

Chapter 2 - Starting at the beginning: the natural numbers

Exercises:

§2.2 Addition

2.2.1. Prove Proposition 2.2.5. (Hint: fix two of the variables and induct on the third.)

Proof. Proposition 2.2.5 claims

$$\text{For any natural numbers } a, b, c, \text{ we have } (a + b) + c = a + (b + c).$$

We use induction. Let a, b, c , be natural numbers.

base case: For $c = 0$, $(a + b) + c = a + (b + c)$ becomes

$$\begin{aligned} (a + b) + 0 &= a + (b + 0) && [c = 0] \\ (a + b) + 0 &= a + (b) && [\text{Lemma 2.2.2.}] \\ (a + b) &= a + (b) && [\text{Definition 2.2.1 and Lemma 2.2.2.}] \\ a + b &= a + b \end{aligned}$$

induction hypothesis: Suppose that $(a + b) + c = a + (b + c)$.

induction step: We must now prove that $(a + b) + (c++) = a + (b + (c++))$.

The left-hand side $(a + b) + (c++)$ becomes

$$(a + b) + (c++) = ((a + b) + c)++ \quad [\text{Lemma 2.2.3.}]$$

while the right-hand side $a + (b + (c++))$ becomes

$$\begin{aligned} a + (b + (c++)) &= a + ((b + c)++) && [\text{Lemma 2.2.3.}] \\ &= (a + (b + c))++ && [\text{Lemma 2.2.3.}] \end{aligned}$$

Thus, $((a + b) + c)++ = (a + (b + c))++$ by the induction hypothesis and we have closed the induction. \square

2.2.2. Prove Lemma 2.2.10. (Hint: use induction.)

Proof. Lemma 2.2.10 claims,

Let a be a positive number. Then there exists exactly one natural number b such that $b++ = a$.

We use induction on a .

base case: Let $a = 1$, with is a positive number. We know that $0++ = 1$. 0 is a natural number by Axiom 2.1 and is unique by Proposition 2.1.6.

induction hypothesis: Suppose that $a = n$ and that there exists exactly one natural number b such that $b++ = a$.

induction step: We must now prove that for $a = n++$ that there exists exactly one natural number b such that $b++ = a$.

For $a = n++$, we know that $n++ = (b++)++$ by the induction hypothesis. From Axiom 2.2 and the induction hypothesis, we know that $b++$ is a natural number. From Proposition 2.1.8 we know that no natural number is equal to its successor and therefore we must have that $b \neq b++$, showing that $b++$ is unique such that $(b++)++ = a$. This closes the induction. \square

2.2.3. Prove Proposition 2.2.12. (Hint: you will need many of the preceding propositions, corollaries, and lemmas.)

Proof. Proposition 2.2.12 claims,

Let a, b, c be natural numbers. Then

- (a) *(Order is reflexive) $a \geq a$.*
- (b) *(Order is transitive) If $a \geq b$ and $b \geq c$, then $a \geq c$.*
- (c) *(Order is anti-symmetric) If $a \geq b$ and $b \geq a$, then $a = b$.*
- (d) *(Addition preserves order) $a \geq b$ if and only if $a + c \geq b + c$.*
- (e) *$a < b$ if and only if $a++ \leq b$.*
- (f) *$a < b$ if and only if $b = a + d$ for some positive number d .*

(a). Since $a = a$, by definition, then by Definition 2.2.11 we must have that $a \geq a$.

(b). If $a \geq b$ and $b \geq c$, then by Definition 2.2.11 we must have that $a = b + n_1$ and $b = c + n_2$ for some natural numbers n_1 and n_2 , respectively. Then $a = (c + n_2) + n_1 = c + (n_2 + n_1)$, since addition is associative (Proposition 2.2.5). Furthermore, $(n_2 + n_1)$ is a natural number from the definition of addition (Definition 2.2.1) and therefore, from Definition 2.2.11, we have that $a \geq c$.

(c). If $a \geq b$ and $b \geq a$, then by Definition 2.2.11 we must have that $a = b + n_1$ and $b = a + n_2$ for some natural numbers n_1 and n_2 , respectively. Then $a = (a + n_2) + n_1 = a + (n_2 + n_1)$ since addition is associative (Proposition 2.2.5). From Lemma 2.2.2, we must have that $(n_2 + n_1) = 0$, and therefore, from the previous equalities, we have that $a = b$.

(d). Note: For *iff* type proofs we must prove both directions.

(\rightarrow): If $a \geq b$, then by Definition 2.2.11 we must have that $a = b + n$ for some natural number n . Let c be some natural number. Then $a + c = b + n + c = b + c + n$ (addition is commutative), so that by Definition 2.2.11 we have that $a + c \geq b + c$.

(\leftarrow): If $a + c \geq b + c$ then by Definition 2.2.11 we must have that $a + c = b + c + n$ for some natural number n . This can be re-written as $a + c = (b + n) + c$ since addition is commutative and associative. Then using the cancellation law, Proposition 2.2.6, we see that $a = b + n$ and therefore, by Definition 2.2.11, we have that $a \geq b$.

(e.)

(\rightarrow): If $a < b$ then by Definition 2.2.11 we must have that $b \geq a$ and $a \neq b$. Therefore, we know that $b = a + n$ for some natural number n and since $a \neq b$ we see that n must be a positive number (if it was 0 we would have a contradiction). From Lemma 2.2.10 there exists exactly one natural number, say c , such that $c++ = n$. Thus, we have $b = a + (c++)$ and from Lemma 2.2.3 we see that this can be formulated as $b = (a + c)++$. Using the commutativity of addition this becomes $b = (c + a)++$ and then using Lemma 2.2.3 again, we conclude that $b = c + (a++)$ and using commutativity one last time we have that $b = (a++) + c$. Therefore, by Definition 2.2.11, we have that $a++ \leq b$.

(\leftarrow): If $a++ \leq b$, then by Definition 2.2.11, we have that $b = (a++) + n$ for some natural number n . From Definition 2.2.1, we can formulate this as $b = (a + n)++$ and then since addition is commutative this becomes $b = (n + a)++$. Then we see from Lemma 2.2.3, we have $b = a + (n++)$ and from Axiom 2.2 we know that $n++$ is a natural number. Thus, from Definition 2.2.11 we see that $b = a + (n++)$ implies $a \leq b$.

(f.)

(\rightarrow): If $a < b$ then by (e) we must have that $a++ \leq b$. By Definition 2.2.11, this means that $b = (a++) + n$ for some natural number n . From Definition 2.2.1 this becomes $b = (a + n)++$ and by Lemma 2.2.3 we then have $b = a + (n++)$. From Axiom 2.2 we know that $(n++)$ is some positive natural number, say d , from Axiom 2.3. Therefore, $b = a + d$ for some positive number d .

(\leftarrow): If $b = a + d$ for some positive number d , then d must be the successor of some natural number, say n . Thus we see that $b = a + (n++)$ and by Lemma 2.2.3 we have $b = (a + n)++$. From commutativity of addition and Lemma 2.2.3 this then becomes $b = (a++) + n$ which by Definition 2.2.11 implies that $a++ \leq b$. Since $b = a + d$ for some positive number d , we must have that $b \neq a$ by Lemma 2.2.2. Therefore, by Definition 2.2.11 we can conclude that $a < b$. \square

2.2.4. Justify the three statements marked (why?) in the proof of Proposition 2.2.13. Let us list the (why?):

1. When $a = 0$ we have $0 \leq b$ for all b .

Any natural number b must either be equal to 0 or equal to some multiple successor of 0, which by the ordering of the natural numbers (Definition 2.2.11) is larger than 0.

2. If $a > b$, then $a++ > b$.

Even though it hasn't been introduced in the textbook yet, instead of proving with the Propositions and Lemmas we will justify this claim with a proof by contrapositive as it the simplicity seems to be calling for it.

If $a++ \not> b$ then we must have that $a++ \leq b$ from the ordering of the natural numbers (Definition 2.2.11). From (e) of Exercise 2.2.3, we then see that we must have $a < b$ which shows that $a \not> b$.

If this seems too hand *wavy* at this point in our cultivation of the foundations of mathematics for your liking, let us justify this claim without using a proof by contrapositive.

First we will prove a corollary from Lemmas 2.2.2 and 2.2.3:

From Lemma 2.2.3, if we set $m = 0$ we have $n + (0++) = (n + 0)++$ and by Lemma 2.2.2 and the fact that $0++ = 1$, we then have $n + 1 = n++$. This shows, using Definition 2.2.11, that $n++ > n$.

Now to the proof. If $a > b$, then from Definition 2.2.11 we know that $a \neq b$ and $a = b + n$ for some positive natural number n . Using the corollary above we have $a++ > a > b$ and therefore $a++ > b$. For the ones that would like even more proof of this, the last step can be seen by noting that $a++ = a + 1$ and using the fact that $a = b + n$ so we must have $a++ = (b + n) + 1 = b + (n + 1)$. From Definition 2.2.11, the result follows.

3. If $a = b$, then $a++ > b$.

If $a = b$ then from the corollary derived in (2) above, we know that for a natural number n that $n++ > n$. Therefore, we must have that $b++ > b$. However, since $a = b$ we see that $a++ = b++$ and therefore, we conclude that $a++ > b$.

2.2.5. Prove Proposition 2.2.14. (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 $n < m_0$.)

Proof. We are going to prove the Strong principle of induction using standard induction. Proposition 2.2.14 claims:

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 $m \geq m_0$.

As the hint suggests, let us define $Q(n)$ to be the property that $P(m)$ is true for all $m_0 \leq m < n$. We prove this by induction on n .

base case: Let $n = 0$ so that we have $Q(0)$ which is the property that ‘if $P(m)$ is true for all $m_0 \leq m < 0$, then $P(0)$ is true’. This is the vacuously true, as there are no natural numbers less than 0, therefore $P(0)$ is true and subsequently so is $Q(0)$.

induction hypothesis: Suppose $Q(n)$ is true, that is, the property that ‘if $P(m)$ is true for all $m_0 \leq m < n$, then $P(n)$ is also true’.

induction step: $Q(n + 1)$ is the claim that ‘if $P(m)$ is true for all $m_0 \leq m < n + 1$, then $P(n + 1)$ is also true’. If $m < n + 1$, from Definition 2.2.11, we conclude that $n + 1 \neq m$ and there is a positive natural number, say d , such that $n + 1 = m + d$. Since d is an arbitrary positive natural number, let $d = 1$. The reason we can do this is because the criteria of $n + 1 \neq m$ and d being a positive natural number are both satisfied by setting $d = 1$, i.e., no rules have been broken. We then arrive at $n + 1 = m + 1$ and using the cancellation law of Proposition 2.2.6, we then have $n = m$. Thus, the inequality $m_0 \leq m < n + 1$ becomes $m_0 \leq n < n + 1$ and from the induction hypothesis we know that $P(n)$ is true and therefore we must have that $P(n + 1)$ is true. Thus, $Q(n + 1)$ is true. This closes the induction. \square

2.2.6. 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 are given a property $P(m)$ such that whenever $P(m++)$ is true, then $P(m)$ is true. We are also given that n is a natural number and that $P(n)$ is also true. We are to prove that $P(m)$ is true for all natural numbers $m \leq n$. We use induction on n .

base case: Let $n = 0$ and suppose that $P(0)$ is true. Then we trivially have that $P(m)$ is true for all natural numbers $m \leq 0$.

induction hypothesis: Suppose that $P(n)$ is true such that $P(m)$ is true for all natural numbers $m \leq n$.

induction step: Suppose that $P(n + 1)$ is true. We now need to prove that $P(m)$ is true for all natural numbers $m \leq n + 1$. $P(m)$ once again is the property that if $P(m++)$ is true, then $P(m)$ is true. Since $P(n + 1)$ is true by hypothesis, then $P(n)$ is true. Since $P(n)$ is true, we must have that $P(m)$ is true for all natural numbers $m \leq n$ by the induction hypothesis. Therefore, we have that $P(m)$ is true for $m \leq n$ as well as for $P(n + 1)$, i.e., for $n + 1$. Thus, $P(m)$ is true for all natural numbers $m \leq n + 1$. This closes the induction. \square

§2.3 Multiplication

2.3.1 Prove Lemma 2.3.2. (Hint: modify the proofs of Lemmas 2.2.2, 2.2.3 and Proposition 2.2.4.)

Proof. Lemma 2.3.2 claims,

$$\text{Let } n, m \text{ be natural numbers. Then } n \times m = m \times n.$$

First, we modify the proofs of Lemmas 2.2.2 and 2.2.3. We will then use this to modify the proof of Proposition 2.2.4.

[*Modification of Lemma 2.2.2 — proving that $0 \times m = 0$*] We use induction on n :

base case: The base case $0 \times 0 = 0$ follows since we know that $0 \times m = m$ for every natural number m , and 0 is a natural number.

induction hypothesis: Suppose that $n \times 0 = n$.

induction step: We must show that $(n++) \times 0 = n++$. By definition of multiplication we know that $(n++) \times 0 = (n \times 0)++$, which is equal to $n++$ since $n \times 0 = n$ from the induction hypothesis. This closes the induction.

[*Modification of Lemma 2.2.3 — proving that $n \times (m++) = n + (n \times m)$*] We use induction on n :

base case: For the base case $n = 0$ we have to prove that $0 \times (m++) = 0 + (0 \times m)$. We know that for any natural number m , that $m++$ is also a natural number and by the definition of multiplication we know that $0 \times (m++) = 0$. Therefore the left-hand side of the equation is equal to 0. By the definition of multiplication the right-hand side $0 + (0 \times m)$ becomes $0 + (0)$ which equals 0. Thus the left and right-hand sides are equal.

induction hypothesis: Suppose that for any natural numbers n, m that $n \times (m++) = n + (n \times m)$.

induction step: We must prove that $(n + 1) \times (m++) = (n + 1) + ((n + 1) \times m)$. Noting that $n + 1 = n++$ this can be re-written as $(n++) \times (m++) = (n++) + ((n++) \times m)$.

The left-hand side is $(n \times m++) + (m++)$ by definition of multiplication, which is equal to $n + (n \times m) + (m++)$ by the induction hypothesis. By the definition of addition we see that this can be further simplified to $(n \times m) + (m + n)++$.

Similarly for the right-hand side, by the definition of multiplication we have $(n++) + (n \times m) + m$. This can be further simplified to $(n \times m) + (n + m)++$ and finally $(n \times m) + (m + n)++$ from the commutativity of addition. As both sides of the equation are equal, this closes the induction.

[Modification of Proposition 2.2.4 — proving that $n \times m = m \times n$] We use induction on n (keeping m fixed):

base case: Let $n = 0$. From the definition of multiplication and the modification of Lemma 2.2.2 above, $0 \times m = 0$ and $m \times 0 = 0$. Therefore, $0 \times m = m \times 0$ for natural numbers n and m .

induction hypothesis: Suppose that $n \times m = m \times n$ for natural numbers n and m .

induction step: We must prove that $(n + 1) \times m = m \times (n + 1)$ for natural numbers n and m . Let us re-write this as $(n++) \times m = m \times (n++)$. The left-hand side is $(n \times m) + m$ by the definition of multiplication while the right-hand side is $m + (m \times n)$ from the modification of Lemma 2.2.3 above. Using the induction hypothesis, we see that both the left-hand and right-hand sides are equal, closing the induction.

Therefore, $n \times m = m \times n$ showing that multiplication is commutative. \square

2.3.2 Prove Lemma 2.3.3. (Hint: prove the second statement first.)

Proof. Lemma 2.3.3 claims,

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.

(\leftarrow): If at least one of n, m is equal to zero then $n \times m$ either takes the form $0 \times m$ or $n \times 0$, which are both equal to zero by the definition of multiplication and modification of Lemma 2.2.2 as seen in the last exercise. Therefore, $n \times m = 0$.

(\rightarrow): If $n \times m = 0$ then since $0 \times m = 0$ by the definition of multiplication we see that $n = 0$ satisfies this equality. However we also know that since $n \times 0 = 0$ by the modification of Lemma 2.2.2 above, we see that $m = 0$ also satisfies this equality. Therefore, at least one of n, m is equal to zero.

In particular, if $n > 0$ and $m > 0$ then $n \geq 1$ and $m \geq 1$. Suppose that $n = 1$. Then $n \times m = 1 \times m = 0 + m = m$ by the definition of multiplication and addition. Since multiplication is commutative this argument also holds for $m = 1$. Either way, we see that nm is also positive. \square

2.3.3 Prove Proposition 2.3.5. (Hint: modify the proof of Proposition 2.2.5 and use the distributive law.)

Proof. Proposition 2.3.5 claims,

For any natural numbers a, b, c , we have $(a \times b) \times c = a \times (b \times c)$.

We keep a and b fixed and use induction on c .

base case: For $c = 0$ we have $(a \times b) \times 0 = a \times (b \times 0)$ and both sides are zero.

induction hypothesis: Suppose that $(a \times b) \times c = a \times (b \times c)$.

induction step: We will prove that $(a \times b) \times (c++) = a \times (b \times (c++))$.

On the left-hand side $(a \times b) \times (c++)$ is $(c++) \times (a \times b)$ from commutativity and then $(c \times (a \times b)) + (a \times b)$ from the definition of multiplication. One more operation of commutativity gives us $((a \times b) \times c) + (a \times b)$.

On the right-hand side $a \times (b \times (c++))$ is $a \times ((c++) \times b)$ from commutativity and then $a \times ((c \times b) + b)$ from the definition of multiplication. Using Proposition 2.3.4 this becomes $(a \times (c \times b)) + (a \times b)$ which is then $(a \times (b \times c)) + (a \times b)$ from commutativity.

From the induction hypothesis, we see that the left-hand and right-hand sides are both equal, closing the induction. \square

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

Proof. Let a, b be natural numbers.

Expanding the left-hand side we have $(a + b)(a + b)$ which becomes $(a + b)a + (a + b)b$ from the distributive law. Using the distributive law once again this becomes $aa + ba + ab + bb$ which is equal to $a^2 + 2ab + b^2$ since multiplication is commutative. \square

2.3.5 Prove Proposition 2.3.9. (Hint: fix q and induct on n .)

Proof. Proposition 2.3.9 claims,

*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 $n = mq + r$.*

We fix q and use induction on n .

base case: Let $n = 0$. Then $n = mq + r$ becomes $0 = mq + r$. Let $m = 0$ and $r = 0$ as zero is a natural number and $r = 0$ satisfies $0 \leq r < q$. The right-hand side becomes $0q + 0 = 0 + 0 = 0$ showing that there exist natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.

induction hypothesis: Suppose that there exist natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.

induction step: We will prove that there exist natural numbers m, r such that $0 \leq r < q$ and $n + 1 = mq + r$.

Note that $n + 1 = mq + r$ becomes $(m_1q + r_1) + 1 = mq + r$ from the induction hypothesis where we know that m_1, r_1 are natural numbers. This becomes $m_1q + (r_1 + 1)$ from associativity of addition and we know that $r_1 + 1 = r_1++$, which is a natural number. Therefore, we see that if we let $m = m_1$ and $r = r_1++$ the left-hand and right-hand sides are equal. This shows that there exist natural numbers m, r such that $0 \leq r < q$ and $n + 1 = mq + r$, closing the induction. \square