Primes: the indivisible and the indispensable (3)

Philomathes • 27 Jan 2025

Proof by Contradiction

You are a newly appointed judge presiding over a mathematics courtroom, and today marks your first trial. You enter the courtroom with a mix of tension and anticipation. Fortunately, seated to your left and right are your aides—‘Defense Counsel’ and ‘Prosecutor’—both known for their wisdom and rationality, though equally renowned for their opposing arguments. Today’s case is as follows:

"Determine whether there are infinitely many prime numbers."

Once the trial begins, as expected, the two sides present their arguments with vigor.

Prosecution’s Claim: There are only finitely many primes.

“Your Honor, as you observed during the process of constructing the Sieve of Eratosthenes, the frequency of primes decreases significantly as numbers grow larger. This decline will persist, eventually reaching zero.”

Defense Counsel’s Argument: There are infinitely many primes.

“Your Honor, the set of natural numbers is infinite, and by the Fundamental Theorem of Arithmetic, every natural number can be uniquely factorized into primes. If the number of primes is finite, it would seem implausible to account for the infinite variety of natural numbers.”

Prosecution’s Rebuttal: “The defense’s argument contains a logical leap. For instance, even with just one prime number, say 2, we could generate as many natural numbers as we wish: $2, 2 \times 2, 2 \times 2 \times 2, \ldots$. The fact that natural numbers are infinite does not necessarily prove the infinity of primes.”

Defense’s]Rebuttal: “The prosecution’s argument also relies on a flawed assumption. A decreasing frequency does not necessarily mean the frequency becomes zero. Consider **square numbers** such as $1, 4, 9, 16, 25, \ldots$. While the frequency of square numbers decreases dramatically, they are still infinite in number.”

After listening to the arguments and counterarguments, you find yourself in deep contemplation. Each side has its merits, yet both are vulnerable to counterpoints. A fundamental question suddenly strikes you: What does it even mean for something to be “infinite”? And how can we prove something is infinite? Without answering these questions first, you realize no verdict can be reached. In a firm, solemn voice, you declare, “The court is adjourned.” [1]

How can we prove something is infinite? The most immediate method might involve "counting one by one." If everything in a set can be counted, it’s finite; if not, it’s infinite. But this approach has a critical flaw—it can only prove something is finite.

For example, suppose you dedicate your entire life to proving that natural numbers are infinite by counting them. Starting from infancy, you mutter, “One, two, three...” and continue for 80 years, tirelessly counting. Let’s assume you reach one billion just before drawing your final breath.[2] What have you proven? Two things:

- There are at least more than a billion natural numbers.
- Life is finite.

Despite your lifelong endeavor, you have not proven the infinitude of natural numbers.

To prove something is infinite, we must instead assume the opposite of what we wish to prove. We then proceed logically under that assumption until we inevitably encounter a contradiction—an inconsistency that cannot be tolerated in the logical framework of mathematics.[3]

This approach is one of the most ingenious strategies in mathematical history. Like a spy infiltrating enemy territory, the proof adopts the opposition’s stance and dismantles it from within. Let us try to prove the infinitude of natural numbers using this method. First, we disguise ourselves as proponents of the claim that natural numbers are finite. But we won’t enter the fray unarmed—we’ll equip ourselves with the following fact:

"If x is a natural number, then $x+1$ is also a natural number."[4]

Let us assume that natural numbers are finite. If we arrange them in ascending order, there must be a largest natural number. Call this number N. Here, we deploy our weapon: If N is a natural number, then $N+1$ must also be a natural number. Furthermore, $N+1 > N$. This contradicts the assumption that N is the largest natural number. Thus, the assumption that natural numbers are finite leads to a contradiction. Therefore, natural numbers must be infinite.

This proof technique is known as **proof by contradiction**, or **reductio ad absurdum** in philosophy, meaning “reduction to absurdity.” Just as a protagonist in a movie sneaks into enemy territory, plants a bomb, and escapes, proof by contradiction infiltrates an opposing claim, reveals an inconsistency, and renders the claim untenable. The charm of proof by contradiction isn’t mine alone to feel. British mathematician G. H. Hardy eloquently praised its beauty in his book *A Mathematician’s Apology*:

"Reductio ad absurdum, which Euclid loved so much, is one of a mathematician’s finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game."

---

1. Engaging with opposing arguments fosters a deeper understanding of mathematics. However, such an approach is not presented as dramatically in academic manuscripts. The courtroom analogy here is a playful dramatization, influenced by the author’s admiration for the game *Ace Attorney*.↩
2. If a person speaks at a pace of two syllables per second, even with uninterrupted counting over an 80-year lifespan, they would only reach 500 million at best, according to calculations by ChatGPT. This limitation arises because the number of syllables required to articulate a number increases as the numbers themselves grow larger.↩
3. German mathematician Georg Cantor once said, “The essence of mathematics is its freedom.”↩
4. Earlier, we defined natural numbers informally as numbers like 1, 2, 3, 4, and so on. However, their formal definition is expressed recursively: 1 is a natural number, and if x is a natural number, then $x + 1$ is also a natural number.↩