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

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

- Multiplication

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

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

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

MONOIDS

A monoid is an algebraic structure with

- a neutral element, say e,
- a binary operation, say $*$,

satisfying

- neutral element laws: $e * x = x = x * e$
- associativity law: $(x * y) * z = x * (y * z)$

A monoid is commutative if

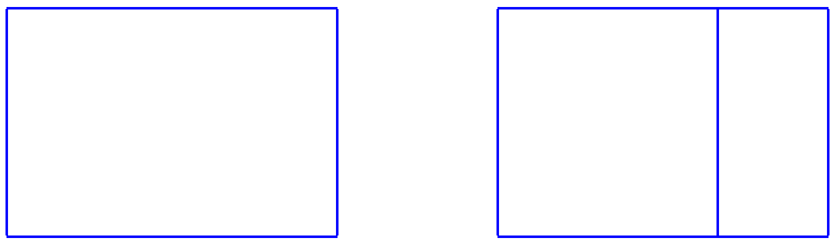
- commutativity: $x * y = y * x$

is satisfied.

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

- Distributive law

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



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

SEMIRINGS

A semiring is an algebraic structure with

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

satisfying the distributive 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.

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

INVERSES

For a monoid with a neutral element e and a binary operation $*$, an element x is said to admit an:

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

GROUPS

A group is a monoid in which every element has an inverse

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

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*.

RINGS

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

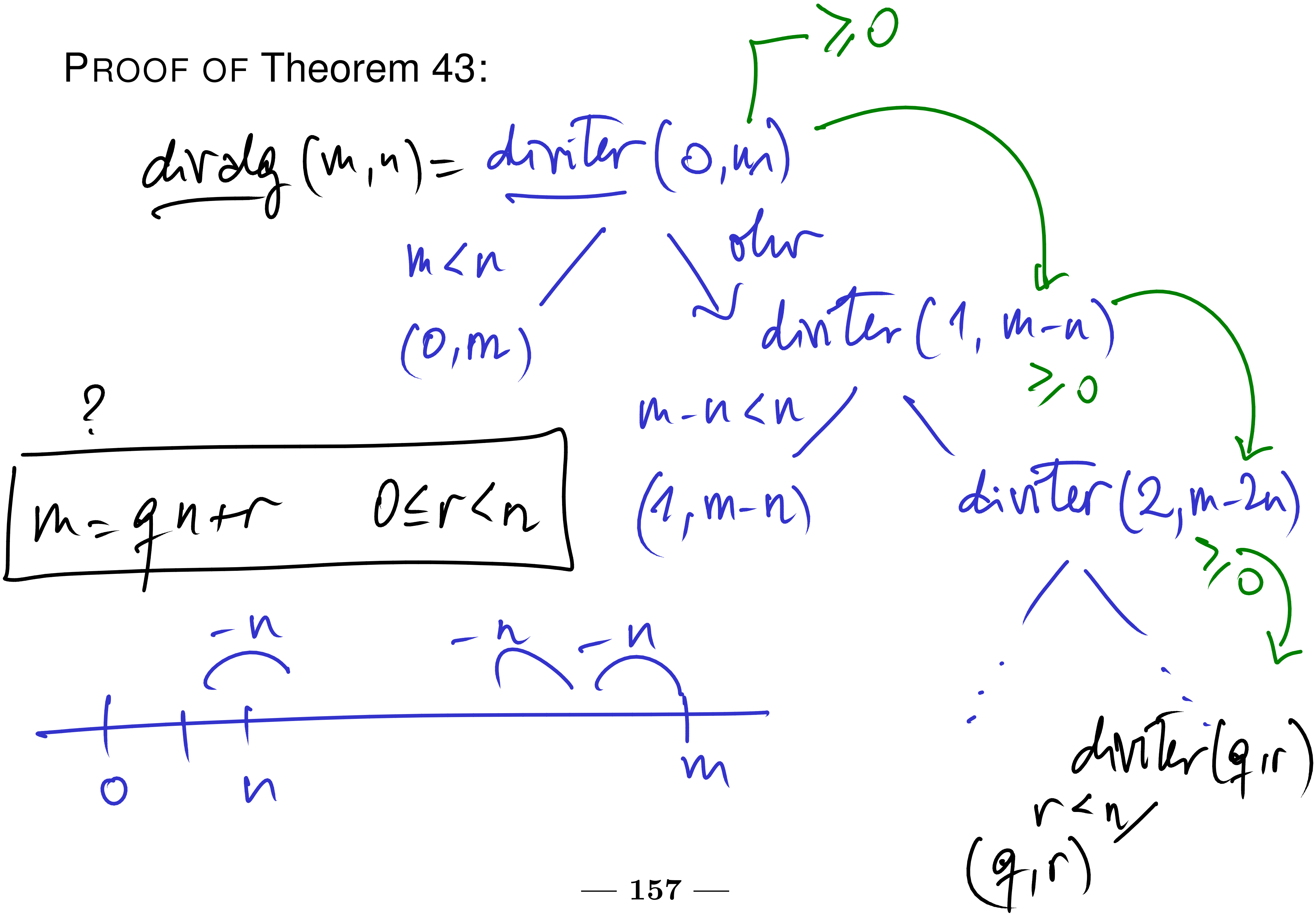
A *field* is a commutative ring in which every element besides 0 has a reciprocal (that is, an inverse with respect to $\otimes$).

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

PROOF OF Theorem 43:

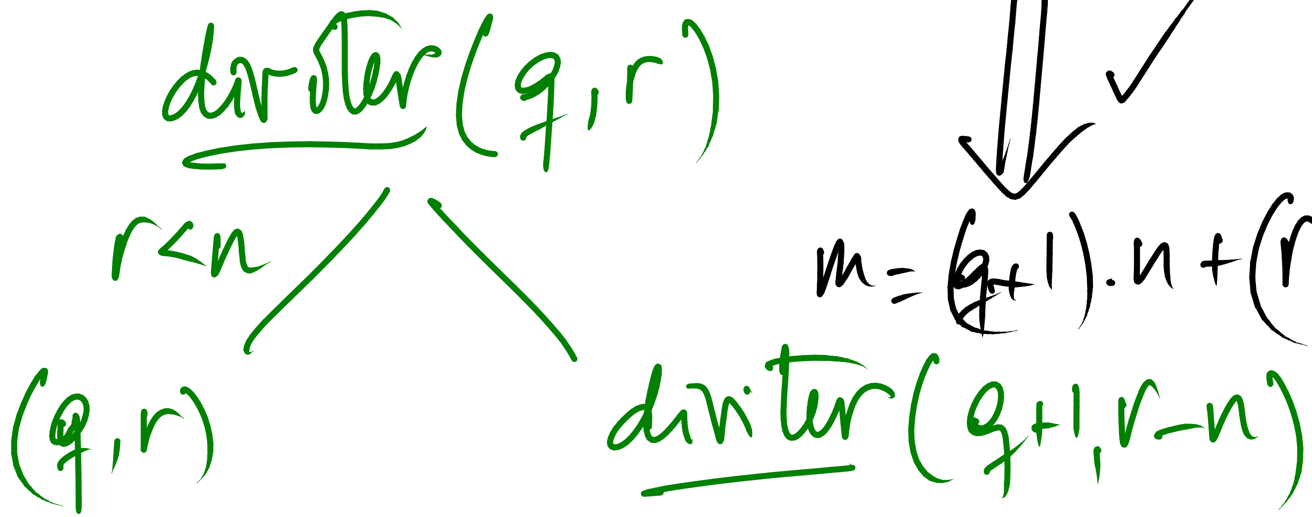


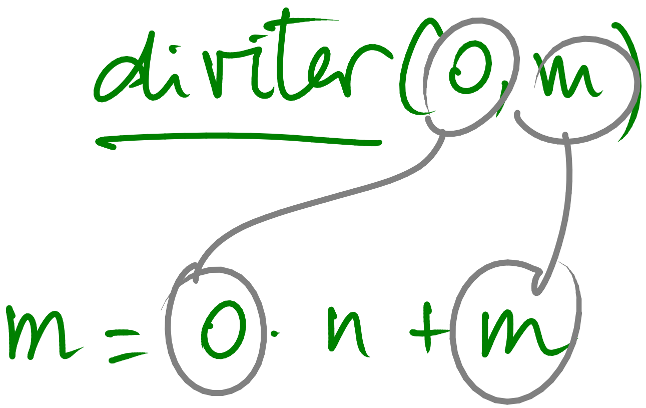
PROOF OF Theorem 43:

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

$$\Downarrow \quad \checkmark$$

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





We have that

m = first arg of diviter $\cdot\, n$
+ second arg of diviter

always holds.

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:

Proposition 46 *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 positive integer.
Let k and l be natural numbers.
($\Longrightarrow$) Assume $k \equiv l \pmod m$.
RTP: $\mathrm{rem}(k,m) = \mathrm{rem}(l,m)$.
So
$k - l = q \cdot m$ for an int. q
$k = q \cdot m + l = q \cdot m + \mathrm{quo}(l,m) \cdot m + \mathrm{rem}(l,m)$
$= (q + \mathrm{quo}(l,m)) \cdot m + \mathrm{rem}(l,m)$.

$$k = (\sim\sim)\cdot m + \underbrace{\underline{\text{rem}}(l, m)}_{0 \le \;\; < m}$$

$\Rightarrow$ $(\sim\sim) = \underline{\text{quo}}(k, m)$, $\quad \underline{\text{rem}}(l, m) = \underline{\text{rem}}(k, m)$

By <u>uniqueness</u>

$(\Leftarrow)$ ... <u>Exercise</u> ...

$\boxtimes$