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 $p_1, \dots, p_r$, 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.

There is one other variant.

Proposition 2.2. *There are an infinite number of primes of the form*

$$p = 6n - 1.$$

The proof is left to the reader.

2.2 Euler's Product Formula

Consider the formal equation

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

This doesn't make sense as it stands, since everything is divergent. However, each term on the left corresponds to a finite product on the right. For example

$$12 = 2^2 \cdot 3 \cdot 1 \cdot 1 \cdots,$$

with 2^2 from the first sum on the right, 3 from the second, and 1 from the remainder.

But now raise each term to the power r:

$$1+2^r+3^r+4^r+\cdots = \left(1+2^r+(2^2)^r+\cdots\right)\left(1+3^r+(3^2)^r+\cdots\right)\left(1+5^r+(5^2)^r+\cdots\right)\cdots.$$

Again, each term on the left corresponds to a finite product on the right. At first sight this doesn't make any more sense.

However, r can be negative, eg if $r=-2$ the equation reads

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

This makes perfect sense; everything is convergent.

The series

$$1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\cdots$$

converges for $s > 1$. This can be seen by comparison with the integral

$$\int_2^\infty \frac{1}{x^s} dx.$$

For

$$\frac{1}{(n+1)^s} < \int_n^{n+1} \frac{1}{x^s} dx < \frac{1}{n^s}$$

and so

$$\int_1^n \frac{1}{x^s} dx < 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots + \frac{1}{n^s} < \int_1^{n+1} \frac{1}{x^s} dx,$$

from which the result follows.

(This is a very useful technique, which is often used in number theory: If $f(x) > 0$ and $f(x) \to 0$ as $x \to \infty$ then

$$\sum f(n) \text{ and } \int f(x) dx$$

converge or diverge together.)

Note that we can sum each of the geometric series on the right of the Product Formula:

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots = \left(1 - \frac{1}{p^s}\right)^{-1}$$

so that the Product Formula takes the form

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

Theorem 2.2. *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 $\int 1/x^r$).