Math 8 Instructor: Padraic Bartlett

Lecture 2: Exploring $\mathbb{Q}$ and $\mathbb{R}$

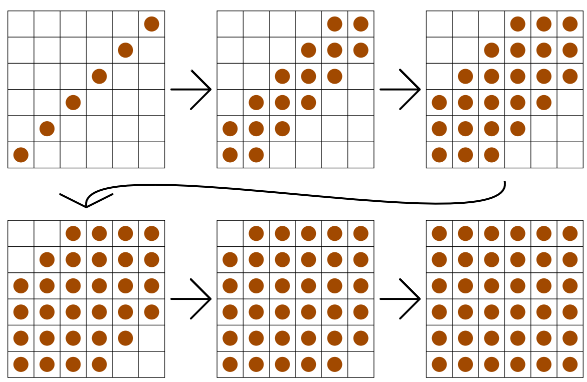
Week 2 *Caltech - Fall, 2011*

1 Random Questions

Question 1. Can you cover a 10×10 chessboard with 4×1 dominoes?

Question 2. Consider the following game you can play on a $n \times n$ board made of 1×1 squares:

1. To start, mark some of the squares on the board as "infected."
2. If a square shares edges with at least two infected squares, mark it as infected as well.
3. Repeat (2) until no more squares are ever marked.



How many squares do you need to infect at the start to insure that the whole board is eventually infected? Can you prove that your number is the smallest number needed?

Question 3. Can you find a collection of disjoint circles with positive radius in $\mathbb{R}^3$, such that every point in $\mathbb{R}^3$ is contained in some circle? (Hint: you cannot do this to $\mathbb{R}^2$! Try showing this first.)

2 Exploring $\mathbb{Q}$ and $\mathbb{R}$

In this week's set of lectures, we explore the **rational** and **real** numbers in three talks. In the first, we will explore **fields**, a class of objects which both $\mathbb{R}$ and $\mathbb{Q}$ are examples of. In the second talk, we will distinguish $\mathbb{R}$ and $\mathbb{Q}$ from other fields and from each other with the new concept of **orderings**; using this idea, we'll explore some key differences between $\mathbb{R}$ and $\mathbb{Q}$, and show that (in a certain sense) these two objects are remarkably intertwined with each other. Finally, in our third lecture, we will study $\mathbb{R}$ and $\mathbb{Q}$ simply as **sets**; specifically, we will introduce the idea of different "sizes" of infinity in a rigorous sense, and use this to study whether $\mathbb{R}$ and $\mathbb{Q}$ are the "same size."

2.1 The Concept of Fields

The concept of **generalization** is central to pretty much everything in mathematics. Whenever a mathematician comes across a useful object, one of her instincts is almost always to take it apart and find out just **why** it is useful!

By way of example, think about the real number system ($\mathbb{R}$) and the rational number system ($\mathbb{Q}$.) Both of these sets are, in some well-defined way, rather "nice" when it comes to performing arithmetic on them: given any pair of real or rational numbers, we can add or multiply them together, divide one by the other if the denominator is nonzero, switch the order of adding or multiplying things around, and do a number of other things. As mathematicians, we are then drawn to attempt to "generalize" just what it is that makes arithmetic so nice in $\mathbb{R}$ and $\mathbb{Q}$: doing this leads you to the following six rules that both $\mathbb{R}$ and $\mathbb{Q}$ obey, called the **field axioms**:

Definition 2.1. Let $\mathcal{F}$ be a set, together with a pair of operations $+, \cdot$ that tell us how[1] to multiply and add elements in $\mathcal{F}$. Then we call $\mathcal{F}$ a **field** if and only if it satisfies the following six rules:

1. **Closure**: For any x, y in $\mathbb{R}$, $x + y$ and $x \cdot y$ are also in $\mathbb{R}$.
2. **Identity**: There are elements $0, 1$ in $\mathbb{R}$, $0 \neq 1$, such that $0 + x = x$ and $1 \cdot x = x$, for any $x \in \mathbb{R}$.
3. **Inverse**: For any $x \in \mathbb{R}, x \neq 0$, there are elements $-x, x^{-1}$ in $\mathbb{R}$ such that $x + (-x) = 0$ and $x \cdot x^{-1} = 1$.
4. **Associativity**: For any $x, y, z \in \mathbb{R}$, $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
5. **Commutativity**: For any $x, y \in \mathbb{R}$, $x + y = y + x$ and $x \cdot y = y \cdot x$.
6. **Distributivity**: For any $x, y, z \in \mathbb{R}$, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Both $\mathbb{R}$ and $\mathbb{Q}$ satisfy these six rules; we omit the proofs here because of time constraints, in favor of getting to some stranger examples. Before we do that, though, it bears noting that there are many sets with addition and multiplication defined on them that are **not** fields – i.e. they aren't well-defined in the way that $\mathbb{R}$ and $\mathbb{Q}$ are! Some examples of things that are not fields are listed below:

1. $\mathbb{N}$. This is because many elements in $\mathbb{N}$ don't have an additive inverse in $\mathbb{N}$. For example, there is no natural number n such that $n + 1 = 0$.
2. $\mathbb{Z}$. This is because many elements in $\mathbb{Z}$ don't have an multiplicative inverse in $\mathbb{Z}$. For example, there is no integer x such that $x \cdot 2 = 1$.

[1] Formally, think of $+$ and $\cdot$ as functions from $\mathcal{F}^2$ to $\mathcal{F}$: i.e. functions that take in any pair of elements a, b in $\mathcal{F}$ and output some other element $a + b, a \cdot b$ in $\mathcal{F}$, which we call the sum or product (respectively) of a and b.

3. The collection of all 2×2 matrices with real entries. This is because multiplication of matrices is (in general) noncommutative: for example,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

while

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

One thing you might have noticed about $\mathbb{R}$ and $\mathbb{Q}$ is that they satisfy a number of things that aren't directly implied by the field axioms! For example, we know that for any number $a \in \mathbb{R}$ or $\mathbb{Q}$, we always have

$$a \cdot 0 = 0.$$

Yet, this property isn't in our axioms above. A natural question to ask, then, is the following: are there fields in which $a \cdot 0 \neq 0$?

Thankfully, there aren't! – as it turns out, the six field axioms above are enough to insure that addition and multiplication are well-behaved in *any* field, and in specific that weird things like $a \cdot 0 \neq 0$ don't happen! We prove this here:

Theorem 4. In any field $\mathcal{F}$, we have $a \cdot 0 = 0$ for any $a \in \mathcal{F}$.

Proof. Pick any $a \in \mathcal{F}$, and examine the quantity $0 \cdot \mathcal{F}$. Because of closure, this is an element of $\mathcal{F}$.

We know that 0 is the additive identity, so we can write $0 = (0 + 0)$. By substituting this in for 0 in our expression $0 \cdot \mathcal{F}$, we've just shown that

$$0 \cdot a = (0 + 0) \cdot a.$$

Applying distributivity then tells us that

$$0 \cdot a = 0 \cdot a + 0 \cdot a.$$

Because $0 \cdot a$ is an element of $\mathcal{F}$, it has an additive inverse $-(0 \cdot a)$. Adding this inverse to both sides gives us

$$-(0 \cdot)a + 0 \cdot a = -(0 \cdot a + (0 \cdot a + 0 \cdot a).$$

Applying associativity to the right hand side gives us

$$-(0 \cdot a) + 0 \cdot a = (-(0 \cdot a) + 0 \cdot a) + 0 \cdot a,$$

and applying the definition of additive inverses gives us

$$0 = 0 + 0 \cdot a.$$

Finally, using that 0 is an additive identity on the right hand side tells us that

$$0 = 0 \cdot a,$$

which is what we wanted to prove. ☐

Another property that both $\mathbb{R}$ and $\mathbb{Q}$ have is that they are both **infinite** sets. Is this also a necessary property of fields?

Perhaps surprisingly enough, the answer is no! We prove this here:

Theorem 2.2. *There are fields $\mathcal{F}, +, \cdot$ with finitely many elements.*

Proof. We need to start somewhere: so, let's try to make the *smallest* field possible. How many elements do we need? Well, we know (by the axioms of identity) that our field must contain at least two elements: 0 and 1, with $0 \neq 1$. Do we need any more elements?

Well, let's try to make multiplication and addition tables with just these two:

+	0	1
0	0	1
1	1	$\square$

$\cdot$	0	1
0	$\diamond_1$	$\diamond_2$
1	$\diamond_2$	1

The axioms of identity force all of the filled-in entries, with the exception of $1+1$ and 0 times anything. We just proved that multiplying anything with 0 yields 0, however: so all of the $\diamond$ symbols must be 0. This just leaves $1+1$: what should this be?

Well: as mathematicians, remember that we are **lazy** wherever we can be. Specifically: to decide what $1+1$ is, the easiest option for us is to use one of the two symbols we have: 0 or 1. But wait! – we know (by the axiom of additive inverse) that there has to be some element to add to 1 to get 0. As $0+1=1\neq 0$, we know that 0 cannot be that element – so 1 must be its own additive inverse, if we're only using 0 and 1! In other words, we can set $1+1=0$, and get the addition/multiplication tables below:

+	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Check the axioms: this is a field! Specifically, this is the field acquired by using **addition mod[2] 2**: in other words, this is the field you get by taking the numbers 0 and 1, adding/multiplying them, and then looking at the remainders after multiplying by 2. Inspired by this observation, we call this field $\mathbb{Z}/2\mathbb{Z}$, and ask ourselves the following natural question: was there something special about 2, or can this work for general n?

Well: let's look at $n=3$. In this case, our set would be the three possible remainders after dividing an integer by 3 – $\{0,1,2\}$ – and our addition/multiplication tables would come from using our normal operations and then taking everything mod 3:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Checking the axioms, this is again a field!

[2]Recall: we write that $a \equiv b \mod c$ iff $a-b$ is a multiple of c: in other words, that a and b are the "same" up to some number of copies of c.

That's encouraging: what about $n = 4$? As before, our set is just $\{0, 1, 2, 3\}$, and our tables are

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tragically, in this case, we don't satisfy all of our axioms: specifically, there is no multiplicative inverse for 2. ☐

So: finite fields exist! In particular, it is not too hard to adapt the arguments above to prove the following theorem:

Theorem 5. $\mathbb{Z}/p\mathbb{Z}$ is a field, for any prime p.

We omit the proof here: find me if you'd like to see how it's done!

It also bears noting that while we showed that $\mathbb{Z}/4\mathbb{Z}$ is not a field, this does not mean that there aren't fields of size 4! In fact, these fields exist:

Theorem 6. There are fields of size p^k, for any prime p and any natural number $k \geq 1$.

The proof of this theorem is far beyond the scope of our course; interested students should come and talk to me for some pointers on where to begin attacking this problem!

2.2 Other Structures on $\mathbb{R}$ and $\mathbb{Q}$: Orderings

As demonstrated above, both $\mathbb{R}$ and $\mathbb{Q}$ are alike in that they are both fields. However, we know that these two sets have more structure than just $+$ and $\cdot$: given any two real numbers, for example, we can also determine which of them is **greater** than the other! This motivates us to introduce the idea of "orderings", which (loosely speaking) are ways of defining "less than" for an entire set. Both $\mathbb{R}$ and $\mathbb{Q}$ have a very special type of ordering, called a **total ordering**, that we define here:

Definition 2.3. Given a set S, a **total ordering** on the set S is a binary relation[3] $<$ that satisfies the following properties:

1. **Antireflexivity**: For any x, $x \not< x$.
2. **Antisymmetry**: For any distinct x, y, either $x < y$ or $y < x$: you can never have both of these statements be true or both be false.
3. **Transitivity**: For any distinct x, y, z such that $x < y$ and $y < z$, we have $x < z$.

In addition, both $\mathbb{R}$ and $\mathbb{Q}$ satisfy a property known as the Archimedean property:

Proposition 2.4. *For any $x > 0, y > 0$, there is some $n \in \mathbb{N}$ such that $nx > y$.*

[3] A **binary relation** on a set is just a function that takes in any pair of elements in the set, and returns true or false. For example, $<$ in the real numbers is a binary relation: $2 < 3$ returns true, while $3 < 2$ returns false.

If you divide through by ny, this statement is equivalent to the claim that for any $x > 0, y > 0$ there is a value of n such that $\frac{1}{n} < \frac{x}{y}$. Because picking both x and y to be > 0 is equivalent to just picking the number $x/y > 0$, we can see that the Archimedean property is equivalent to the following claim:

Proposition 2.5. *For any $x > 0$, there is some $n \in \mathbb{N}$ such that $\frac{1}{n} < x$.*

These two properties are completely equivalent, as we showed above! – in other words, any set that satisfies one of them must satisfy the other. The difference between the two, then, is entirely in the emphasis. In the first wording, the idea that's being conveyed is that for any ridiculously large y and any x, we can eventually find a n such that $nx > y$: in other words, that enough copies of **any** positive number will eventually get to be arbitrarily large. In the second wording, instead of talking about arbitrarily *big* numbers, we're talking about arbitrarily *small* ones: in other words, we're saying that no matter how small of a positive number you pick, there is some value of n such that $\frac{1}{n}$ is smaller. Again, these two propositions are the exact same thing! – they're just different ways of looking at the same problem.

To illustrate the use of this property, consider the following theorem:

Theorem 2.6. *For any $x, y \in \mathbb{R}$ such that $x < y$, there is a element $z \in \mathbb{Q}$ such that $x < z < y$.*

Proof. Look at the quantity $y - x$. By the second formulation of the Archimedean property, there is some $n \in \mathbb{N}$ such that $\frac{1}{n} < y - x$. By the *first* formulation of the Archimedean property, there is some m such that $\frac{m}{n} > y$. Pick m so that it is the smallest integer such that $\frac{m}{n} \geq y$.

We prove our claimed inequality in two parts. First, we start by proving

$$\frac{m-1}{n} < y.$$

To see why this is true, recall how we picked m: we chose m to be the smallest integer where $\frac{m}{n} \geq y$. So, by definition, we know that $\frac{m-1}{n} < y$, because $m - 1$ is a smaller integer than m.

So, the only thing we have to prove is that

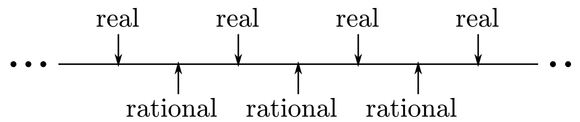
$$x < \frac{m-1}{n}$$

To do this, we simply combine the inequalities $y < \frac{m}{n}$ and $\frac{1}{n} < y - x$:

$$\begin{aligned} y &\leq \frac{m}{n} \\ \Rightarrow y - \frac{1}{n} &\leq \frac{m-1}{n} \\ \Rightarrow y - (y - x) &\leq \frac{m-1}{n} \\ \Rightarrow x &\leq \frac{m-1}{n}. \end{aligned}$$

This finishes our proof. ☐

What have we just proven? Essentially, we've shown that the real line looks like the following picture:



In other words, we've shown that that between any two real numbers, there is a rational number: i.e. the reals and rationals are "intertwined."

2.3 Sizes of Infinity

On one hand, we know that the real numbers contain "more" elements than the rational numbers: things like $\sqrt{2}$ are in $\mathbb{R}$ but not in $\mathbb{Q}$, for example. On the other hand, our "interleaving" result above seems to suggest that the sizes of these two sets might be somewhat similar: after all, if between any two real numbers there's a rational, how many "more" reals could you have?

In this section, we discuss how we can come up with a rigorous way of studying the above question. Let's start with the most basic thing we can ask: what does it mean for two sets to be the same size? In the finite case, this question is rather trivial; for example, we know that the two sets

$$A = \{1, 2, 3\}, \qquad\qquad B = \{A, B, \text{emu}\}$$

are the same size because they both have the same *number* of elements – in this case, 3.

But what about infinite sets? For example, look at the sets

$$\mathbb{N}, \qquad \mathbb{Q}, \qquad \mathbb{R}, \qquad \mathbb{C};$$

are any of these sets the same size? Are any of them larger? By how much?

In the infinite case, the tools we used for the finite – counting up all of the elements – don't work. In response to this, we are motivated to try to find another way to count: in this case, one that involves **functions**.

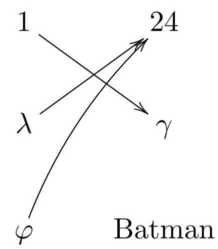
3 Functions (formally defined)

Definition 3.1. A **function** f with domain A and range B, formally speaking, is a collection of pairs (a, b), with $a \in A$ and $b \in B$, such that there is exactly one pair (a, b) for every $a \in A$. More informally, a function $f : A \to B$ is just a map which takes each element in A to some element of B.

Examples 3.2.

- $f : \mathbb{Z} \to \mathbb{N}$ given by $f(n) = 2|n| + 1$ is a function.
- $g : \mathbb{N} \to \mathbb{N}$ given by $f(n) = 2|n| + 1$ is a function; in fact, it is a different function, because it has a different domain!

- The function h depicted below by the three arrows is a function, with domain $\{1, \lambda, \varphi\}$ and range $\{24, \gamma, \text{ Batman}\}$:

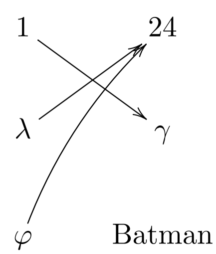


This may seem like a silly example, but it's illustrative of one key concept: functions are just **maps between sets!** Often, people fall into the trap of assuming that functions have to have some nice "closed form" like $x^3 - \sin(x)$ or something, but that's not true! Often, functions are either defined piecewise, or have special cases, or are generally fairly ugly/awful things; in these cases, the best way to think of them is just as a collection of arrows from one set to another, like we just did above.

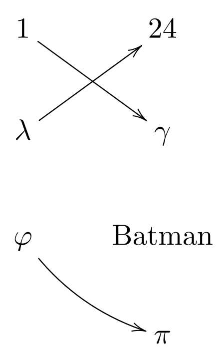
Now that we've formally defined functions and have a grasp on them, let's introduce a pair of definitions that will help us with our question of "size:"

Definition 3.3. We call a function f **injective** if it never hits the same point twice – i.e. for every $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$.

Example 3.4. The function h from before is not injective, as it sends both λ and φ to 24:



However, if we add a new element π to our range, and make φ map to π, our function is now injective, as no two elements in the domain are sent to the same place:



One observation we can quickly make about injective functions is the following:

Proposition 3.5. *If $f : A \to B$ is an injective function and A, B are finite sets , then size(A) $\leq$size(B). (Formally, we write $|A| \leq |B|$, and use the vertical brackets around a set to denote its size.)*

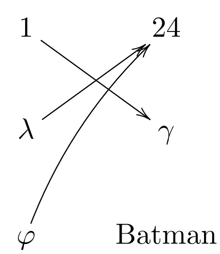
The reasoning for this, in the finite case, is relatively simple:

1. If f is injective, then each element in A is being sent to a different element in B.
2. Thus, you'll need B to have at least $|A|$-many elements to provide that many targets.

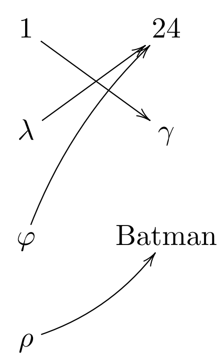
A converse concept to the idea of injectivity is that of **surjectivity**, as defined below:

Definition 3.6. We call a function f **surjective** if it hits every single point in its range – i.e. if for every $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$.

Example 3.7. The function h from before is not injective, as it doesn't send anything to Batman:



However, if we add a new element ρ to our domain, and make ρ map to Batman, our function is now surjective, as it hits all of the elements in its range:



As we did earlier, we can make one quick observation about what surjective functions imply about the size of their domains and ranges:

Proposition 3.8. *If $f : A \to B$ is an surjective function and A, B are finite sets , then $|A| \geq |B|$.*

Basically, this holds true because

1. Thinking about f as a collection of arrows from A to B, it has precisely $|A|$-many arrows by definition, as each element in A gets to go to precisely one place in B.

2. Thus, if we have to hit every element in B, and we start with only $|A|$-many arrows, we need to have $|A| \geq |B|$ in order to hit everything.

So: in the finite case, if $f : A \to B$ is injective, it means that $|A| \leq |B|$, and if f is surjective, it means that $|A| \geq |B|$. This motivates the following definition and observation:

Definition 3.9. We call a function **bijective** if it is both injective and surjective.

Proposition 3.10. *If $f : A \to B$ is an bijective function and A, B are finite sets , then $|A| = |B|$.*

Unlike our earlier idea of counting, this process of "finding a bijection" seems like something we can do with any sets – not just finite ones! As a consequence, we are motivated to make this our **definition** of size! In other words, we have the following definition:

Definition 3.11. We say that two sets A, B are the same size (formally, we say that they are of the same **cardinality**,) and write $|A| = |B|$, if and only if there is a bijection $f : A \to B$.

4 Sizes of Infinity: The Natural Numbers

Armed with a definition of size that can actually deal with infinite sets, let's start with some calculations to build our intuition:

Question 4.1. *Are the sets $\mathbb{N}$ and $\mathbb{N} \cup \{lemur\}$ the same size?*

Answer. Well: we know that they can be the same size if and only if there is a bijection between one and the other. So: let's try to make a bijection! In the typed notes, the suspense is somewhat gone, but (at home) imagine yourself taking a piece of paper, and writing out the first few elements of $\mathbb{N}$ on one side and of $\mathbb{N} \cup \{\text{lemur}\}$ on the other side. After some experimentation, you might eventually find yourself with the following map:

$$\begin{array}{ccc} \boxed{\mathbb{N}} & & \boxed{\mathbb{N} \cup \{\text{lemur}\}} \\ 1 & \longrightarrow & \text{lemur} \\ 2 & \longrightarrow & 1 \\ 3 & \longrightarrow & 2 \\ 4 & \longrightarrow & 3 \\ 5 & \longrightarrow & 4 \\ 6 & \longrightarrow & 5 \\ \vdots & & \vdots \end{array}$$

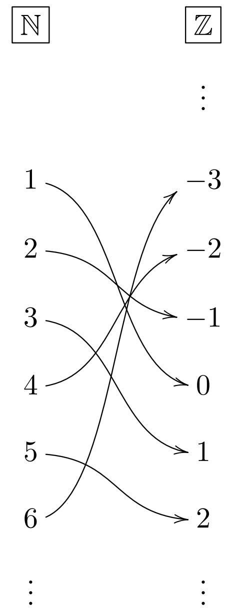
i.e. the map which sends 1 to the lemur and sends $n \to n - 1$, for all $n \geq 2$. This is clearly a bijection; so these sets are the same size!

In a rather crude way, we have shown that adding one more element to a set as "infinitely large" as the natural numbers doesn't do anything to it! – the extra element just gets lost amongst all of the others.

This trick worked for one additional element. Can it work for infinitely many? Consider the next proposition:

Proposition 4.2. *The sets $\mathbb{N}$ and $\mathbb{Z}$ are the same cardinality.*

Proof. Consider the following map:



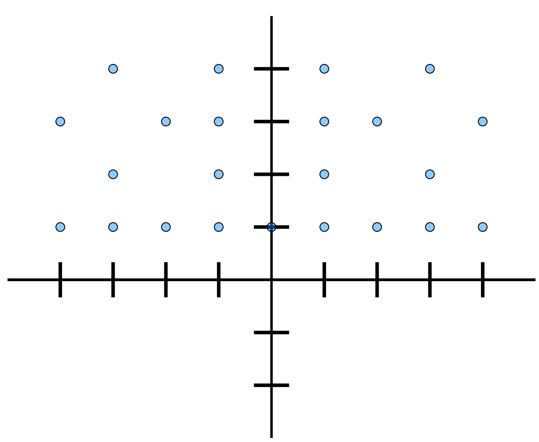
i.e. the map which sends $n \to (n-1)/2$ if n is odd, and $n \to -n/2$ if n is even. This, again, is clearly a bijection; so these sets are the same cardinality. □

So: we can in some sense "double" infinity! Strange, right? Yet, if you think about it for a while, it kind of makes sense: after all, don't the natural numbers contain two copies of themselves (i.e.the even and odd numbers?) And isn't that observation just what we used to turn $\mathbb{N}$ into $\mathbb{Z}$?

After these last two results, you might be beginning to feel like all of our infinite sets are the same size. In that case, the next result will hardly surprise you:

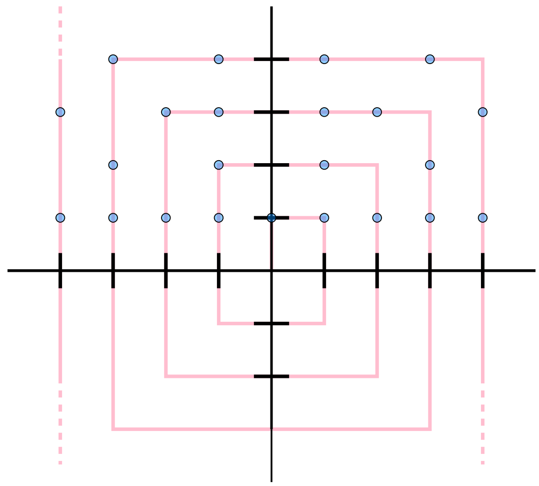
Proposition 4.3. *The sets $\mathbb{N}$ and $\mathbb{Q}$ are the same cardinality.*

Proof. First, take every rational number p/q with $GCD(p, q) = 1$, $p > 0$, and draw a point at (p, q) in the integer lattice $\mathbb{Z}^2$:



In the picture on the previous page, every rational number has exactly one unique representative by one of our blue dots.

Now, on this picture, draw a spiral that starts at $(0, 0)$ and goes through every point of $\mathbb{Z} \times \mathbb{Z}$, as depicted below:



We use this spiral to define our bijection from $\mathbb{N}$ to $\mathbb{Q}$ as follows:

$f(n)$ = *the n-th rational point found by starting at (0,0) and walking along the depicted spiral pattern.*

This function hits every rational number exactly once by construction; thus, it is a bijection from $\mathbb{N}$ to $\mathbb{Q}$. Consequently, $\mathbb{N}$ and $\mathbb{Q}$ are the same size. □

So: we've shown that $\mathbb{N}$ is the same size as $\mathbb{Q}$, the rationals! Before we ask if $\mathbb{N}$ the same size as $\mathbb{R}$, let's study just one more set:

Definition 4.4. A real number r is called **algebraic** if and only if there is some degree n and integer constants $a_0, \ldots a_n$ such that r is a root of the following polynomial:

$$a + 0 + a_1 x + \ldots + a_n x^n.$$

Most numbers you know are algebraic: for example, all of $\mathbb{Q}$ is (they're roots of the polynomial $qx - p$), as is $\sqrt{2}$ (it's a root of $x^2 - 2$) and most other things. Numbers that are not algebraic are called **transcendental**: examples include e and π. In general, showing that a number is transcendental is remarkably difficult: proofs that e and pi are transcendental are remarkably complicated, and take a ridiculous amount of effort. We know very little about the transcendental numbers as compared to the algebraic numbers: for example, it is currently unknown whether $e + \pi$ or $e \cdot \pi$ are transcendental numbers or not.

Theorem 7. $\mathbb{N}$ has the same cardinality as $\mathcal{A}$, the collection of all algebraic numbers.

Proof. For every algebraic number r, there is a polynomial $a_0 + a_1 x + \ldots a_n x^n$ such that r is the k-th root of this polynomial, for some $1 \leq k \leq n$ and some way of ordering the roots of this polynomial.

Therefore, we can uniquely identify every algebraic number by its polynomial, degree, and which root it is: in other words, the map

$$r \mapsto (n, a_0, a_1, \dots a_n, k)$$

uniquely assigns to every algebraic number a distinct sequence of integers.

Now, notice that we can map each of these numbers to a unique rational number. To be explicit, consider the following map that takes in a collection of integers and outputs a number written in base 11 (i.e. with digits $\{0, 1, 2, \dots 9, A\}$) by writing down each $n, a_0, \dots a_n, k$ in base 10 and separating the distinct entries with the 11-th digit A (which we use as a placeholder so we can keep our numbers separate:)

$$(n, a_0, a_1, \dots a_n, k) \mapsto .nAa_0Aa_1Aa_2Aa_3 \dots a_{n-1}Aa_nAk$$

By combining these two maps, we have a way of assigning each algebraic number to a unique rational number. Now, simply plot the rational points hit by this assignment map on the integer lattice $\mathbb{Z}^2$ like we did before, and use the spiral map to make a bijection from $\mathbb{N}$ to these rational points. Combining this with our map (described above) to turn these special rational points into algebraic numbers then gives us our bijection, as claimed. □

So: at this point, it almost seems inevitable that **every** infinte set will wind up having the same size! Well: not quite.

Theorem 4.5. *The sets $\mathbb{N}$ and $\mathbb{R}$ have different cardinalities.*

Proof. (This is Cantor's famous diagonalization argument.) Suppose not – that they were the same cardinalities. As a result, there is a bijection between these two sets! Pick such a bijection $f : \mathbb{N} \to \mathbb{R}$.

For every $n \in \mathbb{N}$, look at the number $f(n)$. It has a decimal representation. Pick a number $a_{n,\text{trash}}$ corresponding to the integer part of $f(n)$, and $a_{n,1}, a_{n,2}, a_{n,3}, \dots$ that correspond to the digits after the decimal place of this decimal representation – i.e. pick numbers $a_{n,i}$ such that

$$f(n) = a_{n,\text{trash}}.a_{n,1}a_{n,2}a_{n,3}\dots$$

For example, if $f(4) = 31.125$, we would pick $a_{4,\text{trash}} = 31, a_{4,1} = 1, a_{4,2} = 2, a_{4,3} = 5$, and $0 = a_{4,4} = a_{4,5} = a_{4,6} = \dots$, because the integer part of $f(4)$ is 31, its first three digits after the decimal place are 1,2, and 5, and the rest of them are zeroes.

Now, get rid of the $a_{n,\text{trash}}$ parts, and write the rest of these numbers in a table, as below:

$f(1)$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$\dots$
$f(2)$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	
$f(3)$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	
$f(4)$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$	$a_{4,4}$	
$\vdots$	$\vdots$				$\ddots$

In particular, look at the entries $a_{1,1}a_{2,2}a_{3,3}\dots$ on the diagonal. We define a number B using these digits as follows:

- Define $b_i = 2$ if $a_{i,i} \neq 2$, and $b_i = 8$ if $a_{i,i} = 2$.
- Define B to the be the number with digits given by the b_i – i.e.

$$B = .b_1 b_2 b_3 b_4 \ldots$$

Because B has a decimal representation, it's a real number! So, because our function f is a bijection, it must have some value of n such that $f(n) = B$. But the n-th digit of $f(n)$ is $a_{n,n}$ by construction, and the n-th digit of B is b_n – by construction, these are different numbers! So $f(n) \neq B$, because they disagree at their n-th decimal place!

This is a contradiction to our original assumption that such a bijection existed. Therefore, we know that no such bijection can exist: as a result, we've shown that the natural numbers are of a strictly "smaller" size of infinity than the real numbers. □

Crazy.