

Sheet 4: Cardinal Numbers

Definition 1 (Cardinality) Two sets, A and B , have the same cardinality if there exists a bijective function $f : A \rightarrow B$. The cardinality of a set A is denoted by $|A|$.

Definition 2 (Finite and Infinite Sets) A set X is finite if it is empty or there is a natural number n and a bijective function $f : X \rightarrow \{1, 2, \dots, n\}$. A set that is not finite is infinite.

Theorem 3 The even positive integers have the same cardinality as the natural numbers.

Proof. Let $f : \mathbb{N} \rightarrow \{2n \mid n \in \mathbb{N}\}$ be defined as $f = 2n$. Let a and b be even, positive integers such that $f(a) = f(b)$. Then $a = 2k$ and $b = 2l$ for some $k, l \in \mathbb{N}$. But then $2k = 2l$ and so $k = l$. Thus f is injective. Then note that $k \in \mathbb{N}$ and so for every even, positive integer, a , there exists a natural number k such that $f(k) = n$. Thus f is surjective. \square

Theorem 4 $|\mathbb{N}| = |\mathbb{Z}|$.

Proof. Define $f : \mathbb{Z} \rightarrow \mathbb{N}$ as

$$f(n) = \begin{cases} 2n & \text{if } n > 0 \\ -2n + 1 & \text{if } n \leq 0. \end{cases}$$

Let $a, b \in \mathbb{Z}$ such that $a \neq b$. Without loss of generality assume that $a > 0$. If $b > 0$ then we have $f(a) = 2a \neq 2b = f(b)$. If $b < 0$ then $f(a)$ is even and $f(b)$ is odd and so $f(a) \neq f(b)$. Lastly assume that $a < 0$ and $b < 0$. Then $f(a) = -2a + 1$ and $f(b) = -2b + 1$ and since $-2a \neq -2b$, clearly $f(a) \neq f(b)$. Since all cases are covered, f is injective. Now let $a \in \mathbb{Z}$. Then a is even or odd. If a is even then $a = 2k$ for some $k \in \mathbb{Z}$ and so $a = f(k)$. If a is odd then $a = 2k + 1 = -2(-k) + 1$ for some $k \in \mathbb{Z}$ and so $a = f(-k)$. Since every natural number is the image of some integer, we have f is surjective. \square

Theorem 5 Every subset of \mathbb{N} is either finite or has the same cardinality as \mathbb{N} .

Proof. Let $A \subseteq \mathbb{N}$ be a subset such that A is not finite. Then A is infinite. Since A is a subset of \mathbb{N} we can order the elements in A . Define a function $f : \mathbb{N} \rightarrow A$ such that $f(n)$ is the n th element of A . This function is injective because for any two $a, b \in \mathbb{N}$, $f(a) < f(b)$ or $f(b) < f(a)$ and so $f(a) \neq f(b)$. The function is surjective because an arbitrary element of A has a place in the order so that it corresponds to some element in \mathbb{N} . Thus we see that if a subset of \mathbb{N} is not finite, then it has the same cardinality as \mathbb{N} . \square

Definition 6 (Countable Sets) A set that has the same cardinality as a subset of \mathbb{N} is countable.

Theorem 7 Every infinite set has a countably infinite subset.

Proof. Create a subset of some infinite set by consecutively taking elements and numbering them in the order they were chosen. We can always choose a next element because the set is infinite. \square

Theorem 8 A set is infinite if and only if there is an injective function from the set into a proper subset of itself.

Proof. Let A be a set and let $B \subsetneq A$ be a proper subset such that there exists an injective function $f : A \rightarrow B$. Suppose that A is finite. Then $|A| = n$ and $|B| = m$ for $m, n \in \mathbb{N}$ and $m < n$. We have f is injective and so for any $a, b \in A$ such that $a \neq b$ we have $f(a) \neq f(b)$. But then $f(A) = \{f(x) \mid x \in A\}$ and since there are n elements in A and f is injective, $|f(A)| = n$. But f maps from A to B and $|B| < n$. This is a contradiction and so A must be infinite.

Let A be an infinite set and let $B \subseteq A$ be a countable subset of A such that $B = \{b_1, b_2, b_3, \dots\}$. Define a function $f : A \rightarrow A$ where

$$f(n) = \begin{cases} n & \text{if } n \notin B \\ b_{2k} & \text{if } n \in B \text{ and } n = b_k. \end{cases}$$

Then f is injective because for any two elements $a, b \in A$ such that $a \neq b$, we have $f(a) \neq f(b)$ if $a \in B$ and $b \notin B$ or $a \notin B$ and $b \in B$. If $a \notin B$ and $b \notin B$ then we have $f(a) = a \neq b = f(b)$. If $a \in B$ and $b \in B$ then $a = b_k$ and $b = b_j$ such that $k \neq j$. Then $f(a) = b_{2k} \neq b_{2j} = f(b)$. But f maps to a proper subset of A because all the elements of B with odd indices are not mapped to. \square

Theorem 9 \mathbb{Q} is countable.

Proof. Let $S = \{A_i \mid i \in \mathbb{Z}\}$ be a countable set of sets where each A_i contains every element of \mathbb{Q} of the form i/q where $q \in \mathbb{Z}$. Note that each A_i is a countable set since \mathbb{Z} is countable. But also S is countable for the same reason. Then by Theorem 11 we have $\bigcup_{A_i \in S} A_i$ is countable. Then for $a/b \in \mathbb{Q}$ we have $a/b \in A_a$ so $\mathbb{Q} \subseteq \bigcup_{A_i \in S} A_i$ and so \mathbb{Q} is a subset of a countable set and must be countable. \square

Theorem 10 The union of two countable sets is countable.

Proof. Let A and B be two countable sets. If either A or B is finite then the problem is trivial: map all the elements of a finite set of size n to the first n natural numbers and then map the first element of the other set to $n + 1$ and so on. So suppose A and B are both infinite. First suppose that $A \cap B \neq \emptyset$. Then we can consider $A \setminus B$ and B . These sets are disjoint and they are both countable since they are subsets of countable sets, but their union is still $A \cup B$. So we can effectively assume that A and B are disjoint. Since A and B are countable there exist functions $f : \mathbb{N} \rightarrow A$ and $g : \mathbb{N} \rightarrow B$. Define a new function $h : \mathbb{N} \rightarrow A \cup B$ such that

$$h(n) = \begin{cases} f(\frac{n+1}{2}) & \text{if } n \text{ is odd} \\ g(\frac{n}{2}) & \text{if } n \text{ is even.} \end{cases}$$

Since A and B are disjoint and because every natural number is either even or odd, h is injective. To show that h is surjective we pick an element $x \in A \cup B$. Then $x \in A$ or $x \in B$. Suppose $x \in A$. Then $x = f(n)$ for some $n \in \mathbb{N}$ since f is surjective. But then $n = \frac{k+1}{2}$ for some $k \in \mathbb{N}$ and so $h(k) = f(n) = x$. Since h is a bijection we have $A \cup B$ is countable. \square

Theorem 11 The union of countably many countable sets is countable.

Proof. Let P be the set of primes, $\{p_1, p_2, p_3, \dots\}$. Consider the set, R , of all primes raised to natural number powers. That is

$$R = \bigcup_{p_i \in P} \{p_i^1, p_i^2, p_i^3, \dots\}.$$

Let $S = \{A_1, A_2, A_3, \dots\}$ be a set of countable sets and let $T = \bigcup_{A_i \in S} A_i = \{a_{i_j} \mid a_{i_j} \text{ is the } j\text{th element of } A_i\}$. Note that some $a_{i_j} \in T$ may belong to multiple sets from S . In this case, let the index correspond to the first set in S for which a_{i_j} belongs. Then let $f : T \rightarrow R$ be a function such that $f(a_{i_j}) = p_i^j$. Note that f must be injective because each $a_{i_j} \in T$ has a unique index and so two distinct elements of T will either be mapped to different primes raised to powers, or to the same prime raised to different powers so their images cannot be equal due to unique factorization. We have f is surjective if S and all of its elements are infinite. In this case we simply consider some element $x \in R$ and note that by definition $x = p_i^j$ for some $p_i \in P$ and $j \in \mathbb{N}$. But since S and its elements are infinite there exists some $A_i \in S$ and some $a_j \in A_i$ such that $f(a_{i_j}) = x$. In the case where S or some $A_i \in S$ are not infinite, there exists some function $g : T \rightarrow R'$ where $R' \subseteq R \subseteq \mathbb{N}$ which is surjective and still holds the injective property that f has. So in all cases we have T is countable. \square

Theorem 12 The set of all finite subsets of a countable set is countable.

Proof. Let P be the set of prime numbers. This set is countable because it is a subset of \mathbb{N} . Define $F = \{A \mid A \text{ is a finite subset of } P\}$ and $G = \{n \in \mathbb{N} \mid n \text{ is a product of distinct primes raised to a single power}\}$. Define $f : F \rightarrow G$ where f takes a finite subset of P and multiplies all the elements together. Let A and B be two distinct finite subsets of P . The product of all the elements in A must be different than that of B because of unique factorization. So we have $f(A) \neq f(B)$. Furthermore, for a given element of \mathbb{N} there exists a unique prime factorization and since $G \subseteq \mathbb{N}$, for all $n \in G$ there exists some $A \in F$ whose elements multiply to n . Thus, f is injective and surjective and since $G \subseteq \mathbb{N}$, the set of all finite subsets of P is countable. Since $|P| = |\mathbb{N}|$, the set of all finite subsets for any countable set is countable. \square

Exercise 13 (Submarine Game) Suppose a submarine is moving in a straight line at a constant speed in the plane such that at each hour, the submarine is at a lattice point. Suppose at each hour you can explode one depth charge at a lattice point that will kill the submarine if it is there. You do not know where the submarine is nor do you know where or when it started. Can you eventually destroy the submarine?

Proof. To find the submarine we need information from three countable sets. First let S be the set of all possible starting points for the submarine. Assume it starts on the hour on a lattice point so that $S = \mathbb{Z} \times \mathbb{Z}$. Then we have the set T of all possible elapsed times which is always a natural number so $T = \mathbb{N}$. Finally we need a speed and direction and so we take V to be the set of all 2-vectors so that $|V| = |\mathbb{Z} \times \mathbb{Z}|$. If we consider $S \times T \times V$ then we have a set which encompasses all possible locations of the sub at any given time. But this set is countable because the union of countably many countable sets is countable. Thus $\mathbb{N} \times \mathbb{N}$ is countable and so the product of any two countable sets is countable (note that S , T and V are all countable). Since the location set is countable we can assign a natural number to every possible location for the sub and so we can eventually destroy it. \square

Exercise 14 (Algorithmic Submarine) Same game, but the submarine is now jumping between lattice points following an algorithm (that you don't know). Can you eventually destroy the submarine now?

Proof. An algorithm is a set of instructions that can be followed by a computer so consequently the set of all algorithms is a countable set. Then, by a similar method to Exercise 13 we take the set of all starting points S and all times elapsed T and then the set of all algorithms A . Then $S \times T \times A$ is a countable set which gives us the position of the sub at any time. Thus we can still assign a natural number to the sub's location at any time so we can eventually destroy it. \square

For a set A let

$$2^A = \{B \mid B \subseteq A\}$$

be the set of subsets of A ; we call it the power set of A .

Theorem 15 For a set A , there is an injective function from A to 2^A .

Proof. For $A = \emptyset$ any function $f : A \rightarrow 2^A$ will vacuously be injective because there are no elements of A . Thus every time we have $a, b \in A$ with $a \neq b$ we have $f(a) \neq f(b)$. For nonempty A let $f : A \rightarrow 2^A$ be a function such that $f(a) = \{a\}$. This function is clearly injective because for all $a, b \in A$ with $a \neq b$ we have $f(a) = \{a\} \neq \{b\} = f(b)$. \square

Theorem 16 For a set A , let P be set of all functions from A to the two point set $\{0, 1\}$. Then $|P| = |2^A|$.

Proof. Let $f : 2^A \rightarrow P$ be a function defined so that for $B \subseteq A$, $f(B)$ maps to some function g with

$$g(a) = \begin{cases} 1 & \text{for } a \in B \\ 0 & \text{for } a \notin B. \end{cases}$$

Let B, C be distinct subsets of A . Without loss of generality, assume that there exists $a \in B$ such that $a \notin C$. Then $f(B)$ gives a function g such that $g(a) = 1$ and $f(C)$ gives a function h such that $h(a) = 0$.

Thus, for $B, C \in 2^A$ with $B \neq C$ we have $f(B) \neq f(C)$. Thus f is injective. For surjectivity, let $g \in P$. Then create a subset $B \subseteq A$ such that $a \in B$ if $g(a) = 1$ and $a \notin B$ if $g(a) = 0$. \square

Theorem 17 *There is a bijection between $2^{\mathbb{N}}$ and infinite sequences of 0's and 1's.*

Proof. Let f be a function from $2^{\mathbb{N}}$ to the set of infinite sequences of 0's and 1's. Define f so that $f(A)$ is a sequence with the n th element as 1 if $n \in A$ and 0 if $n \notin A$. Consider two subsets of \mathbb{N} , A, B with $A \neq B$. Without loss of generality assume that $a \in A$ and $a \notin B$. Then we have $f(A)$ is a sequence with a 1 in the a th place and $f(B)$ is a sequence with a 0 in the a th place. Thus, $f(A) \neq f(B)$ and so f is injective. For surjectivity pick an infinite sequence of 1's and 0's. Create a subset of \mathbb{N} by taking the places of all the 1's and putting them in the subset and excluding the places of the 0's. Since every place in the sequence is a natural number, clearly this subset exists. \square

Theorem 18 (Cantor) *There is no map from the set A onto 2^A .*

Proof. Suppose that there is a bijective function $f : A \rightarrow 2^A$. Then for all $X \subseteq A$ there exists $x \in A$ such that $f(x) = X$. Consider $B = \{x \in A \mid x \notin f(x)\}$. Then there exists $b \in A$ such that $f(b) = B$. In the case where $b \in B$, by definition of B , $b \notin f(b) = B$. In the case where $b \notin B$, then by definition of B , $b \in B$. In either case we have a contradiction and so there exists no such function f . \square

Corollary 19 *There are infinitely many different infinite cardinalities.*

Proof. From Theorem 18 we know that for an infinite set A , $|A|$ and $|2^A|$ are different cardinalities. But then $|2^A|$ and $|2^{2^A}|$ are different cardinalities. We can continue in the process indefinitely so that there cannot be a finite number of infinite cardinalities. \square

Exercise 20 *Find a bijection $f : [0; 1] \rightarrow [0; 1]$.*

Proof. Define a function $f : [0; 1] \rightarrow [0; 1]$ where

$$f(x) = \begin{cases} x & \text{if } x \neq \frac{1}{n} \text{ for } n \in \mathbb{N} \\ \frac{1}{n+1} & \text{if } x = \frac{1}{n} \text{ for } n \in \mathbb{N}. \end{cases}$$

We see that f is surjective because any number not of the form $1/n$ with $n \in \mathbb{N}$ in $[0; 1]$ will have been mapped there by itself. If $y = 1/n$ for $n \in \mathbb{N}$ and $y \in [0; 1]$ then $x = 1/(n-1) \in [0; 1]$ and $f(x) = y$. To show f is injective take $f(a) = f(b)$ for $f(a), f(b) \in [0; 1]$. There are three possibilities. First suppose that $f(a) \neq 1/m$ and $f(b) \neq 1/n$ for all $m, n \in \mathbb{N}$. Then $a = f(a) = f(b) = b$. Secondly we see that if $f(a) = 1/m$ and $f(b) \neq 1/n$ for $m, n \in \mathbb{N}$ then we have $a = 1/(m-1)$ and $b = f(b) \neq 1/n$ for $n \in \mathbb{N}$ so this case is impossible. Thirdly if we have $f(a) = 1/m$ and $f(b) = 1/n$ for $m, n \in \mathbb{N}$ then we have $a = 1/(m-1)$ and $b = 1/(n-1)$. But $f(a) = f(b)$ so $1/m = 1/n$ and $m = n$. Then $a = 1/(m-1) = 1/(n-1) = b$. In all cases we have if $f(a) = f(b)$ then $a = b$ so f is injective. \square

Theorem 21 (Schröder-Bernstein) *If A and B are sets such that there exist injective functions $f : A \rightarrow B$ and $g : B \rightarrow A$, then $|A| = |B|$.*

Theorem 22 $|\mathbb{R}| = |(0; 1)| = |[0; 1]|$

Proof. To show $|\mathbb{R}| = |(0; 1)|$ we define $f : (0; 1) \rightarrow \mathbb{R}$ such that

$$f(x) = \begin{cases} \frac{1}{x} - 2 & \text{if } 0 < x \leq \frac{1}{2} \\ \frac{-1}{1-x} + 2 & \text{if } \frac{1}{2} < x < 1. \end{cases}$$

Pick $a, b \in (0, 1)$ such that $a \neq b$. There are three possibilities. Let $a, b \leq \frac{1}{2}$. Then $f(a) = \frac{1}{a} - 2$ and $f(b) = \frac{1}{b} - 2$ but then since $\frac{1}{a} \neq \frac{1}{b}$ we have $f(a) \neq f(b)$. Now suppose that $a, b > \frac{1}{2}$. Then we have $f(a) = \frac{-1}{1-a} + 2$ and $f(b) = \frac{-1}{1-b} + 2$. But we have $a \neq b$ and so $1-a \neq 1-b$ and $\frac{-1}{1-a} \neq \frac{-1}{1-b}$. Thus

$f(a) \neq f(b)$. Finally without loss of generality consider $a \leq \frac{1}{2}$ and $b > \frac{1}{2}$. Then $f(a) = \frac{1}{a} - 2$ and $f(b) = \frac{-1}{1-b} + 2$. Suppose $f(a) = f(b)$. Then $\frac{1}{a} + \frac{1}{1-b} = 4$. But since $b > \frac{1}{2}$ and $a \leq \frac{1}{2}$ we have a contradiction. Thus $f(a) \neq f(b)$. Therefore f is injective. To show that f is surjective pick an arbitrary element x from \mathbb{R} . If $x > 0$ then $x + 2 > 0$ and so $0 < \frac{1}{x+2} \leq \frac{1}{2}$. Likewise if $x < 0$ then $x - 2 < 0$ and so $\frac{1}{2} < \frac{-1}{x-2} - 1 < 1$. Therefore f is surjective. Thus f is a bijection.

To show that $|(0; 1)| = |[0; 1]|$ we use a similar proof to Exercise 20 and let $f : [0; 1] \rightarrow (0; 1)$ be defined by

$$f(x) = \begin{cases} x & \text{if } x \neq \frac{1}{n} \text{ for } n \in \mathbb{N} \\ \frac{1}{2} & \text{if } x = 0 \\ \frac{1}{n+2} & \text{if } x = \frac{1}{n} \text{ for } n \in \mathbb{N}. \end{cases}$$

Like in Exercise 20 this function maps elements of $[0; 1]$ not of the form $1/n$ for $n \in \mathbb{N}$ to themselves and shifts elements of the form $1/n$. In this case 0 needs to be mapped to $1/2$ because $0 \notin (0; 1)$ so each $1/n$ is shifted two places instead of 1. Similar arguments for surjectivity and injectivity used in Exercise 20 will hold for this function. \square

Theorem 23 *There is an injective function $f : \mathbb{R} \rightarrow 2^{\mathbb{N}}$.*

Proof. We know that \mathbb{Q} is countable and so there exists an injective function $f : \mathbb{Q} \rightarrow \mathbb{N}$. But then there must exist a map from $2^{\mathbb{Q}}$ to $2^{\mathbb{N}}$ because any subset of \mathbb{Q} will map to a subset of \mathbb{N} containing the images of the elements in \mathbb{Q} under f . But each element of \mathbb{R} is a subset of \mathbb{Q} because they are all cuts. We can map every element of \mathbb{R} to $2^{\mathbb{N}}$ using the same map that we have from $2^{\mathbb{Q}}$ to $2^{\mathbb{N}}$ which is injective. \square

Theorem 24 $|\mathbb{R}| = |2^{\mathbb{N}}|$.

Proof. We know that there exists a map from $2^{\mathbb{N}}$ to infinite sequences of 0's and 1's. But we can turn any sequence of 0's and 1's into a real number by expressing it in decimal notation and putting a decimal point in front of it. This real number will be unique because it represents the intersection of an infinite number of enclosed sets. So now we have an injective map from $2^{\mathbb{N}}$ to \mathbb{R} and from Theorem 23 we have an injective function from \mathbb{R} to $2^{\mathbb{N}}$. Thus, by Theorem 21 we have $|\mathbb{R}| = |2^{\mathbb{N}}|$. \square