Exercise 1.3.3 Complete the proof for Lemma 1.3.4. That is, prove that $\cdot$ and $-$ for $\mathbb{Z}$ are well-defined. The proof for $\cdot$ is a bit more complicated than might be expected.

Proof. Let $(a, b), (c, d), (x, y), (z, w) \in \mathbb{N} \times \mathbb{N}$ be arbitrary. Suppose that $[(a, b)] = [(x, y)]$ and $[(c, d)] = [(z, w)]$. Then $a + y = b + x$, and since addition on $\mathbb{N}$ is commutative, $y + a = x + b$. Hence $[(y, x)] = [(b, a)]$ which is the same as $-[(a, b)] = -[(x, y)]$.

Consider the following.

$$\begin{aligned}
(w+z)(x+y) + (c+d)(a+b) &= (w+z)x + (w+z)y + (c+d)a + (c+d)b \\
&= wx + zx + wy + zy + ca + da + cb + db \\
&= xw + zx + yw + yz + ac + da + bc + bd \\
&= (xz + yw) + (ac + bd) +
\end{aligned}$$

$\square$

Exercise 1.3.5 Prove Theorem 1.3.5 (1) (3) (4) (5) (6) (7) (8) (10) (11) (13) (14). Throughout the proofs, we let $x = [(x_0, x_1)]$, $y = [(y_0, y_1)]$ and $z = [(z_0, z_1)]$.

proof of (1).

$$\begin{aligned}
(x + y) + z &= [(x_0 + y_0, x_1 + y_1)] + [(z_0, z_1)] \\
&= [((x_0 + y_0) + z_0, (x_1 + y_1) + z_1)] \\
&= [(x_0 + (y_0 + z_0), x_1 + (y_1 + z_1))] \\
&= [(x_0, x_1)] + [(y_0 + z_0, y_1 + z_1)] \\
&= [(x_0, x_1)] + ([(y_0, y_1)] + [(z_0, z_1)]) \\
&= x + (y + z).
\end{aligned}$$

$\square$

Proof of (3).

$$x + 0 = [(x_0, x_1)] + [(1, 1)] = [(x_0 + 1, x_1 + 1)] = [(x_0, x_1)] = x.$$

One can justify $[(x_0 + 1, x_1 + 1)] = [(x_0, x_1)]$ by $(x_0 + 1) + x_1 = (x_1 + 1) + x_0$ (We've shown commutativity and associativity in $\mathbb{N}$). $\square$

Proof of (4).

$$x + (-x) = [(x_0, x_1)] + [(x_1, x_0)] = [(x_0 + x_1, x_1 + x_0)] = [(1, 1)] = 0.$$

$[(x_0 + x_1, x_1 + x_0)] = [(1, 1)]$ because $x_0 + x_1 + 1 = x_1 + x_0 + 1$ (Apply commutativity, which we've proven on $+$ in $\mathbb{N}$). $\square$

Proof of (5).

$$\begin{aligned}
(xy)z &= [(x_0y_0 + x_1y_1, x_0y_1 + x_1y_0)] \cdot [(z_0, z_1)] \\
&= [(z_0(x_0y_0 + x_1y_1) + z_1(x_0y_1 + x_1y_0), z_1(x_0y_0 + x_1y_1) + z_0(x_0y_1 + x_1y_0))] \\
&= [(x_0y_0z_0 + x_1y_1z_0 + x_0y_1z_1 + x_1y_0z_1, x_0y_0z_1 + x_1y_1z_1 + x_0y_1z_0 + x_1y_0z_0)] \\
&= [(x_0(y_0z_0 + y_1z_1) + x_1(y_1z_0 + y_0z_1), x_0(y_0z_1 + y_1z_0) + x_1(y_1z_1 + y_0z_0))] \\
&= [(x_0, x_1)] \cdot [(y_0z_0 + y_1z_1, y_1z_0 + y_0z_1)] \\
&= x \cdot ([(y_0, y_1)] \cdot [(z_0, z_1)]) \\
&= x(yz).
\end{aligned}$$

Note that we implicitly use properties we've proven for operations on the natural numbers (associativity and commutative for both addition and multiplication). $\square$

Proof of (6).

$$\begin{aligned}
xy &= [(x_0, x_1)] \cdot [(y_0, y_1)] \\
&= [(x_0y_0 + x_1y_1, x_0y_1 + x_1y_0)] \\
&= [(y_0x_0 + y_1x_1, y_0x_1 + y_1x_0)] \\
&= [(y_0, y_1)] \cdot [(x_0, x_1)] \\
&= yx
\end{aligned}$$

□

Proof of (7).

$$\begin{aligned}
x \cdot 1 &= [(x_0, x_1)] \cdot [(1 + 1, 1)] \\
&= [(x_0(1 + 1) + x_1 \cdot 1, x_0 \cdot 1 + x_1(1 + 1))] \\
&= [(x_0 + x_0 + x_1, x_0 + x_1 + x_1)] \\
&= [(x_0, x_1)].
\end{aligned}$$

Since $(x_0 + x_0 + x_1) + x_1 = (x_0 + x_1 + x_1) + x_0$, the final step is justified. □

proof of (8).

$$\begin{aligned}
x(y + z) &= [(x_0, x_1)] \cdot ([(y_0 + z_0, y_1 + z_1)]) \\
&= [(x_0(y_0 + z_0) + x_1(y_1 + z_1), x_0(y_1 + z_1) + x_1(y_0 + z_0))] \\
&= [(x_0y_0 + x_0z_0 + x_1y_1 + x_1z_1, x_0y_1 + x_0z_1 + x_1y_0 + x_1z_0)] \\
&= [((x_0y_0 + x_1y_1) + (x_0z_0 + x_1z_1), (x_0y_1 + x_1y_0) + (x_0z_1 + x_1z_0))] \\
&= [(x_0y_0 + x_1y_1, x_0y_1 + x_1y_0)] + [(x_0z_0 + x_1z_1, x_0z_1 + x_1z_0)] \\
&= [(x_0, x_1)] \cdot [(y_0, y_1)] + [(x_0, x_1)] \cdot [(z_0, z_1)] \\
&= xy + xz.
\end{aligned}$$

□

proof of (10). We show that at least one of $x < y$, $x = y$ or $x > y$ holds. Suppose that $x \not> y$, $x \not< y$ and $x \neq y$. Hence, $x_0 + y_1 \not< x_1 + y_0$ and $y_0 + x_1 \not< y_1 + x_0$. Using the trichotomy of order in $\mathbb{N}$, we can then deduce that $x_0 + y_1 = x_1 + y_0$. However, this contradicts the assumption that $x \neq y$. Hence, at least one of the three statements holds. Now we show that no two statements can hold simultaneously. Suppose that $x < y$ and $x = y$. Then $x_0 + y_1 < x_1 + y_0$ but also $x_0 + y_1 = x_1 + y_0$ which clearly contradicts the trichotomy of order in $\mathbb{N}$. The other cases follow suit similarly. □

proof of (11). Suppose that $x < y$ and $y < z$. So $x_0 + y_1 < x_1 + y_0$ and $y_0 + z_1 < y_1 + z_0$. From the latter, we deduce that $y_1 + z_0 = y_0 + z_1 + q$ for some $q \in \mathbb{N}$. We can add this equality to both sides of the former to get $(x_0 + y_1) + (y_0 + z_1 + q) < (x_1 + y_0) + (y_1 + z_0)$. Then, using the cancellation law, we can simplify this to $x_0 + z_1 + q < x_1 + z_0$. So $x_1 + z_0 = x_0 + z_1 + q + r$ for some $r \in \mathbb{N}$. Since $q + r \in \mathbb{N}$, we get that $x_0 + z_1 < x_1 + z_0$. Hence, $x < z$. □

proof of (13). Suppose that $x < y$ and $z > \hat{0}$. We know, from Theorem 1.3.7 (2), that $z = [(a + 1, 1)]$ for some $a \in \mathbb{N}$. Since $x_0 + y_1 < x_1 + y_0$, multiplying both sides by a yields $ax_0 + ay_1 < ax_1 + ay_0$. Hence,

$$\begin{gathered}
[(ax_0, ax_1)] < [(ay_0, ay_1)] \\
[(ax_0 + x_0 + x_1, ax_1 + x_0 + x_1)] < [(ay_0 + y_0 + y_1, ay_1 + y_0 + y_1)] \\
[(x_0(a + 1) + x_1, x_1(a + 1) + x_0)] < [(y_0(a + 1) + y_1, y_1(a + 1) + y_0)] \\
[(x_0, x_1)][(a + 1, 1)] < [(y_0, y_1)][(a + 1, 1)] \\
xz < yz
\end{gathered}$$

□

proof of (14). Suppose that $\hat{0} = \hat{1}$. So $[(1, 1)] = [(1 + 1, 1)]$. By definition, this means $1 + 1 = 1 + (1 + 1)$. Applying associativity with the law of cancellation for addition, we get $1 = 1 + 1$. This contradicts peano axioms. Hence, $\hat{1} \neq \hat{0}$. $\square$

Exercise 1.3.6 Prove Theorem 1.3.7 (1) (3) (4b) (4c).

proof of (1). Suppose that $i(a) = i(b)$ for some $a, b \in \mathbb{N}$. So $[(a+1, 1)] = [(b+1, 1)]$ and $(a+1)+1 = 1+(b+1)$. Applying the cancellation law twice, we yield $a = b$. As desired. □

proof of (3). This holds true by definition of $\hat{1}$. □

proof of (4b). Let $a, b \in \mathbb{N}$ be arbitrary natural numbers. Then

$$\begin{aligned} i(a)i(b) &= [(a+1, 1)][(b+1, 1)] \\ &= [((a+1)(b+1)+1, a+1+b+1)] \\ &= [(ab+a+b+1+1, a+1+b+1)] \\ &= [(ab+1, 1)] \\ &= i(ab) \end{aligned}$$

□

proof of (4c). ($\Longrightarrow$) Suppose that $a < b$ for some $a, b \in \mathbb{N}$. Using properties of order, we see that $(a+1)+1 < (b+1)+1$. Therefore, $[(a+1, 1)] < [(b+1, 1)]$.

($\Longleftarrow$) Every step in $\Longrightarrow$ can be reversed to yield $\Longleftarrow$. □

Exercise 1.3.7 Let $x, y, z \in \mathbb{Z}$.

1. Prove that $x < y$ if and only if $-x > -y$.

2. Prove that if $z < 0$, then $x < y$ if and only if $xz > yz$.

proof for (1). Suppose that $x < y$. Adding $(-x) + (-y)$ to both sides, we yield $(-y) + ((-x) + x) < (-x) + ((-y) + y)$ which simplifies to $-y < -x$.

Now suppose that $-x > -y$. Adding $x + y$ to both sides gives $y + (x + (-x)) > x + (y + (-y))$ which gives $y > x$ after simplification using the law of additive inverses. □

proof of (2). Suppose that $z < 0$, and suppose that $x < y$. We know from (1) that $-z > -0 = 0$. And we know from Theorem 1.3.5 (13) that $-zx < -zy$. Applying (1) again gives $zx > zy$ which is the desired result.

We prove the converse using constraposition. Suppose that $x \geq y$. Either $x = y$ or $x > y$. In the former, we deduce that $xz = yz$, and therefore, $xz \leq yz$. In the latter, we apply the result we just proved to yield $xz < yz$ which is also equivalent to $xz \leq yz$. □

Exercise 1.3.8 Let $x \in \mathbb{Z}$. Prove that if $x > 0$ then $x \geq 1$. Prove that if $x < 0$ then $x \leq -1$.

Proof. Suppose that $x > 0$, and suppose that $x < 1$. So $0 < x < 1$ which contradicts Theorem 1.3.9. Now suppose that $x < 0$, and that $x > -1$. We deduce that $-1 < x < 0$ which also contadicts Theorem 1.3.9. □

Exercise 1.3.9

1. Prove that $1 < 2$.

2. Let $x \in \mathbb{Z}$. Prove that $2x \neq 1$.

proof of (1). We know $[(1+1+1, 1)] = 2$ and $[(1+1, 1)] = 1$. Since $(1+1)+1 < (1+1+1)+1$, we deduce that $1 < 2$. □

proof of (2). Let $x \in \mathbb{Z}$ be arbitrary. Suppose that $2x = 1$. Since $1 > 0$, we know that $2x > 0$ (Apply Lemma 1.3.8 (11)). And since $2 > 0$, $x > 0$. Since x is positive and $1 < 2$, it must be the case that $x < 2x = 1$. Therefore, $0 < x < 1$. However, we know from Theorem 1.3.9 that no such x can exist. Therefore, we have a contradiction. □

Lemma If $A \subseteq \{x \in \mathbb{Z} : x > \hat{0}\}$, $\hat{1} \in A$, and $a \in A$ implies $a + 1 \in A$, then $A = \{x \in \mathbb{Z} : x > \hat{0}\}$.

Proof. Let $R = \{x \in \mathbb{Z} : x > \hat{0}\}$. Let A be an arbitrary subset of R such that $\hat{1} \in A$. Furthermore, suppose that $a \in A$ implies $a + 1 \in A$. Obviously $i(1) \in A$. Therefore, $1 \in i^{-1}[A]$. Now suppose that $a \in i^{-1}[A]$, meaning $i(a) \in A$. By the properties of A, we know that $i(a) + \hat{1} \in A$. Since $i(a) + \hat{1} = i(a) + i(1) = i(a+1)$, $i(a+1) \in A$. Therefore, $a + 1 \in i^{-1}[A]$. Hence, $i^{-1}[A] = \mathbb{N}$. Therefore, $R \subseteq A$. Since $A \subseteq R$, it must be the case that $A = R$. □

Exercise 1.3.10 Prove that the Well-Ordering Principle (Theorem 1.2.10), which was stated for $\mathbb{N}$ in Section 1.2, still holds when we think of $\mathbb{N}$ as the set of positive integers. That is, let $G \subseteq \{x \in \mathbb{Z} : x > 0\}$ be a non-empty set. Prove that there is some $m \in G$ such that $m \leq g$ for all $g \in G$. Use Theorem 1.3.7.

Proof. Let $R = \{x \in \mathbb{Z} : x > 0\}$. Suppose that there is no $m \in G$ such that $m \leq g$ for all $g \in G$. We will derive a contradiction. Let

$$H = \{a \in R : \text{if } b \in R \text{ and } b \leq a, \text{ then } b \notin G\}.$$

It follows from the definition of H that $H \cap G = \varnothing$. We will show $H = R$, using our previous Lemma in the process. It will then follow that G is empty which gives us our desired contradiction.

Suppose that $\hat{1} \notin H$. Then there is some $q \in R$ such that $q \leq \hat{1}$ and $q \in G$. Since $\hat{0} < q < \hat{1}$ contradicts Theorem 1.3.9 and $\hat{0} < q \leq \hat{1}$, it must be the case that $q = \hat{1}$. Hence, $\hat{1} \in G$. We know, from Theorem 1.2.9 (2) in $\mathbb{N}$, that $1 \leq a$ for all $a \in \mathbb{N}$. If we apply $i : \mathbb{N} \to \mathbb{Z}$ to both sides, we get $\hat{1} \leq i(a)$ for all $a \in \mathbb{N}$. Since $i[\mathbb{N}] = R$, it must be the case that $\hat{1} \leq r$ for all $r \in R$. But this would mean that $\hat{1}$ is a least element of G which is a contradiction to our hypothesis that no such element exists. Therefore, $\hat{1} \in H$.

Now suppose that $a \in H$. Suppose further that $a + \hat{1} \notin H$. Then there is some $p \in R$ such that $p \leq a + \hat{1}$ and $p \in G$. If it were the case that $p \leq a$, then we would have a contradiction due to the fact that $a \in H$. Hence, by the trichotomy of order in $\mathbb{Z}$, we see that $a < p$. Therefore, $a < p \leq a + \hat{1}$. From which follows immediately that $p = a + \hat{1}$. Thus, $a + \hat{1} \in G$. Now let $x \in G$. Suppose that $x < a + \hat{1}$. Since x and a are elements of R, there exists $a_0, x_0 \in \mathbb{N}$ such that $i(a_0) = a$ and $i(x_0) = x$. Hence, $i(x_0) < i(a_0 + 1)$. Via the properties of $i : \mathbb{N} \to \mathbb{Z}$, we have that $x_0 < a_0 + 1$. And using Theorem 1.2.9 (10) for $\mathbb{N}$, we see that $x_0 \leq a_0$. Therefore, $i(x_0) \leq i(a_0)$ and $x \leq a$. Because $a \in H$ it follows that $x \notin G$, which is a contradiction to the fact no such elements such as $a + \hat{1}$ exists in G. It follows that $a + \hat{1} \in H$ and $H = R$. □

Exercise 1.3.11 Prove Theorem 1.3.8 (1) (3) (4) (5) (7) (10) (11).

proof of (1).

$$\begin{aligned} x + z &= y + z \\ x + z + (-z) &= y + z + (-z) \\ x + 0 &= y + 0 \\ x &= y. \end{aligned}$$

□

proof of (3). Consider $x + y + (-x) + (-y) = 0$.

$$\begin{aligned} x + y + (-x) + (-y) &= 0 \\ (x + y) + (-(x + y)) + (-x) + (-y) &= -(x + y) \\ 0 + (-x) + (-y) &= -(x + y) \\ (-x) + (-y) &= -(x + y) \end{aligned}$$

□

proof of (4).

$$\begin{aligned} x &= x \cdot 1 \\ &= x \cdot (1 + 0) \\ &= x \cdot 1 + x \cdot 0 \\ &= x + x \cdot 0 \end{aligned}$$

So $x = x + x \cdot 0$. Adding $-x$ to both sides yields the desired result. $\square$

proof of (5). Suppose that $z \neq 0$ and $xz = yz$. Then $xz + (-(yz)) = 0$ and $xz + (-y)z = (x + (-y))z = 0$. Using Theorem 1.3.5 (9) (Which states that $\mathbb{Z}$ have no zero divisors), we deduce that $x+(-y) = 0$. Therefore, $x = y$. $\square$

proof of (7). Suppose that $\square$