PRIMES AND THE RIEMANN ZETA FUNCTION

MATT DECROSS

Preliminary

Problem 1 (An Interesting Function)**.**

Consider the following function ζ:

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

In lecture, we'll show how this function is mysteriously related to prime numbers. For now, though, we'll look at another interesting feature:

(1) Evaluate $\zeta(2)$ and $\zeta(4)$ (Ans: $\frac{\pi^2}{6}, \frac{\pi^2}{90}$).

(2) Attempt to evaluate $\zeta(1)$. What happens? Explain. (Ans: $\zeta(1)$ is divergent. This is the harmonic series.)

Problem 2 (Introduction to Product Notation)**.**

Mathematicians often introduce more compact notation as a means of simplifying a problem. When expressions get very complicated, sometimes rewriting it in a better way can help you see the solution. In pre-calculus and especially calculus, you've seen notation expressing a sum very compactly. Here we introduce a similar notation for products which we'll use during our lesson:

$$\prod_{n=1}^{k} x_n = x_1 x_2 \dots x_k.$$

Just as we can write infinite sums, we can also write infinite products as:

$$\prod_{n=1}^{\infty} x_n = \lim_{k\to\infty} x_1 x_2 \dots x_k.$$

(1) Write $p!$ in product notation, where $p!$ denotes *p factorial*, the product $p(p-1)\dots 1$. (Ans: $\prod_{n=1}^{p} n$)

(2) Evaluate $\prod_{n=1}^{k} \frac{n}{n+1}$. (Ans: $\frac{1}{n+1}$. This is a *telescoping product.*)

(3) Evaluate $\prod_{n=1}^{\infty} \left(\frac{2n}{2n-1} \cdot \frac{2n}{2n+1}\right)$. The answer should tell you why this product (called Wallis' product) is famous. (Ans: $\frac{\pi}{2}$).

Mathematics is all about studying patterns and structures in numbers, and finding ways to organize these patterns and structures so that they are useful. One of the most fascinating types of numbers to study are the prime numbers.

Definition (Prime Number)**.**

*A **prime number** is a positive integer greater than one that has no positive divisors other than one and itself.*

Example. The positive integer 7 is a prime number, since it has no other positive divisors than itself and one. The positive integer 4, however, is not a prime number, since 2 is a positive divisor of 4.

Why are these numbers so fascinating? Well, it turns out that we can actually represent any integer as a product of only prime numbers! This is the so-called fundamental theorem of arithmetic, proved by the Ancient Greek mathematician Euclid:

Theorem (Fundamental Theorem of Arithmetic)**.**

Every positive integer n greater than one can be represented as a unique product of prime numbers, that is:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

for primes $p_1 < p_2 < \ldots < p_k$ and some set of positive integers $\{\alpha_i\}$.

Example. The positive integer $60 = 2^2 \cdot 3 \cdot 5$. So $60 = \prod_{i=1}^{3} p_i^{\alpha_i}$, where $p_1 = 2$ $p_2 = 3$, $p_3 = 5$, and $\alpha_1 = 2$, $\alpha_2 = \alpha_3 = 1$.

Problem 3 (Square Roots of Primes are Irrational)**.**

Use the Fundamental Theorem of Arithmetic to prove that the square root of any prime p is irrational. Hint: use a proof by contradiction. Suppose the square root of p were rational and try to find an application of the Fundamental Theorem of Arithmetic.

Answer:

Proof by Contradiction. Suppose for the sake of contradiction that $\sqrt{p}$ is rational for an arbitrary prime p. Then by definition we can write $\sqrt{p} = \frac{x}{y}$ for some positive integers x and y. Squaring both sides and rearranging yields $py^2 = x^2$. The prime decompositions of x^2 and y^2 must consist only of primes with even exponents, because squaring doubles all exponents. But then py^2 has a prime decomposition where the exponent of p is odd while x^2 has a decomposition where the exponent of p is even, which contradicts the uniqueness of the prime decomposition by the fundamental theorem of arithmetic. Thus $\sqrt{p}$ is irrational for any arbitrary prime p. □

Euclid spent much of his life investigating the prime numbers, since they had many interesting properties. In particular, he was able to show easily that there are infinitely many prime numbers!

Theorem (Infinitude of the Primes)**.**

There are infinitely many prime numbers.

Proof by Contradiction.

Suppose that there are only finitely many prime numbers. Then in particular there is some largest prime number p. We will use p to show by construction that a prime larger than p must exist, thus contradicting our assumption and showing that indeed infinite primes exist, since for any given prime we may always construct a larger prime.

If p is the largest prime number, let $\{p_i\}$ denote the set of primes up to and including p. Then we may construct the following integer q:

$$q = 1 + \prod_i p_i = 1 + p_1 p_2 \dots p$$

Notably, $q > p$. Since q has remainder one upon division by any of the primes p_1, p_2, $\dots p$; q cannot be divisible by any of these primes. But then either q is prime or the prime factors of q are larger than p. In either case, we have shown that there is a prime larger than p, thus contradicting our assumption that p was the largest prime number. Therefore, there are infinitely many prime numbers. ☐

Example. We demonstrate the method described above in the above proof to show that we can always find a larger prime. Consider the prime number $p = 13$. Then we construct $q = 1 + 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 1 + 30030 = 30031$. But $30031 = 59 \cdot 509$, so we have found a new largest prime number, 509.

So we've established that there are infinitely many prime nubmers. But it seems like there are less prime numbers as we start looking at larger and larger integers. An interesting question, then, is the following: if there are infinitely prime numbers, but they seem to be less close together as we look at larger integers, is there a nice way we can characterize the distribution of prime numbers? For instance, can we find a formula that tells us how many prime numbers are less than some integer n? We can use what we've learned in high school pre-calculus and calculus to try to answer this question.

So what does the distribution of prime numbers have to do with the concepts we learn in high school pre-calculus and calculus, like complex numbers, integrals, and infinite series? Quite a bit actually. It turns out that one of the ways we can use calculus to learn interesting things about the distribution of prime numbers is via an infinite series. In high school calculus, we call this particular series the **p-series**, but in general mathematicians call it something different, after the famous 19th century German mathematician Bernhard Riemann :

Definition (Riemann Zeta Function)**.**

*The **Riemann Zeta Function** $\zeta(s)$ is given by*

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

In particular, notice that $\zeta(1)$ is the **harmonic series** that we have learned about in calculus, which diverges. As we might remember, the p-series was only convergent when the exponent was greater than one. This function is a little more general than the p-series because s can be a complex number, that is, we can write $s = a + bi$ for some real numbers a and b. Later, we'll use the notation $a = \mathrm{Re}(s)$ and $b = \mathrm{Im}(s)$.

Theorem (Convergence of the p-series)**.**

On the real line, the Riemann Zeta Function converges only when $p > 1$.

Proof.

When $p > 1$ we will show that the function converges by the integral test. (Consider the fact that the rectangular approximation / Riemann sum that underestimates the integral is equivalent to the sum. If the integral converges then the sum which is "contained inside" the integral must as well):

$$\int_1^x \frac{1}{x^p}\,dx = \frac{1}{1-p}\frac{1}{x^{p-1}}\bigg|_1^x$$

which clearly converges for $p > 1$.

In all other cases, we require $\lim_{n\to\infty}\frac{1}{n^p} = 0$, but this is not true and we have divergence by the nth term test.

□

Other values of $\zeta(s)$ are also very interesting. For instance $\zeta(2) = \frac{\pi^2}{6}$, and $\zeta(4) = \frac{\pi^4}{90}$, as we have seen. In fact, $\zeta(s)$ evaluated at all the positive even integers has something to do with powers of Pi! This is quite intriguing for mathematicians, who find Pi to be a very beautiful number.

So this function has something to do with Pi somehow, which is pretty cool. But we claim that this function has something to do with the distribution of prime numbers that we want to talk about, since primes are pretty cool too! What does this function have anything to do with primes? Well, the famous 19th-century Swiss mathematician Euler discovered a curious formula that related the Riemann Zeta Function and prime numbers:

Theorem (Euler's Product Formula)**.**

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

Proof.

Note that we're taking the product over the limit of a geometric series, that is,

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \prod_{p \text{ prime}} \left(\sum_{k=1}^{\infty} (p^{-s})^k \right) = \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} \dots \right).$$

Consider the expansion of this product,

$$\left(1 + \frac{1}{p_1^s} + \frac{1}{p_1^{2s}} \dots \right)\left(1 + \frac{1}{p_2^s} + \frac{1}{p_2^{2s}} \dots \right) \dots \left(1 + \frac{1}{p_k^s} + \frac{1}{p_k^{2s}} \dots \right) \dots$$

Performing this multiplication between every individual term, we obtain the sum over every possible combination of products of the individual terms. So when the dust clears,

$$\prod_{p \text{ prime}} \frac{1}{1-p^{-s}} = \sum \frac{1}{p_1^{\alpha_1 s} p_2^{\alpha_2 s} \dots p_n^{\alpha_n s}} = \sum \frac{1}{(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n})^s}$$

where the sum is over all possible sets of primes $\{p_1, \dots p_n\}$ and sets of integers $\{\alpha_1, \dots \alpha_n\}$. But by the fundamental theorem of arithmetic, each integer is represented uniquely by such a product $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, so we have

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

as claimed. □

Alternate Proof.

A famous algorithm called the Sieve of Eratosthenes is a method of finding prime numbers less than some integer. This method works as follows:

(1) Write down a list of all integers up to the cutoff point.

(2) Start by writing down 2, because 2 is prime, and then crossing off all multiples of 2.

(3) Proceeding to the next integer, 3, we see that 3 has not been crossed off yet, so we write down 3 as prime and cross off all multiples of 3.

(4) Continue in the same manner, writing down a number as prime only if it has not been crossed off, and then crossing off all of its multiples. This will generate a list of all primes less than the cutoff.

We employ that method in this proof. Recall that we can write the Riemann Zeta Function as

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots$$

Suppose we add a factor of 2^s to the denominator of every term, that is:

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

Then if we subtract this new series from the first, we will have sieved out all multiples of $\frac{1}{2^s}$ in the series. So we can write:

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \dots$$

Now, inspired by the Sieve of Eratosthenes, we iterate the same procedure to remove all multiples of $\frac{1}{3^s}$ from this new series, and obtain:

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

It seems that we are sieving out all of the primes! Repeating this algorithm ad infinitum yields:

$$\dots\left(1 - \frac{1}{11^s}\right)\left(1 - \frac{1}{7^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1$$

Dividing both sides by the factors on the left hand side, we see that:

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

as claimed □

This relationship is more than just a new formula–it actually tells us very useful information about prime numbers! For instance, we can prove Euclid's claim about the infinitude of the primes in much less space:

Problem 4 (Infinitude of the Primes)**.** Use Euler's product formula to establish the infinitude of the primes. Hint: use a proof by contradiction again! Consider evaluating $\zeta(s)$ at a specific value of s.

Answer: see the below theorem.

Theorem (Infinitude of the Primes)**.**

There are infinitely many prime numbers.

Proof by Contradiction.

Suppose there are only finitely many prime numbers. Then:

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

takes some finite value. But we know $\zeta(1)$ is just the harmonic series, which diverges. This is a contradiction, so there must be infinitely many prime numbers. (Note that this isn't really a proof because we tacitly assumed that there were infinitely many prime numbers in proving Euler's product formula when we used the geometric series formula / sieved out infinite terms, so really we are just recovering an initial assumption. But it's still a cute way to verify the result). □

Great, so we miraculously found a function that can tell us some useful things about prime numbers. But we're still not quite satisfied–we already knew there were infinitely many primes. Can we use this function to tell us more about the distribution of prime numbers, like we wanted? The answer is yes, but we need a more useful form of the function first.

If we recall the original series definition of the Riemann Zeta Function, it was a p-series, which only converges when the exponent is greater than one. We can write $\zeta(s)$ in a different way, though–in the early twentieth century, mathematicians found a way to rewrite the function so that it agreed with the infinite series when $\mathrm{Re}(s) > 1$, but also gave useful values for $\mathrm{Re}(s) < 1$. We need a new function to rewrite the Riemann Zeta Function like this, however. This new function is called the Gamma Function, which has a fancy integral definition that we don't need to worry about too much. The important part is that the Gamma Function is the same as the factorial, for the integers:

Definition (Gamma Function)**.**

*The **Gamma Function** $\Gamma(s)$ is given by*

$$\begin{aligned} \Gamma(s) &= \int_0^\infty x^{s-1}e^{-x}dx\,, && \mathrm{Re}(s) > 0 \\ \Gamma(s) &= (s-1)!\,, && \mathrm{Re}(s) \geq 1 \quad \text{and} \quad \mathrm{Im}(s) = 0. \end{aligned}$$

Using the Gamma Function, it's possible (but nontrivial) to prove that the following relation holds:

Theorem (Functional Equation for the Riemann Zeta Function)**.**

$$\zeta(s) = 2(2\pi)^{s-1}\sin(\pi s/2)\Gamma(1-s)\zeta(1-s), \quad \mathrm{Re}(s) < 1$$

This should be startling. The Riemann Zeta Function is defined as an infinite series which we have proved that (at least for real values) does not converge to the left of $s = 1$. Yet we've somehow found a way of expressing values of the function to the left regardless, which do not blow up. What's going on?

We obtained the above functional relation by playing with some integrals that were equal to the Riemann Zeta Function times the Gamma Function. The integrals we were playing with were actually convergent almost everywhere, but agreed with the the product of the RZF and the Gamma function on $\text{Re}(s) > 1$. This is an example of the concept from complex analysis known as *analytic continuation*; finding different representations of functions that agree on some overlapping set. These help to generalize any particular function by giving finite values for one form of a function in a region where another form might diverge to infinity.

Example. We compute $\zeta(-1)$:

$$\zeta(-1) = 2(2\pi)^{-2}\sin(-\pi/2)\Gamma(2)\zeta(2) = \frac{2}{4\pi^2}(-1)(1!)\left(\frac{\pi^2}{6}\right) = \frac{-1}{12}.$$

Notably, we can analogize $\zeta(-1) = 1 + 2 + 3 + \ldots = \frac{-1}{12}$. Though this is not the same as saying the divergent series $1 + 2 + 3 + \ldots$ converges to a finite value, certain formulas in physics that include the series $1+2+3+\ldots$ are measured experimentally to have finite values agreeing with the result $\frac{-1}{12}$ It's important to realize that we are not saying the series converges! Rather, the analytic continuation of the zeta function takes a finite value at -1, while the zeta function itself does not. It just happens that experiment motivates using the value instead of ∞ in the expression with $1+2+3+\ldots$ in certain physics formulae, which is and *should be* an uncomfortable fact.

We want to use our new functional equation to tell us something useful about the distribution of primes. To do this, we take advantage of the life's work of many mathematicians of the twentieth century, who figured out that the zeros of $\zeta(s)$ had something to do with the distribution of primes. Some of these zeros are easier to find than others:

Remark. From the functional equation for the Riemann Zeta Function, it's clear that the only zeros on the real line (when $\text{Im}(s) = 0$) occur when $\sin(\pi s/2) = 0$. This is true when $s = 0, -2, -4, \ldots$ These zeros are referred to as the *trivial zeros* of the Riemann Zeta Function, in part because they are very easy to find, but also because they do *not* encode any information about primes. Any other zeros are referred to as the *nontrivial zeros* of the zeta function.

Proposition (Riemann Hypothesis)**.** *All* nontrivial *zeros of* $\zeta(s)$ *lie on the line in the complex plane with* $\text{Re}(s) = \frac{1}{2}$.

This hypothesis is one of the most famous and most important unanswered questions of the twentieth and twenty-first century in mathematics (its solution is worth $1M from the Clay Mathematics Institute). Why is this so? Well, it turns out that if this hypothesis is true it tells us something very powerful about the distribution of primes.

In particular, we use the work of the famous late-18th century mathematician Carl Friedrich Gauss, who found that we could approximate the number of primes less than some integer by the following function:

Definition (Logarithmic Integral).

*The **Logarithmic Integral**, given by*

$$Li(x) = \int_2^x \frac{dt}{\ln t}$$

estimates the number of primes less than some integer x.

Example.

$$Li(20) = 8.86014 \approx 9 \qquad \pi(20) = 7$$
$$Li(48) = 16.9096 \approx 17 \qquad \pi(48) = 14$$

The Riemann Zeta Function is important because it tells us how good an estimate $Li(x)$ is for the number of primes less than x. Specifically, we would have the following:

Proposition (The Riemann Hypothesis and Distribution of Primes).

If the Riemann Hypothesis is true, then $Li(x)$ gives the number of primes less than some integer x to within $\sqrt{x}\ln x$.

The end result of our efforts: we've shown that there is a function represented as an infinite series over the complex numbers whose zeros give us information about the distribution of prime numbers!

Addendum: Below I have a precise statement of the theorem I quoted at the end of class:

Theorem. *There exists an* entire *(everywhere analytic/complex differentiable) function with arbitrarily prescribed zeros a_n provided that, in the case of infinitely many zeros, $a_n \to \infty$. Every entire function with these and no other zeros can be written in the form:*

$$f(z) = z^m e^{h(z)} \prod_{n=1}^{\infty} \left(1 - \frac{z}{a_n}\right) e^{\frac{z}{a_n} + \frac{1}{2}\left(\frac{z}{a_n}\right)^2 + \ldots + \frac{1}{m_n}\left(\frac{z}{a_n}\right)^{m_n}}$$

where the product is taken over all $a_n \neq 0$, the m_n and m are certain integers, and $h(z)$ is an entire function.

This was close to my statement from memory, but not quite; there are a few fixes: First, I wrote $g(z)$ in front of the product and claimed that $g(z)$ had no zeros. This is the same as $e^{h(z)}$; the exponential has no zeros. Second, note that the expression in parentheses in slightly different than how I wrote it, but the important part is that it is zero whenever $z = a_n$ for any zero a_n that is nonzero. (Third), the polynomial z^m out in front that I forgot just takes care of the fact that $f(z)$ could have a zero at 0; the m is the multiplicity of this zero (double/triple/etc root). Finally, I wrote $P(z)$ as some arbitrary polynomial in z; from the above theorem however we see that the condition is slightly more constrained.

Example.

$$\sin \pi z = \pi z \prod_{n \neq 0} \left(1 - \frac{z}{n}\right) e^{z/n} = \pi z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right)$$

Note that in the second expression we have combined all the terms n with those at $-n$, killing the exponential and making each term a difference of perfect squares.

The sin function as above is defined as zeros at all of the integers. This motivates the construction of the gamma function. By rearranging the above formulas slightly we can find a function with zeros only at the negative integers. Playing with the properties of this new function, it's possible (but annoying, so I won't write it here. See Ahlfors' *Complex Analysis* p. 198-199 if interested.) to construct some function that satisfies $f(z+1) = zf(z)$. But this is the fundamental definition of the gamma function: $\Gamma(z+1) = z\Gamma(z)$ is the factorial.

We obtain this nice functional definition from playing with the product expansions. The product expansion that we obtain for the Gamma function is the following:

Example.

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

where $\gamma \approx .57722$ *is Euler's constant,* $\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} - \log n\right)$.

From this definition we obtain the fact that the gamma function as the function that blows up at $z = 0, -1, -2, \ldots$ but has no zeros, and this equally suffices. Comparing to the previous example, it is possible (but nonobvious) to see that:

Corollary.

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

I have not proven any of the material presented in this addendum; several of the examples stated have proofs that are theoretically straightforward but involve quite a few lines of tedious computation. The point of this addendum is not necessarily that you follow every statement line-by-line, but rather to motivate why we might care about the theorem I quoted at the end of class.