INFINITY: CARDINAL NUMBERS

BJORN POONEN

1. Some terminology of set theory

$$\begin{aligned}\mathbb{N} &:= \{0, 1, 2, 3, \dots\}\\ \mathbb{Z} &:= \{\dots, -2, -1, 0, 1, 2, \dots\}\\ \mathbb{Q} &:= \text{the set of rational numbers}\\ \mathbb{R} &:= \text{the set of real numbers}\\ \mathbb{C} &:= \text{the set of complex numbers}\end{aligned}$$

(Some authors prefer not to include 0 in $\mathbb{N}$, but including 0 is more natural for many purposes; for example, then $\mathbb{N}$ is exactly the set of possibilities for the size of a finite set. Other authors avoid the issue entirely by using $\mathbb{Z}_{>0}$ to denote the set of positive integers and $\mathbb{Z}_{\geq 0}$ to denote the set of nonnegative integers.)

Let $f : X \to Y$ be a function from a set X to a set Y. Then

$$\begin{aligned}f \text{ is } \textit{injective} \text{ (one-to-one)} &\iff f(x_1) \neq f(x_2) \text{ whenever } x_1 \neq x_2.\\ f \text{ is } \textit{surjective} \text{ (onto)} &\iff \text{for every } y \in Y \text{ there exists } x \in X \text{ such that } f(x) = y.\\ f \text{ is } \textit{bijective} &\iff f \text{ is both injective and surjective}\end{aligned}$$

In the last case, one also says that f is a *bijection* (one-to-one correspondence); then f pairs the elements of X with the elements of Y in such a way that no elements of either set are left unpaired.

2. Cardinal numbers

We already know how to measure the size (synonym: *cardinality*) of a finite set. For example, $\#\{3, 4, 5, 6\} = 4$, $\#\emptyset = 0$, and $\#\{a, \{b, c\}\} = 2$. For centuries, people believed that there was no meaningful way to compare the sizes of infinite sets, but in the late 1800's Cantor developed a system for doing exactly this.

In his system, every set S has a cardinality $\#S$ (alternative notation: $|S|$). If S is finite, then $\#S$ is an ordinary nonnegative integer, as above. But if S is infinite, then $\#S$ is a new kind of "number," called a *cardinal number* or simply a *cardinal*. New symbols are needed: for instance, the cardinal numbers $\aleph_0$ (pronounced aleph-zero, aleph-nought, or aleph-null) and $\mathfrak{c}$ (the "cardinality of the continuum") are defined by

$$\begin{aligned}\aleph_0 &:= \#\mathbb{N},\\ \mathfrak{c} &:= \#\mathbb{R}.\end{aligned}$$

Date: February 7, 1999.

3. Equality of cardinal numbers

We do not introduce a different symbol for *every* individual set, because sometimes two different sets can have the same size. For instance, two finite sets have the same size if and only if one set can be obtained from the other by relabeling the elements; for instance, $\{1,2,3\}$ has the same cardinality as $\{a,b,c\}$. One of the fundamental properties of Cantor's cardinal numbers is that the same should hold for arbitrary sets, finite or not. This can be reworded as follows:

RULE 1: $\#S = \#T \iff$ there exists a bijection $f : S \to T$.

For instance, if $S = \{0,-1,-2,-3,\dots\}$, then $\#\mathbb{N} = \#S$ because there is a bijection $\mathbb{N} \to S$ sending each nonnegative integer n to $-n$:

$$\begin{aligned} 0 &\longleftrightarrow 0 \\ 1 &\longleftrightarrow -1 \\ 2 &\longleftrightarrow -2 \\ 3 &\longleftrightarrow -3 \\ &\vdots \end{aligned}$$

4. Comparing cardinal numbers

RULE 2: $\#S \le \#T \iff$ there exists an injection $f : S \to T$.

Loosely speaking, S is smaller or equal in size to T if and only if one can match the elements of S with elements of T so that all elements of S get used (but maybe some elements of T are left over). For example, there is an injection $\{a,b,c\} \to \mathbb{N}$ sending a to 1, b to 2, and c to 17; this proves that $3 \le \aleph_0$. As a special case of Rule 2, if $S \subseteq T$, then $\#S \le \#T$.

The relations $=$ and $\le$ for cardinals satisfy the same properties as they do for ordinary numbers:

1. $\#S = \#S$ for any set S (reflexivity).
2. If $\#S = \#T$, then $\#T = \#S$ (symmetry).
3. If $\#S = \#T$ and $\#T = \#U$, then $\#S = \#U$ (transitivity).
4. If $\#S = \#T$, then $\#S \le \#T$.
5. If $\#S \le \#T$ and $\#T \le \#U$, then $\#S \le \#U$ (transitivity).
6. For any two sets S and T, either $\#S \le \#T$ or $\#T \le \#S$.
7. If $\#S \le \#T$ and $\#T \le \#S$, then $\#S = \#T$.

The last two are fairly difficult to deduce from the definitions. The last one is called the Schröder-Bernstein Theorem; it says that if there exist injections $S \to T$ and $T \to S$, then there exists a bijection $S \to T$. (This appeared as a problem on one of the monthly contests.)

The other relations like $\ge$, $<$, and $>$ can be defined in terms of $=$ and $\le$. For instance, "$\#S > \#T$" means "$\#T \le \#S$ is true and $\#S = \#T$ is false."

5. An unfortunate situation

If S and T are finite sets, and S is a *proper* subset of T (this means that $S \subseteq T$ but $S \ne T$), then $\#S < \#T$. Unfortunately, this is no longer true when we consider infinite sets!

For example, if $S = \{3, 4, 5, 6, \dots\}$, then S is a proper subset of $\mathbb{N}$, but according to the definition, $\#S = \#\mathbb{N}$, because there is a bijection from S to $\mathbb{N}$:

$$\begin{aligned} 3 &\longleftrightarrow 0 \\ 4 &\longleftrightarrow 1 \\ 5 &\longleftrightarrow 2 \\ 6 &\longleftrightarrow 3 \\ &\vdots \end{aligned}$$

Moreover, this unfortunate situation is unavoidable if we want to keep Rules 1 and 2 (and we do). We just have to live with it.

6. The cardinality of $\mathbb{Z}$

Suppose we want to check whether the set $\mathbb{Z}$ of integers has the same cardinality as $\mathbb{N}$. If we try to set up a bijection from $\mathbb{N}$ to $\mathbb{Z}$ without thinking, we fail because the negative numbers are not used:

$$\begin{aligned} 0 &\longleftrightarrow 0 \\ 1 &\longleftrightarrow 1 \\ 2 &\longleftrightarrow 2 \\ 3 &\longleftrightarrow 3 \\ &\vdots \end{aligned}$$

$$-1, -2, -3, \dots \text{ are not used.}$$

This is only an injection. Does this mean that $\#\mathbb{N} \neq \#\mathbb{Z}$? No! Even though this function did not give a bijection, it is easy to construct other functions $\mathbb{N} \to \mathbb{Z}$ that are bijections, like

$$\begin{aligned} 0 &\longleftrightarrow 0 \\ 1 &\longleftrightarrow 1 \\ 2 &\longleftrightarrow -1 \\ 3 &\longleftrightarrow 2 \\ 4 &\longleftrightarrow -2 \\ 5 &\longleftrightarrow 3 \\ 6 &\longleftrightarrow -3 \\ &\vdots \end{aligned}$$

Thus $\#\mathbb{Z} = \#\mathbb{N} = \aleph_0$, even though $\mathbb{N}$ is a proper subset of $\mathbb{Z}$. (This is similar to the situation in the previous section.)

7. Countable sets

We next show that there is no infinite set strictly smaller than $\mathbb{N}$.

Proposition 1. *If $\#S \leq \aleph_0$, then either S is finite or $\#S = \aleph_0$.*

Proof. Start listing distinct elements of S:

$$s_0, s_1, s_2, s_3, \dots$$

If at some point we run out of elements, then S is finite. Otherwise we have constructed an injection $\mathbb{N} \to S$ sending n to s_n for each $n \in \mathbb{N}$, so $\aleph_0 = \#\mathbb{N} \leq \#S$. But $\#S \leq \aleph_0$ was given, so in this case, $\#S = \aleph_0$. □

A set S is called *countable* if $\#S \leq \aleph_0$, and S is called *countably infinite* if $\#S = \aleph_0$. According to our definition (which not all people agree on), finite sets like $\{1, 2, 3\}$ and $\emptyset$ also are considered to be countable.

The following is an extremely useful tool for calculating cardinalities.

Theorem 2 (Typewriter Principle)**.** *Let S be a set. If there is a way to label each element of S with a finite string of typewriter symbols (like* `fYe*4^!!!@`*) so that no two elements of S are given the same label, then S is countable; i.e., $\#S \leq \aleph_0$. If moreover S is infinite, then $\#S = \aleph_0$.*

Proof. Let T be the set of all finite strings of typewriter symbols. There are fewer than 900 typewriter characters, so we may assign each a three-digit code not beginning with 0. For instance, we might assign

$$a \mapsto 100$$
$$b \mapsto 101$$
$$\% \mapsto 486$$
$$\vdots$$

Let strings of characters be mapped to the concatenation of the character codes; for instance, $ba\%$ would map to $101100486 \in \mathbb{N}$. This gives an injection $T \to \mathbb{N}$, so $\#T \leq \#\mathbb{N} = \aleph_0$. The labelling of S gives an injection $S \to T$, so $\#S \leq \#T \leq \aleph_0$. The final statement follows from Proposition 1. □

Proposition 3. $\#\mathbb{Q} = \aleph_0$.

Proof. Each rational number can be labelled with a string of typewriter symbols representing it like `-75/89`, and $\mathbb{Q}$ is infinite, so the Typewriter Principle shows that $\#\mathbb{Q} = \aleph_0$. □

An *algebraic number* is a complex number that is a zero of some nonzero polynomial with rational coefficients. A *transcendental number* is a complex number that is not algebraic. The set of algebraic numbers is denoted by $\overline{\mathbb{Q}}$. For instance, $\sqrt{2} \in \overline{\mathbb{Q}}$, since $\sqrt{2}$ is a zero of $x^2 - 2$. On the other hand, it is true (but very difficult to prove) that π and e are transcendental.

Proposition 4. $\#\overline{\mathbb{Q}} = \aleph_0$.

Proof. We can describe $-i\sqrt{2}$ as

```
the complex zero of x^2+2 closest to -1.4i
```

Similarly, each $a \in \overline{\mathbb{Q}}$ can be singled out by a finite string of typewriter symbols giving a polynomial with rational coefficients of which it is a zero, together with an approximate description of its location to distinguish it from the other zeros of that polynomial. By the Typewriter Principle, $\#\overline{\mathbb{Q}} = \aleph_0$. □

8. Arithmetic of cardinal numbers

Suppose $S = \{1, 2\}$ and $T = \{1, 2, 3\}$. Relabelling the elements of T yields a set $T' = \{a, b, c\}$ of the same cardinality, but which is disjoint from T. Then $2 + 3 = \#S + \#T = \#(S \cup T') = \#\{1, 2, a, b, c\} = 5$. This observation lets one add cardinal numbers in general: if S and T are arbitrary sets then the sum of the cardinal numbers $\#S$ and $\#T$ is defined to be the cardinality of $S \cup T'$ where T' is obtained from T by relabeling elements so that $S \cap T' = \emptyset$. For example, in the disjoint union

$$\{0, 2, 4, 6, \dots\} \cup \{1, 3, 5, 7, \dots\} = \mathbb{N},$$

all three sets are of cardinality $\aleph_0$, so

$$\aleph_0 + \aleph_0 = \aleph_0.$$

The *Cartesian product* $S \times T$ of two sets S and T is the set of all ordered pairs (s, t) where $s \in S$ and $t \in T$. For example, if $S = \{1, 2\}$ and $T = \{a, b, c\}$, then

$$S \times T = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

so $\#(S \times T) = 6 = 2 \cdot 3$. If S and T are arbitrary sets, then the product of the cardinal numbers $\#S$ and $\#T$ is defined to be $\#(S \times T)$. For instance, the elements of $\mathbb{N} \times \mathbb{N}$ can be described by strings of typewriter symbols like `(5,7)`, so the Typewriter Principle shows that $\#(\mathbb{N} \times \mathbb{N}) = \aleph_0$. Therefore

$$\aleph_0 \cdot \aleph_0 = \aleph_0.$$

These equalities may look strange, but in fact, such behavior is typical: one can prove that if $\aleph$ and $\aleph'$ are cardinal numbers such that $\aleph \leq \aleph'$ and $\aleph'$ is infinite, then $\aleph + \aleph' = \aleph \cdot \aleph' = \aleph'$.

There is no nice way of subtracting or dividing cardinal numbers. But one can exponentiate. If S and T are arbitrary sets, let S^T denote the set of functions from T to S. Note the reversal of order! Then $(\#S)^{(\#T)}$ is defined to be the cardinality of S^T. For example, if $S = \mathbb{N}$ and $T = \{1, 2, 3\}$, then a sample element of S^T might be described by

`the function {1,2,3}->N sending 1 to 12, 2 to 753, and 3 to 489.`

The Typewriter Principle shows that $\#(S^T) = \aleph_0$. Hence $(\aleph_0)^3 = \aleph_0$.

9. The power set

The *power set* $\mathcal{P}(S)$ of a set S is the set of all its subsets. For instance, if $S = \{1, 2, 3\}$, then

$$\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\},$$

so $\#\mathcal{P}(S) = 8$.

For any set S, there is a bijection between $\mathcal{P}(S)$ and the set $\{0, 1\}^S$ of functions $\chi : S \to \{0, 1\}$ that maps the subset T of S to its *characteristic function*

$$\chi_T(s) := \begin{cases} 1, & \text{if } s \in T \\ 0, & \text{if } s \notin T \end{cases}.$$

Therefore $\#\mathcal{P}(S) = \#\left(\{0, 1\}^S\right) = 2^{\#S}$.

10. Cantor's diagonal argument

Now consider the special case $S = \mathbb{N}$. For convenience of notation, we may represent a function $f : \mathbb{N} \to \{0, 1\}$ by a sequence of binary digits. For example, $1011101\cdots$ corresponds to the function f such that $f(0) = 1$, $f(1) = 0$, $f(2) = 1$, $f(3) = 1$, $f(4) = 1$, $f(5) = 0$, $f(6) = 1$, and so on.

Lemma 5. *There is no bijection between* $\mathbb{N}$ *and the set* $\{0, 1\}^{\mathbb{N}}$ *of functions* $f : \mathbb{N} \to \{0, 1\}$.

Proof. The proof is by contradiction. Suppose, there is such a bijection, such as

$$\begin{aligned}
0 &\longrightarrow \text{the function represented by } \mathbf{1}011101\cdots\\
1 &\longrightarrow \text{the function represented by } 0\mathbf{0}11010\cdots\\
2 &\longrightarrow \text{the function represented by } 11\mathbf{0}0011\cdots\\
3 &\longrightarrow \text{the function represented by } 001\mathbf{1}111\cdots\\
4 &\longrightarrow \text{the function represented by } 1110\mathbf{1}01\cdots\\
5 &\longrightarrow \text{the function represented by } 10000\mathbf{1}0\cdots\\
6 &\longrightarrow \text{the function represented by } 101011\mathbf{0}\cdots\\
&\vdots
\end{aligned}$$

Then

$$\text{the function represented by } 0110001\cdots,$$

where the final sequence has been obtained by complementing the binary digits of the (highlighted) diagonal sequence, will not be in the list, since that last sequence differs from each sequence in the list at least in the highlighted digit. This contradicts the assumption that the mapping was a bijection. □

Theorem 6. $\aleph_0 < 2^{\aleph_0}$.

Proof. There exists an injection $\mathbb{N} \to \{0, 1\}^{\mathbb{N}}$, for instance

$$\begin{aligned}
0 &\longrightarrow \text{the function represented by } 1000000\cdots\\
1 &\longrightarrow \text{the function represented by } 0100000\cdots\\
2 &\longrightarrow \text{the function represented by } 0010000\cdots\\
3 &\longrightarrow \text{the function represented by } 0001000\cdots\\
4 &\longrightarrow \text{the function represented by } 0000100\cdots\\
5 &\longrightarrow \text{the function represented by } 0000010\cdots\\
6 &\longrightarrow \text{the function represented by } 0000001\cdots\\
&\vdots
\end{aligned}$$

so $\#\mathbb{N} \le \#\{0, 1\}^{\mathbb{N}}$; in other words $\aleph_0 \le 2^{\aleph_0}$. But Lemma 5 shows that $\#\mathbb{N} \ne \#\{0, 1\}^{\mathbb{N}}$, so $\aleph_0 \ne 2^{\aleph_0}$. Combining these shows that $\aleph_0 < 2^{\aleph_0}$. □

A similar proof shows that $\aleph < 2^{\aleph}$ for every cardinal number $\aleph$. In other words, the power set $\mathcal{P}(S)$ of a set S is always strictly bigger than S.

11. The cardinality of $\mathbb{R}$

We already gave a name to $\#\mathbb{R}$, namely $\mathfrak{c}$, but in fact, this was unnecessary, since we'll soon see that $\#\mathbb{R} = 2^{\aleph_0}$.

Theorem 7 (Typewriter Principle II)**.** *Let S be a set. If there is a way to label each element of S with an infinite sequence of typewriter symbols (like* `a!b!c#d&`$\cdots$*) so that no two elements of S are given the same label, then $\#S \leq 2^{\aleph_0}$.*

Proof. Assign each typewriter symbol a code of exactly 10 binary digits. Concatenating the codes in an infinite sequence of typewriter symbols yields an infinite sequence of binary digits. If we map each element of S to the corresponding binary digit sequence, we get an injection $S \to \{0,1\}^{\mathbb{N}}$. Hence $\#S \leq \#\{0,1\}^{\mathbb{N}} = 2^{\aleph_0}$. □

Theorem 8. *We have $\#\mathbb{R} = 2^{\aleph_0}$; in other words, $\mathfrak{c} = 2^{\aleph_0}$.*

Proof. Any real number can be labelled by its decimal expansion, which is an infinite sequence of typewriter symbols like

$$-386.589734957938798379579057\ldots$$

so Typewriter Principle II implies that $\#\mathbb{R} \leq 2^{\aleph_0}$. On the other hand there is an injection $\{0,1\}^{\mathbb{N}} \to \mathbb{R}$ sending each infinite sequence of 0's and 1's to the corresponding real number having those as the digits past the decimal point; for instance

$$1011101110\ldots \quad \longrightarrow \quad .1011101110\ldots.$$

This injection shows that $\#\{0,1\}^{\mathbb{N}} \leq \#\mathbb{R}$; i.e., $2^{\aleph_0} \leq \#\mathbb{R}$. Combining these shows that $\#\mathbb{R} = 2^{\aleph_0}$. □

We showed earlier that the set $\overline{\mathbb{Q}}$ of algebraic numbers had size only $\aleph_0$, so the same is true for the real algebraic numbers. But $\aleph_0 < 2^{\aleph_0} = \#\mathbb{R}$, so this shows that at least some real numbers are transcendental!

12. The continuum hypothesis

We showed in Proposition 1 that $\aleph_0$ is the smallest infinite cardinal. It can be shown that there a next smallest cardinal called $\aleph_1$; i.e., the only cardinals strictly smaller than $\aleph_1$ are the finite ones and $\aleph_0$. Next come $\aleph_2$, $\aleph_3$, $\ldots$. Where does $\mathfrak{c} = 2^{\aleph_0} = \#\mathbb{R}$ fit into this list, if anywhere? (A priori, it could be bigger than $\aleph_n$ for every $n \in \mathbb{N}$.) We know that $2^{\aleph_0} \geq \aleph_1$, because we proved that $2^{\aleph_0} > \aleph_0$. Cantor conjectured

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

In other words, he believed that there is no set whose cardinality is strictly between that of $\mathbb{N}$ and that of $\mathbb{R}$.

In 1940 Gödel proved that the continuum hypothesis cannot be disproved from the other axioms of set theory. But in 1963 Cohen showed that it could not be proved from these axioms either!

The role of the continuum hypothesis in set theory is similar to the role of the parallel postulate in plane geometry. The parallel postulate (that given a line L and a point P not on L, there exists a unique line L' through P that does not intersect L) cannot be disproved from the other axioms of plane geometry, because it is actually true for the euclidean model of geometry. On the other hand, the parallel postulate cannot be proved either, since it is false in various noneuclidean models of geometry which do satisfy all the other axioms.

Therefore the parallel postulate, or its negation, may be taken as a new axiom. Which one you choose will depend on your vision of what geometry is supposed to be.

Similarly, whether you choose to accept the continuum hypothesis will depend on your idea of what a set is supposed to be.

13. Problems

There are a lot of problems here. Just do the ones that interest you.

1. Each of the following sets has cardinality equal to $\aleph_0$, $2^{\aleph_0}$, or $2^{2^{\aleph_0}}$. Determine which, in each case, and prove it.
   (a) $\{0, 1, 4, 9, 16, \dots\}$
   (b) $\mathbb{Z}[x]$ (the set of polynomials with integer coefficients)
   (c) $\mathbb{Q}[x]$ (the set of polynomials with rational coefficients)
   (d) $\mathbb{R}[x]$ (the set of polynomials with real coefficients)
   (e) $\mathbb{C}$
   (f) The interval $[0, 1]$ of real numbers between 0 and 1 inclusive.
   (g) The set of irrational real numbers.
   (h) The set of transcendental real numbers.
   (i) $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ (the set of Gaussian integers)
   (j) The set of points in the plane.
   (k) The set of lines in the plane.
   (l) The set of functions from $\mathbb{N}$ to $\mathbb{N}$.
   (m) The set of bijections from $\mathbb{N}$ to $\mathbb{N}$.
   (n) The set of functions from $\mathbb{N}$ to $\mathbb{R}$.
   (o) The set of functions from $\mathbb{R}$ to $\mathbb{N}$.
   (p) The set of functions from $\mathbb{R}$ to $\mathbb{R}$.
2. Prove properties 1 through 5 of cardinal numbers listed in Section 4 using only Rules 1 and 2.
3. Let S and T be sets. Prove that if there exists a surjective function $f : S \to T$, then $\#T \leq \#S$.
4. Explain why our definition of $(\#S)^{(\#T)}$ agrees with the usual definition for natural numbers when S and T are finite sets.
5. Show that $\aleph_0^{\aleph_0} = 2^{\aleph_0}$.
6. Show that $\#\mathcal{P}(S) > \#S$ for any set S. (Hint: try to rephrase Cantor's diagonal argument purely in terms of set membership, without reference to sequences.)
7. Show that $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ for any three cardinal numbers α, β, and γ.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu