Primes Are The Building Blocks Of Numbers

From Primes To Riemann

Tariq Rashid

January 17, 2021

Breaking A Number Into Its Factors

- Let's think about the number 12 and its factors.

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

Breaking A Number Into Its Factors

- That 6 can be broken down further. So can that 4.

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

- Can't break these down any further $\rightarrow$ prime.

Breaking A Number Into Its Factors

- If we order those factors by size, we can see the lists are the **same**.

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

- Perhaps every number has a **unique** breakdown of factors ... like DNA is unique to people?

Fundamental Theorem of Arithmetic

- Proof part 1:
  - Show any number can be broken down into a list of **factors that are all prime**.
- Proof part 2:
  - Show this list of primes is **unique**.

FTA Part 1

- Imagine a counting number N, and write it as a product of factors.

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

- Looking at each factor in turn, if it isn't prime we can break it down into smaller factors.

FTA Part 1

- f_1 might be broken down as $f_1 = g_1 \cdot g_2$
- f_2 might be prime p_1.

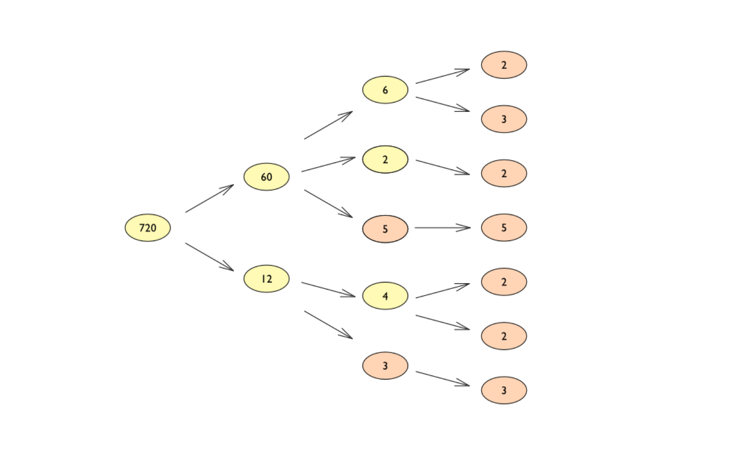
$$\begin{aligned} N &= f_1 \cdot f_2 \cdot f_3 \cdot \ldots \cdot f_n \\ &= (g_1 \cdot g_2) \cdot p_1 \cdot (g_3 \cdot g_4 \cdot g_5) \cdot \ldots \cdot (g_x \cdot g_y) \end{aligned}$$

FTA Part 1

- We can keep repeating this process of breaking down numbers into smaller factors.
- We only stop when we can't break numbers down further $\rightarrow$ **when they're all prime**.

FTA Part 1

- Let's try this process with an example number, 720.



FTA Part 2

- Imagine N can be written as a product of primes in two different ways.

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

- For generality, that second list is longer than the first.

FTA Part 2

- If p_1 is a factor of N from the first list, then it must be in the second list too.

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

- We can repeat the same logic. If p_2 is a fctor of N then it must be in the second list.

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

FTA Part 2

- We can repeat the process until we've cancelled all the prime factors in the shorter first list.

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

- We can simply this.

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

- All the remaining factors q are 1. So the **two lists are equal.**

FTA Summary

1. Any whole number $N > 1$ can be broken down into a list of prime factors.
2. ... and that list of primes is unique to that number.