# CHAPTER 3: CARDINALITY AND COUNTING

WAYNE AITKEN AND LINDA HOLT

*Summer 2019 Edition*

This chapter is devoted to idea of *counting* and *cardinality* for finite sets. These are arguably the most important applications of the natural numbers $\mathbb{N}$. An important result is the *invariance of counting*: it does not matter what order you count a given finite set, the answer will be the same. We also consider cardinality properties of the following: subsets, bijections, injections, surjections, addition, multiplication, subtraction, and exponentiation. We use these ideas to give alternative, set-based proofs of some of the basic laws of arithmetic. These proofs are more insightful than the induction proofs from Chapter 1. Counting principles, such as the pigeonhole principle and the inclusion-exclusion principle, will be also be discussed.

We end with a short discussion of how iteration is related to addition and multiplication. This illustrates an important application for the operations of addition and multiplication, and prepares us for Chapter 4 where multiplication in $\mathbb{Z}$ is developed in terms of iteration.

By the end of the chapter we will have seen three characterizations each of addition and multiplication.

Addition is

(i) iterated successor (Chapter 1),

(ii) what is needed to count disjoint unions,

(iii) what is needed to describe the composition of two iterations.

Multiplication is

(i) iterated addition (Chapter 1),

(ii) what is needed to count cartesian products,

(iii) what is needed to describe the iteration of an iteration.

*Remark* 1. Our focus on counting and cardinality explains why we include 0 as an element of $\mathbb{N}$. Although classifying 0 as a natural number is quite common, some adopt the convention that the integer 1 is the first natural number; this is a reflection of the historical fact that 0 was developed much later than the positive integers. However, the empty set is very common in modern mathematics, and we want to be able to count all finite sets including the empty set. We need 0 as a natural number in order to define the size (cardinality) of the empty set.

## 1. Background and notation

In this section we review some basic facts about the empty set $\varnothing$ and the sets $\{1, \ldots, n\}$ (which we will call $\langle n \rangle$). These will be useful in our discussions of counting later in the chapter. We begin with descriptions of functions to and from the empty set. Since these concern basic set theory, we take them as given (but the proofs are not difficult).

**Proposition 1.** *Let $S$ be a set. There is a unique function $\varnothing \to S$. It is injective. It is surjective if and only if $S$ is also the empty set.*

*On the other hand, there are no functions $S \to \varnothing$ unless $S$ is also the empty set.*

In Chapter 2 we defined the set $\{1, \ldots, n\}$ as $\{x \in \mathbb{N} \mid 1 \leq x \leq n\}$. These sets will be used extensively in this chapter, even if $n = 0$. Observe that, by definition, $\{1, \ldots 0\}$ is the empty set. However, the notation $\{1, \ldots 0\}$ is a bit awkward and may even suggest counting down from 1 to 0, which is not what we want. So in this chapter we introduce the notation $\langle n \rangle$ as an alternative to $\{1, \ldots, n\}$.

**Definition 1.** If $n \in \mathbb{N}$ then

$$\langle n \rangle \stackrel{\text{def}}{=} \{x \in \mathbb{N} \mid 1 \leq x \leq n\}.$$

We can translate results from Chapter 2 to the new notation:

**Proposition 2.** *The set $\langle 0 \rangle$ is the empty set. The set $\langle 1 \rangle$ is $\{1\}$. The set $\langle 2 \rangle$ is $\{1, 2\}$. The set $\langle 3 \rangle$ is $\{1, 2, 3\}$.*

We can continue the above pattern with the following result:

**Proposition 3.** *Let $n \in \mathbb{N}$. Then the set $\langle n + 1 \rangle$ is $\langle n \rangle \cup \{n + 1\}$.*

*Proof.* If $n > 0$ then this just restates a result from Chapter 2. If $n = 0$ this result just states that $\{1\} = \varnothing \cup \{1\}$ which is a special case of a basic set theoretic result. □

*Note.* The above results are labelled as "propositions". From a logical point of view, there is no difference between terms such as "lemma", "proposition", "theorem", and "corollary". These terms all refer to mathematical statements that can be proved. Authors use different terms to emphasize the role of the results in the overall narrative, or the relationship between results. The above were called "propositions" to emphasize that they are not new results, but just restatements of results from before. This allows us to reserve the term "theorem" for new results.

## 2. The invariance of counting

We count a finite set $S$ by assigning a number to each object in $S$. We start by picking an object of $S$ and assigning it 1. Then we assign 2 to another object of $S$ (if there are any more). We continue until we have

assigned a number, $n$ say, to a final element of $S$. We then declare that $S$ has $n$ elements. This is a method we all learn as small children counting, say, apples or Halloween candy.

So in the process of counting a set $S$ of $n$ objects, every integer in $\{1, \ldots, n\}$ is assigned to an element of $S$. In other words, this process defines a function

$$\{1, \ldots, n\} \to S.$$

We assign distinct numbers to distinct objects, so the function is injective (one-to-one). We assign a number to every element of $S$, so the function is surjective (onto). Thus counting a finite set $S$ is really the same thing as building a bijection $\{1, \ldots, n\} \to S$. Recall that we adopted the notation $\langle n \rangle$ for $\{1, \ldots, n\}$, where $\langle 0 \rangle$ is just the empty set.

This informal discussion motivates the following formal definition.

**Definition 2.** Let $S$ be a set. If there is a bijection

$$\langle n \rangle \to S$$

with $n \in \mathbb{N}$, then we say that $S$ *is counted by* $n$. The bijection $\langle n \rangle \to S$ is called a *counting function* or a *counting*.

We can count the objects of a set $S$ in any order we like: we instinctively know that we will get the same result regardless of how we choose to assign the integers. In particular, if we have two countings $f : \{1, \ldots, m\} \to S$ and $g : \{1, \ldots, n\} \to S$ of the same set $S$, we expect that $m = n$. Why do we expect this to hold? Probably very few people are explicitly taught this principle. Is it based on experience or are we hard-wired to believe it? We will pass over such psychological questions. What is important to our axiomatic approach is that we *not* take it for granted. Instead it is a theorem:

**Theorem 4** (Invariance of counting)**.** *Suppose that a set $S$ can be counted by $m$ and $n$. Then $m = n$.*

**Definition 3.** A set $S$ is said to be *finite* if there is an $n \in \mathbb{N}$ such that $S$ is counted by $n$.

Suppose that $S$ is a finite set. Then the *cardinality* or *size* of $S$ is defined to be the element $n \in \mathbb{N}$ such that $S$ can be counted by $n$. This element is unique by the above theorem, so cardinality is well-defined. We write the cardinality of $S$ as $|S|$ or $\#S$.

We will prove the invariance of counting theorem after establishing some lemmas. The main proof will be by induction, and a key step, Lemma 8, will require the following intuitively obvious principle: given any $a \in S$ we can count $a$ last. In other words, suppose that $S$ can be counted by $n$ and that $a \in S$, then we can find a counting function $f : \{1, \ldots, n\} \to S$ where $f(n) = a$. To prove this is possible (Lemma 7), we will first introduce the idea of a *transposition*:

**Definition 4.** Suppose $a, b \in S$. Consider the function $\tau_{(a\,b)} : S \to S$ defined by the rule $a \mapsto b$, $b \mapsto a$, and $x \mapsto x$ if $x$ is not equal to $a$ or $b$.

Observe that if $a = b$ then $\tau_{(a\,b)}$ is by definition the identity map. If $a \neq b$ then $\tau_{(a\,b)}$ is called a *transposition*.

In other words, the function $\tau_{a,b}$ just switches $a$ and $b$: $\tau_{(a\,b)}(a) = b$ and $\tau_{(a\,b)}(b) = a$, but $\tau_{(a\,b)}(c) = c$ when $c \neq a, c \neq b$. These equations can be used to prove the following:

**Lemma 5.** *Suppose $a, b \in S$. Then $\tau^2_{(a\,b)}$ is the identity function on $S$. In other words, $\tau_{(a\,b)} : S \to S$ is its own inverse.*

Since $\tau_{(a\,b)} : S \to S$ has an inverse, we have the following:

**Corollary 6.** *Suppose $a, b \in S$. Then $\tau_{(a\,b)} \colon S \to S$ is a bijection.*

**Lemma 7.** *Suppose that $S$ is a finite set with element $a \in S$, and suppose that $S$ can be counted by $n > 0$. Then there is a bijection $f : \{1, \ldots, n\} \to S$ with the property that $f(n) = a$.*

*Proof.* By Definition 2, there is a bijection $g : \{1, \ldots, n\} \to S$. Form the function $f = \tau_{(a\,b)} \circ g$ where $b = g(n)$. Since $\tau_{(a\,b)}$ and $g$ are bijections, the same is true of the composition $f$. Finally,

$$f(n) = \tau_{(a\,b)}\big(g(n)\big) = \tau_{(a\,b)}(b) = a.$$

□

The following is critical to the proof of the invariance of counting.

**Lemma 8.** *Suppose $S$ is a set, and suppose that $S' = S \cup \{a\}$ where $a \notin S$. If $S'$ can be counted by $n + 1$, then $S$ can be counted by $n$.*

*Proof.* By Lemma 7, we can assume $a$ is counted last. In other words, we have a bijection $f : \langle n + 1 \rangle \to S'$ with $f(n + 1) = a$. Since $f$ is injective, $f(x) \neq a$ if $x < n + 1$. In particular, if $x \in \langle n \rangle$ then $f(x) \in S$.

Define $h \colon \langle n \rangle \to S$ to be the restriction of $f$ to a smaller domain and codomain. In other words, $h(x) = f(x)$ for all $x \in \langle n \rangle$. The only real difference between $f$ and $h$ is the domain and codomain. Observe that $h$ is injective: $h(x) = h(y)$ implies $f(x) = f(y)$, which in turn implies $x = y$ since $f$ is an injection.

Now we will show that $h$ is surjective. Let $y \in S$. If $y \in S$ then, since $f$ is surjective, there is an $x \in \langle n + 1 \rangle$ such that $f(x) = y$. Observe that $a \neq y$ since $a \notin S$. So $x \neq n + 1$ because $f(n + 1) = a \neq y$. Since $x \neq n + 1$ and since

$$\langle n + 1 \rangle = \langle n \rangle \cup \{n + 1\}$$

by Proposition 3, we have that $x \in \langle n \rangle$. So $x$ is in the domain of $h$, and we have $h(x) = f(x) = y$. We conclude that $h$ is surjective.

Since $h$ is a bijection, $S$ is counted by $n$. This establishes the lemma. □

*Remark* 2. The above proof is perfectly valid even for the case $n = 0$, but it is a bit unnatural and overly long for this simple case. In this case, when we restrict $f$ we get a function $h\colon \langle 0\rangle \to S$ which is automatically injective by Proposition 1. The proof of surjectivity given above can be interpreted as a proof that $S$ is empty: assume $y \in S$ (i.e., assume that $S$ is not empty), then there is an element $x \in \langle 1\rangle$ mapping to $y$. But we can show $x \neq 1$. This is a contradiction since $\langle 1\rangle = \{1\}$, so $S$ is empty. Once we know $S$ is empty, then $h$ is a bijection by Proposition 1.

**Exercise 1.** The following lemma is important for the base case of the induction proof of the main theorem. Prove all three claims of this lemma using Proposition 1.

**Lemma 9.** *The empty set $\varnothing$ can be counted by 0. The empty set is the only set that can be counted by 0 (in other words, if a set $S$ is counted by 0, it is empty). Furthermore, the empty set cannot be counted by $n > 0$.*

Now we prove the main theorem:

*Proof. (Theorem 4).* The proof is by induction. We set up the induction by defininining $A$ be the set of all natural numbers $u$ with the property that *any set $T$ that can be counted by $u$ can only be counted by $u$*. Our goal is to show that $A = \mathbb{N}$.

First we consider the base case with $u = 0$. Suppose $T$ is a set that can be counted by 0. By Lemma 9, $T$ must be the empty set, and can only be counted by 0. This implies $0 \in A$ (base case).

Now suppose $n \in A$. We want to show that $n + 1 \in A$ by showing that any set that can be counted by $n+1$, can only be counted by $n+1$. So let $T$ be a set that can be counted by $n + 1$. Our goal is to show that if $T$ can by counted by $p$ then $p = n + 1$. Since $n + 1 > 0$, we have $T$ is nonempty, and so $p > 0$ (Lemma 9). Since $p > 0$, we have $p = m + 1$ for some $m$. Let $a \in T$ (which exists since $T$ is not empty). Let $S$ be the set obtained by removing $a$ from $T$. By Lemma 8, since $T$ can be counted by $m + 1$, the set $S$ can be counted by $m$. Similarly, since $T$ can be counted by $n + 1$, the set $S$ can be counted by $n$. Since $n \in A$, the set $S$ can only be counted by $n$. So $n = m$. Thus $n + 1 = m + 1$.

We conclude that $n + 1 \in A$ if $n \in A$. By the induction axiom, $A = \mathbb{N}$.

Now we are ready to prove the main statement. Suppose that $S$ is a set that can be counted by $m$ and $n$. Since $\mathbb{N} = A$ we must have $n \in A$. By definition of $A$, the set $S$ can only be counted by $n$. Thus $m = n$. □

## 3. Basic properties of counting

**Theorem 10.** *Let $S$ be a finite set. The set $S$ has cardinality 0 if and only if it is empty. The set $S$ has positive cardinality if and only if it is nonempty.*

**Exercise 2.** Use Lemma 9 to prove the above.

**Theorem 11.** *Let $n \in \mathbb{N}$. The set $\langle n\rangle$ is finite and has cardinality $n$.*

**Exercise 3.** Give a very short proof of the above theorem.

**Exercise 4.** Show that if a set $S$ has cardinality 1 then it has a unique element.

The following theorems state that two finite sets have the same size if and only if there is a bijection between them.

**Theorem 12.** *Suppose $S$ is finite of cardinality $n$. If $f : S \to T$ is a bijection, then $T$ is finite and has cardinality $n$.*

**Theorem 13.** *Suppose $S$ and $T$ are finite of cardinality $n$. Then there is a bijection $S \to T$.*

**Exercise 5.** Use bijections to prove the above two theorems. (Do not prove them by induction.)

**Theorem 14.** *Suppose $S$ is finite of cardinality $n$. Suppose $a$ is an element outside $S$. Then the set $S' = S \cup \{a\}$ is finite of cardinality $n+1$.*

*Proof.* By Definition 2, there is a bijection $f\colon \langle n \rangle \to S$. By Proposition 3, we have $\langle n+1 \rangle = \langle n \rangle \cup \{n+1\}$. Observe that $n+1 \notin \langle n \rangle$. Our goal is to extend $f$ to a function $f' : \langle n+1 \rangle \to S'$.

Define $f' : \langle n+1 \rangle \to S'$ as follows: if $x \in \langle n \rangle$ then $f'(x) \stackrel{\text{def}}{=} f(x)$, but let $f'(n+1) \stackrel{\text{def}}{=} a$.

First we show that $f'$ is injective. To do so, suppose that $f'(x) = f'(y)$ where $x, y \in \langle n+1 \rangle$. We wish to show that $x = y$. If $x = y = n+1$ then we are done. If one of the two, $x$ say, is $n+1$, but the other is not then $f'(x) = a$ but $f'(y) = f(y) \in S$. Since $a \notin S$, we get a contradiction. The final case is where $x$ and $y$ are both not $n+1$. In this case, $f'(x) = f(x)$ and $f'(y) = f(y)$, so $f(x) = f(y)$. Thus $x = y$ since $f$ is injective.

Finally, observe that $f'$ is surjective. So $f' : \langle n+1 \rangle \to S'$ is a bijection. By Definition 2, $S'$ is counted by $n+1$. □

**Exercise 6.** Show that $f'$ in the above proof is surjective.

**Exercise 7.** Prove the following corollaries.

**Corollary 15.** *If $S = \{a\}$ then $S$ has cardinality 1.*

**Corollary 16.** *If $S = \{a, b\}$ where $a \neq b$, then $S$ has cardinality 2.*

**Theorem 17.** *If $A$ and $B$ are finite, then so is $A \cup B$.*

*Proof.* We prove the result by induction on the size of $B$. So fix a finite set $A$, and define $S$ as follows

$$S_A \stackrel{\text{def}}{=} \{x \in \mathbb{N} \mid A \cup B \text{ is finite for all sets } B \text{ of size } x\}$$

Since $A$ is an arbitrary finite set, the theorem will be established once we show that $S_A = \mathbb{N}$ regardless of $A$.

If $B$ has size 0, it is empty. So $A \cup B = A$. Thus $A \cup B$ is finite since $A$ is finite. Hence, $0 \in S_A$.

Suppose $n \in S_A$. We must show $n+1 \in S_A$. Let $B$ be a set of size $n+1$. We must show that $A \cup B$ is finite. Since $B$ has nonzero size, it is not empty. Let $b \in B$. Then $B - \{b\}$ has size $n$ by Lemma 8. Since $n \in S_A$, we conclude that $A \cup (B - \{b\})$ is finite. If $b \in A$ then $A \cup B = A \cup (B - \{b\})$, so $A \cup B$ is finite. If $b \notin A$, then we use Theorem 14 and the equality

$$A \cup B = A \cup (B - \{b\}) \cup \{b\}$$

to conclude that $A \cup B$ is finite. We have established that $n+1 \in S_A$.

By the induction axiom, $S_A = \mathbb{N}$ regardless of choice of $A$. The result follows. □

We end this section with two lemmas needed in the next section. These require the concept of ordered pair. Recall from set theory that if $A$ and $B$ are sets, then $A \times B$ is defined to be the set of ordered pairs with first coordinate in $A$ and second coordinate in $B$. Also recall from set theory that given $(a, b)$ and $(a', b')$ in $A \times B$, we have $(a, b) = (a', b')$ if and only if both $a = a'$ and $b = b'$.

**Lemma 18.** *Let $m, n \in \mathbb{N}$. There exists disjoint finite sets $A$ and $B$ such that $A$ has cardinality $m$ and $B$ has cardinality $n$.*

*Proof.* If $m = 0$ let $A = \varnothing$. Otherwise let

$$A = \{(1, x) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq x \leq m\}.$$

In this case, $x \mapsto (1, x)$ is a function $\{1, \ldots, m\} \to A$ with inverse function given by $(1, x) \mapsto x$. Thus the function is a bijection, so $A$ has size $m$.

Similarly, if $n = 0$ let $B = \varnothing$. Otherwise let

$$B = \{(2, x) \in \mathbb{N} \times \mathbb{N} \mid 1 \leq x \leq n\}.$$

In this case, we can define a bijection showing $B$ has size $n$.

Observe that the sets $A$ and $B$ are disjoint since their respective elements have different first coordinates. □

A similar proof gives the following.

**Lemma 19.** *Let $x, y, z \in \mathbb{N}$. There are pairwise disjoint finite sets $A, B, C$ such that $A$ has cardinality $x$, $B$ has cardinality $y$, and $C$ has cardinality $z$.*

**Exercise 8.** Define suitable $A, B, C$ for the above lemma.

## 4. New perspective on addition

In Chapter 1, addition was defined in terms of iteration of successor. However, there are other ways to characterize addition. For example, one might explain to a child that $m + n$ is the number of apples you have if you combine $m$ apples with $n$ additional apples. In other words, if $A$ is a set of $m$ objects, and if $B$ is a set of $n$ objects, then, as long as $A$ and $B$ are disjoint, $m + n$ is the size of $A \cup B$. We now prove the validity of this alternative characterization of addition. It basically follows the pattern of

Theorem 17 but uses a few basic laws of addition (proved in Chapter 1 before the associative and commutative laws).

**Theorem 20.** *Suppose that $A$ and $B$ are disjoint finite sets. Let $m$ be the size of $A$, and let $n$ be the size of $B$. Then $A \cup B$ has size $m+n$.*

*Proof.* We prove this by induction on the size of the second set. Let

$$S = \{u \in \mathbb{N} \mid A \cup X \text{ has size } m+u \text{ for all } X \text{ disjoint from } A \text{ of size } u\}$$

We start by showing $0 \in S$. If $X$ has size 0, then $X$ is the empty set, so $A \cup X = A$. Thus

$$|A \cup X| = |A| = m = m + 0.$$

We have established that $0 \in S$.

Suppose $k \in S$. We must show $k+1 \in S$. Suppose $X$ has size $k+1$, and that $X$ is disjoint from $A$. We must show that $A \cup X$ has size $m + (k+1)$.

Since $k+1 > 0$, the set $X$ is not empty. Let $x \in X$. Then $X - \{x\}$ has size $k$ by Lemma 8. Since $k \in S$, we conclude that $A \cup (X - \{x\})$ has size $m+k$. Now since $A$ and $X$ are disjoint, $x$ is not in $A \cup (X - \{x\})$. So $A \cup X = A \cup (X - \{x\}) \cup \{x\}$ has size $(m+k)+1$ by Theorem 14. By laws of Chapter 1 (before the associative and commutative laws)

$$(m+k)+1 = \sigma(m+k) = m + \sigma(k) = m + (k+1),$$

so $k+1 \in S_m$.

By the induction axiom, $S = \mathbb{N}$. Since $n \in \mathbb{N}$ we have $n \in S$. By definition of $S$, we have $|A \cup B| = m+n$. □

*Remark* 3. The above gives a second characterization of addition.

We now give new proofs of the commutative and associative laws.

**Theorem 21** (Commutative Law)**.** *If $m, n \in \mathbb{N}$, then $m+n = n+m$.*

*Proof.* Let $A$ and $B$ be disjoint sets such that $A$ has size $m$ and $B$ has size $n$ (Lemma 18). Now $A \cup B$ has size $m+n$ by the above theorem, and $B \cup A$ has size $n+m$. Since $A \cup B = B \cup A$, we have $m+n = n+m$. □

**Theorem 22** (Associative Law)**.** *If $x, y, z \in \mathbb{N}$, then $(x+y)+z = x+(y+z)$.*

*Proof.* (sketch). This follows from Lemma 19, and the identity

$$A \cup (B \cup C) = (A \cup B) \cup C.$$

□

**Exercise 9.** Write up the above proof. (You do not need to prove the identity $A \cup (B \cup C) = (A \cup B) \cup C$, since it is part of basic set theory.)

## 5. Subsets and functions

In this section we investigate issues of cardinality for subsets and functions.

It is intuitively obvious that every subset of a finite set is also finite. This intuition is confirmed by the following theorem.

**Theorem 23.** *Every subset of a finite set is itself finite.*

*Proof.* This will be proved by induction on the size of the set. Let

$$S = \{x \in \mathbb{N} \mid \text{all sets } C \text{ of size } x \text{ have only finite subsets}\}.$$

Claim: $0 \in S$. To see this, observe that the only set $C$ of size 0 is the empty set, and the only subset of the empty set is again the empty set. The empty set is finite. So $x = 0$ has the desired property.

Suppose $n \in S$. We must show $n+1 \in S$. To do so, let $C$ be a set of size $n+1$. We claim that all subsets $B \subseteq C$ are finite. If $B = C$ we are done since by assumption $C$ is finite. If $B$ is a proper subset, let $a \in C$ be an element not in $B$. Then $B$ is a subset of $C - \{a\}$. By Lemma 8, $C - \{a\}$ has size $n$. Since $n \in S$, it follows that subsets of $C - \{a\}$ are finite. Thus $B$ is finite. We have established that $n + 1 \in S$.

By the induction axiom, $S = \mathbb{N}$. This establishes the theorem. □

**Theorem 24.** *Let $C$ be a finite set of size $c$. If $A$ is a subset of $C$ of size $a$ then $a \leq c$. If $A$ is a proper subset then $a < c$.*

*Proof.* Consider the set $B$ defined as follows:

$$B \stackrel{\text{def}}{=} C - A = \{x \in C \mid x \notin A\}.$$

Then $B$ is a subset of $C$, so is finite by Theorem 23.

By basic set theory, $A$ and $B$ are disjoint and $A \cup B = C$. In particular, if $b$ is the size of $B$ then $c = a + b$ (Theorem 20). By a property of $\leq$ (Chapter 2) we get $a \leq c$.

Now if $A$ is a proper subset of $C$, there is an element $w \in C$ that is not in $A$. So $w \in B$. Thus $B$ is not empty, and the size $b$ of $B$ is not zero. Thus $a < c$ by definition of $<$ (Chapter 2). □

**Theorem 25.** *Let $f : A \to B$ be an injection where $B$ is finite of size $b$. Then $A$ is also finite and $a \leq b$ where $a$ is the size of $A$. If, in addition, $f$ is not surjective then $a < b$.*

*Proof.* Let $C = f[A]$ be the image of $f$. Since $B$ is finite, the same is true of $C$ (Theorem 23). Let $g : A \to C$ be the function obtained by restriction of codomain. In other words, $g(x)$ is defined to be $f(x)$ for all $x \in A$, and the functions $f$ and $g$ differ only in the choice of codomain. Observe that $g$ is a bijection.

Since $C$ is finite, $A$ is finite and $C$ and $A$ have the same size (Theorem 12). Let $a$ be the common size of $A$ and $C$. Since $C$ is a subset of $B$, $a \leq b$ (Theorem 24). The proof of the final statement is left to the reader. □

**Exercise 10.** Complete the above proof by proving the final statement: "If, in addition, $f$ is not surjective then $a < b$".

**Exercise 11.** Prove the following two corollaries of Theorem 25.

**Corollary 26** (Pigeonhole Principle)**.** *Let $A$ be a finite set of size $a$ and $B$ a finite set of size $b$. If $f : A \to B$ is a function, and if $a > b$, then there are distinct elements of $A$ mapping (via $f$) to the same element of $B$.*

**Corollary 27.** *Let $f : A \to B$ be an injection between two finite sets of the same size. Then $f$ is a bijection.*

*Remark* 4. Informally, the Pigeonhole principles says that if there are more pigeons than pigeonholes, then there is a pigeonhole with more than one pigeon. Think of $A$ as a set of pigeons, and $B$ as a set of pigeonholes.

**Theorem 28.** *Let $g : A \to B$ be a surjection. If $A$ is finite of size $a$ then $B$ is also finite, and the size $b$ of $B$ satisfies the inequality $a \geq b$. If, in addition, $g$ is not injective then $a > b$.*

*Proof.* Let $h\colon \langle a \rangle \to A$ be a counting function (Definition 2). Then $h$ is a bijection, so it is necessarily a surjection. Since $g$ is a surjection, the composition $g \circ h : \langle a \rangle \to B$ is also a surjection.

Now $g \circ h$ might not be injective: there could be distinct integers $x, y \in \langle a \rangle$ with $g(h(x)) = g(h(y))$. We seek a subset $C \subseteq \langle a \rangle$ on which $g \circ h$ is injective. To form $C$, we will want to throw out either $x$ or $y$ whenever the equality $g(h(x)) = g(h(y))$ occurs. Let's agree to always throw out the larger integer. So officially $C$ is defined to be the set of all $x \in \langle a \rangle$ with the property that

$$\forall\, z \in \langle a \rangle\,, \quad g(h(x)) = g(h(z)) \;\Rightarrow\; x \leq z.$$

Let $f$ be the restriction of $g \circ h$ to $C$. We claim that $f : C \to B$ is injective. To see this, suppose that $f(x) = f(y)$ where $x, y \in C$. Since $f$ is a restriction of $g \circ h$, we have $g(h(x)) = g(h(y))$. By the definition of $C$, this implies $x \leq y$ and $y \leq x$. So $x = y$. Thus $f$ is injective.

We claim that $f : C \to B$ is surjective. Let $b \in B$. Since $g \circ h$ is surjective, there is an integer $y$ with $g(h(y)) = b$. Let $x$ be the smallest such integer (existence by well-ordered property). Then $x \in C$, and $f(x) = b$. Thus $f$ is surjective.

So $f$ is a bijection. Since $C \subseteq \langle a \rangle$, and since $\langle a \rangle$ has size $a$, we have that $C$ is finite (Theorem 23) and $|C| \leq a$ (Theorem 24). Since $f$ is a bijection, $B$ is finite and $|B| = |C|$ (Theorem 12). So $|B| \leq a$ as desired.

To establish the second statement, observe that if $g$ is not injective, then $C$ is a proper subset of $\langle a \rangle$. So $|C| < a$ (Theorem 24), giving us $|B| < a$ as desired since $|B| = |C|$. □

**Corollary 29.** *Let $g : A \to B$ be a surjection between two finite sets of the same size. Then $g$ is a bijection.*

**Theorem 30.** *If $A$ is a finite set of size $n$, and if $m \leq n$, then there is a subset $B \subseteq A$ of size $m$.*

*Proof.* Let $f : \langle n \rangle \to A$ be a counting function. Let $B$ be the image of $\langle m \rangle$ under $f$. Observe that $f$ restricts to a bijection $\langle m \rangle \to B$, so $B$ has cardinality $m$. □

In Chapter 2 we showed that $\mathbb{N}$ is well-ordered. In other words, every nonempty subset $S \subseteq \mathbb{N}$ is has a minimum. This leads to a question: which subsets have a maximum?

**Theorem 31.** *Let $S$ be a nonempty subset of $\mathbb{N}$. Then $S$ has a maximum if and only if $S$ is finite.*

*Proof.* If $S$ has a maximum $n$, then $S$ is a subset of $T = \{0, \ldots, n\}$. Observe that $\{0, \ldots, n\} = \{0\} \cup \{1, \ldots, n\}$. So $T$ is finite since it is the union of two finite sets. Since $S$ is the subset of a finite set, it is finite.

Now we prove the converse: if $S \subseteq \mathbb{N}$ is finite and nonempty then it has a maximum. This is proved by induction on the size of $S$. Let $A$ be the set consisting of all $x \in \mathbb{N}$ with the following property: *all nonempty subsets of $\mathbb{N}$ of size $x$ have a maximum.*

Observe $0 \in A$ since there are no nonempty sets of size 0.

Suppose $n \in A$. We must show $n + 1 \in A$. In other words, if $S \subseteq \mathbb{N}$ has size $n + 1$ we must find a maximum $M$. Start with any $s \in S$. If $s$ is a maximum then we are done: $M = s$. Otherwise, $S$ contains an element larger than $s$, so $S - \{s\}$ is nonempty. In fact $S - \{s\}$ is a nonempty set of size $n$. Since $n \in A$, this implies that $S - \{s\}$ has a maximum $M$. Observer that $M$ is a maximum of $S$.

We conclude that if $n \in A$ then $n + 1 \in A$. So, $A = \mathbb{N}$ (induction) as desired. □

**Exercise 12.** Let $S \subseteq \mathbb{N}$ be a nonempty subset. Suppose that $S$ has an upper bound $B \in \mathbb{N}$. Show that $S$ is finite.

## 6. New perspective on multiplication

In Chapter 1 multiplication was defined in terms of iteration of addition. However, there are other ways to characterize multiplication. For example, one can count the number of ordered pairs: if there are $m$ choices for the first coordinate of an ordered pair, and if there are $n$ choices for the second coordinate of an ordered pair, then $m \cdot n$ gives the total number of ordered pairs. In other words, if $A$ is finite of size $m$ and $B$ is finite of size $n$ then the product $m \cdot n$ is the size of $A \times B$. We now prove that this alternative characterization of multiplication is valid.

**Theorem 32.** *Suppose that $A$ and $B$ are finite sets. Let $m$ be the size of $A$, and let $n$ be the size of $B$. Then $A \times B$ is finite with size $m \cdot n$.*

*Proof.* (Induction) Let

$$S = \{u \in \mathbb{N} \mid \text{the size of } A \times X \text{ is } m \cdot u \text{ for all } X \text{ of size } u\}.$$

First we show $0 \in S$. Let $X$ have size 0, so $X$ is empty. Observe that $A \times X$ is also empty since no ordered pair has second coordinate in the empty set. Thus $|A \times X| = 0 = m \cdot 0$. We conclude that $0 \in S$.

Suppose $k \in S$. We must show $k+1 \in S$. In other words, for any $X$ of size $k+1$ we must show $|A \times X| = m(k+1)$.

Since $|X| = k+1$, the set $X$ is not empty. Let $x \in X$. Then $X - \{x\}$ has size $k$ by Lemma 8. Since $k \in S$, we conclude that $A \times (X - \{x\})$ has size $m \cdot k$. Observe that

$$A \times X \;=\; A \times (X - \{x\}) \;\cup\; A \times \{x\}$$

and that the union is disjoint. Also, there is a bijection $A \to A \times \{x\}$, so $A$ and $A \times \{x\}$ have the same size. So, by Theorem 20, $A \times X$ has size $m \cdot k + m$. From Chapter 1, $m \cdot k + m = m \cdot \sigma k = m(k+1)$. So $k+1 \in S$.

By the induction axiom, $S = \mathbb{N}$. Since $n \in \mathbb{N}$ we have $n \in S$. By definition of $S$ we have that $|A \times B| = mn$. □

*Remark* 5. This result is related to a fundamental counting principle: if you have $m$ choices for one property, and $n$ choices for a second property, then there are $mn$ total combinations given by the two choices. For example, if your computer has five fonts and each font comes in plain, bold, and italic style, then there are 15 total combinations of font and style. To see the connection between this principle and the above theorem, think of the two choices as giving the coordinates of an ordered pair. So the number of combinations is the number of ordered pairs.

*Remark* 6. We can write the above theorem as

$$|A \times B| = |A| \cdot |B|.$$

This explains why the symbol $\times$ is popular for cartesian product. Old set theory books sometimes use $+$ for union due to the connection between union and addition, but this notation lost out to $\cup$. If the $+$ notation had survived, we would have, for disjoint unions,

$$|A + B| = |A| + |B|.$$

*Remark* 7. The above theorem gives a new characterization of multiplication. Observe that the above theorem and proof are the first place where we have used multiplication in this chapter. For instance, we have used facts about addition and inequalities from Chapters 1 and 2, but the facts we used were not those dependent on multiplication. So everything so far has been "multiplication free".

The above proof uses just two properties about multiplication from Chapter 1: (i) $0 = m \cdot 0$ and (ii) $m \cdot n + m = m \cdot \sigma n$. These two facts occur in Chapter 1 before the commutative, associative, and distributive laws of multiplication.

We will now give new proofs of the commutative, associative and distributive laws of multiplication, which are independent of the old proofs. They give more insight into why these laws are true than the induction proof of Chapter 1. The commutative law is based on the following easy exercise.

**Exercise 13.** Let $A$ and $B$ be sets. Describe a simple function between $A \times B$ and $B \times A$ involving switching coordinates that works no matter what $A$ and $B$ are. Prove that it is a bijection. This natural bijection is called a *canonical bijection*.

**Theorem 33** (Commutative Law)**.** *If $m, n \in \mathbb{N}$, then $m \cdot n = n \cdot m$.*

*Proof.* Let $A = \langle m \rangle$ and $B = \langle n \rangle$. By Theorem 32, $A \times B$ has size $mn$ and $B \times A$ has size $nm$. By the previous exercise, there is a bijection

$$A \times B \to B \times A.$$

Thus $m \cdot n = n \cdot m$ by Theorem 12. □

**Theorem 34** (Associative Law)**.** *If $x, y, z \in \mathbb{N}$, then $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.*

*Proof.* This is similar to the previous proof. Observe that there is a bijection

$$(A \times B) \times C \to A \times (B \times C)$$

defined by the rule $\big((a, b), c\big) \mapsto \big(a, (b, c)\big)$. □

**Theorem 35** (Distributive Law)**.** *If $x, y, z \in \mathbb{N}$, then $(x + y)z = xz + yz$.*

*Proof.* Let $A, B, C$ be finite sets of size $x, y, z$ respectively, and choose $A$ and $B$ to be disjoint (Lemma 19). Then

$$(A \cup B) \times C = (A \times C) \cup (B \times C).$$

The result follows from Theorem 20 and Theorem 32. □

**Exercise 14.** In the above proof we used the fact that

$$(A \cup B) \times C = (A \times C) \cup (B \times C)$$

and the fact that $A \times C$ and $B \times C$ are disjoint. Show these two facts, and show how the statement of the theorem follows from Theorem 20 and Theorem 32.

*Remark* 8. There is another characterization of multiplication that is commonly used. Suppose $A$ is a set of disjoint finite sets, where each member of $A$ is a set of size $n$. Suppose $A$ is finite of cardinality $m$. Then the union of all the sets in $A$ has $mn$ elements.

For example, if you have five apples, and each apple has three worms, then there are 15 worms total (here each member of $A$ is the set of worms on one particular apple). This principle is closely related to the multiplication principle for cartesian products proved above. In fact, there is a bijection between the union of the sets in $A$ and $A \times \langle n \rangle$.

## 7. New perspective on subtraction

Above we described set-theoretic characterizations of addition and multiplication. There is also a simple set-theoretic characterization of subtraction. For example, informally one might describe $5-2$ to be the number of apples you have when you start with a set of 5 apples, and remove a subset of 2 apples. The following theorem implements this idea.

**Theorem 36.** *Let $A$ be a finite set of size $n$, and let $B$ be a subset of size $m$. Then the set $A - B = \{a \in A \mid a \notin B\}$ has size $n - m$.*

*Proof.* (Sketch) Observe that $A = B \cup (A - B)$. □

**Exercise 15.** Prove the above theorem. Be sure to mention that the subsets on the right-hand side are disjoint. Also refer to Theorem 20 and theorems on subtraction in Chapter 2.

From Section 4 we know that addition gives the size of $A \cup B$ if $A$ and $B$ are finite disjoint sets. What if they are not disjoint? The answer is given by the inclusion-exclusion principle:

**Theorem 37** (Inclusion-exclusion principle)**.** *Let $A$ and $B$ be finite sets that are not necessarily disjoint. Then $A \cup B$ is finite, and*

$$|A \cup B| = \big(|A| + |B|\big) - |A \cap B|.$$

*In other words*

$$|A \cup B| + |A \cap B| = |A| + |B|.$$

**Exercise 16.** Prove the above theorem. Hint: show

$$A \cup B = A \cup \big(B - (A \cap B)\big).$$

Also use the following from Chapter 2: given $x, y, z \in \mathbb{N}$ with $z \leq y$,

$$(x + y) - z = x + (y - z).$$

*Remark* 9. The above idea can be extended to three or more sets.[1] For example, if $A, B, C$ are finite sets, then $A \cup B \cup C$ is finite and $|A \cup B \cup C|$ is given by

$$|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

## 8. New perspective on exponentiation

In Chapter 1 exponentiation was defined in terms of iteration of multiplication. However, there are other ways to characterize exponentiation. For instance, we will see that $n^m$ is the number of functions $A \to B$ where $A$ is finite of size $m$ and where $B$ is finite of size $n$. Because of this, the set of functions $A \to B$ is sometimes written $B^A$:

[1] I do not recommend proving this now. Life is much easier when we have the identity $x - y = x + (-y)$, which is not developed until Chapter 4.

**Definition 5.** Let $A$ and $B$ be sets. Then define $B^A$ to be the set of functions $A \to B$.

**Theorem 38.** *Suppose that $A$ and $B$ are finite sets. Let $m$ be the size of $A$, and let $n$ be the size of $B$. Then $B^A$ is finite with size $n^m$.*

*Proof.* (Induction). Let

$$S = \{u \in \mathbb{N} \mid \ B^X \text{ has size } n^u \text{ for every } X \text{ of size } u\}$$

First we show $0 \in S$. So let $X$ have size 0. In other words $X = \varnothing$. By Proposition 1 there is a unique function $\varnothing \to B$, so the size of $B^\varnothing$ is exactly 1. But $1 = n^0$, so $B^X$ has size $n^0$. Hence, $0 \in S$.

Suppose $k \in S$. We must show $k+1 \in S$. In other words, we must show that if $|X| = k+1$, then $\left|B^X\right| = n^{k+1}$. Since $X$ has size $k+1$, it is not empty. Let $x \in X$. Then $X - \{x\}$ has size $k$ by Lemma 8. Since $k \in S$ (inductive hypothesis), we conclude that $B^{X-\{x\}}$ has size $n^k$.

What is the relationship between functions from $X$ to $B$ and functions from $X - \{x\}$ to $B$? Observe that when you restrict a function $f : X \to B$ to $X - \{x\}$, you get a function $g : (X - \{x\}) \to B$. Note that $g$ defines $f$ at every element in $X$ except $x$. So to describe $f$ in terms of $g$ you also need to know $f(x)$. Consider the function

$$\Phi\colon B^X \to B^{X-\{x\}} \times B$$

that takes a function $f : X \to B$ to $\big(g, f(x)\big)$ where $g$ is the restriction of $f$ described above. The function $\Phi$ has an inverse: given a function $g\colon (X - \{x\}) \to B$ and a value $b \in B$ there is a unique function $f\colon X \to B$ that agrees with $g$ on the set $X - \{x\}$ and at the same time has value $f(x) = b$. Since $\Phi$ has an inverse, it is a bijection.

Since $\Phi\colon B^X \to B^{X-\{x\}} \times B$ is a bijection, we can find the size $B^X$ from the size of $B^{X-\{x\}} \times B$. But $B^{X-\{x\}} \times B$ has size $n^k \cdot n$ by Theorem 32 and the inductive hypothesis. By Theorem 12, $B^X$ must also have size $n^k \cdot n$. From Chapter 1 we know $n^k \cdot n = n^{k+1}$. We have established that $k+1 \in S$.

By the induction axiom, $S = \mathbb{N}$. Since $m \in \mathbb{N}$ it must be in $S$. By the definition of $S$, the set $B^A$ has size $n^m$. □

*Remark* 10. We can write the conclusion of the above theorem as

$$\left|B^A\right| = |B|^{|A|}.$$

*Remark* 11. Under this interpretation, $n^0 = 1$ reflects the fact from Proposition 1 that there is a unique functions $\varnothing \to B$ from the empty set to any given set $B$ of size $n$. This works even if $n = 0$ where $B$ is empty. So the equation $0^0 = 1$ makes sense. This justifies our decision to define $0^0$ to be 1 in Chapter 1.

*Remark* 12. The only exponentiation identities from Chapter 1 used in the above proof are that $n^0 = 1$ and $n^k n = n^{k+1}$. The following give new, independent, proofs of other identities from Chapter 1.

**Theorem 39.** *If $x, y, n \in \mathbb{N}$ then*

$$(xy)^n = x^n y^n.$$

*Proof.* (sketch). Let $A$ be a finite set of size $x$, let $B$ be a finite set of size $y$, and let $C$ be a finite set of size $n$. Choosing a function $f : C \to A \times B$ is the same as choosing two functions $(f_1, f_2)$ with $f_1 : C \to A$ and $f_2 : C \to B$. In other words, there is bijection

$$(A \times B)^C \to A^C \times B^C.$$

The result follows from Theorem 32 and Theorem 38. □

**Theorem 40.** *If $x, m, n \in \mathbb{N}$ then*

$$x^{m+n} = x^m x^n.$$

*Proof.* (sketch). Let $A$ be a finite set of size $x$, let $B$ be a finite set of size $m$, and let $C$ be a finite set of size $n$. Choose $B$ and $C$ to be disjoint. Choosing a function $f : B \cup C \to A$ is the same as choosing two functions $(f_1, f_2)$ with $f_1 : B \to A$ and $f_2 : C \to A$. In other words, there is bijection

$$A^{B \cup C} \to A^B \times A^C.$$

The result follows from Theorem 20, Theorem 32, and Theorem 38. □

**Theorem 41.** *If $n \in \mathbb{N}$ is not 0 then*

$$0^n = 0.$$

*Proof.* (sketch). Let $B$ be the empty set, and let $A$ be a set of size $n > 0$. There are no functions from $A$ into the empty set (Proposition 1). So $B^A$ is empty. The result follows from Theorem 38. □

**Theorem 42.** *If $n \in \mathbb{N}$ then*

$$1^n = 1.$$

*Proof.* (sketch). Let $B = \{1\}$, and let $A$ be a finite set of size $n$. Every function $f : A \to B$ is given by the formula $f(x) = 1$. Thus there is one function in $B^A$. The result follows from Theorem 38. □

**Theorem 43.** *If $x, n, m \in \mathbb{N}$ then*

$$\left(x^m\right)^n = x^{mn}.$$

*Proof.* (sketch). Let $A$ be a finite set of size $x$, let $B$ be a finite set of size $m$, and let $C$ be a finite set of size $n$. Claim: there is a bijection

$$\varphi : (A^B)^C \to A^{B \times C}.$$

To see this, suppose $f : C \to A^B$ is given. Then define $\varphi(f) : B \times C \to A$ by the rule $(b, c) \mapsto \big(f(c)\big)(b)$. This rule makes sense since $f(c)$ is itself a function $B \to A$. It is an exercise to show that $\varphi$ has an inverse. Thus $\varphi$ is a bijection.

The result follows from Theorem 32 and Theorem 38. □

## 9. Laws of iteration

We have two fundamentally different ways of viewing addition: (i) iterated successor (from Chapter 1), and (ii) the size of disjoint unions. In this section we give a third way of looking at addition: (iii) the order of iteration obtained by composing two iterations. We give a similar result for multiplication.

**Theorem 44.** *Let $f : S \to S$ be a function whose domain equals its codomain. If $m, n \in \mathbb{N}$ then*

$$f^m \circ f^n = f^{m+n}.$$

*Proof.* (Induction on $n$). Fix $m \in \mathbb{N}$. Let $A_m = \{x \in \mathbb{N} \mid f^{m+x} = f^m \circ f^x\}$. Observe that $0 \in A_m$ since $f^0$ is the identity (Chapter 1).

Now assume $n \in A_m$. We will show that $n + 1 \in A_m$.

$$\begin{aligned} f^m \circ f^{n+1} &= f^m \circ (f^n \circ f) && \text{(Lemma 45 below)} \\ &= (f^m \circ f^n) \circ f && \text{(Assoc. of } \circ) \\ &= f^{m+n} \circ f && (n \in A_m) \\ &= f^{m+n+1} && \text{(Lemma 45 below)} \end{aligned}$$

So $n + 1 \in A_m$.

By the induction axiom $A = \mathbb{N}$. The result follows. □

The above used the following lemma. Recall that $f^{n+1} = f \circ f^n$ by the iteration axiom of Chapter 1 (actually a theorem: see the optional sections).

**Lemma 45.** *Let $f : S \to S$ be a function whose domain equals its codomain. If $n \in \mathbb{N}$ then*

$$f^{n+1} = f^n \circ f.$$

*Proof.* Let $A = \{x \in \mathbb{N} \mid f^{x+1} = f^x \circ f\}$. Observe that $0 \in A$ since $f^0$ is the identity and $f^1 = f$ (see Chapter 1).

Now assume $n \in A$. We must show that $n + 1 \in A$.

$$\begin{aligned} f^{(n+1)+1} &= f \circ f^{n+1} && \text{(Iteration Axiom/Theorem)} \\ &= f \circ (f^n \circ f) && (n \in A) \\ &= (f \circ f^n) \circ f && \text{(Assoc. of } \circ) \\ &= f^{n+1} \circ f. && \text{(Iteration Axiom/Theorem)} \end{aligned}$$

So $n + 1 \in A$.

By the induction axiom $A = \mathbb{N}$. The result follows. □

**Theorem 46.** *Let $f : S \to S$ be a function whose domain equals its codomain. If $m, n \in \mathbb{N}$ then*

$$(f^m)^n = f^{mn}.$$

**Exercise 17.** Prove the above theorem.

Observe that we now have three fundamental ways to think of multiplication. (i) iterated addition, (ii) size of finite cartesian products, (iii) the index of iteration of an iteration of an iteration.

## 10. Infinite sets

Most of this chapter has been concerned with finite sets. In this chapter we consider briefly infinite sets.

**Definition 6.** A set is *infinite* if it is not finite.

**Theorem 47.** *Suppose that $B$ is infinite and that $A$ is a finite subset of $B$. Then $B - A$ is infinite.*

**Exercise 18.** Use Theorem 17 to prove the above theorem.

**Exercise 19.** Prove the following by induction:

**Theorem 48.** *If $A$ is infinite, then $A$ has subsets of every finite cardinality. In other words, given $n$ there is a subset of $A$ of cardinality $n$.*

There is a converse:

**Theorem 49.** *If $A$ has subsets of every finite cardinality, then $A$ is infinite.*

*Proof.* Suppose not. Then $|A| = a$ for some $a \in \mathbb{N}$. By assumption, $A$ has a subset of size $a + 1$. This contradicts Theorem 24. □

**Theorem 50.** *If there is an injection $\mathbb{N} \to A$ then $A$ is infinite.*

*Proof.* (sketch) Such an injection can be used to produce subsets of every finite cardinality. □

There is another axiom of mathematics, that we have not needed, called the *axiom of choice*. If we assume such an axiom, we can prove the following converse to the above theorem.

**Theorem 51.** *If $A$ is infinite, then there is an injection $\mathbb{N} \to A$.*

The basic idea of the proof is to use the axiom of choice to give a function $h$ that chooses an element $h(B)$ in $A - B$ for each finite subset $B$ of $A$. Next recursively define $B_0 = \varnothing$ and $B_{n+1} = B_n \cup \{h(B_n)\}$. Now consider the function $n \mapsto h(B_n)$ and show it is injective.

*Remark* 13. If there is a bijection between $\mathbb{N}$ and a set $A$ then we say that $A$ is a *countably infinite set*. For example, $\mathbb{N}$ itself is countable (use the identity map). This makes sense since given an infinite amount of time (and infinite patience) you *can* count every element of $\mathbb{N}$. For a general set $A$, if there is a bijection $f\colon \mathbb{N} \to A$, you could use the bijection to do a similar counting of $A$.

The above theorem shows that every infinite set has a countable subset: just take the image of the injection given by the theorem. We will see later that there are infinite sets that are so big that they are not countable. In fact, the real numbers will turn out to be uncountable. Surprisingly, the rational numbers turn out to be countable.