From Euclid to Present: A Collection of Proofs regarding the Infinitude of Primes

Lindsey Harrison

December 14, 2013

Abstract

Prime numbers are considered the basic building blocks of the counting numbers, and thus a natural question is: Are there infinitely many primes? Around 300BC, Euclid demonstrated, with a proof by contradiction, that infinitely many prime numbers exist. Since his work, the development of various fields of mathematics has produced subsequent proofs of the infinitude of primes. Each new and unique proof gives the mathematical community a glimpse into better understanding the prime numbers. Here, we will examine a collection of proofs of the infinitude of primes, and explore why prime numbers are important.

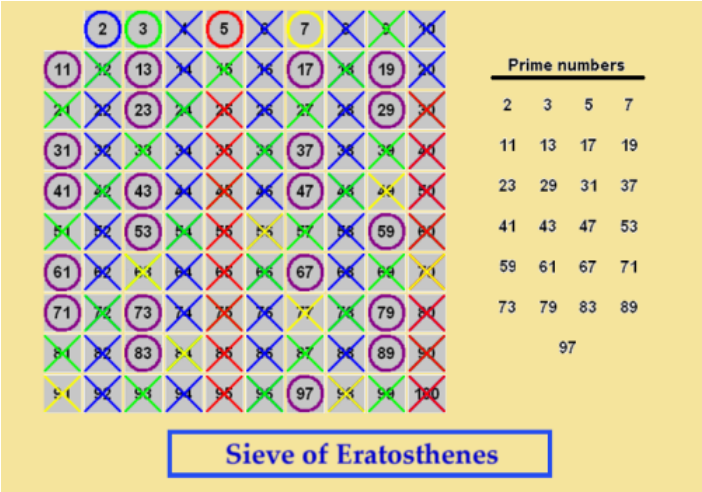
1 Introduction

Paul Erdős, who authored over 1500 papers on number theory, claimed "It will be another million years, at least, before we understand the primes" and yet this has not deterred mathematicians over the centuries from exploring the primes and the properties that make them unique. There is much still to be discovered about the primes, but one property that is certain is that there exist infinitely many prime numbers. In 300BC, Euclid was the first on record to formulate a logical sequence of steps, known as a proof, that there exists infinitely many primes. The progression of rigor in mathematics has inspired mathematicians throughout history to produce new proofs of the infinitude of primes. In the 18th century, Goldbach and Euler both demonstrated the infinitude of primes, but in stark contrast from each other. Goldbach utilized Fermat numbers in his proof while Euler worked with the primes analytically. In the 19th century, Dirichlet pioneered a new field of mathematics which combined analysis and number theory, known as analytic number theory, and proved the infinitude of primes through an arithmetic progression. In the 20th century, Paul Erdős bounded the primes below to prove their infinitude, and University of Colorado professor M. Wunderlich worked with Fibonacci numbers to prove the infinitude of the primes. The final proof we will examine, given by University of North Carolina at Greensboro professor Saidak in 2006, is one of the few direct proofs. While each successive proof verifies the same conclusion, we will follow the development of primes throughout history alongside the advancement of rigor.

2 History of the Primes

Prime numbers are often called the atoms of arithmetic or the building blocks of integers since all other numbers are built off of their existence. It is said mathematician and author Marcus du Sautoy that prime numbers would be there regardless of whether humans had evolved sufficiently to recognize them due to this quality [3]. The first mathematical evidence that individuals knew about prime numbers is the Ishango bone, which dates from around 6500 BC. Discovered in 1960 in the mountains of central Africa, this bone contains rows of notches that hold different mathematical meaning [3]. One group of notches contains the numbers 11, 13, 17, and 19. Note these are the prime numbers between 10 and 20. Like many ancient artifacts, there is debate as to whether these notches give an indication of the understanding of prime numbers or possibly just a collection of numbers, but the Ishango bone still gives insight to the mathematical possibilities of ancient civilizations.

While other civilizations such as the Egyptians and Chinese made some distinctions for prime numbers in their records, the first group of individuals to make great strides in the prime number exploration were the ancient Greeks. Eratosthenes in the third century BC discovered a procedure for determining if a number was prime or composite. While we do not have any surviving records of Eratosthenes, the mathematician Nicomachus of Gerasa attributes the sieve to Eratosthenes in his work *Introduction to Arithmetic I*. Visually the sieve is as follows.



He first started at the number 2 since 1 is neither prime nor composite. Then working through his array of numbers, Eratosthenes crossed off every number that is a multiple of 2. None of these

integers could be prime since they are divisible by 2. After eliminating all the even integers he then proceeded to the next number in his array that was not crossed off which is 3. In the same manner as before he eliminated all integers that were multiples of 3 and hence not prime numbers. Note that once a number has been eliminated there is no need to cross it out again since we already know it is not prime. He kept repeating this process picking up at the next prime and eliminating all the multiples of that prime. This systematic process left a table of prime numbers. There is a rhyme for the sieve that goes as follows.

Sift the Two's and Sift the Three's
The Sieve of Eratosthenes
When the multiples sublime, The numbers that remain are Prime.
-Anonymous

The Sieve of Eratosthenes remains today as the simplest algorithm for determining if a given number is prime; however, the obvious drawback to the sieve is the time it takes to formulate the complete table. If an individual wanted to check to see if a number several digits long was in fact prime, then the most effective means would not be to draw out a table that large. Throughout history there have been many advances in primality testing, but the dawn of the technological era brought about a new light in searching for the primes.

The Great Internet Mersenne Prime Search (GIMPS) was a project that began in 1996 with a computer program that would run through trials of division to determine if a given number is prime. The primality test the software uses for GIMPS is the Lucas-Lehmer primality test which is used on Mersenne numbers. Note a Mersenne number is a number of the form $2^n - 1$, but a Mersenne number can only be a Mersenne prime if n is prime. Therefore all Mersenne primes are of the form $2^p - 1$ where p is prime, but p being prime does not guarantee $2^p - 1$ is prime. The Great Internet Mersenne Prime Search works through volunteers who allow the software to run on their computer in a collaboration with many other computers in search for the next largest Mersenne prime. As to date GIMPS has found 14 of the known 48 Mersenne primes. A total of 11 of these Mersenne primes were the largest known primes recorded at the time of their discovery. The most recent Mersenne prime discovered was the prime $2^{57,885,161} - 1$ which clocks in at $17,425,170$ digits long[6]. The Electronic Frontier Foundation is offering a $\$150,000$ reward for the first prime number over 100 million digits long.

While the search for the next largest prime is exciting, the computer race gives us no better understanding of primes. It is the concept of the proof that gives us without certainty the definitiveness of the behavior of the primes. The proof that there exists infinitely many primes is the essential foundation for the continued search into unlocking the mystery of the primes.

3 Background Information

"The primes are the jewels studded throughout the vast expanse of the infinite universe of numbers that mathematicians have explored down the centuries." [3] The first mathematician we have on record for defining these jewels was Euclid. He was one of the first mathematicians who laid a groundwork in *The Elements* for clearly defining what it meant for a number to be prime and

what specifically makes the prime numbers unique. Book VII of *The Elements* gives the following definitions [5].

Definition 1. *A prime number is one which is measured by a unit alone.*

Definition 2. *Numbers prime to one another are those which are measured by a unit alone as a common measure.*

Reflecting the means of math around the time 300BC, Euclid cast everything in *The Elements* in geometric terms. With modern language we can redefine the terms prime and relatively prime as follows.

Definition 3. *(prime). An integer $p > 1$ is prime if and only if the only positive divisors of p are 1 and itself.*

Definition 4. *(relatively prime). Two integers m and n, with at least one nonzero, are relatively prime, or coprime, if they share no common factors other than 1; that is, the greatest common divisor of m and n is* 1.

We can define all natural numbers greater than 1 that are not prime as composite numbers. What special traits do the prime numbers have that place them above composite numbers with respect to importance? Euclid answered this question in Proposition 32 of VII in *The Elements*. Today this proposition is known as the Fundamental Theorem of Arithmetic.

Theorem 1. *Each natural number $n > 1$ can be written in the form*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where k is a positive integer. Also each a_i is a positive integer, and $p_1 < p_2 < \cdots < p_k$ are distinct primes.

Informally the Fundamental Theorem of Arithmetic simply states that every integer greater than 1 can be written uniquely as a product of primes. It follows from the Fundamental Theorem of Arithmetic that primes are considered to be the building blocks of all integers.

Below are a few results that we will use in subsequent proofs in this paper. Proofs of these results can be found in a traditional Elementary Number Theory textbook[1][7].

Theorem 2. *If p is a prime number and m and n are integers such that $p \mid mn$, then $p \mid m$ or $p \mid n$.*

Theorem 3. *If $p \mid m$ and $p \mid n$, then $p \mid (am + bn)$ for all $a, b \in \mathbb{Z}$; that is, if p divides m and p divides n, then p divides every linear combination of m and n.*

Theorem 4. *Consecutive pairs of integers are relatively prime; that is, $\gcd(n, n+1) = 1$ for each $n \in \mathbb{Z}$.*

4 How Many Primes?

4.1 Euclid

Euclid was the first mathematician known to date to give a formal proof that there are infinitely many prime numbers. This was done in book IX of *The Elements* which dates back to 300BC. There was a lack of symbolic algebra during the time so all the arithmetic was cast in geometric terms. Euclid was a product of this tradition as we can see by his mathematical arguments within *The Elements*. It was not until the year 820 when Arabic mathematician al-Khwarizmi published *Al-Jabr*, known today as the first algebra textbook, that symbolic algebra emerged. Before then numbers were represented as line segments and thus only positive numbers were dealt with since manipulating negative or zero lengths would be absurd. Below is Euclid's proof of infinitely many primes as it is given in *The Elements* [5].

Claim. Prime numbers are more than any assigned multitude of prime numbers.

Proof. Let A, B, and C be the assigned prime numbers. I say that there are more prime numbers than A, B, and C. Take the least number DE measured by A, B, and C. Add the unit DF to DE. Then EF is either prime or not. First, let it be prime. Then the prime numbers A, B, C, and EF have been found which are more than A, B, and C. Next, let EF not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number G. I say that G is not the same with any of the numbers A, B, and C. If possible, let it be so. Now A, B, and C measure DE, therefore G also measures DE. But it also measures EF. Therefore G, being a number, measures the remainder, the unit DF, which is absurd. Therefore G is not the same with any one of the numbers A, B, and C. And by hypothesis it is prime. Therefore the prime numbers A, B, C, and G have been found which are more than the assigned multitude of A, B, and C. Therefore, prime numbers are more than any assigned multitude of prime numbers. □

The different distinct proof techniques had not been fully developed during Euclid's time, but readers today recognize that this is a proof by contradiction. With the development of mathematics throughout history, the definition of measure has been redefined without the geometric casting. With these two developments along with notational ones, Euclid's same proof idea has been modernized as we see in the proof by contradiction below.

Claim. There are infinitely many primes.

Proof. Suppose there are only a finite number of primes. Let

$$\{p_1, p_2, p_3, p_4, \cdots, p_n\}$$

be the complete list of primes in ascending order where $p_1 = 2$ and p_n is the largest prime. Consider the natural number

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

By the Fundamental Theorem of Arithmetic we can deduce that N is divisible by some prime p. Recall that our list of primes is finite so $p \in \{p_1, p_2, p_3, \ldots, p_n\}$. Note that $p|(p_1p_2 \cdots p_n)$. By Theorem 3 it follows that p divides every linear combination of N and $p_1p_2p_3 \cdots p_n$. Specifically, $p|(N - (p_1p_2 \cdots p_n))$ which implies that $p|1$. Thus, $p = \pm 1$, which contradicts that $p \geq 2$ since p is a prime number. In conclusion, we can deduce that our list of finite primes is not complete, and thus the number of primes is infinite. □

A common misconception from this proof is that $N = 2 \cdot 3 \cdot 5 \cdots p_n + 1$ will always result in a prime number. Take $N = 2(3)(5)(7)(11)(13) + 1 = 30031$; however, note that 30031 is not prime since $30031 = 59(509)$. When N is prime, there is a larger prime number than our assumed finitely many primes list. When N is composite, the prime factorization of N will produce at least one prime number that is not already included in our assumed finitely many primes list. This process can continue indefinitely, and thus we arrive that there are infinitely many primes. Throughout the years there have been countless variations of Euclid's proof worked by mathematicians.

4.2 Goldbach

Almost 2000 years after Euclid's proof of the multitude of primes, the German mathematician Christian Goldbach provided a new proof that there exists infinitely many primes. In a 1730 letter correspondence to his close friend and fellow mathematician Leonhard Euler, Goldbach proved there exists infinitely many primes through the use of Fermat numbers[2]. A Fermat number is a positive integer of the form

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

where n is a nonnegative integer. It was conjectured by Pierre de Fermat, a French mathematician, that all Fermat numbers are prime; however, it was the mathematician Euler who disproved this conjecture by showing F_5 is composite. Had Fermat been correct we would have a function that generated prime numbers. Goldbach today is not remembered primarily for the below proof, but instead is remembered for Goldbach's conjecture that states every even integer greater than 2 can be expressed as the sum of two prime numbers. In correspondences with Euler, Goldbach proved the following.

Lemma 1. *If n is a nonnegative integer, then $F_{n+1} - 2 = F_nF_{n-1} \cdots F_1F_0$.*

Proof. We will do a proof by mathematical induction. For each natural number n, let $P(n)$ be the statement

$$F_{n+1} - 2 = F_nF_{n-1} \cdots F_1F_0.$$

Base Case. First we will show that $P(0)$ is true. Note that

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3.$$

Also note that

$$F_{0+1} - 2 = (2^{2^1} + 1) - 2 = 5 - 2 = 3.$$

Hence $F_{0+1} - 2 = F_0$, and it follows that $P(0)$ is true.

Inductive Step. Let $k \in \mathbb{N}$. Assume $P(k)$ is true; that is, assume $F_{k+1} - 2 = F_kF_{k-1} \cdots F_1F_0$.

We will show that $P(k+1)$ is true; that is, we will show $F_{(k+1)+1} - 2 = F_{k+1}F_kF_{k-1}\cdots F_1F_0$. Observe the following

$$\begin{aligned}
F_{k+1}(F_kF_{k-1}\cdots F_1F_0) &= F_{k+1}(F_{k+1}-2) && \text{(by Inductive Hypothesis)}\\
&= (2^{2^{k+1}}+1)(2^{2^{k+1}}+1-2)\\
&= (2^{2^{k+1}}+1)(2^{2^{k+1}}-1)\\
&= (2^{2^{k+1}})^2 - 1\\
&= 2^{2(2^{k+1})} - 1\\
&= 2^{2^{k+2}} - 1\\
&= (2^{2^{k+2}}+1) - 2\\
&= F_{k+2} - 2\\
&= F_{(k+1)+1} - 2.
\end{aligned}$$

Thus $P(k+1)$ is true.

Since $P(1)$ is true and since for each nonnegative integer k, if $P(k)$ is true, then $P(k+1)$ is true, by the Principle of Mathematical Induction, $P(n)$ is true for all nonnegative integers n. Thus if n is a nonnegative integer, then $F_{n+1} - 2 = F_nF_{n-1}\cdots F_1F_0$. □

Lemma 2. *If n is a nonnegative integer, then* $\gcd(F_{n+1},\ F_nF_{n-1}\cdots F_1F_0) = 1$.

Proof. Let n be a nonnegative integer, and let $d = \gcd(F_{n+1},\ F_nF_{n-1}\cdots F_1F_0)$. Hence $d > 0$. We will show that $d = 1$. By the definition of greatest common divisor, $d \mid F_{n+1}$ and $d \mid (F_nF_{n-1}\cdots F_1F_0)$. By Lemma 1 above, $F_{n+1} - 2 = F_nF_{n-1}\cdots F_1F_0$. We deduce that $d|(F_{n+1}-2)$. Be Theorem 3, it follows that d divides every linear combination of F_{n+1} and $F_{n+1}-2$. In particular $d|(F_{n+1}-(F_{n+1}-2))$, which implies $d|2$. Thus $d = 1$ or $d = 2$. Since Fermat Numbers are odd, $2 \nmid F_{n+1}$ and $2 \nmid F_nF_{n-1}\cdots F_1F_0$ for each n. Hence $d \neq 2$. Consequently $d = 1$. Thus if n is a nonnegative integer, then $\gcd(F_{n+1},\ F_nF_{n-1}\cdots F_1F_0) = 1$. □

Claim. There are infinitely many primes.

Proof. Let $F_n = 2^{2^n} + 1$ for each nonnegative integer n. Note there are infinitely many Fermat numbers. Recall from Lemma 2, $\gcd(F_{n+1},\ F_nF_{n-1}\cdots F_1F_0) = 1$; that is, we know F_{n+1} and $F_nF_{n-1}\cdots F_1F_0$ are relatively prime. Thus they share no common factors in their prime factorization form. Thus, $\gcd(F_i, F_j) = 1$ whenever $i \neq j$. By the Fundamental Theorem of Arithmetic, each F_n has a prime factor p_n. Furthermore, since $\gcd(F_i, F_j) = 1$ for $i \neq j$, it follows that $p_n \nmid F_j$ for $j \neq n$. Since this holds for each n and since there exist infinitely many Fermat numbers, we deduce that each Fermat number will generate a new prime number. Consequently, there exist infinitely many primes. □

4.3 Euler

The next proof of the infinitude of primes that we will examine is from the Swiss mathematician, Leonhard Euler who lived from 1707-1783. His contributions to the field of mathematics range far beyond his work with the prime numbers. Euler is best known for his work in the analysis of infinite sequences and series along with exploring new branches of calculus and topology. It is said that Euler formulated more theorems in the field of number theory than all of his predecessors combined[2]. Many of his findings in number theory are contained in his correspondences with fellow mathematician Goldbach. In a letter correspondence to Goldbach in 1751, Euler said "There are some mysteries that the human mind will never penetrate. To convince ourselves we have only to cast a glance at tables of primes and we should perceive that there reigns neither order nor rule." Euler greatly enjoyed computing large prime numbers in his leisure time and proved there exists infinitely many primes. The proof, written in 1737, is by contradiction and applies the Fundamental Theorem of Arithmetic along with knowledge of the divergent harmonic series.

Claim. There are infinitely many primes.

Proof. We will do a proof by contradiction. Assume there is a finite list of primes given by $p_1, p_2, \ldots, p_n$. Consider the product

$$\prod_{i=1}^{n} \left(1 + \frac{1}{p_i} + \frac{1}{{p_i}^2} + \cdots\right).$$

By expanding this product and applying the Fundamental Theorem of Arithmetic, we can see that every natural number appears exactly once in the denominator. So it follows that each term represents a term in the harmonic series. Thus we have

$$\prod_{i=1}^{n} \left(1 + \frac{1}{p_i} + \frac{1}{{p_i}^2} + \cdots\right) = \sum_{k=1}^{\infty} \frac{1}{k}.$$

Note this product is divergent since it equals the harmonic series which diverges. On the other hand,

$$1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots$$

is a geometric series which converges since the common ratio $\dfrac{1}{p_i} < 1$. Thus,

$$\prod_{i=1}^{n} \left(1 + \frac{1}{p_i} + \frac{1}{{p_i}^2} + \cdots\right) = \prod_{i=1}^{n} \left(\frac{1}{1 - \frac{1}{p_i}}\right) = \prod_{i=1}^{n} \left(\frac{p_i}{p_i - 1}\right).$$

It follows that the product on the right is finite since it is the product of finite terms. Hence

$$\prod_{i=1}^{n} \left(1 + \frac{1}{p_i} + \frac{1}{{p_i}^2} + \cdots\right)$$

converges. In summary, we have

$$\sum_{k=1}^{\infty} \frac{1}{k} = \prod_{i=1}^{n} \left(1 + \frac{1}{p_i} + \frac{1}{{p_i}^2} + \cdots\right) = \prod_{i=1}^{n} \left(\frac{p_i}{p_i - 1}\right).$$

We can see that this leads to a contradiction since $\sum_{k=1}^{\infty} \frac{1}{k}$ diverges and $\prod_{i=1}^{n} \left(\frac{p_i}{p_i - 1} \right)$ converges. Thus, it must follow that there are infinitely many primes. □

4.4 Dirichlet

Another German mathematician who made contributions to number theory and prime numbers is Peter Dirichlet who lived from 1805-1859. Specifically in 1837, he published a proof of Dirichlet's theorem on arithmetic progressions. His proof combined concepts in number theory and mathematical analysis giving rise to a new field of mathematics known as analytic number theory. The theorem is as follows.

Theorem 5. *If a and b are relatively prime positive integers, then the arithmetic progression*

$$a, a + b, a + 2b, a + 3b, \ldots$$

contains infinitely many primes.

The proof of Dirichlet's Theorem is quite involved and extensive and is thus left for the interested reader to find in an Analytic Number Theory textbook. We, however, will consider a proof of a special case of Dirichlet's Theorem when $a = 3$ and $b = 4$.

Claim. There are infinitely many primes of the form $4n + 3$ where n is a nonnegative integer.

Proof. We will do a proof by contradiction. Assume that there is only a finite list of primes $p_1, p_2, p_3, \ldots, p_k$ which are of the form $4n + 3$ where n is a nonnegative integer. Consider the number

$$\begin{aligned} N &= 4p_1p_2p_3 \cdots p_k - 1 \\ &= 4[(4n_1 + 3)(4n_2 + 3)(4n_3 + 3) \cdots (4n_k + 3) - 1] + 3 \end{aligned}$$

where $n_1, n_2, \ldots, n_k$ denote nonnegative integers. Note that N is of the form $4n + 3$. If N is prime, then this contradicts that p_k is our largest prime of the form $4n + 3$. Thus assume N is composite. By the Fundamental Theorem of Arithmetic, N must have a prime factorization; that is, $N = q_1q_2 \cdots q_t$ where the q_i's denote prime numbers, not necessarily distinct. Since N is odd, every q_i will be of the form $4n + 3$ or $4n + 1$.
We will first show that at least one of the factors, q_j, is of the form $4n + 3$. Let us suppose not. Then each q_j is of the form $4j + 1$. Consider

$$(4r_1 + 1)(4r_2 + 1) = 4(4r_1r_2 + r_1 + r_2) + 1.$$

Since the product of two numbers of the form $4j + 1$ is also of the form $4j + 1$, we deduce that N is of the form $4j + 1$; however, this contradicts that N is of the form $4n + 3$. Consequently, at least one of the factors, say q_1 is of the form $4n + 3$. Thus, $q_1 \in \{p_1, p_2, \ldots, p_k\}$. So $q_1 = p_i$ for some $i \in \{1, 2, \ldots, k\}$. Since p_i is a prime factor of N, we have $p_i \mid N$. Note that

$$N + 1 = 4p_1p_2p_3 \cdots p_k.$$

It follows that $p_i \mid (N+1)$. Since p_i divides N and p_i divides $N+1$, by Theorem 3, the prime p_i divides each linear combination of N and $N+1$. In particular, $p_i \mid (-1N + (N+1))$ which implies that $p_i \mid 1$. Thus $p_i = \pm 1$, and hence is not prime. However, this contradicts that p_i is a prime number. Consequently, there must be infinitely many primes of the form $4n+3$. □

It is important to note that not all integers in the arithmetic progression of $4n+3$ will be prime. Take $n = 3$ and we have $4(3) + 3 = 12 + 3 = 15$, which we know is not prime. This fact extends to Dirichlet's Theorem as well. If a and b are relatively prime, we are not guaranteed that $a + nb$ is prime for all nonnegative integers n. However, we are guaranteed that if the arithmetic progression is carried out indefinitely, it will contain infinitely many primes.

Claim. There are infinitely many primes.

Proof. Take a and b to be natural numbers that are relatively prime. Then by Dirichlet's Theorem, the arithmetic progression

$$a, a+b, a+2b, a+3b, \ldots$$

contains infinitely many primes. Thus, in conclusion, we have there are infinitely many primes. □

One application of Dirichlet's Theorem is that we can find infinitely many primes ending in a particular sequence of digits. Take 1000 and 999. Theorem 4 tells us that $\gcd(1000, 999) = 1$. Thus consider the arithmetic progression

$$1999, 100999, 1000999, \ldots$$

given by $1000n + 999$. We can conclude with Dirichlet's Theorem, there exist infinitely many primes whose last three digits are given by 999.

4.5 Erdős

The Hungarian mathematician Paul Erdős, 1913-1996, contributes his thoughts on the infinitude of primes in our next proof. First we will show that every integer greater than 1 is the product of a square-free integer and a perfect square. In the proof that there exists infinitely many primes, Erdős fixes a lower bound on the number of primes less than or equal to a given integer and shows this lower bound increases without bound causing the number of primes to behave in the same manner. There do exist better approximations on the number of primes less than or equal to a given integer than the one found in Erdős' proof, yet for the sake of proving that there are infinitely many this lower bound works perfectly.

Lemma 3. Every integer $n > 1$ is the product of a square-free integer and a perfect square.

Proof. Let $n > 1$ be an integer. By the Fundamental Theorem of Arithmetic

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

where the p_j's are distinct primes and k_j's are positive integers. Each k_i is either even or odd, so we can write k_i in the form $2q_i + r_i$ where $r_i = 1$ for odd integers and $r_i = 0$ for even integers. For the odd k_i's, we have

$$p^{k_i} = p^{2q_i + r_i} = p^{2q_1 + 1} = p^1 p^{2q_i}.$$

Since multiplication is both commutative and associative, we regroup our primes and let a be the product of primes of the form p^1 and let b be the product of all the remaining factors of n which are of the form p^{2q_i}. Since a is the product of distinct primes, a is a square-free integer. Since b is the product of primes with even exponents, b is a perfect square. Thus since n is arbitrary, every integer greater than 1 is the product of a square-free integer and a perfect square. □

Claim. There are infinitely many primes.

Proof. Let $n > 1$ be an integer. By Lemma 3, we know n can be factored as the product of a square-free integer and a perfect square. First we would like to count the number of square-free integers less than n. In the proof of Lemma 3, we saw that the square-free product of n is a product of distinct primes. If we view this as a subset of primes, then an upper bound on the number of square-free numbers less than n is given by $2^{\pi(n)}$ where $\pi(n)$ is the number of primes less than or equal to n. Next we would like to count the number of perfect squares less than n. At most we would have $\sqrt{n}$ square numbers less than n because if the number of square numbers was greater than $\sqrt{n}$ then this would imply the square-number squared would be greater than n. This cannot happen since n is the product of a square-free number and perfect square. Hence, at most there are $2^{\pi(n)}$ square-free numbers and $\sqrt{n}$ square numbers less than n. The circumstance which would utilize the extreme upper bound would be when

$$n = q_1 q_2 q_3 \cdots q_t p_1^{2k_1} p_2^{2k_2} p_3^{2k_3} \cdots p_i^{2k_i}$$

such that the square terms and the square-free terms share no common prime. Then we can put a bound on n by the following

$$n \leq 2^{\pi(n)} \sqrt{n}.$$

Through algebra we can obtain a bound on $\pi(n)$ as follows

$$\begin{aligned} n \leq 2^{\pi(n)} \sqrt{n} &\implies \frac{n}{\sqrt{n}} \leq 2^{\pi(n)} \\ &\implies \log_2 \sqrt{n} \leq \log_2 2^{\pi(n)} \\ &\implies \log_2 n^{\frac{1}{2}} \leq \pi(n) \\ &\implies \frac{1}{2} \log_2(n) \leq \pi(n). \end{aligned}$$

Since $\frac{1}{2} \log_2(n)$ is unbounded as n approaches infinity and $\pi(n)$ is bounded below by $\frac{1}{2} \log_2(n)$, we deduce that $\pi(n)$ must be unbounded as n approaches infinity as well. Since $\pi(n)$ is the number of prime numbers less than or equal to an arbitrary n, we can conclude the number of primes is infinite. □

4.6 Wunderlich

In 1965, M. Wunderlich of the University of Colorado proved there exist infinitely many primes in a way mathematicians had not yet seen before through the use of Fibonacci numbers[7]. The Fibonacci sequence is named after Leonardo Fibonacci, an Italian mathematician, who in his 1202 book *Liber Abaci* proposed a question concerning the reproduction rate of rabbits. Fibonacci numbers have the property that, except for the first two, any number is the sum of the two immediately

preceding Fibonacci numbers; that is, $F = \{1, 1, 2, 3, 5, 8, \dots\}$. Wunderlich worked extensively with Fibonacci numbers and the following result will be used in his proof of the infinitude of primes.

Lemma 4. The greatest common divisor of two Fibonacci numbers is again a Fibonacci number; specifically,

$$\gcd(F_m, F_n) = F_d \text{ where } d = \gcd(m, n).$$

For interested readers a proof of this result can be found in Koshy's *Elementary Number Theory with Applications* textbook.

Claim. There are infinitely many primes.

Proof. We will do a proof by contradiction. Assume there exists only a finite number of primes

$$\{2, 3, 5, \dots, 37, 41, 43 \dots p_n\}$$

where p_n denotes the largest prime. We then consider the corresponding Fibonacci numbers

$$F_2, F_3, F_5, \dots, F_{37}, F_{41}, F_{43}, \dots, F_{p_n}.$$

From Lemma 4 we know each of these pairs of Fibonacci numbers is relatively prime since any two pairs of primes share no common factors. By the Fundamental Theorem of Arithmetic each of these Fibonacci numbers is divisible be a prime number, and each prime divisor is different since F_i's are relatively prime. Note we exclude F_2 since $F_2 = 1$ and 1 is not prime. Thus we have n prime numbers and $n - 1$ corresponding Fibonacci numbers. At most one of these corresponding Fibonacci numbers has exactly two prime factors while the others have exactly one prime factor. In particular, F_{37} will have at most two prime factors. On the other hand, note that $F_{37} = 73(149)(2221)$. Hence F_{37} has three prime factors, which is a contradiction. In summary the finite list of primes is incomplete, and it must follow there exists infinitely many primes. □

4.7 Saidak

One of the most recent proofs of the infinitude of primes was given by Filip Saidak, an associate professor at the University of North Carolina at Greensboro in 2006. This proof is unique in that it is a concise direct proof that relies solely on the property that consecutive integers are relatively prime.

Claim. There are infinitely many primes.

Proof. Let n_1 be an arbitrary positive integer. Let $n_2 = n_1(n_1 + 1)$. By Theorem 4, we know $\gcd(n_1, n_1 + 1) = 1$. Since n_1 and $n_1 + 1$ are relatively prime, we know they do not share any common prime factors. It follows that there exists at least two different prime factors p_1 and p_2 such that $p_1 \mid n_1$ and $p_2 \mid (n_1 + 1)$. Next consider $n_3 = n_2(n_2 + 1)$. Again by Theorem 4, we know $\gcd(n_2, n_2 + 1) = 1$. Since n_2 and $n_2 + 1$ are relatively prime, we know they do not share any common prime factors. It follows that there exists at least three different prime factors p_1, p_2, and p_3 such that $(p_1 p_2) | n_2$ and $p_3 | n_2 + 1$. Similarly $n_4 = n_3(n_3 + 1)$ will result in four different prime factors. We can continue this process indefinitely adding a new prime factor with each iteration. Hence there exists infinitely many primes. □

5 Importance of Prime Numbers

Mathematicians continue to be amazed by the prime numbers, and research into the primes will show that there are several other proofs of the infinitude of primes that involve vast branches of mathematics such as topology and analytic number theory. Many of the open conjectures in number theory involve prime numbers. Mathematics believe there exist infinitely many twin primes and yet there has not been a valid proof of the conjecture recorded. Another conjecture concerning the prime numbers is one of the Clay Mathematics Institute's Millennium Prize problems: the Riemann hypothesis. The formal hypothesis, proposed by Bernhard Riemann in 1859, states that all nontrivial zeros of the Riemann zeta function have real part one-half[3]. The implication of the Riemann hypothesis is a distribution mapping of the prime numbers. A look at the prime numbers may suggest their distribution is random, but the Riemann hypothesis states otherwise. Mathematicians dedicate so much time to the study of the primes because, as Jordan Ellenberg, a contributor to Math Horizons states, the understanding of primes may actually be the true understanding of randomness. He follows with "How wonderfully paradoxical: What helps us break down the final mysteries about prime numbers may be new mathematical ideas that structure the concept of structurelessness itself" [4].

In his 1940 essay, *A Mathematician's Apology*, number theorist Godfrey Hardy wrote that the proof that there exists infinitely many primes had only the slightest practical importance. Prime numbers may not appear as though they deserve any more attention than other distinctions of numbers, but with the evolution of internet coding and cryptography, the prime numbers are increasingly important. Cryptology is defined as the "science of concealing the meaning of confidential communications from all except the intended recipients." [8] In early cryptosystems, some type of key would have to be transmitted in secrecy to uphold the security of the message; however, in 1977 Rivest, Shamir, and Adleman proposed a public-key encryption system that would change the face of cryptography forever. Known as RSA, this system is founded in elementary number theory concepts, and the security lies in the inability to factor a number that is the product of two large primes, each over 200 digits. RSA cryptography is now the means by which most of the internet transactions rely on. Whenever an online customer enters his or her credit card number, the website encrypts this long string of numbers so that hackers cannot steal the private information. Without knowledge of the website's particular key, a hacker cannot recover the original string of numbers. The same process is used whenever an email is sent in order to keep the privacy of the information upheld. Knowledge of the two primes is the key to unlocking the secrets that RSA holds.

Lastly, the prime numbers are important because they appear in many number theory concepts. One example of this is when working with modular arithmetic. Note Fermat's little theorem states $a^{p-1} \equiv 1 \pmod{p}$ whenever $\gcd(a, p) = 1$; that is, $a^{p-1} - 1$ is an integer multiple of p where p is prime. Another example is Wilson's theorem which states a natural number $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Proofs of these theorems can be found in any traditional elementary number theory textbook [1][7]. By studying the prime numbers, mathematicians such as Fermat and Wilson were able to better understand the natural numbers. This is primarily because prime numbers are the basic building blocks of the natural numbers since every natural number can be represented in exactly one way as the product of prime powers. By expressing natural numbers in their prime factorization form, mathematicians can easily deduce the greatest common divisor or the least common multiple of a given set of natural numbers.

6 Conclusion

Many properties of all integers can be traced back to the foundation: their prime factors. Although each mathematician gives a subsequent proof of the same claim, each is done in a new manner which reveals more insight into the primes and consequently more insight into the natural numbers as a whole. It was the mathematician Carl Friedrich Gauss who summarized the efforts of all who explore prime numbers in his 1801 work *Disquisitiones Arithmeticae*.

> *The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length... Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.*

There is no way to determine how many new proofs of the infinitude of primes will emerge in later years. In 1996, *The New Book of Prime Number Records* gave that there are eleven distinct proofs of the infinitude of primes, but since then there have been later additions. Research into the different ways to prove the infinitude of primes will produce proofs which utilize various fields of mathematics ranging from analytical proofs by Juan Pablo Pinasco and Junho Peter Whang to a topological proof by Hillel Furstenberg. While the final line in each proof is always a slight variation of a statement of the prime's infinitude, this should not discourage the interested and intrigued reader from exploring how each mathematician arises at this conclusion in their own unique way. New information about the primes is uncovered with each successive proof. Eventually, if the mathematics community is lucky enough, in a million years we will fulfill Erdős' prophecy and unlock the mystery of the primes.

References

[1] Burton, David M. *Elementary Number Theory*. 6th ed. New York, NY: McGraw-Hill, 2007.

[2] Calinger, Ronald. *Classics of Mathematics*. Oak Park, IL: Moore Pub., 1982.

[3] Du, Sautoy Marcus. *The Music of the Primes: Searching to Solve the Greatest Mystery in Mathematics*. New York: HarperCollins, 2003.

[4] Ellenberg, Jordan. *The Beauty of Bounded Gaps*. Math Horizons Sept. 2013: 5-7.

[5] Euclid, and Thomas Little Heath. *The Thirteen Books of Euclid's Elements*. New York: Dover Publications, 1956.

[6] "GIMPS Home." GIMPS Home., 5 Feb. 2013. Web. http://www.mersenne.org/

[7] Koshy, Thomas. *Elementary Number Theory with Applications*. San Diego: Harcourt/Academic, 2002.

[8] Trappe, Wade, and Lawrence C. Washington. *Introduction to Cryptography: With Coding Theory*. Upper Saddle River, NJ: Pearson Prentice Hall, 2006.