THE INFINITY OF PRIMES

ADRIAN PĂCURAR

Contents

1. Introduction 2
2. Euclid's Proof 2
3. Proof Using Fermat Numbers 3
4. Proof Using Group Theory 4
5. Proof Using Euler's Product 5

1. Introduction

The study of prime numbers has been around since antiquity, and even today they hold a special interest in the heart of many mathematicians - there is an entire branch of mathematics dedicated to their study, called number theory. Before we go any further, let's define what a prime number actually is:

Definition 1. A number $p \geq 2$ is prime whenever its only positive divisors are 1 and p.

Primes appear in high school math (or earlier depending on the country you grew up in), when talking about factoring integers, dealing with fractions (greatest common denominator, least common multiple), etc. But usually one has to wait until undergrad and take an introductory number theory course in order to get to learn more about them. One of the oldest and very natural question to ask is "how many primes are there?"

Theorem 1. There are infinitely many primes.

Throughout history there have been numerous proofs of this result. They are all very interesting to read, and some require more knowledge of mathematics to understand than others. I am presenting a few that I have found from various sources here.

2. Euclid's Proof

Proof. Let $\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$ denote the set of prime numbers, and suppose that there are only finitely many primes (r total). Then we can list them in increasing order as follows:

$$\mathbb{P}_r = \{p_1, p_2, \dots, p_r\}.$$

What happens if we multiply them all together, i.e what can we say about the number $p_1 \cdot p_2 \dots p_r$? It will be divisible by all the primes in our list. For example, if r was just 4, then the number $2 \cdot 3 \cdot 5 \cdot 7 = 210$ is divisible by all the primes $2, 3, 5, 7$. Now consider

$$N = p_1 \cdot p_2 \dots p_r + 1$$

which is one more than the product of all primes we just discussed. But then notice that N cannot be divisible by any prime p_i in our list. In other words the only positive divisors of N are going to be 1 and N, which means N is also a prime number (by our definition).

Lastly, notice that N is larger than any prime in our list, and this contradicts the assertion that $\mathbb{P}$ was the set of all primes. We see then that a finite set cannot be the set of all primes (we will always arrive to this contradiction), so there must be infinitely many primes. □

This is the proof I learned when I first took number theory, but is a slight variation of this proof listed in *Proofs From The Book*, which goes as follows: we look at $N = p_1 \cdot p_2 \dots p_r + 1$, which will have some prime divisor p. Now, if p was on our list, then p will divide both N and the product $p_1 \dots p_r = N - 1$.

Any time a prime number divides two numbers A and B, it will also divide their sum and difference, so p must divide $N - (N - 1) = 1$, which is a impossible, since 1 is smaller than any prime.

3. Proof Using Fermat Numbers

Definition 2. The Fermat numbers are numbers of the form $F_n = 2^{2^n} + 1$, where n is a nonnegative integer.

For example, the first few fermat numbers are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_5 = 65537$, etc. They have many interesting properties (see Wikipedia for the basics), but one property of particular interest to us is the recursive formula that they satisfy:

Theorem 2. The Fermat numbers satisfy, for $n \geq 1$

$$F_n = 2 + \prod_{i=0}^{n-1} F_i$$

with initial condition $F_0 = 3$.

Proof. We proceed by induction on n. For the base case ($n = 1$), notice that $F_1 = 5$ and the recursive formula gives $2 + F_0 = 2 + 3 = 5$. Next, using induction, we have

$$\begin{aligned}
2 + \prod_{i=0}^{n} F_i &= 2 + \left(\prod_{i=0}^{n-1} F_i\right) \cdot F_n \\
&= 2 + (F_n - 2)F_n \qquad \text{(by the inductive hypothesis)} \\
&= 2 + (2^{2^n} + 1 - 2)(2^{2^n} + 1) \qquad \text{(since } F_n = 2^{2^n} + 1\text{)} \\
&= 2 + (2^{2^n} - 1)(2^{2^n} + 1) \\
&= 2 + \left(2^{2^n}\right)^2 - 1^2 \\
&= 2^{2 \cdot 2^n} + 1 \\
&= 2^{2^{n+1}} + 1
\end{aligned}$$

but this is precisely F_{n+1}, as needed. □

Corollary 1. The Fermat numbers are relatively prime.

Proof. Pick any two distinct Fermat numbers F_a and F_b, and let d be a common divisor of both. Then d must also divide the difference, i.e. d divides $(2^{2^a} + 1) - (2^{2^b} + 1)$, so d must divide 2. Then the only possible values for d are 1 or 2. But since all Fermat numbers are odd, d cannot be 2, so $d = 1$ (which means the only common factor of F_a and F_b is 1, i.e. they are relatively prime). □

The fact that are infinitely many primes follows immediately from Corollary 1. There are infinitely many Fermat numbers, and since they are all relatively prime, this means that each Fermat number introduces one or more new primes (either the Fermat number itself is a prime, or it factors into new primes that do not divide any of the preceeding Fermat numbers).

4. Proof Using Group Theory

Before presenting the proof, we introduce the definition of a group, and a few examples.

Definition 3. A group is an ordered pair $(G, *)$ where G is a set of elements, and $*$ is a binary operation on G satisfying the following axioms:

(i) $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$ (associativity)
(ii) there exist an identity element $e \in G$ such that for all $a \in G$, $a * e = e * a = a$
(iii) for each $a \in G$, there exist an inverse $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$

A group is called abelian (or commutative) whenever $a * b = b * a$ for all $a, b \in G$. A few examples of abelian groups are listed below:

- The integers $\mathbb{Z}$ under the addition operation $+$
- The nonzero rational numbers $\mathbb{Q} \setminus \{0\}$ under multiplication (the removal of zero ensures the existance of inverses for every element)
- The group $\mathbb{Z}/n\mathbb{Z}$ under addition modulo n
- The group $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$ under multiplication modulo n. For $n = 9$, we obtain $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$. The multiplicative inverses of these elements are $\{1, 5, 7, 2, 4, 8\}$, respectively. When n is prime, $(\mathbb{Z}/n\mathbb{Z})^\times$ will have exactly $n - 1$ elements $\{1, 2, 3, \ldots, n - 1\}$.

Definition 4. The order of an element a in a group G is the smallest integer d such that $a^d = \underbrace{a * a * \cdots * a}_{d \text{ times}} = e$. The order of a group is the size of the group (can be infinite).

Theorem 3. (Lagrance) If G is a finite multiplicative group, the order of any element divides the order of the group.

We need one last definition before we give the proof.

Definition 5. We say $a \equiv b \pmod{n}$ (a is congruent to b modulo n) whenever $n|(a - b)$.

Armed with this information, we are finally ready to give the group theoretic proof of the infinity of primes.

Proof. Suppose the set of all primes $\mathbb{P}$ is finite, and p is the largest prime. Consider the number $2^p - 1$ (numbers of this form are called Mersenne numbers). If we can show that every prime factor q of $2^p - 1$ is larger than p, then we are done (as it would contradict p being the largest prime). Let q be any prime factor of $2^p - 1$. Then by the definition of congruence, we have $2^p \equiv 1 \pmod{q}$.

Consider the (finite) multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$, so the order of element $2 \in (\mathbb{Z}/q\mathbb{Z})^\times$ is p. But then by Lagrange's theorem, p must divide the size of the group, which is $q - 1$. Since $p|(q - 1)$, it follows that p is less than q, as desired. $\square$

5. Proof Using Euler's Product

For this proof, we will need to use the following theorem:

Theorem 4. (Fundamental Theorem Of Arithmetic) Every integer has a unique prime factorization.

Now, suppose $\mathbb{P}$ is the set of all primes. The Euler product for the Riemann zeta function is given by

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}}$$

where the product is taken over all primes. To see why this is true, we can expand $\frac{1}{1-1/p^s}$ using geometric series, so we have

$$\prod_{p\in\mathbb{P}} \frac{1}{1-1/p^s} = \prod_{p\in\mathbb{P}} \sum_{k=0}^{\infty} \left(\frac{1}{p^s}\right)^k = \sum_{k\geq 0} \left(\frac{1}{2^s}\right)^k \times \sum_{k\geq 0} \left(\frac{1}{3^s}\right)^k \times \sum_{k\geq 0} \left(\frac{1}{5^s}\right)^k \times \sum_{k\geq 0} \left(\frac{1}{7^s}\right)^k \times \dots$$

Multiplying the sums out, we obtain something of the form

$$\sum_{r_1,r_2,r_3,\dots\geq 0} \frac{1}{2^{sr_1}3^{sr_2}5^{sr_3}5^{sr_4}\dots} = \sum_{k\geq 0} \frac{1}{n^s}$$

so we have the desired equality given by Euler's product. Finally we use this to argue the infinitude of primes.

Proof. Begin by setting $s = 1$, so we have

$$\prod_{p\in\mathbb{P}} \frac{1}{1-1/p} = \sum_{n\geq 1} \frac{1}{n} = \infty$$

Now, the sum on the RHS is the harmonic series, which diverges to infinity. If $\mathbb{P}$ had only finitely many primes, the LHS would be finite as it would be a product of finitely many factors. Thus $\mathbb{P}$ contains infinitely many primes. □