Quantifiers, Evens, and Odds

Joseph R. Mileti

February 21, 2017

1 Mathematical Statements and Mathematical Truth

Unfortunately, many people view mathematics only as complicated equations and elaborate computational techniques (or algorithms) that lead to the correct answers to a narrow class of problems. Although these are indeed aspects of mathematics, they do not reflect the fundamental nature of the subject. Mathematics, at its core, is about determining *truth*, at least for certain precise mathematical statements. Before we consider some examples, let's recall some notation and terminology for the standard "universes" of numbers:

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of *natural numbers*.
- $\mathbb{N}^+ = \{1, 2, 3, \dots\}$ is the set of positive natural numbers.
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ is the set of *integers*.
- $\mathbb{Q}$ is the set of *rational* numbers, i.e. those numbers that can be written as a fraction (i.e. quotient) of integers. For example, $\frac{1}{2}$, $\frac{-3}{17}$, etc. are all rational numbers. Notice that all integers are rational numbers because we can view 5 as $\frac{5}{1}$, for example.
- $\mathbb{R}$ is the set of *real* numbers, i.e. those numbers that we can express as a possibly infinite decimal. Every rational number is a real number, but π, e, $\sqrt{2}$, etc. are all real numbers that are not rational.

There are more important universes of numbers, such as the complex numbers $\mathbb{C}$, and many others that will be encountered in Abstract Algebra. However, we will focus on the above examples in our study. To denote that a given number n belongs to one of the above collections, we will use the $\in$ symbol. For example, we will write $n \in \mathbb{Z}$ as shorthand for "n is an integer". We will elaborate on how to use the symbol $\in$ more broadly when we discuss general set theory notation.

Returning to our discussion of truth, a mathematical statement is either objectively true or false, without reference to the outside world and without any additional conditions or information. For some examples, consider the following (we've highlighted some key words that we will discuss in the next few sections):

1. $35 + 81$ is equal to 116.
2. The sum of two odd integers is **always** an even integer.
3. The difference of two prime numbers is **always** an even integer.
4. **There exists** a simultaneous solution to the three equations

$$\begin{array}{rcrcrcr} 2x & & & + & 8z & = & 6 \\ 7x & - & 3y & + & 18z & = & 15 \\ -3x & + & 3y & - & 2z & = & -1 \end{array}$$

   in $\mathbb{R}^3$, i.e. **there exists** a choice of real numbers for x, y, and z making all three equations true.

5. The remainder when dividing 333^{2856} by 2857 is 1.
6. **Every** continuous function is differentiable.
7. **Every** differentiable function is continuous.
8. **There exist** positive natural numbers a, b, c with $a^3 + b^3 = c^3$.
9. The digits of π eventually form a repeating sequence.
10. The values of $0, 1, 2, \ldots, 9$ occur with equal frequency (i.e. each about $\frac{1}{10}$ of the time) in the infinite decimal expansion of π.

Which of these 10 assertions are true and which are false? In many cases, the answer is not obvious. Here are the results:

1. True. This statement can be verified by a simple calculation.
2. True. However, it's not immediately obvious how we could ever verify it. After all, there are infinitely many odd numbers, so we can't simply try them all.
3. False. To show that it is false, it suffices to give just one counterexample. Notice that 7 and 2 are prime, but $7 - 2 = 5$ and 5 is not even.
4. False. Again, it may not be obvious how to show that *no* possible choice of x, y, and z exist. We will develop systemic ways to solve such problems later.
5. True. It is possible to verify this by calculation (by using a suitably programmed computer). However, there are better ways to understand why this is true, as you will see in Elementary Number Theory or Abstract Algebra.
6. False. The function $f(x) = |x|$ is continuous everywhere but is not differentiable at 0.
7. True. See Calculus or Analysis.
8. False. This is a special case of something called Fermat's Last Theorem, and it is quite difficult to show (see Algebraic Number Theory).
9. False. This follows from the fact that π is an irrational number, i.e. not an element of $\mathbb{Q}$, but this is not easy to show.
10. We still don't know whether this is true or false! Numerical evidence (checking the first billion digits directly, for example) suggests that it may be true. Mathematicians have thought about this problem for a century, but we still do not know how to answer it definitively.

Recall that a mathematical statement must be either true or false. In contrast, an equation is typically neither true nor false when viewed in isolation, and hence is not a mathematical statement. For example, it makes no sense to ask whether $y = 2x + 3$ is true or false, because it depends on which numbers we plug in for x and y. When $x = 6$ and $y = 15$, then the statement becomes true, but when $x = 3$ and $y = 7$, the statement is false. For a more interesting example, the equation

$$(x + y)^2 = x^2 + 2xy + y^2$$

is not a mathematical statement as given, because we have not been told how to interpret the x and the y. Is the statement true when x is my cat Cayley and y is my cat Maschke? (Adding them together is scary

enough, and I don't even want to think about what it would mean to *square* them.) In order to assign a truth value, we need to provide context for where x and y can come from. To fix this, we can write

"**For all** real numbers x and y, we have $(x+y)^2 = x^2 + 2xy + y^2$",

which is now a true mathematical statement. As we will eventually see, if we replace *real numbers* with 2×2 *matrices*, the corresponding statement is false.

For a related example, it is natural to think that the statement $(x+y)^2 = x^2 + y^2$ is false, but again it is not a valid mathematical statement as written. We can instead say that the statement

"**For all** real numbers x and y, we have $(x+y)^2 = x^2 + y^2$"

is false, because $(1+1)^2 = 4$ while $1^2 + 1^2 = 2$. However, the mathematical statement

"**There exist** real numbers x and y such that $(x+y)^2 = x^2 + y^2$"

is true, because $(1+0)^2$ does equal $1^2 + 0^2$. Surprisingly, there are contexts (i.e. replacing *real numbers* with more exotic number systems) where the corresponding "for all" statement is true (see Abstract Algebra).

Here are a few other examples of statements that are *not* mathematical statements:

- $F = ma$ and $E = mc^2$: Our current theories of physics say that these equations are true in the real world whenever the symbols are interpreted properly, but mathematics on its own is a different beast. As written, these equations are neither true nor false from a mathematical perspective. For example, if $F = 4$, $m = 1$, and $a = 1$, then $F = ma$ is certainly false.
- $a^2 + b^2 = c^2$: Unfortunately, most people "remember" this as the Pythagorean Theorem. However, it is not even a mathematical statement as written. We could fix it by writing "**For all** right triangles with side lengths a, b, and c, where c is the length the hypotenuse, we have that $a^2 + b^2 = c^2$", in which case we have a true mathematical statement.
- Talking Heads is the greatest band of all time: Of course, different people can have different opinions about this. I may believe that the statement is true, but the notion of "truth" here is very different from the objective notion of truth necessary for a mathematical statement.
- Shakespeare wrote *Hamlet*: This is almost certainly true, but it's not a mathematical statement. First, it references the outside world. Also, it's at least conceivable that with new evidence, we might change our minds. For example, perhaps we'll learn that Shakespeare stole the work of somebody else.

In many subjects, a primary goal is to determine whether certain statements are true or false. However, the methods for determining truth vary between disciplines. In the natural sciences, truth is often gauged by appealing to observations and experiments, and then building a logical structure (perhaps using some mathematics) to convince others of a claim. Economics arguments are built through a combination of current and historical data, mathematical modeling, and rhetoric. In both of these examples, truth is always subject to revision based on new evidence. In contrast, mathematics has a unique way of determining the truth or falsity of a given statement: we provide an airtight, logical *proof* that verifies its truth with certainty. Once we've succeeded in finding a correct proof of a mathematical statement, we know that it must be true for all eternity. Unlike the natural sciences, we do not have tentative theories that are extremely well-supported but may be overthrown with new evidence. Thus, mathematics does not have the same types of revolutions like plate tectonics, evolution by natural selection, the oxygen theory of combustion (in place of phlogiston), relativity, quantum mechanics, etc. which overthrow the core structure of a subject and cause a fundamental shift in what statements are understood to be true.

To many, the fact that mathematicians require a complete logical proof with absolute certainty seems strange. Doesn't it suffice to simply check the truth of statement in many instances, and then generalize it

to a universal law? Consider the following example. One of the true statements mentioned above is that there are no positive natural numbers a, b, c with $a^3 + b^3 = c^3$, i.e. we can not obtain a cube by adding two cubes. The mathematician Leonhard Euler conjectured that a similar statement held for fourth powers, i.e. that we can not obtain a fourth power by adding three fourth powers. More formally, he conjectured that there are no positive natural numbers a, b, c, d with $a^4 + b^4 + c^4 = d^4$. For over 200 years it seemed reasonable to believe this might be true, as it held for all small examples and was a natural generalization of a true statement. However, it was eventually shown that there indeed are examples where the sum of 3 fourth powers equals a fourth power, such as the following:

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

In fact, this example is the smallest one possible. Thus, even though $a^4 + b^4 + c^4 \neq d^4$ for all values positive natural numbers a, b, c, and d having at most 5 digits, the statement does not hold generally.

In spite of this example, you may question the necessity of proofs for mathematics relevant to the sciences and applications, where approximations and occasional errors or exceptions may not matter so much. There are many historical reasons why mathematicians have embraced complete, careful, and logical proofs as **the** way to determine truth in mathematics independently from applications. In later math classes, you may explore some of these internal historical aspects, but here are three direct reasons for this approach:

- Mathematics should exist independently from the sciences because sometimes the same mathematics applies to different subjects. It is possible that edge cases which do not matter in one subject (say economics or physics) might matter in another (like computer science). The math needs to be consistent and coherent on its own without reference to the application.
- In contrast to the sciences where two generally accepted theories that contradict each other in some instance can coexist for long periods of time (such as relativity and quantum mechanics), mathematics can not sustain such inconsistencies. As we'll see, one reason for this is that mathematics allows a certain type of argument called proof by contradiction. Any inconsistency at all would allow us to draw all sorts of erroneous conclusions, and the logical structure of mathematics would unravel.
- Unlike the sciences, many areas of math are not subject to direct validation through a physical test. An idea in physics or chemistry, arising from either a theoretical predication or a hunch, can be verified by running an experiment. However, in mathematics we often have no way to reliably verify our guesses through such means. As a result, proofs in mathematics can be viewed as the analogues of experiments in the sciences. In other words, since mathematics exists independently from the sciences, we need an internal check for our intuitions and hunches, and proofs play this role.

2 Quantifiers and Proofs

In the examples of mathematical statements in the previous section, we highlighted two key phrases that appear incredibly often in mathematical statements: **for all** and **there exists**. These two phrases are called *quantifiers* in mathematics, and they form the building blocks of more complicated expressions. Occasionally, these quantifiers appear disguised by a different word choice. Here are a few phrases that mean precisely the same thing in mathematics:

- **For all**: For every, For any, Every, Always, ...
- **There exists**: There is, For some, We can find, ...

These phrases mean what you might expect. For example, saying that a statement of the form "For all a, ..." is true means that whenever we plug in any particular value for a into the ... part, the resulting statement is true. Similarly, saying that a statement of the form "There exists a, ..." is true means that

there is at least one (but possibly more) choice of a value to plug in for a so that the resulting statement is true. Notice that we are *not* saying that there is exactly one choice. Also, be careful in that the phrase "for some" used in everyday conversation could be construed to mean that there need to be several (i.e. more than one) values to plug in for a to make the result true, but in math it is completely synonymous with "there exists".

So how do we prove that a statement that starts with "there exists" is true? For example, consider the following statement:

$$\text{"There exists } a \in \mathbb{Z} \text{ such that } 2a^2 - 1 = 71\text{"}.$$

From your training in mathematics up to this point, you may see the equation at the end and immediately rush to manipulate it using the procedures that you've been taught for years. Before jumping into that, let's examine the logical structure here. In order to convince somebody that the statement is true, we need only find (at least) one particular value to plug in for a so that when we compute $2a^2 - 1$ we obtain 71. Right? In other words, if all that we care about is knowing for sure that the statement is true, we just need to verify that some $a \in \mathbb{Z}$ has this property. Suppose that we happen to stumble across the number 6 and notice that

$$\begin{aligned} 2 \cdot 6^2 - 1 &= 2 \cdot 36 - 1 \\ &= 72 - 1 \\ &= 71. \end{aligned}$$

At this point, we can assert with confidence that the statement is true, and in fact we've just carried out a complete proof. Now you may ask yourself "How did we know to plug in 6 there?", and that is a good question. However, there is a difference between the creative leap (or leap of faith) we took in choosing 6, and the routine verification that it worked. Perhaps we arrived at 6 by plugging in numbers until we got lucky. Perhaps we sacrificed a chicken to get the answer. Perhaps we had a vision. Maybe you copied the answer from a friend or from online (note: don't do this). Now we do care very much about the underlying methods to find a, both for ethical reasons and because sacrificing a chicken may not work if we change the equation slightly. However, for the logical purposes of this argument, the way that we arrived at our value for a does not matter.

We're (hopefully) all convinced that we have verified that the statement "There exists $a \in \mathbb{Z}$ such that $2a^2 - 1 = 71$" is true, but as mentioned we would like to have routine methods to solve similar problems in the future so that we do not have to stumble around in the dark nor invest in chicken farms. Of course, the tools to do this are precisely the material that you learned years ago in elementary algebra. One approach is to perform operations on both sides of the equality with the goal of isolating the a. If we add 1 to both sides, we arrive at $2a^2 = 72$, and after dividing both sides by 2 we conclude that $a^2 = 36$. At this point, we realize that there are two solutions, namely 6 and -6. Alternatively, we can try bringing the 71 over and factoring. By the way, this method found two solutions, and indeed -6 would have worked above. However, remember that proving a "there exists" statement means just finding at least one value that works, so it didn't matter that there was more than one solution.

Let's consider the following more interesting example of a mathematical statement:

$$\text{"There exists } a \in \mathbb{R} \text{ such that } 2a^5 + 2a^3 - 6a^2 + 1 = 0\text{"}.$$

It's certainly possible that we might get lucky and find a real number to plug in that verifies the truth of this statement. But if the chicken sacrificing doesn't work, you may be stymied about how to proceed. However, if you remember Calculus, then there is a nice way to argue that this statement is true without actually finding a particular value of a. The key fact is the Intermediate Value Theorem from Calculus, which says that if $f\colon \mathbb{R} \to \mathbb{R}$ is a continuous function that is positive at some point and negative at another, then it must be 0 at some point as well. Letting $f(x) = 2x^5 + 2x^3 - 6x^2 + 1$, we know from Calculus that $f(x)$ is continuous. Since $f(0) = 1$ and $f(1) = -1$, it follows from the Intermediate Value Theorem that there is an $a \in \mathbb{R}$ (in fact between 0 and 1) such that $f(a) = 0$. Thus, we've proven that the above statement is true,

so long as you accept the Intermediate Value Theorem. Notice again that we've established the statement without actually exhibiting an a that works.

We can make the above question harder by performing the following small change to the statement:

$$\text{“There exists } a \in \mathbb{Q} \text{ such that } 2a^5 + 2a^3 - 6a^2 + 1 = 0\text{”}.$$

Since we do not know what the value of a that worked above was, we are not sure whether it is an element of $\mathbb{Q}$. In fact, questions like this are a bit harder. There is indeed a method to determine the truth of a statement like this, but that's for another course (see Abstract Algebra). The takeaway lesson here is that mathematical statements that look quite similar might require very different methods to solve.

How do we prove that a statement that starts with “for all” is true? For example, consider the following statement:

$$\text{“For all } a, b \in \mathbb{R}, \text{ we have } (a+b)^2 = a^2 + 2ab + b^2\text{”}.$$

In the previous section, we briefly mentioned this statement, but wrote it slightly differently as:

$$\text{“For all real numbers } x \text{ and } y\text{, we have } (x+y)^2 = x^2 + 2xy + y^2\text{”}.$$

Notice that these are both expressing the exact same thing. We only replaced the phrase “real numbers” by the symbol $\mathbb{R}$ and changed our choice of letters. Since the letters are just placeholders for the “for all” quantifier, these two mean precisely the same thing. Ok, so how do we prove the first statement? The problem is that there are infinitely many elements of $\mathbb{R}$ (so infinitely many choices for *each* of a and b), and hence there is no possible way to examine each possible pair in turn and ever hope to finish.

The way around this obstacle is write a general argument that works regardless of the values for a and b. In other words, we're going to take two completely *arbitrary* elements of $\mathbb{R}$ that we will name as a and b so that we can refer to them, and then argue that the result of computing $(a+b)^2$ is the same thing as the result of computing $a^2 + 2ab + b^2$. By taking arbitrary elements of $\mathbb{R}$, our argument will work no matter which particular numbers are actually chosen for a and b. Thus, the way to handle infinitely many choices is to give an argument that works no matter which of the infinitely many choices is taken for a and b.

Now in order to do this, we have to start somewhere. After all, with no assumptions at all about how $+$ and $\cdot$ work, or what squaring means, we have no way to proceed. Ultimately, mathematics starts with basic axioms explaining how certain fundamental mathematical objects and operations work, and builds up everything from there. We won't go into all of those axioms here, but for the purposes of this discussion we will make use of the following fundamental facts about the real numbers:

- Commutative Law (for multiplication): For all $x, y \in \mathbb{R}$, we have $x \cdot y = y \cdot x$.
- Distributive Law: For all $x, y, z \in \mathbb{R}$, we have $x \cdot (y+z) = x \cdot y + x \cdot z$.

These facts are often taken as two (of about 12) of the axioms for the real numbers. It is also possible to prove them from a construction of the real numbers (see Analysis) using more fundamental axioms. In any event, we can use them to prove the above statement follows. Let $a, b \in \mathbb{R}$ be arbitrary. We then have that $a + b \in \mathbb{R}$, and

$$\begin{aligned}
(a+b)^2 &= (a+b) \cdot (a+b) && \text{(by definition)} \\
&= (a+b) \cdot a + (a+b) \cdot b && \text{(by the Distributive Law)} \\
&= a \cdot (a+b) + b \cdot (a+b) && \text{(by the Commutative Law)} \\
&= a \cdot a + a \cdot b + b \cdot a + b \cdot b && \text{(by the Distributive Law)} \\
&= a^2 + a \cdot b + a \cdot b + b^2 && \text{(by the Commutative Law)} \\
&= a^2 + 2ab + b^2 && \text{(by definition).}
\end{aligned}$$

Focus on the logic, and not the algebraic manipulations. First, you should view this chain of equalities by reading it in order. We are claiming that $(a+b)^2$ equals $(a+b)\cdot(a+b)$ in the first line. Then the second line says that $(a+b)\cdot(a+b)$ equals $(a+b)\cdot a+(a+b)\cdot b$ by the Distributive Law. Following this is an assertion that the third and fourth expressions are equal by the Commutative Law, etc. In the second line, notice that $a+b$ is in particular some real number (call it x), and then by viewing $a+b$ also as the sum of two real numbers (playing the role of y and z), we can apply the Distributive Law. If you believe all of the steps, then we have shown that for our completely arbitrary choice of a and b in $\mathbb{R}$, the first and second expressions are equal, the second and third expressions are equal, the third and fourth expressions are equal, etc. Since equality is transitive (i.e. if $x = y$ and $y = z$, then $x = z$), we conclude that $(a+b)^2 = a^2 + 2ab + b^2$. We have taken completely arbitrary $a, b \in \mathbb{R}$, and verified the statement in question, so we can now assert that the "For all" statement is true.

As a quick aside, now that we know that $(a+b)^2 = a^2 + 2ab + b^2$ for all $a, b \in \mathbb{R}$, we can use this fact whenever we have two real numbers. We can even conclude that the statement

$$\text{"For all } a, b \in \mathbb{R}, \text{ we have } (2a+3b)^2 = (2a)^2 + 2(2a)(3b) + (3b)^2\text{"}$$

is true. How does this follow? Consider completely arbitrary $a, b \in \mathbb{R}$. We then have that $2a \in \mathbb{R}$ and $3b \in \mathbb{R}$, and thus we can *apply* our previous result to the two numbers $2a$ and $3b$. We are *not* setting "$a = 2a$" or "$b = 3b$" because it does not make sense to say that $a = 2a$ if a is anything other than 0. We are simply using the fact that if a and b are real numbers, then $2a$ and $3b$ are also real numbers, so we can insert them in for the placeholder values of a and b in our result. Always think of the (arbitrary) choice of letters used in "there exists" and "for all" statements as empty vessels that could be filled with any appropriate value.

We've discussed the basic idea behind proving that a "there exists" or a "for all" statement is true. How do we we prove that such a statement is false? The cheap answer is to prove that its *negation* is true! In other words, if we want to prove that

$$\text{"There exists } a \text{ such that } \ldots\text{"}$$

is false, we can instead prove that

$$\text{"}\mathbf{Not}\text{ (There exists } a \text{ such that } \ldots\text{)"}$$

is true. This sounds great, but now we have this **Not** in the front, so the statement as a whole is no longer a "there exists" statement. However, to show that there does not exist an a with a certain property, we need to show that every a *fails* to have that property. Thus, we can instead show that the statement

$$\text{"For all } a, \text{we have } \mathbf{Not}\ (\ldots)\text{"}$$

is true. For example, suppose that we want to show that the statement

$$\text{"There exists } a \in \mathbb{R} \text{ such that } a^2 + 2a = -5\text{"}$$

is false. By the above discussion, we can instead show that

$$\text{"}\mathbf{Not}\text{ (There exists } a \in \mathbb{R} \text{ such that } a^2 + 2a = -5)\text{"}$$

is true, which is the same as showing that

$$\text{"For all } a \in \mathbb{R}, \text{we have } \mathbf{Not}(a^2 + 2a = -5)\text{"}$$

is true, which is the same as showing that

$$\text{"For all } a \in \mathbb{R}, \text{we have } a^2 + 2a \neq -5\text{"}$$

is true. In other words, we can move the negation past the "there exists" as long as we change it to a "for all" when doing so. How can we show that this last statement is true? Consider an arbitrary $a \in \mathbb{R}$. Notice that

$$\begin{aligned} a^2 + 2a &= (a^2 + 2a + 1) - 1 \\ &= (a+1)^2 - 1 \\ &\geq 0 - 1 \qquad \text{(because squares of reals are nonnegative)} \\ &= -1. \end{aligned}$$

We have shown that given any arbitrary $a \in \mathbb{R}$, we have $a^2 + 2a \geq -1$, and hence $a^2 + 2a \neq -5$. We conclude that the statement

$$\text{"For all } a \in \mathbb{R}, \text{we have } a^2 + 2a \neq -5\text{"}$$

is true, and hence the statement

$$\text{"There exists } a \in \mathbb{R} \text{ with } a^2 + 2a = -5\text{"}$$

is false. Can you see a way to solve this problem using Calculus?

Similarly, if we want to prove that

$$\text{"For all } a, \text{ we have } \ldots\text{"}$$

is false, then we can instead show that

$$\text{"}\mathbf{Not} \text{ (For all } a, \text{ we have } \ldots)\text{"}$$

is true, which is the same as showing that

$$\text{"There exists } a \text{ such that } \mathbf{Not} \ (\ldots)\text{"}$$

is true. In general, we can move a **Not** past one of our two quantifiers at the expense of *flipping* the quantifier to the other type.

Life becomes more complicated when a mathematical statement involves both types of quantifiers in an alternating fashion. For example, consider the following two statements:

1. "For all $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that $m < n$".
2. "There exists $n \in \mathbb{N}$ such that for all $m \in \mathbb{N}$, we have $m < n$".

At first glance, these two statements appear to be essentially the same. After all, they both have "for all $m \in \mathbb{N}$", both have "there exists $n \in \mathbb{N}$", and both end with the expression "$m < n$". Does the fact that these quantifiers appear in different order matter?

Let's examine the first statement more closely. Notice that it has the form "For all $m \in \mathbb{N} \ldots$". In order for this statement to be true, we want to know whether we obtain a true statement *whenever* we plug in a particular natural number for m in the "$\ldots$" part. In other words, we're asking if *all* of the infinitely many statements:

- "There exists $n \in \mathbb{Z}$ such that $0 < n$".
- "There exists $n \in \mathbb{Z}$ such that $1 < n$".
- "There exists $n \in \mathbb{Z}$ such that $2 < n$".

- "There exists $n \in \mathbb{Z}$ such that $3 < n$".
- ...

are true. Looking through each of these, it does indeed appear that they are all true: We can use $n = 1$ in the first one, then $n = 2$ in the second, etc. However, there are infinitely many statements, so we can't actually check each one in turn and hope to finish. We need a general argument that works no matter which value m takes. Now given any *arbitrary* $m \in \mathbb{N}$, we can verify that by taking $n = m + 1$, we obtain a true statement. Here is how we would write this argument up formally.

Proposition 2.1. *For all $m \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that $m < n$.*

Proof. Let $m \in \mathbb{N}$ be arbitrary. We then have that $m+1 \in \mathbb{N}$ and $m < m+1$, so we have shown the existence of an $n \in \mathbb{N}$ with $m < n$ (namely $m + 1$). Since $m \in \mathbb{N}$ was arbitrary, the result follows. □

Let's pause to note a few things about this argument. First, we've labeled the statement as a proposition. By doing so, we are making a claim that the statement to follow is a true statement, and that we will be providing a proof. Alternatively, we sometimes will label a statement as a "theorem" instead of a "proposition" if we want to elevate it to a position of prominence (typically theorems say something powerful, surprising, or incredibly useful). In the proof, we are trying to argue that a "for all" statement is true, so we start by taking an *arbitrary* element of $\mathbb{N}$. Although this m is arbitrary, it is *not* varying. Instead, once we take an arbitrary m, it is now one fixed number that we can use in the rest of the argument. For this particular but arbitrary $m \in \mathbb{N}$, we now want to argue that a certain "there exists" statement is true. In order to do this, we need to exhibit an example of an n that works, and verify it for the reader. Since we have a fixed $m \in \mathbb{N}$ in hand, the n that we pick can depend on that m. In this case, we simply verify that $m + 1$ works as a value for n. As in the examples given above, we do not need to explain why we chose to use $m + 1$, only that the resulting statement is true. In fact, we could have chosen $m + 2$, or $5m + 3$, etc. In the last line, we point out that since $m \in \mathbb{N}$ was arbitrary, and we succeeded in verifying the part inside the "for all" for this m, we can assert that the "for all" statement is true. Finally, the square box at the end of the argument indicates that the proof is over, and so the next paragraph (i.e. this one) is outside the scope of the argument.

Let's move on to the second of our two statements above. Notice that it has the form "There exists $n \in \mathbb{N} \ldots$". In order for this statement to be true, we want to know whether we can find *one* value for n such that we obtain a true statement in the "..." part after plugging it in. In other words, we're asking if *any* of the infinitely many statements

- "For all $m \in \mathbb{N}$, we have $m < 0$".
- "For all $m \in \mathbb{N}$, we have $m < 1$".
- "For all $m \in \mathbb{N}$, we have $m < 2$".
- "For all $m \in \mathbb{N}$, we have $m < 3$".
- ...

is true. Looking through each of these, it appears that every single one of them is false, i.e. *none* of them are true. Thus, it appears that the second statement is false. We can formally prove that it is false by proving that its negation is true. Applying our established rules for how to negate across quantifiers, to show that

"**Not** (There exists $n \in \mathbb{N}$ such that for all $m \in \mathbb{N}$, we have $m < n$)"

is true, we can instead show that

"For all $n \in \mathbb{N}$, **Not** (for all $m \in \mathbb{N}$, we have $m < n$)"

is true, which is same as showing that

$$\text{“For all } n \in \mathbb{N}, \text{ there exists } m \in \mathbb{N} \text{ with } \mathbf{Not}(m < n)\text{”}$$

is true, which is the same as showing that

$$\text{“For all } n \in \mathbb{N}, \text{ there exists } m \in \mathbb{N} \text{ with } m \geq n\text{”}.$$

is true. We now prove that this final statement is true, which is the same as showing that our original second statement is false.

Proposition 2.2. *For all $n \in \mathbb{N}$, there exists $m \in \mathbb{N}$ with $m \geq n$.*

Proof. Let $n \in \mathbb{N}$ be arbitrary. Notice that $n \geq n$ is true, so we have shown the existence of an $m \in \mathbb{N}$ with $m \geq n$. Since $n \in \mathbb{N}$ was arbitrary, the result follows. □

In fact, if we think about it for a moment, we did not have to write a new formal proof here. We wanted to prove that

$$\text{“For all } n \in \mathbb{N}, \text{ there exists } m \in \mathbb{N} \text{ with } m \geq n\text{”}$$

is true. In Proposition 2.1, we showed that

$$\text{“For all } m \in \mathbb{N}, \text{ there exists } n \in \mathbb{N} \text{ with } m < n\text{”}$$

is true. Now remember that the letters are simply placeholders, so we can restate Proposition 2.1 as

$$\text{“For all } n \in \mathbb{N}, \text{ there exists } m \in \mathbb{N} \text{ with } n < m\text{”}$$

which is the same as

$$\text{“For all } n \in \mathbb{N}, \text{ there exists } m \in \mathbb{N} \text{ with } m > n\text{”}.$$

Since we know this is true, we can immediately conclude that the weaker statement in Proposition 2.2 is true as well.

In general, consider statements of the following two types:

1. “For all a, there exists b such that ...”.
2. “There exists b such that for all a, we have ...”.

Let's examine the difference between them in a more informal way. Think about a game with two players where Player I goes first. For the first statement to be true, it needs to be the case that no matter how Player I moves, Player II can respond in such a way so that ... happens. Notice in this scenario Player II's move can depend on Player I's move, i.e. the value of b can depend on the value of a. For the second statement to be true, it needs to be the case that Player I can make a move so brilliant that no matter how Player II responds, we have that ... happens. In this scenario, b needs to be chosen *first* without knowing a, so b can not depend on a in any way.

Finally, let's discuss one last construct in mathematical statements, which is an “if...then...” clause. We call such statements *implications*, and they naturally arise when we want to quantify only over part of a set. For example, the statement

$$\text{“For all } a \in \mathbb{R}, \text{ we have } a^2 - 4 \geq 0\text{”}$$

is false because $0 \in \mathbb{R}$ and $0^2 - 4 < 0$. However, the statement

$$\text{“For all } a \in \mathbb{R} \text{ with } a \geq 2, \text{ we have } a^2 - 4 \geq 0\text{”}$$

is true. Instead of coupling the condition "$a \geq 2$" with the "for all" statement, we can instead write this statement as

$$\text{"For all } a \in \mathbb{R},\ (\text{If } a \geq 2,\ \text{then } a^2 - 4 \geq 0)\text{"}.$$

We often write this statement in shorthand by dropping the "for all" as:

$$\text{"If } a \in \mathbb{R} \text{ and } a \geq 2,\ \text{then } a^2 - 4 \geq 0\text{"}.$$

One convention, that initially seems quite strange, arises from this. Since we want to allow "if...then..." statements, we need to assign truth values to them because every mathematical statement should either be true or false. If we plug the value 3 for a into this last statement (or really past the "for all" in the penultimate statement), we arrive at the statement

$$\text{"If } 3 \geq 2,\ \text{then } 3^2 - 4 \geq 0\text{"},$$

which we naturally say is true because both the "if" part and the "then" part are true. However, it's less clear how we should assign a truth value to

$$\text{"If } 1 \geq 2,\ \text{then } 1^2 - 4 \geq 0\text{"}$$

because both the "if" part and the "then" part are false. We also have an example like

$$\text{"If } -5 \geq 2,\ \text{then } (-5)^2 - 4 \geq 0\text{"},$$

where the "if" part is false and the "then" part is true. In mathematics, we make the convention that an "if...then..." statement is false only when the "if" part is true and the "then" part is false. Thus, these last two examples we declare to be true. The reason why we do this is be consistent with the intent of the "for all" quantifier. In the example

$$\text{"For all } a \in \mathbb{R},\ (\text{If } a \geq 2,\ \text{then } a^2 - 4 \geq 0)\text{"},$$

we do not want values of a with $a < 2$ to have any effect at all on the truth value of the "for all" statement. Thus, we want the parenthetical statement to be true whenever the "if" part is false. In general, given two mathematical statements P and Q, we *define* the following:

- If P is true and Q is true, we say that "If P, then Q" is true.
- If P is true and Q is false, we say that "If P, then Q" is false.
- If P is false and Q is true, we say that "If P, then Q" is true.
- If P is false and Q is false, we say that "If P, then Q" is true.

We can compactly illustrate these conventions with the following simple table, known as a "truth table", where we use T for true and F for false:

P	Q	If P, then Q
T	T	T
T	F	F
F	T	T
F	F	T

Compare these with the simple truth tables that arise from the word "and" and the word "or" (remembering that "or" is always the inclusive or in mathematics, unless stated otherwise):

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

3 Evens and Odds

We will spend this section discussing even and odd integers, and culminate with a proof that $\sqrt{2}$ is irrational. As we've discussed, all mathematics ultimately relies upon a few core concepts and axioms. Thus, whenever we introduce a new word like *even* or *odd*, we need to define it in terms of more basic concepts. We accomplish this using our "there exists" quantifier.

Definition 3.1. *Let $a \in \mathbb{Z}$.*

- *We say that a is* even *if there exists $m \in \mathbb{Z}$ with $a = 2m$.*
- *We say that a is* odd *if there exists $m \in \mathbb{Z}$ with $a = 2m + 1$.*

Since this is our first formal definition, let's pause for a moment to understand the role of definitions in mathematics. First, in contrast to our "if...then" statements, the word "if" when used alone in a definition is really shorthand for "to mean that". Now a mathematical definition tells us *exactly* what we mean by the words or notation that we introduce. There is no more subtlety to add. Every time we use the word "even", we are really just using it so that we do not have to say "there exists $m \in \mathbb{Z}$ with $a = 2m$". In other words, everything about an integer being "even" should *always* eventually go back to the definition.

We can use this definition to now assert that certain integers are even or odd. For example, we can assert that 10 is even because $10 = 2 \cdot 5$ and $5 \in \mathbb{Z}$. We can also see that 71 is odd because we can write $71 = 2 \cdot 35 + 1$ and $35 \in \mathbb{Z}$. Also notice that 0 is even by our definition because $0 = 2 \cdot 0$ and $0 \in \mathbb{Z}$.

Now you might have thought to define the word even in a different way. For example, you could consider defining a to be even if the remainder when dividing a by 2 is 0. This is certainly a natural approach, and for many people that is how it was explained to them when they were young. However, since mathematics terms should be precisely defined down to our ultimately basic concepts, such a definition would require us to work through what we mean by "division" and "remainder" for integers. Although it is certainly possible to do this, our official definition introduces no new concepts and is easier to work with. Eventually, if we were to formally define "division" and "remainder" (like you might do in Elementary Number Theory or Abstract Algebra), then you can *prove* that our official definition means the same thing as the one obtained by such an approach. In general, however, there is no strict rule for choosing which definition to use when several competing alternatives are available. Ideally, we settle in on a definition that is simple, useful, and elegant. In mathematical subjects that have been developed over the course of several centuries, mathematicians have settled on the "right" core definitions over time, but in newer areas finding the "right" definitions is often an important step.

We now prove our first result. We'll write it formally, and then discuss its structure after the proof.

Proposition 3.2. *If $a \in \mathbb{Z}$ is even, then a^2 is even.*

Proof. Let $a \in \mathbb{Z}$ be an arbitrary even integer. Since a is even,we can fix $n \in \mathbb{Z}$ with $a = 2n$. Notice that

$$\begin{aligned} a^2 &= (2n)^2 \\ &= 4n^2 \\ &= 2 \cdot (2n^2). \end{aligned}$$

Since $2n^2 \in \mathbb{Z}$, we conclude that a^2 is even. Since $a \in \mathbb{Z}$ was an arbitrary even integer, the result follows. □

When starting this proof, we have to remember that there is a hidden "for all" in the "if...then...", so we should start the argument by taking an arbitrary $a \in \mathbb{Z}$. However, we're trying to prove an "if...then..." statement about such an a. Whenever the "if..." part is false, we do not care about it (or alternatively we assign it true by the discussion at the end of the previous section), so instead of taking an arbitrary $a \in \mathbb{Z}$, we should take an arbitrary $a \in \mathbb{Z}$ *that is even*. With this even a in hand, our goal is to prove that a^2 is even.

Recall that whenever we think about even numbers now, we should always eventually go back to our definition. Thus, we next unwrap what it means to say that "a is even". By definition of even, we know that there exists $m \in \mathbb{Z}$ with $a = 2m$. In other words, there is at least one choice of $m \in \mathbb{Z}$ so that the statement "$a = 2m$" is true.

Now it's conceivable that there are many m that work (the definition does not rule that out), but there is at least one that works. We invoke this true statement by *picking* some value of $m \in \mathbb{Z}$ that works, and we do this by giving it a name n. This was an arbitrary choice of name, and we could have chosen almost any other name for it. We could have called it k, b, ℓ, x, δ, Maschke, $\heartsuit$, or \$. The only really awful choice would be to call it a, because we have already given the letter a a meaning (namely as our arbitrary element). We could even have called it m, and in the future we will likely do this. However, to avoid confusion in our first arguments, we've chosen to use a different letter than the one in the definition to make it clear that we are now fixing one value that works. We encapsulate this entire paragraph in the key phrase "*we can fix*". In general, when we want to invoke a true "there exists" statement in our argument, we use the phrase *we can fix* to pick a corresponding witness.

Ok, we've successfully taken our assumption and unwrapped it, so that we now have a fixed $n \in \mathbb{Z}$ with $a = 2n$. Before jumping into the algebra of the middle part of the argument, let's think about our goal. We want to show that a^2 is even. In other words, we want to argue that there exists $m \in \mathbb{Z}$ with $a^2 = 2m$. Don't think about the letter. We want to end by writing $a^2 = 2\_\_$ where we whatever we fill in for $\_\_$ is an integer.

With this in mind, we start with what we know is true, i.e. that $a = 2n$, and hope to drive forward with true statements every step of the way until we arrive at our goal. Since $a = 2n$ is true, we know that $a^2 = (2n)^2$ is true. We also know that $(2n)^2 = 4n^2$ is true and that $4n^2 = 2 \cdot (2n^2)$ is true. Putting it all together, we conclude that $a^2 = 2 \cdot (2n^2)$ is true. Have we arrived at our goal? We've written a^2 as 2 times something, namely it is 2 times $2n^2$. Finally, we notice that $2n^2 \in \mathbb{Z}$ because $n \in \mathbb{Z}$. Thus, starting with the true statement $a = 2n$, we have derived a sequence of true statements culminating with the true statement that a^2 equals 2 times some integer. Therefore, by definition, we are able to conclude that a^2 is even. Since a was arbitrary, we are done.

Pause to make sure that you understand all of the logic in the above argument. Mathematical proofs are typically written in very concise ways where each word matters. Furthermore, these words often pack in complex thoughts, such as with the "we may fix" phrase above. Eventually, we will just write our arguments succinctly without all of this commentary, and it's important to make sure that you understand how to unpack both the language and the logic used in proofs.

In fact, we can prove a stronger result than what is stated in the proposition. It turns out that if $a \in \mathbb{Z}$ is even and $b \in \mathbb{Z}$ is arbitrary, then ab is even (i.e. the product of an even integer and *any* integer is an even integer). Try to give a proof! From this fact, we can immediately conclude that the previous proposition is true, because given any $a \in \mathbb{Z}$ that is even, we can apply this stronger result when using a for both of the

values (i.e. for both a and b). Remember that the letters are placeholders, so we can fill them both with the same value if we want. Different letters do not necessarily mean different values!

Let's move on to another argument that uses the definitions of both even and odd.

Proposition 3.3. *If $a \in \mathbb{Z}$ is even and $b \in \mathbb{Z}$ is odd, then $a + b$ is odd.*

Proof. Let $a, b \in \mathbb{Z}$ be arbitrary with a even and b odd. Since a is even, we can fix $n \in \mathbb{Z}$ with $a = 2n$. Since b is odd, we can fix $k \in \mathbb{Z}$ with $b = 2k + 1$. Notice that

$$\begin{aligned} a + b &= 2n + (2k + 1) \\ &= (2n + 2k) + 1 \\ &= 2 \cdot (n + k) + 1. \end{aligned}$$

Now $n + k \in \mathbb{Z}$ because both $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$, so we can conclude that $a + b$ is odd. Since a and b were arbitrary, the result follows. □

This argument is similar to the last one, but now we have two arbitrary elements $a, b \in \mathbb{Z}$, with the additional assumption that a is even and b is odd. As in the previous proof, we unwrapped the definitions involving "there exists" quantifiers to fix witnessing elements n and k. Notice that we had to give these witnessing elements different names because the n that we pick to satisfy $a = 2n$ might be a completely different number from the k that we pick to satisfy $b = 2k + 1$. Once we've unwrapped those definitions, our goal is to prove that $a + b$ is odd, which means that we want to show that $a + b = 2\_\_ + 1$, where we fill in $\_\_$ with an integer. Now using algebra we proceed forward from our given information to conclude that $a + b = 2 \cdot (n + k) + 1$, so since $n + k \in \mathbb{Z}$ (because both $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$), we have reached our goal.

We now ask a seemingly simple question: Is 1 even? We might notice that 1 is odd because $1 = 2 \cdot 0 + 1$ and $0 \in \mathbb{Z}$, but how does that help us? At the moment, we only have our definitions, and it is not immediately obvious from the definitions that a number can not be both even and odd. To prove that 1 is not even, we have to argue that

"There exists $m \in \mathbb{Z}$ with $1 = 2m$"

is false, which is the same as showing that

"**Not**(There exists $m \in \mathbb{Z}$ with $1 = 2m$)"

is true, which is the same as showing that

"For all $m \in \mathbb{Z}$, we have $1 \neq 2m$"

is true. Thus, we need to prove a "for all" statement. We do this now using a new type of argument known as *proof by cases*.

Proposition 3.4. *The integer 1 is not even.*

Proof. We show that $2m \neq 1$ for all $m \in \mathbb{Z}$. Let $m \in \mathbb{Z}$ be arbitrary. We then have that either $m \leq 0$ or $m \geq 1$, giving us two cases:

- *Case 1:* Suppose that $m \leq 0$. Multiplying both sides by 2, we see that $2m \leq 0$, so $2m \neq 1$.
- *Case 2:* Suppose that $m \geq 1$. Multiplying both sides by 2, we see that $2m \geq 2$, so $2m \neq 1$.

Since these two cases exhaust all possibilities for m, we have shown hat $2m \neq 1$ unconditionally. Since $m \in \mathbb{Z}$ was arbitrary, the result follows. □

This is a perfectly valid argument, but it's very specific to the number 1. We would like to prove the far more general result that no integer is both even and odd. We'll introduce a new method of proof to accomplish this task. Up until this point, if we have a statement P that we want to prove is true, we tackle the problem directly by working through the quantifiers one by one. Similarly, if we want to prove that P is false, we instead prove that **Not**(P) is true, and use our rules for moving the **Not** inside so that we can prove a statement involving quantifiers on the outside directly.

However, there is another method to prove that a statement P is true that is beautifully sneaky. The idea is as follows. We *assume* that **Not**(P) is true, and show that under this assumption we can logically derive another statement, say Q, that we *know* to be false. Thus, *if* **Not**(P) was true, *then* Q would have to be both true and false at the same time. Madness would ensue. **Human sacrifice, dogs and cats living together, mass hysteria**. This is inconceivable, so the only possible explanation is that **Not**(P) must be false, which is the same as saying that P must be true. A proof of this type is called a *proof by contradiction*, because under the assumption that **Not**(P) was true, we derived a contradiction, and hence we can conclude that P must be true.

Proposition 3.5. *No integer is both even and odd.*

Before jumping into the proof, let's examine what the proposition is saying formally. If we write it out carefully, the claim is that

"**Not**(There exists $a \in \mathbb{Z}$ such that a is even and a is odd)"

is true. If we were trying to prove this statement directly, we would move the **Not** inside and instead try to prove that

"For all $a \in \mathbb{Z}$, we have **Not**(a is even and a is odd)"

is true, which is the same as showing that

"For all $a \in \mathbb{Z}$, either a is not even or a is not odd"

is true (recalling that "or" is always the inclusive or in mathematics). To prove this directly, we would then need to take an arbitrary $a \in \mathbb{Z}$, and argue that (at least one) of "a is not even" or "a is not odd" is true. Since this looks a bit difficult, let's think about how we would structure a proof by contradiction. Recall that we are trying to prove that

"**Not**(There exists $a \in \mathbb{Z}$ such that a is even and a is odd)"

is true. Now instead of moving the **Not** inside and proving the corresponding "for all" statement directly, we are going to do a proof by contradiction. Thus, we *assume* that

"**Not**(**Not**(There exists $a \in \mathbb{Z}$ such that a is even and a is odd))",

is true, which is the same as assuming that

"There exists $a \in \mathbb{Z}$ such that a is even and a is odd",

is true, and then derive a contradiction. Let's do it.

Proof of Proposition 3.5. Assume, for the sake of obtaining a contradiction, that there exists an integer that is both even and odd. We can then fix an $a \in \mathbb{Z}$ that is both even and odd. Since a is even, we can fix $m \in \mathbb{Z}$ with $a = 2m$. Since a is odd, we may fix $n \in \mathbb{Z}$ with $a = 2n + 1$. We then have $2m = 2n + 1$, so $2(m - n) = 1$. Notice that $m - n \in \mathbb{Z}$ because both $m \in \mathbb{Z}$ and $n \in \mathbb{Z}$. Thus, we can conclude that 1 is even, which contradicts Proposition 3.4. Therefore, our assumption must be false, and hence no integer can be both even and odd. □

Ok, so no integer can be both even and odd. Is it true that every integer is either even or odd? Intuitively, the answer is clearly yes, but it's not obvious how to prove it without developing a theory of division with remainder. It is possible to accomplish this task using a technique called "mathematical induction", but rather than take that fascinating detour, we will leave the argument to later courses (see Elementary Number Theory, Combinatorics, or Abstract Algebra). We will simply assert that the following is true, and you'll have to suffer through the anticipation for a semester.

Fact 3.6. *Every integer is either even or odd.*

Proposition 3.7. *If $a \in \mathbb{Z}$ and a^2 is even, then a is even.*

Before jumping into a proof of this fact, we pause to notice that a direct approach looks infeasible. Why? Suppose that we try to prove it directly by starting with the assumption that a^2 is even. Then, by definition, we can fix $n \in \mathbb{Z}$ with $a^2 = 2n$. Since $a^2 \geq 0$, we conclude that we must have that $n \geq 0$. It is now natural to take the square root of both sides and write $a = \sqrt{2n}$. Recall that our goal is to write a as 2 times some integer, but this looks bad. we have $a = \sqrt{2} \cdot \sqrt{n}$, but $\sqrt{2}$ is not 2, and $\sqrt{n}$ is probably not an integer. We can force a 2 by noticing that $\sqrt{2n} = 2 \cdot \sqrt{\frac{n}{2}}$, but $\sqrt{\frac{n}{2}}$ seems even less likely to be an integer.

Let's take a step back. Notice that Proposition 3.7 looks an awful lot like Proposition 3.2. In fact, one is of the form "If P, then Q" while the other is of the form "If Q, then P". We say that "If Q, then P" is the *converse* of "If P, then Q". Unfortunately, if an "If...then..." statement is true, its converse might be false. For example,

"If $f(x)$ is differentiable, then $f(x)$ is continuous"

is true, but

"If $f(x)$ is continuous, then $f(x)$ is differentiable".

is false. For an even more basic example, the statement

"If $a \in \mathbb{Z}$ and $a \geq 7$, then $a \geq 4$"

is true, but the converse statement

"If $a \in \mathbb{Z}$ and $a \geq 4$, then $a \geq 7$"

is false.

The reason why Proposition 3.2 was easier to prove was that we started with the assumption that a was even, and by squaring both sides of $a = 2n$ we were able to write a^2 as 2 times an integer by using the fact that the square of a integer was an integer. However, starting with an assumption about a^2, it seems difficult to conclude much about a without taking square roots. Here's where a truly clever idea comes in. Instead of looking at the converse of our statement, which says "If $a \in \mathbb{Z}$ and a is even, then a^2 is even", consider the following statement:

"If $a \in \mathbb{Z}$ and a is not even, then a^2 is not even"

Now this statement is a strange twist on the first. We've switched the hypothesis and conclusion around and included negations that were not there before. At first sight, it may appear that this statement has nothing to do with the one in Proposition 3.7. However, suppose that we are somehow able to prove it. I claim that Proposition 3.7 follows. How? Suppose that $a \in \mathbb{Z}$ is such that a^2 is even. We want to argue that a must be even. Well, suppose not. Then a is not even, so by this new statement (which we are assuming we know is true), we could conclude that a^2 is not even. However, this contradicts our assumption. Therefore, it must be the case that a is even!

We want to give this general technique a name. The *contrapositive* of a statement of the form "If P, then Q" is the statement "If **Not**(Q), then **Not**(P)". In other words, we flip the two parts of the "If...then..."

statement and put a **Not** on both of them. In general, suppose that we are successful in proving that the contrapositive statement

$$\text{“If } \mathbf{Not}(\mathsf{Q}), \text{ then } \mathbf{Not}(\mathsf{P})\text{”}$$

is true. From this, it turns out that we can conclude that

$$\text{“If } \mathsf{P}, \text{ then } \mathsf{Q}\text{”}$$

is true. Let's walk through the steps. Remember, we are assuming that we know that “If **Not**(Q), then **Not**(P)” is true. To prove that “If P, then Q” is true, we assume that P is true, and have as our goal to show that Q is true. Now under the assumption that Q is false, we would be able to conclude that **Not**(Q) is true, but this would imply that **Not**(P) is true, contradicting the fact that we are assuming that P is true! The only logical possibility is that the truth of P must imply the truth of Q.

We are now ready to prove Proposition 3.7.

Proof of 3.7. We prove the contrapositive. That is, we show that whenever a is not even, then a^2 is not even. Suppose then that $a \in \mathbb{Z}$ is an arbitrary integer that is not even. Using Fact 3.6, it follows that a is odd. Thus, we can fix $n \in \mathbb{Z}$ with $a = 2n + 1$. We then have

$$\begin{aligned} a^2 &= (2n+1)^2 \\ &= 4n^2 + 4n + 1 \\ &= 2 \cdot (2n^2 + 2n) + 1. \end{aligned}$$

Notice that $2n^2 + 2n \in \mathbb{Z}$ because $n \in \mathbb{Z}$, so we can conclude that a^2 is odd. Using Proposition 3.5, it follows that a^2 is not even. We have shown that if a is not even, then a^2 is not even. Since we've proven the contrapositive, it follows that if a^2 is even, then a is even. □

We can now prove the following fundamental theorem.

Theorem 3.8. *There does not exist $q \in \mathbb{Q}$ with $q^2 = 2$. In other words, $\sqrt{2}$ is irrational.*

Proof. Suppose for the sake of obtaining a contradiction that there does exist $q \in \mathbb{Q}$ with $q^2 = 2$. Fix $a, b \in \mathbb{Z}$ with $q = \frac{a}{b}$ and such that $\frac{a}{b}$ is in lowest terms, i.e. where a and b have no common factors greater than 1. We have

$$\left(\frac{a}{b}\right)^2 = 2,$$

hence

$$\frac{a^2}{b^2} = 2,$$

and so

$$a^2 = 2 \cdot b^2.$$

Since $b^2 \in \mathbb{Z}$, we conclude that a^2 is even. Using Proposition 3.7, it follows that a is even, so we can fix $c \in \mathbb{Z}$ with $a = 2c$. We then have

$$\begin{aligned} 2b^2 &= a^2 \\ &= (2c)^2 \\ &= 4c^2. \end{aligned}$$

Dividing each side by 2, we conclude that

$$b^2 = 2c^2.$$

Since $c^2 \in \mathbb{Z}$, it follows that b^2 is even. Using Proposition 3.7 again, we conclude that b is even. Thus, we can fix $d \in \mathbb{Z}$ with $b = 2d$. We then have

$$q = \frac{a}{b} = \frac{2c}{2d} = \frac{c}{d}.$$

This is a contradiction because $\frac{a}{b}$ was assumed to be in lowest terms, but we have reduced it further. Therefore, there does not exist $q \in \mathbb{Q}$ with $q^2 = 2$. □

We end this section with an interesting fact, which gives another example of proving a "there exists" statement.

Proposition 3.9. *If $a \in \mathbb{Z}$ is odd, then there exist $b, c \in \mathbb{Z}$ with $a = b^2 - c^2$. In other words, every odd integer is the difference of two perfect squares.*

Before jumping into the proof, we first try out some examples:

$$\begin{aligned} 1 &= 1^2 - 0^2 \\ 3 &= 2^2 - 1^2 \\ 5 &= 3^2 - 2^2 \\ 7 &= 4^2 - 3^2 \\ 9 &= 5^2 - 4^2. \end{aligned}$$

There seems to be a clear pattern here, but notice that $9 = 3^2 - 0^2$ as well, so there are sometimes other ways to write numbers as the difference of squares. Nonetheless, to prove a "there exists" statement, we just need to give an example. The above pattern suggests that we can just use adjacent numbers for b and c, and we now give a proof of this fact generally.

Proof. Let $a \in \mathbb{Z}$ be an arbitrary odd integer. By definition, we can fix $n \in \mathbb{Z}$ with $a = 2n + 1$. Notice that $n + 1 \in \mathbb{Z}$ and that

$$\begin{aligned} (n+1)^2 - n^2 &= n^2 + 2n + 1 - n^2 \\ &= 2n + 1 \\ &= a. \end{aligned}$$

Therefore, we shown the existence of b and c (namely $b = n+1$ and $c = n$) for which $a = b^2 - c^2$. Since $a \in \mathbb{Z}$ was an arbitrary odd integer, we conclude that every odd integer is the difference of two perfect squares. □