Lecture 1: Proofs of Euclid’s Theorem

Scribe: Arnav Gupta
IIT Kanpur

Introduction

Prime numbers are one of the most important concepts of number theory. Being the building blocks of natural numbers, it is imperative for mathematicians to know about the basic concepts of prime numbers. The Euclid’s theorem is a theorem in mathematics which states that there are an infinite number of prime numbers. Euclid’s himself provided a proof for this theorem, and over the years many other proofs were proposed for the statement. In this lecture, we shall look at 3 proofs for the same.

1 Euclid’s Proof from ’the book’

This is the proof originally proposed by Euclid. We start off by assuming that there are a finite number of prime numbers. Let’s denote the set of these prime numbers by \( P \), i.e.

\[ P = \{ p_1, p_2, p_3, ..., p_n \} \]

Now, we consider the natural number \( N \), which is defined as the successor the product of all the primes, i.e.

\[ N = p_1p_2p_3...p_n + 1 \]

Now, \( N \) can either be prime or not be prime. If \( N \) is prime, we have \( \forall p_i \in P, N > p_i \). Hence we have found a ‘bigger’ prime not included in \( P \), which contradicts our assumption that there are a finite number of elements in \( P \).

The other case is that \( N \) is not prime. Then, there exists a prime \( p_k > 1 \) which divides \( N \). However, \( \forall p_i \in P \), we have \( 1 \equiv N \pmod{p_i} \). Hence, \( p_k \) is not in \( P \), so we have found a prime which has not been included in \( P \). Hence, we have arrived at a contradiction in this case too.

We can therefore conclude that there are an infinite number of primes by the above argument.

2 Proof by Fermat’s Little Theorem

By contradiction, assume that there are a finite number of primes. Then, let’s denote the largest prime number by \( p \).

Then, we consider the number \( n = 2^p - 1 \). We know that we can factorise any natural number, so let \( q \) be the largest prime number which divides \( n \). Since \( p \) is the largest prime number, we have \( q \leq p \).

Since \( p \) is prime, by Lagrange’s theorem it should be the smallest \( x \) so that \( 1 \equiv 2^x \pmod{q}, x \in \mathbb{N} \)

Also, Fermat’s Little Theorem tells us that if 2 and \( (q-1) \) are coprime, then

\[ 1 \equiv 2^{q-1} \pmod{q} \]

These observations tell us that \( p \) divides \( q - 1 \), \( \Rightarrow \) \( p \leq q - 1 \). However we have already shown earlier that \( q \leq p \), which is a contradiction.

Hence, our initial assumption of finite primes is incorrect, and there exist infinitely many primes.
3 Erdős’s proof

We will prove that the given series $S$ diverges. This will strongly prove that there are an infinite number of primes.

$$S = \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \ldots + \frac{1}{p_n}.$$ 

By contradiction, assume that $S$ converges. Then, Cauchy’s convergence criteria states that there exists an $m$ such that:

$$\sum_{i \geq k+1} \frac{1}{p_i} \leq \frac{1}{2}$$

Let’s consider a natural number $N$. We say that a number is 'big' if it has a prime factor greater than $P_m$, i.e.

$$\exists P_m \ m \geq k+1 \ and \ P_m | N$$

Let these numbers define a set $N_{\text{big}}$. Similarly, we say that a number is 'small' if all of its prime factors are less than $P_{k+1}$. Let these numbers define a set $N_{\text{small}}$. Then, it is easy to see that

$$|N_{\text{big}}| + |N_{\text{small}}| = N$$

Now, we shall prove that this equation will never be satisfied, and hence our initial assumption of assuming convergence was wrong. We have

$$|N_{\text{big}}| \leq \sum_{m \geq k+1} \frac{N}{P_m} \implies |N_{\text{big}}| \leq \frac{N}{2}$$

Now we only need to establish a tight upper bound on $N_{\text{small}}$. For $n \in N_{\text{small}}$, we can write

$$n = p_1^{a_1}p_2^{a_2}p_3^{a_3} \ldots p_k^{a_k}$$

Now, we say $n = a_n b_n^2$, where $a_n$ is constructed by taking the modulo 2 of all powers of the prime factors of $n$. It is easy to see that $\frac{n}{a_n}$ will be a perfect square, hence $b_n$ is defined as its square root.

Finally, we conclude that $|a_n| \leq 2^k$, since each prime in $a_n$ can either be present or not. We also have $|b_n| \leq \sqrt{N}$. Hence

$$|N_{\text{small}}| \leq 2^k \sqrt{N}.$$ 

Since we select $N, k$, we can choose $N$ to be sufficiently large so that

$$\frac{\sqrt{N}}{2} < 2^k$$

Using this, we obtain

$$|N_{\text{small}}| \leq 2^k \sqrt{N} \implies |N_{\text{small}}| < \frac{\sqrt{N}}{2} \times \sqrt{N} \implies |N_{\text{small}}| < \frac{N}{2}$$

So, we conclude $|N_{\text{big}}| + |N_{\text{small}}| < N$, which is a contradiction. Hence, we conclude that our original series $S$ diverges, and consequently there are an infinite number of primes.