

# Riemann's Zeta Function and the Prime Number Theorem

Dan Nichols  
nichols@math.umass.edu

University of Massachusetts

Dec. 7, 2016

Let's begin with the **Basel problem**, first posed in 1644 by Mengoli.  
*Find the sum of the following infinite series:*

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots$$

Let's begin with the **Basel problem**, first posed in 1644 by Mengoli.  
*Find the sum of the following infinite series:*

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots = \frac{\pi^2}{6}$$

- First solved\* by Euler in 1735

$$\sin(\pi x) = \pi x - \frac{(\pi x)^3}{3!} + \frac{(\pi x)^5}{5!} + \dots$$

$$\begin{aligned} \sin(\pi x) &= \pi x(1 - x^2) \left(1 - \frac{x^2}{4}\right) \left(1 - \frac{x^2}{9}\right) \dots \\ &= \pi x + \pi x^3 \left(1 + \frac{1}{4} + \frac{1}{9} + \dots\right) + \pi x^5 (\dots) + \dots \end{aligned}$$

Let's begin with the **Basel problem**, first posed in 1644 by Mengoli.  
*Find the sum of the following infinite series:*

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots = \frac{\pi^2}{6}$$

- First solved\* by Euler in 1735

$$\sin(\pi x) = \pi x - \frac{(\pi x)^3}{3!} + \frac{(\pi x)^5}{5!} + \dots$$

$$\sin(\pi x) = \pi x(1 - x^2) \left(1 - \frac{x^2}{4}\right) \left(1 - \frac{x^2}{9}\right) \dots$$

$$= \pi x + \pi x^3 \left(1 + \frac{1}{4} + \frac{1}{9} + \dots\right) + \pi x^5 (\dots) + \dots$$

- Euler's proof was incomplete; he assumed that a power series can be written as an infinite product of linear polynomials.
  - It's actually true in this case, but not always
- There are about a dozen other crazy ways to prove this.

Riemann's zeta function:

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

- This series converges for real numbers  $s > 1$ , diverges for real numbers  $s \leq 1$
- $s = 1$  is the harmonic series  $\sum_{n=1}^{\infty} \frac{1}{n}$
- The Basel problem is really asking “what is the value of  $\zeta(2)$ ?” **complex function**

# The Euler product formula

A prime number is a natural number whose only divisors are 1 and itself.

Here's the simplest connection between the zeta function and prime numbers:

$$\begin{aligned}\prod_p \left( \frac{1}{1 - p^{-s}} \right) &= \prod_p \left( \sum_{k=0}^{\infty} (p^{-s})^k \right) = \prod_p \left( \sum_{k=0}^{\infty} (p^k)^{-s} \right) \\ &= (1 + 2^{-s} + (2^2)^{-s} + \dots) (1 + 3^{-s} + (3^2)^{-s} + \dots) \dots \\ &= 1^{-s} + 2^{-s} + (2^2)^{-s} + 5^{-s} + (2 \cdot 3)^{-s} + 7^{-s} + (2^3)^{-s} + \dots \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s).\end{aligned}$$

# An application of the Euler product

## Theorem

Let  $X = \{x_1, x_2, \dots, x_s\}$  be a set of  $s$  randomly chosen integers. Let  $P$  be the probability that  $\gcd(X) > 1$ . Then  $P = 1/\zeta(s)$ .

- Let  $p$  be a prime.  $P(x_i \text{ is divisible by } p) = 1/p$ .
- $P(s \text{ random numbers are all divisible by } p) = (1/p)^s$
- $P(\text{at least one } x_i \text{ is not divisible by } p) = 1 - p^{-s}$
- Probability that there is no prime which divides all  $x_i$  is the product of this expression over all primes:

$$\begin{aligned} P &= \prod_p (1 - p^{-s}) \\ &= \frac{1}{\zeta(s)}. \end{aligned}$$

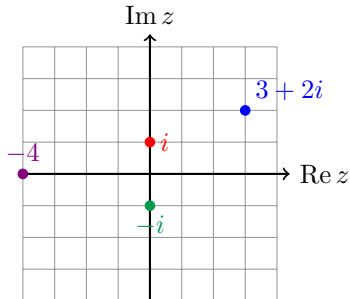
# Two minute intro to complex numbers part 1

$\zeta(s)$  was studied first by Euler as a real function. Riemann was the first to view it as a **complex** function.

## Definition

Let  $i$  be an imaginary number with  $i^2 = -1$ . **Complex numbers** are expressions of the form  $a + bi$  where  $a, b \in \mathbb{R}$ . We call this set  $\mathbb{C}$ .

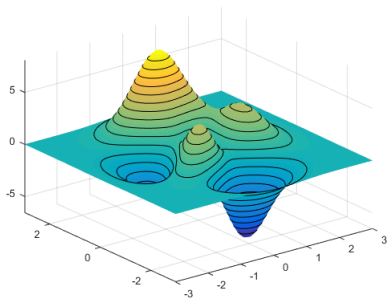
- Let  $z = a + bi$ . The **real part** of  $z$  is  $\operatorname{Re}(z) = a$  and the **imaginary part** is  $\operatorname{Im}(z) = b$ .
- View these as points in the **complex plane**, i.e.  $(x, y) = (\operatorname{Re} z, \operatorname{Im} z)$ .
- **Magnitude** of  $z$  is  $|z| = \sqrt{a^2 + b^2}$  (distance from  $z$  to the origin)





## Two minute intro to complex numbers part 2

- You can add, subtract, multiply, and divide complex numbers
- You can make a function whose input and output are complex numbers, e.g.  $f(z) = z^2$ 
  - $f(2 + i) = (2 + i)^2 = 2^2 + i^2 + 2 * 2 * i = 3 + 4i$
- Hard to graph because both domain and range are 2 dimensional



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

Riemann described the complex zeta function in his 1859 paper *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*.

- $\zeta(s)$  converges for all  $s \in \mathbb{C}$  with  $\operatorname{Re} s > 1$
- There is a **meromorphic continuation** of  $\zeta(s)$  to the rest of  $\mathbb{C}$  (with a simple pole at  $s = 1$ )

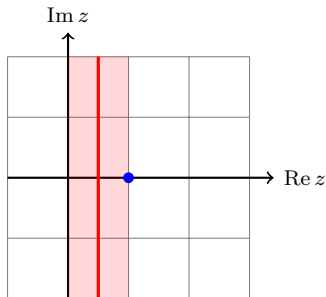
$$\zeta(s) = \frac{\Gamma(1-s)}{2\pi i} \int_C \frac{(-z)^s dz}{e^z - 1 z}$$

- $\zeta(s)$  satisfies a **functional equation**:

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

# The Riemann Hypothesis

The functional equation  $\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s)$  relates values on opposite sides of the **critical line**  $\operatorname{Re} z = 1/2$ :



It's known that all\* zeros of  $\zeta(s)$  lie in the **critical strip**  $0 < \operatorname{Re} z < 1$ .

## Conjecture (Riemann hypothesis)

*All nontrivial zeros of  $\zeta(s)$  have real part  $1/2$ .*

- There are trivial zeroes at all negative even integers
- This is one of the most famous unsolved problems in all of mathematics. If you can solve it, you'll get \$1 million and probably a Fields medal.
- Why is this important?
  - $\zeta(s)$  encodes lots of deep information about  $\mathbb{Z}$
  - Meromorphic complex functions are largely defined by the locations and orders of their zeros and poles.
  - Knowing the zeros is important for computing contour integrals. (more on this later)

- Number theory: branch of mathematics that studies the integers,  $\mathbb{Z}$
- However, in order to understand  $\mathbb{Z}$  we often have to work with other mathematical objects:
  - $\mathbb{Q}$  (rational numbers) and  $\mathbb{C}$  (complex numbers)
  - Finite fields  $\mathbb{F}_q$  (modular arithmetic)
  - Rings and fields of polynomials, e.g.  $\mathbb{Z}[t]$ ,  $\mathbb{F}_q(t)$
  - Geometric objects like algebraic curves
- Goal is to understand arithmetic in  $\mathbb{Z}$ . A major part of this is understanding how composite numbers break down into primes.
  - Another major part is understanding integer solutions to equations like  $x^2 - ny^2 = 1$

- The first few prime numbers are  
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...
- Prime numbers seem to occur less frequently as the numbers get bigger. Can we quantify this?

- The first few prime numbers are  
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...
- Prime numbers seem to occur less frequently as the numbers get bigger. Can we quantify this?
- Euclid, 3rd century BC: there are infinitely many primes

- The first few prime numbers are  
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...
- Prime numbers seem to occur less frequently as the numbers get bigger. Can we quantify this?
- Euclid, 3rd century BC: there are infinitely many primes
- Euler, 1737:  $\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots$  diverges



- The first few prime numbers are  
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...
- Prime numbers seem to occur less frequently as the numbers get bigger. Can we quantify this?
- Euclid, 3rd century BC: there are infinitely many primes
- Euler, 1737:  $\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots$  diverges
- Dirichlet, 1837: any arithmetic sequence  $(a + nd)_{n=0}^{\infty}$  contains infinitely many primes

- The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...
- Prime numbers seem to occur less frequently as the numbers get bigger. Can we quantify this?
- Euclid, 3rd century BC: there are infinitely many primes
- Euler, 1737:  $\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots$  diverges
- Dirichlet, 1837: any arithmetic sequence  $(a + nd)_{n=0}^{\infty}$  contains infinitely many primes
- Hadamard and de la Vallée-Poussin, 1896: **Prime Number Theorem** (with an assist from Riemann)

### Theorem (PNT)

Let  $\pi(x) = \#\{p \in \mathbb{Z} : p \leq x\}$  be the prime counting function. As  $x \rightarrow \infty$ ,  $\pi(x) \sim x / \log x$ . That is,

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x} = 1.$$

# Proving the Prime Number Theorem

Instead of working with  $\pi(x)$  directly, we'll use the von Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \\ 0 & \text{otherwise} \end{cases}$$

and the Chebyshev function

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

The PNT is equivalent to proving that  $\lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1$ .

# Proving the Prime Number Theorem

Here's where  $\zeta(s)$  comes in: it turns out that

$$-\frac{d}{ds} \log \zeta(s) = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}.$$

Then you can do some analysis and prove the following equation:

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \log(2\pi)$$

summing over the zeros  $\rho$  of  $\zeta(s)$ . If you know where the  $\rho$  are, you can prove that this is  $\psi(x) = x - (\text{lower order terms})$ .

Or compute a certain contour integral in the complex plane. Again, need to know the zeros of  $\zeta(s)$ .

# Proving the Prime Number Theorem

- Riemann stated his hypothesis in 1859. For decades afterwards, mathematicians knew that proving the RH would prove the PNT.
- 1896: Hadamard and de la Vallée-Poussin (independently) proved that all nontrivial zeros of  $\zeta(s)$  lie in the critical strip  $0 < \operatorname{Re} z < 1$ .
  - This is weaker than the RH, but it's enough to prove the PNT
- An even better estimate is  $\pi(x) = \int_2^x \frac{1}{\log t} dt$ .

- There are still many unanswered questions about the distribution of primes in  $\mathbb{Z}$ , e.g. twin prime conjecture
- For the past few decades, prime numbers (and number theory in general) have become important because of their use in crypto algorithms
- There are other zeta functions (and  $L$ -functions) for other types of mathematical objects such as number fields, varieties, representations. . .
  - Extended/Generalized Riemann Hypothesis (ERH/GRH): RH for other types of zeta functions
  - Many number theory papers prove important results **if** the GRH is true!

Further reading:

- J. Derbyshire, *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*
- H.M. Edwards, *Riemann's Zeta Function*