

Section 2.3

Exercise 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.

We need to show $m \times 0 = m$ and $n \times (m++) = (n \times m) + n$ before proving the multiplication is commutative.

To show $m \times 0 = m$ we use induction. For the base case $0 \times 0 = 0$ follows since we know that $0 \times m = m$ by definition. Now suppose inductively that $m \times 0 = m$, we need to show $(m++) \times 0 = 0$. By definition $(m++) \times 0 = (m \times 0) + 0 = 0$, hence the induction is closed.

To show $n \times (m++) = (n \times m) + n$, we induct on n . For the base case $0 \times (m++) = (0 \times m) + 0$ follows by the definitions of addition and multiplication. Now suppose inductively $n \times (m++) = (n \times m) + n$, we need to show $n++ \times (m++) = (n++ \times m) + n++$. The left-hand side is $n \times (m++) + (m++) = n \times m + n + m + 1$ by definition of multiplication and the hypothesis. The right-hand side is $(n \times m + m) + n++ = n \times m + n + m + 1$ by definition of multiplication. Thus both sides are equal to each other, and we have closed the induction.

To show multiplication is commutative, we induct on n . For the base case $0 \times m = m \times 0$ follows since both sides equal to zero by definition of multiplication and $m \times 0 = 0$. Now suppose inductively that $n \times m = m \times n$, we need to show $n++ \times m = m \times n++$. The left-hand side is $n \times m + m$ by definition. The right-hand side is $m \times n + m$ by the lemma we've just proved. And by the hypothesis the right-hand then equals to $n \times m + m$. Thus both sides are equal to each other, and we have closed the induction. □

Exercise 2.3.2

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

Proof.

The statement is equivalent to " $n \times m$ is positive iff both n and m are positive".

First we need to show $n \times m$ is positive implies both n and m are positive. For the sake of contradiction that n equals to zero, by definition of multiplication $0 \times m = 0$, a contradiction. Similar contradiction holds for m with Lemma 2.3.2. Thus we have proved the statement.

Then we need to show both n and m are positive implies $n \times m$ is positive. For the sake of contradiction that $n \times m = 0$, by Lemma 2.2.10 there exists exactly one natural number a such that $a++ = n$, thus by definition of multiplication we have $n \times m = (a++) \times m = (a \times m)++$. Since $a \times m$ is a natural number, by Axiom 2.3 $(a \times m)++ \neq 0$, a contradiction. Thus $n \times m$ is positive.

Thus we have proved the original statement.

□

Exercise 2.3.3

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

Proof. We use induction on a . For the base case $(0 \times b) \times c = 0 \times (b \times c)$ follows, since the left-hand side equals to $0 \times c = 0$ by definition of multiplication, and the right-hand side equals to 0 since $b \times c$ is a natural number and 0 times a natural number equals to 0. Now suppose inductively $(a \times b) \times c = a \times (b \times c)$, we need to show $(a++ \times b) \times c = a++ \times (b \times c)$. The left-hand side equals to $(a \times b + b) \times c$ by definition of multiplication, then equals to $(a \times b) \times c + b \times c$ by the distributive law. The right-hand side equals to $a \times (b \times c) + b \times c$ by definition of multiplication. By the hypothesis both sides are equal to each other, thus we have closed the induction.

□

Exercise 2.3.4

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

Proof. $(a + b)^2 = (a + b)^1 (a + b) = (a + b) (a + b)$ by definition of exponentiation. Thus equals to $a \times (a + b) + b \times (a + b) = a \times a + a \times b + b \times a + b \times b$ by the distributive law. $a \times a = a^2$ and $b \times b = b^2$ by definition of exponentiation. $a \times b + b \times a = a \times b + a \times b = 2ab$ since multiplication is commutative and the definition of multiplication. Thus we have proved the statement.

□

Exercise 2.3.5

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

Proof. We use induction on n (keep q fixed). For the base case there exists natural numbers $m = 0, r = 0$ such that $0 \leq r < q$ and $0 = mq + r$. Now suppose inductively there exists m, r such that $0 \leq r < q$ and $n = mq + r$, we need to show there exists m', r' such that $0 \leq r' < q$ and $n = m'q + r'$. Thus $r++ \leq q$ by Proposition 2.2.12 (e). If $r++ < q$, we can simply set $m' = m$ and $r' = r + 1$. Otherwise if $r++ = q$, then $n++ = mq + q = (m++) \times q + 0$, thus we can set $m' = m++$ and $r' = 0$. Thus we have close the induction.

□