Euclid, Euler, Erdős: Exploring the infinitude of the primes

June 20, 2024

Author: Ruben Riemens

Supervisor: Lola Thompson

A bachelor thesis in mathematics

Universiteit Utrecht

Contents

1 Introduction

Over 2000 years ago, famous mathematician Euclid proved in his famous *Elements*, that there exist infinitely many primes. Euclid's arithmetical proof then led to finding the lower bound $\pi(N) > \log(\log(N))$ for $N \geq 2$ where π is the prime counting function $\pi : \mathbb{N} \to \mathbb{N}$, which is given by

$$\pi(N) = \big|\{p \leq N \,:\, p \text{ is prime}\}\big|.$$

Eventually, it was proven independently by mathematicians Jacques Hadamard [6] and Charles Jean de la Vallée Poussin [7] that, in asymptotic notation,

$$\pi(N) \sim \frac{N}{\log{(N)}}.$$

This then tells us that given an arbitrary integer N, the probability that it is prime is given by the limit

$$\lim_{N\to\infty} \frac{\pi(N)}{N} = \lim_{N\to\infty} \frac{1}{\log(N)} = 0,$$

so it follows that while they are infinite, the prime numbers have asymptotic density equal to zero.

A different proof of the infinitude of the prime numbers was an analytical proof written by Leonhard Euler [1], from which we can find as a corollary that the sum running over all primes p

$$\sum_p \frac{1}{p}, \tag{1}$$

is in fact an infinite series. It can then be shown that it diverges. Using Euler's approach to proving the infinitude of the primes and the divergence of (1), we can once again find that for $N \geq 2$, we have that $\pi(N) > \log(\log(N))$ [1].

A third remarkable proof of the infinitude of primes was given by Hungarian mathematican Paul Erdős [1] [5]. This proof uses a combinatorial argument, and while not being the first proof of that nature, it is the first proof of the sharper lower bound for π of

$$\pi(N) \geq \log(N)/(2\log(2)),$$

making Erdős' proof stand out from the previously mentioned ones.

As of 2024, there are roughly 200 different proofs of the infinitude of the primes [8]. The aim of this thesis will be to look at proofs of the infinitude of primes that are either similar to Euclid's, Eulers or Erdős'. That is: the Euclid-like proofs all have an arithmetical argument, the Euler-like proofs all make use of facts from analysis, and the Erdős-like proofs all use ideas from of combinatorics.

We will delve deeper into how these proofs relate to each other, and see a number of creative approaches to proving the infinitude of the primes.

2 Euclid-like arithmetic proofs

In this chapter, we will look at a variety of proofs that share the arithmetic nature which we see in Euclid's original proof of the infinitude of primes. For each proof, we will discuss its similarity to Euclid's proof. We will see proofs where this link takes relatively little work to spot, such as Stieltjes' [9], and see more involved comparisons as we move along the proofs. Eventually we will find a generalized method of categorizing proofs which work by constructing infinite sequences of coprime integers. We start of by recalling what Euclid's proof looks like, and then move on to different proofs.

2.1 Euclid's proof

We first state the following lemma from elementary number theory:

Lemma 2.1. *Any integer that is not equal to* ± 1 *has a prime divisor.*

Throughout this chapter, we will use this property of the integers repeatedly. We will now commence with Euclid's proof:

Theorem 2.2. *There are infinitely many prime numbers.*

Proof. Suppose, for contradiction, that there are only k distinct prime numbers, say $p_1, \ldots, p_k$. Now consider the integer

$$N = 1 + \prod_{i=1}^{k} p_i.$$

Note that for all $1 \leq i \leq k$, we know that $p_i \mid \prod_{i=1}^{k} p_i$. As such, if $p_i \mid N$ we must also have that $p_i \mid 1$, which is never true. It follows that $p_i \nmid N$ for all $1 \leq i \leq k$.

However, since every integer not equal to ± 1 has at least one prime divisor, and $N > 1$, N must have a prime divisor p. We conclude that p is a prime number which is not in our original list, which is a contradiction since we assumed there are precisely k prime numbers.

□

The main argument we see in Euclid's proof is that if there were finitely many prime numbers, doing some arithmetic construction we find out that there exists some integer which has a prime divisor not in our original finite set of prime numbers, which leads to a contradiction. In the following proof done by Stieltjes, we see a very similar argument being used.

2.2 Stieltjes' proof

Proof. Suppose $p_1, \ldots, p_k$ is a finite set of distinct prime numbers and let $AB = p_1 \cdots p_k$ be any factorization of their product. Since AB is squarefree, note that none of the p_i divide both A and B since otherwise p_i^2 would have to divide AB. As such, none of the p_i divide the sum $A + B$, so it has a prime divisor which is not in our original list.

□

As mentioned earlier, even at a glance Stieltjes' proof feels very similar to Euclid's. This becomes especially apparent when we realize we can set $A = 1, B = p_1 \cdots p_k$, in which case we get that $A + B = 1 + p_1 \cdots p_k$. This particular choice of A and B leads to the exact same argument as the one we saw in Euclid's proof.

2.3 Eulers second proof

The following proof is the second proof Euler gave on the infinitude of primes. It uses the fact that the Euler totient function is multiplicative.

Proof. Let $p_1, \ldots p_k$ be any finite list of primes. Since we know that there are at least 2 prime numbers, namely 2 and 3, we can assume without loss of generality that $k \geq 2$. Let φ denote the Euler totient function. Using the multiplicative property of φ we get that

$$\varphi(\prod_{i=1}^{k} p_i) = \prod_{i=1}^{k} \varphi(p_i) = \prod_{i=1}^{k} (p_i - 1).$$

Since we assumed $k \geq 2$ our list of primes contains at least $k-1$ prime numbers which are greater than 2. As such, we have that

$$\prod_{i=1}^{k} (p_i - 1) \geq 2^{k-1} \geq 2,$$

so there exists at least one integer n which is greater than 1 which is coprime to $\prod_{i=1}^{k} p_i$. As such, n has a prime divisor which is coprime to $\prod_{i=1}^{k} p_i$, so we have found a prime number which is not equal to one of $p_1, \ldots, p_k$, from which we can conclude that there are infinitely many prime numbers.

□

To see why this proof is similar to Euclid's, lets take a deeper look at its main punchline. This of course is the result that there exists at least one integer n which is less than and coprime to

$$\prod_{i=1}^{k} p_i.$$

The proof is in essence a slight abstraction of Euclid's argument. Instead of constructing a specific integer which is relatively prime to all primes in the original list, Euler's proof shows that such an integer should exist without giving a specific example.

We can find an explicit example of a possible n that Euler's second proof is alluding to, namely

$$n = -1 + \prod_{i=1}^{k} p_i.$$

This is only a sum of 2 apart from the integer we constructed in Euclid's proof, which goes to show that in the end the argument used in Euler's proof is closely related to Euclid's.

2.4 Furstenberg's topological proof

We will first state Furstenberg's topological proof on the theorem. Afterwards, we will be discussing its similarity to Euclid's well-known elementary number theory proof of the same theorem by exploring an argument given by mathematician Keith Conrad [2].

Before giving Furstenberg's proof, we define the following topology on $\mathbb{Z}$:

We say $U \subseteq \mathbb{Z}$ is open if one of the following holds:

(i) U is the empty set

(ii) For all $a \in U$ there exists an integer $m \geq 1$ such that the *arithmetic progression*

$$a + m\mathbb{Z} := \{a + m \cdot c \,|\, c \in \mathbb{Z}\}$$

is fully contained in U.

Equivalently, we say that U is open if it is empty, or if it can be written as a union of arithmetic progressions. We show that this indeed defines a topology on $\mathbb{Z}$:

1. The empty set and $\mathbb{Z}$ are open:

   The empty set is open by (i), and $\mathbb{Z}$ is open since we can write $\mathbb{Z} = 0 + 1 \cdot \mathbb{Z}$, so it satisfies property (ii).

2. Arbitrary unions of opens are open:

   Let $\{U_i\}_{i \in I}$ be some collection of opens in $\mathbb{Z}$. Pick $a \in \bigcup_{i \in I} U_i$ arbitrarily. Then $a \in U_j$ for some $j \in I$, so there exists an integer $m \geq 1$ such that

$$a + m\mathbb{Z} \subseteq U_j \subseteq \bigcup_{i \in I} U_i,$$

   which is what we wanted to show.

3. Finite intersections of opens are open:

   Let $U_1, \ldots, U_k$ be a finite amount of opens in $\mathbb{Z}$. Observe that if $\bigcap_{i=1}^{k} U_i = \emptyset$, it is open by (i) so we can assume without loss of generality that $\bigcap_{i=1}^{k} U_i \neq \emptyset$. Now pick $a \in \bigcap_{i=1}^{k} U_i$ arbitrarily. Then it follows that for all $i = 1, \ldots, k$ we have some integer $m_i \geq 1$ such that $a + m_i\mathbb{Z} \subseteq U_i$. It follows that $a + m_1 \cdot m_2 \cdots m_k\mathbb{Z} \subseteq U_i$ for all $i = 1, \ldots, k$, so we have that

$$a + m_1 \cdot m_2 \cdots m_k\mathbb{Z} \subseteq \bigcap_{i=1}^{k} U_i,$$

   which is what we wanted to show. We conclude that properties (i) and (ii) define a topology on $\mathbb{Z}$.

Remarks:

a) All non-empty opens in $\mathbb{Z}$ are infinite sets. This follows from the fact that they contain at least one arithmetic progression, which is an infinite set.

b) Arithmetic progressions are both open and closed in $\mathbb{Z}$. The proof of this remark goes as follows:

   Let $a + m\mathbb{Z}$ be some arithmetic progression, then it can be written as the union of arithmetic progressions (namely $a + m\mathbb{Z}$ itself) so it is open.

   Now to show it is closed, note that the complement of $a + m\mathbb{Z}$ is precisely the union of all arithmetic progressions $r + m\mathbb{Z}$ where $1 \leq r \leq m$ and $r \not\equiv a \mod m$, which by the first part of our argument is the union of opens and therefore open.

Furstenberg's proof

Proof. Consider the following union:

$$V := \bigcup_{p \text{ is prime}} p\mathbb{Z}.$$

Note that each individual $p\mathbb{Z}$ is closed in $\mathbb{Z}$ by remark b). By the unique prime divisor property of the integers, we then have that

$$\bigcup_{p \text{ is prime}} p\mathbb{Z} = \mathbb{Z} - \{\pm 1\}$$

so its complement is equal to $\{\pm 1\}$. By remark a), this set is not open since it is a finite non-empty set. This implies that V is not closed.

Since the finite union of closed sets is closed, V can not be a finite union, so there must be infinite prime numbers.

□

Furstenberg's proof mostly makes use of the properties of arithmetic progressions, while the biggest argument made with use of topology is that finite unions of closed sets are closed. We analyze this particular claim further.

To verify that $\bigcup_{i=1}^{k} p_i\mathbb{Z}$ is closed, we need to show its complement

$$I := \bigcap_{i=1}^{k} (\mathbb{Z} - p_i\mathbb{Z}) = \{a \in \mathbb{Z} : p_i \nmid a, i = 1, \dots, k\}$$

is open. Note that this set contains ± 1, which implies it is non-empty. Now this implies we can pick a from the complement arbitrarily. Since $p_1, \dots, p_k$ all don't divide a, this implies that all the p_i don't divide any of the elements of $a + p_1 \cdots p_k\mathbb{Z}$ either, from which we conclude the complement is open, so I is closed.

The main idea behind Furstenberg's proof is that for a finite amount of prime numbers, the intersection I contains arithmetic progressions which makes it open, while the set $\{\pm 1\}$ can not be open due to contradiction with remark a). Now, since we know that $1 \in I$, so is the arithmetic progression $1 + p_1 \cdots p_k\mathbb{Z}$. In other words, the complement of all multiples of prime numbers I can not be equal to $\{\pm 1\}$ since it contains numbers of the form $1 + p_1 \cdots p_k c$ for $c \in \mathbb{Z}$. When choosing $c = 1$, we see that this argument is the exact same as the one that is made in Euclid's proof, so we conclude that they are in fact very similar proofs.

It turns out that Furstenberg's proof of the infinitude of primes, though seemingly unique at first, is in fact a reinterpretation of Euclid's classical proof. After going through the motions of defining a topology on $\mathbb{Z}$, in the end we never ended up needing any arguments that can only be made using topology. Instead, we found that by making small observations to the part of the proof which uses topology, it reveals the same argument as the on from Euclid's proof.

2.5 Goldbach's proof

In the following sections we will be looking at proofs which a priori use a slightly different, approach when compared to Euclid's proof. The first of these proofs we will be going over is Goldbach's [9]. We will eventually see that even though Goldbach's proof may seem to take a different approach than Euclid's, we can find its similarity to Euclid's proof by giving an intermediate proof that uses both Euclid and Goldbach's approach.

In the end, we will find that there is a fairly natural way of changing Euclid's proof into a proof using the method we see in Goldbach's proof. Goldbach's proof goes as follows:

Proof. We define the following sequence $(n_i)_{i\in\mathbb{N}}$ as follows: Set $n_1 = 3$ and define

$$n_{k+1} = 2 + \prod_{j=1}^{k} n_j. \tag{2}$$

We make the following observations:

a) Each n_i is odd. This follows from a simple induction argument.

b) For all $j > i$ we have $n_j \equiv 2 \mod n_i$. We prove this as follows:

   Suppose after all that $j > i$. Then

$$n_j = 2 + \prod_{k=1}^{j} n_k = 2 + n_i\Big(\prod_{k=1,k\neq i}^{j} n_k\Big) \equiv 2 \mod n_i.$$

c) Whenever $i \neq j$, we have that n_i and n_j are relatively prime to eachother. We prove this by combining the previous 2 items as follows:

   Suppose $m \,|\, n_j$ and $m \,|\, n_i$. Without loss of generality assume that $j > i$. Then by b), we must have that $n_j = 2 + n_i k$ for some integer k.

   Since a) tells us n_j is odd, so is $n_i k$. It follows that $n_i k$ and 2 are relatively prime. This implies that $m \,|\, n_j$ if and only if $m \,|\, 2$ and $m \,|\, n_i k$. We conclude $m = 1$ as this is the only integer that divides both even and odd integers.

Now since each new entry to the sequence $(n_i)_{i\in\mathbb{N}}$ is relatively prime to all previous entries and larger than 1, it has a prime divisor which none of the previous entries has. Since the sequence is infinite, so is the set of all primes.

□

Both this proof and Euclid's use some arithmetic construction to conclude that some integer which has a new prime number as a divisor exists, but do so in slightly different ways. It turns out we can do even better in finding out just how related Goldbach's proof is to Euclid's: We will make the connection between Euclid's proof and proofs using infinite coprime integer sequences more clear in section 2.7, where we introduce some theory on dynamical systems.

Before doing this, instead we take a look at a proof by Pólya, and clear up a small misconception surrounding Goldbach and Pólya's proofs.

2.6 Pólya's proof

In the following proof we introduce Fermat numbers, and prove that all Fermat numbers are relatively prime to eachother, from which we conclude the infinitude of primes just like we did with Goldbach's proof.

Proof. We define the n^{th} Fermat number F_n as

$$F_n = 2^{2^n} + 1.$$

We show that all distinct Fermat numbers are relatively prime. Suppose that F_n and F_p are two Fermat numbers. Without loss of generality, we assume that $F_p = F_{n+k}$ for some integer $k \geq 1$. Furthermore, suppose that $m \,|\, F_n$ and $m \,|\, F_{n+k}$. Then note that when setting $x = 2^{2^n}$, we have that $F_n = x + 1$, and $F_{n+k} - 2 = x^{2^k} - 1$.

Note that if we view $F_{n+k} - 2$ as a polynomial in x, it has $x = -1$ as a root. Since each polynomial factors into its roots, we then must have that $x + 1 \,|\, x^{2^k} - 1$, or in other words $F_n \,|\, F_{n+k} - 2$. It follows that $m \mid F_{n+k} - 2$ and $m \mid F_{n+k}$, so $m = 1$ or $m = 2$. Since every Fermat number is odd, $m = 1$.

□

In this proof, we constructed an infinite sequence of relatively prime integers from which we immediately are able to conclude the infinitude of the prime numbers. This is the exact same argument that was made in Goldbach's proof. It becomes especially apparent when we realize that with Goldbach's proof, one can show by induction that

$$n_i = 2^{2^{i-1}} + 1,$$

so the sequence used in Goldbach's proof uses Fermat numbers as well. The recursive definition (2) for n_i seems at first like it gives a slightly different proof compared to Pólya's, when in actuality they are the exact same proofs.

The proof using Fermat numbers is commonly attributed to Pólya due to it being credited in well known number theory works [10], but Goldbach had already written the same proof before Pólya did. Part of this confusion was caused by the fact that while Goldbach was the first to find that the Fermat numbers are relatively prime, he did not use it to make the implication that there are infinitely many prime numbers [11].

2.7 Infinite coprime integer sequences

The main punchline of Euclid's proof is that given any set of relatively prime integers $a_1, \dots a_k$, they are all relative prime to the new integer $a_1 \cdot a_2 \cdots a_{k-1} \cdot a_k + 1$. In the following section, we will take this argument and use it to construct an infinite sequence of coprime integers, and eventually find a way to classify these proofs [12]. In doing this, we will work towards definitively finding the connection between these types of proofs and Euclid's. In the end, we look further into classifying all proofs using these infinite sequences.

Euclid's proof modified

Proof. We define the following sequence of integers: Set $a_0 = 2, a_1 = 3$, and recursively define

$$a_{i+1} = a_0 \cdot a_1 \cdots a_i + 1.$$

We show that $(a_n)_{n\in\mathbb{N}}$ defines a sequence of coprime integers. Let a_m and a_n be two integers from this sequence. Suppose without loss of generality that $m < n$, then note that

$$a_m \mid a_0 \cdot a_1 \cdots a_{n-1} = a_n - 1.$$

As such, we have that

$$\gcd(a_m, a_n) \mid \gcd(a_{n-1}, a_n) = 1.$$

So $\gcd(a_m, a_n) = 1$.

□

Note that alternatively we could have written

$$a_{i+1} = a_0 \cdot a_1 \cdots a_i + 1 = a_i(a_i - 1) + 1 = a_i^2 - a_i + 1,$$

so $a_{i+1} = f(a_i)$ where $f(x) = x^2 - x + 1$. Using this polynomial, we can derive yet another proof. This rephrasing of Euclid's modified proof will introduce a pattern which we will be exploring further afterwards.

Euclid's modified proof rephrased

We introduce the following lemma:

Lemma 2.3. *Let r, s be two distinct integers and let $f \in \mathbb{Z}[x]$. Then $r - s$ divides $f(r) - f(s)$.*

Using this lemma, we can derive the following proof of the infinitude of primes:

Proof. Set $a_0 = 2$, and define recursively $a_{n+1} = f(a_n)$ where $f(x) = x^2 - x + 1$. We show that a_n and a_m are relatively prime whenever $n \neq m$ (or, without loss of generality when $n > m$). Suppose $r \equiv s \mod p$ for any prime p. So by Lemma 2.3. $f(r) \equiv f(s) \mod p$. Suppose that $p \mid a_m$, then it follows that

$$a_{m+1} = f(a_m) \equiv f(0) = 1 \mod p.$$

In general, for any $n = m + k > m$ we have that

$$a_n = a_{m+k} = f(a_{m+k-1}) = f(f(f(\dots(a_m)))) \equiv 1 \mod p,$$

so $a_n \equiv 1 \mod p$ for all $n > m$. It follows that $\gcd(a_n, a_m) = 1$, so they are relatively prime.

□

Orbits in coprime sequence proofs

In the rephrased version of our modified version of Euclid's proof, we used a sequences generated by a polynomial in $\mathbb{Z}[x]$. More generally, the sequence $(x_i)_{i \in N}$ of coprime integers is given inductively by

$$x_{i+1} = f(x_i)$$

for some polynomial f. Such a sequence is an example of a *dynamical system*.

In Euclid's modified proof, we assumed that p divides x_m (so x_m is zero mod p), and then observe that

$$x_n \equiv 1 \mod p$$

for all $n > m$. We introduce the following terminology to make more sense of this.

Definition 2.4. The orbit of $x_m \in (x_i)_{i \in \mathbb{N}}$ under the map f are all elements of the sequence $(x_n)_{n \geq m}$. It is denoted as

$$x_m \to x_{m+1} \to x_{m+2} \to \dots.$$

Definition 2.5. We call the orbit of x_0 under the map f periodic if $x_0 = x_k$ for some $k \geq 0$. We call x_0 pre-periodic if it eventually becomes periodic.

Example 2.6. The orbit of 0 under $f(x) = x^2 - x + 1$, the polynomial we used for Euclid's modified proof, is

$$0 \to 1 \to 1 \to \dots,$$

and 0 is pre-periodic.

From this example we see that Euclid's rephrased proof's main argument is that 0 is (stricly) pre-periodic. After all, if this is the case, whenever an element from the sequence $(x_m)_{m \in \mathbb{N}}$ is zero mod some prime p, all elements which come afterwards are not. This is exactly the property which we want our sequence to have.

One can show that the following lemma is true:

Lemma 2.7. *All dynamical systems have periods of length at most 2.*

This lemma has the following usefull corollary, which we can use to get a classification of infinite coprime integer sequences:

Corollary 2.8. If 0 is pre-periodic for the dynamical system given by $f \in \mathbb{Z}[x]$, then its orbit is one of the following four possibilities:

- The orbit
$$0 \to a \to a \to \dots$$
We get this case using for example the polynomial $f(x) = x^2 - ax + a$.
-
$$0 \to -a \to a \to a \to \dots.$$
This works for $a = -1, -2, 1$ or 2. When $a = 2$, we find for example $f(x) = x^2 - 2$ works.
- The orbit
$$0 \to \pm 1 \to a \to \pm 1 \to \dots,$$
from which the first case is obtained from for example $f(x) = x^2 - ax - 1$. If we replace $f(x)$ with $-f(-x)$, we get the case with flipped signs instead.
- The orbit
$$0 \to \pm 1 \to \pm 2 \to \mp 1 \to \pm 2 \to \dots$$
which follows for example from $f(x) = 1 + x + x^2 - x^3$. If we replace $f(x)$ with $-f(-x)$, we get the case with flipped signs instead.

Example 2.9. The Fermat numbers are a dynamical system under the map $f(x) = x^2 - 2x + 2$:

Proof. Recall that we defined
$$F_n = 2^{2^n} + 1,$$
so
$$F_{n+1} = 2^{2^{n+1}} + 1 = (2^{2^n} + 1)(2^{2^n} - 1) + 2 = F_n(F_n - 2) + 2 = f(F_n).$$
□

If we compute the orbit of 0 under f, we get
$$0 \to 2 \to 2 \to \dots,$$
which corresponds to the first bullet of Corollary 2.8.

From the results of Example 2.6. and Example 2.9. we can conclude that Goldbach/Pólya's proof using Fermat numbers is indeed very similar to Euclid's (modified) proof. After all, they are both proofs in which we show a that all the integers of some dynamical system are relatively prime. In fact, the polynomials used in the proofs even have orbits of the same form.

3 Euler-like analytical proofs

This chapter will focus on proofs that have an analytical flavor similar to Euler's first proof of the infinitude of primes. In particular, we will explore a proof given by Euler which uses the properties of the geometric and harmonic series [1]; a proof by Chebysheff that combines the properties of geometric series with those of the logarithmic function [3]; and a proof by Barnes which combines theory on continued fractions and non-Pellian equations [3] [4]. While these proofs all have a very distinct feel to them, their similarity as proofs with an analytical framework will come to light as well.

3.1 Euler's proof using the geometric and harmonic series

The first proof we will examine is the first proof Euler wrote on the infinitude of primes. It uses a neat observation on the product of a particular set of geometric series and its convergence. The (non-)convergence of particular objects is something which we will very clearly see in Chebysheff's proof as well.

Euler's proof

Proof. Suppose there are only finitely many prime numbers, write $p_1, \dots p_r$. For any fixed prime number p, we consider the following geometric series:

$$\frac{1}{1-1/p} = \sum_{k=0}^{\infty} \frac{1}{p^k}.$$

Let p_m and p_n be 2 arbitrary distinct prime numbers. Then we make the observation that

$$\frac{1}{1-1/p_m} \cdot \frac{1}{1-1/p_n} = \left(\sum_{k_m=0}^{\infty} \frac{1}{p_m^{k_m}} \right) \cdot \left(\sum_{k_n=0}^{\infty} \frac{1}{p_n^{k_n}} \right) = \sum_{k_m=0}^{\infty} \sum_{k_n=0}^{\infty} \frac{1}{p_m^{k_m} p_n^{k_n}},$$

which is precisely the sum of reciprocals of all integers which can be factorized using only p_m and p_n. More generally, we see that

$$\prod_{1 \le i \le r} \frac{1}{1-1/p_i} = \left(\sum_{k_1=0}^{\infty} \frac{1}{p_1^{k_1}} \right) \cdots \left(\sum_{k_r=0}^{\infty} \frac{1}{p_r^{k_r}} \right) = \sum_{k_1=0}^{\infty} \cdots \sum_{k_r=0}^{\infty} \frac{1}{p_1^{k_1} \cdots p_r^{k_r}}.$$

Since the above sum is precisely the sum of reciprocals of all possible prime factorizations of the non-negative integers which can be constructed with $p_1, \dots, p_r$, and all non-negative integers have such a unique prime factorization, we must have that

$$\prod_{1 \le i \le r} \frac{1}{1-1/p_i} = \sum_{k_1=0}^{\infty} \cdots \sum_{k_r=0}^{\infty} \frac{1}{p_1^{k_1} \cdots p_r^{k_r}} = \sum_{n=0}^{\infty} \frac{1}{n},$$

which is the harmonic series. Since the harmonic series diverges, so must

$$\prod_{1 \le i \le r} \frac{1}{1-1/p_i},$$

which is a contradiction since we assumed this to be a finite product of converging series, which we know to be a converging series as well. We conclude the above product must be infinite instead, so there are infinitely many prime numbers.

□

3.2 Chebysheff's proof using the geometric series

The following proof uses an upper bound for a particularly interesting geometric series, to find a lower bound for the sum

$$\sum_{p\leq N} \log(p)/(p-1),$$

with N sufficiently large and p prime. Since the lower bound we end up finding converges as $N \to \infty$, so must the above sum, which is how we conclude there are infinitely many prime numbers. To arrive at our desired lower bound, we introduce some notation and then make some observations.

Notation. Suppose that p is a prime number dividing $N!$. We write $a(p, N)$ for the exponent of p in the unique prime factorization of $N!$.

Observation. One can observe that $a(p, N) = \sum_{k=1}^{\infty} \lfloor N/p^k \rfloor$. After all, for $k = 1$ we see that $\lfloor N/p^k \rfloor = N/p = |\{pm \leq N | m \in \mathbb{N}\}|$. Each of the elements of this set is a multiple of p that occurs in $N!$. Similarly when $k = 2$, the elements from the previous set that contain p in their unique prime factorization twice get detected again, and so on. It follows that indeed $a(p, N) = \sum_{k=1} \lfloor N/p^k \rfloor$. This is known as Legendre's formula.

Observation. We have that

$$a(p, N) = \sum_{k=1}^{\infty} \lfloor N/p^k \rfloor < \sum_{k=1}^{\infty} N/p^k = \sum_{k=1}^{\infty} (N/p)(1/p)^{k-1},$$

which is a geometric series, converging to

$$\frac{N/p}{1-(1/p)} = \frac{N}{p-1}.$$

Chebysheff's proof

Proof. Consider the finite sum

$$\sum_{p\leq N} \log(p)/(p-1).$$

Then from our previous observations and the basic properties of the logarithmic function, we find that

$$\sum_{p\leq N} \log(p)/(p-1) > \sum_{p\leq N} a(p, N)\log(p)/N = \sum_{p\leq N} \log(p^{a(p,N)})/N = \log(N!)/N.$$

It is known that $\log(N!)/N$ converges to $\log(N)$ when we take the limit $N \to \infty$ (the proof follows from substituting Stirling's approximation of $N!$ into the fraction $\log(N!)/(N\log(N))$, and then taking the limit $N \to \infty$), so we can certainly state that

$$\log(N!)/N > \log(N) - 1$$

for N sufficiently large. We conclude that $\sum_{p\leq N} \log(p)/(p-1) > \log(N) - 1$ for N large enough, so when taking the limit $N \to \infty$ the sum cannot be finite and there must therefore be infinitely many primes.

□

We see the analytical nature of Chebysheff's proof clearly when finding the upper bound of $a(p, N)$, as this uses the convergence of the geometric series just like we did in Euler's proof. Another argument from analysis we see in the proof is the convergence of $\log(N!)/N$ to $\log(N)$ when N tends to infinity.

3.3 Barnes' proof using continued fractions

Barnes' proof uses results on continued fractions and non-Pellian equations, a special type of diophantine equation. We start with defining continued fractions and non-Pellian equations to build the theory which we need for Barnes' proof.

Definition. A continued fraction, denoted $[a_0, a_1, a_2, \dots]$, is the fraction

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

Its approximants are the rational numbers obtained from terminating the continued fraction at some point: the 0^{th} approximant is a_0, the 1^{st} is $a_0 + \frac{1}{a_1}$ and so on. We write A_i, B_i for the numerator and denominator respectively of the i^{th} approximant (for $i \in \mathbb{N}$).

Example 3.1. In the standard form we gave above, we see that $A_0 = a_0, B_0 = 1$ since $A_0/B_0 = a_0$ and $A_1 = a_0 \cdot a_1 + 1, B_1 = a_1$ since then $A_1/B_1 = \frac{a_0 \cdot a_1 + 1}{a_1} = a_0 + \frac{1}{a_1}$. In general one can show that for $i > 1$,

$$B_{i+1} = a_{i+1}B_i + B_{i-1}.$$

Lemma 3.2. *Every periodic continued fraction (a continued fraction with eventually periodic iterates) is a quadratic irrational. For $p \in \mathbb{N}$, the continued fraction $[p, p, p, \dots]$ is equal to $\frac{p + \sqrt{p^2 + 4}}{2}$*

We now take a look at non-Pellian equations, and state an important result which we will use to eventually link it back to continued fractions:

Definition. We define the non-Pellian equation as the Diophantine equation of the form

$$x^2 - dy^2 = -1.$$

Lemma 3.3. *Suppose that the simple continued fraction of $\sqrt{d}$ has an odd period m. Then for the non-Pellian equation $x^2 - dy^2 = -1$, all of its positive solutions are of the form $(x, y) = (A_i, B_i)$ with A_i and B_i as before and $i = qm - 1$ with q odd.*

Barnes' proof

Proof. Assume that $p_1, \dots, p_k$ are all the prime numbers. Write $P = \prod_{i=1} p_i$, and $Q = \prod_{i=2} p_i$, where $p_1 = 2$ and Q becomes the product of all odd primes. By the $p = P$ case of Lemma 3.2., we see that

$$[P, P, P, \dots] = \frac{P + \sqrt{P^2 + 4}}{2} = Q + \sqrt{Q^2 + 1}.$$

Observe that since $Q^2 + 1 \equiv 1 \mod p_i$, we see that $p_i \not| \, Q^2 + 1$ for all $i > 1$. This then implies that $Q^2 + 1$ has to be a power of 2.

Note that if $Q^2 + 1$ is an even power of 2, it would follow that $Q + \sqrt{Q^2 + 1}$ is rational which is a contradiction since infinite continued fractions are irrational. It follows that $Q^2 + 1 = 2^{2l+1}$, which we can rewrite as the equality

$$Q^2 - 2 \cdot (2^l)^2 = -1,$$

so the non-Pellian equation has a solution for $x = Q, d = 2, y = Q^2 + 1$. It is known that

$$\sqrt{2} = [1, 2, 2, 2, \dots],$$

which is a periodic continued fraction with period 1. It follows from Lemma 3.3. that all its positive solutions are of the form $(Q, 2^l) = (A_i, B_i)$ for some even integer $i = 2n$. One can show using induction that B_{2n} is an odd integer for all $n \in \mathbb{N}$. So, since 2^l is even for all $l > 1$, we must have that $2^l = B_0$ implying that

$$\frac{Q}{2^l} = \frac{A_0}{B_0} = \frac{1}{1},$$

so $Q = 1$ since $\gcd(Q, 2^l) = 1$. This is a contradiction since clearly $Q > 1$.

□

This proof uses many different properties of continued fractions. Studying these fractions is akin to studying limits, as a continued fraction is precisely the limit of the infinite row

$$[a_0], [a_0, a_1], [a_0, a_1, a_2], \ldots$$

where $[a_0, \ldots, a_n]$ is shorthand notation for the $n-$th approximant of the continued fraction $[a_0, a_1, a_2, \ldots]$. Realizing this fact, it becomes rather clear that Barnes' proof has a very analytical approach.

It almost looks like Euclid's argument gets used when the observation gets made that $p_i \not| Q^2 + 1$ for all $i > 1$, but the fact that this does not hold for $i = 1$ keeps the two arguments from being exactly the same.

4 Erdős-like combinatorial proofs

In this chapter, we will examine proofs which use combinatorics. A well known example of this, is Paul Erdős' proof, which uses combinatorics to derive a lower bound for the prime counting function [5]. This lower bound will be sharper than the one which we can obtain using Euclid's and Euler's proof.

4.1 Erdős' proof

We introduce the following lemma, which is essentially a rephrasing of the unique prime factorization property of the integers larger than 1:

Lemma 4.1. *Let N be a positive integer. Then we can uniquely factorize $N = a^2b$ where a, b are positive integers, and b is squarefree.*

We are now ready to prove the infinitude of primes:

Proof. Suppose, for contradiction, we have finitely many primes, say $p_1, \ldots, p_k$. By Lemma 4.1., for any fixed $N \in \mathbb{N}$ we have that any $1 \leq x \leq N$ can be uniquely written as $x = a^2b$ with a, b as in Lemma 4.1.

Since $a^2 \leq x \leq N$, we observe that $a^2 \leq N$, so in particular $a \leq \sqrt{N}$. Since b is squarefree, and there are exactly k different prime numbers, there are 2^k distinct candidate factorizations for b.

As such, it follows that there are $\sqrt{N}2^k$ different possible ways of writing a^2b given a finite set of prime numbers. Since we are able to do this uniquely for all $1 \leq x \leq N$, it follows that

$$N \leq \sqrt{N}2^k.$$

Squaring both sides and dividing by N yields the inequality

$$N \leq 2^{2k},$$

for all $N \in \mathbb{N}$, which is a contradiction since 2^{2k} is a constant but $\mathbb{N}$ is not bounded from above. We conclude that there must be infinitely many prime numbers.

□

Erdős' proof is very distinct from the Euclid- and Erdős-like proofs we have seen thus far. The proofs from the previous chapters seemed to all contain some sort of construction of a prime divisor which is not a part of the list of primes used in said construction, or explore a certain niche from analysis, where Erdős' proof is more combinatorial in nature. To further illustrate the difference between Euclid and Erdős' proofs, we consider the following corollary that we can derive from it. More precisely, this is the statement which Erdős' original proof was intended for and it is a stronger result than the infinitude of the prime numbers:

Corollary 4.2. Let π be the prime counting function. Then

$$\pi(N) \geq \log(N)/(2\log(2)).$$

Proof. Let $p_1 \ldots, p_{\pi(N)}$ denote all prime numbers less than or equal to N for some $N \in \mathbb{N}$. Then we have that

$$2^{\pi(N)}\sqrt{N} \geq N,$$

so

$$2^{2\pi(N)} \geq N.$$

Taking the base 2 logarithm and dividing by 2 on both sides then yields the inequality

$$\pi(N) \geq \log_2(N)/2 = \log(N)/(2\log(2)).$$

□

Euclid and Euler's proofs also yield a lower bound for the prime counting function, but it is worse than the one we get from Erdős' proof. The lower bound we can derive from Euclid and Euler's proofs was $\pi(N) > \log(\log(N))$ for $N \geq 2$, which contains an extra log when compared to the lower bound we just found.

4.2 Thue's proof

The following proof was given by mathematician Axel Thue in 1897 [14]. Whereas Erdős' proof works by counting unique factorizations in the form of Lemma 4.1., Thue's proof instead focusses on sequences of exponents of unique prime factorizations.

Proof. Assume that $p_1, \ldots, p_k$ are all of the prime numbers. Then we know that for any fixed $n \in \mathbb{N}$ we can uniquely factorise it in the form $n = p_1^{a_1} \cdots p_k^{a_k}$. Furthermore, in this case we can observe that $n < 2^m$ for some $m \in \mathbb{N}$ since $\mathbb{N}$ is not bounded from above. Since we know that 2 is the smallest prime number, substituting $p_1 = 2$ shows us that

$$n = p_1^{a_1} \cdots p_k^{a_k} = 2^{a_1} \cdots p_k^{a_k} < 2^m,$$

from which we see that

$$a_1, a_2, \ldots, a_{k-1}, a_k < m.$$

From this we can conclude that $0 \leq a_i \leq m - 1$ for all $1 \leq i \leq k$, so there are m^k different possible sequences $a_1, \ldots, a_k$ of exponents of the unique prime factorization of n.

Now note that since $m^k < 2^m$ for m sufficiently large, there are not enough ways to uniquely factorise every integer less than 2^m with finitely many prime numbers, so our assumption that there are only finitely many prime numbers must have been wrong.

□

This proof is very similar to the one which Erdős wrote a couple of decades after Thue's proof was published. With both proofs, the main punchline is that given a finite set of prime numbers, you cannot constuct a high enough amount of unique factorizations that satisfy a certain constraint.

In other words, these proofs formalize the intuition that without infinitely many prime numbers, some integers get skipped when going over all unique factorizations we can possibly make using finetely many primes.

4.3 Wunderlich's proof

This proof uses the Fibonacci number sequence, which we define recursively by setting $F_1 = F_2 = 1$, and

$$F_k = F_{k-1} + F_{k-2}.$$

Lemma 4.3. *Given Fibonacci numbers F_n and F_m with gcd$(n, m) = d$. Then gcd$(F_n, F_m) = F_d$.*

We are now ready for Wunderlich's proof [13].

Wunderlich's proof using Fibonacci numbers

Proof. Assume that

$$\{p_1, p_2, p_3, \ldots, p_{12} \ldots, p_k\} = \{2, 3, 5, \ldots, 37, \ldots, p_k\}$$

is the set of all prime numbers. We now consider the Fibonacci numbers with prime index:

$$F_2, F_3, \ldots, F_{37}, \ldots, F_{p_k}$$

By the above lemma, $\gcd(F_{p_i}, F_{p_j}) = 1$ whenever $i \neq j$. It follows that any two Fibonacci numbers with prime index are relatively prime. Aditionally, every prime indexed Fibonacci number (besides $F_2 = 1$) admits has a unique prime divisor. In total we find $k - 1$ distinct prime numbers.

This then implies that there is no single Fibonacci number which has three distinct prime divisors. However: $F_{37} = 73 \cdot 149 \cdot 2221$ is the product of three distinct prime numbers, which is a contradiction.

□

We derive our contradiction from the fact that we cannot construct k prime-indexed Fibonacci numbers using only k primes, which is once again a very combinatorial argument. Note that since we assumed that k is a finite integer, the sequence of prime-indexed Fermat numbers is not an infinite coprime integer sequence as it is assumed to be finite.

4.4 Perott's proof

The following proof is a proof which may seem analytical at first as it starts off by deriving an upper bound for a series, but in actuality we will see its main argument uses mostly combinatorics, so it does have more in common with Erdős' proof than Euler's proof.

We first consider the series

$$\sum_{n=1}^{\infty} \frac{1}{n^2}.$$

Observation. One can show that

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1+\frac{1}{4}+\sum_{n=3}^{\infty} \frac{1}{n^2} < \frac{5}{4}+\sum_{n=3}^{\infty} \frac{1}{n(n-1)} = \frac{5}{4}+\sum_{n=3}^{\infty} \frac{1}{n-1}-\frac{1}{n} = \frac{5}{4}+\sum_{n=2}^{\infty} \frac{1}{n-1}-\sum_{n=3}^{\infty} \frac{1}{n} = \frac{5}{4}+\frac{1}{2} = \frac{7}{4}.$$

We are now ready to state Perott's proof [3].

Proof. Define $\delta = 2 - \sum_{n=1}^{\infty} \frac{1}{n^2}$. Then from our previous observation we know that $\delta > \frac{1}{4}$.

Suppose that $p_1, \ldots p_k$ are all the primes. It follows that the number of squarefree integers less than or equal to N is at most 2^k. We also know that there are at most N/d^2 integers m which are divisible by d^2.

It follows that the number of integers less than or equal to N which are divisible by a square $d^2 > 1$ is bounded from above by the sum

$$\sum_{d=2}^{N} \frac{N}{d^2} = N \cdot \big((\sum_{d=1}^{N} \frac{1}{d^2}) - 1 \big),$$

which after substituting in δ is equal to $N(1-\delta)$. Adding up our upper bounds for squarefree and non-squarefree integers that are less than or equal to N, we find the inequality $N \leq 2^k + N(1-\delta)$, so

$$2^k \geq N\delta > N/4,$$

so we find that $k > \log_2(N/4) = \log_2(N) - 2 = \frac{\log(N)}{\log(2)} - 2$, which is a contradiction for large enough N.

□

The main argument of Perott's proof is once again very similar to the one we see in Erdős' proof. Namely, they share the combinatorial argument that there are at most 2^k squarefree integers contructable with k primes. Repeating a similar argument to the one we did with Erdős' proof, we find that $\pi(N) \geq \frac{\log(N)}{\log(2)} - 2$, which differs from the lower bound we found in Corollary 4.2. only by a factor and a constant.

At first, one might be thrown off by the estimation that was done for δ and conclude the proof has an analytical side to it as well, but the argument in question is very elementary and does not use any big results from analysis.

4.5 Alpoge's proof

This proof uses Van der Waerden's theorem, which goes as follows:

Theorem 4.4 (van der Waerden)**.** *Color all positive integers with one of r different colors. Then for all integers $N \geq 3$ there exists an arithmetic progression of integers in which at least N elements have the same color.*

We also use the following lemma which was proven by Fermat:

Lemma 4.5 (Fermat)**.** *An arithmetic progression cannot contain 4 different squares.*

We are now ready to give Alpoge's proof [12].

Proof. Assume $p_1, \ldots, p_k$ are all the primes. Note that this implies every integer n can be written as

$$n = p_1^{e_1} \cdots p_k^{e_k}.$$

We define r_i to be the parity of e_i. That is:

$$r_i = \begin{cases} 0 & e_i \text{ is even} \\ 1 & e_i \text{ is odd} \end{cases}.$$

Now we consider the integer $R = p_1^{r_1} \cdots p_k^{r_k}$, and we observe that the quotient

$$n/R = p_1^{e_1 - r_1} \cdots p_k^{e_k - r_k}$$

is a square. We now assign the color R to n. Additionally, we observe that there are 2^k different possible choices of R.

Now applying Van der Waerden's theorem for $r = 2^k$ and $N = 4$ to see that there exists an arithmetic progression

$$A, A + D, A + 2D, A + 3D, \quad D \geq 1$$

of integers which all have the color R. In particular, R divides each of these integers, so

$$A/R, (A + D)/R, (A + 2D)/R, (A + 3D)/R$$

is an arithmetic progression with 4 elements. However, we previously observed that whenever n has color R, n/R is a square. This contradicts Fermat's lemma, which states that an arithmetic progression cannot contain 4 different squares. We conclude that our initial assumption that their are finitely many prime numbers must have been wrong, so there are infinitely many primes.

□

This proof fits in nicely between the combinatorial proofs we have found thus far. The assumption that there are finitely many primes was used to conclude that there can only be finitely many squarefree integers R, which is a similar argument to the one that was used in Erdős' proof. The main contradiction then comes from the fact that we have a hard limit on how many integers are divided by that same R, which again is similar to what was done in Erdős' proof.

References

[1] K. Conrad, *The infinitude of the primes*, kconrad.math.uconn.edu, pp. 2 − 6, URL https://kconrad.math.uconn.edu/blurbs/ugradnumthy/infinitudeofprimes.pdf (Accessed 19 June 2024)

[2] K. Conrad, *THE "TOPOLOGICAL" PROOF OF THE INFINITUDE OF PRIMES*, kconrad.math.uconn.edu, pp. 1 − 2, URL https://kconrad.math.uconn.edu/blurbs/ugradnumthy/primestopology.pdf (Accessed 19 June 2024)

[3] T. Yamada, *Proofs of the inifitude of primes*, (2018), tyamada1093.web.fc2.com, pp. 5 − 7, URL https://tyamada1093.web.fc2.com/math/files/infprime.pdf

[4] C.W. Barnes, *THE INFINITUDE OF PRIMES; A PROOF USING CONTINUED FRACTIONS*, L'Enseignement Mathematique, **22** (1976), pp. 314 − 316.

[5] P. Erdős, *Uber die Reihe* $\sum_p 1/p$, Mathematica (Zutphen) B7 (1938), pp. 1 – 2. URL https://users.renyi.hu/∼ p_erdos/1938-13.pdf

[6] J. Hadamard, *Sur la distribution des zéros de la fonction* $\zeta(s)$ *et ses conséquences arithmétiques*, Bulletin de la Société Mathématique de France, **24**, Société Mathématique de France (1896), pp. 199 – 220.

[7] C-J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Annales de la Société scientifique de Bruxelles, 20 B, 21 B, Imprimeur de l'Académie Royale de Belgique (1896), pp. 183 – 256, 281 – 352, 363 – 397, 351 – 368

[8] R. Meštrović, *Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2017) and another new proof*, (2023) v.4, URL https://arxiv.org/pdf/1202.3670 (Accessed 3 June 2024)

[9] P. Pollack, *Not Always Buried Deep: A Second Course in Elementary Number Theory*, (2009), the American Mathematical Society, pp. 2 − 4, URL https://pollack.uga.edu/NABDofficial.pdf

[10] G.H. Hardy & E.M. Wright, *AN INTRODUCTION TO THE THEORY OF NUMBERS*, (1960), Clarendon press (Oxford), v.4, pp. 14, URL https://blngcc.wordpress.com/wp-content/uploads/2008/11/hardy-wright-theory_of_numbers.pdf

[11] Goldbach, Christian: Letter to Euler, 20/31 July 1730, in: Noscemus Wiki, URL http://wiki.uibk.ac.at/noscemus/Letter_to_Euler,_20/31_July_1730 (last revision: 09.02.2022).

[12] A. Granville, *A panopoly of proofs that there are infinitely many primes*, (2017), dms.umontreal.ca, pp. 3 − 4, URL https://dms.umontreal.ca/∼andrew/PDF/LMSNewsletter.pdf

[13] L. Harrison, *From Euclid to Present: A Collection of Proofs regarding the Infinitude of Primes*, www.gcsu.edu (2013), pp. 11 − 12, URL https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/harrison.pdf

[14] A. Bogomolny, *Infinitude of Primes - A. Thue's Proof*, www.cut-the-knot.org, URL https://www.cut-the-knot.org/proofs/ThueInfinitudeOfPrimes.shtml (Accessed on 19 June 2024)