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* $m = q \cdot n + r$.

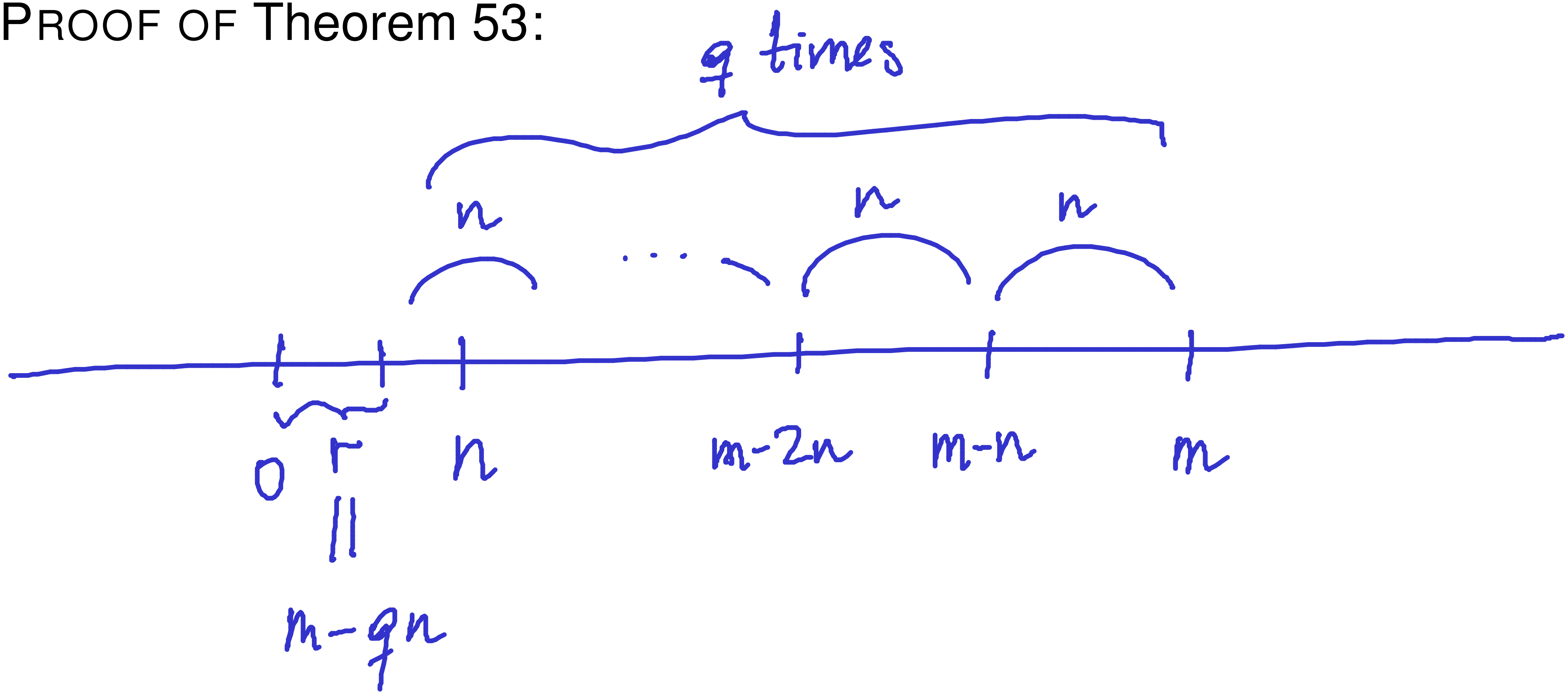
Let m be a nat. and n be a pos. nat.
For uniqueness, assume $q \geq 0$ and (3) $0 \leq r < n$ int. s.t.
(1) $m = q \cdot n + r$ and also $q' \geq 0$ and (4) $0 \leq r' < n$ int. s.t.
(2) $m = q' \cdot n + r'$. We show $q = q'$ and $r = r'$. By (1), $m \equiv r \pmod{n}$
and, by (2), $m \equiv r' \pmod{n}$. Then, $r \equiv r' \pmod{n}$. From (3) and (4),
by a previous result $r = r'$. Moreover $(q - q') \cdot n = r' - r = 0$ and
$q = q'$. $\boxtimes$

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

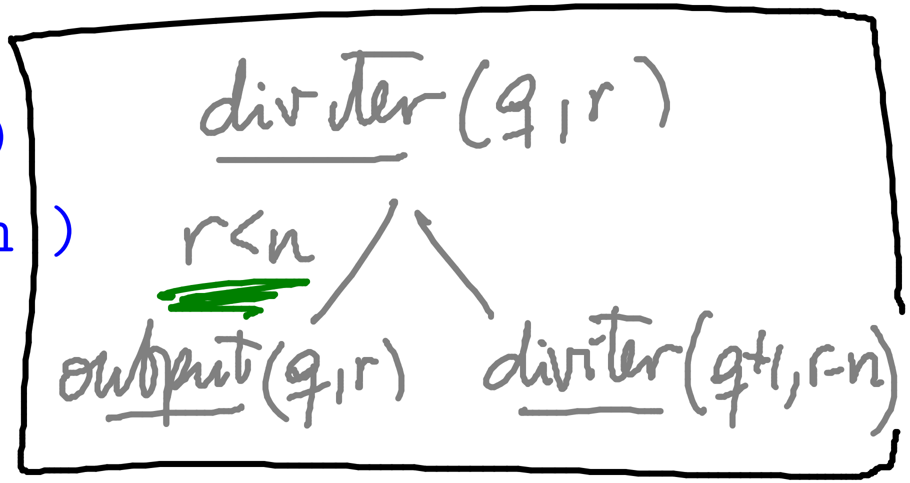
Proof of Theorem 53:



The Division Algorithm in ML:

$\mathrm{divalg}(m,n) = (q,r)$
s.t. $m = q\cdot n + r$ with $0 \le r < n$
whenever $m \geq 0$, $n \geq 1$ int.

```
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
```



$\rightsquigarrow \mathrm{divalg}(m,n) = \mathrm{diviter}(0,m)$

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

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

Termination argument:

$\mathrm{divalg}(m,n)$
$=$
$\mathrm{diviter}(0,m)$

$\mathrm{output}(0,m)$ $\quad$ $\mathrm{diviter}(1,m-n)$

…

$\mathrm{diviter}(q,r)$

$r<n$: $\mathrm{output}(q,r)$ $\quad$ $r \geq n$: $\mathrm{diviter}(q+1,r-n)$

…

NB: The second argument always decreases strictly whilst remaining natural.

Claim:
INVARIANT:
In each call of $\mathrm{diviter}(q,r)$ we have that $m = q\cdot n + r$ is satisfied.

Indeed: (1) in $\mathrm{diviter}(0,m)$ we have $m = 0\cdot n + m$; and (2) if this holds for $\mathrm{diviter}(q,r)$ then it hold for $\mathrm{diviter}(q+1,r-n)$.

Theorem 56 *For every natural number* m *and positive natural number* n*, the evaluation of* $\texttt{divalg}(m, n)$ *terminates, outputting a pair of natural numbers* (q_0, r_0) *such that* $r_0 < n$ *and* $m = q_0 \cdot n + r_0$*.*

PROOF:

Proposition 57 *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 58 *Let* m *be a positive integer.*

1. *For every natural number* n*,*

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

2. *For every integer* k *there exists a unique integer* $[\mathrm{k}]_{\mathrm{m}}$ *such that*

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

PROOF:

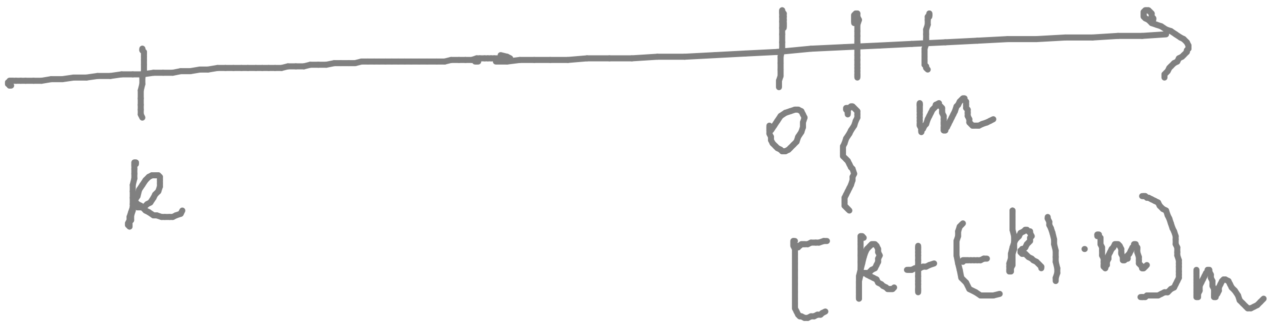
(2) If k is nat. Then $[k]_m = \mathrm{rem}(k,m)$

If k neg. int. Then

$k \equiv k + i \cdot m \pmod m$

$k \equiv k + (-k) \cdot m \pmod m$

$k \equiv [k + (-k) \cdot m]_m$



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 $0 \leq k, l < m$.

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:*

$+_4$	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 61 *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 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:

1 is an int. linear combination of k and m

cf. $(k \ m)\begin{pmatrix} i \\ j \end{pmatrix} = ki + mj$