An Introduction to Prime Number Theory

Aaron Benda

The University of Texas at Austin

abenda@utexas.edu

December 3, 2021

Prime Numbers

A natural number $p > 1$ is called **prime** if its only divisors are 1 and itself.
Numbers which are not prime are called **composite**.
What's so special about prime numbers?
Why should I care about them?

Here's Why

Lemma

Every natural number $n > 1$ is divisible by a prime.

Theorem (The Fundamental Theorem of Arithmetic)

Every natural number > 1 can be factored uniquely into a product of primes.

Lemma (Euclid's Lemma)

If a prime p divides ab, then p divides one of a or b.

Where do the Primes Live?

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23,
24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43,
44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63,
64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83,
84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102,
103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117,
118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132,
133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147,
148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162,
163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177,
178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192,
193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207,
208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222,
223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237,
238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, ...

Primes are Everywhere!

Theorem (Infinitude of Primes)

There are infinitely many prime numbers.

Theorem (Bertrand's Postulate)

For every natural number $n > 1$, there is some prime p satisfying $n < p < 2n$.

Theorem (Dirichlet's Theorem on Arithmetic Progressions)

If $gcd(a, d) = 1$, then the arithmetic progression $(a + nd)_{n \in \mathbb{N}}$ contains infinitely many primes.

Primes are Nowhere!

Theorem

For every natural number $n > 1$, there is a sequence of n consecutive composite natural numbers.

Here is such a sequence (of length $n - 1$):

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

because each $n! + k$ is divisible by k.

Theorem (Primes are Density 0)

If P denotes the set of prime numbers, then

$$\lim_{N \to \infty} \frac{|P \cap [1, N]|}{N} = 0.$$

So... How do the Primes Distribute?

Define the **prime counting function**

$$\pi(x) = \#\{p \leq x \mid p \text{ is prime}\} = \sum_{\substack{p \leq x \\ p \text{ is prime}}} 1 = \sum_{n \leq x} \delta_{n \text{ is prime}}.$$

In other words, $\pi(x)$ is the number of integers less than x which are prime.
Notice that we must clearly have $\pi(x) \leq x$.
From what we have already seen, we know that $\lim_{x \to \infty} \pi(x) = \infty$.
But how quickly does this function grow to infinity? Is it linear?
Logarithmic? What's the deal?

We have an Answer

$$\text{We write } f(x) \sim g(x) \text{ if } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Theorem (The Prime Number Theorem)

$$\pi(x) \sim x/\log(x)$$

But how do we prove that? What methods exist? Give it some thought.

Analysis?

Define the Riemann Zeta function to be

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

Notice this forms an absolutely convergent series on the region $\Re(s) > 1$.

What does ζ have to do with Primes?

The Euler Product!

$$\begin{aligned}
\zeta(s) &= \prod_{p \text{ is prime}} \frac{1}{1-p^{-s}} \\
&= \prod_{p} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots\right) \\
&= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \dots\right)\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \dots\right)\dots \\
&= \sum_{n=1}^{\infty} \frac{1}{n^s}
\end{aligned}$$

Sum over Primes?

Take a logarithm! If we define

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

then we obtain

$$\log(\zeta(s)) = \sum_p \log\left(\frac{1}{1-p^{-s}}\right) = \sum_p \sum_{k\in\mathbb{N}} \frac{1}{kp^{ks}} = \sum_{n\in\mathbb{N}} \frac{\Lambda(n)}{\log(n)} \cdot \frac{1}{n^s}.$$

Differentiating, this gives

$$\frac{\zeta'}{\zeta}(s) = -\sum_{n\in\mathbb{N}} \frac{\Lambda(n)}{n^s}.$$

Analytic Continuation

We need to extend the Zeta function to the rest of the complex plane.
This is known as **analytic continuation**.

Theorem (Analytic Continuation)

Suppose $U \subseteq V \subseteq \mathbb{C}$ and $f : U \to \mathbb{C}$ is analytic. If there are two analytic maps $F, G : V \to \mathbb{C}$ for which $F|_U \equiv f \equiv G|_U$, then we must have $F \equiv G$ on all of V.

Integral Representation of ζ

Define $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$, then one can easily show

$$\frac{\Gamma(s)}{n^s} = \int_0^\infty x^{s-1}e^{-nx}dx, \quad \text{which implies} \quad \zeta(s) = \frac{1}{\Gamma(s)}\int_0^\infty \frac{x^{s-1}}{e^{x-1}}dx.$$

Applying integration by parts, we can obtain an extension of ζ to the half plane $\Re(s) > 0$. Doing it again, we get $\Re(s) > -1$, then $\Re(s) > -2$, and so on.

We get a **meromorphic** function on $\mathbb{C}$, with only one simple pole at $s = 1$.

The Functional Equation, Critical Strip

The integral representation of ζ and Poisson summation yields

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

This implies that $\zeta(-2n) = 0$ for $n \in \mathbb{N}$ (called the **trivial zeros**).

If we take for granted that ζ has no zeros on the line $\Re(s) = 1$, then all nontrivial zeros of ζ are in the region $0 < \Re(s) < 1$.

The Residue Theorem

Theorem (The Residue Theorem)

Let $U \subseteq \mathbb{C}$ be simply connected and open, and $f : U \to \mathbb{C}$ a meromorphic function with poles at points $\{a_1, \ldots, a_n\} \subset U$. Then if γ is a positively oriented, simple closed curve in U, we have that

$$\int_\gamma f(z)dz = 2\pi i \sum_{a_k \in encl(\gamma)} Res(f, a_k),$$

where $Res(f, a_k)$ = the -1^{st} coefficient in the Laurent series expansion for f centered at a_k.

The Critical Calculation

Via our earlier characterization of ζ'/ζ, we can show

$$\sum_{p^k \leq x} \log(p) = \sum_{n \leq x} \Lambda(n) = \int_{c-i\infty}^{c+i\infty} \frac{\zeta'}{\zeta}(s) \cdot \frac{x^s}{s} ds.$$

But now, applying the residue theorem, we can also calculate that

$$\int_{c-i\infty}^{c+i\infty} \frac{\zeta'}{\zeta}(s) \cdot \frac{x^s}{s} ds = x + \sum_{\zeta(\rho)=0} \frac{x^\rho}{\rho} - \log(2\pi).$$

The Punchline

If we set $\psi(x) = \sum_{p^k \leq x} \log(p)$, we have

$$\psi(x) = x + \sum_{\zeta(\rho)=0} \frac{x^\rho}{\rho} - \log(2\pi).$$

As long as $\Re(\rho) < 1$ for every ρ a zero of ζ, we obtain $\psi(x) \sim x$.
But now, for every $\epsilon > 0$, we can show

$$\frac{\psi(x)}{x} \leq \pi(x) \cdot \frac{\log(x)}{x} \leq \frac{1}{1-\epsilon} \cdot \frac{\psi(x)}{x} + \frac{\log(x)}{x^\epsilon},$$

and therefore taking $\epsilon \to 0$, $x \to \infty$, the squeeze theorem yields

$$\pi(x) \sim x / \log(x).$$

A Better Formula and Error Terms

We write $f(x) = O(g(x))$ if there is $C > 0$ such that $|f(x)| \leq Cg(x)$ for all x sufficiently large. It is true that

$$Li(x) = \int_2^x \frac{1}{\log(t)} dt \sim \frac{x}{\log(x)},$$

and this turns out to be a better approximation for $\pi(x)$ than $x/\log(x)$.
In particular, it is known that

$$\pi(x) = Li(x) + O\left(x \cdot e^{-a\sqrt{\log(x)}}\right)$$

Here's a natural question: how much can this error bound be improved?

The Riemann Hypothesis

Conjecture (The Riemann Hypothesis)

All the nontrivial zeros s of the ζ function have $\Re(s) = 1/2$.

The immediate implication is that $|\pi(x) - Li(x)| \leq C \cdot \sqrt{x}\log(x)$.

Open Problems

Conjecture (The Twin Prime Conjecture)

There are infinitely many prime numbers p for which $p + 2$ is also prime.

Conjecture (The Goldbach Conjecture)

Every even number > 2 can be written as the sum of two primes.

Conjecture (Legendre's Conjecture)

There is a prime between any two consecutive squares.

Other Amazing Results!

Theorem (Green-Tao)

There are arbitrarily long arithmetic progressions in the primes.
That is, for every $n \in \mathbb{N}$, there is some even $k \in \mathbb{N}$ and $p \in \mathbb{N}$ such that all of $p, p+k, p+2k, \ldots, p+nk$ are prime.

Theorem (Ternary/Weak Goldbach)

Every odd natural number $n > 5$ can be expressed as the sum of three primes.

Theorem (Bounded Gaps Between Primes)

There is a fixed $N \in \mathbb{N}$ such that there are infinitely many pairs of primes p, q for which $|p - q| \leq N$.

Connection to My Research

For ergodic systems $T : X \to X$, it is known that orbits equidistribute,

Theorem (Birkhoff Ergodic Theorem)

Suppose $T : X \to X$ is ergodic with respect to μ and $f \in L^1(X)$. For μ-a.e. $x \in X$, we have that

$$\frac{1}{n}\sum_{k=0}^{n-1} f(T^k x) \overset{n\to\infty}{\longrightarrow} \int_X f d\mu.$$

But what if we study orbits along subsequences of $\mathbb{N}$? Along primes?

The End