P.12 Existence and Uniqueness

Many ideas in mathematics aren't particularly useful unless we happen to know that something is unique. For instance, the greatest common divisor of two numbers, the prime factorization of an integer, the absolute maximum of a function on a closed interval, and y-intercept of a function are all unique entities.

Goals:

- Prove Existence and Uniqueness Statements
- Use Bezout's Lemma to write proofs

We've already discussed how to prove an existence statement. Our goal now is to prove that the item that we have guaranteed to exist is also unique. In short-hand notation, we'll be proving statements of the form

$$\exists! x,\ P(x).$$

In the statement above, the "!" symbol is read as "unique."

To prove a uniqueness statement we use a process not unlike contradiction. That is, we assume that the item is not unique, and then prove this to be an absurdity. The following example demonstrates this.

Claim 1. If $x \in \mathbb{R}$, there exists unique $y \in \mathbb{R}$ such that $x + y = x$.

Proof. Notice that if we set $y = 0$, then $x + y = x + 0 = x$.

To prove uniqueness, assume that there exists $z \in \mathbb{R}$ such that $z \neq y$ and $x + z = x$. If $x + z = x$, we can subtract x from both sides of the equation to find that $z = 0$, so $z = y$.

Therefore, there exists unique $y \in \mathbb{R}$ such that $x + y = x$. □

1. Prove the following claims. Notice that they are both existence and uniqueness statements, and you'll need to prove both.

Claim 2. If $x \in \mathbb{R}$ and $x \neq 0$, there exists unique $y \in \mathbb{R}$ such that $xy = x$.

Claim 3. If $x \in \mathbb{R}$, there exists unique $y \in \mathbb{R}$ such that $x + y = 0$.

Claim 4. If $x \in \mathbb{R}$ and $x \neq 0$, there exists unique $y \in \mathbb{R}$ such that $xy = 1$.

Claim 5. If $a, b \in \mathbb{R}$ and $a < b$, then there exists unique $M \in \mathbb{R}$ such that

$$b - M = M - a = \frac{b-a}{2}.$$

(Hint: On the real line, $b - a$ is the distance between a and b.)

Existence and uniqueness proofs will be revisited later in this course and will play a major role in your upper level math course (especially Abstract Algebra and Analysis). However, our exposure to a relatively limited amount of mathematics at this point will prevent us from proving them too often.

We move on now to working with some ideas that should be familiar to you.

Definition (Greatest Common Divisor)**.** The *greatest common divisor* of two integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.

Definition (Prime)**.** An integer n is *prime* if it has exactly two positive divisors, 1 and n.

2. Prove the following.

Claim 6. Suppose $a, p \in \mathbb{Z}$. If p is prime then $\gcd(a, p) = 1$ or $\gcd(a, p) = p$.

The next claim is very commonly used in basic number theory and ties together a variety of ideas in basic arithmetic. The text refers to the claim as Proposition 7.1, but the claim is so common that we will refer to it by the name Bezout's Lemma (pronounced BAY-Zoo). The text gives a proof of the claim.

Lemma (Bezout's Lemma)**.** If $a, b \in \mathbb{N}$, then there exists $k, \ell \in \mathbb{Z}$ such that $gcd(a, b) = ka + \ell b$.

3. Use Bezout's Lemma to prove the following claim which is often referred to as Euclid's Lemma.

Claim 7 (Euclid's Lemma)**.** If $a \,|\, (bc)$ and $gcd(a, b) = 1$, then $a \,|\, c$.

4. Prove the following claim in two ways. First, prove the claim using Euclid's Lemma, then prove the claim using only Bezout's Lemma.

Claim 8. Suppose $a, b, p \in \mathbb{Z}$. If p is prime and $p \,|\, (ab)$, then $p \,|\, a$ or $p \,|\, b$.