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

Pf: a magic trick.

Let $T = \{n \in \mathbb{N} \mid n \notin f(n)\}$

---

sidebar: Let's illustrate def'n

e.g. if
$$f(1) = \{1, 7, 10\}$$
$$f(2) = \{1, 3, 5, 7, \ldots\}$$
$$f(3) = \emptyset$$
$$f(4) = \{2, 4, 6, 8, \ldots\}$$
$$\vdots$$

then: $1 \notin T$ since $1 \in f(1)$
$2 \in T$ since $2 \notin f(2)$
$3 \in T$ since $3 \notin f(3)$
$4 \notin T$ since $4 \in f(4)$ .. 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 $n \in T$ then $n \notin f(n)$, by def'n of $T$. Hence $f(n) \neq T$, since $n \in T$ but $n \notin f(n)$

(ii) if $n \notin T$, then $n \in f(n)$, by def'n of $T$. Hence again $f(n) \neq T$ in this case, since now $n \in f(n)$ but $n \notin T$.

Hence in all cases $f(n) \neq T$. Since $n$ was arbitrary we have $f(n) \neq T$ for <u>every</u> $n \in \mathbb{N}$.
But now claim follows: $T \notin \operatorname{Im} f$ hence $f$ is not surjective.
Since $f$ was arbitrary there is <u>no</u> surjection $f : \mathbb{N} \to P(\mathbb{N})$ (hence no bijection)
So $\mathbb{N} \not\approx P(\mathbb{N})$

---

the same proof works in general:
<u>Theorem</u> for any set $A$, there is no surjection $f : A \to P(A)$
<u>Pf</u>: fix $f : A \to P(A)$ 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 $A \lesssim P(A)$ ($f(a) = \{a\}$ defines an injection) above thm shows actually

$$A < P(A) \quad \text{for every set } A.$$

It follows: there are infinitely many infinite cardinalities:

$$\mathbb{N} < P(\mathbb{N}) < P(P(\mathbb{N})) < \cdots$$

---

<u>Def'n</u> if $X$ is infinite and $\mathbb{N} \not\approx X$, we say $X$ is <u>uncountable</u>.

Above says: $P(\mathbb{N})$ is unctbl. Other examples?

<u>Sets of functions</u>

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

↳ we can visualize a given $f \in B$ as an infinite 01-sequence

e.g. if $f(1) = 0$ $f(4) = 0$ can picture $f$ as:
$f(2) = 0$ $f(5) = 1$ $f$ "=" $001011\ldots$
$f(3) = 1$ $f(6) = 1$

Conversely, could write:

$g$ "=" 101010...

to mean $g$ is the function:

$g(1) = 1$ $g(3) = 1$ $g(5) = 1$ ... etc.
$g(2) = 0$ $g(4) = 0$ $g(6) = 0$

<u>Theorem</u> $B$ is uncountable.

<u>Pf</u>: Diagonalize!

<u>Claim</u>: if $H: \mathbb{N} \to B$ is a function, then $H$ is <u>not</u> a surjection

<u>Pf</u>: Define a function $f \in B$ 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:

$(\forall n \in \mathbb{N})$ $f(n) \neq H(n)(n)$

if 1, $f(n) = 0$
if 0, $f(n) = 1$

Hence $f \neq H(n)$ for <u>any</u> $n \in \mathbb{N}$

the claim follows ✓

to illustrate:

e.g if we have

$H(1)(1)$, $H(2)(2)$, $H(3)(3)$

$$
\begin{aligned}
H(1) &= 0\ 1\ 0\ 1\ 0\ 1 \ldots \\
H(2) &= 0\ 0\ 1\ 1\ 0\ 1 \ldots \\
H(3) &= 1\ 1\ 1\ 1\ 1\ 1 \ldots \\
H(4) &= 0\ 0\ 0\ 1\ 1\ 1
\end{aligned}
$$

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 $n$

differ in nth place

# Number theory

"The queen of mathematics"
— Gauss

↳ study of integers + their arithmetic
↳ primes play especially important role

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

① $n$ is prime iff its only positive divisors are $1$ and $n$

② $n$ is composite iff it's not prime
i.e. iff $\exists a, b \in \mathbb{N}$ 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 $m \mid n$ 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 $m | n$ we have $|m| \leq |n|$.

Def'n Given $m, n \in \mathbb{Z}$ — not both $0$ — the greatest common divisor of $m, n$; denoted $\gcd(m, n)$ is the largest $d \in \mathbb{N}$ dividing both $m, n$.

Ex: ① what is $\gcd(42, 60)$?

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

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 42 is largest divisor of 42 and $42 | 0$

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