Def: A set (nonempty) A is called uncountable if it isn't finite and it isn't denumerable.
(Equivalently, there's no surjection $f: \mathbb{N} \longrightarrow A$).

Last time: proved $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$ is uncountable.

Exercise: Prove that $\mathbb{R}$ is uncountable. (Use Contradiction)

More generally: Let $A \subseteq B$. Ex: $B = \mathbb{R}$, $A = [0,1]$.
If A is uncountable, then B is uncountable.

Pf: We've shown that if $A \subseteq B$
B countable $\Rightarrow$ A countable.
Now just take the contrapositive. ∎

Recall: For two sets A, B, we say $|A| = |B|$ if there's a bijection $f: A \longrightarrow B$

Def: We say $|A| \leq |B|$ if there's an injection $f: A \longrightarrow B$.

We say $|A| < |B|$ if there's an injection but there is no bijection. (Ex: $|\mathbb{N}| < |\mathbb{R}|$)

Comment: The statement

"If $\exists$ injection $: A \to B$, then $\exists$ surjection $: B \to A$"

has to be proven. You can prove it. But proving the converse requires the "Axiom of Choice".

Example: If B is countable and $|A| \leq |B|$, then A is countable.

Today: Cantor's Theorem: Let A be a set. Let $P(A) =$ set of all subsets of A ← power set

Then $|A| < |P(A)|$.

Comment: $|\mathbb{N}| < \underset{|\mathbb{R}|}{\underset{\parallel}{|P(\mathbb{N})|}} < |P(P(\mathbb{N}))| < \cdots$ ← we'll discuss this.

First: Let's find an injection $f : A \longrightarrow P(A)$. (Exercise)

Define $f(\underset{\in A}{a}) = \underset{\subseteq A}{\{a\}}$. This is an injection.

So $|A| \leq |P(A)|$.

For finite sets A, $|A| \leq |P(A)|$ because $n < 2^n$.

For infinite sets, we use Cantor diagonalization.

Let's first prove it for $A = \mathbb{N}$.

Notation: Any subset $S \subseteq \mathbb{N}$ corresponds uniquely to a function $f : \mathbb{N} \longrightarrow \{0,1\}$ which can be thought of as an infinite strings of 0's and 1's

Example: $\{2,3,5,7,11,13,\ldots\} \longleftrightarrow 0110101000101\ldots$

Example: $\{3,6,9,12,15,\ldots\} \longleftrightarrow 001001001001\ldots$

1 2 3 4 5 6 7 8 9 10 11 12 ...

Thm: Any function $H : \mathbb{N} \longrightarrow P(\mathbb{N})$ is not surjective.

"Bit-string version"

Pf: Pick some H.

$\boxed{0}\boxed{0}\boxed{1}\boxed{0}\ldots$

represented as a string of 0's and 1's

$H(1) = \boxed{0}\ 1\ 1\ 0\ 1\ 0\ \ldots$

$H(2) = 1\ \boxed{0}\ 1\ 1\ 0\ 1\ \ldots$

$H(3) = 1\ 1\ \boxed{1}\ 0\ 0\ 1\ \ldots$

$H(4) = 0\ 0\ 1\ \boxed{0}\ 1\ 1\ \ldots$

$\vdots$

Construct a new subset $S \subseteq \mathbb{N}$ which is not in this list:

$$S\text{'s } n\text{-th digit is} = \begin{cases} 0 & \text{if } H(n)\text{'s is } 1 \\ 1 & \text{if } H(n)\text{'s is } 0 \end{cases}$$

$S = 1101\ldots$

For every $n \in \mathbb{N}$,

$$\underset{\text{digit}}{S\text{'s } n\text{-th}} \neq \underset{\text{digit.}}{H(n)\text{'s } n\text{-th}} \qquad \text{so} \qquad S \neq H(n)$$

thus $S \subseteq \mathbb{N}$ is not in the image of H

So H is not surjective. $\blacksquare$

Exercises: Convert the proof above to one not involving strings of 0's and 1's.

Exercises: Try to prove Cantor's theorem for any set A, not just $A = \mathbb{N}$. (Hard!)

Thm: There is no surjective function $H: \mathbb{N} \longrightarrow P(\mathbb{N})$.

Pf: Let $H: \mathbb{N} \longrightarrow P(\mathbb{N})$ be any function. (I.e., for each n, $H(n)$ is a subset of $\mathbb{N}$.).

Define a new subset $S \subseteq \mathbb{N}$ by:

For each $n \in \mathbb{N}$, $\quad n \in S \iff n \notin H(n)$. (*)

(that is, $S = \{n \in \mathbb{N} : n \notin H(n)\}$).

For each n, S is different from $H(n)$. (by (*))
Thus, $S \in P(\mathbb{N})$ is not in the image of H.
So H is not surjective. ∎

Thm (Cantor's Thm): For every set A, there is no surjective function $H: A \longrightarrow P(A)$.

Pf: Let $H: A \to P(A)$ be any function. Define a subset $S \subseteq A$ by

$$S = \{a \in A : a \notin H(a)\}.$$

For each $a \in A$, we see $a \in S \iff a \notin H(a)$. and thus $S \neq H(a)$.
So S is not in the image of H. So H is not surjective. ∎

(This proves that $|A| < |P(A)|$ for every set A.).