Math 8: There are infinitely many prime numbers

Spring 2011; Helena McGahagan

LEMMA Every integer $N > 1$ has a prime factorization.

Proof by contradiction: Assume that there is an integer that does not have a prime factorization. Then, let N be the *smallest* such integer. If N were prime, it would have an obvious prime factorization ($N = N$). Therefore, N is not prime. This means N must be divisible by a positive integer other than itself or 1; call this integer r. Then, $1 < r < N$ and $N = r \cdot s$ where s is also an integer. Notice that since $1 < r < N$, we also must have $1 < s < N$. Since N is the smallest number bigger than 1 without a prime factorization, both r and s must have prime factorizations. Therefore, there exist prime numbers $p_1, p_2, ..., p_n$ and $q_1, q_2, ..., q_m$ such that $r = p_1 \cdot p_2 \cdot ... \cdot p_n$ and $s = q_1 \cdot q_2 \cdot ... \cdot q_m$. Then,

$$N = p_1 \cdot p_2 \cdot ... \cdot p_n \cdot q_1 \cdot q_2 \cdot ... \cdot q_m.$$

We have written N as the product of prime numbers. This contradicts the assumption that N does not have a prime factorization. $\square$

THEOREM There are infinitely many prime numbers.

Proof by contradiction: Assume there are finitely many prime numbers. Then, we can say that there are n prime numbers, and we can write them down, in order: Let $2 = p_1 < p_2 < ... < p_n$ be a list of all the prime numbers. The key trick in the proof is to define the integer

$$N = 1 + p_1 \cdot p_2 \cdot ... \cdot p_n.$$

Since $N > p_n$, and p_n is the largest prime number, N is not prime. However, from the lemma, N must have a prime factor. This means one of the primes in our list must divide N; in other words, there exists an integer i with $1 \leq i \leq n$ such that p_i divides N. Since p_i divides both N and the product of all the primes, it must also divide $N - p_1 \cdot p_2 \cdot ... \cdot p_n = 1$. Since $p_i \geq 2$, it is impossible that p_i divides one, so we have a contradiction. Hence, our assumption that there are finitely many prime numbers must have been false. $\square$.

You may have noticed in the proof of the lemma that, when we had at least one positive integer with some property, we assumed that we could take the smallest integer with that property. This is one of the basic axioms in mathematics! There is no way to really prove that it's true, but it matches our intuition about how the natural numbers work. This axiom is known as the "well ordering property" of the natural numbers. In symbols: If $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then $\exists s \in S$ such that $s \leq x$ for every $x \in S$.