Evens, Odds, and Sets

Joseph R. Mileti

January 28, 2015

1 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 1.1. *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 its explained to them when they are 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 has been developed for 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 1.2. *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. If the "if..." part is false, then 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 thing 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 1.3. *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 3 even? We might notice that 3 is odd because $3 = 2 \cdot 1 + 1$ and $1 \in \mathbb{Z}$, 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 3 is not even, we have to argue that

"There exists $m \in \mathbb{Z}$ with $3 = 2m$" is false,

which is the same as showing that the

"**Not**(There exists $m \in \mathbb{Z}$ with $3 = 2m$)" is true,

which is the same as showing that

"For all $m \in \mathbb{Z}$, we have $3 \neq 2m$" is true.

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

Proposition 1.4. *The integer 3 is not even.*

Proof 1 of Proposition 1.4. Let $m \in \mathbb{Z}$ be arbitrary. We have three cases.

- *Case 1:* Suppose that $m \leq 0$. Multiplying both sides by 2, we see that $2m \leq 0$, so $2m \neq 3$.
- *Case 2:* Suppose that $m = 1$. We then have that $2m = 2$, so $2m \neq 3$.
- *Case 3:* Suppose that $m \geq 2$. Multiplying both sides by 2, we see that $2m \geq 4$, so $2m \neq 3$.

Since these three cases exhaust all possibilities for m, we have shown hat $2m \neq 3$ unconditionally. Since $m \in \mathbb{Z}$ was arbitrary, the result follows. □

This is a perfectly valid argument, but let's take this opportunity to introduce another slick method of proof. Up until this point, if we have a statement P, and we want to prove that it 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 can conclude that P must be true.

Let's try to give a proof by contradiction of Proposition 1.4. Recall that we are trying to prove that 3 is not even, so we have to argue that

"**Not**(There exists $m \in \mathbb{Z}$ with $3 = 2m$)" 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 $m \in \mathbb{Z}$ with $3 = 2m$))" is true,

which is the same as assuming that

"There exists $m \in \mathbb{Z}$ with $3 = 2m$" is true,

and derive a contradiction. Let's do it.

Proof 2 of Proposition 1.4. We give a proof by contradiction. Assume instead that 3 is even. We can then fix $n \in \mathbb{Z}$ with $3 = 2n$. Dividing both sides by 2, we conclude that $n = \frac{3}{2}$. Since $\frac{3}{2} \notin \mathbb{Z}$, it follows that $n \notin \mathbb{Z}$. We now have that both $n \in \mathbb{Z}$ and $n \notin \mathbb{Z}$, which is a contradiction. Therefore, our assumption must be false, and hence we conclude that 3 is not even. □

We now generalize this argument to the following.

Proposition 1.5. *No integer is both even and odd.*

Proof. 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 $2(m-n) = 1$. Dividing both sides by 2, we conclude that $m - n = \frac{1}{2}$. Since $m - n \in \mathbb{Z}$, this implies that $\frac{1}{2} \in \mathbb{Z}$, which is a contradiction. Therefore, our assumption must be false, and the result follows. □

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. One can do use this theory using a technique called "mathematical induction", but rather than take that fascinating detour, I 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 1.6. *Every integer is either even or odd.*

Proposition 1.7. *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 1.7 looks an awful lot like Proposition 1.2. 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 1.2 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 1.7. However, suppose that we are somehow able to prove it. I claim that Proposition 1.7 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 $\mathbf{Not}(\mathsf{Q})$, then $\mathbf{Not}(\mathsf{P})$". 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

"If $\mathbf{Not}(\mathsf{Q})$, then $\mathbf{Not}(\mathsf{P})$"

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

"If P, then Q"

is true. Let's walk through the steps. Remember, we are assuming that we know that "If $\mathbf{Not}(\mathsf{Q})$, then $\mathbf{Not}(\mathsf{P})$" 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 $\mathbf{Not}(\mathsf{Q})$ is true, but this would imply that $\mathbf{Not}(\mathsf{P})$ 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 1.7.

Proof of 1.7. 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 1.6, 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 1.5, 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 1.8. *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

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

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 1.7, 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 1.7 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 1.9. *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.*

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. □

2 Sets, Set Construction, and Subsets

2.1 Sets and Set Construction

In mathematics, a set is a collection of elements without regard to repetition or order. Intuitively, a set is a box where the only thing that matters are the objects that are inside it, and furthermore the box does not have more than 1 of any given object. For example, $\{3, 5\}$ is a set with 2 elements. Since all that matters are the elements, we define two sets to be equal if they have the same elements, regardless of how the sets themselves are defined or described.

Definition 2.1. *Given two sets A and B, we say that $A = B$ if A and B have exactly the same elements.*

Since the elements matter, but not the order of them, we have $\{3, 7\} = \{7, 3\}$ and $\{1, 2, 3\} = \{3, 1, 2\}$. Also, although we typically would not even write something like $\{2, 5, 5\}$, if we choose to do so then we would have $\{2, 5, 5\} = \{2, 5\}$ because both have the same elements, namely 2 and 5.

We use $\in$ to represent the fact that a particular object is an element of a certain set. For example, we have $2 \in \{2, 5\}$ and $3 \notin \{2, 5\}$. Since sets are mathematical objects, they may be elements of other sets. For example, we can form the set $S = \{1, \{2, 3\}\}$. Notice that we have $1 \in S$ and $\{2, 3\} \in S$, but $2 \notin S$ and $3 \notin S$. As a result, S has only 2 elements, namely 1 and $\{2, 3\}$. Thinking of a set as a box, one element of S is the number 1, and the other is a different box. The empty set is the unique set with no elements. We can write it as $\{\}$, but instead we typically denote it by $\emptyset$. There is only *one* empty set, because if both A and B have no elements, then they have exactly the same elements for vacuous reasons, and hence $A = B$. Notice that $\{\emptyset\}$ does not equal $\emptyset$. After all, $\{\emptyset\}$ has one element! You can think of $\{\emptyset\}$ as a box that has one empty box inside it.

Notice that sets can be either finite or infinite. At this point, our standard examples of infinite sets are the universes of numbers:

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
- $\mathbb{N}^+ = \{1, 2, 3, \dots\}$.
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- $\mathbb{Q}$ is the set of rational numbers.
- $\mathbb{R}$ is the set of real numbers.

Beyond these fundamental sets, there are various ways to define new sets. In some cases, we can simply list the elements as we did above. Although this often works for small finite sets, it is almost never a good idea to list the elements of a set with 20 or more elements, and it rarely works for infinite sets (unless there is an obvious pattern like $\{5, 10, 15, 20, \dots\}$). One of the standard ways to define a set S is to carve it out

of some bigger set A by describing a certain property that may or may not be satisfied by an element of A. For example, we could define

$$S = \{n \in \mathbb{N} : 5 < n < 13\}.$$

We read this line by saying that S is defined to be the set of all $n \in \mathbb{N}$ such that $5 < n < 13$. Thus, in this case, we are taking $A = \mathbb{N}$, and forming a set S by carving out those elements of A that satisfy the condition that $5 < n < 13$. In other words, think about going through each of element n, checking if $5 < n < 13$ is a true statement, and collecting those $n \in \mathbb{N}$ that make it true into a set that we call S. In more simple terms, we can also describe S as follows:

$$S = \{6, 7, 8, 9, 10, 11, 12\}.$$

It is important that we put the "$\mathbb{N}$" in the above description, because if we wrote $\{n : 5 < n < 13\}$ then it would be unclear what n we should consider. For example, should $\frac{11}{2}$ be in this set? How about $\sqrt{17}$? Sometimes the "universe" of numbers (or other mathematical objects) that we are working within is clear, but typically it is best to write the global set that we are picking elements from in order to avoid such ambiguity. Notice that when we define a set, there is no guarantee that it has any elements. For example, $\{q \in \mathbb{N} : q^2 = 2\} = \emptyset$ by Theorem 1.8. Keep in mind that we can also use words in our description of sets, such as $\{n \in \mathbb{N} : n \text{ is an even prime}\}$. As mentioned above, two sets that have quite different descriptions can be equal. For example, we have

$$\{n \in \mathbb{N} : n \text{ is an even prime}\} = \{n \in \mathbb{N} : 3 < n^2 < 8\}$$

because both sets equal $\{2\}$. Always remember the structure of sets formed in this way. We write

$$\{x \in A : \mathsf{P}(x)\}$$

where A is a known set and $\mathsf{P}(x)$ is a "property" such that given a particular $y \in A$, the statement $\mathsf{P}(y)$ is either true or false.

Another way to describe a set is through a "parametric" description. Rather than carving out a certain subset of a given set by describing a property that the elements must satisfy, we can instead form all the elements one obtains by varying a value through a particular set. For example, consider the following description of a set:

$$S = \{3x^2 + 1 : x \in \mathbb{R}\}.$$

Although the notation looks quite similar to the above (in both case we have curly braces, with a : in the middle), this set is described differently. Notice that instead of having a set that elements are coming from on the left of the colon, we now have a set that elements are coming from on the right. Furthermore, we now have a formula on the left rather than a property on the right. The difference is that for a property, when we plug in an element from the given set, we either obtain a true or false value, but that isn't the case for a formula like $3x^2 + 1$. The idea here is that instead of carving out a subset of $\mathbb{R}$ by using a property (i.e. taking those elements that make the property *true*), we let x vary through all real numbers, plug each of these real numbers x into $3x^2 + 1$, and form the set of all possible outputs. For example, we have $4 \in S$ because $4 = 3 \cdot 1^2 + 1$. In other words, when $x = 1$, the left hand side gives the value 4, so we should put $4 \in S$. Notice also that $4 = 3 \cdot (-1)^2 + 1$, so we can also see that $4 \in S$ because of the "witness" -1. Of course, we are forming a set, so we do not repeat the number 4. We also have $1 \in S$ because $1 = 3 \cdot 0^2 + 1$, and we have $76 \in S$ because $76 = 3 \cdot 5^2 + 1$. Notice also that $7 \in S$ because $7 = 3 \cdot (\sqrt{2})^2 + 1$.

In a general parametric set description, we will have a set A and a *function* $f(x)$ that allows inputs from A, and we write

$$\{f(x) : x \in A\}$$

for the set of all possible outputs of the function as we vary the inputs through the set A. We will discuss the general definition of a function in the next section, but for the moment you can think of them as given by formulas.

Now it is possible and indeed straightforward to turn any parametric description of a set into one where we carve out a subset by a property. In our case of $S = \{3x^2 + 1 : x \in \mathbb{R}\}$ above, we can alternatively write it as

$$S = \{y \in \mathbb{R} : \text{There exists } x \in \mathbb{R} \text{ with } y = 3x^2 + 1\}.$$

Notice how we flipped the way we described by the set by introducing a "there exists" quantifier to form a property. This is always possible for a parametric description. For example, we have

$$\{5n + 4 : n \in \mathbb{N}\} = \{m \in \mathbb{N} : \text{There exists } n \in \mathbb{N} \text{ with } m = 5n + 4\}.$$

Thus, these parametric descriptions are not essentially new ways to describe sets, but they can often be more concise and clear.

By the way, we can use multiple parameters in our description. For example, consider the set

$$S = \{18m + 33n : m, n \in \mathbb{Z}\}.$$

Now we are simply letting m and n vary through all possible values in $\mathbb{Z}$ and collecting all of the values $18m + 33n$ that result. For example, we have $15 \in S$ because $15 = 18 \cdot (-1) + 33 \cdot 1$. We also have $102 \in S$ because $102 = 18 \cdot 2 + 33 \cdot 2$. Notice that we are varying m and n independently, so they might take different values, or the same value (as in the case of $m = n = 2$). Don't be fooled by the fact that we used different letters! As above, we can flip this description around by writing

$$S = \{k \in \mathbb{Z} : \text{There exists } m, n \in \mathbb{Z} \text{ with } k = 18m + 33n\}.$$

2.2 Subsets and Set Equality

Definition 2.2. *Given two sets A and B, we write $A \subseteq B$ to mean that every element of A is an element of B. More formally, $A \subseteq B$ means that for all x, if $x \in A$, then $x \in B$.*

Written more succinctly, $A \subseteq B$ means that for all $a \in A$, we have that $a \in B$. To prove that $A \subseteq B$, one takes a completely arbitrary $a \in A$, and argues that $a \in B$. For example, let $A = \{6n : n \in \mathbb{Z}\}$ and let $B = \{2n : n \in \mathbb{Z}\}$. Since both of these sets are infinite, we can't show that $A \subseteq B$ by taking each element of A in turn and showing that it is an element of B. Instead, we take an *arbitrary* $a \in A$, and show that $a \in B$. Here's the proof.

Proposition 2.3. *Let $A = \{6n : n \in \mathbb{Z}\}$ and $B = \{2n : n \in \mathbb{Z}\}$. We have $A \subseteq B$.*

Proof. Let $a \in A$ be arbitrary. By definition of A, this means that we can fix an $m \in \mathbb{Z}$ with $a = 6m$. Notice then that $a = 2 \cdot (3m)$. Since $3m \in \mathbb{Z}$, it follows that $a \in B$. Since $a \in A$ we arbitrary, we conclude that $A \subseteq B$. □

As usual, pause to make sure that you understand the logic of the argument above. First, we took an arbitrary element a from the set A. Now since $A = \{6n : n \in \mathbb{Z}\}$ and this is a parametric description with an implicit "there exists" quantifier, there must be one fixed integer value of n that puts a into the set A. In our proof, we chose to call that one fixed integer m. Now in order to show that $a \in B$, we need to exhibit a $k \in \mathbb{Z}$ with $a = 2k$. In order to do this, we hope to manipulate $a = 6m$ to introduce a 2, and ensure that the element we are multiplying by 2 is an integer.

What would go wrong if we tried to prove that $B \subseteq A$? Let's try it. Let $b \in B$ be arbitrary. Since $b \in B$, we can fix $m \in \mathbb{Z}$ with $b = 2m$. Now our goal is to try to prove that we can find an $n \in \mathbb{Z}$ with $b = 6n$. It's not obvious how to obtain a 6 from that 2, but we can try to force a 6 in the following way. Since $b = 2m$ and $2 = \frac{6}{3}$, we can write $b = 6 \cdot \frac{m}{3}$. We have indeed found a number n such that $b = 6n$, but we have not

checked that this n is an integer. In general, dividing an integer by 3 does not result in an integer, so this argument currently has a hole in it.

Although that argument has a problem, we can not immediately conclude that $B \not\subseteq A$. Our failure to find an argument does not mean that an argument does not exist. So how can we show that $B \not\subseteq A$? All that we need to do is find just *one example* of an element of B that is not an element of A (because the negation of the "for all" statement $A \subseteq B$ is a "there exists" statement). We choose 2 as our example. However, we need to convince everybody that this choice works. So let's do it! First, notice that $2 = 2 \cdot 1$, so $2 \in B$ because $1 \in \mathbb{Z}$. We now need to show that $2 \notin A$, and we'll do this using a proof by contradiction. Suppose instead that $2 \in A$. Then, by definition, we can fix an $m \in \mathbb{Z}$ with $2 = 6m$. We then have that $m = \frac{2}{6} = \frac{1}{3}$. However, this a contradiction because $\frac{1}{3} \notin \mathbb{Z}$. Since our assumption that $2 \in A$ led to a contradiction, we conclude that $2 \notin A$. We found an example of an element that is in B but not in A, so we conclude that $B \not\subseteq A$.

Recall that two sets A and B are defined to be equal if they have the same elements. Therefore, we have $A = B$ exactly when both $A \subseteq B$ and $B \subseteq A$ are true. Thus, given two sets A and B, we can prove that $A = B$ by performing two proofs like the one above. Such a strategy is called a *double containment* proof. We give an example of such an argument now.

Proposition 2.4. *Let $A = \{7n - 3 : n \in \mathbb{Z}\}$ and $B = \{7n + 11 : n \in \mathbb{Z}\}$. We have $A = B$.*

Proof. We prove that $A = B$ by showing that both $A \subseteq B$ and also that $B \subseteq A$.

- We first show that $A \subseteq B$. Let $a \in A$ be arbitrary. By definition of A, we can fix an $m \in \mathbb{Z}$ with $a = 7m - 3$. Notice that

$$\begin{aligned} a &= 7m - 3 \\ &= 7m - 14 + 11 \\ &= 7(m - 2) + 11. \end{aligned}$$

  Now $m - 2 \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so it follows that $a \in B$. Since $a \in A$ was arbitrary, we conclude that $A \subseteq B$.

- We now show that $B \subseteq A$. Let $b \in B$ be arbitrary. By definition of B, we can fix an $m \in \mathbb{Z}$ with $a = 7m + 11$. Notice that

$$\begin{aligned} a &= 7m + 11 \\ &= 7m + 14 - 3 \\ &= 7(m + 2) - 3. \end{aligned}$$

  Now $m + 2 \in \mathbb{Z}$ because $m \in \mathbb{Z}$, so it follows that $a \in B$. Since $a \in A$ was arbitrary, we conclude that $A \subseteq B$.

We have shown that both $A \subseteq B$ and $B \subseteq A$ are true, so it follows that $A = B$. □

Here is a more interesting example. Consider the set

$$S = \{9m + 15n : m, n \in \mathbb{Z}\}.$$

For example, we have $9 \in S$ because $9 = 9 \cdot 1 + 15 \cdot 0$. We also have $3 \in S$ because $3 = 9 \cdot 2 + 15 \cdot (-1)$ (or alternatively because $3 = 9 \cdot (-3) + 15 \cdot 2$). We can always generate new values of S by simply plugging in values for m and n, but is there another way to describe the elements of S in an easier way? We now show that an integer is in S exactly when it is a multiple of 3.

Proposition 2.5. *We have $\{9m + 15n : m, n \in \mathbb{Z}\} = \{3m : m \in \mathbb{Z}\}$.*

Proof. We give a double containment proof.

- We first show that $\{9m + 15n : m, n \in \mathbb{Z}\} \subseteq \{3m : m \in \mathbb{Z}\}$. Let $a \in \{9m + 15n : m, n \in \mathbb{Z}\}$ be arbitrary. By definition, we can fix $k, \ell \in \mathbb{Z}$ with $a = 9k + 15\ell$. Notice that

$$\begin{aligned} a &= 9k + 15\ell \\ &= 3 \cdot (3k + 5\ell). \end{aligned}$$

  Now $3k+5\ell \in \mathbb{Z}$ because $k, \ell \in \mathbb{Z}$, so it follows that $a \in \{3m : m \in \mathbb{Z}\}$. Since $a \in \{9m+15n : m, n \in \mathbb{Z}\}$ was arbitrary, we conclude that $\{9m + 15n : m, n \in \mathbb{Z}\} \subseteq \{3m : m \in \mathbb{Z}\}$.

- We now show that $\{3m : m \in \mathbb{Z}\} \subseteq \{9m + 15n : m, n \in \mathbb{Z}\}$. Let $a \in \{3m : m \in \mathbb{Z}\}$ be arbitrary. By definition, we can fix $k \in \mathbb{Z}$ with $a = 3k$. Notice that

$$\begin{aligned} a &= 3k \\ &= (9 \cdot (-3) + 15 \cdot 2) \cdot k \\ &= 9 \cdot (-3k) + 15 \cdot 2k. \end{aligned}$$

  Now $-3k, 2k \in \mathbb{Z}$ because $k \in \mathbb{Z}$, so it follows that $a \in \{9m+15n : m, n \in \mathbb{Z}\}$. Since $a \in \{3m : m \in \mathbb{Z}\}$ was arbitrary, we conclude that $\{3m : m \in \mathbb{Z}\} \subseteq \{9m + 15n : m, n \in \mathbb{Z}\}$.

We have shown that both $\{9m+15n : m, n \in \mathbb{Z}\} \subseteq \{3m : n \in \mathbb{Z}\}$ and $\{3m : m \in \mathbb{Z}\} \subseteq \{9m+15n : m, n \in \mathbb{Z}\}$ are true, so it follows that $\{9m + 15n : m, n \in \mathbb{Z}\} = \{3m : m \in \mathbb{Z}\}$. □

2.3 Ordered Pairs and Sequences

In contrast to sets, we define *ordered pairs* in such a way that order and repetition *do* matter. We denote an ordered pair using normal parentheses rather than curly braces. For example, we let $(2, 5)$ be the ordered pair whose first element is 2 and whose second element is 5. Notice that we have $(2, 5) \neq (5, 2)$ despite the fact that $\{2, 5\} = \{5, 2\}$. Make sure to keep a clear distinction between the ordered pair $(2, 5)$ and the set $\{2, 5\}$. We *do* allow the possibility of an ordered pair such as $(2, 2)$, and here the repetition of 2's is meaningful. Furthermore, we do not use $\in$ in ordered pairs, so we would **not** write $2 \in (2, 5)$. We'll talk about ways to refer to the two elements of an ordered pair later.

We can generalize ordered pairs to the possibility of having more than 2 elements. In this case, we have an ordered list of n elements, like $(5, 4, 5, -2)$. We call such an object an *n-tuple*, a *list* with n elements, or a finite *sequence* of length n. Thus, for example, we could call $(5, 4, 5, -2)$ a 4-tuple. It is also possible to have infinite sequences (i.e. infinite lists), but we will wait to discuss these when the time comes.

2.4 Operations on Sets

Aside from listing elements, carving out subsets of a known set using a certain property, and giving a parametric description (which as mentioned above is just a special case of the previous type), there are other ways to build sets by using certain set-theoretic operations.

Definition 2.6. *Given two sets A and B, we define $A \cup B$ to be the set consisting of those elements that are in A or B (or both). In other words, we have*

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

We call this set the union *of A and B.*

Here, as in mathematics generally, we use *or* to mean "inclusive or". In other words, if x is an element of both A and B, then we still put x into $A \cup B$. We give a few examples without proof:

- $\{1, 2, 7\} \cup \{4, 9\} = \{1, 2, 4, 7, 9\}$.
- $\{1, 2, 3\} \cup \{2, 3, 5\} = \{1, 2, 3, 5\}$.
- $\{2n : n \in \mathbb{Z}\} \cup \{2n + 1 : n \in \mathbb{Z}\} = \mathbb{Z}$. This is a restatement of Fact 1.6.
- $\{2n : n \in \mathbb{N}^+\} \cup \{2n + 1 : n \in \mathbb{N}^+\} = \{2, 3, 4, \dots\}$.
- $\{2n : n \in \mathbb{N}^+\} \cup \{2n - 1 : n \in \mathbb{N}^+\} = \{1, 2, 3, 4, \dots\} = \mathbb{N}^+$.
- $A \cup \emptyset = A$ for every set A.

Definition 2.7. *Given two sets A and B, we define $A \cap B$ to be the set consisting of those elements that are in both of A and B. In other words, we have*

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

We call this set the intersection *of A and B.*

Here are a few examples, again without proof:

- $\{1, 2, 7\} \cap \{4, 9\} = \emptyset$.
- $\{1, 2, 3\} \cap \{2, 3, 5\} = \{2, 3\}$.
- $\{1, \{2, 3\}\} \cap \{1, 2, 3\} = \{1\}$.
- $\{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\} = \{6n : n \in \mathbb{Z}\}$.
- $\{3n + 1 : n \in \mathbb{N}^+\} \cap \{3n + 2 : n \in \mathbb{N}^+\} = \emptyset$.
- $A \cap \emptyset = \emptyset$ for every set A.

Definition 2.8. *We say that two sets A and B are* disjoint *if $A \cap B = \emptyset$.*

Definition 2.9. *Given two sets A and B, we define*

$$A \backslash B = \{x : x \in A \text{ and } x \notin B\}$$

and call this set the (relative) complement *of B (in A).*

In many cases where we consider $A \backslash B$, we will have that $B \subseteq A$, but we will occasionally use it even when $B \not\subseteq A$. Here are a few examples:

- $\{5, 6, 7, 8, 9\} \backslash \{5, 6, 8\} = \{7, 9\}$.
- $\{1, 2, 7\} \backslash \{4, 9\} = \{1, 2, 7\}$.
- $\{1, 2, 3\} \backslash \{2, 3, 5\} = \{1\}$.
- $\{2n : n \in \mathbb{Z}\} \backslash \{4n : n \in \mathbb{Z}\} = \{4n + 2 : n \in \mathbb{Z}\}$.
- $A \backslash \emptyset = A$ for every set A.
- $A \backslash A = \emptyset$ for every set A.

Definition 2.10. *Given two sets A and B, we let $A \times B$ be the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$, and we call this set the* Cartesian product *of A and B.*

For example, we have

$$\{1,2,3\} \times \{6,8\} = \{(1,6),(1,8),(2,6),(2,8),(3,6),(3,8)\}$$

and

$$\mathbb{N} \times \mathbb{N} = \{(0,0),(0,1),(1,0),(2,0),\ldots,(4,7),\ldots\}.$$

Notice that elements of $\mathbb{R} \times \mathbb{R}$ correspond to points in the plane.

We can also generalize the concept of a Cartesian product to more than 2 sets. If we are given n sets $A_1, A_2, \ldots, A_n$, we let $A_1 \times A_2 \times \cdots \times A_n$ be the set of all n-tuples $(a_1, a_2, \ldots, a_n)$ such that $a_i \in A_i$ for each i. For example, we have

$$\{1,2\} \times \{3\} \times \{4,5\} = \{(1,3,4),(1,3,5),(2,3,4),(2,3,5)\}.$$

In the special case when $A_1, A_2, \ldots, A_n$ are all the same set A, we use the notation A^n to denote the set $A \times A \times \cdots \times A$ (where we have n copies of A). Thus, A^n is the set of all finite sequences of elements of A of length n. For example, $\{0,1\}^n$ is the set of all finite sequences of 0's and 1's of length n.

Definition 2.11. *Given a set A, we let A^* be the set of all finite sequences of elements of A of any length, including the empty sequence (the unique sequence of length 0).*

Thus, for example, the set $\{0,1\}^*$ is the set of all finite sequences of 0's and 1's. If we use λ to denote the empty sequence and write things like 010 in place of the more precise $(0,1,0)$, then we have

$$\{0,1\}^* = \{\lambda, 0, 1, 00, 01, 10, 11, 000, 001, \ldots\}$$

Notice that if $A \neq \emptyset$, then A^* is an infinite set.

Definition 2.12. *Given two finite sequences σ and τ, we let $\sigma\tau$ be the* concatenation *of σ and τ, i.e. if $\sigma = (a_1, a_2, \ldots, a_m)$ and $\tau = (b_1, b_2, \ldots, b_n)$, then $\sigma\tau = (a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n)$.*