Chapter 1 Two Proofs of the infinitude of Primes 2018-19

v1 [**3** lectures]

One method to show there are infinitely many primes is to start with a sequence $\{a_n\}_{n\geq 1}$ of real numbers such that $a_n \neq 0$ if n is prime and $a_n = 0$ if n is not prime, i.e. composite. If $\sum_{n\leq N} a_n \to \infty$ as $N \to \infty$ then there must be infinitely many primes. Thus we are led to estimating sums and a fundamental idea is to replace the sum by an integral. One way this is achieved is by applying the **important** idea that, for an integrable function f,

$$\operatorname*{glb}_{[a,b]} f(t)\,(b-a) \leq \int_a^b f(t)\,dt \leq \operatorname*{lub}_{[a,b]} f(t)\,(b-a)\,. \tag{1}$$

With $[a,b] = [n, n+1]$, $n \in \mathbb{Z}$, this gives

$$\operatorname*{glb}_{[n,n+1]} f(t) \leq \int_n^{n+1} f(t)\,dt \leq \operatorname*{lub}_{[n,n+1]} f(t)\,.$$

If f is *decreasing* then $\operatorname{glb}_{[n,n+1]} f(t) = f(n+1)$ while $\operatorname{lub}_{[n,n+1]} f(t) = f(n)$ and we get

$$f(n+1) \leq \int_n^{n+1} f(t)\,dt \leq f(n)\,. \tag{2}$$

Lemma 1.1 *For all integers $N \geq 1$,*

$$\int_1^{N+1} f(t)\,dt \leq \sum_{n=1}^{N} f(n) \leq f(1) + \int_1^N f(t)\,dt. \tag{3}$$

Proof For the lower bound in (3) sum the upper inequality in (2) over $n = 1, ..., N$. For the upper bound in (3) sum the lower inequality in (2) over $n = 1, ..., N-1$ and then change the variable of summation from n to $n+1$, though still calling it n. ■

1.2 First Proof

Corollary 1.2 *The sum over the reciprocal of integers n satisfies*

$$\log(N+1) \leq \sum_{1\leq n\leq N} \frac{1}{n} \leq \log N + 1.$$

Proof This follows immediately from Lemma 1.1 with $f(t) = 1/t$. ■

For our proof of the infinitude of primes we will require the following lemma. Recall that the Taylor Series for $-\log(1-x)$ is

$$x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + ...$$

for $|x| < 1$. Thus we might expect x to be a good first approximation to $-\log(1-x)$. The following result quantifies how good an approximation.

Lemma 1.3 *For $0 < x < 1$ we have*

$$0 < -\log(1-x) - x < \frac{x^2}{(1-x)}.$$

Proof For $0 < x < 1$ we have

$$-\log(1-x) = \int_{1-x}^{1} \frac{dt}{t}.$$

As seen in (1)

$$\operatorname*{glb}_{[a,b]} f(t)\,(b-a) \leq \int_a^b f(t)\,dt \leq \operatorname*{lub}_{[a,b]} f(t)\,(b-a).$$

In the present case this gives

$$x < \int_{1-x}^{1} \frac{dt}{t} < \frac{x}{1-x},$$

i.e.

$$x < -\log(1-x) < \frac{x}{1-x},$$

Hence

$$0 < -\log(1-x) - x < \frac{x}{1-x} - x = \frac{x^2}{1-x}.$$

■

Theorem 1.4 *The sum over the reciprocals of primes p satisfies*

$$\sum_{p \leq N} \frac{1}{p} > \log\log(N+1) - 1$$

for $N \geq 2$.

Letting $N \to \infty$ proves that the series $\sum_p 1/p$ diverges which it can only do if it contains a infinite number of terms, i.e. we have an infinitude of primes.

Proof Let

$$\mathcal{N} = \{n \in \mathbb{N} : p|n \Rightarrow p \leq N\}.$$

Note that $1 \in \mathcal{N}$ since there are no primes which divide 1 and so the condition is trivially satisfied.

Another way of writing $\mathcal{N}$ is to list all the primes up to N as $p_1 < p_2 < ... < p_r \leq N$. By the **prime factorisation of integers** every $n \in \mathcal{N}$ can be written as $p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ for some $a_i \geq 0 \ \forall \, 1 \leq i \leq r$ while, conversely, every product $p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ with $a_i \geq 0$ is an element of $\mathcal{N}$. Hence

$$\mathcal{N} = \{p_1^{a_1} p_2^{a_2} ... p_r^{a_r} : a_i \geq 0 \ \forall \, 1 \leq i \leq r\}.$$

Next by **unique** factorisation into prime there is no $n \in \mathcal{N}$ which is represented by two different products $p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$. Thus we get the first equality in

$$\begin{aligned} \sum_{n \in \mathcal{N}} \frac{1}{n} &= \sum_{a_i \geq 0 \ 1 \leq i \leq r} \frac{1}{p_1^{a_1} p_2^{a_2} ... p_r^{a_r}} \\ &= \prod_{i=1}^{r} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \frac{1}{p_i^3} + ...\right) \end{aligned} \tag{4}$$

To see this last equality multiply the product out, taking from each bracket a term of the form $1/p_i^{a_i}$ for some $a_i \geq 0$. Multiplying them together gives a term of the form

$$\prod_{i=1}^{r} \frac{1}{p_i^{a_i}} = \frac{1}{\prod_{i=1}^{r} p_i^{a_i}} = \frac{1}{n},$$

with $n \in \mathcal{N}$.

The result (4) can be written more succinctly as

$$\sum_{n \in \mathcal{N}} \frac{1}{n} = \prod_{p \leq N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ...\right). \tag{5}$$

This IMPORTANT RESULT encapsulates the **unique factorization of integers**. Next each sum in a bracket in (5) is a geometric series and can be summed to

$$\frac{1}{1 - 1/p} = \left(1 - \frac{1}{p}\right)^{-1}.$$

Thus

$$\sum_{n\in\mathcal{N}} \frac{1}{n} = \prod_{p\leq N} \left(1-\frac{1}{p}\right)^{-1}. \tag{6}$$

Importantly If $n \leq N$ then all prime divisors p of n satisfy $p \leq n \leq N$ thus $n \in \mathcal{N}$. That is,

$$n \leq N \implies n \in \mathcal{N} \quad \text{or, equivalently,} \quad \mathcal{N} \supseteq \{1 \leq n \leq N\}.$$

Hence

$$\sum_{n\leq N} \frac{1}{n} \leq \sum_{n\in\mathcal{N}} \frac{1}{n}. \tag{7}$$

Therefore, combining (6), (7) and Corollary 1.2 we obtain

$$\log(N+1) \leq \prod_{p\leq N} \left(1-\frac{1}{p}\right)^{-1}.$$

Take logarithms to get

$$\log\log(N+1) \leq \sum_{p\leq N} -\log\left(1-\frac{1}{p}\right). \tag{8}$$

After Lemma 1.3 above we might consider $1/p$ a good approximation to $-\log(1-1/p)$. For this reason we write

$$\sum_{p\leq N} -\log\left(1-\frac{1}{p}\right) = \sum_{p\leq N} \frac{1}{p} + \sum_{p\leq N} \left(-\log\left(1-\frac{1}{p}\right) - \frac{1}{p}\right). \tag{9}$$

Apply Lemma 1.3 with $x = 1/p$ which is $\leq 1/2$ since primes satisfy $p \geq 2$. Then

$$0 < -\log\left(1-\frac{1}{p}\right) - \frac{1}{p} < \frac{(1/p)^2}{1-1/p} = \frac{1}{p(p-1)}.$$

So

$$0 < \sum_{p\leq N} \left(-\log\left(1-\frac{1}{p}\right) - \frac{1}{p}\right) < \sum_{p\leq N} \frac{1}{p(p-1)} < \sum_{2\leq n\leq N} \frac{1}{n(n-1)},$$

replacing the sum over primes by a larger sum over **all** integers. Note how this latter sum starts at $n = 2$ and **not** 1, because the smallest prime is 2.

Continue using partial fractions

$$\begin{aligned}
\sum_{2\leq n\leq N}\frac{1}{n\left(n-1\right)} &= \sum_{2\leq n\leq N}\left(\frac{1}{n-1}-\frac{1}{n}\right)\\
&= \left(\frac{1}{1}-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\left(\frac{1}{3}-\frac{1}{4}\right)+...\\
&\quad ...+\left(\frac{1}{N-2}-\frac{1}{N-1}\right)+\left(\frac{1}{N-1}-\frac{1}{N}\right)\\
&= 1-\frac{1}{N}, \qquad \text{by cancellation,}\\
&< 1. \qquad (10)
\end{aligned}$$

We say that the sum has "telescoped down", the second term in a bracket cancelling the first term in the next. Thus

$$0<\sum_{p\leq N}\left(-\log\left(1-\frac{1}{p}\right)-\frac{1}{p}\right)<1.$$

Putting this into (9) we find that

$$\sum_{p\leq N}-\log\left(1-\frac{1}{p}\right)<\sum_{p\leq N}\frac{1}{p}+1.$$

By (8) we get

$$\log\log\left(N+1\right)<\sum_{p\leq N}\frac{1}{p}+1,$$

which rearranges to

$$\sum_{p\leq N}\frac{1}{p}>\log\log\left(N+1\right)-1,$$

as required. ■

1.3 The Riemann zeta function

The First Proof of the infinitude of primes was straightforward since we only consider *finite* products (over $p\leq N$) and related *finite* sums (over $n\leq N$) to *finite* integrals. In the next proof we have *infinite* products and relate *infinite* sums to *infinite* integrals.

Definition 1.5 *The **Riemann zeta-function** is defined by*

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

for all $s \in \mathbb{C}$ for which the series converges.

For $s \in \mathbb{C}$ it is standard in this subject area to use the notation $s = \sigma + it$, with σ, $t \in \mathbb{R}$. (Strange to be mixing Greek, σ, with Roman, t, but blame Riemann and his 1859 paper.)

Note that $n^s = n^{\sigma+it}$. Here $n^{it} = e^{it \log n}$. Yet $\left|e^{i\theta}\right| = 1$ for all θ so $\left|e^{it \log n}\right| = 1$ for all $n \geq 1$ and thus

$$|n^s| = \left|n^{\sigma+it}\right| = |n^\sigma| \left|e^{it \log n}\right| = n^\sigma.$$

Example 1.6

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2}$$

is known to converge.

It can be shown, i.e. by Complex Analysis or Fourier Series, that

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6},$$

and this result will be used throughout the course with no further comment.

For $s \in \mathbb{R}$, i.e. a **real** variable we have

Theorem 1.7 *For $s = \sigma$ **real**, the series defining $\zeta(\sigma)$ diverges for all $\sigma \leq 1$ and converges for all $\sigma > 1$ with*

$$\frac{1}{\sigma - 1} \leq \zeta(\sigma) \leq \frac{1}{\sigma - 1} + 1.$$

Proof If $\sigma \leq 0$ then the terms of the series defining $\zeta(\sigma)$ satisfy $1/n^\sigma > 1$, in particular they do not tend to 0 as $n \to \infty$ and so the series cannot converge, i.e. it diverges.

Assume $\sigma > 0$. Lemma 1.1 with $f(u) = 1/u^\sigma$ gives

$$\int_1^{N+1} \frac{du}{u^\sigma} \leq \sum_{n=1}^{N} \frac{1}{n^\sigma} \leq 1 + \int_1^N \frac{du}{u^\sigma},$$

for all $N \geq 1$. Thus

$$\frac{1}{1-\sigma}\left((N+1)^{1-\sigma} - 1\right) \leq \sum_{n=1}^{N} \frac{1}{n^\sigma} \leq 1 + \frac{1}{1-\sigma}\left(N^{1-\sigma} - 1\right), \qquad (11)$$

for $\sigma \neq 1$.

First Case $0 < \sigma \leq 1$**.** If $\sigma = 1$ then, since by Corollary 1.2, $\sum_{n \leq N} 1/N > \log(N+1)$ which tends to ∞ as $N \to \infty$, we deduce that $\sum_{n=1}^{\infty} 1/n$ diverges.

If $0 < \sigma < 1$ then $1 - \sigma > 0$ and so $(N+1)^{1-\sigma} \to \infty$ as $N \to \infty$. Then the left hand inequality of (11) shows that the partial sums of $\sum_{n=1}^{\infty} 1/n^\sigma$ diverge, and so the infinite sum diverges.

Second case $\sigma > 1$**.** Simplify the second inequality in (11) as

$$\sum_{1}^{N} \frac{1}{n^\sigma} \leq 1 + \frac{1}{\sigma - 1}\left(1 - N^{1-\sigma}\right) \leq 1 + \frac{1}{\sigma - 1},$$

using $N > 0$. Then the sequence of partial sums $\sum_{n \leq N} 1/n^\sigma$ is an increasing sequence (positive terms $1/n^\sigma$ are added as N increases) bounded above. Thus, by a first year analysis result, the *sequence of partial sums* converges, which is the definition that the *series* $\zeta(\sigma)$ converges. Also

$$\zeta(\sigma) \leq 1 - \frac{1}{1-\sigma}. \qquad (12)$$

Next, $1 - \sigma < 0$ so $(N+1)^{1-\sigma} \to 0$ as $N \to \infty$. So, in the limit, the first inequality in (11) gives

$$\zeta(\sigma) \geq -\frac{1}{1-\sigma} = \frac{1}{\sigma - 1}. \qquad (13)$$

Combine (12) and (13) to give the displayed conclusion. ■

Note that for **complex** $s = \sigma + it$ Theorem 1.7 says that $\zeta(s)$ converges *absolutely* for $\operatorname{Re} s > 1$ because, for such s,

$$\sum_{n=1}^{\infty}\left|\frac{1}{n^s}\right| = \sum_{n=1}^{\infty}\frac{1}{n^\sigma} = \zeta(\sigma)\,.$$

But if $s = \sigma + it$ with $0 < \sigma \leq 1$ and $t \neq 0$, the Theorem does **not** tell us that $\zeta(s)$ diverges. We will have to wait until later in the course to see that this is the case.

1.4 Infinite Products

Definition 1.8 *Let $\{u_n\}_{n\geq 1}$ be a sequence of complex numbers. Let $p_n = u_1u_2...u_n$ for each n.*

*If the sequence of partial products $\{p_n\}_{n\geq 1}$ converges to a **non-zero** limit p say, as $n \to \infty$, we say that the infinite product $\prod_{r=1}^{\infty} u_r$* **converges to** *p.*

If a finite number of the factors u_n equal 0 and the infinite product obtained by removing these factors converges we say that the infinite product $\prod_{r=1}^{\infty} u_r$ **converges to** *0.*

Otherwise we say that the product is **divergent**.

Thus a convergent infinite product is zero if at least one of its factors is zero.

Assumption If $\{u_n\}_{n\geq 1}$ contains a *finite* number of zeros these are removed and the remaining terms relabeled. That is we are assuming $u_n \neq 0$ for all n. This means we are **only** considering infinite products that converge to a non-zero value.

I will assume without proof the two results.

Unproved Result 1 *If $\prod_{n=1}^{\infty} u_n$ converges, then the product of inverses, $\prod_{n=1}^{\infty} u_n^{-1}$, converges.*

Unproved Result 2 *If the **series** $\sum_{n=1}^{\infty} |a_n|$ is convergent (where the a_n are real or complex and $a_n \neq -1$ for all n, then the **infinite product** $\prod_{n=1}^{\infty}(1 + a_n)$ converges in that the limit*

$$\lim_{N\to\infty}\prod_{n=1}^{N}(1 + a_n)$$

*exists and is **non-zero**.*

This will be applied in examples where the a_n are zero when n is non-prime. We are then assuming that if $\sum_p |a_p|$ is convergent then $\prod_p (1 + a_p)$

is convergent.

Proofs of both results can be found in Appendix C of *The Prime Number Theorem* by G.J.O. Jameson, Pub. London Mathematical Society, Student Text 13, 2003. It can also be found in the Appendix on my web site.

For $s \in \mathbb{C}$, i.e. a **complex variable,** we have

Example 1.9 *For* $\operatorname{Re} s > 1$ *the infinite product*

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

converges and is non-zero.

Solution Assume $\operatorname{Re} s > 1$. Use again the fact that an infinite series over primes of positive terms is less than the series over **all** integers, i.e.

$$\sum_p \left|-\frac{1}{p^s}\right| = \sum_p \frac{1}{p^\sigma} \leq \sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \zeta(\sigma)\,.$$

Thus the series $\sum_p |-1/p^s|$ converges and so, by our Result 2 above, the infinite product

$$\prod_p \left(1 + \left(-\frac{1}{p^s}\right)\right)$$

is convergent for $\operatorname{Re} s > 1$. Then, by the Result 1,

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

converges. ■

For **real** $s > 1$ this result is due to L. Euler, 1737, and for this reason:

Definition 1.10 *Infinite products over primes are known as* ***Euler Products****.*

The product seen in Example 1.9 is often referred to as **the** Euler Product because of

Theorem 1.11 *For* ***complex*** s *satisfying* $\operatorname{Re} s > 1$

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

Proof Let $N > 1$ and $\mathcal{N}$ as seen in the proof of Theorem 1.4. The exponent of s makes no differences to the arguments seen in the proof of Theorem 1.4 and so, by the unique factorization of integers, we have

$$\prod_{p \le N} \left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n \in \mathcal{N}} \frac{1}{n^s}.$$

Consider

$$\left|\zeta(s) - \prod_{p \le N} \left(1 - \frac{1}{p^s}\right)^{-1}\right| = \left|\sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n \in \mathcal{N}} \frac{1}{n^s}\right| = \left|\sum_{n \notin \mathcal{N}} \frac{1}{n^s}\right|.$$

Next we will take the modulus into the series, allowable since the resulting series is convergent as the subsequent argument will show. Thus

$$\left|\sum_{n \notin \mathcal{N}} \frac{1}{n^s}\right| \le \sum_{n \notin \mathcal{N}} \left|\frac{1}{n^s}\right| = \sum_{n \notin \mathcal{N}} \frac{1}{n^\sigma}.$$

Recalling $\mathcal{N} \supseteq \{1, 2, ..., N\}$ we see that $n \notin \mathcal{N}$ implies $n \ge N + 1$. Hence

$$\begin{aligned} \sum_{n \notin \mathcal{N}} \frac{1}{n^\sigma} &\le \sum_{n \ge N+1} \frac{1}{n^\sigma} \\ &\le \sum_{n \ge N+1} \int_{n-1}^{n} \frac{du}{u^\sigma} = \int_N^\infty \frac{du}{u^\sigma} = \frac{1}{(\sigma - 1)\, N^{\sigma - 1}}. \end{aligned}$$

Therefore

$$\left|\zeta(s) - \prod_{p \le N} \left(1 - \frac{1}{p^s}\right)^{-1}\right| \le \frac{1}{(\sigma - 1)\, N^{\sigma - 1}}.$$

Let $N \to \infty$ when the bound here tends to 0 since $\sigma > 1$. This means we have again shown that the infinite product converges but now we know the limit is $\zeta(s)$. ■

Corollary 1.12 *For* $\operatorname{Re} s > 1$

$$\zeta(s) \neq 0.$$

Proof From Example 1.9 we see that the Euler product for $\zeta(s)$ converges which means by definition of convergence for infinite products that the Euler product is non-zero. Thus by Theorem 1.11 we have $\zeta(s) \neq 0$ for $\operatorname{Re} s > 1$. ■

An advert for a substantial part of this course is that we will later prove $\zeta(s) \neq 0$ for $\operatorname{Re} s \geq 1$. This may not look much of an improvement but the fact that $\zeta(s) \neq 0$ for $\operatorname{Re} s = 1$ is equivalent to the Prime Number Theorem, another major result of this course.

1.5 Second Proof

We now come to the promised second proof of the infinitude of primes which is by way of giving a lower bound on the infinite series $\sum_p 1/p^\sigma$.

Theorem 1.13 *For real* $\sigma > 1$

$$\sum_p \frac{1}{p^\sigma} \geq \log\left(\frac{1}{\sigma - 1}\right) - 1.$$

Letting $\sigma \to 1+$ the right hand side diverges and so the limit as $\sigma \to 1+$ of the sum over primes must be infinite. If there were only finite many primes then the limit of the finite sum would be finite, contradiction. Hence there must be infinitely many primes.

Proof Recall that $n \leq N \Rightarrow n \in \mathcal{N}$, so

$$\sum_{1 \leq n \leq N} \frac{1}{n^\sigma} \leq \sum_{n \in \mathcal{N}} \frac{1}{n^\sigma} = \prod_{p \leq N} \left(1 - \frac{1}{p^\sigma}\right)^{-1},$$

as seen in the previous proof for complex s in place of the real σ. Take logarithms,

$$\begin{aligned} \log\left(\sum_{1 \leq n \leq N} \frac{1}{n^\sigma}\right) &\leq \log \prod_{p \leq N} \left(1 - \frac{1}{p^\sigma}\right)^{-1} = \sum_{p \leq N} -\log\left(1 - \frac{1}{p^\sigma}\right) \\ &= \sum_{p \leq N} \frac{1}{p^\sigma} + \sum_{p \leq N} \left(-\log\left(1 - \frac{1}{p^\sigma}\right) - \frac{1}{p^\sigma}\right). \end{aligned} \tag{14}$$

By Lemma 1.3 with $x = 1/p^\sigma$ we have

$$\begin{aligned} 0 &\leq \sum_{p\leq N}\left(-\log\left(1-\frac{1}{p^\sigma}\right)-\frac{1}{p^\sigma}\right) \leq \sum_{p\leq N}\frac{1}{p^\sigma\left(p^\sigma-1\right)} \\ &\leq \sum_{n=2}^{N}\frac{1}{n^\sigma\left(n^\sigma-1\right)} \leq \sum_{n=2}^{N}\frac{1}{n\left(n-1\right)} \qquad \text{since } \sigma > 1 \\ &\leq 1, \end{aligned}$$

for all $N \geq 1$, as seen in an earlier proof. Hence the sum over primes converges and

$$0 \leq \sum_{p}\left(-\log\left(1-\frac{1}{p^\sigma}\right)-\frac{1}{p^\sigma}\right) \leq 1. \tag{15}$$

Let $N \to \infty$ in (14) . On the left hand side the continuity of log gives

$$\lim_{N\to\infty}\log\left(\sum_{1\leq n\leq N}\frac{1}{n^\sigma}\right) = \log\left(\lim_{N\to\infty}\sum_{1\leq n\leq N}\frac{1}{n^\sigma}\right) = \log\zeta(\sigma)$$

for $\sigma > 1$. Rearranging (14) gives

$$\lim_{N\to\infty}\sum_{p\leq N}\frac{1}{p^\sigma} = \log\zeta(\sigma) - \sum_{p}\left(-\log\left(1-\frac{1}{p^\sigma}\right)-\frac{1}{p^\sigma}\right).$$

That is, the sum over primes converges, and the lower bound in the Theorem follows from (15) and Theorem 1.7. ■

In later Chapters we will sharpen and generalise all these methods and results.