PRIME NUMBERS AND THE RIEMANN HYPOTHESIS

NICHOLAS ANDERSON, ANDREW J. HAVENS, BRIAN HYDEFROST, SEAN MURPHY, AND STEVE SARASIN

1. Primes

1.1. **Primes: Definition and Elementary Properties.** Prime numbers are specific elements of the set of positive integers greater than one, which we'll denote by $\mathbb{Z}_{>1}$. They are of great importance in number theory and abstract algebra, as they reveal a significant amount about the structure of the ring of integers. Commonly, we call a natural number *prime* if it has the property that it is divisible only by itself and one. Here, we take divisible to mean evenly divisible, in the sense that a young student would understand prior to being formally introduced to the the notions of rational and irrational numbers. Formally, we may define divisibility as follows:

Definition 1.1. Given integers a and n, we say a divides n, or equivalently, n is divisible by a, if and only if there exists some integer b such that the product of a and b equals n.

Symbolically, we write $a|n$ for "a divides n." The above definition can be conveniently and compactly written in mathematical shorthand as:

$$\text{Given } a, n \in \mathbb{Z},\ a|n \Leftrightarrow \exists\ b \in \mathbb{Z} : n = ab$$

To approach a formal definition of primes, we also define the set of divisors of an integer:

Definition 1.2. Given $n \in \mathbb{Z}$, the set of divisors of the integer n is the set $\mathrm{Div}(n) := \{m \in \mathbb{Z} : m|n\}$. Denote by $\mathrm{Div}^+(n)$ the set of positive divisors of any $n \in \mathbb{Z}^+$, $\mathrm{Div}^+(n) := \{m \in \mathbb{Z}^+ : m|n\}$.

An elegant way of formally defining primes can be given in terms of the set of positive divisors of a natural number. Denoting by $|\mathrm{Div}^+(n)|$ the cardinality of the set $\mathrm{Div}^+(n)$, we may say that a positive integer p is prime if $|\mathrm{Div}^+(p)| = 2$. This allows for the following precise definition of *the set of all primes*: $\mathbb{P} := \{p \in \mathbb{Z}^+ : |\mathrm{Div}^+(p)| = 2\}$. We may, with this definition, construct a partition of the positive integers. There is the set containing one. One is not a prime under this modern definition, since it is the unique integer whose set of positive divisors has cardinality one. Then there is the set of all primes, $\mathbb{P}$. Naturally, we might ask, "what of the remaining positive integers?" These are known as *composites*, because they admit divisors other than one and themselves, and so may be said to be "composed" by products of integers. More precisely, an integer that is not prime (i.e. has more than two elements in its set of positive divisors) may be expressed as the product of some pair of elements of its divisors, not including itself and 1.

The notions of prime and composite integers lie at the center of elementary arithmetic and number theory. Thus one may naturally expect to encounter the following definition distinguishing primes and composites:

Definition 1.3. An integer $p > 1$ is called prime if its only positive divisors are 1 and p; otherwise it is called composite.

It is then logical to present the following elementary theorem that clarifies the relationship between primes and composites:

Theorem 1.1. *Every integer larger than one can be expressed as a product of primes.*

Before venturing to prove this theorem, it is sensible to examine its implications and important questions that it may raise. First, note that by "product of primes" we allow trivial products, and so any prime p may be viewed as a product of primes in the sense that it is equal to p. This theorem then implies that the composites are "built" from the primes in a multiplicative sense. So one may view the primes as building blocks of the integers in the same way that elements are the building blocks of all molecules. One may also wonder whether there are there infinitely many primes, since there are infinitely many integers. But we shall first proceed to prove, by contradiction, that every integer greater than one can be expressed as a product of primes.

Proof. Suppose that there exist integers greater than one which are not expressible as products of primes. Closed subsets of the positive integers admit a well ordering property, and by this we deduce that if there exist integers greater than one that are not expressible as products of primes then there must be some smallest integer with this property, which we shall denote N. Then N cannot be prime, so by definition it must be composite, i.e. $\exists\ a, b \in \mathbb{Z}_{>1} : N = ab$, with $1 < a, b < N$. But, if $a, b < N$, then by our hypothesis, a and b are expressible as products of primes. Then N is expressible as a product of primes, and we have a contradiction. □

So it has been established in a more formal sense that primes build up the integers multiplicatively, i.e. each positive integer greater than one may be expressed as a product of primes. Yet, we have not examined the uniqueness of expressing integers as a particular product of primes. Given all of the well studied structure of integer multiplication, one might expect that prime factorization is unique, and this is the deeper result we are after, known as the Fundamental Theorem of Arithmetic.

Before attempting to prove the Fundamental Theorem of Arithmetic, we introduce the "division algorithm" and Euclid's Lemma. The division algorithm is not a genuine algorithm, but is ultimately the principle behind the algorithmic process of long division (which readily generalizes to the important Euclidean algorithm).

The Division Algorithm. *Given $a, b \in \mathbb{Z}$ with $b > 0$, there is a unique pair of integers q, r such that $a = bq + r$ with $0 \leq r < b$.*

If $r = 0$, by the definition of divisibility, $b|a$.

We now introduce a lemma of Euclid's, originally his proposition 30 in Book VII of *Euclid's Elements*:

Euclid's Lemma. *For $p \in \mathbb{P}$, $a, b \in \mathbb{Z}^+$, $p|ab \Rightarrow p|a$ or $p|b$.*

Though, after Theorem 1.1, it may seem obvious that if a prime divides a product, then it divides one of the factors of the product, the result is not completely trivial to prove, and serves as a good exercise in proof writing. Euclid's Lemma also frequently refers to a generalization of this proposition. This generalization is typically shown using Bézout's Identity, which we regrettably do not discuss. Armed with our statement of Euclid's Lemma, and our first theorem, we may attempt to prove the Fundamental Theorem of Arithmetic.

The Fundamental Theorem of Arithmetic. *Every positive integer greater than one may be expressed as a product of primes, with the product determined uniquely for every integer, up to a reordering of the primes.*

Proof. We prove this result by contradiction. Theorem 1.1 already guarantees that every integer has a prime factorization, so we assume there exists a positive integer n with two different factorizations into primes. We may write:

$$n = p_1 p_2 \dots p_i = q_1 q_2 \dots q_j,$$

where p_1, p_2, $\dots p_i$ and q_1, q_2, $\dots q_j$ are all primes. We may divide both sides by any common primes, and after reindexing (with possibly smaller i and j) obtain a list where no $p_u = q_v$ for any indices u or v, $1 \leq u \leq i,\ 1 \leq v \leq j$. The lists must be nonempty since we presumed that n had two different prime factorizations. But then the equality $n = p_1 p_2 \dots p_i = q_1 q_2 \dots q_j$ violates Euclid's lemma, since clearly, for any p_u, we have by definition 1 that $p_u | n \Rightarrow p_u | q_1 q_2 \dots q_j$, and by Euclid's lemma, p_u must divide some $q_v \neq p_u$. But if q_v is prime, it has no divisors other than 1 and itself, and so cannot be divisible by any p_u, contradicting the equality assumed in our hypothesis. Hence, the prime factorization of any positive integer $n > 1$ must be unique. □

Returning to the question of the infinitude of primes, we note that Euclid provided a proof in his *Elements* over 2000 years ago. He proceeded by contradiction, presuming that there were only finitely many primes. He then considered applying the division algorithm to the product of all primes plus one. We leave the details to the reader. (Hint: show independently or deduce by previous results that every integer greater than one has at least one prime divisor, and show that if there are finitely many primes, then one more than the product of all primes has a prime factor that, by the division algorithm, is not listed when constructing the product.)

1.2. **Prime Locations, The Prime Distribution, and the Prime Number Theorem.** So there is an infinite expanse of primes along the set of positive integers, and every positive integer has a unique prime factorization up to reordering. But how do we find the primes, and where do they live among the composite integers? It is not surprising that the Greeks had an algorithm for locating primes, due to Eratosthenes. The method involves eliminating multiples of known primes, until all that is left in any finite list is the primes. This method is fittingly called the sieve of Eratosthenes.

To apply the sieve to a finite set of numbers one starts by choosing the least element of the set greater than l, and then eliminating all following multiples of that element. If the aforementioned least element has more than two divisors it should also be eliminated from the list, otherwise it is prime and should be left alone. Then the next number that is either not prime or is not a number that is a multiple of the aforementioned least element should be selected, say p. All the multiples of p should be eliminated from the chosen interval and again if p is not prime it too should be eliminated. Then the next number neither prime nor a multiple of the least element or p is selected, say q, and all multiples of q in the set are eliminated, as well as q if it is not prime, and so on. For instance, on the set of integers from two to 100 one would begin first by eliminating all numbers that are multiples of two, of the form $2n$, or in other words all even numbers–two would stay in the list because it is only divisible by 1 and itself. Next all multiples of three on the set would be eliminated and three would remain because it is prime, and so on. If one wishes to find all primes less than a particular integer, the process is considerably more efficient. After eliminating all of the multiples of successive primes starting at 2, the next number remaining in the list will be prime, as it has cannot be a multiple of any of the preceding integers greater than one. Moreover, it is easy to establish that any composite integer n has a prime factor not exceeding $\sqrt{n}$. Thus, to find all primes less than some integer m, it suffices to perform the sieving process with primes up to the $\sqrt{m}$.

Once the sieve is applied to any sufficiently large subset of $\mathbb{Z}$ it can quickly be seen that there is a random distribution of primes between the least and greatest elements of the set. For instance between one and 100 the numbers range from having no integers in between them, e.g. 2 and 3, to

having 5 between them, e.g. 31 and 37. This is more commonly expressed as the difference between two successive primes, wherein 2 and 3 would have a difference of 1 and 31 and 37 would have a difference of 6. There are also several examples of a special case in this interval where primes have a difference of 2 between them, for instance 5 and 7, 29 and 31; these primes are referred to as twin primes. Understanding the distribution of primes has been of prime importance to number theorists, particularly in the modern economy. Prime factorization and primality tests are at the heart of modern cryptographic techniques, such as the RSA public key cryptography system. A thorough understanding of the distribution of primes could potentially lead to more efficient factorization algorithms, which could cripple the security of RSA but also drive new development in cryptography and the efficiency of computerized numerical computations.

One of the most renowned theorems among those of number theory addresses the prime distribution. It is the Prime Number Theorem, or PNT. The drive behind the PNT is a desire to estimate the number of primes less than a given positive real number.

Definition 1.4. Two functions $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$ are said to be asymptotic, denoted $f(x) \sim g(x)$, if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Definition 1.5. The prime counting function is defined as the function $\pi : \mathbb{R} \to \mathbb{Z}_{\geqslant 0}$ such that $\pi(x)$ is the number of primes less than or equal to a given real number x.

The original statement of the prime number theorem follows.

The Prime Number Theorem. $\pi(x) \sim x/\ln(x)$, *i.e. the ratio of* $\pi(x)$ *to* $x/\ln x$ *as* x *grows without bound is unity.*

German mathematician Johann Carl Friedrich Gauss had conjectured that $\pi(x) \sim x/\ln x$ in 1796, when he was merely 19 years old. He also conjectured that $\pi(x) \sim \mathrm{Li}(x)$, where $\mathrm{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ is the *logarithmic integral*. Gauss claimed in a letter to prominent astronomer Johann Franz Encke that his attention had been drawn to these two functions and their relation to the prime counting function circa 1792, when he was 15 years old. French mathematician Adrien-Marie Legendre conjectured in 1798 that $\pi(x)$ could be approximated by $x/(\ln x - 1.08366)$, a result obtained through careful observations built from a table of 400,031 primes (the table was computed by Jurij Vega). Gauss and Legendre were unable to prove either result. It wasn't until 1850 that any significant headway was made. Russian Mathematician Chebyshev was able to prove that $0.92129\,(x/\ln x) < \pi(x) < 1.10555\,(x/\ln x)$ for sufficiently large values of $x \in \mathbb{R}$. He also showed that if any function approximated $\pi(x)$ to the same order as $x/(\ln x)^N$ for large $N \in \mathbb{Z}^+$, then this function was the logarithmic integral $\mathrm{Li}(x)$. It follows from this that Legendre's approximation was inferior to those of Gauss.

In 1896, one century after Gauss had proposed the asymptotic relationship between the prime counting function and $x/\ln x$, French mathematician Jacques Hadamard and Belgian mathematician Charles-Jean-Gustave-Nicholas de la Vallée Poussin gave independent proofs of the PNT, both "non-elementary" (involving ideas from complex analysis, to be discussed later in this paper). The first "elementary proof" of the PNT did not appear until around 1948. Hungarian mathematician Paul Erdős and Norwegian mathematician Atle Selberg had "collaborated" to show the theorem without relying on complex analysis, but a bitter dispute between them occurred and clouded the history behind this accomplishment.

One reasonably simple interpretation of the PNT is in terms of probability. Roughly speaking, the prime number theorem states that if you randomly select a number nearby some large number N, the chance of it being prime is about $1/\ln N$. For example, near $N = 10,000$, we expect about one in

nine numbers to be prime ($\ln N \approx 9.2103$) , whereas near $N = 1,000,000,000$, we only expect one in every 21 numbers to be prime ($\ln \approx 20.7233$). In other words, the average gap between prime numbers near N is roughly $\ln N$. However the actual gap between primes near N could very well be more or less than $\ln N$; it is after all just an approximation, albeit a good one.

1.3. **Prime Deserts and Prime Conjectures.** It can be shown readily that the gaps between primes are not constrained to any definite bound. It is sometimes surprising for students, after learning of both the infinitude of primes and the asymptotic behavior of the prime counting function $\pi(x)$, that there are indeed arbitrarily large "prime deserts". Proving this is relatively simple.

Theorem 1.1. *Given any $n \in \mathbb{Z}^+$, there are at least n consecutive composite integers.*

Proof. Consider the following sequence of integers:

$$(n+1)!+2,\ (n+1)!+3,\ \ldots (n+1)!+n+1.$$

Since $n! := \prod_{k=1}^{n} k$, it is clear that for any integer j with $2 \leq j \leq n+1,\ j|(n+1)!$. Then $j|(n+1)!+j$ since $(n+1)!+j = j\left[\frac{(n+1)!}{j}+1\right]$, and $\frac{(n+1)!}{j}+1 \in \mathbb{Z}$. Thus, each term of the above sequence of consecutive integers is a composite number. □

Note that this does not necessarily give us a gap of size exactly n, as $(n+1)!+1$ and $(n+1)!+n+2$ might not be primes. As of 2007 the largest known prime gap with identified "probable prime" gap ends has length 2254930, with 86853-digit "probable primes" found by H. Rosenthal and J. K. Andersen. Here, the notion of a "probable prime" is the defined in terms of the Miller-Rabin primality test. Explaining this test requires a thorough discussion of modular arithmetic and Fermat's Little Theorem, hence we encourage the reader to investigate this independently. "Probable primes" are sometimes called "commercial primes", as they are used in commercial cryptography. The largest known prime gap with identified proven primes as gap ends has length 337446, with 7996-digit primes found by T. Alm, J. K. Andersen and Francois Morain.

There remain other large questions and conjectures regarding the prime number distribution, prime gaps, and prime characteristics. The unproven conjectures we will discuss are of great pedagogical interest, as they are easy to present, and easily understood even by an audience that is unfamiliar with number theory, yet they remain unproven despite all of the modern attacks made on them.

One such conjecture is the famous twin prime conjecture. It states that there are infinitely many primes p such that $p+2$ is also prime. Clearly not all primes p have twin primes associated with them, look no further than 2 for instance. $2+2=4$ and 4 is not prime as it is divisible by 1, 2 and 4. This conjecture only implies that the aforementioned list is infinitely long. An examination of a list of prime numbers shows that many prime pairs appear in the form p and $p+2$; such pairs are 5 and 7, 17 and 19, 39 and 41, etc. It is implied from numerous sources that the majority of mathematicians believe this conjecture to be true based on heuristic reasoning and circumstantial evidence. In fact, in 1966, Chen Jingrun showed that there are infinitely many primes p such that $p+2$ is either a prime or a product of two primes. Thus far Jingrun's work is the furthest stride towards a solution to this problem.

Another pair of conjectures are Goldbach's strong and weak conjectures, named for Prussian mathematician Christian Goldbach. Goldbach's strong conjecture is often simply referred to as "Goldbach's conjecture" (although it is also referred to as his even or binary conjecture), while the latter is generally just referred to as "Goldbach's weak conjecture" (or sometimes his odd or ternary conjecture). Goldbach's conjecture states that every even integer greater than 3 can be written as the sum of two

primes. Goldbach's weak conjecture follows from the strong conjecture and states that all odd numbers greater than 7 are the sum of three odd primes. Both conjectures have remained unproven since initially stated. Goldbach's conjecture has been worked on over the centuries since its first statement. In 1930, Lev Schnirelmann proved that every even number $n = 4$ is the sum of at most $300,000$ primes and most recently in 1995 Olivier Ramare proved that every even number $n = 4$ is the sum at most 6 primes. Clearly research mathematicians are coming closer to a solution, though no further progress to decrease the number of primes in the sum has been made in about a decade. If the strong Goldbach conjecture is true, the weak Goldbach conjecture will be true by implication. Also, if the weak Goldbach conjecture is proven it would imply that the sum of $2n = 4$ can be comprised of at most 4 primes.

The $n^2 + 1$ conjecture is another simple yet unproven conjecture concerning prime numbers. The conjecture states that there exist an infinite number of primes whose values are of the form $n^2 + 1$ for some integer n. Some primes clearly are of this form, e.g. $2^2 + 1 = 5$, whereas some are not, e.g. 7, since $7 - 1 = 6$ is not a perfect square.

Another point of interest is the infinitude of the set of Mersenne primes, which are primes of the form $2^p - 1$ where p is also a prime number. Though it is not known if there are infinitely many Mersenne primes, there are relatively fast algorithms to find them using modern computers. Nevertheless, to date only 46 Mersenne primes have been found, 12 of which were found by the collaborative computing effort known as the Great Internet Mersenne Prime Search or GIMPS. In recent history all the largest primes found have been Mersenne primes, as is currently the case: the largest known prime as of September/October 2008 is $2^{43,112,609} - 1$. An extension of the Mersenne prime definition is the Mersenne numbers $M_n = 2^n - 1$ where $n \in \mathbb{Z}^+$. These numbers appear in the recurrence relationship for solving the Tower of Hanoi game, and in fact the minimal number of steps to complete a game with a tower of n discs is M_n.

Suppose $q = 2 \cdot p + 1$ is a prime, where p is also a prime. Then q is referred to as a *safe prime*, and p is called a *Sophie Germain prime*. Safe primes are so called because sufficiently large safe primes are useful in cryptography. Sophie Germain primes are named after French mathematician Marie-Sophie Germain. Note that there is a one-to-one correspondence between Sophie Germain primes and safe primes. It is also possible for a Sophie Germain prime to be a safe prime for some other Sophie Germain prime p, i.e. there exist primes p such that $2p + 1$, $2(2p + 1) + 1$ are both prime. A sequence of primes that are both safe and Sophie Germain primes is called a *Cunningham chain*. It is conjectured that there are infinitely many pairs p, q with p a Sophie Germain prime and q a safe prime, and moreover that for any positive integer k there are infinitely many Cunningham chains of length k. This last result would follow from two widely supported conjectures: Dickson's conjecture and Schinzel's Hypothesis H. In fact, Schinzel's Hypothesis H is meant to broadly generalize conjectures like the $n^2 + 1$ and twin prime conjectures.

Throughout the nineteenth century, as analytic methods considerably improved, there was a paradigm shift in the study of number theory. Many highly important conjectures in number theory arose, frequently hinging on advanced algebraic and analytic ideas. Deep ideas about the primes emerged from the study of infinite series and complex numbers. Likewise, seemingly elementary theories such as the Prime Number Theorem were able to be proven using the techniques of complex analysis. Thus, for the remainder of this paper, our focus is on a pivotal complex function and an associated conjecture whose proof remains one of the most sought after accomplishments not only in number theory but in the whole of modern mathematics.

2. The Riemann Hypothesis

2.1. **The Riemann Zeta Function.** Consider the following function, commonly encountered in an undergraduate calculus course:

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

This function is called the Riemann zeta function, so named for the German mathematician Bernhard Riemann, who studied the function considerably. One may notice that we have not given a complete definition of this function in the sense that we have given no domain or codomain. Using techniques widely familiar to undergraduate students of calculus, we show how to determine a natural domain within the set of complex numbers. We will then discuss the historical significance of this series, which can be analytically continued to $\mathbb{C} \setminus \{1\}$, the entire complex plane excluding a simple pole at $s = 1$. We will also see that this function is intimately connected to the prime numbers, and questions about its zeros yield surprising ideas about the character of the prime number distribution.

We begin by examining (1) for $s \in \mathbb{C}$. Let $s = \sigma + it$, and note that:

$$\zeta(\sigma + it) = \sum_{n=1}^{\infty} \frac{1}{n^{\sigma+it}} = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \frac{1}{e^{it \ln n}} \Rightarrow \left| \sum_{n=1}^{\infty} \frac{1}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^\sigma}$$

where $\sigma = \Re(s)$. We may note that for $\Re(s) > 0$, $\left|\frac{1}{x^s}\right|$ decreases as $x \in \mathbb{R}$ increases, and so we may apply the integral test for convergence, from which we see that (1) is well defined for all complex s with $\Re(s) > 1$. Of course, if one attempts to evaluate $\zeta(1)$ using (1), they obtain the well known harmonic series $\sum_{n=1}^{\infty} \frac{1}{n}$, which diverges.

Remarkably, the seemingly inconspicuous infinite series in (1) may also be expressed as the following product over the primes:

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \ , \ \Re(s) > 1, \tag{2}$$

where $\mathbb{P}$ denotes the set of all primes, as before. This is known today as the Euler Product Identity, as it was first put forth in 1748 by Leonhard Euler in his publication *Introductio in Analysin Infinitorum*. We make use of a technique reminiscent of the Sieve of Eratosthenes to show how to obtain (2) from (1). First, we multiply $\zeta(s)$ by $\frac{1}{2^s}$, and note that:

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \ldots + \frac{1}{(2n)^s} \ldots$$

By subtracting this from (1) we "sieve" out the terms with even denominators. Similarly, by forming the expressions $\frac{1}{3^s}\zeta(s)$, $\frac{1}{5^s}\zeta(s)$, and $\frac{1}{7^s}\zeta(s)$ and considering $\left(1 - \frac{1}{7^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s)$, we may note that the terms eliminated in the subtractions are precisely those whose denominators are multiples of 2, 3, 5, or 7. If we continue this sieving process until the the left side is a product over all of the primes, the terms on the left gradually all disappear, except one, since by the Fundamental theorem of Arithmetic, every positive integer greater than one is expressible as a unique product of primes up to reordering. More precisely:

$$\zeta(s) \cdot \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right) = 1,$$

as long as we continue to stipulate that $\Re(s) > 1$ to ensure that $\zeta(s)$ converges. The infinite product also clearly converges under that condition, since for each term $1 - \frac{1}{p^s}$, when $\Re(s) > 1$ we have that $\left|1 - \frac{1}{p^s}\right| < 1$. We thus deduce that (2) is true. This is also provable by expanding each term of the product in (2) as a geometric series:

$$\frac{1}{1 - p_i^{-s}} = \sum_{k=1}^{\infty} \left(p_i^{-s}\right)^k.$$

We then note that the product of geometric sums is itself a sum, featuring all terms of the form $\frac{1}{n^s}$ with n expressible as a product of the form

$$n = \prod_i p_i^{k_i}$$

where p_i are distinct primes and k_i are natural numbers. The Fundamental Theorem of Arithmetic again allows us to deduce that we will see each positive integer n exactly once.

Clearly, both the sum and product forms define an analytic function in the half plane $\Re(s) > 1$, and so a natural question is whether it can be analytically continued to the whole complex plane, excluding the pole at $s = 1$, which corresponds to the harmonic series. There exist natural analytic continuations to $\mathbb{C}\backslash\{1\}$ via contour integrals, and one such continuation will be given in the appendix. There are also globally convergent series representations, such as the following double sum identity conjectured by Knopp in 1930:

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} (-1)^k \binom{n}{k} (k+1)^{-s} \right). \tag{3}$$

This was proven in 1930 by Hasse, but the result was forgotten until Sondow unearthed it in 1994. In modern contexts it is convenient to have a numerical method of evaluating $\zeta(s)$ for arbitrary complex s, and indeed Borwein used Chebyshev polynomials to derive a method that enables relatively rapidly converging computation of $\zeta(s)$. The details do not concern us, as we will only be considering a few special values before giving a conceptual overview of the Riemann Hypothesis and several of its well known implications.

2.2. **Historically Significant Values of $\zeta(s)$.** The question of evaluating (1) in the case where $s = 2$ was first posed by Pietro Mengoli in 1644. Leonhard Euler proposed a solution in 1735, though a truly rigorous proof was not offered until 1741. It came to be known as the Basel Problem, after the town of Basel, which was the hometown of Euler, as well as the Bernoulli family, who had attempted to solve the problem unsuccessfully.

Formally the Basel problem is to provide an exact closed form, with proof, for $\sum_{n=1}^{\infty} n^{-2}$. The startling value discovered by Euler is $\frac{\pi^2}{6}$, which he arrived at in an unorthodox fashion. Euler uses the sinc function $\frac{\sin x}{x}$, expanded as a Maclaurin series at zero, and then invokes the root-linear coefficient theorem to express it as a product of it's roots. He then expands the product to obtain the coefficient on the second order terms, and compares this coefficient with that of the Maclaurin series to deduce the value of $\zeta(2)$. It is the act of equating the sinc function to an infinite product of its roots that prevents his original proof from being rigorous. Augustin Louis Cauchy offered a rigorous proof in his 1821 publication *Cours d'Analyse*. Cauchy's proof involves bounding $\zeta(2)$ between two expressions, derived from trigonometric identities and complex variables. These two expressions are shown to converge to $\frac{\pi^2}{6}$. Modern proofs make use of the Residue theorem from complex Analysis, or Fourier Series, and

can be used to systematically derive closed form expressions for $\zeta(2n)$, with n any positive integer. A discussion of Euler's solution to the Basel Problem is given in the appendix, along with closed forms for $\zeta(2n)$ in terms of Bernoulli numbers.

A value of interest to consider is $\zeta(4) = \frac{\pi^4}{90}$, which shows up explicitly in the computation of the Stefan-Boltzman constant, of great importance in the study of blackbody radiation. Specifically, computation of the constant reduces to computing an integral that is recognizable as $\Gamma(4)\zeta(4)$, where $\Gamma(z)$ is the Gamma function, an analytic extension of factorials to the complex plane excluding certain poles (see Appendix A). It turns out that $\zeta(3)$, known as Apéry's constant, is also of importance to physics and mathematics, though it has no known closed expression. In fact, there are no known closed expressions for the Riemann zeta function at any of the odd positive integers. Curiously, the reciprocal of $\zeta(3)$ gives the probability that any three randomly chosen positive integers will be relatively prime. $\zeta(3)$ acquired the name Apéry's constant from mathematician Roger Apéry, who proved that it was irrational in 1978. It arises in connection with theoretical physics in the evaluation of integrals similar to the one encountered in the derivation of the Stefan-Boltzman constant.

The Riemann zeta function gives rise to certain elegant computations in the field of Bose-Einstein condensate research. The main result obtained by this analysis is that the critical temperature of a Bose-Einstein Condesate (BEC for short) can be given as:

$$T_c = \frac{2\pi\hbar^2}{mk_B}\left(\frac{\rho}{\zeta(D/2)}\right)^{2/D}, \tag{4}$$

where D is the (abstract) number of spacial dimensions (typically 3), $\hbar$ is the reduced Planck's constant, k_B is Boltzman's constant, m is the mass per boson, and ρ is the particle density. An observant student may note that this expression is only well defined if $\zeta(D/2)$ is nonzero for integral $D > 1$. As mathematicians, it is actually natural to ask when, if ever, is $\zeta(s)$ zero, not simply to ensure the validity of the useful expressions we come across in physics and probability, but to more deeply understand the mathematical nature of this function.

2.3. **The Critical Strip and Universality.** Reconsider the Euler Product form given in (2), which converges when $\Re(s) > 1$. Since none of the terms of the product are zero, we can immediately deduce that $\zeta(s)$ is nonzero throughout the half plane $\Re(s) > 1$. As we will later discuss in further detail, it can be shown that the zeros of $\zeta(s)$ occur in two sets: the trivial zeros, which occur at every even negative integer, and the nontrivial zeros, which are confined to the strip $0 < \Re(s) < 1$. This strip is known as the critical strip. It has been shown that, not only do all of the nontrivial zeros fall within this strip, but that they are symmetrically distributed with respect to the so called "critical line" that divides the strip at its center, i.e. complex s with $\Re(s) = \frac{1}{2}$. The properties of the Riemann zeta function and of generalized zeta functions in this strip give rise to some of the deepest modern questions about analytic number theory. Weiner showed that there is an equivalence between the Prime Number theorem and the assertion that $\zeta(s)$ has no zeros of the form $\Re(s) = 1$. In 1896 mathematicians Hadamard and de la Vallée-Poussin separately gave modern analytic proofs of the Prime Number Theorem by showing that $\zeta(s)$ has no zeros with $\Re(s) = 1$. Modern analytic proofs of the Prime Number Theorem rely on rigorously establishing the connection, i.e. starting by showing that $\zeta(s) \neq 0$ when $\Re(s) = 1$, and relying on this and other facts to establish that the prime counting function $\pi(x)$ is of the order $\frac{x}{\ln(x)}$ as x tends to infinity.

In 1975 Sergei Veronin described a remarkable property of $\zeta(s)$ in the (open) right half of the critical strip, known as universality. The essence of zeta function universality is that, given a compact set in the strip $\frac{1}{2} < \Re(s) < 1$ with connected complement, and a continuous function that is holomorphic

on the interior of the set and non-vanishing throughout the set, one can approximate the function uniformly to arbitrary accuracy with the Riemann zeta function by shifting the set vertically within the strip. It was first proven in a slightly less powerful form, where the set is taken to be a disk. Formally, let $0 < r < \frac{1}{4}$ and let $f(s)$ be non-vanishing continuous function on the disk $|s - 3/4| \leqslant r$, that is analytic throughout the interior. Then $\forall\, \epsilon > 0,\ \exists\, \tau \in \mathbb{R}$ such that

$$\max_{|s-3/4|\leqslant r} |\zeta(s + i\tau) - f(s)| < \epsilon. \tag{5}$$

The fact that $f(s)$ is required to be non-vanishing on the disk is no coincidence. In fact, if $\zeta(s)$ can serve as an approximation to itself within the strip in the manner described above, it would imply there are no nontrivial zeros within the strip $\frac{1}{2} < \Re(s) < 1$, and since the nontrivial zeros have a symmetric distribution with respect to the critical line $\Re(s) = \frac{1}{2}$, it would thus imply that all nontrivial zeros of the Riemann zeta-function have $\Re(s) = \frac{1}{2}$. That is, if Veronin's zeta function universality applies to the Riemann zeta function in the sense that it uniformly approximates itself arbitrarily well on compact, simply connected subsets of the strip $\frac{1}{2} < \Re(s) < 1$, then what is now known as the Riemann hypothesis is true. There are generalizations of universality to the broader class of Dirichlet L-functions, with similar consequences for broader generalizations of the Riemann Hypothesis.

2.4. **The Functional Equation and Riemann's Hypothesis.** In 1859, the same year that Charles Darwin published *On the Origin of Species*, Bernhard Riemann published *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, in english, *On the Number of Prime Numbers Less than a Given Quantity.* Of the ideas contained in this paper, the one destined to become the most studied began as a subtle and rather understated conjecture: that the roots of a particular function, $\xi(t)$, are all real. This function $\xi(t)$ was constructed from a functional equation for $\zeta(s)$, and by the unique construction, $\xi(t)$ vanishes precisely when $\zeta(1/2 + it)$ vanishes. We investigate just how this statement arises.

Riemann begins his paper with the Euler product identity (2), known to be equal to (1), and proceeds to construct a functional equation relating the values of $\zeta(s)$ to $\zeta(1-s)$, and valid in the half plane $\Re(s) < 1$. The functional equation, using modern notation, may be given as:

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\tfrac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s), \tag{6}$$

or in symmetric form:

$$\pi^{-s/2}\Gamma\left(\tfrac{s}{2}\right)\zeta(s) = \pi^{(s-1)/2}\Gamma\left(\tfrac{1-s}{2}\right)\zeta(1-s). \tag{7}$$

Examining (6), if one notes that $\Gamma(s)$ is undefined at all negative integers and zero, it is clear that the equation does not suggest that there are any zeros with $\Re(s) > 1$, which is consistent with previous assertions. By letting $s = 2n$, with n a negative integer:

$$\begin{aligned}\zeta(2n) &= 2^{2n}\pi^{2n-1}\sin\left(\tfrac{\pi\cdot 2n}{2}\right)\Gamma(1-2n)\zeta(1-2n)\\ &= 4^n\pi^{2n-1}\sin(\pi n)\Gamma(1-2n)\zeta(1-2n)\\ &= 0 \quad \forall n \in \mathbb{Z}^-,\end{aligned}$$

because $\sin(\pi n) = 0\ \forall n \in \mathbb{Z}$. These roots are called the trivial zeros of the Riemann zeta function precisely because they can be found simply and all at once from the functional equation in the above manner. The greater concern, for Riemann, was investigating the distribution of primes by constructing a formula for the number of primes less than a given quantity. He made use of (7) to this end.

To see why (7) is referred to as the symmetric form, define $\xi(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$, and note that (7) is equivalent to $\xi(s) = \xi(1-s)$. Riemann considers the function when $s = \frac{1}{2} + it$, which he denotes as $\xi(t)$, and expresses in an integral form. He then makes the assertion that it is probable that all of

the roots of $\xi(t)$ are real, which is equivalent to the assertion that all of the nontrivial zeros of the zeta function $\zeta(s)$ have $\Re(s) = \frac{1}{2}$. One should also note that by (7), $\xi(\frac{1}{2} + it) = \xi(\frac{1}{2} - it)$, which implies symmetry about the real axis in the critical strip, and as well the aforementioned symmetry of zeros about the critical line (simply let t lie in $\mathbb{C}$ with $-\frac{1}{2} < \Im(t) < \frac{1}{2}$).

The Riemann Hypothesis. *If $\rho \in \mathbb{C} \setminus \{1\}$ is a nontrivial zero of $\zeta(\rho) = 0$, then $\Re(\rho) = \frac{1}{2}$. Equivalently, if*

$$\xi(t) = \pi^{-(\frac{1}{2}+it)/2}\,\Gamma\left(\left(\tfrac{1}{2} + it\right)/2\right)\zeta(\tfrac{1}{2} + it),$$

and $\alpha \in \mathbb{C}\setminus\{1\}$ is a root of $\xi(\alpha) = 0$, then $\Im(\alpha) = 0$, which is the historical statement of the hypothesis.

Riemann's subtle statement of this assertion belies its true importance. In *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* he writes:

> *... es ist sehr wahrscheinlich, dass alle Wurzeln reell sind. Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich hat indess die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläug bei Seite gelassen, da er für den nächsten Zweck seiner Untersuchung entbehrlich schien.*

which we may translate as:

> *... it is very probable that all roots are real. Certainly one would wish for a stricter proof here; I have meanwhile temporarily put aside the search for this after some fleeting futile attempts, as it appears unnecessary for the next objective of my investigation.*

Though Riemann did not initially see the importance of his own conjecture, he meticulously calculated values of several nontrivial zeros to test this hypothesis. He may have later revisited the hypothesis to build framework of a proof, but if he did, any progress he made was likely lost after his death. We briefly discuss his original intent.

In his original paper, Riemann proceeds to build what is known as an "explicit formula" for the Riemann prime counting function

$$f(x) = \sum_n \frac{1}{n}\pi\left(x^{\frac{1}{n}}\right) = \pi(x) + \frac{1}{2}\pi\left(x^{\frac{1}{2}}\right) + \frac{1}{3}\pi\left(x^{\frac{1}{3}}\right) + \dots \tag{8}$$

which counts both primes and their powers (weighted as fractions). The prime counting function $\pi(x)$ may be recovered from $f(x)$ via a variant of Möbius inversion. The details of the construction for his explicit formula are quite sophisticated, however, the result has a magnificent interpretation. Recall that $\xi(t) = \pi^{-(\frac{1}{2}+it)/2}\Gamma\left(\frac{\frac{1}{2}+it}{2}\right)\zeta(\frac{1}{2} + it)$, and let ρ denote nontrivial zeros of $\zeta(\rho) = 0$. Then the explicit formula is

$$f(x) = \mathrm{Li}(x) - \sum_\rho \mathrm{Li}(x^\rho) - \int_x^\infty \frac{1}{x^2-1}\frac{\mathrm{d}x}{x\ln x} + \ln\xi\,(0)\,, \tag{9}$$

where the sum is computed over all of the nontrivial zeros in order of ascending magnitudes. This ordering is necessary, as the sum is not absolutely convergent, and only when summed in specific order does it relate to the quantities Riemann used in his construction. To examine the result further, we define the Möbius function.

Definition 2.1. Let $\alpha(n)$ be the number of distinct prime factors of $n \in \mathbb{Z}^+$. Then define the Möbius function, $\mu : (Z)^+ \to \{-1, 0, 1\}$ such that:

$$\mu(n) = \begin{cases} (-1)^{\alpha(n)} & \text{if } n \text{ is square-free} \\ 0 & \text{if } n \text{ is not square-free} \end{cases}$$

Riemann then notes that

$$\begin{aligned} \pi(x) &= \sum_n \frac{\mu(n)}{n} f\left(x^{\frac{1}{n}}\right) \\ &= f(x) - \frac{1}{2} f\left(x^{\frac{1}{2}}\right) - \frac{1}{3} f\left(x^{\frac{1}{3}}\right) - \frac{1}{5} f\left(x^{\frac{1}{5}}\right) + \frac{1}{6} f\left(x^{\frac{1}{6}}\right) - \dots \end{aligned}$$

The implication of (9) is that relatively small oscillations in the accuracy of the approximation of $\pi(x)$ by $\mathrm{Li}(x)$ are related to the distribution of the nontrivial zeros of Riemann's zeta function. That these zeros appear explicitly in Riemann's formula is evidence of the deep connection between $\zeta(s)$ and the prime distribution. However, even more profitable results have been conjectured by assuming the truth of the Riemann Hypothesis.

Theorem 2.1. *The following statements hold if and only if the Riemann hypothesis is true:*

a.) $|\pi(x) - \mathrm{Li}(x)| \leq \frac{1}{8\pi}\sqrt{x}\ln x \ \forall x > 2657$.

b.) $\forall \epsilon > 0, \ \exists C_\epsilon \in \mathbb{R}$ *such that* $|\sum_{n=1}^{N} \mu(n)| \leq C_\epsilon N^{\frac{1}{2}+\epsilon}$.

Thus, if the Riemann hypothesis is true, we have that the approximation Gauss provided for $\pi(x)$ is accurate to a surprisingly stable order (nearly square-root error!) and that the Mertens function $M(N) = \sum_{n=1}^{N} \mu(n)$ has an almost square-root order upper bound (Mertens had conjectured in 1890 that the upper bound was always less than or equal to the square-root of N for sufficiently large N, but this was disproved in 1985). These two remarkable consequences tie the hypothesis in more deeply to our understanding of the structure of prime numbers. In the year 2000 the Clay Institute included the Riemann Hypothesis as one of the seven millenium problems. A prize of one million dollars is offered for proof of the hypothesis (equivalently, for proof of one of the above two statements), but the prize is not offered for disproof.

Riemann's zeta function has been generalized to broader number theoretical objects known as Dirichlet series, and associated with their study is a *generalized Riemann hypothesis*. Likewise, there is an extension of the Riemann zeta function to more arbitrary algebraic domains, via Dedekind zeta functions. Associated with the extended zeta functions is the so-called *extended Riemann hypothesis*. Both new hypotheses are again conjectures about the complex nontrivial zeros of the associated Dirichlet or Dedekind zeta functions. The consequences of the truth of the generalized Riemann hypothesis include the truth of the weak Goldbach conjecture, further strengthening of the Prime Number theorem, and the guarantee that the Miller-Rabin primality test and Shanks-Tonelli algorithm both run in polynomial time. Appendix C includes a brief description of both Dirichlet and Dedekind zeta functions.

Ultimately, it is hoped that from prime conjectures to the Riemann hypothesis one can gather the degree to which superficially disparate fields such as number theory and complex analysis are intrinsically connected. The deep relationship between the once mysterious complex numbers and number theory was decisively demonstrated when, one century after the Prime Number theory had been conjectured, it was proven using information about the zeros of the Riemann zeta function in the complex plane. Surely, that is a testament to the beautiful and surprising nature and structure of mathematics.