Proof Techniques

July 5, 2012

Now that we've discussed how to write basic proofs, we should explore some different proof techniques. The proofs we wrote last time were *direct proofs*: we started with the hypotheses and we made a chain of logical deductions to eventually prove the given statement. This is generally the most desirable way to prove something, but it may not always work. Even if it does work, it may not be the best way. To this end, there is another proof technique called **proof by contradiction**.

1 Proof by Contradiction

An alternative to a direct proof is a proof by contradiction, or in Latin, *reduction ad absurdum*. Instead of assuming the hypotheses and directly proving the result, you assume the hypotheses and you *assume that the result is not true*. You then try to make logical deductions until you arrive at a *contradiction*, which is a sort of logical conundrum. This contradiction should then lead you to conclude that there is a faulty assumption somewhere, and the only possibility is the assumption that the result is false. In summary:

Proof by Contradiction: Suppose that you are asked to prove a statement of the form

"If A, then B."

To prove this by contradiction:

1. Assume (A) and (not$B$).
2. Investigate the logical implications of these assumptions. (Use any theorems, definitions, etc. that you know.)
3. Arrive at a contradiction.
4. Conclude that B must be true after all.

There is one thing that should be noted before we continue. A proof by contradiction is not generally considered to be an aesthetically pleasing proof, and the technique should always be used as a last resort. That is, you should always try first to prove something directly, and then attempt a contradiction proof if a direct proof is too difficult. However, contradiction is sometimes the only way, and sometimes it may even give a nicer proof than those that can be obtained directly.

The following example is the oldest known proof by contradiction. There are actually many other known proofs of this statement, but the contradiction proof is still well-known due to its simplicity.

Example 1. Prove that there are infinitely many prime numbers.

Proof. Suppose not - that is, let's assume that there are only finitely many prime numbers, say

$$p_1, p_2, \ldots, p_n.$$

Consider the integer

$$N = p_1 p_2 \ldots p_n + 1.$$

Observe that none of the primes $p_1, \ldots, p_n$ divide N. Since these are all the prime numbers, N has no prime divisors. But every integer can be written as a product of primes, so we have arrived at a contradiction. Therefore, our assumption that there are only finitely many primes must be faulty. We can thus conclude that there must be infinitely many primes. □

Here is another example. The details are a little more straightforward, and you simply need to "follow your nose" after making the necessary assumptions.

Example 2. Suppose that $a \in \mathbb{Z}$. Prove that if a^2 is even, then a is also even.

Proof. Assume that a^2 is even, but that a is odd. Then

$$a = 2n + 1$$

for some $n \in \mathbb{Z}$. If we compute a^2, we get

$$a^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1,$$

which is odd. But we are assuming that a^2 is even, so we have arrived at a contradiction. Therefore, our assumption that a is odd must be invalid, and we can conclude that a must be even. □

Here's one for you to try on your own if you want more practice. You can ask me to check your proof if you want, or you can probably find the proof written down in any number of places.

Exercise: Prove that $\sqrt{2}$ is an irrational number.

2 Mathematical Induction

There is another proof technique, called the *Principle of Mathematical Induction*, which is used in special situations. One generally employs it to prove a statement that depends on an integer n. For example, you might be asked to prove that some formula, written in terms of n, holds for all $n \in \mathbb{Z}$. If you are lucky, you might be able to prove it directly. However, it's possible to envision, at least in principle, a systematic way of writing down such a proof. You could prove the result for $n = 1$, and then use this fact to *induce* the result for $n = 2$. You could then prove it for $n = 3$, then $n = 4$, and so on, proving each case by using the previous one. Obviously we can't actually write a proof this way - it would require a lot of work, and we'd have to prove an infinite number of cases. Fortunately, mathematical induction gives us the ability to do all of this in one fell swoop.

Principle of Mathematical Induction: Suppose that you are asked to prove that a statement $P(n)$, depending on $n \in \mathbb{Z}^+$, is true for all n. To prove this via induction, there are two steps:

Base case: Prove that $P(1)$ is true.

Inductive step: Assume that $P(n-1)$ is true, and use this to prove that $P(n)$ is true.

Example 3. Prove that for all $n \in \mathbb{Z}^+$,

$$1 + 2 + \cdots + n = \frac{1}{2}n(n+1).$$

Proof. We need to check first that the formula holds for $n = 1$. The left side is simply 1, and the right side is

$$\frac{1}{2} \cdot 1 \cdot (1+1) = \frac{1}{2} \cdot 1 \cdot 2 = 1,$$

so the formula holds for $n = 1$.

Now we need to handle the inductive step. Assume that the formula holds for $n-1$, i.e., that

$$1 + 2 + \cdots + (n-1) = \frac{1}{2}(n-1)(n).$$

Then

$$\begin{aligned} 1 + 2 + \cdots + n &= 1 + 2 + \cdots + (n-1) + n \\ &= \frac{1}{2}(n-1)n + n \\ &= \left(\frac{1}{2}(n-1) + 1\right) n \\ &= \left(\frac{1}{2}(n-1+2)\right) n \\ &= \frac{1}{2}n(n+1). \end{aligned}$$

□

Now try the following example, which actually relates to abstract algebra.

Example 4. If G is an abelian group and $a, b \in G$, prove that

$$(ab)^n = a^n b^n$$

for all $n \in \mathbb{Z}^+$.

Proof. For $n = 1$, we simply have

$$(ab)^1 = ab = a^1 b^1,$$

so the base case holds. Now assume that $(ab)^{n-1} = a^{n-1}b^{n-1}$. Then

$$(ab)^n = (ab)^{n-1}(ab) = a^{n-1}b^{n-1}ab$$

by assumption. Since G is abelian,

$$a^{n-1}b^{n-1}ab = a^{n-1}ab^{n-1}b = a^n b^n.$$

Therefore, the result holds by induction. □

If you want to read more about mathematical induction, or if you want to try other problems, Section 1.6 of Herstein is devoted to induction. There are more examples, and there are several exercises that would allow you to practice proofs by induction.