The Prime Number Theorem

A PRIMES Exposition

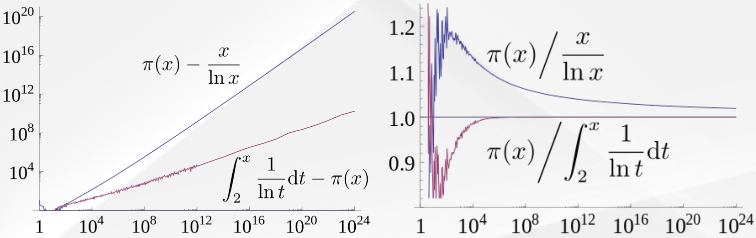
Ishita Goluguri, Toyesh Jayaswal, Andrew Lee
Mentor: Chengyang Shao

TABLE OF CONTENTS

Introduction

- Euclid (300 BC): There are infinitely many primes
- Legendre (1808): for primes less than 1,000,000:

$$\pi(x) \simeq \frac{x}{\log x}$$



- Euler: The product formula

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

so (heuristically)

$$\prod_p \frac{1}{1-p^{-1}} = \log \infty$$

- Chebyshev (1848-1850): if the ratio of $\pi(x)$ and $x/\log x$ has a limit, it must be 1
- Riemann (1859): *On the Number of Primes Less Than a Given Magnitude*, related $\pi(x)$ to the zeros of $\zeta(s)$ using complex analysis
- Hadamard, de la Vallée Poussin (1896): Proved independently the prime number theorem by showing $\zeta(s)$ has no zeros of the form $1+it$, hence the celebrated prime number theorem

Theorem (Maximum Principle)

Let Ω be a domain, and let f be holomorphic on Ω.
(A) $|f(z)|$ cannot attain its maximum inside Ω unless f is constant.
(B) The real part of f cannot attain its maximum inside Ω unless f is a constant.

Theorem (Jensen's Inequality)

Suppose f is holomorphic on the whole complex plane and $f(0) = 1$. Let $M_f(R) = \max_{|z|=R} |f(z)|$. Let $N_f(t)$ be the number of zeros of f with norm $\leq t$ where a zero of multiplicity n is counted n times. Then

$$\int_0^R \frac{N_f(t)}{t} dt \leq \log M_f(R).$$

- Relates growth of a holomorphic function to distribution of its zeroes
- Used to bound the number of zeroes of an entire function

Theorem (Borel-Carathéodory Lemma)

Suppose $f = u + iv$ *is holomorphic on the whole complex plane. Suppose* $u \leq A$ *on* $\partial B(0, R)$. *Then*

$$|f^{(n)}(0)| \leq \frac{2n!}{R^n}(A - u(0))$$

- Bounds all derivatives of f at 0 using only the real part of f
- Used in proof of Hadamard Factorization Theorem to prove that function is a polynomial by taking limit and showing that nth derivative approaches 0

Entire Functions

Definition (Order)

The order of an entire function, f, is the infimum of all possible $\lambda > 0$ such that there exists constants A and B that satisfy

$$|f(z)| \leq Ae^{B|z|^{\lambda}}$$

- $\sin z$, $\cos z$ have order 1
- $\cos\sqrt{z}$ has order $1/2$

Theorem

Let f be an entire function of order λ with $f(0) = 1$. Then, for any $\varepsilon > 0$ there exists a constant, C_ε, that satisfies

$$N_f(R) \leq C_\varepsilon R^{\lambda+\varepsilon}$$

Theorem

Let f be an entire function of order λ with $f(0) = 1$ and $a_1, a_2, \ldots$ be the zeroes of f in non-decreasing order of norms. Then, for any $\varepsilon > 0$,

$$\sum_{n=1}^{\infty} \frac{1}{|a_n|^{\lambda+\varepsilon}} < \infty$$

In other words, the convergence index of the zeros is at most λ.

For example, $\sin z$ and $\cos z$ have order 1, and their zeroes grow linearly while $\cos\sqrt{z}$ has order $1/2$, and its zeroes grow quadratically.

Hadamard Factorization Theorem

Theorem (Hadamard Factorization Theorem)

A complex entire function $f(z)$ of finite order λ and roots a_i can be written as

$$f(z) = e^{Q(z)} \prod_{n=1}^{\infty} \left(1 - \frac{z}{a_n}\right) \exp\left(\sum_{k=1}^{p} \frac{z^k}{k a_n^k}\right)$$

with $p = \lfloor \lambda \rfloor$, and $Q(z)$ being some polynomial of degree at most p

The theorem extends the property of polynomials to be factored based on their roots as

$$k \prod_{i=1}^{n} \left(1 - \frac{z}{a_i}\right).$$

The proof is based off of truncating the first p terms of the series

$$\log\left(1-\frac{z}{a_n}\right) = -\sum_{k=1}^{\infty}\frac{z^k}{k a_n^k}$$

which bounds the magnitude to $O(R^{\lambda+\epsilon})$ and gives rise to the exponential factor. Now,

$$g(z) = \prod_{n=1}^{\infty}\left(1-\frac{z}{a_n}\right)\exp\left(\sum_{k=1}^{p}\frac{z^k}{k a_n^k}\right)$$

has the same roots as $f(z)$ and the polynomial $Q(z)$ is found by taking the logarithm of $f(z)/g(z)$. The degree of Q is determined by bounding the derivatives using the Borel-Carathéodory lemma.

Definition (Reimann ζ Function)

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \; s = \sigma + it, \; \sigma > 1.$$

Theorem (Euler Product Formula)

The zeta function can also be written as

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

The Euler product formula is the analytic equivalent of the unique factorization theorem for integers.

Chebyshev Functions

Definition (Van-Mangoldt Function)

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p \text{ and some } m \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

Definition (Chebyshev Functions)

$$\psi(x) = \sum_{n \leq x} \Lambda(n), \; \vartheta(x) = \sum_{p \leq x} \log p.$$

Theorem

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

Equivalent Asymptotic Expressions

The Chebyshev functions can be related to $\pi(x)$ by the following integral expressions.

Theorem

$$\vartheta(x) = \pi(x)\log x + \int_2^x \frac{\pi(t)}{t}\,dt$$

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}\,dt$$

Studying the asymptotic behavior of the formulas, we see that all of the following expressions are logically equivalent:

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

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

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

The Perron Formula acts as a filter to isolate the first finitely many terms from a Dirichlet series.

Theorem (Perron Formula)

Let $F(s) = \sum_{n=1}^{\infty} f(n)/n^s$ be absolutely convergent for $\sigma > \sigma_a$. Then for arbitrary $c, x > 0$, if $\sigma > \sigma_a - c$,

$$\frac{1}{2\pi i}\int_{c-\infty i}^{c+\infty i} F(s+z)\frac{x^z}{z}dz = \sum_{n\le x}{}^{*}\frac{f(n)}{n^s}$$

where $\sum^*$ means that the last term is halved when x is an integer.

Corollary

For $x > 0$,

$$\int_0^x \frac{\psi(y)}{y}dy = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} -\frac{\zeta'}{\zeta}(s)\frac{x^s}{s^2}ds$$

Reimann Zeta Function Continued

We define a function ξ in terms of Γ, ζ and π to obtain a functional equation that gives information about the symmetry of zero distribution.

Definition

$$\xi(s) = \frac{\Gamma\left(\frac{s}{2}\right)\zeta(s)}{\pi^{s/2}}.$$

Theorem (Functional Equation, Riemann 1859)

$$\xi(s) = \xi(1-s)$$

The proof relies on the Poisson summation formula from Fourier analysis.

$$\frac{\Gamma\left(\frac{s}{2}\right)\zeta(s)}{\pi^{s/2}} = \sum_{n=1}^{\infty}\int_0^{\infty} x^{s/2-1}e^{-n^2\pi x}dx$$
$$= \int_0^{\infty} x^{s/2-1}\Psi(x)dx = \int_0^1 + \int_1^{\infty}$$

where

$$\Psi(x) = \sum_{n=1}^{\infty} e^{-\pi n^2 x}.$$

Using the Poisson summating formula,

$$2\Psi(x) + 1 = \frac{1}{\sqrt{x}}\left(2\Psi\left(\frac{1}{x}\right) + 1\right),$$

substituting into the integral from 0 to 1,

$$\xi(s) = \frac{1}{s(s-1)} + \int_0^1 x^{s/2-3/2}\Psi\left(\frac{1}{x}\right)dx + \int_1^{\infty} x^{s/2-1}\Psi(x)dx.$$

Changing the variable $x \to \frac{1}{x}$

$$\xi(s) = \frac{\Gamma\left(\frac{s}{2}\right)\zeta(s)}{\pi^{s/2}} = \frac{1}{s(s-1)} + \int_1^\infty \left(x^{-s/2-1/2} + x^{s/2-1}\right)\Psi(x)dx$$

Substituting $s = 1 - s$ gives $\xi(s) = \xi(1-s)$.

- The functional relations of $\zeta(s)$ can remarkably be obtained by studying the theory of p-adic numbers.
- Generally, the distance between two numbers is considered using the usual metric $|x-y|$, but for every prime p, a separate notion of distance can be made for $\mathbb{Q}$.
- For a rational number $x = p^n a/b$, $p \nmid a, b$, we define the p-adic absolute value as $|x|_p = p^{-n}$. Then, the p-adic distance between two numbers is defined as $|x-y|_p$.
- The p-adic absolute value is multiplicative, positive definite, and satisfies the strong triangle inequality: $|x-y|_p \leq \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$
- Examples:

$$|7/24|_2 = 8$$

$$|2-27|_5 = 1/25$$

- $\mathbb{Q}$ can be completed under this metric to form the field $\mathbb{Q}_p$
- $\mathbb{Q}_p$ contains a subring, $\mathbb{Z}_p$, which is the completion of $\mathbb{Z}$ under $|\cdot|_p$
- $\mathbb{Z}_p$ can be written using an "infinite p-adic expansion" with no negative powers and numbers in $\mathbb{Q}_p$ have finite negative powers
- Example: in $\mathbb{Q}_5$,

$$\ldots + 5^2 + 5 + 1 = \sum_{n=0}^{\infty} 5^n = \frac{1}{1-5} = -\frac{1}{4} \in \mathbb{Z}_5$$

  and $-1/5 = \ldots 111 \times \frac{4}{5} = \ldots 444.4$
- Letting $\mathbb{Z}_p^\times$ denote the elements of $\mathbb{Z}_p$ for which $|x|_p = 1$, $\mathbb{Q}_p^\times = \bigcup_{n\in\mathbb{Z}} p^n \mathbb{Z}_p^\times$

Adèles and Idèles

- The fields $\mathbb{R}$ and $\mathbb{Q}_p$ can be put together to form what is called the ring of Adèles
- The Adèle ring $\mathbb{A}_{\mathbb{Q}}$ is the collection of sequences $x = \{x_p\}_{p \in \mathbb{P} \cup \{\infty\}}$ for the primes $\mathbb{P}$ and where for each $p \in \mathbb{P}$, $x_p \in \mathbb{Q}_p$ and $x_\infty \in \mathbb{R}$ with almost all $x_p \in \mathbb{Z}_p$
- The Idèle group $\mathbb{I}_{\mathbb{Q}}$ is the collection of Adèles for which almost all $x_p \in \mathbb{Z}_p^\times$ and forms a group under componentwise multiplication
- We can also introduce a topology on $\mathbb{I}_{\mathbb{Q}}$ with open sets being the product of open sets in $\mathbb{R}^\times$ and $\mathbb{Q}_p^\times$, making $\mathbb{I}_{\mathbb{Q}}$ is a locally compact abelian group, a Haar measure, μ, can be formed for it
- Introduce the volume function $\|x\| := |x_\infty| \times \prod_{p \in \mathbb{P}} |x_p|_p$ and the function $\varphi(x) := \exp(-\pi |x_\infty|^2) \prod \mathbf{1}_{\mathbb{Z}_p}(x_p)$ and consider the integral

$$\int_{\mathbb{I}_{\mathbb{Q}}} \varphi(x) \|x\|^s d\mu(x)$$

The integral can be split into the real and p-adic components to obtain

$$\xi(s) = \left(\int_{\mathbb{R}^\times} e^{-\pi|t|^2}|t|^s \frac{dt}{t}\right) \times \left(\prod_p \int_{\mathbb{Z}_p^\times} |x_p|_p^s d\mu_p^\times(x_p)\right).$$

The first integral turns out to be $\Gamma\left(\frac{s}{2}\right)\pi^{-s/2}$ and the latter ones are $\frac{1}{1-p^{-s}}$ which combine to form $\zeta(s)$. So the integral coincides with the $\xi(s)$ introduced before:

$$\xi(s) = \Gamma\left(\frac{s}{2}\right)\zeta(s)\pi^{-s/2}.$$

- The integral can also be evaluated in a different way using the fact that $\mathbb{Q}^\times$ naturally embeds into $\mathbb{I}_\mathbb{Q}$ with constant sequences to form the group of principal idèles
- Taking the integral by considering equivalences classes, $\bar{x}$, of $\mathbb{I}_\mathbb{Q}$ over the principal idèles, it can be shown that

$$\xi(s) = \int_{\|\bar{x}\|>1} (\|\bar{x}\|^s + \|\bar{x}\|^{1-s})(\Theta(\bar{x}) - 1)d\bar{\mu}(\bar{x}) + \int_{\|\bar{x}\|>1} (\|\bar{x}\|^{1-s} - \|\bar{x}\|^{-s})d\bar{\mu}(\bar{x})$$

  for the Jacobi theta function

$$\Theta(\bar{x}) = 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2 \|\bar{x}\|^2}$$

  which gives $\xi(s) = \xi(1-s)$ by using the Poisson summation formula.
- The Poisson identity translates into Fourier analysis on $\mathbb{I}_\mathbb{Q}$.

- We find that this function is asymptotically related to Γ by

$$\xi(s) \sim \Gamma\left(\frac{s}{2}\right)$$

as $s \to +\infty$.

- Using the Hadamard Factorization Theorem, we obtain

$$\xi(s) = \frac{e^{as+b}}{s(1-s)} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho}.$$

- Hence

$$\zeta(s) = \frac{e^{A+Ds}}{s-1} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{s/\rho} \prod_{n=1}^{\infty} \left(1 + \frac{s}{2n}\right) e^{-s/(2n)}.$$

Explicit Formula for Primes

Theorem

For $x > 0$, not equal to an integer,

$$\int_0^x \frac{\psi(y)}{y} dy = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} -\frac{\zeta'}{\zeta}(s) \frac{x^s}{s^2} ds$$

Substituting in

$$\frac{\zeta'}{\zeta}(s) = D - \frac{1}{s-1} + \sum_p \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right) + \sum_{n=1}^{\infty} \left(\frac{1}{s+2n} - \frac{1}{2n} \right),$$

calculating the integrals using the residue theorem, We finally get the explicit formula for primes:

$$\int_0^x \frac{\psi(y)}{y} dy = x - (D+2)\log x - \sum_\rho \frac{x^\rho}{\rho^2} + \left(\frac{\pi^2}{24} + \sum_\rho \frac{1}{\rho^2} \right) - \sum_{n=1}^{\infty} \frac{x^{-2n}}{4n^2}.$$

Theorem (de la Valleé Poussin, Hadamard, 1896)

No zero of $\zeta(s)$ has real part 1.

Proof.

Taking the logarithm of the Euler product representation of $\zeta(s)$, we get

$$\log|\zeta(\sigma+it)| = -\mathrm{Re}\sum_p \log(1-p^{-(\sigma+it)}) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n\sigma}} \cos(nt\log p)$$

So

$$3\log|\zeta(\sigma)| + 4\log|\zeta(\sigma+it)| + \log|\zeta(\sigma+2it)| = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n\sigma}} 2(\cos(nt\log p)+1)^2 \geq 0$$

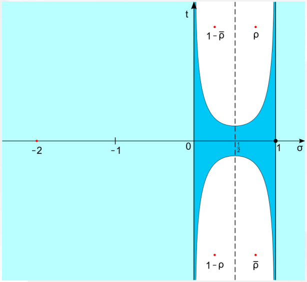
Thus,

$$|\zeta(\sigma)|^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)| \geq 1,\ \sigma > 1.$$

So if $1+it$ is a zero of $\zeta(s)$, then letting $\sigma \downarrow 1$, we arrive at a contradiction. □

Zero-Free Region

Thus, all ρ lie in the strip $0 < Re(\rho) < 1$. So there is a continuous non-increasing function $h : [0, \infty) \to (0, 1)$, such that $\zeta(s)$ is zero-free in the region $\sigma < h(t)$.



We use this fact to bound

$$\left| \sum_{\rho} \frac{x^{\rho}}{\rho^2} \right| = o(x)$$

Thus,

$$\int_0^x \frac{\psi(y)}{y} dy = x + o(x),$$

which is equivalent to the prime number theorem.

Prime Number Theorem with Error Term

The more we increase the bounds on the zero-free region, the better our precision of our estimate will be.

Theorem (de la Vallée Poussin, 1898)

There is a constant $A > 0$ such that $\zeta(s)$ has no zero in the region

$$\sigma < 1 - \frac{A}{\log(2+t)}, \; t \geq 0.$$

We use this to bound $\psi(y)$ and use the relations between the Chebychev functions to $\pi(x)$ to get

$$\pi(x) = \text{Li}(x) + O(xe^{-c\sqrt{\log x}})$$

which is the prime number theorem with error term.