CS70 – SPRING 2026

LECTURE 12: FEB. 26

Today: Countable & Uncountable Sets

OR: Does $\infty = \infty + 1$?

Why?

○ Background for counting

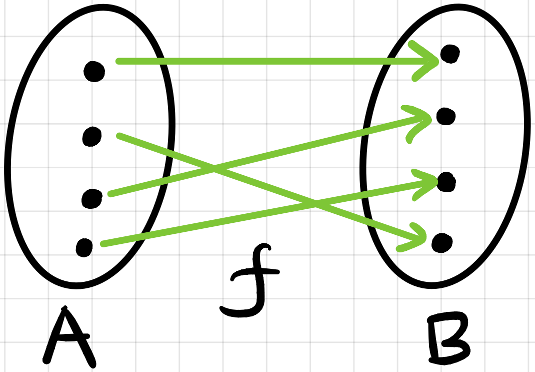
○ Understanding sets like $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$

○ Background for computability (next lecture)

Main Question: When do two sets have the same size (= "cardinality") ?

Finite sets: Easy !

Two finite sets have same size if their elements can be paired up with a bijection:



Defn: A function $f : A \to B$ is a bijection if f is both

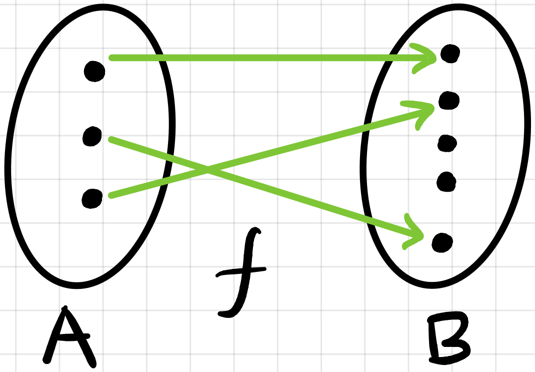
(i) one-to-one (1-1), i.e., "injection"

$$\forall a_1, a_2 \in A \left((a_1 \neq a_2) \Rightarrow f(a_1) \neq f(a_2) \right)$$

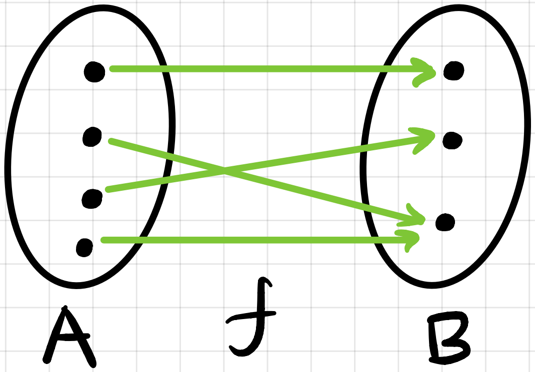
and

(ii) onto, i.e., "surjection"

$$(\forall b \in B)(\exists a \in A)(f(a) = b)$$



f is 1-1 $\Rightarrow |A| \leq |B|$



f is onto $\Rightarrow |A| \geqslant |B|$

f is a bijection $\Longleftrightarrow$ f is 1-1 & onto $\Longleftrightarrow |A| = |B|$

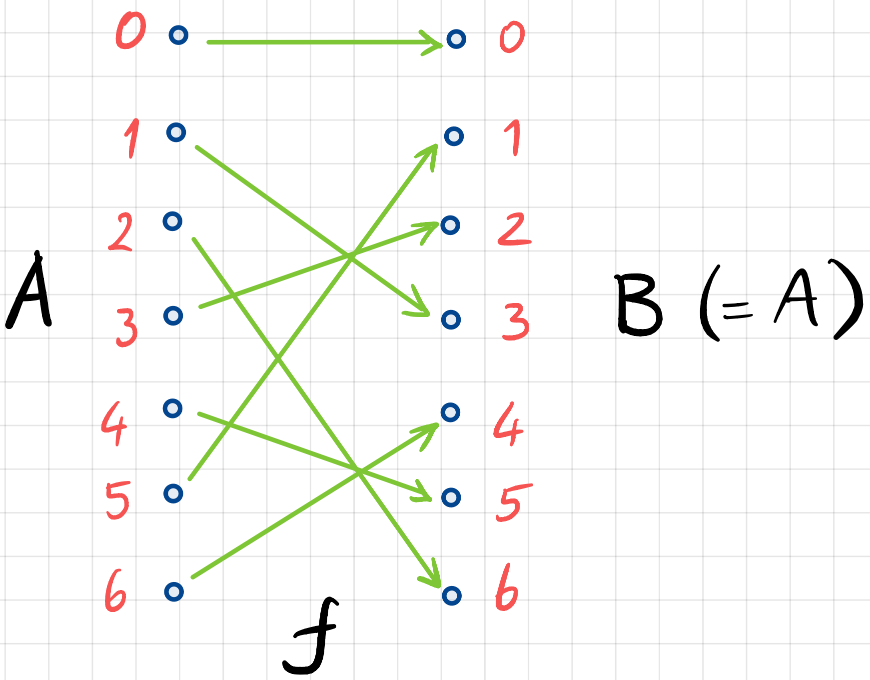
Note : Every 1-1 function has an inverse function.

The inverse of a bijection is also a bijection.

Example: $A = B = \{0, 1, \dots, m-1\}$

Let $\gcd(m, x) = 1$ and define $f(a) = ax \pmod{m}$

E.g. $m = 7$, $x = 3$

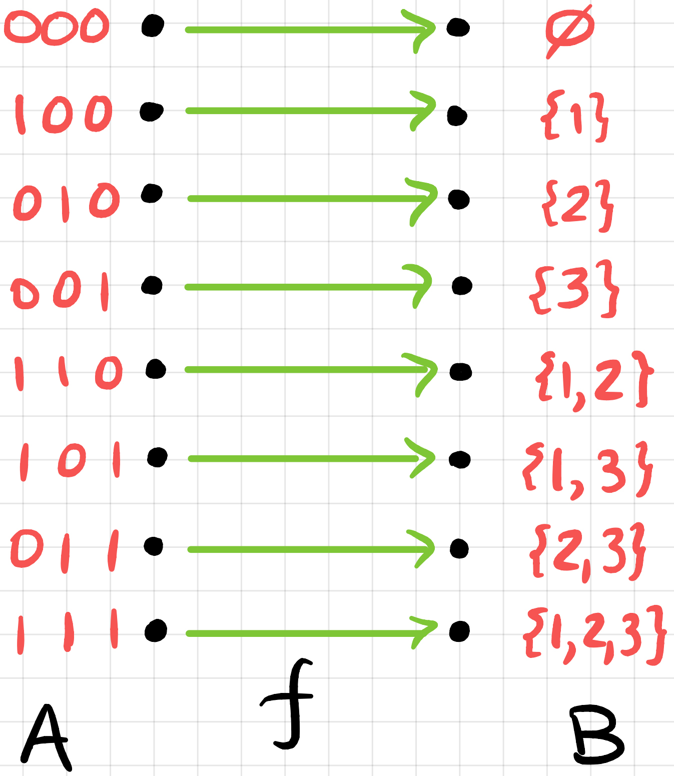


We saw earlier that all the $f(a)$ are distinct, i.e., f is 1-1.

It is also onto because $b = f(a)$ for $a = x^{-1}b \pmod{m}$

Example: $A = \{0, 1\}^n$ — 0-1 strings of length n

$B =$ set of all subsets of $\{1, 2, ..., n\}$



E.g. $n=3$

$$f(a_1 a_2 ... a_n) = \{i : a_i = 1\}$$

This proves that $|A| = |B|$

(Actually both have size 2^n)

What about infinite sets? $(\mathbb{N}, \mathbb{Z}, \mathbb{R}$ etc.$)$

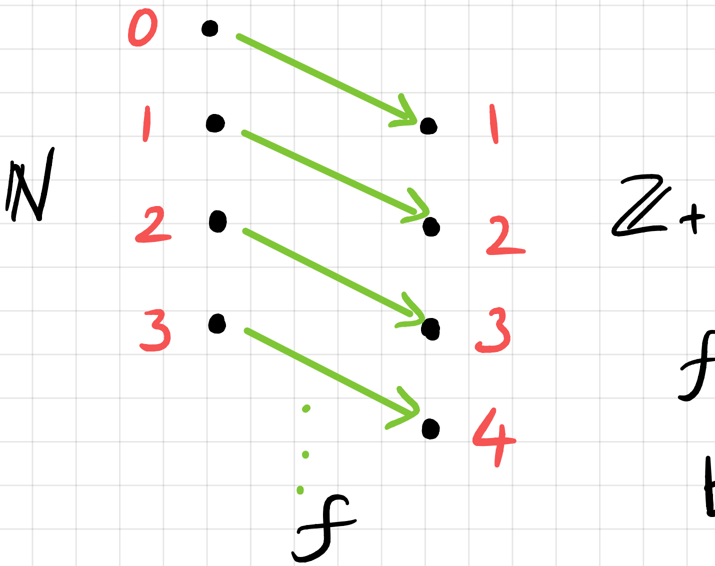
Use the same definition: two sets have same cardinality $\iff$ $\exists$ a bijection between them

Example: $\mathbb{N} = \{0, 1, 2, \dots\}$

$\mathbb{Z}_+ = \{1, 2, 3, \dots\}$

Q: Is $\mathbb{N}$ bigger than $\mathbb{Z}_+$?

A: No!



Note: Hilbert's Grand Hotel
- All rooms 1, 2, 3, ... occupied
- Can we accommodate one more guest?

$f(n) = n+1 \quad \forall n \in \mathbb{N}$

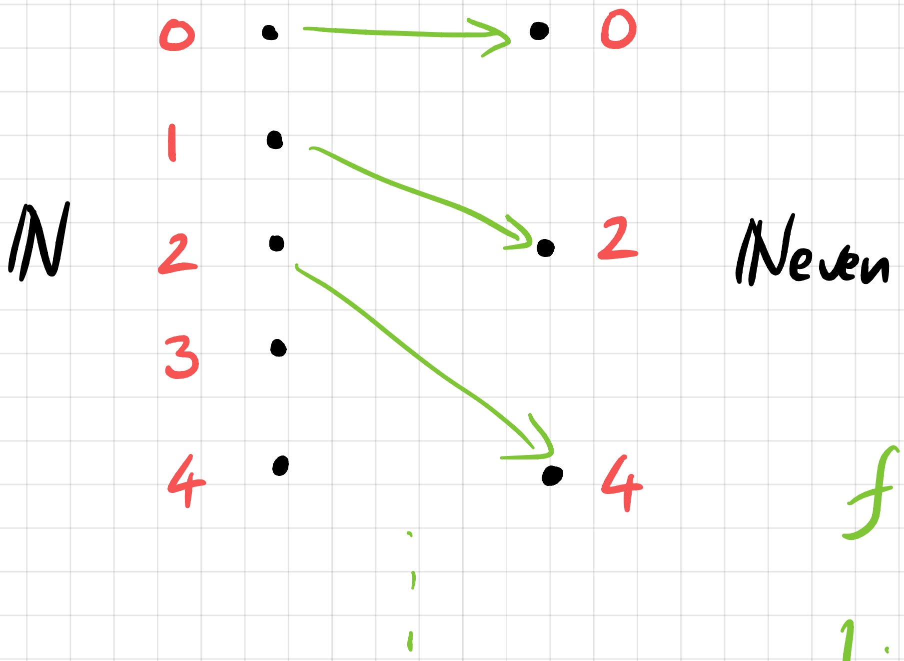
bijection! $\implies |\mathbb{N}| = |\mathbb{Z}_+|$

Example: $\mathbb{N} = \{0, 1, 2, ...\}$

$\mathbb{N}_{even} = \{0, 2, 4, ...\}$

Q: Is $\mathbb{N}$ bigger than $\mathbb{N}_{even}$?

A: No!



$f(n) = 2n$

bijection $\Rightarrow$ $|\mathbb{N}_{even}| = |\mathbb{N}|$

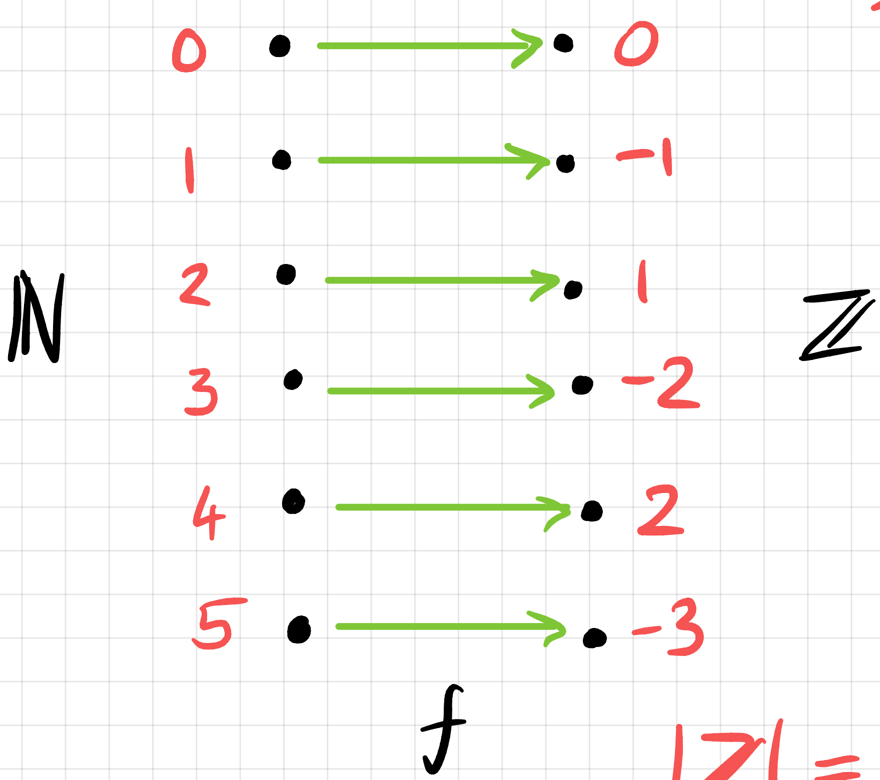
Example: $\mathbb{N} = \{0, 1, 2, \dots\}$

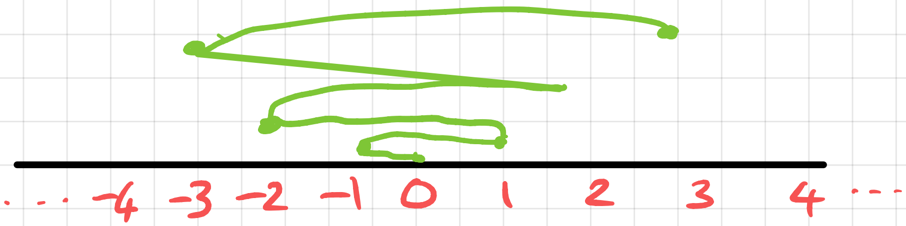
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Q: Is $\mathbb{Z}$ bigger than $\mathbb{N}$?

A: No!

$$f(n) = \begin{cases} \frac{n}{2} & n \text{ even} \\ -\left\lceil \frac{n}{2} \right\rceil & n \text{ odd} \end{cases}$$





$f(n)$ = nth element of $\mathbb{Z}$ visited by green path

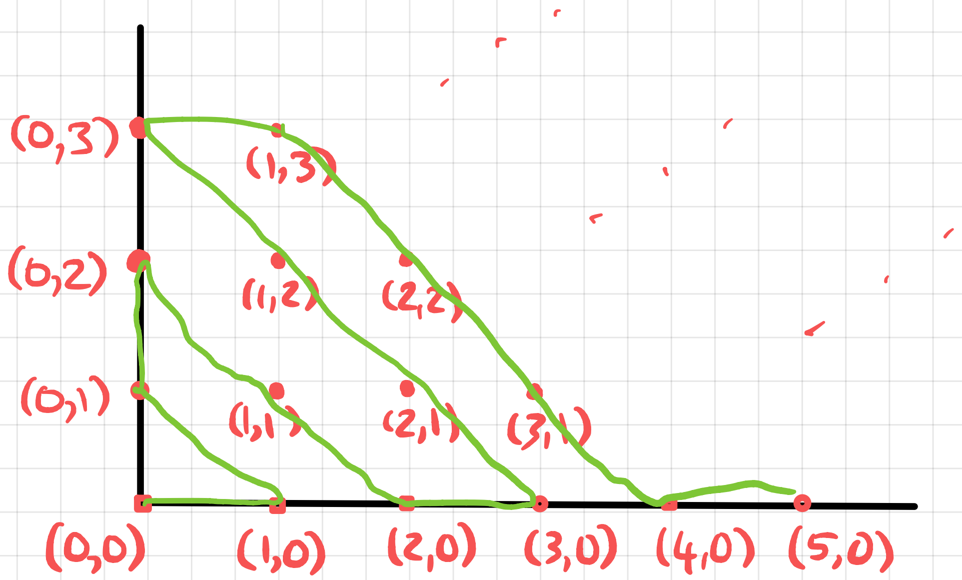
$$|\mathbb{Z}| = |\mathbb{N}|$$

Definition: A set S is **countable** if $\exists$ a bijection between S and $\mathbb{N}$ or some subset of $\mathbb{N}$

Examples (so far)

- every finite set is countable
- $\mathbb{N}$, $\mathbb{Z}_+$, $\mathbb{N}_{even}$ are countable
- $\mathbb{Z}$ is countable

What about $\mathbb{N} \times \mathbb{N}$ (pairs of natural numbers)?



$f(n) =$ nth pair (i,j) visited by green path

f is a bijection

$\Rightarrow |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$

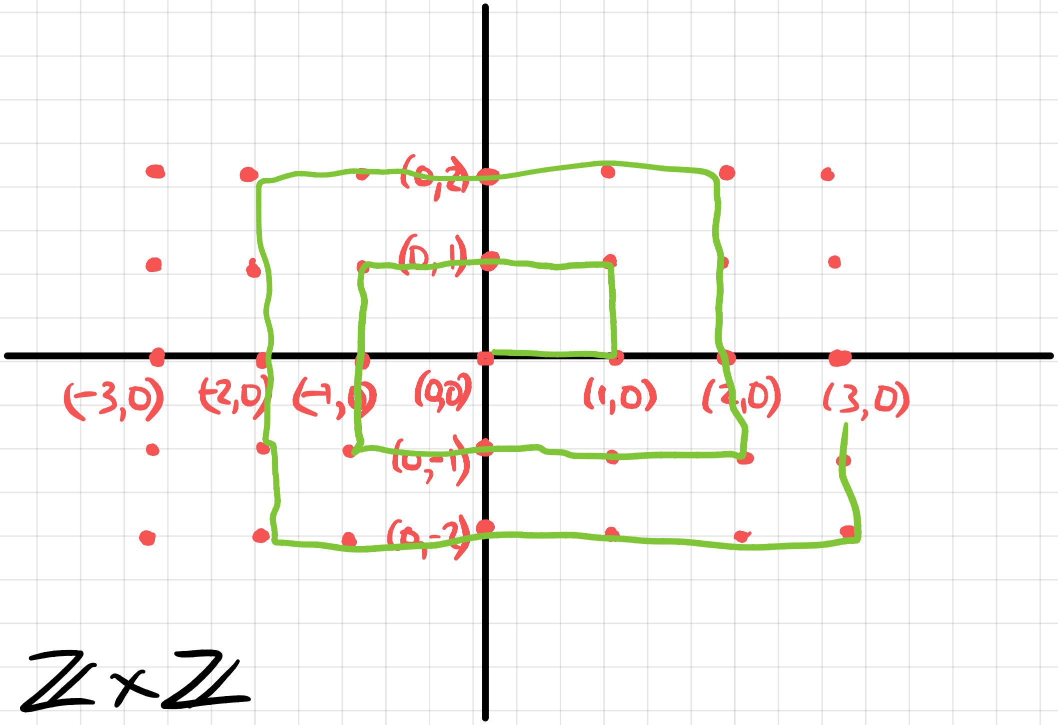
$f(n) =$

What about $\mathbb{Q}$ (rationals) ?

Similar to $\mathbb{N} \times \mathbb{N}$: every rational $q = \frac{a}{b} \to (a,b)$ with $\gcd(a,b) = 1$

So we can think of $\mathbb{Q}$ as a subset of $\mathbb{Z} \times \mathbb{Z}$

Mapping $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$



injection $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$

also injection $f : \mathbb{Q} \to \mathbb{N}$
(since $\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{Z}$)

Theorem [Cantor-Bernstein / Schröder-Bernstein]

If $\exists$ injection $f: A \to B$ and injection $g: B \to A$ then $\exists$ bijection $h: A \to B$

We've shown

injection $f: \mathbb{Q} \to \mathbb{N}$

injection $g: \mathbb{N} \to \mathbb{Q}$ (obvious since $\mathbb{N} \subseteq \mathbb{Q}$)

Hence $\exists$ bijection $h: \mathbb{Q} \to \mathbb{N}$

So $|\mathbb{Q}| = |\mathbb{N}|$

Two more examples:

1. $\{0,1\}^*$ = set of all 0-1 strings (of any length)

Enumerate as: $\overset{f(0)}{\varepsilon}, \overset{f(1)}{0}, \overset{f(2)}{1}, 00, 01, 10, 11, 000, 001, \ldots$

$\longrightarrow \{0,1\}^*$ countable

2. $\mathbb{N}(x)$: polynomials over $\mathbb{N}$ e.g. $6x^3+3x^2+2$

Encode as strings in $\{0,1,2\}^*$:

e.g. $6x^3+3x^2+2 \equiv \underbrace{110}\,2\,\underbrace{11}\,2\,\underbrace{\;}\,2\,\underline{10}$

This is an injection $\mathbb{N}(x) \longrightarrow \{0,1,2\}^*$

But $\{0,1,2\}^*$ is countable as above

$\Rightarrow \mathbb{N}(x)$ countable

Hilbert's Hotel: rooms 1, 2, 3, - - - -

- 1 extra guest shows up
- 10 . . . guests
- infinite # of new guests $\{1, 2, 3, ---\}$
- infinite # of buses, each carrying an infinite # of guests

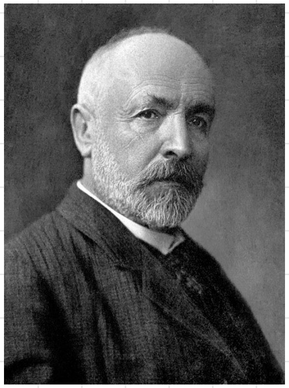
$\{1, 2, 3, \_\_\_\}$

$\{1, 2, 3, \_\_\_\}$

What about the reals, $\mathbb{R}$?

Note: $\exists$ infinitely many rationals between any two reals!

Theorem: $\mathbb{R}$ is uncountable – in fact, so is $[0,1]$



Georg
Cantor

Proof: By contradiction, using diagonalization

Suppose for that $[0,1]$ is countable.

Then it can be enumerated as follows:

$$f(0) = 0.37255\ldots$$
$$f(1) = 0.89898\ldots$$
$$f(2) = 0.19999\ldots$$
$$f(3) = 0.14285\ldots$$
$$\vdots$$

Note: any $r \in [0,1]$ can be written as an infinite decimal (no trailing zeros):

E.g. $1 = 0.9999\ldots$

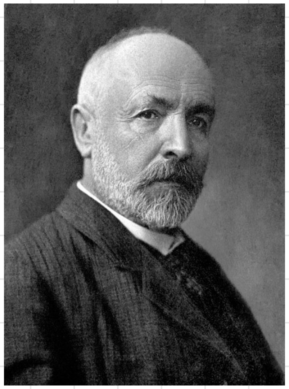
$1/7 = 0.1428571428\ldots$

$0.75 = 0.749999\ldots$

$1/\sqrt{2} = 0.707106\ldots$

$$\left.\begin{array}{l} x = 0.999\ldots \\ 10x = 9.999\ldots \end{array}\right\} \begin{array}{l} 9x = 9 \\ \Rightarrow x = 1 \end{array}$$

<u>Proof</u>: By contradiction, using <u>diagonalization</u>



Georg
Cantor

Suppose for ⨳ that $[0,1]$ is countable.

Then it can be enumerated as follows:

$$
\begin{aligned}
f(0) &= 0.\boxed{3}7255\ldots \\
f(1) &= 0.8\boxed{9}898\ldots \\
f(2) &= 0.19\boxed{9}99\ldots \\
f(3) &= 0.142\boxed{8}5\ldots \\
\vdots &\quad \vdots \qquad \vdots \quad \ddots
\end{aligned}
$$

Look at the <u>diagonal</u> digits

Consider number s that differs from each of these digits in the same place:

$$s = 0.4119\ldots$$

Hence s is not in enumeration ⨳

<u>Claim</u>: s is NOT in the enumeration

<u>Why</u>? Sp. $s = f(i)$ But this isn't true because ith digit of s $\neq$ ith digit of $f(i)$

Power sets

Defn: The power set of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.

If A is finite, we've seen that $|\mathcal{P}(A)| = 2^{|A|}$

What about infinite A ?

How large is $\mathcal{P}(\mathbb{N})$?

Note: $\mathcal{P}(\mathbb{N})$ contains infinite sets such as $\mathbb{N}$, $\{\text{primes}\}$, $\mathbb{N}_{\text{even}}$, etc.

Theorem : $\mathcal{P}(\mathbb{N})$ is uncountable

Proof : Diagonalization!

Sp. for ⨳ that $\mathcal{P}(\mathbb{N})$ is countable. Then $\exists$ enumeration of it as follows:

	0	1	2	3	4	5
$f(0)$	①	0	1	1	0	1
$f(1)$	1	①	1	1	1	1
$f(2)$	0	0	⓪	0	0	0
$f(3)$	1	1	0	①	1	0
⋮			⋮			

Construct set $S \subseteq \mathbb{N}$ by:

$$\rightarrow \quad S = \{ i \in \mathbb{N} : i \notin f(i) \}$$

Then $S \neq f(i)$ for any i, so S not in enumeration ⨳

$\Rightarrow$ $\mathcal{P}(\mathbb{N})$ uncountable.

Actually, $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$!

Proof : We give injections $f : \mathcal{P}(\mathbb{N}) \to [0,1]$ & $g : [0,1] \to \mathcal{P}(\mathbb{N})$

1. $f : \mathcal{P}(\mathbb{N}) \longrightarrow [0,1]$

   for $A \subseteq \mathbb{N}$, define $f(A) = \sum_{i \in A} 10^{-(i+1)}$

   e.g. $f(\mathbb{N}_{even}) = 0.101010\ldots$

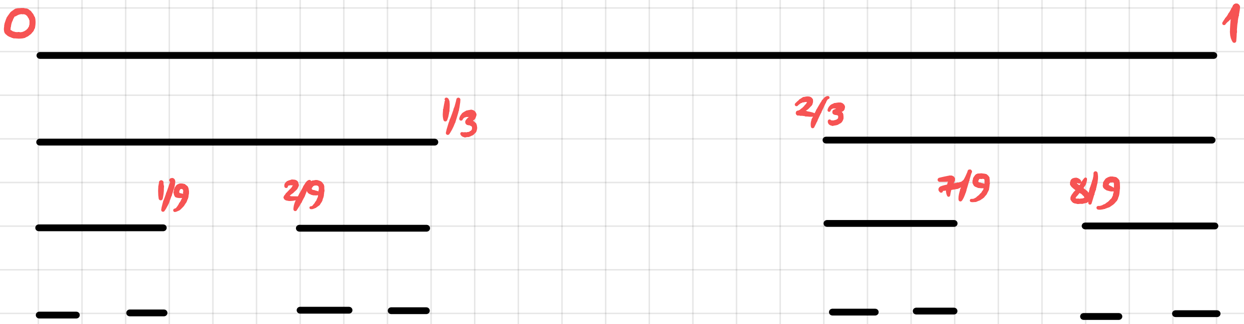
2. $g : [0,1] \longrightarrow \mathcal{P}(\mathbb{N})$

   $g(0.r_1 r_2 r_3 r_4 \cdots) = \{r_1, 10r_2, 100r_3, 1000r_4, \ldots\}$

Exercise : Show that $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$ (or $|[0,1] \times [0,1]| = |[0,1]|$)

(Need to find injection $f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$)

The Cantor Set (a weird uncountable set)



- start with $[0,1]$
- remove $(1/3, 2/3)$ [<u>open</u> interval in center]
- repeat recursively on remaining intervals

$C := \{ x \in [0,1] : x \text{ is not removed} \}$

Measure of C: $1 \to \frac{2}{3} \to \left(\frac{2}{3}\right)^2 \to \cdots \to \left(\frac{2}{3}\right)^n \to \cdots \to 0$ as $n \to \infty$

But: C is not empty!

E.g. C contains endpoints $\{0, 1, 1/3, 2/3, 1/9, 2/9, 7/9, 8/9, \dots\}$

Also contains (e.g.) $1/4$: $\frac{1}{4} < \frac{1}{3}$, $\frac{1}{4} > \frac{2}{9}$, $\frac{1}{4} < \frac{7}{27}$, ...

Theorem : C is uncountable

Proof : Write any $r \in [0,1]$ in ternary

$$\text{E.g. } \frac{1}{3} = 0.1 = 0.0222\ldots$$

$$\frac{2}{3} = 0.2 = 0.1222\ldots$$

First cut : removes all numbers $0.1xxx\ldots$

Second cut : " " " $0.01xxx\ldots$ & $0.21xxx\ldots$

... and so on

Hence :

$$\boxed{x \in C \iff \text{ternary rep}^{n} \text{ of } x \text{ consists only of } 0\text{'s } \& \ 2\text{'s}}$$

Now define injection $f : [0,1] \longrightarrow C$ by

$$f(0.1001110\ldots) = 0.2002220\ldots$$

Since also $C \subseteq [0,1]$ we have $|C| = |[0,1]|$

Orders of Infinity

$|\mathbb{N}| = \aleph_0$ ("aleph-zero")

$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} = \mathbf{c}$ ("cardinality of the continuum")

Higher orders of infinity: $\aleph_1, \aleph_2, \ldots$

Continuum hypothesis: $\aleph_1 = \mathbf{c}$, i.e., there's nothing between $|\mathbb{N}|$ and $|\mathbb{R}|$

Gödel/Cohen: Continuum hypothesis is independent of the axioms of set theory