Math 127: Understanding Number Sets

Mary Radcliffe

In this set of notes, we develop the basic structures of numbers and number sets that we will use throughout the course. Indeed, to this point, we have been exploiting facts about numbers implicitly, without ever making explicit the axioms and structures underlying those facts. Here, we do make these things explicit. We will first start with a construction of the critical number sets we use to do mathematics: natural numbers, integers, rational numbers, and real numbers. Moreover, we will discuss the properties of these number sets, and their fundamental structure. We then turn to a particular focus on the natural numbers that will help us develop and understand the proof technique known as mathematical induction.

1 Making numbers

We would like here to build numbers using the least amount of starting information possible. To that end, we will start with only one thing: a distinguished object which we shall call '1.' Starting from '1,' we will construct the real numbers in their entirety.

1.1 Making natural numbers.

To build the natural numbers, we add one concept to the notion of '1:' adding. That is to say, we would like to define all natural numbers using '1' plus the single operation of adding.

We shall do that as follows. Given the element 1, define the natural numbers as all objects that can be written in the form

$$1 + 1 + \cdots + 1.$$

Use the symbol $\mathbb{N}$ to represent the set containing all the natural numbers. We can define, in general, the operation '+' on $\mathbb{N}$ by the following: if $n, m \in \mathbb{N}$, define $n + m$ to be the natural number obtained by writing n as $1 + 1 + \cdots + 1$ (for some number of 1s), and m as $1 + 1 + \cdots + 1$ (for some, possibly different, number of 1s), and concatenating these expressions with a + in between to build a new natural number. For example, if we wanted to add $1 + 1$ to $1 + 1 + 1$, we would write the sum as $1 + 1 + 1 + 1 + 1$.

We can also define multiplication in the natural numbers as follows: to multiply n by m, replace each 1 that appears in the representation of n as $1 + 1 + \cdots + 1$ with a copy of the representation of m as $1 + 1 + \cdots + 1$. For example, if we wanted to multiply $1 + 1$ by $1 + 1 + 1$, we would write the product as $(1 + 1 + 1) + (1 + 1 + 1)$. The parentheses here are for emphasis only, and not at all necessary for the presentation of the product. We represent a product by concatenation; that is, the product of n with m is represented as nm. We use a natural number as an exponent, written as n^m to indicate the product of n with itself m times.

Under these definitions, we can prove (though we won't here) that our addition and multiplication satisfy some useful properties:

1. Addition is commutative; that is, $n + m = m + n$ for all $n, m \in \mathbb{N}$.
2. Addition is associative; that is $n + (m + \ell) = (n + m) + \ell$ for all $n, m, \ell \in \mathbb{N}$.
3. Multiplication is commutative; that is, $nm = mn$ for all $n, m \in \mathbb{N}$.

4. Multiplication is associative; that is, $(nm)\ell = n(m\ell)$ for all $n, m, \ell \in \mathbb{N}$.
5. Distributivity holds; that is, $n(m + \ell) = nm + n\ell$ for all $n, m, \ell \in \mathbb{N}$.

These properties can be proven from first principles using nothing more than the definitions we have used above as natural numbers constructed by repeated addition of 1. However, these proofs are cumbersome and clunky, in part because of our representation so far.

We can clearly see that we probably need to come up with some other way of denoting these kinds of objects. There is a very good reason that we don't do all of mathematics with tally marks: it's inefficient and limiting. Of course, throughout history there have been various ways to represent natural numbers: Romans had a whole thing with letters, the Babylonians used a base-12 representation, and computers generally prefer a base-2 or base-16 representation. Our current dominant mathematical standard is based on the Arabian system of base-10 representations.

We shall, primarily, choose to represent numbers using standard base-10 presentations, but we include here a full description of a general base-b representation. In order to do so, we will consider one additional number, that is not typically included in $\mathbb{N}$: 0, which we shall represent for a moment as $\boxplus$, indicating a sum of 1s that has no 1s[1].

1.1.1 Base expansions

To construct a base-b representation for $\mathbb{N}$, we work as follows. First, select b symbols, which we shall call $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{b-1}$. We assign value to these symbols as follows:

$$
\begin{aligned}
\alpha_0 :&\quad \boxplus \\
\alpha_1 :&\quad 1 \\
\alpha_2 :&\quad 1+1 \\
\alpha_3 :&\quad 1+1+1 \\
&\ \vdots \\
\alpha_{b-1} :&\quad 1+1+\cdots+1 \quad \text{(here the number 1 appears } b-1 \text{ times)}
\end{aligned}
$$

Given $d_r, d_{r-1}, \ldots, d_1, d_0$, each taking values from $\{\alpha_0, \alpha_1, \ldots, \alpha_{b-1}\}$, the concatenation

$$d_r d_{r-1} \ldots d_1 d_0$$

represents the number in $\mathbb{N}$ calculated as

$$d_r b^r + d_{r-1} b^{r-1} + \cdots + d_1 b + d_0.$$

The standard choice of symbols here is to take $\alpha_0 = 0$, $\alpha_1 = 1$, etc. If we need more symbols than 10 (i.e., if we are working in hexadecimal), it is standard practice to take capital letters $A, B, C, \ldots$ for these symbols.

Now, this construction begs the question: how do we know we can represent all natural numbers in this way? That is, if we decide to exclusively use base-10 representations of numbers (which we are DEFINITELY gonna do) how can we be sure that every natural number has a representation in base 10, and moreover, how can we be sure that these representations are unique? That is, what if there are two different ways to represent the same number? That seems... bad, right?

Don't worry, these fears will be alleviated later on with the use of a theorem known as the Division Theorem. For now, we shall take it on faith that these representations of natural numbers are both defined

[1] Actually, there is a decent amount of arguing about whether or not we should include 0 in the natural numbers. Some mathematicians and textbooks do, and some do not. Our default here will be to exclude 0, but if you are reading from another resource or textbook, you should always clarify whether or not 0 counts as a natural number for that author.

for all $n \in \mathbb{N}$ and unique, and deal with some of the technical details in a later set of notes. From here on out, all natural numbers will be referred to in their base 10 representations, except when necessary to illustrate a concept.

1.2 Making integers.

Alright, very good, we now have a few things going for us. We can add, we can multiply, and we can exponentiate within the set of natural numbers. We even kinda made up 0! And then, inspiration strikes: if we can add 1s on to a number, why can't we take some 1s away?

Great, sounds awesome! So let's try to define subtraction. Given two numbers $n, m \in \mathbb{N}$, define $n - m$ to be the natural number obtained by eliminating one 1 from the representation of n for every 1 seen in the representation of m. So, for example, we would have that if $n = 1+1+1+1+1+1+1$ and $m = 1+1+1+1$, then $n - m = 1+1+1$, since we eliminate one 1 from n for each 1 in m.

But.... ruh roh. We can perform $n - m$, but how do we perform $m - n$? What does it mean to have an operation that can only sometimes be performed? Well.... not much. So we have two options: throw away the operation and call it a day, or make up some new numbers.

Let's choose Door Number 2 here, and come up with a way to represent a difference $n - m$ in the case that m has more 1s in its representation than n. We can do this as follows: define a new number -1 that has the property that for any $n \in \mathbb{N}$, $n + (-1)$ is obtained from n by removing one 1 from the representation for n. If there are no 1s in the representation for n, we instead add one copy of -1. In this way, we have a new kind of number, that is now represented as $(-1) + (-1) + \cdots + (-1)$.

This notation is a bit absurd, so we shall indicate the operation of adding -1 with a new symbol, just $-$ alone. We observe that by definition, $1 - 1 = 0$, and it is not difficult to derive that $2 - 1 - 1 = 0$, and $3 - 1 - 1 - 1 = 0$, etc. Hence, we shall name these new delightful numbers as follows: given $n \in \mathbb{N}$, write $-n$ to indicate the new number, constructed of -1s, that satisfies the property $n + (-n) = 0$. We shall call this new universe of numbers the integers, and we shall use the letter $\mathbb{Z}$ to denote the set of all integers. We note that since $1 + -1 = 0$, even though $0 \notin \mathbb{N}$, we do have that 0 appears in the integers. We define an integer to be positive it appears in the natural numbers, and to be negative if it does not appear in the natural numbers and is nonzero.

As with the naturals, we can define a multiplication on the integers using this construction. We define as follows:

- If n, m are positive integers, define nm as in the natural numbers.
- If n is positive and m is negative, define nm to be the negative of $n(-m)$ as defined in the natural numbers.
- If n is negative and m is positive, define nm to be the negative of $(-n)m$ as defined in the natural numbers.
- If either n or m is 0, define nm to be 0.

Using this definition, one can show, as with the naturals, the basic properties of operations on the integers. In particular, one can prove the same set of properties listed for naturals, but with integers in place of naturals under this definition.

1.3 Making rational numbers.

Now, as we did when we constructed the integers, we find ourselves faced with a question. Our operation of multiplication is defined in such a way that we take a given number of 1s, and then replicate them a certain number of times. We would like to be able to do this backwards; that is, we'd like to be able to take a certain number of 1s, and then instead of repeating an equal block of them, break them down into subgroups of equal size. So we shall define a new operation, called division, to perform this task. Specifically, given n and m positive integers, define n/m to be the number of 1s that appear in each part when the 1s in n are divided into m equal parts. So, for example, if we have $n = 1+1+1+1$ and $m = 1+1$, we write $n/m = 1+1$.

As in the case of subtraction, this works sometimes and does not work other times. In the example above, it's perfectly fine. However (and switching to base-10 notation), what if we wish to perform $5/2$? We have five 1s to place in two equal parts. We can easily place two 1s in each part, but have a 1 remaining and no clear way to deal with it. There are two options to think about this 1. The first is to just perform all division with remainders, so that we don't have to worry about it. This is the strategy we will take later on in the course, when we talk about elementary number theory. The second strategy is to just make up some new numbers, as we did in the previous section on constructing integers.

If we follow Door Number 1, there is a rich theory of numbers available to us that we will explore later. I primarily here just want to give a formal definition of divisibility, as we have used it as an example in previous notes and probably owe ourselves some full rigor.

Definition 1. For $a, b \in \mathbb{Z}$, we say that a *divides* b if b/a is an integer. Put another way, we say that a divides b if there exists an integer d such that $b = ad$. We write a divides b with the notation $a|b$.

Note that the second version of the definition of divisibility is the one we typically prefer in our proofs in previous lectures.

However, let's focus on Door Number 2 yet again. Since we cannot place our 1 in either category in $5/2$, we shall decide to split it up into two halves of a 1, and put half of it into each category. The rules for this number should be that if we doubled it back up again, it should give us 1. Hence we can in general define, for $n \neq 0$, the number $1/n$ to be a number such that $n(1/n) = 1$, where multiplication is as in the integers. Once we have that, we can define m/n in general so that $n(m/n) = m$ (this can also be obtained by noting that $m/n = m(1/n)$, so by the definition we have already given, multiplying by n and taking advantage of commutativity yields the same result).

Note that this definition of $1/n$ does not require n to be positive or negative, just that it is nonzero. We further note that we cannot define a similar number for 0, as it would require that $0(1/0) = 1$, and this is impossible as by definition in the previous part, multiplication by 0 necessarily yields 0. Moreover, we can extend our notion of division to general rational numbers as follows: if $p, q \in \mathbb{Q}$, we define p/q to be a number such that $q(p/q) = p$.

We shall call this set of numbers to be the rational numbers, and use the letter $\mathbb{Q}$ to denote the rationals. As with the previous few number sets, we note that we can prove the basic arithmetic structures on $\mathbb{Q}$ using this definition: commutativity, associativity, distributivity, etc. A few other useful things that we can prove:

1. For $n/m, p/q \in \mathbb{Q}$, we have that $(n/m)/(p/q) = nq/mp$
2. For all $q \in \mathbb{Q}$, $q/1 = q$.
3. If $q \in Q$ is nonzero, then there exists $p \in \mathbb{Q}$ such that $pq = 1$.

1.4 Making real numbers

Finally, we find ourselves in one last pickle. At first, we feel super good about the rational numbers; indeed, for some time a group of natural philosophers called the Pythagoreans deeply believed that this set was a full description of all the numbers. The Pythagoreans hung around doing math and philosophy starting from roughly the late 6th century BCE or early 5th century BCE. But then, a crisis occurred.

A man named Hippasus, a devoted Pythagorean himself, discovered something amazing, and something that we have already seen in previous lectures. He discovered that $\sqrt{2}$ was not a rational number, using effectively the same proof ideas we used before. He showed his discovery to his mathematician philosopher friends, and they were, well, unhappy. The story goes that as a result of this terrible blasphemy, he was drowned at sea as punishment by the Gods (another version of the story has him drowned by his fellow Pythagoreans, so apparently math cults are a bit weird). He was demonized by the Pythagoreans, and they accused him of using his writings just to ruin Pythagoras' reputation.

In any case, his discovery could not remain unheeded for long. By 400 BCE, Plato was writing freely about irrational numbers (mostly square roots), and the shame of Hippasus was largely forgotten. What did become clear, though, was that the numbers as the early Greek mathematicians knew them needed some updating.

So as not to be too Western centric, it's worth noting that Eastern mathematicians, primarily in India, had been happily using irrational numbers since around 800 BCE, and nobody had to die for it. Indian mathematicians as early as the 5th century BCE were beginning to calculate π already, just around the same time Hippasus was getting killed for his so-called blasphemy.

So then, how to define the irrational numbers? How do we fully describe all the numbers that can exist?

I will here give two answers. The first is simple: if we draw a number line, we have already seen how to construct the integers: just take a unit measurement, and then go out unit by unit in either direction. We can define the rationals by dividing unit lengths thereby constructed into equal parts. We will define the real numbers to be all the numbers on the line, regardless of whether they're involved in this equal parts game.

This seemingly works, but it is a bit mysterious nonetheless. What do we mean by "all the numbers on the line?" How can we even be sure there are numbers on the line other than the rationals?

So, here's a slightly more precise definition. We will say that a real number is any number that can be obtain as a limit of rationals. Let's formalize this a bit by giving a full definition of limit.

Definition 2. Let $x_1, x_2, x_3, \ldots$ be a sequence of numbers. We say that x is the limit of these numbers if for any $\epsilon > 0$, there exists some N so that $|x_n - x| < \epsilon$ for any $n \geq N$.

This, of course, is the same definition of limit you have seen in calculus. We are effectively saying that if you choose a tiny little itty bitty distance ϵ, eventually every number in your sequence is within ϵ of the goal point x.

Now, let's quickly justify that every real number can be obtained as a limit of rational numbers. You may recall from your mathematical history that every number with finitely many nonzero decimals is rational. (If you don't remember that, prove it!) So if you have a real number, say, $x = 23.16127858196723....$, you could write it as a limit of the following numbers:

$$
\begin{aligned}
x_1 &= 23 = 23/1 \\
x_2 &= 23.1 = 231/10 \\
x_3 &= 23.16 = 2316/100 \\
x_4 &= 23.161 = 23161/1000 \\
x_5 &= 23.1612 = 231612/10000 \\
&\vdots
\end{aligned}
$$

Hence, if we take the rational numbers, and include all the possible limits of those numbers, we'll get something bigger. This is the set we shall call the real numbers, and use the letter $\mathbb{R}$ to denote it. We say that any number in $\mathbb{R}$ that is not rational is *irrational*, a definition by exclusion. We define multiplication and division in $\mathbb{R}$ by extending them from $\mathbb{Q}$, so that if we wish to multiply or divide with irrational numbers, we can define this by taking the limit of the appropriate product or quotient of the approaching rational numbers.

As with all our previous number sets, the basic properties of addition, subtraction, multiplication, and division can be proven under this construct. The proofs are, well, messy, and we will omit them here.

There are definitely other ways to construct the real numbers, without having to use limits. One of the most common ways to construct these numbers is with an idea called Dedekind Cuts, which we shall come back to later when we have a stronger sense of how to manipulate sets.

One last thing to mention on the reals, that we had in previous number sets but neglected, was a notion of order. That is, given two numbers $a, b \in \mathbb{R}$, we can define $a < b$ if a is to the left of b on the number line. Given this definition, we extend in the usual way to define the symbols $\leq, \geq, >$.

2 Natural numbers, revisited

Before we move on from this world of building numbers, I'd like to spend a bit of time formalizing some of the concepts we discussed in the construction of the naturals. Indeed, since all of our further constructions were built upon the house the naturals reside in, it would behoove us to ensure that the natural numbers have a strong foundation. Hence, we shall turn to a formalization of the natural numbers via the Peano Axioms.

Peano Axioms

Define the natural numbers $\mathbb{N}$ to be a set of numbers that satisfy the following conditions:

1. 1 is a number.
2. If a is a number, there exists a number a^+, called the successor of a, which is also a number.
3. 1 is not the successor of any number.
4. If a and b are numbers, having $a^+ = b^+$, then $a = b$.
5. If a set S contains 1 and has the property that for any $a \in S$, the successor of a is also in S, then S contains every number.

We call the set of numbers constructed under these axioms the natural numbers, and denote them with the symbol $\mathbb{N}$.

The last axiom here is called the Induction Axiom, and it will form the basis of our understanding of mathematical induction in our next set of notes. This axiom ensures that every number other than 1 must be the successor of some previous number, since any set containing only 1 and all successors is the entirety of the natural numbers.

We note that in some cases, the Peano Axioms are given replacing 1 with 0 throughout. This would yield a construction of the natural numbers that includes 0. Here, we prefer a construction of the natural numbers that does not include 0, so we shall begin from 1.

Before we go further, let us first verify that these numbers are in fact different from each other. That is, we wish to ensure that we cannot, at some point, arrive at a number a with $a = a^+$, essentially preventing us from continuing to construct more numbers.

Proposition 1. For all $a \in \mathbb{N}$, we have $a \neq a^+$.

Proof. We shall use all 5 axioms to prove this theorem. Define S to be the set of natural numbers having the property that $a \neq a^+$. We shall use the 5th Axiom to show that S contains all numbers. In order to do so, we have to show two properties: first, that $1 \in S$, and second, that for any $a \in S$, the successor of a is also in S.

For the first, by Axioms 1 and 3, we have that 1 is a number, and 1 is not a successor, so $1 \neq 1^+$. Therefore, $1 \in S$.

For the second, suppose we have $a \in S$. We wish to demonstrate that the successor of a, a^+, is also in S. Assume for the sake of contradiction that $a^+ \notin S$. By definition of S, this implies that $a^+ = (a^+)^+$. Taking $b = a^+$ in Axiom 4, this therefore implies that $a = a^+$, and thus $a \notin S$. This is a contradiction, and hence we must have that $a^+ \in S$.

By Axiom 5, then, we have that as S is a set containing 1 and containing all its successors, that S must contain every number. Therefore, for every $a \in \mathbb{N}$, we have $a \neq a^+$. □

With a similar proof, we can show the following:

Proposition 2. If $a \in \mathbb{N}$ and $a \neq 1$, then a is a successor.

As we described in Section 1.1.1 above, we shall use standard base-10 representations of numbers. We note that the description of successors here is similar to our description of adding 1 in Section 1.1; so 1^+ is effectively the same as $1 + 1$, which we call 2, and 2^+ is the same as $1 + 1 + 1$, which we call 3, etc.

From the Peano axioms, we formally define addition recursively as follows:

$$\begin{aligned}&\text{For any } a, \text{ define } a + 1 = a^+\\&\text{For any } a, b, \text{ define } a + b^+ = (a + b)^+\end{aligned}$$

Since every number other than 1 is necessarily a successor, as detailed in the Induction Axiom, this is a complete definition of addition in the natural numbers.

Let us use the fifth Peano axiom to show that this definition of addition is commutative. We shall assume associativity in this argument; one could prove associativity in a substantively similar way as the proof of commutativity that follows.

Theorem 1. *Addition in $\mathbb{N}$, as defined above, is commutative; that is, for any $a, b \in \mathbb{N}$, we have*

$$a + b = b + a.$$

Proof. Let S be a set, and define S to contain all numbers x such that $x + 1 = 1 + x$.

First, note that $1 \in S$, since $1 + 1 = 1 + 1$.

Now, we wish to use the Induction Axiom above to show that S contains all successors. So let us suppose that $a \in S$. We wish to demonstrate that $a^+ \in S$. Consider:

$$\begin{aligned} 1 + a^+ &= (1 + a)^+ \quad \text{(by definition of addition)}\\ &= (a + 1)^+ \quad \text{(because } a \in S\text{)}\\ &= (a^+)^+ \quad \text{(by definition of the addition } a + 1\text{)}\\ &= a^+ + 1 \quad \text{(by definition of the addition } a^+ + 1\text{)}\end{aligned}$$

Since $1 + a^+ = a^+ + 1$, we thus have that $a^+ \in S$. Therefore, we have shown that S is a set containing 1, and having the property that for any $a \in S$, the successor of a is also in S. By the Induction Axiom, then, $S = \mathbb{N}$, so $1 + a = a + 1$ for every $a \in \mathbb{N}$.

Now, we wish to show that for any $a, b \in \mathbb{N}$, we have that $a + b = b + a$. So far we have shown this is so whenever $b = 1$. To extend this to arbitrary b, we shall define yet another set and apply the Induction Axiom again. Define the set T to contain all natural numbers b so that $a + b = b + a$ for every $a \in \mathbb{N}$. We note that the above argument shows that this is true when $b = 1$, so $1 \in T$. As with the previous argument, we need to show that T contains all its successors, so that if $b \in T$, we also have $b^+ \in T$. The argument is similar to the above. Suppose that $b \in T$. Then consider, for any $a \in \mathbb{N}$:

$$\begin{aligned}
a + b^+ &= (a+b)^+ \quad \text{(by definition of addition)} \\
&= (b+a)^+ \quad \text{(because } b \in T\text{)} \\
&= (b+a)+1 \quad \text{(by definition of addition)} \\
&= 1+(b+a) \quad \text{(because } 1 \in T\text{)} \\
&= (1+b)+a \quad \text{(by associativity)} \\
&= b^+ + a \quad \text{(by definition of addition)}
\end{aligned}$$

Because T is a set that contains 1 and contains all its successors, then, by the Induction Axiom, it therefore must equal all of $\mathbb{N}$. Hence, for all $b \in \mathbb{N}$, we have the property that $a+b = b+a$ for every $a \in \mathbb{N}$. □

In a similar, recursive way, we can formally define multiplication:

$$\begin{aligned}
&\text{For any } a, \text{ define } a \cdot 1 = a \\
&\text{For any } a, b, \text{ define } a \cdot b^+ = a + a \cdot b
\end{aligned}$$

Following the strategy of Theorem 1, we can use the Induction Axiom to prove that under these definitions, addition is associative, multiplication is associative and commutative, and together, the two operations satisfy the distributive properties.

Finally, we totally order $\mathbb{N}$ using the following rule: for $a, b \in \mathbb{N}$, we say that $a < b$ if there exists $c \in \mathbb{N}$ such that $a + c = b$. Again using the Induction Axiom, one can show that under this ordering, every two elements in $\mathbb{N}$ are comparable (that is, for any $a, b \in \mathbb{N}$, with $a \neq b$, we must have either $a < b$ or $b < a$, but not both.)

Theorem 2. *Let $a, b \in \mathbb{N}$, with $a \neq b$. Then either $a < b$ or $b < a$, but not both.*

Proof. Define a set S so that $a \in S$ if and only if, for every $b \neq a$, either $a < b$ or $b < a$.

Consider $a = 1$. Then if $b \neq 1$, we must have that b is a successor, so there exists some $c \in \mathbb{N}$ such that $b = c^+$. But then $b = 1 + c$, and hence by definition, $1 < b$. Therefore, for every $b \neq 1$, we have that $1 < b$.

Therefore, for every $b \neq 1$, we have that $1 < b$, so $1 \in S$.

Now, let us show the second point of Axiom 5, namely that if $a \in S$, then a^+ is also in S.

Suppose that $a \in S$. Let $b \neq a^+$. We consider three cases.

Case 1: $b = a$. Then $a^+ = b+1$, and hence $b < a^+$. **Case 2:** $b < a$. Then there exists c with $b+c = a$. Hence, $b + c^+ b + c + 1 = a + 1 = a^+$, so $b < a^+$. **Case 3:** $b > a$. Then there exists c with $a + c = b$. Since by hypothesis $b \neq a^+$, it must be that $c \neq 1$. Thus, c must be a successor, so there exists $d \in \mathbb{N}$ such that $c = d^+$. Thus, $b = a + c = a + d^+ = a + d + 1 = a + 1 + d = a^+ + d$, and therefore $b > a^+$.

In any case, we have that if $a \in S$, then for every $b \neq a^+$, either $a^+ < b$ or $b < a^+$, so $a^+ \in S$. By the Inductive Axiom, then, since $1 \in S$ and S contains its successors, $S = \mathbb{N}$.

Hence, for every $a \in \mathbb{N}$, for every $b \neq a$, one of $a < b$ and $b < a$ is true.

To show that they are not both true, suppose for the sake of contradiction that there exists $b, a \in \mathbb{N}$ having $a < b$ and $b < a$. Then there exist $c, d \in \mathbb{N}$ such that $a = b + c$ and $b = a + d$. But then $a = b + c = a + d + c$, which is impossible[2]. Therefore, we cannot have both $a < b$ and $b < a$. □

This axiomatic structure can be extended in the obvious ways to define $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ as we did in Section 1. The most important piece here is the Induction Axiom; indeed, in a secret way, the proofs of Theorems 1 and 1 is our first foray into mathematical induction. We shall spend the next set of notes delving further into mathematical induction, with some perhaps less abstract applications.

[2]You may wish to prove that for all $a \in \mathbb{N}$ and for all $b \in \mathbb{N}$, $a + b \neq a$.