How Many Primes Are There?

From Primes To Riemann

Tariq Rashid

January 14, 2021

Do Primes Fizzle Out?

- Every multiple of 2 is not prime.
- Every multiple of 3 is not prime.
- Every multiple of 4 is not prime.
- Every multiple of 5 is not prime. ...

- All these multiples are reducing the probability that a large number is prime.

Intuition Is Not Proof

- Intuition is not proof.
- Lots of examples are not proof.

- A proof is a watertight logical argument that leads to a conclusion we can't argue with.

Euclid's Proof (300BC)

- Let's start by assuming there are a **finite** number of primes.

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

Euclid's Proof (300BC)

- Let's create a new number x by multiplying all those 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.

Euclid's Proof (300BC)

- Let's create another y in the same way, but this time add 1.

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

- Is y prime? There are only two options:
  - option 1 - yes it is prime
  - option 2 - no it is not prime

Euclid's Proof (300BC)

- Option 1 - yes, y is prime.
  - We just found a new prime that isn't in the original list !

Euclid's Proof (300BC)

- Option 2 - no, it is not prime.
  - So it must have factors from our list of primes $p_1, p_2, p_3, \dots p_n$.
- That means y can be divided by one of the primes p_i exactly.

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

- That second part doesn't divide without a remainder!
- But that means y can't be divided by any of the known primes. So it must be a new prime, not in the original list.

Euclid's Proof (300BC)

- Both of these options tell us the original list of primes is incomplete.
- That that's the proof.
  - No finite list of primes can be a complete list of primes.
  - So there are infinitely many primes.

Proof By Contradition

- Normal Proof
  - valid assumptions $\rightarrow$ valid logical steps $\rightarrow$ valid conclusion
- Proof By Contradiction
  - **invalid** assumptions $\rightarrow$ valid logical steps $\rightarrow$ **invalid** conclusion

A Common Misunderstanding

- It's 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 primes. This is wrong.
- The proof only asks **what happens if** we say $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n + 1$ is a prime, assuming a limited list of primes $p_1, p_2, p_3, p_4 \ldots p_n$.
- We can easily prove $p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot \ldots \cdot p_n + 1$ is not always prime with just one **counterexample**.
  - $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$ which is not prime because $30031 = 59 \times 509$.