1 Primes Are The Building Blocks Of Numbers

We saw earlier that positive whole numbers have factors if they're not a prime number. Let's explore this a little further.

Breaking A Number Into Its Factors

Let's think about the number 12 and its factors. We can think of two combinations straight away.

$$12 = 2 \times 6$$
$$12 = 3 \times 4$$

Looking again at those factors we can see that 6 itself can be broken down into smaller factors 3 and 2. That 4 can also be broken down into factors 2 and 2.

$$12 = 2 \times (3 \times 2)$$
$$12 = 3 \times (2 \times 2)$$

We can't break these smaller factors down any further, which means they're prime numbers. Both combinations now look very similar. If

we re-order those factors by size we can see they are in fact exactly the same.

$$12 = 2 \times 2 \times 3$$
$$12 = 2 \times 2 \times 3$$

Perhaps every number can be broken down into a series of prime factors that is unique to that number, much like DNA is unique to individuals. Let's prove it.

Fundamental Theorem Of Arithmetic

We'll split this proof into two steps.

- First we'll show that any positive whole number can be broken down into a series of factors that are all prime.
- Second we'll show this series of primes is unique to that number.

Let's imagine a number N and write it out as a product of factors.

$$N = f_1 \cdot f_2 \cdot f_3 \cdot \ldots \cdot f_m$$

We can look at each of these factors f_i in turn. If a factor is not prime, we can break it down into smaller factors. For example, the factor f_1 might be broken down as $f_1 = g_1 \cdot g_2$. If a factor is prime, $f_2 = p_1$ for example, we leave it because we can't break it into smaller factors.

$$N = (g_1 \cdot g_2) \cdot p_1 \cdot (g_3 \cdot g_4 \cdot g_5) \cdot \ldots \cdot (g_x \cdot g_y)$$

If we keep repeating this process, all the factors will eventually be prime. How can we be so sure? Well, if any number in the series isn't prime, we can apply the process again, breaking that number down into smaller factors. The only thing that stops us applying the process again is when all the factors are eventually prime.

Figure 1.1 shows an example of this iterative process applied to the number 720.

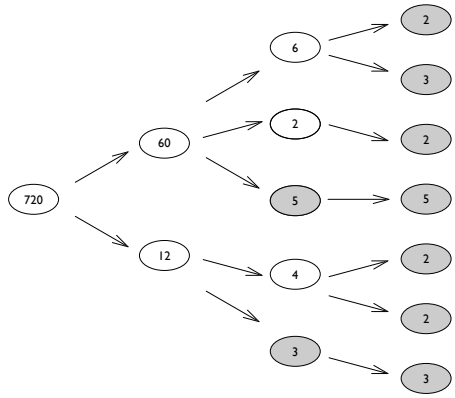

Figure 1.1: Breaking 720 into factors until only primes remain.

We can now write N as a product of these primes.

$$N = p_2 \cdot p_3 \cdot p_1 \cdot p_5 \cdot p_4 \cdot p_6 \cdot p_7 \cdot \ldots \cdot p_n$$

These primes won't necessarily be in order of size. They may also repeat, for example p_1 might be the same as p_7. It doesn't matter. We've shown that any positive whole number can be written as a product of primes.

Let's now show that this series of primes is unique to that number N. For the moment, imagine this isn't true and a number N can be written as a product of two different series of primes.

$$N = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_a$$
$$N = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_a \cdot q_b \cdot q_c \cdot q_d$$

These primes are not necessarily in order of size, and some might be repeated, so p_2 could be the same as p_4. Again, we won't let that bother us. To keep our argument general, we'll assume that the number of primes in the second series, d, is larger than the number of primes in the first series, a.

Now, we can see that p_1 is a factor of N. That means it must also be a factor of the second series. That means p_1 is one of the factors q_i. Because we we didn't assume any order in these primes, let's say it is q_1. That means we can divide both series by $p_1 = q_1$.

$$\cancel{p_1} \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_a = \cancel{q_1} \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_a \cdot q_b \cdot q_c \cdot q_d$$

We can apply the same logic again. The first series has a factor p_2 which means it must also be a factor of the second series. We can say that $p_2 = q_2$, and divide both series by this factor.

$$\cancel{p_1} \cdot \cancel{p_2} \cdot p_3 \cdot \ldots \cdot p_a = \cancel{q_1} \cdot \cancel{q_2} \cdot q_3 \cdot \ldots \cdot q_a \cdot q_b \cdot q_c \cdot q_d$$

We can keep doing this until all the factors in the first series have been matched up with factors in the second series. It doesn't matter if a prime repeats, for example if p_1 is the same as p_3, the factors will still be matched correctly, in this case $p_1 = q_1$ and $p_3 = q_3$.

$$\cancel{p_1} \cdot \cancel{p_2} \cdot \cancel{p_3} \cdot \ldots \cdot \cancel{p_a} = \cancel{q_1} \cdot \cancel{q_2} \cdot \cancel{q_3} \cdot \ldots \cdot \cancel{q_a} \cdot q_b \cdot q_c \cdot q_d$$

Let's simplify the algebra.

$$1 = q_b \cdot q_c \cdot q_d$$

What we've just shown is that if a number N can be written as two separate series of prime factors, their factors can be paired up as being equal, and if any are left over, they must equal 1. That is, the two series are identical.

We've shown that any whole number N can be decomposed into a series of prime factors, and this series of primes is unique to that number. This is rather profound, and is called the Fundamental Theorem of Arithmetic.