1 Primes Are Elusive

If we listed all the counting numbers $1, 2, 3, 4, 5, \ldots$, excluded 1, and then crossed out all the multiples of $2, 3, 4, \ldots$ we'd be left with the primes. This sieving process emphasises that primes are defined more by what they are not, than by what they are.

If there was a simple pattern in the primes, we'd be able to encode it into a simple formula for generating them. For example, the triangle numbers 1,3,6,10,15,... can be generated by the simple expression $\frac{1}{2}n(n+1)$. The prime numbers, however, have resisted attempts by mathematicians over hundreds of years to find precise and simple patterns in them.

One of the first questions anyone enthusiastic about prime numbers asks is whether a polynomial can generate the n^{th} prime. Let's prove that prime numbers are so elusive that no polynomial in n can generate the n^{th} prime.

No Polynomial Generates Only Primes

A **polynomial** in n is has the following general form, simple yet flexible.

$$P(n) = a + bn + cn^2 + dn^3 + \ldots \alpha n^\beta$$

Let's say that $b, c, d, \ldots \alpha$ are not all zero. This way we exclude trivial polynomials like $P(n) = 7$ that only generate a single value no matter what n is.

Let's start our proof by assuming that there is indeed a $P(n)$ that generates only primes, given a counting number n. When $n = 1$, it generates a prime, which we can call p_1.

$$p_1 = P(1) = a + b + c + d + \ldots + \alpha$$

Now let's try $n = (1 + p_1)$.

$$P(1 + p_1) = a + b(1 + p_1) + c(1 + p_1)^2 + d(1 + p_1)^3 + \ldots$$

That looks scary, but all we need to notice is that if we expand out all the terms, we'll have two kinds, those with p_1 as a factor, and those without. We can collect together all those terms with p_1 as a factor and call them $p_1 \cdot X$.

$$P(1 + p_1) = (a + b + c + d + e + \ldots \alpha) + p_1 \cdot X$$

We then notice that $(a + b + c + d + e + \ldots \alpha)$ is actually p_1.

$$\begin{aligned} P(1 + p_1) &= p_1 + p_1 \cdot X \\ &= p_1(1 + X) \end{aligned}$$

This is divisible by p_1 but shouldn't be because $P(1+p_1)$ is supposed to be a prime. This contradition means the starting assumption that there is a polynomial $P(n)$ that can generate only primes is wrong.

We've actually proved a stronger statement than we intended. We intended to prove that there is no polynomial $P(n)$ that generates the n^{th} prime. We ended up proving that no polynomial $P(n)$ can generate only primes.