Math 127: Infinite Cardinality

Mary Radcliffe

1 Definitions

Recall that when we defined finiteness, we used the notion of bijection to define the size of a finite set. In particular, we defined a finite set to be of size n if and only if it is in bijection with $[n]$.

For infinite sets, this strategy doesn't quite work. What set do we take to biject to in order to define infinity? It's not immediately clear that there is a "canonical" set we can use for the definition. So instead, we use a definition for infinite sets based on what was a theorem in the world of finite sets.

Definition 1. Let X and Y be infinite sets. We say that $|X| = |Y|$ if there exists a bijection $f : X \to Y$.

We say a set X is *countably infinite* if $|X| = |\mathbb{N}|$. If X is infinite, but it is not countably infinite, we say that X is *uncountably infinite*, or just *uncountable*.

A set X is called *countable* if it is either finite or countably infinite.

It can be a bit confusing that the word *countable* does not imply countably infinite. In general, you can think of *countable* as really meaning that a set is *enumerable*. We saw in lecture that when talking about finite sets, we have the following:

Proposition 1. A set X is finite if and only if the elements of X can be enumerated in a terminating list as $X = \{x_1, x_2, \dots, x_n\}$.

For countably infinite sets, we have a similar structure:

Proposition 2. A set X is countably infinite if and only if the elements of X can be enumerated in an interminable list as $X = \{x_1, x_2, x_3, \dots\}$.

The proof of this proposition is immediate from the definition: if X is countably infinite, then there exists a bijection $f : \mathbb{N} \to X$, which immediately provides a way to enumerate the elements of X, taking $x_i = f(i)$.

Hence, we can think of the word "countable" as really being about enumeration. A set is countable if it can be enumerated, regardless of if the enumeration terminates.

Example 1. $\mathbb{Z}$ is countable.
Actually, you've already proven this, even though you may not have realized it. In Homework 6, problem 15, you saw the following function $f : \mathbb{N} \to \mathbb{Z}$

$$f(x) = \begin{cases} \frac{x}{2} & x \text{ is even} \\ -\frac{x-1}{2} & x \text{ is odd} \end{cases}.$$

You proved in that homework exercise that f is a bijection. That means that we have a bijection

from $\mathbb{N}$ to $\mathbb{Z}$, and therefore by definition $\mathbb{Z}$ is countably infinite.
Another way to approach this, of course, is to attempt to enumerate (aka, list) the elements of $\mathbb{Z}$. Certainly we can list the elements of $\mathbb{Z}$; there are many ways to do so. Here is one:

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \dots\}.$$

The fact that $\mathbb{Z}$ is the same size as $\mathbb{N}$ may be a bit surprising. Indeed, $\mathbb{N}$ is a proper subset of $\mathbb{Z}$, and in fact there are infinitely many elements of $\mathbb{Z}$ that are not a part of $\mathbb{N}$. Nevertheless, they are the same size! We will find this happens a lot in the world of infinity.

2 Countable Infinity

Here, let's consider how our favorite set operations and functions interact with countable sets. We begin with a characterization of countability:

Theorem 1. *Let X be a nonempty set. The following are equivalent:*

1. *X is countable.*
2. *There exists a surjection $f : \mathbb{N} \to X$.*
3. *There exists an injection $g : X \to \mathbb{N}$.*

Before we write the proof, a quick word on the phrasing "the following are equivalent," which is sometimes abbreviated as TFAE. This construction is a short hand for saying "there is an if and only if between each of the following statements." Here, if we think of the three statements as propositions p_1, p_2, p_3, the theorem is stating $p_1 \Leftrightarrow p_2 \Leftrightarrow p_3$.

In proving TFAE type theorems, it's common to prove a cycle of implications. That is, instead of proving $p_1 \Leftrightarrow p_2$, and also $p_2 \Leftrightarrow p_3$, and also $p_1 \Leftrightarrow p_3$, we would prove the shorter set of statements $p_1 \Rightarrow p_2$, and $p_2 \Rightarrow p_3$, and $p_3 \Rightarrow p_1$. These three implications are sufficient to get all parts of the if and only ifs on the three propositions, since if we start from any one proposition we can follow a series of implications to any other.

That being said, let's prove Theorem 1.

Proof. Let X be a nonempty set.

$(1 \Rightarrow 2)$ Suppose that X is countable. We wish to show that there exists a surjection $f : \mathbb{N} \to X$. We consider two cases, according as whether X is finite.

Case 1: X is finite. Then for some $n \in \mathbb{N}$, there exists a bijection $h : [n] \to X$. Let $x_0 \in X$ be some element of X. Define $f : \mathbb{N} \to X$ by

$$f(k) = \begin{cases} h(k) & 1 \leq k \leq n \\ x_0 & k \geq n+1 \end{cases}.$$

Since h is bijective, $f([n]) = h([n]) = X$, and hence f is a surjective function.

Case 2: X is infinite. Since X is countable, we must therefore have that X is countably infinite. Then by definition, there exists a bijection $f : \mathbb{N} \to X$, which is by definition surjective.

$(2 \Rightarrow 3)$ Suppose there exists a surjective function $f : \mathbb{N} \to X$. We wish to show that there exists an injection $g : X \to \mathbb{N}$. This is proven in HW7 Problem 1.

($3 \Rightarrow 1$) Suppose there exists an injective function $g: X \to \mathbb{N}$. We wish to show that X is countable. If X is finite, we are done.

Suppose, then, that X is an infinite set and there exists an injective function $g: X \to \mathbb{N}$. Let $S = g(X) \subseteq \mathbb{N}$. Since g is injective, and X is infinite, we have that S is also infinite. Moreover, as $S \subseteq \mathbb{N}$, we can write $S = \{s_1, s_2, s_3, \dots\}$ by taking $s_1 = \min(S)$, $s_2 = \min(S \backslash \{s_1\})$, $s_3 = \min(S \backslash \{s_1, s_2\})$, etc. Hence we have that S is a countably infinite set. Moreover, the function $g': X \to S$ defined by $g'(x) = g(x) \forall x \in X$ is a bijection, and hence $|X| = |S|$. Therefore, X is countably infinite.

□

This theorem will allow us to prove that sets are countable, even if we don't know that the functions we construct are exactly bijective, and also without actually knowing if the sets we consider are finite or countably infinite. Let's see an example of this in action.

Example 2. If X and Y are countable sets, then $X \cup Y$ is also a countable set.

Proof. Suppose that X and Y are countable. By Theorem 1, there exists surjective functions $f : \mathbb{N} \to X$ and $g : \mathbb{N} \to Y$.
Define a function $h : \mathbb{N} \to (X \cup Y)$ by

$$h(k) = \begin{cases} f(\frac{k}{2}) & k \text{ is even} \\ g(\frac{k+1}{2}) & k \text{ is odd} \end{cases}.$$

Since f and g are surjective, we have that $h(\mathbb{N}) = f(\mathbb{N}) \cup g(\mathbb{N}) = X \cup Y$, and thus h is a surjective function. Hence, by Theorem 1, we have that $X \cup Y$ is countable. □

In the above example, we are able to determine that the set we wish to consider is countable, even without knowing whether or not X or Y is countably infinite or finite, and without knowing what their intersection looks like.

Using the result of Theorem 1, we can also prove the following, which is assigned as a homework exercise. This allows us to take advantage of the structure of Theorem 1 when it is more convenient to use a different set from $\mathbb{N}$.

Theorem 2. *Let X be a nonempty set, and let Y be a countably infinite set. Then TFAE:*

1. *X is countable.*
2. *There exists a surjective function $f : Y \to X$.*
3. *There exists an injective function $g : X \to Y$.*

The following theorem will be quite useful in determining the countability of many sets we care about.

Theorem 3. *Let $n \in \mathbb{N}$, and let $X_1, X_2, \dots, X_n$ be nonempty countable sets. Then $\prod_{i=1}^{n} X_i = X_1 \times X_2 \times \cdots \times X_n$ is countable.*

Proof. We work by induction on n. The base case, that $n = 1$, is trivial, as $\prod_{i=1}^{n} X_i = X_1$, which is countable by hypothesis.

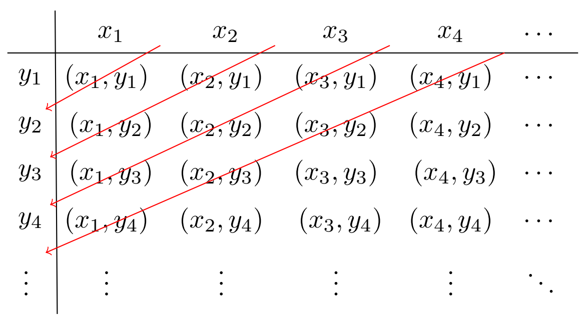
For the sake of illustration, we consider also the case that $n = 2$. The technique for this case will also be used in the inductive step, so it is worth our time to consider it.

Let X_1, X_2 be countable sets. Write $X_1 = \{x_1, x_2, x_3, \dots\}$, and write $X_2 = \{y_1, y_2, y_3, \dots\}$; we note that these enumerations can be terminating, or not. Recall that $X_1 \times X_2 = \{(x, y) \mid x \in X_1, y \in X_2\}$. We can visualize the elements of $X_1 \times X_2$ in a table, as follows:

	x_1	x_2	x_3	x_4	$\cdots$
y_1	(x_1, y_1)	(x_2, y_1)	(x_3, y_1)	(x_4, y_1)	$\cdots$
y_2	(x_1, y_2)	(x_2, y_2)	(x_3, y_2)	(x_4, y_2)	$\cdots$
y_3	(x_1, y_3)	(x_2, y_3)	(x_3, y_3)	(x_4, y_3)	$\cdots$
y_4	(x_1, y_4)	(x_2, y_4)	(x_3, y_4)	(x_4, y_4)	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Now, in order to show that $X_1 \times X_2$ is countable, it suffices to show that $X_1 \times X_2$ is enumerable. Using the table, we cannot enumerate the set by tracing first the rows or the columns; if X_2 is infinite, then enumerating along the first row will never terminate, and we will never arrive at the second row! So, we will have to be more clever.

Our clever idea will be as follows. While it's true that the rows and columns of the matrix are potentially infinite in length, the diagonals of the matrix are not. So we can try to enumerate by following the diagonals:



	x_1	x_2	x_3	x_4	$\cdots$
y_1	(x_1, y_1)	(x_2, y_1)	(x_3, y_1)	(x_4, y_1)	$\cdots$
y_2	(x_1, y_2)	(x_2, y_2)	(x_3, y_2)	(x_4, y_2)	$\cdots$
y_3	(x_1, y_3)	(x_2, y_3)	(x_3, y_3)	(x_4, y_3)	$\cdots$
y_4	(x_1, y_4)	(x_2, y_4)	(x_3, y_4)	(x_4, y_4)	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Following these paths, we achieve the following enumeration for $X_1 \times X_2$:

$$X_1 \times X_2 = \{(x_1, y_1), (x_2, y_1), (x_1, y_2), (x_3, y_1), (x_2, y_2), (x_1, y_3), (x_4, y_1), (x_3, y_2), (x_2, y_3), (x_1, y_4), \dots\}$$

Another way to think of this enumeration is as follows: we enumerate (x_i, y_j) by first listing all the elements with $i + j = 2$, then listing all the elements with $i + j = 3$, then listing all the elements with $i + j = 4$, and so on. Each of these is a finite set, and hence this will yield a full enumeration of all of $X_1 \times X_2$.

Now, for the inductive step, suppose that we know that the Cartesian product of any n countable sets is itself countable. Consider the product $X_1 \times X_2 \times \cdots \times X_n \times X_{n+1}$, all of which are countable.

Put $Y = X_1 \times X_2 \times \cdots \times X_n$. Note that there is a bijection $f : Y \times X_{n+1} \to X_1 \times X_2 \times \cdots \times X_n \times X_{n+1}$, by $((a_1, a_2, \dots, a_n), a_{n+1}) \mapsto (a_1, a_2, \dots, a_n, a_{n+1})$. Moreover, by the induction hypothesis, Y is countable.

Applying the technique above to the product $Y \times X_{n+1}$, since both Y and X_{n+1} are countable, we have that $Y \times X_{n+1}$ is countable. Moreover, $Y \times X_{n+1}$ is in bijection with $X_1 \times X_2 \times \cdots \times X_n \times X_{n+1}$, and hence $X_1 \times X_2 \times \cdots \times X_n \times X_{n+1}$ is also countable.

Thus, as the result is true for any n by induction, the theorem holds. □

It is important to note that this theorem applies only to a finite length Cartesian product; if we wish to take an infinite length Cartesian product, things can go very differently for us, which we shall see in Section 3 below. However, this theorem has an immediate, delightful corollary:

Corollary 1. *The set of rational numbers $\mathbb{Q}$ is countably infinite.*

Proof. Recall from Example 1 that $\mathbb{Z}$ is countable. Since there is an injection $f : \mathbb{Z}\backslash\{0\} \to \mathbb{Z}$ defined by $f(x) = x$ for all x, by Theorem 2, we also have that $\mathbb{Z}\backslash\{0\}$ is countable. Therefore, by Theorem 3, we have that $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ is countable.

Consider the function $g : \mathbb{Z} \times (\mathbb{Z}\backslash\{0\}) \to \mathbb{Q}$ defined by $g((a, b)) = \frac{a}{b}$. Note that this is well defined, as $b \neq 0$. Moreover, since every element of $\mathbb{Q}$ can be expressed in at least one way as a ratio of integers with a nonzero denominator, we have that g is surjective. But then by Theorem 2, we have that $\mathbb{Q}$ is countable.

Finally, $\mathbb{Q}$ is not finite, as $\mathbb{N} \subseteq \mathbb{Q}$, and any subset of a finite set must also be finite.

Therefore, $\mathbb{Q}$ is countably infinite. □

Amazing! So we have then that three of our favorite number sets are all countably infinite. Indeed, though $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$, all three sets have the exact same cardinality, and are in bijection with each other!

Finally, we note the following theorem, whose proof is left as a homework exercise.

Theorem 4. *Let $X_1, X_2, X_3, \ldots$ be a countable list of countable sets. Then $\bigcup_{i=1}^{\infty} X_i$ is countable.*

The proof will look similar to that of Theorem 3: if we can write the elements of the union in a table, we can then trace the diagonals of the table to enumerate the elements. A word on the proof: be careful with notation! It gets, well, messy.

3 Uncountable Infinity

So, if $\mathbb{N}, \mathbb{Z}$, and $\mathbb{Q}$ are all the same size, what about $\mathbb{R}$? Is that also countable?

Sadly, no. The real numbers are a whole new ballgame. What we will actually prove here is that the real numbers between 0 and 1 are not countable; this will certainly imply that the set of all real numbers is not countable.

To prove that, we're gonna have to do a little work. This is a classic argument called Cantor's Diagonalization, and in order to employ it, we need a Lemma first.

Lemma 1. *Every real number between 0 and 1 can be represented uniquely in base 10 representation as $0.d_1d_2d_3\ldots$, where the d_i represent digits between 0 and 9, and the digits have the property that $\forall n \in \mathbb{N}$, $\exists m \geq n$, $d_m \neq 9$.*

Let's think carefully about what this is saying. First, we want to represent our numbers in base 10; no problem there, we already did that long ago in our notes on Understanding Number Sets. The last part of the statement is saying that we do not want a representation that ends in just a bunch of 9s forever. As we have seen before, $0.9999\cdots = 1$, so a decimal that terminates in all 9s can be simplified. For example:

$$0.12362574999999\cdots = 0.12362574 + 0.0000000099999\cdots = 0.12362574 + 0.00000001 = 0.12362575.$$

Hence, we'd like to forbid a decimal from going to all 9s. Moreover, the Lemma claims that if we are able to do so, then the decimal representation of the number is unique.

Proof. [Proof of Lemma 1] That each number can be represented as a decimal in base 10 expansion is already known; we need only prove uniqueness of the representation under the condition that no representation terminates in all 9s.

Suppose that x is a real number between 0 and 1, and that we have two decimal representations of x that satisfy the given condition; that is, we can write $x = 0.d_1d_2d_3\cdots = 0.c_1c_2c_3\ldots$, neither of which terminate with infinitely many 9s. We work by induction to show that $d_n = c_n$ for all n.

For the base case, consider d_1, c_1. Suppose that $d_1 \neq c_1$; wolog say that $d_1 < c_1$. Note then that $x = 0.c_1c_2c_3\cdots \geq 0.c_1$. On the other hand, since at least one d_n, for $n \geq 2$ is not a 9, we have that $x - 0.d_1 = 0.0d_2d_3\cdots < 0.1$, and thus $x < 0.(d_1+1) \leq 0.c_1$. Hence, $0.c_1 \leq x < 0.c_1$, which is impossible. Therefore, $d_1 = c_1$.

For induction, suppose that for some $n \in \mathbb{N}$ we know that $d_k = c_k$ for all $k \leq n$.

Consider $y = 10^n x - d_1d_2\ldots d_n = 0.d_{n+1}d_{n+2}d_{n+3}\cdots = 0.c_{n+1}c_{n+2}c_{n+3}\ldots$. By repeating the above argument, we obtain that $d_{n+1} = c_{n+1}$.

Therefore, by induction, we have that $d_n = c_n$ for all n, and hence the desired decimal representation of x is unique. □

Theorem 5. *The set of real numbers between* 0 *and* 1 *is uncountable.*

Proof. We work by contradiction. Write $X = \{x \in \mathbb{R} \mid 0 < x < 1\}$. Suppose that X is countable. Clearly X is infinite, and hence by definition, there exists a bijection $f : \mathbb{N} \to X$.

For each $n \in \mathbb{N}$, write $f(n) = 0.d_1^{(n)}d_2^{(n)}d_3^{(n)}\ldots$ to be the unique decimal representation of $f(n)$ guaranteed by Lemma 1.

Define $y \in X$ with decimal representation $y = 0.y_1y_2y_3\ldots$, where for each $n \in \mathbb{N}$, we define

$$y_n = \begin{cases} d_n^{(n)} - 1 & \text{if } d_n^{(n)} \neq 0, 1 \\ 1 & \text{if } d_n^{(n)} = 0 \\ 2 & \text{if } d_n^{(n)} = 1 \end{cases}$$

Note that y satisfies the condition in Lemma 1, since in fact none of the digits of y are 9s. Moreover, by definition $0 < y < 1$, since none of the digits of y are 0s. Therefore, $y \in X$, and hence since f is a bijection, $y = f(n)$ for some $n \in \mathbb{N}$.

Therefore, $y = 0.y_1y_2y_3\cdots = 0.d_1^{(n)}d_2^{(n)}d_3^{(n)}\cdots = f(n)$. By Lemma 1, we must therefore have that $y_i = d_i^{(n)}$ for all $i \in \mathbb{N}$. But by definition, $y_n \neq d_n^{(n)}$, and hence we have a contradiction.

Therefore, it must be the case that X is not countable. Since X is infinite, then, X is uncountable. □

This theorem shows that a particular subset of $\mathbb{R}$ is uncountable, which of course implies that $\mathbb{R}$ itself is uncountable. Moreover, we can form a bijection from X described in the Theorem to $\mathbb{R}$, as follows.

Example 3. The set $X = \{x \in \mathbb{R} \mid 0 < x < 1\}$ is in bijection with $\mathbb{R}$.

Proof. Define a function $f : X \to \mathbb{R}$ by $f(x) = \frac{2x-1}{x-x^2}$. Note that as $0, 1 \notin X$, this is a well-defined function. We claim it is a bijection. To demonstrate this, we show an inverse.
Let $g : \mathbb{R} \to X$ be defined by $g(y) = \frac{y-2+\sqrt{4+y^2}}{2y}$ for $y \neq 0$, and $g(0) = \frac{1}{2}$. We first claim that this is well-defined; we need to show that $g(y) \in X$ for all y. Note that for all $y \neq 0$, $\sqrt{4+y^2} < \sqrt{4+4y+y^2} = |2+y|$, and hence $g(y) < \frac{y-2+|2+y|}{2y} \leq 1$. Moreover, for all $y \neq 0$, $\sqrt{4+y^2} > \sqrt{4-4y+y^2} = |y-2|$, and hence $g(y) > \frac{y-2+|y-2|}{2y} \geq 0$.
Therefore, g is well defined. Moreover, we have for $x = \frac{1}{2}$, by definition $g \circ f(x) = x$. For $x \neq \frac{1}{2}$,

$$
\begin{aligned}
g \circ f(x) &= g\left(\frac{2x-1}{x-x^2}\right) \\
&= \frac{\frac{2x-1}{x-x^2} - 2 + \sqrt{4 + \left(\frac{2x-1}{x-x^2}\right)^2}}{2\frac{2x-1}{x-x^2}} \\
&= \frac{\frac{2x^2-1}{x-x^2} + \sqrt{\frac{4x^2-4x+1+4(x-x^2)^2}{(x-x^2)^2}}}{\frac{4x-2}{x-x^2}} \\
&= \frac{2x^2-1+\sqrt{4x^2-4x+1+4x^2-8x^3+4x^4}}{4x-2} \\
&= \frac{2x^2-1+\sqrt{4x^4-8x^3+8x^2-4x+1}}{4x-2} \\
&= \frac{2x^2-1+\sqrt{(2x^2-2x+1)^2}}{4x-2} \\
&= \frac{4x^2-2x}{4x-2} = x
\end{aligned}
$$

Thus $g \circ f \equiv \iota_X$. Similarly, one can show that $f \circ g \equiv \iota_{\mathbb{R}}$. Therefore, g is an inverse to f, and in particular, then, f is a bijection. □

Hence, we have that since X is uncountable, and $|X| = |\mathbb{R}|$, also we know that $\mathbb{R}$ is uncountable.

A similar type of argument as in the proof of Theorem 5 can be used (and will be, in homework!) to prove the following.

Theorem 6. *Let X be any set. Then $|X| < |\mathcal{P}(X)|$.*

We have already proven this theorem for finite sets in previous homework. For infinite sets, it is equally true. Note what this implies: if we have one set of infinite size, then we can generate infinitely many different sizes of infinity by repeatedly taking power sets. Indeed, the following sets

$$\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})), \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))), \ldots$$

are all of different cardinality, increasing in size from left to right. Moreover, it is not too difficult to show the following.

Theorem 7. *The set $\mathbb{R}$ is in bijection with $\mathcal{P}(\mathbb{N})$.*

To prove this theorem one can work with binary representations of elements in X, rather than decimal representations as was done in Lemma 1 and Theorem 5. We have seen, in the finite counting notes, that $\mathcal{P}(X)$ is in bijection with the strings of 0s and 1s; we can use this to construct a bijection with decimal representations of numbers.

3.1 The Continuum Hypothesis and Incompleteness

Ok, so we have a bunch of infinities. But every set we've actually looked at takes only one of two sizes. In some cases, we like to give a name to the sizes of infinity; these are cardinal numbers, and in fact they have a whole algebra of their own, which we here omit. But a fundamental question then arises:

Are these all the possible sizes of infinity?

To be really specific, let's consider a question. We know that $\mathbb{N}$ and $\mathbb{R}$ have different cardinalities; we proved that in the work above. So here is a question.

Is there any set S such that $|\mathbb{N}| < |S| < |\mathbb{R}|$?

That is to say, can we construct a set whose size is in between that of $\mathbb{N}$ and $\mathbb{R}$? Or is there nothing in between? Even more, what about the other sizes of infinity? We saw above that $|\mathcal{P}(X)| \neq |X|$ for any X, so an even more general version of our question above could be phrased as follows:

Let X be an infinite set. Is there any set S such that $|X| < |S| < |\mathcal{P}(X)|$?

I would love to answer this question for you, and I think a lot of mathematicians would. We have just one problem here:

The answer to this question cannot be known.

Now that sounds a little bit crazy, and it feels pretty bad. But this is the question that lead to a famous, important theorem in mathematics known as Gödel's Incompleteness Theorem. We're not going to get into the nitty gritty details here, but the broad strokes of the idea are like this. First we rephrase our question as a proposition. This proposition is often referred to as the Continuum Hypothesis.

p: There does not exist any set S with $|\mathbb{N}| < |S| < |\mathbb{R}|$.

Then the "answer" to the question just becomes the truth value of the proposition: if the proposition is True, then no such S exists, and if the proposition is False, then such a set does exist, and we have not found all the infinities.

In the 1940s, a mathematician named Gödel proved something resembling the following statement:

Using the standard mathematical axioms, p cannot be proven to be False.

In the 1960s, a mathematican named Cohen followed up with something resembling the following statement:

Using the standard mathematical axioms, p cannot be proven to be True.

Let's be very clear about what is being said here. What Gödel and Cohen are doing is not a proof that the statement is true or false, but a proof about proofs themselves. Specifically, what Gödel proved is that there is no proof that the statement is false. This does not, of course, mean that there IS a proof that the statement is true, as we see in Cohen's follow up theorem. Indeed, the set of proofs that one can write using the standard set of axioms about mathematics simply DO NOT INCLUDE a proof about this statement. Its truth cannot be known, at all.

Well, fine. We could get around this, if we wanted, by simply adding a new axiom that asserts that p is either true or false, depending upon your preference. Gödel and Cohen's work actually shows that this is a logically consistent thing to do; the Continuum Hypothesis can be taken as either true or false and nothing about the existing axiomatic structure will break.

But even before this work, in the 1930s, Gödel proved a theorem that might make this solution less than satisfying. This result is known as the Gödel Incompleteness Theorem.

Suppose you have an axiomatic system of mathematics. Then you can make statements that are neither provable nor unprovable in that system.

That is to say, assuming the truth value of the Continuum Hypothesis does not end this conundrum. At some point, mathematics will bump up into another proposition that cannot be proven true and cannot be proven false. Gödel's Incompleteness Theorem says that this is unavoidable: you will never be able to create an axiom system for which every proposition has a knowable truth value.

This, of course, is very sad-making for mathematicians. Our whole schtick is caring about problems for which proofs or disproofs are not known. We may never know, working on a problem, whether the truth of that question is even knowable, let alone how to solve it ourselves.

Incidentally, both Gödel and Cantor, after successful careers studying the nature of infinity, ended their lives completely crazy. Cantor died in a mental institution, after having moved in and out of sanatoria for the last 34 years of his life. Gödel was paranoid that people were out to get him; he died of starvation after refusing to eat for months, claiming all his food was being poisoned. (Cohen seemed to do just fine for himself, giving lectures on mathematics and the continuum problem up until his death in 2007.)