THE L-FUNCTION OF AN ELLIPTIC CURVE

Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Fix a prime p and define an integer sequence having an initial value that (as we will soon see) is well-chosen, and then subsequent values that are normalized counts of the elliptic curve reduced modulo powers of p,

$$\begin{aligned} t_1(E) &= 2, \\ t_{p^e}(E) &= p^e + 1 - |\widetilde{E}(\mathbb{F}_{p^e})|, \quad e \geq 1. \end{aligned}$$

The form of the Weierstrass equation of E shows that we expect $|\widetilde{E}(\mathbb{F}_{p^e})| = p^e + 1$ on average, so $t_{p^e}(E)$ measures the deviation of the true count from its naively expected value.

1. The Recurrence Satisfied by the Solution-Counts

Theorem 1.1. *Let 1_E be the trivial character modulo N, i.e.,*

$$1_E(p) = \begin{cases} 1 & \text{if } p \nmid N, \\ 0 & \text{if } p \mid N. \end{cases}$$

Then the normalized solution-counts satisfy the recurrence

$$t_{p^e}(E) = t_p(E) t_{p^{e-1}}(E) - 1_E(p) p t_{p^{e-2}}(E), \quad e \geq 2.$$

Easy part of proof. We discuss the case $p \nmid N$.

Modern mathematical machinery (the Tate module of an elliptic curve, the associated ℓ-adic Galois representation) shows that for a 2-by-2 matrix A with characteristic polynomial

$$X^2 - t_p(E)X + p,$$

the normalized solution-counts satisfy the condition

$$t_{p^e}(E) = \operatorname{tr}(A^e), \quad e \geq 1.$$

Also, we have chosen $t_1(E) = 2$ to extend the displayed formula to $e = 0$.

Let α and β be the eigenvalues of A. Thus for $e \geq 2$,

$$\begin{aligned} \operatorname{tr}(A^e) &= \alpha^e + \beta^e \\ &= (\alpha + \beta)(\alpha^{e-1} + \beta^{e-1}) - \alpha\beta(\alpha^{e-2} + \beta^{e-2}) \\ &= \operatorname{tr}(A)\operatorname{tr}(A^{e-1}) - p \operatorname{tr}(A^{e-2}). \end{aligned}$$

The desired recurrence follows. □

2. The Counting Zeta Function as an Euler Factor

Definition 2.1. *The* **counting zeta function of E at p** *is*

$$Z_p(E, X) = \exp\left(\sum_{e \geq 1} \frac{t_{p^e}(E)}{e} X^e \right).$$

By the recurrence of the previous section, the counting zeta function is an elaborate encoding of only *one* piece of information: $t_p(E)$. However, it is very useful encoding.

Proposition 2.2. *The counting zeta function of E at p takes the form*

$$Z_p(E,X) = (1 - t_p(E)X + 1_E(p)pX^2)^{-1}.$$

Proof. This is a matter of taking the logarithmic derivative. Compute (abbreviating $t_*(E)$ to t_*) that

$$(\log Z_p(E,X))' = \frac{1}{X}\sum_{e\geq 1} t_{p^e}X^e \overset{\text{call}}{=} \frac{1}{X}\cdot S.$$

Split off the initial term and then use the recurrence to study the sum,

$$\begin{aligned} S &= t_pX + \sum_{e\geq 2} t_{p^e}X^e \\ &= t_pX + t_pX\sum_{e\geq 2} t_{p^{e-1}}X^{e-1} - 1_E(p)pX^2\sum_{e\geq 2} t_{p^{e-2}}X^{e-2} \\ &= t_pX + t_pX\cdot S - 1_E(p)pX^2(S+2). \end{aligned}$$

Regroup to get

$$S(1 - t_pX + 1_E(p)pX^2) = X(t_p - 1_E(p)2pX),$$

so that $(\log Z_p(E,X))' = (1/X)S$ is now

$$\begin{aligned} (\log Z_p(E,X))' &= -\frac{-t_p + 1_E(p)2pX}{1 - t_pX + 1_E(p)pX^2} \\ &= (-\log(1 - t_pX + 1_E(p)pX^2))' \\ &= (\log((1 - t_pX + 1_E(p)pX^2)^{-1}))'. \end{aligned}$$

Thus the two logarithms themselves agree up to an additive constant; set $X = 0$ to see that the constant is 0. So the counting zeta function $Z_p(E,X)$ and the Euler factor $(1 - t_pX + 1_E(p)pX^2)^{-1}$ agree, and the proof is complete. □

3. The L-Function

Definition 3.1. *The L-function of the elliptic curve E is*

$$L(E,s) = \prod_p Z_p(E,p^{-s}) = \prod_p (1 - t_p(E)p^{-s} + 1_E(p)p^{1-2s})^{-1}.$$

The definition is purely formal, but one can show that in some right half plane of complex s-values, $L(E,s)$ converges absolutely and converges uniformly on compacta. The L-function encodes the values $\{t_p(E) : p \text{ prime}\}$.

Proposition 3.2. *The L-function of E expands as*

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

where

$$\begin{aligned} a_1 &= 1, \\ a_p &= t_p(E), \\ a_{p^e} &= a_p a_{p^{e-1}} - 1_E(p) p a_{p^{e-2}}, \quad e \geq 2, \\ a_{mn} &= a_m a_n, \quad \gcd(m,n) = 1. \end{aligned}$$

Conversely, given an integer sequence $\{a_n\}$ satisfying the displayed conditions, the corresponding Dirichlet Series has an Euler factorization,

$$\sum_{n\geq 1} a_n n^{-s} = \prod_p (1 - t_p(E)p^{-s} + 1_E(p)p^{1-2s})^{-1}.$$

Proof. Fix a prime p. Multiply the prime-power recurrence in the proposition statement by p^{-es} and sum over $e \geq 2$ to show, after a little algebra, that the prime-power recurrence is equivalent to

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

If also $a_1 = 1$ then this becomes

$$\sum_{e=0}^{\infty} a_{p^e} p^{-es} \cdot (1 - a_p p^{-s} + \chi(p)p^{1-2s}) = 1. \tag{2}$$

Conversely, suppose (2) holds. Let $s \to +\infty$ to show that $a_1 = 1$, and so does (1), implying the prime-power recurrence. So the condition $a_1 = 1$ and the prime-power recurrence are equivalent to

$$\sum_{e=0}^{\infty} a_{p^e} p^{-es} = (1 - a_p p^{-s} + \chi(p)p^{1-2s})^{-1} \quad \text{for } p \text{ prime.} \tag{3}$$

Before continuing, note that the Fundamental Theorem of Arithmetic (positive integers factor uniquely into prime powers) implies that for a function g of prime powers (exercise),

$$\prod_p \sum_{e=0}^{\infty} g(p^e) = \sum_{n=1}^{\infty} \prod_{p^e \| n} g(p^e). \tag{4}$$

The notation $p^e \| n$ means that p^e is the highest power of p that divides n, and we are assuming that g is small enough to justify formal rearrangements.

Now, if (3) holds along with the multiplicativity condition of the proposition then compute

$$\begin{aligned} L(s,f) = \sum_{n=1}^{\infty} a_n n^{-s} &= \sum_{n=1}^{\infty} \left(\prod_{p^e \| n} a_{p^e} \right) n^{-s} && \text{by multiplicativity} \\ &= \sum_{n=1}^{\infty} \prod_{p^e \| n} a_{p^e} p^{-es} = \prod_p \sum_{e=0}^{\infty} a_{p^e} p^{-es} && \text{by (4)} \\ &= \prod_p (1 - a_p p^{-s} + \chi(p)p^{1-2s})^{-1} && \text{by (3),} \end{aligned}$$

giving the Euler product expansion.

Conversely, given the Euler product expansion, compute (using the geometric series formula and (4))

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

So $a_n = \prod_{p^r\|n} b_{p,r}$, giving the multiplicativity condition of the proposition and showing in particular that $b_{p,r} = a_{p^r}$. This in turn implies (3), implying $a_1(E) = 1$ and the prime-power recurrence of the proposition. □

4. Eigenforms and Modularity

For any complex number τ in the upper half plane (i.e., $\mathrm{Im}(\tau) > 0$), define a related number $q = e^{2\pi i\tau}$. A function of the form

$$f(\tau) = \sum_{n\geq 1} a_n q^n$$

where the coefficients a_n satisfy the conditions

$$\begin{aligned}a_1 &= 1,\\ a_{p^e} &= a_p a_{p^{e-1}} - 1_E(p)p a_{p^{e-2}}, \quad e\geq 2,\\ a_{mn} &= a_m a_n, \quad \gcd(m,n)=1\end{aligned}$$

is sometimes (*but not always!*) a **weight-2 Hecke eigenform**, a very special kind of **modular form**. The function is entirely determined by the values $\{a_p : p \text{ prime}\}$.

We have shown that every elliptic curve E over $\mathbb{Q}$ gives rise to a function f that might be a weight-2 Hecke eigenform: If the L-function of the elliptic curve is

$$L(E,s) = \sum_{n\geq 1} a_n n^{-s} \qquad \text{(determined entirely by the } \{t_p(E) : p \text{ prime}\})$$

then the function is constructed using the same coefficients,

$$f(\tau) = \sum_{n\geq 1} a_n q^n \qquad \text{(also determined entirely by the } t_p(E)).$$

We naturally wonder whether f is in fact an eigenform.

One of the most famous theorems of 20th century mathematics asserts that the answer is yes,

All rational elliptic curves arise from modular forms.

Taniyama first suggested in the 1950's that a statement along these lines might be true, and a precise conjecture was formulated by Shimura. A 1967 paper of Weil provided strong theoretical evidence for the conjecture. The theorem was proved for a large class of elliptic curves in the 1990's by Wiles with a key ingredient supplied by joint work with Taylor, completing the proof of Fermat's Last Theorem after some 350 years. The Modularity Theorem was proved completely by Breuil, Conrad, Diamond, and Taylor around 2000.