What’s a proof?

Roughly, a proof is a demonstration that a statement is True (or False) based on the assumption that certain basic statements are True. In other words, a proof demonstrates that a particular statement logically follows from a set of axioms (the set of assumed basic statements). There is a huge collection of statements (theorems and stuff) that have been shown to follow from a small set of axioms, and we’ll kind of start in the middle, accepting a bunch of statements as being True, but pretending that a bunch of other statements haven’t proven yet, so we can practice.

**Example 1.** To illustrate that we do proofs all the time, and to give more of a feeling about what’s important, let’s look at a simple algebra problem. Find all solutions to the equation

\[ x^2 - 5 = 4. \]

One of the “True” statements in real number algebra is that

If you add the same constant to both sides of an equation, then the solutions of the new equation will be the same as the solutions of the old equation.

Therefore, the equation

\[ x^2 = 9. \]

has the same solutions as the original one. We’d finish off with an implicit theorem which might be stated as

**Given an equation of the form** \( x^2 = a \), with \( a \geq 0 \), \( x = \sqrt{a} \) and \( x = -\sqrt{a} \) are solutions.

We would write our answer something like

\[ x = \pm 3. \]

Note that we figured out what the solutions were, and proved that what we were going to get were the correct solutions at the same time. Given the numbers \( \pm 3 \) beforehand, it would be easy to prove that these are solutions. We would also have to do more work to show that there weren’t any other solutions.

**Existence Proofs**

To prove a statement of the form \( \exists x, P(x) \), we need to show that there is at least one \( x \) that makes \( P(x) \) True. One way to do this is to find one such \( x \), and then demonstrate that \( P(x) \) is True for that \( x \).

**Example 2.** Show that the equation \( x^2 - 5 = 4 \) has a solution. In fancy language,

Show that \( \exists x \), such that \( x^2 - 5 = 4 \).

Note that the task is to show that a solution exists, not to show how we would find a solution.

Proof: Consider the value \( x = -3 \). Note that

\[ (-3)^2 - 5 = 9 - 5 = 4. \]

Done.

We pulled \( -3 \) out of the air, and showed that \( (-3)^2 - 5 \) is equal to 4.
Logically, existence proofs can be easy. Of course most of the time, the hard part is finding your example. Often an existence proof is really a proof that some general statement is False, so the example is what we’ve called a counter example. For instance, if you were a mathematician studying integration, a goal might be to find a process that would allow you to compute any anti-derivative. As a first step, you should figure out if every function actually had an anti-derivative to find. If you couldn’t prove that, you might try to find a counter example. If you found a counter example, the next question might be to start categorizing which functions have anti-derivatives.

**Example 3.** Here’s a cool example of an existence proof that doesn’t explicitly give an example. This one almost gives an example, but there are existence proofs that don’t even come close to giving an example.

Show that there exist irrational numbers \( x \) and \( y \), such that \( x^y \) is rational.

Consider the two expressions

\[
\sqrt{2}^\sqrt{2} \quad \text{and} \quad \left( \sqrt{2}^\sqrt{2} \right)^\sqrt{2}.
\]

We’ll take it as fact that \( \sqrt{2} \) is irrational. So if \( \sqrt{2}^\sqrt{2} \) is rational, we have an example, and we’re done. That isn’t at all clear, however. If, on the other hand, \( \sqrt{2}^\sqrt{2} \) is irrational, then the second expression must be our example, because

\[
\left( \sqrt{2}^\sqrt{2} \right)^\sqrt{2} = \sqrt{2}^\sqrt{2} \cdot \sqrt{2} = \sqrt{2}^2 = 2,
\]

which is rational.

**Standard Form of an Existence Proof**

I’ll show you “interesting” things from time to time, but I’ll mostly have you doing “boring” stuff. Therefore, when you do an existence proof, I’ll want you to give the same thing every time. You’ll say “Consider \( \langle \text{your example} \rangle \).” And then you’ll demonstrate that your example is actually an example.

**Example 4.** Remember that disproving a “for every” statement is an existence proof. Disprove the statement

Every prime number is odd.

Assume the definition that an integer \( x \) even, if \( x = 2z \) for some integer \( z \). An integer is odd, if it is not even.

Proof: Consider the prime number 2. Since \( 2 = 2 \cdot 1 \), 2 is even, and therefore, not odd.

We’ll have to negotiate what things are obvious, and what things need to be demonstrated. As we move on, this will become less of an issue.

**Quiz 03A**

1. You may assume that given \( x^2 = a \) with \( a \geq 0 \), \( x = \sqrt{a} \) and \( x = -\sqrt{a} \) are both solutions, and there aren’t any others. Disprove the statement “The equation \( x^2 = a \) has two solutions for all \( a \geq 0 \).

2. Disprove the statement “All quadratic equations have two solutions.”

3. Disprove the statement “All quadratic equations have at least one real solution.”

4. Disprove the statement “All integers have a prime factorization with fewer than five factors.” (A prime factorization is like \( 12 = 2 \cdot 2 \cdot 3 \).
5. Disprove the statement “Given any three positive numbers \(x, y,\) and \(z,\) there is a triangle with sides of those three lengths.

**How do you prove a \(\forall\)?**

The basic idea is that you take a generic example that has only the properties that all the members of the group have, and show what you want to show about that generic example. We then conclude that whatever is true about the generic example must also be true for each member of the group.

**Example 5.** Show that every \(x\) that is a multiple of 6 is also a multiple of 2.

Proof: Let \(x\) be a multiple of 6. This means that \(x = 6 \cdot z,\) for some integer \(z.\) Therefore, \(x = 6 \cdot z = 2 \cdot 3 \cdot z.\) Since \(3z\) is an integer, then \(z\) is 2 times an integer, and therefore, a multiple of 2.

Note that \(x\) is our generic example, and we have only assumed about it what is true of every multiple of 6. What’s true of \(x\) must be true of any multiple of 6.

**Quiz 03B**

1. Show that every multiple of 10 is a multiple of 5.

**Homework 03**

Prove or disprove the following statements.

1. Every multiple of 6 is a multiple of 4.
2. There exists a multiple of 6 that is a multiple of 4.
3. Every multiple of 12 is a multiple of 3.
4. There exists a multiple of 4 that is a not an even number.
5. There exists two different irrational numbers \(x\) and \(y,\) such that \(x^y\) is rational. Hint: This is like the example in class, just try something different from \(\sqrt{2}^\sqrt{2}.\)

Answers on next page.
Quiz 03A

1) Consider the equation $x^2 = 0$. We know that $x = \sqrt{0} = 0$ and $x = -\sqrt{0} = 0$ are the only solutions to this equation, so this equation only has one solution.

2) Consider the equation $x^2 = 0$. It only has one solution $x = 0$, as was shown in Problem 1.

3) Consider the equation $x^2 = -1$. We know that for any real number $x$, $x^2 \geq 0$. Therefore, no real number could be a solution.

4) Consider the integer 216. Its prime factorization is $216 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$, which has six factors.

5) Consider the numbers 1, 1, and 5. No triangle has those sides. If $\triangle ABC$ is a triangle, and $AB = BC = 1$, then it must be that $AC < 2$, and so $AC = 5$ is impossible.

Quiz 03B

1) Let $x$ be a multiple of 10. Therefore, $x = 10z$ for some integer $z$. This means that $z = 5(2z)$, and $x$ is a multiple of 5.

HW 03

1) (False) Consider the integer 18. 18 is not a multiple of 4. If it were, we would have $18 = 4z$, and $z = 4.5$, which is not an integer.

2) (True) Consider the integer 12. Since $12 = 6 \cdot 2$, it is indeed a multiple of 6. Since $12 = 4 \cdot 3$, it is a multiple of 4.

3) (True) Let $x$ be a multiple of 12. Then $x = 12z$ for some integer $z$. Therefore, $x = 3(4z)$, and so $x$ is a multiple of 3.

4) (False) [To disprove, we must show that every multiple of 4 is even.] Let $x$ be a multiple of 4. Then $x = 4z$ for some integer $z$. Therefore, $x = 2(2z)$, which is an even number.

5) You could use $\sqrt{3}^\sqrt{2}$ and $\left(\sqrt{3}^\sqrt{2}\right)^\sqrt{2}$. The main thing are the two $\sqrt{2}$ exponents in the second example that becomes a square. You could do something similar with cubes, etc.