Natural numbers

In the beginning there were the natural numbers

\[ \mathbb{N} : 0, 1, \ldots, n, n+1, \ldots \]

generated from zero by successive increment; that is, put in ML:

```ml
datatype
    N = zero | succ of N
```

The basic operations of this number system are:

- **Addition**

- **Multiplication**
The *additive structure* \((\mathbb{N}, 0, +)\) of natural numbers with zero and addition satisfies the following:

- **Monoid laws**
  
  \[
  0 + n = n = n + 0 \quad \text{and} \quad (l + m) + n = l + (m + n)
  \]

- **Commutativity law**
  
  \[
  m + n = n + m
  \]

and as such is what in the mathematical jargon is referred to as a *commutative monoid*. 
Also the *multiplicative structure* \((\mathbb{N}, 1, \cdot)\) of natural numbers with one and multiplication is a commutative monoid:

- **Monoid laws**
  
  \[ 1 \cdot n = n = n \cdot 1, \quad (l \cdot m) \cdot n = l \cdot (m \cdot n) \]

- **Commutativity law**
  
  \[ m \cdot n = n \cdot m \]
The additive and multiplicative structures interact nicely in that they satisfy the

- **Distributive law**

\[ l \cdot (m + n) = l \cdot m + l \cdot n \]

and make the overall structure \((\mathbb{N}, 0, +, 1, \cdot)\) into what in the mathematical jargon is referred to as a **commutative semiring**.
Cancellation

The additive and multiplicative structures of natural numbers further satisfy the following laws.

- **Additive cancellation**
  
  For all natural numbers $k, m, n$,
  
  $$k + m = k + n \implies m = n.$$  

- **Multiplicative cancellation**
  
  For all natural numbers $k, m, n$,
  
  if $k \neq 0$ then $k \cdot m = k \cdot n \implies m = n$. 

Inverses

Definition 41

1. A number $x$ is said to admit an **additive inverse** whenever there exists a number $y$ such that $x + y = 0$. 
Inverses

Definition 41

1. A number $x$ is said to admit an additive inverse whenever there exists a number $y$ such that $x + y = 0$.

2. A number $x$ is said to admit a multiplicative inverse whenever there exists a number $y$ such that $x \cdot y = 1$. 
Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:
Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

(i) the **integers** 

\[ \mathbb{Z} : \ldots -n, \ldots, -1, 0, 1, \ldots, n, \ldots \]

which then form what in the mathematical jargon is referred to as a **commutative ring**, and

(ii) the **rationals** \( \mathbb{Q} \) which then form what in the mathematical jargon is referred to as a **field**.
The division theorem and algorithm

Theorem 42 (Division Theorem)  For every natural number $m$ and positive natural number $n$, there exists a unique pair of integers $q$ and $r$ such that $q \geq 0$, $0 \leq r < n$, and $m = q \cdot n + r$. 
The division theorem and algorithm

Theorem 42 (Division Theorem) For every natural number \( m \) and positive natural number \( n \), there exists a unique pair of integers \( q \) and \( r \) such that \( q \geq 0 \), \( 0 \leq r < n \), and \( m = q \cdot n + r \).

Definition 43 The natural numbers \( q \) and \( r \) associated to a given pair of a natural number \( m \) and a positive integer \( n \) determined by the Division Theorem are respectively denoted \( \text{quo}(m, n) \) and \( \text{rem}(m, n) \).
The Division Algorithm in ML:

```ml
fun divalg( m, n )
  = let
    fun diviter( q, r )
      = if r < n then ( q, r )
         else diviter( q+1, r-n )
    in
    diviter( 0, m )
  end

fun quo( m, n ) = #1( divalg( m, n ) )
fun rem( m, n ) = #2( divalg( m, n ) )
```
Theorem 44  For every natural number $m$ and positive natural number $n$, the evaluation of $\text{divalg}(m, n)$ terminates, outputing a pair of natural numbers $(q_0, r_0)$ such that $r_0 < n$ and $m = q_0 \cdot n + r_0$.

Proof: