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

$$\underbrace{\overbrace{*\cdots*}^{m}\overbrace{*\cdots\cdots*}^{n}}_{m+n}$$

- Multiplication

$$m\left\{\begin{array}{c}\overbrace{*\cdots\cdots\cdots\cdots*}^{n}\\ \vdots \quad m\cdot n \quad \vdots\\ *\cdots\cdots\cdots\cdots*\end{array}\right.$$

Group = monoid with inverses

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

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

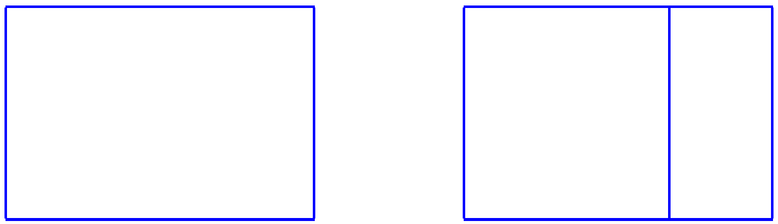
- Commutativity law

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

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

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

Inverses

Definition 42

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

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 $x \cdot y = 1$.*

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*.

Lemma 43. For integers q, n and r with $n > 0$ & $0 \le r < n$,

$$0 = q \cdot n + r \Rightarrow q = 0 \ \& \ r = 0.$$

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* $q \ge 0$, $0 \le r < n$, *and* $m = q \cdot n + r$. $= q' \cdot n + r'$

Proof of Lemma 43: Assume $0 = q \cdot n + r$. Proof by contradiction, $0 = (q - q') \cdot n + (r - r')$

assuming $q \neq 0$, i.e. (1) $q > 0$ or (2) $q < 0$.

Case 1 $q > 0$. Then $q \cdot n + r > 0$ ※

Case 2 $q < 0$. Then $q \cdot n + r \le -n + r < -n + n = 0$. ※

Thus $q = 0$ and $0 = 0 \cdot n + r$, so $r = 0$. ⊠

Lemma 43 gives the uniqueness part of Thm. 43.

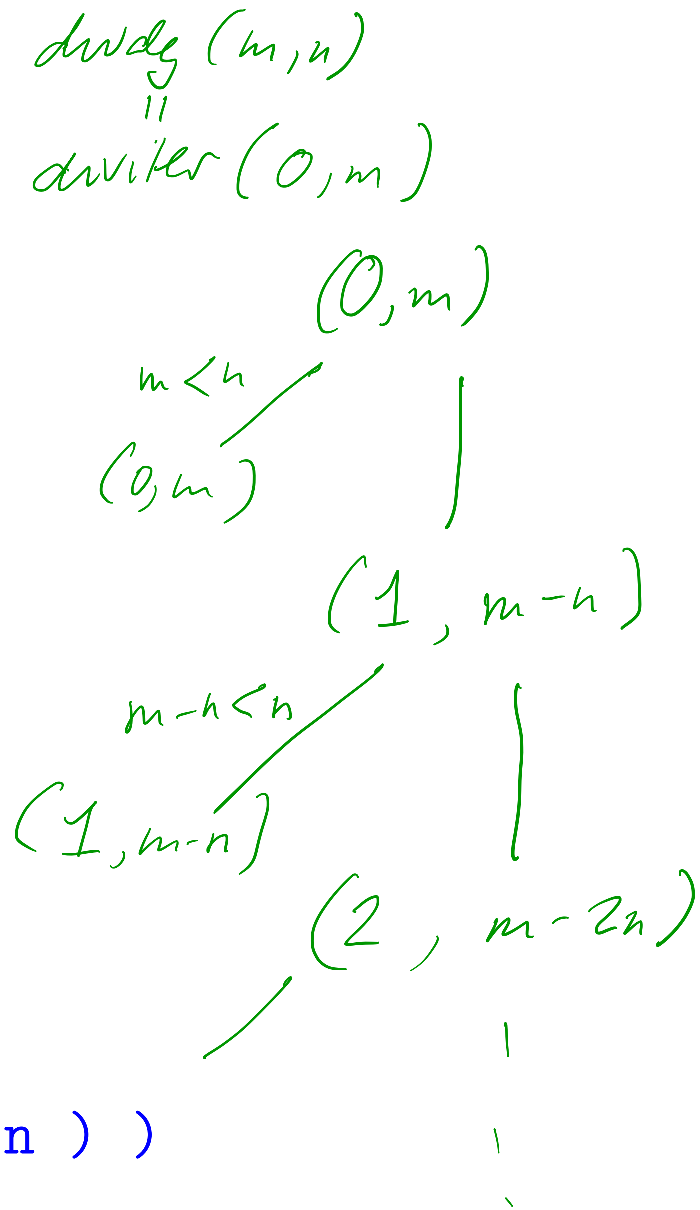
The division theorem and algorithm

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

ad hoc semantics
via computation sequences

The Division Algorithm in ML:

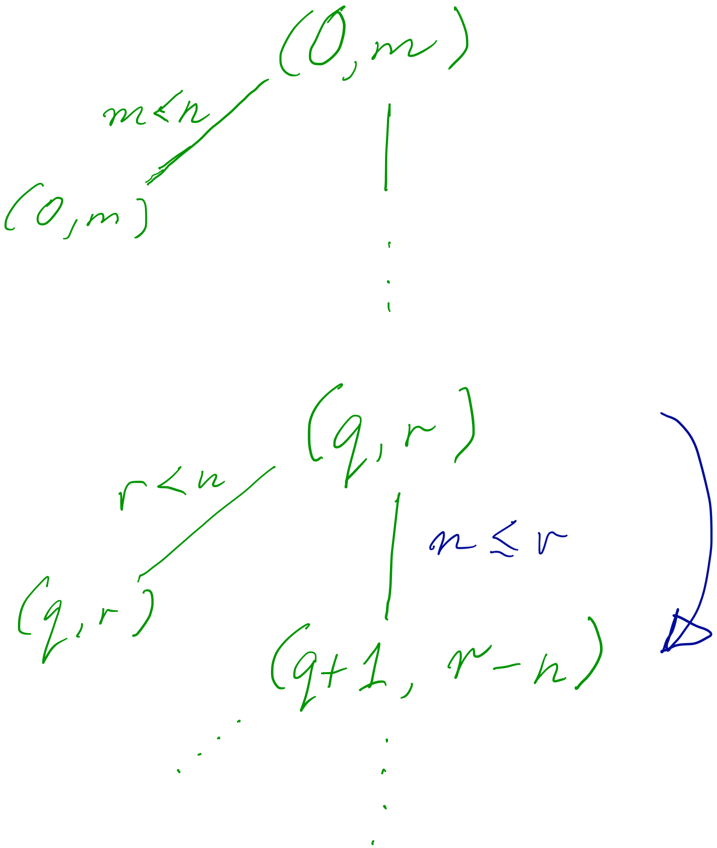



```
fun divalg( m , n )
  = let
      fun diviter( q , r )
        = if r < n then ( q , r )
          else diviter( q+1 , r-n )
    in
      diviter( 0 , m )
    end

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

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

Theorem 45 *For every natural number* m *and positive natural number* n*, the evaluation of* $\texttt{divalg}(m, n)$ *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: (Idea)

✓ $0 \leq 0 \;\&\; 0 \leq m \;\&\; m = 0 \cdot n + m$



INVARIANT:

$0 \leq q \;\&\; 0 \leq r \;\&\; m = q \cdot n + r$

$\Downarrow$ (as assume $n \leq r$)

✓ $0 \leq q+1 \;\&\; 0 \leq r-n \;\&$

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