CONSEQUENCES OF THE RIEMANN HYPOTHESIS

DARREN YAO

ABSTRACT. The Riemann zeta function $\zeta(s)$ is one of the most fundamental functions in mathematics, and is one of the main objects of research in analytic number theory. Much of this subject originates from an 1859 paper by Bernhard Riemann titled *On the Number of Primes Less Than a Given Magnitude*, which establishes the study of the prime-counting function in terms of various complex-analytic ideas. Arguably the most important open problem in pure mathematics, the Riemann hypothesis, concerns the Riemann zeta function. In this paper, we begin with some background content about the Riemann zeta function, so that we can introduce the Riemann hypothesis. This is followed by a discussion of some applications of the Riemann hypothesis to topics such as the error term of the Prime Number Theorem, the squarefree number counting function, and primality testing.

1. Introduction

In calculus class, we learned that $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges. In the study of infinite series, we learned that $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, and $\sum_{n=1}^{\infty} \frac{1}{n^3}$ is an irrational number known as Apery's constant. These are special cases of the Dirichlet series

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

On the complex plane, this series converges when $\Re s > 1$. Within this zone of convergence, we can write

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_{x=0}^{\infty} \frac{x^{s-1}}{e^x - 1} dx$$

where the Gamma function is defined as follows:

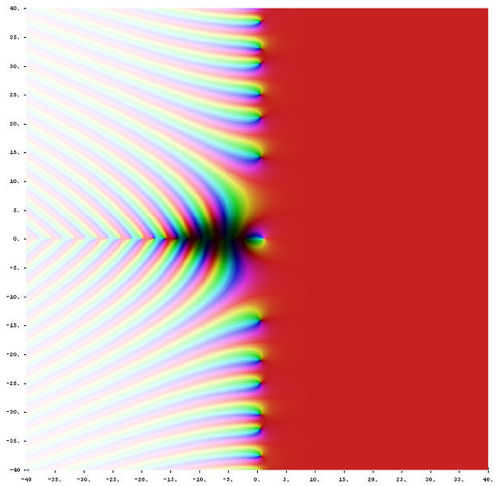
$$\Gamma(s) = \int_{x=0}^{\infty} x^{s-1} e^{-x} dx$$

To expand the region where the function is defined, we can use a technique called analytic continuation:

Definition 1.1 (Analytic Continuation)**.** Let f_1 and f_2 be analytic functions on domains Ω_1 and Ω_2, respectively, such that $\Omega_1 \cap \Omega_2$ is not empty and $f_1 = f_2$ on $\Omega_1 \cap \Omega_2$. Then, f_2 is called an analytic continuation of f_1 to Ω_2 and vice versa. If it exists, this analytic continuation is unique.

Outside of the original region of convergence, then, the Riemann zeta function, also denoted $\zeta(s)$, is defined by analytically continuing the sum of the Dirichlet series.

The Riemann zeta function can be plotted with domain coloring, as shown in the following diagram, where the hue represents the angle, and the brightness of the color represents the magnitude, where colors close to black represent values near zero. [Wik21]



Next, we'll introduce some specific values of the Riemann zeta function, as well as known roots, and some other properties.

The analytic continuation of this Riemann zeta function to the entire complex plane actually corresponds to certain methods of assigning values to not-necessarily-convergent series. For example, $\zeta(-1) = -\frac{1}{12}$, corresponding to $1 + 2 + 3 + \cdots = -\frac{1}{12}$, and $\zeta(\infty) = 1$, which should seem rather intuitive.

The Riemann zeta function can be written in terms of an infinite product, known as the Euler product:

Theorem 1.2. *For any positive integer n, we have*

$$\zeta(n) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-n}}$$

Proof. The proof is by method of prime sieve, where we essentially filter out multiples of each prime in succession

$$\zeta(n) = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \cdots$$

$$\zeta(n)\left(\frac{1}{2^n}\right) = \frac{1}{2^x} + \frac{1}{4^x} + \cdots$$

$$\zeta(n)\left(1 - \frac{1}{2^n}\right) = 1 + \frac{1}{3^x} + \frac{1}{5^x} + \frac{1}{7^x} + \frac{1}{9^x} + \cdots$$

$$\zeta(n)\left(1 - \frac{1}{2^n}\right)\left(1 - \frac{1}{3^n}\right) = 1 + \frac{1}{5^x} + \frac{1}{7^x} + \frac{1}{11^x} + \cdots$$

Repeating for all primes, we end up with all the $\left(1 - \frac{1}{p^n}\right)$ terms, and $\zeta(n)$, on the left. Some more basic algebra yields the desired result. ■

This leads to an interesting property about random selection of integers:

Theorem 1.3. *Given any two positive integers selected uniformly at random, the probability that they are relatively prime is $\frac{1}{\zeta(2)}$.*

Proof. Given a prime p, the probability that any randomly selected positive integer is divisible by p is $\frac{1}{p}$. Therefore, the probability that two randomly selected integers are both divisible by p is $\frac{1}{p^2}$.

In order for the two randomly selected positive integers to be relatively prime, for **every** prime p, at least one of the integers must not be divisible by p. The probability of this is $1 - \frac{1}{p^2}$. We can simply multiply the probabilities over all p to get our answer. ■

In fact, we can generalize this result.

Corollary 1.4. *Given any n integers selected uniformly at random, the probability that they are relatively prime is $\frac{1}{\zeta(n)}$. The proof is essentially the same, just replace the p^2 with p^n.*

Related to the above is the following result about the distribution of squarefree numbers:

Theorem 1.5. *Given a positive integer selected uniformly at random, the probability that it is squarefree (not divisible by the square of any integer) is $\frac{1}{\zeta(2)}$.*

Proof. Again, the technique used in this proof is essentially the same as the one we used in Theorem 1.3. In order for an integer to be squarefree, it must not be divisible by p^2 for all primes p. For any given p, the probability that a randomly selected positive integer is not divisible by p^2 is $1 - \frac{1}{p^2}$. Multiplying over all primes p, we get $\prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)}$, as desired. We'll revisit this function later, once we learn about the Riemann hypothesis. ■

Furthermore, there is a result known as Riemann's functional equation, which relates the Riemann zeta function to the Gamma function:

Proposition 1.6 (Riemann's functional equation)**.**

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

Proposition 1.7. *Due to the properties of the sine function in the above functional equation, we can find that the Riemann zeta function has zeros at the negative even integers. These are referred to as the **trivial zeros**.*

However, these are not the only zeros. The Riemann zeta function also has other zeros. A few of them are, approximately, $\frac{1}{2} + 14.134725i$, $\frac{1}{2} + 21.022040i$, and $\frac{1}{2} + 25.010858i$. You might notice that all of these have real part $\frac{1}{2}$. This motivates the following...

Conjecture 1.8 (The Riemann Hypothesis)**.** *The Riemann Hypothesis states that all of the Riemann zeta function's nontrivial zeros have real part $\frac{1}{2}$.*

Proof. Left as an exercise to the reader. ■

The Riemann Hypothesis is widely considered to be pure mathematics's most important open problem, and is a central conjecture in analytic number theory.

2. Littlewood's Theorem

Littlewood's theorem is a result about the Prime Number Theorem's error term. In order to understand this, we must first introduce some necessary definitions:

Definition 2.1. The logarithmic integral is a nonelementary function used to asymptotically estimate the distribution of prime numbers:

$$li(x) = \int_0^x \frac{dt}{\ln t}.$$

Theorem 2.2 (Prime Number Theorem)**.** *Let $\pi(x)$ denote the number of primes less than or equal to x. Then,*

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

Knowing that the asymptotic quotient is 1, we might now be interested in knowing what $\pi(x) - li(x)$ looks like. In fact, J. E. Littlewood not only bounded the error of $\pi(x) - li(x)$, but also showed that it changes sign infinitely many times. [Ing35]

Theorem 2.3.

(1) *There are arbitrarily large values of x for which $\pi(x) > li(x) + \frac{1}{3}\frac{\sqrt{x}}{\log x} \log\log\log x$*

(2) *There are arbitrarily large values of x for which $\pi(x) < li(x) - \frac{1}{3}\frac{\sqrt{x}}{\log x} \log\log\log x$.*

Therefore, it can be concluded that there are infinitely many values of x for which $\pi(x) > li(x)$, and infinitely many values of x for which $\pi(x) < li(x)$.

Proof. The proof of this theorem is over a dozen pages and is therefore beyond the scope of this paper. In brief, Littlewood deduced this proof from the truth of the Riemann hypothesis, and also from the falsity of the Riemann hypothesis, showing that it is always true. ■

Littlewood's proof was nonconstructive; it did not find any number x bounding the sign change. Later, Skewes [Ske33] showed that the first sign change of $\pi(x) - li(x)$ must satisfy $x < e^{e^{e^{79}}}$, assuming the Riemann hypothesis. This number is known as Skewes's number. Later results proved the bound $x < e^{e^{e^{e^{7.705}}}}$ independently of the Riemann hypothesis.

Through brute force computing power, the current best bounds are $10^{19} < x < 1.39716 \cdot 10^{316}$ assuming the Riemann hypothesis. [Bü] [SD11a]

3. Counting Squarefree Numbers

In Theorem 1.5, we looked at the distribution of squarefree numbers as $n \to \infty$. Now, we can bound them for all n:

Theorem 3.1. *For $n \geq 1$, the number of squarefree positive integers less than or equal to n, denoted by $Q(x)$, satisfies $Q(x) = \frac{6}{\pi^2} + O(\frac{1}{\sqrt{n}})$.*

Proof. We follow Conrad's proof. [Con20]

Lemma 3.2.

$$\sum_{d>y} \frac{\mu(d)}{d^2} = O\left(\frac{1}{y}\right)$$

Let $\mu_2(n) = |\mu(n)|$. Then,

$$\mu_2(n) = \sum_{d:d^2|n} \mu(d)$$

because both sides are multiplicative, and at prime powers, 1 if squarefree and 0 if not.

Then,

$$Q(x) = \sum_{n=1}^{x} u_2(n) = \sum_{n=1}^{x} \sum_{d:d^2|n} \mu(d) = \sum_{d \leq \sqrt{x}} \mu(d) \left\lfloor \frac{x}{d^2} \right\rfloor$$

Then, we have

$$Q(x) = \sum_{d \leq \sqrt{x}} \mu(d) \left(\frac{x}{d^2} + O(1) \right) = \left(\sum_{d \leq \sqrt{x}} \frac{\mu(d)}{d^2} \right) x + O(\sqrt{x}).$$

For $y \geq 1, \sum_{d \leq y} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2} - \sum_{d > y} \frac{\mu(d)}{d^2}$.
Therefore,

$$Q(x) = \left(\frac{6}{\pi^2} + O(\frac{1}{\sqrt{x}}) \right) x + O(\sqrt{x}) = \frac{6}{\pi^2} x + O(\sqrt{x}).$$

Dividing by x yields the desired result. ■

Using the Riemann hypothesis, Axer reduced the bound on $Q(x)$ from $O(\sqrt{x})$ to $O(x^r)$ for some $r < \frac{1}{2}$. [SD11b] In Theorem 3.1, we proved the error bound on $Q(x)$ in three steps:

- Write $Q(x)$ in terms of a Mobius function multiplied by a floor function. Separate the floor function into an integer term and a residue term.
- Show $\sum_{d > \sqrt{x}} \frac{\mu(d)}{d^2} = O(\frac{1}{\sqrt{x}})$, so $x \sum_{d > \sqrt{x}} \frac{\mu(d)}{d^2} = O(\sqrt{x})$
- Bound $\sum_{d \leq \sqrt{x}} \mu(d) \frac{x}{d^2}$ with $O(\sqrt{x})$

Using the Riemann hypothesis, Axer improved the bounds in the second and third steps, dependent on the Riemann hypothesis:

Theorem 3.3.

- *In the second step,* $\sum_{d > \sqrt{x}} \frac{\mu(d)}{d^2} is O_\epsilon(1/x^{3/4-\epsilon})$, *so* $x \sum_{d > \sqrt{x}} \frac{\mu(d)}{d^2} is O_\epsilon(1/x^{1/4+\epsilon})$
- *In the third step,* $\sum_{d \leq \sqrt{x}} \mu(d) \{ \frac{x}{d^2} \} = O_\epsilon(x^{2/5+\epsilon})$.

Proof. A brief sketch of the proof is as follows: we can split up the sum $Q(x) = \sum_{n \leq x} \sum_{d^2|n} \mu(d)$ into three sums, as follows: Let $\alpha \in (0, \frac{1}{2})$.

$$Q(x) = \sum_{d^2\delta \leq x} \mu(d) = \sum_{\substack{d^2\delta \leq x \\ d \leq x^{1/2-\alpha}}} \mu(d) + \sum_{\substack{d^2\delta \leq x \\ d > x^{1/2-\alpha}}} \mu(d)$$

$$= \sum_{\substack{d^2\delta \leq x \\ d \leq x^{1/2-\alpha}}} \mu(d) + \sum_{\substack{d^2\delta \leq x \\ \delta < x^{2a}}} \mu(d) + \sum_{\substack{d \leq x^{1/2-\alpha} \\ \delta \leq x^{2a}}}$$

$$= S_1 + S_2 - S_3$$

Here, Axer uses the Riemann hypothesis equivalent $\sum_{n \leq x} \mu(x) = O(x^{1/2-\epsilon})$ to bound S_1, S_2, S_3 as follows:

$$S_1 = \frac{6}{\pi^2} x + O_\epsilon(x^{1/4+\alpha(3/2)+\epsilon(1/2-\alpha)}) + O(x^{1/2-\alpha})$$

$$S_2 = O_\epsilon(x^{1/4+\alpha(3/2)+\epsilon(1/2-\alpha)})$$

$$S_3 = O_\epsilon(x^{1/4+\alpha(3/2)+\epsilon(1/2-\alpha)})$$

We choose the most convenient α value of $\frac{1}{10}$ which simplifies the exponent in S_1. Plugging in the α values and simplifying, we get our desired result:

$$Q(x) = \left(\frac{6}{\pi^2}\right) + O_\epsilon(x^{2/5+\epsilon(2/5)}).$$

■

4. The Generalized Riemann Hypothesis

The regular Riemann hypothesis concerns only the analytic continuation of the sum $\sum \frac{1}{n^s}$. The generalized Riemann hypothesis generalizes the numerator to all Dirichlet character functions, which are a specific type of arithmetic function. [Str08]

Definition 4.1. A Dirichlet character is a function $\chi : \mathbb{Z} \to \mathbb{C}$ satisfying these properties:

(1) Periodicity: There exists a positive integer k, such that for all n, $\chi(n) = \chi(n+k)$. In other words, if $m \equiv n \mod (k)$, then $\chi(m) = \chi(n)$.
(2) GCD: If $\gcd(n,k) > 1$ then $\chi(n) = 0$, and otherwise if $\gcd(n,k) = 1$ then $\chi(n) > 0$.
(3) Total multiplicativity: $\chi(mn) = \chi(m)\chi(n)$ for all integers m, n.

It trivially follows that $\chi(1) = 1$.

Essentially, a Dirichlet character can be thought of as a homomorphism from $\mathbb{Z}/n\mathbb{Z} to \mathbb{C}/n\mathbb{C}$.

Proposition 4.2. *For all n such that $\gcd(n,k) = 1$, $\chi(n)$ is a $\phi(k)$-th root of unity.*

Proof. By Euler's theorem, we have $n^{\phi(k)} = 1 \pmod{k}$. Therefore, $\chi(n^{\phi(k)}) = \chi(1) = 1$ by periodicity, and $\chi(a^{phi(k)}) = \chi(a)^{\phi(k)}$ by multiplicativity. This completes the proof. ■

Definition 4.3. Given a Dirichlet character χ, let the corresponding Dirichlet L-function be defined as

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for some complex number s.

Now, we can finally introduce the generalized Riemann hypothesis.

Conjecture 4.4 (Generalized Riemann hypothesis)**.** *For every Dirichlet L-function, all nontrivial zeros (meaning zeros not on the real line) have real part $\frac{1}{2}$.*

5. Primality Testing

One important application of the generalized Riemann hypothesis is to show that the Miller-Rabin primality test always runs reasonably quickly.

First, let's introduce Carmichael numbers and the Miller-Rabin primality test:

Definition 5.1. A Carmichael number is a composite number n satisfying

$$b^{n-1} \equiv 1 \pmod{n}$$

for all b relatively prime to n.

Equivalently, Carmichael numbers satisfy

$$b^n = b$$

for all integers b.

Algorithm 1: Miller-Rabin Primality Testing

```
input  : an integer $n$
output: whether $n$ is a probable prime
if $n > 2$ and $n$ is even then
    return composite
end
Choose $x \in \{1, 2, \ldots, n-1\}$ ;
Compute each of the numbers $x^t, x^{2t}, x^{4t}, \ldots, x^{2^s \cdot t} \pmod{n}$ ;
if $x^{n-1} \not\equiv 1 \pmod{n}$ then
    return composite
end
for $i = 1, 2, \ldots, s$ do
    if $x^{2^i \cdot t} \equiv 1 \pmod{n}$ and $x^{2^{i-1}t} \not\equiv \pm 1 \pmod{n}$ then
        return composite
    end
end
return probably prime
```

It can be proven that the Miller-Rabin primality test always returns prime when n is prime, composite when n is composite and non-Carmichael with probability at least $\frac{1}{2}$, and composite when n is Carmichael with probability at least $\frac{3}{4}$.

Definition 5.2. For a Carmichael number n, let x be a Miller-Rabin witness if the Miller-Rabin algorithm returns "composite" when x is the value in $\{1, 2, \ldots, s\}$ randomly chosen by the algorithm.

Remark 5.3. The Miller-Rabin function runs in $O(\log^3 n)$, which is polynomial in the number of digits of n. This can be easily determined using the fact that multiplication is $O(\log^2 n)$ and simply counting the number of operations.

Given the above, we can determine that the Miller-Rabin primality test always runs in polynomial time:

Theorem 5.4. *[Kle10] Assuming the generalized Riemann hypothesis, for every composite number n, the set $\{1, 2, \ldots, 2\ln^2 n\}$ contains a Miller-Rabin witness for n. Therefore, if GRH is true, we can apply Miller-Rabin to check primality of any number n in $O(\log^5 n)$.*

References

[Bü] J. Büthe. An analytic method for bounding $\psi(x)$. *Mathematics of Computation*, 87.

[Con20] K. Conrad. *Analytic Number Theory.* University of Connecticut, 2020.

[Ing35] A. Ingham. A note on the distribution of primes. *University of Cambridge*, pages 200–211, 1935.

[Kle10] B. Kleinberg. Orbits of antichains revisited. *Introduction to Algorithms (CS 482)*, 2010.

[SD11a] D. Stoll and P. DeMichel. The impact of $\zeta(s)$ complex zeros on $\pi(x)$ for $x < 10^{10^{13}}$. *Mathematics of Computation*, 80(276):2381–2394, 2011.

[SD11b] D. Stoll and P. DeMichel. Über einige grenzwertsätze. *Sitzungsberichte Akad. Wiss. Wien,*, (120):1253–1298, 2011.

[Ske33] S. Skewes. On the difference $\pi(x) - li(x)$ (i). *Journal of the London Mathematical Society*, 1933.

[Str08] A. Strombergsson. *Analytic Number Theory.* Uppsala University, Uppsala University, 2008.

[Wik21] Wikipedia. *Riemann zeta function $\zeta(s)$ in the complex plane.* Wikipedia, 2021.

Email address: darren.yao@gmail.com