Chapter 3

Proofs

"A mathematician's reputation rests on the number of bad proofs they have given."
– Abraham Samoilovitch Besicovitch

1. What is a proof?

To cut right to the chase: a proof is simply an explanation. Except that it is an airtight, 100%-convincing or foolproof explanation. You may have seen a well intention-ed but joy-draining version of these things in a previous Geometry course; in that class, **shudders**, a "proof" required a two-column format consisting of "statements" and "reasons." You likely came away with the impression that proofs were mostly about correct styling choices and citing arbitrarily-numbered facts from a textbook, and, OH-MY-GAUSS!!!!!, this couldn't be further from the truth.

Mathematicians do not talk like this. We share ideas and proofs the way a lot of regular, normal people talk about anything: on groupchats or via Twitter. We also simply write *proofs* like we write anything else, using regular sentences and paragraphs. And the point of the proof itself is to convey clear, step-by-step thinking that our readers can follow. So clear and carefully laid-out, in fact, that the readers cannot help but be convinced by the explanation.

Of course, all of this begs a natural question: if a *proof* is nothing more than an explanation, then *what, exactly, do proofs explain?* I am so very glad you asked. Established mathematical facts go by a variety of names, but probably the most important one is "**Theorem**." A **Theorem** is a mathematical fact (that can be explained by a **proof**), but it is often one that is regarded as important or significant. For example, one part of the **Fundamental Theorem of Calculus** states

> If a function $f : [a, b] \to \mathbb{R}$ is continuous, then
>
> $$\int_a^b f(x)\,dx = F(b) - F(a), \text{ where } F'(x) = f(x).$$

You may have noticed that the Theorem above has the form of an if-then or conditional statement, and, generally speaking, ***the vast majority of Theorems are if-then or if-and-only-if statements***. We will see proofs of interesting and significant if-then (and iff) statements, but we will also want to practice proving smaller or bite-sized Theorems, too. Mathematicians distinguish **Theorems** from these "mini-**Theorems**" by giving them different names:

Type of Statement	Name(s)
important $P \Rightarrow Q$ important $P \iff Q$	**Theorem**
small $P \Rightarrow Q$ small $P \iff Q$	**Proposition** **Claim** **Lemma**

The term "**Proposition**" will be used throughout this text to refer to these mini-theorems, with some notable exceptions. Before we dive deeper into the *proofs* that explain such **Propositions** and **Theorems**, you should be aware that these often require careful use of established **Definitions** and familiar mathematical facts (e.g. that $0 + x = x$ for all real numbers x).

At this point in our text you have learned about sets and so we can (and will!) examine Propositions and Theorems about those objects, but we also need to practice proving Propositions about *other* things, too, and so we will need to introduce new definitions along the way. Here is an example of a familiar Proposition (and its proof), one that requires official definitions.

Example 1.1. *Consider the following proposition and the proof that explains it.*

Proposition. 2 is the only prime number that is even.

Proof. *Suppose $n \in \mathbb{N}$ is even and prime (we will show that $n = 2$).*
By definition of even, $\exists\, a \in \mathbb{N}$, $n = 2a$.
It follows that 2 divides n, and that a divides n.
Since n is prime this means that $a = 1$ and that $n = 2$, completing the proof. □

Perhaps not all of the details or words in the example above make perfect sense to you (that ending square symbol, "□," means the proof is officially over, for example), but that's OK! Hopefully the main ideas of the proof make *enough* sense right now; the details will follow after you read and work through the remaining sections.

The point of this example is this: we need to have a definition of the word "**even**" in order for the second line to be meaningful. Thankfully we have already established this definition, but notice that the third line really needs an official definition of "**divides**," and that the last line also needs a precise definition of "**prime**." Indeed, if one wanted to prove **the Fundamental Theorem of Calculus** they would need to use definitions of **continuous** and **definite integral**.

All of this is to say that we should right here and right now collect some definitions so that we can practice writing proofs of interesting and varied Propositions.

1.1. Some Useful Definitions To Have on Hand. The following definitions are all about natural numbers, $\mathbb{N}$, or integers, $\mathbb{Z}$. They may *seem* like overkill, but because we need our proofs to be 100%-foolproof, the concepts they use need to be discussed with care and precision.

Definition 3.1. (Divides & Divisors). *An integer $a \in \mathbb{Z}$ is said to* ***divide*** *another integer, $b \in \mathbb{Z}$, if $\exists\, q \in \mathbb{Z}$ such that*

$$b = q \cdot a.$$

*This is notated by writing $a|b$, where the line "$|$" is pronounced "****divides****." For instance, you are already aware that 5 divides 10, but now we can write $5|10$; this is a true statement because*

$$10 = 2 \cdot 5.$$

We also use the word ***divisor*** *in this situation. That is, the phrase "a* ***divides*** *b" can be restated as "a* ***is a divisor of*** *b." This allows us to write and speak sentences like "5 is a* ***divisor of*** *10." Indeed, one can write down* all *of the divisors of 10 (or any integer):*

$$\text{the set of the divisors of } 10 \ = \{-10, -5, -2, -1, 1, 2, 5, 10\}\,.$$

*Make certain you can use the definitions of "****divides****" and "****divisors****" to understand why each number in the set above belongs there. A good way to check that you're understanding these is to answer a questions like these:* what are all the divisors of 9? What about the divisors of 5? 100? 24?

*Note: These definitions only apply to integers, even though you know how to divide other types of numbers (like rationals and reals). Also, some us the synonym "****factor****" for "****divisor****."*

Definition 3.2. (Multiple). *An integer $b \in \mathbb{Z}$ is said to be* ***a multiple of*** *another integer $a \in \mathbb{Z}$ if $\exists\, q \in \mathbb{Z}$ such that*

$$b = q \cdot a.$$

In other words, the phrase "b ***is a multiple of*** *a" is another way of saying "a|b." (Also "b* ***is a multiple of*** *a" means "a is a divisor of b.") For instance, we can say "10 is a multiple of 5."*

Definition 3.3. (Prime). *A natural number $p \in \mathbb{N}$ is a* ***prime number*** *if it has exactly two (positive) divisors. For instance, 7 is prime because the only natural numbers that divide it are 1 and 7. 10 is* ***not prime*** *because it has more than two (positive) divisors, and 1 is* ***not prime*** *because it only has one, single (positive) divisor.*

Compare this definition with the more common one that sounds something like this: "a number p is prime if it is only divisible by 1 and itself."