SIX PROOFS OF THE INFINITUDE OF PRIMES

ALDEN MATHIEU

1. Introduction

The question of how many primes exist dates back to at least ancient Greece, when Euclid proved the infinitude of primes (circa 300 BCE). Later mathematicians improved the efficiency of identifying primes and provided alternative proofs for the infinitude of primes. We consider 6 such proofs here, demonstrating the variety of approaches.

We follow Ronan O'Gorman's presentation of the material from [1], including a proof of Lagrange's Theorem.

2. Infinitude of Primes

In the proofs below, we denote the set of prime numbers $\mathbb{P} = \{2, 3, 5, ...\}$. We also use two key facts:

2.1. **First Fact.** The set of natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$ is unbounded, because there is a natural ordering on $\mathbb{N}$ and we can always add 1 to the "largest" $n \in \mathbb{N}$ to generate an even larger one.

2.2. **Second Fact.** Prime factorization is unique. That is, for all natural numbers $n \neq \pm 1$, we can uniquely represent n as the product of primes: $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, p_i \in \mathbb{P}, k_i \in \mathbb{Z}$ and $k_i \neq 0, \forall i$.

The below proofs consist of repackaging these two facts increasingly cleverly, observed O'Gorman.

3. Euclid (300 BCE)

Euclid included this proof in his *Elements* (Book IX, Proposition 20). Of course, that was in Greek.

Theorem 3.1. *The set of primes is infinite.*

Proof. Assume there exists finitely many primes. That is, $\mathbb{P} = \{p_1, p_2, \cdots, p_r\}$ for $r < \infty$. Consider the product $\pi = p_1 \cdots p_r$ and using our First Fact, add 1: $\pi = p_1 \cdots p_r + 1$.

By the Second Fact, we can factorize π into primes. So there exists $q \in \mathbb{P}$ such that $q \mid \pi$, and thus q also divides $p_1 \cdots p_r$. Thus, $q \mid 1 \implies q = 1$. But then $q \notin \mathbb{P}$, a contradiction. So a finite set cannot contain all primes. □

4. Goldbach (1742)

Goldbach follows a similar approach, while making more specific demands on the form of the prime.

Date: 19 September 2018.

4.1. **Fermat numbers.** We define a Fermat number to be of the form $F_n = 2^{2^n} + 1$ for $n = 0, 1, 2, \ldots$ Goldbach noted that this form means all Fermat numbers are relatively prime. We prove this below.

Theorem 4.1. *All Fermat numbers are relatively prime.*

Proof. Assume there exists $q \in \mathbb{P}$ and let F_k and F_n be Fermat numbers. If $q \mid F_k$ and $q \mid F_n (k < n)$, then $q \mid 2$. Hence, $q = 1$ or 2 (by our Second Fact). But it is clear on inspection that all Fermat numbers are odd, so $q \nmid 2$. Thus, $q = 1$ and F_k, F_n are relatively prime. □

The following proof was omitted from O'Gorman's presentation for time but we include it here for completeness.

Theorem 4.2. *We can generate Fermat numbers using the recursion* $\prod_{k=0}^{n-1} F_k = F_n - 2$ $(n \geq 1)$.

Proof. We prove the recursion by induction on n.
For $n = 1, F_0 = 3, F_1 - 2 = 3 \implies F_1 = 5$.
Thus we have, by arithmetic and substitution,

$$\begin{aligned}\prod_{k=0}^{n} F_k = (\prod_{k=0}^{n-1} F_k)F_n &= ((2^{2^n} + 1) - 2)(2^{2^n} + 1) \\ &= (2^{2^n} - 1)(2^{2^n} + 1) \\ &= 2^{2^{n+1}} - 1 \\ &= (2^{2^{n+1}} + 1) - 2 = F_{n+1} - 2\end{aligned}$$

It follows immediately that since the only common divisor any of them share is $q = 1$, there are infinitely many primes. □

5. Mersenne Primes

Similar to the two previous proofs, we consider prime "Mersenne numbers," named for the 17th-century friar Marin Mersenne who studied them.

We first state and prove Lagrange's Theorem, which will be used in the proof regarding Mersenne primes.

Theorem 5.1 (Lagrange's Theorem)**.** *If G is a finite multiplicative group and $U \subseteq G$ a subgroup, then the order of U divides the order of G.*

Proof. Consider the binary relation $a \sim b :\leftrightarrow ba^{-1} \in U$. We confirm it is a valid equivalence relation:

Reflexive $a \sim a \implies aa^{-1} \in U \implies e \in U$, where e indicates the multiplicative identity, by definition of a subgroup.

Symmetric If $a \sim b \implies ba^{-1} \in U$, then $(ba^{-1})^{-1} \in U$ because the subgroup is closed under taking inverses. $b^{-1}a \in U \implies ab^{-1} \in U$, therefore $b \sim a$.

Transitive

$$\begin{aligned} a \sim b, b \sim c &\implies ba^{-1} \in U \\ &\implies (ba^{-1})(cb^{-1}) \in U \\ &\implies ea^{-1}c \in U \\ &\implies a^{-1}c \in U \\ &\implies ca^{-1} \in U \therefore a \sim c \end{aligned}$$

Thus it is indeed a valid equivalence relation and hence it forms a partition.

The equivalence class of a, $[a]$, is the right coset $Ua = \{xa : x \in U\}$. Since the order of Ua equals the order of U, we see that G decomposes into equivalence classes of size $|U| \implies |U|$ divides $|G|$. □

5.1. **Mersenne numbers.** We define a Mersenne number to be of the form $M_n = 2^n + 1$ for $n \in \mathbb{Z}$. Note that M_n is not necessarily prime. Specifically, if n is not prime (ie, composite: $n = ab$ for some $a, b, \in \mathbb{Z}$) then $2^n - 1$ is also not prime (since $2^a - 1 \mid 2^{ab} - 1, 2^b - 1 \mid 2^{ab} - 1$). Thus, a Mersenne prime requires a prime power.

Theorem 5.2. *Suppose $\mathbb{P}$ finite, and p is the largest prime. Let $q \in \mathbb{P}$ be prime such that $q \mid 2^p - 1$. Then $q > p$.*

Proof. If $q \mid 2^p - 1 \implies 2^p \equiv 1 \pmod{q}$. Since p is prime by assumption, this means that $|2| = p$ in the group of multiplicative integers mod q ($\mathbb{Z}_q^*$).

Assume $2^n = 1$, $n < p$. Then $\gcd(n, p) = 1$ and thus there exists $x, m \in \mathbb{N}$ such that $mn = xp + 1$, by the Euclidean algorithm. So $1 \equiv 2^n$ for some $n \in \mathbb{N} \implies 1^m \equiv 2^{mn} \equiv 2^{xp+1} \equiv 2(2^p)^x \equiv 2 \pmod{q}$, because $1 \not\equiv 2 \bmod q$ for any $q \in \mathbb{P}$.

By Lagrange's Theorem, we therefore have that the order of every element divides the order of the group, thus $p \mid |\mathbb{Z}_q^*| = q - 1$ and hence $p < q$.

But p was the largest prime by assumption, so we have a contradiction; hence, the set of primes $\mathbb{P}$ is not finite. □

6. Euler (1737)

This proof, involving the manipulation of infinite series, is O'Gorman's least favorite. While [1] relies on a proof using logarithms, we follow O'Gorman's presentation in using harmonic series.

Let $\mathbb{P} = \{p_1, p_2, p_3, \cdots\}$ be the set of primes in increasing order. Let $\pi(n)$ be the function that couns the number of primes less than or equal to $n \in \mathbb{R} : \pi(n) := \#\{p \in \mathbb{P}, p \leq n\}$. Let H_n be the harmonic series: $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{a}$, which we know diverges by first year analysis.

Theorem 6.1. *H_n diverges, thus $\pi(n)$ diverges, and thus the number of primes is infinite.*

Proof. Let $\sigma_n = \sum_{m \in \mathbb{N}} \frac{1}{m}$ where m has only prime divisors $\leq n$. Note that $H_n < \sigma_n$ (because H_n is contained in it) though we do not know if σ_n converges.

But because both series have exclusively positive terms, by first year analysis, we know that if they are convergent, then they are absolutely convergent.

We rearrange σ_n, using our Second Fact:

$$\sigma_n \leq \prod_{k=1}^{\pi(n)} \sum_{i \geq 0} (\frac{1}{p^i})$$

Since the sum is positive and geometric, it converges; thus we have an absolutely convergent series and equality:

$$\sigma_n = \prod_{k=1}^{\pi(n)} \sum_{i \geq 0} (\frac{1}{p^i})$$

We examine the formula for a geometric series:

$$\prod_{k=1}^{\pi(n)} \frac{1}{1 - \frac{1}{p^k}} \text{ and note that } p^k \geq k + 1.$$

After rearrangement and computation, we get

$$\prod_{k=1}^{\pi(n)} 1 + \frac{1}{p^k - 1} \leq \prod_{k=1}^{\pi(n)} 1 + \frac{1}{k} = \prod_{k=1}^{\pi(n)} 1 + \frac{k+1}{k}$$

Because the right hand side is a telescoping series equal to $\pi(n) + 1$, we have $H_n < \pi(n) + 1$, and since H_n diverges, $\pi(n) + 1$ must also diverge. Hence, the quantity of primes is infinite. □

7. Fürstenberg (1955)

This proof, written while Fürstenberg was an undergraduate in New York, relies on topology and proof by contradiction.

Theorem 7.1. *P cannot be finite.*

Proof. We define sets $N_{a,b} = \{a + nb : n \in \mathbb{Z}\}$ where $a, b \in \mathbb{Z}$ and $b > 0$. We define a topology on $\mathbb{Z}(\tau)$ such that $A \in \tau$ if and only if $\forall a \in A, \exists b \in \mathbb{N}$ such that $N_{a,b} \in A$. O'Gorman omitted the proof that τ forms a topology but it is easily verified:

- $\emptyset$ is open by definition, and the whole space $\mathbb{Z}$ is $N_{1,0}$ and hence also open.
- Any union of open sets is open: let $\cup_{i=1} A_i$ be a union of open sets and let $x \in \cup_{i=1} A_i$. Thus for any a_j such that $N_{a_j,x}$ belongs to the open set A_j, $N_{a_j,x}$ also belongs to the union.
- Any finite intersection of open sets is open: let A_i, A_j be open and let x be in their intersection. Then $\exists a_i$ such that $N_{a_i,x} \in A_i$ and $\exists a_j$ such that $N_{a_j,x} \in A_j$. We pick $a = \text{lcm}(a_i, a_j)$, which means $N_{a,x} = A_i \cap A_j$.

Hence, this defines a valid topology τ on $\mathbb{Z}$.

We observe that any $A \neq \emptyset$ in the topology τ is infinite, because by the First Fact, $\mathbb{N}$ is infinite.

$N_{a,b} = \mathbb{Z} \setminus \cup_{i=1}^{b-1} N_{a+i,b}$ where the union $\cup_{i=1}^{b-1} N_{a+i,b}$ is an open set. Hence, $N_{a,b}$ is the complement of an open set and therefore closed.

By the Second Fact, for all integers $n \pm 1$, $n \in N_{0,p}$ for some prime $p \in \mathbb{P}$. We consider the set {-1, 1}. By the above, this clearly equals $\mathbb{Z} \setminus \cup_{p \in \mathbb{P}} N_{0,p}$.

If $\mathbb{P}$ were finite, this union would be a finite union of closed sets and hence closed. As the complement of a closed set, $\{-1, 1\}$ would be open and thus would be infinite, a contradiction.

We conclude $\mathbb{P}$ must be infinite. □

8. Erdös (1938)

Similiar to Euler's proof, this is O'Gorman's favorite. We prove the infinitude of primes, and get that the sum of reciprocals of primes diverge for free.

Theorem 8.1. *$\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverges and hence $\mathbb{P}$ is infinite.*

Proof. We assume $\sum_{p \in \mathbb{P}} \frac{1}{p}$ converges. If so, then there exists some $k \in \mathbb{N}$ such that $\sum_{i \geq k} \frac{1}{p_i} < \frac{1}{2}$. Then we can extend this to arbitrary $N \in \mathbb{N}$:

$$\sum_{i \geq k} \frac{N}{p_i} < \frac{N}{2} \tag{1}$$

This is useful becasue it tells us something about "big primes" and we can show that there isn't enough "small primes."

We define "big primes" $B_n := \{m < n : p_i \mid m \text{ for some } i \geq k\}$ and "small primes" $S_n := \{m < n : p_i \mid m \text{ for some } i < k\}$. Therefore, all numbers are divisible by some B_n, S_n.

We can form a partition since $\#B_n + \#S_n = n$. Note that the floor function $\lfloor \frac{N}{p_i} \rfloor$ counts the multiples of $p_i \in \mathbb{Z}$. This places a bound, using (1) :

$$B_n \leq \sum_{i \geq k} \lfloor \frac{N}{p_i} \rfloor < \frac{N}{2} \tag{2}$$

For every $m \in S_n$, we write m as

$$m = a_m b_m^2 \tag{3}$$

where a_m is square-free and equals 1 copy of each prime divisor raised to an odd power.

Thus by our Second Fact, m is the product of distinct "small primes." Due to $\#S_n$, there are 2^{k-1} possibilities for a_m.

Returning to (3), $b_m^2 \leq m < n$, so $b_m \leq \sqrt{m} < \sqrt{n} \implies \#S_n = 2^{k-1}\sqrt{n}$. We choose n large, such that $\sqrt{n} > 2^k \implies 2^{k-1} < \frac{\sqrt{n}}{2} \implies \#S_n < \frac{\sqrt{n}\sqrt{n}}{2} = \frac{n}{2}$. But by (2), $\#S_n + \#B_n < n$, a contradiction. Hence, $\mathbb{P}$ must be infinite.

□

References

[1] Martin Aigner and Günter M. Ziegler. *Proofs from The Book*, chapter 1, pages viii+308. Springer-Verlag, Berlin, fifth edition, 2014. Including illustrations by Karl H. Hofmann.