

The Art of Mathematical Proof

Will Dengler

March 4, 2019

1 Introduction

What is a math proof? That is, after all, why you are reading this article - to answer this innocent looking question. Well I'm not going to answer that, at least not right away. Instead, I want you to think about the following statements:

- The sum of two even integers is even.
- The sum of two odd integers is even.
- The sum of an even and an odd integer is odd.

You know these statements to be true, but how do you know they are true, *why* are they true? Maybe you quickly added some examples in your head, each example affirming your belief in these statements. That may be good enough to have satiated any doubt you had; after all, patterns often arise in numbers - no doubt something you noticed in your math courses growing up. However, this form of confirmation doesn't answer the more important question - *why* are these statements true? All of mathematical theory is focused around answering the question of *why*: *why* is this statement true; *why* is this impossible; *why* must this object exist; *why* will this process always yield a correct result... you get the point. In order to answer every *why* we encounter, mathematics employs the mathematical proof. Quite simply, a mathematical proof is the 'proof' that something must be, or can't be possibly be true.

We are all familiar with the stereotypical child whom is constantly asking *why*: *why* do I have to go to school; *why* is it important to get a job; *why* do we need money; etc. Mathematicians share many things in common with this stereotype. They are constantly questioning why, and if the given explanation is not to their satisfaction, they will then question why the very

explanation must be true, and continue on doing so until you've eliminated all doubt in their minds. However, unlike our imaginary child, it is possible to eliminate a mathematician's doubt. But in order for us to do so, we must present our mathematician with a logical argument that demonstrates the validity of our statement without leaving any possibility unaddressed. This logical argument is what mathematics refers to as a proof.

Now that you have an idea of what a math proof is, you're probably wondering what one looks like. A proof starts with the facts at hand "I have two even integers, therefore I can represent the first number as $2 * j$ and the second as $2 * k$, where j and k are integers because even numbers are defined to be 2 times some integer.", then deduces what must be true given those facts, "Therefore, I can represent their sum as $(2 * j + 2 * k)$ ". With the new information, more facts can then be uncovered "We can then factor out the 2 from this representation: $(2 * j + 2 * k) = 2 * (j + k)$. The number $(j + k)$ must be an integer because the sum of two integers is an integer." This process continues on until the truth of the statement is uncovered, "I've shown that the sum of the two even numbers is equal to 2 times the integer $(j + k)$, which means that this number is even by definition."

Don't worry if you don't see why the argument above does in fact prove that the sum of two integers is even, we'll come back to it soon. Instead, focus on the nature of the argument. Notice that there's no references to a specific example; that each step in the argument was coupled with a justification; that evenness was given an explicit definition - these are the hallmarks of a proof.

Okay, that's great, Will, can you now tell me exactly what a proof is, and how I can go about writing one? Well I can't... there's no easy way to define what a proof is, nor a simple set of rules I can give for writing one - it'd be like defining the color red, sure I could tell you its wavelength, but that doesn't come close to explaining it. What I can do however is teach you how to recognize what is a proof and what's not, as well as the tools to begin to start proving things on your own.

2 The Fundamentals of Theory

In mathematics, definitions are the building blocks of all theory. A definition unambiguously and efficiently describes an 'object'. From the definition springs all math theory - first, the properties that are inherent to the definition of the object are proved. From there, more complex facts are uncovered, and then more, and more, and more (you get where I'm going). Each new fact uses the previous facts and definitions to show that it too must also be

true. This process of building up facts endows mathematics with enormous accountability. By the very nature of our exploration, we can always be confident that the facts we discover are in fact true, no matter how far-fetched or complicated they appear.

Let's start with one of the most simple definitions - the set of integers. We'll define the set of integers \mathbb{Z} to be the counting numbers $1, 2, 3, \dots$ along with 0 , and the negative numbers $-1, -2, -3, \dots$. We can represent the integers in set notation:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

and we'll define an integer to be any number within the set of integers.

The attentive reader may have noticed that in the introduction proof, I justified that the sum of j and k was an integer because both j and k are integers. We'll accept this statement as fact without proving it to be true. Although simply accepting something to be true seems perilous and illogical, there are times when we cannot escape having to do so. When we accept a statement as fact without proving it, we call it an axiom. An axiom does not need to be proven; instead, the truth of an axiom is self-evident (think of an axiom like existence - you know you exist, but it's very difficult to quantify a justification for that belief). As such, we never arbitrarily perscribe something axiomatic; rather, we only do so when it is necessary and appropriate.

From our axioms and definitions we then derive lemmas and theorems. A lemma is simply a statement that has been proven to be true, such as: "The sum of two even integers is even." Theorems are no different than lemmas in their design; however, they're generally attributed to more important or complex statements. You can think of lemmas as the building blocks to theorems - it is often the case a lemma is proven for the express purpose of being used within the proof of a theorem.

That's all there is to math theory. We start with some self evident truths - our axioms. We then define an 'object' or two and explore all the truths held within it, spitting out lemmas and theorems along the way.

3 Evenness - What is it?

Before we can take a closer look at the proof from the introduction, we'll need to start with definition of what it means to be even:

Definition

An integer, n , is even if $n = 2 * j$ for some integer j .

Let's take the time to examine this definition in some detail. There are several things of note contained in the simple sentence above. First, we see that this definition is defining a specific type of integer, specifically, an even integer. How does it do this? Our definition states a property that an arbitrary integer n must have for it to be even; in particular, that there must exist another integer j such that $n = 2 * j$. What exactly does this mean? In a simplified perspective, you can think of the definition as a test of evenness that could be applied to any specific integer. Is 6 even? Of course it is. Why? Because we can write $6 = 2 * 3$. Whenever we look at a specific example, we simply replace the symbols in our definition with the specifics. In this last example, we substituted 6 for n , and then were able to see that j must be 3. While it is possible to think of a definition like a test, it is so much more than that. A definition describes the essence of a mathematical object. It is efficient in the sense that it gives no more detail than necessary. We could have stated in our definition that an even number also has the property that the sum of two even numbers is also even. While this is true, it is excessive to our understanding of evenness. It is merely consequential to an integer's evenness rather than fundamental to it. A property is consequential if it can be proved using the definition, but itself does not imply the definition. Fundamental properties are a bit more complicated, but we'll address them later on.

If you're wondering if there's anything special about the letters n and j used within the definition - there's not. We must often speak abstractly in mathematics, and when doing so it helps to ascribe symbols to the objects which we are referring. The symbols we choose are arbitrary. For example, our definition of evenness could have easily been stated using the letters m and z , or greek characters α and ω , or even the words *flamigo* and *shrimp*. It is also important to note that we don't have to refer to every even integer as n just because that was the symbol used within the definition. In fact, in most cases it would be impossible to do so. For instance, if I want to reference both 4 and 6 symbolically, then I couldn't possibly call them both n ; otherwise $4 = n = 6$ and that's just nonsense! Instead, we can just decide on some new symbols on the spot such as $\alpha = 4$ and $x = 6$. As long as we tell our audience what a new symbol refers to when we introduce it, we can confidently use it in place of its original reference.

4 The Sum of Two Even Integers is Even

Now that we have our definition of evenness, we can begin to tackle this proof. But to begin handling this proof, we first need to determine what exactly it means to show that the sum of two integers is indeed even. Not only that, our argument has to be structured in a way such that regardless of the two even integers chosen, we clearly demonstrate that their sum is even. Now if you're wondering how you could possibly show that it's true for every pair of even integers, or why the proof in the introduction does fulfill this requirement, don't worry - you are not alone! The solution to our problem is actually quite simple, all we have to do is look back to what an even integer is defined to be. If you're wondering how such an abstract definition can help us, again, don't worry, I'm about to explain. Our problem is that we need to show for any two even integers, their sum is even. Well to do that, we need two even integers (obviously!), but we don't want to pick two specific integers. Instead, we need a description of two even integers that could apply to any specific pair. Here we go...

→ Assume I have two even integers n and m .

Will, really? Yes, really! We need a description that fits any two even integers, and that description certainly does so. If you're wondering how this statement could possibly be helpful just look back to your definition of an even integer, and you'll find that the statement above contains a bit more information than it lets on at first:

→ Since n is even, there exists some integer j such that $n = 2 * j$.

→ Similarly, since m is also even, there exists some integer k such that $m = 2 * k$.

The specific values of j and k aren't relevant, all that's important is that they exist, and that we can represent our even integers n and m using them. Let's circle back now to the real problem, how do we show that the sum of n and m is even as well. To do this, let's give the sum a name - let's call it s . More formally:

→ let $s = n + m$.

Once again, we do not care about the specific value of s , we only care that it is the sum of n and m . Now that we have s , we must ask ourselves a very

important question - what does it mean to show that s is even. Once again, I refer you to the definition of what it means to be even - s is even if there exists some integer p such that $s = 2 * p$. Let's take a recap of all the things we know:

→ We have two even integers $n = 2 * j$ and $m = 2 * k$, for some integers j and k .

→ We defined the sum of n and m as the integer $s = n + m$.

So what next? Well, let's try substituting $2 * j$ for n and $2 * k$ for m in our representation of s :

→ $s = n + m = 2 * j + m = 2 * j + 2 * k$.

Why can we do this? Since n is equal to $2 * j$ we can use them interchangeably - they refer to the same exact value. You can think of $2 * j$ as a nickname for n - while they may look different, they actually refer to the same thing. Now we all should know what's coming next (after all, I told you only a few paragraphs ago), we are going to factor out the 2:

→ $s = 2 * j + 2 * k = 2 * (j + k)$.

It was no accident that I choose the sum of two integers is an integer as our example axiom; I needed it for what comes next:

→ Since both j and k are integers, their sum $(j + k) = p$ is also an integer.

What's the value of p ? Once again, it's not important, all we need to know is that p is an integer. Finally, we can put it all together by substituting p for $j + k$:

→ $s = 2 * (j + k) = 2 * p$.

→ Therefore, since p is an integer, and s is equal to $2 * p$, s is even by definition.

→ Furthermore, s is not only even, it's also the sum of n and m - which were represented in such a way that our argument could apply to any pair of even integers!

And that's all there is to it - we've now proven our statement that the

sum of two even integers is even. If you're still a little unsure why the above proves our statement, don't worry - they'll be a few more proofs before the end of this article. If you are uneasy, try re-reading the proof and writing out each step along the way. As you write down each step, ask yourself: why does this argument apply to any integer(s); why am I able to deduce this information from the previous step(s); why is this particular statement true; and what am I accomplishing with this step? You may even try thinking about the proof as if it were a court case, "The sum of two even integers has been accused of being even itself, and we have gathered here today to hear arguments assessing the validity of this accusation". You may also find it helpful to read the following condensed version of the proof:

Lemma

The sum of two even integers is also even.

Proof

Assume I have two even integers n and m .

Since n is even, there exists some integer j such that $n = 2 * j$.

Similarly, since m is also even, there exists some integer k such that $m = 2 * k$.

let $s = n + m$.

Then, $s = n + m = 2 * j + m = 2 * j + 2 * k$.

Then, $s = 2 * j + 2 * k = 2 * (j + k)$.

Since both j and k are integers, their sum $(j + k) = p$ is also an integer.

Thus, we can represent s as $s = 2 * (j + k) = 2 * p$.

Since p is an integer, and s is equal to $2 * p$, s is even by definition.

Furthermore, s is not only even, it's also the sum of n and m .

Thus we have completed our proof.

Q.E.D

5 The Oddities of Oddness

Definition

An integer, n is odd if $n = 2 * j + 1$ for some integer j .

Look familiar? It shouldn't come as much surprise that the definition of oddness is incredibly similar to that of evenness; after all, there seems to be a natural duality between the two concepts. Now, let's take a deeper look at

this definition. First, let's confirm that it makes sense with a few examples: $3 = 2 * 1 + 1$, $5 = 2 * 2 + 1$, $-39 = 2 * -20 + 1$. Great, everything seems to check out. Now let's dig a little deeper. What if I were instead define an odd integer as follows:

Definition

An integer, n , is odd if $n = 2 * j + 3$ for some integer j .

Despite this definition looking different from our original, it isn't actually any less correct. Again, let's look at our examples: $3 = 0 * 1 + 3$, $5 = 1 * 2 + 3$, $-39 = 2 * -20 + 3$. Everything seems to work out fine once again. But how can this be; could we be overlooking something? We are not, and in order to make certain of this, we are going to prove that the two definitions actually define the same thing. In particular, we are going to prove that any integer written with our first definition can be written in the form of our second definition, and vice versa.

Lemma

For any integer, n , there exists an integer, j , such that $n = 2 * j + 1$ if and only if there also exists an integer, k , such that $n = 2 * k + 3$.

Proof

Assume I have an odd integer, n , defined by our first definition.

Therefore, there exists an integer j such that $n = 2 * j + 1$.

Now, we must show that there exists some integer, k , such that $n = 2 * k + 3$. By doing this, we will have shown that for any integer defined using our first definition, it also fits the description of our second definition.

Since j is an integer, I can subtract 1 from it, let's call this difference k . Formally, let $k = j - 1$.

Now we will use basic algebraic manipulation to 'coax' the second definition from our first.

$$n = 2 * j + 1 = 2 * (j + 0) + 1 = 2 * (j + (-1 + 1)) + 1$$

The above may seem strange or unhelpful, but it is in fact the key to our proof. By expanding out multiplication by 2 to include $-1 + 1 = 0$, we haven't changed the meaning of our equation thanks to the laws of algebra. However, we have converted our equation to a more useful form as will be

revealed in the next step:

$$n = 2 * (j - 1) + 2 * 1 + 1 = 2 * (j - 1) + 3.$$

Now we've got the 3 we need for our second definition. What's more, we can substitute k for $j - 1$ since that's what we defined k to be only a few lines earlier:

$$\text{Then, } n = 2 * (j - 1) + 3 = 2 * k + 3.$$

Therefore, n is also odd in accordance with our second definition!

What exactly does this mean? We've now proved that if we start with our first definition, then we meet the criteria of our second definition. Does this mean we have shown that the two definitions are actually the same? Not quite, we still need to show that if we start with the second definition then we will meet the criteria for the first one. Why do we need to do this? To explain that, I'm going to talk about chocolate ice cream. If I am eating chocolate ice cream, then I am happy. However, that doesn't mean chocolate ice cream is happiness. Chocolate ice cream does not define happiness, it merely implies happiness. Why's that? Because you cannot make the argument that if I am happy, then I must be eating chocolate ice cream. After all, other things make me happy as well! For instance, my happiness may be the result of petting a puppy. However, if it was always the case that I was only happy if I were eating chocolate ice cream, then one could logically argue that happiness and chocolate ice cream are the same thing to me. This same principle can be applied to explain why we must prove that if we start with the second definition of oddness, then the first definition holds. Without any further delay, let us now prove this statement as well.

Assume I have an odd integer, m , defined by our second definition.

Therefore, there exists an integer p such that $m = 2 * p + 3$.

Similar to the first part of the proof, we must this time show that there exists some integer, q , such that $m = 2 * q + 1$. Once again, we will use some clever algebra to show this to be the case.

$$m = 2 * p + 3 = 2 * (p + 1 - 1) + 3 = 2 * (p + 1) - 2 + 1 + 3 = 2 * (p - 1) + 1.$$

Hopefully you know what comes next:

$$\text{Let } q = p - 1.$$

Then, $n = 2 * q + 1$.

Thus, n is odd in accordance with our first definition!

Q.E.D

Now we've completed our proof, and by doing so, removed all doubt as to whether our two different definitions were actually defining the same thing. In fact, we could have chosen any odd integer to add to our $2 * j$ term, and have accurately defined oddness (try proving it's the same if we had chosen 7 instead). When a property of an object could be used to define that object, then that property is fundamental to the object. It is important to remember that a fundamental property does not need to be used to define an object; however, we do have the option to do so. As such, we will use our original definition of oddness throughout the remainder of this article.

6 Split Personality

Now that we have definitions for both even and odd integers, we are going to prove that an integer cannot be both even and odd. Yes, we all 'know' that this statement is true, but our stubborn mathematicians seem to doubt anything we say without any proof (they're not always the easiest group to get along with). Unfortunately, they do have a point. If someone were to (incorrectly) state that a number could be both even and odd; we would be unable to refute their claims! As such, unless we prove this obvious statement, it would be improper for us to claim its truth.

Before we dive into our proof, let's first think about what we need to show in order to prove that an integer can't be both even and odd. To accomplish our goal, we are going to use a technique often termed *contradiction*. In a contradictory proof, we endow an object with two or more conflicting properties. In the problem at hand, our object will be an integer, and the conflicting properties will be even and oddness. We then 'innocently' explore all the truths that lead from our object endowed with conflicting properties. However, our exploration won't actually be so innocent. We know that we are exploring the land of the impossible, a place outside of logic. As we stumble about this false reality we've created, we will surely encounter many strange things, things that defy logic. It is our task to choose one of these strange encounters to explore in detail. Why? Because we are searching for proof that the very thing in front of us can't possibly exist. We may know we've stepped outside of the realm of possibility; unfortunately, our friends back at home aren't going to believe us without proof. So what exactly does proof you've stumbled into the realm of impossibility look like? It looks like

an equation that when solved reveals that an integer is equal to two different values at the same time; or a set that is somehow both empty and nonempty; or an integer that is both less than and greater than some other integer. These are but a tiny few of all the absurdities we might run into, but they perfectly illustrate the type of information we are seeking. Each statement is something that we know can't be true; each statement is a *contradiction*. Once we've found our contradiction we can start to pull at the very fabric with which we've woven the impossible. How do we do this? We simply start working backwards from the contradiction until we've stepped back into reality. Once we've made it back to reality, we've identified the culprit of our journey - it's the statement the sent us into the realm of impossibility in the first place! With the knowledge of the culprit statement, and proof that it leads to a contradiction, we can now confidently assert that culprit statement must actually be false, for we now know that it can't possibly be true.

This is exactly how we are going to prove that an integer can't be both even and odd at the same time. We'll start with some integer; then we'll assume it's both even and odd. We'll stumble along until we find a *contradiction*. Then we'll trace that contradiction's origins back to our assumption that our integer was both even and odd. At that point, we will have shown that it's impossible for the integer to be both even and odd! Why? Because if it is both even and odd, then reality is falling apart in front of us! Without further ado, let us now prove this statement:

Lemma

An integer cannot be both even and odd.

Proof

Let n be any integer.

Assume n is both even and odd.

Now that we've made our assumption that will fling us out of reality, it's time to start exploring:

Then, there exists some integer j such that $n = 2 * j$ because n is even.

Similarly, there exists some integer k such that $n = 2 * k + 1$ because n is also odd.

Let's take a closer look at the *integer* j ...

Since $n = 2 * j$, we can apply divide both sides of this equation by 2 in

order to solve for j , which gives us, $j = \frac{n}{2}$.

If you were wondering why we need to explore the realm of impossibility in order to find a contradiction, the answer should now be clear - our false reality appears to be real at first! So let's continue exploring, hopefully we don't have to go much further... Why don't we see what happens when we substitute $2 * k + 1$ for n in our equation for j ...

Substituting gives us, $j = \frac{n}{2} = \frac{2*k+1}{2} = \frac{2*k}{2} + \frac{1}{2} = k + \frac{1}{2}$.

Subtracting k from both sides of this equation yields, $j - k = \frac{1}{2}$. But j and k are both integers, so their difference, $d = j - k$, is also an integer (you should prove this for yourself).

Substituting once again gives us, $d = \frac{1}{2}$.

Wait a minute, d is an integer, and $\frac{1}{2}$ is not contained within the set of integers - this can't possibly be; this must be the contradiction we've been looking for!

Now it's time to work backwards from our contradiction...

How did we know d was an integer? We used the fact that difference of two integers is also an integer; however, since you proved this for yourself (right?), then we can all agree that this statement comes from reality, so it could not be what led us to our contradiction.

Let's keep moving further back...

How did we come to $d = \frac{1}{2}$? Well we were able to do so using simple algebra, and simple algebra also comes from reality, so that too is not the culprit. What came before our algebra? We substituted $2 * k + 1$ for n in our representation of j . Substitution also comes from reality, so the act of it is not the culprit. However, the *reason* we could perform this substitution was! Why were we able to substitute $2 * k + 1$ for n in our representation of j ? Because we had defined n to be odd; and where did we get our equation for j ? From the fact that n is also even! If we had only assumed n was one of even or odd, we would have never been able to perform our substitution; therefore, we'd never have been able to show that $\frac{1}{2}$ had somehow managed to sneak its way into the set of integers!

Thus, we can conclude that it was incorrect of us to have assumed our integer n both even and odd; and since we chose n to be any integer, we now can confidently state that it's incorrect to assume any integer can be both even and odd!

Q.E.D

7 Tying Up Loose Ends

Now that we've got definitions for even and oddness, and we are confident that an integer can't both be even and odd, we can finally prove the other two statements from the introduction.

Lemma

The sum of two odd integers is even.

Proof

Assume n and m are odd integers.

Then there exists integers j and k such that $n = 2 * j + 1$ and $m = 2 * k + 1$.

Let $s = n + m$.

Substituting, $s = n + m = 2 * j + 1 + 2 * k + 1 = 2 * j + 2 * k + 2$.

We can now factor out the 2, $s = 2 * (j + k + 1)$.

Let $p = j + k + 1$.

We know that p must be an integer because the sum of j and k is an integer, and 1 plus that value is also an integer.

Thus, $s = n + m = 2 * (j + k + 1) = 2 * p$, and is therefor even by definition.

Q.E.D