The division theorem and algorithm

Theorem 43 (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* $m = q \cdot n + r$.

$\forall$ nat. m, pos. nat. n. Existence:

$(\exists$ int $q, r.\ q \geq 0,\ 0 \leq r < n,\ m = q \cdot n + r)$

Uniqueness.

$$\wedge \left[\forall q, q', r, r'.\ q, q' \geq 0,\ 0 \leq r, r' < n,\ m = q \cdot n + r \wedge m = q' \cdot n + r' \implies (q = q' \wedge r = r') \right]$$

Uniqueness

Assume nat. m, pos. nat. n.

Assume q, q', r, r'. $q, q' \geq 0$, $0 \leq r, r' < n$, (3)

$m = q \cdot n + r$ (1) $\wedge$ $m = q' \cdot n + r'$ (2)

RTP: $q = q' \wedge r = r'$

From (1) and (2) $(q - q')n = r' - r$ (4)

Case (i): Suppose $r' \geq r$. So that $r' - r$ is a natural..

That by (3) is $< n$, and by (4) is a multiple of n..

Therefore $q - q' = 0$ and hence $q = q'$.

$q \cdot n + r = m = q \cdot n + r'$ As $q = q'$

By cancellation, $r = r'$.

Case $r \geq r'$: Consider $(q' - q) \cdot n = r - r'$ and proceed analogously.

$\boxtimes$

The division theorem and algorithm

Theorem 43 (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 44 *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 $\mathrm{quo}(m, n)$ and $\mathrm{rem}(m, n)$.*

PROOF OF Theorem 43:

$$
\begin{tikzcd}[column sep=small]
 & \mathrm{divalg}(m,n) \arrow[d, phantom, "\shortparallel"] & & & \\
 & \mathrm{diviter}(0,m) \arrow[dl, "m<n"'] \arrow[dr] & & & \\
(0,m) & & \mathrm{diviter}(1,m-n) \arrow[dl, "m-n<n"'] \arrow[dr] & & \\
 & (1,m-n) & & \mathrm{diviter}(2,m-2n) \arrow[dl, "m-2n<n"'] \arrow[dr] & \\
 & & (2,m-2n) & & \ddots
\end{tikzcd}
$$

Partial Correctness

$m = 0 \cdot n + m$ ✓

$\text{diviter}(0, m)$

$m < n$

$(0, m)$

$\text{diviter}(q_i, r_i)$

$r_i < n$

(q_i, r_i)

$\text{diviter}(q_{i+1}, r_{i+1})$

where $q_{i+1} = q_i + 1$

$r_{i+1} = r_i - n$

__Assume__

$m = q_i \cdot n + r_i$

__RTP__:

$m \overset{?}{=} q_{i+1} \cdot n + r_{i+1}$ ✓

$$(q_i + 1) \cdot n + (r_i - n)$$

$$\|$$

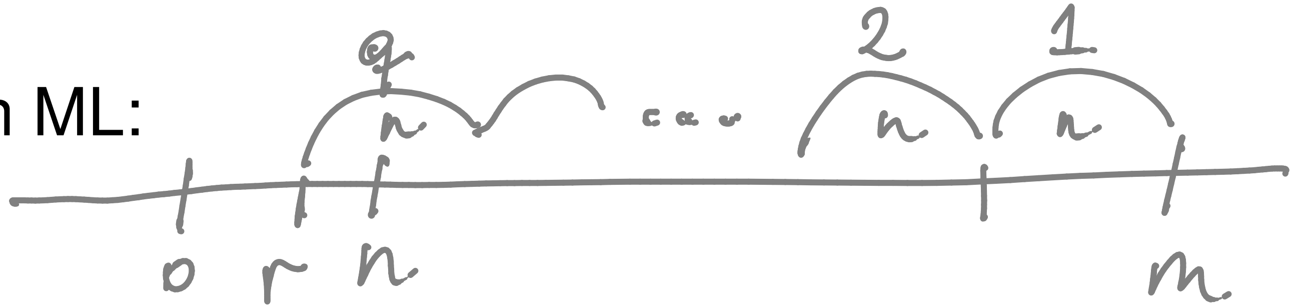
$$q_i \cdot n + n + r_i - n = q_i \cdot n + r_i = m$$

If the computation terminates in step k then
$m = q_k \cdot n + r_k$ and $r_k < n$.

Total correctness: We need show the algorithm terminates. At each call of <u>diviter</u>(q, r) either $r < n$ an we are done or we have a call <u>diviter</u>$(q+1, r-n)$ with smaller, but positive, second argument.

$\boxtimes$

The Division Algorithm in 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
```

$$\boxed{\begin{array}{c} 0 \leq q,\quad 0 \leq r < n \\ m = q \cdot n + r \end{array}}$$

```
fun quo( m , n ) = #1( divalg( m , n ) )

fun rem( m , n ) = #2( divalg( m , n ) )
```

Theorem 45 *For every natural number* m *and positive natural number* n*, the evaluation of* $\texttt{divalg}(m, n)$ *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:

$$k = \underline{quo}(k,m)\cdot m + \underline{rem}(k,m)$$

Proposition 46 *Let* m *be a positive integer. For all natural numbers* k *and* l*,* $l = \underline{quo}(l,m)\cdot m + \underline{rem}(l,m)$

$$k \equiv l \pmod{m} \iff \mathrm{rem}(k,m) = \mathrm{rem}(l,m) \quad .$$

PROOF: Let m be a positive integer. Let k, l be nat.

($\Leftarrow$) Easy.

($\Rightarrow$) Assume $k - l = i\cdot m$ for some i int.

$$\begin{aligned} k - l &= i\cdot m \\ &\| \\ &\left(\underline{quo}(k,m) - \underline{quo}(l,m)\right)\cdot m + \left(\underline{rem}(k,m) - \underline{rem}(l,m)\right) \end{aligned}$$

Then $\underline{rem}(k,m) - \underline{rem}(l,m) = 0$

So $\underline{rem}(k,m) = \underline{rem}(l,m)$. $\boxtimes$

Corollary 47 *Let m be a positive integer.*

1. *For every natural number n,*

$$n \equiv \mathrm{rem}(n, m) \pmod{m} \quad .$$

Since

$$n = \underline{\mathrm{quo}}(n, m) \cdot m + \underline{\mathrm{rem}}(n, m)$$

we have $n - \mathrm{rem}(n, m)$ is a multiple of m $\boxtimes$

PROOF:

Corollary 47 *Let m be a positive integer.*

1. *For every natural number n,*

$$n \equiv \mathrm{rem}(n, m) \pmod{m} \quad .$$

2. *For every integer k there exists a unique integer $[k]_m$ such that*

$$0 \leq [k]_m < m \quad \textit{and} \quad k \equiv [k]_m \pmod{m} \quad .$$

PROOF:

Idea