October 7, 2021 (improved since class)
Cedars Math
Mr. Rasmusen

Euclid's Proof That the Number of Primes Is Infinite

Definition.
A prime is a number that is (a) greater than 1 and (b) divisible only by itself and 1. (By "divisible", we mean divisible evenly, without remainder)

Examples.
1. The number 7 is prime, because it is divisible only by 1 times 7.
2. The number 10 is *not* prime, because it is divisible by 1 times 10, but also by 2 times 5.

Theorem.
The number of primes is infinite.

Proof:
Step 1. *If and only if* the number of primes is finite, there is a biggest prime. Call it B. We will be showing that B is impossible; it can't exist because whatever candidate prime number you pick for B, we can find a bigger prime number.

Step 2. Multiply all the prime numbers together from 2 to B to create the number $K = 2 \cdot 3 \cdot 5 \cdots B$. The number K is the least primish number possible, since it can be divided by every prime in existence. K is not prime, since it be divided not just by 1 times K but by 2, by 3, by 5, and so forth. Also, K is bigger than B, the biggest prime number.

Step 3. Create the number $N = K + 1$ by adding 1 to K. Since K is bigger than B, so is N. Under our tentative assumption that B is the biggest prime, N can't be prime.

Step 3A. N is not divisible by any of the primes $2, 3, 5, \ldots, B$ because K is divisible by all of them and that means dividing N, which equals $K + 1$, by any of them would result in a remainder of 1.

Step 4. Since N is not prime, it is divisible by some prime numbers. Pick one of those prime numbers and call it D.

Step 5. The number D can't be any of the primes from 2 to B, because Step 3A told us that N isn't divisible by any of them. This is the key step in the proof.

Step 6. But if D isn't a prime number between 2 and B, that means it has to be a prime number bigger than B.

Step 7. But if D is bigger than B, that's saying there is a prime number (D) bigger than what we said was the biggest prime number (B). So for any prime number we choose as B because we think it's the biggest, there's going to be an even bigger prime number.

Step 8. Since there is no biggest prime, there must be an infinite number of primes. *Quod erat demonstrandum.*

This is not literally Euclid's proof, but it uses the idea of his proof. I relied on https://primes.utm.edu/notes/proofs/infinite/euclid
Long proofs are faster to understand than short proofs, but here is a short version:

Short version of the proof. If the number primes is infinite, there is a biggest prime, B. Let $K \equiv 2 \cdot 3 \cdot 5 \cdots B$, and let $N \equiv K+1$. The number N is not divisible by any prime in $2, 3, 5, \ldots, B$ because K is divisible by all of those numbers and for $N = K + 1$ there would be a remainder of 1. But since $N > B$, the number N is not prime and is divisible by some prime D. That prime D is not in $2, 3, 5, \ldots, B$, so it must be bigger than B, but that contradicts there being a biggest prime, B. Q.E.D.