Claim: Suppose \( f: \mathbb{N} \to \mathcal{P}(\mathbb{N}) \) is a fixed function (any function). Then \( f \) is not surjective.

\[ T = \{ n \in \mathbb{N} \mid n \notin f(n) \} \]

Sidebar: Let's illustrate def'n

\[ \begin{align*}
  f(1) &= \{1, 7, 10\} \\
  f(2) &= \{1, 3, 5, 7, \ldots\} \\
  f(3) &= \emptyset \\
  f(4) &= \{2, 9, 6, 8, \ldots\} \\
  \vdots
\end{align*} \]

Then: \( 1 \notin T \) since \( 1 \in f(1) \)

\( 2 \in T \) since \( 2 \notin f(2) \)

\( 3 \notin T \) since \( 3 \in f(3) \)

\( 4 \notin T \) since \( 4 \in f(4) \) \( \ldots \) etc.

So in this case would have

\[ T = \{2, 3, \ldots\} \]
Claim: \((\forall n \in \mathbb{N})\ f(n) \neq T\)

**PF:** Fix \(n \in \mathbb{N}\)

(i) If \(n \notin T\) then \(n \notin f(n)\), by defn of \(T\). Hence \(f(n) \neq T\), since \(n \notin T\) but \(n \notin f(n)\)

(ii) If \(n \notin T\), then \(n \in f(n)\), by defn of \(T\).

Hence again \(f(n) \neq T\) in this case, since a new \(n \in f(n)\) but \(n \notin T\).

Hence in all cases \(f(n) \neq T\). Since \(n\) was arbitrary we have \(f(n) \neq T\) for every \(n \in \mathbb{N}\).

But now claim follows: \(T \notin \text{Img} f\) hence \(f\) is not surjective.

Since \(f\) was arbitrary there is no surjection \(f: \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})\) (hence no bijection)

So \(\mathbb{N} \not\sim \mathcal{P}(\mathbb{N})\)

The same proof works in general: Theorem for any set \(A\), there is no surjection \(f: A \rightarrow \mathcal{P}(A)\)

**PF:** Fix \(f: A \rightarrow \mathcal{P}(A)\) and let \(T = \{a \in A \mid a \notin f(a)\}\)

Then \(\forall a \in A, \ f(a) \neq T\) (by same arg)
Since it's always the case that \( A \leq P(A) \) (\( f(a) = \{a\} \) defines an injection) above there shows actually 
\[ A \leq P(A) \] for every set \( A \).

It follows: there are infinitely many infinite cardinals:
\[ N < P(N) < P(P(N)) < \ldots \]

**Defn** if \( x \) is infinite \& and \( N \times x \), we say \( x \) is uncountable.

Above says: \( P(N) \) is unctbl. Other examples?

**Sets of functions**

Let \( B = \{ f \in N \times \{0,1\} \mid f : N \to \{0,1\} \text{ is a function} \} \) be the set of functions from \( N \) to \( \{0,1\} \).

So we can visualize a given \( f \in B \) as an infinite 01-sequence

\[ f(1) = 0 \quad f(4) = 0 \quad f(2) = 0 \quad f(5) = 1 \quad f(7) = 0 \quad f(6) = 1 \quad f(8) = 1 \quad \cdots \]

**e.g.** if \( f(1) = 0 \) \( f(4) = 0 \) can picture \( f \) as:

\[ f = 0010110 \ldots \]
Conversely, could write:

g^n = 101010...

to mean \( g \) is the function:

\[
\begin{align*}
g(1) &= 1 \\
g(2) &= 0 \\
g(3) &= 1 \\
g(4) &= 0 \\
g(5) &= 1 \\
g(6) &= 0
\end{align*}
\]

... etc.

Theorem B is uncountable.

Pf: Diagonalize!

Claim: if \( H: \mathbb{N} \rightarrow \mathbb{B} \) is a function, then

\( H \) is not a surjection

Pf: Define a function \( f: \mathbb{B} \rightarrow \mathbb{B} \) as follows:

\[
f(n) = \begin{cases} 
1 & \text{if } H(n)(n) = 0 \\
0 & \text{if } H(n)(n) = 1
\end{cases}
\]

then by the very def'n of \( f \) we have:

\[
(\forall n \in \mathbb{N}) \quad f(n) \neq H(n)(n)
\]

Hence \( f \neq H(n) \) for any \( n \in \mathbb{N} \)

the claim follows.
To illustrate:

E.g. if we have

\[ H(1) = 01010101 \ldots \]
\[ H(2) = 00110101 \ldots \]
\[ H(3) = 11111111 \ldots \]
\[ H(4) = 00011111 \]

In this case would have

\[ f = 1100 \ldots \]

Hence: \( f \neq H(n) \) for any \( n \)!

Why: \( f(n) \neq H(n)(n) \) for any \( n \)

\[ \text{differ in 1st place} \]
Number theory

"The queen of mathematics"
- Gauss

- study of integers and their arithmetic
- primes play especially important role

**Def'n** Fix $n \in \mathbb{N}$, $n \geq 1$.

1. $n$ is prime iff its only positive divisors are 1 and $n$.
2. $n$ is composite iff it is not prime.
   
   i.e. if $a, b \in \mathbb{N}$ with $1 < a, b < n$ s.t. $n = ab$

- We proved (by strong induction): any $n > 1$ can be written as a product of primes.

- You'll prove: there's a unique way to do this.

**Def'n** Given $m, n \in \mathbb{Z}$ we say $m$ is a divisor of $n$ iff $m | n$ i.e. $\exists k \in \mathbb{Z}$


$n = mk$. 
Note: every \( n \in \mathbb{Z} \) is a divisor of 0 since \( 0 = 0 \cdot n \). But if \( n \neq 0 \) and \( m, n \in \mathbb{Z} \) we have \( |m| \leq |m| \).

Def. Given \( m, n \in \mathbb{Z} \), \( n \neq 0 \), the greatest common divisor of \( m, n \), denoted \( \gcd(m, n) \), is the largest \( d \in \mathbb{N} \) dividing both \( m \) and \( n \).

Ex: 1. what is \( \gcd(42, 60) \)?

Divisors of 42 = \{\( \pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42 \}\)

Divisors of 60 = \{\( \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60 \}\)

Common divisors = \{\( \pm 1, \pm 2, \pm 3, \pm 6 \}\}

\( \Rightarrow \gcd(42, 60) = 6 \).

2. \( \gcd(42, 0) = 42 \), since each 42 is largest divisor of 42 and 42 | 0.

3. \( \gcd(-42, -60) = 6 \) too (still positive).