

# Lecture # 1: Euler factorization, the $\zeta$ -function, and the distribution of primes.

Noah Snyder

June 24, 2002

## 1 Some Elementary Results on the Distribution of Primes

The beginning of Analytic Number Theory can be traced to a paper of Euler's. His investigations began with one of the oldest and most important questions in number theory: "How many primes are there?" For example, on average how many primes are in a given interval of the integers? How far can this distribution vary from the average? How random is this distribution?

A few of these questions can be answered with completely elementary methods. For example, it is easy to see that sequences of the form  $(n! + 2, n! + 3, n! + 4, \dots, n! + n)$  show that there are arbitrarily long gaps between prime numbers. In contrast is the following result due to Euclid:

**Theorem 1.1 (Euclid).** *There are infinitely many primes.*

*Proof.* Suppose there were finitely many primes,  $p_1, p_2, \dots, p_n$ . Then consider the number

$$Q = p_1 \cdots p_n + 1.$$

Clearly this number is not divisible by any prime. But it is also bigger than 1 and so (by descent) must be divisible by some prime. This is a contradiction, therefore there must be infinitely many primes.  $\square$

Although this method is certainly adequate to show that there are infinitely many primes, it does not seem to show that there are very many primes, because  $Q$  is a relatively large number compared to  $p_n$ . To quantify such questions of how the primes distributed, we introduce the following functions:

**Definition 1.2.** *Let  $\pi(x)$  be the number of positive primes less than or equal to  $x$ . Let  $p_n$  be the  $n$ th positive prime.*

Euclid's result, therefore, says that  $\lim_{x \rightarrow \infty} \pi(x) = \infty$ , or, alternately, that  $p_n$  is actually defined for all positive  $n$ . On the other hand, the result on composites mentioned above says that  $\limsup_{n \rightarrow \infty} p_n - p_{n-1} = \infty$ , or, alternately, that for any  $n$ ,  $\pi(x+n) = \pi(x)$  for infinitely many  $x$ .

It will also be very useful to have good notation for approximating the growth of functions.

**Definition 1.3.** *We say that  $f(x) = g(x) + O(h(x))$  if  $\frac{f(x)-g(x)}{h(x)}$  is bounded as  $x \rightarrow \infty$ . We say that  $f(x) = g(x) + o(h(x))$  if  $\frac{f(x)-g(x)}{h(x)}$  goes to zero as  $x \rightarrow \infty$ . We say that  $f(x) \sim g(x)$  if  $\frac{f(x)}{g(x)}$  goes to 1 as  $x \rightarrow \infty$ .*

Occasionally we will also use these same notations for different limit points (usually as  $x$  approaches 0 or 1). Notice that  $f(x) \sim g(x)$  is the same as saying  $f(x) = g(x) + o(g(x))$ . Also notice that  $\sim$  (which is called asymptotic equality) is an equivalence relation.

A closer look at Euclid's result allows us to get slightly stronger information on the growth of  $\pi(x)$  and  $p_n$ .

**Proposition 1.4.**  $p_n < e^{e^n}$ . Hence,  $\pi(x) > \log \log x$ .

*Proof.* This theorem is obvious if  $n = 1$ . If  $n > 1$ , Euclid's construction actually says that

$$p_n \leq p_1 \cdot p_2 \cdots p_{n-1} + 1 \leq k p_1 \cdot p_2 \cdots p_{n-1}$$

for any  $\frac{7}{6} < k$ . Combining the first  $n$  such equations, we see that:

$$p_n \leq k p_1 \cdot p_2 \cdots p_{n-1} \leq k^2 (p_1 \cdots p_{n-2})^2 \leq k^4 (p_1 \cdots p_{n-3})^4 \leq \dots \leq (2k)^{(2^n)}.$$

Clearly we can pick  $k$  such that  $2k < e$ . □

This result shows that, for example, there are at least 2 primes smaller than 100 or that there are at least 3 primes less than 10,000. This is clearly a horrible underestimate as  $\pi(100) = 25$  and  $\pi(10,000) = 1,229$ .

There are other classical proofs of the infinitude of primes based on similar constructive methods which give similar bounds. For example, consider Goldbach's proof of Proposition 1.4:

Consider the Fermat numbers,  $F_n = 2^{2^n} + 1$ . Fermat claimed that these were all prime, but Euler found a counterexample. However, they can still be used to prove the infinitude of primes because of the following lemma:

**Lemma 1.5.**  $\gcd(F_n, F_m) = 1$  so long as  $n$  and  $m$  are distinct.

*Proof.* Without loss of generality, take  $n < m$ . Suppose some prime  $p$  divides both  $F_n$  and  $F_m$ . Then  $-1 \equiv 2^{2^n} \pmod{p}$  and  $-1 \equiv 2^{2^m} \pmod{p}$ . Squaring the first equation  $m - n$  times shows that  $1 \equiv 2^{2^m} \pmod{p}$ , which contradicts the second equation (clearly  $p$  must be odd since all the Fermat numbers are odd). Therefore, all the Fermat numbers are pairwise relatively prime. □

Now we can conclude another proof of Proposition 1.4 using this lemma. If all the Fermat numbers were relatively prime, then each must be divisible by a different prime from all the others. So,  $p_n \leq F_n = 2^{2^n} + 1$ . Thus, we have  $\pi(x) > \log \log x$ .

**Challenge 1.** Find other elementary proofs of the prime number theorem and see if any of them give a substantively better bound on the growth of  $\pi$ .

## 2 Euler Factorization

Obviously we would like to find a much better lower bound for  $\pi(x)$  than  $\log \log x$ . The first proof of the infinitude of primes which allows us a substantively better bound is Euler's proof which can be found in his book *Introduction to Analysis of the Infinite*. Here he actually shows that  $\sum_{p \text{ prime}} 1/p$  diverges.

Since  $\sum_{n=1}^{\infty} e^{-e^n}$  clearly converges extremely rapidly, Euler's result will give us a substantively better estimate on the growth of  $\pi(x)$ . Furthermore, the argument itself is exceptional because it does not use constructive algebraic arguments like Euclid's and Goldbach's, but rather an argument based on the properties of a certain analytic function. Euler argued as follows:

"Let us consider the expression

$$\frac{1}{(1 - \alpha z)(1 - \beta z)(1 - \gamma z) \cdots}$$

"When the division is carried out, we obtain the series  $1 + Az + Bz^2 + Cz^3 + \dots$ . It is clear that the coefficients  $A, B, C$ , etc. depend on the numbers  $\alpha, \beta, \gamma$ , etc. in the following way:  $A$  is the sum of the numbers taken singly;  $B$  is the sum of the products taken two at a time;  $C$  is the sum of the products taken three at a time, etc., where we do not exclude products of the same factor.

"If for  $\alpha, \beta, \gamma$ , etc. we substitute the reciprocals of some power of all the primes and let

$$P = \frac{1}{\left(1 - \frac{1}{2^n}\right) \left(1 - \frac{1}{3^n}\right) \left(1 - \frac{1}{5^n}\right) \cdots},$$

then  $P = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \dots$ , where all natural numbers occur with no exception.

“Because we can express the sum of the series  $P = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n} + \dots$  as a product of factors, it is convenient to use logarithms. We have

$$\log P = -\log\left(1 - \frac{1}{2^n}\right) - \log\left(1 - \frac{1}{3^n}\right) - \log\left(1 - \frac{1}{5^n}\right) - \dots$$

“If we use natural logarithms, then

$$\log P = 1\left(\frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{5^n} + \dots\right) + \frac{1}{2}\left(\frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{5^{2n}} + \dots\right) \dots$$

“If  $n = 1$ , then  $P = 1 + \frac{1}{2} + \frac{1}{3} + \dots = \log\left(\frac{1}{1-1}\right) = \log(\infty)$ . Then

$$\log \log \infty = 1\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots\right) + \frac{1}{2}\left(\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{5^2} + \dots\right) + \dots$$

“But these series, except for the first ones, not only have finite sums, but the sum of all of them taken together is still finite, and reasonably small. It follows that the first series  $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \dots$  has an infinite sum.” (Chapter XV of Euler’s *Introduction to the Analysis of the Infinite*.)

As is to be expected, Euler’s argument lacks rigor at a few points, but in this case the questionable steps are easy to identify and deal with. First we need to place the series which he discusses on a firmer foundation.

**Proposition 2.1.** *The series*

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

*converges uniformly on the interval  $[c, \infty)$  for any  $c > 1$ .*

*Proof.* Since  $n^{-s}$  is monotonically decreasing for positive  $s$ , for any  $N$  and  $M$  and any  $s \geq c > 1$ ,

$$\sum_{n=N}^M n^{-s} \leq \int_N^{\infty} x^{-s} dx = \frac{N^{1-s}}{s-1} < \frac{1}{c-1},$$

which shows uniform convergence. □

The key step in Euler’s proof is the following fact known as the Euler factorization of the zeta function.

**Proposition 2.2.** *The product  $\prod_p \frac{1}{1-p^{-s}}$  converges uniformly on the interval  $[c, \infty)$  for any  $c > 1$ . (Here as always we use the notation  $\prod_p$  (resp.  $\sum_p$ ) to denote a product (resp. sum) over all positive primes.) Furthermore for  $s > 1$ ,*

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

*Proof.* The important points are that  $\frac{1}{1-p^{-s}} = \sum_{k=0}^{\infty} p^{-ks}$  and that every positive integer factors uniquely as a product of prime powers. We consider the finite product,

$$\prod_{p < N} \sum_{k=0}^{\infty} p^{-ks} = \sum_{n \in S_N} n^{-s},$$

where  $S_N$  is the set of all integers which are products of primes less than  $N$ . But clearly  $[1, N) \subseteq S_N$ . Therefore,

$$\left| \prod_{p < N} \sum_{k=0}^{\infty} p^{-ks} - \sum_{n < N} n^{-s} \right| = \varepsilon(N, s) < \sum_{n > N} n^{-s} < sN^{1-s}. \quad (2.1)$$

Since the right hand side goes to zero as  $N$  gets large, uniformly on the interval  $[c, \infty)$  for any  $c > 1$ , our theorem is proved. □

These two results combine to give us the key formula in the middle of Euler's argument:

$$\log \zeta(s) = \sum_p -\log \left(1 - \frac{1}{p^s}\right). \quad (2.2)$$

Using the Taylor expansion for  $\log$  is legitimate here because  $0 < 1 - \frac{1}{p^s} < 1$ , and we can exchange the order of summation because all the series involved converge uniformly and absolutely. Therefore, we find that

$$\begin{aligned} \log \zeta(s) &= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^n s} = \sum_{n=1}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s} \\ &= \sum_p \frac{1}{p^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s}. \end{aligned} \quad (2.3)$$

Thus far we have simply been rephrasing Euler's arguments in the language of modern analysis. The point where we need to do extra work is at the end. Essentially, we want to take the limit as  $s \rightarrow 1$ . Then the left hand side blows up, while the right hand side consists of the series we're interested in plus some finite part. But, unlike Euler, we can not say the left hand side is  $\log \log \infty$ .

We can, however, still conclude that

$$\lim_{s \rightarrow 1^+} \sum_p \frac{1}{p^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s}$$

cannot be finite.

First, we want to show that the terms with  $k > 1$  on the right hand side of Equation 2.3 are small under the same limit. This is just another simple integral test:

$$\begin{aligned} \sum_{n=2}^{\infty} \frac{1}{n} \sum_p \frac{1}{p^n s} &< \int_2^{\infty} \int_2^{\infty} x^{-1} y^{-sx} dy dx = \int_2^{\infty} s^{-1} x^{-2} 2^{-sx} dx \\ &< \frac{1}{4s} \int_2^{\infty} 2^{-sx} dx = \frac{1}{8s^2} 2^{-2s} < \frac{1}{32}. \end{aligned}$$

So clearly the sum of the rest of the series converges in the limiting case, just as Euler claimed. This implies that  $\lim_{s \rightarrow 1^+} \sum_p \frac{1}{p^s}$  cannot be finite.

**Theorem 2.3 (Euler).**  $\sum_p \frac{1}{p}$  diverges.

*Proof.* For the sake of contradiction, suppose that  $\lim_{N \rightarrow \infty} \sum_{p < N} p^{-1}$  were actually finite. Then  $\sum_{p > N} p^{-1}$  would give a uniform bound on the term  $\sum_{p > N} \frac{1}{p^s}$ . Hence,  $\sum_p \frac{1}{p^s}$  would converge uniformly for all  $s \geq 1$ .

Thus the interchange of limits would be valid, and

$$\lim_{N \rightarrow \infty} \sum_{p < N} \frac{1}{p^{-1}} = \lim_{N \rightarrow \infty} \lim_{s \rightarrow 1^+} \sum_{p < N} \frac{1}{p^{-s}} = \lim_{s \rightarrow 1^+} \lim_{N \rightarrow \infty} \sum_{p < N} \frac{1}{p^{-s}} = \lim_{s \rightarrow 1^+} \sum_p \frac{1}{p^s}$$

would also be finite. This is clearly a contradiction.  $\square$

This proves the theorem which Euler set out to prove. Already this result shows powerful things such as,  $p_n$  grows faster on average than  $n^r$  does for any  $r > 1$ . However, Euler claimed something

stronger. Not only did he say that  $\sum_p \frac{1}{p}$  diverged, he claimed that it was  $\log \log \infty$ . By this expression Euler seems to mean, in modern notation, that

$$\sum_{p < N} \frac{1}{p} = \log \log N + O(1).$$

In order to prove this result using Euler's methods, we would simply have to show that the Euler factorization was approximately valid for a finite sum and  $s = 1$ , i.e.

$$\left| \prod_{p < N} \frac{1}{1 - p^{-1}} - \sum_{n < N} n^{-1} \right| < \varepsilon(N, 1)$$

for some nice error function. Alas, a little computation shows that this claim is not true at all. Our computation in Theorem 2.2 shows that the error function  $\varepsilon(N, s)$  does not behave well as  $s \rightarrow 1$ .

In order to prove this result we will need a bit more information about the  $\zeta(s)$  near  $s = 1$ . For many of Euler's papers in which he considers the Euler factorization and functions like his  $\zeta$ -function, rather than considering the series,  $\zeta(s) = \sum_n n^{-s}$ , he instead looks at an alternating series:

**Definition 2.4.**  $\tilde{\zeta}(s) = \sum_n (-1)^{n+1} n^{-s}$ .

This new series has the distinct advantage of converging (conditionally) for all  $s > 0$  by the alternating series test. If we group terms in pairs, then the series actually converges absolutely for all  $s > 0$ .

This new function also has an Euler factorization:

$$\begin{aligned} \tilde{\zeta}(s) &= \sum_n (-1)^n n^{-s} = (1 - 2^{-s} - 4^{-s} - \dots)(1 + 3^{-s} + 9^{-s} - \dots)(1 + 5^{-s} + 25^{-s} - \dots) \dots \\ &= \left(2 - \frac{1}{1 - 2^{-s}}\right) \prod_{p \neq 3} \left(\frac{1}{1 - p^{-s}}\right). \end{aligned} \quad (2.4)$$

This factorization is very similar to that of the old  $\zeta$ -function. In fact, we have the formula

$$\zeta(s) = \frac{\frac{1}{1 - 2^{-s}}}{2 - \frac{1}{1 - 2^{-s}}} \tilde{\zeta}(s) = \frac{1}{2 - 2^{1-s} - 1} \tilde{\zeta}(s) = \frac{1}{1 - 2^{1-s}} \tilde{\zeta}(s).$$

This new expression for  $\zeta(s)$  now makes sense for any  $s > 0$  except for  $s = 1$  where it clearly blows up. This lets us get a much firmer grasp on the behavior of  $\zeta$  near 1.

**Theorem 2.5.** (cf. Janusz's *Number Fields*, pp. 144-145)

$$\lim_{s \rightarrow 1} (s - 1)\zeta(s) = 1.$$

*Proof.* If we write

$$(s - 1)\zeta(s) = \frac{s - 1}{1 - 2^{1-s}} \tilde{\zeta}(s),$$

the limit as  $s \rightarrow 1$  actually makes sense. By a standard result from analysis,  $\lim_{s \rightarrow 1} \tilde{\zeta}(s) = \log 2$ . By L'hôpital's rule,

$$\lim_{s \rightarrow 1} \frac{s - 1}{1 - 2^{1-s}} = \frac{1}{\log 2}.$$

Thus,  $\lim_{s \rightarrow 1} (s - 1)\zeta(s) = 1$ . □

Therefore, by Theorem 2.5, if we consider the series

$$(1 - s)\zeta(s) = \sum_n \frac{1 - s}{n^s},$$

it will converge uniformly in  $s$  for  $s \in [1, \infty)$ . Hence the error term  $(1 - s)\varepsilon(N, s)$  actually does remain bounded as  $s \rightarrow 1$ . Thus we have shown,

**Lemma 2.6.**

$$\lim_{s \rightarrow 1} (1-s) \left| \prod_{p < N} \frac{1}{1-p^{-1}} - \sum_{n < N} n^{-s} \right| < \lim_{s \rightarrow 1} \varepsilon(N, s) < \varepsilon(N),$$

for some error function  $\varepsilon(N)$  which goes to zero as  $N$  gets large.

□

**Theorem 2.7.**

$$\sum_{p < N} \frac{1}{p} = \log \log N + O(1).$$

*Proof.* By the lemma for all  $N$  and  $s > 1$ ,

$$(s-1) \prod_{p < N} \frac{1}{1-p^{-1}} = (s-1) \sum_{n < N} n^{-s} + O(1),$$

where by  $O(1)$  we mean the error is bounded as  $N \rightarrow \infty$  and as  $s \rightarrow 1^+$ . If we take logs of both sides and use an earlier lemma,

$$\log(s-1) + \sum_{p < N} p^{-s} = \log(s-1) + \log \sum_{n < N} n^{-s} + O(1).$$

Now we can cancel the  $\log(1-s)$  terms and the terms we are left with are all bounded as  $\lim_{s \rightarrow 1}$ . Thus,

$$\sum_{p < N} \frac{1}{p} = \log \sum_{n < N} n^{-1} + O(1) = \log \log N + O(1).$$

□

Clearly it follows that there are infinitely many primes. In fact, we can extract from this theorem a very good idea of how fast  $\pi(x)$  and  $p_n$  grow.

We will extend  $p_n$  to some monotonic real valued function  $p_x$  to get

$$\int_1^X \frac{1}{p_x} dx = \log \log X + O(1). \tag{2.5}$$

We would really like to “differentiate” this equation to get something like

$$\frac{1}{p_x} \approx \frac{d}{dx} \log \log x = \frac{1}{\log x} \frac{1}{x}.$$

This would imply that  $p_x \approx x \log x$ . However, although integrating preserves estimates, differentiating clearly does not. (For example, consider the fact that  $x \sin x = O(x)$ , but  $\sin x + x \cos x = \frac{d}{dx} x \sin x \neq O(1)$ .)

What this does tell us though is that  $p_n$  can not grow *significantly faster* than  $n \log n$ . Similarly, we can see that  $\pi(x)$  can not grow significantly slower than  $\frac{x}{\log x}$ .

This phrase “significantly faster” (resp. slower) can mean any of a number of things, for example,

**Proposition 2.8.** For any constant  $k > 1$  and  $N$ , there exists some  $n > N$ ,  $p_n \geq kn \log n$ .

*Proof.* Suppose to the contrary that for some constants  $k < 1$  and  $N$ ,  $p_n < kn \log n$  for all  $n > N$ . Thus, if  $n > N$ ,

$$\frac{1}{p_n} < \frac{1}{k n \log n}.$$

Integrating yields

$$\sum_{N < n < x} \frac{1}{p_n} < \frac{1}{k} (\log \log x - \log \log N)$$

for all  $x > N$ . But by Equation 2.5, this means that for some constant  $c$ ,

$$\log \log x < c - \frac{1}{k}(\log \log N) + \frac{1}{k}(\log \log x).$$

Since  $k > 1$ , this last equation is clearly false for large enough  $x$ . □

To show a more concrete result, like  $p_n \sim n \log n$ , one would need to prove something stronger about the smoothness of  $p_n$ .

It is worth noting that simply showing that there are infinitely many primes does not require any of the above arguments. We can simply note that if there were finitely many primes, then, by looking at the supposed finite Euler factorization,  $\lim_{s \rightarrow 1} \zeta(s)$  would be finite.

Throughout this course we will try to emulate Euler's argument, by finding a connection between number theoretic information and analytic functions and then extracting more and more number theoretic information from better and better results concerning these analytic functions.