1 How Many Primes Are There?

At first thought it might seem obvious that there is an unending supply of prime numbers.

If we think a little longer, a bit of doubt might intrude on our certainty. A small number like 6 has factors 2 and 3. There aren't many more options to try as factors. Larger numbers like 720 have more numbers smaller than them, and that means more numbers which could be factors.

Let's think about this another way. Every multiple of 2 is not a prime number, every multiple of 3 is not a prime number, every multiple of 4 is not a prime number, and so on. All these multiples are reducing the probability that a large number is prime.

We might be tempted to think that eventually prime numbers just fizzle out. Instead of relying on intuition, let's decide the matter with rigorous mathematical proof.

Proof There Are Infinitely Many Primes

A proof is not an intuition, nor is it a set of convincing examples. A proof is a watertight logical argument that leads to a conclusion we can't argue with.

The proof that there is no limit to the number of primes is ancient and rather elegant, due to Euclid around 300 BC, and a nice one to have as our first example.

Lets start by assuming the number of primes is not endless but finite.

If there are n primes, we can list them.

$$p_1, p_2, p_3, p_4 \ldots p_n$$

We can create a new number x by multiplying all these primes together.

$$x = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n$$

This x is clearly not a prime number. It's full of factors like p_1 , p_3 and p_n.

Let's make another number y in the same way, but this time we'll add 1.

$$y = p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n + 1$$

Now y could be a prime number, or it could not be a prime number. These are the only two options for any positive whole number.

If y is prime then we have a problem because we've just found a new prime number which isn't part of the original finite set $p_1, p_2 \ldots p_n$. How do we know it's not part of the original set? Well y is bigger than any of the primes in the list because we created it by multiplying them all together, and adding 1 for good measure.

So perhaps y is not a prime. In this case, it must have factors. And the factors must be one or more of the known primes $p_1, p_2 \ldots p_n$. That means y can be divided by one of those primes p_i exactly, leaving no remainder. Let's write this out.

$$\frac{y}{p_i} = \frac{p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n}{p_i} + \frac{1}{p_i}$$

The first part divides neatly without a remainder because p_i is one of the primes $p_1, p_2 \ldots p_n$. The second part doesn't divide neatly at all.

That means y can't be divided by any of known primes. Which again suggests it is a new prime, not in the original list.

Both of these options point to the original list of primes being incomplete.

And that's the proof. No finite list of primes can be a complete list of primes. So there are inifintely many primes.

A Common Misunderstanding

It is easy to think that $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n + 1$ is a way of generating prime numbers. This is not correct. The proof only asks what the consequences are if $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n + 1$ is prime, under the assumption that we have a limited list of primes $p_1, p_2, p_3, p_4 \ldots p_n$.

We can prove that $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n + 1$ is not always prime by finding just one counter-example. If we use prime numbers 3 and 5, we can see that $3 \cdot 5 + 1 = 16$ which is not prime.