A great deal of history exists surrounding the total number of prime numbers. Arguably the first mathematician to prove that there are infinitely many prime numbers was Euclid. Euclid gave his well-known proof of this fact in Book IX, Proposition 20, of the *Elements*. Here’s how Euclid stated his theorem:

**Theorem:** *Prime numbers are more than any assigned multitude of prime numbers.*

Note the subtle difference here between how we might describe an “infinite set” versus the way Euclid is describing it. In more modern-day language, we would write the following:

**Theorem:** *There are infinitely many prime numbers.*

What’s really cool about the way Euclid states the theorem is that it hints at exactly how he will prove the result! Namely, he assumes (in order to contradict) that there are only finitely many primes and he writes down the set of ALL such primes. Then he shows that there has to be another prime outside the set, and this process can be done ad infinitum. Theorem proved.

Here now is a modern-day proof of this result which is modeled very heavily off of Euclid’s proof (although it is not identical to his).

**Proof:** Assume, with the goal of reaching a contradiction, that there are only finitely many primes. Since there are only finitely many of them, we can give them ALL names (and the key word here is ALL). Call them \( p_1, p_2, \ldots, p_r \). (Editorial sidenote: In Euclid’s proof, he assumes there are only three primes in our list....) Now consider the number \( N = (p_1 \times p_2 \times \ldots \times p_r) + 1 \). There are two possibilities for this number \( N \).

The first possibility is that it is a prime. But if so, then we have a contradiction because it is clearly larger than any of the primes in our list, so it is a NEW prime. That’s a contradiction to the fact that we had already listed ALL the primes.

The second possibility is that \( N \) is not prime. Then Euclid has already proven to us that \( N \) must have a prime factor. Let’s call that special prime factor \( P \). Then we know \( P \mid N \). We also know that this \( P \) must be one of the primes in our list of ALL primes. So \( P \mid p_1 \times p_2 \times \ldots \times p_r \) since \( P \) is
one of the primes in that list. This implies $P \mid 1$. But this is a contradiction also, because $P$ must be greater than 1 (since it is a prime).

Therefore, no matter what, we have contradicted the fact that we had written down ALL the primes. Since we could continue doing this ad infinitum, we have proven that no such finite list of ALL the primes can be written. So there must be infinitely many primes.

Notice a few things here:

1) This proof is not a “constructive” proof. We do not build an infinite list of primes in the process. This is a proof by contradiction.
2) This proof does not give us any indication as to how we would actually find infinitely many primes. This will be the subject of several of our later lectures in this course.

© 2010, James A. Sellers