Inverses

Definition 42

1. *A number* x *is said to admit an* additive inverse *whenever there exists a number* y *such that* $x + y = 0$*.*

Consider a monoid with binary operation $*$ and neutral element e. An inverse for x is a y s.t. $x*y=e$ and $y*x=e$.

Inverses

Definition 42

1. *A number* x *is said to admit an* additive inverse *whenever there exists a number* y *such that* $x+y=0$.
2. *A number* x *is said to admit a* multiplicative inverse *whenever there exists a number* y *such that* $x \cdot y = 1$.

Inverses, when they exist, are unique.

Suppose y and z are inverses of x

<u>RTP</u> $y = z$?

$$\begin{aligned} y &= y * e \\ &= y * (x * z) \\ &= (y * x) * z \\ &= e * z \\ &= z \end{aligned}$$

$\boxtimes$

```
-- Proposition
Uniqueness :
  -- Consider
  ( M : Set ) ( e : M ) ( _*_ : M → M → M )
  -- a set M with an element e and a binary operation * such that
  ( y*[x*z]=[y*x]*z : -- * is associative
      ∀{ y x z : M } → ( y * ( x * z ) ) == ( ( y * x ) * z ) )
  ( [y*e]=y : -- e is right neutral
      ∀{ y : M } → y == ( y * e ) )
  ( [e*z]=z : -- e is left neutral
      ∀{ z : M } → ( e * z ) == z )
  -- For all
  ( x y z : M )
    -- if
    → ( ( y * x ) == e ) -- y is a left inverse of x
    -- and
    → ( e == ( x * z ) )  -- z is a right inverse of x
    -- then
    → ( y == z )
    -- they are equal
```

```
-- Proof
Uniqueness M e _*_ y*[x*z]=[y*x]*z y=[y*e] [e*z]=z x y z [y*x]=e e=[x*z]
  = y
      =⟨ y=[y*e] ⟩
    ( y * e )
      =⟨ e=[x*z] |in-ctx y*- ⟩
    ( y * ( x * z ) )
      =⟨ y*[x*z]=[y*x]*z ⟩
    ( ( y * x ) * z )
      =⟨ [y*x]=e |in-ctx -*z ⟩
    ( e * z )
      =⟨ [e*z]=z ⟩
    z
      =
 where
   y*- : M → M
   y*- a = y * a
   -*z : M → M
   -*z a = a * z
```

Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

(i) the *integers*

$$\mathbb{Z} \ : \quad \ldots -n\,, \ \ldots\,, \ -1\,, \ 0\,, \ 1\,, \ \ldots\,, \ n\,, \ \ldots$$

which then form what in the mathematical jargon is referred to as a *commutative ring*, and

(ii) the *rationals* $\mathbb{Q}$ which then form what in the mathematical jargon is referred to as a *field*.

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

Proof Suppose q, r and q', r' are such integers.

RTP: $q = q'$ and $r = r'$

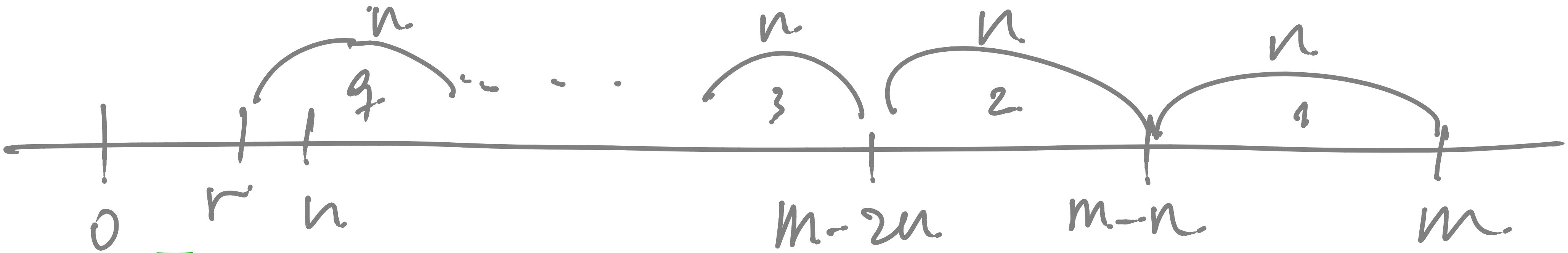
① $q \geq 0$, $0 \leq r < n$

$m = q \cdot n + r$

② $q' \geq 0$, $0 \leq r' < n$ $\Rightarrow$ $q \cdot n + r = q' \cdot n + r'$ wlog $r \geq r'$

$m = q \cdot n' + r'$ $\Rightarrow$ $(q - q') \cdot n = r - r' \geq 0 \Rightarrow q - q' = 0$

$\Rightarrow r = r'$ ☒



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

Termination argument: The second component of the pair diviter(q,r) decreases in each step while it remains positive throughout the computation.

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
```

Established an invariant (q,r) of the computation

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

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

divalg(m,n)
$\shortparallel$ $m = 0 \cdot n + m$
diviter(0,m)

$m < n$: (0,m)

$m \geq n$: diviter(1,m-n) $m = 1 \cdot n + (m-n)$

$m = q \cdot n + r$
diviter(q,r)

$m = (q+1)n + (r-n)$
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:

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.

($\Leftarrow$) Assume $\mathrm{rem}(k,m) = \mathrm{rem}(l,m)$.

Know $k = q \cdot m + \mathrm{rem}(k,m)$ $\quad l = q' \cdot m + \mathrm{rem}(l,m)$

Consider $k - l = (q - q') \cdot m$ hence $k \equiv l \pmod{m}$

($\Rightarrow$) Exercise.

$\boxtimes$

Corollary 47 *Let m be a positive integer.*

1. *For every natural number n,*

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

NB: $0 \leq \mathrm{rem}(n,m) < m$

For the purpose of working with congruences modulo m, we need only focus on $0, 1, \ldots, m-1$

PROOF:

$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

Corollary 47 *Let m be a positive integer.*

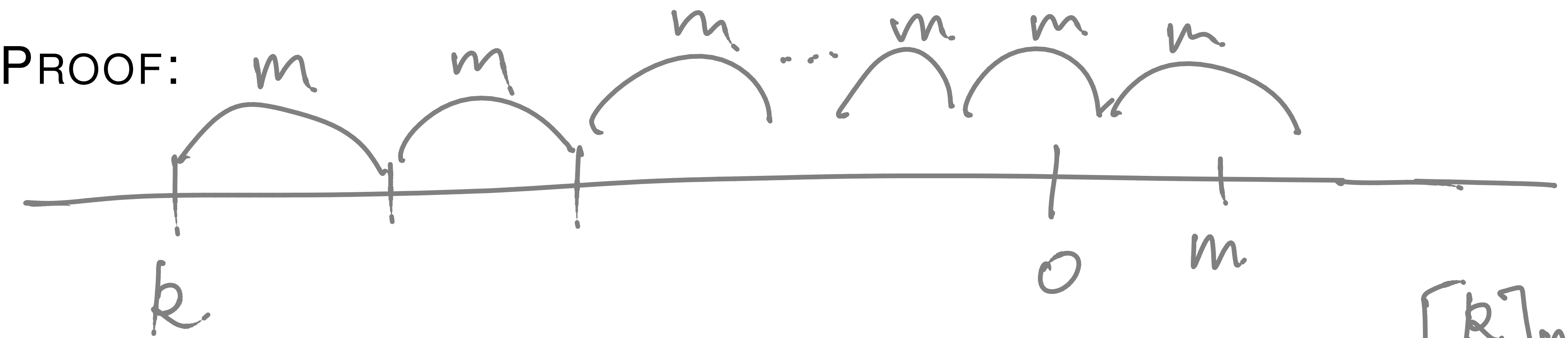
1. *For every natural number n,*

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

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:



$[k]_m$

$k \equiv k + i\,m \pmod{m} \quad \forall i \in \mathbb{Z}$

Take $i = |k|$ Consider $\underline{\mathrm{rem}}(k + |k| \cdot m, m)$

Modular arithmetic

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

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

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 $0 \leq k, l < m$.