1

Beginnings

1.1 A naive approach to the natural numbers

1.1.1 Preschool: foundations of the natural numbers

One of the first things we learn in mathematics is the counting chant: one, two, three, four, five .... We quickly learn how to count to higher and higher numbers, and finally, the day comes when we realize that we can continue on counting forever. At that point, believe it or not, we have all the necessary assumptions we need to discover all of mathematics. The counting numbers are often called *whole numbers*, but mathematicians call them *natural numbers*. We can express our childhood discovery in four adult principles:

- There is a unique first natural number.
- Every natural number has a unique immediate successor.
- Every natural number except the first has a unique immediate predecessor.
- Every natural number is an eventual successor of the first.

Algebra begins when we introduce symbols to express these principles. Now there is a unique first natural number; we will write it as 1. Every natural number has a unique immediate successor. There are many choices for denoting the successor of a natural number. In a more rigorous course on the foundations of mathematics, we might write the successor of a natural number n as $s(n)$. We will choose a notation that anticipates later definitions. The successor of a natural number n will be written as $n + 1$. Notice that this is not addition (yet); $n + 1$ means "the successor of n," no more and no less. Every natural number except the first has a unique immediate predecessor. Again, we choose a notation with an eye on what is coming later. If $n \neq 1$, the predecessor of a natural number n will be written as $n - 1$. This is not subtraction; it is simply the symbol for the predecessor. The relationship between successors and predecessors can be described using this notation. Notice that $1 - 1$ is not defined because the first number does not have a predecessor.

An Introduction to Proof through Real Analysis, First Edition. Daniel J. Madden and Jason A. Aubrey.

Remark. If n is a natural number, then $(n + 1) - 1 = n$.

Remark. If n is a natural number and $n \neq 1$, then $(n - 1) + 1 = n$.

These are our first algebraic results. Note that they are nothing more than symbolic representations of the meanings of the words "successor" and "predecessor." Thus, $(n + 1) - 1 = n$ is just a symbolic statement that means "the predecessor of the successor of a natural number n is just the number n." Thus, $(n - 1) + 1 = n$ means "the successor of the predecessor of a natural number n other than the first number 1 is just the number n." That is all algebra really is: the encoding of ideas expressed in words into symbolic representations of those ideas.

The fourth principle is the hardest to precisely express in symbols. However, in this first chapter, we are just setting some groundwork to make later logically rigorous mathematics easier. We are willing to forgo some rigor to lay this groundwork. To say this more clearly, we are not going to restrict ourselves to completely logical proofs and definitions until the end of this chapter.

The fourth principle states: Every natural number is an eventual successor of the first. That is, every natural number is the successor of the successor of the successor of … the successor of 1. The loose notation for this is: if n is a natural number, then n can be written as

$$n = (((\ldots((1 + 1) + 1) + \ldots + 1) + 1) + 1. \tag{1.1}$$

The use of the ellipsis in this bit of algebra kills any hope of making an unambiguous statement. It should be clear what this means: n is made up of a series of (+1)s, each of which signals the successor of a previous number. This is not the best way to begin a course in rigorous mathematics, and soon we will need to replace it with something else.

There is one more bit of notation we set for dealing with these basic principles. We say m is an eventual successor of n if

$$m = (((\ldots((n + 1) + 1) + \ldots + 1) + 1) + 1. \tag{1.2}$$

Again, the use of ellipsis kills any rigor this idea might have. When m is an eventual successor of n, we say "m is greater than n"; and we write $m > n$. Actually, we might prefer to move smaller to larger and write $n < m$ and say "n is less than m." This leads to some algebra, and a careful name for an important algebraic property:

Remark. Let k, m and n be natural numbers. If $n < m$ and $m < k$, then $n < k$.

We can refer to this remark by saying, "The order of the natural numbers is *transitive*."

This remark is true because $n < m$ means

$$m = (((\ldots((n+1)+1)+\ldots+1)+1)+1, \tag{1.3}$$

and $m < k$ means

$$k = (((\ldots((m+1)+1)+\ldots+1)+1)+1. \tag{1.4}$$

Equality means that m is exactly the same as the expression that follows the equal sign. So we can "substitute" that expression for the m in the later equation.

$$k = (((\ldots((\ldots(n+1)\ldots+1)+\ldots+1)+1)+1. \tag{1.5}$$

So, indeed, k is an eventual successor of n.

Finally, suppose that we have natural numbers n and m. Since we have not said otherwise, they could be the same. Thus, it might be that $n = m$. Both numbers are eventual successors of 1. If $n \neq m$, one of the two must be an eventual successor of 1 that appears before the first. Thus, either $n < m$ or $m < n$. This leads to our final observation about the order of the natural numbers and another mathematical term.

Remark. If n and m are natural numbers, then exactly one of the following must be true: $n < m$; $m < n$; or $n = m$.

We refer to this remark by saying, "The order on the natural numbers has *trichotomy*."

Thus, if $n < m$ is not true, then either $m < n$ or $n = m$. We have notation that allows us to abbreviate this further. We write $n \leq m$ to mean either $n < m$ or $n = m$. Similarly, we write $n \geq m$ to mean either $n > m$ or $n = m$. There is no notational shortcut for saying either $n > m$ or $n < m$ other than $n \neq m$.

1.1.2 Kindergarten: addition and subtraction

The first use we learn for numbers is for counting things. We learn names and symbols for all the eventual successors of 1.

$$\begin{aligned} 1+1 &= 2. \\ (1+1)+1 &= 3. \\ ((1+1)+1)+1 &= 4. \\ (((1+1)+1)+1)+1 &= 5. \\ \cdots\cdots &= \cdots \end{aligned} \tag{1.6}$$

In the early grades, we add the two numbers 2 and 5 by creating two sets (say, of marbles), one with 2 marbles and another set with 5 marbles. We combine the two sets into one and count to find a total of 7 marbles. We learn that the notation for this is $2 + 5 = 7$.

$$
\begin{aligned}
2 &= 1 + 1; \\
5 &= (((1 + 1) + 1) + 1) + 1; \\
2 + 5 &= (1 + 1) + ((((1 + 1) + 1) + 1) + 1) \\
&= (((((1 + 1) + 1) + 1) + 1) + 1) + 1) \\
&= 7.
\end{aligned} \tag{1.7}
$$

While a main goal in elementary school arithmetic is learning the algorithm for adding natural numbers, this would be pointless without a few years of counting and combining so that we know what the addition algorithm does for us. This algorithm is a theoretical method that allows us to avoid long counts. We eventually learn how to find that $27 + 35 = 62$ without knowing what objects we are trying to count. The concrete problem of counting combined sets becomes the abstract problem of adding numbers. We learn what addition is mostly by repeated counting. Later, we learn a shortcut that uses an arithmetic procedure. But addition has never been taught by someone defining it for us, until now.

As adults we need to invent (or define) an operation on natural numbers where two natural numbers n and m are combined to produce a new natural number. We denote this new number as $n + m$. We define this new number by writing n and m as eventual successors of 1:

$$
\begin{aligned}
n &= (((\dots((1 + 1) + 1) + \dots + 1) + 1) + 1; \\
m &= (((\dots((\mathbf{1} + \mathbf{1}) + \mathbf{1}) + \dots + \mathbf{1}) + \mathbf{1}.
\end{aligned} \tag{1.8}
$$

Then

$$
\begin{aligned}
n + m = {} & [(((\dots((1 + 1) + 1) + \dots + 1) + 1) + 1] \\
& + [(((\dots((\mathbf{1} + \mathbf{1}) + \mathbf{1}) + \dots + \mathbf{1}) + \mathbf{1}] \\
= {} & (((\dots((1 + 1) + 1) + \dots + 1) + 1) + 1) \\
& + \cdots + \mathbf{1}) + \mathbf{1}) + \mathbf{1}) + \dots \mathbf{1}) + \mathbf{1}.
\end{aligned} \tag{1.9}
$$

The imprecision of the ellipsis almost renders this definition useless, but the bold 1s help a bit. In a course on the rigorous foundations of mathematics, we would need to do much better than this. Luckily, years of combining sets of marbles allows us to realize what we are trying to say in this study with the aforementioned definition. This almost unintelligible definition does lead to one very important algebraic fact. It is clear that the definition of addition is just the rearrangement of the parenthesis around 1s and +s. Thus, we have an algebraic fact about the addition of counting numbers: parentheses do not matter.

Remark. If k, m, and n are natural numbers, then $(k + n) + m = k + (n + m)$.

We refer to this by saying, "Addition of natural numbers is *associative*."
A few other algebraic facts follow just as quickly.

Remark. If m and n are natural numbers, then $n < n + m$.

We refer to this by paraphrasing Euclid, "The whole is greater than the part."

Remark. If k, m, and n are natural numbers and $n < m$, then $n + k < m + k$.

We refer to this by saying, "Addition of natural numbers respects the order."
If we remember our lessons from counting blocks, we realize that it doesn't make a difference which set of blocks we start with when we combine the two sets – the total always comes out the same. We can turn this observation into another useful algebraic fact.

Remark. If m and n are natural numbers, then $m + n = n + m$.

We refer to this by saying, "Addition of natural numbers is *commutative*."
The first step after learning the arithmetic operation of addition is the introduction of a new operation, subtraction. At first we learned it as the solution to an addition puzzle, such as "What number added to 5 gives 7?" We all recall the problem: Fill in the box

$$5 + [\ ] = 7. \tag{1.10}$$

Only later, after we understood this type of question better, did we learn a procedure for subtracting. Soon we learned that there were two arithmetic operations: addition and subtraction. As mathematicians, we will not talk about subtraction as its own operation, but rather look at it in terms of addition. It is not that there is anything wrong with thinking of subtraction as its own operation, but just that it will help later algebraic ideas to try to keep the language focused on addition. Subtraction will still be a possibility, but we will not fully admit it, but rather refer to the following property of the natural numbers:

Remark. If n and m are natural numbers with $n < m$, then there exists a unique natural number k so that $m = n + k$.

We refer to this by saying, "There is a conditional subtraction on the natural numbers."
We say that this subtraction is conditional because we cannot subtract the natural number n from m unless $n < m$ (and get a natural number as a result). Of course, one of our first orders of business will be to create the integers as a larger collection of numbers that removes this condition on subtraction. As for notation, it is no surprise that we will eventually write k as $m - n$. Thus,

the sign "−" for subtraction is still there. For at least a while, we will not take advantage of this notation because we are trying to avoid treating subtraction as an operation. The reason for this should be clearer when we start to discuss the integers where things work better algebraically.

There are two other "subtraction" properties that we will use frequently.

Remark. If k, n, and m are natural numbers with $n + k = m + k$, then $n = m$.

Remark. If k, n, and m are natural numbers with $n + k < m + k$, then $n < m$.

Rather than talking about these in terms of subtraction, we will refer to these as "cancellation properties of addition."

1.1.3 Grade school: multiplication and division

Once we know that we can add any two natural numbers, we can use that to invent a new operation, multiplication. Two natural numbers n and m are combined to produce a new natural number. We denote this new number as $n \cdot m$ or nm. We define this new number by writing n as eventual successor of 1:

$$n = (((\dots((1 + 1) + 1) + \dots + 1) + 1) + 1. \tag{1.11}$$

Then

$$n \cdot m = (((\dots((m + m) + m) + \dots + m) + m) + m. \tag{1.12}$$

Again, because of the ellipsis, the only reason this might be considered a definition is because we already know what it means: to find $n \cdot m$ add m to itself n times. For example,

$$3 \times 7 = (7 + 7) + 7. \tag{1.13}$$

As we move on to a discussion of the properties of multiplication, we lose any pretense of rigor. We need to refer to geometric intuition to justify our observations. Luckily, we spent endless hours playing with various objects in the elementary grades, developing this intuition just to understand the multiplication properties. A geometric representation of $n \cdot m$ is the number of objects arranged in a rectangle n blocks wide and m blocks long. A geometric representation of $(n \cdot m) \cdot k$ is the number of objects arranged in k rectangles each n blocks wide and m blocks long and stacked into a 3-D box. If we turn an n by m rectangle on its side, it turns into a rectangle that is m objects wide and n objects long. So we have our first algebraic property of multiplication.

Remark. If m and n are natural numbers, then $m \cdot n = n \cdot m$.

We refer to this by saying, "Multiplication of natural numbers is *commutative*."

If we pile k of these rectangles one on top of each other, we get a box n blocks wide, m blocks long, and k blocks high. The number of blocks in the box is $k \cdot (n \cdot m)$. But if we stack m walls of rectangles that are m blocks long and k blocks high, we get the same box. The number of blocks in the box is $m \cdot (n \cdot k)$. But by commutativity of multiplication, we can say

Remark. If k, m and n are natural numbers, then $(k \cdot n) \cdot m = k \cdot (n \cdot m)$.

We refer to this by saying, "Multiplication of natural numbers is *associative*."

The next observation follows directly from the definition of multiplication.

Remark. If n is a natural number, then $n \cdot 1 = 1 \cdot n = n$.

We refer to this by saying, "1 is a multiplicative identity."

If $n < m$, then m is an eventual successor of n, and we can write

$$\begin{aligned} m &= (((\ldots((n+1)+1)+\ldots+1)+1)+1 \\ &= (\ldots(.(\mathbf{1}+\mathbf{1})+\ldots\mathbf{1})+\ldots+1)+1)+1. \end{aligned} \tag{1.14}$$

So

$$\begin{aligned} m \cdot k &= (\ldots(.(\mathbf{k}+\mathbf{k})+\ldots\mathbf{k})+\ldots+k)+k)+k \\ &= (\ldots(kn+k)\ldots+k)+k)+k. \end{aligned} \tag{1.15}$$

So we know $k \cdot n < k \cdot m$. Thus,

Remark. If k, m, and n are natural numbers and $n < m$, then $n \cdot k < m \cdot k$.

We refer to this by saying, "Multiplication of natural numbers respects the order."

Notice that we have defined three things for the natural numbers: an order $<$, and two operations: addition $+$ and multiplication $\cdot$. We know how addition interacts with the order. Addition respects the order. We know how multiplication interacts with the order; multiplication respects the order. Next, we see how multiplication interacts with addition. We leave a geometric justification of this as an exercise.

Remark. If k, m, and n are natural numbers, then $k \cdot (n + m) = k \cdot n + k \cdot m$.

We refer to this by saying, "Multiplication of natural numbers distributes over addition."

If we were reluctant to talk about subtraction of natural numbers simply because to subtract n from m we must know $n < m$, we are definitely going to wait before we discuss division of natural numbers. Division of natural numbers is a much more complicated procedure involving remainders as well as quotients. We will get to it, but not just now.

Still we would like some division-like algebraic results to make things easier. We have two painfully obvious observations:

Remark. If k, n, and m are natural numbers with $n \cdot k = m \cdot k$, then $n = m$.

Remark. If k, n, and m are natural numbers with $n \cdot k < m \cdot k$, then $n < m$.

We refer to either of these as "cancellation properties of multiplication." Be warned, however, these are very dangerous. We are basically going to find safer replacements for them as soon as we can.

These are "painfully" obvious because while they are quite obvious after years of practicing arithmetic, the justifications that they are correct are rather painful to follow. There are a few ingredients in this justification: trichotomy, the results of multiplication are unique, multiplication respects order, and logical reasoning. Let us give a justification a try.

We know that the results of multiplication are unique; however we multiply two numbers m and k, the result will always be the same. Thus, we can state this algebraically as: if $n = m$, then for all natural numbers k, we have $n \cdot k = m \cdot k$. We really want to be clear about what this says.

$$\text{If it is true that } n = m, \text{ then it absolutely must be true that } n \cdot k = m \cdot k.$$

(We are just being resolute about our earlier statement.) But then, if we ever see that $n \cdot k = m \cdot k$ is false, then there is no way that $n = m$ could be true. This is to say:

$$\text{If } n \cdot k \neq m \cdot k, \text{ then } n \neq m.$$

Let us remember this for now.

Because multiplication respects order, we know that if k, m, and n are natural numbers and $n < m$, then $n \cdot k < m \cdot k$. So assuming that k, m, and n are natural numbers, if it is true that $n < m$, then it absolutely must be the case that $n \cdot k < m \cdot k$. So as before, if we ever see that $n \cdot k < m \cdot k$ is false, then there is no way that $n < m$ could be true. So

$$\text{If } n \cdot k < m \cdot k \text{ is not true, then } n < m \text{ is not true either.}$$

But by trichotomy, saying that $n \cdot k < m \cdot k$ is false is the same as saying $n \cdot k \geq m \cdot k$. By basically the same argument, we can also say:

$$\text{If } m \cdot k < n \cdot k \text{ is not true, then } m < n \text{ is not true either.}$$

Now we can justify our first statement that, if $n \cdot k = m \cdot k$, then $n = m$. Suppose it is true that $n \cdot k = m \cdot k$. Then by trichotomy, both $(n \cdot k < m \cdot k)$ and $(m \cdot k < n \cdot k)$ are not true. (Trichotomy says *exactly* one must be true.) By our two observations, we know ($n < m$) is not true, and ($m < n$) is not true. But trichotomy leaves only one possibility. It must be that $n = m$. Thus, as we said in our second remark: if k, n, and m are natural numbers with $n \cdot k < m \cdot k$, then $n < m$.

Next, we justify our second statement that, if $n \cdot k < m \cdot k$, then $n < m$. Suppose $n \cdot k < m \cdot k$. Then by trichotomy, both ($n \cdot k = m \cdot k$) and ($m \cdot k < n \cdot k$) are not true. By the first observation, we know that ($n \cdot k \neq m \cdot k$) implies $n \neq m$. The last observation says that ($m \cdot k < n \cdot k$) is not true implies that ($m < n$) is not true. But again, trichotomy leaves only one possibility. It must be that $n < m$.

It was a bit painful to follow these justifications of those simple remarks, but we do now see that they are simply consequences of trichotomy and a unique result from multiplication. One of our goals is to create an algebraic and logical language that makes arguments such as this easier to understand.

There is only one last remark we need to make about the natural numbers.

Remark. Let n and m be natural numbers with $n \leq m \leq n + 1$, then either $n = m$ or $m = n + 1$.

We refer to this by saying, "The natural numbers are discrete."

Again, the justification for this depends on the statements in the earlier remarks. Suppose $n < m < n + 1$. Then by subtraction (whoops), we know that there is a natural number k so that $m = n + k$. But then $n + k = m$ and $m < n + 1$. So by transitivity, $n + k < n + 1$. But we have a cancellation rule for addition; so $k < 1$. But since every natural number is an eventual successor of 1 and trichotomy holds, this cannot happen.

The purpose of algebra is to help make all these justifications easier to manage.

1.1.4 Natural numbers: basic properties and theorems

We have just reviewed several years of elementary school arithmetic so that we can identify and name various basic algebraic properties of the natural numbers. They are as follows:

- There is a first natural number, which we call 1.
- There is an order on the natural numbers.
- The order is transitive.
- The order has trichotomy.
- For any two natural numbers n and m, there is a unique natural number $n + m$.
- This addition is associative.
- This addition is commutative.
- If m and n are natural numbers, then $n < n + m$.
- If k, m, and n are natural numbers and $n < m$, then $n + k < m + k$.

- If n and m are natural numbers with $n < m$, then there exists a unique natural number k so that $m = n + k$.
- If k, n, and m are natural numbers with $n + k = m + k$, then $n = m$.
- If k, n, and m are natural numbers with $n + k < m + k$, then $n < m$.
- For any two natural numbers n and m, there is a unique natural number $n \cdot m$.
- This multiplication is associative.
- This multiplication is commutative.
- The natural number 1 is a multiplicative identity.
- If k, m, and n are natural numbers and $n < m$, then $n \cdot k < m \cdot k$.
- If k, n, and m are natural numbers with $n \cdot k = m \cdot k$, then $n = m$.
- If k, n, and m are natural numbers with $n \cdot k < m \cdot k$, then $n < m$.
- If m and n are natural numbers and $n \leq m \leq n + 1$, then either $m = n$ or $m = n + 1$.
- Multiplication distributes over addition.

1.2 First steps in proof

There are, of course, many more true facts about the natural numbers, but they all should follow from these basic properties. We will state many further facts about these numbers as theorems. We will prove these theorems by using the aforementioned basic properties. If our justifications for these properties are accepted and are correct, then the theorems we prove by using them must be perfectly true. Granted our justifications of these properties are a bit dicey, but we are going to have to start being rigorous somewhere, and it will be easier starting by assuming a list of basic properties such as those aforementioned.

Let us now use these properties to *prove* something.

1.2.1 A direct proof

The first proof we will give is called a *direct proof*. Suppose that we wish to prove a statement of the form "If P, then Q." In a direct proof of this statement, we begin by assuming P. Then we *deduce* Q using P and any other assumptions we have available. Let us now prove the statement

If n is a natural number, then $(n + 1)^2 = n^2 + 2n + 1$

using a direct proof. This is of the form "If P, then Q" where P is the statement "n is a natural number" and Q is the statement "$(n + 1)^2 = n^2 + 2n + 1$." We will begin the proof by assuming that n is a natural number. Knowing that, we can use all of the basic properties of the natural numbers listed earlier. So we will use those assumptions to deduce that $(n + 1)^2 = n^2 + 2n + 1$.

Theorem 1.2.1. *If n is a natural number, then* $(n + 1)^2 = n^2 + 2n + 1$.

Proof. Assume that n is a natural number. Then $n + 1$ is a natural number because addition is always defined. Then

$$(n + 1)^2 = (n + 1)(n + 1), \tag{1.16}$$

because that is what the exponent means.

$$(n + 1)(n + 1) = (n + 1)n + (n + 1) \cdot 1, \tag{1.17}$$

by the distributive property.

$$(n + 1)n + (n + 1) \cdot 1 = (n + 1)n + (n + 1), \tag{1.18}$$

because 1 is a $\cdot$ identity.

$$(n + 1)n + (n + 1) = n(n + 1) + (n + 1), \tag{1.19}$$

because $\cdot$ is commutative.

$$n(n + 1) + (n + 1) = (n \cdot n + n \cdot 1) + (n + 1), \tag{1.20}$$

by the distributive property.

$$(n \cdot n + n \cdot 1) + (n + 1) = (n \cdot n + n) + (n + 1), \tag{1.21}$$

because 1 is a $\cdot$ identity.

$$(n \cdot n + n) + (n + 1) = (n^2 + n) + (n + 1), \tag{1.22}$$

because that is what the exponent means.

$$(n^2 + n) + (n + 1) = n^2 + (n + (n + 1)), \tag{1.23}$$

because $+$ is associative.

$$n^2 + (n + (n + 1)) = n^2 + ((n + n) + 1), \tag{1.24}$$

because $+$ is associative.

$$n^2 + ((n + n) + 1) = n^2 + ((n \cdot 1 + n \cdot 1) + 1), \tag{1.25}$$

because 1 is a $\cdot$ identity.

$$n^2 + ((n \cdot 1 + n \cdot 1) + 1) = n^2 + (n(1 + 1) + 1), \tag{1.26}$$

by the distributive property.

$$n^2 + (n(1 + 1) + 1) = n^2 + (n \cdot 2 + 1), \tag{1.27}$$

because that is what 2 means.

$$n^2 + (n \cdot 2 + 1) = n^2 + (2n + 1), \tag{1.28}$$

because $\cdot$ is commutative.

$$n^2 + (2n + 1) = n^2 + 2n + 1, \tag{1.29}$$

because $+$ is associative, this is unambiguous.

Thus, we have

$$(n+1)^2 = n^2 + 2n + 1. \tag{1.30}$$

□

This is a completely algebraic proof; it is also a completely boring proof to anyone who knows algebra. This is the stuff of middle school algebra and is not the kind of proof that should give us any problems. While we should be able to justify any step in any algebraic part of any proof we give, there is rarely a reason to do so. In addition, we can take advantage of algebra's disregard for the rules of proper language composition. Notice that each step in the aforementioned proof is a full English sentence with a subject, a verb (always "equals"), and an object followed by a prepositional phrase. This is how a paragraph should be in any English composition.

But in an algebraic proof, we can violate one the major rules of good writing: no run-on sentences. The aforementioned proof is completely over the top for mathematical adults. In any work past a high school text, it would be written more like:

$$\begin{aligned}(n+1)^2 &= (n+1)(n+1) \\ &= (n+1)n + (n+1) \\ &= n^2 + n + n + 1 \\ &= n^2 + 2n + 1.\end{aligned} \tag{1.31}$$

Even this might be longer that necessary. Notice that this is a run-on English sentence. It has one subject, $(n+1)^2$, several objects, and one word "equals" used as a verb four times. This is unacceptable in an English composition, but perfectly acceptable in an algebraic proof. We need to remember that this proof is an abbreviation of the full proof written earlier as a composition. Each equal sign has two subjects: the object of the previous line, and by deduction, the original subject of the sentence. The conclusion drawn from the four intermediate sentences is that the original subject is equal to the final object.

In this study, we will not bother to do much more than outline an algebraic proof such as this. This does not, however, reduce at all our need for detailed algebraic proofs. As humans we will make algebra mistakes, and we need to be ready to find them before someone else does. Finding an algebraic mistake is often nothing more than giving a complete and thorough line-by-line step through the use of our basic properties until the error reveals itself.

1.2.2 Mathematical induction

Unfortunately, not all theorems about the natural numbers are easily proved by a direct proof or simple algebra. Consider

For all natural numbers n, $2 \cdot (1 + 2 + 3 + \ldots (n-1) + n) = n(n+1)$.

The dreaded rigor killer, ellipsis, appears again. Mathematics has notation that allows us to write such a summation in a more precise mathematical way. However, in this case, it is pretty clear what this claim is: if we add all the numbers starting at 1 and stop when we get to n and then double the result, the answer would be the same as if we multiplied n by its successor. Unfortunately, the only direct proof of this involves using geometric intuition. This is a perfectly fine proof, but there is an alternate proof that uses a much more general method with many more applications.

We will prove this claim using a "proof by mathematical induction." Such a proof is a two-step process. Both steps must be completed successfully for the proof to be valid. The first step is to prove that the result is true for the first natural number. The second step takes advantage of a logical loophole. To prove a statement of the form "If something, then something else," one may assume that something is true. Once something is assumed true for a valid logical reason, we can use that assumption to draw additional conclusions. The second step in induction is to prove the following: "If the statement is true for a particular natural number, then it will be true for its successor."

If we can accomplish both these steps, we will know

- that the statement is true for 1;
- that anytime the statement is true for a particular number, it will be true for its successor.

So we know that the statement is true for 1, and 1 is certainly a particular number. Since the statement is true for 1, it is true for the successor of 1. But 2 is a particular number, and the statement is true for it; so because we have proved the second step of induction, the statement is true for the successor of 2. Because every natural number is an eventual successor of 1, we will eventually know that the statement is true for any number.

Here is the claim written as a theorem, and this is followed by its (mostly rigorous) proof. Notice that, as we write out exactly what we are proving, our statement about n reappears three times. It may look like we are proving or assuming the same thing over and over. But a more careful look reveals that in each statement, the meaning of the variable n changes. Thus, the statements are actually about different numbers.

Theorem 1.2.2. *For all natural numbers n,* $2 \cdot (1 + 2 + 3 + \ldots (n-1) + n) = n(n+1)$.

Proof. The proof is by induction on n. Thus, we will actually prove two other mini theorems:

1. If $n = 1$, then $2 \cdot (1 + 2 + 3 + \ldots (n-1) + n) = n(n+1)$.

2. If for a particular $n = n_0$,

$$2 \cdot (1 + 2 + 3 + \dots (n-1) + n) = (n+1)n, \tag{1.32}$$

then for $n = n_0 + 1$,

$$2 \cdot (1 + 2 + 3 + \dots (n-1) + n) = n(n+1). \tag{1.33}$$

Proof of Step 1. Assume that $n = 1$. To prove that two expressions are the same, consider them one at a time. First, $(1 + 2 + 3 + \dots (n-1) + n)$ means start at 1 and stop when you get to n. But we are working under the assumption that $n = 1$. So

$$(1 + 2 + 3 + \dots (n-1) + n) = 1. \tag{1.34}$$

So

$$2 \cdot (1 + 2 + 3 + \dots (n-1) + n) = 2 \cdot 1 = 2. \tag{1.35}$$

Now consider the other expression, $n(n+1)$. We are still assuming $n = 1$.

$$(n+1)n = (1+1) \cdot 1 = 2. \tag{1.36}$$

Since $2 = 2$, we have shown that if $n = 1$, then $2 \cdot (1 + \dots (n-1) + n) = n(n+1)$. ■

Proof of Step 2. Assume for a particular $n = n_0$, $2 \cdot (1 + \dots (n-1) + n) = n(n+1)$. Thus, we can say

$$2 \cdot (1 + \dots (n_0 - 1) + n_0) = n_0.(n_0 + 1). \tag{1.37}$$

Under this assumption, we want to prove, for $n = n_0 + 1$, that we also have $2 \cdot (1 + 2 + 3 + \dots (n-1) + n) = n(n+1)$. That is to say, we want to show

$$2 \cdot (1 + 2 + \dots ((n_0 + 1) - 1) + (n_0 + 1)) = (n_0 + 1)((n_0 + 1) + 1). \tag{1.38}$$

To prove that two expressions are equal, we consider each side. Consider $2 \cdot (1 + \dots ((n_0 + 1) - 1) + (n_0 + 1))$. We have

$$\begin{aligned} &2 \cdot (1 + \dots ((n_0 + 1) - 1) + (n_0 + 1)) \\ &= 2 \cdot [(1 + 2 + 3 + \dots n_0) + (n_0 + 1)] \\ &= 2 \cdot [1 + 2 + 3 + \dots n_0] + 2[n_0 + 1] \\ &= n_0(n_0 + 1) + 2(n_0 + 1) \end{aligned} \tag{1.39}$$

because that is the assumption we are working under in this step. Then

$$\begin{aligned} &2 \cdot (1 + \dots ((n_0 + 1) - 1) + (n_0 + 1)) \\ &= n_0(n_0 + 1) + 2(n_0 + 1) \\ &= (n_0 + 2)(n_0 + 1). \end{aligned} \tag{1.40}$$

Next, consider the other side, $(n_0 + 1)((n_0 + 1) + 1)$.

$$(n_0 + 1)((n_0 + 1) + 1) = (n_0 + 1)(n_0 + 2). \tag{1.41}$$

The two expressions are equal. So we have proved: if for a particular $n = n_0$, we have $2 \cdot (1 + 2 + 3 + \ldots (n - 1) + n) = (n + 1)n$, then for $n = n_0 + 1$, we have $2 \cdot (1 + 2 + 3 + \ldots (n - 1) + n) = n(n + 1)$. ■

These two steps complete the proof by induction. So we have proved: for all natural numbers n, $2 \cdot (1 + 2 + 3 + \ldots (n - 1) + n) = n(n + 1)$. □

There are a few final comments on this write-up. Much of the exposition is a matter of taste, but no matter what, the proof must be an English essay. It may contain some headings, but everything in the content should be a full sentence. This includes the algebraic calculations. The logic is easier if all statements to be proved are written in the "If P, then Q" form. The proof of one of these statements should begin with "Assume P." After that assumption, the goal becomes to prove Q. The use of n_0 to stand for a particular value of n in the induction step is completely optional. With more experience in writing induction proofs, it becomes a distraction. However, even with experience, the second step of an induction step can get rather confusing when the statement being proved is long. Using the n_0 can be a valuable tool in fighting through that kind of confusion. For beginners, it is not a bad idea to take the time to use that extra notation so that it will always be available when needed.

1.3 Problems

1.1 (a) Use $n = 2$, $m = 3$, and $k = 4$ to provide an example of the distributive property $n(m + k) = nm + nk$ using either ellipsis arguments or a geometric construction.

(b) Provide a justification of the general distributive property $n(m + k) = nm + nk$ using either ellipsis arguments or a geometric construction.

1.2 Provide justifications for the cancellation properties of addition. (Hint: look at the justifications for multiplication.)

1.3 Prove that for all natural numbers n, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

1.4 Be careful while reading these formulas.

(a) Prove that for all natural numbers n, $\sum_{k=1}^{n} (2k - 1) = n^2$.

(b) Prove that for all natural numbers n, $\sum_{k=1}^{n} 2k - 1 = n^2 + n - 1$.

1.5 Prove that for all natural numbers n, $n^2 \geq n$.

1.6 Prove that for all natural numbers $n \geq 2$, $n^2 \geq n + 2$. (Hint: when trying to prove an inequality $a \leq b$, it can help to write the objective as $a \leq\, ? \leq b$. Then the idea is to find a value we can use in place of the question mark. If we can prove the two inequalities $a \leq\, ?$ and $? \leq b$, the result we want follows from transitivity. If we are lucky, one of these two inequalities is already known to be true.)

1.7 Prove that for all natural numbers n, $\prod_{k=1}^{n} \left(1 + \frac{1}{k}\right) = n + 1$. (Hint: the symbol $\prod$ is similar to the symbol $\sum$ except it means multiply instead of add.)

1.8 Let n be any natural number greater than or equal to 7.

(a) Prove that if there is a natural number q so that $n = 7 \cdot q$, then $n + 1 = 7 \cdot q + 1$.
(b) Prove that if there are natural numbers q and r so that $n = 7 \cdot q + r$ and $r < 6$, then there is a natural number r' so that $n + 1 = 7 \cdot k + r'$ with $r' < 7$.
(c) Prove that if there are natural numbers q and r so that $n = 7 \cdot q + r$ and $r = 6$, then there is a natural number q' so that $n + 1 = 7 \cdot q'$.
(d) Prove the following statement using induction.

> For all natural numbers $n \geq 7$, either there exists a natural number q so that $n = 7q$ or there exists a pair of natural numbers q and r so that $n = 7q + r$ with $r < 7$.