Slides

for Part IA CST 2015/16

Discrete Mathematics

<www.cl.cam.ac.uk/teaching/1516/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

What are we up to?

- Learn to read and write, and also work with, mathematical arguments.
- Doing some basic discrete mathematics.
- Getting a taste of computer science applications.

What is Discrete Mathematics ?

from *Discrete Mathematics (second edition)* by N. Biggs

Discrete Mathematics is the branch of Mathematics in which we deal with questions involving finite or countably infinite sets. In particular this means that the numbers involved are either integers, or numbers closely related to them, such as fractions or 'modular' numbers.

What is it that we do ?

In general:

Build mathematical models and apply methods to analyse problems that arise in computer science.

In particular:

Make and study mathematical constructions by means of definitions and theorems. We aim at understanding their properties and limitations.

Lecture plan

I. Proofs.

II. Numbers.

III. Sets.

IV. Regular languages and finite automata.

Proofs

Objectives

- To develop techniques for analysing and understanding mathematical statements.
- To be able to present logical arguments that establish mathematical statements in the form of clear proofs.
- To prove Fermat's Little Theorem, a basic result in the theory of numbers that has many applications in computer science.

Proofs in practice

We are interested in examining the following statement:

$\boxed{\text{The product of two odd integers is odd.}}$

This seems innocuous enough, but it is in fact full of baggage.

Proofs in practice

We are interested in examining the following statement:

The product of two odd integers is odd.

This seems innocuous enough, but it is in fact full of baggage. For instance, it presupposes that you know:

- what a statement is;
- what the integers $(\ldots,-1,0,1,\ldots)$ are, and that amongst them there is a class of odd ones $(\ldots,-3,-1,1,3,\ldots)$;
- what the product of two integers is, and that this is in turn an integer.

More precisely put, we may write:

$$\boxed{\text{If } m \text{ and } n \text{ are odd integers then so is } m \cdot n.}$$

More precisely put, we may write:

$$\boxed{\text{If } m \text{ and } n \text{ are odd integers then so is } m \cdot n.}$$

which further presupposes that you know:

- what variables are;
- what

  if ... then ...

  statements are, and how one goes about proving them;
- that the symbol "$\cdot$" is commonly used to denote the product operation.

Even more precisely, we should write

$\boxed{\text{For all integers } m \text{ and } n\text{, if } m \text{ and } n \text{ are odd then so is } m \cdot n.}$

which now additionally presupposes that you know:

- what

  for all . . .

  statements are, and how one goes about proving them.

Thus, in trying to understand and then prove the above statement, we are assuming quite a lot of *mathematical jargon* that one needs to learn and practice with to make it a useful, and in fact very powerful, tool.

Some mathematical jargon

Statement

A sentence that is either true or false — but not both.

Example 1

$$\text{‘}e^{i\pi} + 1 = 0\text{’}$$

Non-example

‘This statement is false’

Predicate

A statement whose truth depends on the value of one or more variables.

Example 2

1. ‘$e^{ix} = \cos x + i \sin x$’

2. *‘the function f is differentiable’*

Theorem

A very important true statement.

Proposition

A less important but nonetheless interesting true statement.

Lemma

A true statement used in proving other true statements.

Corollary

A true statement that is a simple deduction from a theorem or proposition.

Example 3

1. *Fermat's Last Theorem*

2. *The Pumping Lemma*

Conjecture

A statement believed to be true, but for which we have no proof.

Example 4

1. *Goldbach's Conjecture*
2. *The Riemann Hypothesis*
3. *Schanuel's Conjecture*

Proof

Logical explanation of why a statement is true; a method for establishing truth.

Proof

Logical explanation of why a statement is true; a method for establishing truth.

Logic

The study of methods and principles used to distinguish good (correct) from bad (incorrect) reasoning.

Example 5

1. *Classical predicate logic*
2. *Hoare logic*
3. *Temporal logic*

Axiom

A basic assumption about a mathematical situation.

Axioms can be considered facts that do not need to be proved (just to get us going in a subject) or they can be used in definitions.

Example 6

1. *Euclidean Geometry*
2. *Riemannian Geometry*
3. *Hyperbolic Geometry*

Definition

An explanation of the mathematical meaning of a word (or phrase).

The word (or phrase) is generally defined in terms of properties.

Warning: It is vitally important that you can recall definitions precisely. A common problem is not to be able to advance in some problem because the definition of a word is unknown.

Definition, theorem, intuition, proof in practice

Proposition 8 *For all integers m and n, if m and n are odd then so is $m \cdot n$.*

Definition, theorem, intuition, proof in practice

Definition 7 *An integer is said to be* <u>odd</u> *whenever it is of the form* $2 \cdot i + 1$ *for some (necessarily unique) integer* i*.*

Proposition 8 *For all integers* m *and* n*, if* m *and* n *are odd then so is* $m \cdot n$*.*

Intuition:

PROOF OF Proposition 8:

Simple and composite statements

A statement is *simple* (or *atomic*) when it cannot be broken into other statements, and it is *composite* when it is built by using several (simple or composite statements) connected by *logical* expressions (e.g., if. . . then. . . ; . . . implies . . . ; . . . if and only if . . . ; . . . and. . . ; either . . . or . . . ; it is not the case that . . . ; for all . . . ; there exists . . . ; etc.)

Examples:

'2 is a prime number'

'for all integers m and n, if $m \cdot n$ is even then either n or m are even'

Implication

Theorems can usually be written in the form

$$\boxed{\begin{array}{l}\textbf{if} \text{ a collection of } \textit{assumptions} \text{ holds,} \\ \textbf{then} \text{ so does some } \textit{conclusion}\end{array}}$$

or, in other words,

$$\boxed{\text{a collection of } \textit{assumptions} \textbf{ implies} \text{ some } \textit{conclusion}}$$

or, in symbols,

$$\boxed{\text{a collection of } \textit{hypotheses} \implies \text{some } \textit{conclusion}}$$

NB Identifying precisely what the assumptions and conclusions are is the first goal in dealing with a theorem.

The main proof strategy for implication:

To prove a goal of the form

$$P \implies Q$$

assume that P is true and prove Q.

NB *Assuming* is not *asserting*! Assuming a statement amounts to the same thing as adding it to your list of hypotheses.

Proof pattern:

In order to prove that

$$\mathrm{P} \implies \mathrm{Q}$$

1. Write: Assume P.
2. Show that Q logically follows.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$
$\vdots$	

After using the strategy

Assumptions	Goal
	Q
$\vdots$	
P	

Proposition 8 *If m and n are odd integers, then so is $m \cdot n$.*

PROOF:

An alternative proof strategy for implication:

To prove an implication, prove instead the equivalent statement given by its contrapositive.

Definition:

the *contrapositive* of ‘P implies Q’ is ‘not Q implies not P’

Proof pattern:

In order to prove that

$$P \implies Q$$

1. Write: We prove the contrapositive; that is, ... and state the contrapositive.
2. Write: Assume 'the negation of Q'.
3. Show that 'the negation of P' logically follows.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$
$\vdots$	

After using the strategy

Assumptions	Goal
	not P
$\vdots$	
not Q	

Definition 9 *A real number is:*

- rational *if it is of the form m/n for a pair of integers m and n; otherwise it is* irrational*.*
- positive *if it is greater than 0, and* negative *if it is smaller than 0.*
- nonnegative *if it is greater than or equal 0, and* nonpositive *if it is smaller than or equal 0.*
- natural *if it is a nonnegative integer.*

Proposition 10 *Let x be a positive real number. If x is irrational then so is $\sqrt{x}$.*

PROOF:

Logical Deduction
— Modus Ponens —

A main rule of *logical deduction* is that of *Modus Ponens*:

> From the statements P and $P \implies Q$,
> the statement Q follows.

or, in other words,

> If P and $P \implies Q$ hold then so does Q.

or, in symbols,

$$\frac{P \qquad P \implies Q}{Q}$$

The use of implications:

To use an assumption of the form $\mathrm{P} \implies \mathrm{Q}$, aim at establishing P.
Once this is done, by Modus Ponens, one can conclude Q and so further assume it.

Theorem 11 *Let* P_1*,* P_2*, and* P_3 *be statements. If* $P_1 \implies P_2$ *and* $P_2 \implies P_3$ *then* $P_1 \implies P_3$*.*

PROOF:

Bi-implication

Some theorems can be written in the form

$$\boxed{\text{P is equivalent to Q}}$$

or, in other words,

$$\boxed{\text{P implies Q, and vice versa}}$$

or

$$\boxed{\text{Q implies P, and vice versa}}$$

or

$$\boxed{\text{P if, and only if, Q}} \qquad \boxed{\text{P iff Q}}$$

or, in symbols,

$$\boxed{P \iff Q}$$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: $(\Longrightarrow)$ and give a proof of $P \implies Q$.
2. Write: $(\Longleftarrow)$ and give a proof of $Q \implies P$.

Proposition 12 *Suppose that n is an integer. Then, n is even iff n^2 is even.*

PROOF:

Divisibility and congruence

Definition 13 *Let* d *and* n *be integers. We say that* d *divides* n*, and write* $d \mid n$*, whenever there is an integer* k *such that* $n = k \cdot d$*.*

Example 14 *The statement* $2 \mid 4$ *is true, while* $4 \mid 2$ *is not.*

Definition 15 *Fix a positive integer* m*. For integers* a *and* b*, we say that* a *is congruent to* b *modulo* m*, and write* $a \equiv b \pmod{m}$*, whenever* $m \mid (a - b)$*.*

Example 16

1. $18 \equiv 2 \pmod{4}$
2. $2 \equiv -2 \pmod{4}$
3. $18 \equiv -2 \pmod{4}$

Proposition 17 *For every integer n,*

1. *n is even if, and only if, $n \equiv 0 \pmod 2$, and*
2. *n is odd if, and only if, $n \equiv 1 \pmod 2$.*

PROOF:

The use of bi-implications:

To use an assumption of the form $P \iff Q$, use it as two separate assumptions $P \implies Q$ and $Q \implies P$.

Universal quantification

Universal statements are of the form

> **for all** individuals x of the universe of discourse, the property $P(x)$ holds

or, in other words,

> no matter what individual x in the universe of discourse one considers, the property $P(x)$ for it holds

or, in symbols,

$$\boxed{\forall x.\, P(x)}$$

Example 18

2. *For every positive real number x, if x is irrational then so is $\sqrt{x}$.*

3. *For every integer n, we have that n is even iff so is n^2.*

The main proof strategy for universal statements:

To prove a goal of the form

$$\forall x.\, P(x)$$

let x stand for an arbitrary individual and prove $P(x)$.

Proof pattern:

In order to prove that

$$\forall x.\, P(x)$$

1. Write: Let x be an arbitrary individual.

2. Show that $P(x)$ holds.

Proof pattern:

In order to prove that

$$\forall x.\, P(x)$$

1. Write: Let x be an arbitrary individual.

   Warning: Make sure that the variable x is new (also referred to as fresh) in the proof! If for some reason the variable x is already being used in the proof to stand for something else, then you must use an unused variable, say y, to stand for the arbitrary individual, and prove $P(y)$.

2. Show that $P(x)$ holds.

Scratch work:

Before using the strategy

Assumptions	Goal
	$\forall x.\, P(x)$
$\vdots$	

After using the strategy

Assumptions	Goal
	$P(x)$ (for a new (or fresh) x)
$\vdots$	

The use of universal statements:

To use an assumption of the form $\forall x.\, P(x)$, you can plug in any value, say a, for x to conclude that $P(a)$ is true and so further assume it.

This rule is called *universal instantiation*.

Proposition 19 *Fix a positive integer* m*. For integers* a *and* b*, we have that* $a \equiv b \pmod{m}$ *if, and only if, for all positive integers* n*, we have that* $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$*.*

PROOF:

Equality axioms

Just for the record, here are the axioms for *equality*.

- Every individual is equal to itself.

$$\forall x.\ x = x$$

- For any pair of equal individuals, if a property holds for one of them then it also holds for the other one.

$$\forall x. \forall y.\ x = y \implies \big(P(x) \implies P(y)\big)$$

NB From these axioms one may deduce the usual intuitive properties of equality, such as

$$\forall x. \forall y. \, x = y \implies y = x$$

and

$$\forall x. \forall y. \forall z. \, x = y \implies (y = z \implies x = z) \quad .$$

However, in practice, you will not be required to formally do so; rather you may just use the properties of equality that you are already familiar with.

Conjunction

Conjunctive statements are of the form

$$\boxed{P \textbf{ and } Q}$$

or, in other words,

$$\boxed{\text{both } P \text{ and also } Q \text{ hold}}$$

or, in symbols,

$$\boxed{P \wedge Q} \qquad \text{or} \qquad \boxed{P \mathbin{\&} Q}$$

The proof strategy for conjunction:

To prove a goal of the form

$$P \wedge Q$$

first prove P and subsequently prove Q (or vice versa).

Proof pattern:

In order to prove

$$P \wedge Q$$

1. Write: Firstly, we prove P. and provide a proof of P.
2. Write: Secondly, we prove Q. and provide a proof of Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \wedge Q$
$\vdots$	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	P		Q
$\vdots$		$\vdots$	

The use of conjunctions:

To use an assumption of the form $P \wedge Q$,
treat it as two separate assumptions: P and Q.

Theorem 20 *For every integer n, we have that $6 \mid n$ iff $2 \mid n$ and $3 \mid n$.*

PROOF:

Existential quantification

Existential statements are of the form

> **there exists** an individual x in the universe of discourse for which the property $P(x)$ holds

or, in other words,

> **for some** individual x in the universe of discourse, the property $P(x)$ holds

or, in symbols,

$$\boxed{\exists x.\, P(x)}$$

Example: The Pigeonhole Principle.

Let n be a positive integer. If $n+1$ letters are put in n pigeonholes then there will be a pigeonhole with more than one letter.

Theorem 21 (Intermediate value theorem) *Let f be a real-valued continuous function on an interval $[a, b]$. For every y in between $f(a)$ and $f(b)$, there exists v in between a and b such that $f(v) = y$.*

Intuition:

The main proof strategy for existential statements:

To prove a goal of the form

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

find a ***witness*** for the existential statement; that is, a value of x, say w, for which you think $P(x)$ will be true, and show that indeed $P(w)$, i.e. the predicate $P(x)$ instantiated with the value w, holds.

Proof pattern:

In order to prove

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

1. Write: $\mathrm{Let}\ w = \ldots$ (the witness you decided on).
2. Provide a proof of $P(w)$.

Scratch work:

Before using the strategy

Assumptions	Goal
	$\exists x. P(x)$
$\vdots$	

After using the strategy

Assumptions	Goals
	$P(w)$
$\vdots$	

$w = \ldots$ (the witness you decided on)

Proposition 22 *For every positive integer* k*, there exist natural numbers* i *and* j *such that* $4 \cdot k = i^2 - j^2$*.*

PROOF:

The use of existential statements:

To use an assumption of the form $\exists x.\, P(x)$, introduce a new variable x_0 into the proof to stand for some individual for which the property $P(x)$ holds. This means that you can now assume $P(x_0)$ true.

Theorem 24 *For all integers* l, m, n, *if* $l \mid m$ *and* $m \mid n$ *then* $l \mid n$.

PROOF:

Unique existence

The notation

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

stands for

the *unique existence* of an x for which the property $P(x)$ holds .

That is,

$$\exists x.\, P(x) \;\wedge\; \Big(\forall y.\, \forall z.\, \big(P(y) \wedge P(z)\big) \implies y = z\Big)$$

Disjunction

Disjunctive statements are of the form

$$\boxed{P \text{ or } Q}$$

or, in other words,

$$\boxed{\text{either } P,\ Q, \text{ or both hold}}$$

or, in symbols,

$$\boxed{P \vee Q}$$

The main proof strategy for disjunction:

To prove a goal of the form

$$P \vee Q$$

you may

1. try to prove P (if you succeed, then you are done); or
2. try to prove Q (if you succeed, then you are done); otherwise
3. break your proof into cases; proving, in each case, either P or Q.

Proposition 25 *For all integers* n*, either* $n^2 \equiv 0 \pmod 4$ *or* $n^2 \equiv 1 \pmod 4$*.*

PROOF:

The use of disjunction:

To use a disjunctive assumption

$$P_1 \vee P_2$$

to establish a goal Q, consider the following two cases in turn: (i) assume P_1 to establish Q, and (ii) assume P_2 to establish Q.

Scratch work:

Before using the strategy

Assumptions	Goal
	Q
$\vdots$	
$P_1 \vee P_2$	

After using the strategy

Assumptions	Goal	‖	Assumptions	Goal
	Q	‖		Q
$\vdots$		‖	$\vdots$	
P_1		‖	P_2	

Proof pattern:

In order to prove Q from some assumptions amongst which there is

$$P_1 \vee P_2$$

write: We prove the following two cases in turn: (i) that assuming P_1, we have Q; and (ii) that assuming P_2, we have Q. Case (i): Assume P_1. and provide a proof of Q from it and the other assumptions. Case (ii): Assume P_2. and provide a proof of Q from it and the other assumptions.

A little arithmetic

Lemma 27 *For all positive integers* p *and natural numbers* m*, if* $m = 0$ *or* $m = p$ *then* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF:

Lemma 28 *For all integers* p *and* m*, if* p *is prime and* $0 < m < p$ *then* $\binom{p}{m} \equiv 0 \pmod{p}$.

PROOF:

Proposition 29 *For all prime numbers* p *and integers* $0 \leq m \leq p$*, either* $\binom{p}{m} \equiv 0 \pmod{p}$ *or* $\binom{p}{m} \equiv 1 \pmod{p}$*.*

PROOF:

A little more arithmetic

Corollary 33 (The Freshman's Dream) *For all natural numbers m, n and primes p,*

$$(m+n)^p \equiv m^p + n^p \pmod{p} \ .$$

PROOF:

Corollary 34 (The Dropout Lemma) *For all natural numbers* m *and primes* p,

$$(m+1)^p \equiv m^p + 1 \pmod{p} \ .$$

Proposition 35 (The Many Dropout Lemma) *For all natural numbers* m *and* i, *and primes* p,

$$(m+i)^p \equiv m^p + i \pmod{p} \ .$$

PROOF:

The Many Dropout Lemma (Proposition 35) gives the fist part of the following very important theorem as a corollary.

Theorem 36 (Fermat's Little Theorem) *For all natural numbers* i *and primes* p*,*

1. $i^p \equiv i \pmod{p}$*, and*
2. $i^{p-1} \equiv 1 \pmod{p}$ *whenever* i *is not a multiple of* p*.*

The fact that the first part of Fermat's Little Theorem implies the second one will be proved later on .

Btw

1. Fermat's Little Theorem has applications to:
   (a) primality testing[a],
   (b) the verification of floating-point algorithms, and
   (c) cryptographic security.

[a] For instance, to establish that a positive integer m is not prime one may proceed to find an integer i such that $i^m \not\equiv i \pmod{m}$.

Negation

Negations are statements of the form

$$\boxed{\text{not } P}$$

or, in other words,

$$\boxed{P \text{ is not the case}}$$

or

$$\boxed{P \text{ is absurd}}$$

or

$$\boxed{P \text{ leads to contradiction}}$$

or, in symbols,

$$\boxed{\neg P}$$

A first proof strategy for negated goals and assumptions:

If possible, reexpress the negation in an *equivalent* form and use instead this other statement.

Logical equivalences

$$
\begin{array}{rcl}
\neg(\,P \Longrightarrow Q\,) & \Longleftrightarrow & P \wedge \neg Q \\
\neg(\,P \Longleftrightarrow Q\,) & \Longleftrightarrow & P \Longleftrightarrow \neg Q \\
\neg(\forall x.\, P(x)) & \Longleftrightarrow & \exists x.\, \neg P(x) \\
\neg(P \wedge Q) & \Longleftrightarrow & (\neg P) \vee (\neg Q) \\
\neg(\exists x.\, P(x)) & \Longleftrightarrow & \forall x.\, \neg P(x) \\
\neg(P \vee Q) & \Longleftrightarrow & (\neg P) \wedge (\neg Q) \\
\neg(\neg P) & \Longleftrightarrow & P \\
\neg P & \Longleftrightarrow & (P \Rightarrow \mathbf{false})
\end{array}
$$

Theorem 37 *For all statements* P *and* Q*,*

$$(\mathrm{P} \implies \mathrm{Q}) \implies (\neg\mathrm{Q} \implies \neg\mathrm{P}) \quad .$$

PROOF:

Proof by contradiction

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg\mathsf{P} \implies \mathbf{false}$

Proof by contradiction

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg P \implies \mathbf{false}$

Proof pattern:

In order to prove

$$P$$

1. Write: We use proof by contradiction. So, suppose P is false.
2. Deduce a logical contradiction.
3. Write: This is a contradiction. Therefore, P must be true.

Scratch work:

Before using the strategy

Assumptions	Goal
	P
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$\neg P$	

Theorem 38 *For all statements* P *and* Q,

$$(\neg \mathrm{Q} \implies \neg \mathrm{P}) \implies (\mathrm{P} \implies \mathrm{Q}) \quad .$$

PROOF:

Lemma 40 *A positive real number* x *is rational iff*

$$\exists \textit{ positive integers } m, n : \quad x = m/n \ \wedge\ \neg\big(\exists \textit{ prime } p :\ p \mid m \ \wedge\ p \mid n\big) \tag{$\dagger$}$$

PROOF:

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*

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

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

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

- Multiplication

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

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

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

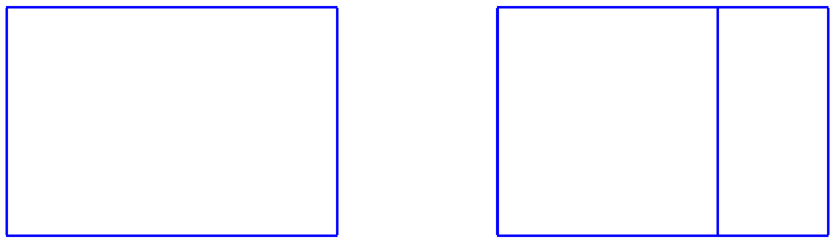
- Commutativity law

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

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 41

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

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

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 ) )
```

Theorem 44 *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 45 *Let* m *be a positive integer. For all natural numbers* k *and* l*,*

$$k \equiv l \pmod{m} \iff \mathrm{rem}(k, m) = \mathrm{rem}(l, m) \quad .$$

PROOF:

Corollary 46 *Let m be a positive integer.*

1. *For every natural number n,*

$$n \equiv \mathrm{rem}(n, m) \pmod{m} \quad .$$

PROOF:

Corollary 46 *Let m be a positive integer.*

1. *For every natural number n,*

$$n \equiv \mathrm{rem}(n, m) \pmod{m} \quad .$$

2. *For every integer k there exists a unique integer $[k]_m$ such that*

$$0 \leq [k]_m < m \quad \textit{and} \quad k \equiv [k]_m \pmod{m} \quad .$$

PROOF:

Modular arithmetic

For every positive integer m, the *integers modulo* m are:

$$\mathbb{Z}_m \;:\quad 0\ ,\quad 1\ ,\quad \ldots\ ,\quad m-1\ .$$

with arithmetic operations of addition $+_m$ and multiplication $\cdot_m$ defined as follows

$$\begin{aligned} k +_m l &= [k+l]_m &= \mathrm{rem}(k+l, m)\ , \\ k \cdot_m l &= [k \cdot l]_m &= \mathrm{rem}(k \cdot l, m) \end{aligned}$$

for all $0 \leq k, l < m$.

Example 48 *The addition and multiplication tables for* $\mathbb{Z}_4$ *are:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	3
2	2
3	1

	multiplicative inverse
0	$-$
1	1
2	$-$
3	3

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.

Example 49 *The addition and multiplication tables for* $\mathbb{Z}_5$ *are:*

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	4
2	3
3	2
4	1

	multiplicative inverse
0	—
1	1
2	3
3	2
4	4

Surprisingly, every non-zero element has a multiplicative inverse.

Proposition 50 *For all natural numbers* $m > 1$, *the modular-arithmetic structure*

$$(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$$

is a commutative ring.

NB Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses .

Important mathematical jargon: Sets

Very roughly, sets are the mathematicians' data structures. Informally, we will consider a *set* as a (well-defined, unordered) collection of mathematical objects, called the *elements* (or *members*) of the set.

Set membership

The symbol '$\in$' known as the *set membership* predicate is central to the theory of sets, and its purpose is to build statements of the form

$$x \in A$$

that are true whenever it is the case that the object x is an element of the set A, and false otherwise.

Defining sets

The set	of even primes	is	$\{2\}$
	of booleans		$\{\mathbf{true}, \mathbf{false}\}$
	$[-2..3]$		$\{-2, -1, 0, 1, 2, 3\}$

Set comprehension

The basic idea behind set comprehension is to define a set by means of a property that precisely characterises all the elements of the set.

Notations:

$$\{ x \in A \mid P(x) \} \quad , \qquad \{ x \in A : P(x) \}$$

Greatest common divisor

Given a natural number n, the set of its *divisors* is defined by set comprehension as follows

$$D(n) = \{ \, d \in \mathbb{N} : d \mid n \, \} \quad .$$

Example 52

1. $D(0) = \mathbb{N}$
2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 68, \\ 72, 102, 136, 153, 204, 306, 408, 612, 1224 \end{array} \right\}$

Remark Sets of divisors are hard to compute. However, the computation of the greatest divisor is straightforward. :)

Going a step further, what about the *common divisors* of pairs of natural numbers? That is, the set

$$\mathrm{CD}(m,n) = \{\, d \in \mathbb{N} : d \mid m \wedge d \mid n \,\}$$

for $m, n \in \mathbb{N}$.

Example 53

$$\mathrm{CD}(1224, 660) = \{\, 1, 2, 3, 4, 6, 12 \,\}$$

Since $\mathrm{CD}(n,n) = \mathrm{D}(n)$, the computation of common divisors is as hard as that of divisors. But, what about the computation of the *greatest common divisor*?

Lemma 55 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $m \equiv m' \pmod{n}$*. Then,*

$$\mathrm{CD}(m, n) = \mathrm{CD}(m', n) \quad .$$

PROOF:

Lemma 57 *For all positive integers* m *and* n,

$$\mathrm{CD}(\mathrm{m},\mathrm{n}) = \begin{cases} \mathrm{D}(\mathrm{n}) & \text{, } \textit{if } \mathrm{n} \mid \mathrm{m} \\ \mathrm{CD}\big(\mathrm{n}, \mathrm{rem}(\mathrm{m},\mathrm{n})\big) & \text{, } \textit{otherwise} \end{cases}$$

Lemma 57 *For all positive integers m and n,*

$$\mathrm{CD}(m,n) = \begin{cases} \mathrm{D}(n) & \text{, } \textit{if } n \mid m \\ \mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, } \textit{otherwise} \end{cases}$$

Since a positive integer n is the greatest divisor in $\mathrm{D}(n)$, the lemma suggests a recursive procedure:

$$\gcd(m,n) = \begin{cases} n & \text{, if } n \mid m \\ \gcd\big(n, \mathrm{rem}(m,n)\big) & \text{, otherwise} \end{cases}$$

for computing the *greatest common divisor*, of two positive integers m and n. This is

Euclid's Algorithm

gcd

```
fun gcd( m , n )
  =  let
       val ( q , r ) = divalg( m , n )
     in
       if r = 0 then n
       else gcd( n , r )
     end
```

Example 58 ($\mathrm{gcd}(13, 34) = 1$)

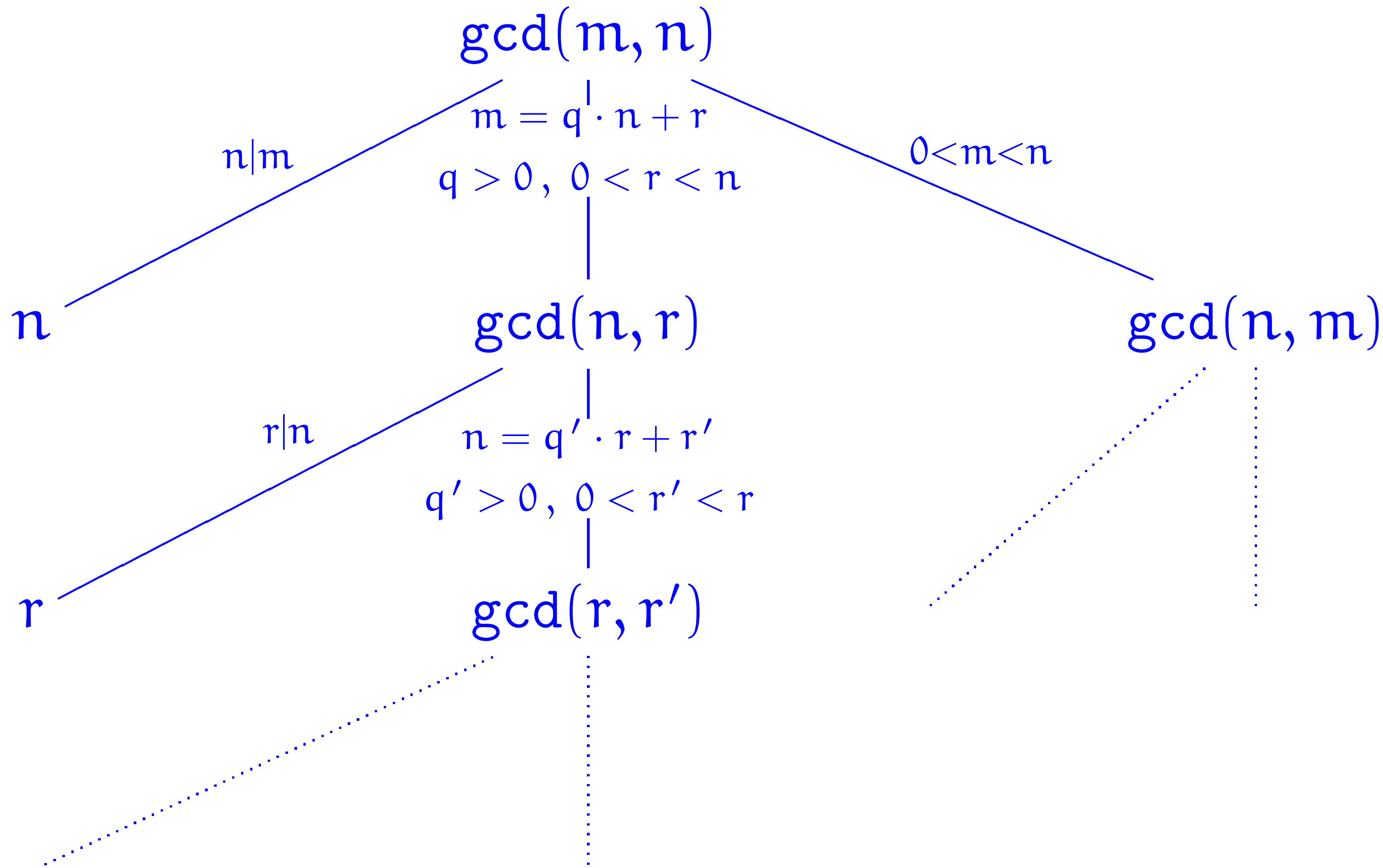
$$
\begin{aligned}
\mathrm{gcd}(13, 34) &= \mathrm{gcd}(34, 13) \\
&= \mathrm{gcd}(13, 8) \\
&= \mathrm{gcd}(8, 5) \\
&= \mathrm{gcd}(5, 3) \\
&= \mathrm{gcd}(3, 2) \\
&= \mathrm{gcd}(2, 1) \\
&= 1
\end{aligned}
$$

Theorem 59 *Euclid's Algorithm* $\mathtt{gcd}$ *terminates on all pairs of positive integers and, for such* m *and* n, $\mathtt{gcd}(m, n)$ *is the greatest common divisor of* m *and* n *in the sense that the following two properties hold:*

(i) *both* $\mathtt{gcd}(m, n) \mid m$ *and* $\mathtt{gcd}(m, n) \mid n$, *and*

(ii) *for all positive integers* d *such that* $d \mid m$ *and* $d \mid n$ *it necessarily follows that* $d \mid \mathtt{gcd}(m, n)$.

PROOF:


gcd(m, n)
n|m
m = q · n + r
q > 0 , 0 < r < n
0<m<n
n
gcd(n, r)
gcd(n, m)
r|n
n = q′ · r + r′
q′ > 0 , 0 < r′ < r
r
gcd(r, r′)

Fractions in lowest terms

```
fun lowterms( m , n )
  = let
      val gcdval = gcd( m , n )
    in
      ( m div gcdval , n div gcdval )
    end
```

Some fundamental properties of gcds

Lemma 61 *For all positive integers* l, m, *and* n,

1. ***(Commutativity)*** $\gcd(m, n) = \gcd(n, m)$,
2. ***(Associativity)*** $\gcd\big(l, \gcd(m, n)\big) = \gcd(\gcd(l, m), n)$,
3. ***(Linearity)***[a] $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m, n)$.

PROOF:

[a] Aka (Distributivity).

Euclid's Theorem

Theorem 62 *For positive integers* k, m, *and* n, *if* $k \mid (m \cdot n)$ *and* $\gcd(k, m) = 1$ *then* $k \mid n$.

PROOF:

Corollary 63 (Euclid's Theorem) *For positive integers* m *and* n*, and prime* p*, if* $p \mid (m \cdot n)$ *then* $p \mid m$ *or* $p \mid n$*.*

Now, the second part of Fermat's Little Theorem follows as a corollary of the first part and Euclid's Theorem.

PROOF:

Fields of modular arithmetic

Corollary 64 *For prime p, every non-zero element i of $\mathbb{Z}_p$ has $[i^{p-2}]_p$ as multiplicative inverse. Hence, $\mathbb{Z}_p$ is what in the mathematical jargon is referred to as a field.*

Extended Euclid's Algorithm

Example 65 ($\mathtt{egcd}(34, 13) = \big((5, -13), 1\big)$)

$$
\begin{array}{rl||rcrcrcr||}
 & \gcd(34, 13) & 34 & = & 2\cdot & 13 & + & 8 \\
= & \gcd(13, 8) & 13 & = & 1\cdot & 8 & + & 5 \\
= & \gcd(8, 5) & 8 & = & 1\cdot & 5 & + & 3 \\
= & \gcd(5, 3) & 5 & = & 1\cdot & 3 & + & 2 \\
= & \gcd(3, 2) & 3 & = & 1\cdot & 2 & + & 1 \\
= & \gcd(2, 1) & 2 & = & 2\cdot & 1 & + & 0 \\
= & 1 & & & & & &
\end{array}
$$

Extended Euclid's Algorithm

Example 65 ($\mathtt{egcd}(34, 13) = \big((5, -13), 1\big)$)

$$
\begin{array}{rl||rcrrcr||rcrrr}
 & \gcd(34, 13) & 34 & = & 2\cdot & 13 & + & 8 & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13, 8) & 13 & = & 1\cdot & 8 & + & 5 & 5 & = & 13 & -1\cdot & 8 \\
= & \gcd(8, 5) & 8 & = & 1\cdot & 5 & + & 3 & 3 & = & 8 & -1\cdot & 5 \\
= & \gcd(5, 3) & 5 & = & 1\cdot & 3 & + & 2 & 2 & = & 5 & -1\cdot & 3 \\
= & \gcd(3, 2) & 3 & = & 1\cdot & 2 & + & 1 & 1 & = & 3 & -1\cdot & 2 \\
= & \gcd(2, 1) & 2 & = & 2\cdot & 1 & + & 0 & & & & & \\
= & 1 & & & & & & & & & & &
\end{array}
$$

$$
\begin{array}{rl||rrrr}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & & & & \\
 & & & & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & & & & \\
 & & & & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & & & & \\
 & & & & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rlccc}
 & \gcd(34,13) & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 & = & 13 & -1\cdot & 8 \\
 & & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & & = & \multicolumn{3}{l}{-1\cdot 34+3\cdot 13} \\
= & \gcd(8,5) & 3 & = & 8 & -1\cdot & 5 \\
= & \gcd(5,3) & 2 & = & 5 & -1\cdot & 3 \\
= & \gcd(3,2) & 1 & = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rcrc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & & & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rcccc}
 & \gcd(34,13) & 8 = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 = & 13 & -1\cdot & 8 \\
 & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 = & 8 & -1\cdot & 5 \\
 & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 = & 5 & -1\cdot & 3 \\
 & & = & \overbrace{-1\cdot 34+3\cdot 13} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)} \\
 & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 = & 3 & -1\cdot & 2
\end{array}
$$

$$
\begin{array}{rl||rclcl}
 & \gcd(34,13) & 8 & = & 34 & -2\cdot & 13 \\
= & \gcd(13,8) & 5 & = & 13 & -1\cdot & 8 \\
 & & & = & 13 & -1\cdot & \overbrace{(34-2\cdot 13)} \\
 & & & = & -1\cdot 34+3\cdot 13 & & \\
= & \gcd(8,5) & 3 & = & 8 & -1\cdot & 5 \\
 & & & = & \overbrace{(34-2\cdot 13)} & -1\cdot & \overbrace{(-1\cdot 34+3\cdot 13)} \\
 & & & = & 2\cdot 34+(-5)\cdot 13 & & \\
= & \gcd(5,3) & 2 & = & 5 & -1\cdot & 3 \\
 & & & = & \overbrace{-1\cdot 34+3\cdot 13} & -1\cdot & \overbrace{(2\cdot 34+(-5)\cdot 13)} \\
 & & & = & -3\cdot 34+8\cdot 13 & & \\
= & \gcd(3,2) & 1 & = & 3 & -1\cdot & 2 \\
 & & & = & \overbrace{(2\cdot 34+(-5)\cdot 13)} & -1\cdot & \overbrace{(-3\cdot 34+8\cdot 13)}) \\
 & & & = & 5\cdot 34+(-13)\cdot 13 & &
\end{array}
$$

Linear combinations

Definition 66 *An integer* r *is said to be a* linear combination *of a pair of integers* m *and* n *whenever*

> *there exist a pair of integers* s *and* t, *referred to as the* coefficients *of the linear combination, such that*
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \quad ;$$
>
> *that is*
>
> $$s \cdot m + t \cdot n = r \quad .$$

Theorem 67 *For all positive integers* m *and* n*,*

1. $\gcd(m, n)$ *is a linear combination of* m *and* n*, and*
2. *a pair* $\mathrm{lc}_1(m, n)$*,* $\mathrm{lc}_2(m, n)$ *of integer coefficients for it, i.e. such that*

$$\begin{bmatrix} \mathrm{lc}_1(m, n) & \mathrm{lc}_2(m, n) \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = \gcd(m, n) \quad ,$$

can be efficiently computed.

Proposition 68 *For all integers m and n,*

1. $\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \quad \wedge \quad \begin{bmatrix} 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$ *;*

2. *for all integers s_1, t_1, r_1 and s_2, t_2, r_2,*

   $$\begin{bmatrix} s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 \quad \wedge \quad \begin{bmatrix} s_2 & t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_2$$

   implies

   $$\begin{bmatrix} s_1 + s_2 & t_1 + t_2 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r_1 + r_2 \quad ;$$

3. *for all integers k and s, t, r,*

   $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \text{ implies } \begin{bmatrix} k \cdot s & k \cdot t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = k \cdot r \quad .$$

gcd

```
fun  gcd( m , n )
= let
    fun  gcditer(          r1   ,  c as          r2  )
    = let
        val (q,r) = divalg(r1,r2)   (* r = r1-q*r2 *)
      in
        if r = 0
        then  c
        else  gcditer(  c ,                      r  )
      end
  in
    gcditer(          m   ,          n  )
  end
```

egcd

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (q,r) = divalg(r1,r2)    (* r = r1-q*r2 *)
      in
        if r = 0
        then lc
        else egcditer( lc , ((s1-q*s2,t1-q*t2),r) )
      end
  in
    egcditer( ((1,0),m) , ((0,1),n) )
  end
```

```
fun gcd( m , n ) = #2( egcd( m , n ) )

fun lc1( m , n ) = #1( #1( egcd( m , n ) ) )

fun lc2( m , n ) = #2( #1( egcd( m , n ) ) )
```

Multiplicative inverses in modular arithmetic

Corollary 72 *For all positive integers* m *and* n*,*

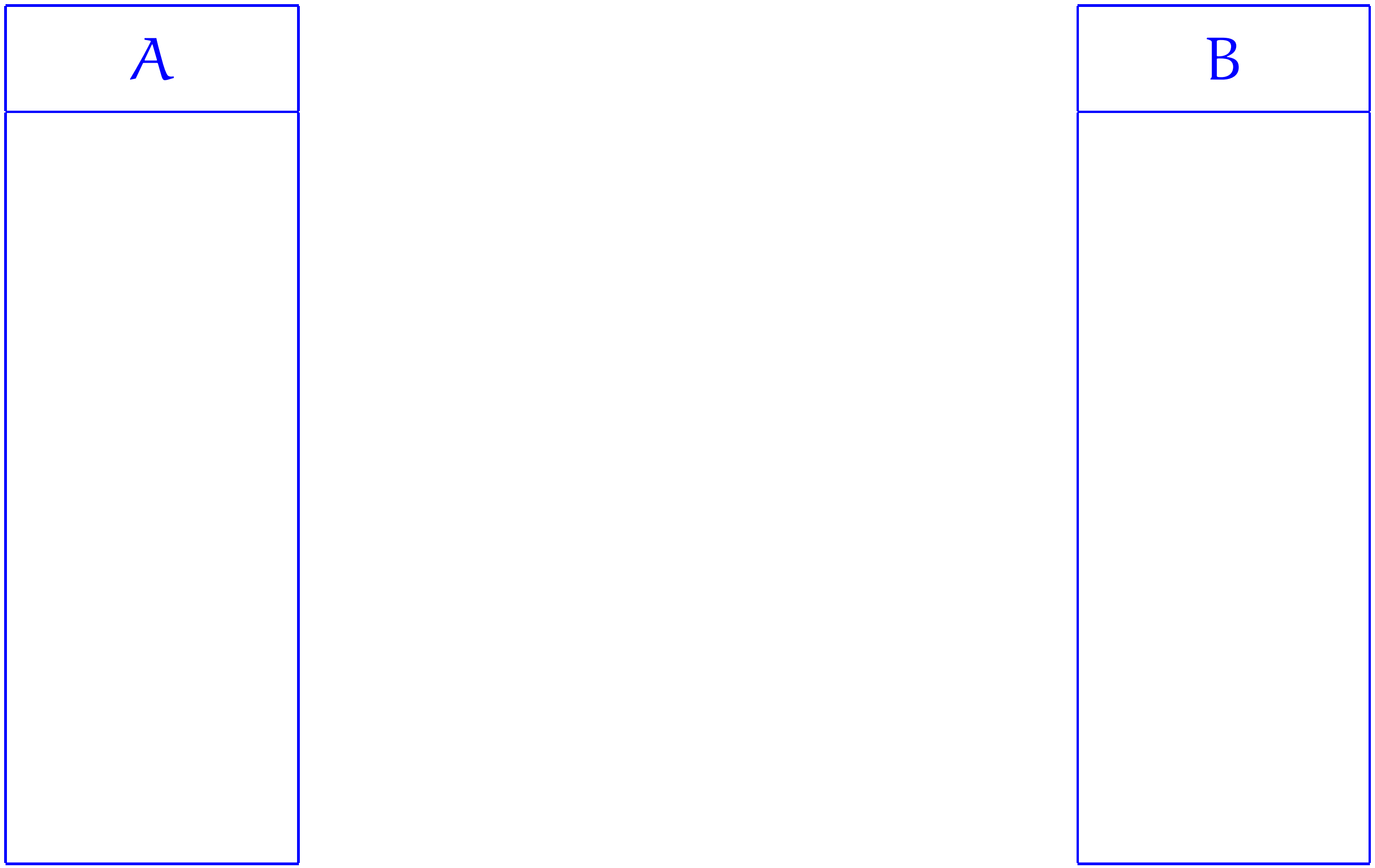
1. $n \cdot \mathrm{lc}_2(m,n) \equiv \gcd(m,n) \pmod{m}$*, and*

2. *whenever* $\gcd(m,n) = 1$*,*

   $\big[\mathrm{lc}_2(m,n)\big]_m$ *is the multiplicative inverse of* $[n]_m$ *in* $\mathbb{Z}_m$.

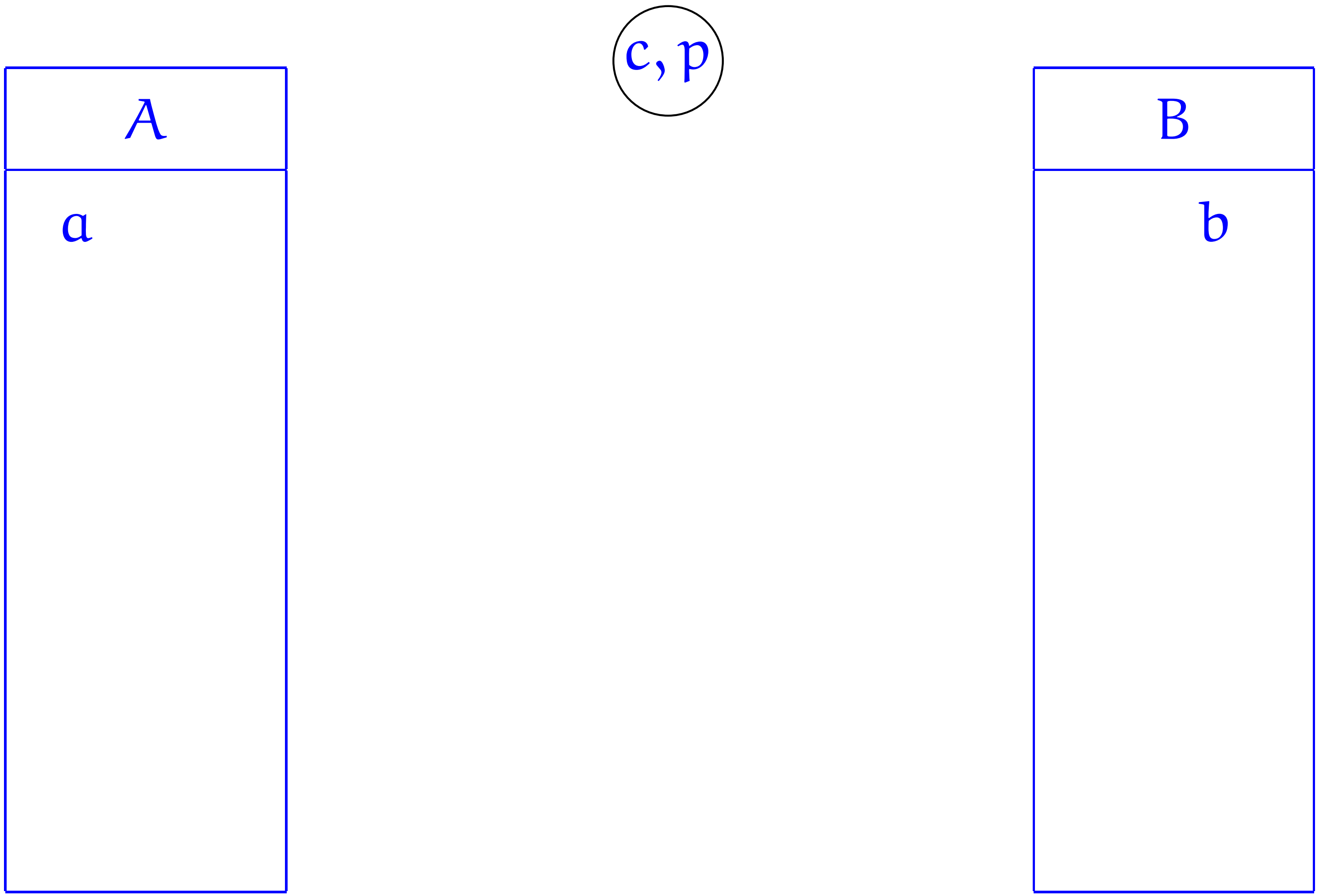
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

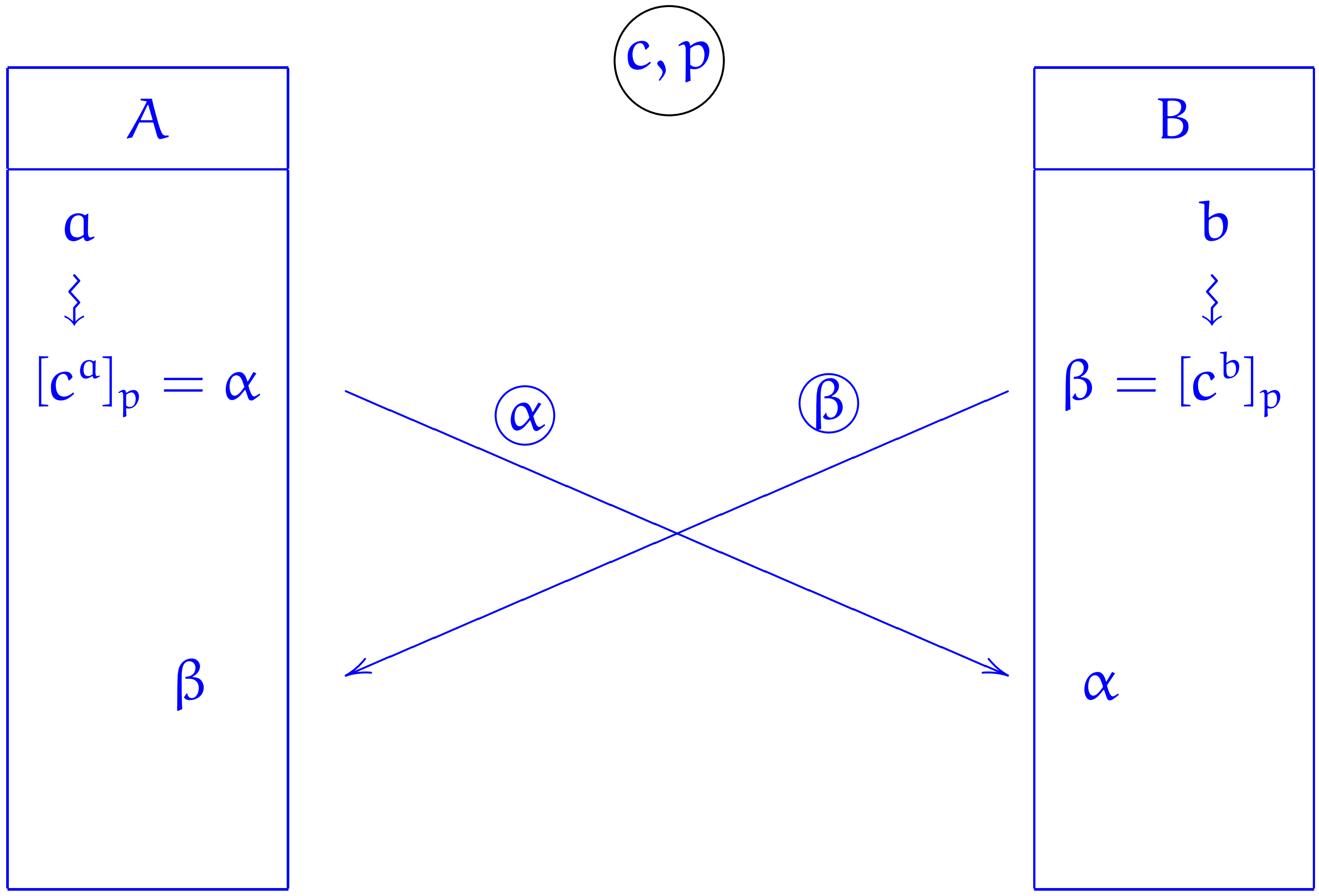
Shared secret key

c, p

A	B
a	b
$\Downarrow$	$\Downarrow$
$[c^a]_p = \alpha$	$\beta = [c^b]_p$

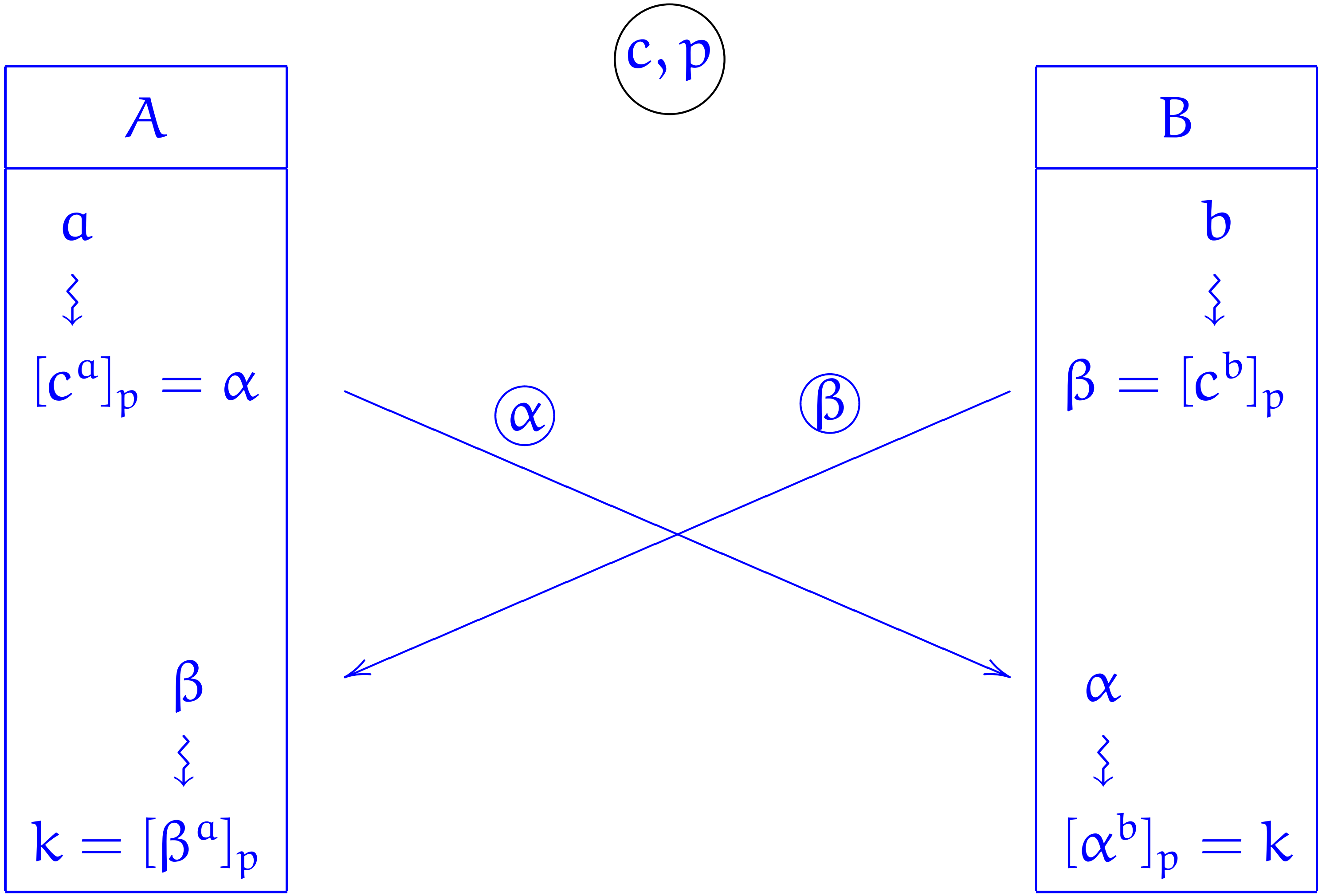
Diffie-Hellman cryptographic method

Shared secret key



Diffie-Hellman cryptographic method

Shared secret key



Key exchange

Lemma 73 *Let* p *be a prime and* e *a positive integer with* $\gcd(p-1, e) = 1$. *Define*

$$d = \left[\, \mathrm{lc}_2(p-1, e)\, \right]_{p-1} \quad .$$

Then, for all integers k,

$$(k^e)^d \equiv k \pmod{p} \quad .$$

PROOF:

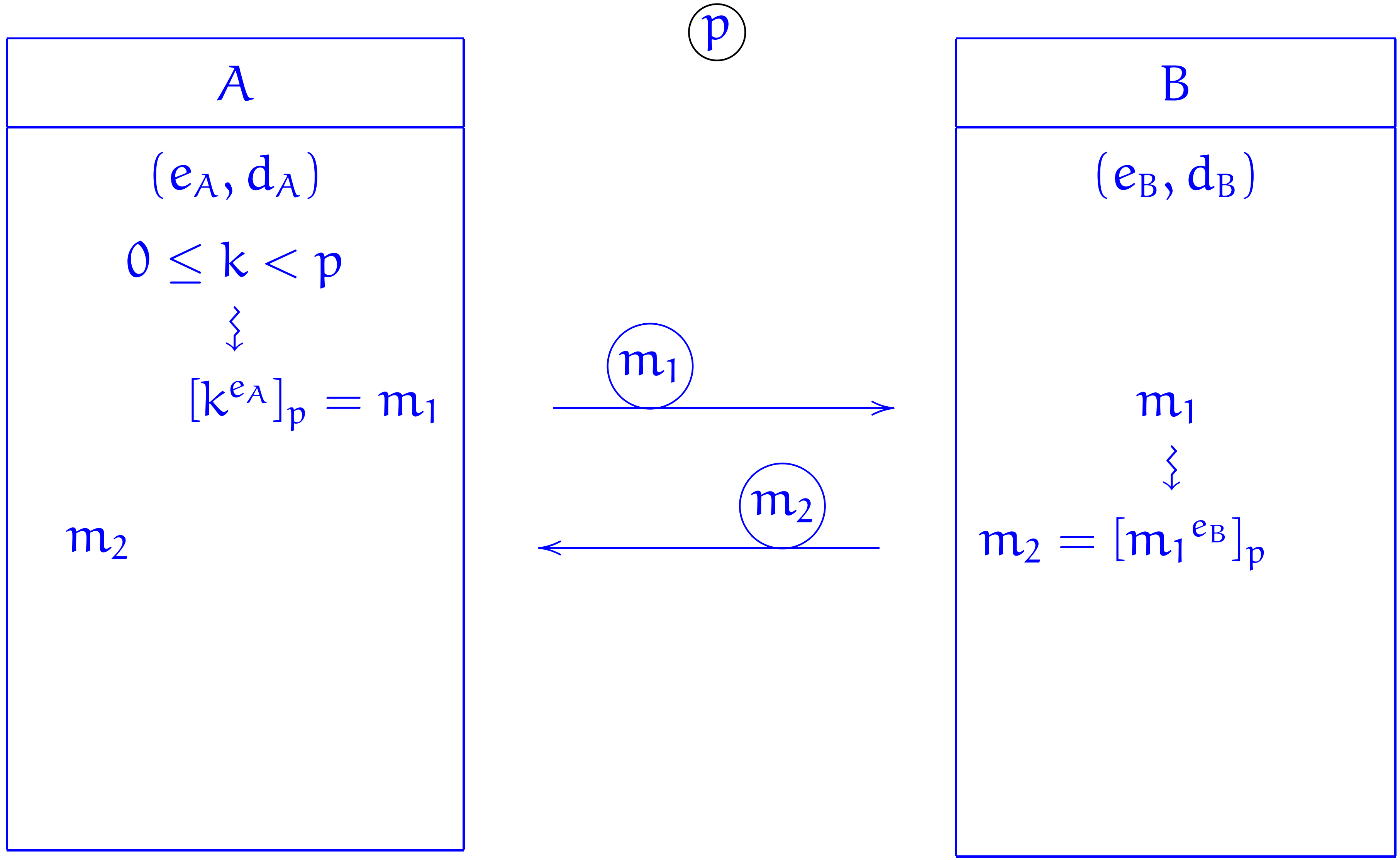
A	B

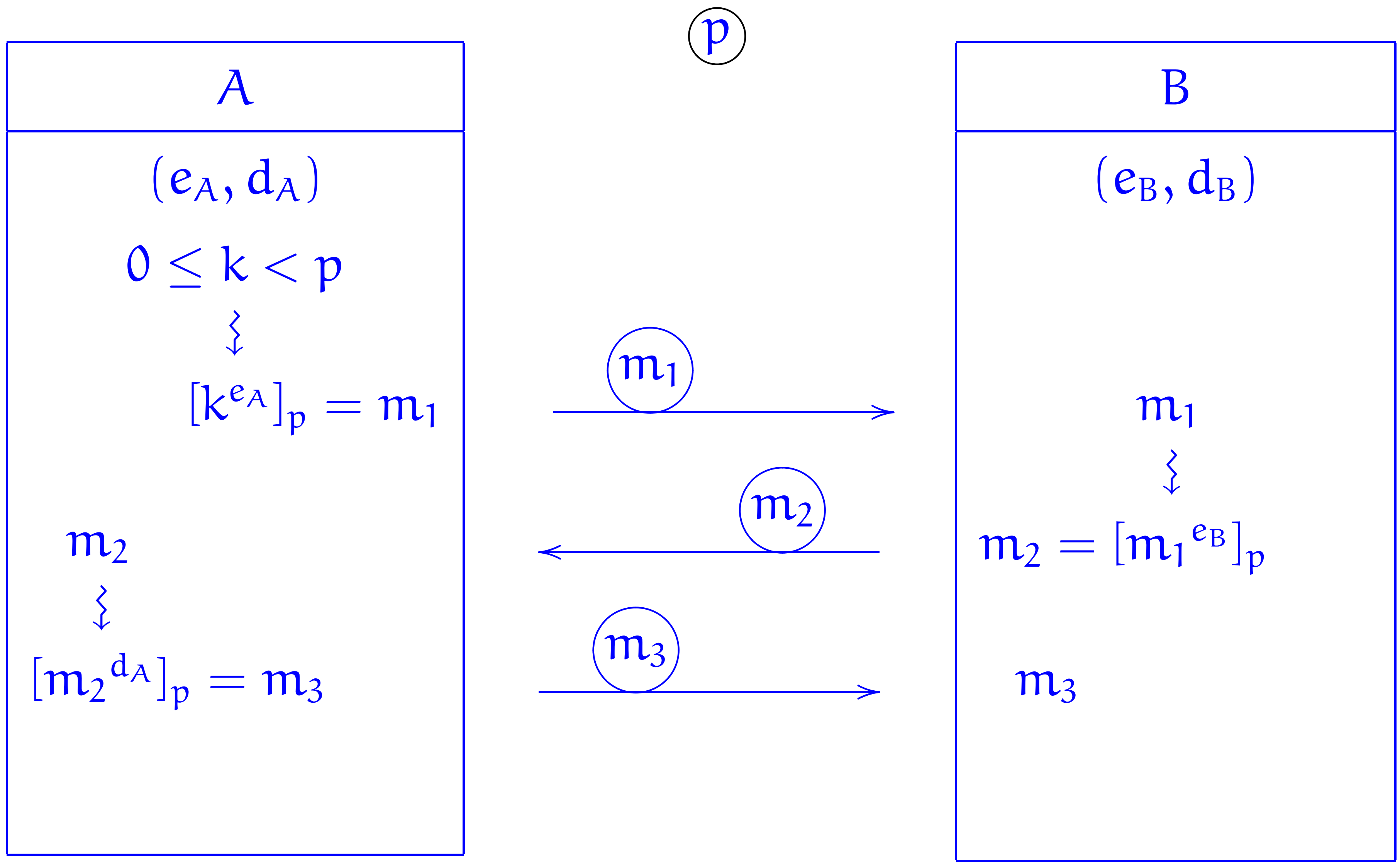
p

A	B
(e_A, d_A)	(e_B, d_B)
$0 \le k < p$	

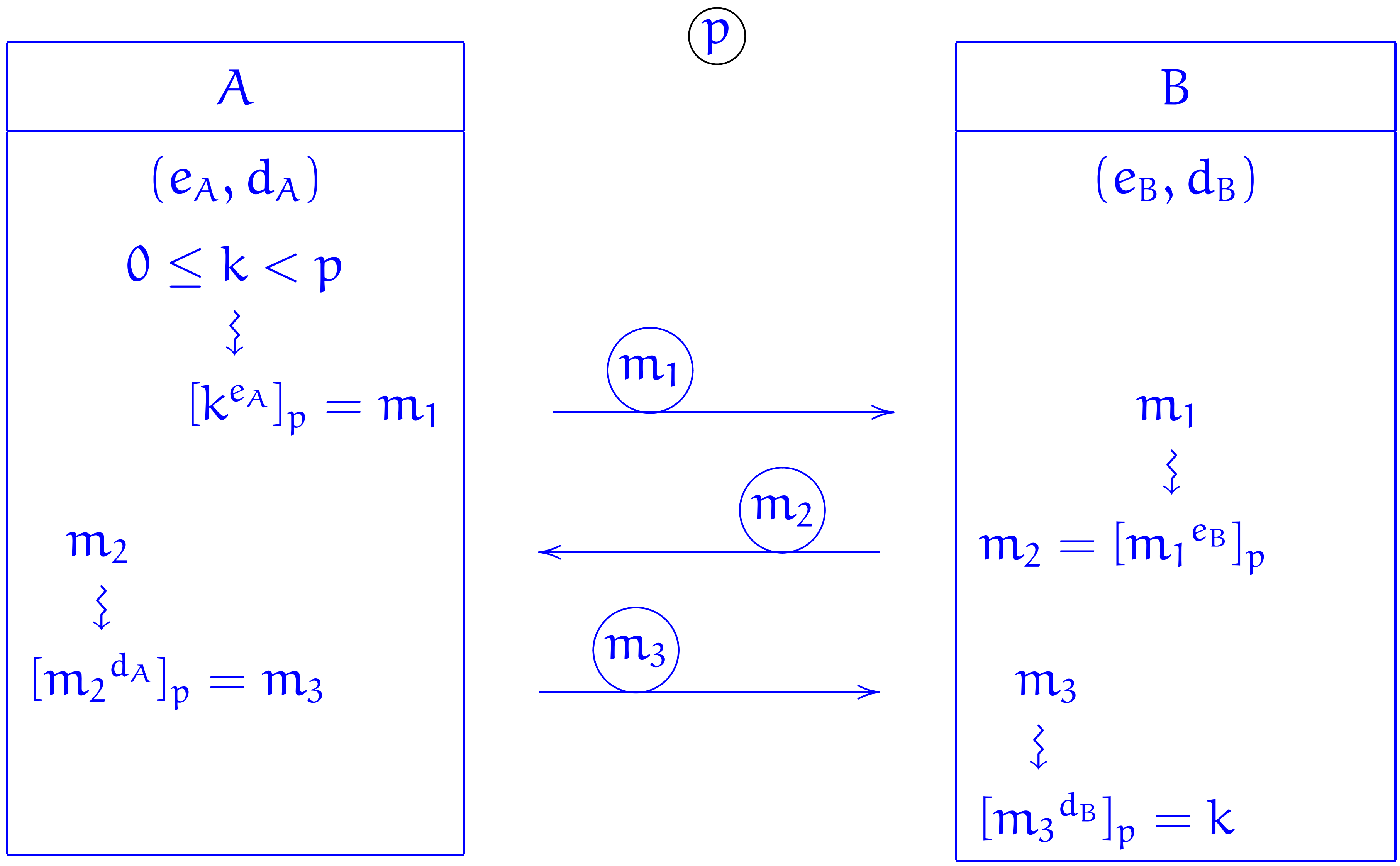
p

A		B
(e_A, d_A)		(e_B, d_B)
$0 \leq k < p$		
$\rightsquigarrow$		
$[k^{e_A}]_p = m_1$	$\xrightarrow{m_1}$	m_1


p
A
B
(e_A, d_A)
0 ≤ k < p
[k^{e_A}]_p = m_1
m_1
m_2
(e_B, d_B)
m_1
m_2 = [m_1^{e_B}]_p
m_2



p
A
B
(e_A, d_A)
$0 \leq k < p$
$[k^{e_A}]_p = m_1$
m_2
$[m_2{}^{d_A}]_p = m_3$
m_1
m_2
m_3
(e_B, d_B)
m_1
$m_2 = [m_1{}^{e_B}]_p$
m_3


p
A
B
(e_A, d_A)
0 ≤ k < p
[k^{e_A}]_p = m_1
m_2
[m_2^{d_A}]_p = m_3
m_1
m_2
m_3
(e_B, d_B)
m_1
m_2 = [m_1^{e_B}]_p
m_3
[m_3^{d_B}]_p = k

Natural Numbers and mathematical induction

We have mentioned in passing that the natural numbers are generated from zero by succesive increments. This is in fact the defining property of the set of natural numbers, and endows it with a very important and powerful reasoning principle, that of *Mathematical Induction*, for establishing universal properties of natural numbers.

Principle of Induction

Let $P(m)$ be a statement for m ranging over the set of natural numbers $\mathbb{N}$.

If

- the statement $P(0)$ holds, and
- the statement

  $$\forall n \in \mathbb{N}.\ \big(\ P(n) \implies P(n+1)\ \big)$$

  also holds

then

- the statement

  $$\forall m \in \mathbb{N}.\, P(m)$$

  holds.

Binomial Theorem

Theorem 29 *For all* $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \quad .$$

PROOF:

Principle of Induction

from basis ℓ

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

If

- $P(\ell)$ holds, and
- $\forall\, n \geq \ell$ in $\mathbb{N}.\ \big(\, P(n) \implies P(n+1) \,\big)$ also holds

then

- $\forall\, m \geq \ell$ in $\mathbb{N}.\ P(m)$ holds.

Principle of Strong Induction

from basis ℓ and Induction Hypothesis $P(m)$.

Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.
If both

- $P(\ell)$ and
- $\forall\, n \geq \ell$ in $\mathbb{N}.\, \Big(\big(\forall\, k \in [\ell..n].\, P(k)\big) \implies P(n+1) \Big)$

hold, then

- $\forall\, m \geq \ell$ in $\mathbb{N}.\, P(m)$ holds.

Fundamental Theorem of Arithmetic

Proposition 74 *Every positive integer greater than or equal* 2 *is a prime or a product of primes.*

PROOF:

Theorem 75 (Fundamental Theorem of Arithmetic) *For every positive integer* n *there is a unique finite ordered sequence of primes* $(p_1 \leq \cdots \leq p_\ell)$ *with* $\ell \in \mathbb{N}$ *such that*

$$n = \prod(p_1, \ldots, p_\ell) \quad .$$

PROOF:

Euclid's infinitude of primes

Theorem 78 *The set of primes is infinite.*

PROOF:

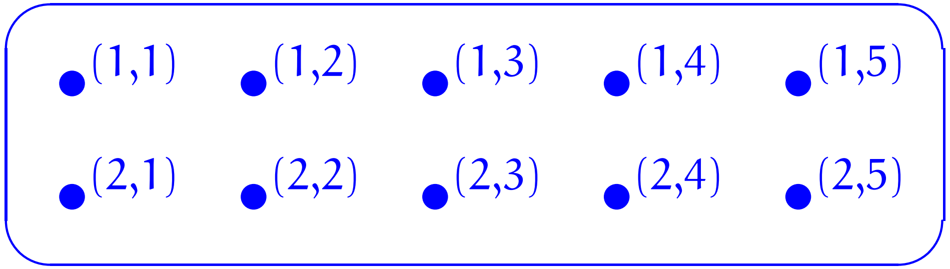
Sets

Objectives

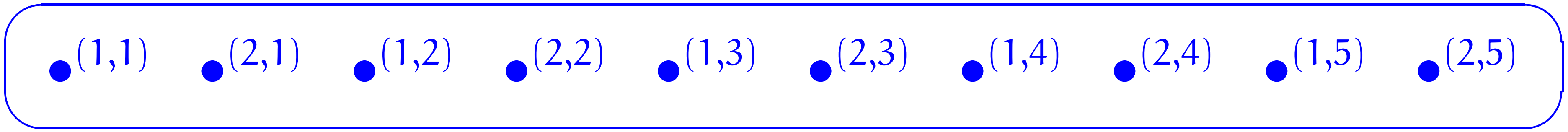
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

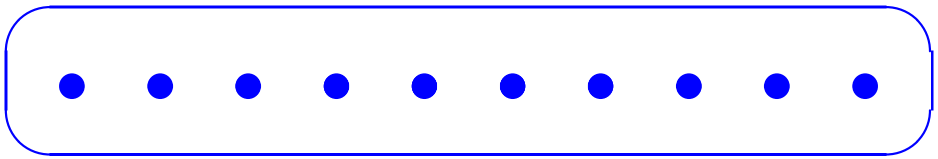
It has been said that a set is like a mental "bag of dots", except of course that the bag has no shape; thus,



may be a convenient way of picturing a certain set for some considerations, but what is apparently the same set may be pictured as



or even simply as



for other considerations.

Naive Set Theory

We are not going to be formally studying Set Theory here; rather, we will be *naively* looking at ubiquitous structures that are available within it.

Extensionality axiom

$\boxed{\text{Two sets are equal if they have the same elements.}}$

Thus,

$$\forall \text{ sets } A, B.\ A = B \iff (\forall x.\, x \in A \iff x \in B) \quad .$$

Example:

$$\{0\} \neq \{0,1\} = \{1,0\} \neq \{2\} = \{2,2\}$$

Subsets and supersets

Separation principle

For any set A and any definable property P, there is a set containing precisely those elements of A for which the property P holds.

$$\{ x \in A \mid P(x) \}$$

Russell's paradox

Empty set

$\emptyset$ or $\{\,\}$

defined by

$$\forall x.\, x \notin \emptyset$$

or, equivalently, by

$$\neg(\exists x.\, x \in \emptyset)$$

Cardinality

The *cardinality* of a set specifies its size. If this is a natural number, then the set is said to be *finite*.

Typical notations for the cardinality of a set S are $\#S$ or $|S|$.

Example:

$$\#\emptyset = 0$$

Powerset axiom

For any set, there is a set consisting of all its subsets.

$$\mathcal{P}(U)$$

$$\forall X.\ X \in \mathcal{P}(U) \iff X \subseteq U \quad .$$

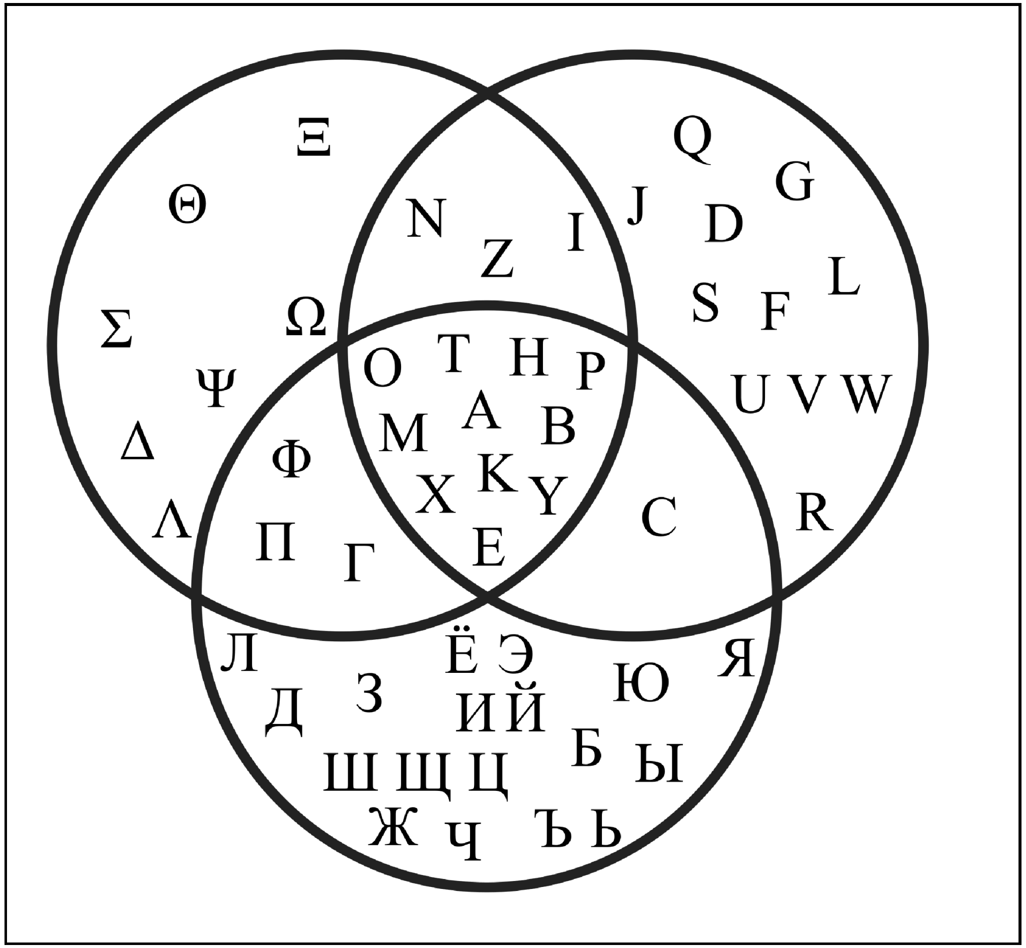
Hasse diagrams

Proposition 81 *For all finite sets* $\mathcal{U}$,

$$\#\,\mathcal{P}(\mathcal{U}) = 2^{\#\mathcal{U}} \quad .$$

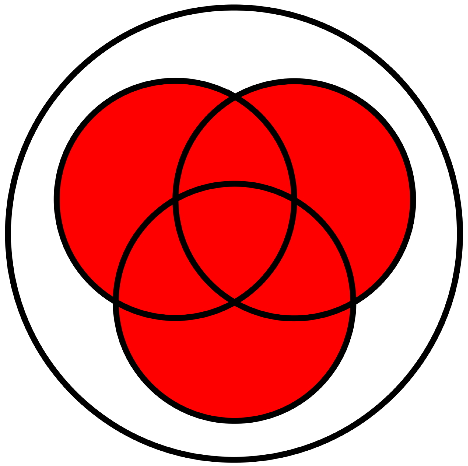
PROOF IDEA:

Venn diagrams[a]

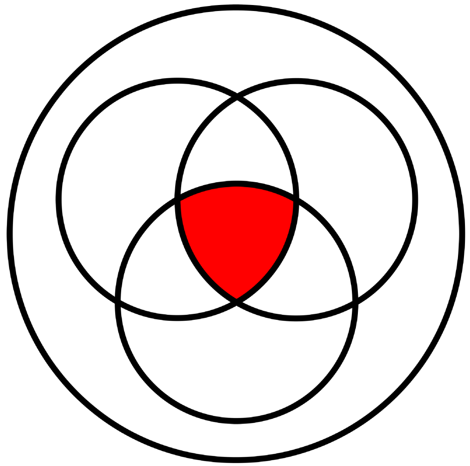


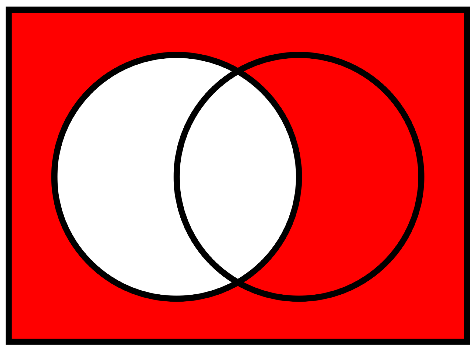
[a]From http://en.wikipedia.org/wiki/Intersection_(set_theory) .

Union



Intersection





Complement

The powerset Boolean algebra

$$\left(\ \mathcal{P}(U)\ ,\ \emptyset\ ,\ U\ ,\ \cup\ ,\ \cap\ ,\ (\cdot)^c\ \right)$$

For all $A, B \in \mathcal{P}(U)$,

$$A \cup B = \{x \in U \mid x \in A \vee x \in B\} \in \mathcal{P}(U)$$

$$A \cap B = \{x \in U \mid x \in A \wedge x \in B\} \in \mathcal{P}(U)$$

$$A^c = \{x \in U \mid \neg(x \in A)\} \in \mathcal{P}(U)$$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

$$(A \cup B) \cup C = A \cup (B \cup C) \;, \quad A \cup B = B \cup A \;, \quad A \cup A = A$$

$$(A \cap B) \cap C = A \cap (B \cap C) \;, \quad A \cap B = B \cap A \;, \quad A \cap A = A$$

- The union operation $\cup$ and the intersection operation $\cap$ are associative, commutative, and idempotent.

$$(A \cup B) \cup C = A \cup (B \cup C) \ , \quad A \cup B = B \cup A \ , \quad A \cup A = A$$

$$(A \cap B) \cap C = A \cap (B \cap C) \ , \quad A \cap B = B \cap A \ , \quad A \cap A = A$$

- The *empty set* $\emptyset$ is a neutral element for $\cup$ and the *universal set* $\mathcal{U}$ is a neutral element for $\cap$.

$$\emptyset \cup A \ = \ A \ = \ \mathcal{U} \cap A$$

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

$$\emptyset \cap A = \emptyset$$

$$\mathcal{U} \cup A = \mathcal{U}$$

- The empty set $\emptyset$ is an annihilator for $\cap$ and the universal set $\mathcal{U}$ is an annihilator for $\cup$.

$$\emptyset \cap A = \emptyset$$

$$\mathcal{U} \cup A = \mathcal{U}$$

- With respect to each other, the union operation $\cup$ and the intersection operation $\cap$ are distributive and absorptive.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad , \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cup (A \cap B) \; = \; A \; = \; A \cap (A \cup B)$$

- The complement operation $(\cdot)^{\mathrm{c}}$ satisfies complementation laws.

$$A \cup A^{\mathrm{c}} = \mathcal{U} \ , \quad A \cap A^{\mathrm{c}} = \emptyset$$

Proposition 82 *Let* U *be a set and let* $A, B \in \mathcal{P}(U)$.

1. $\forall X \in \mathcal{P}(U).\ A \cup B \subseteq X \iff (A \subseteq X \wedge B \subseteq X)$.
2. $\forall X \in \mathcal{P}(U).\ X \subseteq A \cap B \iff (X \subseteq A \wedge X \subseteq B)$.

PROOF:

Corollary 83 *Let* U *be a set and let* $A, B, C \in \mathcal{P}(U)$.

1. $$C = A \cup B$$

iff

$$[A \subseteq C \wedge B \subseteq C]$$

$$\wedge$$

$$[\forall X \in \mathcal{P}(U).\ (A \subseteq X \ \wedge\ B \subseteq X) \implies C \subseteq X]$$

2. $$C = A \cap B$$

iff

$$[C \subseteq A \wedge C \subseteq B]$$

$$\wedge$$

$$[\forall X \in \mathcal{P}(U).\ (X \subseteq A \ \wedge\ X \subseteq B) \implies X \subseteq C]$$

Sets and logic

$\mathcal{P}(\mathcal{U})$	$\{\,\textbf{false}\,,\ \textbf{true}\,\}$
$\emptyset$	**false**
$\mathcal{U}$	**true**
$\cup$	$\vee$
$\cap$	$\wedge$
$(\cdot)^{c}$	$\neg(\cdot)$

Pairing axiom

$\boxed{\text{For every } a \text{ and } b\text{, there is a set with } a \text{ and } b \text{ as its only elements.}}$

$$\{\,a\,,\,b\,\}$$

defined by

$$\forall x.\, x \in \{a, b\} \iff (x = a \lor x = b)$$

NB The set $\{a, a\}$ is abbreviated as $\{\,a\,\}$, and referred to as a *singleton*.

Examples:

- $\#\{\emptyset\} = 1$
- $\#\{\{\emptyset\}\} = 1$
- $\#\{\emptyset, \{\emptyset\}\} = 2$

Ordered pairing

For every pair a and b, the set

$$\{\{a\},\{a,b\}\}$$

is abbreviated as

$$\langle a,b\rangle$$

and referred to as an *ordered pair*.

Proposition 84 (Fundamental property of ordered pairing)
For all a, b, x, y,

$$\langle a, b\rangle = \langle x, y\rangle \iff \big(a = x \ \wedge \ b = y\big) \quad .$$

PROOF:

Products

The *product* $A \times B$ of two sets A and B is the set

$$A \times B = \{\, x \mid \exists\, a \in A, b \in B.\, x = (a, b) \,\}$$

where

$$\begin{array}{l} \forall a_1, a_2 \in A, b_1, b_2 \in B. \\ \quad (a_1, b_1) = (a_2, b_2) \iff (a_1 = a_2 \,\wedge\, b_1 = b_2) \end{array} \quad .$$

Thus,

$$\forall\, x \in A \times B.\, \exists!\, a \in A.\, \exists!\, b \in B.\, x = (a, b) \quad .$$

Proposition 86 *For all finite sets* A *and* B*,*

$$\#(A \times B) = \#A \cdot \#B \quad .$$

PROOF IDEA:

Big unions

Definition 87 *Let* $\mathcal{U}$ *be a set. For a collection of sets* $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{U}))$*, we let the* big union *(relative to* $\mathcal{U}$*) be defined as*

$$\bigcup \mathcal{F} \;=\; \big\{\, x \in \mathcal{U} \mid \exists A \in \mathcal{F}.\, x \in A \,\big\} \;\in \mathcal{P}(\mathcal{U}) \quad .$$

Proposition 88 *For all* $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{U})))$,

$$\bigcup \left(\bigcup \mathcal{F} \right) = \bigcup \left\{ \bigcup \mathcal{A} \in \mathcal{P}(\mathbb{U}) \;\middle|\; \mathcal{A} \in \mathcal{F} \right\} \in \mathcal{P}(\mathbb{U}) \quad .$$

PROOF:

Big intersections

Definition 89 *Let* U *be a set. For a collection of sets* $\mathcal{F} \subseteq \mathcal{P}(U)$, *we let the* big intersection *(relative to* U*) be defined as*

$$\bigcap \mathcal{F} = \{ x \in U \mid \forall A \in \mathcal{F}. x \in A \} \quad .$$

Theorem 90 *Let*

$$\mathcal{F} = \left\{ S \subseteq \mathbb{R} \;\middle|\; (0 \in S) \wedge \left(\forall x \in \mathbb{R}.\, x \in S \implies (x+1) \in S\right) \right\} .$$

Then, (i) $\mathbb{N} \in \mathcal{F}$ *and* (ii) $\mathbb{N} \subseteq \bigcap \mathcal{F}$*. Hence,* $\bigcap \mathcal{F} = \mathbb{N}$*.*

PROOF:

Union axiom

$\boxed{\text{Every collection of sets has a union.}}$

$$\bigcup \mathcal{F}$$

$$x \in \bigcup \mathcal{F} \iff \exists X \in \mathcal{F}.\, x \in X$$

For *non-empty* $\mathcal{F}$ we also have

$$\bigcap \mathcal{F}$$

defined by

$$\forall x.\ x \in \bigcap \mathcal{F} \iff \big(\forall X \in \mathcal{F}. x \in X\big) \quad .$$

Disjoint unions

Definition 91 *The* disjoint union $A \uplus B$ *of two sets* A *and* B *is the set*

$$A \uplus B \;=\; \big(\{1\} \times A\big) \cup \big(\{2\} \times B\big) \quad .$$

Thus,

$$\forall\, x.\, x \in (A \uplus B) \iff \big(\, \exists a \in A.\, x = (1, a)\,\big) \;\vee\; \big(\, \exists b \in B.\, x = (2, b)\,\big)\,.$$

Proposition 93 *For all finite sets* A *and* B*,*

$$A \cap B = \emptyset \implies \#(A \cup B) = \#A + \#B \quad .$$

PROOF IDEA:

Corollary 94 *For all finite sets* A *and* B*,*

$$\#(A \uplus B) = \#A + \#B \quad .$$

Relations

Definition 96 *A* <u>(binary) relation</u> R *from a set* A *to a set* B

$$R : A \rightarrow\!\!\!\!\!+\!\!\!\!\rightarrow B \quad \textit{or} \quad R \in \mathrm{Rel}(A, B) \quad ,$$

is

$$R \subseteq A \times B \quad \textit{or} \quad R \in \mathcal{P}(A \times B) \quad .$$

Notation 97 *One typically writes* $a \, R \, b$ *for* $(a, b) \in R$*.*

Informal examples:

- Computation.
- Typing.
- Program equivalence.
- Networks.
- Databases.

Examples:

- Empty relation.
  $\emptyset : A \twoheadrightarrow B$ $\qquad (a\ \emptyset\ b \iff \textbf{false})$

- Full relation.
  $(A \times B) : A \twoheadrightarrow B$ $\qquad (a\ (A \times B)\ b \iff \textbf{true})$

- Identity (or equality) relation.
  $\mathrm{id}_A = \{\ (a, a) \mid a \in A\ \} : A \twoheadrightarrow A$ $\qquad (a\ \mathrm{id}_A\ a' \iff a = a')$

- Integer square root.
  $R_2 = \{\ (m, n) \mid m = n^2\ \} : \mathbb{N} \twoheadrightarrow \mathbb{Z}$ $\qquad (m\ R_2\ n \iff m = n^2)$

Internal diagrams

Example:

$$R = \{\ (0,0),(0,-1),(0,1),(1,2),(1,1),(2,1)\ \} : \mathbb{N} \longrightarrow\!\!\!\!\!\!\!+\ \mathbb{Z}$$

$$S = \{\ (1,0),(1,2),(2,1),(2,3)\ \} : \mathbb{Z} \longrightarrow\!\!\!\!\!\!\!+\ \mathbb{Z}$$

Relational extensionality

$$R = S : A \longrightarrow\!\!\!\!\!\!\!+\; B$$

iff

$$\forall a \in A.\, \forall b \in B.\; a\,R\,b \iff a\,S\,b$$

Relational composition

Theorem 99 *Relational composition is associative and has the identity relation as neutral element.*

- *Associativity.*

  For all $R : A \rightarrowtriangle B$, $S : B \rightarrowtriangle C$, *and* $T : C \rightarrowtriangle D$,

  $$(T \circ S) \circ R = T \circ (S \circ R)$$

- *Neutral element.*

  For all $R : A \rightarrowtriangle B$,

  $$R \circ \mathrm{id}_A = R = \mathrm{id}_B \circ R \quad .$$

Relations and matrices

Definition 100

1. *For positive integers* m *and* n, *an* $(m \times n)$-matrix M *over a semiring* $(S, 0, \oplus, 1, \odot)$ *is given by entries* $M_{i,j} \in S$ *for all* $0 \leq i < m$ *and* $0 \leq j < n$.

Theorem 101 *Matrix multiplication is associative and has the identity matrix as neutral element.*

Relations from $[m]$ to $[n]$ and $(m \times n)$-matrices over Booleans provide two alternative views of the same structure.

This carries over to identities and to composition/multiplication .

Directed graphs

Definition 105 *A* directed graph (A, R) *consists of a set* A *and a relation* R *on* A *(i.e. a relation from* A *to* A*).*

Corollary 107 *For every set A, the structure*

$$(\,\mathrm{Rel}(A)\,,\ \mathrm{id}_A\,, \circ\,)$$

is a monoid.

Definition 108 *For $R \in \mathrm{Rel}(A)$ and $n \in \mathbb{N}$, we let*

$$R^{\circ n} = \underbrace{R \circ \cdots \circ R}_{n \text{ times}} \in \mathrm{Rel}(A)$$

be defined as id_A for $n = 0$, and as $R \circ R^{\circ m}$ for $n = m + 1$.

Paths

Proposition 110 *Let* (A, R) *be a directed graph. For all* $n \in \mathbb{N}$ *and* $s, t \in A$, $s \; R^{\circ n} \; t$ *iff there exists a path of length* n *in* R *with source* s *and target* t.

PROOF:

Definition 111 *For* $R \in \mathrm{Rel}(A)$, *let*

$$R^{\circ *} = \bigcup \{ R^{\circ n} \in \mathrm{Rel}(A) \mid n \in \mathbb{N} \} = \bigcup_{n \in \mathbb{N}} R^{\circ n} \quad .$$

Corollary 112 *Let* (A, R) *be a directed graph. For all* $s, t \in A$, $s \; R^{\circ *} \; t$ *iff there exists a path with source* s *and target* t *in* R*.*

The $(n \times n)$-matrix $M = \mathrm{mat}(R)$ of a finite directed graph $([n], R)$ for n a positive integer is called its <u>*adjacency matrix*</u>.

The adjacency matrix $M^* = \mathrm{mat}(R^{\circ *})$ can be computed by matrix multiplication and addition as M_n where

$$\begin{cases} M_0 &= I_n \\ M_{k+1} &= I_n + (M \cdot M_k) \end{cases}$$

This gives an algorithm for establishing or refuting the existence of paths in finite directed graphs.

Preorders

Definition 113 *A* preorder $(P , \sqsubseteq)$ *consists of a set* P *and a relation* $\sqsubseteq$ *on* P *(i.e.* $\sqsubseteq \, \in \mathcal{P}(P \times P)$*) satisfying the following two axioms.*

- *Reflexivity.*

$$\forall x \in P. \; x \sqsubseteq x$$

- *Transitivity.*

$$\forall x, y, z \in P. \; (x \sqsubseteq y \; \wedge \; y \sqsubseteq z) \implies x \sqsubseteq z$$

Examples:

- $(\mathbb{R}, \leq)$ and $(\mathbb{R}, \geq)$.
- $(\mathcal{P}(A), \subseteq)$ and $(\mathcal{P}(A), \supseteq)$.
- $(\mathbb{Z}, \mid)$.

Theorem 115 *For* $R \subseteq A \times A$, *let*

$$\mathcal{F}_R \;=\; \{\, Q \subseteq A \times A \;\mid\; R \subseteq Q \;\wedge\; Q \text{ *is a preorder* } \} \quad .$$

Then, (i) $R^{\circ *} \in \mathcal{F}_R$ *and* (ii) $R^{\circ *} \subseteq \bigcap \mathcal{F}_R$. *Hence,* $R^{\circ *} = \bigcap \mathcal{F}_R$.

PROOF:

Partial functions

Definition 116 *A relation* $R : A \rightarrowtail\!\!\!\!\!+ B$ *is said to be* functional*, and called a* partial function*, whenever it is such that*

$$\forall a \in A.\, \forall\, b_1, b_2 \in B.\ a\, R\, b_1 \,\wedge\, a\, R\, b_2 \implies b_1 = b_2 \quad .$$

Theorem 118 *The identity relation is a partial function, and the composition of partial functions yields a partial function.*

NB

$$f = g : A \rightharpoonup B$$

iff

$$\forall a \in A. \left(f(a)\downarrow \iff g(a)\downarrow \right) \wedge f(a) = g(a)$$

Example: The following defines a partial function $\mathbb{Z} \times \mathbb{Z} \rightharpoonup \mathbb{Z} \times \mathbb{N}$:

- for $n \geq 0$ and $m > 0$,
  $(n, m) \mapsto \big(\,\mathrm{quo}(n, m)\,,\ \mathrm{rem}(n, m)\,\big)$
- for $n \geq 0$ and $m < 0$,
  $(n, m) \mapsto \big(\,-\mathrm{quo}(n, -m)\,,\ \mathrm{rem}(n, -m)\,\big)$
- for $n < 0$ and $m > 0$,
  $(n, m) \mapsto \big(\,-\mathrm{quo}(-n, m) - 1\,,\ \mathrm{rem}(m - \mathrm{rem}(-n, m), m)\,\big)$
- for $n < 0$ and $m < 0$,
  $(n, m) \mapsto \big(\,\mathrm{quo}(-n, -m) + 1\,,\ \mathrm{rem}(-m - \mathrm{rem}(-n, -m), -m)\,\big)$

Its domain of definition is $\{\,(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid m \neq 0\,\}$.

Proposition 119 *For all finite sets* A *and* B*,*

$$\#(A \rightharpoonup B) \; = \; (\#B + 1)^{\#A} \quad .$$

PROOF IDEA:

Functions (or maps)

Definition 120 *A partial function is said to be* total*, and referred to as a* (total) function *or* map*, whenever its domain of definition coincides with its source.*

Theorem 121 *For all* $f \in \mathrm{Rel}(A, B)$*,*

$$f \in (A \Rightarrow B) \iff \forall\, a \in A.\, \exists!\, b \in B.\ a\, f\, b \quad .$$

Proposition 122 *For all finite sets A and B,*

$$\#(A \Rightarrow B) = \#B^{\#A} \quad .$$

PROOF IDEA:

Theorem 123 *The identity partial function is a function, and the composition of functions yields a function.*

NB

1. $f = g : A \to B$ iff $\forall\, a \in A.\, f(a) = g(a)$.

2. For all sets A, the identity function $\mathrm{id}_A : A \to A$ is given by the rule

   $$\mathrm{id}_A(a) = a$$

   and, for all functions $f : A \to B$ and $g : B \to C$, the composition function $g \circ f : A \to C$ is given by the rule

   $$\big(g \circ f\big)(a) = g\big(f(a)\big) \quad .$$

Bijections

Definition 124 *A function* $f : A \to B$ *is said to be* bijective*, or a* bijection*, whenever there exists a (necessarily unique) function* $g : B \to A$ *(referred to as the* inverse *of* f*) such that*

1. g *is a* retraction *(or* left inverse*) for* f*:*

   $$g \circ f = \mathrm{id}_A \quad ,$$

2. g *is a* section *(or* right inverse*) for* f*:*

   $$f \circ g = \mathrm{id}_B \quad .$$

Proposition 126 *For all finite sets A and B,*

$$\# \operatorname{Bij}(A, B) = \begin{cases} 0 & , \textit{if } \#A \neq \#B \\ n! & , \textit{if } \#A = \#B = n \end{cases}$$

PROOF IDEA:

Theorem 127 *The identity function is a bijection, and the composition of bijections yields a bijection.*

Definition 128 *Two sets* A *and* B *are said to be* isomorphic *(and to have the* same cardinatity*) whenever there is a bijection between them; in which case we write*

$$A \cong B \quad \textit{or} \quad \#A = \#B \quad .$$

Examples:

1. $\{0, 1\} \cong \{\mathbf{false}, \mathbf{true}\}$.
2. $\mathbb{N} \cong \mathbb{N}^{+}$, $\mathbb{N} \cong \mathbb{Z}$, $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$, $\mathbb{N} \cong \mathbb{Q}$.

Equivalence relations and set partitions

- Equivalence relations.

- Set partitions.

Theorem 131 *For every set A,*

$$\mathrm{EqRel}(A) \cong \mathrm{Part}(A) \quad .$$

PROOF:

Calculus of bijections

- $A \cong A \quad , \quad A \cong B \implies B \cong A \quad , \quad (A \cong B \wedge B \cong C) \implies A \cong C$

- If $A \cong X$ and $B \cong Y$ then

$$\mathcal{P}(A) \cong \mathcal{P}(X) \quad , \quad A \times B \cong X \times Y \quad , \quad A \uplus B \cong X \uplus Y \quad ,$$

$$\mathrm{Rel}(A, B) \cong \mathrm{Rel}(X, Y) \quad , \quad (A \rightharpoonup B) \cong (X \rightharpoonup Y) \quad ,$$

$$(A \Rightarrow B) \cong (X \Rightarrow Y) \quad , \quad \mathrm{Bij}(A, B) \cong \mathrm{Bij}(X, Y)$$

- $A \cong [1] \times A$, $(A \times B) \times C \cong A \times (B \times C)$, $A \times B \cong B \times A$
- $[0] \uplus A \cong A$, $(A \uplus B) \uplus C \cong A \uplus (B \uplus C)$, $A \uplus B \cong B \uplus A$
- $[0] \times A \cong [0]$, $(A \uplus B) \times C \cong (A \times C) \uplus (B \times C)$
- $\big(A \Rightarrow [1]\big) \cong [1]$, $\big(A \Rightarrow (B \times C)\big) \cong (A \Rightarrow B) \times (A \Rightarrow C)$
- $\big([0] \Rightarrow A\big) \cong [1]$, $\big((A \uplus B) \Rightarrow C\big) \cong (A \Rightarrow C) \times (B \Rightarrow C)$
- $([1] \Rightarrow A) \cong A$, $\big((A \times B) \Rightarrow C\big) \cong \big(A \Rightarrow (B \Rightarrow C)\big)$
- $(A \rightharpoonup B) \cong \big(A \Rightarrow (B \uplus [1])\big)$
- $\mathcal{P}(A) \cong \big(A \Rightarrow [2]\big)$

Characteristic (or indicator) functions

$$\mathcal{P}(A) \cong \big(A \Rightarrow [2] \big)$$

Finite cardinality

Definition 133 *A set* A *is said to be* finite *whenever* $A \cong [n]$ *for some* $n \in \mathbb{N}$*, in which case we write* $\#A = n$.

Theorem 134 *For all* $m, n \in \mathbb{N}$,

1. $\mathcal{P}\big([n]\big) \cong [2^n]$
2. $[m] \times [n] \cong [m \cdot n]$
3. $[m] \uplus [n] \cong [m + n]$
4. $\big([m] \rightharpoonup [n]\big) \cong \big[(n+1)^m\big]$
5. $\big([m] \Rightarrow [n]\big) \cong [n^m]$
6. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$

Infinity axiom

$\boxed{\text{There is an infinite set, containing } \emptyset \text{ and closed under successor.}}$

Bijections

Proposition 135 *For a function* $f : A \to B$*, the following are equivalent.*

1. f *is bijective.*
2. $\forall\, b \in B.\, \exists!\, a \in A.\, f(a) = b$.
3. $$\begin{array}{l} \big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big) \\ \wedge \\ \big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big) \end{array}$$

Surjections

Definition 136 *A function* $f : A \longrightarrow B$ *is said to be* surjective*, or a* surjection*, and indicated* $f : A \twoheadrightarrow B$ *whenever*

$$\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b \quad .$$

Theorem 137 *The identity function is a surjection, and the composition of surjections yields a surjection.*

The set of surjections from A to B is denoted

$$\mathrm{Sur}(A, B)$$

and we thus have

$$\mathrm{Bij}(A, B) \subseteq \mathrm{Sur}(A, B) \subseteq \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \quad .$$

Enumerability

Definition 139

1. *A set A is said to be* enumerable *whenever there exists a surjection $\mathbb{N} \twoheadrightarrow A$, referred to as an* enumeration*.*

2. *A* countable *set is one that is either empty or enumerable.*

Examples:

1. A bijective enumeration of $\mathbb{Z}$.

$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$

2. A bijective enumeration of $\mathbb{N} \times \mathbb{N}$.

	0	1	2	3	4	5	$\cdots$
0							
1							
2							
3							
4							
$\vdots$							

Proposition 140 *Every non-empty subset of an enumerable set is enumerable.*

PROOF:

Countability

Proposition 141

1. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *are countable sets.*
2. *The product and disjoint union of countable sets is countable.*
3. *Every finite set is countable.*
4. *Every subset of a countable set is countable.*

Axiom of choice

Every surjection has a section.

Injections

Definition 142 *A function* $f : A \to B$ *is said to be* injective, *or an* injection, *and indicated* $f : A \rightarrowtail B$ *whenever*

$$\forall a_1, a_2 \in A. \left(f(a_1) = f(a_2) \right) \implies a_1 = a_2 \quad .$$

Theorem 143 *The identity function is an injection, and the composition of injections yields an injection.*

The set of injections from A to B is denoted

$$\mathrm{Inj}(A, B)$$

and we thus have

$$\begin{tikzcd}
& \mathrm{Sur}(A, B) \arrow[dr, phantom, sloped, "\subseteq"] & \\
\mathrm{Bij}(A, B) \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\supseteq"] & & \mathrm{Fun}(A, B) \subseteq \mathrm{PFun}(A, B) \subseteq \mathrm{Rel}(A, B) \\
& \mathrm{Inj}(A, B) \arrow[ur, phantom, sloped, "\subseteq"] &
\end{tikzcd}$$

with

$$\mathrm{Bij}(A, B) = \mathrm{Sur}(A, B) \cap \mathrm{Inj}(A, B) \quad .$$

Proposition 144 *For all finite sets A and B,*

$$\#\mathrm{Inj}(A, B) = \begin{cases} \binom{\#B}{\#A} \cdot (\#A)! & \text{, if } \#A \leq \#B \\ 0 & \text{, otherwise} \end{cases}$$

PROOF IDEA:

Relational images

Definition 147 *Let* $R : A \longrightarrow\!\!\!\!\!+\; B$ *be a relation.*

- *The* direct image *of* $X \subseteq A$ *under* R *is the set* $\overrightarrow{R}(X) \subseteq B$, *defined as*

$$\overrightarrow{R}(X) \;=\; \{\, b \in B \mid \exists x \in X .\, x \mathrel{R} b \,\} \;.$$

NB *This construction yields a function* $\overrightarrow{R} : \mathcal{P}(A) \to \mathcal{P}(B)$.

- *The* inverse image *of* $Y \subseteq B$ *under* R *is the set* $\overleftarrow{R}(Y) \subseteq A$, *defined as*

$$\overleftarrow{R}(Y) \;=\; \{\, a \in A \mid \forall\, b \in B.\, a \mathrel{R} b \implies b \in Y \,\}$$

NB *This construction yields a function* $\overleftarrow{R} : \mathcal{P}(B) \to \mathcal{P}(A)$.

Replacement axiom

The direct image of every definable functional property on a set is a set.

Set-indexed constructions

For every mapping associating a set A_i to each element of a set I, we have the set

$$\bigcup_{i \in I} A_i \;=\; \bigcup \left\{ A_i \mid i \in I \right\} \;=\; \left\{ a \mid \exists\, i \in I.\, a \in A_i \right\} \quad .$$

Examples:

1. Indexed disjoint unions:

$$\biguplus_{i \in I} A_i \;=\; \bigcup_{i \in I} \{i\} \times A_i$$

2. Finite sequences on a set A:

$$A^* \;=\; \biguplus_{n \in \mathbb{N}} A^n$$

3. Finite partial functions from a set A to a set B:

$$(A \rightharpoonup_{\mathrm{fin}} B) \;=\; \biguplus_{S \in \mathcal{P}_{\mathrm{fin}}(A)} (S \Rightarrow B)$$

where

$$\mathcal{P}_{\mathrm{fin}}(A) = \{\, S \subseteq A \mid S \text{ is finite} \,\}$$

4. Non-empty indexed intersections: for $I \neq \emptyset$,

$$\bigcap_{i \in I} A_i \;=\; \{\, x \in \bigcup_{i \in I} A_i \mid \forall i \in I .\, x \in A_i \,\}$$

5. Indexed products:

$$\prod_{i \in I} A_i \;=\; \left\{\; \alpha \in (I \Rightarrow \bigcup_{i \in I} A_i) \;\middle|\; \forall i \in I .\, \alpha(i) \in A_i \;\right\}$$

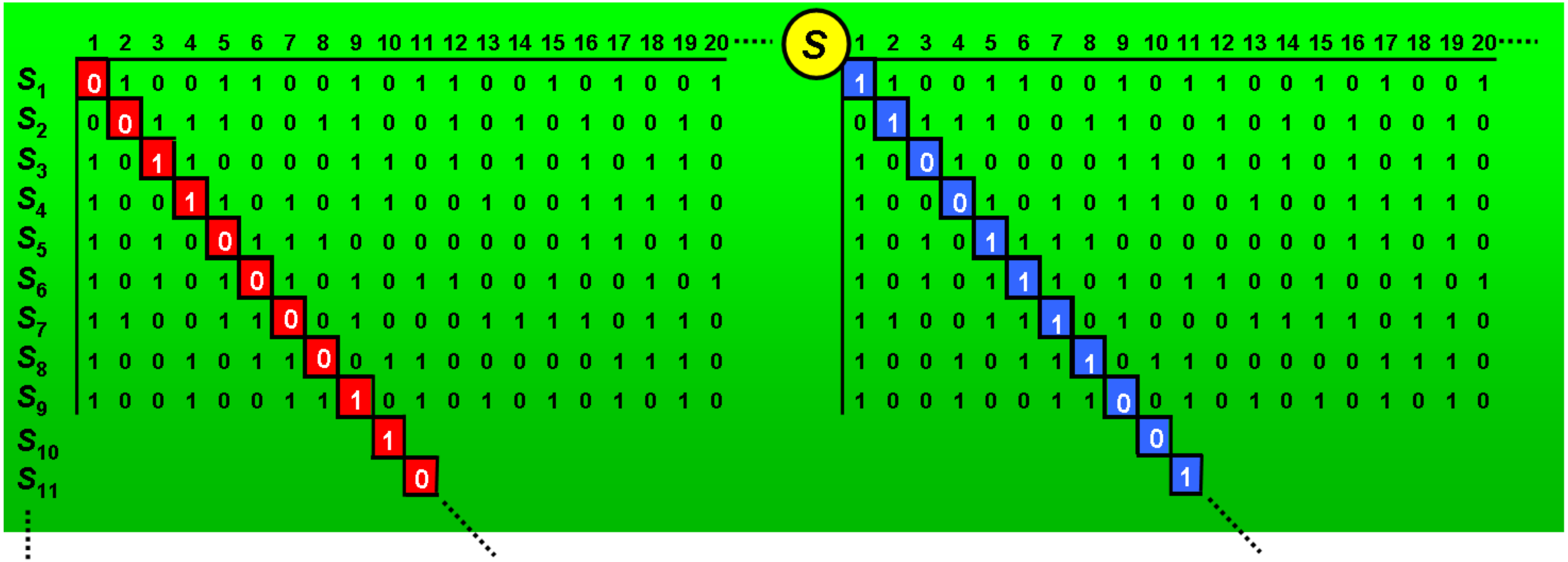
Proposition 150 *An enumerable indexed disjoint union of enumerable sets is enumerable.*

PROOF:

Corollary 152 *If X and A are countable sets then so are A^*, $\mathcal{P}_{\text{fin}}(A)$, and $(X \rightrightarrows_{\text{fin}} A)$.*

THEOREM OF THE DAY

Cantor's Uncountability Theorem *There are uncountably many infinite 0-1 sequences.*



Proof: Suppose you *could* count the sequences. Label them in order: $S_1, S_2, S_3, \ldots$, and denote by $S_i(j)$ the j-th entry of sequence S_i. Now define a new sequence, S, whose i-th entry is $S_i(i) + 1 \pmod 2$. So S is $S_1(1)+1, S_2(2)+1, S_3(3)+1, S_4(4)+1, \ldots$, with all entries remaindered modulo 2. S is certainly an infinite sequence of 0s and 1s. So it must appear in our list: it is, say, S_k, so its k-th entry is $S_k(k)$. But this is, by definition, $S_k(k) + 1 \pmod 2 \neq S_k(k)$. So we have contradicted the possibility of forming our enumeration. QED.

The theorem establishes that the real numbers are *uncountable* — that is, they cannot be enumerated in a list indexed by the positive integers $(1, 2, 3, \ldots)$. To see this informally, consider the infinite sequences of 0s and 1s to be the binary expansions of fractions (e.g. $0.010011\ldots = 0/2 + 1/4 + 0/8 + 0/16 + 1/32 + 1/64 + \ldots$). More generally, it says that the set of subsets of a countably infinite set is uncountable, and to see *that*, imagine every 0-1 sequence being a different recipe for building a subset: the i-th entry tells you whether to include the i-th element (1) or exclude it (0).

Georg Cantor (1845–1918) discovered this theorem in 1874 but it apparently took another twenty years of thought about what were then new and controversial concepts: 'sets', 'cardinalities', 'orders of infinity', to invent the important proof given here, using the so-called *diagonalisation method*.

Web link: www.math.hawaii.edu/~dale/godel/godel.html. There is an interesting discussion on mathoverflow.net about the history of diagonalisation: type 'earliest diagonal' into their search box.

Further reading: *Mathematics: the Loss of Certainty* by Morris Kline, Oxford University Press, New York, 1980.

Created by Robin Whitty for www.theoremoftheday.org

Unbounded cardinality

Theorem 153 (Cantor's diagonalisation argument) *For every set A, no surjection from A to $\mathcal{P}(A)$ exists.*

PROOF:

Definition 154 *A* fixed-point *of a function* $f : X \to X$ *is an element* $x \in X$ *such that* $f(x) = x$.

Theorem 155 (Lawvere's fixed-point argument) *For sets* A *and* X, *if there exists a surjection* $A \twoheadrightarrow (A \Rightarrow X)$ *then every function* $X \to X$ *has a fixed-point; and hence* X *is a singleton.*

PROOF:

Corollary 156 *The sets*

$$\mathcal{P}(\mathbb{N}) \;\cong\; \big(\mathbb{N} \Rightarrow [2]\big) \;\cong\; [0,1] \;\cong\; \mathbb{R}$$

are not enumerable.

Corollary 157 *There are* non-computable *infinite sequences of bits.*

Foundation axiom

$\boxed{\text{The membership relation is well-founded.}}$

Thereby, providing a

Principle of $\in$*-Induction* .