Cardinality, Cantor and Continuum: Set Theory of the Infinite

Giacobbe Riccardo

April 2026

1 Introduction: Cardinality and Finite Sets

The concept of cardinality of a set is used to formalize the notion of *"number of elements in a set"*. At first this seems pointless, everybody can tell how many elements there are, just count them! However we will see that the concept of cardinality is more precise and allows to quantify elements where counting might not be possible.

Definition 1. *Two sets X and Y have the same cardinality if there is a bijection $f : X \to Y$.*
Two sets X and Y have different cardinality if there is no bijection $f : X \to Y$.
A set A has lesser or equal cardinality than a set B if there is an injective function $f : A \to B$.

If you can find some way to put all the elements of both sets in a one-to-one correspondence, then they must have the same amount of elements. Two sets with same cardinality are said to be equinumerous. These three statements provide relationships of cardinality between sets, while the following one allows to determine absolutely the cardinality of certain sets.

Definition 2. *A set is finite and has cardinality n if there is a bijection $f : X \to S$ where $S = \{i \in \mathbb{N} \mid i < n\}$.*

Example 1. *Let us consider the set $A = \{6, 7\}$. We see that the function $f : A \to S \mid f(n) = n - 6$ where $S = \{i \in \mathbb{N} \mid i < 2\} = \{0, 1\}$. Thus the set A has cardinality of 2, and it is expressed with the following notation: $|A| = 2$.*

This is all a fancier way of stating the obvious, where is the nuance that i promised? Things start to get interesting when we abandon finite sets and start to look towards infinity.

2 Infinite Sets: $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$

If, given a certain set, there is no bijection for any value of n, then the set is said to be infinite. The set $\mathbb{N} = \{0, 1, 2, 3 \dots\}$ is infinite, so is the set $\mathbb{Q}$. But are they the same size? To answer the question we must first provide an intuitive way of understanding countability.

Definition 3. *A set X is countable if it is finite or if it is infinite and there is a bijection $f : X \to \mathbb{N}$. A set X is uncountable if it is infinite and if there is no bijection between the set X and the set $\mathbb{N}$.*

In simple terms, you can count the elements of a countable set one by one. Even if our countable set in infinite, there is still a way to put elements one after the other, just like when we count elements of $\mathbb{N}$, starting from 0 and going on to 1 and so on. The cardinality of any infinite countable set is denoted with aleph-null: $|\mathbb{N}| = \aleph_0$.

Example 2. *One example is the set of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. If we start from zero and count the elements in increasing order, we will skip all the negative numbers. One correct order to count them is the following: 0, -1, 1, -2, 2 ..., which is represented by the following bijection:*

$$f_{\mathbb{N}\to\mathbb{Z}} : \mathbb{N} \to \mathbb{Z} \mid f_{\mathbb{N}\to\mathbb{Z}}(n) = (-1)^n \lceil \frac{n}{2} \rceil \tag{1}$$

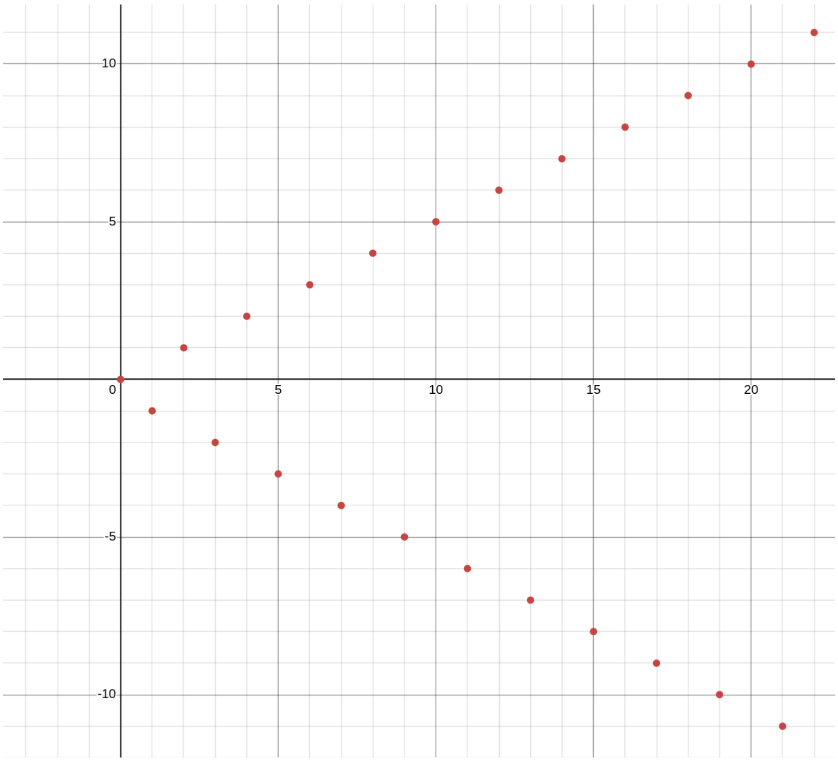

Figure 1: Graphical representation of bijection $f_{\mathbb{N}\to\mathbb{Z}}$ Link.

When dealing with finite sets, obviously every set has greater cardinality than any of their proper subsets. Note however that $\mathbb{N}$ is a proper subset of $\mathbb{Z}$, despite the two sets being equinumerous.
Dealing with discrete sets, like $\mathbb{N}$, is relatively simple, where discrete means that there is a gap between numbers. However $\mathbb{Q}$ is not discrete, it is dense. Given two rational numbers $a < b$, $\frac{a+b}{2}$ will always lie between them, which might make it seem impossible to enumerate the elements of $\mathbb{Q}$, after all, there is no smallest rational number greater than zero.

Theorem. $|\mathbb{N} \times \mathbb{N}| = \aleph_0$

Proof. *We start considering the function* f*:*

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \mid f(n; m) = 2^n 3^m \tag{2}$$

The Fundamental Theorem of Arithmetic states that every natural number greater than 1 has one unique prime factorization. Thus, given 2 different elements in $\mathbb{N} \times \mathbb{N}$ $a = (n; m)$ *and* $b = (n'; m')$, $f(a)$ *must differ from* $f(b)$*, as they are distinct products of primes. Therefore* f *is an injection between the domain and co-domain, and* $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$*. We know* $\mathbb{N} \times \mathbb{N}$ *to be infinite so it must be equinumerous to* $\mathbb{N}$ *to satisfy the previous inequality.*

But what has that got to do with anything? I was talking about $\mathbb{Q}$! Calm down, as you will see this result is necessary in proving that $\mathbb{N}$ and $\mathbb{Q}$ have equal cardinality.

Theorem. $|\mathbb{Q}| = \aleph_0$

Proof. *Since we have previously established a bijection* $f_{\mathbb{N}\to\mathbb{Z}}$ *between* $\mathbb{N}$ *and* $\mathbb{Z}$*, the following function proves that* $\mathbb{N} \times \mathbb{N}$ *has the same cardinality as* $\mathbb{Z} \times \mathbb{N}$*:*

$$g : \mathbb{N} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{N} \mid g(n, m) = (f_{\mathbb{N}\to\mathbb{Z}}(n); m) \tag{3}$$

Thanks to the previous theorem, we know that $\mathbb{N}$ *and* $\mathbb{N}\times\mathbb{N}$ *have equal cardinality. Thus* $\mathbb{N}$ *and* $\mathbb{Z}\times\mathbb{N}$ *are equinumerous. The last thing we need (i promise) is to show* $|\mathbb{Q}| = |\mathbb{Z}\times\mathbb{N}|$*.*
Consider the following function $q : \mathbb{Q} \to \mathbb{Z}\times\mathbb{N}$ *such that:*

$$\forall r \in \mathbb{Q}\ q(r) = (a;b) \tag{4}$$

Where

$$\frac{a}{b+1} = r \tag{5}$$

and the fraction is reduced to minimum terms.
Note that the $+1$ *is necessary since no rational number has denominator zero. This function is injective, thus* $|\mathbb{Q}| \leq |\mathbb{Z}\times\mathbb{N}|$*.*
Since $\mathbb{Z}\times\mathbb{N}$ *is countable, and* $\mathbb{Q}$ *is infinite, it must also be countable to satisfy the inequality.*

An intuitive argument for the countability of $\mathbb{Q}^+$ is the following: consider the positive rational numbers arranged in a grid such as the image below, then the line allows one to count the rationals one by one, proving the countability of the set.

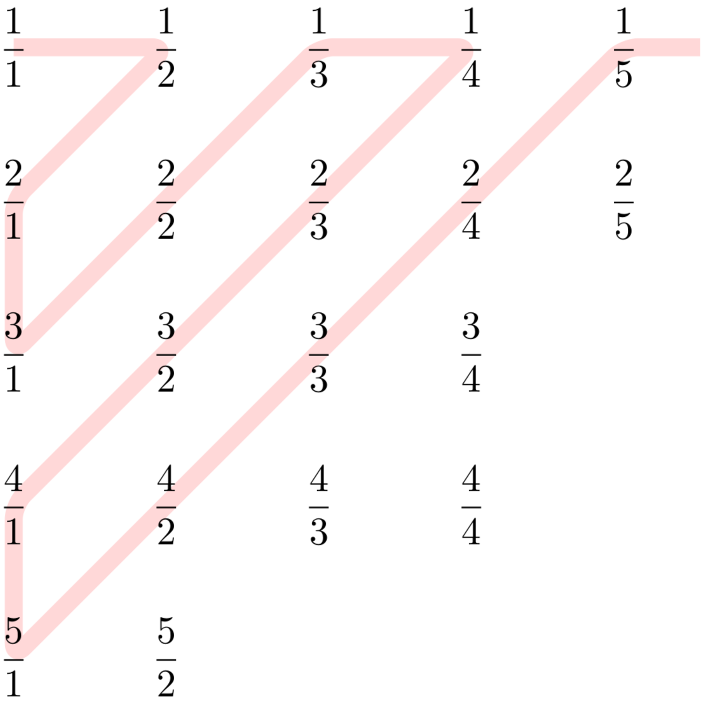

Figure 2: Graphical representation of enumeration of $\mathbb{Q}$

3 Cantor's Theorem, $\mathbb{R}$ and Continuum Hypothesis

After much work in showing to be equal the cardinality of $\mathbb{N}$, $\mathbb{Z}$ and (surprisingly) $\mathbb{Q}$, we arrive at the true core of this essay, Cantor's theorem and the cardinality of $\mathbb{R}$. Cantor's theorem uses the concept of power set as defined below:

Definition 4. *The power set* $\mathcal{P}(A)$ *of a given set* A *is defined to be the set of all subsets of* A*:*

$$a \in \mathcal{P}(A) \iff a \subseteq A \tag{6}$$

Cantor's Theorem. *Given any set A, the power set $\mathcal{P}(A)$ has cardinality strictly greater that that of A.*

This is a relatively simple statement, but it holds great importance. In particular it is true for every set, including infinite ones, which allows for the creation of a hierarchy of infinite sets, the next one larger than the previous one. We will not delve into this infinite recursion of sets and power sets, but we will prove the theorem and use it sparingly.

Proof. *To prove that $|A| < |\mathcal{P}(A)|$, we must prove the existence of an injective function $f : A \to \mathcal{P}(A)$ and that a bijection between the two sets cannot exist. We begin with a proof of the first statement with the following function f:*

$$f : A \to \mathcal{P}(A) \mid p(a) = \{a\} \tag{7}$$

which is clearly injective but not bijective, as the empty set is not in the image of the function, nor are any subsets of A with more than one item, if they exist. To show the impossibility of a bijection between the two sets, it suffices to prove that no surjective function can exist.
Aiming for a contradiction we suppose the existence of a surjective function g, and consider the set B:

$$B = \{x \in A \mid x \notin g(x)\} \subseteq A \tag{8}$$

Due to the surjectivity of g, there must be $z \in A \mid g(z) = B$.
If $z \in g(z) = B$, then there is a contradiction, as $z \in g(z) \implies z \notin B$.
However if $z \notin g(z) = B$, still there is a contradiction, as $z \notin g(z) \implies z \in B$.
Thus no surjective function can exist between A and $\mathcal{P}(A)$, and $|A| < \mathcal{P}(A)$.

Given any finite set A, $|\mathcal{P}(A)| = 2^{|A|}$. This notation is extended for infinite sets, for example: $|\mathcal{P}(\mathbb{N})| = 2^{\aleph_0}$.

The only main set of numbers we still need to consider is $\mathbb{R}$. Cantor himself was able to prove rigorously with a simple proof the uncountability of $\mathbb{R}$, whose cardinality is represented by $\mathfrak{c}$. This particular proof takes the name of "Cantor's Diagonal Argument".

Theorem. $\aleph_0 < \mathfrak{c}$

Proof. *We start by assuming that $\mathbb{R}$ is countable. This implies that the interval $(0;1)$ must also be countable, so there must be at least one sequence of numbers $\{a, b, c, d \dots\}$ in the interval such that all of the values in the interval appear only once in the sequence.*

$$a = 0.a_1a_2a_3a_4\dots$$

$$b = 0.b_1b_2b_3b_4\dots$$

$$c = 0.c_1c_2c_3c_4\dots$$

$$d = 0.d_1d_2d_3d_4\dots$$

$$\dots$$

Here each number is represented with infinite decimal expansion. Now we consider the number $x = x_1x_2x_3x_4\dots$, where the nth digit of x differs from the nth digit of the nth number of the sequence. We see now that x is in the interval, but it differs at least in one decimal place from any number already in the sequence. This contradicts the initial assumption that such a sequence can exist, thus $(0;1)$ is uncountable. The interval has same cardinality as $\mathbb{R}$ as a whole, as evidenced by the function f:

$$f : \mathbb{R} \to (0;1) \mid f(x) = \frac{arctan(x)}{\pi} + \frac{1}{2} \tag{9}$$

Thus $\mathbb{R}$ is uncountable and $\aleph_0 < \mathfrak{c}$.

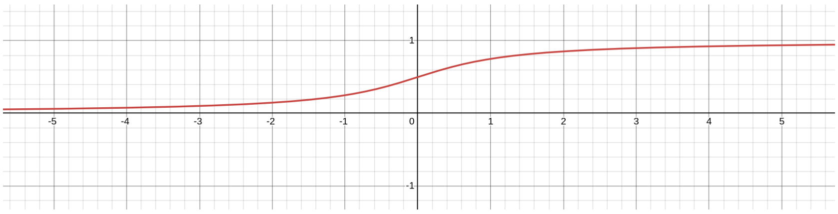

Figure 3: Bijection from $\mathbb{R}$ to $(0;1)$ Link.

This proof however is not able to provide a bijection between $\mathcal{P}(\mathbb{N})$ and $\mathbb{R}$, which implies that $2^{\aleph_0} = \mathfrak{c}$. Such a bijection exists, but i am not able to provide a simple and short proof, you will have to trust me blindly.

Having shown that $\aleph_0 < \mathfrak{c}$, one might wonder if there is any set with size greater than $\mathbb{N}$ but smaller than $\mathbb{R}$, and Cantor himself believed the answer to be no. This would mean that, given $\aleph_0$, the next greatest cardinality, denoted with $\aleph_1$, is equal to $2^{\aleph_0}$.

Continuum Hypothesis. $\aleph_1 = 2^{\aleph_0}$.

The statement is not a theorem, and there is no proof. In fact, and this is the last surprising point of the essay, it is independent from the rules of set theory, meaning that one can choose freely whether the proposition holds or not.

4 Brief History of Set Theory

Although set theory is the foundation of all modern mathematics, in the historical context,it was incredibly controversial.

Mathematician Georg Cantor is the father of set theory, but his approach lacked mathematical rigor, as his study was not based on axioms, but sets and operations upon them were described using natural language. Cantor and his work were widely criticized, with many pointing out paradoxes within the theory or rejecting it entirely, possibly contributing to his mental health problems. Cantor was obsessed with proving the Continuum Hypothesis, but he died in 1918 before succeeding, and debates on the hypothesis continued until resolution by Paul Cohen.

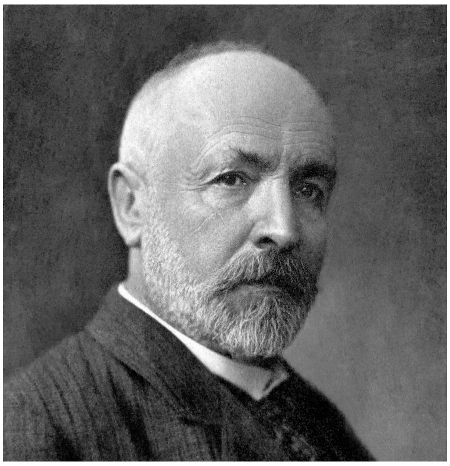

Figure 4: Georg Cantor

It was Zermelo and Frankel who postulated nine axioms of set theory, in an attempt to solve the paradoxes and formalize Cantor's work.

This was not without further controversy: the last axiom (the Axiom of Choice or AC) allowed for the creation of infinite sets, and with it one is allowed to prove seemingly absurd statements.

One example of this is the Banach-Tarski theorem, which makes it possible to transform one ball into two of the same size, by just partitioning the original ball and rearranging the subsets. Much like the Continuum Hypothesis, debates on the Axiom of Choice persisted until Cohen was able to resolve them.

The theory based upon the first eight axioms is named ZF (Zermelo-Frankel) set theory, while ZFC denotes ZF with AC.

Another mathematician is crucial to understand the history of modern mathematics: David Hilbert. He defended and praised Cantor for his theory and he firmly believed that mathematics could be constructed from a finite number of axioms and could be provably consistent and complete, meaning that it could be proven that the theory had no contradictions, and that every true statement could be proven.

Figure 5: David Hilbert

His dreams of consistency and completeness were shattered when Kurt Godel showed that mathematics necessarily cannot prove its consistency, and it necessarily contains truths that are not provable. Godel also showed that the Axiom of Choice and the Continuum Hypothesis were consistent with the ZF system, signifying that ZF alone could not disprove those two statements. Paul Cohen, almost one hundred years later than Cantor's first theory, proved that ZF is unable to prove AC and the Continuum Hypothesis. Thus ZF can neither prove nor disprove AC and the Continuum Hypothesis, which are both said to be independent, and one can choose freely whether they are true or not.

With this surprising and curious note we end this essay on set theory, having shown the most notable fundamental results.