The division theorem and algorithm

Theorem 53 (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 54 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 $\text{rem}(m, n)$.
PROOF OF Theorem 53:

\[0 \leq m - qn < n\]

\[m = i \cdot n + r_i\]
The Division Algorithm in ML:

\[ \text{divalg}(m, n) = \text{diviter}(0, m) \]

\[
\begin{align*}
\text{fun divalg}(m, n) &= \text{let} \\
\quad \text{fun diviter}(q, r) &= \text{if } r < n \text{ then } (q, r) \\
\quad &\quad \text{else diviter}(q+1, r-n) \\
\quad \text{in} \\
\quad \text{diviter}(0, m) \end{align*}
\]

\[ \text{fun quo}(m, n) = \#1(\text{divalg}(m, n)) \]

\[ m = q \cdot n + r \quad \Rightarrow \quad m = (q+1) \cdot n + (r-n) \]

\[ \text{fun rem}(m, n) = \#2(\text{divalg}(m, n)) \]

\[ (\star) \quad \text{NB: } m = \text{first arg of } \text{diviter} \times n \]  
\[ \quad + \text{second arg of } \text{diviter} \]  

\[ \text{NB: Suppose } (\star) \text{ holds for } \text{diviter}(q, r) \]

Then it also holds for \[ \text{diviter}(q+1, r-n) \].
Theorem 56  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:**

$$
\begin{align*}
\text{divalg}(q, r) & \quad r \geq 0 \\
\text{r < n} & \quad r > n \quad r - n \geq 0 \\
(q, r) & \quad \text{divalg}(q+1, r-n)
\end{align*}
$$

For all calls of $\text{divalg}(a, b)$ we have $m = a \cdot n + b$.
Proposition 57  Let $m$ be a positive integer. For all natural numbers $k$ and $l$,

$$k \equiv l \pmod{m} \iff \text{rem}(k, m) = \text{rem}(l, m)$$

**Proof:** Let $m$ be a positive integer. Consider natural numbers $k$ and $l$.

$(\Rightarrow)$ \[ k = \text{quo}(k, m) \cdot m + \text{rem}(k, m) \]

\[ l = \text{quo}(l, m) \cdot m + \text{rem}(l, m) \]

Assume $k = l$ Then \[ \text{rem}(k, m) = \text{rem}(l, m) \]

and \[ \text{rem}(k, m) = \text{rem}(l, m) \]

$(\Leftarrow)$ Exercise.
Corollary 58 Let \( m \) be a positive integer.

1. For every natural number \( n \),
   \[
   n \equiv \text{rem}(n, m) \pmod{m}.
   \]

2. For every integer \( k \) there exists a unique integer \([k]_m\) such that \( 0 \leq [k]_m < m \) and \( k \equiv [k]_m \pmod{m} \).

PROOF:

(2) Say \( k \) is a nat. Then \([k]_m = \text{rem}(k, m)\). For \( k < 0 \) an integer, \([k]_m = [k + am]_m\)

\[ [k]_m = m - \text{rem}(-k, m) \text{ if } \text{rem}(-k, m) \neq 0 \text{ for a s.t. } \]

Exercise. \[ 0 \quad m \quad k+am \geq 0 \]

\[ \not\exists \]

\[ 182-a \]
Modular arithmetic

For every positive integer $m$, the integers modulo $m$ are:

$$\mathbb{Z}_m : 0, 1, \ldots, m-1.$$ 

with arithmetic operations of addition $+_m$ and multiplication $\cdot_m$ defined as follows

$$k+_m l = [k+l]_m = \text{rem}(k+l, m),$$

$$k \cdot_m l = [k \cdot l]_m = \text{rem}(k \cdot l, m)$$

for all $0 \leq k, l < m$. 
For \( k \) and \( l \) in \( \mathbb{Z}_m \),
\[
  k +_m l \quad \text{and} \quad k \cdot_m l
\]
are the unique modular integers in \( \mathbb{Z}_m \) such that
\[
  k +_m l \equiv k + l \pmod{m} \\
  k \cdot_m l \equiv k \cdot l \pmod{m}
\]
Example 60  The addition and multiplication tables for $\mathbb{Z}_4$ are:

\[
\begin{array}{c|cccc}
+ & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2 \\
\end{array}
\quad
\begin{array}{c|cccc}
\cdot & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 \\
2 & 0 & 2 & 0 & 2 \\
3 & 0 & 3 & 2 & 1 \\
\end{array}
\]

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.
From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

<table>
<thead>
<tr>
<th>additive inverse</th>
<th>multiplicative inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>2</td>
<td>-2</td>
</tr>
<tr>
<td>3</td>
<td>-3</td>
</tr>
</tbody>
</table>

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.
Example 61 *The addition and multiplication tables for $\mathbb{Z}_5$ are:*

\[
\begin{array}{c|ccccc}
+_{5} & 0 & 1 & 2 & 3 & 4 \\
\hline
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 0 & 1 \\
3 & 3 & 4 & 0 & 1 & 2 \\
4 & 4 & 0 & 1 & 2 & 3 \\
\end{array}
\quad \quad
\begin{array}{c|ccccc}
\cdot_{5} & 0 & 1 & 2 & 3 & 4 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & 3 & 4 \\
2 & 0 & 2 & 4 & 1 & 3 \\
3 & 0 & 3 & 1 & 4 & 2 \\
4 & 0 & 4 & 3 & 2 & 1 \\
\end{array}
\]

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.
From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

<table>
<thead>
<tr>
<th>additive inverse</th>
<th>multiplicative inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Surprisingly, every non-zero element has a multiplicative inverse.
Proposition 62  For all natural numbers $m > 1$, the modular-arithmetic structure

$$(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$$

is a commutative ring.

**NB** Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses.
Proposition 63  Let $m$ be a positive integer. A modular integer $k$ in $\mathbb{Z}_m$ has a reciprocal if, and only if, there exist integers $i$ and $j$ such that $k \cdot i + m \cdot j = 1$.

PROOF:  Let $m$ be a positive integer.

Let $k$ be a natural number smaller than $m$.

($\Rightarrow$) Let $l$ be a reciprocal of $k$; that is, $0 \leq l < m$ and $k \cdot l \equiv 1 \pmod{m}$. In other words, $k \cdot l - 1 = j \cdot m$ for some int. $j$.

Then, $k \cdot l + (-j) \cdot m = 1$ and $i_0 = l$ and $j_0 = -j$ are int. with the property $k \cdot i_0 + m \cdot j_0 = 1$. 

— 192 —
(⇐) Assume: \( \exists i, j, \text{int. } k \cdot i + m \cdot j = 1 \) (*)

\[
RTD: \exists \ell \text{ in } \mathbb{Z}_m. \ k \cdot \ell \equiv 1 \pmod{m}.
\]

From (*), let \( i_0, j_0 \) be integers such that

\[
k \cdot i_0 + m \cdot j_0 = 1
\]

Then,

\[
1 = k \cdot i_0 + m \cdot j_0 \equiv k \cdot i_0 \pmod{m}
\]

and consider \( \ell = [i_0]_m \) in \( \mathbb{Z}_m \)

So \( 1 \equiv k \cdot i_0 \equiv k \cdot \ell \pmod{m}. \) \( \Box \)
**Definition 64** An integer $r$ is said to be a **linear combination** of a pair of integers $m$ and $n$ whenever there are integers $s$ and $t$ such that $s \cdot m + t \cdot n = r$.

**Proposition 65** Let $m$ be a positive integer. A modular integer $k$ in $\mathbb{Z}_m$ has a reciprocal if, and only if, $1$ is an integer linear combination of $m$ and $k$. 