Chapter 2

Euclid's Theorem

Theorem 2.1. *There are an infinity of primes.*

This is sometimes called Euclid's Second Theorem, what we have called Euclid's Lemma being known as Euclid's First Theorem.

Proof. Suppose to the contrary there are only a finite number of primes, say

$$p_1, p_2, \ldots, p_r.$$

Consider the number

$$N = p_1 p_2 \cdots p_r + 1.$$

Then N is not divisible by p_i for $i = 1, \ldots, r$, since N has remainder 1 when divided by each of these primes.

Take any prime factor q of N. (We know from the Fundamental Theorem that there is such a prime.)

Then q differs from all of the primes $p_1, \ldots, p_r$, since it divides N.

Hence our assumption that the number of primes is finite is untenable. □

2.1 Variants on Euclid's proof

Proposition 2.1. *There are an infinite number of primes of the form*

$$p = 4n - 1.$$

Proof. Suppose there are only a finite number of such primes, say

$$p_1, p_2, \ldots, p_r.$$

Consider the number

$$N = 4p_1 p_2 \cdots p_r - 1.$$

Since N is odd, it is a product of odd prime factors.

Any odd number is of the form $4n + 1$ or $4n - 1$. If all the prime factors of N were of the form $4n + 1$ their product N would be of this form. Since it is not, we conclude that N has a prime factor of the form $4n - 1$.

This must differ from $p_1, \ldots, p_r$, since none of these primes divides N.

Hence we have a further prime of the form $4n - 1$, contradicting our original assumption. □

Rather suprisingly, perhaps, we cannot show in the same way that there are an infinity of primes of the form $4n + 1$, although that is true.

2.2 The zeta function

Having established that there are an infinity of primes, the question arises: How are these primes distributed? Riemann's zeta function is the major tool in this study.

Definition 2.1. *Riemann's zeta function $\zeta(s)$ is defined by*

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots,$$

when this series converges.

Although Riemann's name is given to this function, it was in fact introduced by Euler. However, Euler only considered the function for real s. Riemann's contribution was to consider the function for complex s, in a revolutionary paper "On the number of primes less than a given value", published in 1859, using the theory of complex functions laid down by Cauchy some 20 years before.

Note that the terms in the series can be defined, for real and complex s, by

$$n^{-s} = e^{-s \ln n}.$$

We see from this that

$$n^{-(x+iy))} = e^{-x \ln n}\, e^{-iy \ln n},$$

and so

$$|n^{-s}| = n^{-\Re(s)},$$

since $|e^{i\theta}| = 1$ for all real θ.

A simple but useful tool allows us to determine when the series converges.

Lemma 2.1. *If $f(x)$ is a monotone function then*

$$\sum f(n) \text{ converges} \iff \int^{\infty} f(x)dx \text{ converges.}$$

The lower limits on each side so not matter; it is sufficient that $f(x)$ is defined for $x \geq X$.

One might think it should be specified that $f(x)$ is continuous. But in fact any monotone function $f(x)$ is necessarily Riemann integrable (and so Lebesgue integrable). This follows from the fact that $f(x)$ has only an enumerable set of discontinuities, so the partitions in Riemann sums can be chosen with end-points avoiding these points.

Proof. We may assume (replacing $f(x)$ by $-f(x)$ if necessary) that $f(x)$ is decreasing. We may also assume that $f(x) \to 0$ as $x \to \infty$; for we know that $f(x)$ tends to a limit ℓ (possibly $-\infty$), and if $\ell \neq 0$ then it is easy to see that both sum and integral diverge.

If $n \leq x \leq n+1$ then

$$f(n) \leq f(x) \leq f(n+1).$$

Hence

$$f(n) \le \int_n^{n+1} f(x)dx \le f(n+1).$$

Thus

$$f(m)+f(m+1)+\cdots+f(n-1) \ge \int_m^n f(x)dx \ge f(m+1)+f(m+2)+\cdots+f(n),$$

from which the result follows. □

Proposition 2.2. *The series for $\zeta(s)$ converges for $\Re(s) > 1$.*

Proof. For real $s > 1$ this follows from the previous lemma, since

$$\int x^{-s}dx = -\frac{1}{s-1}x^{-(s-1)}.$$

And it follows from this that $\sum n^{-s}$ is absolutely convergent if $\Re(s) > 1$, since $|n^{-s}| = n^{-\Re(s)}$. □

2.3 Euler's Product Formula

If $a_1, a_2, \ldots$ is an infinite sequence of real of complex numbers, we say that the infinite product $a_1 a_2 \cdots$ converges to $\ell \neq 0$ if the partial products

$$A_n = a_1 a_2 \cdots a_n$$

converge to ℓ. (If $A_n \to 0$ then we say that the product *diverges* to 0.)

If the a_n are real and positive we can convert an infinite product to an infinite series by taking logarithms:

$$\prod a_n \text{ converges } \iff \sum \ln a_n \text{ converges.}$$

Because of this logarithmic connection we usually take the product in the form $\prod(1 + a_n)$. This allows us to pass to complex a_n provided $|(|a_n) < 1$, since in that case

$$\ln(1 + a_n) = a_n - \frac{1}{2}a_n^2 + \frac{1}{3}a_n^3 - \frac{1}{4}a_n^4 + \cdots .$$

Lemma 2.2. *Suppose $\sum a_n^2$ is absolutely convergent. Then*

$$\prod(1 + a_n) \text{ converges } \iff \sum a_n \text{ converges.}$$

In particular the product is convergent if the series is absolutely convergent.

Proof. Since

$$\begin{aligned}
|\frac{1}{2}a_n^2 - \frac{1}{3}a_n^3 + \frac{1}{4}a_n^4 - \cdots| & \\
&\le \frac{1}{2}|a_n|^2 + \frac{1}{3}|a_n|^3 + \frac{1}{4}|a_n|^4 + \cdots \\
&\le \frac{1}{2}\left(|a_n|^2 + |a_n|^3 + |a_n|^4 + \cdots\right) \\
&= \frac{1}{2}\,\frac{|a_n|^2}{1-|a_n|^2} \\
&\le |a_n|^2,
\end{aligned}$$

if $|a_n| \le 1/2$.

It follows that

$$|\ln \prod_M^N (1+a_n) - \sum_M^N a_n| \le \sum_M^N |a_n|^2$$

provided $|a_n| \le 1/2$ for $n \in [M, N]$, from which the result follows. □

Theorem 2.2. *For $\Re(s) > 1$,*

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

where the infinite product extends over all prime numbers p.

Proof. The formula can be written

$$1 + 2^{-s} + 3^{-s} + 4^{-s} + \cdots =$$
$$\left(1 + 2^{-s} + 2^{-2s} + \cdots\right)\left(1 + 3^{-s} + 3^{-2s} + \cdots\right)\left(1 + 5^{-s} + 5^{-2s} + \cdots\right)\cdots .$$

If $n = 2^{e_2}3^{e^3}5^{e_5}\cdots$ then

$$n^{-s} = 2^{-e_2 s}3^{-e^3 s}5^{-e_5 s}\cdots ;$$

and we see that n^{-s} on the left is matched by $2^{-e_2 s}$ from the first factor on the right, $3^{-e_3 s}$ from the second factor, and so on.

□

Theorem 2.3. *The series*

$$\sum \frac{1}{p}$$

(where p runs over the primes) diverges.

Proof. Taking $s = 1$ in the above formula, the series

$$\sum \frac{1}{n}$$

diverges. So the product

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

also diverges.

It follows that the inverse

$$\prod \left(1 - \frac{1}{p}\right) = 0,$$

ie the partial product

$$P_n = \prod_1^n \left(1 - \frac{1}{p}\right) \to 0$$

as $n \to \infty$.

We say that the infinite product 'diverges to 0'.

Taking logarithms, it follows that

$$\sum_p \log\left(1 - \frac{1}{p}\right) = -\infty.$$

Recall that

$$\log(1-x) = -x + x^2/2 - x^3/3 + \cdots .$$

If x is small, say $|x| < 1/2$, we can combine the second and later terms:

$$\begin{aligned} |x^2/2 - x^3/3 + \cdots| &\le x^2/2(1 + x + x^2 + \cdots) \\ &= \frac{x^2}{2(1-x)} \\ &\le x^2. \end{aligned}$$

Thus

$$\frac{1}{p} = -\log(1 - \frac{1}{p}) + a_p.$$

where $\sum a_p$ converges, since

$$|a_p| \le \frac{1}{p^2},$$

and $\sum 1/p^2$ converges with $\sum 1/n^2$.

We conclude that $\sum 1/p$ is the sum of a divergent series and a convergent series, and therefore diverges. □

Note that

$$\sum_p \frac{1}{p^r}$$

converges for $r > 1$, since

$$\sum_n \frac{1}{n^r}$$

converges (by comparison with the integral $\int 1/x^r$).

2.4 Dirichlet's Theorem

Theorem 2.4. *There are an infinity of primes in any arithmetic sequence*

$$a + dn \quad (n = 0, 1, 2, \dots)$$

with $d > 0$ *and* $\gcd(a, d) = 1$.