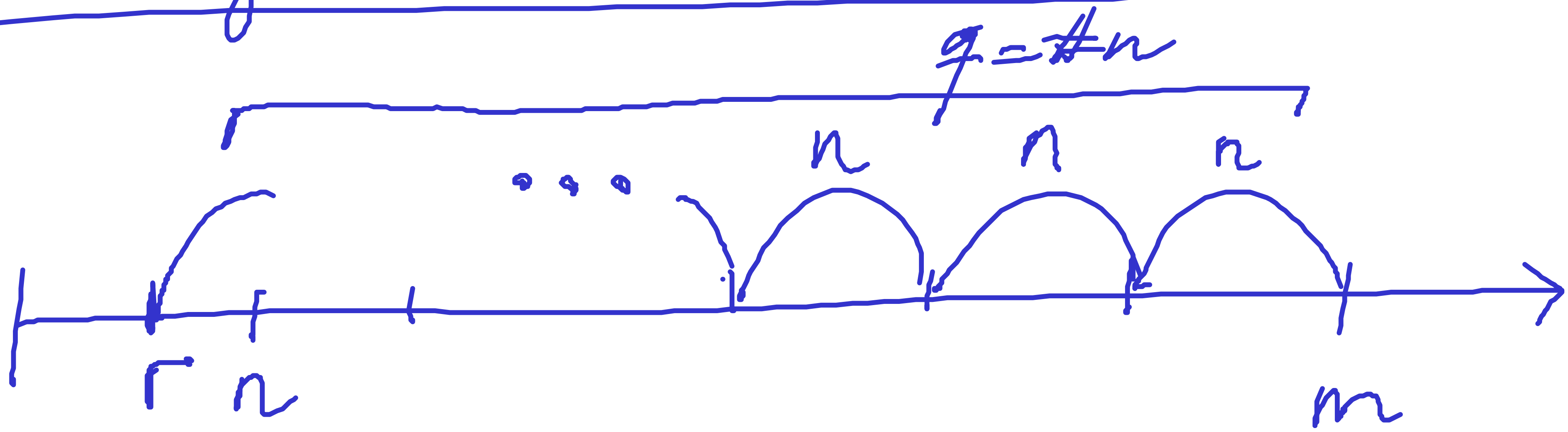
The division theorem and algorithm

$\exists!$

Theorem 38 (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 39 *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* $\mathrm{rem}(m, n)$.

Division by iterated substraction



divalg : int * int → int * int

The Division Algorithm in ML:

divalg (m,n)
↓
diviter (0,m)

```
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
```

diviter (q,r) $\xrightarrow{r<n}$ output (q,r)
↓
diviter (q+1,r-n)

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

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

$$\begin{tikzcd}
(0,m) \arrow[r, "m<n"] \arrow[d] & (0,m) \\
(1,m-n) \arrow[r, "m-n<n"] \arrow[d] & (1,m-n) \\
(2,m-2n) \arrow[r] \arrow[d] & (2,m-2n) \\
(i,m-in) \arrow[r] \arrow[d] & (i,m-in) \\
{} &
\end{tikzcd}$$

terminates $\rightsquigarrow$ by contradiction divider

$$(q, r) \xrightarrow{r < n} (q, r)$$

$$\begin{array}{c}(q, r) \\ \downarrow \\ (q+1, r-n)\end{array}$$

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

$$\Downarrow$$

$$m = (q+1) \cdot n + (r-n)$$

✓

$$P(x, y) \equiv (m = x \cdot n + y)$$

$$P(q, r) \Longrightarrow P(q+1, r-n)$$

$$P(0, m) \text{ holds} \equiv (m = 0 \cdot n + m) \checkmark$$

Theorem 40 *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: Establishes the existence part of the division theorem.

Let us show such a pair is <u>unique</u>.

Assume (q_1, r_1) s.t. $0 \leq r_1 < n$ and $m = q_1 \cdot n + r_1$

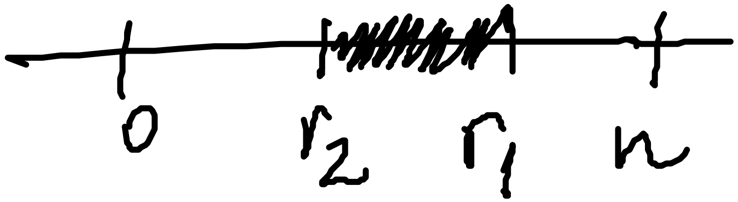
Assume (q_2, r_2) s.t. $0 \leq r_2 <$ and $m = q_2 \cdot n + r_2$

We show $q_1 = q_2$ and $r_1 = r_2$.

$$m = q_1 \cdot n + r_1 \qquad 0 \le r_1 < n$$

$$m = q_2 \cdot n + r_2 \qquad 0 \le r_2 < n$$

$$\Rightarrow (q_1 - q_2) \cdot n + (r_1 - r_2) = 0 \quad (*)$$



<u>Case 1</u>: $r_1 \geq r_2 \Rightarrow r_1 - r_2 \geq 0$

$$\Rightarrow r_1 - r_2 < n$$

$$r_1 - r_2 = (q_2 - q_1) \cdot n$$

$$(q_2 - q_1) \cdot n < n$$

$$\Updownarrow$$

$$q_2 - q_1 = 0$$

$$\Updownarrow$$

$$q_1 = q_2$$

<u>Case 2</u>: $r_2 > r_1$

$\Rightarrow$

$$m - q_1 \cdot n = r_1$$

$$\parallel \qquad \text{because } q_1 = q_2$$

$$m - q_2 \cdot n = r_2$$

$\square$

Checking the congruence of numbers is decidable

Proposition 41 *Let* m *be a positive integer. For all integers* k *and* l,

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

PROOF: Assume k and l arbitrary integers.

($\Longrightarrow$) Assume $k \equiv l \pmod m$; that is, $\exists$ int i $k - l = i m$. By the division thm $l = q \cdot m + \underset{\mathrm{rem}(l,m)}{r}$ for unique q & $0 \leq r < m$. Then,

$k = l + i m = (q + i) \cdot m + r$ with $0 \leq r < m$

Hence $\underbrace{r = \mathrm{rem}(k,m)}$. $\Rightarrow$ by uniqueness of remainders

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

$$k - l = \underline{\text{quo}}(k, m) \cdot m + \underline{\text{rem}}(k, m) - \left(\underline{\text{quo}}(l, m) \cdot m + \underline{\text{rem}}(l, m)\right)$$

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

$\square$

Corollary 42 *Let* m *be a positive integer.*

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

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

$$\Updownarrow$$

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

Exercise

PROOF:

Corollary 42 *Let m be a positive integer.*

1. *For every natural number n,*

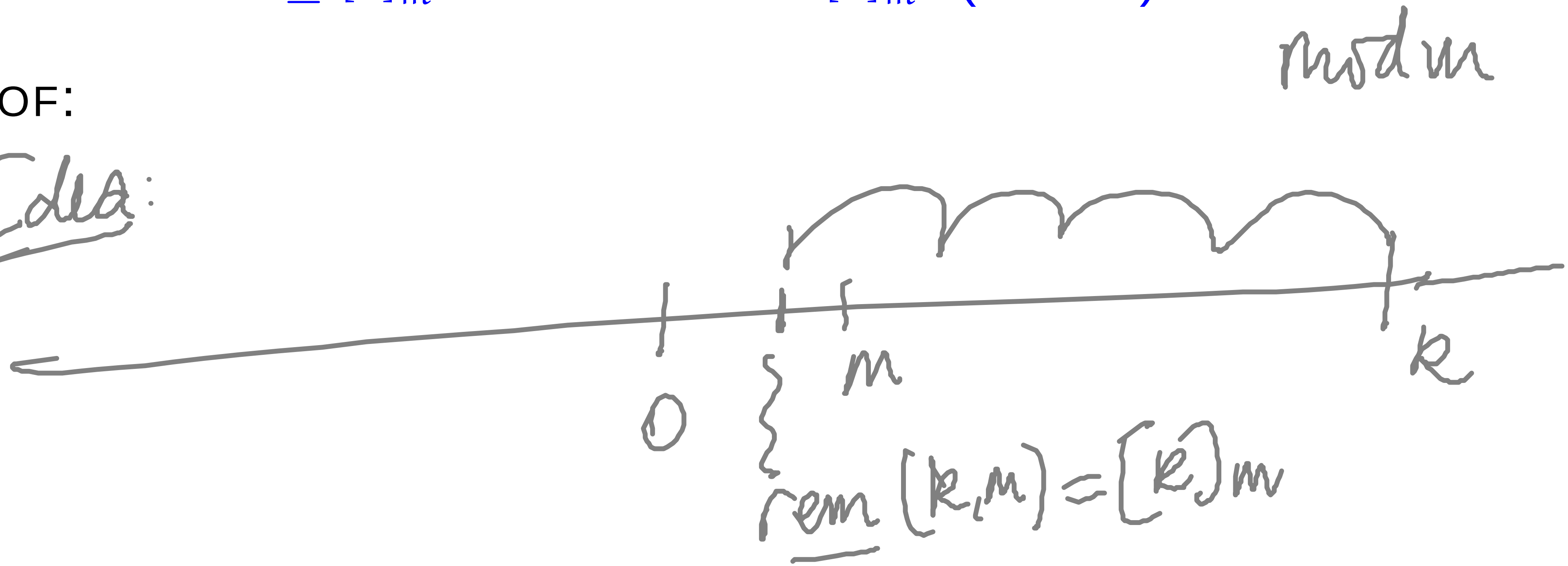
$$n \equiv \mathrm{rem}(n, m) \pmod{m} \quad .$$

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

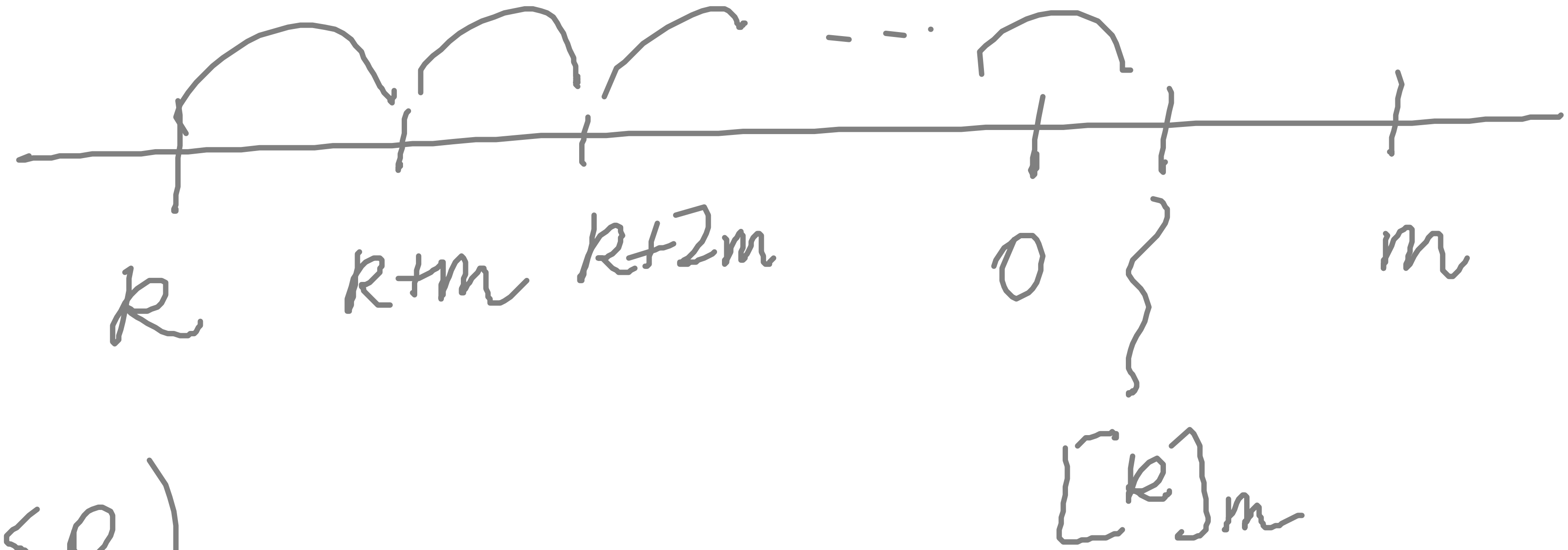
$$0 \leq [k]_m < m \quad \textit{and} \quad k \equiv [k]_m \pmod{m} \quad .$$

PROOF:

Idea:



mod m



$(k<0)$

$$k + |k| \cdot m \geq 0$$

$$\underline{\text{rem}}(k + |k| \cdot m, m) = [k]_m \equiv k$$

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

$$k +_m l = [k+l]_m \quad , \quad k \cdot_m l = [k \cdot l]_m$$

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

$\parallel$ rem$(k+l, m)$ $\qquad$ $\parallel$ rem$(k \cdot l, m)$

Boolean OR and

$$(\mathbb{Z}_2, +_2, \cdot_2)$$

Example 44 *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 45 *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.