Numbers

Objectives

- Get an appreciation for the abstract notion of number system, considering four examples: natural numbers, integers, rationals, and modular integers.
- Prove the correctness of three basic algorithms in the theory of numbers: the division algorithm, Euclid's algorithm, and the Extended Euclid's algorithm.
- Exemplify the use of the mathematical theory surrounding Euclid's Theorem and Fermat's Little Theorem in the context of public-key cryptography.
- To understand and be able to proficiently use the Principle of Mathematical Induction in its various forms.

Natural numbers

In the beginning there were the *natural numbers*

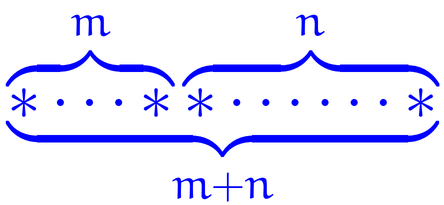
$$\mathbb{N} : \quad 0 , \quad 1 , \quad \ldots , \quad n , \quad n+1 , \quad \ldots$$

generated from *zero* by successive increment; that is, put in ML:

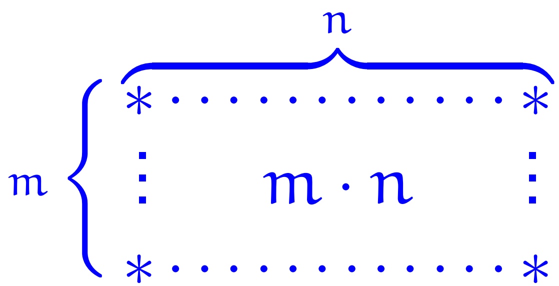
```
datatype
  N = zero | succ of N
```

The basic operations of this number system are:

- Addition



- Multiplication



we are allowed to write $l+m+n$

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

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

Example MONOID

$$(\alpha\ list,\ nil,\ @)$$

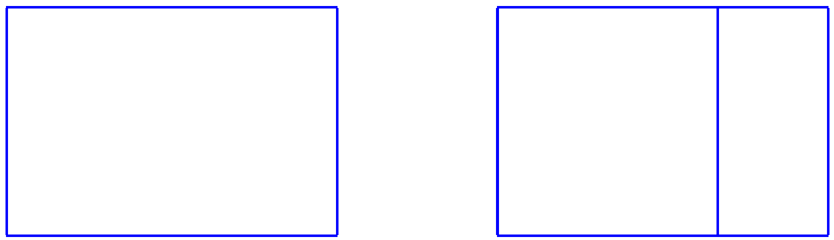
$$l @ nil = l = nil @ l$$

$$(l_1 @ l_2) @ l_3 = l_1 @ (l_2 @ l_3).$$

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

- Distributive law

$$l \cdot (m + n) \quad = \quad l \cdot m + l \cdot n$$



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

Exercise: • Let $*$ be a binary operation that is associative and commutative. Then, if $*$ has a neutral element (i.e. an e s.t. $e*x = x = x*e$) Then this neutral element is unique.

Inverses

Definition 41

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

• Inverses, when they exist, are unique.

Inverses

Definition 41

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:

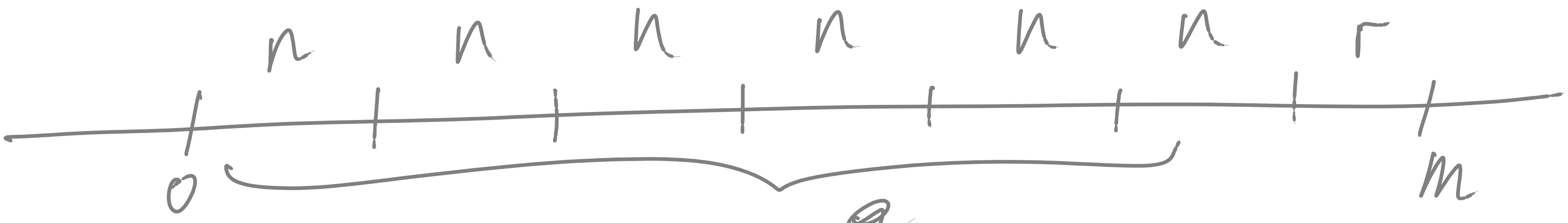
Extending the system of natural numbers to: (i) admit all additive inverses and then (ii) also admit all multiplicative inverses for non-zero numbers yields two very interesting results:

(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

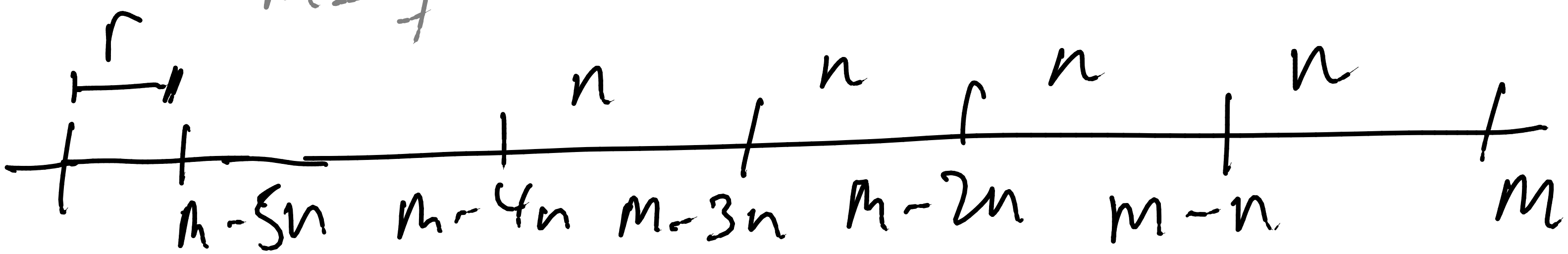
Theorem 42 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$, $0 \leq r < n$, *and* $m = q \cdot n + r$.

Let m be a nat. and n be a po. nat.

∃! int q and r. q≥0, 0≤r<n

m=q·n+r.

Algorithm



The division theorem and algorithm

Theorem 42 (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 43 *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* $\mathrm{rem}(m, n)$*.*

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 ) )
```

In each iteration diviter maintains the INVARIANCE that m equals the first component of the diviter pair times n plus the second component of the pair.

$m = q \cdot n + r$

output (q, r) if $r < n$; if $r \geq n$, diviter $(q+1, r-n)$

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

The INVARIANCE holds at the very beginning because $m = 0 \cdot n + m$

quotient, remainder: $m = q \cdot n + r$ and $0 \leq r < n$

PARTIAL CORRECTNESS

Theorem 44 *For every natural number* m *and positive natural number* n*, the evaluation of* $\mathtt{divalg}(\mathrm{m},\mathrm{n})$ *terminates, outputing a pair of natural numbers* $(\mathrm{q}_0,\mathrm{r}_0)$ *such that* $\mathrm{r}_0 < \mathrm{n}$ *and* $\mathrm{m} = \mathrm{q}_0 \cdot \mathrm{n} + \mathrm{r}_0$*.*

PROOF:

As for uniqueness:

(*) Suppose $0 \le r_i < n$, $m = q_i \cdot n + r_i$ $i = 1, 2$

Then we show that necessarily

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

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

$\Rightarrow \ldots$ □

in ML: k mod m

Proposition 45 *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: Let m be a pos. int. Let k and l be nat.

($\Longrightarrow$) By assumption, $k - l = p \cdot m$ for some int. p.

$= (q - q') \cdot m + \underline{rem}(k,m) - \underline{rem}(l,m)$ for some q, q'.

$\Longrightarrow \ldots \Longrightarrow \underline{rem}(k,m) - \underline{rem}(l,m) = 0$

($\Longleftarrow$) $k = q \cdot m + \underline{rem}(k,m)$, $l = q' \cdot m + \underline{rem}(l,m)$

$k - l = (q - q') \cdot m + \underline{rem}(k,m) - \underline{rem}(l,m)$

$= (q - q') \cdot m$ by assumption. ∎