3.2 The infinitude of primes

The highlight of this section is Theorem 3.16, which states that there are infinitely many primes. In case you forgot, here is the definition of a prime number.

**Definition 3.12.** A natural number $p$ is called prime iff $p$ is divisible by exactly two distinct natural numbers (namely, 1 and $p$ itself).

**Exercise 3.13** Is 1 a prime number? Explain your answer.

The first known proof of Theorem 3.16 is in Euclid’s *Elements* (c. 300 BCE). Euclid stated it as follows:

**Proposition IX.20.** Prime numbers are more than any assigned multitude of prime numbers.

There are a few interesting observations to make about Euclid’s proposition and his proof. First, notice that the statement of the theorem does not contain the word “infinity.” The Greek’s were skittish about the idea of infinity. Thus he proved that there were more primes than any given finite number. Today we’d say that they are infinite. In fact, Euclid proved that there are more than three primes and concluded that there were more than any finite number. While you would lose points for such a proof in this class, we can forgive Euclid for this less-than-rigorous proof; in fact, it is easy to turn his proof into the general one that you will give below. Lastly, Euclid’s proof was geometric. He was viewing his numbers as line segments with integral length. The modern concept of number was not developed yet.

Prior to tackling a proof of Theorem 3.16, we need to prove a couple lemmas. The proof of the first lemma is provided for you.

**Lemma 3.14.** The only natural number that divides 1 is 1.

**Proof.** Let $m$ be a natural number that divides 1. We know that $m \geq 1$ because 1 is the smallest positive integer. Since $m$ divides 1, there exists $k \in \mathbb{N}$ such that $1 = mk$. Since $k \geq 1$, we see that $mk \geq m$. But $1 = mk$, and so $1 \geq m$. Thus, we have $1 \leq m \leq 1$, which implies that $m = 1$, as desired.

**Lemma 3.15** Let $p$ be a prime number and let $n \in \mathbb{Z}$. If $p$ divides $n$, then $p$ does not divide $n + 1$.

Now, we are ready to prove the following important theorem.

**Theorem 3.16** There are infinitely many prime numbers.

---

[vii]This section is derived from work of Dave Richeson of Dickinson College.
[viii]Hint: Use a proof by contradiction and utilize the previous lemma.
[ix]Hint: Use a proof by contradiction. In this case, there are finitely many primes. Consider the product of all of them and then add 1.