Proofs

Kevin Gold

September 12, 2017

Modular arithmetic can be surprising in how it works. How do we know that the properties we've described are *always* true in modular arithmetic? The properties of modular numbers weren't discovered through experiments, but through a different way of knowing: mathematical proofs, of the kind that you encountered in your high school geometry class. It's somewhat surprising to think about it, but mathematicians (and theoretical computer scientists) make discoveries about the world just by thinking rigorously about it. Unlike the findings of many other disciplines, good proofs tend to survive the test of time, since they require only careful thought to verify. We continue to use mathematical results today that were developed thousands of years ago. (Contrast this with the technical documentation from a decade ago that people are always cleaning out of their offices.)

Over the course of your computer science studies, you will be presented with a variety of proofs for things - proofs that algorithms work, that they are fast, that certain computations are possible or impossible. Like jazz, you can't quite appreciate a good proof until you've tried to create one yourself; and even if you don't end up using proofs in your final place of employment, you probably *will* occasionally need to make compelling arguments. (It's said Abraham Lincoln kept a copy of Euclid's book of proofs, the *Elements*, in his saddlebags, so that he could always remember what a really compelling argument looks like.)

In this chapter, we'll study the basics of creating proofs.

1 Elements of a Proof

A proof logically guides the reader from what he or she already knows to the conclusion that another statement must be logically true. A proof doesn't need to contain equations, or even any numbers or mathematical symbols at all. It is usually composed of sentences, with mathematical symbols used only when they make the argument clearer. The main requirement is that every statement must clearly follow from either a definition, a theorem we have already established, or a statement earlier in the proof.

Let us take as a statement to be proven the "additive inverse property" of modular numbers. Recall that Z_n is the set of integers in the range [0, $n-1$].

Theorem 1. *Every a in $\mathbb{Z}_n$ has an additive inverse b in $\mathbb{Z}_n$ such that $(a+b) = 0$.*

Proof(?): The number $n-a$ serves as this inverse, since $a+(n-a) \bmod n = n \bmod n = 0 \bmod n$.

The proof gives enough explanation to thoroughly satisfy a reader that yes, every number mod n has an additive inverse, because it's clear $n-a$ when added to a produces n, which is equivalent to 0 mod a.

But wait, are we certain that $n-a$ is always a number in $\mathbb{Z}_n$? Double-checking the boundaries, we see that when a is 0, $n-a$ is n, which is out of bounds. When a is $n-1$, $n-a$ is 1, which is fine. This is the kind of thing that causes a "bug" in a proof - we forgot to think about a corner case. Of course the statement is true, but our logic is faulty. We can correct it as follows:

Proof. If a = 0, the additive inverse is 0. For $a > 0$, the number $n-a$ serves as this inverse, since $a + (n-a) \mod n = n \mod n = 0 \mod n$. □

The symbol at the end is called a "tombstone" and indicates to the reader that the proof is done. (Some mathematicians write "QED" instead to mean "I proved it"; the letters stand for a Latin phrase that means "that which was to be proven.")

This second proof is correct, while the first was not, just because we were a bit sloppy and made a claim that we hadn't quite thought through.

We can usually assume a knowledge of high school mathematics when doing proofs, including anything you know through algebra.

Theorem 2. *(Distributive property) For all n, $c(a+b) \bmod n = (ca+cb) \bmod n$.*

Proof. The distributive property holds in the integers, so $c(a+b) = ca+cb$. Applying the modulo operator to both sides proves the equation. □

We'll next explore some useful proof techniques.

2 Cases and "Without Loss of Generality"

Sometimes a statement has different reasons for being true depending on what object you're talking about. It's therefore useful to break the proof into *cases*, where you prove the statement is true for different reasons in different situations. We saw a tiny example of this in the previous section, where our argument for the existence of an additive inverse was slightly different for the additive inverse of 0.

Theorem 3. *If $a \bmod 2 = b \bmod 2$, then $(a+b) \bmod 2 = 0$.*

Proof. Either a and b are both $1 \bmod 2$, or a and b are both $0 \bmod 2$. In the first case, the sum is $2 \bmod 2 = 0 \bmod 2$. In the second case, the sum is also clearly $0 \bmod 2$. □

Occasionally the different cases don't really matter - they're only trivially different, and you only need to point out to the reader that they don't matter. In this case, you can make an assumption "without loss of generality" - pick a case and prove it, and the reader can assume the other cases work similarly.

Theorem 4. *The sum of an even number and an odd number is odd.*

Proof. Suppose we have two numbers x and y, and without loss of generality, let us assume x is even. Then $x \bmod 2$ is 0, $y \bmod 2$ is 1, and their sum mod 2 is therefore 1, meaning that $x + y$ must be odd. □

Here, we could have separately proven the case where x was odd and y was even, but a reasonable reader would conclude that the logic for that case would be identical. It's still polite when making an assumption "without loss of generality" to point out that (a) an assumption is being made and (b) it does not really matter. The phrase "without loss of generality" accomplishes these things.

3 Proof by Contradiction

One of the most useful methods of proof is a proof by contradiction. This is where you assume the opposite of what you want to prove, and proceed to show that the assumption results in a logical impossibility. If the opposite of what you want to prove is impossible, then what you want to prove must be true.

Euclid used this technique over two thousand years ago to prove that there are an infinite number of *prime* numbers - numbers that have no divisors besides themselves and 1.

Theorem 5. *There are infinitely many primes.*

Proof. Suppose, for the sake of contradiction, that there are only a finite number of primes; let $\mathcal{S} = \{p_1, p_2, \ldots, p_n\}$ be the set of **all** prime numbers. Now consider the number

$$P = p_1 \cdot p_2 \cdots p_n + 1.$$

Now P must be either prime or composite. If P is prime, it must be in the list. But this cannot happen since it is larger than any number in the list. And if P is composite, it must be divisible by a prime in $\mathcal{S}$ since, by assumption, all primes are in $\mathcal{S}$. However, the remainder after P is divided by any p_i is 1, not 0. So P is not divisible by any p_i in the list. We have found a contradiction with both the idea that P is prime and the idea that P is composite, and it must be one or the other. Thus, our assumption that there are a finite number of primes must be false. □

Notice the use here of not only contradiction, but cases as well. Proofs can combine several different techniques. We'll later cover a technique for proving statements about an infinite number of objects, called *proof by induction*. That will be yet another technique that could be combined with these techniques. On the other hand, some proofs rely on clever arguments that don't have an easily categorized strategy at all.

4 Tips for doing proofs

- Consider starting by writing down what you are given at the top of your page, and what you would like to prove at the bottom of the page. For example, if you wished to prove "the square of an even number is an even number," you could start with "Suppose x is an even number," and end with "therefore, x^2 is even."
- Consider what follows from the definitions of your terms. "Suppose x is an even number" could be followed with "Therefore, $x = 2y$ for some integer y." Even if you're not sure yet where you're going, you may see how to get to the end after you make a little progress.
- Working backwards is also possible. If the last statement on your page is "therefore, x^2 is even," you might write before it "therefore, $x^2 = 2z$ for some integer z" in the hopes that you can prove this somehow.
- Always check your assumptions and test corner cases. What if your even number is zero? If your argument still holds for these cases, you don't need any extra text. But you might sometimes need separate arguments for special cases.
- If you aren't sure who your audience should be and what you can assume, imagine you are trying to convince a smart but skeptical classmate.

5 Summary

We know mathematical facts through proofs, which are logical arguments that one statement follows from another. Proving a mathematical fact could involve particular techniques such as proof by cases (breaking down the argument according to different possible situations) or proof by contradiction (deriving a logical impossibility by assuming the opposite of what is to be proven), but proofs don't necessarily need to use any special technique at all. In constructing proofs, try to develop understandable arguments that make no unfounded assumptions; each statement should logically follow from the last, making your reader nod along with the argument until the end instead of sitting up and objecting, "But how do you know *that*?"

More proofs are in your textbook, and you might now have a better appreciation of what they are trying to do and how they are constructed.