The Riemann Hypothesis for Function Fields

Trevor Vilardi

MthSc 952

1 Function Fields

Let $F = \mathbb{F}_q$ be the finite field with q elements (q is a prime power).

Definiton 1. *Let $K/F(x)$ be an extension of F. If*

1. *K contains at least one element, x, that is transcendental over F.*
2. *K/F is a finite algebraic extension.*

Then we call K a function field in one variable over F, and F is called the constant field of K.

The elements of K can be thought of as rational functions. We will associate with K an invariant $g \in \mathbb{N}$ called the genus of K which comes from the algebraic geometric interpretation of K as the function field of some algebraic curve of genus g.

Definiton 2. *A prime in K is a discrete valuation ring, R, with maximal ideal P such that*

1. *$F \subset R$*
2. *$\text{Frac}(R) = K$.*

We will usually refer to the prime R as P, and we denote the Ord function associated with P by $\text{Ord}_P(*)$. Also note that $\deg P = [R/P : F]$.

Example 1. Let $K = \mathbb{F}_5(x)$, and $A = \mathbb{F}_5[x]$. If $P \in A$ is a monic irreducible, then the localization at P, $A_P = \{\frac{f}{g} | f, g \in A, g \notin P\}$ is a prime of K.

K contains one more prime besides those that come from monic irreducible polynomials. Let $A' = \mathbb{F}_5[x^{-1}]$, and $P = (x^{-1})$. Then the localization of A' at P', $A'_{P'}$, is a prime of K, and is called the prime at infinity, and is usually denoted ∞.

It can be shown that these are the only primes of K.

2 Divisors

Let $\mathcal{D}_K$ be the free abelian group generated by the primes of K. We call $\mathcal{D}_K$ the group of divisors of K.

For $D \in \mathcal{D}_{\mathrm{K}}$

$$D = \sum_P a(P) \cdot P$$

where the sum is over all primes, P, and the $a(P) \in \mathbb{Z}$ are uniquely determined by D. If $a(P) \geq 0$ for all P we say D is an effective divisor which we denote by $D \geq 0$. We define the degree of D to be

$$\deg(D) = \sum_P a(P) \cdot \deg P.$$

Note that $\deg : \mathcal{D}_{\mathrm{K}} \to \mathbb{Z}$ is a homomorphism with kernel denoted ${\mathcal{D}_{\mathrm{K}}}^0$.

Definiton 3. *Let $a \in K^*$. Then the divisor of a, denoted (a), is*

$$(a) = \sum_P \mathrm{Ord}_P(a) \cdot P$$

Note that $\mathrm{Ord}_P(a) = 0$ for all but finitely many P, hence $(a) \in \mathcal{D}_{\mathrm{K}}$.

Example 2. Let K be as in example 1. Consider $a = \frac{(x+1)^2(x^2+3)(x^2+2)^3}{(x^2+x+1)} \in K$. Note that all factors are irreducible and hence generate a prime of K. For finite primes, P, $\mathrm{Ord}_P(f)$ gives the highest power of P that divides f, and $\mathrm{Ord}_\infty(f) = -\deg(f)$. Recalling that we extend the Ord function to rational functions by $\mathrm{Ord}\left(\frac{f}{g}\right) = \mathrm{Ord}(f) - \mathrm{Ord}(g)$ we get

$$(a) = 2 \cdot (x+1) + 1 \cdot (x^2+3) + 3 \cdot (x^2+2) + (-1) \cdot (x^2+x+1) + (-8) \cdot \infty.$$

The degree of P is simply the degree of the irreducible which generates it, while the degree of ∞ is 1. This gives

$$\deg((a)) = 2 \cdot 1 + 1 \cdot 2 + 3 \cdot 2 - 1 \cdot 2 - 8 \cdot 1 = 0$$

as we will see it must be.

We can define a homomorphism from K^* to $\mathcal{D}_{\mathrm{K}}$ by the map $a \mapsto (a)$. The image of this mapping is called the group of principle divisors and is denoted $\mathcal{P}_K$.

If $\mathrm{Ord}_P(a) = m > 0$ we say that P is a zero of order m of a. Similarly, if $\mathrm{Ord}_P(a) = -n < 0$ we say that P is a pole of order n of a.

We will need the following facts concerning principle divisors. For $a \in K^*$

1. $(a) = 0$ if and only if $a \in F^*$

2. $\deg((a)) = 0$.

Definiton 4. *$D_1, D_2 \in \mathcal{D}_\mathrm{K}$ are said to be linearly equivalent if, denoted $D_1 \sim D_2$, if $D_1 - D_2 = (a)$ for some $a \in K^*$.*

We call the quotient group $Cl_K = \mathcal{D}_\mathrm{K}/\mathcal{P}_K$ the group of divisor classes. Since $\deg((a)) = 0$ for all $(a) \in \mathcal{P}_K$ the map $\deg : Cl_K \to \mathbb{Z}$ is a homomorphism.

Definiton 5. *The kernel of* $\deg : Cl_K \to \mathbb{Z}$ *is denoted* Cl_K^0*, and* $|Cl_K^0| = h_K$ *is called the class number of* K*.*

Note that, analogously to classical algebraic number theory, the class number, h_K, is finite.

Now we will define the important counting functions we will need. Let

$$a_n = \#\{\text{primes of degree } n\}$$
$$b_n = \#\{\text{effective divisors of degree } n\}.$$

Both a_n and b_n are finite for all n. Also, from these definitions we get that $a_n \leq b_n$. To see this, note that we can associate any prime P with the divisor $1 \cdot P$. Since the divisor has the same degree as the prime this gives an injection from the set of primes of degree n and the effective divisors of degree n. Hence $a_n \leq b_n$.

3 Zeta functions

For $A \in \mathcal{D}_\mathrm{K}$ the norm of A is

$$NA = q^{\deg(A)}.$$

Note that $N(A + B) = NANB$.

Definiton 6. *The zeta function of* K *is*

$$\zeta_\mathrm{k}(s) = \sum_{A \geq 0} NA^{-s}.$$

Since $NA^{-s} = q^{-ns}$, where $\deg(A) = n$, this is equivalent to

$$\zeta_\mathrm{k}(s) = \sum_{n=1}^{\infty} \frac{b_n}{q^{ns}}.$$

Like the classical Riemann-zeta function, $\zeta_{\mathrm{k}}(s)$ has an Euler product

$$\zeta_{\mathrm{k}}(s) = \prod_P \left(1 - \frac{1}{NP^s}\right)^{-1} = \prod_{n=1}^{\infty} \left(1 - \frac{1}{q^{ns}}\right)^{-a_n}$$

The Riemann hypothesis for function fields states that the zeros of ζ_{k} lie on the line $Re(s) = \frac{1}{2}$. Or, in more detail.

Theorem 1 (The Riemann Hypotheis for Function Fields)**.** If K is a global function field whose constant field, F, has q elements, then all of the zeros of $\zeta_{\mathrm{k}}(s)$ lie on the line $Re(s) = \frac{1}{2}$.

Next we want to show that $\zeta_{\mathrm{k}}(s)$ converges. For $n > 2g - 2$ we have

$$b_n = h_K \frac{q^{n-g+1} - 1}{q - 1}$$

hence $b_n = O(q^n)$. So combined with $\zeta_{\mathrm{k}}(s) = \sum_{n=1}^{\infty} b_n q^{-ns}$ we see that $\zeta_{\mathrm{k}}(s)$ converges absolutely for $Re(s) > 1$. To see that the Euler product converges, we need to show that $\sum_{n=1}^{\infty} a_n |q^{-ns}|$ converges. But this follows immediately from the fact that $a_n \leq b_n = O(q^n)$.

Theorem 2. Let g be the genus of K. Then there exists $L_K(u) \in \mathbb{Z}[u]$ with $\deg L_K(u) = 2g$ such that

$$\zeta_{\mathrm{k}}(s) = \frac{L_K(u)}{(1 - q^{-s})(1 - q^{1-s})}.$$

This holds for all s such that $Re(s) > 1$, and the right hand side provides analytic continuation of $\zeta_{\mathrm{k}}(s)$ to all of $\mathbb{C}$.

Proof. Let $u = q^{-s}$. Then

$$\zeta_{\mathrm{k}}(s) = Z_K(u) = \sum_{n=0}^{\infty} b_n u^n.$$

For $n > 2g - 2$ we have $b_n = h_K \frac{q^{n-g+1}-1}{q-1}$. Substituting this yields

$$Z_K(u) = \sum_{n=0}^{2g-2} b_n u^n + \sum_{m=2g-1}^{\infty} h_K \frac{q^{m-g+1} - 1}{q - 1} u^m \tag{1}$$

$$= \sum_{n=0}^{2g-2} b_n u^n + \frac{h_K}{q-1} \left(\frac{q^g}{1 - qu} - \frac{1}{1 - u}\right) u^{2g-1} \tag{2}$$

$$= \frac{L_K(u)}{(1 - u)(1 - qu)} \tag{3}$$

Going from (1) to (2) is accomplished simply by summing the geometric series. For the second equality all that is needed is to note that, when we combine the terms in parentheses, $q-1$ divides the numerator. Then simply combining with the common denominator gives the result. Note that this will also show that $L_K(u)$ has the desired degree. From (3) all that's left is to substitute q^{-s} for u. □

Corollary 1.

1. $\zeta_{\mathrm{k}}(s)$ has simple poles at $s = 0$ and $s = 1$.
2. $L_K(0) = 1$.
3. $L'_K(0) = a_1 - 1 - q$.
4. $L_K(1) = h_K$.

Proof.

1. All that's needed is to show $L_K(q^{-1}) \neq 0$ which we will show later.
2. Simply substitute 0.
3. We have $L_K(u) = (1-u)(1-qu)Z_K(u)$. Differentiating this yields
$$L'_K(u) = -(1-qu)Z_K(u) + Z'_K(u)(1-u)(1-qu) - q(1-u)Z_K(u)$$
so $L'_K(0) = -1 + b_1 - q$. All that's left is to note that $a_1 = b_1$.
4. From (2) we see that $\lim_{u\to 1}(u-1)Z_K(u) = \frac{h_K}{q-1}$, and from (3) we see that $\lim_{u\to 1}(u-1)Z_K(u) = \frac{-L_K(u)}{1-q}$. So $L_K(1) = h_K$. □

Since $L_K(0) = 1$ we can factor $L_K(u) = \prod_{i=1}^{2g}(1-\pi_i u)$. From this we can see that the Riemann hypothesis is equivalent to $|\pi_i| = \sqrt{q}$ for $1 \leq i \leq 2g$.

Like the classical Riemann-zeta function, the zeta function of a function field also satisfies a functional equation. Set
$$\xi_K(s) = q^{(g-1)s}\,\zeta_{\mathrm{k}}(s).$$
Then for all $s \in \mathbb{C}$
$$\xi_K(1-s) = \xi_K(s).$$
This implies that
$$L_K(q^{-1}u^{-1}) = q^{-g}u^{-2g}L_K(u).$$
Thus any zero of $L_K(q^{-1}u^{-1})$ is also a zero of $L_K(u)$. So factoring $L_K(q^{-1}u^{-1}) = \prod_{i=1}^{2g}(1-\frac{\pi_i}{q}u^{-1})$ shows that $\frac{q}{\pi_i}$ is a zero of $L_K(u)$ for all $1 \leq i \leq 2g$. Hence the map $\pi_i \mapsto \frac{q}{\pi_i}$ is a permutation of the roots of $L_K(u)$.

There is also an analogue of the prime number theorem which states:

Theorem 3.

$$a_N = \#\{P|\deg(P = N)\} = \frac{q^N}{N} + O(\frac{q^{\frac{N}{2}}}{N}).$$

Like in the classical case the prime number theorem is connected to the Riemann hypothesis. Our strategy for proving the Riemann hypothesis will be to show that $a_1 = q + O(\sqrt{q})$ implies $|\pi_i| = \sqrt{q}$.

Before proving the Riemann hypothesis we will need some results. Let $F_n = \mathbb{F}_{q^n}$ and $K_n = F_n K$, then K_n is called a constant field extension of K. We have

$$L_{K_n}(u) = \prod_{i=1}^{2g} (1 - \pi_i^n u)$$

which implies that we can prove the theorem for any $K_{n'}$, and it will hold for all other n. This is important because to prove $a_1 = q + O(\sqrt{q})$ we need to impose some restrictions on K. But we can find n large enough that the conditions always hold, so we can just assume they hold from the start.

Let $N_n(K) = \sum_{d|n} d a_d$, then $N_1(K) = a_1$ and $N_1(K_n) = q^n + O(q^{\frac{n}{2}})$.

Proof of the Riemann Hypothesis. We also need these two important facts which we will not prove

i $N_1(K_n) = N_n(K)$

ii $Z_K(u) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n(K)}{n} u^n\right)$

From ii we get

$$u\frac{Z_K'(u)}{Z_K(u)} = \sum_{n=1}^{\infty} N_1(K_n) u^n.$$

We can also write $Z_K(u)$ as

$$Z_K(u) = \prod_{i=1}^{2g} \frac{1 - \pi_i u}{(1-u)(1-qu)}$$

thus

$$\begin{aligned} u\frac{Z_K'(u)}{Z_K(u)} &= \sum_{n=1}^{\infty} (q^n + 1 - \pi_1^n - \pi_2^n - ... - \pi_{2g}^n) u^n \\ &= \sum_{n=1}^{\infty} q^n + u^n - \sum_{i=1}^{2g} \sum_{n=1}^{\infty} (\pi_i) u^n. \end{aligned}$$

Putting these together we get

$$\sum_{n=1}^{\infty}(N_1(K_n) - q^n - 1)u^n = -\sum_{i=1}^{2g}\sum_{n=1}^{\infty}(\pi_i u)^n.$$

Since$N_1(K_n) = q^n + O(q^{\frac{n}{2}})$, the left hand side has radius of convergence $R \geq q^{-\frac{1}{2}}$.

The right hand side has radius of convergence $R = \min_{1\leq i\leq 2g}\{|\pi_i^{-1}|\}$, so $|\pi_i^{-1}| \geq q^{-\frac{1}{2}}$ for all $1 \leq i \leq 2g$, hence $|\pi_i^1| \leq q^{\frac{1}{2}}$ for all $1 \leq i \leq 2g$.

Since the map $\pi_i \mapsto \frac{q}{\pi_i}$ is a permutation of the π_i we have for some j

$$|\pi_i| = \left|\frac{q}{\pi_j}\right| \geq \frac{q}{\sqrt{q}} = \sqrt{q}$$

for all i. Thus $|\pi_i| = \sqrt{q}$ for all i, which is equivalent to the Riemann hypothesis. □