Infinity

From counting to categories

Contents

1 A part can be as large as the whole

Let us begin with a question that sounds elementary and yet completely changes the way we think about size:

Are there more natural numbers, or more even numbers?

Let

$$\mathcal{E} = \{0, 2, 4, 6, \dots\} \subset \mathbb{N}.$$

Because there are also odd numbers, ordinary intuition suggests that $\mathcal{E}$ should be smaller than $\mathbb{N}$. But now consider the function

$$f : \mathcal{E} \to \mathbb{N}, \qquad f(2n) = n.$$

Its inverse is

$$f^{-1} : \mathbb{N} \to \mathcal{E}, \qquad f^{-1}(n) = 2n.$$

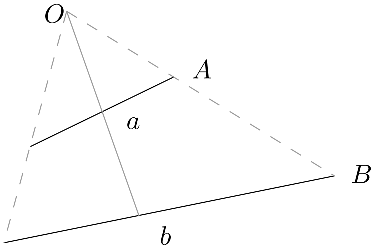
So every even number matches exactly one natural number, and every natural number matches exactly one even number.

In other words, there is a *bijection* between $\mathcal{E}$ and $\mathbb{N}$. Therefore

there are just as many even numbers as natural numbers.

This is impossible for finite sets, but it happens naturally for infinite ones.

A geometric example is just as surprising. Consider two segments A and B, with B longer than A:



Projecting from the point O sends each point of A to exactly one point of B, and conversely each point of B comes from exactly one point of A. So again the two sets have the same size.

This raises the real question:

How do we count infinite sets?

Definition 1.1. *A set X is called* infinite *if there exists a proper subset $Y \subsetneq X$ and a bijection $X \to Y$.*

This is often called *Dedekind infinity.* It captures the idea that an infinite set can be put into one-to-one correspondence with a proper part of itself.

2 Countable infinity

2.1 Natural numbers and integers

The set of integers looks larger than the set of natural numbers because it extends in both positive and negative directions. But that appearance is misleading.

Define

$$f : \mathbb{N} \to \mathbb{Z}, \qquad f(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even,} \\ -\frac{n+1}{2}, & \text{if } n \text{ is odd.} \end{cases}$$

Then

$$0 \mapsto 0, \quad 1 \mapsto -1, \quad 2 \mapsto 1, \quad 3 \mapsto -2, \quad 4 \mapsto 2, \quad \ldots$$

So we can list all integers in a sequence:

$$0, -1, 1, -2, 2, -3, 3, \ldots$$

Hence $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality.

2.2 Why the rationals are still countable

At first sight, the set of rational numbers should be much bigger than the set of integers. Between any two integers there are infinitely many rational numbers. Nevertheless, Cantor showed that the rational numbers are still countable.

The positive rational numbers are fractions

$$\frac{p}{q} \qquad (p, q \in \mathbb{N}_{>0}).$$

Imagine arranging them in an infinite grid: row p, column q, entry p/q.

$$\begin{tikzcd}
1/1 \arrow[d] & 1/2 \arrow[r] & 1/3 \arrow[dl] & 1/4 \arrow[r] & 1/5 \arrow[dl] & 1/6 \arrow[r] & \cdots \\
2/1 \arrow[ur] & 2/2 \arrow[dl] & 2/3 \arrow[ur] & 2/4 \arrow[dl] & 2/5 \arrow[ur] & 2/6 & \cdots \\
3/1 \arrow[d] & 3/2 \arrow[ur] & 3/3 \arrow[dl] & 3/4 \arrow[ur] & 3/5 & 3/6 & \cdots \\
4/1 \arrow[ur] & 4/2 \arrow[dl] & 4/3 \arrow[ur] & 4/4 & 4/5 & 4/6 & \cdots \\
5/1 \arrow[d] & 5/2 \arrow[ur] & 5/3 & 5/4 & 5/5 & 5/6 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{tikzcd}$$

The idea is to move through the grid along successive diagonals:

$$\frac{1}{1}, \quad \frac{1}{2}, \frac{2}{1}, \quad \frac{3}{1}, \frac{2}{2}, \frac{1}{3}, \quad \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \quad \ldots$$

Each diagonal contains only finitely many fractions, so it can be traversed completely before moving to the next one.

Two points are important.

1. Every positive rational number appears somewhere in the grid.
2. Some numbers appear more than once, because

   $$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \cdots .$$

   So, when a fraction is not in lowest terms, we simply skip it.

For example, the beginning of the list of *reduced* positive fractions is

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{3}{1}, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}, \ldots$$

This already gives a way to label every positive rational number with a natural number.

To obtain all rational numbers, include 0 and alternate positive and negative fractions, for instance:

$$0, 1, -1, \frac{1}{2}, -\frac{1}{2}, 2, -2, \frac{1}{3}, -\frac{1}{3}, \ldots$$

Hence $\mathbb{Q}$ is countable.

Remark 2.1. *There are* two different *famous "diagonal" ideas associated with Cantor:*

- *a* diagonal enumeration *used to list the rationals;*
- *a* diagonal construction *used to prove that the reals cannot be listed.*

They go in opposite directions: the first builds a list, the second proves that no list can possibly exist.

3 A larger infinity: the real numbers

The next question is the decisive one:

Can the real numbers be listed like the integers and rationals?

Cantor's answer is *no.* The interval

$$J = (0, 1)$$

already contains too many numbers to be counted by $\mathbb{N}$.

3.1 The setup of the contradiction

Assume, for contradiction, that there is a bijection

$$\mathbb{N} \longrightarrow J.$$

Then we could arrange all numbers in $(0, 1)$ in a list:

$$x_0, x_1, x_2, \ldots$$

where each x_n has a decimal expansion

$$x_n = 0.a_{n0}a_{n1}a_{n2}a_{n3}\ldots$$

with digits $a_{nk} \in \{0, 1, 2, \ldots, 9\}$.

So the list would look like this:

index in $\mathbb{N}$	supposed complete list of numbers in $J = (0, 1)$
0	$x_0 = 0.a_{00}a_{01}a_{02}a_{03}a_{04}\ldots$
1	$x_1 = 0.a_{10}a_{11}a_{12}a_{13}a_{14}\ldots$
2	$x_2 = 0.a_{20}a_{21}a_{22}a_{23}a_{24}\ldots$
3	$x_3 = 0.a_{30}a_{31}a_{32}a_{33}a_{34}\ldots$
$\vdots$	$\vdots$

This table is worth reading very carefully.

- Row n contains the decimal digits of the number x_n.
- Column k records the k-th decimal digit of all numbers in the list.
- The *diagonal digits* are

  $$a_{00}, a_{11}, a_{22}, a_{33}, \ldots$$

  obtained by taking one digit from row 0, then one from row 1, then one from row 2, and so on.

Now we build a new number

$$z = 0.e_0e_1e_2e_3\dots$$

by changing the diagonal digits. To avoid the usual ambiguity of decimal expansions such as

$$0.24999\cdots = 0.25,$$

we choose each e_n to be either 1 or 2:

$$e_n = \begin{cases} 1, & \text{if } a_{nn} \neq 1, \\ 2, & \text{if } a_{nn} = 1. \end{cases}$$

In particular, $e_n \neq a_{nn}$ for every n.

This immediately implies the key property:

- z differs from x_0 in the first chosen diagonal digit;
- z differs from x_1 in the second chosen diagonal digit;
- z differs from x_2 in the third chosen diagonal digit;
- and, in general, z differs from x_n in the n-th diagonal position.

So z cannot equal x_0, and cannot equal x_1, and cannot equal x_2, and so on. Therefore z is *not* in the list.

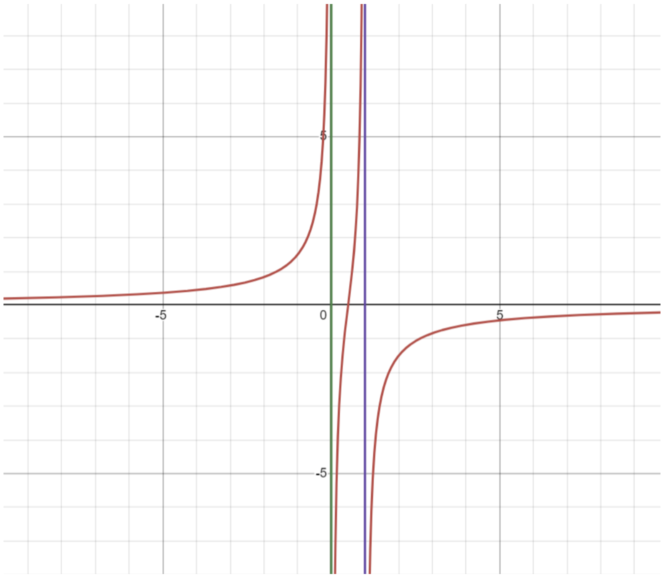
But $z \in (0,1)$, because it is a decimal number beginning with 0. and its digits are only 1 and 2. This contradicts the assumption that the list contained *every* element of $(0,1)$.

Hence no bijection $\mathbb{N} \to J$ exists.

Theorem 3.1. *The interval $J = (0,1)$ is not countable.*

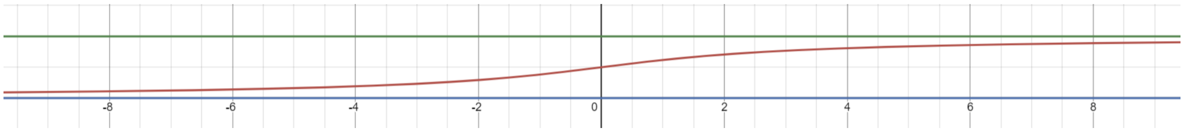
The interval $(0,1)$ already has the same cardinality as all of $\mathbb{R}$. One explicit bijection is

$$\phi : (0,1) \to \mathbb{R}, \qquad \phi(x) = \frac{2x-1}{x-x^2}.$$



The inverse function is

$$\phi^{-1} : \mathbb{R} \to (0,1), \qquad \phi^{-1}(y) = \frac{2}{\sqrt{y^2+4}+2-y}.$$



Therefore, if $\mathbb{R}$ were countable, then $(0,1)$ would also be countable, which we have just proved is impossible.

So the real numbers form a strictly larger infinity than the natural numbers.

4 Cardinality

Definition 4.1. *Two sets X and Y have the same* cardinality *if there exists a bijection $X \to Y$.*

For finite sets, cardinality is just the number of elements. For infinite sets, cardinality is a new kind of number, called a *transfinite cardinal*.

Definition 4.2. *Let X and Y be sets.*

- $\operatorname{card}(X) \leq \operatorname{card}(Y)$ *if and only if there exists an injective map $X \to Y$;*
- $\operatorname{card}(X) \geq \operatorname{card}(Y)$ *if and only if there exists a surjective map $X \to Y$;*
- $\operatorname{card}(X) = \operatorname{card}(Y)$ *if and only if there exists a bijection $X \to Y$.*

The cardinality of $\mathbb{N}$ is denoted by $\aleph_0$ and is called *aleph-zero*. The cardinality of $\mathbb{R}$ is often denoted by c, for *continuum*.

Definition 4.3. *A set is called* countable *if it is finite or has cardinality $\aleph_0$.*

Thus $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are countable, while $\mathbb{R}$ is not.

Informally, every infinite set should contain a countably infinite subset. One tries to prove this by choosing distinct elements one after another:

$$x_0,\ x_1,\ x_2,\ \ldots$$

This shows heuristically that an infinite set must have at least $\aleph_0$ elements. To make this completely rigorous in full generality, one needs a form of the Axiom of Choice; see, for example, [Hal60, Jec03].

5 The Cantor–Bernstein theorem

Suppose we know that X injects into Y and Y injects into X. Is that enough to conclude that they have the same cardinality? For finite sets the answer is yes, but for infinite sets this is far from obvious.

Theorem 5.1 (Cantor–Bernstein)**.** *If* $\operatorname{card}(X) \leq \operatorname{card}(Y)$ *and* $\operatorname{card}(Y) \leq \operatorname{card}(X)$*, then* $\operatorname{card}(X) = \operatorname{card}(Y)$.

Proof. By assumption, there exist injective maps

$$f : X \to Y, \qquad g : Y \to X.$$

We will construct a bijection $h : X \to Y$.

Define

$$X_0 := X \setminus g(Y),$$

and recursively

$$X_{n+1} := g\big(f(X_n)\big) \qquad (n \geq 0).$$

Set

$$C := \bigcup_{n\geq 0} X_n \subseteq X.$$

Now define

$$h : X \to Y$$

by

$$h(x) := \begin{cases} f(x), & \text{if } x \in C, \\ g^{-1}(x), & \text{if } x \notin C. \end{cases}$$

This is well defined. Indeed, if $x \notin C$, then in particular $x \notin X_0$, so

$$x \in g(Y).$$

Since g is injective, there is a unique $y \in Y$ such that $g(y) = x$, and therefore $g^{-1}(x)$ makes sense.

We claim that h is bijective.

First we prove that h is injective. Suppose that $h(x) = h(x')$.

If both $x, x' \in C$, then

$$f(x) = f(x'),$$

hence $x = x'$ because f is injective.

If both $x, x' \notin C$, then

$$g^{-1}(x) = g^{-1}(x'),$$

so $x = x'$.

It remains to rule out the mixed case. Assume $x \in C$ and $x' \notin C$. Then

$$f(x) = g^{-1}(x').$$

Applying g, we get

$$g(f(x)) = x'.$$

Since $x \in C$, there exists $n \geq 0$ such that $x \in X_n$, and therefore

$$x' = g(f(x)) \in g(f(X_n)) = X_{n+1} \subseteq C,$$

contradicting $x' \notin C$. Thus the mixed case is impossible, and h is injective.

Now we prove that h is surjective. Let $y \in Y$, and set

$$x := g(y) \in X.$$

If $x \notin C$, then

$$h(x) = g^{-1}(x) = g^{-1}(g(y)) = y.$$

If $x \in C$, then $x \notin X_0$ because $x \in g(Y)$, so in fact $x \in X_n$ for some $n \geq 1$. By definition of X_n,

$$x \in X_n = g(f(X_{n-1})),$$

so there exists $z \in X_{n-1} \subseteq C$ such that

$$x = g(f(z)).$$

Since g is injective and $x = g(y)$, it follows that

$$y = f(z) = h(z).$$

Hence y lies in the image of h.

Therefore h is both injective and surjective, so it is a bijection. This proves that $\operatorname{card}(X) = \operatorname{card}(Y)$. □

This result is powerful because it says that two opposite injections are enough to produce a bijection, even if the two injections seem unrelated.

6 The square and the interval

After learning that $\mathbb{R}$ is larger than $\mathbb{N}$, a natural guess is that the square

$$K = (0,1) \times (0,1) \subset \mathbb{R}^2$$

should be larger than the interval $J = (0,1)$. After all, the square is two-dimensional, while the interval is one-dimensional. Surprisingly, they have the same cardinality.

Lemma 6.1. *Let $a > 1$ be a real number. Then*

$$\sum_{n=1}^{\infty} \frac{1}{a^n} = \frac{1}{a-1}.$$

More generally, if $|r| < 1$, then

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1-r}.$$

Proof. We prove the second formula first. For every integer $N \geq 0$, let

$$S_N = 1 + r + r^2 + \cdots + r^N.$$

Multiplying by $1 - r$, we get

$$(1-r)S_N = (1 + r + r^2 + \cdots + r^N) - (r + r^2 + \cdots + r^{N+1}) = 1 - r^{N+1}.$$

Therefore

$$S_N = \frac{1 - r^{N+1}}{1-r}.$$

Now assume $|r| < 1$. Then $r^{N+1} \to 0$ as $N \to \infty$, so passing to the limit gives

$$\sum_{n=0}^{\infty} r^n = \lim_{N\to\infty} S_N = \lim_{N\to\infty} \frac{1 - r^{N+1}}{1-r} = \frac{1}{1-r}.$$

To obtain the first formula, apply this with $r = \frac{1}{a}$. Since $a > 1$, we have $\left|\frac{1}{a}\right| < 1$, and hence

$$\sum_{n=0}^{\infty} \frac{1}{a^n} = \frac{1}{1-\frac{1}{a}} = \frac{a}{a-1}.$$

Subtracting the first term 1, we find $\sum_{n=1}^{\infty} \frac{1}{a^n} = \frac{a}{a-1} - 1 = \frac{1}{a-1}$. ☐

Remark 6.2. *A small subtlety must be addressed before interleaving decimal digits. Decimal expansions are not always unique. For example,*

$$0.999999\ldots = 1.$$

Indeed, Lemma 6.1 yields

$$0.999999\ldots = \sum_{n=1}^{\infty} \frac{9}{10^n} = 9 \sum_{n=1}^{\infty} \frac{1}{10^n} = 9 \cdot \frac{\frac{1}{10}}{1 - \frac{1}{10}} = 1.$$

More generally, every terminating decimal admits a second expansion ending in infinitely many 9's; for instance,

$$0.5000\ldots = 0.4999\ldots.$$

To avoid this ambiguity, from now on we make the following canonical choice*: every real number in $(0,1)$ will always be written in its unique decimal expansion that is* not eventually equal to 9*. In other words, we never use decimal expansions with a tail of the form*

$$\ldots 999999 \ldots$$

Proposition 6.3. *Let $J = (0, 1)$ and $K = J \times J$. Write each $x \in J$ in its canonical decimal expansion*

$$x = 0.a_1 a_2 a_3 \ldots, \qquad y = 0.b_1 b_2 b_3 \ldots,$$

where the expansion is not eventually equal to 9. Then the rule

$$F : K \to J, \qquad F(x, y) = 0.a_1 b_1 a_2 b_2 a_3 b_3 \ldots$$

defines an injective map.

Proof. First we check that F is well defined. Since we have fixed the canonical decimal expansion of each element of J, the digits a_i and b_i are uniquely determined. We must also check that the decimal

$$0.a_1 b_1 a_2 b_2 a_3 b_3 \ldots$$

represents a point of J. Clearly it lies in $[0, 1]$. It cannot be equal to 1, because its decimal expansion is not eventually equal to 9: if from some point on all digits $a_1, b_1, a_2, b_2, \ldots$ were equal to 9, then both sequences (a_i) and (b_i) would themselves be eventually equal to 9, contradicting the fact that x and y are written in canonical form. It is also not equal to 0, since this would force $x = y = 0$, impossible because $x, y \in (0, 1)$. Hence $F(x, y) \in (0, 1) = J$.

Now let $(x, y), (x', y') \in K$ and suppose that

$$F(x, y) = F(x', y').$$

Write

$$x = 0.a_1 a_2 a_3 \ldots, \qquad y = 0.b_1 b_2 b_3 \ldots,$$

and

$$x' = 0.a'_1 a'_2 a'_3 \ldots, \qquad y' = 0.b'_1 b'_2 b'_3 \ldots$$

in canonical form. Then

$$0.a_1 b_1 a_2 b_2 a_3 b_3 \ldots = 0.a'_1 b'_1 a'_2 b'_2 a'_3 b'_3 \ldots$$

as canonical decimal expansions. Therefore the digits must agree term by term:

$$a_i = a'_i, \qquad b_i = b'_i \qquad \text{for every } i \geq 1.$$

It follows that $x = x'$ and $y = y'$. Thus F is injective. □

Remark 6.4. *The map F is not surjective. For example, consider*

$$z = 0.19191919 \ldots \in J.$$

If $z = F(x, y)$, then the odd-position digits would give

$$x = 0.111111 \ldots,$$

while the even-position digits would give

$$y = 0.999999 \ldots = 1,$$

which is impossible since y should belong to $J = (0, 1)$. Hence $z \notin \mathrm{Im}(F)$.

On the other hand, the map

$$J \to K, \qquad x \mapsto \left(x, \frac{1}{2}\right)$$

is clearly injective. By Cantor–Bernstein, $\mathrm{card}(K) = \mathrm{card}(J) = c$.

7 Power sets are larger

If the square did not produce a bigger infinity, what should we try next? Cantor's answer was the *power set*.

For any set X, let $\mathcal{P}(X)$ be the set of all subsets of X.

Theorem 7.1 (Cantor)**.** *For every set X, there is no surjective map*

$$X \to \mathcal{P}(X).$$

Proof. Assume that $\varphi : X \to \mathcal{P}(X)$ is surjective. Define

$$D = \{x \in X \mid x \notin \varphi(x)\}.$$

Since $D \subseteq X$, it is an element of $\mathcal{P}(X)$. Because φ is surjective, there exists some $z \in X$ such that

$$\varphi(z) = D.$$

Now ask whether $z \in D$.

If $z \in D$, then by the definition of D we must have $z \notin \varphi(z) = D$, contradiction.

If $z \notin D$, then by the definition of D we must have $z \in \varphi(z) = D$, contradiction.

So no such z can exist. Therefore D is not in the image of φ, contradicting surjectivity. ☐

Corollary 7.2. *For every set X,*

$$\operatorname{card}(X) < \operatorname{card}(\mathcal{P}(X)).$$

Proof. The map

$$X \to \mathcal{P}(X), \qquad x \mapsto \{x\}$$

is injective. Cantor's theorem says there is no surjection in the opposite sense. Hence $\mathcal{P}(X)$ is strictly larger. ☐

Applying the theorem repeatedly gives an endless tower of larger and larger infinities:

$$\aleph_0 < c < \operatorname{card}(\mathcal{P}(\mathbb{R})) < \operatorname{card}(\mathcal{P}(\mathcal{P}(\mathbb{R}))) < \cdots .$$

Definition 7.3. *Let X be a set and let $A \subseteq X$. The* characteristic function *of A is the map*

$$\chi_A : X \to \{0,1\}, \qquad \chi_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A. \end{cases}$$

Thus a subset $A \subseteq X$ can be encoded by a 0-1 valued function on X.

Definition 7.4. *Let X be a set. Since the assignment*

$$A \longmapsto \chi_A$$

gives a bijection between $\mathcal{P}(X)$ and the set $\{0,1\}^X$ of all functions $X \to \{0,1\}$, we write

$$2^{\operatorname{card}(X)} := \operatorname{card}(\mathcal{P}(X)) = \operatorname{card}(\{0,1\}^X).$$

In particular,

$$2^{\aleph_0} = \operatorname{card}(\mathcal{P}(\mathbb{N})).$$

Proposition 7.5. *We have*

$$\operatorname{card}(\mathcal{P}(\mathbb{N})) = c.$$

Equivalently,

$$2^{\aleph_0} = c.$$

Proof. Let $J = (0,1)$. Since $\operatorname{card}(J) = \operatorname{card}(\mathbb{R}) = c$, it is enough to prove that

$$\operatorname{card}(\mathcal{P}(\mathbb{N})) = \operatorname{card}(J).$$

We first construct an injection

$$\Phi : \mathcal{P}(\mathbb{N}) \longrightarrow J.$$

Given $A \subseteq \mathbb{N}$, define

$$\Phi(A) := \sum_{n=0}^{\infty} \frac{2\chi_A(n)}{3^{n+1}}.$$

Equivalently, $\Phi(A)$ is the real number in $(0,1)$ whose ternary expansion has digit 2 in position $n+1$ if $n \in A$, and digit 0 otherwise.

We claim that Φ is injective. Let $A \neq B$, and let m be the smallest integer such that

$$\chi_A(m) \neq \chi_B(m).$$

Without loss of generality, assume $\chi_A(m) = 1$ and $\chi_B(m) = 0$. Then

$$\Phi(A) - \Phi(B) = \frac{2}{3^{m+1}} + \sum_{n>m} \frac{2(\chi_A(n) - \chi_B(n))}{3^{n+1}}.$$

Hence

$$\Phi(A) - \Phi(B) \geq \frac{2}{3^{m+1}} - \sum_{n>m} \frac{2}{3^{n+1}}.$$

Now

$$\sum_{n>m} \frac{2}{3^{n+1}} = 2 \sum_{k=m+2}^{\infty} \frac{1}{3^k} = 2 \cdot \frac{1/3^{m+2}}{1 - 1/3} = \frac{1}{3^{m+1}},$$

so

$$\Phi(A) - \Phi(B) \geq \frac{1}{3^{m+1}} > 0.$$

Therefore $\Phi(A) \neq \Phi(B)$, and Φ is injective.

Next we construct an injection

$$\Psi : J \longrightarrow \mathcal{P}(\mathbb{N}).$$

For each $x \in J$, write x in binary form

$$x = 0.b_0 b_1 b_2 \dots \qquad (b_i \in \{0,1\}),$$

using the *canonical* binary expansion, namely the one which is not eventually equal to 1. Then define

$$\Psi(x) := \{\, n \in \mathbb{N} \mid b_n = 1 \,\}.$$

This map is injective, because two distinct numbers in J have distinct canonical binary expansions, hence determine different subsets of $\mathbb{N}$.

We have therefore found injections

$$\mathcal{P}(\mathbb{N}) \hookrightarrow J \qquad \text{and} \qquad J \hookrightarrow \mathcal{P}(\mathbb{N}).$$

By the Cantor–Bernstein theorem,

$$\operatorname{card}(\mathcal{P}(\mathbb{N})) = \operatorname{card}(J) = c.$$

This proves the claim. $\square$

8 Why there is no set of all sets

Cantor's theorem leads to a dramatic conclusion. Suppose there were a set $\mathcal{I}$ containing *all* sets. Then every subset of $\mathcal{I}$ would also be a set, hence an element of $\mathcal{I}$. So

$$\mathcal{P}(\mathcal{I}) \subseteq \mathcal{I},$$

which would imply

$$\mathrm{card}(\mathcal{P}(\mathcal{I})) \leq \mathrm{card}(\mathcal{I}).$$

But Cantor's theorem says exactly the opposite:

$$\mathrm{card}(\mathcal{I}) < \mathrm{card}(\mathcal{P}(\mathcal{I})).$$

Contradiction.

Therefore:

there is no set of all sets.

This is closely related to Russell's paradox. If $\mathcal{I}$ were a set of all sets, one could define

$$X = \{F \in \mathcal{I} \mid F \notin F\}.$$

Then ask: is $X \in X$?

- If $X \in X$, then by definition $X \notin X$.
- If $X \notin X$, then by definition $X \in X$.

Again we get a contradiction.

This is the famous *Russell paradox*, often retold as the barber story:

> In a village there is a barber who shaves exactly those people who do not shave themselves. Who shaves the barber?

The paradox shows that not every collection can be treated as a set.

9 The Continuum Hypothesis

We have proved that

$$\aleph_0 < c.$$

A natural question is whether there exists an intermediate cardinal between them.

The *Continuum Hypothesis* (CH) says that there is no cardinal strictly between $\aleph_0$ and c.

9.1 Zermelo–Fraenkel set theory

At this point one may ask a natural question: if not every collection is a set, then what exactly is a set, and how do mathematicians decide which collections are allowed?

The standard modern answer is given by *ZFC*, which stands for *Zermelo–Fraenkel set theory with the Axiom of Choice*. It is the most widely used axiomatic framework for mathematics.

The basic idea is the following. Instead of trying to define a set informally once and for all, one writes down a list of axioms describing how sets behave and how new sets can be constructed from old ones. In this theory, sets are the fundamental objects, and all of mathematics can in principle be built from them.

Very roughly, the axioms of ZFC say that:

- two sets are equal if they have the same elements;
- there exists an empty set;
- if a and b are sets, then $\{a, b\}$ is a set;
- if X is a set, then the union of all elements of X is a set;
- if X is a set, then its power set $\mathcal{P}(X)$ is a set;
- there exists an infinite set;
- given a set, one may form subsets defined by a property, but only *inside an already existing set*;
- the image of a set under a definable map is again a set;
- sets are built in stages, so pathological loops such as $X \in X$ are ruled out;
- one may choose one element from each set in a family of nonempty sets (this is the Axiom of Choice).

The crucial point is that ZFC does *not* allow arbitrary collections to be sets. This is exactly what prevents contradictions such as Russell's paradox. For example, one is not allowed to start with "the set of all sets" and then form subsets of it, because in ZFC there is no such set in the first place.

So ZFC provides a rigorous answer to the question "what is a set?": a set is any object that can exist according to the axioms of the theory.

This does not mean that every mathematical question can be answered inside ZFC. In fact, one of the deepest discoveries of twentieth-century logic is that some natural statements, such as the Continuum Hypothesis, can neither be proved nor disproved from the axioms of ZFC, assuming ZFC itself is consistent. Thus ZFC is powerful enough to formalize most of mathematics, but not so powerful as to settle every possible question.

- In 1940, Gödel proved that CH cannot be disproved from the usual axioms of set theory, assuming those axioms are consistent [Gö40].
- In 1963, Cohen proved that CH cannot be proved from those axioms either [Coh66].

So CH is *independent* of the standard axioms of set theory (ZFC): one can build mathematically legitimate universes in which CH is true, and others in which CH is false.

This was one of the greatest discoveries of twentieth-century logic.

10 A final historical turn: the birth of category theory

The story of infinity does not end with set theory. In fact, the paradoxes surrounding "the set of all sets" helped mathematicians realize that foundations had to be handled with great care. At the same time, mathematics itself was becoming more structural: what mattered was often not the internal nature of an object, but the maps between objects and the way constructions behaved across different areas.

This is one of the roads that led to *category theory*. In the early 1940s, Samuel Eilenberg and Saunders Mac Lane were studying problems in algebraic topology and homological algebra. They noticed that many constructions were not isolated formulas: they were *systematic correspondences* between whole mathematical worlds, and these correspondences respected composition and identity maps. To describe this cleanly, they introduced the notions of *category*, *functor*, and *natural transformation* in their 1945 paper *General Theory of Natural Equivalences* [EL45].

The guiding idea was revolutionary:

> *do not look only at mathematical objects; look at the arrows between them, and at the patterns formed by those arrows.*

For example:

- sets with functions between them form a category;
- groups with homomorphisms form a category;
- topological spaces with continuous maps form a category.

A functor then becomes a rule that transports objects and arrows from one category to another, preserving structure. This was exactly the right language for comparing topological constructions with algebraic ones [Lan98, LS09].

Later, category theory became much more than a language. Grothendieck used it to reshape algebraic geometry and homological algebra, Kan developed adjoint functors, and Lawvere explored categorical foundations for mathematics. In that sense, the historical path runs from questions about sets and infinity to a broader vision of mathematics as a network of structures and structure-preserving maps [Lan98].

So the “genesis” of category theory can be summarized in three stages:

1. **Need for organization.** Mathematics had accumulated many constructions that looked similar in different subjects.
2. **Need for naturality.** Eilenberg and Mac Lane wanted to formalize when a construction is *natural*, not arbitrary.
3. **Shift of viewpoint.** The focus moved from elements to morphisms, from isolated objects to relations between objects.

That shift has shaped large parts of modern mathematics.

References

[Coh66] Paul J. Cohen, *Set theory and the continuum hypothesis*, W. A. Benjamin, New York, 1966.

[EL45] Samuel Eilenberg and Saunders Mac Lane, *General theory of natural equivalences*, Transactions of the American Mathematical Society **58** (1945), no. 2, 231–294.

[G4̈0] Kurt Gödel, *The consistency of the continuum hypothesis*, Annals of Mathematics Studies **3** (1940).

[Hal60] Paul R. Halmos, *Naive set theory*, Van Nostrand, Princeton, NJ, 1960.

[Jec03] Thomas Jech, *Set theory*, 3 ed., Springer, Berlin, 2003.

[Lan98] Saunders Mac Lane, *Categories for the working mathematician*, 2 ed., Springer, New York, 1998.

[LS09] F. William Lawvere and Stephen H. Schanuel, *Conceptual mathematics: A first introduction to categories*, 2 ed., Cambridge University Press, Cambridge, 2009.