19. Cardinal arithmetic

Definition 19.1. *Let A and B be two sets. We write $|A| \leq |B|$ if there is an injective function $f\colon A \longrightarrow B$.*

We write $|A| < |B|$ if in addition there is no surjective function $g\colon A \longrightarrow B$.

Lemma 19.2. *Let A, B and C be three sets.*

(1) $|A| \leq |B|$ and $|B| \leq |A|$ if and only if $|A| = |B|$.
(2) If $|A| \leq |B|$ and $|B| \leq |C|$ then $|A| \leq |C|$.

Proof. We first prove (1). ($\Longleftarrow$) is easy; if $f\colon A \longrightarrow B$ is a bijection then f is invertible. The inverse $g\colon B \longrightarrow A$ is a bijection. In particular f and g are injective.

Now we turn to ($\Longrightarrow$). As $|A| \leq |B|$ there is an injective map $f\colon A \longrightarrow B$. As $|B| \leq |A|$ there is an injective map $g\colon B \longrightarrow A$. By (18.2) A and B have the same cardinality, so that $|A| = |B|$. This is (1).

We now prove (2).

As $|A| \leq |B|$ there is an injective map $f\colon A \longrightarrow B$. As $|B| \leq |C|$ there is an injective map $g\colon B \longrightarrow C$. The composition $g \circ f\colon A \longrightarrow C$ is an injective map from A to C. Therefore $|A| \leq |C|$. $\square$

Theorem 19.3 (Cantor's Theorem)**.** *If A is a set then*

$$|A| < |\wp(A)|.$$

Proof. Suppose the result does not hold. The function

$$g\colon A \longrightarrow \wp(A),$$

which sends an element a of A to the singleton set which contains a,

$$g(a) = \{\, a \,\}$$

is easily seen to be injective.

Therefore there is a surjection $f\colon A \longrightarrow \wp(A)$. We will derive a contradiction.

Let

$$B = \{\, a \in A \mid a \notin f(a) \,\}.$$

Then $B \subset A$ so that $B \in \wp(A)$. As f is surjective, it follows that we may find $b \in A$ such that $f(b) = B$.

There are two cases. First suppose that $b \in B$. Then $b \in f(b)$ so that $b \notin B$, by definition of B. This is a contradiction.

Otherwise $b \notin B$. Then $b \notin f(b)$ so that $b \in B$, by definition of B. This is a contradiction.

Either way we get a contradiction and so there is no surjective function. Thus the cardinality of the powerset is greater than the cardinality of A. $\square$

Corollary 19.4. *$\wp(\mathbb{Z})$ is uncountable.*

Proof. This is immediate from (19.3). $\square$

In fact we already showed that the powerset of the integers is in bijection with $(0,1)$. So (19.4) is another proof of the fact that the reals are uncountable.

Here is one way to view all of this. We can define addition of cardinals by taking the cardinality of the disjoint union of two sets of the appropriate cardinality.

Definition 19.5. *$\aleph_0$ is the cardinality of the natural numbers.*

We have
$$\aleph_0 + \aleph_0 = \aleph_0,$$
since the even and odd integers have cardinality $\aleph_0$ and their union is the integers, which has cardinality $\aleph_0$.

We can also define the product of two cardinals, by taking the cardinality of the product of two sets of the appropriate cardinality. We have
$$\aleph_0 \cdot \aleph_0 = \aleph_0,$$
since
$$|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|.$$
and the cardinality of the natural numbers is $\aleph_0$.

Theorem 19.6.
$$|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|.$$

Proof. It is enough to prove that
$$|(0,1) \times (0,1)| = |(0,1)|,$$
since $|\mathbb{R}| = |(0,1)|$. Let
$$f\colon (0,1) \longrightarrow (0,1) \times (0,1)$$
be the function which sends a real number
$$a = 0.a_1a_2a_2 = 0.r_1s_1r_2s_2r_3s_3\ldots,$$
to the pair of real numbers
$$r = 0.a_1a_2a_5\ldots \qquad \text{and} \qquad s = 0.a_2s_4s_6\ldots.$$
Now define a function
$$g\colon (0,1) \times (0,1) \longrightarrow (0,1)$$

in the following way. Given a pair of real numbers (r, s), write down their decimal expansions:

$$r = 0.r_1r_2r_3\ldots \qquad \text{and} \qquad s = 0.s_1s_2s_3\ldots.$$

Let

$$a = 0.a_1a_2a_2 = 0.r_1s_1r_2s_2r_3s_3\ldots,$$

so that the nth digit of a is defined as follows:

$$a_n = \begin{cases} s_k & \text{if } n = 2k \text{ is even} \\ r_k & \text{if } n = 2k-1 \text{ is odd.} \end{cases}$$

The function g sends the pair (r, s) to the real number $a \in (0, 1)$.

It is not hard to see that f and g are inverses of each other. Thus f is invertible and so it is a bijection. □

In words f simply divides the digits of a into their odd and even parts to get r and s. g reverses this process by interleaving the digits of r and s to get the digits of a. Note that f and g are far from being continuous.

We can define cardinal exponentiation, by taking the cardinality of the set of all functions between two sets of the appropriate cardinality. Cantor's theorem then says that something dramatically different happens in the case of exponentiation. Recall the power set of X is in bijection with the set of functions from X to 2, 2^X. We then have

$$\begin{aligned} 2^{\aleph_0} &= |2^{\mathbb{N}}| \\ &= |\wp(\mathbb{N})| \\ &> |\mathbb{N}| \\ &= \aleph_0. \end{aligned}$$

Starting with $\aleph_0$ we can exponentiate to get more and more infinite cardinals. We already saw that $2^{\aleph_0}$ is the cardinality of the real numbers. Cantor spent his whole life trying to prove:

Conjecture 19.7 (Continuum hypothesis)**.** *There are no cadinals $\beth$ between $\aleph_0$ and $2^{\aleph_0}$, that is, if*

$$\aleph_0 \leq \beth < 2^{\aleph_0}$$

then $\beth = \aleph_0$.

Around sixty years after Cantor made this conjecture, the following was proved:

Theorem 19.8 (Kurt Gödel)**.** *There is a model of set theory in which the continuum hypothesis is true.*

However thirty years later:

Theorem 19.9 (Paul Cohen)**.** *There is a model of set theory in which the continuum hypothesis is false.*

In other words, the continuum hypothesis is independent of the other axioms of set theory. We get to choose if we want it to be true or not.

We end this section with a proof of Schröder-Bernstein:

Proof of (18.2). There is no harm in assuming that A and B have no elements in common. We label the elements x of $A \cup B$ with three different colours, red, blue and green, determined by the ancestry of the element. We colour the elements of $A \cup B$ recursively, that is, step by step.

If $x \in A$ and there is no element y of B such that $g(y) = x$ then we label x red. If $x \in B$ and there is no element y of A such that $f(y) = x$ then we label y blue. This is the zeroth step. Suppose that the elements we have coloured are $A_0 \cup B_0$.

If $y \in B_0$, so that y is coloured blue, then we colour $x = g(y) \in A$ blue as well. If $y \in A_0$, so that y is coloured red, then we colour $x = f(y) \in B$ red. We have now coloured the elements of $A \cup B$ that can trace their lineage one step back. Call these elements $A_1 \cup B_1$. This is the first step.

Suppose we have defined $A_0, A_1, A_2, \dots, A_n$ and $B_0, B_1, B_2, \dots, B_n$. We let $A_{n+1} = g(B_n)$ and $B_{n+1} = f(A_n)$ and use the same colours, that is we colour B_{n+1} the same colour as A_n and A_{n+1} the same colour as B_n. This is the nth step.

At the end of this process we have defined two infinite sequences

$$A_0, A_1, A_2, \dots \qquad \text{and} \qquad B_0, B_1, B_2, \dots .$$

We coloured the elements of the first sequence with even indices and the elements of the second sequence with odd indices, red, and we coloured the elements of the first sequence with odd indices and the elements of the second second with even indices, blue.

If there are any elements of $A \cup B$ which are not coloured red or blue at the end of this process then we colour these elements green. These are the elements of $A \cup B$ which have infinitely many ancestors.

Define a function

$$h \colon A \longrightarrow B,$$

by the following rule:

$$h(a) = \begin{cases} f(a) & \text{if } a \text{ is coloured red} \\ b & \text{if } a \text{ is coloured blue and } g(b) = a \\ f(a) & \text{if } a \text{ is coloured green.} \end{cases}$$

We check that h is a bijection. Note that f and g preserve the red-blue-green colouring. If $a \in A$ then a and $f(a)$ have the same colouring. If a is red or blue then $f(a)$ is red or blue by definition. If a is green then a has infinitely many ancestors and so $f(a)$ has infinitely many ancestors. But then $f(a)$ is green. Thus h preserves the red-blue-green colouring as well.

First we check injectivity. Suppose $h(a_1) = h(a_2)$. Then a_1 and a_2 have the same colour. If they are both red or green then $h(a_i) = f(a_i)$ and so $f(a_1) = f(a_2)$. But then $a_1 = a_2$ as f is injective. If a_1 and a_2 are both blue then $a_1 = g(b) = a_2$, where $b = h(a_1) = h(a_2)$. Thus h is injective.

Now we check surjectivity. Suppose that $b \in B$. If b is red or green then we may find $a \in A$ such that $f(a) = b$. In this case $h(a) = f(a) = b$. If b is blue then let $g(b) = a$. Then a is blue and so $h(a) = b$, by definition of h. Thus h is surjective.

Thus h is a bijection. $\square$