

CS70 — SPRING 2026

LECTURE 12: FEB. 26

Today: Countable & Uncountable Sets

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

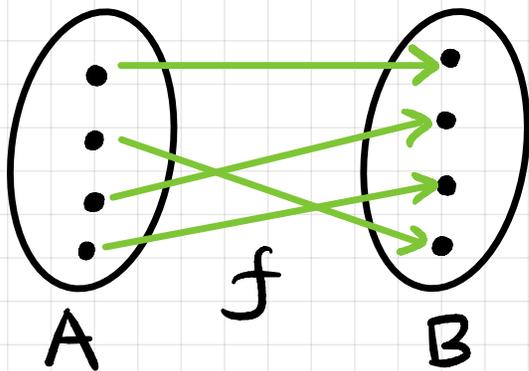
Why?

- Background for counting
- Understanding sets like \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} , ...
- 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 $f: A \rightarrow B$ is a bijection if f is both

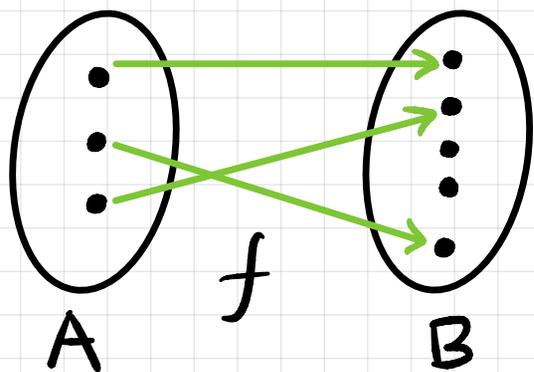
(i) one-to-one (1-1), i.e.,

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

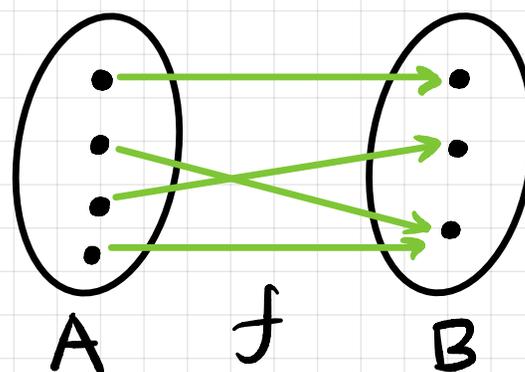
and

(ii) onto, i.e.,

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



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



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

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

Note: Every 1-1 function has an inverse function.
The inverse of a bijection is also a bijection.

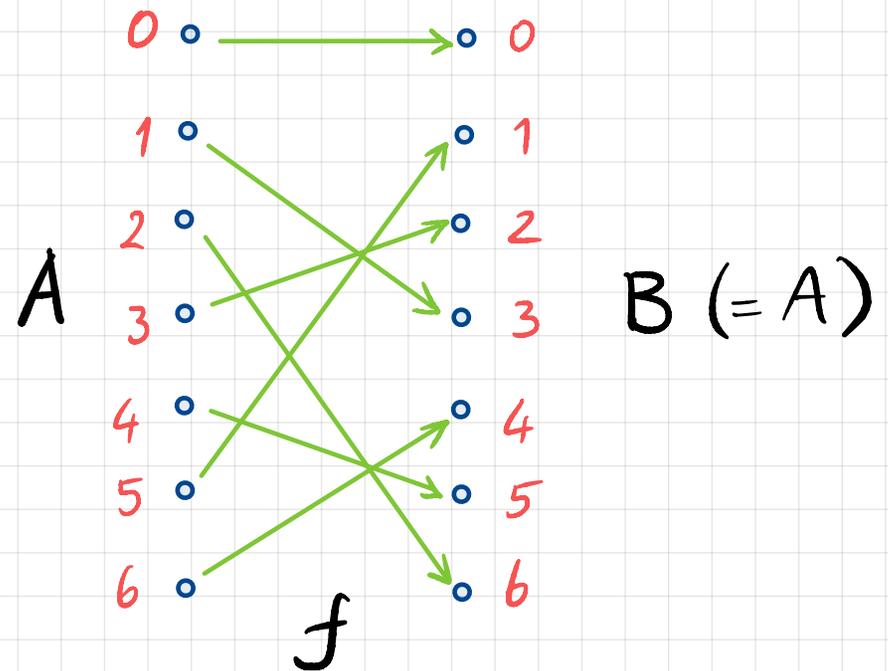
Example: $A = B = \{0, 1, \dots, m-1\}$

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

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

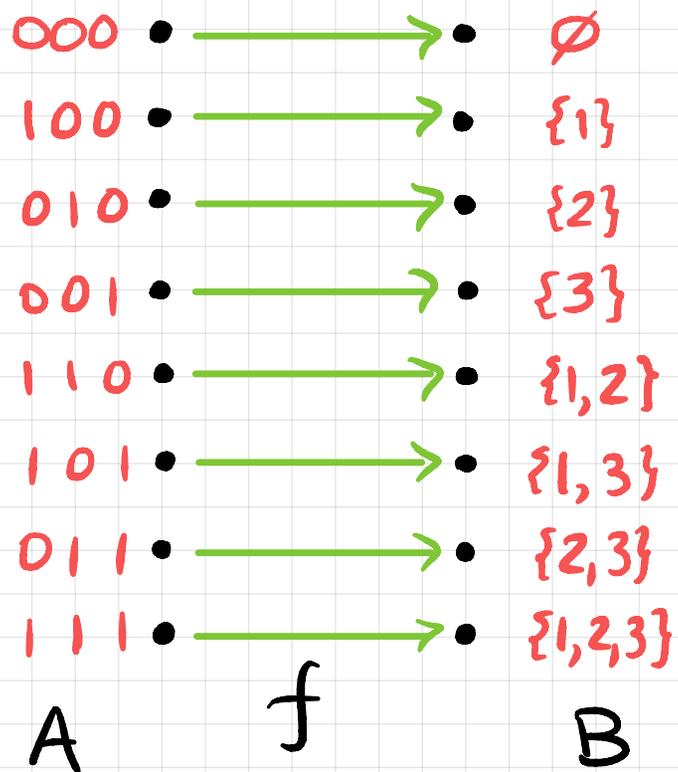
We saw earlier that all the $f(a)$ are distinct, i.e., f is 1-1.

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 $\{1, 2, \dots, n\}$



E.g. $n=3$

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

This proves that $|A| = |B|$
(Actually both have size 2^n)

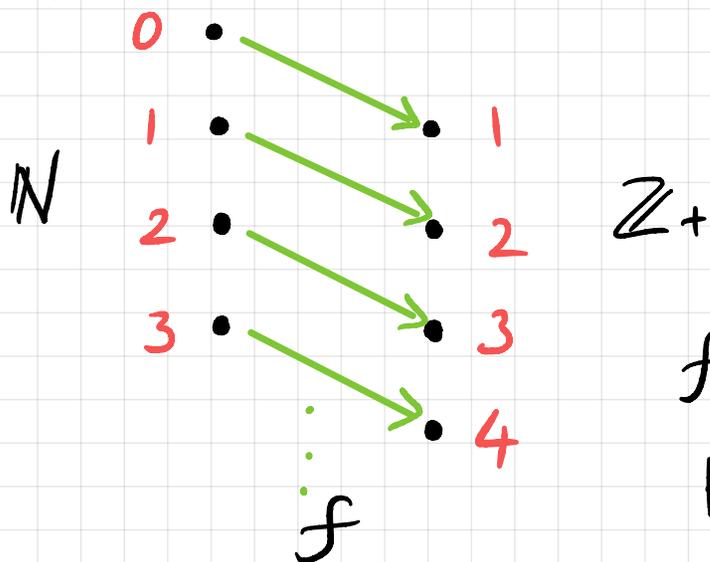
What about infinite sets ? (\mathbb{N} , \mathbb{Z} , \mathbb{R} etc.)

Use the same definition: two sets have same cardinality $\Leftrightarrow \exists$ 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! $\Rightarrow |\mathbb{N}| = |\mathbb{Z}_+|$

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

$N_{\text{even}} = \{0, 2, 4, \dots\}$

Q: Is N bigger than N_{even} ?

A: No!

	0	•		•	0
	1	•			
N	2	•		•	2
	3	•			
	4	•		•	4
		⋮			
		⋮			

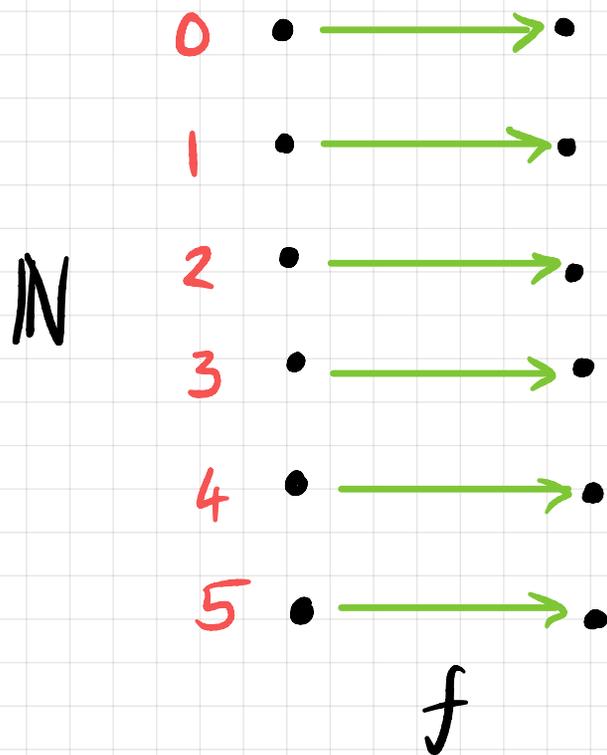
N_{even}

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

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

Q: Is Z bigger than N ?

A: No!

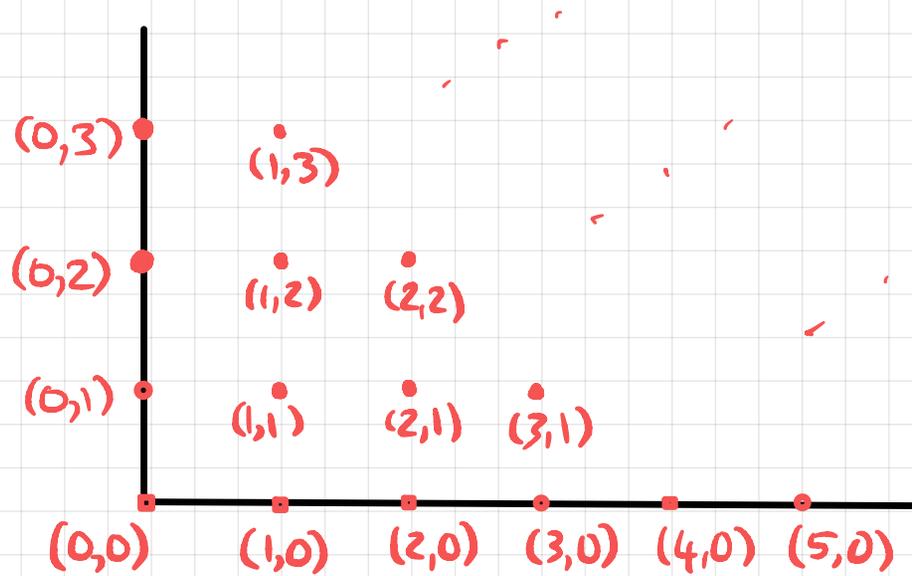


Definition: A set S is countable if \exists a bijection between S and \mathbb{N} or some subset of \mathbb{N}

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) ?



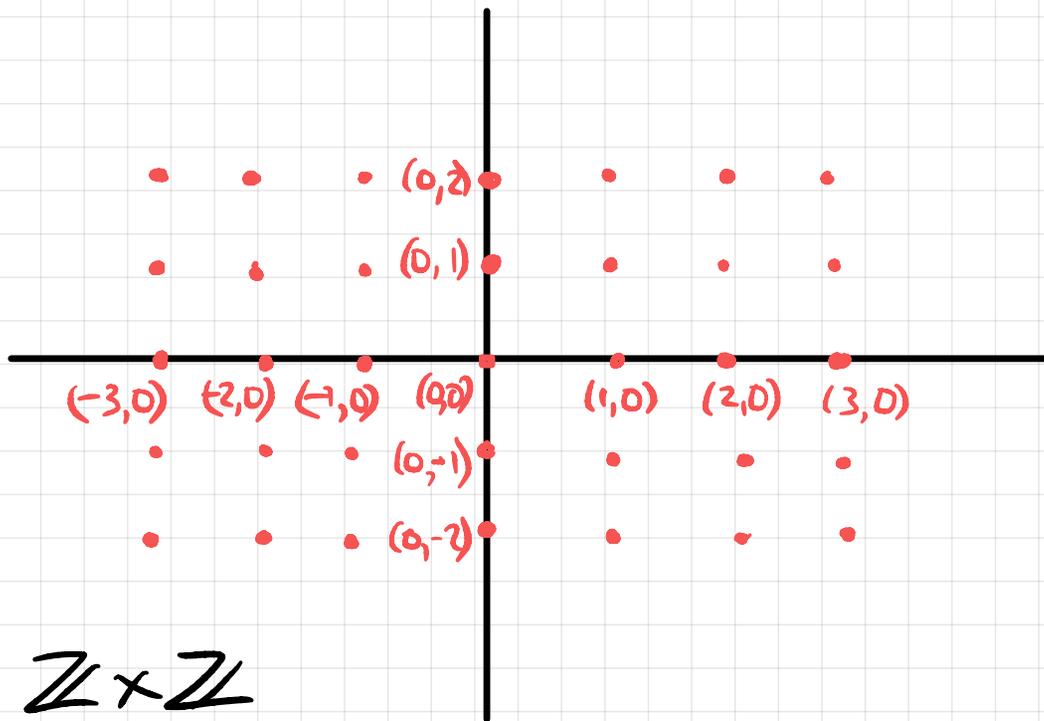
$$f(n) =$$

What about \mathbb{Q} (rationals) ?

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

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

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



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

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

Theorem [Cantor - Bernstein / Schröder - Bernstein]

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

We've shown

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

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

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

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

Two more examples:

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

Enumerate as: $\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, \dots$

$\rightarrow \{0, 1\}^*$ 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. $6x^3 + 3x^2 + 2 \equiv$

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

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

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

What about the reals, \mathbb{R} ?

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

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

Proof: By contradiction, using diagonalization

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

Then it can be enumerated as follows:

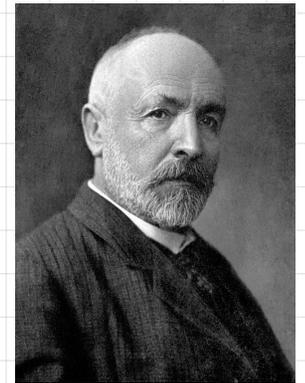
$$f(0) = 0.37255 \dots$$

$$f(1) = 0.89898 \dots$$

$$f(2) = 0.19999 \dots$$

$$f(3) = 0.14285 \dots$$

\vdots
 \vdots
 \vdots



Georg
Cantor

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

$$\text{E.g. } 1 = 0.9999 \dots$$

$$\frac{1}{7} = 0.1428571428 \dots$$

$$0.75 = 0.749999 \dots$$

$$\frac{1}{\sqrt{2}} = 0.707106 \dots$$

Proof: By contradiction, using diagonalization

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

Then it can be enumerated as follows:

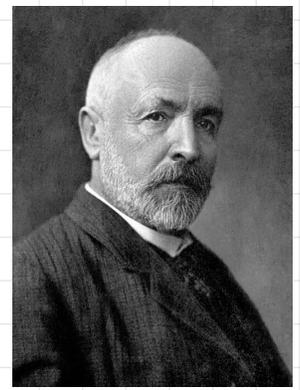
$$f(0) = 0.37255 \dots$$

$$f(1) = 0.89898 \dots$$

$$f(2) = 0.19999 \dots$$

$$f(3) = 0.14285 \dots$$

\vdots \vdots \vdots



Georg
Cantor

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}_{even} , etc.

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

Proof : Diagonalization!

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

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

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

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

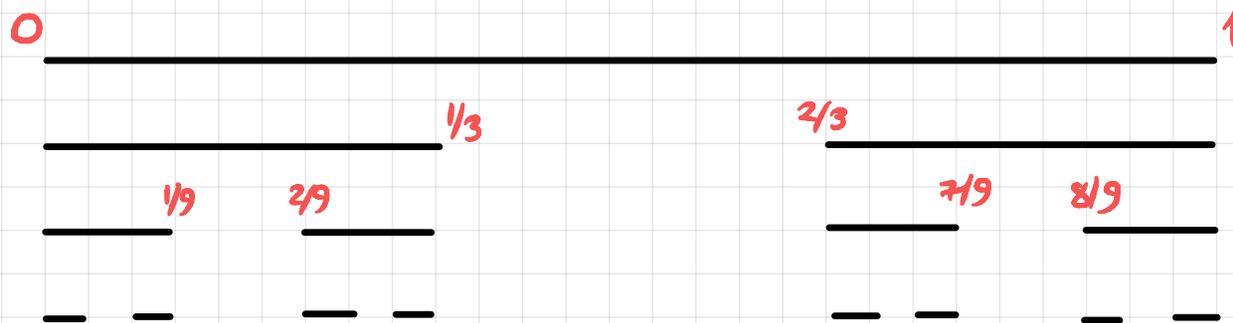
e.g. $f(\mathbb{N}_{\text{even}}) = 0.101010\dots$

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

$g(0.r_1r_2r_3r_4\dots) = \{r_1, 10r_2, 100r_3, 1000r_4, \dots\}$

Exercise: Show that $|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|$ (or $|[0, 1] \times [0, 1]| = |[0, 1]|$)
(Need to find injection $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$)

The Cantor Set (a weird uncountable set)



- start with $[0, 1]$
- remove $(\frac{1}{3}, \frac{2}{3})$ [open interval in center]
- repeat recursively on remaining intervals

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

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

But : C is not empty !

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

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

Theorem: C is uncountable

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

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

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

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

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

... and so on

Hence: $x \in C \iff$ ternary rep.ⁿ of x consists only of 0's & 2's

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

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

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

Orders of Infinity

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

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

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

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

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