Zeta Functions

Dan Normand

Supervisors: Prof. Franz Pedit, Jason McGibbon

2015 - 2016

Contents

1 Background

Much of the work done on the first three sections of this thesis unsurprisingly rely on results from complex analysis. Many times our goal will be to show that a function we defined is analytic in a region, or that an integral, sum, or product converges. Instead of working through these questions when we encounter them, we develop some machinery now which we can apply later. This has the benefit of allowing us to more closely understand the actual functions we are working with as opposed to getting caught up in minor details, and this contributes to a more fluid, cohesive paper.

While the last section does involve some algebra, not much beyond rudimentary group and ring theory is used. For that reason I postpone the discussion of the machinery we use there until we reach that section of the paper.

1.1 Sequences, Series, Products

Let $Z = \{z_n\}$ be a set of complex numbers indexed by $\mathbb{N}$. We then say that Z is a *sequence* of complex numbers. We say that a sequence *approaches a limit*, or *has a limit*, or *converges* if there is some complex number ω such that for all $\epsilon > 0$, there exists some $N \in \mathbb{N}$ such that for all $n \geq N$,

$$|\omega - z_n| < \epsilon$$

Symbolically, we write this as

$$\lim_{n\to\infty} z_n = \omega \text{ or } z_n \to \omega$$

We say that ω is the *limit* of the sequence. It is not hard to show that if a sequence has a limit that the limit is unique, i.e. that if a sequence converges then it converges to exactly one limit.

There is an additional way to define convergence. We say a sequence $\{z_n\}$ is a *Cauchy sequence* if for any $\epsilon > 0$ there exists some $N \in \mathbb{N}$ such that for all $m, n \geq N$,

$$|z_m - z_n| < \epsilon$$

It is interesting to note that all convergent sequences are Cauchy. This is easy to see since, if $z_n \to \omega$,

$$|z_n - z_m| \leq |z_n - \omega| + |z_m - \omega|$$

Then there is some N_1, N_2 such that for all $n \geq N_1, m \geq N_2$, $|z_n - \omega|, |z_m - \omega| < \frac{\epsilon}{2}$, hence

$$|z_n - z_m| < \epsilon$$

We may now define series. Given a sequence of complex numbers $\{z_n\}$, we may define the *infinite series* (commonly referred to as simply *series*) as the limit of the sequence of partial sums, $\{S_n\}$, where

$$S_n = \sum_{m=0}^{n} z_m$$

if this limit exists. If the limit *does* exist, we write

$$\lim_{n\to\infty} S_n = \lim_{n\to\infty} \sum_{m=0}^{n} z_m = \sum_{m=0}^{\infty} z_m$$

There are many ways to tell if a *real* series converges or diverges. For that reason in the next section we examine how to turn complex series into real series. The one condition I will note here is that if $\lim_{n\to\infty} z_n \neq 0$, then the series $\sum z_n$ does not converge [5, 8].

Again, given a sequence of complex numbers $\{z_n\}$, we can define an *infinite product* as the limit of partial products P_n, where

$$P_n = \prod_{m=0}^{n} z_n$$

if this limit exists. If the limit *does* exist, we write

$$\lim_{n\to\infty} P_n = \lim_{n\to\infty} \prod_{m=0}^{n} z_n = \prod_{m=0}^{\infty} z_n$$

We will develop the machinery to determine if an infinite product converges or diverges momentarily, but it is obvious that if $z_n \not\to 0$ or $z_n \not\to 1$ then the product will not converge [5].

1.2 Absolute Convergence, Uniform Convergence

We now look at what it means for a series to converge *absolutely*. Given the series

$$\sum_{n=0}^{\infty} z_n$$

we say this series converges absolutely if the real series

$$\sum_{n=0}^{\infty} |z_n|$$

converges. If the name were not suggestive enough, absolute convergence of a series implies convergence of a series: by the triangle inequality we have that

$$|\sum_{m=0}^{n} z_n| \leq \sum_{m=0}^{n} |z_n|$$

Since the series on the right converges, this implies the series on the left must converge. There are cases in which a series converges but not absolutely, this is called *conditional* convergence and it is a weaker condition than absolute convergence. As such, we only focus on absolutely convergent series. Absolute convergence of series implies certain useful properties. The first is that we may rearrange the indexing of an absolutely convergent series without altering the total.

Lemma 1.1: Suppose the series $\sum z_n$ converges absolutely. Then any rearrangement of the series converges absolutely and to the same limit. If the double sum $\sum_n \sum_m z_{n,m}$ converges absolutely, then the series obtained by switching the order of summation also converges absolutely and to the same limit [5].

Proof: Let $f : \mathbb{N} \to \mathbb{N}$ be a bijection. Then the series defined by

$$\sum_{n=0}^{\infty} z_{f(n)}$$

is a permutation of the original series. We then define partial sums as

$$T_n = \sum_{m=0}^{n} z_{f(n)}$$

for this series. Let L be the limit of the original series. Given $\epsilon > 0$, we wish to show that there exists some N such that for all $n \geq N$,

$$|T_n - L| < \epsilon$$

For all $n, m \in \mathbb{N}$, we have that

$$|T_n - L| = |T_n - S_m + S_m - L| \leq |T_n - S_m| + |S_m - L|$$

Since we assume the original series converges absolutely, there is some M such that for all $m \geq M$, $|S_m - L| < \frac{\epsilon}{2}$. Similarly, since the original series converges absolutely, the series defined by the remainders

$$r_k = \sum_{k+1}^{\infty} |z_n|$$

must go to 0 as $n \to \infty$. Then there is some K such that for all $k \geq K$, $r_k < \frac{\epsilon}{2}$. Let $m \geq \max\{K, M\}$. Since f is a bijection, there are n_i such that $f(n_1) = 1, f(n_2) = 2, \ldots, f(n_m) = m$. Then for any $n \geq \max\{n_1, n_2, \ldots, n_m\}$, we have that

$$|T_n - S_m| < r_k < \frac{\epsilon}{2}$$

and we are done. The second claim about iterated sums follows immediately from the first.

Similar to series, infinite products may converge absolutely. We say the infinite product

$$\prod_{n=0}^{\infty} z_n$$

converges absolutely if and only if the series

$$\sum_{n=0}^{\infty} \log(z_n)$$

converges absolutely [5]. Take note that this is the *complex* logarithm and so we must be careful about how we choose the branch of logarithm to use (this is done by choosing finitely many z_n until, since the limit of the sequence must be 1, $z_n = 1 - w_n$, where $|w_n| < 1$. We can then take the series definition of the logarithm which is convergent in a small disc about any point[5]). This makes sense since

$$\prod_{m=0}^{n} z_m = e^{\log\left(\prod_{m=0}^{n} z_m\right)} = e^{\sum_{m=0}^{n} \log(z_m)}$$

Since these partial sums converge absolutely and exponentiation is a continuous operation, this shows that the limit exists and that the infinite product converges.

We may also define a parallel condition for integration. A real function $f(t)$ is said to be *absolutely* integrable if

$$\int_0^{\infty} |f(t)| dt$$

exists [5]. If this quantity does exist, we say

$$\lim_{n\to\infty}\int_0^n |f(t)|dt = \int_0^\infty |f(t)|dt$$

We make use of this when we begin speaking about analytic functions.

It is natural then to consider sequences and series of *functions*. In this case, there are two forms of convergences: *point-wise* convergence and *uniform* convergence. Let U be an open set of complex numbers, and let $\{f_n(z)\}$ be a sequence of functions on U. We say that $f_n \to f$ *point wise* on U if $f(z)$ is defined on U and for any $z \in U$ we can get the sequence of functions arbitrarily close to $f(z)$ at that point. Formally, $f_n \to f$ point wise if for $\epsilon > 0$, for all $z \in U$, there is some N such that for all $n \geq N$,

$$|f_n(z) - f(z)| < \epsilon$$

For this definition, it is important to note that *our choice of* N *is dependent on* z. On the other hand, we say $f_n \to f$ *uniformly* if for all $z \in U$ we can get the sequence of functions arbitrarily close to f. Formally, $f_n \to f$ uniformly if for $\epsilon > 0$, there is some N such that for all $z \in U$ and for all $n \geq N$,

$$|f_m(z) - f(z)| < \epsilon$$

In this case, the choice of N *does not* depend on z. An equivalent definition of uniform convergence is: for $\epsilon > 0$ there exists an N such that for all $n \geq N$,

$$\sup_{z\in U} |f_n(z) - f(z)| = ||f_n(z) - f(z)|| < \epsilon$$

It follows immediately that uniform convergence implies point-wise convergence and is the stronger condition [8]. Sequences and series of functions which converge uniformly often preserve certain qualities of functions, hence our interest in uniform convergence.

We say that a sequence of functions is *Cauchy with respect to the supremum norm* [5] if for any $\epsilon > 0$, there exists an N such that for all $m, n \geq N$,

$$||f_m(z) - f_n(z)|| < \epsilon$$

Lemma 1.2: If a sequence of functions is Cauchy with respect to the supremum norm then it converges uniformly.

Proof: For each $z \in U$, let

$$f(z) = \lim_{n \to \infty} f_n(z)$$

Given $\epsilon > 0$, there exists N such that, for all $n, m \geq N$,

$$||f_n(z) - f_m(z)|| < \frac{\epsilon}{2}$$

Let $n \geq N$. Choose $m \geq N$ such that

$$|f_m(z) - f(z)| < \frac{\epsilon}{2}$$

Then

$$|f_n(z) - f(z)| \leq |f_n(z) - f_m(z)| + |f_m(z) - f(z)| < \epsilon$$

since this is true for all $z \in U$, this implies that for all $n \geq N$,

$$||f(z) - f_n(z)|| < \epsilon$$

and this completes the proof.

This allows us to easily check the uniform convergence of a series.

Theorem 1.1: Let $\{f_n\}$ be a sequence of functions defined on an open set U such that for all n,

$$0 \leq ||f_n|| \leq c_n$$

where $\{c_n\}$ is a real valued sequence. If $\sum c_n$ converges, then $\sum f_n$ converges uniformly and absolutely.

Proof: This is done by looking at the difference of the partial sums.

$$||S_n - S_m|| \leq \sum_{k=m+1}^{n} ||f_k|| \leq \sum_{k=m+1}^{n} c_k$$

By the assumption that the rightmost series converges it is also Cauchy, hence for any $\epsilon > 0$ there exists an N such that for all $n, m \geq N$,

$$\sum_{k=m+1}^{n} c_k < \epsilon$$

and this proves the claim.

We now move onto the discussion of analytic functions, which are intricately related to series.

1.3 Analytic Functions

Analytic functions can be considered the heart of complex analysis. Indeed, much of the work done in the first few sections of this thesis relate to proving where various functions are analytic. We say that a function $f(z)$ is *analytic* at a point z_0 if there is a power series representation for f at z_0 which is absolutely convergent [5]. That means there is a disc of radius r centered at z_0 such that for z with $|z - z_0| < r$,

$$f(z) = \sum_{n=0}^{\infty} c_n (z - z_0)^n$$

and the above series converges absolutely for $|z - z_0| < r$. If a function f is analytic at every point $z \in U$, where U is an open set then we say f is *analytic on U*. As it turns out, if you can show that a function is analytic at a point, you can show that it is analytic at every point inside the radius of convergence.

Lemma 1.3: Suppose f is analytic at z_0, i.e.

$$f(z) = \sum_{n=0}^{\infty} c_n (z - z_0)^n$$

for all $z \in D(z_0, r)$ and that the series is absolutely convergent in this disc. Then f is analytic at every $z \in D(z_0, r)$.

Proof:

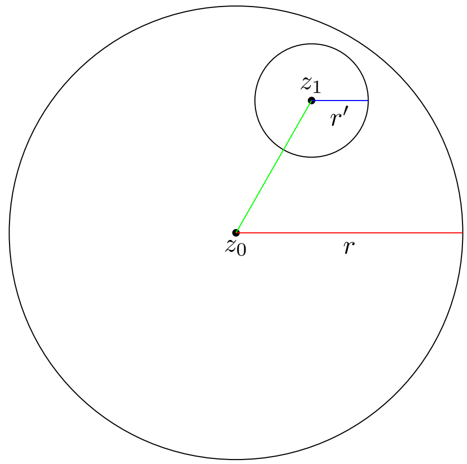

Figure 1

Choose $z_1 \in D(z_0, r)$. Then there is some r' such that $|z_1 - z_0| + r' < r$. Consider any z such that $|z - z_1| < r'$ (see figure 1). Note that

$$z - z_0 = ((z - z_1) + (z_1 - z_0))$$

hence

$$(z - z_0)^n = ((z - z_n) + (z_1 - z_0))^n$$

but then

$$f(z) = \sum_{n=0}^{\infty} c_n \left(\sum_{m=0}^{n} \binom{n}{m} (z_1 - z_0)^{n-m} (z_1 - z_0)^m \right)$$

However, we have that

$$|z - z_1 + z_1 - z_0| \le |z - z_1| + |z_1 - z_0| < r$$

and so the series

$$\sum_{n=0}^{\infty} |c_n| (|z - z_1| + |z_1 - z_0|)^n = \sum_{n=0}^{\infty} |c_n| \left(\sum_{m=0}^{n} \binom{n}{m} |z_1 - z_0|^{n-m} |z - z_1|^m \right)$$

converges absolutely. By Lemma 1.1 we can then switch the order of summation to get

$$f(z) = \sum_{m=0}^{\infty} \left(\sum_{n=m}^{\infty} c_n \binom{n}{m} (z_1 - z_0)^{n-m} \right) (z - z_1)^m$$

However, this is only if $|z - z_1| < r'$, but we just showed that the above series is absolutely convergent in this disc, hence f is analytic at z_1. Since our choice of z_1 was arbitrary this implies that f is analytic on $D(z_0, r)$.

It then follows that, since the standard topology on the complex plane is the metric topology, if every open disc in an open set U has a point where f is analytic then f is analytic on U. The standard method then for showing that a function is analytic on an open set U is to show that it is analytic in an arbitrary open disc in U.

We turn our attention now to uniform limits of analytic functions and applications to integration and summation.

<u>Lemma 1.4</u>: Let $f_n \to f$ uniformly on an open set U, where each f_n is analytic. If γ is a path in U, then

$$\lim_{n\to\infty} \int_\gamma f_n(z)dz = \int_\gamma f(z)dz$$

Proof: Since γ is the continuous image of a compact interval, it should have finite length, $L(\gamma)$. Then

$$\left| \int_\gamma f_n(z)dz - \int_\gamma f(z)dz \right| = \left| \int_\gamma f_n(z) - f(z)dz \right| \leq ||f_n(z) - f(z)||L(\gamma)$$

Since $f_n \to f$ uniformly, we can then make $||f_n(z) - f(z)||$ as small as necessary. This concludes the proof. Note that since the above is independent of z that the convergence is uniform.

<u>Lemma 1.5</u>: Let $\sum f_n$ converge uniformly on an open set U, where each f_n is analytic on U. If γ is a path in U, then

$$\int_\gamma \left(\sum_{n=0}^{\infty} f_n(z) \right) dz = \sum_{n=0}^{\infty} \left(\int_\gamma f_n(z)dz \right)$$

<u>Proof</u>: Again, we use partial sums. We have that

$$\int_\gamma \left(\sum_{m=0}^{n} f_m(z) \right) dz = \sum_{m=0}^{n} \left(\int_\gamma f_m(z)dz \right)$$

by the linearity of integration. But then we have by lemma 1.3 that

$$\lim_{n\to\infty}\int_\gamma \left(\sum_{m=0}^{\infty} f_m(z)\right) dz = \int_\gamma \left(\sum_{n=0}^{\infty} f_m(z)\right) dz = \lim_{n\to\infty}\sum_{m=0}^{n}\left(\int_\gamma f_m(z)dz\right)$$
$$= \sum_{n=0}^{\infty}\left(\int_\gamma f_n(z)dz\right)$$

We now ask the most important question of the section: what conditions are necessary to make the limiting function analytic?

Theorem 1.2: Let $f_n \to f$ uniformly on an open set U. If each f_n is analytic on U then f is analytic on U.

Proof: Let γ be any simple closed contour in U. By Cauchy-Gorsat we know that for all n,

$$\int_\gamma f_n(z)dz = 0$$

By lemma 1.3 this implies

$$\lim_{n\to\infty}\int_\gamma f_n(z)dz = \lim_{n\to\infty} 0 = 0 = \int_\gamma f(z)dz$$

f then satisfies Morera's Theorem and hence is analytic on U.

The following corollary is immediate [5, 8]

Corollary 1.1: Let $f_n \to f$, $\sum g_n(z)$ converge uniformly on an open set U. Then

1. $$\sum_{n=0}^{\infty} g_n(z)$$

   is analytic.

2. If each

$$\int_\gamma f_n(z)dz$$

is analytic then

$$\int_\gamma f(z)dz$$

is analytic.

3. If each

$$\int_\gamma f_n(z)dz$$

is analytic then

$$\int_\gamma \left(\sum_{n=0}^{\infty} f_n(z)\right) dz = \sum_{n=0}^{\infty} \left(\int_\gamma f_n(z)dz\right)$$

is analytic.

We finally focus on a few lemmas which are slightly more focused for later applications. Before we do so, we must define one last type of uniform convergence. Let $f(t,z)$ be a function of two variables; t a real variable and z a complex variable which belongs to U. The integral

$$\int_0^\infty f(t,z)dt = \lim_{n\to\infty} \int_0^n f(t,z)dz$$

is said to be *uniformly convergent* for $z \in U$ if, given $\epsilon > 0$, there exists N such that for any n_1, n_2 with $N < n_1 < n_2$,

$$\left| \int_{n_1}^{n_2} f(t,z)dt \right| < \epsilon$$

Notice that this is very similar to being Cauchy [5].

Lemma 1.6: Let I be an interval of real numbers, not necessarily finite. Let $\{I_n\}$ be a sequence of compact intervals which increases to I with $I_n \subset I$. Let U be an open set of complex numbers and let $f(t,z)$ be continuous on $I \times U$. If

$$\int_I f(t,z)dt$$

is uniformly convergent for all z in any compact subset K of U, and for each t the function $z \mapsto f(t,z)$ is analytic, then

$$F(z) = \int_I f(t,z)dt$$

is analytic on U.

Proof: For each n define

$$F_n(z) = \int_{I_n} f(t,z)dt$$

Let γ be any simple closed contour in U. Then

$$\int_\gamma F_n(z)dz = \int_\gamma \int_{I_n} f(t,z)dtdz$$

since f is continuous on $I_n \times \gamma$ and both of these are compact sets, by Fubini's Theorem we can swap the order of integration to get

$$\int_\gamma F_n(z)dz = \int_{I_n} \int_\gamma f(t,z)dzdt = \int_{I_n} 0dt = 0$$

since we assume $f(t,z)$ is analytic for all $t \in I$. This then implies that each $F_n(z)$ is analytic in U. However, due to the uniform convergence over compact sets, this implies that

$$\int_\gamma F(z)dz = \lim_{n\to\infty} \int_\gamma F_n(z)dz = 0$$

so by Morera's Theorem $F(z)$ is analytic on U.

Lemma 1.7: Let η be a path in $\mathbb{C}$. Let $s \in U$, U an open set of complex numbers. Let $f(z,s)$ be a continuous function on $\eta \times U$. If for each $z \in \eta$ the function $s \mapsto f(z,s)$ is analytic, then

$$F(s) = \int_\eta f(z,s)dz$$

is analytic on U.

Proof: The idea is almost identical to the previous lemma. We know that η is the continuous image of a compact, real interval, hence

$$F(s) = \int_a^b f(\eta(t),s)\eta'(t)dt$$

Let γ be any simple closed contour in U. Then

$$\int_\gamma F(s)ds = \int_\gamma \int_a^b f(\eta(t), s)\eta'(t)dtds$$

By the continuity of $f(\eta(t), s)\eta'(t)$ and the fact that γ, $[a, b]$ are compact spaces, we may again use Fubini's theorem to interchange the order of integration so that

$$\int_\gamma F(s)ds = \int_a^b \eta'(t) \int_\gamma f(\eta(t), s)dsdt = \int_a^b \eta'(t)(0)dt = 0$$

By Morera's Theorem, F is then analytic on U.

1.4 The Gamma Function

Before we begin discussing the object of our study, namely the zeta function, we do what mathematicians often must: study something seemingly unrelated. The Gamma function has a rich history with notable contributions to its development made by giants such as Euler and Gauss [2]. The study of the Gamma function began as a way to try and find a function which, when restricted to $\mathbb{N}$, was equivalent to $n!$. In this attempt many have succeeded and the function was analytically extended to accept complex numbers as its arguments. There are many definitions for the Gamma function, Euler notably developed his integral expression which we will consider in this section, but we focus on one which I believe more succinctly displays its basic analytic properties. We then show the equivalence to Euler's integral expression from which we derive many of the familiar properties of the Gamma function.

We define the Gamma function as [5]

$$\Gamma(z) = \frac{e^{-\gamma z}}{z} \prod_{n=1}^{\infty} \frac{ne^{\frac{z}{n}}}{z+n}$$

where γ is the Euler-Mascheroni constant

$$\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \ln(n)\right)$$

Our immediate concern should be checking where this is analytic, where it is defined, and if it has any obvious zeros.

Theorem 1.3: $\Gamma(z)$ is a meromorphic function with simple poles at $z = 0$ and the negative integers. Additionally, it is nowhere zero.

Proof: We notice immediately that the Gamma function is a product of two functions; $\frac{e^{\frac{z}{n}}}{z}$ and the infinite product. The first factor is easily dealt with: it has an obvious simple pole at $z = 0$, but no others. Similarly, it is nowhere zero. It then follows that the only zeros of the Gamma function come from the infinite product and unless the infinite product has a zero or a pole at $z = 0$ that $\Gamma(z)$ will have a simple pole at $z = 0$.

We then must turn to the infinite product. Suppose for any z_0 there is some open disc U containing z_0 such that for every n there is some c_n so that,

$$\left\|\log\left(\frac{ne^{\frac{z}{n}}}{z+n}\right)\right\| \leq c_n$$

If $\sum c_n$ converges, then by Corollary 1.1 the series

$$\sum_{n=1}^{\infty} \log\left(\frac{ne^{\frac{z}{n}}}{z+n}\right)$$

is analytic on U. Since exponentiation is a continuous operation, this implies that

$$\prod_{n=1}^{\infty} \frac{ne^{\frac{z}{n}}}{z+n} = e^{\sum_{n=1}^{\infty} \log\left(\frac{ne^{\frac{z}{n}}}{z+n}\right)}$$

is analytic on U.

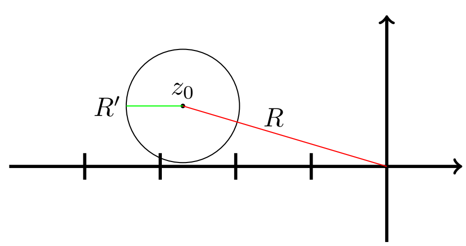

Figure 2

Fix any z_0 such that z is not a negative integer. Let $|z_0| = R$. There is then some R' such that the open disc centered at z_0 does not contain any negative integers (see Figure 2). For any z such that $|z - z_0| < R'$ we then have that

$$\sum_{n=1}^{\infty} \log\left(\frac{ne^{\frac{z}{n}}}{z+n}\right) = \sum_{n=1}^{\infty}(\log(ne^{\frac{z}{n}}) - \log(z+n))$$

We see immediately why we cannot choose a negative integer, it would cause the logarithm to diverge to negative infinity. We will consider what type of pole this induces shortly.

Note that $z+n = n(1+\frac{z}{n})$, hence

$$\sum_{n=1}^{\infty}(\log(ne^{\frac{z}{n}})) - \log(z+n)) = \sum_{n=1}^{\infty}\left(\frac{z}{n} - \log(1+\frac{z}{n})\right)$$

Fix N such that for all $n \geq N$, $\frac{R+R'}{n} < \frac{1}{2}$. Then

$$\left|\frac{z}{n}\right| = \frac{|z-z_0+z_0|}{n} \leq \frac{|z-z_0|+|z_0|}{n} < \frac{R+R'}{n} < \frac{1}{2}$$

We can then use the series expansion for the logarithm to get that

$$\sum_{n=1}^{\infty}\log\left(\frac{ne^{\frac{z}{n}}}{z+n}\right) = \text{finite} + \sum_{N}^{\infty}\left(\frac{z}{n} - \sum_{m=1}^{\infty}(-1)^{m+1}\frac{z^m}{mn^m}\right)$$

For each n the logarithm function we initially defined is analytic inside of the disc $|z-z_0| < R'$, so it has a maximum on the boundary of the disc, and hence the supremum norm of the function exists on the disc. Therefore, for the first $N-1$ terms we have that $c_n = ||\log||$ on the disc, and this takes care of the finite piece. We omit the finite section from here on out to save space. We then have that

$$\sum_{n=N}^{\infty}\log\left(\frac{ne^{\frac{z}{n}}}{z+n}\right) = \sum_{N}^{\infty}\left(\frac{z}{n} - \sum_{m=1}^{\infty}(-1)^{m+1}\frac{z^m}{mn^m}\right)$$

$$= \sum_{N}^{\infty}\left(\frac{z}{n} - \frac{z}{n} + \sum_{m=2}^{\infty}(-1)^m\frac{z^m}{mn^m}\right) = \sum_{N}^{\infty}\sum_{m=2}^{\infty}(-1)^m\frac{z^m}{mn^m}$$

$$= \sum_{N}^{\infty}\sum_{m=0}^{\infty}(-1)^m\frac{z^{m+2}}{(m+2)n^{m+2}}$$

However, for all z in the disc we have that

$$\left|\sum_{m=0}^{\infty}(-1)^m\frac{z^{m+2}}{(m+2)n^{m+2}}\right| \leq \sum_{m=0}^{\infty}\frac{|z|^{m+2}}{(m+2)n^{m+2}} = \left(\frac{|z|}{n}\right)^2\sum_{m=0}^{\infty}\frac{|z|^m}{(m+2)n^m}$$

$$\leq \left(\frac{|z|}{n}\right)^2\sum_{m=0}^{\infty}\left(\frac{|z|}{n}\right)^m < \left(\frac{R+R'}{n}\right)^2\sum_{m=0}^{\infty}\left(\frac{1}{2}\right)^m$$

$$= \frac{2(R+R')^2}{n^2}$$

Therefore for all $n \geq N$, we have that $c_n = \frac{2(R+R')^2}{n^2}$. It is then clear that $\sum c_n$ is a finite number of terms and then a convergent infinite series, and hence converges. This proves that the infinite product is analytic in any disc which does not contain a negative integer. However, this is the entire complex plane minus the negative integers. We then ask what type pole exists at the negative integers. Well, for any specific integer, n_0, we have that

$$\prod_{n=1}^{\infty} \frac{ne^{\frac{z}{n}}}{z+n} = \frac{n_0 e^{\frac{z}{n_0}}}{z+n_0} \prod_{n \neq n_0}^{\infty} \frac{ne^{\frac{z}{n}}}{z+n}$$

where the infinite product on the right is understood to be the same as the left excluding the case when $n = n_0$. However, this infinite product is seen to be analytic at $-n_0$ by the same argument as above. However,

$$\frac{n_0 e^{\frac{z}{n_0}}}{z+n_0}$$

has a simple pole at $z = -n_0$. Therefore, the infinite product has a simple pole at all negative integers.

Lastly, we make use of the fact that an infinite product is zero if and only if there is a term which is zero [5]. However, it is clear that

$$\frac{ne^{\frac{z}{n}}}{z+n}$$

is nowhere zero for any n. This then tells us that both factors of the Gamma function are nowhere zero, which implies that the Gamma function is nowhere zero. Since one factor is meromorphic with a simple pole at $z = 0$ and the other factor is meromorphic with simple poles at the negative integers, this implies the Gamma function is meromorphic with poles at $z = 0$ and the negative integers, which proves the theorem.

There is an alternative definition for the Gamma function which is not hard to see.

Lemma 1.8:

$$\Gamma(z) = \lim_{n\to\infty} \frac{n!n^z}{z(z+1)\cdots(z+n)}$$

Proof: We have that

$$\lim_{n\to\infty} \frac{n!n^z}{z(z+1)\cdots(z+n)} = \frac{1}{z} \lim_{n\to\infty} n^z \prod_{m=1}^{n} \frac{m}{z+m}$$

By definition, we have that

$$n^z = e^{z\log(n)} = e^{z(-1-\frac{1}{2}-\cdots-\frac{1}{n}+\log(n))}e^{z(1+\frac{1}{2}+\cdots+\frac{1}{n})}$$

$$= e^{z(-1-\frac{1}{2}-\cdots-\frac{1}{n}+\log(n))}\prod_{m=1}^{n} e^{\frac{z}{m}}$$

Then

$$\lim_{n\to\infty}\frac{n!n^z}{z(z+1)\cdots(z+n)} = \lim_{n\to\infty}\frac{e^{z(-1-\frac{1}{2}-\cdots-\frac{1}{n}+\log(n))}}{z}\prod_{m=1}^{\infty}\frac{me^{\frac{z}{m}}}{z+m}$$

$$= \frac{e^{-\gamma z}}{z}\prod_{n=1}^{\infty}\frac{ne^{\frac{z}{n}}}{z+n} = \Gamma(z)$$

We now wish to find an integral expression for the Gamma function. With this, some of the familiar properties of the function become readily apparent and the integral expression is central to Riemann's development of the zeta function.

Lemma 1.9: For $Re(z) > 0$, we have that

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt$$

Proof: Note that while we *could* show that the function defined by this integral is analytic for $Re(z) > 0$ using the tools we have already developed, it suffices to show that it is absolutely convergent and equal to $\Gamma(z)$ in this domain. Since the Gamma function is analytic in this domain it will imply the integral is analytic. We the first tackle the issue of absolute convergence. We break the integral into three parts:

$$\int_0^\infty e^{-t}t^{z-1}dt = \int_0^1 e^{-t}t^{z-1}dt + \int_1^N e^{-t}t^{z-1}dt + \int_N^\infty e^{-t}t^{z-1}dt$$

so that

$$\left|\int_0^\infty e^{-t}t^{z-1}dt\right| \le \left|\int_0^1 e^{-t}t^{z-1}dt\right| + \left|\int_1^N e^{-t}t^{z-1}dt\right| + \left|\int_N^\infty e^{-t}t^{z-1}dt\right|$$

For the rightmost integral, we have that

$$\left|\int_N^\infty e^{-t}t^{z-1}dt\right| \leq \int_N^\infty |e^{-t}t^{z-1}|dt = \int_N^\infty e^{-t}t^{Re(z)-1}dt$$

Choose N to be the smallest real number such that $e^{\frac{t}{2}} \geq t^{Re(z)-1}$ for all $t \geq N$ (note that if $Re(z) \leq 1$, $N = 1$ satisfies this condition hence the middle integral vanishes). Then

$$\left|\int_N^\infty e^{-t}t^{z-1}dt\right| \leq \int_N^\infty e^{-t}e^{\frac{t}{2}}dt = \int_N^\infty e^{-\frac{t}{2}}dt$$
$$= 2e^{-\frac{N}{2}}$$

Therefore the rightmost integral converges. For the middle integral, we have that

$$\left|\int_1^N e^{-t}t^{z-1}dt\right| \leq \int_1^N e^{-t}t^{Re(z)-1}dt$$

However, $e^{-t}t^{Re(z)-1}$ is continuous on the interval $[1, N]$, hence it is bounded, say by B, so that

$$\int_1^N e^{-t}t^{z-1}dt \leq B(N-1)$$

Finally, we use integration by parts for the first integral:

$$\left|\int_0^1 e^{-t}t^{z-1}dt\right| \leq \int_0^1 e^{-t}t^{Re(z)-1}dt$$
$$= \left.\frac{e^{-t}t^{Re(z)}}{Re(z)}\right|_0^1 + \frac{1}{Re(z)}\int_0^1 e^{-t}t^{Re(z)}dt$$
$$= \frac{1}{Re(z)}\left(e^{-1} + \int_0^1 e^{-t}t^{Re(z)}dt\right)$$

Now $e^{-t}t^{Re(z)}$ is continuous on the compact interval $[0, 1]$, and is then bounded, say by B', so that

$$\left|\int_0^1 e^{-t}t^{z-1}dt\right| \leq \frac{e^{-1} + B'}{Re(z)}$$

Therefore all together,

$$\int_0^\infty e^{-t}t^{z-1}dt$$

converges absolutely if $Re(z) > 0$.

Now we must show that this integral is equivalent to the Gamma function. This is a two step process. The first step is to use integration by parts and induction to prove that

$$\int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1}dt = \frac{n!n^z}{z(z+1)\cdots(z+n)}$$

Then we show that

$$\lim_{n\to\infty}\int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1}dt = \int_0^\infty e^{-t}t^{z-1}dt$$

by lemma 1.8, this then implies that for $Re(z) > 0$,

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt$$

We begin using a simple substitution of variables: let $u = \frac{t}{n}$. Then

$$\int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1}dt = n^z\int_0^1 (1-u)^n u^{z-1}du$$

Integration by parts then gives

$$n^z\int_0^1 (1-u)^n u^{z-1}du = n^z\left(\left.\frac{(1-u)^n u^z}{z}\right|_0^1 + \frac{n}{z}\int_0^1 (1-u)^{n-1}u^z du\right)$$

$$= \frac{n^z n}{z}\int_0^1 (1-u)^{n-1}u^z du$$

We now use the same process to show that

$$\int_0^1 (1-u)^{n-k}u^{z+(k-1)}du = \frac{n-k}{z+k}\int_0^1 (1-u)^{n-(k+1)}u^{z+k}du$$

We have that

$$\int_0^1 (1-u)^{n-k}u^{z+(k-1)}du$$

$$= \frac{1}{z+k}\left((1-u)^{n-k}u^{z+k}\big|_0^1 + (n-k)\int_0^1 (1-u)^{n-(k+1)}u^{z+k}du\right)$$

$$= \frac{n-k}{z+k}\int_0^1 (1-u)^{n-(k+1)}u^{z+k}du$$

Induction then tells us that

$$\int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1}dt = \frac{n^z(n)\cdots(2)}{z(z+1)\cdots(z+n-1)}\int_0^1 u^{z+n-1}du$$

However,

$$\int_0^1 u^{z+n-1} du = \frac{1}{z+n}$$

hence

$$\int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1} dt = \frac{n! n^z}{z(z+1)\cdots(z+n)}$$

Now we wish to show that

$$\lim_{n\to\infty} \int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1} dt = \int_0^\infty e^{-t} t^{z-1} dt$$

Then we need to show that for all $\epsilon > 0$ there is some N such that for all $n \geq N$,

$$\left| \int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1} dt - \int_0^\infty e^{-t} t^{z-1} dt \right| < \epsilon$$

Note that

$$\left| \int_0^n \left(1-\frac{t}{n}\right)^n t^{z-1} dt - \int_0^\infty e^{-t} t^{z-1} dt \right|$$
$$= \left| \int_0^n \left(e^{-t} - \left(1-\frac{t}{n}\right)^n\right) t^{z-1} dt + \int_n^\infty e^{-t} t^{z-1} dt \right|$$
$$\leq \left| \int_0^n \left(e^{-t} - \left(1-\frac{t}{n}\right)^n\right) t^{z-1} dt \right| + \left| \int_n^\infty e^{-t} t^{z-1} dt \right|$$

We have already shown in proving the absolute convergence of the integral that

$$\left| \int_n^\infty e^{-t} t^{z-1} dt \right| \leq 2e^{-\frac{n}{2}}$$

Therefore we can choose N_1 to be the smallest real number such that for all $n \geq N_1$,

$$2e^{-\frac{n}{2}} < \frac{\epsilon}{2}$$

Taking care of the remainder is slightly more complicated. We need to develop some bounds. First we show that

$$0 \leq \left(1-\frac{t}{n}\right) \leq e^{-\frac{t}{n}}$$

for all $t \in [0, n]$. We do this by noting that at $t = 0$, both sides are 1. Taking derivatives of both sides gives

$$-\frac{1}{n} \leq -\frac{e^{-\frac{t}{n}}}{n}$$

or equivalently

$$1 \geq e^{-\frac{t}{n}}$$

since this holds, this implies the derivative of the right side is always greater than the left which proves the first bound [5]. Since both sides are positive, we can raise them to the n^{th} power to get

$$0 \leq \left(1 - \frac{t}{n}\right)^n \leq e^{-t}$$

so that

$$0 \leq e^{-t} - \left(1 - \frac{t}{n}\right)^n$$

Lastly, by the same methods we have that

$$e^{-t} - \left(1 - \frac{t}{n}\right)^n \leq \frac{t^2 e^{-t}}{n}$$

where again this holds for all $t \in [0, n]$. Then we have that

$$\left| \int_0^n \left(e^{-t} - \left(1 - \frac{t}{n}\right)\right) t^{z-1} dt \right| \leq \frac{1}{n} \int_0^n e^{-t} t^{Re(z)+1} dt$$

However, by the same trick we used to show absolute convergence of the original integral expression, we know that

$$\int_0^n e^{-t} t^{Re(z)+1} dt$$

converges, say to B_z. Since $e^{-t} t^{Re(z)+1} \geq 0$ for all $t \geq 0$, we then have that

$$\left| \int_0^n \left(e^{-t} - \left(1 - \frac{t}{n}\right)\right) t^{z-1} dt \right| \leq \frac{1}{n} \int_0^\infty e^{-t} t^{Re(z)+1} dt$$

$$= \frac{B_z}{n}$$

Then choose N_2 such that for all $n \geq N_2$,

$$\frac{B_z}{n} < \frac{\epsilon}{2}$$

Let $N = \max\{N_1, N_2\}$. It then follows that for all $n \geq N$, we have have

$$\left| \int_0^n \left(1 - \frac{t}{n}\right)^n t^{z-1} dt - \int_0^\infty e^{-t} t^{z-1} dt \right| < \epsilon$$

and this proves the lemma.

We now derive some additional properties of the Gamma function which will prove useful.

Lemma 1.10:

$$\Gamma(1) = 1$$

Proof: Simply plug $z = 1$ into the integral expression to get

$$\Gamma(1) = \int_0^\infty e^{-t} dt = -e^{-t}\Big|_0^\infty = 1$$

Lemma 1.11:

$$\Gamma(z) = (z-1)\Gamma(z-1)$$

Proof: This is a simple application of integration by parts:

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt = -e^{-t} t^{z-1}\Big|_0^\infty + (z-1) \int_0^\infty e^{-t} t^{z-1} dt$$

$$= (z-1)\Gamma(z-1)$$

Note that even though we derived this relation in the half of the complex plane with $Re(z) > 0$, it relates two analytic functions and holds everywhere both functions are analytic [5, 8]. It follows immediately that if $n \in \mathbb{N}$, $\Gamma(n) = (n-1)!$.

Lemma 1.12:

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$$

Proof: We must return to the product form of the Gamma function for this. We also use the fact that the complex sine has the Euler product [5, 8]

$$\sin(\pi z) = \pi z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right)$$

By lemma 1.11 we know that

$$\Gamma(1-z) = (-z)\Gamma(-z) = e^{\gamma z} \prod_{n=1}^{\infty} \frac{ne^{-\frac{z}{n}}}{n-z}$$

Then

$$\Gamma(z)\Gamma(1-z) = \frac{1}{z} \prod_{n=1}^{\infty} \frac{n^2}{n^2 - z^2}$$

$$= \frac{\pi}{\pi z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right)} = \frac{\pi}{\sin(\pi z)}$$

We have now derived the essential facts we need about the Gamma function. There are many additional properties which prove useful; Riemann himself used many when he derived his formula for $\xi(s)$, what he considered the more *natural* form of the zeta function. However, the work required to reach these properties does not justify their utility in the scope of this paper; what we have proven already will be more than sufficient for a cursory examination of the Riemann Zeta Function.

2 The Riemann Zeta Function

The harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

has been known to diverge since the at least the 1700's. Euler later showed that the series

$$\sum_{n=1}^{\infty} \frac{1}{n^2}$$

actually converges, and has a value of $\frac{\pi^2}{6}$. In fact it is not hard to show that a sum of the form

$$\sum_{n=1}^{\infty} \frac{1}{n^x}$$

converges for $x > 1$ real. It is then natural to extend this series definition to the complex numbers, of the form

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

By the above, it is not hard to show that this converges for $Re(s) > 1$. This is a specific form of a Dirichlet series; as the name suggests series of these forms were studied by Dirichlet.

2.1 Euler, the Product Form

One of the most important results about this specific Dirichlet series was found by Euler, decades prior. Euler successfully found a product representation for the series, and this enables us to more easily determine analytic properties of the series.

Lemma 2.1: For $Re(s) > 1$,

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

where the product on the right is understood to be an infinite product over all primes.

Proof: We have that

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \prod_p \left(\sum_{n=0}^{\infty} \left(\frac{1}{p^s} \right)^n \right)$$

We write this out somewhat more explicitly.

$$= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots \right) \left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots \right) + \left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \cdots \right) \cdots$$

Suppose we want to create $\frac{1}{n^s}$ for any positive integer n out of the above. Unique factorization of the integers says that if $n = p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}$ then we can create $\frac{1}{n^s}$ by pulling a factor of $\frac{1}{p_i^{k_i s}}$ out of each sum over p_i, and 1 everywhere else. Since this factorization is unique, this is the *only* way we can create this factor out of the above. Since we wish to do this with every integer, we have that

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Dirichlet made use of the above identity in his own ways, including measuring densities of certain types of primes. It was not until his student, Riemann, made use of the series that Euler's relation and the connection to primes was truly unveiled.

2.2 Definition, Derivation

Riemann's first objective was to find an *analytic continuation* of the series which remains valid for all of $\mathbb{C}$ (or almost all of it). That is, his goal was to find a function which when restricted to $Re(s) > 1$ was equal to the Dirichlet series. Riemann succeeded, and the function he defined became know as the *Riemann Zeta Function*, $\zeta(s)$.

Before we can define the zeta function, we must define a contour in the plane. We define *Hankel Contour* as the contour η which starts at $+\infty$ on the real axis, travels to $\epsilon > 0$ on the real axis, circles the origin counter clockwise, and then once it reaches the positive axis again returns down the real axis to $+\infty$ (see figure 3).

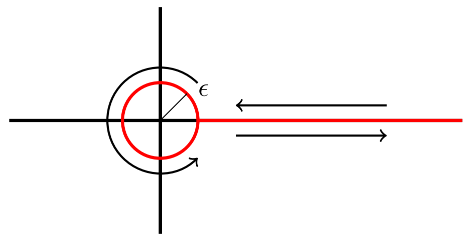

Figure 3: The Hankel Contour, η

We now define the function

$$H(s) = \int_{\eta} \frac{(-z)^s}{e^z - 1} \frac{dz}{z}$$

and we seek to prove two key facts about $H(s)$.

Lemma 2.2: $H(s)$ is entire [2, 5].

Proof: We begin by breaking up the integral. For shorthand, let

$$f(z, s) = \frac{(-z)^s}{z(e^z - 1)}$$

Then we have that

$$H(s) = \int_{\infty}^{\epsilon} f(z, s) dz + \int_{C_\epsilon} f(z, s) dz + \int_{\epsilon}^{\infty} f(z, s) dz$$

where C_ϵ is understood to be the circle of radius ϵ about the origin. It would seem as if the left and right integrals would cancel each other, but this is not the case [3, 6]. We examine why. Complex exponentiation is implicitly defined by the complex logarithm. In this case, we have that

$$(-z)^s = e^{s \log(-z)}$$

where

$$\log(z) = \ln |z| + i \arg(z)$$

The range of $\arg(z)$ is dependent on the branch of logarithm we choose. In our case, we choose the branch which has argument of $-\pi$ for negative integers. In the left integral, we then have that

$$f(z,s) = \frac{(-z)^s}{z(e^z-1)} = \frac{e^{s(\ln(z)-i\pi)}}{z(e^z-1)} = e^{-i\pi s}\frac{e^{\ln(z)}}{z(e^z-1)} = e^{-i\pi s}\frac{z^{s-1}}{e^z-1}$$

By the time we reach the right integral, the argument has increase by 2π by going around C_ϵ. This then implies that on the right integral,

$$f(z,s) = \frac{(-z)^s}{z(e^z-1)} = \frac{e^{s(\ln(z)+i\pi)}}{z(e^z-1)} = e^{i\pi s}\frac{e^{\ln(z)}}{z(e^z-1)} = e^{i\pi s}\frac{z^{s-1}}{e^z-1}$$

so that

$$H(s) = (e^{i\pi s} - e^{i\pi s})\int_\epsilon^\infty \frac{z^{s-1}}{e^z-1}dz + \int_{C_\epsilon} f(z,s)dz$$

By lemma 1.7, the integral over C_ϵ is then entire since for any s in any disc in $\mathbb{C}$, for all $z \in C_\epsilon$, the function $s \mapsto f(z,s)$ is analytic. Similarly, it is not hard to show that the integral over $[\epsilon, \infty)$ fits the conditions of lemma 1.6 for any s and is hence entire. We have that

$$\left|\int_{n_1}^{n_2} \frac{z^{s-1}}{e^z-1}dz\right| \leq \int_{n_1}^{n_2} \frac{z^{Re(s)-1}}{|e^z-1|}dz \leq \int_{n_1}^{n_2} z^{Re(s-1)}e^{-z}dz$$

We can again use the trick that the exponential function outgrows any positive real power [8]. Choose N_1 such that for all $z \geq N_1$, $e^{\frac{z}{2}} \geq z^{Re(s)-1}$. Then

$$\left|\int_{n_1}^{n_2} \frac{z^{s-1}}{e^z-1}dz\right| \leq \int_{n_1}^{n_2} e^{-\frac{z}{2}}dz = 2(e^{-\frac{n_1}{2}} - e^{-\frac{n_2}{2}})$$
$$\leq 2e^{-\frac{n_1}{2}}$$

Choose N_2 such that for all $z \geq N_2$, $2e^{-\frac{z}{2}} < \epsilon$. Let $N = \max\{N_1, N_2\}$. This shows the uniform convergence of the integral.

Since the exponential function is entire this the implies that $H(s)$ is entire, and this concludes the proof.

Lemma 2.3: Except for multiples of 2π, $H(s)$ is independent of ϵ [3].

Proof: To do this we define two new contours: U_ϵ and L_ϵ. The contour U_ϵ starts at 1 on the positive real axis, travels to ϵ on the positive real axis, circles the origin counter clockwise until it reaches the negative real axis at $-\epsilon$ and then travels along the negative real axis to -1. L_ϵ starts at -1, travels along the negative real axis to $-\epsilon$, where it then circles the origin counter clockwise until it reaches the positive real axis at ϵ

and then travels along the positive real axis to 1. The case where $\epsilon < 1$ is illustrated in figure 4.

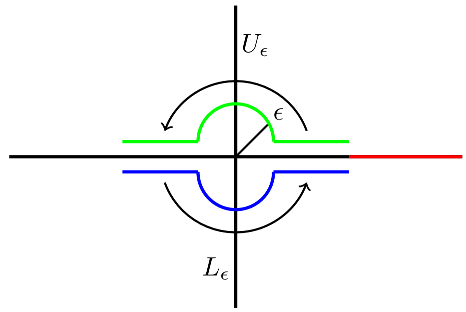

Figure 4: The U_ϵ, L_ϵ contours are separated from the real axis slightly to make distinguishing them easier.

It follows that

$$H(s) = \int_\infty^1 f(z,s)dz + \int_{U_\epsilon} f(z,s)dz + \int_{L_\epsilon} f(z,s)dz + \int_1^\infty f(z,s)dz$$

Why? When z is on the negative axis on either U_ϵ or L_ϵ, since the argument does not change between the contours the integrals *do* cancel and the resulting contour is η. However, as long as ϵ is not a multiple of 2π, this implies that $f(z,s)$ is analytic on U_ϵ, L_ϵ. This implies the integrals are only dependent on the start and end point which do no vary based on ϵ. This concludes the proof.

Finally, we can define the Riemann zeta function. The Riemann zeta function is defined as

$$\zeta(s) = \frac{\Gamma(1-s)}{2\pi i}\int_\eta \frac{(-z)^{s-1}}{e^z - 1}\frac{dz}{z} = \frac{\Gamma(1-s)H(s)}{2\pi i}$$

We will develop a bit of machinery before we tackle analyzing the analytic properties of the zeta function. The first order of business is to verify that

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

for $Re(s) > 1$.

Lemma 2.4: For $Re(s) > 1$,

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

Proof: We begin by examining what happens to $H(s)$ when $Re(s) > 1$. We do this by examining what happens as $\epsilon \to 0$. We have that

$$H(s) = (e^{i\pi s} - e^{-i\pi s}) \int_{\epsilon}^{\infty} \frac{z^{s-1}}{e^z - 1} dz + \int_{C_\epsilon} \frac{(-z)^s}{e^z - 1} \frac{dz}{z}$$

We then show that the integral

$$\int_0^{\infty} \frac{z^{s-1}}{e^z - 1} dz$$

converges absolutely and that

$$\int_{C_\epsilon} \frac{(-z)^s}{e^z - 1} \frac{dz}{z} \to 0$$

For the first, we have that

$$\left| \int_{\epsilon}^{\infty} \frac{z^{s-1}}{e^z - 1} dz \right| < \int_{\epsilon}^{\infty} \frac{z^{Re(s)-1}}{|e^z - 1|} dz < \int_{\epsilon}^{\infty} z^{Re(s)-1} e^{-z} dz$$
$$= \int_{\epsilon}^{N} z^{Re(s)-1} e^{-z} dz + \int_{N}^{\infty} z^{Re(s)-1} e^{-z} dz$$

where again we choose N such that for all $z \geq N$ $e^{\frac{z}{2}} \geq z^{Re(s)-1}$. This shows the convergence of the rightmost integral. Since $Re(s) > 1$, $z^{Re(s)-1} e^{-z}$ is nonsingular near 0, hence

$$\int_0^{N} z^{Re(s)-1} e^{-z} dz$$

exists. This in turn implies the absolute convergence of

$$\int_0^{\infty} \frac{z^{s-1}}{e^z - 1} dz$$

For the second piece, we have

$$\int_{C_\epsilon} \frac{(-z)^s}{e^z - 1} \frac{dz}{z} = i \int_0^{2\pi} \frac{e^{s(\ln|\epsilon e^{i\theta}| - i\pi)}}{e^{\epsilon e^{i\theta}} - 1} d\theta$$
$$= i \int_0^{2\pi} \frac{e^{s(\ln|\epsilon| - i(\pi - \theta))}}{e^{\epsilon e^{i\theta}} - 1} d\theta$$

so that

$$\left|\int_{C_\epsilon} \frac{(-z)^s}{e^z-1}\frac{dz}{z}\right| \le 2\pi\epsilon\left|\frac{e^{s(\ln|\epsilon|-i(\pi-\theta))}}{e^{\epsilon e^{i\theta}}-1}\right| = 2\pi\epsilon\frac{\epsilon^{Re(s)}e^{Im(s)(\pi-\theta)}}{|e^{\epsilon e^{i\theta}}-1|}$$

$$\le 2\pi e^{\pi Im(s)}\epsilon^{Re(s)}\frac{\epsilon}{|e^{\epsilon e^{i\theta}}-1|}$$

For ω sufficiently close to the origin we have that [3]

$$|e^{\omega}-1| \ge |e^{\omega}|-1$$

Which implies that the above goes to 0 as $\epsilon \to 0$ [3].

This then shows that for $Re(s) > 1$,

$$H(s) = (e^{i\pi s}-e^{-i\pi s})\int_0^\infty \frac{z^{s-1}}{e^z-1}dz = 2i\sin(\pi s)\int_0^\infty \frac{z^{s-1}}{e^z-1}dz$$

so that

$$\zeta(s) = \Gamma(1-s)\frac{\sin(\pi s)}{\pi}\int_0^\infty \frac{z^{s-1}}{e^z-1}dz$$

Lemma 1.12 then tells us that

$$\zeta(s) = \frac{1}{\Gamma(s)}\int_0^\infty \frac{z^{s-1}}{e^z-1}dz$$

Looking at the integral we have that

$$\int_0^\infty \frac{z^{s-1}}{e^z-1}dz = \int_0^\infty \left(z^{s-1}\sum_{n=1}^{\infty}\left(\frac{1}{e^z}\right)^n\right)dz$$

The sum is bounded by a geometric series, hence it converges uniformly. By theorem 1.1 we can then interchange the order of summation and integration. Then

$$\int_0^\infty \frac{z^{s-1}}{e^z-1}dz = \sum_{n=1}^{\infty}\left(\int_0^\infty e^{-nz}z^{s-1}dz\right)$$

Perform a substitution of variables: let $z = \frac{t}{n}$ hence

$$\int_0^\infty \frac{z^{s-1}}{e^z-1}dz = \sum_{n=1}^{\infty}\left(\frac{1}{n^s}\int_0^\infty e^{-t}t^{s-1}dt\right)$$

$$= \sum_{n=1}^{\infty}\frac{1}{n^s}\int_0^\infty e^{-t}t^{s-1}dt = \Gamma(s)\sum_{n=1}^{\infty}\frac{1}{n^s}$$

This finally yields

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

exactly as desired.

We now somewhat understand *what* the Riemann zeta function is. Before we can begin discussing how it behaves, we need to develop one more crucial tool.

2.3 The Riemann Functional Equation

Riemann did more than just develop an analytic continuation for the zeta function. He also found a *functional equation* for the zeta function; he found an expression which relates the zeta function in one domain to another. We have already seen an example of one such equation in the Gamma function, lemma 1.11. This in turn lead to an almost complete characterization of the zeta function.

As usual, we begin by defining a contour. Denote by μ_n the contour which starts on the real axis at $(2n+\frac{1}{2})\pi$, circles the origin counter clockwise until it again reaches the positive real axis, where it then travels down the real axis to ϵ, circles the real axis clockwise, and then returns down the real axis to $(2n+\frac{1}{2})\pi$.

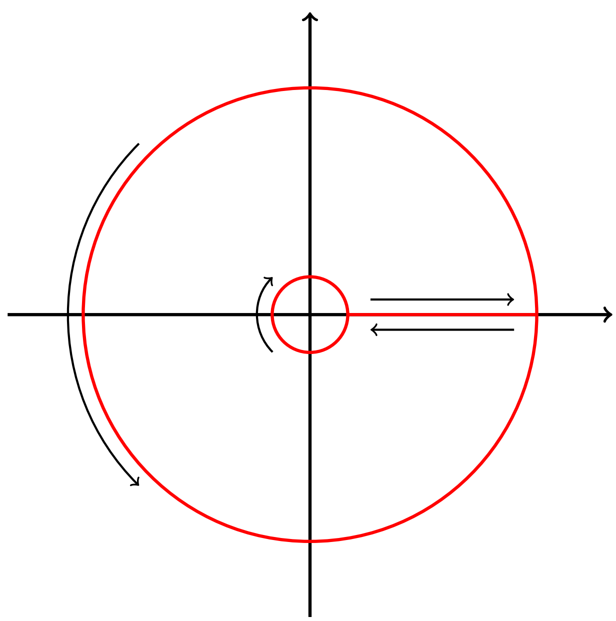

Figure 5: The contour μ_n

Denote by η_n the piece of the Hankel contour, η, which starts and ends at $(2n+\frac{1}{2})\pi$ instead of $+\infty$. It follows that $\eta_n \to \eta$ as $n \to \infty$. If we define C_n to be the circle of radius $(2n+\frac{1}{2})\pi$, it follows that

$$\int_{\mu_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z} = \int_{C_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z} - \int_{\eta_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z}$$

Or equivalently,

$$H(s) = \lim_{n\to\infty} \int_{C_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z} - \int_{\mu_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z}$$

If we can show the limiting behavior of these integrals we can determine an alternate expression for $H(s)$.

<u>Lemma 2.5</u>: If $Re(s) < 0$, then

$$\lim_{n\to\infty} \int_{C_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z} = 0$$

<u>Proof</u>: Let $R = (2n + \frac{1}{2})\pi$ for shorthand. We then have that

$$\left|\int_{C_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z}\right| \leq 2\pi R\frac{|z|^{Re(s)-1}}{|e^z - 1|}$$

$$= 2\pi\frac{R^{Re(s)}}{|e^z - 1|}$$

and this goes to 0 as $R \to \infty$ due to the exponential factor in the denominator [2, 3, 5].

<u>Lemma 2.6</u>:

$$\int_{\mu_n} \frac{(-z)^s}{e^z - 1}\frac{dz}{z} = -2\pi i \sum_{m=1}^{n} \left((2\pi mi)^{s-1} + (-2\pi mi)^{s-1}\right)$$

<u>Proof</u>: Since μ_n is a closed contour, we can use the residue theorem to evaluate the integral. It follows that there are simple poles at each $2\pi mi$, $-2\pi mi$ for m a positive integer greater than one but less than or equal to n. It is easy to see that these are simple poles since the order of the zero in the denominator is 1;

$$\frac{d}{dz}(e^z - 1) = e^z \neq 0$$

Then we have that

$$\int_{\mu_n} \frac{(-z)^s}{e^z - 1} \frac{dz}{z} = 2\pi i \sum_{m=1}^{n} Res(2\pi mi) + Res(-2\pi mi)$$

Because these are simple poles, we can use the fact that

$$Res(z_0) = \frac{g(z_0)}{h'(z_0)}$$

to get that

$$Res(2\pi mi) = -\frac{(-2\pi mi)^{s-1}}{1}$$

and

$$Res(2\pi mi) = -\frac{(2\pi mi)^{s-1}}{1}$$

so that

$$\int_{\mu_n} \frac{(-z)^s}{e^z - 1} \frac{dz}{z} = -2\pi i \sum_{m=1}^{n} \left((2\pi mi)^{s-1} + (-2\pi mi)^{s-1}\right)$$

and this concludes the proof.

We now have enough to develop the functional equation.

Theorem 2.1:

$$\zeta(s) = (2\pi)^{s-1} \frac{\sin(\frac{\pi s}{2})}{\pi} \Gamma(1-s)\zeta(1-s)$$

Proof: From lemmas 2.5 and 2.6 we have that

$$H(s) = \lim_{n\to\infty} 2\pi i \sum_{m=1}^{n} \left((2\pi mi)^{s-1} + (-2\pi mi)^{s-1}\right)$$

However,

$$((2\pi mi)^{s-1} + (-2\pi mi)^{s-1}) = ((2\pi i)^{s-1} + (-2\pi i)^{s-1})m^{s-1}$$

$$= (2\pi)^{s-1}(i^{s-1} + (-i)^{s-1})m^{s-1} = \frac{2\pi}{i}(i^s - (-i)^s)m^{s-1}$$

$$= \frac{2\pi}{i}(e^{i\frac{\pi s}{2}} - e^{-\frac{\pi s}{2}})m^{s-1} = (2\pi)^{s-1} 2\sin(\frac{\pi s}{2})m^{s-1}$$

So that, for $Re(s) < 0$,

$$H(s) = \lim_{n\to\infty}(2\pi)^s i \sin(\frac{\pi s}{2})\sum_{m=1}^{n}\frac{1}{m^{1-s}} = (2\pi)^s i\sin(\frac{\pi s}{2})\zeta(1-s)$$

Plugging into the zeta function gives

$$\zeta(s) = (2\pi)^{s-1}\sin(\frac{\pi s}{2})\Gamma(1-s)\zeta(1-s)$$

which proves the theorem.

There is one precaution we must take: this relations holds only when both sides are analytic. We have not yet discussed where the zeta function is analytic. As it turns out, the above will hold so long as neither $s, 1-s = 0$.

2.4 Analytic Properties of the Zeta Function

We may now finally begin to break down the behavior of the zeta function. Where it is analytic and where its zeroes are located are of central importance in many additional theorems; we show in the next section how a proof of the prime number theorem is dependent on the behavior of the zeta function about a pole, and where its zeros lie.

Theorem 2.2: $\zeta(s)$ is meromorphic with only a simple pole at $s = 1$.

Proof: Note that the location of the pole should be somewhat intuitive, at $s = 1$ the series representation approaches the harmonic series, which diverges. The fact that it is the *only* pole is less obvious.

By definition, we have that

$$\zeta(s) = \frac{\Gamma(1-s)}{2\pi i}H(s)$$

However, lemma 2.2 tells us $H(s)$ is entire and theorem 1.3 tells us $\Gamma(1-s)$ is meromorphic with simple poles at the positive integers. This in turn implies that *at worst* ζ has simple poles at the integers. However, for $Re(s) > 1$, we have that

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

By corollary 1.1, this implies $\zeta(s)$ is analytic in any disc in the half of the plane with $Re(s) > 1$. This in turn implies that $\zeta(s)$ is analytic for $Re(s) > 1$, so there can be no poles at $s = 2, 3, 4, \ldots$. This should be intuitively obvious since we have already seen that

$$\zeta(2) = \frac{\pi^2}{6}$$

As it turns out, $H(s)$ has zeros at the positive integers greater than 1, which cancel the simple poles of $\Gamma(1-s)$ there [5]. Knowing that the series representation is analytic is sufficient, however, and so we omit this proof. Therefore, the only simple pole left unaccounted for is $s = 1$ which we have shown by inspection of the series representation is not canceled by $H(s)$.

Theorem 2.3: $\zeta(s)$ has no zeroes for $Re(s) > 1$. Similarly, the only zeros for $Re(s) < 0$ are the negative, even integers $z = -2, -4, -6, \ldots$.

Proof: For $Re(s) > 0$, we make use of the fact that

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

Again, an infinite product is zero if and only if there is a factor which is zero. However, for all s with $Re(s) > 1$,

$$\frac{1}{1 + \frac{1}{p^s}} \neq 0$$

which proves the first half of the theorem. For the second piece, we make use of the functional equation. For $Re(s) < 0$ we have that

$$\zeta(s) = (2\pi)^{s-1} \frac{\sin(\frac{\pi s}{2})}{\pi} \Gamma(1-s)\zeta(1-s)$$

If $Re(s) < 0$, this in turn implies that $Re(1-s) > 1$. By the above, this means $\zeta(1-s)$ contributes no zeros. Similarly, we know $\Gamma(1-s)$ is analytic in this domain, and that it is also no where zero and hence does not contribute any zeros. $(2\pi)^{s-1}$ is entire and it is not hard to show that it is also never zero. This means that the only zeros of $\zeta(s)$ for $Re(s) < 0$ are contributed by the sin factor. The complex sin only has zeros for real arguments, specifically only at the zeros of the real valued sin [5]. This then implies that $\zeta(s)$ has zeros at the negative even integers. Since these zeros are easily found they are referred to as the *trivial zeros* of the zeta function.

Corollary 2.1: $\zeta(s)$ has no zeros for $Re(s) = 1$ or $Re(s) = 0$.

Proof: This is in essence, more of a trick than an insightful method. However, it does prove what we claim. We start with the product form of the zeta function: for $Re(s) > 1$

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

Since this product is absolutely convergent, it implies that

$$\log(\zeta(s)) = \sum_p \log\left(\frac{1}{1 - \frac{1}{p^s}}\right) = -\sum_p \left(1 - \frac{1}{p^s}\right)$$

is absolutely convergent. For all p, $|\frac{1}{p^s}| < 1$ so that we can use the series expansion for log to get

$$\log(\zeta(s)) = -\sum_p \left(-\sum_{m=1}^{\infty} \frac{(p^- s)^m}{m}\right) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}$$

hence

$$\zeta(s) = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}}\right\}$$

Again, this holds only for $Re(s) > 1$. Let $s = x + iy$. We now show that

$$|\zeta(x + iy)| = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{\cos(my\log(p))}{mp^{mx}}\right\}$$

We have

$$\zeta(x + iy) = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{mx+imy}}\right\} = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{p^{-imy}}{mp^{mx}}\right\}$$

$$= \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{e^{-imy\log(p)}}{mp^{mx}}\right\} = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{\cos(my\log(p)) - i\sin(my\log(p))}{mp^{mx}}\right\}$$

$$= \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{\cos(my\log(p))}{mp^{mx}}\right\} \exp\left\{i \sum_p \sum_{m=1}^{\infty} \frac{-\sin(my\log(p))}{mp^{mx}}\right\}$$

However, for any real θ, we have that $|e^{i\theta}| = 1$. This implies that

$$|\zeta(x+iy)| = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{\cos(my\log(p))}{mp^{mx}}\right\}$$

Assume that $\zeta(1+iy) = 0$ for some $y \neq 0$. Define the function

$$f_y(x) = \zeta(x)^3 \zeta(x+iy)^4 \zeta(x+i2y)$$

We note that this is a complex valued, real analytic function. $\zeta(x+iy)$ has already shown to be a meromorphic function with simple pole at $x+iy = 1$. But if $x+iy = 1$, $\zeta(x)^3$ has a pole of order three, however by assumption $\zeta(x+iy)^4$ has a zero of order four, hence f has a zero at $x = 1$. It immediately follows that $|f(1)| = 0$ and $\lim_{x\to 1^+} |f(x)| = 0$. Now assume that $x > 1$ and look at $|f(x)|$:

$$|f(x)| = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{3 + 4\cos(my\log(p)) + \cos(2my\log(p))}{mp^{mx}}\right\}$$

Let $\theta = my\log(p)$ for shorthand. By the double angle formula, we have that

$$3 + 4\cos(\theta) + \cos(2\theta) = 3 + 4\cos(\theta) + 2\cos^2(\theta) - 1 = 2(1 + 2\cos(\theta) + \cos^2(\theta))$$

$$= 2(1+\cos(\theta))^2$$

So that

$$|f(x)| = \exp\left\{\sum_p \sum_{m=1}^{\infty} \frac{2(1+\cos(\theta))^2}{mp^{mx}}\right\}$$

Note that

$$\frac{2(1+\cos(\theta))^2}{mp^{mx}} \geq 0$$

by our choice of x and the fact that $m, p \geq 1$. Then

$$|f(x)| \geq e^0 = 1$$

for all $x > 1$. But then $\liminf_{x\to 1^+} |f(x)| = 1$, which contradicts the fact that $\lim_{x\to 1^+} |f(x)| = 0$, hence

$\zeta(1+iy) \neq 0$. Since we have already shown there is a simple pole at $s = 1$, this implies $\zeta(s) \neq 0$ for s with $Re(s) = 1$. The functional equation then tells us that, except for $z = 0$, $\zeta(s) \neq 0$ for s with $Re(s) = 0$. Because there is a pole at $s = 1$, the functional equation does not immediately apply when we try and evaluate $\zeta(0)$. However, the zero of sin cancels this pole. It is not hard to then show that $\zeta(0) = -\frac{1}{2}$ [2].

With the development of these tools we have almost completely constructed a basic characterization of the zeta function. For $Re(s) > 1$ it behaves like a familiar series. For $Re(s) < 0$ it behaves like the product of this series with a few other familiar functions. In these regions we know where the zeta function is analytic and the location of its zeros. It is only in the strip $0 \leq Re(s) \leq 1$ that the zeta function has the possibility to behave erratically. For this reason, it is called *the critical strip*, illustrated below in figure 6.

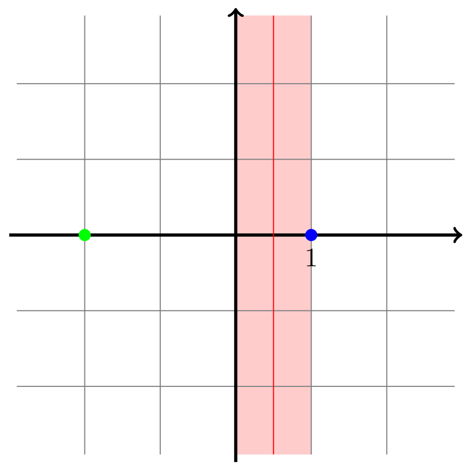

Figure 6: The critical strip is shaded red. The blue dot represents the pole of ζ, the green is the first nontrivial zero, and the red line is the line with $Re(s) = \frac{1}{2}$.

2.5 The Riemann Hypothesis

This paper would be remiss if it had no mention of the Riemann Hypothesis. In fact, the rest of this paper could easily be devoted to the work that has been done over the past 150 years on proving or disproving the hypothesis. However, the aim of this paper is to study zeta functions, and while studying the truth or falseness of the hypothesis would certainly contribute to this study I feel as if the scope of the paper would be too narrow.

In studying his zeta function, Riemann made a conjecture about one of the most basic properties of a function: the location of its zeros. He had already succeeded in showing that the only zeros outside of the critical strip were the trivial zeros. Again however, the behavior of the zeta function inside of the critical strip is much more difficult to understand. He made the following guess which he deemed “very likely” to be true:

The Riemann Hypothesis: All nontrivial zeros of the zeta function lie on the line with real part $\frac{1}{2}$.

and there the conjecture has stood for the last 150 years. Much progress has been made in the attempts prove the hypothesis. Hundreds of thousands of zeros, if not millions, have been calculated and found to lie on this line. There are ways to narrow down the regions of the critical strip which cannot have a zero. Many, many brilliant mathematicians have also agreed that it is very likely to be true. However, no proof (or disproof) has been found.

Riemann himself did not initially concern himself with his guess. Certainly he attempted a proof but was unable to find one. In the context of his work however, “On the number of primes less than a given magnitude”, the exact location of the nontrivial zeros was not important; the fact they lay somewhere within the critical strip was enough for his purposes at the time.

Many results have been proven on the assumption of the Riemann Hypothesis. However, his work was pivotal enough to prove many important results even without the truth of his hypothesis. We examine one such result to see just how powerful a tool Riemann’z zeta function is.

3 The Prime Number Theorem

Already we have seen work that suggests Riemann'z zeta function is intricately connected to the prime numbers. There is Euler's product formula over the primes, or the fact that the title of Riemann's paper in which he developed the zeta function was "On the number of primes less than a given magnitude". There is one result related to the primes which Riemann's work, with a bit of additional machinery, is sufficient to prove: the Prime Number Theorem. We define the *prime counting function* as

$$\pi(x) = \sum_{p \leq x} 1$$

or the function which returns how many primes are less than or equal to a real number x. The Prime Number Theorem states

$$\pi(x) \sim \frac{x}{\ln(x)}$$

or equivalently

$$\lim_{x \to \infty} \frac{\pi(x)\ln(x)}{x} = 1$$

To be incredibly vague, this means that $\pi(x)$ "behaves like" $\frac{x}{\ln(x)}$ for very large x. Variants of this statement can be traced all the way back to Gauss [2], and perhaps even further. However, there was no definitive proof of the theorem even while Riemann worked on it. In fact, the proof did not come until a few decades after Riemann's passing.

The Prime Number Theorem was proven independently and simultaneously in 1896 by Hadamard and Poussin. Their proofs both were based in the realm of Riemann's work a few decades prior as well as developments from others such as Chebyshev and von Mangoldt. The proofs themselves are elegant and display much of the behavior of the zeta function itself. However, their proofs are lengthy and fairly complicated; in place of either of these proofs I choose to use D.J. Newman's proof which, while less revealing about the zeta function itself, is concise and satisfactory.

3.1 Chebyshev, $\vartheta(x)$ and $\Phi(s)$

We begin by defining a few functions. The first is called *Chebyshev's first function*, and is given by

$$\vartheta(x) = \sum_{p \leq x} \ln(p)$$

The second is given by

$$\Phi(z) = \sum_p \frac{\ln(p)}{p^z}$$

We prove a few facts about these functions, much of which was known to Chebyshev prior to Hadamard and Poussin proving the prime number theorem.

Lemma 3.1: $\Phi(z)$ is analytic for $Re(z) > 1$.

Proof: Consider any open disc in the right half plane. We have that

$$|\Phi(z)| \leq \sum_p \left| \frac{\ln(p)}{p^z} \right| = \sum_p \frac{\ln(p)}{p^{Re(z)}}$$

Similar to how the exponential function outgrows any positive power of x, the logarithm eventually grows slower than any positive power of x [8]. Then for any $\epsilon > 0$ there is some x_0 such that for all $x \geq x_0$, $\ln(x) \leq x^\epsilon$. Then the above becomes

$$\sum_p \frac{\ln(p)}{p^{Re(z)}} \leq \text{finite} + \sum_{p'} \frac{p^\epsilon}{p^{Re(z)}} = \text{finite} + \sum_{p'} \frac{1}{p^{Re(z)-\epsilon}}$$

where p' is the first prime greater than x_0. However,

$$\sum_{p'} \frac{1}{p^{Re(z)-\epsilon}} \leq \sum_{n=p'}^{\infty} \frac{1}{n^{Re(z)-\epsilon}}$$

and we know that this series converges by a basic p-test when $Re(z) - \epsilon > 1$ which is the same as $Re(z) > 1$. By corollary 1.1 this shows that $\Phi(z)$ is analytic in an arbitrary disc in the half plane, hence it is analytic for $Re(s) > 1$.

Lemma 3.2: $\zeta(s) - \frac{1}{s-1}$ is analytic for $Re(s) > 0$.

Proof: For $Re(s) > 1$ we have that

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^{\infty} \frac{dx}{x^s} = \sum_{n=1}^{\infty} \int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{x^s} \right) dx$$

However, we have that

$$\left|\int_n^{n+1}\left(\frac{1}{n^s}-\frac{1}{x^s}\right)dx\right| \leq \max_{n\leq x\leq n+1}\left|\frac{1}{n^s}-\frac{1}{x^s}\right| = \max_{n\leq x\leq n+1}\left|\int_n^x \frac{s}{x^{s+1}}dx\right|$$
$$\leq \max_{n\leq x\leq n+1}\left|\frac{s}{x^{s+1}}(x-n)\right| \leq \max_{n\leq x\leq n+1}\left|\frac{s}{x^{s+1}}\right|$$

Finally,

$$\max_{n\leq x\leq n+1}\left|\frac{s}{x^{s+1}}\right| \leq \max_{n\leq x\leq n+1}\frac{|s|}{x^{Re(s)+1}} = \frac{|s|}{n^{Re(s)+1}}$$

However, the series

$$\sum_{n=1}^{\infty}\frac{|s|}{n^{Re(s)+1}}$$

converges for $Re(s) > 0$, which implies by corollary 1.1 that $\zeta(s) - \frac{1}{s-1}$ is analytic for $Re(s) > 0$. It may seem odd that we return to prove an additional fact about the zeta function, but as we will see in the next lemma that $\Phi(s)$ is related to $\zeta(s)$.

Lemma 3.3: $\Phi(s)$ is meromorphic for $Re(s) > \frac{1}{2}$. Similarly, $\Phi(s) - \frac{1}{s-1}$ is analytic for $Re(s) \geq 1$.

Proof: We return to the Euler product for the zeta function. For $Re(s) > 1$,

$$\zeta(s) = \prod_p (1-\frac{1}{p^s})^{-1}$$

Again,

$$\log(\zeta(s)) = \log\left(\prod_p (1-\frac{1}{p^s})^{-1}\right) = -\sum_p \log(1-\frac{1}{p^s})$$

We then apply logarithmic differentiation to yield that

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \frac{\frac{\ln(p)}{p^s}}{1-\frac{1}{p^s}} = -\sum_p \frac{\ln(p)}{p^s-1}$$

Going back a step, we have that

$$\frac{1}{p^s-1} = \frac{1}{p^s}\frac{1}{1-\frac{1}{p^s}}$$

The right side is a geometric series, hence

$$\frac{1}{p^s - 1} = \frac{1}{p^s}\sum_{n=1}^{\infty}\left(\frac{1}{p^s}\right)^n = \sum_{n=0}^{\infty}\left(\frac{1}{p^s}\right)^{n+1}$$

and

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\ln(p)}{p^s} + \sum_p \sum_{n=0}^{\infty} \frac{\ln(p)}{p^{s(n+2)}}$$

which, by definition, is

$$-\frac{\zeta'(s)}{\zeta(s)} = \Phi(s) + \sum_p \sum_{n=0}^{\infty} \frac{\ln(p)}{p^{s(n+2)}}$$

By theorem 2.2, $-\frac{\zeta'(s)}{\zeta(s)}$ is meromorphic with simple pole at $s = 1$ and poles at any zeros of the zeta function. All that remains is to understand the behavior of the double sum. We have that

$$\sum_p \sum_{n=0}^{\infty} \frac{\ln(p)}{p^{s(n+2)}} = \sum_p \left(\frac{\ln(p)}{p^{2s}} \sum_{n=0}^{\infty} \frac{1}{p^{sn}}\right)$$

Again, the rightmost series is a geometric series for $Re(s) > 0$, hence

$$\sum_{n=0}^{\infty} \frac{1}{p^{sn}} = \frac{1}{1 - \frac{1}{p^s}}$$

This is dependent on p, however;

$$\left|\sum_{n=1}^{\infty}\left(\frac{1}{p^s}\right)^n\right| = \left|\frac{1}{1 - \frac{1}{p^s}}\right|$$

Now if we assume that $Re(s) > \frac{1}{2}$ for reasons that will soon be apparent, we have that

$$p^{Re(s)} \geq \sqrt{2}$$

Hence

$$1 - \frac{1}{\sqrt{2}} \leq 1 - \frac{1}{p^{Re(s)}}$$

and

$$0 \leq \frac{1}{1 - \frac{1}{p^{Re(s)}}} \leq \frac{1}{1 - \frac{1}{\sqrt{2}}}$$

The reverse triangle inequality gives that

$$\left||1| - \left|\frac{1}{p^s}\right|\right| = 1 - \frac{1}{p^{Re(s)}} \leq \left|1 - \frac{1}{p^s}\right|$$

so that in totality we have

$$\left|\frac{1}{1-\frac{1}{p^s}}\right| \leq \frac{1}{1-\frac{1}{\sqrt{2}}} = \beta$$

Then

$$\left|\sum_p \sum_{n=0}^{\infty} \frac{\ln(p)}{p^{s(n+2)}}\right| \leq \beta \sum_p \frac{\ln(p)}{p^{2Re(s)}}$$

However, by lemma 3.1 we have shown that the rightmost series converges for $Re(s) > \frac{1}{2}$. This implies that this double series is absolutely and uniformly convergent, therefore by corollary 3.1 defines an analytic function for $Re(s) > \frac{1}{2}$. This in turn implies that $\Phi(s)$ is meromorphic for $Re(s) > \frac{1}{2}$ with poles at $s = 1$ and the zeros of the zeta function. It is interesting to note that if it can be proven that the only pole of $\Phi(s)$ is at $s = 1$ that this, in turn, implies the truth of the Riemann hypothesis. Since $\Phi(s)$, $\frac{1}{s-1}$ both have a simple pole at $s = 1$, this implies that in $\Phi(s) - \frac{1}{s-1}$ the poles cancel [5] and hence $\Phi(s) - \frac{1}{s-1}$ is analytic for $Re(s) \geq 1$ since we have already shown there are no zeros of ζ with $Re(s) = 1$.

Lemma 3.4: For $Re(s) > 1$,

$$\Phi(s) = s\int_1^{\infty} \frac{\vartheta(x)}{x^{s+1}}dx$$

Proof: We prove this by calculating the integral between successive primes and summing these pieces, i.e.

$$\int_1^{\infty} \frac{\vartheta(x)}{x^{s+1}}dx = \sum_{i=0}^{\infty} \int_{p_i}^{p_{i+1}} \frac{\vartheta(x)}{x^{s+1}}dx$$

where it is understood that p_{i+1} is the next largest prime after p_i, and for convenience we allow the zeroth prime to be 1. We begin with

$$\int_1^{2} \frac{\vartheta(x)}{x^{s+1}}dx$$

In this interval we have that $\vartheta(x) = 0$ so that

$$\int_0^\infty \frac{\vartheta(x)}{x^{s+1}} dx = 0$$

For the interval $[2, 3)$ we have that $\vartheta(x) = \ln(2)$ so that

$$\int_2^3 \frac{\vartheta(x)}{x^{s+1}} dx = \ln(2) \int_2^3 \frac{dx}{x^{s+1}} = -\frac{\ln(2)}{s} \left[\frac{1}{x^s} \right]_2^3$$

$$= \frac{\ln(2)}{s2^s} - \frac{\ln(2)}{s3^s}$$

We now do this calculation in general. Note that $\vartheta(p_{i+1}) = \vartheta(p_i) + \ln(p_{i+1})$. Then

$$\int_{p_i}^{p_{i+1}} \frac{\vartheta(x)}{x^{s+1}} dx = -\frac{\vartheta(p_i)}{s} \left[\frac{1}{x^s} \right]_{p_i}^{p_{i+1}}$$

$$= \frac{\vartheta(p_i)}{sp_i^s} - \frac{\vartheta(p_i)}{sp_{i+1}^s}$$

By the same method it is not hard to show that

$$\int_{p_{i+1}}^{p_{i+2}} \frac{\vartheta(x)}{x^{s+1}} dx = \frac{\vartheta(p_{i+1})}{sp_{i+1}^s} - \frac{\vartheta(p_{i+1})}{sp_{i+2}^s}$$

But then

$$\int_{p_i}^{p_{i+2}} \frac{\vartheta(x)}{x^{s+1}} dx = \frac{\vartheta(p_i)}{sp_i^s} + \frac{\ln(p_{i+1})}{sp_{i+1}^s} - \frac{\vartheta(p_{i+1})}{sp_{i+2}^s}$$

It then follows that by working backwards inductively we get

$$\int_1^{p_n} \frac{\vartheta(x)}{x^{s+1}} dx = \sum_{i=1}^{n-1} \frac{\ln(p_i)}{sp_i^s} - \frac{\vartheta(p_{n-1})}{sp_n^s}$$

Letting $n \to \infty$ we find that

$$\int_1^\infty \frac{\vartheta(x)}{x^{s+1}} dx = \sum_p \frac{\ln(p)}{sp^s} + \lim_{n\to\infty} \frac{\vartheta(p_{n-1})}{sp_n^s} = \frac{\Phi(s)}{s} + \lim_{n\to\infty} \frac{\vartheta(p_{n-1})}{sp_n^s}$$

The last thing we need to show is then obviously that

$$\lim_{n\to\infty} \frac{\vartheta(p_{n-1})}{sp_n^s} = 0$$

We have that

$$\left|\frac{\vartheta(p_{n-1})}{sp_n^s}\right| < \frac{\vartheta(p_n)}{|s|p_n^{Re(s)}} < \frac{\vartheta(p_n)}{p_n^{Re(s)}} < \frac{n\ln(p_n)}{p_n^{Re(s)}} < \frac{p_n\ln(p_n)}{p_n^{Re(s)}} = \frac{\ln(p_n)}{p_n^{Re(s)-1}}$$

We again make use of the fact that the logarithm grows slower than any positive power of x. Choose $0 < \epsilon < Re(s) - 1$. Then there is some N such that for all $n \geq N$, $\ln(p_n) < p_n^\epsilon$. Therefore

$$\frac{\ln(p_n)}{p_n^{Re(s)-1}} < \frac{p_n^\epsilon}{p_n^{Re(s)-1}} = \frac{1}{p_n^{Re(s)-1-\epsilon}}$$

By construction, $Re(s) - 1 - \epsilon > 0$, so that $p_n^{Re(s)-1-\epsilon} \to \infty$ as $n \to \infty$, hence

$$\lim_{n\to\infty} \frac{\vartheta(p_{n-1})}{sp_n^s} = 0$$

as claimed and this implies

$$\int_1^\infty \frac{\vartheta(x)}{x^{s+1}}dx = \frac{\Phi(s)}{s}$$

which proves the lemma.

We have proven about everything we need to for these two functions. We now examine *why* we developed these tools and how they help us prove the prime number theorem.

3.2 Newman's Approach

As previously mentioned, we use D.J. Newman's proof of the prime number theorem instead of Hadamard's or Poussin's proof. Newman's approach is very straightforward. It was know by Chebyshev, Hadamard, and Poussin that proving

$$\vartheta(x) \sim x$$

would prove the prime number theorem (we explain why in the next few sections)[2]. The difficulty faced by everyone mentioned above was proving this asymptotic behavior. Newman develops an analytic theorem which proves the integral

$$\int_1^\infty \frac{\vartheta(x) - x}{x^2}dx$$

converges [4, 11]. This convergence, in turn implies the exact asymptotic behavior we seek to prove. We will prove this in good time. First, we need to state and prove the analytic theorem.

3.3 The Analytic Theorem

The integral we wish to show converges is entirely real. However, we must use complex analysis to prove that it does converge.

Theorem 3.1: Given a piecewise continuous function $f(t)$ which is bounded, say by B for all real $t \geq 0$, if

$$g(z) = \int_0^\infty f(t)e^{-zt}dt$$

exists and is analytic for $Re(z) > 0$ and can be extended to $Re(z) \geq 0$, then

$$\int_0^\infty f(t)dt$$

exists and equals $g(0)$.

Proof: We begin by defining the function

$$g_T(z) = \int_0^T f(t)e^{-zt}dt$$

It is not hard to see that this integral is absolutely convergent regardless of z, and hence is entire [4, 5, 11]. Our goal is then to show that

$$\lim_{T\to\infty} g_T(0) = g(0)$$

which will prove the theorem.

We begin, as always, by defining a contour. Choose some real $R > 0$. We know the interval $[-Ri, Ri]$ on the imaginary axis is compact. Since we assume g can be extended to be analytic on this interval, that means at every point on this interval there is a small disc where g is analytic. This then forms a covering of the interval. By the compactness of the interval, there is some finite sub covering which implies there is a $\delta > 0$ such that g is actually analytic for $Re(z) \geq -\delta$ [5]. We define the contour S which is a semicircle of radius R for $Re(z) \geq 0$. For $Re(z) < 0$, S follows the circle of radius R until it reaches $Re(z) = -\delta$, where it drops vertically until it can follow along the circle again. The piece of the contour with $Re(z) \geq 0$ is denoted S_+, with $Re(z) < 0$ S_-. The contour is illustrated in figure 7.

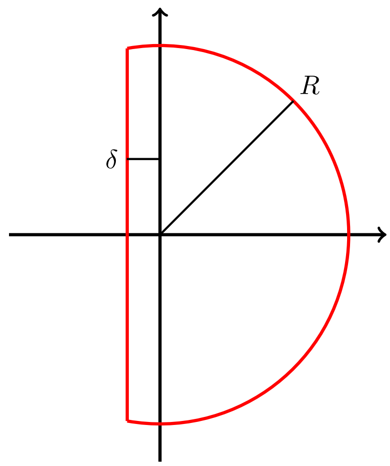

Figure 7: The contour S.

By our construction, $g(z)$ is analytic on and inside of S. It follows then that since $g_T(z)$ is entire we may apply Cauchy's integral formula to calculate the value of the difference. However, this will not immediately yield results. Instead, we consider the function

$$h(z) = (g(z) - g_T(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)$$

Since we are multiplying the difference by an entire function, h is also analytic inside of and on S and note that

$$h(0) = g(0) - g_T(0)$$

we now apply Cauchy's integral formula to h to get that

$$g(0) - g_T(0) = \frac{1}{2\pi i}\int_S (g(z) - g_T(z))e^{zT}\left(1 + \frac{z^s}{R^2}\right)\frac{dz}{z}$$

First, it is easy to see that

$$\int_S = \int_{S_+} + \int_{S_-}$$

and that

$$\int_{S_-} (g(z) - g_T(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}$$

$$= \int_{S_-} g(z)e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{dz}{z} - \int_{S_-} g_T(z)e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{dz}{z}$$

therefore

$$|g(0) - g_T(0)|$$
$$\leq \frac{1}{2\pi}\left(\left|\int_{S_+}\right| + \left|\int_{S_-} g(z)e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{dz}{z}\right| + \left|\int_{S_-} g_T(z)e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{dz}{z}\right|\right)$$

We now find appropriate bounds for each of these integrals. First, we prove a useful result. If $|z| = R$, then

$$\left|e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{1}{z}\right| = \frac{2e^{Re(z)T}|Re(z)|}{R^2}$$

The exponential factor is not hard to see: the imaginary factor has norm 1. For the rest, we pull a factor of $\frac{1}{R}$ out of the parenthesis and multiply the $\frac{1}{z}$ in to get that

$$\left|\left(1+\frac{z^2}{R^2}\right)\frac{1}{z}\right| = \left|\frac{R}{z} + \frac{z}{R}\right|\frac{1}{R}$$

Letting $z = x + iy$ and using the fact that for all $z \neq 0$, $\frac{1}{z} = \frac{x-iy}{|z|^2}$, we get that

$$\left|\frac{R}{z} + \frac{z}{R}\right|\frac{1}{R} = \left|\frac{R(x-iy) + R(x+iy)}{R^2}\right|\frac{1}{R} = \frac{2|Re(z)|}{R^2}$$

and this prove the claim. We now show that

$$\left|\int_{S_+} (g(z) - g_T(z))e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{dz}{z}\right| < \frac{2B\pi}{R}$$

.

For $Re(z) > 0$, we have that

$$g(z) - g_T(z) = \int_T^\infty f(t)e^{-zt}dt$$

hence

$$|g(z) - g_T(z)| \leq \int_T^\infty |f(t)e^{-zt}|dt = B\int_T^\infty e^{-Re(z)t}dt$$
$$= \frac{Be^{-Re(z)T}}{Re(z)}$$

With that done, we have that

$$\left|\int_{S_+} \frac{h(z)}{z} dz\right| \leq \pi R \left|\frac{(g(z) - g_T(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)}{z}\right| < \frac{2B\pi}{R}$$

which we get by multiplying the above bounds together. We now show that

$$\left|\int_{S_-} (g(z) - g_T(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}\right| < \frac{2B\pi}{R}$$

Note that the integrand is analytic except at $z = 0$. We can then deform S_- to the semicircle of radius R with $Re(z) < 0$, since it has the same end points. We then just need to find a bound on $g_T(z)$. We have that

$$|g_T(z)| = \left|\int_0^T f(t)e^{-zt}dt\right| \leq B\int_0^T e^{-Re(z)t}dt = -\frac{B}{Re(z)}\left(e^{-Re(z)T} - 1\right)$$

$$< -\frac{Be^{-Re(z)T}}{Re(z)}$$

Using the above bounds, we get that

$$\left|\int_{S_-} g_T(z)e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}\right| < \frac{2B\pi}{R}$$

since $\frac{|Re(z)|}{Re(z)} = -1$. For the last integral, we do something a bit different. We show that

$$\left|\int_{S_-} g(z)e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}\right| \to 0$$

uniformly as $T \to \infty$. Note that the only piece of this integral which is dependent on T is the exponential function. Since the integrand is analytic on S_- and that this path is compact if R is finite, then the integrand is bounded. It follows that

$$\left|\int_{S_-} g(z)e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}\right| \leq \pi RCe^{Re(z)T}$$

where

$$\left|g(z)\left(1 + \frac{z^2}{R^2}\right)\frac{1}{z}\right| \leq C$$

for $z \in S_-$. Since $Re(z) < 0$ it follows that $\pi RCe^{Re(z)T} \to 0$ uniformly as $T \to \infty$.

We now put it all together. Choose $\epsilon > 0$. Then choose R such that

$$\frac{2\pi B}{R} < \frac{2\pi\epsilon}{3}$$

so that

$$\left| \int_{S_+} (g(z) - g_T(z)) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} \right| < \frac{2\pi\epsilon}{3}$$

and

$$\left| \int_{S_-} g_T(z) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} \right| < \frac{2\pi\epsilon}{3}$$

Now we can choose T_0 such that, for all $T \geq T_0$,

$$\left| \int_{S_-} g(z) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} \right| < \frac{2\pi\epsilon}{3}$$

so that

$$|g(0) - g_T(0)| < \frac{1}{2\pi} \left(\frac{2\pi\epsilon}{3} + \frac{2\pi\epsilon}{3} + \frac{2\pi\epsilon}{3} \right) = \epsilon$$

for all $T \geq T_0$, which implies

$$\lim_{T \to \infty} g_T(0) = g(0)$$

which proves the theorem.

It may seem erratic, but we now have all of the machinery necessary to prove the Prime Number Theorem.

3.4 Asymptotics

Finally we put everything we've proven together to prove the Prime Number Theorem. We begin by proving that the integral Newman uses converges.

Lemma 3.5: For $Re(z) \geq 0$,

$$\frac{\Phi(z+1)}{z+1} - \frac{1}{z} = \int_0^\infty \frac{\vartheta(e^t) - e^t}{e^{(z+1)t}} dt$$

Proof: First note that, by lemma 3.3 the expression on the left is analytic for $Re(z) \geq 0$. Then we have that

$$\int_0^\infty \frac{\vartheta(e^t) - e^t}{e^{(z+1)t}} dt = \int_0^\infty \frac{(\vartheta(e^t) - e^t)e^t}{e^{(z+2)t}} dt$$

Let $e^t = x$ so that

$$\int_0^\infty \frac{(\vartheta(e^t) - e^t)e^t}{e^{(z+2)t}} dt = \int_1^\infty \frac{\vartheta(x) - x}{x^{z+2}} dx = \int_1^\infty \frac{\vartheta(x)}{x^{z+2}} dx - \int_1^\infty \frac{dx}{x^{z+1}}$$

$$= \frac{\Phi(z+1)}{z+1} - \frac{1}{z}$$

Lemma 3.6: For all $x \geq 0$,

$$\vartheta(x) < 2\ln(2)x$$

Proof: This is due to Chebyshev. We have that

$$2^{2n} = \sum_{j=0}^{2n} \binom{2n}{j} \geq \binom{2n}{n} \geq \prod_{n<p\leq 2n} p$$

This follows since

$$\binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{(n+1)(n+2)\cdots(2n)}{n!}$$

Since this is guaranteed to be an integer and no prime $n < p \leq 2n$ can be divided by any factor of $n!$, the inequality follows.

we then have that

$$\prod_{n<p\leq 2n} p \leq 2^{2n}$$

Taking the logarithm of both sides yields

$$\sum_{n<p\leq 2n} \ln(p) \leq 2n\ln 2$$

Let $n = 2^{k-1}$. Then we have that

$$\sum_{2^{k-1}<p\leq 2^k} \ln(p) \leq 2^k \ln(2)$$

We can inductively drop k by 1 all the way down to 1 to get that

$$\sum_{p\leq 2^k} \ln(p) \leq (2^k + 2^{k-1} + \ldots + 1)\ln(2) < 2^{k+1}\ln(2) = 2\ln(2)(2^k)$$

However, let $x = 2^k$, which then implies

$$\sum_{p\leq x} \ln(p) = \vartheta(x) < 2\ln(2)x$$

<u>Lemma 3.7</u>: The integral

$$\int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$$

converges.

<u>Proof</u>: We wish to use theorem 3.1 that we just developed but we need to get the above integral into the correct form. Let

$$f(t) = (\vartheta(e^t) - e^t)e^{-t}$$

and consider the integral

$$\int_0^\infty \frac{\vartheta(e^t) - e^t}{e^t} dt$$

Like the above lemma, substitute $e^t = x$ to show that

$$\int_0^\infty \frac{\vartheta(e^t) - e^t}{e^t} dt = \int_1^\infty \frac{\vartheta(x) - x}{x^2} dx$$

This implies that if we can show that $f(t)$ satisfies the conditions of theorem 3.1 then the above integral converges. We first check that it is globally bounded. We have that

$$|(\vartheta(e^t) - e^t)e^{-t}| = |\vartheta(e^t)e^{-t} - 1| \leq \vartheta(e^t)e^{-t} + 1$$

However, we showed in lemma 3.6 that

$$\vartheta(x) \leq 2\ln(2)x$$

for all $x \in [0, \infty)$. Then

$$|(\vartheta(e^t) - e^t)e^{-t}| = |\vartheta(e^t)e^{-t} - 1| \leq 2\ln(2)e^t e^{-t} + 1 = 2\ln(2) + 1$$

hence the function is globally bounded. Similarly, $\vartheta(x)$ is piecewise continuous since it is locally constant between consecutive primes. Then if we can show that there is some

$$g(z) = \int_0^\infty f(t)e^{-zt}dt$$

which is analytic for $Re(z) \geq 0$, then this proves the lemma. However,

$$\int_0^\infty f(t)e^{-zt}dt = \int_0^\infty \frac{\vartheta(e^t) - e^t}{e^{(z+1)t}}dt = \frac{\Phi(z+1)}{z+1} - \frac{1}{z}$$

by lemma 3.5, in which we showed that this is analytic for $Re(z) \geq 0$. This concludes the proof of the lemma.

Lemma 3.8: $\vartheta(x) \sim x$.

Proof: Note that the above is equivalent to saying [5]

1. Given $\lambda > 1$, the set of x such that $\lambda x \leq \vartheta(x)$ is bounded.

2. Given $0 < \lambda < 1$, the set of x such that $\vartheta(x) \leq \lambda x$ is bounded.

If this were not the case, then clearly $\lim_{x\to\infty} \vartheta(x) \neq x$. We now assume that neither of the above are true and show that this implies that

$$\int_1^\infty \frac{\vartheta(x) - x}{x^2}dx$$

does not converge. First, assume 1 is false. Then we can continually choose arbitrarily large x_0 such that $\lambda x_0 < \vartheta(x_0)$. Choose one such x_0. Consider

$$\int_{x_0}^{\lambda x_0} \frac{\vartheta(x) - x}{x^2} dx$$

Because $\vartheta(x)$ is a monotonically increasing function, we have for all $x \in [x_0, \lambda x_0]$ that $\lambda x_0 \leq \vartheta(x_0) \leq \vartheta(x)$ by our assumption. Then

$$\int_{x_0}^{\lambda x_0} \frac{\vartheta(x) - x}{x^2} dx \geq \int_{x_0}^{\lambda x_0} \frac{\lambda x_0 - x}{x^2} dx = \int_{1}^{\lambda} \frac{\lambda - t}{t^2} dt$$

and it is obvious that the integral on the right is positive. We can continue and choose some x_1 such that $x_1 > \lambda x_0$ and then the same process shows that

$$\int_{x_1}^{\lambda x_1} \frac{\vartheta(x) - x}{x^2} dx \geq \int_{1}^{\lambda} \frac{\lambda - t}{t^2} dt$$

It then follows that

$$\int_{1}^{\infty} \frac{\vartheta(x) - x}{x^2} dx = \sum_{n=0}^{\infty} \left(\int_{x_n}^{\lambda x_n} \frac{\vartheta(x) - x}{x^2} dx \right) + \cdots$$

where each x_n is chosen inductively as above; it is an infinite sum because of our assumption that the set in 1 is not bounded. However, the terms in the infinite sum are bounded below by a positive constant, hence the series does not converge which implies the integral does not converge, the first contradiction.

The proof for the second piece is almost identical to the first. Now we assume 2 is false. We can then choose our x_n's as before. However, now note that

$$\int_{\lambda x_n}^{x_n} \frac{\vartheta(x) - x}{x^2} dx \leq \int_{\lambda x_n}^{x_n} \frac{\lambda x_n - x}{x^2} dx = \int_{\lambda}^{1} \frac{\lambda - t}{t^2} dt$$

It is clear by inspection that the integral on the right is negative, and that this bound is independent of our choice of x_n. So again, we have that

$$\int_{1}^{\infty} \frac{\vartheta(x) - x}{x^2} dx = \sum_{n=0}^{\infty} \left(\int_{\lambda x_n}^{x_n} \frac{\vartheta(x) - x}{x^2} dx \right) + \cdots$$

where again the sum diverges since the terms are bounded above by a negative constant which forces the integral to diverge, our second contradiction.

Since we showed the convergence of the integral in lemma 3.7, this implies that 1,2 are true and that

$$\vartheta(x) \sim x$$

We can now finish with a result that was also known to Chebyshev [2].

<u>Theorem 3.2</u>:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

<u>Proof</u>: By definition, we have that

$$\vartheta(x) = \sum_{p \leq x} \ln(p)$$

Then

$$\vartheta(x) = \sum_{p \leq x} \ln(p) \leq \sum_{p \leq x} \ln(x) = \ln(x) \sum_{p \leq x} 1 = \ln(x)\pi(x)$$

So we have show that for $x > 1$,

$$\frac{\vartheta(x)}{x} \leq \pi(x)\frac{\ln(x)}{x}$$

Now, choose x, y such that $1 < y < x$. Then

$$\pi(x) = \pi(y) + \sum_{y < p \leq x} 1 \leq \pi(y) + \sum_{y < p \leq x} \frac{\ln(p)}{\ln y} = \pi(y) + \frac{1}{\ln(y)} \sum_{y < p \leq x} \ln(p)$$

$$\leq \pi(y) + \frac{1}{\ln(y)} \sum_{p \leq x} \ln(p) = \pi(y) + \frac{\vartheta(x)}{\ln(y)} \leq y + \frac{\vartheta(x)}{\ln(y)}$$

Let $y = \frac{x}{\ln^2(x)}$, which certainly falls within our range of $(1, x)$ if we choose x sufficiently large. Substituting in yields

$$\pi(x) \leq \frac{x}{\ln^2(x)} + \frac{\vartheta(x)}{\ln(\frac{x}{\ln^2(x)})} = \frac{x}{\ln^2(x)} + \frac{\vartheta(x)}{\ln(x) - \ln(2\ln(x))}$$

Then

$$\pi(x)\frac{\ln(x)}{x} \leq \frac{1}{\ln(x)} + \frac{\vartheta(x)}{x}\frac{\ln(x)}{\ln(x) - \ln(2\ln(x))}$$

so that

$$\frac{\vartheta(x)}{x} \leq \pi(x)\frac{\ln(x)}{x} \leq \frac{1}{\ln(x)} + \frac{\vartheta(x)}{x}\frac{\ln(x)}{\ln(x) - \ln(2\ln(x))}$$

For sufficiently large x. Taking the limit and using the facts that $\vartheta(x) \sim x$ and that $\ln(x)$ grows faster than $\ln(2\ln(x))$ gives

$$1 \leq \lim_{x\to\infty} \pi(x)\frac{\ln(x)}{x} \leq 1$$

hence

$$\pi(x) \sim \frac{x}{\ln(x)}$$

This concludes the section of this thesis dedicated to the Riemann zeta function. There is much more that can be said; both about the function itself and applications of the function and associated hypothesis. Instead of delving into further technical detail, we instead take a step back and try an generalize the idea of a zeta function. Can we define a zeta function which can be applied to more general objects? Does it behave like the Riemann zeta function when applied to the proper object? How does it behave in general? These are the questions we now aim to answer.

4 The Zeta Function Over a Ring

The very first question we should ask is how do we define the zeta function "in general"? As we have previously seen there are many definitions that we could use. The very first is perhaps the most suggestive. For $Re(s) > 1$ we saw that

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

This definition of the zeta function required no more than addition and complex exponentiation. What if we restrict S? Suppose instead we let $s \in \mathbb{N}$. Well then the above definition of the zeta function only requires addition, exponentiation (multiplication the actual requirement), and division. Can we generalize more than this? The answer is yes, but we need some algebra to do so.

We remind the reader of the definition of a ring. A set R equipped with the binary operations $+, \times$ is a *ring with unity*, simply a ring from this point on, if [7, 9].

1. R under $+$ is an abelian group, that is:

    (a) There is some $0 \in R$ such that for all $r \in R$, $r + 0 = 0 + r = r$.

    (b) For any $r_1, r_2 \in R$, $r_1 + r_2 \in R$.

    (c) For any $r \in R$ there is some $-r \in R$ such that $r + (-r) = (-r) + r = 0$.

    (d) $r_1 + r_2 = r_2 + r_1$ for all $r_1, r_2 \in R$.

2. $\times$ has an identity element, 1, such that for all $r \in R$, $1 \times r = r \times 1 = r$.

3. $\times$ is associative so that $(r_1 \times r_2) \times r_3 = r_1 \times (r_2 \times r_3)$ for all $r_1, r_2, r_3 \in R$.

4. $\times$ distributes across $+$ so that $r_1 \times (r_2 + r_3) = r_1 \times r_2 + r_1 \times r_3$ for all $r_1, r_2, r_3 \in R$.

We additionally develop some notation. Let $n \in \mathbb{N}$. For any $r \in R$, denote

$$nr = \sum_{i=1}^{n} r = r + r + \cdot + r(n \text{ times})$$

where

$$0r = 0$$

and

$$r^n = \prod_{i=1}^{n} r = r \times r \times \cdots \times r(n \text{ times})$$

where

$$r^0 = 1$$

We now have enough to build a zeta function which we can apply to *any* ring.

4.1 Definition, Examples

Before we can build the zeta function, we must construct some sets. We define the set[1] generated by r under $+$ as

$$\langle r, + \rangle = \{a \in R | a = nr, n \in \mathbb{Z}_{>0}\}$$

For shorthand we call this set the *r-stack*. Next we wish to isolate the elements in the r-stack which have multiplicative inverses. We call this *the invertible r-stack*, formally

$$\mathcal{S}_r^{-1} = \left\{ a \in R | a \in \langle r, + \rangle \text{ and } \exists \frac{1}{r} \in R \right\} = \langle r, + \rangle \cap (R)^{\times}$$

Finally, we take the set of multiplicative inverses of elements in the invertible r-stack. We call this the *inverted r-stack*, formally

$$\mathcal{I}_r = \left\{ a \in R | \frac{1}{r} \in \mathcal{S}_r^{-1} \right\}$$

We can now define the zeta function over a ring R for natural arguments s and invertible element r, $\zeta_R(s, r)$. We have that

$$\zeta_R(s, r) = \sum_{a \in \mathcal{S}_r^{-1}} \frac{1}{a^s} = \sum_{a \in \mathcal{I}_r} a^s$$

The most natural choice for r is 1. For that reason, if r is not included as an argument of the zeta function or as a subscript of a set it should be assumed that $r = 1$. The choice of r acts somewhat like a "reindexing" of the zeta function. Certainly it makes sense that if we choose some $r = n1$ this would be roughly equivalent to summing only the n^{th} multiples. For an example of how this differs, choose some z_0 on

[1]Note that this need not be a monoid: 0 may not be an element of this set

the unit circle on the complex plane. Then $\langle z_0, +\rangle$ is a line of equidistant points extending from the origin, and $\mathcal{I}_{z_0}$ is a line of points approaching the origin, as illustrated in figure 8.

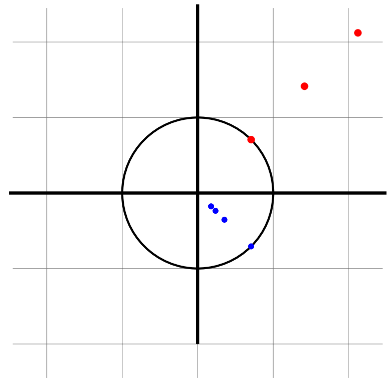

Figure 8: The red dots represent the first few terms of $\langle z_0, +\rangle$, the blue dots represent the first few terms of $\mathcal{I}_{z_0}$

Before we examine any properties of these sets or the zeta function, it would be pertinent to first work some examples. Given any ring R, why is ζ_R defined? We know that there is some $1 \in R$ and $\frac{1}{1} = 1$. Therefore, if nothing else, $1 \in \mathcal{I}$ hence the zeta function is defined. Let's consider some common rings. We have that

$$\zeta_{\mathbb{Z}}(s) = 1$$

Why? Clearly we have that

$$\mathcal{S} = \mathbb{Z}_+$$

However, for all $n \in \mathbb{Z}_+$ other than 1 no element has a multiplicative inverse in $\mathbb{Z}$ which implies $\mathcal{I} = \{1\}$. Extending $\mathbb{Z}$ to $\mathbb{Q}$ somewhat fixes this issue: it is interesting to note that $\zeta_{\mathbb{Q}}(s) \notin \mathbb{Q}$ for any s, an observation which is addressed in the additional conjectures section. Extending $\mathbb{Q}$ to $\mathbb{R}$ fixes this issue except at $s = 1$. It is also worth noting that $\zeta_{\mathbb{R}}(s) = \zeta_{\mathbb{C}}(s)$ which is exactly the Riemann zeta function for natural s.

Even though these are some of the most familiar rings, they are not the most simple to examine. We examine a specific type of ring, and collect and extrapolate data on finite versions of these rings.

4.2 Algebraic Properties

The most important question we aim to answer with this section is, given a ring R, in general how does $\zeta_R(s, r)$ "behave"? How does its behavior vary based on r? Can we relate its behavior to a ring which we can more easily study? It turns out that we can answer versions of some of these question. However, we must first develop some tools to do so.

Lemma 4.1: Let $ord_+(r) = n$. For all natural m such that $0 \leq m < n$, mr is distinct.

Proof: Pick m_1, m_2 in the above range and such that $m_1 > m_2$. Suppose that $m_1 r = m_2 r$. Then $(m_1 - m_2)r = 0$. However, $0 < m_1 - m_2 < n$, which contradicts the choice of n being the additive order of r.

Lemma 4.2: Let $ord_+(r) = n$. Then $\langle r, + \rangle = \{a \in R | a = mr \text{ for } 0 \leq m < n\}$. Additionally, $|\langle r, + \rangle| = n$.

Proof: We have that

$$\langle r, + \rangle = \{1r, 2r, \ldots, (n-1)r, nr\}$$

since

$$(n+1)r = nr + r = r$$

and this would start a cycle. However, note that by definition

$$nr = 0 = 0r$$

hence

$$\langle r, + \rangle = \{a \in R | a = mr \text{ for } 0 \leq m < n\}$$

by lemma 4.1 each of these elements is unique and this concludes the proof.

Lemma 4.3: If $ord_+(r)$ is finite for all $r \in R$, then

$$\max_{r \in R}\{|\langle r, + \rangle|\} = |\langle 1, + \rangle|$$

Proof: Suppose not and there is some r such that $|\langle r, + \rangle| > |\langle 1, + \rangle|$. We know that

$$\langle r, + \rangle = \{a \in R | a = mr \text{ for } 0 \leq m < n\}$$

by lemma 4.2 and lemma 4.1 tells us each of these elements must be unique. However, this implies that $ord_+(r) > ord_+(1)$ and so there must be some m_1, m_2 such that $m_1 \neq m_2$ but $m_1 1 = m_2 1$. Then we have that

$$m_1 r = m_1(r \cdot 1) = r \cdot (m_1 1) = r \cdot (m_2 1) = m_2 r$$

a contradiction.

We now define a function. Suppose $ord_+(r) = n$. Let $\iota : \langle r, + \rangle \to \mathbb{Z}_n$. By lemma 4.2 we know that for each $a \in \langle r, + \rangle$, $a = mr$ for some $0 \leq m < n$. Then we define $\iota(a) = m$. This ends up being a very useful function.

Lemma 4.4: ι is a bijection.

Proof: First we show injectivity. Assume that $\iota(a_1) = \iota(a_2)$. Then $m_1 = m_2$ for some $0 \leq m_1, m_2 < n$. Then $a_1 = m_1 r = m_2 r = a_2$.

For surjectivity, choose some $m \in \mathbb{Z}_n$. Then by lemma 4.2 there is some $a \in \langle r, + \rangle$ such that $\iota(a) = m$.

Lemma 4.5: If $ord_+(r) = n$ then ι is a *group* isomorphism. If r is idempotent, then ι is a ring isomorphism.

Proof: First we show that ι is always a group isomorphism. Choose some $a_1 = m_1 r, a_2 = m_2 r$. Then

1. $\iota(0) = \iota(0r) = 0$

2. $\iota(a_1 + a_2) = \iota((m_1 + m_2)r) = m_1 + m_2 = \iota(a_1) + \iota(a_2)$

This proves that ι is a homomorphism and lemma 4.4 implies that this is then a group isomorphism. If r is idempotent then $r^2 = r$. Then

1. $\iota(1r) = 1$

2. $\iota(a_1 a_2) = \iota((m_1 m_2)r^2) = \iota((m_1 m_2)r) = m_1 m_2 = \iota(a_1)\iota(a_2)$

This proves that ι is a ring homomorphism and again lemma 4.4 proves that it is a ring isomorphism.

It is important to take a moment to consider why r being idempotent allows for this to be a ring isomorphism. If anything were to fail, it would be the multiplicativity condition. It is not always true that

$$m_1 m_2 r^2$$

is an element of $\langle r, + \rangle$. For instance, let our ring be $\mathcal{M}_{2\times 2}(\mathbb{Z}_2)$, the ring of 2 by 2 squares matrices with entries from $\mathbb{Z}_2$. Let

$$r = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

It is not hard to see that

$$\langle r, + \rangle = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

however,

$$r^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

so clearly $r^2 \notin \langle r, + \rangle$.

It is also worth noting that r being idempotent is sufficient, but not necessary for ι to be a ring isomorphism. For instance, let $R = \mathbb{Z}_6$ and let $r = 2$. We have that $ord_+(2) = 3$, and

$$\langle 2, + \rangle = \{0, 2, 4\}$$

It is not hard to see that this *is* isomorphic to $\mathbb{Z}_3$ via ι. However, $2^2 = 4$ and hence 2 is not idempotent. This does however bring us to one of the most important theorems of the section.

Theorem 4.1: If $ord_+(r) = n$ and r is idempotent then $\zeta_R(s, r)$ is completely determine by $\zeta_{\mathbb{Z}_n}(s)$, that is

$$\boxed{\zeta_R(s, r) = \iota^{-1}(\zeta_{\mathbb{Z}_n}(s))}$$

Proof: By lemma 4.4 we know that ι^{-1} must exist. Since $\langle r, +\rangle$ is isomorphic to $\mathbb{Z}_n$ and ring isomorphisms preserve units, this implies that $\mathcal{S}_r^{-1} \cong (\mathbb{Z}_n)^\times$. Since $\mathcal{S}_r^{-1}$ is finite, we can then use the properties of ring isomorphisms to get that

$$\iota\left(\zeta_R(s,r)\right) = \iota\left(\sum_{a\in\mathcal{I}_r} a^s\right) = \sum_{a\in\mathcal{I}_r} \iota(a)^s = \sum_{m\in(\mathbb{Z}_n)^\times} m^s = \zeta_{\mathbb{Z}_n}(s)$$

Applying ι^{-1} to both sides proves the theorem.

Corollary 4.1: Let R be a finite ring. If $r \in R$ is idempotent then $\zeta_R(s,r)$ is completely determined by $\zeta_{\mathbb{Z}_n}(s)$ for some n.

Proof: If R is finite then this implies that $ord_+(r) = n$ for some n. Applying the theorem proves corollary. Note that 1 is always idempotent so that in particular $\zeta_R(s)$ is always completely determined by $\zeta_{\mathbb{Z}_n}(s)$ if R is finite.

This result which makes good sense once we think about it can be quite powerful. For instance, consider $\mathcal{M}_{n\times n}(\mathbb{Z}_k)$. If r is an idempotent element of this ring, then $\zeta_R(s,r)$ behaves the same regardless of our choice of n. Even if $n = 100,000,000,000,000$, if $k = 2$ and r is idempotent then $\zeta_R(s,r)$ behaves essentially like $\zeta_{\mathbb{Z}_2}(s)$ (we will see in a while that this is actually constant which makes the result even more striking).

There is a special type of ring which we also wish to consider. Let R be a ring such that either $R = \langle 1, +\rangle$ or $R \setminus \{0\} = \langle 1, +\rangle$. We then call R *additively generable.*

Lemma 4.6: If R is an additively generable ring then R is a commutative ring.

Proof: This should be somewhat obvious: if R can be formed using only addition which, by definition is abelian, then it would make sense for it to be commutative. In fact, this is basically the proof methodology. Let $r_1, r_2 \in R$. Then we have that $r_1 = n_1 1, r_2 = n_2 1$ for some natural n_1, n_2. Then

$$r_1 \cdot r_2 = n_1 1 \cdot n_2 1 = (n_1 n_2)\cdot 1 = (n_2 n_1)\cdot 1 = n_2 1 \cdot n_1 1 = r_2 \cdot r_1$$

<u>Lemma 4.7</u>: If R is additively generable then $\mathcal{S}^{-1} = \mathcal{I}$. If R is an additively generable *field*, then $\mathcal{I} = R \setminus \{0\}$.

<u>Proof</u>: Suppose that $r \in \mathcal{S}^{-1}$. Since R is additively generable, this implies that $r^{-1} \in \mathcal{S}^{-1}$ which implies that $r \in \mathcal{I}$. Similarly, suppose $r \in \mathcal{I}$. Then $r^{-1} \in \mathcal{S}^{-1}$, however since R is additively generable this implies that $r \in \mathcal{S}^{-1}$. If R is a field then that simply implies every nonzero element belongs to $\mathcal{S}^{-1}$ which we have just shown implies $\mathcal{I} = R \setminus \{0\}$.

4.3 Results for $\zeta_{\mathbb{Z}_n}$, $2 \leq n \leq 1,000$

In order to get our foot in the door, what we need is some data to study. This allows us to form conjectures which can potentially be easily proven or disproven. Over the winter months I collected data on the zeta function over $\mathbb{Z}_n$ for $2 \leq n \leq 3,000$, resulting in many millions of points of data. From a few initial observations I built conjectures about how the zeta function behaves for specific types of integers, and based off of these cases, built a characterization for any arbitrary n. The rest of the work was based on proving (or disproving) these conjectures, which is the content of the following sections. Before we continue on, we list some of the data used.

	$\zeta_{\mathbb{Z}_3}(s)$	$\zeta_{\mathbb{Z}_{13}}(s)$	$\zeta_{\mathbb{Z}_{27}}(s)$	$\zeta_{\mathbb{Z}_{25}}(s)$	$\zeta_{\mathbb{Z}_{21}}(s)$	$\zeta_{\mathbb{Z}_{30}}(s)$
$s = 1$	0	0	0	0	0	0
$s = 2$	2	0	18	0	0	20
$s = 3$	0	0	0	0	0	0
$s = 4$	2	0	18	20	0	8
$s = 5$	0	0	0	0	0	0
$s = 6$	2	0	18	0	12	20
$s = 7$	0	0	0	0	0	0
$s = 8$	2	0	18	20	0	8
$s = 9$	0	0	0	0	0	0
$s = 10$	2	0	18	0	0	20
$s = 11$	0	0	0	0	0	0
$s = 12$	2	12	18	20	12	8
$s = 13$	0	0	0	0	0	0
$s = 14$	2	0	18	0	0	20
$s = 15$	0	0	0	0	0	0
$s = 16$	2	0	18	20	0	8
$s = 17$	0	0	0	0	0	0
$s = 18$	2	0	18	0	12	20
$s = 19$	0	0	0	0	0	0
$s = 20$	2	0	18	20	0	8
$s = 21$	0	0	0	0	0	0
$s = 22$	2	0	18	0	0	20
$s = 23$	0	0	0	0	0	0
$s = 24$	2	12	18	20	12	8

The above is only a sampling of the data I have collected. The collection seems a bit arbitrary, and there might not be a noticeable pattern to those who do not know what to look for. The key is that the first two columns represent the zeta function over $\mathbb{Z}_p$ where p is a prime greater than 2. The next two columns represent the zeta function over $\mathbb{Z}_{p^k}$ where again p is prime and $k > 1$. The last two represent zeta over $\mathbb{Z}_{p_1 \cdots p_n}$ for a few distinct primes p_i.

4.4 Characterization of $\zeta_{\mathbb{Z}_n}(s)$

If you have taken a look at any of the collected data you might have noticed that it appears as if I stopped computations at arbitrary arguments. There is in fact a very good reason for choosing to stop computations at the numbers I did, and it is because of one of the most important traits about the zeta function over the modular integers.

First, we must give a definition. The *Euler phi function*, $\varphi(n)$, counts the number of coprime positive integers less than a positive integer n [7, 9, 10]. Explicitly, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the unique prime factorization of n then we have that

$$\varphi(n) = (p_1 - 1)p_1^{k_1-1}(p_2 - 1)p_2^{k_2-1} \cdots (p_r - 1)p_r^{k_r-1}$$

Alongside this function, Euler developed a theorem

Euler's Theorem: If $a \in \mathbb{Z}_n$ has a multiplicative inverse then

$$a^{\varphi(n)} = 1$$

We will not bother with the proof, it is very much the same as Fermat's Little theorem [10]. Also worth noting is that this is not the original statement of the theorem, but a perfectly equivalent interpretation.

Lemma 4.8: $\zeta_{\mathbb{Z}_n}(s)$ is periodic with period $\varphi(n)$.

Proof: Consider $\zeta_{\mathbb{Z}_n}(\varphi(n) + s)$. We have that

$$\zeta_{\mathbb{Z}_n}(\varphi(n) + s) = \sum_{a \in (\mathbb{Z}_n)^\times} a^{\varphi(n)+s} = \sum_{a \in (\mathbb{Z}_n)^\times} a^{\varphi(n)} a^s = \sum_{a \in (\mathbb{Z}_n)^\times} a^s = \zeta_{\mathbb{Z}_n}(s)$$

This ends up being an immensely useful lemma especially when it comes to computation time as it implies that there can be *at most* $\varphi(n)$ distinct values for the zeta function.. The same methods allow us to see one more useful fact.

Lemma 4.9: $\zeta_{\mathbb{Z}_n}(\varphi(n)) = \varphi(n)$.

Proof: We have that

$$\zeta_{\mathbb{Z}_n}(\varphi(n)) = \sum_{n \in (\mathbb{Z}_n)^\times} a^{\varphi(n)} \equiv \sum_{n \in (\mathbb{Z}_n)^\times} 1$$

However, by definition we have that $|(\mathbb{Z}_n)^\times| = \varphi(n)$, hence

$$\zeta_{\mathbb{Z}_n}(\varphi(n)) = \varphi(n)$$

4.4.1 Characterization of $\zeta_{\mathbb{Z}_p}(s)$

We turn our attention to a special case of $\mathbb{Z}_n$. When n is prime, call it p, then $\mathbb{Z}_p$ is a finite field, that is it is a finite, commutative ring in which all nonzero elements have multiplicative inverses. Intuitively, this should seem like a "nicer" case to work with: there are no "gaps" in our sum, we simply raise every nonzero element of $\mathbb{Z}_p$ to some power and sum them. Further, there are considerably stronger results for finite fields than there are for simple rings, many we make use of.

As a remarkable curiosity, the behavior of the zeta function over $\mathbb{Z}_n$ appears to behave very much so on the prime factors of n. In that sense, it is not an unreasonable guess to think that we can understand these more complicated cases by studying the "nicer" ones.

Lemma 4.10: $\zeta_{\mathbb{Z}_2}(s) = 1$ for all s.

Proof: Since $\mathbb{Z}_2$ is clearly an additively generable finite field, by lemma 4.7 we have that $\mathcal{I} = \mathbb{Z}_2 \setminus \{0\} = \{1\}$, hence

$$\zeta_{\mathbb{Z}_2}(s) = 1^s = 1$$

Lemma 4.11: $\zeta_{\mathbb{Z}_p}(1) = 0$ for all primes $p > 2$.

Proof: In this case, as an integer sum we have that

$$\sum_{n=1}^{p-1} n = \frac{p(p-1)}{2}$$

Taking both sides modulo p then yields

$$\zeta_{\mathbb{Z}_p}(1) = 0$$

as the integer sum on the left modulo p is exactly the zeta function over $\mathbb{Z}_p$, a trick we use often in the coming sections.

Lemma 4.12: $\zeta_{\mathbb{Z}_p}(p-1) = p-1$ for all primes $p > 2$.

Proof: We have that $\varphi(p) = p-1$, hence by lemma 4.9 it follows immediately that

$$\zeta_{\mathbb{Z}_2}(p-1) = \varphi(p) = p-1$$

Lemma 4.13: Given any $k \in (\mathbb{Z}_p)^\times$, $k(\mathbb{Z}_p)^\times$ is a permutation of the group of units, that is $k(\mathbb{Z}_p)^\times = (\mathbb{Z}_p)^\times$.

Proof: We can actually prove a more general statement from which this follows. If R is a ring and $r \in (R)^\times$ then

$$r(R)^\times = (R)^\times$$

If we can prove this, the lemma follows immediately. In that case, pick $r \in (R)^\times$ and define the function $f_r : (R)^\times \to (R)^\times$ by

$$f_r(u) = ru$$

For every $r \in (R)^\times$ we have that $f_r((R)^\times) \subseteq (R)^\times$. Our goal is to show that f_r is injective for every r; if we show that f_r is injective, this implies that $|f_r((R)^\times)| = |(R)^\times|$, hence $f_r((R)^\times) = (R)^\times$ and clearly $r(R)^\times = f_r((R)^\times)$.

Pick $u, w \in (R)^\times$ such that $u \neq w$. We wish to show that $f_r(u) \neq f_r(w)$. Suppose that $f_r(u) = f_r(w)$. Then we have that

$$ru = rw$$

Because $r \in (R)^\times$, we can multiply both sides by r^{-1} to get

$$u = w$$

a contradiction. Hence $f_r(u) \neq f_r(w)$ if $u \neq w$, and so f_r is injective. Because our choice of r was arbitrary, this concludes the proof.

Lemma 4.14: For each $k = 2, 3, \ldots, p-2$, there is some $a \in (\mathbb{Z}_p)^\times \setminus \{1\}$ such that $a^k = a$.

We don't give a full proof here as it follows from the primitive root theorem [7, 9, 10].

Theorem 4.2: For all primes $p > 2$ we have that

$$\zeta_{\mathbb{Z}_p}(s) = \begin{cases} p-1 & : s \equiv 0 \pmod{p-1} \\ 0 & : \text{else} \end{cases}$$

Proof: Lemmas 4.8, 4.11, and 4.12 immediately take care of the cases when $s \equiv 1, p-1 \pmod{p}$, so by lemma 4.8 we need only worry about the cases when $1 < s < p-1$. Fix such an s. We have that

$$\zeta_{\mathbb{Z}_p}(s) = \sum_{n \in (\mathbb{Z}_p)^\times} n^s$$

by lemma 4.13, there is then some $a \neq 1, 0$ such that $a^s = a$. Multiply through the sum by a, which then gives that

$$a\zeta_{\mathbb{Z}_p}(s) = \sum_{n \in (\mathbb{Z}_p)^\times} an^s = \sum_{n \in (\mathbb{Z}_p)^\times} (an)^s$$

However, by lemma 4.12 this is just a permutation. Since $\mathbb{Z}_p$ is an abelian group, this implies that

$$\sum_{n = \in (\mathbb{Z}_p)^\times} (an)^s = \sum_{n \in (\mathbb{Z}_p)^\times} n^s$$

or equivalently that

$$a\zeta_{\mathbb{Z}_p}(s) = \zeta_{\mathbb{Z}_p}(s)$$

By assumption, $a \neq 1, 0$ hence the only possible way this holds is if

$$\zeta_{\mathbb{Z}_p}(s) = 0$$

.

4.4.2 Characterizaion of $\zeta_{\mathbb{Z}_{p^k}}(s)$

We now turn our attention to the case when n is a prime power, i.e. $n = p^k$ for some prime p. The reasoning behind this is not immediately apparent, however we will soon find that, similar to the case when $n = p$ for p prime, this ends up being a "nice" case. Also similar to the case when $n = p$ for p prime, the general behavior for *any* n we will show is dependent on the behavior over these prime powers.

Unfortunately, the proofs of these cases are not quite as "clean" as the case when n is prime. We need a little bit more machinery before we proceed.

Lemma 4.15: Given p an odd prime, the group of units $(\mathbb{Z}_{p^k})^{\times}$ is cyclic, i.e. there is some $a \in (\mathbb{Z}_{p^k})^{\times}$ such that

$$(\mathbb{Z}_{p^k})^{\times} = \langle a, \cdot \rangle$$

Similarly, this element has a very special form: we have that

$$a = b(p+1)$$

where obviously both $b, p+1 \in (\mathbb{Z}_{p^k})^{\times}$ and $ord_{\times}(b) = (p-1)$ and $ord_{\times}(p+1) = p^{k-1}$.

On the other hand, if $p = 2$ and $k \geq 3$, the group of units $(\mathbb{Z}_2^k)^{\times}$ *is not* cyclic, however it can be generated by any linear combination of the elements $-1, 5$, i.e.

$$(\mathbb{Z}_{2^k})^{\times} = \langle -1, 5, \cdot \rangle$$

The proof of this lemma is included in [10]. We make frequent use of all of the above facts.

Lemma 4.16: Let $p \neq 2$ be prime, and let a be the generator for $(\mathbb{Z}_{p^k})^\times$ specified by lemma 4.15. Then

$$a^s - 1$$

is a divisor of zero if and only if $s \equiv 0 \pmod{p-1}$.

Proof: By definition, the only divisors of zero in $\mathbb{Z}_{p^k}$ are the elements whose equivalence class representatives as integers share a common divisor with p^k, i.e. they are a multiple of p. This implies that $a^s - 1$ is a zero divisor if and only if

$$a^s - 1 \equiv 0 \pmod{p}$$

or equivalently

$$a^s \equiv 1 \pmod{p}$$

However, we have that

$$a^s = b^s(p+1)^s$$

so that $a^s - 1$ is a divisor of zero if and only if

$$b^s(p+1)^s \equiv 1 \pmod{p}$$

However, clearly we have that

$$b^s(p+1)^s \equiv b^s \pmod{p}$$

But we also have

$$b^s \equiv 1 \pmod{p}$$

if and only if $s \equiv 0 \pmod{p-1}$. One direction is clear, the other needs a bit of explanation. If $s \equiv 0 \pmod{p-1}$ then by the order condition on b we have that $b^s \equiv 1 \pmod{p^k}$ which implies the congruence modulo p. The other direction is less clear. The way the element b is chosen in lemma 4.15 is such that it also has order $p-1$ in $\mathbb{Z}_p$ via the primitive root theorem [10], and this concludes the proof of this lemma.

Lemma 4.17: Let $p \neq 2$ be prime, let a be the generator for $(\mathbb{Z}_{p^k})^\times$ as specified by lemma 4.15. Then

$$(a^s - 1)\zeta_{\mathbb{Z}_{p^k}}(s) = 0$$

for all $s \in \mathbb{N}$.

Before we prove this lemma, note that this is the condition we reached in the n prime case. However, now we see via lemma 4.16 that this does not always ensure that $\zeta = 0$.

Proof: Consider $a, s, \varphi(p^k)$ all as *integers* (really the only one that could cause confusion is a). Now, *as an integer sum*, we have the relation

$$(a^s)^{\varphi(p^k)+1} - 1 = (a^s - 1) \sum_{j=0}^{\varphi(p^k)} (a^s)^j = (a^s - 1) \left(\sum_{j=1}^{\varphi(p^k)} (a^j)^s + 1 \right)$$

Doing a little algebra then gives

$$(a^{\varphi(p^k)})^s a^s - a^s = (a^s - 1) \sum_{j=1}^{\varphi(p^k)} (a^j)^s$$

There's nothing saying we can't consider this equality modulo p^k, so taking the left side yields

$$(a^{\varphi(p^k)})^s a^s - a^s \equiv 1^s a^s - a^s \equiv 0 \pmod{p^k}$$

and the right side does not appear to give anything yet. However, note that

$$\zeta_{\mathbb{Z}_{p^k}}(s) = \sum_{u \in (\mathbb{Z}_{p^k})^\times} u^s$$

But we know that a generates $(\mathbb{Z}_{p^k})^\times$, i.e. that a^j is a distinct unit of $\mathbb{Z}_{p^k}$ for $j = 1, 2, \ldots, \varphi(p^k)$. But then, since there are exactly $\varphi(p^k)$ units in $\mathbb{Z}_{p^k}$ and we sum each of them exactly once in the zeta function, we get that

$$\zeta_{\mathbb{Z}_{p^k}}(s) = \sum_{u \in (\mathbb{Z}_{p^k})^\times} u^s = \sum_{j=1}^{\varphi(p^k)} (a^j)^s$$

where it is understood that the rightmost sum is *as elements of the ring* $\mathbb{Z}_{p^k}$. However, taking the integer sum

$$\sum_{j=1}^{\varphi(p^k)} (a^j)^s$$

modulo p^k is the same as considering the sum as elements of the ring, hence we get that

$$(a^s - 1)\zeta_{\mathbb{Z}_{p^k}}(s) = 0$$

since congruence modulo p^k is the same as equivalence in the ring $\mathbb{Z}_{p^k}$.

We need to construct some sets and do a little manipulation before we can prove the major theorem of this section.

Lemma 4.18: Let $\alpha = (p+1)$ and $\beta = lp^r(p-1)$ where $p \not| l$, and r is zero or a positive integer strictly less than $k-1$. Define the set

$$\mathcal{A} = \{\alpha^{j\beta} : j \in \mathbb{N}\} \subseteq (\mathbb{Z}_{p^k})^\times$$

Then $\mathcal{A}$ has exactly p^{k-r-1} distinct elements which correspond to the elements $\alpha^{j\beta}$ for $j = 1, 2, \ldots, p^{k-r-1}$.

Proof: Let $k = j + p^{k-r-1}$. We wish to show that

$$\alpha^{k\beta} = \alpha^{j\beta}$$

This then implies that there can be *at most* p^{k-r-1} distinct elements in $\mathcal{A}$, those being the elements which correspond to $j = 1, 2, \ldots, p^{k-r-1}$.

We have that

$$\alpha^{k\beta} = \alpha^{(j+p^{k-r-1})\beta} = \alpha^{j\beta}\alpha^{p^{k-r-1}\beta}$$

However, we have that

$$\alpha^{p^{k-r-1}\beta} = (p+1)^{lp^{k-1}(p-1)} = \left((p+1)^{p^{k-1}}\right)^{l(p-1)}$$

$$= 1^{l(p-1)} = 1$$

So

$$\alpha^{k\beta} = \alpha^{j\beta}$$

As we mentioned, this implies that there are *at most* p^{k-r-1} distinct elements in $\mathcal{A}$. Our goal now is to show that for $i, j = 1, 2, \ldots, p^{k-r-1}$ and $i \neq j$ that

$$\alpha^{i\beta} \neq \alpha^{j\beta}$$

Assume without loss of generality that $1 \leq i < j \leq p^{k-r-1}$. We have that

$$\alpha^{i\beta} = \alpha^{j\beta}$$

if and only if

$$\alpha^{i\beta}(\alpha^{(j-i)\beta} - 1) = 0$$

i.e.

$$\alpha^{(j-i)\beta} = 1$$

But this is equivalent to saying

$$(p+1)^{l(j-i)p^r(p-1)} = 1$$

By the order condition imposed on the element $p+1$ in lemma 4.15, we know that this is true if and only if $p^{k-r-1} | l(j-i)(p-1)$. Clearly, we have that $p \not| l$ by assumption and $p \not| (p-1)$ since $p-1 < p$. This then implies that $p^{k-r-1} | (j-i)$. However, we have that $0 < j-i < p^{k-r-1}$, hence $p^{k-r-1} \not| (j-i)$. This in turn proves that if $i, j = 1, 2, \ldots, p^{k-r-1}$ with $i \neq j$ then

$$\alpha^{i\beta} \neq \alpha^{j\beta}$$

And this proves the lemma.

A few quick remarks. First, note that $|\mathcal{A}| = p^{k-r-1}$ by construction. Also note that $|\mathcal{A}| | \varphi(p^k)$, that is

$\varphi(p^k) = (p-1)p^r|\mathcal{A}|$. We will use these facts later on. Before we do so, we must construct another set.

<u>Lemma 4.19</u>: Let r be zero or a positive integer strictly less than $k-1$. Define the set

$$\mathcal{B} = \{(p^{r+1}j + 1) : j \in \mathbb{N}\} \subseteq (\mathbb{Z}_{p^k})^\times$$

Then $\mathcal{B}$ has exactly p^{k-r-1} distinct elements which correspond to the elements $(p^{r+1}j+1)$ when $j = 1, 2, \ldots, p^{k-r-1}$.

<u>Proof</u>: We use the same methodology as in lemma 4.18. Let $k = j + p^{k-r-1}$. We then want to show that

$$(p^{r+1}k + 1) = (p^{r+1}j + 1)$$

We have that

$$(p^{r+1}k + 1) = (p^{r+1}(j + p^{k-r-1}) + 1) = (p^k + p^{r+1}j + 1)$$

$$= (p^{r+1}j + 1)$$

as $p^k = 0$ in $\mathbb{Z}_{p^k}$. This again implies there are *at most* p^{k-r-1} distinct elements in $\mathcal{B}$. Now assume that $1 \leq i < j \leq p^{k-r-1}$. We want to show that

$$(p^{r+1}j + 1) \neq (p^{r+1}k + 1)$$

Assume otherwise. Then we get that

$$p^{r+1}(j - i) = 0$$

But this is true only if $p^{k-r-1}|(j-i)$, which by construction is clearly false. Hence this shows that $\mathcal{B}$ has exactly p^{k-r-1} distinct elements which correspond to the elements $(p^{r+1}j+1)$ when $j = 1, 2, \ldots, p^{k-r-1}$.

We have then built two seemingly unrelated sets which are both subsets of the group of units, and both have the same number of elements. It is then natural to try and compare them.

Lemma 4.20: If $\mathcal{A}$ is the set defined in lemma 4.18 and $\mathcal{B}$ is the set defined in lemma 4.19 then

$$\mathcal{A} = \mathcal{B}$$

Proof: The idea of the proof is straightforward. Note that we have already shown that $|\mathcal{A}| = |\mathcal{B}|$. To prove the lemma, it is then sufficient to show that if $a \in \mathcal{A}$, then $a \in \mathcal{B}$. To do so, we try and characterize the elements of $\mathcal{B}$ in a "nicer" way. We have that

$$(p^{r+1}j + 1)$$

is an element of $\mathcal{B}$. Note, that if you consider the above *as an integer*, then we have that

$$(p^{r+1}j + 1) \equiv 1 \pmod{p^{r+1}}$$

But it's also clear that if we have some $b \in \mathbb{Z}_{p^k}$ such that, as an integer,

$$b \equiv 1 \pmod{p^{r+1}}$$

then *as an integer*,

$$b = jp^{r+1} + 1$$

and since b corresponds to an element in $\mathbb{Z}_{p^k}$, this implies that $j = 1, 2, \ldots, p^{k-r-1}$, and so taking the above modulo p^k shows that

$$b \in \mathcal{B} \Leftrightarrow b \equiv 1 \pmod{p^{r+1}}$$

Our goal then is to show that for each j,

$$\alpha^{j\beta} \equiv 1 \pmod{p^{r+1}}$$

We have that

$$\alpha^{j\beta} = (p+1)^{jlp^r(p-1)} = \left((p+1)^{p^r}\right)^{jl(p-1)}$$

Let's consider this *as an integer* so that we may employ the binomial expansion theorem. As an integer, we get that

$$\left((p+1)^{p^r}\right)^{jl(p-1)} = \left(p^{p^r} + \sum_{j=1}^{p^r-1} \binom{p^r}{j} p^j + 1\right)^{jl(p-1)}$$

We make two quick notes. First, for every term in the sum, we have that $p^r | \binom{p^r}{j}$ [5], so that we have that p^{r+1} divides every term of the sum. We also note that for all odd primes, $p^r \geq r+1$ so that p^{r+1} divides p^{p^r}. But these two facts imply that, taking both sides of the above modulo p^{r+1},

$$\alpha^{j\beta} \equiv (1)^{jl(p-1)} \equiv 1 \pmod{p^{r+1}}$$

Therefore, this implies that for each j, $\alpha^{j\beta} \in \mathcal{B}$. This in turn implies that $\mathcal{A} \subseteq \mathcal{B}$, and since $|\mathcal{A}| = |\mathcal{B}|$, this proves the lemma.

We now have enough machinery to develop the following theorem.

<u>**Theorem 4.3**</u>: Let $p \neq 2$ be prime. The for all $k \in \mathbb{N}$ we have that

$$\zeta_{\mathbb{Z}_{p^k}}(s) = \begin{cases} (p-1)p^{k-1} & : s \equiv 0 \pmod{p-1} \\ 0 & : \text{else} \end{cases}$$

<u>Proof</u>: First note that theorem 4.2 proves the case when $k = 1$. Next, suppose that $s \not\equiv 0 \pmod{p-1}$. Then lemma 4.16 implies that $a^s - 1$ is a unit. Lemma 4.17 tells us that

$$(a^s - 1)\zeta_{\mathbb{Z}_{p^k}}(s) = 0$$

Combining these facts allows us to cancel the $a^s - 1$ factor and get that if $s \not\equiv 0 \pmod{p-1}$ then

$$\zeta_{\mathbb{Z}_{p^k}}(s) = 0$$

That was the easy section of the proof. The next piece requires a little bit of manipulation. Suppose then that $s \equiv 0 \pmod{p-1}$, that is $s = m(p-1)$ for some natural m. By the periodicity of the zeta function over $\mathbb{Z}_n$, we know that we need only consider $m \leq p^{k-1}$ and when $m = p^{k-1}$ we know that $\zeta_{\mathbb{Z}_{p^k}}(s) = \varphi(p^k)$. Hence, we consider only $m < p^{k-1}$. Let r be the greatest power of p such that $p^r | m$. Note that clearly r is at least zero and is strictly less than $k-1$. We may then write $m = lp^r$ where $p \not| l$. But then, let us consider what our zeta function looks like. From the proof of lemma 4.17, we have that

$$\zeta_{\mathbb{Z}_{p^k}}(s) = \sum_{j=1}^{\varphi(p^k)} (a^j)^s = \sum_{j=1}^{\varphi(p^k)} (a^s)^j$$

$$\sum_{j=1}^{\varphi(p^k)} (a^{lp^r(p-1)})^s$$

$$= \sum_{j=1}^{\varphi(p^k)} (p+1)^{ljp^r(p-1)}$$

By the order condition on b established in lemma 4.15. However, we've shown in lemma 4.18 that this can be rewritten as

$$= \sum_{j=1}^{\varphi(p^k)} \alpha^{j\beta}$$

We also established right after that lemma that

$$\varphi(p^k) = (p-1)p^r|\mathcal{A}|$$

so that the above is equivalent to

$$= (p-1)p^r \sum_{j=1}^{|\mathcal{A}|} \alpha^{j\beta}$$

By lemma 4.20, we've shown that this is equivalent to

$$= (p-1)p^r \sum_{j=1}^{|\mathcal{B}|}(p^{r+1}j+1) = ((p-1)p^r)\left(p^{r+1}\sum_{j=1}^{|\mathcal{B}|} j + |\mathcal{B}|\right)$$

Using the fact that $|\mathcal{B}| = p^{k-r-1}$ we get

$$= (p-1)p^{2r+1}\sum_{j=1}^{|\mathcal{B}|} j + (p-1)p^{k-1}$$

We use our favorite trick of considering the above as an integer one last time. As an integer sum, we have that

$$\sum_{j=1}^{|\mathcal{B}|} j = p^{k-r-1}\frac{p^{k-r-1}+1}{2}$$

so that as an integer, we get the above is

$$= (p-1)p^{k+r}\frac{p^{k-r-1}+1}{2} + (p-1)p^{k-1}$$

Because p is an odd prime, the division by two is defined above. But then the left term in the sum is divisible by p^k since $r \geq 0$, so taking the above modulo p^k yields that

$$\zeta_{\mathbb{Z}_{p^k}}(s) = (p-1)p^{k-1}$$

and this concludes the proof of the theorem.

We are not yet done. We still need to consider the case when $p = 2$. Though we no longer have the cyclic condition, the proof follows a similar format. We have already proven the case of $k = 1$ when $p = 2$. We do the $k = 2$ case by hand and the prove the rest in full generality.

Lemma 4.21: We have that

$$\mathbb{Z}_{2^2}(s) = \begin{cases} 2 & : s \text{ even} \\ 0 & : s \text{ odd} \end{cases}$$

Proof: Note that we have $\langle 1, + \rangle = \mathbb{Z}_{2^2}$, so that

$$\zeta_{\mathbb{Z}_{2^2}}(s) = 1^s + 3^s$$

Also note that if s is even then $1^s = 3^s = 1$ which in turn implies that if s is odd $1^s = 1, 3^s = 3$. Then

$$\mathbb{Z}_{2^2}(s) = \begin{cases} 1+1=2 & : s \text{ even} \\ 1+3=0 & : s \text{ odd} \end{cases}$$

and we are done.

Now we talk about how we generate the group of units of $\mathbb{Z}_{2^k}$ for $k \geq 3$. We said that this group of units is generated by -1 and 5 which means if $u \in (\mathbb{Z}_{2^k})^\times$ then

$$u = (-1)^i(5)^j$$

for some $i = 1, 2$ and some $j = 1, 2, \ldots, 2^{k-2}$ (also note that this implies that the order of 5 in $\mathbb{Z}_{2^k}$ is 2^{k-2} [10]). This then implies that our zeta function is given as follows:

$$\zeta_{\mathbb{Z}_{2^k}}(s) = \sum_{i=1}^{2} \left(\sum_{j=1}^{2^{k-2}} (-1)^{is}(5)^{js} \right)$$

This looks quite nasty, but we can drastically simplify it in a moment. First, we need a new tool.

Lemma 4.22: Let $n > 2$. Then

$$\zeta_{\mathbb{Z}_n}(s) = 0$$

if s is odd.

Proof: This is actually quite a strong statement that ends up being very easy to prove. We do it in three steps. First, we show that if u is a unit, then $-u$ is a unit. Then we show that $u \neq -u$. Lastly, we show that $(-u)^s = -u^s$ and this implies the lemma.

Consider $\mathbb{Z}_n$ for any $n > 2$. By definition, $-1 = n - 1$ in this ring. However, for all $n > 2$ we have that $n - 1$ and n are coprime. This implies that -1 is a unit. Clearly the product of two units is itself a unit (hence why we can refer to *the group* of units), therefore if u is a unit, then $(-1)u = -u$ is a unit.

Next, we show that $u \neq -u$. By definition, if $u \in \mathbb{Z}_n$ then $-u = n - u$. But $n - u = u$ only if $2u = n$. But this implies that u and n would not be coprime, hence u is not a unit. Therefore, if u is a unit in $\mathbb{Z}_n$ for $n > 2$ then $u \neq -u$.

Finally, we have that if s is odd, then $(-u)^s = (-1)^s u^s = (-1)u^s = -u^s$. But this implies that, since $\varphi(n)$ is even for all $n > 2$, we can rewrite the zeta function as

$$\zeta_{\mathbb{Z}_n}(s) = \sum_{j=1}^{\frac{\varphi(n)}{2}} u_i^s - u_i^s$$

where we enumerate the units from 1 to $\frac{\varphi(n)}{2}$ (as the additive inverse make up the other half). But then clearly this implies

$$\zeta_{\mathbb{Z}_n}(s) = 0$$

Lemma 4.22 ends up being very useful in considering the $p = 2$ for $k \geq 3$ case as it implies we need only consider even powers of s, which as we will see helps to simplify things.

We now repeat many of the same arguments we made for the $p \neq 2$ case with minor modifications.

Lemma 4.23: Let r be a positive integer strictly less than $k-2$, and suppose that $2 \not| l$. Define the set

$$\mathcal{A}_2 = \{5^{jl2^r} : j \in \mathbb{N}\}$$

Then $\mathcal{A}_2$ has exactly 2^{k-r-2} distinct elements which correspond to the elements when $j = 1, 2, \ldots, 2^{k-r-2}$.

Proof: Let $k = j + 2^{k-r-2}$. Then

$$5^{lk2^r} = 5^{lj2^r}5^{l2^{k-2}} = 5^{lj2^r}\left(5^{2^{k-2}}\right)^l$$

$$= 5^{lj2^r}(1)^l = 5^{lj2^r}$$

This implies that there are *at most* 2^{k-r-2} distinct elements of $\mathcal{A}_2$. Suppose $1 \leq i < j \leq 2^{k-r-2}$. Then

$$5^{lj2^r} = 5^{li2^r}$$

if and only if

$$5^{l(j-i)2^r} = 1$$

which is true if and only if $2^{k-r-2}|l(j-i)$, which by construction it clearly does not. This then proves the lemma.

Much like in the $p \neq 2$ we want to try and linearize this set in terms of j.

Lemma 4.23: Let r be as in lemma 4.22 and define the set

$$\mathcal{B}_2 = \{(2^{r+2}j + 1) : j \in \mathbb{N}\}$$

Then $\mathcal{B}_2$ has exactly 2^{k-r-2} distinct elements which correspond to the elements when $j = 1, 2, \ldots, 2^{k-r-2}$.

Proof: Again, let $k = j + 2^{k-r-2}$. Then

$$(2^{r+2}k+1) = (2^{r+2}(j+2^{k-r-2})+1) = (2^{r+2}j+2^k+1) = (2^{r+2}j+1)$$

Hence $\mathcal{B}_{\in}$ has at most 2^{k-r-2} distinct elements. Suppose $1 \leq i < j \leq 2^{k-r-2}$. Then

$$(2^{r+2}j+1) = (2^{r+2}i+1)$$

if and only if

$$2^{r+2}(j-i) = 1$$

which is true if and only if $2^{k-r-2}|(j-i)$, which is never possible. This proves the lemma.

We again have two subsets of the group of units with the same number of elements. Our goal is again to compare them.

Lemma 4.24: Given $\mathcal{A}_2$ as in lemma 4.22 and $\mathcal{B}_2$ as in lemma 4.23, then

$$\mathcal{A}_2 = \mathcal{B}_2$$

.

Proof: We use the same trick as before, showing that if $a \in \mathcal{A}_2$ then $a \in \mathcal{B}$. By the same logic as in lemma 4.20 it's clear that

$$b \in \mathcal{B}_2 \Leftrightarrow b \equiv 1 \pmod{2^{r+2}}$$

Pick any $5^{jl2^r} \in \mathcal{A}_2$. Note that

$$5^{jl2^r} = (2^2+1)^{jl2^r}$$

We then consider this as an integer and use the binomial expansion theorem to get that

$$(2^2+1)^{jl2^r} = \left(2^{2^{r+1}} + \sum_{k=1}^{2^r-1} \binom{2^r}{k} 2^{2k} + 1\right)^{jl}$$

Then we have that $2^r | \binom{2r}{j}$ for every term in the sum [5] hence 2^{r+2} divides every term in the sum. Similarly, for all $r > 1$ we have that $2^{r+1} \geq r+1$ so that $2^{r+2} | 2^{2^{r+1}}$. Taking everything above modulo 2^{r+2} then yields that

$$5^{jl2^r} \equiv 1^{jl} \equiv 1 \pmod{2^{r+2}}$$

hence if $a \in \mathcal{A}_2$, then $a \in \mathcal{B}_2$ which implies $\mathcal{A}_2 \subseteq \mathcal{B}_2$. Since $|\mathcal{A}_2| = |\mathcal{B}_2|$, this completes the proof of the lemma.

We now have enough to build a full characterization for the $p = 2$ case.

<u>Theorem 4.4</u>: Given $p = 2$ and $k \geq 2$ we have that

$$\zeta_{\mathbb{Z}_{2^k}}(s) = \begin{cases} 2^{k-1} & : s \text{ even} \\ 0 & : s \text{ odd} \end{cases}$$

<u>Proof</u>: Note that the case when $k = 1$ breaks this characterization unlike when $p \neq 2$. The case when $k = 2$ is prove by lemma 4.21. The zeros are proven by lemma 4.22. All we have to do is consider what happens when s is even. Note that we have shown

$$\zeta_{\mathbb{Z}_{2^k}}(s) = \sum_{i=1}^{2} \left(\sum_{j=1}^{2^{k-2}} (-1)^{is}(5)^{js} \right)$$

However, if s is even then the -1 term is simply 1, hence

$$\zeta_{\mathbb{Z}_{2^k}}(s) = 2 \sum_{j=1}^{2^{k-2}} (5)^{js}$$

Also note that if s is even we have that $s = l2^r$ where $2 \not| l$ and by the periodicity of the zeta function we only need to consider r which are positive integers strictly less than $k-1$. When $r = k-1$ then we get that $\zeta_{\mathbb{Z}_{2^k}}(s) = 2^{k-1}$. Then we may rewrite the zeta function as

$$\zeta_{\mathbb{Z}_{2^k}}(s) = 2\sum_{j=1}^{2^{k-2}} (5)^{jl2^r}$$

But then we are simply summing elements of $\mathcal{A}_2$. We know that $|\mathcal{A}_2| = 2^{k-r-2}$ which clearly divides 2^{k-2} as $r \geq 1$. But then we may rewrite again to get

$$= 2^{r+1}\sum_{j=1}^{|\mathcal{A}_2|} 5^{jl2^r}$$

And by lemma 4.24 we have that this is equal to

$$2^{r+1}\sum_{j=1}^{|\mathcal{B}_2|}(2^{r+2}j+1) = 2^{r+3}\sum_{j=1}^{|\mathcal{B}_2|} j + 2^{k-1}$$

We lastly consider the above as an integer. We get that

$$\sum_{j=1}^{|\mathcal{B}_2|} j = 2^{k-r-3}(2^{k-r-2}+1)$$

so the above as an integer is

$$= 2^k(2^{k-r-2}+1) + 2^{k-1}$$

Taking this modulo 2^k and using the fact that $2^k \equiv 0 \pmod{2^k}$ yields that

$$\zeta_{\mathbb{Z}_{2^k}}(s) = 2^{k-1}$$

if s is odd.

We have then finally built a full characterization for $\mathbb{Z}_{p^k}$. As a recap, we have that if $p \neq 2$ then

$$\zeta_{\mathbb{Z}_{p^k}}(s) = \begin{cases} (p-1)p^{k-1} & : s \equiv 0 \pmod{p-1} \\ 0 & : \text{else} \end{cases}$$

and if $p = 2$ then

$$\zeta_{\mathbb{Z}_{2^k}}(s) = \begin{cases} 1 & : k = 1 \\ 2^{k-1} & : k > 1 \text{ and } s \text{ even} \\ 0 & : k > 1 \text{ and } s \text{ odd} \end{cases}$$

As we will see in the next section, this information is all we need to build a characterization of $\zeta_{\mathbb{Z}_n}$ *for all* $n \geq 2$.

4.4.3 Full Characterization

The question of how the zeta function over $\mathbb{Z}_n$ behaves is at it's core an algebraic one. We need to understand the ring structure of $\mathbb{Z}_n$ in order to understand the behavior over it. We have the following lemma.

Lemma 4.25: Given any positive integer $n \geq 2$ with prime factorization

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

Then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{k_r}}$$

via the isomorphism ψ which takes an equivalence class m, and maps the integer which corresponds to m to $(m, m, \ldots, m)$ in the direct sum. This is a well known fact but we include the proof anyways [7, 9].

Proof: We have that

$$\psi(m + l) = (m + l, m + l, \ldots, m + l)$$

$$= (m, m, \ldots, m) + (l, l, \ldots, l) = \psi(m) + \psi(l)$$

and

$$\psi(ml) = (ml, ml, \ldots, ml)$$

$$= (m, m, \ldots, m)(l, l, \ldots, l) = \psi(m)\psi(l)$$

So that this is clearly an isomorphism. We also have that the order of both rings is clearly equal (and equal to n). The lemma immediately follows if we can show that ψ is injective. Suppose $m \neq l$ and consider

$\psi(m), \psi(l)$. We have that $\psi(m) = \psi(l)$ if and only if

$$(m-l, m-l, \ldots, m-l) = (0, 0, \ldots, 0)$$

But this then implies that for each $i = 1, 2, \ldots, r$, $p_i^{k_i} | (m-l)$. But because each $p_i^{k_i}$ is coprime to $p_j^{k_j}$ if $j \neq i$, this implies that $n|(m-l)$, which can clearly never happen as $|m-l| < n$. This shows that ψ is injective, and hence proves the lemma.

The isomorphism specified in lemma 4.25 ends up being the key to unlocking the behavior of the zeta function over $\mathbb{Z}_n$ for arbitrary $n \geq 2$.

<u>**Theorem 4.5**</u>: Let n have prime factorization as in lemma 4.25. We then have that

$$\zeta_{\mathbb{Z}_n}(s) = \psi^{-1} \begin{pmatrix} \varphi\left(\frac{n}{p_1^{k_1}}\right) \zeta_{\mathbb{Z}_{p_1^{k_1}}}(s) \\ \varphi\left(\frac{n}{p_2^{k_2}}\right) \zeta_{\mathbb{Z}_{p_2^{k_2}}}(s) \\ \vdots \\ \varphi\left(\frac{n}{p_r^{k_2}}\right) \zeta_{\mathbb{Z}_{p_r^{k_r}}}(s) \end{pmatrix}$$

The column on the right is an element of the direct sum specified in lemma 4.25; we switch from row to column notation to save space.

<u>Proof</u>: We need two quick facts to prove this. First, if a, b are coprime positive integers then $\varphi(a)\varphi(b) = \varphi(ab)$ [7]. Second, $(u_1, u_2, \ldots, u_r)$ is a unit in the direct sum specified in lemma 4.25 if and only if u_i is a unit in $\mathbb{Z}_{p_i^{k_i}}$. This follows immediately from the definition of being a unit [7, 9].

Consider $\psi(\zeta_{\mathbb{Z}_n}(s))$. We have that

$$\psi(\zeta_{\mathbb{Z}_n}(s)) = \psi\left(\sum_{u \in (\mathbb{Z}_n)^\times} u^s\right) = \sum_{u \in (\mathbb{Z}_n)^\times} \psi(u)^s$$

$$= \begin{pmatrix} \sum_{\oplus^\times} w_{1,j_1} \\ \sum_{\oplus^\times} w_{2,j_2} \\ \vdots \\ \sum_{\oplus^\times} w_{r,j_r} \end{pmatrix}$$

Let me explain the notation on the right. The sums are understood to be taken over *all of the units* in the direct sum. Then w_{i,j_i} represents the units of $\mathbb{Z}_{p_i^{k_i}}$: the first index, i represents which prime factor you're working with, and the second index $j_i = 1, 2, \ldots, \varphi(p_i^{k_i})$ represents which unit within $\mathbb{Z}_{p_i^{k_i}}$ you're working with.

Fix w_{i,j_i}. With this element, we can choose any of the $\varphi(p_1^{k_1})$ units in the first component, any of the $\varphi(p_2^{k_2})$ units in the second component and so on to construct a unit in the direct sum. But this gives us a total of

$$\varphi(p_1^{k_1}) \cdots \varphi(p_{i-1}^{k_{i-1}}) \varphi(p_{i+1}^{k_{i+1}}) \cdots \varphi(p_r^{k_r})$$

distinct units we can create in the direct sum keeping w_{i,j_i} fixed. Then since $p_i^{k_i}$ is coprime to $p_j^{k_j}$ if $i \neq j$, we have that there are exactly $\varphi\left(\frac{n}{p_i^{k_i}}\right)$ distinct units in the direct sum we can create by holding w_{i,j_i} fixed. However, this can be done *for each* unit in the i^{th} components, hence we really get that the above is equal to

$$= \begin{pmatrix} \varphi\left(\frac{n}{p_1^{k_1}}\right) \sum_{(\mathbb{Z}_{p_1^{k_1}})^\times} w_1 \\ \varphi\left(\frac{n}{p_2}{}^{k_2}\right) \sum_{(\mathbb{Z}_{p_2^{k_2}})^\times} w_2 \\ \vdots \\ \varphi\left(\frac{n}{p_r}{}^{k_r}\right) \sum_{(\mathbb{Z}_{p_r^{k_r}})^\times} w_r \end{pmatrix}$$

which, by definition, is exactly

$$= \begin{pmatrix} \varphi\left(\frac{n}{p_1^{k_1}}\right) \zeta_{\mathbb{Z}_{p_1^{k_1}}}(s) \\ \varphi\left(\frac{n}{p_2^{k_2}}\right) \zeta_{\mathbb{Z}_{p_2^{k_2}}}(s) \\ \vdots \\ \varphi\left(\frac{n}{p_r^{k_2}}\right) \zeta_{\mathbb{Z}_{p_r^{k_r}}}(s) \end{pmatrix}$$

Applying ψ^{-1} to both sides completes the proof.

There are several small additional details you can deduce about the zeta function from this theorem, we briefly discuss one here.

Corollary 4.2: $\zeta_{\mathbb{Z}_n}(s)$ has period at most

$$l.c.m(p_1 - 1, p_2 - 1, \ldots, p_r - 1)$$

if n has prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$.

Proof: Let ρ be the $l.c.m$ specified. Then

$$\zeta_{\mathbb{Z}_n}(s+\rho) = \psi^{-1} \begin{pmatrix} \varphi\left(\frac{n}{p_1^{k_1}}\right) \zeta_{\mathbb{Z}_{p_1^{k_1}}}(s+\rho) \\ \varphi\left(\frac{n}{p_2^{k_2}}\right) \zeta_{\mathbb{Z}_{p_2^{k_2}}}(s+\rho) \\ \vdots \\ \varphi\left(\frac{n}{p_r^{k_2}}\right) \zeta_{\mathbb{Z}_{p_r^{k_r}}}(s+\rho) \end{pmatrix}$$

$$= \psi^{-1} \begin{pmatrix} \varphi\left(\frac{n}{p_1^{k_1}}\right) \zeta_{\mathbb{Z}_{p_1^{k_1}}}(s) \\ \varphi\left(\frac{n}{p_2^{k_2}}\right) \zeta_{\mathbb{Z}_{p_2^{k_2}}}(s) \\ \vdots \\ \varphi\left(\frac{n}{p_r^{k_2}}\right) \zeta_{\mathbb{Z}_{p_r^{k_r}}}(s) \end{pmatrix} = \zeta_{\mathbb{Z}_n}(s)$$

This corollary can really save computation time depending on n. For instance, if $n = 30 = 2 \cdot 3 \cdot 5$ then that implies that $\zeta_{\mathbb{Z}_{30}}(s)$ has period at most $l.c.m(1, 2, 4) = 4$ instead of $\varphi(30) = 8$ as previously established. Similarly, the higher powers of primes we take, the more this corollary eases computation time.

Consider what we've shown. We showed that for any finite ring R, the zeta function over R, $\zeta_R(s)$ is determined by the zeta function over $\mathbb{Z}_n$ for some n. But then we've managed to break down the zeta function over $\mathbb{Z}_n$ into something which is dependent on the zeta functions over the prime factors of n. Additionally, we've shown that the zeta functions over these prime factors are regular and easy to compute, giving us a quick and efficient way of determining the behavior of the zeta function over *all finite rings*. Further, the same machinery we developed to do this tells us that the zeta function over *any ring* R can be computed in the same way if we index it by some invertible, finite order, idempotent element r. In this way, we've actually developed a large and overarching characterization for the zeta function over a ring as a whole.

4.5 Additional Conjectures

Though we have built a fairly large characterization for the behavior of the zeta function over a ring, there are many additional ideas which we could examine. Additionally there are several questions we have yet to ask that may have important consequences to our general theory behind the zeta function. We list and explain a few of them here to indicate further directions of research.

1. Is the behavior of the zeta function over fields special? What about finite field extensions? If $\mathbb{F}$ is a finite field then it is a well known result that $\mathbb{F}$ has order p^k for some prime p and some positive integer k. It is not hard to show that the behavior of zeta over $\mathbb{F}$ is completely determined by the behavior of zeta over $\mathbb{Z}_p$. But does this hold in general? If F is a field, not necessarily finite, and $F \subseteq E$ is a finite extension of F, is the behavior of zeta over E completely determined by the behavior of zeta over F? Further, it is important to note that $\mathbb{R}$ is not a finite extension of $\mathbb{Q}$. However, short of the issue of convergence, these return the same values.

2. What about the convergence of the zeta function. How de we even define convergence? Many of the rings we apply the zeta function to have no natural metric, and so what metric must we develop and apply to ensure the convergence of the zeta function, if such a metric even exists? For instance, $\zeta_{\mathbb{R}}(1)$ does not converge as it is given by the Harmonic series.

3. What about the completeness of the rings we take the zeta function over? In one of our very first examples we showed that $\zeta_{\mathbb{Q}}(2) \notin \mathbb{Q}$. Is there a way to define a topology on our rings such that it guarantees the completeness of these spaces?

4. How should we go about trying to classify infinite rings? It is incredibly more difficult to compute the zeta function over an infinite ring without extensive knowledge of how that ring itself behaves. Developing some isomorphism theorems may be useful here.

5. What happens to the behavior of the zeta function if we alter its construction? Suppose we let r simply be an invertible element of the ring R with finite additive order, but we do not require it to be idempotent. What happens then? What happens if we do not even require it to have finite order? Also note that, in the $\mathbb{Z}_p$ case, we are simply summing s^{th} powers of all non-zero elements of this ring as it is a finite field. What if, only for *finite* fields, we change the definition of the zeta function to exactly that, i.e. it takes s^{th} powers of all non-zero elements of the ring as opposed to only those generated additively by the unitary element? How does this alter the behavior of the zeta function?

6. In general, is there an associated product form to the zeta function? We know via Euler that this holds when we allow our rings to be $\mathbb{R}$ or $\mathbb{C}$, but is there a way to define this product for any ring? The product form ends up being incredibly fruitful in the development of the Riemann zeta function, perhaps it would be equally as useful here.

7. What applications does the zeta function have to modern day ring/field theory? The Riemann zeta function was successfully used to talk about primes in the ring $\mathbb{Z}$, is there an equivalent formulation or idea for prime elements of an arbitrary ring?

8. What additional applications does the zeta function have? Certainly it may be used to ease computations in certain specialized situations, but what kind of situations could we expect these to arise in?

We have learned about the zeta function that began the development of such functions and areas of study such as analytic number theory. We studied applications and results of that historical zeta function. We then set out on our own; we developed a generalization which could be applied to a more general algebraic object, one which "mimicked" the historical zeta function and reduced down to the actual Riemann zeta function when applied to the correct object. Further, we studied how this new generalization behaves and built a sound characterization of it for special elements and special rings. With this in hand, we looked at future research related to this new zeta function. Though some parts of the development of this thesis were not groundbreaking, and though the zeta function we developed is not hard to understand, what we've managed to show is a remarkable curiosity, and with years of background information and inspiration, the potential for future research related to this development is nothing short of exhilarating.

References

[1] Beals, Richard. *Analysis: An Introduction.* Cambridge: Cambridge University Press, 2004. Print.

[2] Edwards, H.M. *Riemann's Zeta Function.* New York: Academic Press, 1974. Print.

[3] Jekel, David. "The Riemann Zeta Function." *The University of Washington.* n.p., 6 June 2013. Web. $https://www.math.washington.edu/\ morrow/336_13/papers/david.pdf$

[4] Korevaar, J. "On Newman's Quick Way to the Prime Number Theorem." *Mathematical Intelligencer* Vol 4 (1982): 108-115. Print.

[5] Lang, Serge. *Complex Analysis: Fourth Edition.* New York: Springer, 1999. Print.

[6] Miličić, Dragan. "Notes on Riemann's Zeta Function." *The University of Utah.* n.p.,n.d. Web. $http://www.math.utah.edu/\ milicic/zeta.pdf$

[7] Pinter, Charles C. New York: McGraw-Hill, 1990. Print.

[8] Rudin, Walter. *Principles of Mathematical Analysis: Third Edition.* New York: McGraw-Hill, 1976.

[9] Saracino, Dan. *Abstract Algebra - A First Course: Second Edition*. Long Grove: Waveland Press, 1980.

[10] Steinberger, Mark. "Units in $\mathbb{Z}_n$." *University at Albany: State University of New York*. n.p.,n.d. Web. *http : //www.albany.edu/ mark/units.pdf*

[11] Zaiger, D. "Newman's Short Proof of the Prime Number Theorem." *The American Mathematical Monthly* Vol. 104.8 (1997): 705-708. Print.