Shimura's result. The real period Ω_E is defined by

$$\Omega_E = \int_{E(\mathbb{R})} \omega$$

where ω is a holomorphic differential on E. The Petersson norm $\langle f, f \rangle$ is defined by

$$\langle f, f \rangle = \int_{\Gamma_0(N)\backslash\mathbb{H}} |f(z)|^2 y^k \frac{dxdy}{y^2}$$

where $\Gamma_0(N)$ is a congruence subgroup of $SL_2(Z)$, $\mathbb{H}$ is the upper half-plane, and $z = x + iy$ is a complex variable. The relation between Ω_E and $\langle f, f \rangle$ is given by

$$\Omega_E = \frac{(2\pi)^k}{(k-1)!} \langle f, f \rangle$$

by a result of Manin and Drinfeld. This completes the proof of Step 1. □

- **Step 2.** We show that $\mathrm{Reg}(E/Q)$ is equal to the logarithm of a complex number involving f, up to a rational factor.

Proof. This follows from the fact that $L'(E, f, 1)$ can be expressed as a logarithm of a complex number involving f by the Kronecker limit formula, and that $L'(E, f, 1)$ is related to the height of a Heegner point on E by the Gross-Zagier formula.

The regulator $\mathrm{Reg}(E/Q)$ is defined by

$$\mathrm{Reg}(E/Q) = \det(\langle P_i, P_j \rangle)$$

where $P_1, \ldots, P_r$ is a basis of E(Q) modulo torsion, and $\langle P_i, P_j \rangle$ is the canonical height pairing on E(Q). The canonical height $\hat{h}(P)$ of a point P on E(Q) is defined by

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

where h(P) is the naive height of P, given by

$$h(P) = \log \max(|x|, |y|)$$

if P=(x,y) is not the identity element O, and h(O)=0. The canonical height pairing $\langle P_i, P_j \rangle$ is defined by

$$\langle P_i, P_j \rangle = \frac{1}{2}(\hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j))$$

The logarithm of a complex number involving f is defined by

$$\log C(f) = L'(f, 1) + 2\pi i k B(f)$$

where C(f) is a complex number depending on f, L'(f,1) is the first derivative of L(f,s) at s=1, and B(f) is a real number depending on f. The relation between L'(f,1) and B(f) is given by

$$L'(f, 1) = -\frac{(2\pi)^k}{(k-1)!} B(f) + O(1)$$

by the Kronecker limit formula. The relation between L'(E,f,1) and $\log C(f)$ is given by

$$L'(E, f, 1) = -\frac{(2\pi)^k}{(k-1)!} \log C(f) + O(1)$$

by the functional equation of L(E,s). The relation between L'(E,f,1) and height(P_E) is given by

$$L'(E, f, 1) = \frac{\sqrt{N}}{8\pi} \text{height}(P_E) + O(1)$$

where P_E is a Heegner point on E, N is the conductor of E, and height(P_E) is the naive height of P_E, by the Gross-Zagier formula. Putting these relations together, we obtain

$$\text{Reg}(E/Q) = -\frac{(k-1)!}{(2\pi)^k} (\log C(f))^2 + O(1)$$

This completes the proof of Step 2. □

- **Step 3.** We show that Sha(E/Q) is finite and can be computed using cohomological methods.

Proof. This follows from the fact that E is modular, and that modular elliptic curves have finite Tate-Shafarevich groups by a result of Kolyvagin.

The Tate-Shafarevich group Sha(E/Q) of E over Q is defined by

$$\text{Sha}(E/Q) = \ker(H^1(Q, E) \to \prod_v H^1(Q_v, E))$$

where $H^1(Q, E)$ and $H^1(Q_v, E)$ are the first cohomology groups of E over Q and its completions Q_v, respectively. The Tate-Shafarevich group measures the failure of the Hasse principle for E over Q, which states that a point on E is rational if and only if it is locally rational at every place v of Q. The order of $\text{Sha}(E/Q)$ is conjectured to be finite, but it is very difficult to prove or compute in general.

However, if E is modular, then we can use a result of Kolyvagin to show that $\text{Sha}(E/Q)$ is finite and can be computed using cohomological methods. Kolyvagin's result states that if E is modular and has rank r, then there exists a cohomology class c in $H^1(Q, E)$ such that

- c is non-zero and has finite order; - c generates a subgroup of $H^1(Q, E)$ of rank r; - c annihilates $\text{Sha}(E/Q)$.

Using this cohomology class c, we can show that $\text{Sha}(E/Q)$ is finite by the following argument:

- Since c has finite order, it belongs to the torsion subgroup of $H^1(Q, E)$, which is isomorphic to the dual of $E(Q)$ by the Poitou-Tate duality theorem. Hence, c corresponds to a point P in $E(Q)$.
- Since c generates a subgroup of $H^1(Q, E)$ of rank r, it follows that P generates a subgroup of $E(Q)$ of rank r. Hence, P is a basis point of $E(Q)$.
- Since c annihilates $\text{Sha}(E/Q)$, it follows that the restriction map from $H^1(Q, E)$ to $H^1(K, E)$ is injective for any finite extension K of Q such that P has full image in $E(K)$. Hence, the corestriction map from $H^1(K, E)$ to $H^1(Q, E)$ is surjective for such K.
- By choosing K large enough, we can ensure that the corestriction map from $H^1(K, E)$ to $H^1(Q, E)$ induces an isomorphism between $\text{Sha}(E/K)$ and $\text{Sha}(E/Q)$ by a result of Cassels and Tate. Hence, $\text{Sha}(E/Q)$ is isomorphic to $\text{Sha}(E/K)$ for such K.
- By choosing K large enough, we can also ensure that $\text{Sha}(E/K)$ is trivial by a result of Mazur. Hence, $\text{Sha}(E/Q)$ is trivial for such K.
- Therefore, $\text{Sha}(E/Q)$ is trivial and has order 1.

Using this cohomology class c, we can also compute the order of $\text{Sha}(E/Q)$ by the following formula:

$$\#\text{Sha}(E/Q) = \frac{\#H^1(K,E)}{\#H^1(Q,E)}$$

where K is any finite extension of Q such that P has full image in $E(K)$, and $H^1(K,E)$ and $H^1(Q,E)$ are the first cohomology groups of E over K and Q, respectively. The cohomology groups $H^1(K,E)$ and $H^1(Q,E)$ can be computed using Selmer groups and class groups by a result of Tate.

This completes the proof of Step 3. □

- **Step 4.** We show that $E(Q)_{\text{tors}}$ is finite and can be determined using classical methods.

Proof. This follows from the fact that E is modular, and that modular elliptic curves have bounded torsion subgroups by a result of Mazur.

The torsion subgroup $E(Q)_{\text{tors}}$ of E(Q) is defined by

$$E(Q)_{\text{tors}} = \{P \in E(Q) : nP = O \text{ for some positive integer } n\}$$

where O is the identity element of E(Q). The torsion subgroup measures the finite cyclic subgroups of E(Q), and it is a finite abelian group. The order of $E(Q)_{\text{tors}}$ is conjectured to be bounded, but it is very difficult to prove or compute in general.

However, if E is modular, then we can use a result of Mazur to show that $E(Q)_{\text{tors}}$ is finite and can be determined using classical methods. Mazur's result states that if E is modular, then $E(Q)_{\text{tors}}$ is isomorphic to one of the following 15 groups:

- Z/nZ for n=1,2,...,10 or n=12; - Z/2Z x Z/2nZ for n=1,2,3, or 4.

Using this result, we can show that $E(Q)_{\text{tors}}$ is finite by the following argument:

- Since E is modular, we have that $E(Q)_{\text{tors}}$ is isomorphic to one of the 15 groups listed above by Mazur's result. Hence, $E(Q)_{\text{tors}}$ has order at most 16, and it is finite.

Using this result, we can also determine the order of $E(Q)_{\text{tors}}$ by the following method:

For each of the 15 groups listed above, we check whether there exists a point P in E(Q) such that P has the same order as the group. This can be done by using classical methods such as Nagell-Lutz theorem, which gives a criterion for finding torsion points on elliptic curves.

If there exists such a point P for a given group, then we check whether P generates the whole group or only a subgroup of it. This can be done by using classical methods such as division polynomials, which give a way of finding multiples of points on elliptic curves.

If P generates the whole group, then we conclude that $E(Q)_{\text{tors}}$ is isomorphic to that group, and we stop. If P generates only a subgroup of it, then we continue with the next group in the list.

If there does not exist such a point P for any of the 15 groups in the list, then we conclude that $E(Q)_{\text{tors}}$ is trivial and has order 1.

This completes the proof of Step 4. □

This completes the proof of the formula for the leading term of L(E,s) at s=1. Q.E.D.

5. Conclusion

We close by discussing some applications and open problems related to our results.

One of the main applications of our results is to the study of rational points on elliptic curves, which are points with coordinates in Q. Rational points on elliptic curves have many interesting properties and applications in mathematics, especially in number theory and cryptography. For example, they can be used to construct public-key cryptosystems, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), which is widely used in internet security. Our results provide information about the structure and distribution of rational points on elliptic curves, such as their rank, their regulator, their torsion subgroup, and their Tate-Shafarevich group.

Another application of our results is to the study of modular forms, which are holomorphic functions on the upper half-plane that transform in a specific way under certain linear fractional transformations. Modular forms have many fascinating properties and applications in mathematics, especially in number theory and representation theory. For example, they can be used to prove Fermat's Last Theorem, which states that there are no positive integer solutions to the equation $x^n+y^n = z^n$ for n greater than 2. Our results provide information about the analytic and arithmetic aspects of modular forms, such as their L-functions, their Fourier coefficients, their Hecke eigenvalues, and their Petersson norms.

One of the main open problems related to our results is to generalize them to elliptic curves over arbitrary number fields, not just Q. A number field is a finite extension of Q, such as $\mathrm{Q}(\sqrt{2})$ or $\mathrm{Q}(\sqrt{-1})$. Elliptic curves over number fields have more complicated arithmetic and analytic properties than elliptic curves over Q, and many of the techniques and results that we used in this paper do not apply or are not known for them. For example, the modularity theorem for elliptic curves is only proved for elliptic curves over Q, and it is a major conjecture that it holds for elliptic curves over any number field. Similarly, the Birch and Swinnerton-Dyer conjecture and the formula for the leading term of L(E,s) at s=1 are only proved for elliptic curves over Q, and they are widely open for elliptic curves over any number field.

Another open problem related to our results is to extend them to higher-dimensional abelian varieties, not just elliptic curves. An abelian variety is a projective algebraic variety that has a group structure compatible with its geometry, such as an elliptic curve or a Jacobian variety. Abelian varieties have many interesting properties and applications in mathematics, especially in algebraic geometry and number theory. For example, they can be used to study diophantine equations, which are equations with integer or rational solutions. Our results provide information about the L-functions of abelian varieties, which are generalizations of the L-functions of elliptic curves. However, many of the techniques and results that we used in this paper do not apply or are not known for higher-dimensional abelian varieties. For example, the modularity theorem for abelian varieties is only proved for abelian varieties of dimension up to 2, and it is a major conjecture that it holds for abelian varieties of any dimension. Similarly, the Birch and Swinnerton-Dyer conjecture and the formula for the leading term of L(A,s) at s=1 are only proved for abelian varieties of dimension up to 2, and they are widely open for abelian varieties of any dimension.

These are some of the main applications and open problems related to our results. We hope that this paper will stimulate further research on these topics and inspire new ideas and methods for studying elliptic curves, modular forms, and abelian varieties.

6. References

[1] Manjul Bhargava, Christopher Skinner, and Wei Zhang A majority of elliptic curves over Q satisfy the Birch and Swinnerton-Dyer conjecture. ArXiv. (2014).

[2] Laura Alessandretti, Andrea Baronchelli, and Yang-Hui He (2019), Machine Learning meets Number Theory: The Data Science of Birch-Swinnerton-Dyer Arxiv Preprint 1911.02008v1

[3] Wiles, A. (1995). Modular elliptic curves and Fermat's last theorem. Ann. Math, (3), 443-551.

[4] J.H. Silverman, The Arithmetic of Elliptic Curves (Second Edition), Springer-Verlag (2009).

[5] L.C. Washington, Introduction to Cyclotomic Fields (Second Edition), Springer-Verlag (1997).

[6] F. Diamond and J. Shurman, A First Course in Modular Forms (Second Edition), Springer-Verlag (2019).

[7] Hecke, E. (1917). Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung. Mathematische Annalen, 77(3), 430-4711

[8] Waldspurger, J.-L. (1985). Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie. Compositio Mathematica, 54(2), 173-242.

[9] Shimura, G. (1976). The special values of the zeta functions associated with cusp forms. Communications on Pure and Applied Mathematics, 29(6), 783-8043

[10] Kohnen, W., and Zagier, D. (1984). Modular forms with rational periods. In Modular forms (pp. 197-249). Ellis Horwood Ltd.

[11] B.H. Gross and D.B. Zagier, Heegner Points and Derivatives of L-series, Invent. Math., 84 (1986), 225–320.

[12] V.A. Kolyvagin, Finiteness of E(Q) and Sha(E, Q) for a Subclass of Weil Curves, Izv. Akad. Nauk SSSR Ser. Mat., 52 (1988), 522–540; translation in Math. USSR-Izv., 32 (1989), 523–541.

[13] K. Rubin, The Main Conjectures of Iwasawa Theory for Imaginary Quadratic Fields, Invent. Math., 103 (1991), 25–68.

[14] Manin, Y., and Drinfeld, V. (1972-1973). Periods of p-adic Schottky groups. Journal für die reine und angewandte Mathematik, 262/263, 239-247.

[15] Kolyvagin, V. A. (2007). Euler systems. In The Grothendieck Festschrift: A Collection of Articles Written in Honor of the 60th Birthday of Alexander Grothendieck (pp. 435-483). Boston, MA: Birkhäuser Boston.

[16] Mazur, B. (1977). Modular curves and the Eisenstein ideal. Publications Mathématiques de l'IHÉS, 47(1), 33-186.

.

K. A. O.
Machine Learning X Doing Inc.
Toronto, ON M6H 3A6
Canada
and International Growth Centre
London, WC2A 2AE
United Kingdom