A Quick Tutorial to Proof Structure

James Camano

December 24, 2020

Contents

Chapter 1

Introduction

1.1 Goals of this Booklet

The main goal of this booklet is to provide a clear introduction to logical proof structure - a way of formalizing reasoning. I hope that by the end of the booklet, you have gained a few mathematical tools to use to prove various things. I aim to do this by providing a large breath of examples throughout that involve familiar math involving numbers, basic geometry, and a bit of calculus.

I write this booklet as a first-glance introduction to formal proof structure, **primarily** for readers who have not had prolonged exposure to this set of techniques before. To be sure, I would not consider this booklet to be a textbook in any sense, but rather as a pocket guide for utilizing some of the most powerful tools in math. In this way, I aim for a balance of rigour: as much of it that does not distract away from the fundamental idea of the proof itself, which is the technique being used. For example, when we speak about functions, we will be thinking about them as "mathematical machines" that take a number as its input and returns a unique number as its output - rather than the more fundamental set formulation.

To be sufficiently concise, this paper must assume a few things. In particular, this paper asks for a familiarity of high school mathematics: that in the realm of algebra, factoring, functions, variables, et cetera. A section that defines the preliminary requirements is provided in the next chapter.

Proofs in mathematics consist of symbolic relationships (e.g. expressions and equations) and natural language to describe the logic being applied. As is a feature of math, the way that we provide these descriptions require a certain structure. This fact is useful to keep in mind as we explore different examples in this booklet.

1.2 Why?

Even a quick search on the web gives handfuls of professional resources for math learning. So a question that I have anticipated while I have been writing this booklet is "*Why make another?*" My answer to this is that though there are many resources written by professionals and instructors who *were* once students, this resource is written by someone who *is* a student. I think that, counter-

intuitively, my position affords me a few advantages. I believe that I can relate my thoughts and ideas more naturally to people who are around my skill range: the manner of speaking and relaying thoughts among children is much more fluid than when interacting with other age groups and I think the analogy carries here.

Since I am not writing this expecting professional gain, I have a larger freedom to illustrate mathematical ideas at a more intuitive level and choose to be more rigourous at will; it is easier see the forest in spite of the trees. For an example, while it is true that functions can be rigourously defined in terms of "relations" which can be rigourously defined in terms of "sets" (whatever these things mean), it is important that we can still *interpret* what a function is: a "machine" that spits out a unique output for every input. It is important that despite definitions, we still understand how to manipulate them. For example, we can always add the output of two functions to create a new function, we can multiply them, we can take their derivatives, etc.

Finally, since this is *not* a textbook, there are no assignments. There is no pressure to get a good mark, no pressure to understand every single little detail in the book and no pressure to cram. This booklet was written for the express love of math and learning, and if it inspires you then may you continue on the path of more complex and beautifully rigourous math.

1.3 Transparency

As is the case in any learning endeavour, one is bound to make mistakes. Being able to recognize a flaw in a piece of work and correcting it to make the work better allows us to grow. Mathematics is no different. While perhaps we will make a mistake or two in an exercise or in a proof, I will admit to some mistakes in writing that I have subsequently tried to correct in the hope that this product is all the more better for it:

- In the first stages of writing this booklet I have written it for an imaginary audience who already knows of the content I am writing about. Of course this defeats the purpose of the booklet, so I have revised my mindset in writing this current version.
- The starting point of the booklet should not be what is the most elementary, but what is most *natural* and *familliar*. This way, when we are more aquatinted to proofs we can tackle these harder elementary proofs.
- I had started with an obscene amount of prerequisites for the book as opposed to naturally defining them by example. This prerequisite knowledge hurts the reachability of the booklet so I have endeavoured to have the minimum amount of prerequisite knowledge.

I believe being transparent here is important: it forms us a common ground where we can talk about mathematics without fear.

1.4 Enter Reasoning

It is important to answer a few questions about the nature of proofs before we get to proving.

Who Proves? In daily life, we are bombarded with questions about the world that need answering: "Is it raining today?", "Will the bus arrive at 10:15 this morning?", "Do I meet the qualifications for this job?" et cetera. Questions like these vary in complexity and impact on our lives, and in most cases we want to be right in our conclusions, especially when these judgments affect our decisions on other questions down the line. Thus, in this way, those who want to understand are those who prove.

When to Prove? Whenever we are curious about some phenomenon, it is natural to ask questions about its nature. Finding answers to these questions increases our understanding; it shines light on that phenomenon. Our answers inform how we interact with these objects, and determine other questions we might ask about them. Thus, we prove whenever we are curious.

What are Proofs? Proofs are the art of reason. A proof requires the application of logic to knowledge to to discover new facts about the subject at hand. There is a tangible power to a proof: it **asserts** unequivocally that something is true; its veracity is independent of time, space, language or culture - conditional on that it is "correct". A proof distinguishes what is true and what is false.

Proofs lend themselves especially well to mathematics in large part because the subject is so pure. Mathematical definitions are necessarily unambiguous and the investigation process follows a strict procedure where each step must be unchallengable. However, proofs are not drab things. As we will see, these rules we give ourselves will give life to beautiful scenery.

Why Prove? To prove is to wield the scepter of reason. We engage reason so that we can answer questions. We answer questions so that we can direct our decisions. We prove because we are naturally curious, and to be curious is to be human.

That might strike as too mystical or ethereal. If so, then notice that many scientific advancements in physics, chemistry, biology and even the humanities are solidly based upon logical proofs. The effect of proofs surrounds us. Devices such as our phones that allow us to interact with each other from far distances instantaneously or structures such as bridges that stand the test of time or technology that sends people to the moon all rely on concepts rigourously proven; guaranteeing that these things will work. Thus, proofs empower the fields that use them.

1.5 Motivation

Is it necessarily true that you need to have some insight of the divine to discover mathematical truths? I would argue that this is not the case at all: you just need a starting point plus a little curiousity. To see what I mean, let's add up the odd numbers in order starting from 1:

$$1 = 1$$
$$1 + 3 = 4$$
$$1 + 3 + 5 = 9$$
$$1 + 3 + 5 + 7 = 16$$
$$...$$

Do you see a pattern? How about when we reverse the equalities?

$$1 = 1$$
$$4 = 1 + 3$$
$$9 = 1 + 3 + 5$$
$$16 = 1 + 3 + 5 + 7$$
$$25 = 1 + 3 + 5 + 7 + 9$$
$$...$$

It seems we can conjecture that *adding consecutive odd numbers in order, we can generate consecutive squares of integers.* Let's see if we can convince ourselves of this. Since we have perfect squares on the left-hand-side (LHS) of our equations, it is reasonable to analyze the structure of a square.

Well, the most basic square is the 1x1 square. Lets give this square a name, say, S_1. We know the area is the product of the side lengths: $1 \times 1 = 1$. But how do we connect this to the square S_2 of side length 2 and area $2 \times 2 = 4$? Lets try *extending* S_1.

For the rest of this document, we turn to answer the question: **How to Prove?**

Chapter 2

Preliminaries

2.1 Definitions

In order to formalize our reasoning on objects which have properties like numbers, vectors, or shapes, we need to first make **mathematically clear** what we mean when we talk about numbers, vectors or shapes.

Example 2.1. *Definition of the even and odd numbers*

Given the non-negative integers $0, 1, 2, \ldots$, we want to characterize the even numbers from the odd numbers.

The even numbers are those numbers that are evenly divisible by 2:

$$(0, 2, 4, 6 \ldots) = (2 \cdot 0, 2 \cdot 1, 2 \cdot 2, 2 \cdot 3 \ldots)$$

. We define even numbers as those numbers of the form $2 \cdot k$, where k is some non-negative whole number.

The odd numbers are those numbers not evenly divisible by 2:

$$\begin{aligned}(1, 3, 5, \ldots) &= (0 + 1, 2 + 1, 4 + 1, \ldots) \\ &= (2 \cdot 0 + 1, 2 \cdot 1 + 1, 2 \cdot 2 + 1, \ldots)\end{aligned}$$

We define the odd numbers are defined by those numbers of the form $2 \cdot k + 1$, where k is some non-negative whole number.

A definition of something formalizes precisely what characterizes that object. If we are to show that some object O fits our definition, then we must show that O has exactly those properties listed in the definition.

Example 2.2. *Definition of even and odd functions*

As stated in the introduction, a function is a "mathematical machine" that takes an input and returns an output that is unique for that input. That is, a function f satisfies the condition:

$$\text{If } a = b, \text{ then } f(a) = f(b).$$

The complete set of input values that f can take is called its domain and we denote it by $\text{Dom}(f)$, and the complete set of f's output values is called its range, and we denote it by $\text{Ran}(f)$.

We will say that a function f_E is an *even function* if it satisfies the following condition for all input values x in $\text{Dom}(f_E)$:

$$f_E(-x) = f_E(x)$$

We will say that a function f_O is an *odd function* if it satisfies the following condition for all input values x in $\text{Dom}(f_O)$:

$$f_O(-x) = -f_O(x)$$

Examples of even functions are $f(x) = x^2, g(x) = \ln(|x|)$ and $h(x) = \cos(x)$. Examples of odd functions are $t(x) = \tan(x)$, $u(x) = x$ and $v(x) = 0$, as is easily verifiable.

2.2 Conventions

Assigning a Number to a Letter

The mathematical statement:

$$x = 2.2$$

assigns the number 2.2 to the letter x, and allows us to use x in place of 2.2. If we expect the value of x to take on different values, then we call x a variable. If we require the value of x to stay the same, then we call x a constant.

This notation is especially useful if we want to store the effect of an operation without explicitly calculating it. This allows us a simple yet powerful freedom to algebraically manipulate our values:

Example 2.3. *Variable Manipulation*

Let $a = p/q$ and $b = r/s$ where q, r, s are not equal to 0. We wish to find the value of $a \div b$. Assign $D = a/b$. We have:

$$D = a/b \tag{2.1}$$
$$bD = p/q \qquad \text{multiplying both sides by } b \tag{2.2}$$
$$(r/s)D = p/q \tag{2.3}$$
$$rD = p/q \cdot s, \qquad \text{multiplying both sides by } s \tag{2.4}$$
$$D = (p/q) \cdot (s/r) \qquad \text{multiplying by } 1/r \tag{2.5}$$

So $\dfrac{p}{q} \div \dfrac{r}{s} = \dfrac{p}{q} \cdot \dfrac{s}{r}$, as expected.

Assigning a Mathematical Object to a Letter

In the same way as numbers, we can also use variables to refer to mathematical objects other than numbers. We may say that $x = (2, 9)$, $y = 5 + 3i$, $z = f$ (where $f(x) = x^2$), et cetera.

Quantifiers

2.3 Properties of Equality

Suppose that two mathematical objects (numbers, ordered pairs, matrices, ...) a and b are the same object, or equal. We express this as $a = b$.

Then to express what we mean by a is the same as b, we assume that the following statements are true:

(a) If $a = b$ and $b = c$, then $a = c$. This property is called **transitivity**.

(b) If $a = b$ then $b = a$. This property is called **symmetry**.

(c) $a = a$ (a is equal to itself). This property is called **reflexivity**.

2.4 Inequalities

In addition to equality between two numbers a and b, we can express relationships between them in the form of inequality operators:

- We say that $a < b$ if $b = a + c$, for some *positive* number c.
- We say that $a > b$ if $b < a$.
- If either of the above are satisfied, then $a \neq b$.

Theorem 1. *Let $a, b \in \mathbb{R}$ such that $a = b$. Then $a - b = 0$*

Proof. If $a - b \neq 0$, then either $a - b > 0$ or $a - b < 0$.

So, if $a - b > 0$, then $a = b + c$, for some $c \in \mathbb{R}, c > 0$. That is to say $a > b$, which contradicts our assumption that $a = b$. In the other case, $b = a + c$, meaning that $b > a$, giving us another contradiction. □

2.5 Sets

We define a set to be an unordered (and possibly infinite) collection of unique objects called elements, or members. We denote a set by surrounding its elements by curly braces, as in the following example:

Example 2.4. *Finite Sets*

- Let S_1 be the set of non-negative integers which are less than 10. Then $S_1 = \{0, 1, 2, ..., 9\}$, and S_1 has 10 elements.
- Let S_2 be the set of integers whose square is equal to 16. Then $S_2 = \{-4, 4\}$, and S_2 has 2 elements.

- Let S_3 be the set of odd numbers that are evenly divisible by 2. Then $S_3 = \{\}$, as S_3 has 0 elements. A set with no elements is called the **empty set**, and is denoted with $\emptyset$.

A set is unordered in the sense that the order for which we list its elements does not affect it. So, from the above example, $S_2 = \{4, -4\}$ as well. A set is a collection of unique objects in the sense that the number of times that an element appears in the set does not affect it. So, $S_2 = \{-4, -4, 4\}$. If a is a member of a set S, we denote this by $a \in S$. If a is not a member of S, then we denote this as $a \notin S$.

We can describe a set in two ways. One way, called an extensive description, is to write down all of its elements as we have done in the above example. The other way, called an intensive description, is to write down the form of an arbitrary element in the set, followed by a rule that the form takes. Symbolically:

$$\{\langle \text{form} \rangle : \langle \text{rule} \rangle\}$$

The latter description is helpful when describing infinite sets.

Example 2.5. *Infinite Sets*

- Let S_4 be the set of integers. Then $S_4 = \{..., -2, -1, 0, 1, 2, ...\}$. We denote the integer set as $\mathbb{Z}$.
- Let S_5 be the set of all perfect squares. Then $S_5 = \{0, 1, 4, ...\}$ (extensive description) and equivalently, $S_5 = \{n^2 : n \in \mathbb{Z}\}$ (intensive description)
- Let S_6 be the set of values x that satisfy $-2 \leq x$ and $x \leq -1$. Then $S_6 = \{x : x \in \mathbb{R}, -2 \leq x \leq 1\}$, where the comma in the rule is a shorthand for "and".

  We call S_6 an interval, and we denote it by $[-2, 1]$. If instead we required $-2 < x \leq 1$ then we would denote it by $(-2, 1]$.
- Let S_7 be the set of all points (x, y) on the cartesian plane that lie on the unit circle. Then $S_7 = \{(x, y) : x^2 + y^2 = 1 \text{ and } x, y \in [-1, 1]\}$.

Some important number sets are defined in section 2.10.1.

2.6 Operations on Sets

2.7 The Sum Operator

In this booklet, we will encounter additions of multiple summands such as:

$$S = 1 + 4 + 9 + ... + 100.$$

Explicitly writing each summand is laborious, so we express this sum with the shorthand:

$$S = \sum_{i=1}^{10} i^2.$$

The symbol $\sum$ (big sigma) is known as the **sum operator**. In general, the sum operator takes the form:

$$\sum_{i=a}^{b} f(i) = f(a) + f(a+1) + \ldots + f(b-1) + f(b),$$

For $a, b \in \mathbb{N}$ and $a \leq b$. We call i the index, which ranges sequentially from a to b. We call the function f the sum term, where the value $f(i)$ exists for all values that i takes.

Example 2.6. *Finite Sums*

1. Let $a = 1; b = 4; f(i) = (-1)^i/i$. We have:

$$\sum_{i=0}^{4} \frac{(-1)^i}{i} = \frac{(-1)^1}{1} + \frac{(-1)^2}{2} + \frac{(-1)^3}{3} + \frac{(-1)^4}{4} \tag{2.6}$$

$$= -1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} \tag{2.7}$$

$$= -\frac{1}{2} - \frac{1}{3} + \frac{1}{4} \tag{2.8}$$

$$= -\frac{7}{12} \tag{2.9}$$

2. Let $a = -2, b = 2; f(x) = 1/x$. We have:

$$\sum_{x=-2}^{2} \frac{1}{x} = \frac{1}{-2} + \frac{1}{-1} + \frac{1}{0} + \frac{1}{1} + \frac{1}{2} \tag{2.10}$$

$$= \frac{1}{0}, \qquad \text{simplifying} \tag{2.11}$$

So this sum is undefined, as $f(x)$ is undefined when $x = 0$.

It should be noted that there is usually no unique way to describe a sum in sum notation. The first sum could have been expressed as $\sum_{i=-2}^{6} (i+2)^2$, and the sum in expression (2.6) could have been expressed as $\sum_{i=0}^{4} \cos(i\pi)/i!$.

All the familliar properties of regular sums apply to $\sum$.

Property 2.1. (Scalar Distributivity) Let $c \in \mathbb{R}$. Then

$$c \sum_{i=a}^{b} f(i) = \sum_{i=a}^{b} c \cdot f(i).$$

Property 2.2. (Combination) Let $a, b \in \mathbb{Z}$ such that $a \leq b$. Then:

$$\sum_{i=a}^{b} (f(i) + g(i)) = \sum_{i=a}^{b} f(i) + \sum_{i=a}^{b} g(i).$$

2.8 Operator Properties

Expressions like -7, $2.2 + 3$, $2.2 - 3$ can be deconstructed into two parts: *operators* and *operands*. In this context, $+$ is an operator that acts on the operands 2.2 and 3 in the set of real numbers. Since $+$ acts on two numbers, we call it a binary operator. The symbol $-$ is an operator that acts on the single integer 7, so we see it as a unary operator.

More generally, let $\circ$ denote some operation on a set of one or more mathematical objects S. Then we say that $\circ$ is defined over S.

Let $x, y \in S$. If $\circ x$ is a valid operation, then we call $\circ$ a unary operator. If $x \circ y$ is a valid operation, then we call $\circ$ a binary operator. Unless conventionally specified by BEDMAS / PEMDAS, we will use parentheses ( ) and square brackets [ ] to denote operator precedence.

We describe a few useful properties of binary operators:

- If for every $a, b \in S$ we have $a \circ b = b \circ a$, then we say that $\circ$ is *transitive*.
- If for every $a, b, c \in S$ we have $(a \circ b) \circ c = a \circ (b \circ c)$, then we say that $\circ$ is *associative*.
- Let $\circ_1$ and $\circ_2$ be defined on the set A. respectively. If $a \circ_1 (b \circ_2 c) = (a \circ_1 b) \circ_2 (a \circ_1 c) = (b \circ_2 c) \circ_1 a$ then we say that $\circ_1$ *distributes over* $\circ_2$.

We will assume the following of our binary operators:

Property 2.3. Common Properties of Binary Operators

- $+$ (addition) and $\cdot$ (multiplication) is transitive and associative over $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \overline{\mathbb{Q}}$ and $\mathbb{R}$.
- $-$ is associative over $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \overline{\mathbb{Q}}$ and $\mathbb{R}$.

We will define the division operation in the following way. Given $p, q \in \mathbb{R}$ where $q \neq 0$ we say that $p/q = r$ is equivalent to $p = rq$ for some $r \in \mathbb{R}$.

2.9 Operative Closure

We say that a set S is **closed** under a certain operation if for *any* two elements $a, b \in S$, the resulting object c that is the result of the operation between a and b *is also* in S. The following properties are true:

- $\mathbb{N}$ is closed under addition and multiplication, but not subtraction and division.
- $\mathbb{Z}$ is closed under addition, multiplication and subtraction, but not division.

$\mathbb{N}$ is not closed under subtraction, as $(8) - (9) = -1 \notin \mathbb{N}$ and $\mathbb{Z}$ is not closed under division as $(3) \div (2) = 1.5 \notin \mathbb{Z}$.

2.10 Common Definitions

2.10.1 Number Sets

- The set $\mathbb{N} = \{0, 1, 2, ...\}$ is called the natural number set.
- The set $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ is called the integer set.
- The set of all numbers that are equal to a ratio of any two integers $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$ is called the rational number set.
- The set of all numbers that are not equal to any ratio of two integers $\overline{\mathbb{Q}} = \{..., \phi, \sqrt{2}, e, \pi, ...\}$ is called the irrational number set.
- The combined set of the rationals and irrationals $\mathbb{R} = \mathbb{Q} \cup \overline{\mathbb{Q}}$ is called the real number set.

2.10.2 Common Properties of Number Sets

Let S be some set of numbers, and let $+$ and $\times$ be defined on S.

- If there is a member $z \in S$ such that for all elements $a \in S$, $a+z = z+a = a$, then we call z an *additive identity* of S.
- If there is a member $k \in S$ such that for all elements $a \in S$, $ka = ak = a$, then we call k an *multiplicative identity* of S.
- If there is a member $b \in S$ such that for some element $a \in S$, $b + a = a + b = 0$, then we call b an *additive inverse* of S.
- If for all elements $p \in S, p \neq z$, there is an element q such that $pq = qp = k$, we call q a *multiplicative inverse* of p.

These properties are part of a set known as *field properties*. The sets $\mathbb{R}, \mathbb{Z}$ and $\mathbb{Q}$ are examples of fields, whereas $\mathbb{N}$ and $\overline{\mathbb{Q}}$ are not. These properties will be fundamental in our discussion on direct proofs.

Example 2.7. $\mathbb{Q}$ *Exhibits the Above Properties*

$z = 0$ is a natural choice for the additive identity. Since $0 = 0/1$ can be expressed as a ratio of two integers, it exists in $\mathbb{Q}$. $k = 1 = 1/1$ is our choice for a multiplicative identity.

For additive inverses, let $p = a/b$ for $a, b\mathbb{Z}; b \neq 0$. Then choose the number $b = -a/b$. We have that $p + q = (a - a)/b = 0$. Finally, for a multiplicative inverse, let $p = a/b$ such that $a, b \in \mathbb{Z}$; $a, b \neq 0$. Let $q = b/a$. $pq = ab/ab = 1$, as wanted.

2.10.3 Functions

- For $n \in \mathbb{N}$, define the function:

$$n! = \begin{cases} 1, & \text{if } n = 0, \\ n \cdot (n-1) \cdots 2 \cdot 1, & \text{if } n > 0 \end{cases} \tag{2.12}$$

  $n!$ is known as the factorial function, and it describes the total number of ways to order n unique objects.

- For $n \in \mathbb{N}$, $c_0, ..., c_n \in \mathbb{R}$, define the function:

$$p(x) = \sum_{i=0}^{n} c_i x^i \tag{2.13}$$

$$= c_0 + c_1 x + ... + c_n x^n. \tag{2.14}$$

  Then, $p(x)$ is called a polynomial. If $c_n \neq 0$, (i.e, $c_n x^n$ is not equal to 0) then $p(x)$ is a polynomial of degree n. Polynomials describe phenomena whose instantanous rate of change is of a smaller order than the value of the function itself at a given point.

- For $k, b \in \mathbb{R}$ such that $b > 0$, define the function $f(x)$:

$$f(x) = kb^x \tag{2.15}$$

  Then $f(x)$ is known as an exponential function. The value b is known as the *base* and k is the coefficient. Exponentials describe phenomena whose instantanous rate of change is of equal or larger order than the value of the function itself.

  A special exponential function deserves mention. Define the number $e = \lim_{x\to\infty}(1 + 1/x)^x = 2.71828....$ The function $g(x) = e^x$ is known as the natural exponential function.

- Given the above definition of the class of exponential functions $f(x)$, define the function:

$$\log_b(x) = f^{-1}(x) \tag{2.16}$$

  Where, for a one-to-one function $y = h(x)$ defined on the set B, $h^{-1}(y) = x$, or equivalently, $h^{-1}(h(x)) = x$. In another sense, the graph of h^{-1} is $h(x)$, but reflected along the line $y = x$.

  Since $f(x)$ is one-to-one on all of its x-values, f^{-1} is defined on all values $f(x)$.

2.11 Optional: A Primer on Symbolic Logic

Chapter 3

Bad Proofs

Here, we explore examples of what **not** to do, and what consistutes bad form and holes in our reasoning. Wherever possible, we correct the mistakes made in our first try.

3.1 Types of Bad Form

As we have previously stated, proofs are the power of reasoning and so our proofs are only as strong as our reason. No matter what proof style we use or how eloquently we present our proof, if one deduction is faulty then the whole proof is rejected. The mathematical court holds zero reservations.

The issue boils down to logical validity and circularity. An argument that is logically valid means that every deduction is justified by the definitions or deductions *preceding* it.[1] On the other hand, a circular argument is one that assumes that its conclusion is true. Though a circular argument is logically valid (of course, if A is true then A is true), its discoveries hold no value until the assumed condition is independently proven.

We will explore these cases of bad proofs:

1. Non-exhaustive Cases,
2. Deductive Inconsistency,
3. Circular Logic, and
4. Ill-definiteness.

Note that an invalid argument for some claim does not necessarily permit us to conclude that the claim is false. To show that an argument is faulty is an argument - a proof - in itself. So by studying bad form we are participating in a logical exercise.

3.2 Non-exhaustive Cases

Consider the following (erroneous) claim:

[1] I will not attempt to define the term "justified" except for requiring that the deduction makes sense, taking prior information into consideration.

Claim 1. *Let* $n \leq 10$, $n \in \mathbb{N}$. *The number* $n! = n \cdot (n-1) \cdots 2 \cdot 1$ *is* ***not divisible*** *by 81.*

Proof. Since all the factors of $n!$ for $n < 10$ are factors in 10!, it follows that 10! is not divisible by 81, then the claim is true.

Notice that

$$10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10.$$

None of these integer factors are a multiple of 81, as wanted. □

This "proof" is invalid because it did not consider all the *possible* factors that come from combining the integer factors of 10!. We show that, in fact, 9! is divisible by 81:

Proof.

$$\begin{aligned} 9! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 && && (3.1)\\ &= 3 \cdot 3 \cdot 9 \cdot (2 \cdot 4 \cdot 5 \cdot 2 \cdot 7 \cdot 8), && \text{factoring} && (3.2)\\ &= 81 \cdot (2 \cdot 4 \cdot 5 \cdot 2 \cdot 7 \cdot 8) && && (3.3) \end{aligned}$$

So, indeed, $9! = 81k$, for some $k \in \mathbb{N}$, and thus the above claim is false. □

3.3 Inconsistency

Consider the (incorrect) claim for numbers in $\mathbb{R}$:

Claim 2. $0 = 1$

Proof. Let $a = 1, b = a$. Then:

$$\begin{aligned} a &= b && \text{commutativity of } = && (3.4)\\ \implies a^2 &= b^2 && && (3.5)\\ \implies a^2 &= ab && && (3.6)\\ \implies a^2 - b^2 &= ab - b^2 && && (3.7)\\ \implies (a+b)(a-b) &= b(a-b) && && (3.8)\\ \implies a + b &= b && \text{dividing by } (a-b) && (3.9)\\ \implies a &= 0 && && (3.10)\\ \implies 1 &= 0 && a = 1, \text{ by definition} && (3.11) \end{aligned}$$

□

The symbol $\implies$ loosely stands for "implies", or "it follows that". We discuss this in section 2.11.

Of course, the lines from equation (3.9) downward do not hold, as the operation performed is a division by zero. A division by zero by any number never yields a finite number, so the deduction is invalid in $\mathbb{R}$.

3.4 Circular Logic

We incorrectly prove the **correct** claim:

Claim 3. *Let $x, y \in \mathbb{R}$ such that $0 \leq x \leq y$. Then $x^2 \leq y^2$.*

Proof.

$$x \leq y \qquad \text{by assumption} \tag{3.12}$$
$$\implies x^2 \leq y^2 \qquad \text{squaring both sides.} \tag{3.13}$$

□

Perhaps because of its conciseness, this proof may seem to hold at first sight. But notice that the proof essentially restates the claim statement: equation (3.12) restates the first sentence (the condition), and equation (3.13) restates the second sentence (the consequent). The transition between these two equations *assumes* that the claim that we are trying to prove true, is true - hence circularity.

We retry the proof of the claim:

Proof.

$$x \leq y \tag{3.14}$$
$$\implies x - y \leq 0 \tag{3.15}$$
$$\implies (x - y)(x + y) \leq 0 \qquad - \text{ multiplied by } + \text{ is } - \tag{3.16}$$
$$\implies x^2 - y^2 \leq 0 \qquad \text{distributing} \tag{3.17}$$
$$\implies x^2 \leq y^2 \qquad \text{adding } y^2 \text{ on both sides} \tag{3.18}$$

□

3.5 Ill-definiteness

Ill-definiteness refers to some definition or condition for an object that has no satisfying member, or whose value is undefined. To assign x to be an even odd number or an odd even number, for example, is a ill-defined assignment as there is no number that is both even and odd at the same time. Another example is letting b to be the largest number in the interval $[0, 1)$.

Of course, if one is doubtful, then they must *prove* that the definition is ill-defined.

Example 3.1. *There is no largest number in the interval $[0, 1)$.*

Proof. Let $a \in [0, 1)$. Then $0 \leq a < 1$. Consider the value $A = (a + 1)/2$. We show that $a < A < 1$, proving that for any choice of a, we can always choose a

larger number in the interval.

$$A = \frac{a+1}{2} \tag{3.19}$$
$$> \frac{a+a}{2}, \qquad \text{since } a < 1, \text{ so } a + a < a + 1. \tag{3.20}$$
$$= \frac{2a}{2} \tag{3.21}$$
$$= a \tag{3.22}$$

So $a < A$. Similarly:

$$A = \frac{a+1}{2} \tag{3.23}$$
$$< \frac{1+1}{2}, \qquad 1 > a. \tag{3.24}$$
$$= \frac{2}{2} \tag{3.25}$$
$$= 1 \tag{3.26}$$

We conclude that $a < A < 1$, as wanted. □

An argument that claims and uses the existence of an ill-defined object is a contradiction, because no such object exists.

When we explore *Proofs by Contradiction* in Chapter 5, we will actually leverage these concepts of ill-definiteness to prove our claims. The reason why this is a valid method of proof is because we *want* to reach a contradiction and one way is showing that a definition that we use is ill-defined.

3.6 Disproving

Questions

1. Consider the following argument for the theorem: If $a, b \in \mathbb{R}$ such that $a = b$, then $a + c = b + c$

   Proof. We deduce the following:

$a = b$	
$a - b = 0$	
$(a - b) + (c - c) = 0$	since $c - c = 0$
$(a + c) + (-b + -c) = 0$	commutativity of $\mathbb{R}$
$a + c = b + c$	adding $b + c$ on both sides

   □

   What is wrong with this proof?

2. In Example 3.1 we asserted that there is no largest value in $[0, 1)$. One might raise an objection with the counterexample that the number $0.999... = 0.\bar{9}$ is the largest number in the set. Show the surprising fact that $0.\bar{9}$ is actually equal to 1. (Hint: $1/3 = 0.\bar{3}$).

3. Show that there is no smallest member of $(0, 1]$.

4. Suppose someone gives you the following proof that there is a integer that is both even and odd:

   Proof. Let $a = 2n + 1$ and $a = 2m$ for some integers $m, n \in \mathbb{Z}$. Then $2n + 1 = 2m$ means $n = (2m - 1)/2$. Thus, a is both even and odd when $(2m - 1)/2$ is an integer. As wanted. □

   What is wrong with this proof?

5. Suppose someone gives you the following proof that for any two numbers $a, b \in \mathbb{Z}$, $(a + b)^2 = a^2 + b^2$:

   Proof. We have two cases to check:

   Case 1: $a = b$

   Case 2: $a \neq b$ □

Chapter 4

Direct Proofs

Just as the name implies, a **direct proof** is a method of proving that uses known facts to directly prove a given statement. We might synonymise the term "direct proof" with "straightforward reasoning".

Example 4.1. *Cookies*

Alice, Bill, and Claire love chocolate-chip cookies. With their combined efforts, they are able to finish a cookie jar from full capacity in very short time. One morning, the three discover that one cookie remains in the jar and they decide to work out the logistics of sharing it later in the day. They come back that afternoon to find that the cookie jar has been releved of its treat. Alice asks with genuine curiousity: "who ate the cookie?", to which Claire replies: "I don't know!". Our job is to figure out who ate the cookie.

Assume that in this scenario, (1) a person speaks with complete sincerity and (2) only Alice, Bill or Claire could have eaten the cookie.

We deduce that Alice couldn't have been the one to eat the cookie, since she asked the question and we assumed sincerity. Thus either Bill or Claire had eaten the cookie. Just as quickly we find that Claire is innocent for the following reason: *if* she did eat the cookie, then she would have known who ate the cookie: namely herself.

Thus the only person left is Bill. Since either Alice, Claire or Bill could have eaten the cookie, and we know that neither Alice nor Claire did it, we conclude that Bill must have eaten the cookie.

Example 4.2. *Simplifying Taxes*

At the grocery, one finds that the total base price for thier items is multiplied by some scaling constant t. As of writing this document, in Toronto, Canada, $t = 1.13$. Suppose that our grocery list is:

Item	Price
Bag of Apples	1.75
French Baguette	1.25
Bag of Coffee Grounds	7.00

So, our base price is $b = 1.75 + 1.25 + 7.00 = 10.00$ dollars. Thus, our final price is $t \times b = 1.13(10.00)$ dollars.

What we really want to know is how much more we are going to pay after taxes, so we focus on the 13% corresponding to the decimal 0.13. Mentally computing 13% of 10.00 is not the easiest task. An easier task is computing 10% of 13.0 since it involves just moving the decimal place 1 place left. The numbers that we calculate are the same since by associatvity:

$$t \times b = 0.13 \times 10 = \frac{13}{100} \times 10 = 0.1 \times 13.$$

Next, suppose that we forget to buy items on our shipping list, so we buy each item seprately on multiple trips. So the tax is applied to each item:

$$(1.13 \times 1.75) + (1.13 \times 1.25) + (1.13 \times 7.00)$$

We are concerned with whether buying these items seperately actually costs us more than buying them all at once. But we know that by factoring out the common coefficient 1.13:

$$(1.13 \times 1.75) + (1.13 \times 1.25) + (1.13 \times 7.00) = 1.13(1.75 + 1.25 + 7.00)$$

So buying each item individually wastes us no more money than buying the entire list at once (time, however, is another story).

When we formalize our straightforward reasoning, we must also formalize our reasoning's structure. The proof structure, in order, is:

1. The statement to be proved (the claim),
2. Relevant definitions,
3. Logical deductions that follow from the definitions, and
4. The final conclusions.

So, applying this structure to the first example in this chapter, we have:

1. Bill is the one who ate the cookie,
2. (1) Everyone in this scenario speaks with sincerity, and (2) Either one of Alice, Bill or Claire could have eaten the cookie.
3. The deductions that lead us to show that neither Alice nor Claire ate the cookie.
4. Because of (2), Bill must have eaten the cookie.

In general, the structure will be assumed implicit so we won't enumerate the deductive structure in our proofs.

We start off by proving some naturally understood properties of the real numbers.

4.1 Proofs with Algebra

The tools of algebra give extreme expressive power in our proof structure.

Example 4.3. *Mutually Inclusive Definitions*

The definition of odd and even functions might lead you to believe that odd and even functions are mutually exclusive. We show that due to one special function, this is not the case.

Claim 4. *The function $z(x) = 0$ is the only function that is both an even function and an odd function.*

Proof. Let f be some function that has the property that it is both even and odd. Then, for all $x \in \text{Dom}(f)$, f must also satisfy the following:

$$\begin{aligned} 2f(x) &= f(x) + f(x) && && (4.1)\\ &= f(x) + f(-x) && f \text{ is even} && (4.2)\\ &= f(x) + (-f(x)) && f \text{ is odd} && (4.3)\\ &= f(x) - f(x) && && (4.4)\\ &= 0 && && (4.5) \end{aligned}$$

By the transitive property of equality, we have that expressions (4.1) and (4.5) are equal. Thus $2f(x) = 0$, meaning that $f(x) = 0 = z(x)$ by dividing by 2 on both sides.

We conclude that if f is both even and odd, then it is necessarily equal to z, the additive function identity. □

Note a technicality: z must have the property that if $x \in \text{Dom}(z)$, then $-x \in \text{Dom}(z)$. For example, the function $z'(x) = 0$ defined on $x \in [1, 2]$ is neither even nor odd, while $z''(x) = 0$ defined on $x \in [-2, -1] \cup [1, 2]$ is.

The example above illustrates the power of a proof: out of the infinite possibilities and combinations of functions, we assert that only one function fits the criteria.

Example 4.4. *The sum of two odd numbers is even*

Theorem 2. *Let a and b be odd numbers. Then $a + b$ is an even number.*

Proof. We may express a and b as:

$$\begin{aligned} a &= 2n + 1, && \text{and}\\ b &= 2m + 1; && \text{for } n, m \in \mathbb{Z} \end{aligned}$$

This comes from the definitions of odd numbers. As a verifying example, $a = -7, b = 3$ if $n = -4$ and $m = 1$. Adding a and b, we immediately get the desired result:

$$\begin{aligned} a + b &= (2n + 1) + (2m + 1) && \text{by definition of } a \text{ and } b\\ &= (2n + 2m) + (1 + 1) && \text{commutativity of } \mathbb{Z}\\ &= 2(n + m + 1) && \text{simplifying} \end{aligned}$$

Since the sum of an integer and another integer will always be an integer, we conclude that $a + b$, by definition, is an even number, as wanted.

□

In this case, we used the known definitions of odd numbers and properties of simple algebra to achieve our desired result.

Aside from finding nice properties of various objects, proofs allow us to develop algebraic tools:

Theorem 3. *Let $a, b \in \mathbb{R}$ such that $a = b$. Then, for all $c \in \mathbb{R}$, $a + c = b + c$.*

Proof. We deduce:

$$\begin{aligned} a + c &= a + 0 + c && && (4.6)\\ &= a + (b - a) + c, && \text{since } b = a && (4.7)\\ &= (a - a) + b + c, && \text{commutativity of } + && (4.8)\\ &= b + c && && (4.9) \end{aligned}$$

So, by the transitivity of equality, we have $a + c = b + c$, as wanted. □

Theorem 4. *Let $a, b \in \mathbb{R}$ such that $a = b$. Then for all $c \in \mathbb{R}$, $ca = cb$.*

Proof.

$$\begin{aligned} ca &= ca \cdot (1) && && (4.10)\\ &= ca \cdot (b/a) && \text{because } b = a \text{ means } b = 1 \cdot a && (4.11)\\ &= cb \cdot (a/a) && \text{commutativity of } \cdot && (4.12)\\ &= cb && && (4.13) \end{aligned}$$

Thus, $ca = cb$, as wanted. □

Before we start the next section, it might be worthwhile to note in passing that, unless the proof is trivial, proofs require us to observe and describe a phenomenon in more than one way; to glean an additional perspective. And when we combine our knowledge, we lead ourselves to new truths. This is especially true when we prove Pythagoras' Theorem next.

4.2 Proofs with Geometry

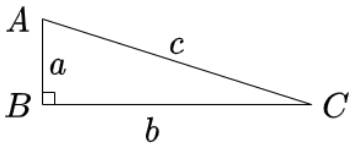
Theorem 5. *$\times$ distributes over $+$. That is, for $a, b, c \in \mathbb{R}$, $a(b+c) = ab+bc = (b + c)a$.*

Corollary 4.1. *Let $a, b, c, d \in \mathbb{R}$. Then $(a + b)(c + d) = ac + ad + bc + bd$.*

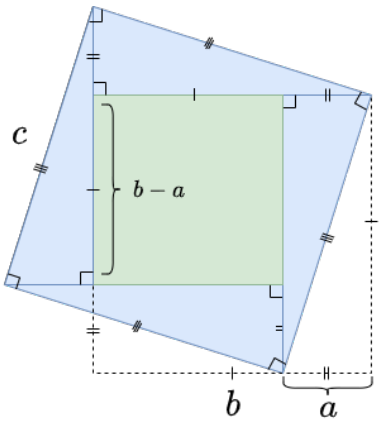
Proof. See questions. □

Theorem 6. *(Pythagoras' Theorem) Given any right-angled triangle $\triangle ABC$ where AC is the hypotenuse, we have:*

$$|AB|^2 + |BC|^2 = |AC|^2.$$



(a) An arbitrary right angle $\triangle ABC$ with side lengths $|AB| = a, |BC| = b, |AC| = c$.



(b) Square A_{WXYZ} constructed from $\triangle ABC$.

Figure 4.1: Crucial Shapes of the Pythagorean Theorem proof.

Proof. Let $\triangle ABC$ be an arbitrary right-angled triangle, and let $a \equiv |AB|$, $b \equiv |BC|$ and $c \equiv |AC|$ We construct the square $\square WXYZ$ by connecting four similar triangles base side to hight side as in Figure 4.1.

The area of $WXYZ$, A_{WXYZ}, is equal to c^2 because $|WX| = |AC|$. However, we can compute its A_{WXYZ} a different way. By our construction, we find that A_{WXYZ} is equal to the four triangle areas plus the smaller square in the middle. The side of the square is equal to $|BC| - |AC| = b - a$. So, at last we get:

$$\begin{aligned} A_{WXYZ} &= 4(ba/2) + (b-a)^2 && \text{from above} && (4.14)\\ &= 2ba + (b^2 - 2ba + a^2) && \text{by Corollary 4.1} && (4.15)\\ &= b^2 + a^2 && && (4.16) \end{aligned}$$

So, $c^2 = A_{WXYZ} = b^2 + a^2$ and so our result follows by transitivity. □

With this powerful tool in hand, we prove the more general case:

Theorem 7 (Cosine Law)**.** *Given any triangle $\triangle ABC$, denote the longest side as AC and denote the angle that the line segment AB makes with BC. Then*

$$|AC|^2 = |AB|^2 + |BC|^2 - |AB||BC|\cos(\theta).$$

And so the cosine law leads us to this result.

Corollary 4.2. *Let $a, b, c \in \mathbb{R}$ be lengths such that $a \leq b \leq c$. Then, a triangle can be formed with lenghts a, b, c iff $a - b < c < a + b$.*

Proof. [$\dot{\Longrightarrow}$] Suppose that $\triangle ABC$ is a triangle, where AC is the longest side with length c. Then, $\triangle ABC$ satisfies the cosine law. Since $-1 \leq cos(\theta) \leq 1$,

we get:

$$c^2 = a^2 + b^2 - 2ab\cos(\theta) \tag{4.17}$$
$$> a^2 + b^2 - 2ab, \qquad \text{When } \theta = 0 \tag{4.18}$$
$$= (a-b)^2, \qquad \text{By Corollary 4.1} \tag{4.19}$$

and

$$c^2 < a^2 + b^2 + 2ab, \qquad \text{When } \theta = \pi \tag{4.20}$$
$$= (a+b)^2. \tag{4.21}$$

Taking square roots of the inequalities, we achieve our desired result.

[$\Longleftarrow$] Suppose that $a, b, c; a < b < c$ are positive lengths such that $|b-a| < c < a+b$. We wish to prove that we can make a triangle out of these lengths.

From the proof of the opposide direction, it is easy to see that $c^2 = a^2 + b^2 - 2ab\cos(\theta)$ for some $\theta \in (0, \pi)$. Construct a triangle $\triangle ABC$ such that AB is parallel on the x-axis with length a, and BC extends from AB's left-most point, turning π radians counter-clockwise as in Figure

Using Pythagoras' Theorem, we calculate $|AC|^2$:

$$|AC|^2 \tag{4.22}$$
$$= (a + b\sin(\theta - \pi/2))^2 - (b\cos(\theta - \pi/2))^2 \tag{4.23}$$
$$= a^2 - 2ab\cos(\theta) + b^2\cos^2(\theta) + b^2\sin^2(\theta) \qquad \text{Translating sin, cos right} \tag{4.24}$$
$$= a^2 - 2ab\cos(\theta) + b^2(\sin^2(\theta) + \cos^2(\theta)) \tag{4.25}$$
$$= a^2 + b^2 - 2ab\cos(\theta) \tag{4.26}$$
$$= c^2 \tag{4.27}$$

So $|AC| = c$, as wanted. □

Chapter 5

Indirect Proofs

An indirect proof method is a method in which the proof does not explicitly prove the desired predicate [1]. An indirect proof resorts to proving another statement, for whose validity it immediately follows (or in other words, implies) the desired predicate's validity. We provide a classic example. [2]

Example 5.1. *Prove that there are infinitely many prime numbers.*

Proof. Let p be a prime number. Then p satisfies the following conditions:

1. $p \in \mathbb{N}$
2. $p \geq 2$, and
3. The only factors of p are 1 and p, that is, no number other than 1 and p divides p evenly.

Suppose to the contrary that there exists a finite number n of prime numbers. Then,we may, theoretically, gather the entire collection of these primes. Let us exhaustively describe this collection as $F = \{p_1, p_2, ..., p_n\}$ [3].
Let the number p' be the *product of all of the primes in* F. We must have:

$$p' = p_1 \cdot p_2 \cdot ... \cdot p_n$$

We see that p' is definitely divisible by all of the primes in existence in F (by supposition).
Consider the number $p'' = p' + 1$. Notice that this number is not divisible by any of the primes in existence - to see this, notice that by dividing p'' by any $p \in F$, we always will get a remainder of 1[4].

[1] A *predicate* is a formal statement in mathematics that can either be seen as a true statement or a false statement. Predicates are what this note might informally refer to as 'statements'

[2] This is known as Euclid's Argument of infinite primes.

[3] This is known as a set, and the way we have described it is called an *exhaustive* description of a set.

[4] Rigorously, we would consult a mathematical construct known as the *division algorithm* - however, I believe the preceding argument intuitively suffices.

It becomes clear that the only factors of p'' are 1, and p'' itself. We have effectively generated a *new* prime number that was not in F, our supposed 'complete' set of all prime numbers. We have reached a contradiction, and we could not have possibly constructed a finite collection of prime numbers in the first place. The desired result follows. □

The 'indirect' portion of this proof is in the supposition statement. We suppose that the statement we are trying to prove is false, and by flawless logical reduction from this negation, we reach a contradiction. We then argue that the only flaw in our logic was the supposition itself, therefore, the actual desired conclusion must be true. Thus, by resorting to proving another related statement, the desired statement is proven[5]. (This specific indirect proof technique is known as a *Proof by Contradiction.*)

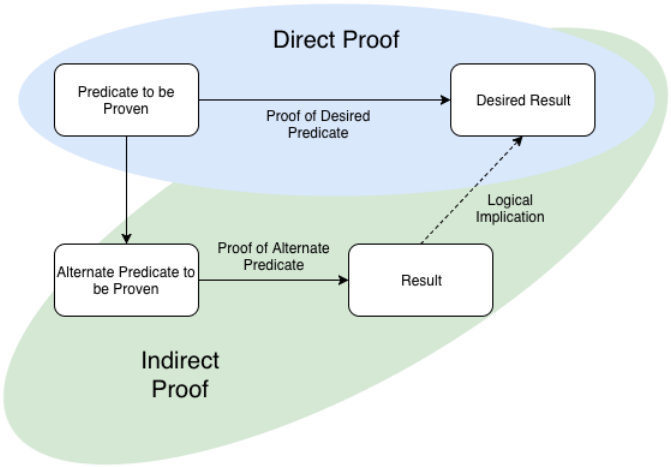


Figure 5.1: The algorithmic difference between the two types of proof structure.

[5]Notice that the 'equivalent' statement that we have proven can be stated as: "It is not the case that the set of prime numbers is finite".

Chapter 6

Mathematical Induction

The proof technique of Mathematical Induction is powerful and widely used tool

6.1 "Induction"

In daily life, we are exposed to events that strenghthen our conviction of a statement. For example, imagine that, whenever you pay attention to it, the morning bus that goes to the subway always arrives at 10:15 AM at the stop in front of your house. Of course, you would have more conviction toward the statement "The bus always arrives at 10:15 AM at the stop in front of my house" after the 500th time the bus arrives on time as opposed to the 2nd time. This process is induction in action.

Induction, roughly speaking, refers to the process by which our confidence in a statement is supported by the number of verifying examples of that statement. Our confidence increases with the number of examples that support our hypothesis.

The following point is critical. Unless we are able to verify our hypothesis for all (potentially infintite) instances, then we will never achieve complete certainty of our statements. How could we be sure that tomorrow, next week, or next year, our bus will be late?

6.2 Mathematical Induction

In a similar vein to the above, consider the statement: for every $n \in \mathbb{N}, n \geq 4, n^2 < 2^n$. We know that this is true, and one could go about calculating the values for both n^2 and 2^n, for $n = 1$ and then comparing those values to verify the predicate, repeating the process for $n = 2$, then $n = 3, \ldots$ However, the analogous problem presents itself here: what if there was some number $M \in \mathbb{N}$ that is beyond the scope of conceivable human (and computer) discovery[1]? How do we verify the predicate for such an uncomputably large number? And even numbers of that magnitude larger?

[1] For example, Graham's Number

6.3 Proofs by Induction

The structure of a

Chapter 7

Appendix

7.1 Part A

Chapter 8

Questions

1. Let $n \in \mathbb{N}, n > 2$ and $n|2 = 0$ (that is, there is no remainder when dividing n by 2). Prove that n is not prime.
2. Prove directly that the sum of an even integer and another even integer (not necessarily the same integer) is even.

   — What can you conclude about the sum of an odd integer and an even integer? Can you directly prove it?
3. (**Challenge**) Prove that any odd number is equal to a difference of squares[1].

   — Hint: This difference of squares is not unique.

   — Hint: This proof is facilitated by *constructing* the difference of squares.
4. (*Binomial Expansion Theorem of degree* 2) Prove geometrically that $(a + b)^2 = a^2 + 2ab + b^2$.
5. Let $a, b, c, d \in \mathbb{R}$; where $b, c, d \neq 0$. Prove that $\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c}$. (You may assume that $\frac{a}{b} \cdot \frac{b}{a} = 1$, under the appropriate conditions.)
6. Prove $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$, by induction.
7. Prove $\sum_{i=1}^{n} i^3 = (\sum_{i=1}^{n} i)^2$.
8. (**Challenge**) Prove, by induction that the degree-sum of the internal angles of n-sided polygon is equal to $(n - 2) * 180$:
   - (*Base Case*): What is the simplest shape for which this fact can be verified?
   - (*Induction Hypothesis*): What may we use for our index value?
   - (*Induction Step*): Construct an arbitrary shape S, that has k sides.

     — Argue there are 2 ways of creating a new side from an arbitrary side s_i in S. Name this new shape S'.

     — For each of the cases detailed above, verify that S' satisfies the relevant angle equation, keeping in mind the number of sides in S'.

[1] A difference of squares is of the form $(a^2 - b^2)$, where $a, b \in \mathbb{Z}$

9. (**Challenge**) Using geometric arguments, directly prove the *Pythagorean Theorem* for a right-angle triangle ΔABC, where $|AB| = |BC|$ (that is, where the base and height of ΔABC are equal.)

10. (**Challenge**)

    (a) Consider the *last digit* of $2^2, 2^6,$ and 2^{10}. Do you see a pattern?

    (b) Is this pattern true *for all* $2^n, n \in \mathbb{N}$? If not, then what should n be?

    (c) Prove this pattern for all numbers 2^n, for whatever n must be in 10b).