THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

DEPARTMENT OF MATHEMATICS

Zeta Function of Curves Over Finite Field and Its Rationality

YIFEI ZHANG
2022

A thesis
submitted in partial fulfillment
of the requirements
for baccalaureate degree
in Mathematics
with honors in Mathematics

Reviewed and approved* by the following:

Mihran Papikian
Professor of Mathematics
Thesis Supervisor

Nathanial Brown
Professor of Mathematics
Honors Adviser

*Electronic approvals are on file.

Abstract

In this thesis, we are set to explore a zeta function over finite field: an analogy to Riemann zeta function, and prove its rationality with techniques of p-adic numbers.

Table of Contents

Acknowledgements

Here I am compelled to acknowledge Professor Mihran Papikian's advice and help all along this two years for how lucky I am to run into a professor like him who willingly gave me the chance to work with him without knowing me too well and led me through a beautiful journey of mathematics. This thesis and potentially many of my future work is impossible without him. Moreover, he with his intelligence and patience, certainly set a model of mathematician that I will doggedly emulate. I cannot thank him enough.

Chapter 1

Introduction

One of the most celebrated open problem today is the Riemann Hypothesis, which states

The real part of every nontrivial zero of the Riemann zeta function is $\frac{1}{2}$.

Definition 1.1 The Riemann Zeta function is initially defined as follow:

$$\begin{aligned}\zeta(s) &:= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)\end{aligned}$$

This expression has a natural domain in $\mathbb{C}$ which is all the complex number with real part greater than 1, and on that natural domain, $\zeta(s)$ is holomorphic. Via analytic continuation, $\zeta(s)$ extends to a unique meromorphic function on $\mathbb{C}$ with the unique pole at 1, which produces the Riemann zeta function we are talking about (we still denote this by $\zeta(s)$).

Moreover, Let $\Gamma(s)$ be the gamma function, and define the "full" zeta function

$$\zeta_{\mathbb{Q}}(s) := \pi^{s/2}\Gamma(s/2)\zeta(s)$$

and we may have a functional equation $\zeta_{\mathbb{Q}}(s) = \zeta_{\mathbb{Q}}(1-s)$. Since gamma function does not have a zero, $\zeta_{\mathbb{Q}}(s)$, on its domain, has the exactly same zeros as the $\zeta(s)$. The factors of $\zeta_{\mathbb{Q}}$, i.e. all the term like $\left(1 - \frac{1}{p^s}\right)$ and the gamma function term, are in one-to-one correspondence to the places of $\mathbb{Z}$: the gamma function factor corresponds to the only archimedean place and the prime factors correspond to the non-archimedean place. One group of zeros of zeta functions are all negative even integer, which we call trivial zero. Except those, other zeros are called non-trivial zeros which are predicted to have real part $\frac{1}{2}$ by Riemann Hypothesis.

One of the reasons for the importance of Riemann Hypothesis is the richness of its consequences. For example, assume the hypothesis, one can give a nice error term for the prime number theorem. More explicitly, one can write

$$\pi(x) = \mathrm{Li}(x) + \mathcal{O}(\sqrt{x}\log(x))$$

where π is the prime counting function and Li is the Eulerian logarithmic integral, which well measures the distribution of prime numbers. There are much more consequences and implication of Riemann hypothesis which we do not list here.

While the Riemann Hypothesis still remains mysterious, the zeta function of variety over finite fields are much more thoroughly studied. In this passage, we focus this type of zeta function, which is defined on page 5. In Chapter 2, we explore this zeta function by giving 3 equivalent forms of it and explain the analogy between it and the Riemann zeta function, and then we conclude the chapter with a few explicit examples and an observation. A lot of results from Lorenzini's *An invitation to arithmetic geometry* are cited in this chapter.

In Chapter 3, we equip $\mathbb{Q}$ with p-adic absolute value and construct a complete field $\mathbb{Q}_p$ with respect to the induced metric. Further, we study the algebraic and analytic property of $\mathbb{Q}_p$ and produce an algebraic closed and complete field that contains $\mathbb{Q}_p$, which is denoted by $\mathbb{C}_p$. In Chapter 4, we study some general properties of power series over $\mathbb{Q}_p$ and $\mathbb{C}_p$ and give a few examples. It is concluded with a technical lemma. These two chapters follows mainly the outline of Gouvêa's *p-adic Numbers* and set us up for the main proof in the next chapter.

In Chapter 5, we connect $\mathbb{F}_q$ to $\mathbb{C}_p$ through the $\mathbb{C}_p$ valued character, extend the notion of trace, determinant and characteristics polynomials to linear transformations over $\mathbb{C}_p[[x]]$. With those, we show the zeta function is a quotient between two entire functions, and those two entire functions will turn out to be polynomials. This chapter follows Koblitz's *p-adic numbers, p-adic analysis, and zeta-functions* and filled in some gaps that were left as exercise in the book.

Chapter 2

Zeta Functions of Curves Over $\mathbb{F}_q$

Definition 2.1 A ***projective plane curve*** C over a field k defined by a homogeneous polynomial $F \in k[x, y, z]$ is

$$\{[x : y : z] \in \mathbb{P}(\overline{k}^3) : F(x, y, z) = 0\}$$

We call a curve C over k defined by $F \in k[x, y, z]$ a ***singular curve*** if there exist $p \in C$ such that

$$\nabla F(p) = (0, 0, 0)$$

k'-***rational points*** in C, denoted by $C(k')$ for a subfield k' of $\overline{k}$ is the set

$$\{[x : y : z] : x, y, z \in k'\}$$

If a curve is not singular, then we call it a ***nonsingular curve*** or ***smooth curve***. Additionally, the curve defined by a homogeneous polynomial is called a ***complete curve***.

It's worth to point out that if the polynomial F defines a smooth curve, F has to be absolutely irreducible, i.e. irreducible in $\overline{k}[x, y, z]$, a fortiori irreducible in $k[x, y, z]$. As a result, the ring $k[x, y, z]/(F)$ is integral domain.

Definition 2.2 The ***field of rational function*** over C, denoted by $k(C)$, is the subfield of $Frac(k[x, y, z]/(F))$ which consists of the following

$$\left\{ \frac{\text{class of } f}{\text{class of } g} \;\middle|\; \begin{array}{l} f \text{ and } g \text{ are two homogeneous polynomials of the same} \\ \text{degrees and class of } g \text{ is not } 0. \end{array} \right\}$$

An element of $k(C) \ni \phi = \frac{\text{class of } f}{\text{class of } g}$ (from now on we will just write $\phi = \frac{f}{g}$) is called a ***rational function*** on C, and define $\phi(p) := \frac{f(p)}{g(p)}$ for $p \in C$ and $g(p) \neq 0$. Naturally, we define domain of ϕ in the following way.

$$Dom(\phi) := \left\{ p \in C \;\middle|\; \text{there exists } f, g \text{ such that } \phi = \frac{f}{g} \text{ and } g(p) \neq 0. \right\}$$

Indeed, for any $\lambda \neq 0$, $\phi(\lambda p) = \frac{f(\lambda p)}{g(\lambda p)} = \frac{\lambda^d f(p)}{\lambda^d g(p)} = \phi(p)$ where d is the common degree of f and g, so the value of $\phi(p)$ does does not depend on the choice of representative of p.
If $\phi = \frac{f}{g} = \frac{f'}{g'}$ and $g(p) \neq 0$ and $g'(p) \neq 0$, then according to the property of fraction field we know $fg' - f'g = hF$ for some $h \in k[x, y, z]$. Plug in p we get $\frac{f(p)}{g(p)} = \frac{f'(p)}{g'(p)}$ since $F(p) = 0$. Therefore $\phi(p)$ doesn't depend upon the representation of ϕ.

Thus, the field of rational function over a curve we just defined does live up to its name, as each of its element (so called rational function) give a well-defined function from its domain to k.

Proposition 2.3. For smooth C defined by an absolutely irreducible homogeneous $F \in k[x, y, z]$, $k(C)$ is a finite algebraic extension of $k(x)$ where x is an indeterminate.

Proof. Since F is irreducible, we can assume it to be a homogenization of $f(x,y)$ such that $deg(f) = deg(F)$ and $F(x,y,z) = z^{deg(f)}f(x/z, y/z)$. We know that f is irreducible too. Then the map $\psi : k(C) \longrightarrow Frac(k[x,y]/(f))$ given by

$$\frac{a(x,y,z)}{b(x,y,z)} \longrightarrow \frac{a(x,y,1)}{b(x,y,1)}$$

gives an isomorphism. f being irreducible in $k[x,y]$ gives us that f is irreducible in $k(x)[y]$, assuming $deg_y(f) > 0$. Hence (f) is maximal in $k(x)[y]/(f)$ and there is an canonical identification between $Frac(k[x,y]/(f))$ and
$k(x)[y]/(f)$. Given this we have $k(x) \hookrightarrow k(x)[y]/(f) \cong k(C)$ and it's clear that the extension is finite. □

Definition 2.4 A ***place*** in $k(C)$ is a maximal ideal of a discrete valuation ring whose field of fraction is $k(C)$, which is in one-to-one correspondence to the surjective valuation on $k(C)$ that is trivial on k. The ***residue field*** at a place v, denoted by k_v, is the corresponding D.V.R quotient by its (unique) maximal ideal.

Now we turn to the case when $k = \mathbb{F}_q$.

Definition 2.5 Let C be a smooth curve over $\mathbb{F}_q$. Define $q_v := \#k_v$ which is known to be finite since we are working over $\mathbb{F}_q$ and

$$\zeta_C(s) := \prod_v \left(1 - q_v^{-s}\right)^{-1}$$

call it ***Zeta Functions of curve*** C ***over*** $\mathbb{F}_q$ where v ranges over all places of $k(C)$. Recall that each place of $\mathbb{Z}$ corresponds to a prime p, and the local field at p is exactly of size p, hence the connection to Riemann zeta function.

Proposition 2.6. Places of $k(C)$ are in one-to-one correspondence to orbits of $C(\bar{k})$ under the action of $Gal(\overline{k}/k)$ where the action of $\delta \in Gal(\overline{k}/k)$ is given by $[x : y : z] \longrightarrow [\delta(x) : \delta(y) : \delta(z)]$.

Proof. See 3.9 in chapter 7 of [3]. □

Definition 2.7 For any $p = [c_0 : c_1 : c_2] \in C$, we define ***field of definition over k*** of the point p, denoted by $k(p)$, as $k(c_j/c_i, c_l/c_i)$ for i such that $c_i \neq 0$. It can be verified that it does not depend on the choice of c_i.

Lemma 2.8. If a place v corresponds to the orbit of p under $Gal(\overline{k}/k)$, then we have

$$q_v = \#k(p)$$

and we let $deg(v)$ be the number of elements in the orbit that corresponds to v, we have

$$q_v = q^{deg(v)}$$

Moreover, let b_d denote the number of v's such that $deg(v) = d$, then we have

$$\sum_{d|n} db_d = \#C(k')$$

where $[k' : k] = n$, i.e. $k = \mathbb{F}_q$ and $k' = \mathbb{F}_{q^n}$.

Proof. See 3.10 in chapter 7 of [3]. □

Given these, we have the following

$$\begin{aligned}
Log(\zeta_C(s)) &= Log(\prod_v \left(1-q_v^{-s}\right)^{-1}) \\
&= Log(\prod_d^{\infty} \left(1-q^{-ds}\right)^{-b_d}) \\
&= \sum_d^{\infty} -b_d Log(1-q^{-ds}) \\
&= \sum_d^{\infty} \left(b_d \sum_{k=1}^{\infty} \frac{q^{-kds}}{k} \right) \\
&= \sum_n^{\infty} \left(\sum_{k,d,\ kd=n} \frac{b_d}{k} \right) q^{-ns} \\
&= \sum_n^{\infty} \left(\sum_{d|n} \frac{db_d}{n} \right) q^{-ns} \\
&= \sum_n^{\infty} (\#C(\mathbb{F}_{q^n}) \frac{q^{-ns}}{n})
\end{aligned}$$

Therefore we have the equivalent expression

$$\zeta_C(s) = \exp(\sum_n^{\infty} (\#C(\mathbb{F}_{q^n}) \frac{q^{-ns}}{n}))$$

Fix an embedding of $\mathbb{A}^2$ in $\mathbb{P}^2$ given by

$$(a,b) \mapsto [a:b:1]$$

and $\mathbb{P}^2 \setminus \mathbb{A}^2$ is called **infinity**. Let ω range over the places of $k(C)$ that do not correspond to an orbit that entirely lies in infinity (which means it's disjoint from infinity), consider the following expression

$$\prod_{\omega} \left(1-q_{\omega}^{-s}\right)^{-1}$$

and assume $F(x,y,z)$ is the homogenization of $f(x,y)$, then each ω corresponds to an orbit in $\{(a,b) : a,b \in \overline{k}\}$ acted by $(a,b) \mapsto (\sigma(a),\sigma(b))$ which in turn corresponds (see 3.2 in chapter 7 of [3]) to the maximal ideal ker($\phi_{(a,b)}$) in $k[x,y]/(f)$ where $\phi_{(a,b)} : k[x,y]/(f) \longrightarrow \overline{k}$ is given by

$$g(x,y) \mapsto \phi_{(a,b)}(g(x,y)) = g(a,b)$$

Notice that $g(\sigma(a),\sigma(b)) = \sigma(g(a,b))$, so we did associate an orbit to a maximal ideal. Also each element in $\overline{k}$ is of finite multiplicative order, so the image of $\phi_{(a,b)}$ is a field (which is in fact

$k(a,b)$), hence ker($\phi_{(a,b)}$) is indeed a maximal ideal, denoted by m_ω. Looking more closely we have in fact

$$\#((k[x,y]/(f))/m_\omega) = \#k(a,b) = q_\omega$$

As $F(x,y,z)$ is assumed to be nonsingular, $k[x,y]/(f)$ is a Dedekind domain (see 2.7 in chapter 7 of [3]) hence each ideal is a unique product of maximal ideals. If we define $||I|| := \#(k[x,y]/(f))/I$ we have

$$||m_\omega|| = q_\omega$$

$$||I|| = \prod_{\substack{m_i \in Max(k[x,y]/(f)) \\ m_i | I}} ||m_i||^{e_i}$$

where $I = \prod m_i^{e_i}$. We have the following

$$\begin{aligned}\prod_\omega \left(1 - q_\omega^{-s}\right)^{-1} &= \prod_{m \in Max(k[x,y]/(f))} (1 - ||m||^{-s})^{-1} \\ &= \prod_{m \in Max(k[x,y]/(f))} \sum_{k=0}^{\infty} ||m||^{-ks} \\ &= \sum_I ||I||^{-s}\end{aligned}$$

where I ranges over all the ideal of $k[x,y]/(f)$ (including the whole ring). Recall that each ideal in $\mathbb{Z}$ is (n) and $\#\mathbb{Z}/(n) = n$, and here we see the connection to Riemann zeta function! Notice that C can have only finitely many points at infinity, hence there are only finitely many places corresponding to the orbits lie over infinity, call them $v_1, v_2, ..., v_r$. We can rewrite the zeta function as

$$\zeta_C(s) = \sum_I ||I||^{-s} \prod_{i=1}^{r} \left(1 - q_{v_i}^{-s}\right)^{-1}$$

Enough of these equivalent expressions of zeta function for now, we are going to compute a few concrete example before delving further into it.

Example 2.9. Let $C = \mathbb{P}^1_{\mathbb{F}_q}$, specifically, we can consider C over $\mathbb{F}_q$ given by $F[x,y,z] = y$. As noted above, each place in $\mathbb{F}_q(C)$ either corresponds to orbit of $[a : 0 : 1]$ or $[1 : 0 : 0]$. Let's denote the place by v_∞ if it's the latter case. $deg(v_\infty) = [\mathbb{F}_q(1) : \mathbb{F}_q] = 1$ and there are exactly q^d monic polynomials of degree d (in bijection with the ideal) and we have

$$\begin{aligned}\zeta_C(s) &= (1 - q_{v_\infty}^{-s})^{-1} \Big(\sum_{I \subseteq \mathbb{F}_q[x]} ||I||^{-s} \Big) \\ &= (1 - q^{-s})^{-1} \Big(\sum_{d=0} q^d q^{d(-s)} \Big) \\ &= \frac{1}{(1 - q^{-s})(1 - q^{1-s})}\end{aligned}$$

Alternatively we may use the second expression since $\#C(\mathbb{F}_{q^n}) = q^n + 1$ is rather clear for each n. Indeed

$$\begin{aligned}
\zeta_C(s) &= \exp(\sum_n^\infty (\#C(\mathbb{F}_{q^n})\frac{q^{-ns}}{n})) \\
&= \exp(\sum_n^\infty ((q^n+1)\frac{q^{-ns}}{n})) \\
&= \exp(\sum_n^\infty (\frac{q^{n(1-s)}}{n}))\exp(\sum_n^\infty (\frac{q^{-ns}}{n})) \\
&= \exp(-Log(1-q^{1-s}))\exp(-Log(1-q^s)) \\
&= \frac{1}{(1-q^{-s})(1-q^{1-s})}
\end{aligned}$$

Remark 2.10. If we let b_d denote the number of irreducible polynomial in $\mathbb{F}_q[x]$ (hence the number of places in $\mathbb{F}_q(x)$ that do not correspond to infinity) and let $C = \mathbb{P}^1_{\mathbb{F}_q}$. Lemma 2.8 and example 2.9 gives

$$\sum_{d|n} db_d = \#C(\mathbb{F}_{q^n}) - 1 = q^n$$

A direct application of Mobius inversion gives us

$$b_n = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

Example 2.11. Let q be a prime power such that 2 and 3 does not divides q, and let C be over $\mathbb{F}_q$ given by $F[x,y,z] = y^2 - x^2 - xz$. We can check that C is a smooth curve and F is absolutely irreducible. We can study $C(F_{q^n})$ geometrically. To begin with, we examine the points that does not lie in infinity, which are in correspondence with the loci of $f(x,y) = F(x,y,1) = y^2 - x^2 - x$, denoted by $V(f)$. Let

$$l_k := \{(t, kt) : t \in \mathbb{F}_{q^n}\}$$

and

$$l_\infty := \{(0, t) : t \in \mathbb{F}_{q^n}\}$$

which are the lines pass thru $(0,0)$. We observe that for $k^2 \neq 1$

$$l_k \cap V(f) = \{(\frac{1}{k^2-1}, \frac{k}{k^2-1}), (0,0)\}$$

and the rest of the lines intersect with $V(f)$ only at $(0,0)$. There are apparently exactly 2 points at infinity, namely $[1:1:0]$ and $[-1:1:0]$. We get

$$\#C(\mathbb{F}_{q^n}) = 1 + q^n - 2 + 2 = q^n + 1$$

and based on previous calculation we have again

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

We end this section with an observation.

Proposition 2.12. If C is given by $F(x,y,z) = f(x,y) + az^{p^e}$ where $f(x,y)$ is a homogeneous polynomial of degree p^e, therefore so is F, $a \neq 0$, and q is a power of p such that $F \in \mathbb{F}_q[x,y,z]$, then we have $\#C(\mathbb{F}_{q^n}) = q^n + 1$. Consequently, its zeta function is

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

Proof. Let $g(x,y) = F(x,y,1)$, retain the notation from the previous example, and WLOG assume g is monic in y and $a = -1$, so $g(x,y) = f(x,y) - 1$. We have for k such that $f(1,k) \neq 0$

$$l_k \cap V(g) = \{(\frac{1}{f(1,k)^{1/p^e}}, \frac{k}{f(1,k)^{1/p^e}})\}$$

$$l_\infty \cap V(g) = \{(0,1)\}$$

so in the first affine piece, F has $q^n - s + 1$ loci, where s is the number of k such that $f(1,k) = 0$. In the complement of the first affine piece, i.e the infinity, we found it's $\{[1 : k : 0] : k \text{ such that } f(1,k) = 0\}$, which contains exactly s elements. Also notice that $F(0,1,0) \neq 0$, so we found all of the loci, whose number is $q^n + 1$. For the case when f is not monic in y, notice that we lose a point in the affine piece, namely $l_\infty \cap V(f)$ but we gain a point in infinity, namely $[0:1:0]$. Routine computation gives its zeta function. □

Given these examples, one may want to guess that $\zeta_C(s)$ is always a rational function in variable q^{-s}. Indeed, it has been proved by Bernard Dwork in 1960 with p-adic analysis which we will discuss in the next section.

Chapter 3

p-adic Numbers

As mentioned earlier, all the non-archimedean places of $\mathbb{Q}$ corresponds to prime numbers, which naturally give rise to non-archimedean absolute values on $\mathbb{Q}$. Completion of $\mathbb{Q}$ with respect to the absolute value that corresponds to a prime p gives us an interesting field to study, which is denoted by $\mathbb{Q}_p$ as an analogy to $\mathbb{R}$ (which is the completion of $\mathbb{Q}$ with respect to the archimedean absolute value). Aside from being an intrinsically interesting field, it has many application in Number Theory. For instance, one of my favorite motivations for p-adic numbers is the Hasse-Minkowski theorem which states that a quadratic homogeneous rational-coefficient polynomial has a non-trivial rational solution if and only if it has a non-trivial solution in every completion of of Q (which consists of $\mathbb{R}$ and Q_p for each p).

Now we can fix a prime number p, and its respective p-adic field $\mathbb{Q}_p$ will be constructed as follow.

Definition 3.1 For each $a \in \mathbb{Z}$, write $a = p^k b$ where $p \nmid b$, we define its ***valuation*** at p as

$$v_p(a) := k$$

In other word, $v_p(a)$ is the largest integer k such that $p^k | a$.
For $r = \frac{a}{b} \in \mathbb{Q}$, we let

$$v_p(r) := v_p(a) - v_p(b)$$

Correspondingly we define ***p-adic absolute value*** $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}$ by letting

$$|r|_p := p^{-v_p(r)}$$

Proposition 3.2. For each $a, b \in \mathbb{Q}$, we may have the following

$$v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$$

$$v_p(ab) = v_p(a) + v_p(b)$$

$$|a+b|_p \leq \max\{|a|_p, |b|_p\}$$

$$|ab|_p = |a|_p |b|_p$$

Such an absolute value is called a non-archimedean absolute value. When $v_p(a) \neq v_p(b)$ the inequality becomes equality, and in fact, this holds for all non-archimedean absolute value and valuation. Additionally, it's not hard to see the p-adic absolute value induces a metric on $\mathbb{Q}$.

Proof. See 2.1.3 in [1]. □

With such a metric, we can have a Cauchy sequence $\{x_n\}$ that doesn't converge, for example

$$x_n = \sum_{k=0}^{n} p^{k^2}$$

If we look more carefully we can also show that each Cauchy sequence has an eventual constant valuation and absolute value, so we can assign that as the absolute value of the Cauchy sequence. If two Cauchy sequence differ by a sequence converges to 0, then they will be assigned the same

absolute value, which leads to the following: Quotient the ring of Cauchy sequence by the ideal consists of sequence that converges to 0 (it can be verified that it is maximal ideal), we get our $\mathbb{Q}_p$. Based on our previous discussion, each class of Cauchy sequence, hence each element of $\mathbb{Q}_p$, has an natural valuation and absolute value, so we extended v_p and $|\cdot|_p$ to $\mathbb{Q}_p$, a field which is a non-trivial completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Up to now, we extend v_p and $|\cdot|_p$ from $\mathbb{Q}$ to $\mathbb{Q}_p$ while everything in Proposition 3.2 still holds. Therefore we can show that addition and multiplication by a certain element are continuous with respect to this metric.

Proposition 3.3. For each $r \in \mathbb{Q}$ such that $|r|_p \leq 1$, there exists a unique sequence $\{x_n\}_{n=0}^{\infty}$ such that each $x_n \in \{0, 1, ..., p-1\}$ and r=$\lim_n \sum_{k=0}^{n} x_k p^k$.

Proof. Let $r = \frac{a}{b}$, $p \nmid b$, pick $\{x_n\}_{n=0}^{\infty}$ such that

$$\sum_{k=0}^{n} x_n p^n \equiv ab^{-1} \pmod{p^{n+1}}$$

□

Write $r_i = \sum_{n=0}^{\infty} x_{i,n} p^n$, if $\{r_i\}$ is a Cauchy sequence, then for each n, $x_{i,n}$ must be eventually constantly x, call it x_n. So the limit of r_i in $\mathbb{Q}_p$ can be written as $\sum_{k=0}^{\infty} x_n p^n$. Adjust by p we can have the for general $x \in \mathbb{Q}_p$

$$x = \sum_{n=k}^{\infty} x_n p^n$$

where k may be negative.

Definition 3.3 The ***valuation ring*** of a field k with a valuation v is the following

$$\{x \in k : v(x) \geq 0\}$$

In the case of $\mathbb{Q}_p$, we denote the valuation ring of it by $\mathbb{Z}_p$.

A quick observation on the representation of each p-adic integer gives us that its residue field is $\mathbb{F}_p$ and the image of each element in $\mathbb{Z}_p$ in the residue field is the coefficient of p^0 in its series representation.

Now one may wonder, how does $\mathbb{Q}_p$ behave algebraically? Well, it's certainly not algebraically closed. For example, if the image of u is not a square in the residue field, there cannot exist a square root of u in $\mathbb{Q}_p$. On this note, Hensel's lemma enables us to solve $f(x) \in \mathbb{Z}_p[x]$ by solving its image in $\mathbb{F}_p[x]$.

Theorem (Hensel's Lemma). Let $F(x) \in \mathbb{Z}_p[x]$. Suppose there exist $a_1 \in \mathbb{Z}_p$ such that $|F(a_1)|_p < 1$ and $|F'(a_1)|_p = 1$, let

$$a_n := a_{n-1} - \frac{F(a_n)}{F'(a_n)}$$

for all $n > 1$, then $\{a_n\}$ converges and its limit, call it a, is the unique p-adic integer such that $|a - a_1|_p < 1$ and $F(a) = 0$.

Proof. See theorem 4.5.3 in [1]. □

Notice that finding a_1 such that $|F(a_1)|_p < 1$ is equivalent to finding an $a_1 \in \mathbb{F}_p$ such that

$$F(a_1) \equiv 0 \pmod{p}$$

On the other hand, we may lift an irreducible polynomial in $\mathbb{F}_p[x]$ to a monic irreducible polynomial in $\mathbb{Z}_p[x]$ which is also irreducible in $\mathbb{Q}_p$, since $\mathbb{Z}_p$ is a UFD (with the unique prime element p) and $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$. In particular, the algebraic closure of $\mathbb{Q}_p$ is not a finite extension since we can find an irreducible polynommial in $\mathbb{F}_p[x]$ of arbitrarily high degree.

Before we turn our focus on the extension of $\mathbb{Q}_p$, I would like to mention the the following

Definition 3.3 ***Techmüller representative*** is the p distinct solutions to $x^p - x$, which can be written as $\{0, t, t^2, ..., t^{p-1}\}$, whose existence is guaranteed by Hensel's lemma. Moreover, as its name suggested, we can use them as the coefficient of p^n to represent each element of $\mathbb{Q}_p$, which is sometimes more natural than to use the standard representative, namely $\{0, 1, ..., p-1\}$.

Now it's time to consider algebraic number over $\mathbb{Q}_p$. For each algebraic number α over $\mathbb{Q}_p$, we can verify that the absolute value given by $||\alpha||_p := ||N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)||_p^{\frac{1}{[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]}}$, where N is the usual field norm, is again a non-archimedean absolute value on the algebraic closure $\overline{\mathbb{Q}_p}$. Equivalently, we can also have $v_p(\alpha) := v_p(N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha))/[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$. It's worth to note that the image of $\overline{\mathbb{Q}_p}$ under v_p is $\mathbb{Q} \subset \mathbb{R}$, and the residue field of the valuation ring

$$\{x \in \overline{\mathbb{Q}_p} : ||x||_p \geq 1\}$$

is $\overline{\mathbb{F}_p}$. Due to this, the valuation ring is no longer a PID, and in contrast to the case of finite extenstion of $\mathbb{Q}_p$, we do not have a nice series representation of element of $\overline{\mathbb{Q}_p}$.

We also want to remark that $\overline{\mathbb{Q}_p}$ is not complete anymore.

Remark 3.5. Pick integers $f_0, f_1, ...$ such that $f_i < f_{i+1}$ and $f_i | f_{i+1}$, and ζ_i is $p^{f_i} - 1$th root of unity, consider $c = \sum_{i=0}^{\infty} \zeta_i p^i$. If $\overline{\mathbb{Q}_p}$ is complete, then c is an algebraic number since $||\zeta_i||_p = 1$ for each i. $c \equiv \zeta_0 \pmod{p}$ gives us that $\mathbb{Q}_p(\zeta_0) \subset \mathbb{Q}_p(c)$ hence $[\mathbb{Q}_p(c) : \mathbb{Q}_p] \geq [\mathbb{Q}_p(\zeta_0) : \mathbb{Q}_p] = f_0$, and consider $(c - \zeta_0)/p$ and repeat. We can show $[\mathbb{Q}_p(c) : \mathbb{Q}_p] \geq f_i$ for all i, but $f_i > i$ apparently, so c is not algebraic.

Proposition 3.6. For any field K that has characteristics 0 and is complete with respect to a non-archimedean absolute value $|\cdot|$, let

$$f(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$$

be a monic irreducible polynomial of degree n, then exist $\varepsilon > 0$ such that for all

$$g(x) = \sum_{i=0}^{n} b_i x^i \in K[x]$$

monic degree n polynomial, if $|a_i - b_i| < \varepsilon$ for all i, then g is irreducible as well.

Proof. See 6.8.3 in [1]. □

Let $\mathbb{C}_p$ denote the completion of $\overline{\mathbb{Q}_p}$ (exactly the same when we construct $\mathbb{Q}_p$ by completing $\mathbb{Q}$), given the previous proposition, we have the following.

Theorem 3.7. $\mathbb{C}_p$ is algebraically closed and complete with respect to $|| \cdot ||_p$.

Proof. Completeness naturally follows from that it is a completion of $\overline{\mathbb{Q}_p}$. Let $f(x)$ be a monic irreducible polynomial in $\mathbb{C}_p[x]$, let ε be the one in proposition 3.6, since $\overline{\mathbb{Q}_p}$ is dense in $\mathbb{C}_p$, we can find $g(x) \in \overline{\mathbb{Q}_p}[x]$ satisfies the condition in 3.6, hence we have g is irreducible in $\mathbb{C}_p$ therefore in $\overline{\mathbb{Q}_p}$. Since $\overline{\mathbb{Q}_p}$ is algebraically closed, degree of $g(x)$ is 1, so is the degree of $f(x)$, implying the algebraic closedness of $\mathbb{C}_p$. □

Chapter 4

p-adic Analysis

Having introduced $\mathbb{C}_p$, we can start talking about analysis on p-adic numbers. More specifically, we will focus on how power series with coefficients in $\mathbb{C}_p$ (elements of $\mathbb{C}_p[[X]]$) behaves. Indeed, to some extent it is easier to do analysis over $\mathbb{C}_p$ than to do analysis over real or complex numbers, for a series over $\mathbb{C}_p$ converges if and only if its terms goes to 0, due to that $|\cdot|_p$ is a non-Archimedean norm. In particular, there is no such thing as "conditional convergence" for a power series over $\mathbb{C}_p$.

Proposition 4.1. For each $f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathbb{C}_p[[X]]$, let

$$r := \frac{1}{\limsup |a_n|_p^{1/n}}$$

Consider $x \in \mathbb{C}_p$, if $|x|_p > r$, $f(x)$ diverges and if $|x|_p < r$, $f(x)$ converges. In other words, r is the radius of convergence of $f(X)$.

Proof. Everything lies in the fact that $|\cdot|_p$ is a non-Archimedean absolute value, so $f(x)$ converges if and only if $\lim |a_n x^n| = 0$. □

What about x such that $|x|_p = r$? Things are simplified a little over $\mathbb{C}_p$. Indeed, $f(x)$ converges for $|x|_p = r$ if and only if $\lim |a_n| r^n = 0$ (hence the lack of conditional convergence).

Proposition 4.2. The function given by a power series is continuous wherever it converges.

Proof. If $x \neq 0$, then for$|x'|$ in a small enough neighborhood of x has the same norm as x, and observe

$$\begin{aligned}
|f(x) - f(x')|_p &= |\sum_{i=0}^{\infty} a_i (x^i - x'^i)|_p \\
&= \max_n \{|a_n|_p |x^i - x'^i|_p\} \\
&= \max_n \{|a_n|_p |x - x'|_p | \sum_{i=1}^{n} x^{n-i} x'^{i-1}|_p\} \\
&\leq \max_n \{|a_n|_p |x - x'|_p |x|_p^{n-1}\} \\
&= \frac{|x - x'|_p}{|x|_p} \max_n \{|a_n|_p |x|_p^n\}
\end{aligned}$$

□

Corollary 4.3. Considering the usual definition of derivative, then differentiation of a function given by power series is the differentiation by terms.

Now we can consider some usual function p-adically.

Definition 4.4 We define p-adic logarithm and p-adic exponential function as follow

$$\log_p(1 + X) := \sum_{i=1}^{\infty} (-1)^{i+1} x^i / i$$

$$\exp_p(X) := \sum_{i=0}^{\infty} x^i / n!$$

Some computation gives that $\log_p(1+X)$ converges at x if and only if $|x|_p < 1$, while $\exp_p(X)$ converges at x if and only if $|x| < p^{-1/(p-1)}$.

Given some formal power series itentities over $Q[[X,Y]]$ some close examination of composition of power series, we have

$$\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y)$$

$$\exp_p(x+y) = \exp_p(x)\exp_p(y)$$

For $|x|_p < p^{-1/(p-1)}$

$$\log_p(\exp(x)) = x$$

$$\exp_p(\log(1+x)) = 1+x$$

Another interesting power series to consider p-adically is the binomial series.

Definition 4.5

$$B_{a,p}(X) := \sum_{i=0}^{\infty} \frac{a(a-1)\cdots(a-i+1)}{i!} X^i$$

Some computation gives that if $|a|_p > 1$, then $B_{a,p}(X)$ converges if and only if $|x|_p < p^{-1/(p-1)}/|a|_p$, while $|a|_p < 1$, it converges at least for all $|x|_p < p^{-1/(p-1)}$. In addition, we do have a more accurate convergence when $a \in \mathbb{Z}_p$.

Proposition 4.6. When $a \in \mathbb{Z}_p$, $B_{a,p}(X) \in \mathbb{Z}_p[[X]]$. In particular, $B_{a,p}(x)$ converges at least when $|x|_p < 1$.

Proof. Recall that integers are dense in $\mathbb{Z}_p$. For each i, the polynomial $\frac{a(a-1)\cdots(a-i+1)}{i!}$ on a is continuous.
For each integer a_n, $\frac{a_n(a_n-1)\cdots(a_n-i+1)}{i!} \in \mathbb{Z} \subset \mathbb{Z}_p$. Now pick a_n that converges to a, the result follows. □

Again, by the formal identities on $\mathbb{Q}[[X]]$, given convergence we have

$$(B_{m/n,p}(x))^n = (1+x)^m$$

So we can write $B_{m/n,p}(x) = (1+x)^{m/n}$

We have another technical lemma.

Lemma 4.7. Let $F(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{Q}_p[[X]]$ i.e., $a_0 = 1$, $F(X) \in 1 + X\mathbb{Z}_p[[X]]$ if and only if $F(X^p)/(F(X))^p \in 1 + pX\mathbb{Z}_p[[X]]$.

Proof. To show the direct implication, we know that

$$F(X)^p \equiv F(X^p) \pmod{p}$$

therefore

$$F(X)^p/F(X^p) - 1 \equiv 0 \pmod{p}$$

hence $F(X^p)/(F(X))^p \in 1 + pX\mathbb{Z}_p[[X]]$.

Conversely suppose $F(X^p) = (F(X))^p G(X)$ where $G(X) = \sum_{i=0}^{\infty} b_i X^i \in 1 + pX\mathbb{Z}_p[[X]]$. We know that $a_0 = 1$, so a proof by induction is quite inviting. Assume that $a_i \in \mathbb{Z}_p$ for all $i < n$ and equate the coefficient of X^n on both side. We found that $a_{n/p}$ (is 0 if n/p is not integer) equals $pa_n + b_n$ plus bunch of terms like $b_{i_0} a_{i_1} a_{i_2} \cdots a_{i_p}$ where $\sum_{j=0}^{p} i_j = n$ and none of i_j's is n. Notice that if $i_0 \neq 0$, then $b_{i_0} \in p\mathbb{Z}_p$ and $a_{i_j} \in \mathbb{Z}_p$, then $b_{i_0} a_{i_1} a_{i_2} \cdots a_{i_p} \in p\mathbb{Z}_p$. If $a_{n/p} = 0$, then if it follows that $pa_n \in p\mathbb{Z}_p$ implies $a_n \in \mathbb{Z}_p$. Otherwise, notice that the term $a_{n/p}^p$ is also on the right hand side, and $a_{n/p}^p - a_{n/p} \in p\mathbb{Z}_p$, hence the conclusion. □

By similar argument we can extend this to the following statement: for $F(X,Y) \in 1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$, we have $F(X,Y) \in 1 + X\mathbb{Z}_p[[X,Y]] + Y\mathbb{Z}_p[[X,Y]]$ if and only if $F(X^p, Y^p)/(F(X,Y))^p \in 1 + pX\mathbb{Z}_p[[X,Y]]$

We end this section with an application of this lemma to a series that will be useful later on. Let $F(X,Y) := (1+Y)^X \prod_{i=1}^{\infty} (1+Y^{p^i})^{(X^{p^i} - X^{p^{i-1}})/(p^{i-1})}$ where exponent is given by the binomial series. $1 + Y \in 1 + \mathbb{Z}_p[[Y]]$ implies $(1+Y^p)/(1+Y)^p = 1 + YG(Y)$ where $G(Y) \in p\mathbb{Z}_p[[Y]]$ by lemma 4.7. We have

$$(1+Y^p)^X/(1+Y)^{pX} = (1+YG(Y))^X = \sum_{i=0}^{\infty} \frac{X(X-1)\cdots(X-i+1)}{i!}(YG(Y))^i$$

Notice that $G(Y)^i \in p^i\mathbb{Z}_p[[Y]]$, so

$$F(X^p, Y^p)/(F(X,Y))^p = (1+Y^p)^X/(1+Y)^{pX} \in 1 + pX\mathbb{Z}_p[[X]] + pY\mathbb{Z}_p[[Y]]$$

which gives us that $F(X,Y) \in 1 + X\mathbb{Z}_p[[X,Y]] + Y\mathbb{Z}_p[[X,Y]] \subset \mathbb{Z}_p[[X,Y]]$ by lemma 4.7 again.

Chapter 5

Rationality of Zeta Function

In this section we will demonstrate that $\zeta_C(s)$ (developed in the second section) is a rational function of q^{-s} using p-adic techniques developed in the third and fourth section. We do this by following and filling some gaps in the proof given in [2]. To begin with, we explore a connection between $\mathbb{F}_q$ and $\mathbb{C}_p$ to take advantage of p-adic analysis we just developed.

Definition 5.1 A $\mathbb{C}_p$***-valued character*** of a finite group G is a homomorphism from G to $\mathbb{C}_p^\times$.

A natural example of $\mathbb{C}_p$-valued character of additive group of $\mathbb{F}_p$ is

$$a \mapsto \varepsilon^a$$

where ε is a p-th primitive root of unity and observe consider a as an integer whose image in $\mathbb{F}_p$ is a. Moreover, let

$$\text{Tr } a := \sum_{\sigma \in Gal(\mathbb{F}_q/\mathbb{F}_p)} \sigma(a) = \sum_{n \geq 0,\ p^n < q} a^{p^n}$$

Tr a is fixed by everything in $Gal(\mathbb{F}_q/\mathbb{F}_p)$ so it is in $\mathbb{F}_p$. It's also additive, so we have a character of $\mathbb{F}_q$ given by

$$a \longrightarrow \varepsilon^{\text{Tr } a}$$

Now considering $F(X, Y)$ given in Lemma 4.7, it's easy to verify that

$$(1+Y)^{t+t^p+\cdots+t^{p^{s-1}}} = F(t, Y)F(t^p, Y)\cdots F(t^{p^{s-1}}, Y)$$

We set $\Theta(T) = F(T, \varepsilon - 1)$, and given that $\text{ord}_p(\varepsilon - 1) \geq 1/(p-1)$ (observe that the minimal polynomial of $(\varepsilon - 1)$ has degree $p-1$ and constant term p), we can verify that n-th coefficient of Θ has order greater than or equal to $n/(p-1)$, which gives its convergence in the unit disk. Moreover, given the Teichmuller representative a_t of $a \in \mathbb{F}_q = \mathbb{F}_{p^s}$, we can show that $\sum_{n\geq 0}^{s-1} a_t^{p^n} - Tr\ a = pu$ where u is a p-adic integer. Hence, observing that ε is a p-th root of 1,

$$\varepsilon^{Tr\ a} = \varepsilon^{\sum_{n\geq 0}^{s-1} a_t^{p^n} - pu} = \varepsilon^{\sum_{n\geq 0}^{s-1} a_t^{p^n}} \varepsilon^{-pu} = \varepsilon^{\sum_{n\geq 0}^{s-1} a_t^{p^n}}$$

Therefore, the character of $a \in \mathbb{F}_q$ can be given by

$$\Theta(a_t)\Theta(a_t^p)\cdots\Theta(a_t^{p^{s-1}})$$

Definition 5.2 Consider $\mathbb{C}_p[[x_1, x_2, \cdots, x_n]]$. Let $u := (u_1, u_2, \cdots, u_n)$ where u_k are integers greater than or equal to 0. Then we denote $x_1^{u_1}\cdots x_n^{u_n}$ by x^u. Given suitable context, we also use $u + w$ to denote $(u_1 + w_1, \cdots, u_n + w_n)$, ku to denote $(ku_1, \cdots, ku_n)$ and k to denote $(k, \cdots, k)$. We define the following linear maps on $\mathbb{C}_p[[x_1, x_2, \cdots, x_n]]$:

$$T_q : \sum a_u x^u \mapsto \sum a_{qu} x^u,$$
$$G : r \mapsto Gr,$$

where $G \in \mathbb{C}_p[[x_1, x_2, \cdots, x_n]]$ and Gr is series multiplication. Also, we can show that $G \circ T_q = T_q \circ G_q$ where $G_q(x) = G(x^q)$. We also have the linear map

$$\Psi_{q,G} := T_q \circ G.$$

In addition, we define

$$R_0 := \left\{ \sum g_w x^w \mid \text{there exists an } M > 0 \text{ such that for all } w,\ \text{ord}_p(g_w) \geq M|w| \right\},$$

where $|w| := w_1 + w_2 + \cdots + w_n$. It's clear that R_0 is a subring of $\mathbb{C}_p[[x_1, x_2, \cdots, x_n]]$. One primary example in R_0 is $\Theta(ax^w)$ if $\text{ord}_p(a) \geq 0$.

Definition 5.3 Let A be a linear map over $\mathbb{C}_p[[x_1, x_2, \cdots, x_n]]$, we may denote A as an "infinite" matrix $\{a_{w,v}\}$ where w and v ranges over all n-tuple of natural numbers and $a_{w,v}$ is the coefficient of x^w in $A(x^v)$. Moreover, since all n-tuple of natural numbers are countable, we can fix an enumeration and treat w and v as positive integers when suitable.

$$b_m := (-1)^m \sum_{\substack{u_1 < u_2 < \cdots < u_m, \\ \sigma \text{ is a permutation of the u's}}} sgn(\sigma) a_{u_1,\sigma(u_1)} \cdots a_{u_m,\sigma(u_m)}$$

and given convergence of each b_m we define

$$\det(1 - AT) := \sum b_m T^m$$

Also we define

$$TrA := \sum_w a_{w,w}$$

In our case, we are interested in A that is the matrix of $\Psi_{q,G}$ when $G \in R_0$. We found $\Psi_{q,G}(x^v) = \sum_u g_{qu-v} x^u$ therefore

$$a_{w,v} = g_{qw-v}$$

The convergence of TrA follows immediately from the definition of R_0.
As to b_m, assuming $qu_i - \sigma(u_i)$ does not have negative component for all i's(if there is a negative component then $g_{qu_i-\sigma(u_i)}$=0 and the following still holds), we have the following

$$\begin{aligned}
\text{ord}_p(a_{u_1,\sigma(u_1)} \cdots a_{u_m,\sigma(u_m)}) &= \text{ord}_p(g_{qu_1-\sigma(u_1)} \cdots g_{qu_m-\sigma(u_m)}) \\
&\geq M(|qu_1 - \sigma(u_1)| + \cdots + |qu_m - \sigma(u_m)|) \\
&\geq M(q \sum |u_i| - \sum |\sigma(u_i)|) \\
&= M(q-1) \sum |u_i|
\end{aligned}$$

It's clear that for each B, there are only finitely many choices of m distinct u_i's such that $\sum |u_i| < B$, hence the convergence of b_m for each m and that

$$\inf \left\{ \frac{1}{m} \sum_{i=1}^{m} |u_i| \mid u_i\text{'s are distinct} \right\} \to \infty \text{ as } m \to \infty$$

which gives us

$$\frac{1}{m} \text{ord}_p(b_m) \to \infty \text{ as } m \to \infty$$

Therefore $\det(1 - AT)$ is a well defined power series and gives an entire function.

Proposition 5.4. Use the previous notation and let $G \in R_0$. We have the following identity

$$(q^s-1)^n \mathrm{Tr}(\Psi_{q,G}^s) = \sum_{\substack{x\in\mathbb{C}_p^n,\\ x^{(q^{s-1})}=(1,1,\cdots,1)}} G(x)G(x^q)\cdots G(x^{q^{s-1}})$$

Proof. First assume $s=1$. Notice that

$$\sum_{x^{q-1}=(1,\cdots,1)} x^w = \prod_{i=1}^n (\sum_{x^{q-1}=1} x^{w_i})$$

and

$$\sum_{x^{q-1}=1} x^k = \begin{cases} q-1, & \text{if } q \mid k, \\ 0, & \text{otherwise.} \end{cases}$$

so we can have

$$\begin{aligned} \sum_{x^{q-1}=(1,1,\cdots,1)} G(x) &= \sum_w g_w (\sum_{x^{q-1}=(1,1,\cdots,1)} x^w) \\ &= \sum_w (q-1)^n g_{(q-1)w} \\ &= (q-1)^n Tr\Psi_{q,G} \end{aligned}$$

General case follows from $T_q^s = T_{q^s}$ and $G \circ T_q = T_q \circ G_q$ □

Proposition 5.5. Let $G \in R_0$, A be the matrix of $\Psi_{q,G}$, then we have

$$\det(1-AT) = \exp(-\sum_s \mathrm{Tr}(\Psi_{q,G}^s)T^s/s)$$

and it's an entire function.

Proof. Let A_i denote the finite matrix $\{a_{w,v}\}_{w,v\le i}$, and this

$$\det(1-A_iT) = \exp(-\sum_s \mathrm{Tr}(A_i^s)T^s/s)$$

follows immediately after a change of basis to make A_i upper-triangular.
Now we only need to prove $\det(1-A_iT)$(resp. $\exp(-\sum_s \mathrm{Tr}(A_i^s)T^s/s)$) converge to $\det(1-AT)$ (resp. $\exp(-\sum_s \mathrm{Tr}(A^s)T^s/s)$ coefficient-wise. Let $b_{m,i}$ denote the coefficient of T^m in $\det(1-A_iT)$, and we have

$$b_{m,i} = (-1)^m \sum_{\substack{u_1<u_2<\cdots<u_m\le i,\\ \sigma \text{ is a permutation of the u's}}} sgn(\sigma) a_{u_1,\sigma(u_1)}\cdots a_{u_m,\sigma(u_m)}$$

Therefore

$$b_m - b_{m,i} = (-1)^m \sum_{\substack{u_1<u_2<\cdots<u_m,\\ \sigma \text{ is a permutation of the u's,}\\ \text{at least one of the } u\text{'s is greater than } i}} sgn(\sigma) a_{u_1,\sigma(u_1)} \cdots a_{u_m,\sigma(u_m)}$$

and $\text{ord}_p(b_m - b_{m,i})$ clearly goes to infinity as i goes to infinity by our estimation of $\text{ord}_p(a_{u_1,\sigma(u_1)} \cdots a_{u_m,\sigma(u_m)})$ after definition 5.3, hence the coefficient-wise convergence of $\det(1 - A_i T)$ to $\det(1 - AT)$.
On the other hand, to show $\exp(-\sum_s \text{Tr}(A_i^s)T^s/s) \to \exp(-\sum_s \text{Tr}(A^s)T^s/s)$ coefficient by coefficient, we only need to show that for each s,

$$TrA_i^s \to TrA^s \text{ as } i \text{ goes to infinity}$$

Observing that

$$TrA_i^s = \sum_{1\le k_1,\cdots,k_s\le i} a_{k_1,k_2} a_{k_2,k_3} \cdots a_{k_s,k_1}$$

and

$$TrA^s = \sum_{1\le k_1,\cdots,k_s} a_{k_1,k_2} a_{k_2,k_3} \cdots a_{k_s,k_1}$$

Similar estimation gives

$$\begin{aligned} \text{ord}_p(a_{k_1,k_2} a_{k_2,k_3} \cdots a_{k_s,k_1}) &= \text{ord}_p(g_{qk_1-k_2}) + \cdots + \text{ord}_p(g_{qk_s-k_1}) \\ &\ge M(|qk_1 - k_2| + \cdots + |qk_s - k_1|) \\ &\ge M(q-1)\sum_{t=1}^{s} |k_t| \end{aligned}$$

and the desired convergence follows at once. The fact that it gives an entire function is discussed after definition 5.3. □

With this much preparation, we are ready to study zeta function itself and demonstrate its rationality.

Definition 5.6 Let $N_s = \#\{\text{loci of } f(x_1, \cdots, x_n) \text{ in } \mathbb{F}_{q^s}^n\}$ and
$N'_s = \#\{\text{loci of } f \text{ in } \mathbb{F}_{q^s}^n \text{ that does not have a zero component}\}$, we define

$$Z(H_f, T) = \exp(\sum N_s T^s/s)$$

$$Z'(H_f, T) = \exp(\sum N'_s T^s/s)$$

This is the affine version of $\zeta_C(s)$ after a change of variable (replace q^{-s} with T) and generalized it to any hypersurface, as opposed to ζ_C we introduced earlier is limited to non-singular curves. Certainly, the rationality of Z immediately implies the rationality of $\zeta_C(s)$ in variable of q^{-s}

Proposition 5.7. $Z'(H_f, T)$ is a quotient of two entire functions (given by power series), and so is $Z(H_f, T)$, for arbitrary f.

Proof. First we prove that if $Z'(H_f, T)$ is entire then $Z(H_f, T)$ is entire as well. We use $N'_{s,x_{i_1},\cdots,x_{i_k}}$ to denote the number of loci of $f_{x_{i_1},\cdots,x_{i_k}}$ in $\mathbb{F}_q^s$ that does not have zero component where $f_{x_{i_1},\cdots,x_{i_k}}$ is obtained by plugging 0 into $x_{i_1}, \cdots, x_{i_k}$ in f. The inclusion-exclusion principle gives us

$$N_s - N'_s = \sum_{k=1}^{n} \sum_{i_1<\cdots<i_k} (-1)^{k-1} N'_{s,x_{i_1},\cdots,x_{i_k}}$$

The add-multiply property of exponential power series gives us

$$\frac{Z(H_f,T)}{Z'(H_f,T)} = \frac{\prod_{k \text{ odd}} \prod_{i_1<\cdots<i_k} Z'(H_{f_{x_{i_1},\cdots,x_{i_k}}},T)}{\prod_{k \text{ even}} \prod_{i_1<\cdots<i_k} Z'(H_{f_{x_{i_1},\cdots,x_{i_k}}},T)}$$

By our assumption, $Z(H_f, T)$ is entire. Now we are left to prove $Z'(H_f, T)$ is entire for arbitrary f. From linear independence of automorphism we know Tr over $\mathbb{F}_{q^s}$ is not a zero function. Combining that with its additivity, we derived that for any $u \in \mathbb{F}_{q^s}$,

$$\sum_{x_0 \in \mathbb{F}_{q^s}} \varepsilon^{\text{Tr}(x_0 u)} = \begin{cases} q^s, & u = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Subtract $x_0 = 0$ from the summation we have

$$\sum_{x_0 \in \mathbb{F}_{q^s}^{\times}} \varepsilon^{\text{Tr}(x_0 u)} = \begin{cases} q^s - 1, & u = 0, \\ -1, & \text{otherwise.} \end{cases}$$

Given this, some elementary counting gives

$$\begin{aligned} \sum_{x_0,x_1,\cdots,x_n \mathbb{F}_{q^s}^{\times}} \varepsilon^{\text{Tr}(x_0 f(x_1,\cdots,x_n))} &= (q^s-1)N'_s - ((q^s-1)^n - N'_s) \\ &= q^s N'_s - (q^s-1)^n \end{aligned}$$

Recall the power series representation of $\mathbb{C}_p$ valued character and notations we developed in definition 5.1, and write $x_0 f(x_1, \cdots, x_n) = \sum_w a_w x^w$ and we let $F(x_0, \cdots, x_n) := \sum_w a_{wt} x^w \in \mathbb{C}_p[x_0, \cdots, x_n]$ where $a_w t$ is the Teichmuller representation of a_w. We know that given a w and $x = (x_0, \cdots, x_n) \in \mathbb{F}_{q^s}^{n+1}$

$$\begin{aligned} \varepsilon^{\text{Tr}(a_w x^w)} &= \varepsilon^{\text{Tr}(a_{wt} x_t^w)} \text{ where } x_t = (x_{0t}, \cdots, x_{nt}) \in \mathbb{C}_p^{n+1} \\ &= \Theta(a_{wt} x_t^w)\Theta(a_{wt}^p x_t^{pw}) \cdots \Theta(a_{wt}^{p^{rs-1}} x_t^{p^{rs-1}w}) \end{aligned}$$

where r is such that $p^r = q$. Also notice that $\{x \in \mathbb{C}_p^{n+1} | x^{q^s-1} = (1, \cdots, 1)\}$= $\{(x_{0t}, \cdots, x_{nt}) | x_i \in \mathbb{F}_{q^s}^{\times}, x_{it} \text{ is the Teichmuller representation of } x_i\}$ Put everything together we attain

$$q^s N'_s = (q^s-1)^n - \sum_{\substack{x \in \mathbb{C}_p^{n+1}, \\ x^{q^s-1} = (1,1,\cdots,1)}} \prod_w (\Theta(a_{wt} x^w)\Theta(a_{wt}^p x^{pw}) \cdots \Theta(a_{wt}^{p^{rs-1}} x^{p^{rs-1}w}))$$

where r is such that $p^r = q$.
If we define $G(x) := \prod_w \Theta(a_{wt}x^w)\Theta(a_{wt}^p x^{pw}) \cdots \Theta(a_{wt}^{p^{r-1}} x^{p^{r-1}w})$ and observing that $a_{wt}^q = a_{wt}$ for each w, we can rewrite the above as

$$q^s N_s' = (q^s - 1)^n - \sum_{\substack{x \in \mathbb{C}_p^{n+1}, \\ x^{q^s-1} = (1,1,\cdots,1)}} \prod_w G(x)G(x^q)\cdots G(x^{q^{s-1}})$$

Since $\Theta \in R_0$, $G \in R_0$ clearly, and proposition 5.4 applies at once. Let A be the matrix of $\Psi_{q,G}$ We can write

$$N_s' = \frac{(q^s-1)^n - (q^s-1)^{n+1}\mathrm{Tr}(A^s)}{q^s}$$

Plug this expression into $Z'(H_f, T)$ and apply proposition 5.5, and the desired result follows immediately. □

Proposition 5.8. Let $F(x) = \sum a_i x^i \in k[[x]]$ where k is a field and define matrix

$$A_{s,m} := \begin{bmatrix} a_s & a_{s+1} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & \cdots & \cdots & a_{s+2m} \end{bmatrix}$$

Let$N_{s,m} := detA_{s,m}$, If there exist an m such that there exists S and $N_{s,m} = 0$ for all $s > S$, then F is rational.

Proof. Choose m to be the smallest with such S, and we claim that $N_{s,m-1} \neq 0$ for all $s > S$. Assume otherwise, then vectors

$$\{(a_s, \cdots, a_{s+m-1}), (a_{s+1}, \cdots, a_{s+m}), \cdots, (a_{s+m-1}, a_{s+m-2})\}$$

are linearly dependent and they satisfy a non-trivial linear relation. Assume the first vector is involved in this linear relation, then some elementary row operations can make $A_{s,m}$ into

$$\mathscr{A}_{s,m} = \begin{bmatrix} 0 & 0 & \cdots & \beta \\ a_{s+1} & a_{s+2} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & \cdots & \cdots & a_{s+2m} \end{bmatrix}$$

The bottom-right m minor of $\mathscr{A}_{s,m}$ is $A_{s+1,m-1}$, and the upper-left m minor of it is $A_{s+1,m-1}$ after the same row operations. $0 = N_{s,m} = \det(\mathscr{A}_{s,m}) = \beta \det(A_{s-1,m+1})$ up to a sign, so either β or $\det(A_{s-1,m+1})$ equals 0. In either cases, $\det(A_{s-1,m+1})$ has to be zero. It's even easier to verify that $\det(A_{s-1,m+1}) = 0$ if the first vector does not involve in the linear relation. What we just showed is that $N_{s,m} = 0$ and $N_{s,m-1}$ implies $N_{s+1,m-1} = 0$. Together with our assumption we deduce that if $s > S$ and $N_{s,m-1} = 0$, then $N_{s+1,m-1} = 0$, then $N_{s+2,m-1} = 0$ and so on, which contradicts the minimality of m. The upshot is that in $A_{s,m}$ for each $s > S$, the last row has to be a linear combination of the previous rows since $N_{s,m} = 0$ and $N_{s,m-1} \neq 0$.

Now let's fix an $s_0 > S$ and a non-zero vector $v = (c_0, c_1, \cdots, c_m)$ such that $A_{s_0,m}(v) = 0$, then we know $A_{s_0+1,m}(s) = (0, \cdots, 0, \beta)$,since the first m rows of $A_{s_0+1,m}$ is the last m rows of $A_{s_0,m}$. But the last row of $A_{s_0+1,m}$ is a linear combination of previous rows, we have $\beta = 0$ hence $A_{s_0+1,m}(v) = 0$. Repeating this, we find $A_{s,m}(v) = 0$ for all $s \geq s_0$. More specially, we can check that this means $F(x)(\sum_{i=0}^{m} c_{m-i}x^i)$ is a polynomial, hence the result. □

Here is one last auxiliary result before the final proof.

Proposition 5.9. Let f be a polynomial in n variables, then the coefficient of T^s in $Z(H_f, T)$ is integer and less than or equal to q^{ns} for each s.

Proof. First we associate an integer $s(x)$ to $x \in \{\text{loci of } f \text{ in } \overline{\mathbb{F}_q}^n\}$ where $s(x)$ is the smallest s such that $x \in \mathbb{F}_{q^s}^n$, and we define an equivalence relation $\sim$ by having $x \sim y$ if and only $s(x) = s(y)$ and there exists a $\sigma \in Gal(\mathbb{F}_{q^{s(x)}}/\mathbb{F}_q)$ such that $\sigma(x) = y$(σ acts on x by acting on each component of x). Given an x, we found that no non-identity element in $Gal(\mathbb{F}_{q^{s(x)}}/\mathbb{F}_q)$ fix x (otherwise each component lies in the fixed field), so the class of x, denoted by $[x]$, has $|Gal(\mathbb{F}_{q^{s(x)}}/\mathbb{F}_q)| = s(x)$ elements. So each class $[x]$ contribute $s(x)$ to N_s if and only if $s(x)|s$, and we can write

$$Z(H_f, T) = \prod_{[x]} \exp(\sum_j s(x)T^{js(x)}/s)$$

and $\exp(\sum_j s(x)T^{js(x)}/s) = (\exp(-Log(1 - T^{s(x)})))^{s(x)} = \dfrac{1}{(1 - T^{s(x)})^{s(x)}}$ which gives us that each coefficient is integer. The maximal possible coefficients are achieved in

$$\exp(\sum_s q^{ns}T^s/s) = \frac{1}{1 - q^nT} = 1 + q^nT + q^{2n}T^2 \cdots$$

hence our bound of coefficients holds. □

Theorem 5.10. $Z(H_f, T)$ is rational.

Proof. Let $Z = Z(H_f, T)$, then $Z = A/B$ where A and B are entire. By p-adic Weierstrass preparation theorem (see theorem 7.2.10 in [1]), we have $B = P/G$ where P is a polynomial and G is a series that converges in the disk of radius q^{2n}. We let $F = A \cdot G$, which converges in the disk of radius q^{2n} as well. We write

$$F = \sum b_iT^i,\ P = \sum_{i=0}^{e} c_iT^i,\ Z = \sum a_iT^i$$

and we have

$$F = P \cdot Z$$

Equating the coefficient gives

$$b_{j+e} = a_{j+e} + c_1a_{j+e-1} + \cdots + c_ea_j$$

Now let $A_{s,m}$ denote the matrix associate to Z as in proposition 5.8. Pick $m > 2e$ and

$$A_{s,m} := \begin{bmatrix} a_s & a_{s+1} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & \cdots & \cdots & a_{s+2m} \end{bmatrix}$$

After some row operations on $A_{s,m}$ using the linear relation above we have

$$\mathscr{A}_{s,m} := \begin{bmatrix} a_s & a_{s+1} & \cdots & a_{s+e-1} & b_{s+e} & \cdots & b_{s+m} \\ a_{s+1} & a_{s+2} & \cdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ a_{s+m} & \cdots & \cdots & a_{s+e+m-1} & b_{s+e+m} & \cdots & b_{s+2m} \end{bmatrix}$$

We also know that $N_{s,m} = \det(A_{s,m})$ equals to $\det(\mathscr{A}_{s,m})$ up to a sign.
Looking at $A_{s,m}$, by our bounds of a_k given in proposition 5.9,

$$|N_{s,m}|_\infty \leq (m+!)!q^{n(m+1)(s+2m)} = (m+!)!q^{ns(m+1)}q^{2mnm+1}$$

where the $|\cdot|_\infty$ is the usual absolute value. On the other hand, we know F converges in disk of radius q^{2n}, so for all s large enough, $|b_s|_p < q^{-2ns}$ and if we look at $\mathscr{A}_{\cdot}$ and recall that a_s are integers (so $|a_s|_p \leq 1$) and $m > 2e$ we have

$$|N_{s,m}|_p < (q^{-2n(s+e)})^{m-e+1} < q^{-2ns(m/2+1)} = q^{-ns(m+2)}$$

Put them together we have that for s large enough

$$|N_{s,m}|_\infty |N_{s.m}|_p < (m+1)!\frac{q^{ns(m+1)}q^{2mnm+1}}{q^{ns(m+2)}} = (m+1)!\frac{q^{2mnm+1}}{q^{ns}} < 1$$

While $N_{s,m}$ is clearly an integer, the only integer x such that $|x|_\infty |x|_p < 1$ is 0, so for s large enough, $N_{s.m} = 0$. By proposition 5.8, $Z(H_f, T)$ is rational. □

This result gives the rationality of the factors of $\zeta_C(s)$ that do not correspond to orbits that lie over infinity, i.e., consider $f(x, y)$ to be $F(x, y, 1)$. Since there are only finitely many places at infinity, rationality of $\zeta_C(s)$ follows immediately. More explicitly, we can write the following:

Remark 5.11. Let C be a complete non-singular curve given by F, considering the expression of $\zeta_C(s)$ given after lemma 2.8, we can immediately write down

$$\zeta_C(s) = Z(H_f, q^{-s}) \cdot Z(H_g, q^{-s}) \cdot Z(H_h, q^{-s})$$

where $f(x, y) := F(x, y, 1)$, $g(x) := F(x, 1, 0)$, $h := F(1, 0, 0)$ and $H_f \subseteq \mathbb{F}_q^2$, $H_g \subseteq \mathbb{F}_q^1$, $H_h \subseteq \mathbb{F}_q^0$. Therefore, $\zeta_C(s)$ is rational in variable q^{-s}.

Bibliography

[1] Fernando Q. Gouvêa *p-adic Numbers*, third ed., Universitext, Springer, Cham, [2020] ©2020, An introduction

[2] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984.

[3] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics, vol. 9, American Mathematical Society, Providence, RI, 1996.

Yifei Zhang

CONTACT INFORMATION
(814) 699-1923
yfz5308@psu.edu

EDUCATION

Pennsylvania State University-University Park, PA, 08/2018
Schreyer Honors College
B.S. Mathematics, Graduate Option
GPA: 3.93
Expected Graduation: 05/2022

HONORS AND AWARDS

Honor Program in Schreyer Honor College
Dean's List for all semesters

ACTIVITIES AND EXPERIENCE

Pennsylvania State University

Served as Learning Assistant for MATH140 Caculus with Analytic Geometry 08/2021-12/2021
- Held and facilitated Evening Session to support students' excellence.
- Answered questions during problem-solving class twice a week.

Partook in Putnam Mathematical Competition 12/2019

Served as Learning Assistant for Physics211 General Physics: Mechanics 01/2019-05/2019
- Answered questions during each class three times a week.

Participated in International Collegiate Programming Contest 11/2018
- Attained third Place at East Central NA Regional.

THESIS AND PROJECT

ZETA FUNCTION OF CURVES OVER FINTE FIELD
Zeta Function Of Curves Over Finite Field And Its Rationality (in progress)
- Read about and understood p-adic numbers and Arithmetic Geometry under the guidance of my Professor over the course of a year.
- Aimed to simplify the proof of the rationality of Zeta Function when the object of interest restricted to Complete Smooth Curves over Finite Field for the following year.

SKILLS AND QUALIFICATION

Languages: Proficient in Chinese and English.
Programming: Proficient in Mathematica, C++, Python and advanced Algorithms.