Semirings

Definition 44 *A* semiring *(or* rig*) is an algebraic structure with*

- *a* commutative monoid *structure, say* $(0, \oplus)$,
- *a* monoid structure*, say* $(1, \otimes)$,

satifying the distributivity laws*:*

- $0 \otimes x = 0 = x \otimes 0$
- $x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$, $(y \oplus z) \otimes x = (y \otimes x) \oplus (z \otimes x)$

A semiring is commutative *whenever* $\otimes$ *is.*

The *additive structure* $(\mathbb{N}, 0, +)$ of natural numbers with zero and addition satisfies the following:

- Monoid laws

$$0 + n = n = n + 0 \quad , \quad (l + m) + n = l + (m + n)$$

- Commutativity law

$$m + n = n + m$$

and as such is what in the mathematical jargon is referred to as a *commutative monoid*.

Also the *multiplicative structure* $(\mathbb{N}, 1, \cdot)$ of natural numbers with one and multiplication is a commutative monoid:

- Monoid laws

$$1 \cdot n = n = n \cdot 1 \quad , \quad (l \cdot m) \cdot n = l \cdot (m \cdot n)$$

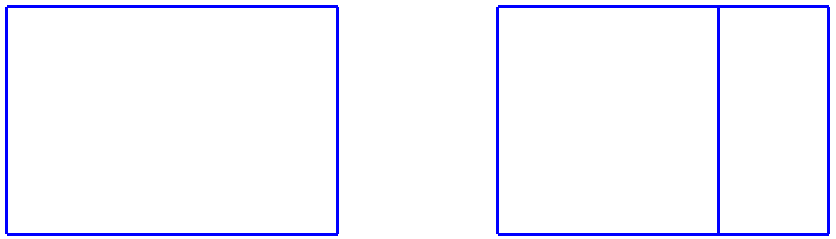
- Commutativity law

$$m \cdot n = n \cdot m$$

The additive and multiplicative structures interact nicely in that they satisfy the

- Distributive laws

$$\begin{aligned} l \cdot 0 &= 0 \\ l \cdot (m + n) &= l \cdot m + l \cdot n \end{aligned}$$



and make the overall structure $(\mathbb{N}, 0, +, 1, \cdot)$ into what in the mathematical jargon is referred to as a *commutative semiring*.

Cancellation

The additive and multiplicative structures of natural numbers further satisfy the following laws.

- Additive cancellation

  For all natural numbers k, m, n,

  $$k + m = k + n \implies m = n \quad .$$

- Multiplicative cancellation

  For all natural numbers k, m, n,

  if $k \neq 0$ then $k \cdot m = k \cdot n \implies m = n \quad .$

Example: (α list, @, nil) monoid.
allows cancellation
$l @ a = l @ b \Rightarrow a = b$

Definition 45 *A binary operation* $\bullet$ *allows* cancellation *by an element* c

- on the left*: if* $c \bullet x = c \bullet y$ *implies* $x = y$
- on the right*: if* $x \bullet c = y \bullet c$ *implies* $x = y$

Example: The append operation on lists allows cancellation by any list on both the left and the right.

Inverses

Definition 46 *For a monoid with a neutral element e and a binary operation $\bullet$, and element x is said to admit an*

- inverse on the left *if there exists an element ℓ such that $\ell \bullet x = e$*
- inverse on the right *if there exists an element r such that $x \bullet r = e$*
- inverse *if it admits both left and right inverses*

Proposition 47 *For a monoid $(e, \bullet)$ if an element admits an inverse then its left and right inverses are equal.*

PROOF: Let x be an element with left inverse ℓ and right inverse r. That is, $\ell \cdot x = e = x \cdot r$.

Then, $r = e \cdot r = (\ell \cdot x) \cdot r = \ell \cdot (x \cdot r) = \ell \cdot e = \ell$ ⊠

Groups

Definition 49 *A* group *is a monoid in which every element has an inverse.*

An Abelian group *is a group for which the monoid is commutative.*

Inverses

Definition 50

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* $x \cdot y = 1$.

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*

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

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*.

Rings

Definition 51 *A* ring *is a semiring* $(0, \oplus, 1, \otimes)$ *in which the commutative monoid* $(0, \oplus)$ *is a group.*

A ring is commutative *if so is the monoid* $(1, \otimes)$*.*

Fields

Definition 52 *A* field *is a commutative ring in which every element besides* 0 *has a reciprocal (that is, and inverse with respect to* $\otimes$*).*

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

Uniqueness:

(*) $\left\{ \begin{array}{l} q \geq 0,\ 0 \leq r < n : m = q \cdot n + r \\ q' \geq 0,\ 0 \leq r' < n : m = q' \cdot n + r' \end{array} \right\} \Rightarrow \begin{array}{l} q = q' \\ r = r' \end{array}$

Assume (*). Then $m - r = q \cdot n \Rightarrow m \equiv r \pmod{n}$

$m - r' = q' \cdot n \Rightarrow m \equiv r' \pmod{n}$

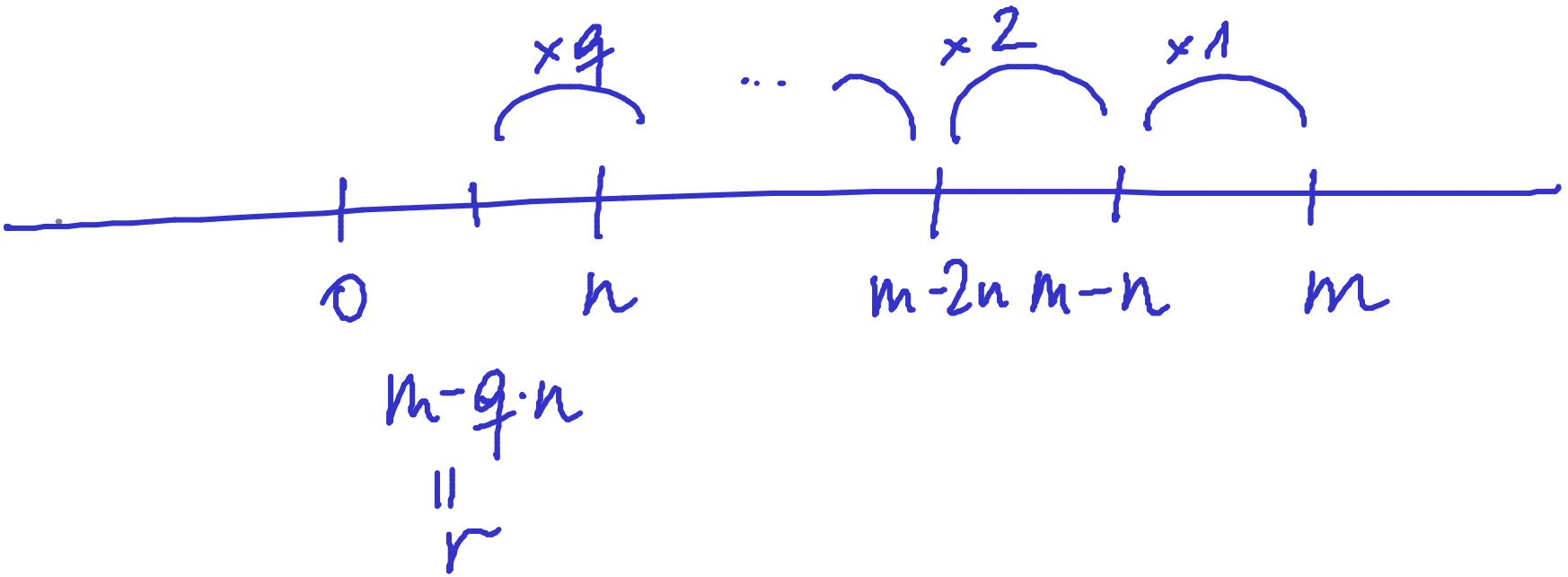
Thus, $r \equiv r'$ and since $0 \leq r, r' < n$, $r = r'$. So also $q = q'$. ☒

The division theorem and algorithm

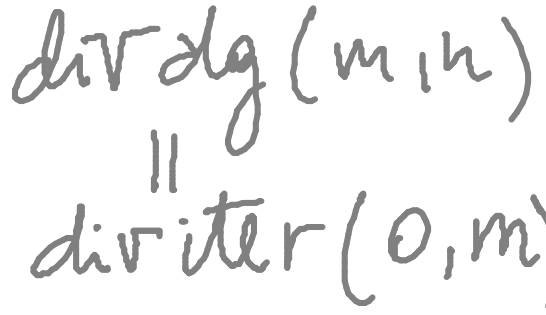
Theorem 53 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $\mathrm{q} \geq 0$, $0 \leq \mathrm{r} < \mathrm{n}$, *and* $\mathrm{m} = \mathrm{q} \cdot \mathrm{n} + \mathrm{r}$.

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

NB: $m = quo(m,n) \cdot n + rem(m,n)$


×q
...
×2
×1
0
n
m-2n
m-n
m
m-q·n
=
r

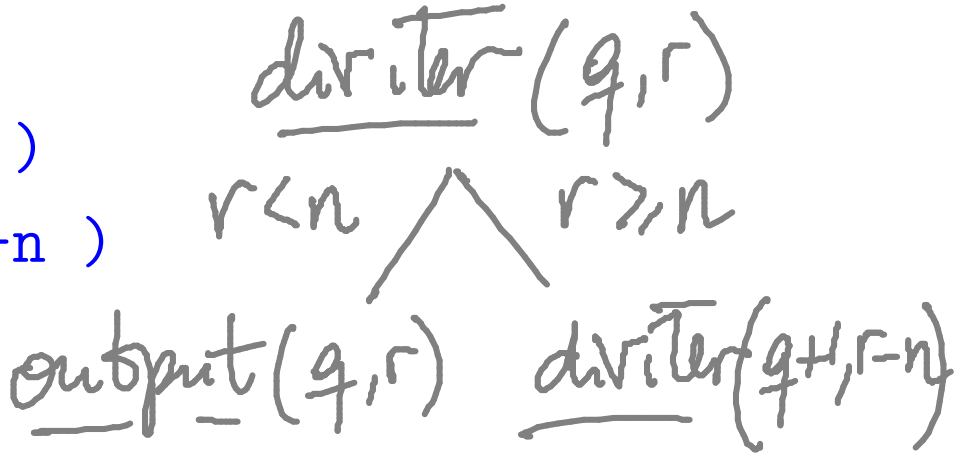
The Division Algorithm in ML:




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

total correctness

partial correctness

PROOF:

$m = 0 \cdot n + m$

divalg (m,n)

=

diviter (0,m)

$m < n$ / $m \geq n$

output (0,m)

diviter (1, m-n)

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

For termination note that the second argument of diviter decreases in the natural numbers.

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

=

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

diviter (q,r)

$r < n$

output (q,r)

diviter (q+1, r-n)

$m = q \cdot n + r$?

Proposition 57 *Let* m *be a positive integer. For all natural numbers* 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:

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:

If k is a nat. number take $[k]_m = \underline{rem}(k,m)$.

If k is a negative integer: