Chapter 2

Starting at the Beginning: The Natural Numbers

6/15:

- This text will begin by reviewing high school level material, but as rigorously as possible.
  - It will teach the skill of proving complicated properties from simpler ones, allowing you to understand why an "obvious" statement really is obvious.
  - One particularly important skill is the use of **mathematical induction**.
  - We will strive to eliminate **circularity**.

  Circularity: "Using an advanced fact to prove a more elementary fact, and then later using the elementary fact to prove the advanced fact" (Tao, 2016, p. 14).
- The number systems used in real analysis, listed in order of increasing sophistication, are the **naturals** $\mathbb{N}$[1], the **integers** $\mathbb{Z}$, the **rationals** $\mathbb{Q}$, and the **reals** $\mathbb{R}$.
  - **Complex numbers** $\mathbb{C}$ will only be used much later.
- This chapter will answer the question, "How does one actually *define* the natural numbers?"

2.1 The Peano Axioms

- **Peano Axioms**: First laid out by Guiseppe Peano, these are a standard way to define the natural numbers. They consist of Axioms 2.1-2.5, which follow.
  - From these five axioms and some from set theory, we can build all other number systems, create functions, and do algebra and calculus.
- How do you define operations on the naturals?
  - Complicated operations are defined in terms of simpler ones: Exponentiation is repeated multiplication, multiplication is repeated addition, and addition is repeated **incrementing**.
- **Incrementing**: The most fundamental operation — best thought of as counting forward by one number.
  - Incrementing is one of the fundamental concepts that allows us to define the natural numbers.
  - Let[2] $n{+}{+}$ denote the increment, or **successor**, of n.

[1] Note that in this text, the natural numbers will include 0. The natural numbers without 0 will be called the **positive integers** $\mathbb{Z}^+$.

[2] This notation is pulled from some computer languages such as *C*.

- For example, $3{+}{+} = 4$ and $(3{+}{+}){+}{+} = 5$.

- Let $x := y$ denote the statement, "x is defined to equal y."
- At this point, we can begin defining the natural numbers.

  Axiom 2.1. *0 is a natural number.*

  Axiom 2.2. *If n is a natural number, then $n{+}{+}$ is also a natural number.*

- To avoid having to use incrementation notation for every number, we adopt a convention.

  Definition 2.1. We define 1 to be the number $0{+}{+}$, 2 to be the number $(0{+}{+}){+}{+}$, 3 to be the number $((0{+}{+}){+}{+}){+}{+}$, etc.

- From these axioms, we can already prove things.

  Proposition 2.1. *3 is a natural number.*

  Proof. By Axiom 2.1, 0 is a natural number. By Axiom 2.2, $0{+}{+} = 1$ is a natural number. By Axiom 2.2 again, $1{+}{+} = 2$ is a natural number. By Axiom 2.2 again, $2{+}{+} = 3$ is a natural number. □

- It seems like Axioms 2.1 and 2.2 have us pretty well covered. However, what if the number system wraps around (e.g., if $3{+}{+} = 0$)? We can fix this with the following.

  Axiom 2.3. *0 is not the successor of any natural number; i.e., we have $n{+}{+} \neq 0$ for every natural number n.*

- We can now prove that $4 \neq 0$ (because $4 = 3{+}{+}$, $3 \in \mathbb{N}$, and $n{+}{+} \neq 0$).
- However, there are still issues — what if the number system hits a ceiling at 4, e.g., $4{+}{+} = 4$?
- A good way to prevent this kind of behavior is via the following.

  Axiom 2.4. *Different natural numbers must have different successors, i.e., if $n, m \in \mathbb{N}$ and $n \neq m$, then $n{+}{+} \neq m{+}{+}$. Equivalently*[3]*, if $n{+}{+} = m{+}{+}$, then $n = m$.*

- We can now prove propositions like the following, extending our anti-wrap around proving ability.

  Proposition 2.2. *6 is not equal to 2.*

  Proof. Suppose $6 = 2$. Then $5{+}{+} = 1{+}{+}$, so by Axiom 2.4, $5 = 1$. Then $4{+}{+} = 0{+}{+}$, so by Axiom 2.4, $4 = 0$, which contradicts our proof that $4 \neq 0$. □

6/16:

- Before going any further, we're going to need an **axiom schema**.
- **Axiom schema**: An axiom that functions as "a template for producing an (infinite) number of axioms, rather than a single axiom in its own right" (Tao, 2016, p. 20).

  Axiom 2.5 (Principle of mathematical induction)**.** *Let $P(n)$ be any property pertaining to a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(n{+}{+})$ is also true. Then $P(n)$ is true for every natural number n.*

- Axiom 2.5 allows us to exclude numbers such as $0.5, 1.5, 2.5, \ldots$ from our number system because $P(n)$ is only true for $n \in 0, 1, 2, \ldots$

[3] This is an example of reformulating an implication using its **contrapositive** (see Section A.2). In the converse direction, it is the **axiom of substitution** (see Section A.7).

- Proposition 2.1.11 in Tao, 2016 is an excellent template for an induction proof.
- Note that there is only one natural number system — we could call $\{0, 1, 2, \dots\}$ and $\{O, I, II, III, \dots\}$ different number systems, but they are **isomorphic**, since a one-to-one correspondence exists between their elements and they obey the same rules.
- An interesting property of the naturals is that while every element is finite (0 is finite; if n is finite, then $n{+}{+}$ is finite), the set is infinite.
- In math, we define the natural numbers **axiomatically** as opposed to **constructively** — "we have not told you what the natural numbers are... we have only listed some things you can do with them... and some of the properties that they have" (Tao, 2016, p. 22).
  - This is the essence of treating objects **abstractly**, caring only about the properties of objects, not what they are or what they mean.
  - "The great discovery of the late nineteenth century was that numbers can be understood abstractly via axioms, without necessarily needing a concrete model; of course a mathematician can use any of these models [e.g., counting beads] when it is convenient, to aid his or her intuition and understanding, but they can also be just as easily discarded when they begin to get in the way [of understanding -3, $1/3$, $\sqrt{2}$, $3 + 4i$, ...]" (Tao, 2016, p. 23).
- With the axioms (and the concept of a function, which does not rely on said axioms), we can introduce recursive definitions, which will be useful in defining addition and multiplication.

  Proposition 2.3 (Recursive definitions)**.** *Suppose for each natural number n, we have some function $f_n : \mathbb{N} \to \mathbb{N}$ from the natural numbers to the natural numbers. Let c be a natural number. Then we can assign a unique natural number a_n to each natural number n, such that $a_0 = c$ and $a_{n++} = f_n(a_n)$ for each natural number n.*

  Proof. (Informal[4]) We use induction. First, a single value c is given to a_0 (no other value $a_{n++} := f_n(a_n)$ will be assigned to 0 by Axiom 2.3). Given that a_n has a unique value, a_{n++} will have a unique value $f_n(a_n)$, distinct from any other a_{m++} by Axiom 2.4. □

2.2 Addition

- We can define addition recursively.

  Definition 2.2 (Addition of natural numbers)**.** Let m be a natural number. To add zero to m, we define $0 + m := m$. Now suppose inductively that we have defined how to add n to m. Then we can add $n{+}{+}$ to m by defining $(n{+}{+}) + m := (n + m){+}{+}$.
  - If we want to find $2 + 5$, we can find $0 + 5 = 5$, $1 + 5 = (0{+}{+}) + 5 = (0 + 5){+}{+} = 5{+}{+} = 6$, $2 + 5 = (1{+}{+}) + 5 = (1 + 5){+}{+} = 6{+}{+} = 7$.
- Let's now prove commutativity.

  Lemma 2.1. *For any natural number n, $n + 0 = n$.*

  Proof. Use induction. Since $0 + m = m$ for all $m \in \mathbb{N}$ and $0 \in \mathbb{N}$, $0 + 0 = 0$, proving the base case. If $n + 0 = n$, then $(n{+}{+}) + 0 = (n + 0){+}{+} = n{+}{+}$. This closes the induction. □

  Lemma 2.2. *For any $n, m \in \mathbb{N}$, $n + (m{+}{+}) = (n + m){+}{+}$.*

[4] "Strictly speaking, this proposition requires one to define the notion of a **function**, which we shall do in the next chapter. However, this will not be circular, as the concept of a function does not require the Peano axioms. Proposition [2.3] can be formalized more rigorously in the language of set theory; see Exercise 3.5.12" (Tao, 2016, p. 23).

Proof. We keep m fixed and induct on n. Base case: if $n = 0$, then $0 + (m{+}{+}) = (m){+}{+} = (0 + m){+}{+}$. Induction step: if $n + (m{+}{+}) = (n + m){+}{+}$, then

$$\begin{aligned} (n{+}{+}) + (m{+}{+}) &= (n + (m{+}{+})){+}{+} && \text{Definition 2.2} \\ &= ((n + m){+}{+}){+}{+} && \text{Induction hypothesis} \\ &= ((n{+}{+}) + m){+}{+} && \text{Definition 2.2} \end{aligned}$$

This closes the induction. □

Proposition 2.4 (Addition is commutative)**.** *For any natural numbers n and m, $n + m = m + n$.*

Proof. For all $m \in \mathbb{N}$, Definition 2.2 gives us $0+m = m$ and Lemma 2.1 gives us $m+0 = m$. Since both of the previous statements equal m, $0+m = m+0$. Suppose inductively that $n \in \mathbb{N}$ and $n+m = m+n$. If this is true, then

$$\begin{aligned} (n{+}{+}) + m &= (n + m){+}{+} && \text{Definition 2.2} \\ &= (m + n){+}{+} && \text{Induction hypothesis} \\ &= m + (n{+}{+}) && \text{Lemma 2.2} \end{aligned}$$

This closes the induction. □

- And associativity (see Exercise 2.2.1).
- The next proposition deals with cancelling. Although we cannot use subtraction or negative numbers to prove it, it will be instrumental in allowing us to define subtraction and integers later.

  Proposition 2.5 (Cancellation law)**.** *Let a, b, c be natural numbers such that $a + b = a + c$. Then we have $b = c$.*

  Proof. We induct on a (keeping b, c fixed). Consider the base case $a = 0$. If $0+b = 0+c$ by assumption and $0+b = b$ and $0+c = c$ by Definition 2.2, then $b = c$. Suppose inductively that $a+b = a+c$ implies that $b = c$. We must prove that $(a{+}{+}) + b = (a{+}{+}) + c$ implies $b = c$. This may be done as follows.

  $$\begin{aligned} (a{+}{+}) + b &= (a{+}{+}) + c && \text{Given} \\ (a + b){+}{+} &= (a + c){+}{+} && \text{Definition 2.2} \\ a + b &= a + c && \text{Axiom 2.4} \\ b &= c && \text{Induction hypothesis} \end{aligned}$$

  □

- **Positive natural numbers**: A natural number $n \neq 0$.

  Proposition 2.6. *If a is positive and b is a natural number, then $a + b$ is positive (and hence $b + a$ is also by Proposition 2.4).*

  Proof. We induct on b (keeping a fixed). In the base case, if $b = 0$, then $a + 0 = a$ (a positive number) by Lemma 2.1. Suppose inductively that $a + b$ is positive. Then $a + (b{+}{+}) = (a + b){+}{+}$ by Lemma 2.2, and $(a+b){+}{+}$ is positive by Axiom 2.3 — $a + (b{+}{+})$ is equal to the successor of a natural number, and the successor of a natural number is never 0, thus always positive. This closes the induction. □

  Corollary 2.1. *If $a, b \in \mathbb{N}$ and $a + b = 0$, then $a = 0$ and $b = 0$.*

  Proof. Suppose for the sake of contradiction that $a \neq 0$ or $b \neq 0$. If $a \neq 0$, then a is positive, and hence $a + b = 0$ is positive by Proposition 2.6, a contradiction. Similarly, if $b \neq 0$, then b is positive, and hence $a + b = 0$ is positive by Proposition 2.6, a contradiction. Thus, a and b must both be zero. □

- See Exercise 2.2.2 for another property of positive natural numbers.
- With addition, we can begin to order the natural numbers.

  Definition 2.3 (Ordering of the natural numbers)**.** Let $n, m \in \mathbb{N}$. We say that n is **greater than or equal to** m and write $n \geq m$ or $m \leq n$ iff we have $n = m + a$ for some $a \in \mathbb{N}$. We say that n is **strictly greater than** m and write $n > m$ or $m < n$ iff $n \geq m$ and $n \neq m$.

- Note that $n{+}{+} > n$ for any n.
- See Exercise 2.2.3 for more on ordering.
- We can now prove the trichotomy.

  Proposition 2.7 (Trichotomy of order for natural numbers)**.** *Let a and b be natural numbers. Then exactly one of the following statements is true: $a < b$, $a = b$, or $a > b$.*

  Proof. See Exercise 2.2.4 to fill in the gaps.

  First, show that no two (or three) of the statements can hold simultaneously. If $a < b$ or $a > b$, then $a \neq b$ by definition. Also, if $a > b$ and $a < b$, then $a = b$, a contradiction.

  Second, show that at least one of the statements is always true. We induct on a (keeping b fixed). When $a = 0$, we have $0 \leq b$ for all b (see Exercise 2.2.4a), so we either have $0 = b$ or $0 < b$, which proves the base case. Now suppose inductively that we have proven the proposition for a. From the trichotomy of a, there are three cases: $a < b$, $a = b$, and $a > b$. If $a > b$, then $a{+}{+} > b$ (see Exercise 2.2.4b). If $a = b$, then $a{+}{+} > b$ (see Exercise 2.2.4c). If $a < b$, then $a{+}{+} \leq b$ by Proposition 2.9. Thus, either $a{+}{+} = b$ or $a{+}{+} < b$. This closes the induction. □

6/17:
- With order, we can obtain a stronger version of induction (see Exercise 2.2.5).
  - Strong induction is usually used with $m_0 = 0$ or $m_0 = 1$.

Exercises

6/16:
1. Prove the following proposition. Hint: fix two of the variables and induct on the third.

   Proposition 2.8 (Addition is associative)**.** *For any natural numbers a, b, c, we have $(a + b) + c = a + (b + c)$.*

   Proof. We first need a lemma.

   Lemma 2.3. *The sum of two natural numbers $n + m$ is a natural number.*

   Proof. We induct on n (keeping m fixed). By Axiom 2.1, $0 \in \mathbb{N}$. Since $m \in \mathbb{N}$, by Definition 2.2, $0 + m$ (the sum of two natural numbers) equals m (a natural number). Thus, the base case holds. Suppose inductively that $n + m$ is a natural number. Then $(n{+}{+}) + m = (n + m){+}{+}$ by Definition 2.2, $n + m$ is a natural number by the induction hypothesis, and $(n + m){+}{+}$ is a natural number by Axiom 2.2. This closes the induction. □

   Now we induct on a (keeping b, c fixed). By the lemma, $b + c$ is a natural number and can be treated as such. Consider the base case $a = 0$. In this case, $0 + (b + c) = b + c$ and $0 + b = b$ by Definition 2.2, so $0 + (b + c) = b + c = (0 + b) + c$. Now suppose inductively that $a + (b + c) = (a + b) + c$. Then

   $$\begin{aligned} (a{+}{+}) + (b + c) &= (a + (b + c)){+}{+} && \text{Definition 2.2} \\ &= ((a + b) + c){+}{+} && \text{Induction hypothesis} \\ &= ((a + b){+}{+}) + c && \text{Definition 2.2} \\ &= ((a{+}{+}) + b) + c && \text{Definition 2.2} \end{aligned}$$

   This closes the induction. □

2. Prove the following lemma. Hint: use induction.

   Lemma 2.4. *Let a be a positive number. Then there exists exactly one natural number b such that $b{+}{+} = a$.*

   Proof. We induct on a. Consider the base case $a = 1$. $1 = 0{+}{+}$ by definition, and by Axiom 2.4, 0 is the only b satisfying $1 = b{+}{+}$. Now suppose inductively that a has only one b satisfying $b{+}{+} = a$. Then $a{+}{+}$ has only one natural number (namely a) satisfying $a{+}{+} = a{+}{+}$. This closes the induction. □

3. Prove the following proposition. Hint: you will need many of the preceding propositions, corollaries, and lemmas.

   Proposition 2.9 (Basic properties of order for natural numbers)**.** *Let a, b, c be natural numbers. Then*

   (*a*) (*Order is reflexive*) $a \geq a$.

   Proof. By Lemma 2.1, $a = a + 0$. The previous expression is in the form $n = m + a$; thus, by Definition 2.3, $a \geq a$. □

   (*b*) (*Order is transitive*) *If $a \geq b$ and $b \geq c$, then $a \geq c$.*

   Proof. If $a \geq b$ and $b \geq c$, then $a = b + n$ and $b = c + m$, respectively, for some $n, m \in \mathbb{N}$. Substituting, $a = (c + m) + n$. By Proposition 2.8, $a = c + (m + n)$. By Lemma 2.3, $m + n$ is a natural number. The previous expression is in the form $n = m + a$; thus, by Definition 2.3, $a \geq c$. □

   (*c*) (*Order is anti-symmetric*) *If $a \geq b$ and $b \geq a$, then $a = b$.*

   Proof. If $a \geq b$ and $b \geq a$, then $a = b + n$ and $b = a + m$, respectively, for some $n, m \in \mathbb{N}$. Substituting, $a = (a + m) + n$. By Proposition 2.8, $a = a + (m + n)$. By Lemma 2.1, $a + 0 = a + (m + n)$. By Proposition 2.5, $0 = m + n$. By Corollary 2.1, m and n both equal 0. Thus, $a = b + 0 = b$ (or $b = a + 0 = a$) by Lemma 2.1. □

   (*d*) (*Addition preserves order*) *$a \geq b$ iff $a + c \geq b + c$.*

   Proof. If $a + c \geq b + c$, then $a + c = (b + c) + n$ for some $n \in \mathbb{N}$. Then

   $$\begin{aligned} c + a &= n + (b + c) && \text{Proposition 2.4} \\ c + a &= (n + b) + c && \text{Proposition 2.8} \\ c + a &= c + (n + b) && \text{Proposition 2.4} \\ a &= n + b && \text{Proposition 2.5} \\ a &= b + n && \text{Proposition 2.4} \end{aligned}$$

   Thus, $a \geq b$. □

   (*e*) *$a < b$ iff $a{+}{+} \leq b$.*

   Proof. If $a{+}{+} \leq b$, then $b = (a{+}{+}) + n$ for some $n \in \mathbb{N}$. Then

   $$\begin{aligned} b &= (a + n){+}{+} && \text{Definition 2.2} \\ &= a + (n{+}{+}) && \text{Lemma 2.2} \end{aligned}$$

   Since $n{+}{+}$ is a natural number (Axiom 2.2), the above proves that $a \leq b$. By Axiom 2.3, $n{+}{+} \neq 0$. Thus, $b \neq a$ (suppose for the sake of contradiction that $b = a$. Then $b = b + 0 = a + (n{+}{+})$ implies by Proposition 2.5 that $0 = n{+}{+}$, a contradiction). By definition, since $a \leq b$ and $b \neq a$, $a < b$. □

   (*f*) *$a < b$ iff $b = a + d$ for some positive number d.*

Proof. As a positive number, d is a natural number by definition. Thus, $b = a + d$ implies $a \leq b$. Since d is a positive number, $d \neq 0$. For the reasons outlined in the previous proof, this implies that $b \neq a$. Thus, $a < b$. □

4. Justify the three statements marked (why?) in the proof of Proposition 2.7.

   (a) *If n is a natural number, then $0 \leq n$.*

   Proof. We induct on n. By Proposition 2.9, $0 \geq 0$, proving the base case. Suppose inductively that $n \geq 0$. We know that $n{+}{+} \geq n$ (since $n{+}{+} = (n + 0){+}{+} = n + 0{+}{+}$), so by Proposition 2.9, $n{+}{+} \geq n$ and $n \geq 0$ transitively imply $n{+}{+} \geq 0$. □

   (b) *Let a, b be natural numbers. Then if $a > b$, $a{+}{+} > b$.*

   Proof. We first need a lemma.

   Lemma 2.5. *If $a > b$ and $b > c$, then $a > c$.*

   Proof. If $a > b$ and $b > c$, then $a = b + n$ and $b = c + m$, respectively, for some positive numbers n, m. Substituting, $a = (c + m) + n$. By Proposition 2.8, $a = c + (m + n)$. By Proposition 2.6, $m + n$ is a positive number. Thus, by Proposition 2.9, $a > c$. □

   $a{+}{+} > a$. By the lemma, $a{+}{+} > a$ and $a > b$ imply that $a{+}{+} > b$. □

   (c) *Let a, b be natural numbers. Then if $a = b$, $a{+}{+} > b$.*

   Proof. $a{+}{+} > a$. Since $a = b$, substituting gives $a{+}{+} > b$. □

6/17: 5. Prove the following proposition. Hint: define $Q(n)$ to be the property that $P(m)$ is true for all $m_0 \leq m < n$; note that $Q(n)$ is vacuously true when $n < m_0$.

Proposition 2.10 (Strong principle of induction)**.** *Let m_0 be a natural number, and let $P(m)$ be a property pertaining to an arbitrary natural number m. Suppose that for each $m \geq m_0$, we have the following implication: if $P(m')$ is true for all natural numbers $m_0 \leq m' < m$, then $P(m)$ is also true. (In particular, this means that $P(m_0)$ is true, since in this case the hypothesis is vacuous.) Then we can conclude that $P(m)$ is true for all natural numbers $m \geq m_0$.*

Proof. Let n be a natural number satisfying $n \geq m_0$ and let $Q(n)$ be the property that $P(m)$ is true for all $m_0 \leq m < n$. We induct on n.

For the base case $n = 0$, we want to show that $Q(0)$ is true. Since $0 \leq m_0$ (Exercise 2.2.4a), either $0 = m_0$ or $0 < m_0$ (Proposition 2.7). We treat these cases separately. If $0 = m_0$, then $Q(0)$ is vacuously true (since there is no $m \in \mathbb{N}$ such that $0 \leq m < 0$, of course $P(m)$ is true for all $0 \leq m < 0$ [because there are no cases, $P(m)$ is true in all cases; it's also false, but that's besides the point.]) If $0 < m_0$, then $Q(0)$ is also vacuously true (since there is no $m \in \mathbb{N}$ such that $0 < m_0 \leq m < 0$).

Suppose inductively that for some $n \geq m_0$, $Q(n)$ is true, i.e., "$P(m)$ is true for all $m_0 \leq m < n$" is true. We want to show that $Q(n{+}{+})$ is true. By the definition of P in the hypothesis, $Q(n)$ is true implies $P(n)$ is true. Thus, $P(m)$ is true for all $m_0 \leq m < n{+}{+}$, so $Q(n{+}{+})$ is true. This closes the induction.

Since $Q(n)$ is true for all $n \geq m_0$, $P(n)$ is true for all $n \geq m_0$ (proof modified from Ojo, 2019). □

6. Let n be a natural number, and let $P(m)$ be a property pertaining to the natural numbers such that whenever $P(m{+}{+})$ is true, then $P(m)$ is true. Suppose that $P(n)$ is also true. Prove that $P(m)$ is true for all natural numbers $m \leq n$; this is known as the **principle of backwards induction**. Hint: apply induction to the variable n.

Proof. We induct on n. For the base case $n = 0$, we want to show that $P(m)$ is true for all natural numbers $m \leq n$. Since we are supposing that $P(n) = P(0)$ is true and 0 is the only number $m \in \mathbb{N}$ satisfying $m \leq 0$, the base case is true.

Suppose inductively that we have proved for $P(n)$ true that $P(m)$ is true for all natural numbers $m \leq n$. We want to show that for $P(n{+}{+})$ true, $P(m)$ is true for all natural numbers $m \leq n{+}{+}$. If $P(n{+}{+})$ is true, then clearly $P(m)$ is true for all natural numbers $m = n$. By definition, $P(n{+}{+})$ true implies $P(n)$ true, and $P(n)$ true implies that $P(m)$ is true for all natural numbers $m \leq n$. Thus, $P(m)$ is true for all natural numbers $m \leq n$ or $m = n{+}{+}$; these two statements can be combined into $m \leq n{+}{+}$. This closes the induction. □

2.3 Multiplication

6/18:

- At this point, all properties of addition can be used without supplying a justification.
- The definition of multiplication is very similar to the definition of addition.

  Definition 2.4 (Multiplication of natural numbers)**.** Let m be a natural number. To multiply 0 to m, we define $0 \times m := 0$. Now suppose inductively that we have defined how to multiply n to m. Then we can multiply $n{+}{+}$ to m by defining $(n{+}{+}) \times m := (n \times m) + m$.

- See Exercise 2.3.1 for a proof of the commutativity of multiplication.
- At this point, we abbreviate $n \times m$ as nm and use the convention that multiplication takes precedence over addition (i.e., $ab + c = (a \times b) + c$).
- See Exercise 2.3.2 for a proof of the zero product property.
- We can now prove the distributive law.

  Proposition 2.11 (Distributive law)**.** *For any natural numbers a, b, c, we have $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$.*

  Proof[5]*.* Since multiplication is commutative, we need only show the first identity $a(b+c) = ab+ac$. We keep a and b fixed, and use induction on c. Let's prove the base case $c = 0$, i.e., $a(b+0) = ab+a0$. The left-hand side is ab, while the right-hand side is $ab + 0 = ab$, so we are done with the base case. Now let us suppose inductively that $a(b+c) = ab+ac$, and let us prove that $a(b+(c{+}{+})) = ab+a(c{+}{+})$. The left-hand side is $a((b+c){+}{+}) = a(b+c)+a$, while the right-hand side is $ab+ac+a = a(b+c)+a$ by the induction hypothesis, and so we can close the induction. □

- See Exercise 2.3.3 for a proof of the associativity of multiplication.
- Bringing back order, we can prove that multiplication preserves order.

  Proposition 2.12 (Multiplication preserves order)**.** *If a, b are natural numbers such that $a < b$, and c is positive, then $ac < bc$.*

  Proof. Since $a < b$, we have $b = a + d$ for some positive d. Multiplying by c and using the distributive law, we obtain $bc = ac + dc$. Since c, d are positive, dc is positive, and hence $ac < bc$ as desired. □

- Although we still haven't introduced division, we can introduce a multiplicative analogy of the cancellation law.

  Corollary 2.2 (Cancellation law)**.** *Let a, b, c be natural numbers such that $ac = bc$ and c is non-zero. Then $a = b$.*

[5] Note that this could be accomplished by induction on a. However, for the sake of introducing new concepts, I will transcribe the alternative method from Tao, 2016.

Proof[6]. By the Proposition 2.7, we have three cases: $a < b$, $a = b$, or $a > b$. Suppose first that $a < b$, then by Proposition 2.12, we have $ac < bc$, which contradicts our hypothesis that $ac = bc$. We can obtain a similar contradiction when $a > b$. Thus, the only possibility is that $a = b$, as desired. □

- At this point, we can deduce all of the rules of algebra involving addition and multiplication (see Exercise 2.3.4 for such an example).
- With addition and multiplication now defined, we will rarely see incrementation moving forward. Regardless, we can always use $n{+}{+} = n + 1$ to describe it (this is not circular since $n + 1$ was originally defined from $n{+}{+}$).
- See Exercise 2.3.5 for a proof of the Euclidean algorithm.
  - This algorithm marks the beginning of **number theory**, which is important but will not be covered any further in this text.
- The definition of exponentiation is very similar to the definitions of addition and multiplication.

  Definition 2.5 (Exponentiation of natural numbers)**.** Let m be a natural number. To raise m to the power 0, we define $m^0 := 1$; in particular, we define $0^0 := 1$. Now suppose recursively that m^n has been defined for some natural number n. Then we define $m^{n++} := m^n \times m$.

- Exponentiation will not be explored too deeply here — wait until after we define the integers and rationals.

Exercises

1. Prove the following lemma. Hint: modify the proofs of Lemmas 2.1 and 2.2 and Proposition 2.4.

   Lemma 2.6 (Multiplication is commutative)**.** *Let n, m be natural numbers. Then $n \times m = m \times n$.*

   Proof. We first need two lemmas.

   Lemma 2.7. *For any natural number n, $n \times 0 = 0$.*

   Proof. We induct on n. For the base case $n = 0$, Definition 2.4 gives us $0 \times 0 = 0$. Suppose inductively that $n \times 0 = 0$. Then $(n{+}{+}) \times 0 = (n \times 0) + 0$ by Definition 2.4, which equals $0 + 0$ by the induction hypothesis, which equals 0. This closes the induction. □

   Lemma 2.8. *Let n, m be natural numbers. Then $n \times (m{+}{+}) = (n \times m) + n$.*

   Proof. We induct on n (keeping m fixed). For the base case $n = 0$, Definition 2.4 gives us $0 \times (m{+}{+}) = 0$ and $(0 \times m) + 0 = 0$. Thus, $0 \times (m{+}{+}) = (0 \times m) + 0$, proving the base case. Suppose inductively that $n \times (m{+}{+}) = (n \times m) + n$. Then

   $$\begin{aligned}
   (n{+}{+}) \times (m{+}{+}) &= (n \times (m{+}{+})) + m && \text{Definition 2.4} \\
   &= ((n \times m) + n) + m && \text{Induction hypothesis} \\
   &= ((n \times m) + m) + n \\
   &= ((n{+}{+}) \times m) + n && \text{Definition 2.4}
   \end{aligned}$$

   This closes the induction. □

[6] This could be accomplished by induction on c.

Now for the primary proof, we induct on n (keeping m fixed). For the base case $n = 0$, Definition 2.4 gives us $0 \times m = 0$ while Lemma 2.7 gives us $m \times 0 = 0$. Thus, $0 \times m = m \times 0$, proving the base case. Now suppose inductively that $n \times m = m \times n$. Then

$$\begin{aligned} (n{+}{+}) \times m &= (n \times m) + m && \text{Definition 2.4} \\ &= (m \times n) + m && \text{Induction hypothesis} \\ &= m \times (n{+}{+}) && \text{Lemma 2.8} \end{aligned}$$

This closes the induction. □

2. Prove the following lemma. Hint: prove the second statement first.

Lemma 2.9 (Positive natural numbers have no zero divisors)**.** *Let n, m be natural numbers. Then $n \times m = 0$ if and only if at least one of n, m is equal to zero. In particular, if n and m are both positive, then nm is also positive.*

Proof. We begin by proving the second statement. We induct on n (keeping m fixed). For the base case, n is actually equal to 1 (since 1 is the smallest positive number). We want to show that $1m$ is positive. By Definition 2.4, $1m = 0m + m = 0 + m = m$, which is positive by assumption. Suppose inductively that nm is positive. Then $(n{+}{+})m = nm + m$. Since $nm + m$ is the sum of two positive numbers, it is positive (Proposition 2.6). This closes the induction.

Suppose for the sake of contradiction that n, m are both positive natural numbers and $nm = 0$. Since $nm = 0$, it is not positive by definition. But this contradicts the previous assertion that nm must be positive if n, m are both positive. Thus, at least one of n, m is not positive, implying by definition that at least one of n, m is equal to 0. □

3. Prove the following proposition. Hint: modify the proof of Proposition 2.8 and use the distributive law.

Proposition 2.13 (Multiplication is associative)**.** *For any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.*

Proof. We first need a lemma.

Lemma 2.10. *For any natural numbers n, m, the product nm is a natural number.*

Proof. We induct on n (keeping m fixed). For the base case $n = 0$, $0m = 0$ by Definition 2.4, which is a natural number. Now suppose inductively that nm is a natural number. Then $(n{+}{+})m = nm + m$, which is the sum of two natural numbers. By Lemma 2.3, $nm + m$ is a natural number. This closes the induction. □

Now for the primary proof, we induct on a (keeping b, c fixed). For the base case $a = 0$, $(0 \times b) \times c = 0 \times c = 0$ by two applications of Definition 2.4. Also, $0 \times (b \times c) = 0$ by Definition 2.4 and the lemma (which asserts that bc can be treated as a natural number). Thus, $(0 \times b) \times c = 0 \times (b \times c)$ transitively, proving the base case. Now suppose inductively that $(a \times b) \times c = a \times (b \times c)$. Then

$$\begin{aligned} ((a{+}{+}) \times b) \times c &= ((a \times b) + b) \times c && \text{Definition 2.4} \\ &= (a \times b) \times c + b \times c && \text{Proposition 2.11} \\ &= a \times (b \times c) + b \times c && \text{Induction hypothesis} \\ &= (a{+}{+}) \times (b \times c) && \text{Definition 2.4} \end{aligned}$$

This closes the induction. □

4. Prove the identity $(a + b)^2 = a^2 + 2ab + b^2$ for all natural numbers a, b.

Proof. We first need two lemmas.

Lemma 2.11. *For any natural numbers n, m, $nm = \underbrace{m + \cdots + m}_{n \text{ times}}$.*

Proof. We induct on n (keeping m fixed). For the base case $n = 0$, $0m = 0$ by Definition 2.4. 0 is equal to the sum of zero m's, proving the base case. Suppose inductively that

$$nm = \underbrace{m + \cdots + m}_{n \text{ times}}$$

Then

$$(n{+}{+})m = nm + m = \underbrace{m + \cdots + m}_{n \text{ times}} + m = \underbrace{m + \cdots + m}_{n{+}{+} \text{ times}}$$

This closes the induction. □

Lemma 2.12. *For any natural numbers n, m, $m^n = \underbrace{m \times \cdots \times m}_{n \text{ times}}$.*

Proof. We induct on n (keeping m fixed). For the base case $n = 0$, $m^0 = 1$ by Definition 2.5. 1 is equal to the product of zero m's, proving the base case. Suppose inductively that

$$m^n = \underbrace{m \times \cdots \times m}_{n \text{ times}}$$

Then

$$m^{n{+}{+}} = m^n \times m = \underbrace{m \times \cdots \times m}_{n \text{ times}} \times m = \underbrace{m \times \cdots \times m}_{n{+}{+} \text{ times}}$$

This closes the induction. □

Now for the primary proof:

$$\begin{aligned}
(a+b)^2 &= (a+b)(a+b) && \text{Lemma 2.12} \\
&= (a+b)a + (a+b)b && \text{Proposition 2.11} \\
&= aa + ba + ab + bb && \text{Proposition 2.11} \\
&= a^2 + ba + ab + b^2 && \text{Lemma 2.12} \\
&= a^2 + (ab + ab) + b^2 && \text{Lemma 2.6} \\
&= a^2 + 2ab + b^2 && \text{Lemma 2.11}
\end{aligned}$$

□

5. Prove the following proposition. Hint: fix q and induct on n.

Proposition 2.14 (Euclidean algorithm)**.** *Let n be a natural number, and let q be a positive number. Then there exist natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.*

Proof. We induct on n (keeping q fixed). For the base case $n = 0$, choose $m = 0$ and $r = 0$. In both cases, 0 is a natural number, and in the latter case, 0 satisfies $0 \leq 0 < q$ since $0 \leq 0$ by Proposition 2.9 and $0 < q$ for all positive q. Since m, r meet all necessary conditions, $0q + 0 = 0$ by Definition 2.4 and 2.2, and $n = 0$ by hypothesis, the base case holds.

Suppose inductively that $n = mq + r$. We want to show that $n{+}{+} = m'q + r'$ for some m', r' satisfying the conditions that m and r must satisfy, respectively. To begin, we can show an equality between m, r and m', r' as follows.

$$\begin{aligned} m'q + r' &= n{+}{+} \\ &= n + 1 \\ &= mq + r + 1 \end{aligned}$$

From this, it would seem logical to choose $m' := m$ and $r' := r + 1$. However, since $r < q$, $r + 1 \leq q$, so by Proposition 2.7 we have two cases to consider. If $r + 1 < q$, it will indeed suffice to choose $m' := m$ and $r' := r + 1$. Both of these choices satisfy all of the necessary requirements. If $r + 1 = q$, we must choose differently. Choose $m' := m + 1$ and $r' := 0$. It may be more difficult to understand these choices, but they do work: $m + 1$ and 0 are both natural numbers, 0 satisfies $0 \leq 0 < q$ as discussed earlier, and the following shows that the choices maintain the equality with $n{+}{+}$.

$$\begin{aligned} (m + 1)q + 0 &= mq + q \\ &= mq + r + 1 \\ &= n + 1 \\ &= n{+}{+} \end{aligned}$$

With both cases treated, the induction may be closed. □