Analytic Number Theory in Function Fields (Lecture 7)

Julio Andrade

j.c.andrade.math@gmail.com
http://julioandrade.weebly.com/

University of Oxford

TCC Graduate Course
University of Oxford, Oxford
01 May 2015 - 11 June 2015

Content

Introduction

In this lecture we will study some mean values of L-functions over function fields.

- Average values of the class number over $\mathbb{F}_q(T)$.
- Mean values of L-functions at the central point.

In his famous work *Disquisitiones Mathematicae*, C.F. Gauss considered the arithmetic of binary quadratic forms $ax^2 + 2bxy + cy^2$ defined over the integers $\mathbb{Z}$.

The discriminant of such a form is by definition $D = 4b^2 - 4ac$. He defined an equivalence between such forms and showed that equivalent forms have the same discriminant. Moreover, he showed that the number of equivalence classes o forms with the same discriminant is finite. Call that number h_D.

Based on extensive numerical evidence he made two conjectures about the average value of these class numbers h_D.

Conjecture

1. *Let $D = -4k$ vary over all negative even discriminants with $1 \leq k \leq N$. Then*
$$\sum_{1 \leq k \leq N} h_D \sim \frac{4\pi}{21\zeta(3)} N^{3/2}.$$
2. *Let $D = 4k$ vary over all positive even discriminants such that $1 \leq k \leq N$. Then*
$$\sum_{1 \leq k \leq N} h_D R_D \sim \frac{4\pi^2}{21\zeta(3)} N^{3/2}.$$

The number R_D in the second conjecture is closely related to the regulator of the real quadratic number field $\mathbb{Q}(\sqrt{D})$. In fact, the both conjectures can be reformulated in terms of orders $\mathcal{O}$ in quadratic number fields where the class number h are interpreted in terms of the size of the Picard group of $\mathcal{O}$, $\mathrm{Pic}(\mathcal{O})$, i.e., invertible fractional ideals of $\mathcal{O}$ modulo principal ideals.

Both of these conjectures have been proved.

We will consider the function field analogue of Gauss's conjectures. As usual, instead of $\mathbb{Z}$ and $\mathbb{Q}$ we consider the pair $A = \mathbb{F}_q[T]$ and $k = \mathbb{F}_q(T)$. For the remainder of this lecture, we assume that the characteristic of $\mathbb{F}$ is odd.
Let $m \in A$ be any non-square polynomial, and consider the quadratic function field $K = k(\sqrt{m})$. Write $m = m_0 m_1^2$, where m_0 is square-free. The polynomial m_0 is well defined up to the square of a constant. Define $\mathcal{O}_m$ to be the ring $A + A\sqrt{m} \subset K$. It is an A-order, i.e., it is a ring, finitely generated as an A-module, and its quotient field is K.

Proposition

With the notations introduced above, the integral closure of A in K is $\mathcal{O}_{m_0}$. The ring $\mathcal{O}_m$ is a subring of $\mathcal{O}_{m_0}$ and the polynomial m_1 is a generator of the annihilator of the A-module $\mathcal{O}_{m_0}/\mathcal{O}_m$. Finally, if O is any A-order in K, then $\mathcal{O} = \mathcal{O}_m$ for some $m \in A$.

Definition

Let $m \in A$, m not a square, and let $\mathcal{O}_m \subset k(\sqrt{m})$ be the A-order described above. $Pic(\mathcal{O}_m)$, the Picard group of $\mathcal{O}_m$, is the group of invertible fractional ideals of $\mathcal{O}_m$ modulo the subgroup of principal fractional ideals. The class number h_m is defined to be the cardinality of this group.

Definition

If $m \in A$, m a non-square, define $\chi_m(a)$ as follows:

$$\chi_m(a) = \left(\frac{m}{a}\right)_2.$$

Recall that if P is irreducible, then $\chi_m(P) = 0$ if $P \mid m$, and if $P \nmid m$ then $\chi_m(P) = 1$ if m is a square modulo P and -1 otherwise. If a is a product of irreducibles one extends $\chi_m(P)$ by multiplicativity, i.e., if $a = \prod_{i=1}^{t} P_i$, then $\chi_m(a) = \prod_{i=1}^{t} \chi_m(P_i)$.

If $m = m_0 m_1^2$ we have $\chi_m(a) = \chi_{m_0}(a)$ whenever $(a, m) = 1$. However, if P is an irreducible such that $P \mid m_1$ and $P \nmid m_0$, then we have $\chi_m(P) = 0$, whereas $\chi_{m_0}(P) \neq 0$.

Define $L(s, \chi_m)$ as follows:

$$L(s, \chi_m) = \sum_{n \text{ monic}} \frac{\chi_m(n)}{|n|^s} = \prod_{P \nmid m} \left(1 - \frac{\chi_m(P)}{|P|^s}\right)^{-1}.$$

Notice that if $m = m_0 m_1^2$, we have

$$L(s, \chi_m) = \prod_{P | m_1} \left(1 - \frac{\chi_{m_0}(P)}{|P|^s}\right) L(s, \chi_{m_0}).$$

When m is square-free, the next proposition shows that $L(s, \chi_m)$ is closely related to the Artin L-function associated to the abelian extension $k(\sqrt{m})/k$.

Proposition

Suppose m is square-free. Consider the quadratic extension $K = k(\sqrt{m})$ of k. Let $L_\infty(s, \chi_m)$ be 1 if ∞ is ramified in K, $(1 - q^{-s})^{-1}$ if ∞ splits in K, and $(1 + q^{-s})^{-1}$ if ∞ is inert in K. Then

$$L_\infty(s, \chi_m) L(s, \chi_m)$$

is the Artin L-function associated to the unique non-trivial character of $Gal(K/k)$.

We are now in a position to state the connection between $L(1, \chi_m)$ and class numbers. If $m \in A$, recall the definition $\mathrm{sgn}_2(m)$. This is 1 if the leading coefficient of m is a square in $\mathbb{F}^*$ and is -1 if it is not.

Theorem

Let $m \in A$ be a square-free polynomial of degree M. Then,

1. *If M is odd, $L(1, \chi_m) = \frac{\sqrt{q}}{\sqrt{|m|}} h_m$.*
2. *If M is even and $sgn_2(m) = -1$, $L(1, \chi_m) = \frac{q+1}{2\sqrt{|m|}} h_m$.*
3. *If M is even and $sgn_2(m) = 1$, $L(1, \chi_m) = \frac{q-1}{\sqrt{|m|}} h_m R_m$. Here R_m is the regulator of the ring $\mathcal{O}_m$.*

Proof of the Theorem

Set $K = k(\sqrt{m})$. From previous proposition and some other results (Proposition 14.9 - Rosen's book) we derive

$$\zeta_K(s) = \zeta_k(s) L_\infty(s, \chi_m) L(s, \chi_m).$$

Multiply both sides of this equation by $s - 1$ and take the limit as $s \to 1$. One finds

$$\frac{h_K}{q^{g-1}(q-1)\log(q)} = \frac{1}{q^{-1}(q-1)\log(q)} L_\infty(1, \chi_m) L(1, \chi_m).$$

Simplifying, we obtain

$$h_K q^{-g} = L_\infty(1, \chi_m) L(1, \chi_m). \tag{2.1}$$

We know that the genus g of K is $\frac{M-1}{2}$ in case 1 and $\frac{M}{2} - 1$ in cases 2 and 3. Proposition 14.6 in Rosen's book shows that in case 1, ∞ is ramified, in case 2, ∞ is inert, and in case 3, ∞ splits. By using Proposition 14.7 in Rosen's book, we find $h_m = h_K$, $h_m = 2h_K$, and $h_m R_m = h_K$ in cases 1,2 and 3 respectively.

Continuation of the Proof

Let's consider case 1. We have $g = \frac{M-1}{2}$ and $L_\infty(1, \chi_m) = 1$. Also, $h_m = h_K$. Substituting this information into equation from the previous slide, and noting $\sqrt{|m|} = q^{M/2}$, we find

$$\frac{h_m \sqrt{q}}{\sqrt{|m|}} = L(1, \chi_m).$$

This proves case 1.
To deal with case 2 we note $g = \frac{M}{2} - 1$, $L_\infty(1, \chi_m) = (1 + q^{-1})^{-1}$, and $h_m = 2h_K$. Substituting into equation from the previous slide, we find

$$\frac{h_m}{2} \frac{q}{\sqrt{|m|}} = \left(1 + \frac{1}{q}\right)^{-1} L(1, \chi_m).$$

Case 2 of the theorem is immediate from this.

The last case, case 3, is done in exactly the same way.

Proposition

Let $m \in A$ be a non-square and write $m = m_0 m_1^2$ with m_0 square-free. Then,

$$\frac{h_m R_m}{\sqrt{|m|}} = \frac{h_{m_0} R_{m_0}}{\sqrt{|m_0|}} \prod_{P|m_1} (1 - \chi_{m_0}(P)|P|^{-1}). \tag{2.2}$$

Theorem

All the assertions about the class number given in the previous theorem remain valid if $m \in A$ is a non-square polynomial.

Proof.

Suppose $m = m_0 m_1^2$ with m_0 square-free. From the definitions,

$$L(s, \chi_m) = L(s, \chi_{m_0}) \prod_{P|m_1} (1 - \chi_{m_0}(P)|P|^{-s}).$$

If follows from the equation given in the last proposition that

$$\frac{h_m R_m}{\sqrt{|m|}} \frac{1}{L(1, \chi_m)} = \frac{h_{m_0} R_{m_0}}{\sqrt{|m_0|}} \frac{1}{L(1, \chi_{m_0})}.$$

With the help of this equation and the previous proposition the result follows. □

From the last theorem, we see that the task of averaging class numbers reduces to the task of averaging the numbers $L(1, \chi_m)$. It turns out that it is no harder to average $L(s, \chi_m)$ for any value of s. This is what we shall do.
To begin with, notice that

$$L(s, \chi_m) = \sum_{n \text{ monic}} \frac{\chi_m(n)}{|n|^s} = \sum_{d=0}^{\infty} \left(\sum_{\substack{n \text{ monic} \\ \deg(n)=d}} \chi_m(n) \right) q^{-ds}.$$

Definition

For $d \in \mathbb{Z}$, $d \geq 0$, define

$$S_d(\chi_m) = \sum_{\substack{n \text{ monic} \\ \deg(n)=d}} \chi_m(n)$$

.

Using this definition, we can rewrite $L(s, \chi_m)$ as $\sum_{d=0}^{\infty} S_d(\chi_m) q^{-ds}$. This sum is actually finite as we have seen before.

Lema

If $m \notin \mathbb{F}^*$ is not a square, $S_d(\chi_m) = 0$ for $d \geq M = \deg(m)$.

Proof.

By the reciprocity law, we have

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{q-1}{2}Md}\mathrm{sgn}(m)^d.$$

Call the quantity on the right of this equation c_d. Then, we have $\chi_m(n) = c_d(n/m)$. Thus, if $d \geq M$,

$$S_d(\chi_m) = c_d \sum_{\substack{n \text{ monic} \\ \deg(n)=d}} \left(\frac{n}{m}\right) = 0,$$

by the Proof of the Proposition on Lecture 3. □

Corollary

If $m \notin \mathbb{F}^*$ is not a square, then

$$L(s, \chi_m) = \sum_{d=0}^{M-1} S_d(\chi_m) q^{-ds},$$

a polynomial of degree at most $M-1$ in q^{-s}.

Our goal is to understand the sums $\sum_{\deg(m)=M} L(s, \chi_m)$ or the same sums restricted to monic polynomials m of degree M. By the corollary we are reduced to considering the sums $\sum_{\deg(m)=M} S_d(\chi_m)$ where $d < M$.

Definition

Let M and N be non-negative integers and n a monic polynomial of degree N. Define $\Phi_n(M)$ to be the number of monic polynomials m of degree M such that $gcd(n, m) = 1$. Define $\Phi(N, M)$ to be the number of pairs (n, m) of monic polynomials such that $deg(n) = N$, $deg(m) = M$, and $gcd(n, m) = 1$.

Note that

$$\sum_{\substack{n \text{ monic} \\ \deg(n)=N}} \Phi_n(M) = \Phi(N, M).$$

Also, it is obvious that $\Phi(N, M) = \Phi(M, N)$.

Proposition

$\Phi(0, M) = q^M$ *and if* $M, N \geq 1$, *then*

$$\Phi(N, M) = q^{M+N}\left(1 - \frac{1}{q}\right).$$

Proof of the Proposition

From the definition, $\Phi(0, M)$ is equal to the number of monic polynomials of degree M which we know is q^M. This proves the first assertion. To prove the second assertion, call two pairs (n, m) and $(n^{'}, m^{'})$ equivalent if $\gcd(n, m) = \gcd(n^{'}, m^{'})$. Breaking the set $\{(n, m) : \deg(n) = N, \deg(m) = M\}$ into equivalence classes and counting leads to the identity

$$q^{N+M} = \sum_{d=0}^{\min(N,M)} q^d \Phi(N - d, M - d).$$

Suppose $M, N \geq 1$. The proof now proceeds by induction on the number $M + N$. The smallest value this number can have is 2, in which case the formula yields $q^2 = \Phi(1, 1) + q\Phi(0, 0)$, or $\Phi(1, 1) = q^2 - q = q^2(1 - q^{-1})$. Now suppose the formulais correct for all pairs $N^{'}, M^{'} \geq 1$ with $N^{'} + M^{'} < N + M$. We may also suppose, by symmetry, that $N \leq M$. Then

$$q^{M+N} = \Phi(N, M) + \sum_{d=1}^{N-1} q^d \Phi(N - d, M - d) + q^N \Phi(0, M - N).$$

Continuation of the Proof

For $1 \leq d \leq N-1$ we have $\Phi(N-d, M-d) = q^{M+N-2d}(1-q^{-1})$ whereas by the first part of the proof, $\Phi(0, M-N) = q^{M-N}$. Substituting into the above formula and simplifying slightly,

$$q^{M+N} = \Phi(N,M) + q^{M+N} \sum_{d=1}^{N-1} q^{-d}(1-q^{-1}) + q^M = \Phi(N,M) + q^{M+N-1}.$$

The second assertion now follows immediately.

It is convenient to extend the definition of $\Phi(N,M)$ to half integers by defining $\Phi(N/2, M) = 0$ if N is odd.

Proposition

Suppose $1 \leq d \leq M-1$. *Then*

$$\sum_{\substack{m \text{ monic} \\ deg(m)=M}} S_d(\chi_m) = (q-1)^{-1} \sum_{deg(m)=M} S_d(\chi_m) = \Phi(d/2, M).$$

Proof of the Proposition

To begin with assume all sums are over monics. Then

$$\sum_{\deg(m)=M} S_d(\chi_m) = \sum_{\deg(m)=M} \sum_{\deg(n)=d} \left(\frac{m}{n}\right) = \sum_{\deg(n)=d} \sum_{\deg(m)=M} \left(\frac{m}{n}\right).$$

If n is not a square $(*/n)$ is a non-trivial character modulo n. Thus, in this case, since $M > \deg(n) = d$,

$$\sum_{\deg(m)=M} \left(\frac{m}{n}\right) = 0,$$

by the Proof of the Proposition on the third lecture.
Now, suppose that $n = n_1^2$ is a square. Then $(m/n) = (m/n_1)^2 = 1$ whenever $\gcd(m, n_1) = 1$ and $(m/n_1)^2 = 0$ otherwise. It follows that

$$\sum_{\deg(m)=M} \left(\frac{m}{n}\right) = \sum_{\deg(m)=M} \left(\frac{m}{n_1}\right)^2 = \Phi_{n_1}(M).$$

Continuation of the Proof

Thus

$$\sum_{\deg(m)=M} S_d(\chi_m) = \sum_{\deg(n_1)=d/2} \Phi_{n_1}(M) = \Phi(d/2, M).$$

To do the general case, let $\alpha \in \mathbb{F}^*$ and sum over all αm as m runs through the monics of degree M. The above calculation shows the answer is again equal to $\Phi(d/2, M)$. It follows that if we sum over all polynomials of degree d the answer is $(q-1)\Phi(d/2, M)$. This completes the proof.

We now have all the information we need to state our main results about averages of L-functions. We begin with the easiest case, averaging over all monics of fixed odd degree.

Theorem

Let M be odd and positive. We have, for all $s \in B$ with $s \neq \frac{1}{2}$,

$$q^{-M} \sum_{deg(m)=M} L(s, \chi_M) = \frac{\zeta_A(2s)}{\zeta_A(2s+1)} - \left(1 - \frac{1}{q}\right) (q^{1-2s})^{\frac{M+1}{2}} \zeta_A(2s).$$

For $s = \frac{1}{2}$, we have

$$q^{-M} \sum_{deg(m)=M} L(\tfrac{1}{2}, \chi_m) = 1 + \left(1 - \frac{1}{q}\right) \left(\frac{M-1}{2}\right).$$

Proof of the Theorem

We know that $L(s,\chi_m) = \sum_{d=0}^{M-1} S_d(\chi_m) q^{-ds}$. From this, and the previous two propositions, we find

$$\sum_{\deg(m)=M} L(s,\chi_m) = \sum_{d=0}^{M-1} \left(\sum_{\deg(m)=M} S_d(\chi_m) \right) q^{-ds}$$

$$= q^M + \Phi(1,M) q^{-2s} + \Phi(2,M) q^{-4s} + \cdots + \Phi((M-1)/2, M) q^{-(M-1)s}$$

$$= q^M \left(1 + \left(1 - \frac{1}{q} \right) \left[q^{1-2s} + (q^{1-2s})^2 + \cdots + (q^{1-2s})^{\frac{M-1}{2}} \right] \right).$$

Continuation of the Proof

The result for $s = \frac{1}{2}$ follows from this by substitution. For $s \neq \frac{1}{2}$ we sum the geometric series to derive

$$q^{-M} \sum_{\deg(m)=M} L(s, \chi_m) = 1 + \left(1 - \frac{1}{q}\right) q^{1-2s} \frac{1 - (q^{1-2s})^{\frac{M-1}{2}}}{1 - q^{1-2s}}$$

$$= 1 + \left(1 - \frac{1}{q}\right) \frac{q^{1-2s}}{1 - q^{1-2s}} - \left(1 - \frac{1}{q}\right) (q^{1-2s})^{\frac{M+1}{2}} \zeta_A(2s).$$

We have used the fact that $\zeta_A(s) = (1 - q^{1-s})^{-1}$. A close look at the last line shows that it only remains to identify the sum of the first two terms with a quotient of zeta values. This follows from the calculation

$$1 + \left(1 - \frac{1}{q}\right) \frac{q^{1-2s}}{1 - q^{1-2s}} = \frac{\zeta_A(2s)}{\zeta_A(2s+1)}.$$

Corollary

If $\Re(s) > \frac{1}{2}$, *then*

$$q^{-M} \sum_{deg(m)=M} L(s, \chi_m) \to \frac{\zeta_A(2s)}{\zeta_A(2s+1)},$$

as $M \to \infty$ *through odd values.*

Corollary

If M *is odd and positive, then*

$$q^{-M} \sum_{deg(m)=M} h_m = \frac{\zeta_A(2)}{\zeta_A(3)} q^{\frac{M-1}{2}} - q^{-1}.$$

Proof.

Follows from the theorem and the fact that $L(1, \chi_m) = h_m \frac{\sqrt{q}}{\sqrt{|m|}}$. □

We are left with considerations of the two cases where $\deg(m) = M$ is even and the leading coefficient of m is either a square in $\mathbb{F}^*$ or a non-square. The results we have in this case are:

Theorem

Let M be even and positive. The following sums are over all non-square monic polynomials of degree M.

1. *Suppose $s \neq \frac{1}{2}$ or 1. Then*

$$q^{-M} \sum L(s, \chi_m) = \frac{\zeta_A(2s)}{\zeta_A(2s+1)} - \left(1 - \frac{1}{q}\right) (q^{1-2s})^{M/2} \zeta_A(2s)$$
$$-q^{-M/2} \left(\frac{\zeta_A(2s)}{\zeta_A(2s+1)} - \left(1 - \frac{1}{q}\right) (q^{1-s})^{M} \zeta_A(s) \right).$$

2. *For $s = 1$ we have*

$$q^{-M} \sum L(1, \chi_m) = \frac{\zeta_A(2)}{\zeta_A(3)} - q^{-M/2} \left(2 + \left(1 - \frac{1}{q}\right) (M-1) \right).$$

Corollary

If $Re(s) > \frac{1}{2}$, *then as* $M \to \infty$ *though even integers,*

$$q^{-M} \sum L(s, \chi_m) \to \frac{\zeta_A(2s)}{\zeta_A(2s+1)}.$$

Corollary

With the hypotheses of the theorem, we have

$$q^{-M} \sum h_m R_m = (q-1)^{-1} \left(\frac{\zeta_A(2)}{\zeta_A(3)} q^{M/2} - \left(2 + \left(1 - \frac{1}{q} \right) (M-1) \right) \right).$$

I want to conclude this lecture by mentioning a refinement and generalization of the above results. The first refinement is to consider only polynomials m that are square-free. In this case, $\mathcal{O}_m$ is the integral closure of $A = \mathbb{F}[T]$ in $K = k(\sqrt{m})$. Thus the class numbers h_m are similar to the class numbers associated to quadratic number fields. In the language of binary quadratic forms, we would be restricting consideration to forms with fundamental discriminants. Averaging in this case is surprisingly difficult.

Definition

For $s \in \mathbb{C}$, $\Re(s) \geq \frac{1}{2}$, define

$$c(s) = \prod_P (1 - |P|^{-2} - |P|^{-(2s+1)} + |P|^{-(2s+2)}).$$

It is easy to see the product converges uniformly and absolutely in the region under consideration.

For simplicity we state the next theorem for the region $\Re(s) \geq 1$. But we have full results concerning the region $\Re(s) \geq \frac{1}{2}$.

Theorem

Let $\epsilon > 0$ be given and assume $s \in \mathbb{C}$ with $\Re(s) \geq 1$.

1. *If $M = 2n+1$ is odd, then*

$$(q-1)^{-1}(q^M - q^{M-1})^{-1} \sum_m L(s, \chi_m) = \zeta_A(2)\zeta_A(2s)c(s) + O(q^{-n(1-\epsilon)}),$$

   where the sum is over all square-free m such that $deg(m) = M$.

2. *If $M = 2n$ is even, then*

$$2^{-1}(q-1)^{-1}(q^M - q^{M-1})^{-1} \sum_m L(s, \chi_m) = \zeta_A(2)\zeta_A(2s)c(s) + O(q^{-n(1-\epsilon)}),$$

   where the sum is over all square-free m such that $deg(m) = M$ and $sgn_2(m) = 1$, or over all square-free m with $deg(m) = M$ and $sgn_2(m) = -1$.