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

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

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* $\mathtt{divalg}(m, n)$ *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:

Proposition 45 *Let* m *be a positive integer. For all natural numbers* k *and* l*,*

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

PROOF:

Corollary 46 *Let m be a positive integer.*

1. *For every natural number n,*

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

PROOF:

Corollary 46 *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:

Modular arithmetic

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

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

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

$$\begin{aligned} k +_m l &= [k+l]_m = \mathrm{rem}(k+l, m) \;, \\ k \cdot_m l &= [k \cdot l]_m = \mathrm{rem}(k \cdot l, m) \end{aligned}$$

for all $0 \leq k, l < m$.

Example 48 *The addition and multiplication tables for* $\mathbb{Z}_4$ *are:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

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:

	additive inverse
0	0
1	3
2	2
3	1

	multiplicative inverse
0	—
1	1
2	—
3	3

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.

Example 49 *The addition and multiplication tables for* $\mathbb{Z}_5$ *are:*

$+_5$	0	1	2	3	4
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

$\cdot_5$	0	1	2	3	4
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

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:

	additive inverse
0	0
1	4
2	3
3	2
4	1

	multiplicative inverse
0	—
1	1
2	3
3	2
4	4

Surprisingly, every non-zero element has a multiplicative inverse.

Proposition 50 *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

.