A Constructive Proof of Euclid's Theorem

T. Donaldson

October 29, 2019

What follows is a *constructive* proof of Euclid's theorem (that there are infinitely many primes): the proof actually shows how to create an infinite set of primes.

Definition. *Suppose* $P = \{p_1, p_2, \ldots, p_n\}$ *is a finite and non-empty set of primes. The* ***Euclid number of P****, denoted* ***E****, is* $E = 1 + p_1 \cdot p_2 \cdot \ldots \cdot p_n$.

For example, if $P = \{2\}$, then it's Euclid number is $1 + 2 = 3$. If instead $P = \{5, 11\}$, then it's Euclid number is $1 + 5 \cdot 11 = 56$.

Lemma. *If* E *is the Euclid number of the set of primes* A*, then no prime divisor of* E *is in* A.

Proof. Suppose p_i is also a prime divisor of E, and p_i is in A. That means p_i divides both $E - 1$ (the product of all the primes in A) and E. Since $(E - 1) + E = -1$, then by part e) of theorem 4.3 from the textbook, p_i must also divide -1. But since $p_i > 1$ that's impossible, and so if p_i is a prime divisor of E it cannot also be in A. $\square$

The essential idea of this proof is that if a and n are positive integers, and both $a|n$ and $a|(n+1)$, then $a = 1$. This implies a prime cannot divide two consecutive integers (such as $E - 1$ and E).

Theorem (Euclid's theorem)**.** *There are an infinite number of primes.*

Proof. Consider the following process:

1. Let $A = \{2\}$.
2. Calculate the Euclid number E of A.
3. Add the smallest prime divisor p of E to A. By the previous lemma, we know p cannot be in A, and so this step always increases the size of A by 1.
4. Go to step 2.

Since A increases in size forever, and it only contains primes, there must be an infinite number of primes. $\square$