Number systems

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.

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

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

- Multiplication

$$\mathfrak{m}\left\{\begin{array}{ccc} \multicolumn{3}{c}{\overbrace{\hphantom{* \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot *}}^{\mathfrak{n}}} \\ * & \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot & * \\ \vdots & \mathfrak{m} \cdot \mathfrak{n} & \vdots \\ * & \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot & * \end{array}\right.$$

Example

(αlist, nil, @) is a monoid | is a neutral element for

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

- Monoid laws

associativity

$(l @ m) @ n = l @ (m @ n)$

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

$\mathrm{nil} @ l = l = l @ \mathrm{nil}$

expressions such as $l+m+n$ are not ambiguous.

- Commutativity law

$$m + n = n + m$$

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

is a monoid, which is not commutative in general (though unit list is)

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

- Monoid laws

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

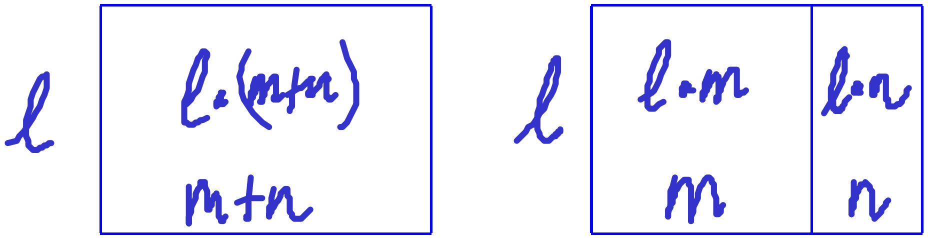
- Commutativity law

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

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

- Distributive law

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



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

Example $(\{0,1\}, 0, \vee, 1, \&)$ 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,

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

In general, let $(M, e, *)$ be a commutative monoid.
An element x in M has an inverse if there is a y in M such that $x * y = e$.

Inverses

$z * x * y = (x * z) * y = e * y = y$

Definition 37

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

Proposition: The inverse of an element is unique.

PROOF Let y and z be inverses for x; that is,

(1) $\boxed{x * y = e}$ and (2) $\boxed{x * z = e}$. We show $y = z$.

By (1) $\boxed{z * x * y} = z * e = z$.

$\square$

How do we prove

there exists a unique

$$\exists! x .\ P(x)$$

$$\iff \left(\exists x .\ P(x)\right) \ \& \ \left[\forall x_1, x_2 .\ P(x_1) \ \& \ P(x_2) \Rightarrow (x_1 = x_2)\right]$$

Inverses

Definition 37

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

(i) the *integers*

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

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*.

Idea Understand m/n but within $\mathbb{Z}$.

The division theorem and algorithm

Theorem 38 (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* $m = q \cdot n + r$.

Given m, division by n results in a quotient q and a remainder r, such that $m = q \cdot n + r$

below n

An Argument

with a hidden use of mathematical induction in the form of the well-ordering principle

Given m and n, collect all the natural numbers of the form

$$m - kn$$

for k in the integers.

In particular, $m = m - 0 \cdot n$ so the above makes sense.

From this collection, let r be the smallest such. Claim r is as described in the Thm.