The Riemann Hypothesis over Function Fields aka The Hasse-Weil Bound

Unit 29

Gil Cohen

January 28, 2025

Overview

Recap

Throughout this unit $\mathsf{K} = \mathbb{F}_q$, where $q = p^m$ for some prime p and $m \geq 1$. We will consider a function field F/K with genus g and prime divisors $\mathbb{P}$.

The group of divisors is denoted as $\mathcal{D}$. The group of principal divisors of F/K is denoted as

$$\mathcal{P} = \left\{(x) \mid x \in \mathsf{F}^\times\right\},$$

and $\mathcal{C} = \mathcal{D}/\mathcal{P}$ is called the divisor class group.

Preliminaries

Definition 1

For $m \in \mathbb{Z}$ define

$$\mathcal{S}_m = \{\mathfrak{p} \in \mathbb{P} \mid \deg \mathfrak{p} \leq m\},$$
$$\mathcal{C}_m = \{\mathfrak{a} \in \mathcal{D} \mid \deg \mathfrak{a} = m\}/\mathcal{P}.$$

Further, let

$$h = |\mathcal{C}_0|.$$

Lemma 2

For every $m \in \mathbb{Z}$ the sets $\mathcal{S}_m, \mathcal{C}_m$ as well as the set

$$\mathcal{T}_m = \{\mathfrak{a} \in \mathcal{D} \mid \mathfrak{a} \geq 0 \text{ and } \deg \mathfrak{a} \leq m\}$$

are finite. In particular, $h < \infty$.

Preliminaries

Proof.

$$\mathcal{S}_m = \{\mathfrak{p} \in \mathbb{P} \mid \deg \mathfrak{p} \leq m\}$$

First, if $\mathrm{F} = \mathrm{K}(x)$ then $\mathcal{S}_m \setminus \mathfrak{p}_\infty$ is in bijection with irreducible polynomials of degree $\leq m$ over K. Hence, as K is finite, $|\mathcal{S}_m| < \infty$.

For a general function field F/K, take $x \in \mathrm{F} \setminus \mathrm{K}$. Let $\mathfrak{p} \in \mathcal{S}_m$ and consider the place $\mathfrak{q}$ of $\mathrm{K}(x)/\mathrm{K}$ which lies under $\mathfrak{p}$. As

$$\mathrm{K} \subseteq \mathrm{K}(x)_\mathfrak{q} \subseteq \mathrm{F}_\mathfrak{p}$$

we have that $\deg \mathfrak{q} \leq \deg \mathfrak{p} \leq m$.

Therefore, with every $p \in \mathcal{S}_m$ we can associate a place $\mathfrak{q}$ of $\mathrm{K}(x)/\mathrm{K}$ of degree at most m. As there are only finitely many places of F/K above any given place of $\mathrm{K}(x)/\mathrm{K}$, we conclude that $|\mathcal{S}_m| < \infty$.

That $\mathcal{T}_m$ is finite readily follows.

Proof.

$$\mathcal{C}_m = \{\mathfrak{a} \in \mathcal{D} \mid \deg \mathfrak{a} = m\}/\mathcal{P}$$

We turn to prove that $|\mathcal{C}_m| < \infty$. Assume first $m \geq 2g$, and take $[\mathfrak{a}] \in \mathcal{C}_m$. By Riemann-Roch,

$$\dim \mathfrak{a} = \deg \mathfrak{a} - g + 1 \geq 1$$

and so $\exists x \in \mathcal{L}(\mathfrak{a}) \setminus \{0\}$. Hence, $\mathfrak{a}' \triangleq (x) + \mathfrak{a}$ satisfies $\mathfrak{a}' \geq 0$ and $[\mathfrak{a}'] = [\mathfrak{a}]$. This establishes a one to one map $\mathcal{C}_m \hookrightarrow \mathcal{T}_m$, and so $|\mathcal{C}_m| \leq |\mathcal{T}_m| < \infty$.

For $m < 2g$, let $\mathfrak{b} \in \mathcal{D}$ be such that $\deg \mathfrak{b} \triangleq d \geq 2g - m$. Then, the bijection

$$\{\mathfrak{a} \in \mathcal{D} \mid \deg \mathfrak{a} = m\} \to \{\mathfrak{a}' \mid \deg \mathfrak{a}' = m + d\}$$
$$\mathfrak{a} \mapsto \mathfrak{a} + \mathfrak{b}$$

induces a one to one map $\mathcal{C}_m \hookrightarrow \mathcal{C}_{d+m}$, and the proof follows. □

Definition 3

Define the *del* of a function field F/K as

$$\partial = \min \{\deg \mathfrak{b} \mid \mathfrak{b} \in \mathcal{D} \text{ and } \deg \mathfrak{b} > 0\}.$$

We will soon prove that $\partial = 1$, namely, that every function field has a degree one divisor. For now, we start by establishing

Claim 4

For every $n \in \mathbb{Z}$ the following hold:

1. $\exists \mathfrak{b} \in \mathcal{D}$ with $\deg \mathfrak{b} = n$ iff $\partial \mid n$;
2. $|\mathcal{C}_n| = h$ if $\partial \mid n$ and otherwise $\mathcal{C}_n = \emptyset$; and
3. $\partial \mid 2g - 2$.

Proof.

1. if $\mathfrak{b} \geq 0$ is such that $\deg b = \partial$ then $k\mathfrak{b}$ is a divisor of degree $k\partial$ for every $k \in \mathbb{Z}$. In the other direction, take any $\mathfrak{a} \in \mathcal{D}$, and let $n = \deg \mathfrak{a}$. Then, $n = k\partial + r$ for some k and $0 \leq r < \partial$, and

$$\deg(\mathfrak{b} - k\mathfrak{a}) = r.$$

   Unless $r = 0$, this stands in contradiction to the minimality of ∂.
2. By (the proof of) Lemma 2, $\mathcal{C}_n$ is in bijection with $\mathcal{C}_0$ whenever there exists a degree-n divisor, and so in such case $|\mathcal{C}_n| = |\mathcal{C}_0| = h$. If no such divisor exists then, of course, $\mathcal{C}_n = \emptyset$.
3. Lastly, Item 3 follows from Item 1 by taking a canonical divisor whose degree, recall, is $2g - 2$.

Preliminaries

Lemma 5

Let F/K *be a function field, and* $\mathfrak{a} \in \mathcal{D}$*. Then,*

$$|\{\mathfrak{b} \in \mathcal{D} \mid \mathfrak{b} \geq 0, \mathfrak{b} \sim \mathfrak{a}\}| = \frac{q^{\dim \mathfrak{a}} - 1}{q - 1}.$$

Proof.

The proof follows as there is a bijection between

$$X = \{(x) \mid x \in \mathcal{L}(\mathfrak{a}) \setminus \{0\}\}$$

and the set on the LHS. Indeed, if $\mathfrak{b} \sim \mathfrak{a}$ then there exists $x \in \mathrm{F}^\times$ such that $\mathfrak{b} = \mathfrak{a} + (x)$. For $\mathfrak{b} \geq 0$, this means that $x \in \mathcal{L}(\mathfrak{a})$. In the other direction, if $0 \neq x \in \mathcal{L}(\mathfrak{a})$ then we can define $\mathfrak{b} = \mathfrak{a} + (x)$ which is indeed non-negative and, clearly, $\mathfrak{b} \sim \mathfrak{a}$.

The proof follows as X has the required size. □

Preliminaries

One can reformulate Lemma 5 as saying that for every $C \in \mathcal{C}$,

$$|\{\mathfrak{b} \in \mathrm{C} \mid \mathfrak{b} \geq 0\}| = \frac{q^{\dim C} - 1}{q - 1}, \tag{1}$$

where recall $\dim C$ is the common value $\dim \mathfrak{b}$ of all divisors $\mathfrak{b} \in C$.

Definition 6

For $n \geq 0$ define

$$A_n = |\{\mathfrak{b} \in \mathcal{D} \mid \deg \mathfrak{b} = n, \mathfrak{b} \geq 0\}|.$$

As a corollary of Equation 1, we obtain

$$A_n = \sum_{C \in \mathcal{C}_n} \frac{q^{\dim C} - 1}{q - 1}. \tag{2}$$

Preliminaries

In particular, by the Riemann-Roch Theorem and by Claim 4, for every $n > 2g - 2$,

$$A_n = \begin{cases} h \cdot \frac{q^{n+1-g}-1}{q-1} & \text{if } \partial \mid n, \\ 0 & \text{otherwise..} \end{cases} \tag{3}$$

Definition 7

For $\mathfrak{a} \in \mathcal{D}$ we define the norm of $\mathfrak{a}$ by

$$\mathrm{N}\mathfrak{a} = q^{\deg \mathfrak{a}}.$$

Note that

1. $\mathrm{N}(\mathfrak{a} + \mathfrak{b}) = \mathrm{N}\mathfrak{a} \cdot \mathrm{N}\mathfrak{b}$, and
2. For $\mathfrak{p} \in \mathbb{P}$, $\mathrm{N}\mathfrak{p} = |\mathrm{F}_{\mathfrak{p}}|$.

Overview

The Zeta and Zi functions of a function field

Definition 8

The Zeta Function of a function field F/K is the complex-valued function

$$\zeta_{F/K}(s) = \sum_{0 \leq \mathfrak{a} \in \mathcal{D}_{F/K}} \frac{1}{(N\mathfrak{a})^s} = \sum_{0 \leq \mathfrak{a} \in \mathcal{D}_{F/K}} q^{-s \deg \mathfrak{a}}. \tag{4}$$

Setting $t = q^{-s}$, we write $Z(t) = \zeta(s)$, and call it the Zi function, namely,

$$Z(t) = \sum_{0 \leq \mathfrak{a} \in \mathcal{D}_{F/K}} t^{\deg \mathfrak{a}} = \sum_{n=0}^{\infty} A_n t^n. \tag{5}$$

So Z is the generating function for the sequence $A_0, A_1, \ldots$.

Equation 4 should be compared with Riemann's classical zeta function

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

The Zeta and Zi functions of a function field

Theorem 9

$\mathrm{Z}(t)$ converges for $|t| < q^{-1}$ (hence, $\zeta(s)$ converges for $\mathrm{Re}\, s > 1$). Moreover, for such t,

1. *If $g = 0$ then*

$$\mathrm{Z}(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right) \in \mathbb{Q}(t).$$

2. *For $g \geq 1$,*

$$\mathrm{Z}(t) = \frac{1}{q-1}\left(F(t) + hG(t)\right)$$

where

$$F(t) = \sum_{\substack{C \in \mathcal{C} \\ 0 \leq \deg C \leq 2g-2}} q^{\dim C} t^{\deg C} \in \mathbb{Q}[t]$$

$$G(t) = \frac{q^{1-g}(qt)^{2g-2+\partial}}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}} \in \mathbb{Q}(t).$$

Proof.

The "hence" assertion follows by observing that $|q^{-s}| = q^{-\operatorname{Re} s}$ and so

$$\operatorname{Re} s > 1 \quad \Longleftrightarrow \quad |q^{-s}| < q^{-1}.$$

The case $g = 0$. In the problem sets, using Riemann-Roch, you proved that in genus 0 function fields every degree 0 divisor is principle, and so

$$h = |\mathcal{C}_0| = 1.$$

Hence, by Equation 3,

$$\begin{aligned} Z(t) &= \sum_{n=0}^{\infty} A_n t^n = \sum_{k=0}^{\infty} A_{\partial k} t^{\partial k} = \sum_{k=0}^{\infty} \frac{q^{\partial k+1} - 1}{q-1} t^{\partial k} \\ &= \frac{1}{q-1} \left(q \sum_{k=0}^{\infty} (qt)^{\partial k} - \sum_{k=0}^{\infty} t^{\partial k} \right) \\ &= \frac{1}{q-1} \left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}} \right). \end{aligned}$$

Proof.

The case $g > 0$. By Equation 2 and by Riemann-Roch,

$$\begin{aligned} \mathrm{Z}(t) &= \sum_{n=0}^{\infty} A_n t^n = \sum_{n=0}^{\infty} \sum_{C \in \mathcal{C}_n} \frac{q^{\dim C} - 1}{q-1} \cdot t^n \\ &= \frac{1}{q-1} \left(\sum_{n=0}^{2g-2} \sum_{C \in \mathcal{C}_n} q^{\dim C} t^n + \sum_{n=2g-1}^{\infty} \sum_{C \in \mathcal{C}_n} q^{n+1-g} t^n - \sum_{n=0}^{\infty} \sum_{C \in \mathcal{C}_n} t^n \right) \\ &= \frac{1}{q-1} \left(F(t) + hG(t) \right), \end{aligned}$$

where

$$F(t) = \sum_{n=0}^{2g-2} \left(\sum_{C \in \mathcal{C}_n} q^{\dim C} \right) t^n = \sum_{\substack{C \in \mathcal{C} \\ 0 \le \deg C \le 2g-2}} q^{\dim C} t^{\deg C}$$

Proof.

and using Claim 4 we get that

$$\begin{aligned} G(t) &= \sum_{n=2g-1}^{\infty} \frac{|\mathcal{C}_n|}{h} q^{n+1-g} t^n - \sum_{n=0}^{\infty} \frac{|\mathcal{C}_n|}{h} t^n \\ &= q^{1-g} \sum_{\substack{n=2g-2+\partial \\ \partial | n}}^{\infty} (qt)^n - \sum_{\substack{n=0 \\ \partial | n}}^{\infty} t^n \\ &= \frac{q^{1-g}(qt)^{2g-2+\partial}}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}. \end{aligned}$$

□

The Zeta and Zi functions of a function field

Recap.

$$\mathrm{Z}(t) = \frac{1}{q-1}\left(F(t) + hG(t)\right)$$

where $F(t) \in \mathbb{Q}[t]$ and

$$G(t) = \frac{q^{1-g}(qt)^{2g-2+\partial}}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}.$$

As a corollary we see that $\mathrm{Z}(t)$ is defined for $|t| < q^{-1}$. Moreover, $\mathrm{Z}(t)$ can be extended (in the sense of analytic continuation) to a rational function on $\mathbb{C}$, where the unique poles of the extension are whenever $t^{\partial} = 1$ and $t^{\partial} = q^{-\partial}$. Furthermore, these poles are simple.

Therefore, $\zeta(s)$ as defined in Equation 4 converges for $\mathrm{Re}\,(s) > 1$. However, by the continuation of $\mathrm{Z}(t)$, we see that $\zeta(s)$ can be extended to a holomorphic function on $\mathbb{C}$ excluding the lines $\mathrm{Re}\,(s) = 0$ and $\mathrm{Re}\,(s) = 1$.

Euler-like product formula

Theorem 10

For $\mathrm{Re}\,(s) > 1$ and $|t| < q^{-1}$, we can write $\zeta(s)$ and $\mathrm{Z}(t)$ as the following infinite absolutely converging products:

$$\mathrm{Z}(t) = \prod_{\mathfrak{p} \in \mathbb{P}} \frac{1}{1 - t^{\deg \mathfrak{p}}}$$

$$\zeta(s) = \prod_{\mathfrak{p} \in \mathbb{P}} \frac{1}{1 - (\mathrm{N}\mathfrak{p})^{-s}}.$$

This should be compared with Euler product formula

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Euler-like product formula

Proof.

The formula for the ζ function follows by the one for Z as $\mathrm{N}\mathfrak{p} = q^{\deg p}$.

It can be shown using standard arguments that the RHS of the above equation involving $\mathrm{Z}(t)$ converges absolutely for $|t| < q^{-1}$. This is mostly because

$$\sum_{\mathfrak{p}\in\mathbb{P}} |t^{\deg \mathfrak{p}}| \leq \sum_{n=1}^{\infty} A_n t^n < \infty.$$

Due to the absolute convergence, we can write

Euler-like product formula

Proof.

$$\begin{aligned}\prod_{\mathfrak{p}\in\mathbb{P}} \frac{1}{1-t^{\deg \mathfrak{p}}} &= \prod_{\mathfrak{p}\in\mathbb{P}} \sum_{k(\mathfrak{p})=0}^{\infty} \left(t^{\deg \mathfrak{p}}\right)^{k(\mathfrak{p})} \\ &= \sum_{k} \prod_{\mathfrak{p}\in\mathbb{P}} t^{k(\mathfrak{p})\deg \mathfrak{p}} \\ &= \sum_{k} t^{\left(\sum_{\mathfrak{p}} k(\mathfrak{p})\deg \mathfrak{p}\right)} \\ &= \sum_{\mathfrak{a}\geq 0} t^{\deg \mathfrak{a}} = \mathrm{Z}(t),\end{aligned}$$

where we iterate over all k in $\mathbb{P} \to \mathbb{N}$ with finite support. □

As a corollary of Theorem 10, we have that for $\mathrm{Re}\,(s) > 1$, $\zeta(s) \neq 0$. Similarly, for $|t| < q^{-1}$, $\mathrm{Z}(t) \neq 0$.

Overview

Schmidt's Theorem, $\partial = 1$

Recall that in this unit we let $\mathsf{K} = \mathbb{F}_q$. K has a unique degree-r extension which is denoted by K_r. We denote the corresponding constant function field extension, $\mathsf{K}_r\mathsf{F}/\mathsf{K}_r$ by $\mathsf{F}_r/\mathsf{K}_r$.

From a prior unit (which we haven't covered), we know that the genus of F_r is the same as that of F. Moreover, if $\mathfrak{a}$ is a divisor of F/K, we can view it as a divisor of $\mathsf{F}_r/\mathsf{K}_r$ (vie the conorm), where the degree and dimension of $\mathfrak{a}$ remain unchanged.

Lemma 11

Let $\mathfrak{p}$ be a prime divisor of F/K with degree $\deg \mathfrak{p} = m$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_d$ be all the prime divisors of $\mathsf{F}_r/\mathsf{K}_r$ lying above $\mathfrak{p}$, with possible repetitions. Then, $\mathfrak{P}_1, \ldots, \mathfrak{P}_d$ are all distinct. Moreover, for every $i \in [d]$,

$$\deg \mathfrak{P}_i = \frac{m}{\gcd(r, m)},$$

and $d = \gcd(r, m)$.

Schmidt's Theorem, $\partial = 1$

Proof.

We saw that as F_r/F is a separable constant field extension, $\mathfrak{p}$ is unramified in F_r.

Fix $i \in [d]$. By a theorem from the constant function field extensions unit,

$$(\mathrm{F}_r)_{\mathfrak{P}_i} = \mathrm{K}_r\mathrm{F}_{\mathfrak{p}}$$

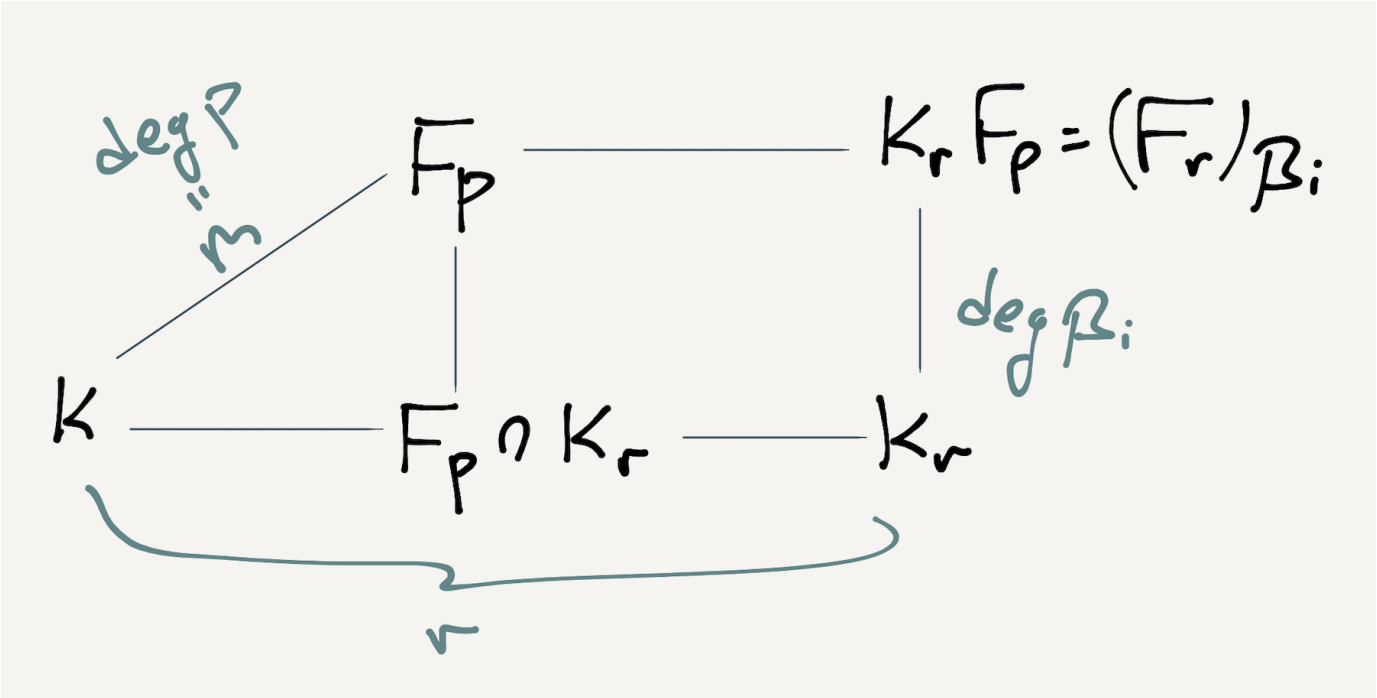
and so

$$\begin{aligned}\deg \mathfrak{P}_i &= [\mathrm{K}_r\mathrm{F}_{\mathfrak{p}} : \mathrm{K}_r] = [\mathrm{F}_{\mathfrak{p}} : (\mathrm{F}_{\mathfrak{p}} \cap \mathrm{K}_r)] \\ &= \frac{[\mathrm{F}_{\mathfrak{p}} : \mathrm{K}]}{[(\mathrm{F}_{\mathfrak{p}} \cap \mathrm{K}_r) : \mathrm{K}]} = \frac{\deg \mathfrak{p}}{\gcd(r, m)}.\end{aligned}$$

Now, $\deg \mathfrak{p} = d \deg \mathfrak{P}_i$, and so

$$d = \gcd(r, m).$$

Schmidt's Theorem, $\partial = 1$



Schmidt's Theorem, $\partial = 1$

Theorem 12

Let Z_r be the Zi function that corresponds to $\mathrm{F}_r/\mathrm{K}_r$. Then,

$$\mathrm{Z}_r(t^r) = \prod_{\xi^r=1} \mathrm{Z}(\xi t).$$

Proof.

As on both sides we have meromorphic functions, it suffices to prove equality for $|t| < q^{-1}$. By Theorem 10,

$$\mathrm{Z}_r(t^r)^{-1} = \prod_{\mathfrak{p}\in\mathbb{P}} \prod_{\mathfrak{P}/\mathfrak{p}} (1 - (t^r)^{\deg \mathfrak{P}})$$

whereas

$$\prod_{\xi^r=1} \mathrm{Z}(\xi t) = \prod_{\mathfrak{p}\in\mathbb{P}} \prod_{\xi^r=1} (1 - (\xi t)^{\deg \mathfrak{p}}).$$

Schmidt's Theorem, $\partial = 1$

Proof.

Thus, it suffices to prove that for every $\mathfrak{p}$,

$$\prod_{\mathfrak{P}/\mathfrak{p}} (1 - (t^r)^{\deg \mathfrak{P}}) = \prod_{\xi^r = 1} (1 - (\xi t)^{\deg \mathfrak{p}}).$$

Let $m = \deg \mathfrak{p}$ and $d = \gcd(r, m)$. By Lemma 11 it suffices to prove that

$$\left(1 - (t^r)^{\frac{m}{d}}\right)^d = \prod_{\xi^r = 1} (1 - (\xi t)^m).$$

Write $k = \frac{r}{d}$. Note that for ξ a primitive r-th root of unity it holds that ξ^m is a primitive k-th root of unity. Thus, the map $\xi \mapsto \xi^m$ is a surjective homomorphism from the group of r-roots of unity to the group of k-roots of unity. In particular, every element in the range has preimage of size $\frac{r}{k} = d$.

Schmidt's Theorem, $\partial = 1$

Proof.

Hence, the RHS is given by the d-th power of

$$\prod_{\eta^k=1}(1-\eta t^m).$$

Therefore it suffices to prove that

$$1 - t^{km} = \prod_{\eta^k=1}(1-\eta t^m). \tag{6}$$

This is indeed the case as the k-th roots of unity are exactly to roots of the polynomial

$$T^k - 1 = \prod_{\eta^k=1} T - \eta,$$

and substituting t^{-m} for T implies Equation 6. □

Schmidt's Theorem, $\partial = 1$

Theorem 13 (Schmidt's Theorem)

$$\partial = 1$$

Proof.

By Equation 3

$$\mathrm{Z}(t) = \sum_{k=0}^{\infty} A_{\partial k} t^{\partial k}.$$

Thus, for ξ a ∂-root of unity, $\mathrm{Z}(\xi t) = \mathrm{Z}(t)$. By Theorem 12,

$$\mathrm{Z}_{\partial}(t^{\partial}) = \mathrm{Z}(t)^{\partial}.$$

The proof then follows as at $t = 1$, the LHS has a simple pole whereas the RHS has a pole of order ∂. □

Schmidt's Theorem, $\partial = 1$

Corollary 14

If $g = 0$ then F/K is the rational function field and

$$\mathrm{Z}(t) = \frac{1}{(1-t)(1-qt)}.$$

For $g \geq 1$, we have that

$$\mathrm{Z}(t) = \frac{1}{q-1}\left(F(t) + hG(t)\right),$$

where

$$F(t) = \sum_{\substack{C \in \mathcal{C} \\ 0 \leq \deg C \leq 2g-2}} q^{\dim C} t^{\deg C} \in \mathbb{Q}[t]$$

$$G(t) = \frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t} \in \mathbb{Q}(t).$$

Schmidt's Theorem, $\partial = 1$

Proof.

The case $g \geq 1$ follows immediately by Theorem 9 and since we now know $\partial = 1$.

As for the case $g = 0$, since $\partial = 1$, F/K has a degree-one divisor and so, by a result you proved in the problem sets, F/K must be the rational function field. □

Corollary 14 implies that

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)}$$

for some $L(t) \in \mathbb{Q}[t]$ a polynomial of degree at most $2g$.

Overview

The function equation

Theorem 15

For every t (namely, treated as formal power series),

$$\mathrm{Z}(t) = q^{g-1}t^{2g-2}\mathrm{Z}\left(\frac{1}{qt}\right).$$

Proof.

This assertion is easy to verify for $g = 0$, so assume $g \geq 1$. It suffices to prove the functional equation for $F(t)$ and $G(t)$. To verify that

$$G(t) = \frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t}$$

satisfies

$$G(t) = q^{g-1}t^{2g-2}G\left(\frac{1}{qt}\right)$$

is a straightforward calculation.

The functional equation

Proof.

So we turn to show the same for $F(t)$. We have that

$$q^{g-1}t^{2g-2}F\left(\frac{1}{qt}\right) = q^{g-1}t^{2g-2}\sum_{\substack{C\in\mathcal{C}\\ 0\le \deg C\le 2g-2}} q^{\dim C}\left(\frac{1}{qt}\right)^{\deg C}$$

$$= \sum_{\substack{C\in\mathcal{C}\\ 0\le \deg C\le 2g-2}} q^{\dim C-\deg C+g-1}t^{2g-2-\deg C}.$$

The functional equation

Proof.

Let $\mathcal{W}$ be the canonical class. By Riemann-Roch,

$$\deg \mathcal{W} = 2g - 2,$$
$$\dim(\mathcal{W} - C) = \dim C - \deg C + g - 1.$$

So we can continue and write

$$\cdots = \sum_{\substack{C \in \mathcal{C} \\ 0 \le \deg C \le 2g-2}} q^{\dim C - \deg C + g - 1} t^{2g-2-\deg C}$$
$$= \sum_{\substack{C \in \mathcal{C} \\ 0 \le \deg C \le 2g-2}} q^{\dim(\mathcal{W}-C)} t^{\deg(\mathcal{W}-C)}.$$

Observe that as $C \in \mathcal{C}$ iterates over all divisors of degree $0, 1, \ldots, 2g-2$, so is $\mathcal{W} - C$, and so the RHS is indeed $F(t)$.

Corollaries

Now that we have established the functional equation,

$$\mathrm{Z}(t) = q^{g-1} t^{2g-2} \mathrm{Z}\left(\frac{1}{qt}\right).$$

we will draw interesting corollaries.

First, denote by N the number of rational prime divisors. Note that

$$N = A_1 = |\{\mathfrak{b} \mid \deg \mathfrak{b} = 1 \text{ and } \mathfrak{b} \geq 0\}|.$$

Note also that $A_0 = 1$.

Corollaries

We further denote by $\mathrm{Z}_0(t)$ the Zi function of $\mathbb{F}_q(x)/\mathbb{F}_q$. By Theorem 9 and since $\partial = 1$ (Theorem 13), we have that

$$\mathrm{Z}_0(t) = \frac{1}{(1-t)(1-qt)}$$

But

$$\mathrm{Z}(t) = \frac{L(t)}{(1-t)(1-qt)}$$

and so

$$L(t) = \frac{\mathrm{Z}(t)}{\mathrm{Z}_0(t)}.$$

From this we get a functional equation for the L-function

$$L(t) = \frac{\mathrm{Z}(t)}{\mathrm{Z}_0(t)} = \frac{q^{g-1}t^{2g-2}\mathrm{Z}(\frac{1}{qt})}{q^{-1}t^{-2}\mathrm{Z}_0(\frac{1}{qt})} = q^g t^{2g} L\left(\frac{1}{qt}\right).$$

Corollaries

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right).$$

We know that $\deg L \leq 2g$. Write

$$L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}.$$

Then,

$$\sum_{i=0}^{2g} a_i t^i = q^g t^{2g} \sum_{j=0}^{2g} a_j (qt)^{-j} = \sum_{j=0}^{2g} a_j q^{g-j} t^{2g-j} = \sum_{i=0}^{2g} a_{2g-i} q^{i-g} t^i$$

Comparing coefficients, we see that for every $i = 0, 1, \ldots, 2g$,

$$a_{2g-i} = a_i q^{g-i}.$$

Corollaries

Recap

$$L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} \qquad \text{and} \qquad a_{2g-i} = a_i q^{g-i}.$$

Now,

$$\begin{aligned} L(t) &= (1-t)(1-qt)\mathrm{Z}(t) \\ &= (1-t)(1-qt)(A_0 + A_1 t + \cdots) \\ &= A_0 + (A_1 - (q+1)A_0)t + \cdots \\ &= 1 + (N - (q+1))t + \cdots . \end{aligned}$$

Therefore,

$$\begin{aligned} a_0 &= 1 \\ a_1 &= N - (q+1) \\ a_{2g} &= q^g . \end{aligned}$$

In particular, $\deg L = 2g$.

Corollaries

To recap, we proved the following corollary

Corollary 16

The L function of a function field over $\mathbb{F}_q$ with genus g is of degree $2g$ taking the form

$$L(t) = 1 + (N - (q+1))t + \cdots + a_{2g} q^g t^{2g}.$$

Moreover, for every $i = 0, 1, \ldots, 2g$,

$$a_{2g-i} = a_i q^{g-i}.$$

For example, for an elliptic curve over $\mathbb{F}_q$, $g = 1$ and so

$$\begin{aligned} L(t) &= a_0 + a_1 t + a_2 t^2 \\ &= 1 + (N - (q+1))t + qt^2. \end{aligned}$$

The roots of the L function

Write

$$L(t) = \prod_{i=1}^{2g}(1 - \omega_i t),$$

where $\omega_1^{-1}, \ldots, \omega_{2g}^{-1}$ are the roots of L. We have that

Theorem 17

$$q^g = \prod_{i=1}^{2g} \omega_i$$

$$N - (q+1) = -\sum_{i=1}^{2g} \omega_i.$$

Moreover, we can order the ω_i-s so that for every $i = 1, 2, \ldots, g$,

$$\omega_i \omega_{g+i} = q.$$

The roots of the L function

Proof.

As

$$L(t) = \prod_{i=1}^{2g}(1 - \omega_i t),$$

we have that

$$\prod_{i=1}^{2g} \omega_i = a_{2g} = q^g.$$

Moreover,

$$-\sum_{i=1}^{2g} \omega_i = a_1 = N - (q+1).$$

The roots of the L function

Proof.

Recall again that

$$L(t) = \prod_{i=1}^{2g}(1 - \omega_i t),$$

Now,

$$\begin{aligned} L(t) &= q^g t^{2g} L\left(\frac{1}{qt}\right) \\ &= \frac{(qt)^{2g}}{\prod_{i=1}^{2g} \omega_i} \prod_{i=1}^{2g}\left(1 - \frac{\omega_i}{qt}\right) \\ &= \prod_{i=1}^{2g}\left(\frac{qt}{\omega_i} - 1\right) = \prod_{i=1}^{2g}\left(1 - \frac{qt}{\omega_i}\right), \end{aligned}$$

and so the sequence $(\frac{q}{\omega_i})_{i\in[2g]}$ is a permutation of the sequence $(\omega_i)_{i\in[2g]}$.

The roots of the L function

Proof.

After rearranging, noting that the permutation can have fixed points corresponding to values $\pm\sqrt{q}$, we can write the ω_i-s as

$$\omega_1, \frac{q}{\omega_1}, \ldots, \omega_k, \frac{q}{\omega_k}$$

for some $0 \leq k \leq g$ and with additional m copies of $\sqrt{q}$ and n copies of $-\sqrt{q}$.

To conclude the proof, we ought to prove that both m and n are even. But indeed,

$$2k + m + n = 2g,$$

and so it suffices to prove that n is even which follows since

$$q^g = \prod_{i=1}^{2g} \omega_i = q^k q^{m/2} (-1)^n q^{n/2} = (-1)^n q^g.$$

Overview

The Riemann Hypothesis over Function Fields

We are finally ready to state the Riemann Riemann Hypothesis over function fields which is in fact a theorem(!) - the fundamental Hasse-Weil Theorem.

Theorem 18

Using the notation above, the following three equivalent statements hold:

1. *The roots of* $\zeta(s)$ *all lie on the line* $s = \frac{1}{2}$ *in the complex plane.*
2. *The roots of* $\mathrm{Z}(t)$ *all lie on the circle of radius* $|t| = q^{-1/2}$.
3. $|\omega_i| = \sqrt{q}$ *for all* $i \in [2g]$.

An important corollary is

Theorem 19

$$|N - (q+1)| \leq 2g\sqrt{q}.$$

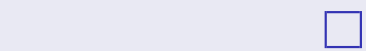
Proof.

Recall that

$$-\sum_{i=1}^{2g} \omega_i = a_1 = N - (q+1),$$

and so

$$|N - (q+1)| \leq \sum_{i=1}^{2g} |\omega_i| = 2g\sqrt{q}.$$



The Riemann Hypothesis over Function Fields

Given the unit on constant field extensions (which takes 2–3 hours to cover), we will need an additional 3–4 hours to prove the Riemann Hypothesis for function fields. This means we're not too far! However, since time is running short, I'll illustrate some components of the proof by proving a weaker yet still non-trivial variant.

Theorem 20

For every $r \in \mathbb{N}$,

$$L_r(t) = \prod_{i=1}^{2g} (1 - \omega_i^r t).$$

In particular, RH holds for F/K *iff it holds for* $\mathrm{F}_r/\mathrm{K}_r$.

Proof.

By Theorem 12,

$$Z_r(t^r) = \prod_{\xi^r=1} Z(\xi t),$$

and so

$$L_r(t^r) = \frac{Z_r(t^r)}{(Z_0)_r(t^r)} = \frac{\prod_{\zeta^r=1} Z(\zeta t)}{\prod_{\zeta^r=1} Z_0(\zeta t)}$$

$$= \prod_{\zeta^r=1} L(\zeta t) = \prod_{\zeta^r=1} \prod_{i=1}^{2g} (1-\omega_i \zeta t) = \prod_{i=1}^{2g} (1-\omega_i^r t^r),$$

where the last equality follows by the identity $T^r - 1 = \prod_{\zeta^r=1} (T-\zeta)$, substituting $T = \omega_i^{-1} t^{-1}$.

Clearly then,

$$|\omega_i| = \sqrt{q} \quad \Longleftrightarrow \quad |\omega_i^r| = \sqrt{q^r}.$$

The Riemann Hypothesis over Function Fields

Theorem 21

If $\exists c \in \mathbb{R}$ *such that for all* $r \in \mathbb{N}$

$$|N_r - (q^r + 1)| \leq cq^{r/2}$$

then RH holds for F/K.

Proof.

Consider the function

$$M(t) = -\sum_{i=1}^{2g} \frac{1}{1 - \omega_i t} \in \mathrm{C}(t).$$

This is a holomorphic function at a neighborhood of 0. Denote by R its convergence radius, noting that the only singularity (indeed poles) it has are at ω_i^{-1} for $i = 1, \ldots, 2g$, hence

$$R = \min_i |\omega_i^{-1}|.$$

Proof.

On the other hand, by Taylor expanding $M(t)$ around 0, we have that

$$M(t) = \sum_{r=0}^{\infty} \left(-\sum_{i=1}^{2g} \omega_i^r \right) t^r$$

By Theorem 17 and Theorem 20

$$N_r - (q^r + 1) = -\sum_{i=1}^{2g} \omega_i^r.$$

Thus,

$$M(t) = \sum_{r=0}^{\infty} (N_r - (q^r + 1)) t^r.$$

Proof.

$$M(t) = \sum_{r=0}^{\infty} (N_r - (q^r + 1))t^r.$$

Per our assumption,

$$\exists c \ \forall r \quad |N_r - (q^r + 1)| \leq cq^{r/2},$$

this series convergence for $|t| < q^{-1/2}$. Hence,

$$\min_i |\omega_i^{-1}| = R \geq q^{-1/2},$$

and so $|\omega_i| \leq \sqrt{q}$ for all $i \in [2g]$. But by Theorem 17, $\prod_i \omega_i = q^g$, and so $|\omega_i| = \sqrt{q}$ for all $i \in [2g]$, namely, RH holds for F/K.

The Riemann Hypothesis over Function Fields

With these results, we prove the following weak version of RH.

Theorem 22

Let F/K *be a function field over* $\mathbb{F}_q$ *such that* q *is an even power of a prime, satisfying* $q > (g+1)^4$. *Assume further that* F/K *has a prime divisor of degree* 1. *Then,*

$$N - (q+1) < (2g+1)\sqrt{q}.$$

Proof.

Denote the degree 1 prime divisor by $\mathfrak{p}$, and let

$$\begin{aligned} q' &= \sqrt{q} \\ m &= q' - 1 \\ n &= q' + 2g \\ r &= m + q'n \end{aligned}$$

Proof.

$$q' = \sqrt{q} \qquad m = q' - 1$$
$$n = q' + 2g \qquad r = m + q'n$$

Then

$$\begin{aligned} r &= (q' - 1) + q'(q' + 2g) \\ &= (2g + 1)q' + (q')^2 - 1 \\ &= (2g + 1)\sqrt{q} + q - 1 \end{aligned}$$

Hence, the bound we wish to prove

$$N - (q + 1) < (2g + 1)\sqrt{q}$$

can be expressed as

$$N - 1 \leq r.$$

Proof.

For $k \in \mathbb{N}$ let

$$I_k = \{0 \leq i \leq k \mid \mathcal{L}((i-1)\mathfrak{p}) \neq \mathcal{L}(i\mathfrak{p})\},$$

and for $i \in I_k$ denote by u_i and element in $\mathcal{L}(i\mathfrak{p}) \setminus \mathcal{L}((i-1)\mathfrak{p})$. As

$$\dim \mathcal{L}(i\mathfrak{p}) - \dim \mathcal{L}((i-1)\mathfrak{p}) = 1$$

for $i \in I_k$, we have that $\{u_i \mid i \in I_k\}$ is a basis of $\mathcal{L}(k\mathfrak{p})$.

Claim 23

The set $\{u_i \mid i \in I_m\}$ (recall $m = q' - 1$) is linearly independent when the coefficients are taking from q' powers of F (denoted $\mathrm{F}^{q'}$).

Proof.

Otherwise, there is $\emptyset \neq I \subseteq I_m$ such that

$$\sum_{i \in I} y_i^{q'} u_i = 0,$$

where $y_i \in \mathrm{F}^\times$. Clearly $|I| > 1$, and therefore there must be $i, j \in I$ distinct such that the corresponding valuations are equal, namely,

$$q' v_{\mathfrak{p}}(y_i) + i = v_{\mathfrak{p}}(y_i^{q'} u_i) = v_{\mathfrak{p}}(y_j^{q'} u_j) = q' v_{\mathfrak{p}}(y_j) + j$$

and so $i \equiv j \mod q'$, in contradiction to $0 \leq i, j \leq m = q' - 1$. □

We turn back to the proof of Theorem 22.

Proof.

As an immediate corollary of Claim 23 we have that the set

$$\left\{ u_i u_j^{q'} \mid i \in I_m, j \in I_n \right\}$$

is linearly independent over K. Define

$$\mathcal{L} = \mathrm{Span}_{\mathrm{K}}(u_i u_j^{q'} \mid i \in I_m, j \in I_n)$$
$$\mathcal{L}' = \mathcal{L}\left((mq' + n)\mathfrak{p}\right)$$

By the above,

$$\dim_{\mathrm{K}} \mathcal{L} = |I_m||I_n| = \dim(m\mathfrak{p}) \dim(n\mathfrak{p}).$$

Proof.

Recap.

$$q' = \sqrt{q} \qquad m = q' - 1$$
$$n = q' + 2g \qquad r = m + q'n$$

and $\dim_K \mathcal{L} = |I_m||I_n| = \dim(m\mathfrak{p})\dim(n\mathfrak{p})$. Hence, by Riemann-Roch

$$\begin{aligned}\dim_K \mathcal{L} &\geq (m - g + 1)(n - g + 1)\\ &= (q' - g)(q' + g + 1)\\ &= q - g^2 + q' - g.\end{aligned}$$

Per our assumption,

$$q' = \sqrt{q} > (g+1)^2 = g^2 + 2g + 1$$

and so

$$\dim_K \mathcal{L} > q + g + 1$$

Proof.

As for $\mathcal{L}'$

$$\deg \mathcal{L}' = mq' + n = (q' - 1)q' + (q' + 2g) = q + 2g > 2g - 2.$$

Thus, by Riemann-Roch,

$$\dim_K \mathcal{L}' = (q + 2g) - g + 1 = q + g + 1$$

Therefore,

$$\dim_K \mathcal{L} > \dim_K \mathcal{L}'.$$

To be continued...