L-functions and Elliptic Curves

Nuno Freitas

Universität Bayreuth

January 2014

Motivation

Let $m(P)$ denote the logarithmic Mahler measure of a polynomial $P \in \mathbb{C}[x^{\pm 1}, y^{\pm 1}]$.

- In 1981, Smyth proved the following formula:

  $$m(1 + x + y) = L'(\chi_{-3}, -1),$$

  where χ_{-3} is the Dirichlet character associated to the quadratic field $\mathbb{Q}(\sqrt{-3})$.
- In 1997, Deninger conjectured the following formula

  $$m(x + \frac{1}{x} + y + \frac{1}{y} + 1) = L'(E, 0),$$

  where E is the elliptic curve that is the projective closure of the polynomial in the left hand side.

Our goal: Sketch the basic ideas that allow to make sense of the right hand side of these formulas.

The Riemann Zeta function

The L-functions are constructed on the model of the Riemann Zeta function $\zeta(s)$, so let us recall properties of this function.

The **Riemann Zeta function** $\zeta(s)$ is defined on $\mathbb{C}$, for $\mathrm{Re}(s) > 1$, by the formula

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

Euler showed that

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

In particular, Euler's equality provides an alternative proof of the existence of infinitely many prime numbers.

The Riemann Zeta function

Theorem (Riemann)

The Riemann Zeta function $\zeta(s)$ *can be analytical continued to a meromorphic function of the complex plane. Its only pole is at* $s = 1$*, and its residue is 1.*
Moreover, the function Λ *defined by*

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

satisfies the functional equation

$$\Lambda(s) = \Lambda(1 - s).$$

The Gamma function

The function Γ in the previous theorem is defined by

$$\Gamma(s) := \int_0^\infty e^{-t} t^{s-1} dt.$$

It admits a meromorphic continuation to all $\mathbb{C}$ and satisfies the functional equation

$$\Gamma(s+1) = s\Gamma(s).$$

The function $\Gamma(s/2)$ has simple poles at the negative even integers. To compensate these poles we have $\zeta(-2n) = 0$. These are called the **trivial zeros** of $\zeta(s)$.

Conjecture (Riemann Hypothesis)

All the non-trivial zeros of $\zeta(s)$ *satisfy* $Re(s) = 1/2$.

Analytic *L*-functions

Definition

A **Dirichlet series** *is a formal series of the form*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad \textit{where } a_n \in \mathbb{C}.$$

We call an **Euler product** *to a product of the form*

$$F(s) = \prod_p L_p(s).$$

The factors $L_p(s)$ are called the **local Euler factors***.*

An **analytic *L*-function** *is a Dirichlet series that has an Euler product and satisfies a certain type of functional equation.*

Dirichlet characters

A function $\chi : \mathbb{Z} \to \mathbb{C}$ is called a **Dirichlet character** modulo N if there is a group homomorphism $\tilde{\chi} : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ such that

$$\chi(x) = \tilde{\chi}(\, x \pmod{N}) \quad \text{if} \quad (x, N) = 1$$

and

$$\chi(x) = 0 \quad \text{if } (x, N) \neq 1.$$

Moreover, we say that χ is **primitive** if there is no strict divisor $M \mid N$ and a character $\tilde{\chi}_0 : (\mathbb{Z}/M\mathbb{Z})^* \to \mathbb{C}^*$ such that

$$\chi(x) = \tilde{\chi}_0(\, x \pmod{M}) \quad \text{if} \quad (x, M) = 1.$$

In particular, if $N = p$ is a prime every non-trivial character modulo N is primitive. Moreover, any Dirichlet character is induced from a unique primitive character $\tilde{\chi}_0$ as above. We call M its conductor.

Dirichlet L-functions

Definition

We associate to a Dirichlet character χ an L-function given by

$$L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

For example,

$$L(\chi_{-3}, s) = \sum_{n=1}^{\infty} \left(\frac{n}{3}\right) \frac{1}{n^s} = 1 - \frac{1}{2^s} + \frac{1}{4^s} - \frac{1}{5^s} + ...,$$

where the sign is given by the symbol

$$\left(\frac{n}{3}\right) = \begin{cases} 1 & \text{if n is a square mod 3} \\ -1 & \text{if n is not a square mod 3} \\ 0 & \text{if } 3 \mid n \end{cases}$$

Dirichlet L-functions

Let χ be a Dirichlet character. We say that χ is **even** if $\chi(-1) = 1$; we say that χ is **odd** if $\chi(-1) = -1$.

Define also, if χ is even,

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

or, if χ is odd,

$$\Lambda(\chi, s) := \pi^{-(s+1)/2}\Gamma((s+1)/2)L(\chi, s)$$

Dirichlet L-functions

Theorem

Let χ be a primitive Dirichlet character of conductor $N \neq 1$. Then, $L(\chi, s)$ has an extension to $\mathbb{C}$ as an entire function and satisfies the functional equation

$$\Lambda(\chi, s) = \epsilon(\chi) N^{1/2-s} \Lambda(\overline{\chi}, 1-s),$$

where

$$\epsilon(\chi) = \begin{cases} \frac{\tau(\chi)}{\sqrt{N}} & \text{if } \chi \text{ is even} \\ -i\frac{\tau(\chi)}{\sqrt{N}} & \text{if } \chi \text{ is odd} \end{cases}$$

and

$$\tau(\chi) = \sum_{x \pmod N} \chi(x) e^{2i\pi x/N}$$

Elliptic Curves

Definition

An **elliptic curve** *over a field k is a non-singular projective plane curve given by an affine model of the form*

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

where all $a_i \in k$. Write $O = (0:1:0)$ for the point at infinity.

The **change of variables** fixing O are of the form

$$x = u^2x' + r \qquad y = u^3y' + u^2sx' + t,$$

where $u, r, s, t \in \bar{k}$, $u \neq 0$. If $\mathrm{char}(k) \neq 2, 3$, after a change of variables, E can be writen as

$$y^2 = x^3 + Ax + B, \qquad A, B \in k, \quad \Delta(E) = 4A^3 + 27B^2.$$

If $\Delta(E) \neq 0$ then E is **nonsingular**.

Example

Consider the curve

$$E : y^2 = x^3 - 2x + 1,$$

having attached quantities

$$\Delta = 2^4 \cdot 5 \neq 0, \quad j = 2^{11} \cdot 3^3 \cdot 5^{-1}.$$

Another example

Consider the set defined by

$$x + \frac{1}{x} + y + \frac{1}{y} + 1 = 0$$

Multiplication by xy followed by homogenization gives

$$x^2y + yz^2 + y^2x + xz^2 + xyz = 0.$$

Applying the isomorphism $(x, y, z) \mapsto (y, x - y, z - x)$ yelds

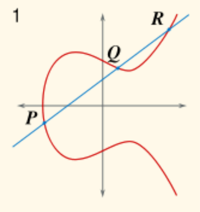
$$x^3 - 2x^2z + xyz - y^2z + xz^2 = 0.$$

After setting $z = 1$ and rearranging we get the elliptic curve with conductor 15 given by

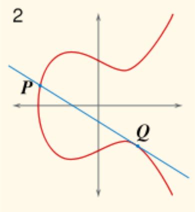
$$y^2 - xy = x^3 - 2x^2 + x.$$

Theorem

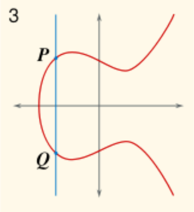
Let E/k be an elliptic curve. There is an abelian group structure on the set of points $E(\bar{k})$.



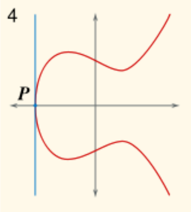
$P + Q + R = 0$



$P + Q + Q = 0$



$P + Q + 0 = 0$



$P + P + 0 = 0$

Theorem (Mordell–Weil)

Let E/k be an elliptic curve over a number field k. The group $E(k)$ is finitely generated.

Example

Consider the curve

$$E : y^2 = x^3 - 2x + 1,$$

having attached quantities

$$\Delta = 2^4 \cdot 5 \neq 0, \quad j = 2^{11} \cdot 3^3 \cdot 5^{-1}.$$

Its rational torsion points are

$$E(\mathbb{Q})_{\mathsf{Tor}} = \{O, (0 : -1 : 1), (0 : 1 : 1), (1 : 0 : 1)\},$$

and they form a cyclic group of order 4.

Reduction modulo p

Let $E/\mathbb{Q}$ be an elliptic curve. There exists a model $E/\mathbb{Z}$ such that $|\Delta(E)|$ is minimal. For such a model and a prime p, we set $\tilde{a}_i = a_i \pmod{p}$ and consider the reduced curve over $\mathbb{F}_p$

$$\tilde{E}: \quad y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6.$$

It can be seen that $\tilde{E}$ has at most one singular point.

Definition (type of reduction)

Let p be a prime. We say that E

- has **good reduction** at p if $\tilde{E}$ is an elliptic curve.
- has **bad multiplicative reduction** at p if $\tilde{E}$ admits a double point with two distinct tangents. We say it is **split** or **non-split** if the tangents are defined over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, respectively.
- has **bad additive reduction** at p if $\tilde{E}$ admits a double point with only one tangent.

The Conductor of an elliptic curve.

Definition

The **conductor** N_E *of an elliptic curve* $E/\mathbb{Q}$ *is an integer. It is computed by Tate's algorithm, and is of the form*

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

where the exponents f_p *satisfy*

$$f_p = \begin{cases} 0 & \textit{if } E \textit{ has good reduction at } p, \\ 1 & \textit{if } E \textit{ has bad multiplicative reduction at } p, \\ 2 & \textit{if } E \textit{ has bad additive reduction at } p \geq 5, \\ 2+\delta_p,\ 0 \leq \delta_p \leq 6 & \textit{if } E \textit{ has bad additive reduction at } p = 2, 3. \end{cases}$$

In particular, $N_E \mid \Delta(E)$ *for the discriminant associated with any model of* E*.*

Example

Consider the curve

$$E : y^2 = x^3 - 2x + 1, \qquad \text{which is a minimal model}$$

having attached quantities

$$\Delta = 2^4 \cdot 5, \quad j = 2^{11} \cdot 3^3 \cdot 5^{-1}.$$

The reduction type at $p = 5$ is bad split multiplicative reduction and at $p = 2$ is bad additive reduction. Furthermore,

$$N_E = 2^3 \cdot 5 = 40$$

Its rational torsion points are

$$E(\mathbb{Q})_{\mathsf{Tor}} = \{O, (0 : -1 : 1), (0 : 1 : 1), (1 : 0 : 1)\} \cong (\mathbb{Z}/4\mathbb{Z})$$

Artin Zeta Function

Let $E/\mathbb{F}_p$ be an elliptic curve given by

$$y^2 + a_1xy + a_3y - x^3 + a_2x^2 + a_4x + a_6 = 0.$$

Consider the associated Dedekind domain

$$A = \mathbb{F}_p[X, Y]/(E)$$

For a non-zero ideal $\mathcal{I}$ of A we define its norm

$$N(\mathcal{I}) = \#(A/\mathcal{I}).$$

The Zeta function associated to A is

$$\zeta_A(s) = \sum_{\mathcal{I} \neq 0} \frac{1}{N(\mathcal{I})^s} = \prod_{\mathcal{P}} \frac{1}{1 - N(\mathcal{P})^{-s}}$$

Definition

For $s \in \mathbb{C}$ such that $Re(s) > 1$, we set

$$\zeta_E(s) = \frac{1}{1 - p^{-s}} \zeta_A(s)$$

Artin Zeta Function

Theorem (Artin)

Let $E/\mathbb{F}_p$ be an elliptic curve and set

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

Then,

$$\zeta_E(s) = \frac{1 - a_E \cdot p^{-s} + p \cdot p^{-2s}}{(1 - p^{-s})(1 - p \cdot p^{-s})}$$

and

$$\zeta_E(s) = \zeta_E(1 - s).$$

The Hasse-Weil L-function of $E/\mathbb{Q}$

Let $E/\mathbb{Q}$ be an elliptic curve. For a prime p of good reduction, let $\tilde{E}$ be the reduction of E mod p, and set

$$L_p(s) = (1 - a_{\tilde{E}} \cdot p^{-s} + p \cdot p^{-2s})^{-1}.$$

Define also Euler factors for primes p of bad reduction by

$$L_p(s) = \begin{cases} (1 - p^{-s})^{-1} & \text{if E has bad split multiplicative reduction at } p \\ (1 + p^{-s})^{-1} & \text{if E has bad non-split mult. reduction at } p, \\ 1 & \text{if E has bad additive reduction at } p. \end{cases}$$

Definition

The L-function of E is defined by

$$L(E, s) = \prod_p L_p(s)$$

A really brief incursion into modular cuspforms

- A modular form is a function on the upper-half plane that satisfies certain transformation and holomorphy conditions.
- Let $N \geq 1$ be an integer. Define

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\}$$

- In particular, a cuspform f for $\Gamma_0(N)$ (of weight 2) admits a Fourier expansion

$$f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^{n/N}, \quad a_n(f) \in \mathbb{C}, \quad q = e^{2\pi i \tau}.$$

- There is a family of Hecke operators $\{T_n\}_{n \geq 1}$ acting on the $\mathbb{C}$-vector space of cuspforms for $\Gamma_0(N)$ of weight 2.
- To a cuspform that is an eigenvector of all T_n we call an **eigenform**. Furthermore, we assume they are **normalized** such that $a_1(f) = 1$.

The L-function of an eigenform

Definition

The L-function attached to an eigenform for $\Gamma_0(N)$ is defined by

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

Theorem

Let f be an eigenform for $\Gamma_0(N)$ of weight 2. The function $L(f,s)$ has an entire continuation to $\mathbb{C}$. Moreover, the function

$$\Lambda_f(s) := (\frac{\sqrt{N}}{2\pi})^{-s}\Gamma(s)L(f,s)$$

satisfies the functional equation

$$\Lambda_f(s) = w\Lambda_f(2-s),$$

where $w = \pm 1$.

Modularity and the L-function of $E/\mathbb{Q}$

Theorem (Wiles, Breuil–Conrad–Diamond–Taylor)

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. There is an eigenform f for $\Gamma_0(N_E)$ (of weight 2) such that

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

Corollary

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Define the function

$$\Lambda_E(s) := (\frac{\sqrt{N_E}}{2\pi})^{-s}\Gamma(s)L(E,s).$$

The function $L(E,s)$ has an entire continuation to $\mathbb{C}$ and $\Lambda_E(s)$ satisfies

$$\Lambda_E(s) = w\Lambda_E(2-s),$$

where $w = \pm 1$.

Example

Consider the curve

$$E : y^2 = x^3 - 2x + 1, \quad \Delta = 2^4 \cdot 5 \neq 0, \quad j = 2^{11} \cdot 3^3 \cdot 5^{-1}.$$

It has conductor $N_E = 2^3 \cdot 5 = 40$.The cuspform of weight 2 for $\Gamma_0(40)$ corresponding to E by modularity is

$$f := q + q^5 - 4q^7 - 3q^9 + O(q^{10}).$$

The rational torsion points are

$$E(\mathbb{Q})_{\mathsf{Tor}} = \{O, (0 : -1 : 1), (0 : 1 : 1), (1 : 0 : 1)\} \cong (\mathbb{Z}/4\mathbb{Z})$$

The BSD conjecture

Theorem (Mordell–Weil)

Let $E/\mathbb{Q}$ be an elliptic curve. Then the group $E(\mathbb{Q})$ is finitely generated. More precisely,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{Tor} \oplus \mathbb{Z}^{r_E}$$

Conjecture (Birch–Swinnerton-Dyer)

The rank r_E of the Mordell-Weil group of an elliptic $E/\mathbb{Q}$ is equal to the order of the zero of $L(E, s)$ at $s = 1$.

Example

Consider the curve

$$E : y^2 = x^3 - 2x + 1, \quad \Delta = 2^4 \cdot 5 \neq 0, \quad j = 2^{11} \cdot 3^3 \cdot 5^{-1}.$$

It has conductor $N_E = 2^3 \cdot 5 = 40$. The cuspform of weight 2 for $\Gamma_0(40)$ corresponding to E by modularity is

$$f := q + q^5 - 4q^7 - 3q^9 + O(q^{10}).$$

The rational torsion points are

$$E(\mathbb{Q})_{\mathrm{Tor}} = \{O, (0 : -1 : 1), (0 : 1 : 1), (1 : 0 : 1)\} \cong (\mathbb{Z}/4\mathbb{Z})$$

Moreover, the rank $r_E = 0$ since the function $L(E, s)$ satisfies

$$L(E, 1) = 0.742206236711.$$

Thus $E(\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})$.

Counting Points on Varieties

Let $V/\mathbb{F}_q$ be a projective variety, given by the set of zeros

$$f_1(x_0, \ldots, x_N) = \cdots = f_m(x_0, \ldots, x_N) = 0$$

of a collection of homogeneous polynomials. The number of points in $V(\mathbb{F}_{q^n})$ is encoded in the zeta function

Definition

The **Zeta function** *of $V/\mathbb{F}_q$ is the power series*

$$Z(V/\mathbb{F}_q; T) := \exp(\sum_{n \geq 1} \# V(\mathbb{F}_{q^n}) \frac{T^n}{n})$$

The Zeta function of the Projective space

Let $N \geq 1$ and $V = \mathbb{P}^N$. A point in $V(\mathbb{F}_{q^n})$ is given by homogeneous coordinates $(x_0 : .. : x_N)$ with x_i not all zero. Two choices of coordinates give the same point if they differ by multiplication of a non-zero element in $\mathbb{F}_{q^n}$. Hence,

$$\#V(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni} \qquad \text{so}$$

$$\log Z(V/\mathbb{F}_q; T) = \sum_{n=0}^{\infty} (\sum_{i=0}^{N} q^{ni}) \frac{T^n}{n} = \sum_{i=0}^{N} -\log(1 - q^i T).$$

Thus,

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

The Zeta function of $E/\mathbb{F}_p$

Theorem

Let $E/\mathbb{F}_p$ be an elliptic curve and define

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

Then,

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

Moreover,

$$1 - a_E T + pT^2 = (1-\alpha)(1-\beta) \quad \textit{with} \quad |\alpha| = |\beta| = \sqrt{p}$$

Note that by setting $T = p^{-s}$ we obtain the equality

$$Z(E/\mathbb{F}_p; p^{-s}) = \zeta_E(s)$$

Example

Consider the curve $E : y^2 = x^3 - 2x + 1$ which has bad additive reduction at 2.
Let $p = 2$. Its mod p reduction is given by

$$\tilde{E}_2 : (y-1)^2 = x^3$$

and satisfies $\#\tilde{E}_2(\mathbb{F}_{2^n}) = 2^n + 1$. Hence,

$$\begin{aligned} \log Z(\tilde{E}_2/\mathbb{F}_{2^n}; T) &= \sum_{n=1}^{\infty} \frac{2^n+1}{n} T^n \\ &= \log(\frac{1}{1-2T}) + \log(\frac{1}{1-T}) \end{aligned}$$

Thus,

$$Z(\tilde{E}_2/\mathbb{F}_{2^n}; T) = \frac{1}{(1-2T)(1-T)}$$

Bibliography

- C.J. Smyth, *On measures of polynomials in several variables,* Bull. Austral. Math. Soc. **23** (1981), 49–63;
- C. Deninger, *Deligne periods of mixed motives, K-theory and the entropy of certain $\mathbb{Z}^n$-actions*, J. Amer. Math. Soc. **10**:2 (1997), 259–281;
- J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer, 1986;
- F. Diamond and J. Shurman, *A First Course on Modular Forms*, GTM **228**, Springer, 2005;