The Hasse-Weil L-Function of an Elliptic Curve

[Koblitz]: II

The Congruence Zeta-Function (Local Zeta Function)

Set $q = p^k$, for some prime p. The notation $\mathbb{F}_q$ stands for the finite field with q elements.

Definition. Let C be a projective plane curve defined over $\mathbb{F}_q$. The zeta function of C over $\mathbb{F}_q$ is given by the formal power series

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

where

$$\exp(u) = \sum_{k=0}^{\infty}\frac{u^k}{k!}.$$

The Congruence Zeta-Function (Local Zeta Function)

Proposition. Let E be an elliptic curve defined over $\mathbb{F}_q$. There is an integer a_E such that

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

and the roots have the property $|\alpha| = |\beta| = \sqrt{q}$. Furthermore

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

Hasse-Weil L-Fucntions

Let E be an elliptic curve defined over $\mathbb{Q}$. We make substitution $T = p^{-s}$ in $Z(E/\mathbb{F}_p; T)$, and define Hasse-Weil L-series $L(E, s)$ by

$$L(E, s) = \frac{\zeta(s)\zeta(s-1)}{\Pi_p Z(E/\mathbb{F}_p; p^{-s})},$$

where $\zeta(s)$ is the *Riemann zeta function* defined by

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s}, \text{ for } Re(s) > 1$$

and we can express $\zeta(s)$ as $\zeta(s) = \prod_{primes\, p} \frac{1}{1 - p^{-s}}$. Thus, we have

$$L(E, s) =* \prod_{p:good} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Reduction

Let E be an elliptic curve defined over $\mathbb{Q}$ given by a Weierstrass equation

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

The reduction of E modulo p, denoted $\widetilde{E}$, is the curve over $\mathbb{F}_p$ defined by the equation

$$\widetilde{E} : y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x^2 + \widetilde{a_4}x + \widetilde{a_6},$$

where $\widetilde{a}_i$ denotes reduction modulo p. (The curve $\widetilde{E}$ may be singular).

Definition. We say that

(1) E has *good (stable) reduction* if $\widetilde{E}$ is non-singular.

(2) E has *multiplicative (semi-stable) reduction* if $\widetilde{E}$ admits a double point with two distinct tangents. (E has a node.) And the reduction is called *split* if the tangent directions are defined over $\mathbb{F}_p$, otherwise it is *non-split*.

(3) E has *additive (unstable) reduction* if $\widetilde{E}$ admits a double point with only one tangent. (E has a cusp.)

In cases (2) and (3), E is naturally said to have *bad reduction*.

L-Fucntions

For each prime p, if E has good reduction at p, let

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

The local factor of the L-series of E at p is

$$L_p(T) = 1 - a_p T + pT^2.$$

We extend the definition of $L_p(T)$ to the case that E has bad reduction by setting

$$L_p(T) = \begin{cases} 1 - T, & \text{if } E \text{ has split multiplicicative reduction at } p, \\ 1 + T, & \text{if } E \text{ has non-split multiplicicative reduction at } p, \\ 1, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

Definition. We define the L-function of the elliptic curve by

$$L(E/\mathbb{Q}, s) = \prod_p L_p(p^{-s})^{-1}.$$

Conductor of $E/\mathbb{Q}$

Let E be an elliptic curve defined over $\mathbb{Q}$. For each prime p, we define

$$f_p(E/\mathbb{Q}) = \begin{cases} 0, & \text{if } E \text{ has good reduction at } p, \\ 1, & \text{if } E \text{ has multiplicicative reduction at } p, \\ 2 + \delta_p, & \text{if } E \text{ has additive reduction at } p, \end{cases}$$

where $\delta_p = 0$ if $p \nmid 6$. The invariant δ_p may be computed using Ogg's formula in "Elliptic curves and wild ramification".

The conductor of E is defined to be

$$N_E := \prod_p p^{f_p}$$

Remark. The minimal discriminant is a measure of the bad reduction of E. Another such measure is the conductor of $E/\mathbb{Q}$.

As an application of Modularity Theorem...

Functional Equation of $L(E, s)$. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N_E. The L-function $L(E, s)$ can be extended analytically to an entire fuction on the whole complex s-plane. Define

$$\Lambda(s) := \left(\frac{\sqrt{N_E}}{2\pi}\right)^s \Gamma(s)L(E, s),$$

where $\Gamma(\cdot)$ is the Gamma function. Then $\Lambda(s)$ satisfies the functional equation

$$\Lambda(s) = \pm\Lambda(2 - s).$$

Goal: Zeta-Function of E_n

Let E_n be the elliptic curve $E_n: \; y^2 = x^3 - n^2 x$.

Theorem. Let p be a prime with $p \nmid 2n$. Then

$$Z(E_n/\mathbb{F}_p; T) = \frac{1 - a_E T + pT^2}{(1-T)(1-pT)} = \frac{(1-\alpha T)(1-\overline{\alpha} T)}{(1-T)(1-pT)},$$

where

$$\alpha = \begin{cases} i\sqrt{p}, & \text{if } p \equiv 3 \mod 4, \\ a + bi, & \text{if } p \equiv 1 \mod 4, \end{cases}$$

where $a, b \in \mathbb{Z}$, $a^2 + b^2 = p$ and $a + bi \equiv \left(\frac{n}{p}\right) \mod 2 + 2i$

Counting Points

- Let χ be a group homomorphism from $\mathbb{F}_q^\times$ to $\mathbb{C}^\times$. Usually, we say χ is a multiplicative characters on $\mathbb{F}_q^\times$.
- Let $\widehat{\mathbb{F}_q^\times}$ denote the group of multiplicative characters on $\mathbb{F}_q^\times$.
- Extend $\chi \in \widehat{\mathbb{F}_q^\times}$ to $\mathbb{F}_q$ by setting $\chi(0) = 0$.
- Denote $\overline{\chi}$ the complex conjugation of χ, $\overline{\chi} = \chi^{-1}$.

Lemma. If $a \in \mathbb{F}_q^\times$ and $m \mid (q-1)$, then

$$\#\{y \in \mathbb{F}_q : y^m = a\} = \sum_{\chi^m=1} \chi(a),$$

where the sum runs over all characters $\chi \in \widehat{\mathbb{F}_q^\times}$ whose order divides n.

Proposition. For any prime power $q = p^r$ with $p \nmid 2n$, we have

$$\#E_n(\mathbb{F}_q) = \begin{cases} 1 + q, & \text{if } q \equiv 3 \mod 4 \\ 1 + q + \chi_2(n)\left(J(\chi_2, \chi_4) + J(\chi_2, \overline{\chi_4})\right), & \text{if } q \equiv 1 \mod 4 \end{cases}$$

where χ_2 is the quadratic character, χ_4 is a character of exact order 4 of $\mathbb{F}_q^\times$, and

$$J(A, B) := \sum_{x \in \mathbb{F}_q} A(x) B(1 - x)$$

is the Jacobi sum of the characters A and B.

Remarks.

- The curves $E_n:\ y^2 = x^3 - n^2x$ and $C:\ y^2 = x^4 + n^2/4$ are $\mathbb{Q}$-isomorphic (as hyperelliptic curves).
- For a non-singular curve C of the form $x^n - y^m = d$, we have

$$\#C(\mathbb{F}_q) \quad \text{"}=\text{"} \quad 1 + q + \sum_{i,j} J(\chi_m^i, \chi_n^j),$$

  if $n \mid q-1$ and $m \mid q-1$, where χ_k is a character of exact order k of $\mathbb{F}_q^\times$.

Rationality of $Z(E_n)$ – ideas

- For a given character $A \in \widehat{\mathbb{F}_q^\times}$, the Gauss sum of A is defined to be

$$g(A) := \sum_{x \in \mathbb{F}_q^\times} A(x) \zeta_p^{\mathrm{Tr}_{\mathbb{F}_p}^{\mathbb{F}_q}(x)}.$$

  We have the following realtion between Gauss sums and Jacobi sums:

$$J(A, B) = \frac{g(A)g(B)}{g(AB)} \quad \text{if } A \neq \overline{B}.$$

- Hasse-Davenport Relation. Let $\mathbb{F}$ be a finite field and $\mathbb{F}_s$ an extension field over $\mathbb{F}$ of degree s. If $\chi \neq \varepsilon \in \widehat{\mathbb{F}^\times}$ and $\chi_s = \chi \circ N_{\mathbb{F}_s/\mathbb{F}}$ a character of $\mathbb{F}_s$. Then

$$(-g(\chi))^s = -g(\chi_s).$$

Rationality of $Z(E_n)$ – ideas

- When $p \equiv 1 \mod 4$, let χ_2 be the quadratic character and χ_4 a character of order 4 of $\mathbb{F}_p^\times$. Denote $\alpha = -\chi_2(n)J(\chi_2, \chi_4)$. Then

$$\#E_n(\mathbb{F}_{p^r}) = 1 + p^r - \alpha^r - \overline{\alpha}^r.$$

- When $p \equiv 3 \mod 4$, let χ_2 be the quadratic character and χ_4 a character of order 4 of $\mathbb{F}_{p^2}^\times$. Denote $\alpha = -J(\chi_2, \chi_4) = -p$. Then, for $r \geq 1$,

$$\#E_n(\mathbb{F}_{p^{2s+1}}) = 1 + p^{2r-1},$$

$$\#E_n(\mathbb{F}_{p^{2r}}) = 1 + p^{2r} - \alpha^r - \overline{\alpha}^r.$$

$$-\ln(1 - x) = \sum_{n \geq 1} \frac{x^n}{n}$$

Reformulate Zeta-Function of E_n

Let E_n be the elliptic curve $E_n: \; y^2 = x^3 - n^2 x$.

- When $p \equiv 1 \mod 4$,

$$(1-T)(1-pT)Z(E_n/\mathbb{F}_p; T) = \prod_{(\mathfrak{p})|p} (1 - \alpha_{\mathfrak{p}} T),$$

  where $\alpha_{\mathfrak{p}} = a + bi \in \mathbb{Z}[i]$ such $\mathfrak{p} = (\alpha_{\mathfrak{p}})$ and $\alpha_{\mathfrak{p}} \equiv \left(\frac{n}{p}\right) \mod 2+2i$.
- When $p \equiv 3 \mod 4$,

$$(1-T)(1-pT)Z(E_n/\mathbb{F}_p; T) = 1 + pT^2$$

- **Weil.** Jacobi Sums as "Grossencharaktere". (also called Hecke character : an idèle class character)
- **$L(E_n, s)$.**

$$L(E_n, s) = \frac{1}{4} \sum_{a+bi \in \mathbb{Z}[i]} \frac{\psi_n(a+bi)}{(a^2+b^2)^s},$$

where

$$\psi_n(x) = x\psi_n'(x), \quad \psi_n(x) = \begin{cases} \psi_1'(x)\left(\frac{n}{x \cdot \overline{x}}\right), & x \text{ is coprime to } 2n, \\ 0, & \text{otherwise}, \end{cases}$$

where $\psi_1'(x)$ is a multiplicative character of order 4 on $(\mathbb{Z}[i]/(2+2i))^\times$ such that $\psi_1'(x)x \equiv 1 \mod 2+2i$.

Remark. For a CM elliptic curve E defined over $\mathbb{Q}$, there exists an imaginary CM field K and a Hecke character ψ of K such that $L(\psi, s)$ is the Hasse-Weil L-function of E. That is,

$$L(\psi, s) = L(E, s).$$

Functional Equation of $L(E_n, s)$. The L-function $L(E_n, s)$, $Re(s) > 3/2$, can be extended analytically to an entire fuction on the whole complex s-plane. Define

$$\Lambda(s) := \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(E_n, s), \quad N = \begin{cases} 32n^2, & n \text{ odd}, \\ 16n^2, & n \text{ even}, \end{cases}$$

where $\Gamma(\cdot)$ is the Gamma function. Then $\Lambda(s)$ satisfies the functional equation

$$\Lambda(s) = \begin{cases} \Lambda(2-s), & n \equiv 1, 2, 3 \mod 8, \\ -\Lambda(2-s), & n \equiv 5, 6, 7 \mod 8. \end{cases}$$

Weak BSD Conjecture

- Weak Birch and Swinnerton-Dyer Conjecture.

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

  $L(E, 1) = 0$ if and only if E has infinitely many rational points.

- Coates-Wiles. Let E be an elliptic curve defined over $\mathbb{Q}$ with CM. If $\mathrm{rank}(E(\mathbb{Q})) > 0$, then $L(E, 1) = 0$.
- Proposition II.6.12. In case $n \equiv 5, 6, \text{or } 7 \mod 8$, if the weak BSD conjecture holds for E_n, then n is a congruent number.
- Gross-Zagier. For $n \equiv 5, 6, \text{or } 7 \mod 8$, the elliptic curve E_n has non-zero rank if $\mathrm{ord}_{s=1} L(E_n, s) = 1$.

$L(E_n, 1) =?$ for $n \equiv 1, 2, \text{or } 3 \mod 8$.