

Prime Number Theorem I

Nikhil Srivastava

December 2, 2015

In the next two lectures I'll present a rough sketch of the proof of the prime number theorem. I will focus on a few key ideas and skip many (substantial) technical details. The point is not to give you a full proof (which would take several weeks), but to demonstrate some of the methods we have learned in the course.

Euclid proved that there are infinitely many primes. But you can ask more refined questions, such as: what percentage of the integers are prime? How rare are the primes? Apart from being very natural, such questions have applications in cryptography, where most schemes are based on generating very large primes.

For a positive real x , let $\pi(x)$ denote the number of primes less than or equal to x . The Prime Number Theorem, proven by Hadamard and de la Vallée Poussin in 1896, says that

$$\pi(x) \sim \frac{x}{\log x},$$

where \sim means asymptotic to, i.e.

$$f \sim g \Leftrightarrow \lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1.$$

1 Euler's Product Formula

For the rest of the lecture we will use Riemann's notation $s = \sigma + it$ instead of $z = x + iy$. The Riemann Zeta Function is defined as:

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

This definition makes sense because the series is absolutely convergent for $\operatorname{Re}(s) > 1$. Moreover, the series is uniformly convergent in every strip $\operatorname{Re}(s) \geq a > 1$. This means that it defines an analytic function in $\operatorname{Re}(s) > 1$ (we will extend this to almost the entire complex plane next time).

The reason this function is related to primes is the following formula due to Euler:

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1} \quad \operatorname{Re}(s) > 1,$$

where the right hand side is an infinite product, interpreted as a limit of partial products. To see why this formula holds, we observe that

$$\prod_{p \leq N} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \leq N} (1 + p^{-s} + p^{-2s} \dots) = \sum_{k_1, \dots, k_N} (p_1^{k_1} p_2^{k_2} \dots p_N^{k_N})^{-s} = \sum_{n \text{ product of } p \leq N} \frac{1}{n^s}.$$

The key is that by the unique factorization property, each integer appears exactly once on the right hand side. If you tried to do this with any other set of integers, you would double count. Taking a limit gives the formula (you will see another way to do this in the homework).

The product formula already tells us some interesting things about the primes, for instance, that the number of primes is infinite. If it were finite, $\zeta(2)$ would be rational, but we know it is irrational.

It also tells us something about the zeros of ζ , namely that $\zeta(s) \neq 0$ whenever $\text{Re}(s) > 1$. Since the infinite sum converges uniformly the infinite product also converges uniformly, and by Hurwitz' theorem the limit cannot have any zeros in the set $\text{Re}(s) > 1$ since each finite product does not.

2 A Discontinuous Integral

We are interested in the function $\pi(x) = \sum_{p \leq x} 1$. We will now show how to write such a sum as a certain integral of the zeta function. The first step is to turn the product over primes in Euler's identity into a sum by taking a logarithmic derivative:

$$\begin{aligned} -\frac{d}{ds} \log \zeta(s) &= \frac{d}{ds} \log \prod_p (1 - 1/p^s) \\ &= \frac{d}{ds} \sum_p \log(1 - 1/p^s) \\ &= \sum_p \frac{d}{ds} \log(1 - 1/p^s) \quad \text{by uniform convergence} \\ &= \sum_p \frac{\log(p)(1/p^s)}{1 - 1/p^s} \\ &= \sum_p \sum_k \frac{\log(p)}{p^{ks}} \\ &= \sum_n \frac{\Lambda(n)}{n^s}, \end{aligned}$$

where $\Lambda(n)$ is the von Mangoldt function:

$$\Lambda(n) = \begin{cases} \log(p) & p \text{ is a prime power} \\ 0 & \text{otherwise} \end{cases}.$$

This is not quite the prime function but it isn't that far – the logarithm is a very slowly varying function. It turns out that if we can our hands on $\sum_{n \leq x} \Lambda(n)$ there is a way to remove the $\log(p)$ weights as well as the contribution from the prime powers (which I will explain later), yielding $\pi(x)$. There are currently two issues to doing this: the sum we have right now is over all the integers, not just the integers upto x , and there's this n^s term which unlike the log seems like it's actually going to screw up the weighting substantially.

Both issues are handled by the same device. So far we've many times gone from partial sums to infinite sums by taking a limit, but complex analysis offers us a way to go in the other direction

as well. For instance, you know that you can extract coefficients of a Taylor or Laurent series by computing an integral. This is something like that but for a series which is not a power series.

The key observation is that when $c > 0$:

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{y^s}{s} ds$$

equals zero when $y > 1$ and one when $y < 1$. This is a simple exercise involving contour integration which you will do in the homework (or maybe you have already done). Thus, if we multiply both sides of the above identity by y^s/s and integrate term by term, we are able to extract only those terms of the series where $n < x$:

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} ds = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \sum_n \frac{\Lambda(n)}{n^s} \frac{x^s}{s} ds.$$

At this point I would like to take the integral inside the sum, and I can almost do it because the sum does converge uniformly in a strip containing the contour of integration. But it actually doesn't work because the contour of integration is infinite, and the usual uniform convergence/ML estimate argument only works for finite contours. There is a (rather technical) way to show that you can still swap the sum and the integral; I will skip this and just write:

$$\int_{c-i\infty}^{c+i\infty} -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} ds = \sum_n \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \Lambda(n) (x/n)^s \frac{1}{s} ds = \sum_{n < x} \Lambda(n).$$

We now move on to showing that removing the weights and throwing away the prime powers doesn't really change anything. The main claim is:

$$\text{If } \sum_{n < x} \Lambda(n) \sim x \text{ then } \pi(x) \sim \frac{x}{\log x}.$$

Proof. There are two steps here. The first is that $\Lambda(n)$ is counting not just primes but prime powers. The second is that these primes (and powers) are being counted with weights that are $\log(p)$. We will now show that both of these introduce changes that are negligible if all we are interested in doing is showing that $\pi(x) \sim x/\log(x)$.

First, we have

$$\sum_{p^k < x} \Lambda(x) = \sum_{p < x} \log(p) + \sum_{p^2 < x} \log(p) + \dots$$

The latter term is at most $\sqrt{x} \log(x)$, and there are at most $\log(x)$ terms, so the total contribution is $\sqrt{x} \log^2 x = o(x)$. So we have

$$\sum_{n < x} \Lambda(n) + o(x) = \sum_{p < x} \log(p) =: \psi(x).$$

We will now remove the weights. Observe that if we had just reweighted the primes by $\log(x)$ then we would be done. The intuition is that most of the contribution comes from primes where the weight is really close to $\log(x)$ anyway. In particular:

$$\psi(x) = \sum_{p < x/\log^2 x} \log p + \sum_{x > p > x/\log^2 x} \log(p)$$

is at least

$$0 + (\pi(x) - \pi(x/\log^2 x))(\log x - \log \log(x) - \log(2))$$

and at most

$$x/\log(x) + (\pi(x) - \pi(x/\log^2 x))\log(x).$$

Rearranging we get

$$\frac{\psi(x) - x/\log(x)}{\log(x)} \leq \pi(x) - \pi(x/\log^2 x) \leq \frac{\psi(x)}{\log x - \log \log(x) - \log(2)}.$$

Taking a limit as $x \rightarrow \infty$ gives

$$\pi(x) - \pi(x/\log^2 x) \sim \frac{x}{\log(x)}$$

Since $\pi(x/\log^2 x) \leq x/\log^2 x = o(x)$ we can ignore it and we get what we wanted. \square

The upshot is that if we can show that the integral

$$\frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} -\frac{\zeta'}{\zeta}(s) \frac{x^s}{s} ds$$

is asymptotic to x then we are done. We will sketch how to do this next time by defining an analytic continuation of ζ to the entire complex plane minus a pole at $s = 1$, and then applying the residue theorem.