Hoper edei deixai.

Finley Pumford

March 2026

From Wales

1 Introduction.

Despite being an atheist, the mathematician Paul Erdős often mentioned that there exists a metaphorical collection of all the perfect mathematical proofs, called *The Book*, where God keeps the most insightful and elegant proof of every mathematical theorem. Among the many candidates for such a collection, there is a proof that I believe emerges superior.

Over 2000 years ago, Euclid proved that there are an infinite number of prime numbers. That proof stands today exactly as it stood then. It is a proof nearly everyone studying mathematics knows of, but if I were to ask you to prove that there are an infinite number of primes in a different way, could you? If I were to ask you how many proofs there are for this theorem, what would you guess? Ten? A hundred?

There are at least two hundred known proofs of this theorem. Proofs that have emerged from virtually every corner of mathematics - Algebra, Number Theory, Analysis and even Topology. In this essay, we're going to prove some, closely following the paths mathematicians have strolled through in the past, each perhaps a page in *The Book*.

2 Euclid's theorem.

Let's start where it all began. After all this extravagant praise for this proof, it is only fair if we demonstrate it ourselves.

We want to propose that there is an infinite number of primes, so let's assume opposite. Since, we're considering a finite number of primes, that means that there is one largest prime and that all primes can be listed as:

$$p_1,\ p_2,\ p_3 \dots,\ p_n$$

Consider the new number:

$$Q = \ p_1 \cdot p_2 \cdot p_3 \cdot \ \ldots \ \cdot p_n \ + \ 1$$

We have considered the product of every single prime plus 1. This ensures that Q is not divisible by any prime in the list.

Take any prime p_i from the list. When we divide Q by p_i we get:

$$\frac{Q}{p_i} = \frac{p_1 \cdot p_2 \cdot p_3 \cdot \ \ldots \ \cdot p_n \ + \ 1}{p_i}$$

The product $p_1 \cdot p_2 \cdot p_3 \cdot \ \ldots \ \cdot p_n$ is clearly divisible by p_i because it is one of the factors, but when we add the $+1$ we get a remainder 1. This means two things.

Q must either:

1. Be prime itself - then we have found a new prime not in our list.
2. Have a prime factor not in our list.

Either way, there is a prime number outside the original list.

This contradicts our statement that we had listed all primes. Therefore, there must be infinitely many primes.

3 Saidak's proof.

Another proof now, this one from 2006. The key thing we need to take in is very simple. It is that any two consecutive integers are coprime.

Considering the statement, let's think of any integer $n > 1$. Since n and $n + 1$ are coprime, their greatest common divisor is 1. Also, since $n > 1$, the product $n(n + 1)$ has at least two distinct prime factors.

Now set $n_1 = n(n+1)$, and observe that n_1 and n_1+1 are consecutive, therefore they are coprime.

This implies that $n_1(n_1 + 1)$ has at least one more prime factor than n_1 alone, giving at least three distinct prime factors. Repeating this process indefinitely gives a new distinct prime each time, so the number of primes is unbounded.

4 Erdős's proof.

After mentioning his name so much, it would be unfair to not include his proof. Erdős takes a different approach. The key idea is that every integer n can be written as a product $n = rs^2$, where r is not divisible by the square of any integer (this means no prime appears more than once in its factorization) and s is a positive integer.

Now, let's say there are only k primes. Consider all integers up to a large number N. How many times can we build the rs^2 form?

For s^2, we need $s \leq \sqrt{N}$, so there are at most $\sqrt{N}$ choices. For r, since it's a product of distinct primes and we only have k primes to choose from, each prime is either a factor of r or not. This gives at most 2^k possibilities.

Therefore, the total number of integers up to N we can build is at most $2^k \cdot \sqrt{N}$. But there are exactly N integers up to N, so we need $2^k \cdot \sqrt{N} \geq N$
This gives $2^k \geq \sqrt{N}$. Now, we take logarithms of both sides.

$$klog2 \geq \frac{1}{2} logN$$

Rearranging we get that

$$k \geq \frac{logN}{2log2}$$

So the number of primes up to N must be at least $\frac{logN}{2log2}$. This grows without bound as $N \to \infty$, confirming that no finite k can satisfy, and confirming that there are an infinite number of primes.

5 Euler's product formula.

The two proofs from Euclid and Saidak are admired for their elegance and how short they are. We are going to prove that there are an infinite number of primes once again, this time turning to a more sophisticated approach, involving the zeta function, defined for $s > 1$ by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

This function sums the reciprocal powers of all positive integers. At first glance, it seems like it has no direct relation to prime numbers at all. However, its significance is that it can be expressed entirely in terms of prime numbers.
Euler showed that this function is equal to an infinite product over all prime numbers:

$$\zeta(s) = \prod_{p \ prime} \frac{1}{1 - p^{-s}}$$

To understand this identity, we are going to first express it as a geometric series.

$$\frac{1}{1 - p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ ...$$

When we multiply out each terms of this infinite product, we get:

$$\frac{1}{p_1^{a_1} p_2^{a_2} p_3^{a_3} ... p_k^{a_k}}$$

The Fundamental Theorem of Arithmetic states that every positive integer $n \geq 1$ is either prime or can be expressed as a unique product of prime numbers.

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

Therefore, each integer corresponds to exactly one combination of the terms chosen from the product, and no integer is repeated. This means that expanding this product generates exactly one term for $\frac{1}{n^s}$ for each positive integer n. This shows that the product is equal to the zeta function.

Now that we understand how the zeta function and Euler product are related, we can deduce that there are infinite primes once again. We now know that:

$$\prod_{p\ prime} \frac{1}{1 - p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

If there were only a finite number of primes, the LHS would be a finite product, giving a finite number for $\zeta(1)$. However, the zeta function diverges at $s = 1$ because the series grows without bound as shown:

$$\zeta(1) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 \ + \ \frac{1}{2} \ + \ \frac{1}{3} \ + \ ...$$

Since the Euler product equals the zeta function, a finite set of primes would give a finite product, which contradicts the divergence, showing that there must be an infinite number of primes.

Bonus proof!

This proof uses the zeta function once again and is complicated if we don't accept a few assumed results, but it was too good not to talk about.
The assumed results being:

$\rightarrow \quad \zeta(2) = \frac{\pi^2}{6}$

This identity is known as the Basel problem, first solved by Euler in 1734. There are many proofs, my favorite using the Taylor series of $sin(x)$.

$\rightarrow \quad \pi$ is irrational.

The fact that π is irrational implies that π^2 is also irrational, which is the case we are interested in.

Now, since $\frac{\pi^2}{6}$ is equal to the zeta function, it is also equal to the Euler product.

$$\frac{\pi^2}{6} = \prod_{p\ prime} \frac{1}{1 - p^{-2}}$$

If there were a finite number of primes, the RHS would be a finite product of rational numbers, and hence rational. But our LHS is irrational. This is a contradiction, therefore there are infinite primes.

6 Fermat numbers proof.

We are now going to take a completely different approach, this time using Fermat numbers, defined as $F_n = 2^{2^n} + 1$.
The first few Fermat numbers are $F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$.

The key tool in this proof is taking in this useful identity. We claim that for all $n \geq 1$:

$$F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1} = F_n - 2.$$

To see why, we can notice that for any x we have $x^2 - 1 = (x-1)(x+1)$ (Difference of two squares).
Setting$x = 2^{2^n}$ gives:

$$\left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2^{n+1}} - 1.$$

This tells us that $(2^{2^n} - 1) \cdot F_n = F_{n+1} - 2$. We also note that $2^{2^n} - 1 = (2^{2^{n-1}} - 1) \cdot F_{n-1}$, and unravelling this all the way down to $n = 0$ gives $2^{2^n} - 1 = F_0 F_1 \cdots F_{n-1}$.
Substituting back:

$$F_0 \cdot F_1 \cdots F_{n-1} \cdot F_n = F_{n+1} - 2,$$

which is exactly the identity, shifted by one.
Checking the base case $n = 1$: $F_0 = 3 \quad \text{and} \quad F_1 - 2 = 5 - 2 = 3$.

Take any two Fermat numbers F_m and F_n with $m < n$, and suppose some integer d divides both of them.
By the identity $F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1} = F_n - 2, \quad F_m$ appears as one of the factors in the product $F_0 \cdot F_1 \cdots F_{n-1}$, so F_m divides that product, which equals $F_n - 2$. Since d divides F_m, it also divides $F_n - 2$. But d also divides F_n, so it must divide the difference:

$$F_n - (F_n - 2) = 2.$$

So d divides 2, meaning $d = 1$ or $d = 2$. However, every Fermat number is odd (since 2^{2^n} is even, so $2^{2^n} + 1$ is odd), so d cannot be 2. Therefore $d = 1$: the two Fermat numbers share no common factor other than 1.

The sequence $F_0, F_1, F_2, \ldots$ is infinite. Every integer greater than 1 has at least one prime factor, so each F_n has a prime factor p_n. Since any two Fermat numbers share no common factor, the primes $p_0, p_1, p_2, \ldots$ must all be different from one another. This gives us infinitely many primes.

7 Conclusion.

We have just explored 7 proofs (including the bonus) of the exact same theorem, all arriving at the same route, just from a different path. From Euclid's classic proof all the way to Euler's infinite product.

So which proof belongs in *The Book*?

The proof using Euler's product is powerful, Erdős's is the most clever, but no matter what, I keep returning to Euclid's proof. What I want you as the reader to consider is the difference between the non analytical proofs. Are they all just Euclid's proof in disguise? There is something especially remarkable about a proof that stays intact for over two thousand years. Furthermore, it's not only historical, but the clearest and simplest argument.

The very existence of *The Book* implies that some proofs are explicitly better than others. Though, I am not sure I truly agree. I believe your choice probably says more about what type of mathematician you are. Someone drawn to structure will love Euler's product formula. Someone who values economy won't look further than Euclid.

Perhaps that is the real lesson after all.

Hoper edei deixai.

References

[1] Aigner, M. and Ziegler, G. (2018). *Proofs from THE BOOK*. Springer.

[2] Saidak, F. (2006). A new proof of Euclid's theorem. *American Mathematical Monthly*, 113(10), p.937.

[3] Apostol, T. (1976). *Introduction to Analytic Number Theory*. Springer.

[4] Caldwell, C. and Peter, T. (n.d.). *Many Proofs that there are Infinitely Many Primes*. DePaul University. Available at: `https://math.depaul.edu/tpeter21/ManyPrimeProofs.pdf`

[5] Saidak, F. (2006). A new proof of Euclid's theorem. *American Mathematical Monthly*, 113(10), p.937. Available at: `https://www-users.york.ac.uk/~ss44/cyc/p/primeprf.htm`

[6] Sullivan, B. (2013). *The Basel Problem*. Carnegie Mellon University. Available at: `https://www.math.cmu.edu/~bwsulliv/basel-problem.pdf`

[7] Goldfeld, D. (2003). The Erdős–Selberg dispute. Columbia University. Available at: `https://www.math.columbia.edu/~goldfeld/ErdosSelbergDispute.pdf`

[8] Cook, J. (2011). *Erdős's proof of infinitely many primes*. Available at: https://www.johndcook.com/blog/2011/10/25/erdos-proof/

[9] Isaac, R. (2012). *Fermat Numbers*. University of Alberta. Available at: https://www.math.ualberta.ca/~isaac/math324/s12/fermat_numbers.pdf

[10] Conrad, K. (n.d.). *Infinitude of Primes*. University of Connecticut. Available at: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/infinitudeofprimes.pdf