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

$$\mathfrak{m}\left\{\overbrace{\begin{matrix} * & \cdots\cdots\cdots\cdots & * \\ \vdots & \mathfrak{m}\cdot\mathfrak{n} & \vdots \\ * & \cdots\cdots\cdots\cdots & * \end{matrix}}^{\mathfrak{n}}\right.$$

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*.

Commutative monoid laws of addition

$$\underbrace{\;}_{0}\underbrace{*\cdots*}_{n} = \underbrace{*\cdots*}_{n} = \underbrace{*\cdots*}_{n}\underbrace{\;}_{0}$$

neutral element laws

$$\overbrace{*\cdots*\;*\cdots*}^{\ell+m}\overbrace{*\cdots*}^{n} = \overbrace{*\cdots*}^{\ell}\overbrace{*\cdots*\;*\cdots*}^{m+n}$$

associativity law

$$\overbrace{*\cdots*}^{m}\overbrace{*\cdots*}^{n} = \overbrace{*\cdots*}^{n}\overbrace{*\cdots*}^{m}$$

commutativity law

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.

Example

- The ML type α list with neutral element nil and binary operation @ (append) is a monoid.
- int list is a commutative monoid.

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

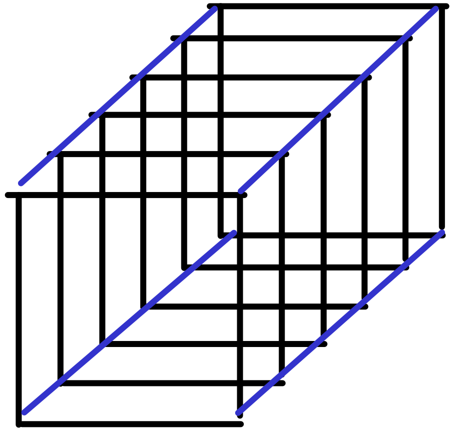
- Monoid laws

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

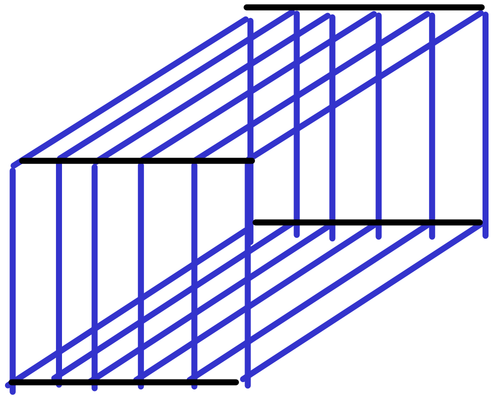
- Commutativity law

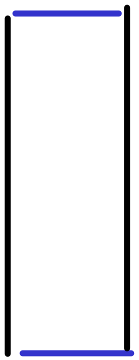
$$m \cdot n = n \cdot m$$

$$1\left[\,\underbrace{* \cdots\cdots *}_{n}\right. = \underbrace{* \cdots\cdots *}_{n} = \left.\underbrace{\begin{matrix} * \\ \vdots \\ * \end{matrix}}_{1}\,\right]n$$



=



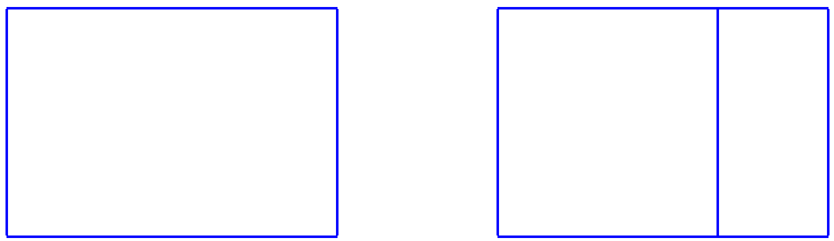


=

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

- Distributive laws $\quad \ell \cdot 0 = 0$

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



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

CANCELLATION

A binary operation $*$ allows cancellation by an element c

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

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

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

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

PROOF: Let x be an element with left inverse ℓ (so that $\ell * x = e$) and right inverse r (so that $x * r = e$).

Then,

$$r = e * r = (\ell * x) * r = \ell * (x * r) = \ell * e$$
$$= \ell$$

$\boxtimes$

Proposition. For a monoid $(e, *)$ if an element has an inverse then it is cancellable.

PROOF: Let c be an element with inverse $\bar{c}$.

<u>RTP</u> $\forall x, y.\ c * x = c * y \Rightarrow x = y$

and $\forall x, y.\ x * c = y * c \Rightarrow x = y$

Assume x and y arbitrary such that $c * x = c * y$

$$(\bar{c} * c) * x = \bar{c} * (c * x) = \bar{c} * (c * y)$$

$$(\bar{c} * c) * x = e * x = x$$

$$\bar{c} * (c * y) = (\bar{c} * c) * y = e * y = y \qquad \boxtimes$$

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.

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*.

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 $\otimes$).