The L-functions of Elliptic Curves and Modular Forms

Tianxiang Liu

Advisor: Dinesh S. Thakur

Abstract

In 1995, the Fermat's Last Theorem was resolved by Andrew Wiles as a consequence of the proof of the Taniyama-Shimura-Weil conjecture for semistable elliptic curves, which built an important connection between elliptic curves and modular forms. This paper is a survey on elliptic curves, modular forms and their L-functions. At the end, we will understand the Taniyama-Shimura-Weil conjecture and numerically verify it.

1 Introduction

In 1637, French mathematician Pierre de Fermat wrote in the margin of the book Diophantus' Arithmetica that he found a proof of the statement that for $n \geq 3$, no three positive integers satisfy the equation $a^n + b^n = c^n$. He also claimed that he found a marvellous proof but margin is too small to contain it. The proof was not achieved until Andrew Wiles and his student Richard Taylor's proof of the Taniyama-Shimura-Weil conjecture, which now is known as the modularity theorem, for semistable elliptic curves[wil95]. This led to a contradiction, if a nontrivial solution exists, based on the work of Frey, Serre and Ribet.

In this paper, the concepts of elliptic curves and modular forms are introduced. Moreover, we will define the L-functions attached to elliptic curves over $\mathbb{Q}$ and modular forms. We study

the analytic and arithmetic properties of these L-functions including their Euler product, analytic continuation functional equations and special values. At the end, we will state the Taniyama-Shimura-Weil conjecture, and numerically test it with elliptic curves with small conductors.

2 L-functions

An *L-function* is a function $L(s)$, usually given as an infinite series of the form

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

where the variable s takes complex value, usually on a half plane where the series converge, and coefficients a_n are also complex numbers.

Example 2.1. The simplest and most famous series is the Riemann zeta function:

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

which converges on the half plane $Re(s) > 1$. The connection between $\zeta(s)$ and number theory comes from the fact that $\zeta(s)$ has an *Euler product*:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-1}},$$

where the product runs over all the prime numbers. An important consequence of the Euler product is that any information about the distribution of the zeros of $\zeta(s)$ can be translated into the information about the distribution of the prime numbers among the natural numbers. Let $\pi(x)$ be the prime-counting function, i.e. $\pi(x)$ is the number of primes p, $1 < p \leq x$.

The famous prime number theorem asserts that the limit

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{log(x)}}$$

tends to 1. In other words, $\frac{x}{log(x)}$ is a good approximation to the prime counting function. It was not proved until 1896 when J. Hadamard and Ch. de la Vallé Poussin established the result independently. Both of their proofs utilize the complex analytic properties of the Riemann zeta function.

Another important property of $\zeta(s)$ is presented in the following theorem.

Theorem 2.2. *The Riemann zeta function $\zeta(s)$ for $Re(s) > 1$ can be analytically continued to the whole complex plane except for a simple pole at $s = 1$. Furthermore, let*

$$\Lambda(s) := \pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s),$$

where $\Gamma(s)$ is the Gamma function defined by the improper integral

$$\int_0^\infty t^{s-1}e^{-t}dt$$

for $Re(s) > 0$, then $\Lambda(s)$ is invariant under $s \mapsto 1 - s$, i.e. $\zeta(s)$ satisfies the functional equation

$$\pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-(1-s)/2}\Gamma(\frac{1-s}{2})\zeta(1-s).$$

Proof. (proof of the functional equation)

By replacing $\zeta(s)$ by the infinite sum, we find

$$\begin{aligned}\pi^{-s}\Gamma(s)\zeta(2s) &= \sum_{n=1}^{\infty}\int_0^{\infty}(\pi n^2)^{-s}t^{s-1}e^{-t}dt \\ &= \sum_{n=1}^{\infty}\int_0^{\infty}t^{s-1}e^{-\pi n^2 t}dt \\ &= \int_0^{\infty}t^{s-1}(\theta(it)-\frac{1}{2})dt\end{aligned}$$

where the second equality is done by a change of variable $t \mapsto \pi n^2 t$, and

$$\begin{aligned}\theta(\tau) &= \frac{1}{2}\sum_{-\infty}^{\infty}e^{\pi i n^2\tau} \qquad (\mathrm{Im}\tau > 0) \\ &= \frac{1}{2}+\sum_{n=1}^{\infty}e^{\pi i n^2\tau}\end{aligned}$$

is the basic *theta-function*. $\theta(\tau)$ is holomorphic on the upper half plane, and satisfies

$$\begin{aligned}&\theta(\tau+2) = \theta(\tau) \\ &\theta(-1/\tau) = (\frac{\tau}{i})^{1/2}\theta(\tau),\end{aligned} \tag{1}$$

where the square root is defined on $Re(z) > 0$ to be real on the real axis. The proof of (1) is an application of the Poisson summation formula and the fact that the Fourier transform of $e^{-\pi x^2}$ is itself. In other words, $\theta(\tau)$ is a modular form, which will defined later, of half weight for the group $G(2)$ generated by $\tau \mapsto \tau+2$ and $\tau \mapsto -1/\tau$. The functional equation for $\zeta(s)$ is a consequence of identity (1):

$$\begin{aligned}\pi^{-s}\Gamma(s)\zeta(2s) &= \int_1^{\infty}t^{s-1}(\theta(it)-\frac{1}{2})dt + \int_0^1 t^{s-1}(\theta(it)-\frac{1}{2})dt \\ &= \int_1^{\infty}t^{s-1}(\theta(it)-\frac{1}{2})dt - \frac{1}{2s} + \int_1^{\infty}t^{-s-1}\theta(\frac{i}{t}) \\ &= \int_1^{\infty}(t^{s-1}+t^{1/2-s-1})(\theta(it)-\frac{1}{2})dt - \frac{1}{2s} - \frac{1}{1-2s},\end{aligned}$$

which is invariant under $s \mapsto \frac{1}{2}-s$. □

Remark. The last step of proof shows that the function equation of $\theta(\tau)$ can be transformed into the functional equation of $\zeta(s)$ by Mellin transform. By a similar reasoning, the functional equation of $\theta(\tau)$ can be derived from the functional equation of $\zeta(s)$. The following theorem, known as the Hecke's converse theorem, generalizes the above theorem and shows that $\zeta(s)$ and some other L-functions are determined by their functional equation.

Theorem 2.3. *Given a sequence of complex numbers a_0, a_1, ..., a_n, ... $= O(n^c)$, given $\lambda > 0$, $k > 0$, $C = \pm 1$, form*

$$\phi(s) = \sum_{n=1}^{\infty} a_n n^{-s} \qquad \Phi(s) = (\frac{2\pi}{\lambda})^{-s}\Gamma(s)\phi(s) \qquad f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/\lambda}.$$

The following two conditions are equivalent:

(A) $\Phi(s) + \frac{a_0}{s} + \frac{Ca_0}{k-s}$ *is entire and bounded in every vertical strip and satisfies the functional equation* $\Phi(k-s) = C\Phi(s)$*;*

(B) $f(-\frac{1}{\tau}) = C(\frac{\tau}{i})^k f(\tau)$.

Example 2.4. In 1826, German mathematician Peter Gustav Lejeune Dirichlet proved the following theorem:

Theorem 2.5 (Dirichlet)**.** *Let $N \geq 1$ and a be a positive integers such that $gcd(a, N) = 1$. Let P_a be the set of prime numbers such that $p \equiv a (mod\ N)$. Then the set P_a has density $\frac{1}{\phi(N)}$ (ϕ is the Euler's totient function) in the sense that the ratio*

$$\left(\sum_{p \in P_a} \frac{1}{p^s}\right) \Big/ \left(log \frac{1}{s-1}\right)$$

tends to $\frac{1}{\phi(N)}$ as s tends to 1.

In other words, the set of primes are "equally distributed" among the residue classes modulo N which are relative prime to N. An immediate result from this theorem is that

for each pair (a, N) as above, there are infinitely many primes $p \equiv a \pmod{N}$. This result was conjectured by Legendre, and is now known as the Dirichlet's theorem on arithmetic progression.

Dirichlet's proof uses the properties of the Dirichlet's L-functions, which are series in the form

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

where $\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}$ is a *Dirichlet character*. For the integers n that are not relatively prime to N, $\chi(n) = 0$. Just like the Riemann zeta function, Dirichlet L-functions have Euler products:

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

He showed that for every nontrivial character χ modulo N, $L(1, \chi) \neq 0$ or ∞ and the equality

$$log(\zeta(s)) + \sum_{\substack{\chi \bmod N \\ \chi \neq 1}} \chi(a)^{-1} log(L(s, \chi)) = \phi(N) \left(\sum_{p \equiv a \bmod N} \frac{1}{p^s} \right) + g(s)$$

with $g(1)$ finite. Using the fact that $\zeta(s)$ diverges at $s = 1$, we can conclude that the sum $\sum_{p \equiv a \bmod N} \frac{1}{p^s}$ diverges and hence is an infinite sum.

3 Elliptic Curves over $\mathbb{Q}$

Definition 3.1. An *elliptic curve* over $\mathbb{Q}$ is a smooth cubic projective curve E defined over $\mathbb{Q}$, with at least one point $\mathcal{O} \in E$.

For every elliptic curve E over a field K with $char(K) \neq 2, 3$, there exists a curve $\hat{E}$ given by the cubic equation

$$zy^2 = x^3 + Axz^2 + Bz^3, \ A, B \in K \text{ with } 4A^3 + 27B^2 \neq 0$$

that is isomorphic to E. In general, E is isomorphic to a model $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, which is called a *Weierstrass equation* or *Weierstrass model*. One reason that the theory of elliptic curves is so rich is that they can be equipped with a group structure. Given an elliptic curve E over $\mathbb{Q}$. Let P and Q be two points on the curve and l be the line that goes through P and Q (if $P = Q$, we let l be the tangent line at P). If l meets the third point R on the curve, then $P + Q$ is defined to be the reflection of R about the x-axis (see figure 1). If the line is vertical, then $P + Q = \mathcal{O}$, which is defined to be the point at ∞ and is outside the affine coordinates. Since the curve is defined by a cubic equation, one of these two conditions will happen. The above operation is commutative, associative, and hence makes $(E, +)$ an abelian group with the identity $\mathcal{O}$.

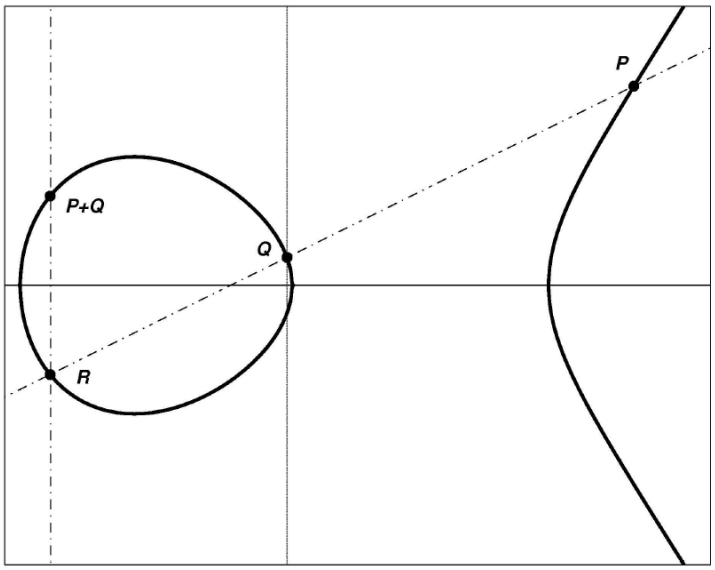

Figure 1: Addition of points [4]

In 1922, Mordell proves that $E(\mathbb{Q})$ is actually a finitely generated abelian group. In other words, there exists finitely many points $P_1, P_2, ..., P_n$ such that any points $Q \in E(\mathbb{Q})$ can be written as a linear combination

$$Q = \sum_{i=1}^{n} a_i P_i,$$

with some $a_i \in \mathbb{Z}$. As a consequence of the mordell's theorem,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{torsion}} \oplus \mathbb{Z}^r$$

for some nonnegative integer r, which we call the *rank* of $E(\mathbb{Q})$.

Definition 3.2. Let E be an elliptic curve over $\mathbb{Q}$ given by the equation $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Q}$. The *discriminant* Δ_E of E is defined to be

$$\Delta_E = -16(4A^3 + 27B^2).$$

An elliptic E' is said to be the *minimal model* for E if it is isomorphic to E and it has the smallest integer discriminant among all the curves that are isomorphic to E.

Before defining the L-function of $E(\mathbb{Q})$, we need to define the type of singularities of cubic curves. Let $\tilde{E}$ be a cubic curve over a field K given by a Weierstrass equation

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

with a singular point $P = (x_0, y_0)$. We write the Taylor expansion of $f(x, y)$ around (x_0, y_0) as follows:

$$\begin{aligned} f(x, y) - f(x_0, y_0) &= \lambda_1(x - x_0)^2 + \lambda_2(x - x_0)(y - y_0) + \lambda_3(y - y_0)^2 - (x - x_0)^3 \\ &= ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3 \end{aligned}$$

for some $\lambda_i \in K$ and $\alpha, \beta \in \bar{K}$, an algebraic closure of K.

Definition 3.3. The singular point $P \in \tilde{E}$ is a *node* if $\alpha \neq \beta$. The geometric interpretation

is that there are two different tangent lines to $\tilde{E}$ at P given by

$$y - y_0 = \alpha(x - x_0), \qquad y - y_0 = \beta(x - x_0).$$

If $\alpha = \beta$, we say P is a *cusp* and there is a unique tangent line at P.

Let E be an elliptic curve over $\mathbb{Q}$ given by a minimal model. For each prime p, we can reduce the coefficients of the cubic equation modulo p and consider the set of points over $\mathbb{F}_p$ that satisfy the reduced equation. This is a cubic curve $\tilde{E}$ over $\mathbb{F}_p$. We say that E has *good reduction* modulo p if $\tilde{E}$ is smooth and hence is an elliptic curve. If $\tilde{E}$ is singular at a point P, then we say E has *bad reduction* at p. In this case, we further distinguish two cases:

(1) If $\tilde{E}$ has a cusp at P, then we say E has *additive* reduction.

(2) If $\tilde{E}$ has a node at P, then we say E has *multiplicative (or semistable)* reduction. If the slopes of the tangent lines are in $\mathbb{F}_p$, then the reduction is said to be *split* multiplicative. Otherwise, it is *non-split* multiplicative.

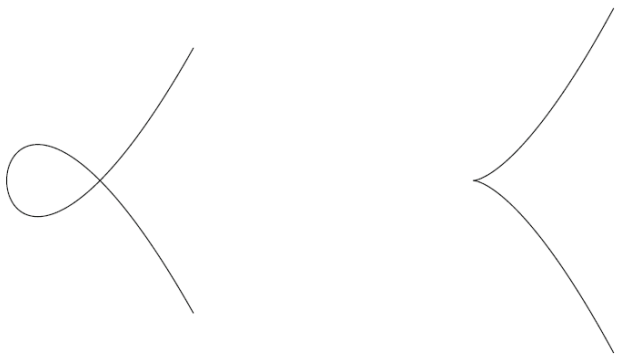

Figure 2: node and cusp [4]

Now we are ready to define the L-function of an elliptic curve over $\mathbb{Q}$. Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation:

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

with coefficients $a_i \in \mathbb{Z}$. For each prime p, let N_p be the number of points in the projective coordinates over $\mathbb{F}_p$, i.e.

$$N_p = |\{\mathcal{O}\} \cup \{(x, y) \in \mathbb{F}_p : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \equiv 0 \bmod p\}|.$$

Let $a_p = p + 1 - N_p$. We define the *local part at p of the L-series* as the following:

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

The *L-function* of the elliptic curve E is the product

$$L(E, s) = \prod_{p \geq 2} \frac{1}{L_p(p^{-s})}.$$

The product converges and gives an holomorphic function on the half plane $Re(s) > \frac{3}{2}$. This follows from Hasse's bound $|a_p| \leq 2\sqrt{p}$. The L-functions of elliptic curves over $\mathbb{Q}$ were conjectured to have analytic continuation to the whole complex and satisfy certain functional equation relating the value at s and $2 - s$. It now becomes a theorem due to be the proof of the Taniyama-Shimura-Weil conjecture. However, before the value of $L(E, s)$ makes sense at $s = 1$, Bryan Birch and Sir Peter Swinnerton-Dyer conjectured that the order of vanishing of $L(E, s)$ at $s = 1$ is equal to the rank r of E. This is amazing because if it's true, then the L-function is able to relate the solution counting of the curve over finite fields to the group structure of E, so we have a more computable tool to study the elliptic curves over $\mathbb{Q}$.

The last definition in this section is the *conductor* of an elliptic curve. Given an elliptic

curve $E/\mathbb{Q}$, for each prime p, define the quantity f_p as the following:

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

where δ_p is a technical invariant.

Definition 3.4. The *conductor* $N_{E/\mathbb{Q}}$ of $E/\mathbb{Q}$ is defined to be

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

The conductor is an important constant connecting the elliptic curves to the modular forms. The primes dividing $N_{E/\mathbb{Q}}$ are exactly the primes dividing the discrimiant of E because the curve is nonsingular if and only if the discriminant is non-zero.

4 Modular Forms

The *modular group* is the group of 2-by-2 invertible matrices with integer entries and determinant 1,

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

This group is generated by two matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Let $\mathcal{H}$ denote the *upper half plane*

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

Any matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ acts on $\tau \in \mathcal{H}$ by linear fractional transformation

$$M\tau = \frac{a\tau + b}{c\tau + d}.$$

It turns out that this group action is well defined as

$$\mathrm{Im}(M\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2},$$

which implies $M\tau \in \mathcal{H}$.

Definition 4.1. Let k be an integer. A meromorphic function $f : \mathcal{H} \longrightarrow \mathbb{C}$ is *weakly modular of weight k* if

$$f(M\tau) = (c\tau + d)^k f(\tau) \text{ for } M \in SL_2(\mathbb{Z}), \tau \in \mathcal{H}.$$

Since $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, any weakly modular function f satisfies

$$f(\tau) = f(T\tau) = f(\tau + 1).$$

The periodicity implies that f has a Fourier expansion

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

Definition 4.2. f is a *modular form of weight k* if

(a) f is holomorphic on $\mathcal{H}$.

(b) f is weakly modular of weight k.

(c) f is holomorphic at ∞, i.e. the Fourier coefficients a_n are zero for all $n < 0$.

The third condition is equivalent to that $|f(yi)|$ remains bounded and tends to a_0 as y tends to ∞.

Definition 4.3. f is a *cusp form of weight* k if it is a modular form of weight k and $a_0 = 0$.

given $N \geq 1$, we are also interested in the following subgroups of $SL_2\mathbb{Z}$:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0, a \equiv d \equiv 1 \bmod N \right\}$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : b \equiv c \equiv 0, a \equiv d \equiv 1 \bmod N \right\}$$

We say that a subgroup Γ of $SL_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma(N)$ is a subgroup of Γ and N is the level of the congruence subgroup. We can define the modular form (cusp form resp.) of weight k for a congruence subgroup Γ by simply replacing $SL_2(Z)$ by Γ. Being a congruence subgroup guarantees that f has a Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n\tau/N}$. The set of modular forms of weight k for G form a vector space over $\mathbb{C}$, which is denoted by $M_k(\Gamma)$ ($S_k(\Gamma)$ for the space of cusp forms).

Let Γ_1 and Γ_2 be two congruence subgroups. For each $\alpha \in GL_2^+(\mathbb{Q})$, the set

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$$

is a *double coset* in $GL_2^+(\mathbb{Q})$. Γ_1 acts on the double coset by left multiplication. The orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is in fact a finite disjoint union $\cup_{j=1}^{n}\Gamma_1\beta_j$.

Definition 4.4. The *weight* k $\Gamma_1\alpha\Gamma_2$ operator takes function $f \in M_k(\Gamma_1)$ to

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k,$$

where $\{\beta_j\}$ are orbit representatives, and the symbol $f[\beta]$ is defined to be

$$f[\beta]_k(\tau) = f[\begin{pmatrix} a & b \\ c & d \end{pmatrix}]_k(\tau) = (det\beta)^{k-1} j(\beta,\tau)^{-k} f(\beta_j), \tau \in \mathcal{H}$$

where $j(\beta,\tau)$ is the automorphy factor $c\tau + d$.

The double coset operator is well defined as it is independent of the choice of representatives $\{\beta_j\}$. Moreover, $[\Gamma_1 \alpha \Gamma_2]_k$ takes $S_k(\Gamma_1)$ to $S_k(\Gamma_2)$.

Now we define several operators, known as the Hecke operators, on the space of modular forms and cusp forms whose eigenvalues are closely related to the solution counting N_p of elliptic curves over $\mathbb{Q}$ in section 3.

Definition 4.5. For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, a *diamond operator* is defined to be $\langle d \rangle : M_k(\Gamma_1(N)) \longrightarrow M_k(\Gamma_1(N))$ given by

$$\langle d \rangle f = f[\alpha]_k \text{ for any } \alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N) \text{ with } \delta \equiv d \pmod{N}$$

Definition 4.6. Given a prime p, the p^{th} *Hecke operator* is defined to be $T_p : M_k(\Gamma_1(N)) \longrightarrow M_k(\Gamma_1(N))$ given by

$$T_p f = f[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N)]_k.$$

T_p has an explicit formula given by

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f\big[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \big]_k, & \text{if } p|N, \\ \sum_{j=0}^{p-1} f\big[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \big]_k + f\big[\begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \big]_k, & \text{if } p \nmid N, \text{ where } mp - nN = 1. \end{cases}$$

We extend the diamond operator to all $n \in \mathbb{Z}^+$ by letting $\langle n \rangle = 0$ if $(n, N) > 1$, just like how the Dirichlet character is defined. The diamond operator $\langle n \rangle$ is totally multiplicative in

the sense that $\langle mn\rangle = \langle m\rangle\langle n\rangle$. To define T_n, first let

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p\rangle T_{p^{r-2}}, \text{ for } n \geq 2. \tag{2}$$

For each $n \in \mathbb{Z}^+$, let

$$T_n = \prod T_{p_i^{r_i}}, \text{ where } n = \prod p_i^{r_i}. \tag{3}$$

Then, for $n, m \in \mathbb{Z}^+, (m, n) = 1$, $T_{mn} = T_m T_n$, i.e. T_n is multiplicative.

We form the series $g(s)$ with coefficients in T_n:

$$g(s) = \sum_{n=1}^{\infty} T_n n^{-s}.$$

As a consequence of (2) and (3), $g(s)$ has Euler product

$$g(s) = \prod_p (1 - T_p p^{-s} + \langle p\rangle p^{k-1-2s})^{-1}. \tag{4}$$

Definition 4.7. A nonzero modular form $f \in M_k(\Gamma_1(N))$ is an *eigenform* if it is an eigenvector for all T_n and $\langle n\rangle$ simultaneously, $n \in \mathbb{Z}^+$. f is said to be *normalized* if the first Fourier coefficient a_1 is 1. Then each Fourier coefficient a_n appears as an eigenvalue of T_n.

Given a Dirichlet character χ modulo N, the χ-eigenspace is defined to be

$$M_k(N, \chi) = \{f \in M_k(\Gamma_1(N)) : f[\gamma]_k = \chi(d_\gamma) f \text{ for all } \gamma \in \Gamma_0(N)\},$$

where d_γ denotes the lower right entry of γ.

For each modular form $f \in M_k(\Gamma_1(N))$ with Fourier expansion $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$, define its L-function to be

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

$L(f, s)$ converges on $Re(s > k)$ and if f is a cusp form, then it converges on $Re(s) >$

$k/2+1$. The following theorem addresses the equivalence between the condition of f being an normalized eigenform and that its L-function has an Euler product.

Theorem 4.8. *Let $f \in M_k(N,\chi) \subseteq M_k(\Gamma_1(N))$, $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$. The following are equivalent:*

(a) f is a normalized eigenform.

(b) L(s,f) has an Euler product

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

Recall that the functional equation of the basic theta function θ was transformed into a function equation of its Mellin transform, which results in the functional equation for $\zeta(s)$. Does similar result hold for other modular forms? The answer is yes for $S_k(\Gamma_1(N))$. If $k = 2$, then it is exactly what the functional equation of $L(E,s)$ looks like acoording to the modularity theorem.

Before stating the theorem, we define the operator $W_N : S_k(\Gamma_1(N)) \longrightarrow S_k(\Gamma_1(N))$ by

$$f \mapsto i^k N^{1-k/2} f\Big[\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \Big]_k.$$

W_N is an involution and decompose $S_k(\Gamma_1(N))$ into two eigenspaces

$$S_k(\Gamma_1(N))^{\pm} = \{f \in S_k(\Gamma_1(N)) : W_N f = \pm f\}.$$

Theorem 4.9. *Suppose $f \in S_k(\Gamma_1(N))^{\pm}$, let*

$$\Lambda_N(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,f).$$

Then Λ_N can be analytically continued to the entire complex plane and satisfies the functional

equation

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

Consequently, $L(s,f)$ can be analytically continued to the entire complex plane.

Proof.

$$\begin{aligned}\Lambda_N(s) &= N^{s/2}\int_0^\infty f(it)t^{s-1}dt \\ &= \int_0^\infty f(it/\sqrt{N})t^{s-1}dt \\ &= \int_1^\infty f(it/\sqrt{N})t^{s-1}dt + \int_0^1 f(it/\sqrt{N})t^{s-1}dt\end{aligned}$$

Since $f(it/\sqrt{N})$ is of order $e^{2\pi t/\sqrt{N}}$, the first integral converges to an entire function. Also applying the definition of W_N,

$$\begin{aligned}(W_N f)(i/(\sqrt{N}t)) &= i^k N^{1-k/2} f\Big[\begin{pmatrix}0 & -1\\ N & 0\end{pmatrix}\Big]_k (i/(\sqrt{N}t)) \\ &= i^k N^{1-k/2} N^{k-1}(Ni/(\sqrt{n}t))^{-k} f(\frac{-1}{Ni/(\sqrt{N}t})) \\ &= t^k f(it/\sqrt{N}).\end{aligned}$$

Then the second integral can be written as

$$\begin{aligned}\int_0^1 f(it/\sqrt{N})t^{s-1}dt &= \int_0^1 (W_N f)(i/(\sqrt{N}t))t^{s-k-1}dt \\ &= \int_1^\infty (W_N f)(it/\sqrt{N})t^{k-s-1}dt\end{aligned}$$

Thus,

$$\Lambda_N(s) = \int_1^\infty (f(it/\sqrt{N})t^s + (W_N f)(it/\sqrt{N})t^{k-s})\frac{dt}{t}.$$

Since $W_N f = \pm f$, we have $\Lambda_N(s) = \pm\Lambda_N(k-s)$ □

5 The Taniyama-Shimura-Weil Conjecture

Definition 5.1. An elliptic curve E defined over $\mathbb{Q}$ is *modular* if there is a cusp form $f_E(\tau)$ such that

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

The Taniyama-Shimura-Weil Conjecture said that all elliptic curves over $E/\mathbb{Q}$ are modular. Given an elliptic curve $E/\mathbb{Q}$, we expect the modular form f_E to have be a normalized eigenform because of Theorem 4.8 and because $L(E, s)$ is defined by an Euler product. Also, f_E must have weight 2 because of Theorem 4.9 and the conjectural functional equation of $L(E, s)$. What's more, f_E is expected to be an element of $S_k(\Gamma_0(N))$ where N is the conductor of E.

Given an elliptic curve $E/\mathbb{Q}$ with equation $y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$, we can numerically verify its modularity by doing the following steps:

(1) Compute the conductor N of E.

(2) For primes $p < 100$, calculate the number of points N_p on $E(\mathbb{F}_p)$ with the help of computers. Let $a_p = p + 1 - N_p$.

(3) For $p \nmid N$, compare a_p to the table of Hecke eigenvalues, which is on pg. 265 of [2]. A part of the table is on the last page. If the elliptic curve is modular, then we expect the a_p matches with the Hecke eigenvalue of certain cusp form with level N.

The following is a pseudocode for step (2):

Algorithm 1 solution counting

Set primeset = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97]

Set apvalue be an empty array.

for $p \in$ primeset **do**

Set $n_p = 1$

for x in range(0, p) **do**

for y in range(0, p) **do**

if $y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ **then**

n_p+=1

end if

end for

end for

apvalue.append($p + 1 - n_p$)

end for

return apvalue

We obtain a sequence of a_p value from the solution counting over finite fields, which we can use to compare with the Hecke eigenvalue table.

Example 5.2 ($E : y^2 + y = x^3 - x$)**.** The discriminant of E is 37, which means the only possible bad reduction is at 37. In fact, E has multiplicative reduction at 37, so the conductor of E is 37. Following step, we input the coefficients $a_1 = 0, a_2 = 0, a_3 = 1, a_4 = -1, a_6 = 0$. The sequence of a_p we get is [-2, -3, -2, -1, -5, -2, 0, 0, 2, 6, -4, -1, -9, 2, -9, 1, 8, -8, 8, 9, -1, 4, -15, 4, 4], which agrees with the row 37A(A) on pg. 265 of [2].

Example 5.3 ($E : y^2+xy+y = x^3+4x-6$)**.** The discriminant of E is $-21952 = -1 \cdot 2^6 \cdot 7^3$. Therefore, the possible bad reductions are 2 and 7. It turns out that E has multiplicative reduction at both 2 and 7, so the conductor N is 14. Following step 2, we get the sequence

[-1, -2, 0, 1, 0, -4, 6, 2, 0, -6, -4, 2, 6, 8, -12, 6, -6, 8, -4, 0, 2, 8, -6, -6, -10], which agrees with the row 14A(C).

Example 5.4 ($E : y^2 + xy + y = x^3 - 6x + 4$)**.** The discriminant of E is $1188 = 2^2 \cdot 3^3 \cdot 11$. Therefore, the possible bad reductions are 2, 3 and 11. It turns out that E has multiplicative reduction at all three primes, so the conductor N is 66. Following step 2, we get the sequence [-1, 1, 0, 2, -1, -4, -6, -4, 6, 6, 8, -10, 6, 8, -6, 0, 0, 8, -4, 6, 2, 14, -12, -6, 14], which agrees with the row 66A(A).

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97	W_q
11A(B)	−2	−1	1	−2	−	4	−2	0	−1	0	7	3	−8	−6	8	−6	5	12	−7	−3	4	−10	−6	15	−7	
14A(C)	+	−2	0	−	0	−4	6	2	0	−6	−4	2	6	8	−12	6	−6	8	−4	0	2	8	−6	−6	−10	
15A(C)	−1	+	−	0	−4	−2	2	4	0	−2	0	−10	10	4	8	−10	−4	−2	12	−8	10	0	12	−6	2	
17A(C)	−1	0	−2	4	0	−2	−	−4	4	6	4	−2	−6	4	0	6	−12	−10	4	−4	−6	12	−4	10	2	
19A(B)	0	−2	3	−1	3	−4	−3	−	0	6	−4	2	−6	−1	−3	12	−6	−1	−4	6	−7	8	12	12	8	
20A(B)	−	−2	+	2	0	2	−6	−4	6	6	−4	2	6	−10	−6	−6	12	2	2	−12	2	8	6	−6	2	
21A(B)	−1	−	−2	+	4	−2	−6	4	0	−2	0	6	2	−4	0	6	12	−2	4	0	−6	−16	−12	−14	18	
24A(B)	−	+	−2	0	4	−2	2	−4	−8	6	8	6	−6	4	0	−2	4	−2	−4	8	10	−8	−4	−6	2	
26A(B)	+	1	−3	−1	6	−	−3	2	0	6	−4	−7	0	−1	3	0	−6	8	14	−3	2	8	12	−6	−10	
26B(D)	−	−3	−1	1	−2	+	−3	6	−4	2	4	3	0	−5	13	12	−10	−8	−2	−5	−10	−4	0	6	14	
27A(B)	0	−	0	−1	0	5	0	−7	0	0	−4	11	0	8	0	0	0	−1	5	0	−7	17	0	0	−19	
30A(A)	+	−	+	−4	0	2	6	−4	0	−6	8	2	−6	−4	0	−6	0	−10	−4	0	2	8	12	18	2	
32A(B)	−	0	−2	0	0	6	2	0	0	−10	0	−2	10	0	0	14	0	−10	0	0	−6	0	0	10	18	
33A(B)	1	+	−2	4	−	−2	−2	0	8	−6	−8	6	−2	0	8	6	−4	6	−4	0	−14	−4	12	−6	2	
34A(A)	−	−2	0	−4	6	2	+	−4	0	0	−4	−4	6	8	0	−6	0	−4	8	0	2	8	0	−6	14	
35A(B)	0	1	+	−	−3	5	3	2	−6	3	−4	2	−12	−10	9	12	0	8	−4	0	2	−1	12	−12	−1	
36A(A)	−	+	0	−4	0	2	0	8	0	0	−4	−10	0	8	0	0	0	14	−16	0	−10	−4	0	0	14	
37A(A)	−2	−3	−2	−1	−5	−2	0	0	2	6	−4	+	−9	2	−9	1	8	−8	8	9	−1	4	−15	4	4	
37B(C)	0	1	0	−1	3	−4	6	2	6	−6	−4	−	−9	8	3	−3	12	8	−4	−15	11	−10	9	6	8	
38A(D)	+	1	0	−1	−6	5	3	−	3	9	−4	2	0	8	0	−3	9	−10	5	−6	−7	−10	−6	−12	−10	
38B(A)	−	−1	−4	3	2	−1	3	+	−1	−5	−8	−2	−8	4	8	−1	15	2	3	2	9	−10	−6	0	−2	
39A(B)	1	+	2	−4	4	−	2	0	0	−10	4	−2	6	−12	0	6	12	−2	−8	0	2	8	4	−2	10	
40A(B)	+	0	−	−4	4	−2	2	4	4	−2	−8	6	−6	−8	4	6	−4	−2	8	0	−6	0	−16	−6	−14	
42A(A)	−	+	−2	+	−4	6	2	−4	8	−2	0	−10	−6	−4	0	6	4	6	4	8	10	0	−4	−6	−14	
43A(A)	−2	−2	−4	0	3	−5	−3	−2	−1	−6	−1	0	5	+	4	−5	−12	2	−3	2	2	−8	15	−4	7	
44A(A)	−	1	−3	2	+	−4	6	8	−3	0	5	−1	0	−10	0	−6	3	−4	−1	15	−4	2	6	−9	−7	
45A(A)	1	−	+	0	4	−2	−2	4	0	2	0	−10	−10	4	−8	10	4	−2	12	8	10	0	−12	6	2	
46A(A)	+	0	4	−4	2	−2	−2	−2	−	2	0	−4	6	10	0	−4	12	−8	−10	0	6	−12	14	−6	6	
48A(B)	+	−	−2	0	−4	−2	2	4	8	6	−8	6	−6	−4	0	−2	−4	−2	4	−8	10	8	4	−6	2	
49A(A)	1	0	0	−	4	0	0	0	8	2	0	−6	0	−12	0	−10	0	0	4	16	0	8	0	0	0	
50A(E)	+	1	−	2	−3	−4	−3	5	6	0	2	2	−3	−4	12	6	0	2	−13	12	11	−10	−9	15	2	
50B(A)	−	−1	+	−2	−3	4	3	5	−6	0	2	−2	−3	4	−12	−6	0	2	13	12	−11	−10	9	15	−2	
51A(A)	0	−	3	−4	−3	−1	+	−1	9	6	2	−4	−3	−7	−6	−6	6	8	−4	12	2	−10	−6	0	−16	
52A(B)	−	0	2	−2	−2	+	6	−6	8	2	10	−6	−6	4	−2	6	−10	−2	10	10	2	−4	−6	−6	2	
53A(A)	−1	−3	0	−4	0	−3	−3	−5	7	−7	4	5	6	−2	−2	+	−2	−8	−12	1	−4	−1	−1	−14	1	
54A(E)	+	−	3	−1	−3	−4	0	2	−6	6	5	2	−6	−10	6	9	12	8	14	0	−7	8	−3	−18	−1	
54B(A)	−	+	−3	−1	3	−4	0	2	6	−6	5	2	6	−10	−6	−9	−12	8	14	0	−7	8	3	18	−1	
55A(B)	1	0	−	0	+	2	6	−4	4	6	−8	−2	2	4	−12	−2	4	−10	−16	8	14	8	−4	10	10	
56A(C)	−	0	2	+	−4	2	−6	8	0	6	8	−2	2	−4	−8	6	0	−6	−4	−8	10	16	8	−6	−6	
56B(A)	+	2	−4	−	0	0	−2	−2	8	2	4	−6	−2	8	−4	−10	6	4	−12	0	−14	−8	6	10	−2	
57A(E)	−2	+	−3	−5	1	2	−1	+	−4	−2	−6	0	0	−1	−9	10	−8	−1	8	−12	−11	16	12	−6	−10	
57B(B)	1	−	−2	0	0	6	−6	+	4	2	8	−10	−2	−4	12	−6	−12	−2	−4	0	10	0	16	−2	10	
57C(F)	−2	−	1	3	−3	−6	3	+	4	−10	2	8	−8	−1	3	−6	0	7	8	12	−11	0	4	10	−2	
58A(A)	+	−3	−3	−2	−1	3	−4	−8	0	+	3	−8	−2	7	11	1	−4	4	−4	−2	−12	−7	0	−6	−6	
58B(B)	−	−1	1	−2	−3	−1	8	0	4	+	−3	8	2	−11	13	−11	0	−8	−12	2	4	15	4	−10	−2	
61A(A)	−1	−2	−3	1	−5	1	4	−4	−9	−6	0	8	5	−8	4	6	9	+	−7	−8	−11	3	4	−4	−14	
62A(A)	−	0	−2	0	0	2	−6	4	8	2	+	10	−6	8	−8	−6	−12	−6	−12	8	10	−8	8	−6	2	
63A(A)	1	−	2	+	−4	−2	6	4	0	2	0	6	−2	−4	0	−6	−12	−2	4	0	−6	−16	12	14	18	
64A(B)	−	0	2	0	0	−6	2	0	0	10	0	2	10	0	0	−14	0	10	0	0	−6	0	0	10	18	
65A(A)	−1	−2	+	−4	2	+	2	−6	−6	2	−10	−2	−6	10	4	2	6	2	−4	6	−6	−12	−16	2	−2	
66A(A)	+	−	0	2	+	−4	−6	−4	6	6	8	−10	6	8	−6	0	0	8	−4	6	2	14	−12	−6	14	
66B(E)	−	+	2	−4	+	−6	2	4	4	6	0	6	−6	4	−12	2	12	−14	4	−12	−6	−4	4	10	−14	

Figure 3: Hecke eigenvalue table [2]

References

[1] Gary Cornell, Joseph H. Silverman, and Glenn Stevens. *Modular forms and Fermat's last theorem*. Springer, 2007.

[2] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, 1992.

[3] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*. Springer, 2016.

[4] Álvar Lozano-Robledo. *Elliptic curves, modular forms, and their L-functions*. American Mathematical Society, 2011.

[5] Andrew Ogg. *Modular forms and Dirichlet series*. W.A. Benjamin, 1969.

[6] Jean-Pierre Serre. *A course in arithmetic*. Springer, 1973.

[7] Andrew Wiles. "Modular elliptic curves and Fermat's last theorem". In: *The Annals of Mathematics* 141.3 (1995), p. 443. DOI: 10.2307/2118559.