DIVISION THEOREM AND ALGORITHM

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

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:

<u>Uniqueness</u> Let

$$\left.\begin{array}{ll} m = q_1 \cdot n + r_1 & 0 \le r_1 < n \\ m = q_2 \cdot n + r_2 & 0 \le r_2 < n \end{array}\right] (*)$$

<u>RTP</u> $r_1 = r_2$ and $q_1 = q_2$

From $(*)$, we have $m \equiv r_1 \pmod n$ $\quad 0 \le r_1 < n$

and $m \equiv r_2 \pmod n$ $\quad 0 \le r_2 < n$

Therefore, by a previous proposition, $r_1 = r_2$.

Moreover, $q_1 n = q_2 n$ and, by cancellation, $q_1 = q_2$.

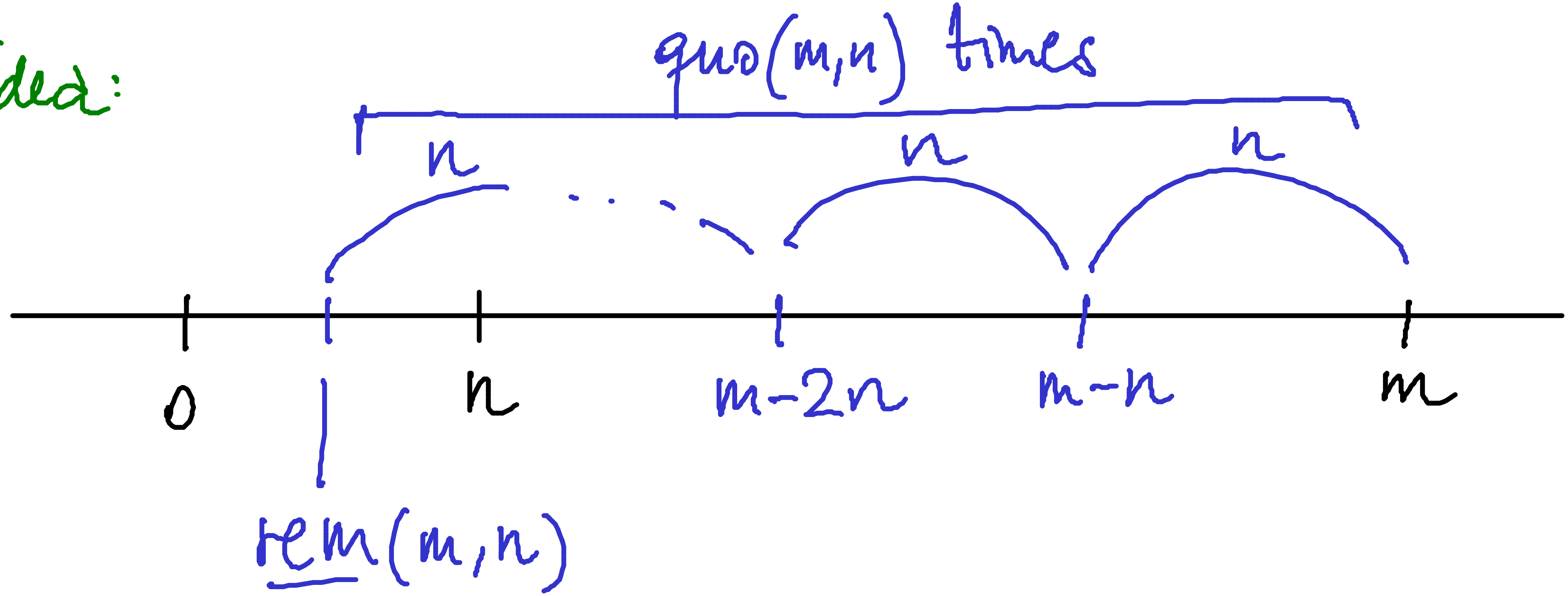
Given a natural number m and a positive integer n, it remains to show that there are natural numbers $\underline{quo}(m,n)$ and $\underline{rem}(m,n)$, the latter below n, such that

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

We will in fact compute them by means of the

DIVISION ALGORITHM

Idea:



That is:

$$\mathrm{quo}(m,n) = \text{if } m<n \text{ then } 0 \text{ else } 1+\mathrm{quo}(m-n,n)$$

$$\mathrm{rem}(m,n) = \text{if } m<n \text{ then } m \text{ else } \mathrm{rem}(m-n,n)$$

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 ) )
```

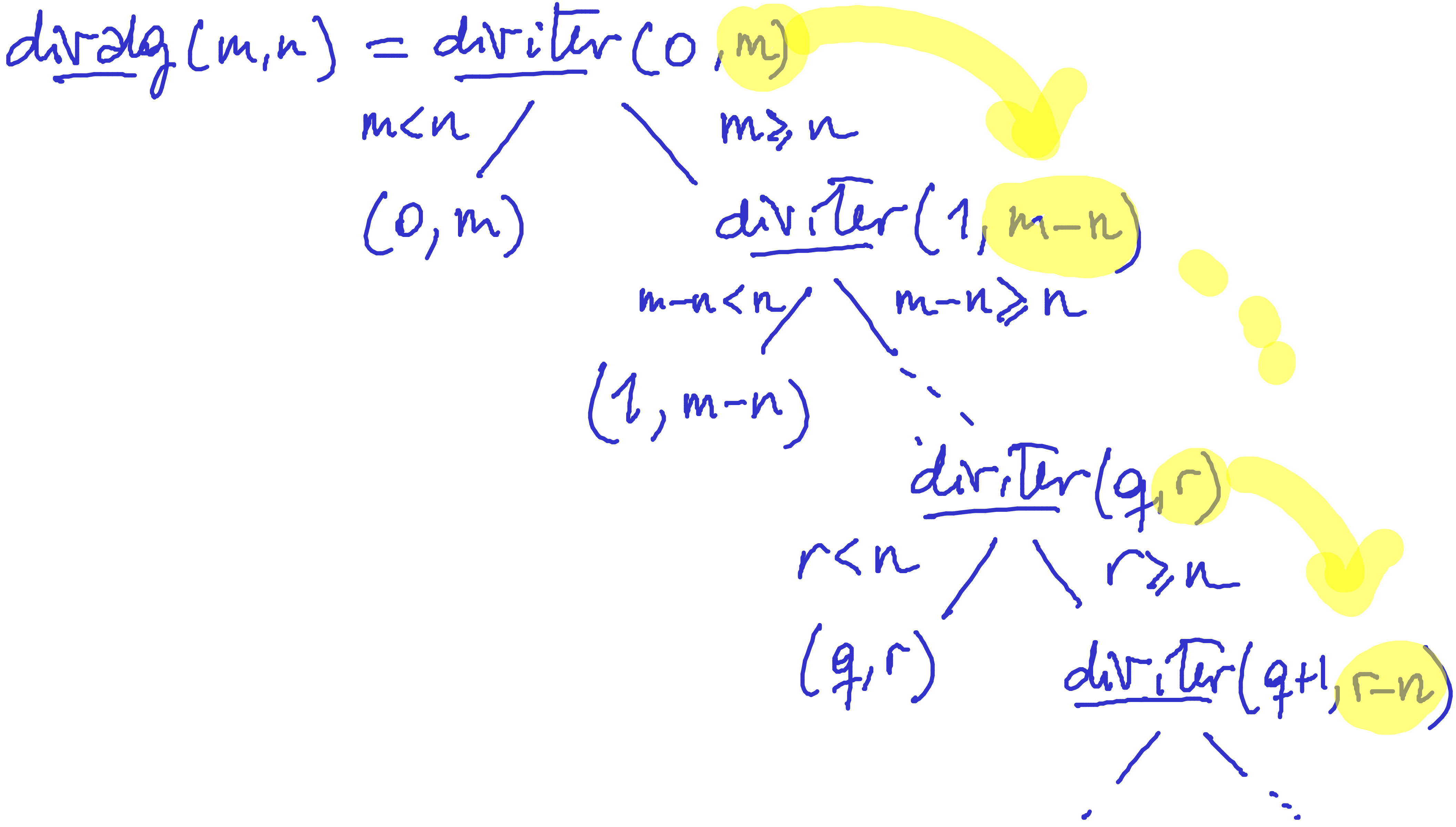
Computation Tree

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

- $m<n$: $(0,m)$
- $m \geq n$: $\underline{\text{diviter}}(1, m-n)$
  - $m-n<n$: $(1, m-n)$
  - $m-n \geq n$: …
    - $\underline{\text{diviter}}(q,r)$
      - $r<n$: (q,r)
      - $r \geq n$: $\underline{\text{diviter}}(q+1, r-n)$
        - …
        - …

Theorem 45 *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:



divalg(m,n) = diviter(0,m)
m<n
m≥n
(0,m)
diviter(1,m−n)
m−n<n
m−n≥n
(1,m−n)
diviter(q,r)
r<n
r≥n
(q,r)
diviter(q+1,r−n)

As for partial correctness; i.e. that

$$m = \underline{quo}(m,n) \cdot n + \underline{rem}(m,n) \qquad (*)$$
$$0 \le \underline{rem}(m,n) < n$$

We show the invariant property that on all calls of $\underline{diviter}(q,r)$ one has

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

The last call will therefore yield $(*)$.

$$m = 0\cdot n + m\,,\quad m \geq 0$$

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

$$\begin{tikzcd}[column sep=small]
 & \underline{\mathrm{diviter}}(0,m) \arrow[dl, "m<n"'] \arrow[dr, "m\geq n"] & & & \\
(0,m) & & \underline{\mathrm{diviter}}(1,m-n) \arrow[dl, "m-n<n"'] \arrow[dr, dashed, "m-n\geq n"] & & \\
 & (1,m-n) & & \underline{\mathrm{diviter}}(q,r) \arrow[dl, "r<n"'] \arrow[dr, "r\geq n"] & \\
 & & (q,r) & & \underline{\mathrm{diviter}}(q+1,r-n) \arrow[dl, dashed] \arrow[dr, dashed] \\
 & & & \cdots & & \cdots
\end{tikzcd}$$

Suppose $m = qn + r$, $r \geq 0$

If $r<n$ then

$\underline{\mathrm{quo}}(m,n) = q$

$\underline{\mathrm{rem}}(m,n) = r$

satisfy the required properties

Otw $r \geq n$ and we note that the invariant is maintained as

$$m = (q+1)n + (r-n)\,,\quad r-n \geq 0\,.$$

Proposition 46 *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: Let m be a positive integer.
Let k and l be natural numbers.

($\Longrightarrow$) Assume $k \equiv l \pmod{m}$

Then, $k = l + im$ for some integer i

$$= [\,\mathrm{quo}(l,m) + i\,] \cdot m + \mathrm{rem}(l,m)$$

Therefore $\mathrm{rem}(k,m) = \mathrm{rem}(l,m)$

Let m be a positive integer.

Let k and l be natural numbers.

($\Leftarrow$) Assume: $\underline{\text{rem}}(k,m) = \underline{\text{rem}}(l,m)$

Then, $k - l = \left[\underline{\text{quo}}(k,m) - \underline{\text{quo}}(l,m)\right] \cdot m$

$\qquad + \left[\underline{\text{rem}}(k,m) - \text{rem}(l,m)\right]$

$\qquad = \left[\underline{\text{quo}}(k,m) - \underline{\text{quo}}(l,m)\right] \cdot m$

$\boxtimes$

Corollary 47 *Let m be a positive integer.*

1. *For every natural number n,*

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

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:

$$[k]_m = \text{if } \underline{\mathrm{rem}}(k, m) = 0 \ \underline{\text{then}}\ 0$$
$$\underline{\text{else}} \text{ if } k > 0 \ \underline{\text{then}}\ \underline{\mathrm{rem}}(k, m)$$
$$\underline{\text{else}}\ m - \underline{\mathrm{rem}}(-k, m)$$