Chapter 2: Starting from the Natural Numbers

Definitions and Proofs

The Peano Axioms

Axiom 1
0 is a natural number.

Axiom 2
If N is a natural number, then $S(N)$ is also a natural number.

Axiom 3
0 is not the successor of any natural number.
$S(N) \neq 0$ for every natural number N.

Axiom 4
Different natural numbers must have different successors.
If N, M are natural numbers and $N \neq M$, then $S(N) \neq S(M)$. Equivalently, if $S(N) = S(M)$, then $N = M$.

Axiom 5 (Principle of Mathematical Induction)
Let $P(N)$ be any property pertaining to a natural number N. Suppose $P(0)$ is true, and suppose that whenever $P(N)$ is true, $P(S(N))$ is also true.
Then $P(N)$ is true for every natural number N.

Recursive Definition
Suppose for each natural number N, we have a function f_n: $N \rightarrow N$ 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 $a_{s(N)} = f_n(a_n)$ for each natural number N.

Proof.
Using induction, prove base case, where $N = 0$.
Only 1 value of a_0, which makes $a_0 = c$.
(None of the other definitions $a_{s(n)} = f_n(a_n)$ will redefine the value of a_0, because of Axiom 3.
Thus, base case proven.

Suppose inductively that the procedure gives a single value to a_n. Then it gives a single value to $a_{s(n)} = f_n(a_n)$.
(None of the other definitions $a_{s(m)} = f_m(a_m)$ will redefine the value of $a_{s(n)}$, because of Axiom 4.
Induction completed. a_n is defined for each natural value n, with a single value assigned to each a_n.
□

Definition: Addition of Natural Numbers
Addition is a function that maps two natural numbers (two elements of N) to another one. It is defined recursively as:

$0 + m := m \rightarrow (1)$

$S(N) + m := S(N + m) \rightarrow (2)$

Example:

$0 + m = m$		(Definition 1)
$1 + m$	$= S(0) + m$	
	$= S(0 + m)$	(Definition 2)
	$= S(m)$	(Definition 1)
$2 + m$	$= S(1) + m$	
	$= S(1 + m)$	(Definition 2)
	$= S(m)$	

<u>Definition: Positive Natural Numbers</u>

A natural number N is said to be positive if and only if it is not equal to zero.

<u>Definition: Ordering of Natural Numbers</u>

Let N and M be natural numbers.

N □ M or $M \leq N$ if and only if $N = M + a$ for some natural number a.

N is strictly greater than M, $N > M$ or $M > N$ if and only if N □ M and $N \neq M$

$S(N) > N$ for any N, thus there is no largest natural number N.

<u>Definition: Multiplication of Natural Numbers</u>

Multiplication is a function mapping two natural numbers to another one. It is defined recursively as:

$0 \times m := 0 \rightarrow (1)$

$S(N) \times m := (N \times m) + m \rightarrow (2)$

Example:

$0 \times m = 0$	(by definition 1)
$1 \times m = S(0) \times m = (0 \times m) + m = m$	(by definition 2)

<u>Definition: Exponentiation of Natural Numbers</u>

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 $m^{s(n)} := m^n \times m$

Proposition 1: 3 is a natural number

Proof.
0 is a natural number. (Axiom 1)
S(0) = 1 is a natural number. (Axiom 2)
S(1) = 2 is also a natural number. (Axiom 2)
Hence, S(2) = 3 is a natural number. (Axiom 2)

Proposition 2: 4 is not equal to 0.

Proof.
By definition, 4 = S(3).
3 is a natural number. (Axiom 1 and 2, or Proposition 1)
S(3) $\neq$ 0 (Axiom 3)
Hence, 4 $\neq$ 0.

Proposition 3: 6 is not equal to 2.

Proof by contradiction.
Suppose 6 = 2. Then S(5) = S(1), which leads to 5 = 1. (Axiom 4)
S(4) = S(0)
Then, 4 = 0 (Axiom 4)
This contradicts Proposition 2.

Proposition 4: A certain property P(N) is true for every natural number N.

Using the Principle of Mathematical Induction (Axiom 5),

1. Verify base case, where $N = 0$
   Prove P(0).
2. Suppose inductively that P(N) is true for every natural number N.
   P(N) is proven.
3. Prove for P(S(N)).
   Insert proof here, assuming P(N) is true.

Closes induction, thus P(N) is true for every natural number N.

Proposition 5: The sum of two natural numbers is a natural number.

Proof.
Induct on m, keeping n fixed.
Let N be a natural number, $M + N$ is a natural number.

Proving base case, $M = 0$.

$0 + N = N$ (Addition Definition)

Since N is a natural number, the base case is proven.
Induction Step:
Suppose M is a natural number, $M + N$ is a natural number.

Prove $S(M) + N$ is a natural number.
$S(M) + N = S(M + N)$ (Addition Definition)

Since $M + N$ is a natural number (Induction Step)
$S(M + N)$ is also a natural number. (Axiom 2)

<u>Lemma 6: For any natural number M, $M + 0 = M$.</u>

Proof.
Prove base case, $M = 0$.
$0 + 0 = 0$ (Addition Definition 1: $0 + M = M$)
Base case is proven.

Induction case:
Suppose $M + 0 = M$

Prove $S(M) + 0 = S(M)$.
$S(M) + 0$
$= S(M + 0)$ (Addition Definition 2)
$= S(M)$ (Induction Step)

<u>Lemma 7: For any natural numbers N and M, $N + S(M) := S(N + M)$</u>

Proof.
Induction on N, keeping M fixed.
Base case, $N = 0$.
$0 + S(M)$
$= S(0 + M)$ (Addition Definition 2)
$= S(M)$ (Addition Definition 1)
Base Case is proven.

Induction case:
Suppose $N + S(M) := S(N + M)$.

Prove $S(N) + S(M) = S(S(N) + M)$.

LHS: $S(N) + S(M)$
$= S(N + S(M))$ (Addition Definition 2)
$= S(S(N + M))$ (Induction Case)

RHS: $S(S(N) + M)$
$= S(S(N + M))$ (Addition Definition 2)

Close induction.

Proposition 8: (Addition is Commutative) For any natural numbers N and M, $N + M = M + N$

Proof.
Induction on N, keeping M fixed.
Base case, $N = 0$.
LHS: $0 + M = M$ (Addition Definition 1)
RHS: $M + 0 = M$ (Lemma 6)

Hence, the base case is proven.

Induction Case:
Suppose $N + M = M + N$

Prove $S(N) + M = M + S(N)$
LHS: $S(N) + M$
$= S(N + M)$ (Addition Definition 2)
RHS: $M + S(N)$
$= S(M + N)$ (Lemma 7)
$= S(N + M)$ (Induction Step)

Close induction.

Proposition 9: (Addition is Associative) For any natural numbers A, B, C, $(A + B) + C = A + (B + C)$

Proof.
Induction on A, keeping B and C fixed.

Prove base case, $A = 0$
$(0 + B) + C = 0 + (B + C)$
LHS: $(0 + B) + C$
$= B + C$ (Addition Definition 1: $0 + M = M$)
RHS: $0 + (B + C)$
$= B + C$ (Addition Definition 1: $0 + M = M$)
Hence, $(0 + B) + C = 0 + (B + C)$ as required.

Induction Step:
Suppose $(A + B) + C = A + (B + C)$

Prove $(S(A) + B) + C = S(A) + (B + C)$
LHS: $(S(A) + B) + C$
$= S(A + B) + C$ (Addition Definition 2)
$= S(A + B + C)$ (Addition Definition 2)

RHS: $S(A) + (B + C)$

$= S(A + B + C)$ (Addition Definition 2)

Close induction.

Proposition 10: Cancellation Law. Let natural numbers *A, B, C such that* $A + B = A + C$, *implies* $B = C$

Proof.
Induction on A, keeping B and C fixed.

Prove base case, $A = 0$
$0 + B = 0 + C$
$B = C$ (Addition Definition 1)

Induction Step:
Suppose $A + B = A + C$, *implies* $B = C$

Prove $S(A) + B = S(A) + C$, *implies* $B = C$
$S(A + B) = S(A + C)$ (Addition Definition 2)
$A + B = A + C$ (Axiom 4)
$B = C$ is implied. (Induction Step)

Proposition 11: If A is positive and B is a natural number, then $A + B$ is positive (and hence so is $B + A$)

Proof.
Induction on B, keeping A fixed.

Prove base case, $B = 0$
$A + B = A + 0 = A$ (Lemma 6)
Since A is positive, the base case is proven.

Induction Step:
Suppose $A + B$ is positive

Prove $A + S(B)$ is positive.
$A + S(B) = S(A + B)$ (Lemma 7)
Since $S(A + B) \neq 0$ (Axiom 3), and $S(A + B)$ is a natural number (Axiom 2), hence $S(A + B)$ is positive. (Definition of Positive Numbers)

Corollary 12: If A and B are natural numbers such that $A + B = 0$, then $A = 0$ and $B = 0$.

Proof by Contradiction.

Suppose $A \neq 0$ *or* $B \neq 0$.

$A \neq 0$ shows that A is positive (Definition of Positive Numbers)
Hence, $A + B = 0$ is positive (Proposition 11).

Contradicts the Definition of Positive Numbers.

$B \neq 0$ then B is positive.
Hence, $A + B = 0$ is positive (Proposition 11).
Contradicts the Definition of Positive Numbers.

Therefore, $A = 0$ and $B = 0$

Lemma 13: Let A be a positive number. Then there exists exactly one natural number B such that $S(B) = A$.

Proof.

Prove the base case, $B = 0$.
$S(0) = 1$
0 is a natural number. (Axiom 1)
1 is also a natural number. (Axiom 2)
There can only be one unique successor for 0, which is 1. (Axiom 4)
Since 1 is also a positive number, the base case is proven.

Induction case: There exists exactly one natural number B such that $S(B)$ is a positive number.

Prove S(S(B)) is positive.

S(B) is positive (Induction case).
S(B) is natural. (Axiom 2)
S(S(B)) is also natural. (Axiom 2)
S(S(B)) is not zero. (Axiom 3)
Hence, S(S(B)) is positive. (Definition of Positive Numbers)

Proposition 14: (Basic Properties of Order for Natural Numbers)
Let A, B and C be natural numbers. Then

a. Order is reflexive. A □ A.

    Proof.

    Since A □ A, $A = A + n$ for some natural number n (Definition of Order)
    Let $n = 0$,
    $A + n$ *(0 is a natural number, Axiom 1)*
    $= A + 0$ *(Lemma 6)*
    $= A$
    Hence, A □ A *as required.*

b. Order is transitive. If $A \square B$ *and* $B \square C$ *, the* $A \square C$.

Proof.

$A = B + n$ *and* $B = C + m$ for some natural numbers n and m. (Definition of Order)
Hence, $A = C + (m + n)$. (Definition of Order)
Therefore, $A \square C$.

c. Order is antisymmetric. If $A \square B$ and $B \square A$, then $A = B$.

Proof.

$A \square B$ *implies* $A = B + n$
$B \square A$ *implies* $B = A + m$
$A =(A + m) + n$
$A = A + (m + n)$ (Associative Law)

$m + n$ is zero for the previous statement to be true. (Definition of Addition)
$m + n = 0$
Hence, $m = 0$ *and* $n = 0$ (Corollary 12)

As such, $A = B$.

d. (Addition preserves order) $A \square B$ *if and only if* $A + C \square B + C$

$A + C \square B + C$
$A + C = B + C + m$
$A = B + m$
Hence, $A \square B$ if and only if $A + C \square B + C$.

$A \square B$
$A = B + m$
$B + m + C \square B + C$
Hence, true by definition *and* $A + C \square B + C$ *if and only if* $A \square B$.

e. $A < B$ if and only if $S(A) \leq B$

$A < B$ *implies that* $B = A + d$*, where* $d > 0$. *(Definition of Order)*
$B = A + S(C)$
$B = S(A+C)$
$S(A+C) \square S(A)$
$B \square S(A)$
$S(A) \leq B$

f. $A < B$ *if and only if* $B = A + d$ *for some positive number* d.

$A < B$ implies that $B = A + d$, where $d > 0$. (Definition of Order)
Since $d > 0$, d is positive. (Definition of Positive Numbers)

or

$B = A + d$, *then* B □ A
Prove $B \neq A$.
Suppose for contradiction B = A, then by cancellation, d = 0.
Which means D is not positive, thus a contradiction.

Proposition 15: (Trichotomy of Order of Natural Numbers)
Let A and B be natural numbers. Then exactly one of the following statements is true: $A < B$, $A = B$, $B < A$.

Proof.
No more than one of the statements can hold true at the same time.

If $A < B$, then $A \neq B$.
If $B < A$, then $A \neq B$.

However, if $A < B$ *and* $B < A$, *then* $A = B$. *(Proposition 14).*
Hence, a contradiction with the two earlier statements.

One of the statements is true.
Induction on A, keep B fixed.
Base case:
When $A = 0$,
$0 \leq B$
Since B is a natural number, B might be zero. (Axiom 1)
So either $0 = B$ or $0 < B$.
The base case is proven.

Suppose $A < B$, $A = B$, $B < A$.

Prove S(A) for each statement.

$B < A$, *then* $B < S(A)$
$A = B + d$
$d = S(c)$ for some natural number c
$A = B + S(c)$
$A = S(B + c)$ *(Definition of Addition)*
$S(A) = S(S(B + c))$ (Axiom 4)
$B < S(S(B + c))$

If $A = B$, *then* $S(A) > B$.
$S(A) = S(B)$ (Axiom 4)
$S(B) > B$

If $A < B$,
$S(A) \leq B$ (Proposition 14e)
Then either $S(A) = B$ or $S(A) < B$.

Close induction.

Proposition 16 (Strong Principle of Induction)
Let m0 be a natural number, and let P(m) be a property pertaining to an arbitrary natural number m. Suppose that for each m ≥ m0, we have the following implication: if P(m) is true for all natural numbers m0 ≤ m < m, then P(m) is also true. (In particular, this means that P(m0) is true, since in this case the hypothesis is vacuous.) Then we can conclude that P(m) is true for all natural numbers m ≥ m0.

Hints: Define Q(n) to be the property that P(m) is true for all m0 ≤ m < m; note that Q(n) is vacuously true when n < m0.

Proof.

Let Q(n) be the property that P(m) is true for all m0 ≤ m < n. Given this definition of Q, we can restate the hypothesis for P as follows: for each m ≥ m0, if Q(M) is true then P(M) is also true. We will prove by induction that Q(n) is true for all natural numbers n.

We first want to show Q(0), which says that P(m) is true for all m0 ≤ m < m. This is vacuously true since there is no natural number strictly less than zero: m < 0 means m ≤ 0 and m ≠ 0. So we have some natural number a such that 0 = m + a, but this means m = 0 by Corollary 2.2.9, which contradicts the fact that m ≠ 0. So P(m) is true for all such numbers, because none exist.

Now suppose inductively that we have shown Q(n) is true. We want to show that Q(S(n)) is true, i.e. we want to show that P(m)is true for all m0 ≤ m < S(n). So let m be a natural number and suppose m0 ≤ m < S(n). Our goal is to show that P(m) is true.

Since m0 ≤ m < S(n), we claim that either m0 ≤ m < n or m = n. This is because m < S(n) implies S(m) ≤ S(n) by Proposition 2.2.12(e) which implies m ≤ n by Proposition 2.2.12(d). We know m = n or m ≠ n; in the latter case we thus have m < n, so m0 ≤ m < n. Thus we see that either m0 ≤ m < n or m = n.

Since Q(n) is true, we know that P(m) is true for all m0 ≤ m < n. Thus in the case where m0 ≤ m < n, we already know that P(m) is true

To complete the proof we must show that P(m) is true in the case m = n, i.e. we must show that P(n) is true. Since m0 ≤ m < S(n), by transitivity of order m0 < S(n), so m0 ≤ S(n) which means m0 ≤ n. Since m0 ≤ n, we can use the hypothesis for P, which says that if Q(n) is true then P(n) is also true. Since Q(n) is true by inductive hypothesis, we see that P(n) is true as desired.

This completes the induction, and we have that Q(n) is true for all natural numbers n. Our original goal was to show that P(m) is true for all natural numbers m ≥ m0. So let m ≥ m0. Then we know that Q(S(M) is true. Since m0 ≤ m < S(m), we see that P(m) is true as required.

Source: https://taoanalysis.wordpress.com/2020/04/01/exercise-2-2-5/

Proposition 17: Principles of Backwards Induction
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.
For the statement to prove via induction, use the following: if P(n) is true, then P(m) is true for all $m \leq n$.

Let P be a property pertaining to the natural numbers such that whenever P(S(m)) is true, P(m) is true.

Let Q(n) be the following statement: if P(n) is true, then P(m) is true for all $m \leq n$.

We shall show that Q(n) is true for all n using induction. For the base case, we must show Q(0). So suppose that P(0) is true. We want to show that P(m) is true for all $m \leq 0$. By definition of inequality (definition 2.2.11), $m \leq 0$ means that $0 = m + a$ for some natural number a . By corollary 2.2.9, we have $m = 0$. In other words, $m \leq 0$ implies $m = 0$, so showing that P(m) for all $m \leq 0$ is equivalent to showing P(0), which we already know. This completes the base case.

Now suppose Q(n) is true. We must show that Q(S(n)) is true. So suppose that P(S(n)) is true. We need to show that P(m) is true for all $m \leq S(n)$. We know that whenever P(S(m))is true, P(m) is true, so for $m = n$ in particular this means that if P(S(n)) is true then P(n) is true. Since P(S(n)) is true, we see that P(n) is true. By the induction hypothesis we thus have P(m) for all $m \leq n$. Now let $m \leq S(n)$. We want to show that P(m) is true. If we can show that $m \leq n$ or $m = S(n)$, then we will be done, because in either case we have already shown that P(m) is true. To show that $m \leq n$ or $m = S(n)$, we will show that $m \neq S(n)$ implies $m \leq n$. Suppose $m \neq S(n)$. This means $m < S(n)$ by definition 2.2.11. By proposition 2.2.12(e), we have $S(m) \leq S(n)$, i.e. $m + 1 \leq n + 1$. By proposition 2.2.12(d) this means $m \leq n$ as required. This closes the induction.

Now let n be a natural number, and suppose P(n) is true. By our work above, we know that Q(n) is true. This means that P(m) is true for all natural numbers $m \leq n$ as required.

Source: https://taoanalysis.wordpress.com/2020/03/16/exercise-2-2-6/

Proposition 18: (Multiplication is commutative). Let N, M be natural numbers. Then $N \times M = M \times N$.

Prove $0 \times M = M \times 0$

Base case: $M = 0$
LHS: $0 \times 0 = 0$ (Multiplication Definition 1)
RHS: $0 \times 0 = 0$
The base case is proven.

Induction case:
Assume $0 \times M = M \times 0$

Prove for $S(M)$
$0 \times S(M) = S(M) \times 0$

LHS: $0 \times S(M) = 0$ (Multiplication Definition 1)
RHS: $S(M) \times 0 = (M \times 0) + 0 = 0 + 0 = 0$ (Multiplication Definition 2, Induction Case)
Close induction. Proven that $0 \times M = M \times 0$

Prove that $M \times S(N) = (M \times N) + M$

Induction on M, keep N fixed.
Base case: $M = 0$

$0 \times S(N) = (0 \times N) + 0$
LHS: $0 \times S(N) = 0$ (Multiplication Definition 1)
RHS: $(0 \times N) + 0 = 0$
Base case is proven.

Assume that $M \times S(N) = (M \times N) + M$

Prove for $S(M)$
$S(M) \times S(N) = (S(M) \times N) + S(M)$
LHS: $S(M) \times S(N)$
$= (M \times S(N)) + S(M)$ (Multiplication Definition 2)
$= ((M \times N) + M) + S(M)$ (Induction Case)
$= (M \times N) + M + S(M)$
RHS: $(S(M) \times N) + S(M)$
$= (N \times M) + M + S(M)$ (Multiplication Definition 2)
Close induction. Proven that $M \times S(N) = (M \times N) + M$

Proof.
Induction on N, keep M fixed.

Base case when $N = 0$.
LHS: $0 \times M = 0$ (Multiplication Definition 1)
RHS: $M \times 0 = 0$ (Proven earlier)

Induction Case:
Assume $N \times M = M \times N$

Prove for $S(N)$
LHS: $S(N) \times M = (N \times M) + M$ (Multiplication Definition 2)
RHS: $M \times S(N)$

$= (M \times \mathrm{N}) + \mathrm{M}$ (Proven earlier)
$= (N \times M) + \mathrm{M}$ (Induction case)

Close induction. Proven that $N \times M = M \times N$

Lemma 19: (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 by Contradiction.
Assuming that $n \neq 0$ and $m \neq 0$, n and m are both positive. (Definition of Natural Numbers)
$n = \mathrm{S}(p)$ so $n \times m = \mathrm{S}(p) \times m = (p \times m) + m = 0$
So, $(p \times m) = 0$ and $m = 0$ (Corollary 12)
Contradiction since m is positive (Definition of Natural Numbers)
So at least one of n, m is equal to zero.

Prove that at least one of n, m is equal to zero, then $n \times m = 0$.
If $m = 0$, then $n \times 0 = 0$ (Commutative Law)
If $n = 0$, the $0 \times m = 0$ (Multiplication Definition 1)

Prove that the multiplication of natural numbers n and m is also a natural number.

Base case, $n = 0$.
$0 \times m = 0$
Thus, the base case is proven.

Assume multiplication of natural numbers n and m is also a natural number.

Since $n = \mathrm{S}(p)$ so $n \times m = \mathrm{S}(p) \times m = (p \times m) + m$ is a natural number, since $(p \times m)$ is a natural number. (Induction case)

Prove that if n and m are both positive, then nm is also positive.

nm is a natural number, so let $nm = 0$.
As proven earlier, at least one of n, m is equal to zero, then $n \times m = 0$.
But n and m are both positive, thus a contradiction.

Proposition 20: (Distributive law). For any natural numbers a, b, c, we have $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Proof.
Since multiplication is commutative, show only the first statement.
Prove base case, $c = 0$.
LHS: $a(b + 0) = ab$
RHS: $ab + a0 = ab + 0 = ab$
The base case is proven.

Assume that $a(b + c) = ab + ac$

Proven for S(c)
LHS: $a(b + S(c)) = a(S(b+c)) = a(b + c) + a = ab + ac + a$
RHS: $ab + aS(c) = ab + a(c+1) = ab + ac + a$

Proposition 21: (Multiplication is associative). For any natural numbers $a, b, c,$ we have $(a \times b) \times c = a \times (b \times c)$.

Proof.

Prove base case, $c = 0$.
LHS: $(a \times b) \times 0 = a \times b$ (Proven earlier)
RHS: $a \times (b \times 0) = a \times 0 = a$ (Multiplication Definition)

Proposition 22: (Multiplication preserves order). If a, b are natural numbers such that $a < b$, and c is positive, then $ac < bc$.

Proof.
Since $a < b$, then $b = a + d$ for some positive d.
Multiply both sides by c, $bc = ac + dc$
Since d *and* c are both positive, then dc is also positive. *(Lemma 19)*
So $ac < bc$ as desired.

Corollary 23: (Cancellation law). Let a, b, c be natural numbers such that $ac = bc$ and c is non-zero. Then $a = b$.

Proof.
By the trichotomy of order, (Proposition 15) $A < B$ *and* $B < A$, *then* $A = B$.
Suppose that $A > B$, then $AC > BC$, hence a contradiction. (Proposition 22)
Suppose that $A < B$, then $AC < BC$, hence a contradiction.
$A = B$ is the only possibility.

Proposition 2.3.9 (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.
Fix q and induct on n.
Prove the base case, $n = 0$.
$0 = mq + r$
Hence, r and m are 0, (Corollary 12)
So $0 \leq 0 < q$ which is true.

Now suppose inductively that there are natural numbers m, r such that $0 \leq r < q$ and $n = mq + r$.

We must show that there are natural numbers m', r' such that $0 \leq r' < q$ and $n + 1 = m'q + r'$.

We have two cases, $r + 1 = q$ and $r + 1 \neq q$. If $r + 1 = q$, we can take $m' := m + 1$ and $r' := 0$. Then $0 \leq r' = 0 < q$ and we have $m'q + r'$ equal to $(m+1)q + 0$ by definition of m', r', which equals $mq + q$ by the distributive law, which equals $mq + r + 1$ by using $q = r + 1$, which equals $n + 1$ by the inductive hypothesis $n = mq + r$. Thus $m' q + r' = n + 1$ as required.

Now suppose $r + 1 \neq q$. In this case, $r < q$ from the inductive hypothesis gives $r + 1 \leq q$, so $r + 1 < q$. So we can take $r' := r + 1$ and $m' := m$. Now $0 \leq r' < q$ by what we just showed, and $m' q + r' = mq + r + 1 = n + 1$ by definition of m', r' and the inductive hypothesis $n = mq + r$.

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

Proof.
$(a + b)^2 = (a + b)^1(a + b) = (a + b)(a + b)$ (Definition of Exponentiation)

$(a + b)(a + b)$

$= a(a + b) + b(a + b)$ (Distributivity Law)

$= aa + ab + ba + bb$ (Commutative Law)

$= a^2 + ab + ab + b^2$ (Definition of Exponentiation)

Show that *ab + ab = 2ab*

$2ab = 2 \times ab = (1 \times ab) + ab = ab + ab$

$= a^2 + 2ab + b^2$