

Function fields: Basics

Douglas Ulmer
University of Arizona

June 3, 2006

Number fields

$$\mathbb{Q}$$

$$\mathbb{Z}$$

p (positive) prime

$$\mathfrak{p} = (p) \subset \mathbb{Z}$$

$$\mathbb{Z}/\mathfrak{p} = \mathbb{F}_p$$

$$N \mathfrak{p} = p$$

Function fields

$$F = \mathbb{F}_q(t)$$

$$R = \mathbb{F}_q[t]$$

f (monic) irreducible

$$\mathfrak{p} = (f) \subset R$$

R/\mathfrak{p} finite field with $q^{\deg f}$ elements

$$N \mathfrak{p} = q^{\deg f}$$

Number fields

$$|\rho^a \frac{m}{n}|_{\mathfrak{p}} = \rho^{-a} \text{ (non-arch)}$$

$$|x|_{\infty} = \text{usual } |x| \text{ (arch)}$$

Function fields

$$|f^a \frac{g}{h}|_{\mathfrak{p}} = q^{-a \deg f} \text{ (non-arch)}$$

$$|\frac{g}{h}|_{\infty} = q^{\deg g - \deg h} \text{ (non-arch)}$$

Every absolute value on \mathbb{Q} or F is (equivalent to) one of these. For general global fields (finite extensions of \mathbb{Q} or F) absolute values are more convenient than ideals.

The (Dedekind) zeta function of F is defined by the usual Euler product:

$$\zeta_F(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$$

The product converges absolutely in $\Re s > 1$, has a meromorphic continuation (poles at $s = 0, 1$), satisfies a functional equation for $s \rightarrow 1 - s$.

In fact, $\zeta_F(s)$ is pretty trivial from an analytic point of view:

$$\zeta_F(s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})}$$

RH is trivial here: $\zeta_F(s)$ has no zeroes!

Exercise: Check displayed equation. (It's easier if you take the log of ζ .)

Let K/F be a quadratic extension, say $K = F(\sqrt{h})$ with $h \in R$ square-free. Define χ by

$$\chi(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } K \\ -1 & \text{if } \mathfrak{p} \text{ is inert in } K \\ 0 & \text{if } \mathfrak{p} \text{ ramifies in } K \end{cases}$$

Define

$$L(\chi, s) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p}) N \mathfrak{p}^{-s})^{-1}$$

Converges absolutely in $\Re s > 1$, has an analytic continuation to all s , satisfies a functional equation for $s \rightarrow 1 - s$.

RH: Zeroes of $L(\chi, s)$ lie on $\Re s = 1/2$

In fact, $L(\chi, s)$ is a polynomial in q^{-s} :

$$L(\chi, s) = P(q^{-s})$$

where $P(T) \in \mathbb{Z}[T]$ has degree $2g = \deg h - 1$ ($\deg h$ odd) or $\deg h - 2$ ($\deg h$ even).

Note that $L(\chi, s)$ is periodic with period $2\pi i / \log q$ and up to periodicity it has only finitely many zeroes.

Exercise: The functional equation is $\Lambda(s) = q^{gs} L(\chi, s) = \Lambda(1 - s)$.
What does this say about the polynomial P ?

Let's consider an elliptic curve over $F = \mathbb{F}_q(t)$, say defined by

$$y^2 = x^3 + ax + b \quad a, b \in R = \mathbb{F}_q[t]$$

where $\Delta = -16(4a^3 + 27b^2) \neq 0$ and $j = 2 \cdot 3 \cdot a^3 / \Delta \notin \mathbb{F}_q$. Reduce mod $\mathfrak{p} \subset R$ and count points:

$$\#E(R/\mathfrak{p}) = N\mathfrak{p} + 1 - a_{\mathfrak{p}}$$

Define the L -function:

$$L(E, s) = \prod_{\text{good } \mathfrak{p}} (1 - a_{\mathfrak{p}} N \mathfrak{p}^{-s} + N \mathfrak{p}^{1-2s})^{-1} \prod_{\text{bad } \mathfrak{p}} (\dots)^{-1}$$

The product converges absolutely in $\Re s > 3/2$, extends analytically to all s , and satisfies a functional equation for $s \rightarrow 2 - s$. Its zeroes lie on $\Re s = 1$. It turns out that $L(E, s)$ is a polynomial in q^{-s} whose degree can be computed in term of the bad reduction of E .

Upshot: All the L -functions you know about over number fields have analogues over function fields. They are rational functions in q^{-s} and have good analytic properties (analytic continuation, functional equation, RH).

Let F be a function field. Consider $\text{Gal}(\overline{F}/F)$. For each place \mathfrak{p} of F , it has a decomposition group $D_{\mathfrak{p}}$ (well-defined up to conjugation), an inertia group $I_{\mathfrak{p}} \subset D_{\mathfrak{p}}$ and Frobenius element $Fr_{\mathfrak{p}}$ generating $D_{\mathfrak{p}}/I_{\mathfrak{p}}$.

All the L -functions above are related to representations of $\text{Gal}(\overline{F}/F)$. Let $\sigma : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_r(\mathbb{Q}_{\ell})$ be a continuous homomorphism. We say that σ is unramified at \mathfrak{p} if $\sigma(I_{\mathfrak{p}}) = \{id\}$. In this case, $\sigma(Fr_{\mathfrak{p}})$ is well-defined up to conjugation.

The L -function of a representation $\sigma : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_r(\mathbb{Q}_\ell)$ is given by the scary formula

$$L(\sigma, s) = \prod_{\mathfrak{p}} \det(1 - \sigma(Fr_{\mathfrak{p}}) N_{\mathfrak{p}}^{-s} |(\mathbb{Q}_\ell^r)^{I_{\mathfrak{p}}})^{-1}$$

As a first example, when σ is the trivial representation, we get the ζ -function.

Let K/F be a quadratic extension. We have a corresponding quotient $\sigma : \text{Gal}(\overline{F}/F) \rightarrow \text{Gal}(K/F) = \{\pm 1\}$. The connection with the Dirichlet character χ is that

$$\chi(\mathfrak{p}) = \sigma(Fr_{\mathfrak{p}})$$

for all \mathfrak{p} where σ is unramified. So the general formula on the last slide gives back the L -function attached to K :

$$L(\sigma, s) = L(\chi, s)$$

In the elliptic curve case, $\text{Gal}(\overline{F}/F)$ acts on the ℓ -power torsion points of E :

$$V_\ell(E) = (\varprojlim_m E[\ell^m]) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^2$$

and $\sigma : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}(V_\ell(E)) \cong \text{GL}_2(\mathbb{Q}_\ell)$.

For good \mathfrak{p} , the local factor is

$$\det(1 - \sigma(Fr_{\mathfrak{p}}) N \mathfrak{p}^{-s} | V_\ell(E)) = (1 - a_{\mathfrak{p}} N \mathfrak{p}^{-s} + N \mathfrak{p}^{1-2s})$$

(and “the bad factors are good”) so $L(\sigma, s) = L(E, s)$.

The heavy machine of ℓ -adic cohomology “computes” L -functions as reversed characteristic polynomials. For a continuous representation $\sigma : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_r(\mathbb{Q}_\ell)$, we have cohomology groups $H^i(\sigma)$ ($i = 0, 1, 2$) which are finite dimensional \mathbb{Q}_ℓ -vector spaces with an action of the q -power Frobenius Fr_q . Then the main result is

$$L(\sigma, s) = \frac{\det(1 - Fr_q q^{-s} | H^1(\sigma))}{\det(1 - Fr_q q^{-s} | H^0(\sigma)) \det(1 - Fr_q q^{-s} | H^2(\sigma))}$$

For example, when $F = \mathbb{F}_q(t)$ and σ is trivial, $H^0(\sigma) = \mathbb{Q}_\ell$ with trivial Fr_q action, $H^1(\sigma) = 0$, and $H^2(\sigma) = \mathbb{Q}_\ell$ with Fr_q acting by multiplication by q . So we recover

$$\begin{aligned}
 L(\sigma, s) &= \frac{\det(1 - Fr_q q^{-s} | H^1(\sigma))}{\det(1 - Fr_q q^{-s} | H^0(\sigma)) \det(1 - Fr_q q^{-s} | H^2(\sigma))} \\
 &= \frac{1}{(1 - q^{-s})(1 - q^{1-s})}
 \end{aligned}$$

For most σ (e.g., those associated to quadratic extensions or elliptic curves), $H^0(\sigma) = H^2(\sigma) = 0$ and so

$$L(\sigma, s) = \det(1 - Fr_q q^{-s} | H^1(\sigma))$$

and $L(\sigma, s)$ is a polynomial in q^{-s} . This shows that it has an analytic continuation to an entire function of s . The functional equation is related to Poincaré duality and RH is a statement about the size of the eigenvalues of Fr_q .

Upshot: For most representations σ , there is a matrix A (the action of Fr_q on $H^1(\sigma)$) such that $L(\sigma, s)$ is the reversed characteristic polynomial of $q^{-s}A$.

When the representation σ is self-dual (i.e., it admits a non-degenerate equivariant pairing), then the cohomology group $H^1(\sigma)$ is also self-dual, but of the opposite sign. In other words, a symmetric pairing on σ induces a skew-symmetric pairing on $H^1(\sigma)$ and a skew-symmetric pairing on σ induces a symmetric pairing on $H^1(\sigma)$.

For example, when $\sigma : \text{Gal}(\overline{F}/F) \rightarrow \{\pm 1\}$ is the character associated to a quadratic extension of F , σ has an obvious symmetric pairing and so $H^1(\sigma)$ has a skew-symmetric pairing. Thus the matrix A that calculates the quadratic Dirichlet L -function $L(\chi, s)$ is (a scalar multiple of) a *symplectic* matrix.

The representation $\sigma : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}(V_\ell(E))$ attached to an elliptic curve has a skew-symmetric pairing (the Weil pairing) and so $H^1(\sigma)$ has a symmetric pairing. Thus the matrix A that calculates the elliptic curve L -function $L(E, s)$ is (a scalar multiple of) an *orthogonal* matrix.

The L -functions we are considering vary in families. For example, quadratic extensions K of F have the form $K = F(\sqrt{h})$ with $h \in \mathbb{F}_q[t]$ square-free. We can vary h and get an infinite family of L -functions $L(\chi_h, s)$.

For elliptic curves, we consider E defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_q[t]$ with $\Delta = -16(4a^3 + 27b^2) \neq 0$. Varying a and b , we get an infinite collection of L -functions $L(E_{a,b}, s)$.

For both families we can ask how the zeroes of these L -functions vary in the family.

In order to make statistical statements about, say, low-lying zeroes in a family of L -functions, we should order the family, or more generally, write the family as a union of finite sets of L -functions, then take a limit.

In the case of quadratic extension L -functions, we could look at fields $K_h = F(\sqrt{h})$ for $h \in \mathbb{F}_q[t]$ of bounded degree and form the corresponding $L(\chi_h, s)$. Since there are only finitely many $h \in \mathbb{F}_q[t]$ of degree $\leq D$, we get finitely many L -functions for each D .

Similarly, if we look at $a, b \in \mathbb{F}_q[t]$ of bounded degree, we get finitely many elliptic curves $E_{a,b}$ with L -functions $L(E_{a,b}, s)$.

Continuing with the example of quadratic L -functions, for each h we have a symplectic matrix A_h such that $L(\chi_h, s)$ is the reversed characteristic polynomial of $q^{1/2-s}A_h$. The size of A_h is $\deg h - 1$ or $\deg h - 2$. So for each degree bound D we get finitely many symplectic matrices (roughly q^D of them) of size approximately D . One can then make conjectures about low-lying zeroes, pair correlations, etc., which amount to conjectures about the eigenvalues of the A_h . All of these conjectures are wide open.

Katz and Sarnak had the idea of changing the problem so that one gets infinitely many matrices in a group of finite size (and one can prove things).

Specifically, fix a degree D and for each positive integer n consider square-free polynomials $h \in \mathbb{F}_{q^n}[t]$ of degree $\leq D$. The number of such h is asymptotic to q^{nD} as $n \rightarrow \infty$. For each h we have a matrix A_h in a symplectic group of size roughly D . We let n tend to infinity and ask how the A_h are distributed in this symplectic group.

Similarly, taking $a, b \in \mathbb{F}_{q^n}[t]$ of bounded degree, we have matrices $A_{a,b}$ all in an orthogonal group of a fixed size. Letting n tend to ∞ , we can ask how these matrices are distributed.

Katz and Sarnak, building on work of Deligne on the Weil conjectures, showed that as $n \rightarrow \infty$, the A_h become equidistributed in the symplectic group as $n \rightarrow \infty$. Similarly, the matrices $A_{a,b}$ computing elliptic curve L -functions become equidistributed in the orthogonal group as $n \rightarrow \infty$.

In the next lecture I will explain what this means and give some idea about how to prove it.