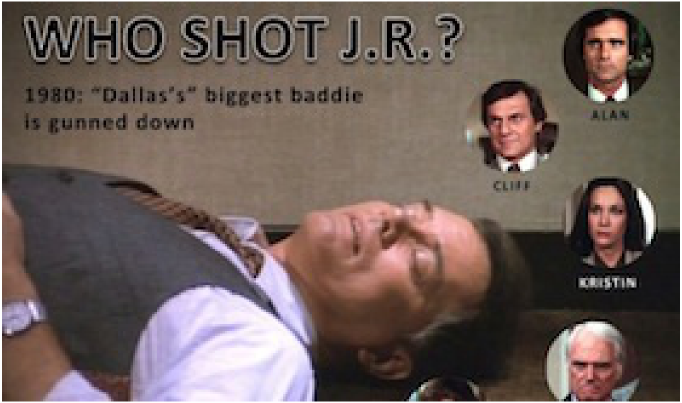
Introduction to L-functions: The Artin Cliffhanger...



Artin L-functions

- Let K/k be a Galois extension of number fields, V a finite-dimensional $\mathbb{C}$-vector space and (ρ, V) be a representation of $\mathrm{Gal}(K/k)$.
- (unramified) If $\mathfrak{p} \subset k$ is unramified in K and $\mathfrak{p} \subset \mathfrak{P} \subset K$, put

$$L_{\mathfrak{p}}(s,\rho) = \det{}^{-1}\left(I_V - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho\left(\sigma_{\mathfrak{P}}\right)\right).$$

  Depends only on conjugacy class of $\sigma_{\mathfrak{P}}$ (i.e., only on $\mathfrak{p}$), not on $\mathfrak{P}$.
- (general) If G acts on V and H subgroup of G, then

$$V^H = \{v \in V : h(v) = v, \forall h \in H\}.$$

  With $\rho|_{V^{I_{\mathfrak{P}}}} : \mathrm{Gal}(K/k) \to GL\left(V^{I_{\mathfrak{P}}}\right)$.

$$L_{\mathfrak{p}}(s,\rho) = \det{}^{-1}\left(I - N_{k/\mathbb{Q}}(\mathfrak{p})^{-s}\rho|_{V^{I_{\mathfrak{P}}}}\left(\sigma_{\mathfrak{P}}\right)\right).$$

Definition

For $\mathrm{Re}(s) > 1$, the **Artin L-function** belonging to ρ is defined by

$$L(s,\rho) = \prod_{\mathfrak{p} \subset k} L_{\mathfrak{p}}(s,\rho).$$

Artin's Conjecture

Conjecture (Artin's Conjecture)

If ρ is a non-trivial irreducible representation, then $L(s,\rho)$ has an analytic continuation to the whole complex plane.

- We can prove meromorphic.
- Proof.
  (1) Use Brauer's Theorem:

$$\chi = \sum_i n_i \mathrm{Ind}\left(\chi_i\right),$$

with χ_i one-dimensional characters of subgroups and $n_i \in \mathbb{Z}$.
(2) Use Properties (4) and (5).
(3) $L\left(s,\chi_i\right)$ is meromorphic (Hecke L-function).

Introduction to L-functions: Hasse-Weil L-functions

Paul Voutier

CIMPA-ICTP Research School,
Nesin Mathematics Village
June 2017

A "formal" zeta function

- Let N_m, $m = 1, 2, \ldots$ be a sequence of complex numbers.

$$Z(u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m u^m}{m}\right)$$

- With some sequences, if we have an Euler product, this does look more like zeta functions we have seen.
  Let's see how...

Local zeta function

- Let F be a field and let $f(\mathbf{x}) \in F[x_0, \ldots, x_n]$ be a homogeneous polynomial (all monomials have same total degree).
  Let $V_f(F)$ be the set of F-points in $\mathbb{P}^n(F)$.
- Let $q = p^r$, then there is a unique field $\mathbb{F}_q$ containing $\mathbb{Z}/p\mathbb{Z}$.
  For any positive integer m, there is a unique field $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$.
- Let N_m be the number of points in $V_f(\mathbb{F}_{q^m})$.
- $$Z_{f,q}(u) = \exp\left(\sum_{m=1}^{\infty} \frac{|V_f(\mathbb{F}_{q^m})|\, u^m}{m}\right),$$
  called the local or congruence zeta function of f.
  More generally, we consider $Z_{V,q}(u)$ for any variety V defined over $\mathbb{F}_q$.

Examples

- A single point: $n = 1$ and $f = x_1$. $V_f = \{[1,0]\}$, so $N_m = 1$ and

$$Z_{f,q}(u) = \exp\left(\sum_{m=1}^{\infty} \frac{u^m}{m}\right) = \exp\left(-\log(1-u)\right) = \frac{1}{1-u}.$$

- A projective line: $n = 2$ and $f = x_1$.
  $V_f = \{[f,0,1] : f \in \mathbb{F}_{q^m}\} \cup \{[1,0,0]\}$, so $N_m = q^m + 1$ and

$$Z_{f,q}(u) = \exp\left(\sum_{m=1}^{\infty} \frac{(qu)^m}{m}\right) \exp\left(\sum_{m=1}^{\infty} \frac{u^m}{m}\right) = \frac{1}{(1-u)(1-qu)}.$$

- Notice that both of these are rational functions of u.
- There is a deep conjecture of Tate relating the order of the pole at $u = q^{-1}$ to the geometry of the hypersurface.

Example (Elliptic Curves)

- Elliptic curve, E, defined over $\mathbb{F}_q$:

$$Z_{E,q}(u) = \frac{1 - a_{E,q}u + qu^2}{(1-u)(1-qu)},$$

  where $a_{E,q} = q + 1 - N_1$.
- Hasse: $|a_{E,q}| \leq 2\sqrt{q}$.
- Write $1 - a_{E,q}u + qu^2 = (1 - \alpha u)(1 - (q/\alpha)u)$.
  $N_m = q^m + 1 - \alpha^m - (q/\alpha)^m$.
  Special case: $N_1 = q + 1 - \alpha - q/\alpha$ (so we can determine α from N_1).
  Thus from N_1 we can obtain N_m for all m.
- α is a quadratic imaginary algebraic number.

$$|\alpha| = q^{1/2}.$$

  Isn't $1/2$ important for roots of other zeta functions too...?

History

- Artin: introduced these zeta functions. Hyperelliptic curves: $y^2 = f(x)$. (1923) his thesis!! (no pressure. . .)
- For many elliptic curves, he proved that $|\alpha| = q^{1/2}$.
  An analogue of the Riemann hypothesis.
- Hasse (1934):
  This Riemann hypothesis holds for all elliptic curves.
- Weil (1948):
  Proved a generalisation for all nonsingular curves.

  Weil did much more too, but first some other guy. . .

  Fast Fourier transform, least squares, find lost asteroids,. . .
  Gauss.

Weil

Weil proved the following for smooth projective curves, $\mathcal{C}$, over $\mathbb{F}_q$.

- $$Z_{\mathcal{C},q}(u) = \frac{P(u)}{(1-u)(1-qu)},$$

  where $P(u) \in \mathbb{Z}[u]$ with constant coefficient 1.
  If $\mathcal{C}$ is the reduction mod p of a variety, $\tilde{\mathcal{C}}$, over $\mathbb{Q}$, then $\deg(P) = 2g$, g is the genus (or Betti number) of $\tilde{\mathcal{C}}$.
- If α is a reciprocal root of P, then $|\alpha| = q^{1/2}$.

Key Point

The geometry of the object over the complex numbers is connected with its arithmetic properties.

Weil Conjectures (1949)

V a non-singular n-dimensional projective algebraic variety over $\mathbb{F}_q$.

- (Rationality) $Z_V(u)$ is a rational function of u. More precisely,

$$\frac{P_1(u)\cdots P_{2n-1}(u)}{P_0(u)\cdots P_{2n}(u)},$$

where each $P_i(u) \in \mathbb{Z}[u]$ with $P_0(u) = 1 - u$, $P_{2n}(u) = 1 - q^n u$, and

$$P_i(u) = \prod_j (1 - \alpha_{i,j} u) \quad \text{for } i = 1, \ldots, 2n-1.$$

- (Riemann hypothesis) For all $1 \le i \le 2n-1$ and all j,

$$|\alpha_{i,j}| = q^{i/2}$$

- (Functional equation) Let E be the Euler characteristic of V.

$$Z_V\left(q^{-n}u^{-1}\right) = \pm q^{\frac{nE}{2}} u^E Z_V(u),$$

- (Betti numbers) If V is a (good) reduction mod p of a non-singular projective variety $\tilde{V}$ defined over a number field, then the degree of P_i is the i-th Betti number of the space of complex points of $\tilde{V}$.

Weil Conjectures (Status)

All proven!

- (Rationality) Dwork (1959): rationality holds much more generally. For any algebraic set. Non-singular condition not needed.
- (Functional equation) Grothendieck (1965).
- (Betti numbers) Grothendieck (1965).
- (Riemann hypothesis) This was the hardest one. Finally proven by Deligne in 1974.
- Key motivation for modern development of algebraic geometry.

Euler Product (I)

- Do what we do before with local factors.
  E.g., recall that for a single point, $Z(u) = 1/(1-u)$. So
  $$\prod_p Z\left(p^{-s}\right) = \prod_p \left(1 - p^{-s}\right)^{-1} = \zeta(s).$$
  So "strange" initial definition fits with our previous examples.
- Restrict now to curves.

$$\begin{aligned} L_{\mathcal{C}}(s) &= \frac{\zeta(s)\zeta(s-1)}{\prod_p Z_{\mathcal{C},p}\left(p^{-s}\right)} = \prod_p \left(P\left(p^{-s}\right)\right)^{-1} \\ &= \prod_p \left(1 + b_1 p^{-s} + \cdots + b_{2g} p^{-2gs}\right)^{-1} \\ &= \prod_p \left(1 - \alpha_{1,1} p^{-s}\right)^{-1} \cdots \left(1 - \alpha_{1,2g} p^{-s}\right)^{-1}. \end{aligned}$$

Euler Product (ζ vs L vs ...)

- ζ: $\zeta_V(s) = \prod_p Z_{V,p}(p^{-s})$.
- L-function: from Weil conjectures, $Z_{V,p}(T)$ is a product of terms. For good primes,

$$L_p\left(H^j(V), s\right) = \det\left(I - \mathrm{Frob}_p p^{-s} | H^j(V)\right)^{-1} \quad \text{j=0,...,2n.}$$

  For bad primes,

$$L_p\left(H^j(V), s\right) = \det\left(I - \mathrm{Frob}_p p^{-s} | H^j(V)^{I_p}\right)^{-1} \quad \text{j=0,...,2n.}$$

  L-function definition:

$$L\left(H^j(V), s\right) = \prod_p L_p\left(H^j(V), s\right) \quad \text{j=0,...,2n.}$$

- The connection between them:

$$\zeta_V(s) = \prod_{j=0}^{2n} L\left(H^j(V), s\right)^{(-1)^j}.$$

  For curves: we use $L_V(s)$ for $L\left(H^1(V), s\right)$.

Elliptic Curves: local zeta function

- Elliptic curve, E, defined over $\mathbb{F}_q$, with discriminant, Δ_E:

$$Z_{E,q}(u) = \frac{1 - a_{E,q}u + qu^2}{(1-u)(1-qu)}.$$

- E is an elliptic curve over $\mathbb{F}_q$ only if $p \nmid \Delta_E$ (good reduction).
- $p|\Delta_E$. Three kinds of bad reduction can happen.
  (1) E mod q has a cusp (a double point with one tangent), so $a_{E,q} = 0$.
  Also called **additive reduction**.
  (2) E mod q has a node with a pair of tangents in $\mathbb{F}_q$, so $a_{E,q} = 1$.
  Also called **split multiplicative reduction**.
  (3) E mod q has a node with a pair of tangents in a quadratic extension of $\mathbb{F}_q$, so $a_{E,q} = -1$.
  Also called **nonsplit multiplicative reduction**.
  For any bad reduction, we have

$$Z_{E,q}(u) = \frac{1 - a_{E,q}u}{(1-u)(1-qu)}.$$

Elliptic Curves: Hasse-Weil L-function

- Hasse-Weil L-function:

$$L_E(s) = \prod_{p \mid \Delta_E} \left(1 - a_{E,p} p^{-s}\right)^{-1} \prod_{p \nmid \Delta_E} \left(1 - a_{E,p} p^{-s} + p p^{-2s}\right)^{-1}$$

- Exercise: $L_E(s)$ converges and is analytic for all $\mathrm{Re}(s) > 3/2$.

Conjecture

Let E be an elliptic curve defined over any number field K. $L_E(s)$ has an analytic continuation to the entire complex plane and satisfies a functional equation relating its values at s and $2 - s$.

- Eichler and Shimura (independently) proved that this is true for elliptic curves defined over $\mathbb{Q}$ with a "modular parametrisation".

Theorem (Modularity Theorem, Wiles and others)

Every elliptic curve defined over $\mathbb{Q}$ has a modular parametrisation.

- The conjecture holds for all elliptic curves defined over $\mathbb{Q}$.

- Let E be an elliptic curve defined over $\mathbb{Q}$.
  Complete L-function

$$\Lambda_E(s) = \underbrace{N_E^{s/2}(2\pi)^{-s}\Gamma(s)}_{\text{local factor at infinity}} L_E(s),$$

  $N_E \in \mathbb{Z}$ is the **conductor** – a more refined version of discriminant.
- $\Lambda_E(s)$ is an entire function satisfying

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

  where $w = \pm 1$ is the **sign of the functional equation**.
  Parity conjecture: w determines the parity of $\mathrm{ord}_{s=1}(L_E(s))$.

Birch Swinnerton-Dyer: Statement

Tate (1974)

This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite!

Conjecture (Birch Swinnerton-Dyer)

Let E be an elliptic curve over $\mathbb{Q}$.
(a) *$L_E(s)$ has a zero at $s = 1$ of order equal to the rank, r, of $E(\mathbb{Q})$.*
(b)

$$\lim_{s \to 1} \frac{L_E(s)}{(s-1)^r} = \frac{2^r |\text{Ш}| R}{|E_{tors}(\mathbb{Q})|^2} (\text{local factors}).$$

Ш – Tate-Shafarevich group, an analogue of the ideal class group. The obstruction group to local-global principle.
R – the elliptic regulator.

Birch Swinnerton-Dyer: Status

- Known results for elliptic curves over $\mathbb{Q}$:

$$\begin{aligned} L_E(1) \neq 0 \quad & \Longrightarrow \mathrm{rank}(E(\mathbb{Q})) = 0, \\ L_E(1) = 0 \text{ and } L'_E(1) \neq 0 \quad & \Longrightarrow \mathrm{rank}(E(\mathbb{Q})) = 1. \end{aligned}$$

  Kolyvagin and Gross-Zagier (plus modularity).
- Bhargava and Shanker: average rank ≤ 0.885.
  Bhargava, Skinner, Zhang: B-SD(a) is true for $> 66\%$ of elliptic curves.
- conjecture: 50% of curves have rank 0 and 50% have rank 1.

Conjecture

All but finitely many $E/\mathbb{Q}$ have rank at most 21.
All $E/\mathbb{Q}$ have rank at most 28.