Wednesday,
March 6

Can a countable set be finite? No. By definition, a countable set has a one-to-one correspondence with $\mathbb{Z}_{>0}$, so a countable set must have infinitely many elements.

A set A is countable if and only if you can enumerate the elements of A, i.e. $A = \{x_1, x_2, x_3, \ldots\}$. We can't do this for $(0,1)$ (we proved this), but we can for $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. As written, it's not clear that we can enumerate $\mathbb{Z}$, but we can write $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$, which should make it clearer that $\mathbb{Z}$ can be enumerated (the above set lists all elements of $\mathbb{Z}$ with a first element, then a second, then a third, and so on, eventually hitting all of $\mathbb{Z}$).

A car can be safe. A car can be fun to drive. It can be both. It can be neither. This is like functions, which can be injective, surjective, both or neither.

Last time, we showed that
$$f: \mathbb{Z}_{\geq -2} \to 4\mathbb{Z}_{>0} - 1$$
$$n \longmapsto 4n + 11$$

is a function that is both injective and surjective, and $g: \mathbb{Z}_{>0} \to \mathbb{Z}_{\geq 0}$ defined by $g(n)$ is the exponent of the largest power of 2 dividing n is a surjective function, but not an injective one (for example, $g(4) = g(12)$).

$$G: \mathbb{Z} \to \mathbb{Z}$$
$$x \mapsto x^2$$
is a function, but it's not injective ($G(4) = G(-4)$) and it's not surjective ($-1 \in \mathbb{Z}$, but there's no $n \in \mathbb{Z}$ such that $G(n) = -1$).

$$F: \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$$
$$x \longmapsto x^2$$
is a function. It's not surjective for the same reason G isn't surjective, but F is injective ($F(x) = F(y) \Rightarrow x^2 = y^2 \Rightarrow x^2 - y^2 = 0 \Rightarrow (x-y)(x+y) = 0 \Rightarrow x = \pm y$. Since x and y are both positive, $x = y$).

Reminder: A function from a set A to a set B sends an element of A to exactly one element of B.

These examples show us that functions can be injective, surjective, both, or neither. If a function happens to be both, it's a one-to-one correspondence.

(Note: we've started referring to functions as nouns, when in the past, we've treated them as verbs acting on numbers. This also comes up in linear algebra!)

Notation: Given $f: A \to B$ a function, if f is injective, we write $f: A \hookrightarrow B$. If f is surjective, we write $f: A \twoheadrightarrow B$.

(Note using the new notation: $A \approx B$ iff $\exists f: A \hookrightarrow\!\!\!\!\rightarrow B$.)

If $A \hookrightarrow B$, then intuitively B is at least as large as A. (This makes sense — if every element of A gets mapped to a different element of B, there have to be at least as many elements of B as there are of A, or else we'd have to send two elements of A to the same element of B.)

If $A \hookrightarrow B$ and $A \not\approx B$, then B is strictly larger than A. (This makes sense with the same reasoning as above — since B must be at least as large as A, and it isn't the same size as A, B must be larger than A.)

For example, $\mathbb{Z}_{>0} \hookrightarrow (0,1)$, but we showed that $\mathbb{Z}_{>0} \not\approx (0,1)$.

$$x \longmapsto \frac{1}{x+1}$$

Question: Given a set S, can you produce a strictly larger set?

Answer: Yes.., the power set of S ($P(S)$).

Theorem: $S \hookrightarrow P(S)$ and $S \not\approx P(S)$. In words, P(S) is strictly larger than S.

Proof: $S \hookrightarrow P(S)$. This sends every element of S to a unique

$$x \longmapsto \{x\}.$$

element of $P(S)$, so $S \hookrightarrow P(S)$. Now we'll prove any $f: S \to P(S)$ can't be surjective.

Pick any function $f: S \to P(S)$. Consider $A := \{x \in S : x \notin f(x)\}$. Clearly, $A \subseteq S$. We claim that A isn't an output of f. Suppose $f(a) = A$. Then either $a \in A$ or $a \notin A$. If $a \in A$, $a \notin f(a) = A$, which is a contradiction. If $a \notin A$, $a \in f(a) = A$, which is a contradiction. Thus, A isn't an output of f. Contradiction! Q.E.D.

Quick continuum hypothesis note: if we have two sets S and $P(S)$, is there a set with a cardinality between S and $P(S)$? We don't know! Kurt Gödel proved that this can't be disproven, and Paul Cohen proved that this can't be proven!