1 Existence Arguments

One fascinating, and often troubling, kind of proof is the *existence* proof: such a proof entails not showing that general rules hold, but that there is some object (numeric or otherwise) with a particular property. In the simplest case, this is basically the opposite of a counterexample: we demonstrate the existence of an object with certain properties simply by constructing such an object.

Proposition 1. *There is an integer x such that $x \equiv 2 \pmod 3$, and $x \equiv 6 \pmod 8$.*

Proof. Consider $x = 14$. Since $3 \mid 14 - 2$, it is the case that $14 \equiv 2 \pmod 3$, and since $8 \mid 14 - 6$, it is the case that $14 \equiv 6 \pmod 8$. □

This is a pretty simplistic argument, but it's satisfactory. More intriguing is the case where, at the end of the argument, you aren't assured of havign a specific example:

Proposition 2. *There are irrational numbers a and b such that a^b is rational.*

Proof. Consider $\sqrt{2}^{\sqrt{2}}$. This is a real number, so it must be either rational or irrational. We shall consider these two cases:

Case I: $\sqrt{2}^{\sqrt{2}}$ is rational. Then $a = \sqrt{2}$ and $b = \sqrt{2}$ are a pair satisfying the criteria of the proposition: both a and b are well-known to be irrational, and by the supposition of this case, a^b is rational.

Case II: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then $a = \sqrt{2}\sqrt{2}$ and $b = \sqrt{2}$ are a pair satisfying the criteria of the proposition: by the supposition of this case, a is irrational, and b is well-known to be irrational. Some simple arithmetic will show that a^b is rational:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

□

The peculiar thing about this proof is that even though it's a proof that something exists, it doesn't actually provide the object in question: it tells us without a shadow of a doubt that one of two things is the object we seek, but not which one (note: $\sqrt{2}^{\sqrt{2}}$ is in fact irrational, so $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ are in fact the pair we seek, but this argument doesn't actually prove that, and the argument which does prove it is a lot more complicated).

Such an existence proof, which doesn't actually give a specific example, is known as a *nonconstructive* proof, which can be fairly frustrating, since if something exists, surely we should be able to pin it down!

This isn't actually the first time we've seen existence proofs, though. In MATH 205 you almost surely encountered the following:

Theorem 1 (Intermediate Value Theorem)**.** *If f is a function which is continuous on the closed interval $[a, b]$ and y is a real number between $f(a)$ and $f(b)$, then there is a number c such that $a \leq c \leq b$ and $f(c) = y$.*

This asserts the existence of a solution c to the equation $f(x) = y$, but doesn't tell us its value. Nonetheless, we can use this theorem to assert a great deal about the *existence* of solutions to various equations.

Proposition 3. *Any polynomial of odd degree has at least one zero.*

Proof. Let us denote our polynomial as $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ with n odd and $a_n \neq 0$. Since $f(x)$ is zero whenever $-f(x)$ is zero, we may WLOG assume $a_n > 0$. Consider $g(x) = \frac{f(x)}{x^n} = a_n + \frac{a_{n-1}}{x} + \frac{a_{n-2}}{x^2} + \frac{a_{n-3}}{x^3} + \cdots + \frac{a_0}{x^n}$. Note that $\lim_{n\to\pm\infty} g(x)$ is positive (namely, it is a_n), so there must be a high-magnitude negative number A such that $g(A) \approx a_n$ and a large positive B such that $g(B) \approx a_n$. Since $A < 0$ and n is odd, $A^n < 0$; given that $g(A) \approx a_n$ and a_n is positive, we know $g(A) > 0$ and thus $f(A) = A^n g(A) < 0$. Likewise, since B is positive and $g(B) > 0$, it follows that $f(B) = B^n g(B) > 0$. Polynomial functions are continuous, so we may invoke the Intermediate Value Theorem on f between A and B; since $f(A) < 0$ and $g(B) > 0$, it follwos that there is some c in $[A, B]$ such that $f(c) = 0$. □

A stronger result than mere existence is uniqueness. Once we know an object exists, its uniqueness is usually proven in one of two ways:

- Give names to two objects satisfying the condition: show that they must be equal.
- Assume the existence of two nonequal objects satisfying the condition: derive a contradiction.

Here is an example of the second method applied to demonstrating uniqueness of a polynomial zero.

Proposition 4. *For positive real number k and and real number ℓ, the quintic $f(x) = x^5 + kx + \ell$ has exactly one zero.*

Proof. The above theorem guarantees existence of at least one real zero; now we must show it is unique. Suppose there are two distinct zeroes a and b of this quintic; we are thus presuming that $f(a) = f(b) = 0$, and that $a \neq b$. Since $a \neq b$, we may assume WLOG that $a < b$. Now let us note that $f'(x) = 5x^4 + k$. Since $5x^4 \geq 0$ for all x and $k > 0$, we see that $f'(x) > 0$ for all x, so $f(x)$ is increasing throughout its domain: thus, since $a < b$, it is the case that $f(a) < f(b)$; in other words, $0 < 0$, which is a patent absurdity. □

Now an example of the first approach:

Proposition 5. *For nonzero real m and real b and y, the equation $mx + b = y$ has at most one solution x.*

Proof. Suppose this equation has solutions x_1 and x_2. Then $mx_1 + b = y$ and $mx_2 + b = y$. Thus $mx_1 + b = mx_2 + b$, so $mx_1 = mx_2$. Since m is nonzero, it then follows that $\frac{mx_1}{m} = \frac{mx_2}{m}$, or that $x_1 = x_2$. Since two arbitrary solutions were shown to be identical, this equation has at most one solution. □