Notes

for Part IA CST 2023/24

Discrete Mathematics

<www.cl.cam.ac.uk/teaching/2324/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

Dr Jon Sterling

js2878@cl.cam.ac.uk

A Zen story

from the Introduction of
Mathematics Made Difficult by C.E. Linderholme

One of the great Zen masters had an eager disciple who never lost an opportunity to catch whatever pearls of wisdom might drop from the master's lips, and who followed him about constantly. One day, deferentially opening an iron gate for the old man, the disciple asked, 'How may I attain enlightenment?' The ancient sage, though withered and feeble, could be quick, and he deftly caused the heavy gate to shut on the pupil's leg, breaking it.

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.

Application areas

algorithmics - compilers - computability - computer aided verification - computer algebra - complexity - cryptography - databases - digital circuits - discrete probability - model checking - network routing - program correctness - programming languages - security - semantics - type systems

Lecture plan

I. Proofs.

II. Numbers.

III. Sets.

IV. Regular languages and finite automata.

I. Proofs

1. Preliminaries (pages 11–13) and introduction (pages 14–40).
2. Implication (pages 42–56) and bi-implication (pages 57–63).
3. Universal quantification (pages 63–76) and conjunction (pages 77–85).
4. Existential quantification (pages 85–100).
5. Disjunction (pages 104–115) and a little arithmetic (pages 116–132).
6. Negation (pages 132–152).

II. Numbers

7. Number systems (pages 153–174).
8. The division theorem and algorithm (pages 175–187) and modular arithmetic (pages 187–197).
9. On sets (pages 197–205), the greatest common divisor (pages 206–213), and Euclid's algorithm (pages 214–237) and theorem (pages 237–244).
10. The Extended Euclid's Algorithm (pages 244–258) and the Diffie-Hellman cryptographic method (pages 258–263).
11. The Principle of Induction (pages 264–282), the Principle of Induction from a basis (pages 282–286), and the Principle of Strong Induction from a basis (pages 286–307).

III. Sets

12. Extensionality, subsets and supersets, separation, Russell's paradox, empty set, powerset, Hasse and Venn diagrams (pages 308–334).

13. The powerset Boolean algebra, unordered and ordered pairing, products, big unions, big intersections (pages 335–371).

14. Disjoint unions, relations, internal diagrams, relational composition, matrices (pages 372–393).

15. Directed graphs, reachability, preorders, reflexive-transitive closure (pages 394–404).

16. Partial functions, (total) functions, bijections, equivalence relations and set partitions (pages 405–433).

17 Calculus of bijections, characteristic (or indicator) functions, finite and infinite sets, surjections (pages 434–446).

18. Enumerability and countability, choice, injections, Cantor-Bernstein-Schroeder theorem (pages 447–459).

19. Direct and inverse images, replacement and set-indexing, unbounded cardinality, foundation (pages 460–484).

Preliminaries

Complementary reading:

- Preface and Part I of *How to Think Like a Mathematician* by K. Houston.

Some friendly advice

by K. Houston from the Preface of

How to Think Like a Mathematician

- It's up to you.
- Think for yourself.
- Observe.
- Seek to understand.
- Collaborate.
- Be active.
- Question everything.
- Prepare to be wrong.
- Develop your intuition.
- Reflect.

Study skills

Part I of *How to Think Like a Mathematician*
by K. Houston

- Reading mathematics
- Writing mathematics
- How to solve problems

Proofs

Topics

Proofs in practice. Mathematical jargon: statement, predicate, theorem, proposition, lemma, corollary, conjecture, proof, logic, axiom, definition. Mathematical statements: implication, bi-implication, universal quantification, conjunction, existential quantification, disjunction, negation. Logical deduction: proof strategies and patterns, scratch work, logical equivalences. Proof by contradiction. Divisibility and congruences. Fermat's Little Theorem.

Complementary reading:

- ▶ Parts II, IV, and V of *How to Think Like a Mathematician* by K. Houston.
- ▶ Chapters 1 and 8 of *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.
- ★ Chapter 3 of *How to Prove it* by D. J. Velleman.
- ★ Chapter II of *The Higher Arithmetic* by H. Davenport.

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; and that, in passing, will allow you to solve the following . . .

Puzzle

5 pirates have accumulated a tower of n cubes each of which consists of n^3 golden dice, for an unknown (but presumably large) number n. This treasure is put on a table around which they sit on chairs numbered from 0 to 4, and they are to split it by simultaneously taking a die each with every tick of the clock provided that five or more dice are available on the table. At the end of this process there will be r remaining dice which will go to the pirate sitting on the chair numbered r. What chair should a pirate sit on to maximise his gain?

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. 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:

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

which further presupposes that you know:

- what variables are;
- what

  $$\text{if} \ldots \text{then} \ldots$$

  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'

Euler's Identity *With τ and e the mathematical constants*

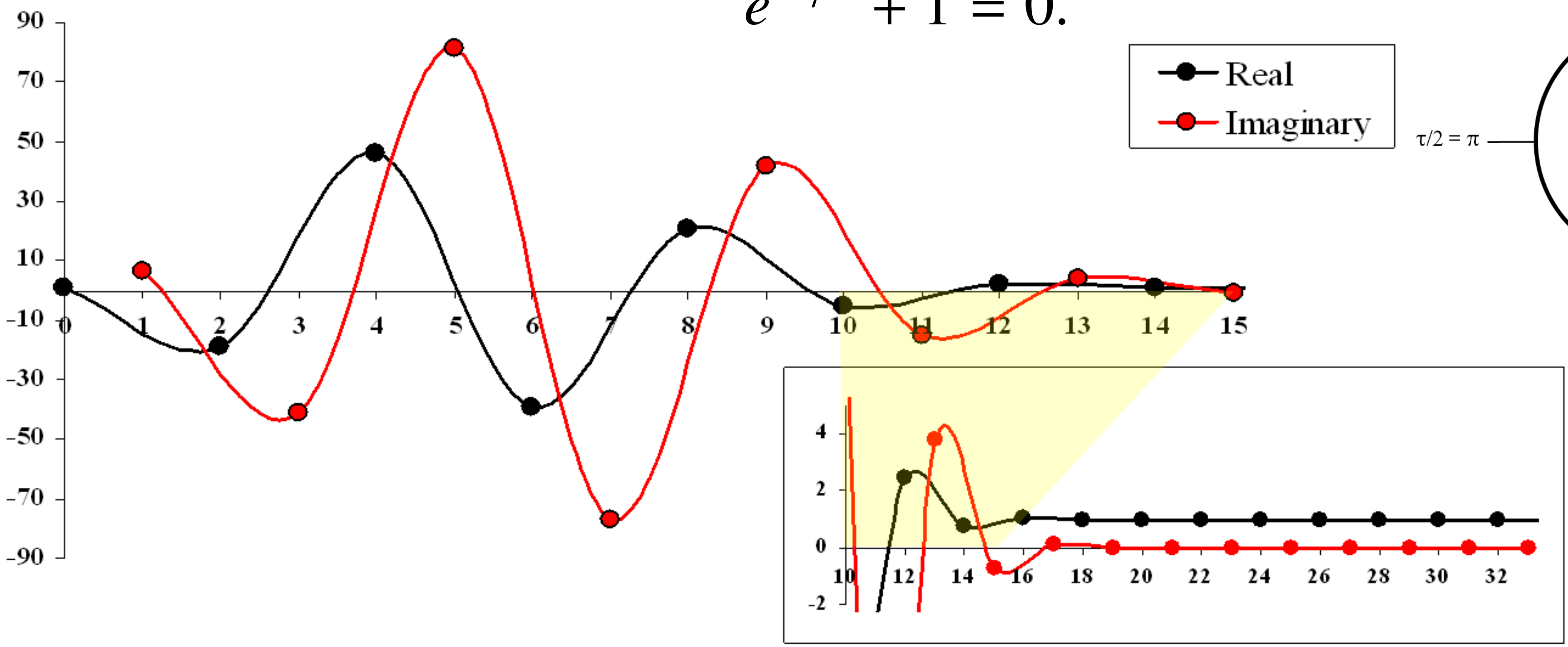
$$\tau = 2\pi = 6.2831853071\ 7958647692\ 5286766559\ 0057683943\ 3879875021\ 1641949889\ 1846156328\ 1257241799\ 7256069650\ 6842341359\ldots$$

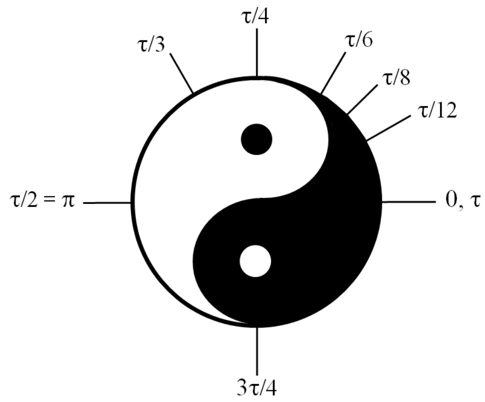
and

$$e = 2.7182818284\ 5904523536\ 0287471352\ 6624977572\ 4709369995\ 9574966967\ 6277240766\ 3035354759\ 4571382178\ 5251664274\ldots$$

(the first 100 places of decimal being given), and using i to denote $\sqrt{-1}$, we have

$$e^{i\tau/2} + 1 = 0.$$





Squaring both sides of $e^{i\tau/2} = -1$ gives $e^{i\tau} = 1$, encoding the defining fact that τ radians measures one full circumference. The calculation can be confirmed explicitly using the evaluation of e^z, for any complex number z, as an infinite sum: $e^z = 1 + z + z^2/2! + z^3/3! + z^4/4! + \ldots$. The even powers of $i = \sqrt{-1}$ alternate between 1 and -1, while the odd powers alternate between i and $-i$, so we get two separate sums, one with i's (the imaginary part) and one without (the real part). Both converge rapidly as shown in the two plots above: the real part to 1, the imaginary to 0. In the *limit* equality is attained, $e^{i\tau} = 1 + 0 \times i$, whence $e^{\tau i} = 1$. The value of $e^{i\tau/2}$ may be confirmed in the same way.

Combining as it does the six most fundamental constants of mathematics: 0, 1, 2, i, τ and e, the identity has an air of magic. J.H. Conway, in The Book of Numbers, traces the identity to Leonhard Euler's 1748 *Introductio*; certainly Euler deserves credit for the much more general formula $e^{i\theta} = \cos\theta + i\sin\theta$, from which the identity follows using $\theta = \tau/2$ radians (180°).

Web link: `fermatslasttheorem.blogspot.com/2006/02/eulers-identity.html`

Further reading: *Dr Euler's Fabulous Formula: Cures Many Mathematical Ills,* by Paul J. Nahin, Princeton University Press, 2006

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

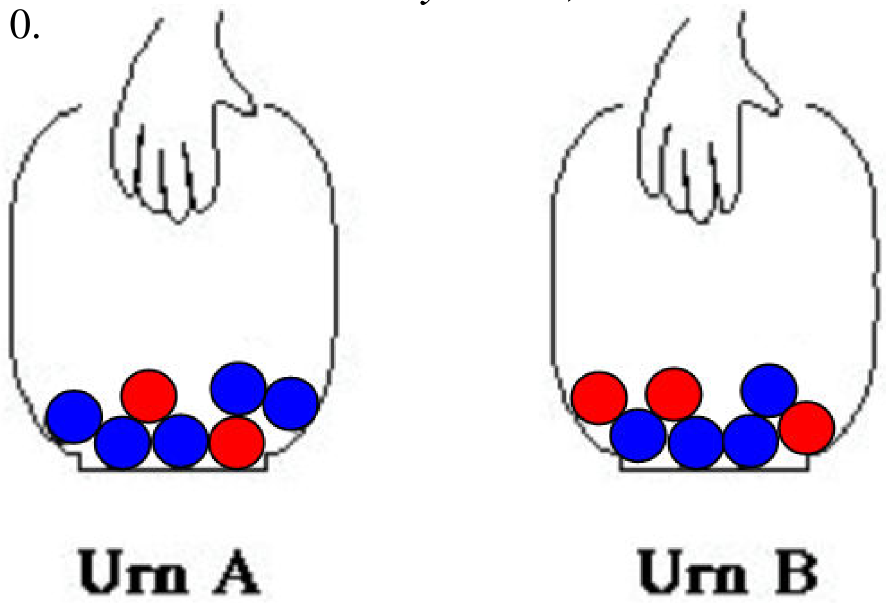
1. *Fermat's Last Theorem*
2. *The Pumping Lemma*

THEOREM OF THE DAY

Fermat's Last Theorem *If x, y, z and n are integers satisfying*

$$x^n + y^n = z^n,$$

then either $n \leq 2$ or $xyz = 0$.



It is easy to see that we can assume that all the integers in the theorem are positive. So the following is a legitimate, but totally different, way of asserting the theorem: we take a ball at random from Urn A; then replace it and take a 2nd ball at random. Do the same for Urn B. The probability that both A balls are blue, for the urns shown here, is $\frac{5}{7} \times \frac{5}{7}$. The probability that both B balls are the same colour (both blue or both red) is $(\frac{4}{7})^2 + (\frac{3}{7})^2$. Now the Pythagorean triple $5^2 = 3^2 + 4^2$ tells us that the probabilities are equal: $\frac{25}{49} = \frac{9}{49} + \frac{16}{49}$. What if we choose $n > 2$ balls with replacement? Can we again fill each of the urns with N balls, red and blue, so that taking n with replacement will give equal probabilities? Fermat's Last Theorem says: only in the trivial case where all the balls in Urn A are blue (which includes, vacuously, the possibility that $N = 0$.)

Another, much more profound restatement: if $a^n + b^n$, for $n > 2$ and positive integers a and b, is again an n-th power of an integer then the elliptic curve $y^2 = x(x - a^n)(x + b^n)$, known as the **Frey curve**, cannot be modular (is not a rational map of a modular curve). So it is enough to prove the **Taniyama-Shimura-Weil conjecture:** all rational elliptic curves are modular.

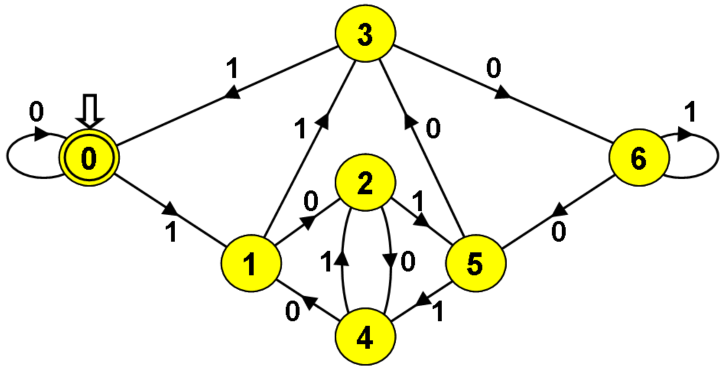
Fermat's innocent statement was famously left unproved when he died in 1665 and was the last of his unproved 'theorems' to be settled true or false, hence the name. The non-modularity of the Frey curve was established in the 1980s by the successive efforts of Gerhard Frey, Jean-Pierre Serre and Ken Ribet. The Taniyama-Shimura-Weil conjecture was at the time thought to be 'inaccessible' but the technical virtuosity (not to mention the courage and stamina) of Andrew Wiles resolved the 'semistable' case, which was enough to settle Fermat's assertion. His work was extended to a full proof of Taniyama-Shimura-Weil during the late 90s by Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor.

Web link: math.stanford.edu/~lekheng/flt/kleiner.pdf

Further reading: *Fermat's Last Theorem* by Simon Singh, Fourth Estate Ltd, London, 1997.

THEOREM OF THE DAY

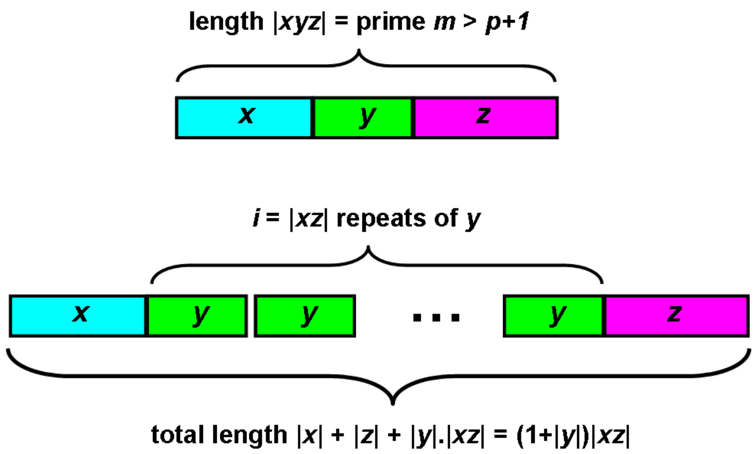
The Pumping Lemma *Let $\mathcal{L}$ be a regular language. Then there is a positive integer p such that any word $w \in \mathcal{L}$ of length exceeding p can be expressed as $w = xyz$, $|y| > 0$, $|xy| \leq p$, such that, for all $i \geq 0$, xy^iz is also a word of $\mathcal{L}$.*



repeat

input	0	1	0	1	0	0	1	1	0	0	1
state	0	1	2	5	3	6	6	6	5	3	0
accept	✓										✓

The set {x : $x = 7k$, x in base 2 } is a regular language



The set {a^n : n prime} is not a regular language

Regular languages over an alphabet Σ (e.g. $\{0, 1\}$) are precisely those strings of letters which are 'recognised' by some *deterministic finite automaton* (DFA) whose edges are labelled from Σ. Above left, such a DFA is shown, which recognises the language consisting of all positive multiples of 7, written in base two. The number $95 \times 7 = 665 = 2^9 + 2^7 + 2^4 + 2^3 + 2^0$ is expressed in base 2 as 1010011001. Together with any leading zeros, these digits, read left to right, will cause the edges of the DFA to be traversed from the initial state (heavy vertical arrow) to an accepting state (coincidentally the same state, marked with a double circle), as shown in the table below the DFA. Notice that the bracketed part of the table corresponds to a cycle in the DFA and this may occur zero or more times without affecting the string's recognition. This is the idea behind the pumping lemma, in which p, the 'pumping length', may be taken to be the number of states of the DFA.

So a DFA can be smart enough to recognise multiples of a particular prime number. But it cannot be smart enough recognise all prime numbers, even expressed in *unary* notation ($2 = aa$, $3 = aaa$, $5 = aaaaa$, etc). The proof, above right, typifies the application of the pumping lemma in disproofs of regularity : assume a recognising DFA exists and exhibit a word which, when 'pumped' must fall outside the recognised language.

This lemma, which generalises to context-free languages, is due to Yehoshua Bar-Hillel (1915–1975), Micha Perles and Eli Shamir.

Web link: www.seas.upenn.edu/~cit596/notes/dave/pumping0.html (and don't miss www.cs.brandeis.edu/~mairson/poems/node1.html!)

Further reading: *Models of Computation and Formal Languages* by R Gregory Taylor, Oxford University Press Inc, USA, 1997.

Conjecture

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

Example 4

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

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

Definition 7 *An integer is said to be* odd *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:

YOUR PROOF OF Proposition 8 (on page 31):

MY PROOF OF Proposition 8 (on page 31): Let m and n be arbitrary odd integers. Thus, $m = 2 \cdot i + 1$ and $n = 2 \cdot j + 1$ for some integers i and j. Hence, we have that $m \cdot n = 2 \cdot k + 1$ for $k = 2 \cdot i \cdot j + i + j$, showing that $m \cdot n$ is odd.

Warning: Though the scratch work

$$\boxed{\begin{array}{l} \qquad m = 2 \cdot i + 1 \qquad n = 2 \cdot j + 1 \\ \therefore \\ \begin{aligned} m \cdot n &= (2 \cdot i + 1) \cdot (2 \cdot j + 1) \\ &= 4 \cdot i \cdot j + 2 \cdot i + 2 \cdot j + 1 \\ &= 2 \cdot (2 \cdot i \cdot j + i + j) + 1 \end{aligned} \end{array}}$$

contains the idea behind the given proof,

I will not accept it as a proof!

Mathematical proofs ...

A *mathematical proof* is a sequence of logical deductions from axioms and previously proved statements that concludes with the proposition in question.

The axiom-and-proof approach is called the *axiomatic method*.

. . . in computer science

Mathematical proofs play a growing role in computer science (e.g. they are used to certify that software and hardware will *always* behave correctly; something that no amount of testing can do).

For a computer scientist, some of the most important things to prove are the correctness of programs and systems —whether a program or system does what it's supposed to do. Developing mathematical methods to verify programs and systems remains and active research area.

Writing good proofs

from Section 1.9 of *Mathematics for Computer Science*
by E. Lehman, F.T. Leighton, and A.R. Meyer

- State your game plan.
- Keep a linear flow.
- A proof is an essay, not a calculation.
- Avoid excessive symbolism.
- Revise and simplify.
- Introduce notation thoughtfully.
- Structure long proofs.
- Be wary of the “obvious”.
- Finish.

How to solve it

by G. Polya

- You have to understand the problem.
- Devising a plan.

  Find the connection between the data and the unknown. You may be obliged to consider auxiliary problems if an immediate connection cannot be found. You should obtain eventually a plan of the solution.
- Carry out your plan.
- Looking back.

  Examine the solution obtained.

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’

Proof Structure

Assumptions	Goals
statements that may be used for deduction	statements to be established

Implication

Theorems can usually be written in the form

> **if** a collection of *assumptions* holds,
> **then** so does some *conclusion*

or, in other words,

> a collection of *assumptions* **implies** some *conclusion*

or, in symbols,

> a collection of *hypotheses* $\implies$ some *conclusion*

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

Implications

- How to *prove* them as goals.
- How to *use* them as assumptions.

How to prove implication goals

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

$$P \implies Q$$

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 $m \cdot n$.*

YOUR PROOF:

MY PROOF: Assume that m and n are odd integers. That is, by definition, assume that $m = 2 \cdot i + 1$ for some integer i and that $n = 2 \cdot j + 1$ for some integer j. Hence, we have that $m \cdot n = (2 \cdot i + 1) \cdot (2 \cdot j + 1) = 2 \cdot (2 \cdot i \cdot j + i + j) + 1$ and thus $m \cdot n = 2 \cdot k + 1$ for the integer $k = 2 \cdot i \cdot j + i + j$, showing that $m \cdot n$ is indeed odd.

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 $\sqrt{x}$ is rational then so is x.*

YOUR PROOF:

MY PROOF: Assume that x is a positive real number and that $\sqrt{x}$ is a rational number. That is, by definition, $\sqrt{x} = m/n$ for some integers m and n. It follows that $x = m^2/n^2$ and, since m^2 and n^2 are natural numbers, we have that x is a rational number as required.

How to use implication assumptions

Logical Deduction by 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 $P \implies Q$, 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 $P_1 \implies P_3$.*

Scratch work:

	Assumptions	Goal
		P_3
(i)	P_1, P_2, and P_3 are statements.	
(ii)	$P_1 \implies P_2$	
(iii)	$P_2 \implies P_3$	
(iv)	P_1	

Now, by Modus Ponens from (ii) and (iv), we have that

(v) $\quad P_2$ holds

and, by Modus Ponens from (iii) and (v), we have that

$\quad P_3$ holds

as required.

Homework Turn the above scratch work into a proof.

NB Often a proof of $P \implies Q$ factors into a chain of implications, each one a manageble step:

$$\begin{aligned} P &\implies P_1 \\ &\implies P_2 \\ &\vdots \\ &\implies P_n \\ &\implies Q \end{aligned}$$

which is shorthand for

$$P \implies P_1 \quad , \quad P_1 \implies P_2 \quad , \quad \ldots \quad , \quad P_n \implies Q \quad .$$

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 $Q \implies P$.

Divisibility and congruence

Definition 12 *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* $n = k \cdot d$*.*

Btw Other terminologies for the notation $d \mid n$ are 'd is a factor of n', 'n is divisible by d', and 'n is a multiple of d'.

Example 13 *The statement* $2 \mid 4$ *is true, while* $4 \mid 2$ *is not.*

NB The symbol "$\mid$" is *not* an operation on integers; it is a *predicate*, i.e. a property that a pair of integers may or may not have between themselves.

Definition 14 *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 15

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

NB The notion of congruence vastly generalises that of even and odd:

Proposition 16 *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,* $n \equiv 1 \pmod{2}$*.*

Homework Prove the above proposition.

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 quantifications

- How to *prove* them as goals.
- How to *use* them as assumptions.

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 17

1. *Proposition 8 (on page 31).*
2. *(Proposition 10 on page 50) For every positive real number x, if $\sqrt{x}$ is rational then so is x.*
3. *(Proposition 42 on page 147) For every integer n, we have that n is even iff so is n^2.*
4. *Proposition 16 (on page 61).*

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.

   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)
$\vdots$	

Example:

Assumptions	unprovable Goal
$\vdots$	for all integers n, $n \geq 1$
$n > 0$	
$\vdots$	

How to use universal statements

Assumptions

$$\vdots$$

$$\forall x.\, x^2 \geq 0$$

$$\vdots$$

$$\pi^2 \geq 0$$

$$e^2 \geq 0$$

$$0^2 \geq 0$$

$$\vdots$$

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 18 *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 $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$.*

YOUR PROOF:

MY PROOF: Let m and a, b be integers with m positive.

$(\Longrightarrow)$ Assume that $a \equiv b \pmod{m}$; that is, by definition, that $a - b = k \cdot m$ for some integer k. We need show that for all positive integers n,

$$n \cdot a \equiv n \cdot b \pmod{n \cdot m} \ .$$

Indeed, for an arbitrary positive integer n, we then have that $n \cdot a - n \cdot b = n \cdot (a - b) = n \cdot k \cdot m$; so that $n \cdot m \mid (n \cdot a - n \cdot b)$, and hence we are done.

$(\Longleftarrow)$ Assume that for all positive integers n, we have that $n \cdot a \equiv n \cdot b \pmod{n \cdot m}$. In particular, we have this property for $n = 1$, which states that $1 \cdot a \equiv 1 \cdot b \pmod{1 \cdot m}$; that is, that $a \equiv b \pmod{m}$.

Equality in proofs

Examples:

- If $a = b$ and $b = c$ then $a = c$.
- If $a = b$ and $x = y$ then $a + x = b + x = b + y$.

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.

Conjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.

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,

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

The proof strategy for conjunction:

To prove a goal of the form

$$P \land Q$$

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 $P \land Q$,
treat it as two separate assumptions: P and Q.

Theorem 19 *For every integer n, we have that $6 \mid n$ iff $2 \mid n$ and $3 \mid n$.*

YOUR PROOF:

MY PROOF: Let n be an arbitrary integer.

$(\Longrightarrow)$ Assume $6 \mid n$; that is, $n = 6 \cdot k$ for some integer k.

Firstly, we show that $2 \mid n$; which is indeed the case because $n = 2 \cdot (3 \cdot k)$.

Secondly, we show that $3 \mid n$; which is indeed the case because $n = 3 \cdot (2 \cdot k)$.

$(\Longleftarrow)$ Assume that $2 \mid n$ and that $3 \mid n$. Thus, $n = 2 \cdot i$ for an integer i and also $n = 3 \cdot j$ for an integer j. We need prove that $n = 6 \cdot k$ for some integer k. The following calculation shows that this is indeed the case:

$$6 \cdot (i - j) \; = \; 3 \cdot (2 \cdot i) - 2 \cdot (3 \cdot j) \; = \; 3 \cdot n - 2 \cdot n \; = \; n \; .$$

Existential quantifications

- How to *prove* them as goals.
- How to *use* them as assumptions.

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 [a] .

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.

---

[a] See also page 377.

Theorem 20 (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: 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 21 *For every positive integer* k*, there exist natural numbers* i *and* j *such that* $4 \cdot k = i^2 - j^2$*.*

Scratch work:

k	i	j
1	2	0
2	3	1
3	4	2
$\vdots$		
n	$n+1$	$n-1$
$\vdots$		

YOUR PROOF OF Proposition 21:

MY PROOF OF Proposition 21: For an arbitrary positive integer k, let $i = k + 1$ and $j = k - 1$. Then,

$$\begin{aligned} i^2 - j^2 &= (k+1)^2 - (k-1)^2 \\ &= k^2 + 2 \cdot k + 1 - k^2 + 2 \cdot k - 1 \\ &= 4 \cdot k \end{aligned}$$

and we are done.

Proposition 22 *For every positive integer n, there exists a natural number l such that $2^l \leq n < 2^{l+1}$.*

YOUR PROOF:

MY PROOF: For an arbitrary positive integer n, let $l = \lfloor \log n \rfloor$. We have that

$$l \leq \log n < l + 1$$

and hence, since the exponential function is increasing, that

$$2^l \leq 2^{\log n} < 2^{l+1} \; .$$

As, $n = 2^{\log n}$ we are done.

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

YOUR PROOF:

MY PROOF: Let l, m, and n be arbitrary integers. Assume that $l \mid m$ and that $m \mid n$; that is, that

$$(\dagger) \quad \exists \text{ integer } i \,.\; m = i \cdot l$$

and that

$$(\ddagger) \quad \exists \text{ integer } j \,.\; n = j \cdot m \quad .$$

From $(\dagger)$, we can thus assume that $m = i_0 \cdot l$ for some integer i_0 and, from $(\ddagger)$, that $n = j_0 \cdot m$ for some integer j_0. With this, our goal is to show that $l \mid n$; that is, that there exists an integer k such that $n = k \cdot l$. To see this, let $k = j_0 \cdot i_0$ and note that $k \cdot l = j_0 \cdot i_0 \cdot l = j_0 \cdot m = n$.

Unique existence

The notation

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

stands for

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

This may be expressed in a variety of equivalent ways as follows:

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

2. $\exists x.\, \big(P(x) \wedge \forall y.\, P(y) \implies y = x\big)$

3. $\exists x.\, \forall y.\, P(y) \iff y = x$

where the first statement is the one most commonly used in proofs.

Example: The congruence property modulo m uniquely characterises the natural numbers from 0 to $m-1$.

Proposition 24 *Let m be a positive integer and let n be an integer.*

Define

$$P(z) \;=\; [\, 0 \leq z < m \;\wedge\; z \equiv n \pmod{m} \,] \quad .$$

Then

$$\forall\, x, y.\, P(x) \;\wedge\; P(y) \;\implies\; x = y \quad .$$

Your proof:

MY PROOF: Let m be a positive integer and let n be an integer.

Let x and y be arbitrary and assume: (1.1) $0 \leq x < m$ and (1.2) $x \equiv n \pmod{m}$; and (2.1) $0 \leq y < m$ and (2.2) $y \equiv n \pmod{m}$.

From (1.2) and (2.2), $x - y = k \cdot m$ for some integer k. Therefore, by (1.1) and (2.1), $k \cdot m = x - y < m$; and so $k \leq 0$. Analogously, by (1.1) and (2.1), $-k \cdot m = y - x < m$; and so $-k \leq 0$. Thus, $k = 0$ and $x = y$.

A proof strategy

To prove

$$\forall\, x.\, \exists!\, y.\, P(x, y) \quad ,$$

for an arbitrary x construct the unique witness and name it, say as $f(x)$, showing that

$$P\big(x, f(x)\big)$$

and

$$\forall\, y.\, P(x, y) \implies y = f(x)$$

hold.

Disjunctions

- How to *prove* them as goals.
- How to *use* them as assumptions.

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 $n^2 \equiv 1 \pmod 4$.*

YOUR PROOF:

MY PROOF SKETCH: Let n be an arbitrary integer.

We may try to prove that $n^2 \equiv 0 \pmod{4}$, but this is not the case as $1^2 \equiv 1 \pmod{4}$.

We may instead try to prove that $n^2 \equiv 1 \pmod{4}$, but this is also not the case as $0^2 \equiv 0 \pmod{4}$.

So we try breaking the proof into cases. In view of a few experiments, we are led to consider the following two cases:

(i) n is even.

(ii) n is odd.

and try to see whether in each case either $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$ can be established.

In the first case (i), n is of the form $2 \cdot m$ for some integer m. It follows that $n^2 = 4 \cdot m^2$ and hence that $n^2 \equiv 0 \pmod 4$.

In the second case (ii), n is of the form $2 \cdot m + 1$ for some integer m. So it follows that $n^2 = 4 \cdot m \cdot (m+1) + 1$ and hence that $n^2 \equiv 1 \pmod 4$.

NB The proof sketch contains a proof of the following:

Lemma 26 *For all integers* n*,*

1. *if* n *is even, then* $n^2 \equiv 0 \pmod{4}$*; and*

2. *if* n *is odd, then* $n^2 \equiv 1 \pmod{4}$*.*

Hence, for all integers n*, either* $n^2 \equiv 0 \pmod{4}$ *or* $n^2 \equiv 1 \pmod{4}$*.*

Another proof strategy for disjunction:

Proof pattern:

In order to prove

$$P \vee Q$$

write: If P is true, then of course $P \vee Q$ is true. Now suppose that P is false. and provide a proof of Q.

NB This arises from the main proof strategy for disjunction where the proof has been broken in the two cases:

(i) P holds.

(ii) P does not hold.

Scratch work:

Before using the strategy

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

After using the strategy

Assumptions	Goal
	Q
$\vdots$	
not P	

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* $\binom{p}{m} \equiv 1 \pmod{p}$*.*

YOUR PROOF:

MY PROOF: Let p be an arbitrary positive integer and m an arbitrary natural number.

From $m = 0$ or $m = p$, we need show that $\binom{p}{m} \equiv 1 \pmod{p}$. We prove the following two cases in turn: (i) that assuming $m = 0$, we have $\binom{p}{m} \equiv 1 \pmod{p}$; and (ii) that assuming $m = p$, we have $\binom{p}{m} \equiv 1 \pmod{p}$.

Case (i): Assume $m = 0$. Then, $\binom{p}{m} = 1$ and so $\binom{p}{m} \equiv 1 \pmod{p}$.

Case (ii): Assume $m = p$. Then, $\binom{p}{m} = 1$ and so $\binom{p}{m} \equiv 1 \pmod{p}$.

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

YOUR PROOF:

MY PROOF: Let p and m be arbitrary integers. Assume that p is prime and that $0 < m < p$. Then, $\binom{p}{m} = p \cdot [\frac{(p-1)!}{m! \cdot (p-m)!}]$ and since the fraction $\frac{(p-1)!}{m! \cdot (p-m)!}$ is in fact a natural number[a], we are done.

[a]Provide the missing argument, noting that it relies on p being prime and on m being a positive integer less than p. (See Corollary 85 on page 241.)

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

YOUR PROOF:

MY PROOF: Let m be a natural number less than or equal a prime number p. We establish that either $\binom{p}{m} \equiv 0 \pmod{p}$ or $\binom{p}{m} \equiv 1 \pmod{p}$ by breaking the proof into three cases:

$$\text{(i) } m = 0 \quad , \quad \text{(ii) } 0 < m < p \quad , \quad \text{(iii) } m = p$$

and showing, in each case, that either $\binom{p}{m} \equiv 0 \pmod{p}$ or $\binom{p}{m} \equiv 1 \pmod{p}$ can be established.

Indeed, in the first case (i), by Lemma 27 (on page 116), we have that $\binom{p}{m} \equiv 1 \pmod{p}$; in the second case (ii), by Lemma 28 (on page 118), we have that $\binom{p}{m} \equiv 0 \pmod{p}$; and, in the third case (iii), by Lemma 27 (on page 116), we have that $\binom{p}{m} \equiv 1 \pmod{p}$.

Binomial Theorem

Theorem 30 (Binomial Theorem)[a] *For all natural numbers* n*,*

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

Corollary 31

1. *For all natural numbers* n*,* $(z + 1)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} \cdot z^k$

2. $2^n \;=\; \sum_{k=0}^{n} \binom{n}{k}$

Corollary 32 *For all prime numbers* p*,* $2^p \equiv 2 \pmod{p}$*.*

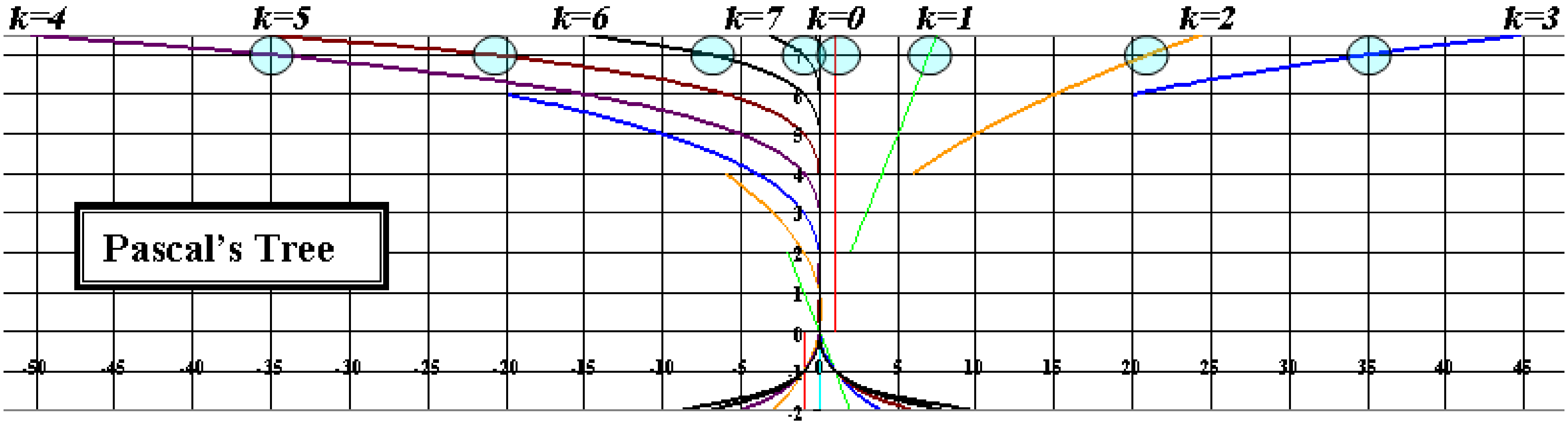
---

[a] See page 270.

THEOREM OF THE DAY

The Binomial Theorem *For n a positive integer and real-valued variables x and y,*

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



Given n distinct objects, the binomial coefficient $\binom{n}{k} = n!/k!(n-k)!$ counts the number of ways of choosing k. Transcending its combinatorial role, we may instead write the binomial coefficient as: $\binom{n}{k} = \frac{n}{k} \times \frac{n-1}{k-1} \times \cdots \times \frac{n-(k-1)}{1}$; taking $\binom{n}{0} = 1$. This form is defined when n is a real or even a complex number. In the above graph, n is a real number, and increases continuously on the vertical axis from -2 to 7.5. For different values of k, the value of $\binom{n}{k}$ has been plotted but with its sign reversed on reaching $n = 2k$, giving a discontinuity. This has the effect of spreading the binomial coefficients out on either side of the vertical axis: we recover, for integer n, a sort of (upside down) Pascal's Triangle. The values of the triangle for $n = 7$ have been circled.

If the right-hand summation in the theorem is extended to $k = \infty$, the result still holds, provided the summation converges. This is guaranteed when n is an integer or when $|y/x| < 1$, so that, for instance, summing for $(4+1)^{1/2}$ gives a method of calculating $\sqrt{5}$.

The binomial theorem may have been known, as a calculation of poetic metre, to the Hindu scholar Pingala in the 5th century BC. It can certainly be dated to the 10th century AD. The extension to complex exponent n, using generalised binomial coefficients, is usually credited to Isaac Newton.

Web link: www.iwu.edu/~lstout/aesthetics.pdf an absorbing discussion on the aesthetics of proof.

Further reading: *A Primer of Real Analytic Functions, 2nd ed.* by Steven G. Krantz and Harold R. Parks, Birkhäuser Verlag AG, 2002, section 1.5.

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

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

YOUR PROOF: [a]

[a]Hint: Use Proposition 29 (on page 120) and the Binomial Theorem (Theorem 30 (on page 122)).

MY PROOF: Let m, n, and p be natural numbers with p prime.

Here are two arguments.

1. By the Binomial Theorem (Theorem 30 on page 122),

   $$(m+n)^p - (m^p + n^p) = p \cdot \left[\sum_{k=1}^{p-1} \frac{(p-1)!}{k! \cdot (p-k)!} \cdot m^{p-k} \cdot n^k \right] .$$

   Since for $1 \leq k \leq p-1$ each fraction $\frac{(p-1)!}{k! \cdot (p-k)!}$ is in fact a natural number, we are done.

2. By the Binomial Theorem (Theorem 30 on page 122) and Proposition 29 (on page 120),

   $$(m+n)^p - (m^p + n^p) = \sum_{k=1}^{p-1} \binom{p}{k} \cdot m^{p-k} \cdot n^k \equiv 0 \pmod{p} .$$

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

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,*

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

YOUR PROOF: [a]

[a] Hint: Consider the cases $i = 0$ and $i > 0$ separately. In the latter case, iteratively use the Dropout Lemma a number of $i = \underbrace{1 + \cdots + 1}_{i \text{ ones}}$ times.

MY PROOF: Let m and i be natural numbers and let p be a prime. Using the Dropout Lemma (Corollary 34) one calculates i times, for j ranging from 0 to i, as follows:

$$
\begin{aligned}
(m+i)^p &\equiv \big(m+(i-1)\big)^p + 1 \\
&\equiv \cdots \\
&\equiv \big(m+(i-j)\big)^p + j \\
&\equiv \cdots \\
&\equiv m^p + i
\end{aligned}
$$

Fermat's Little Theorem

The Many Dropout Lemma (Proposition 35) gives the first 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 (see page 239) .

Every natural number i not a multiple of a prime number p has a *reciprocal* modulo p, namely i^{p-2}, as $i \cdot (i^{p-2}) \equiv 1 \pmod{p}$.

Btw

1. The answer to the puzzle on page 17 is:

   on the chair numbered 1

   because, by Fermat's Little Theorem, either $n^4 \equiv 0 \pmod{5}$ or $n^4 \equiv 1 \pmod{5}$.

2. Fermat's Little Theorem has applications to:

   (a) primality testing[a],

   (b) the verification of floating-point algorithms, and

   (c) cryptographic security.

---

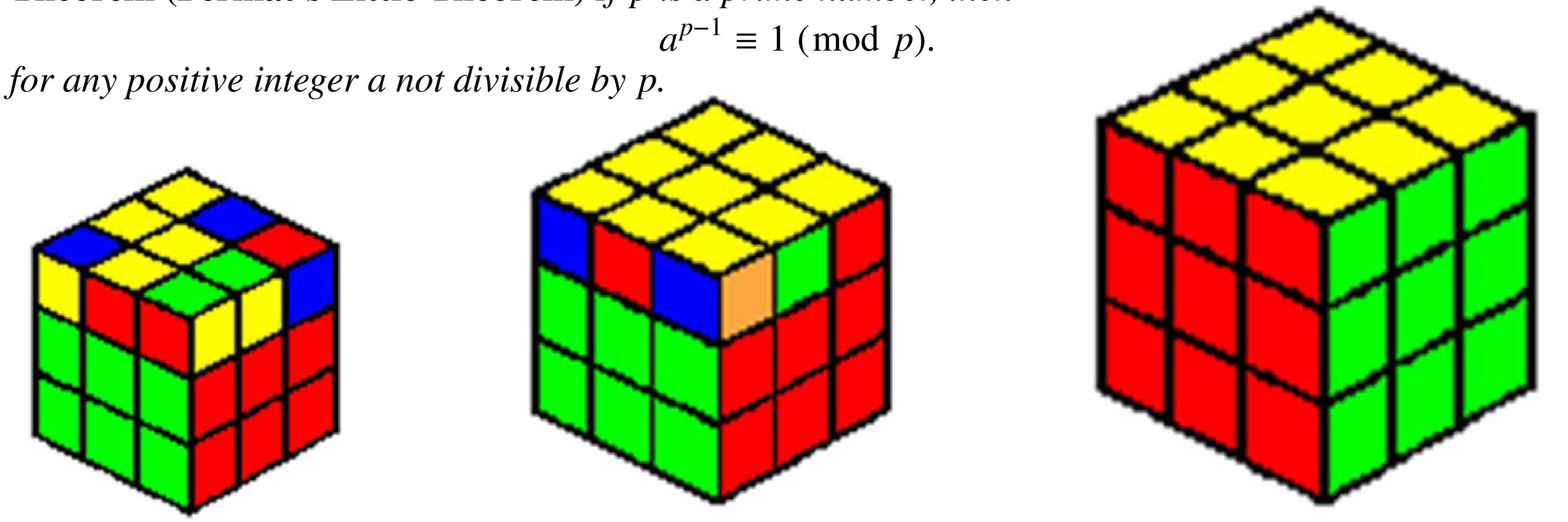
[a] For instance, to establish that a positive integer m is not prime one may proceed to find an integer i such that $i^m \not\equiv i \pmod{m}$.

THEOREM OF THE DAY

Theorem (Fermat's Little Theorem) *If p is a prime number, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

for any positive integer a not divisible by p.



Suppose $p = 5$. We can imagine a row of a copies of an $a \times a \times a$ Rubik's cube (let us suppose, although this is not how Rubik created his cube, that each is made up of a^3 little solid cubes, so that is a^4 little cubes in all.) Take the little cubes 5 at a time. For three standard 3×3 cubes, shown here, we will eventually be left with precisely one little cube remaining. Exactly the same will be true for a pair of 2×2 'pocket cubes' or four of the 4×4 'Rubik's revenge' cubes. The 'Professor's cube', having $a = 5$, fails the hypothesis of the theorem and gives remainder zero.

The converse of this theorem, that $a^{p-1} \equiv 1 \pmod{p}$, for some a not dividing p, implies that p is prime, does not hold. For example, it can be verified that $2^{340} \equiv 1 \pmod{341}$, while 341 is not prime. However, a more elaborate test *is* conjectured to work both ways: remainders add, so the Little Theorem tells us that, modulo p, $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv \overbrace{1 + 1 + \ldots + 1}^{p-1} = p - 1$. The 1950 conjecture of the Italian mathematician Giuseppe Giuga proposes that this *only* happens for prime numbers: a positive integer n is a prime number if and only if $1^{n-1} + 2^{n-1} + \ldots + (n-1)^{n-1} \equiv n - 1 \pmod{n}$. The conjecture has been shown by Peter Borwein to be true for all numbers with up to 13800 digits (about 5 complete pages of digits in 12-point courier font!)

Fermat announced this result in 1640, in a letter to a fellow civil servant Frénicle de Bessy. As with his 'Last Theorem' he claimed that he had a proof but that it was too long to supply. In this case, however, the challenge was more tractable: Leonhard Euler supplied a proof almost 100 years later which, as a matter of fact, echoed one in an unpublished manuscript of Gottfried Wilhelm von Leibniz, dating from around 1680.

Web link: www.math.uwo.ca/~dborwein/cv/giuga.pdf. The cube images are from: www.ws.binghamton.edu/fridrich/.

Further reading: *Elementary Number Theory, 6th revised ed.,* by David M. Burton, MacGraw-Hill, 2005, chapter 5.

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

$$\neg(P \implies Q) \iff P \wedge \neg Q$$

$$\neg(P \iff Q) \iff P \iff \neg Q$$

$$\neg(\forall x. P(x)) \iff \exists x. \neg P(x)$$

$$\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$$

$$\neg(\exists x. P(x)) \iff \forall x. \neg P(x)$$

$$\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$$

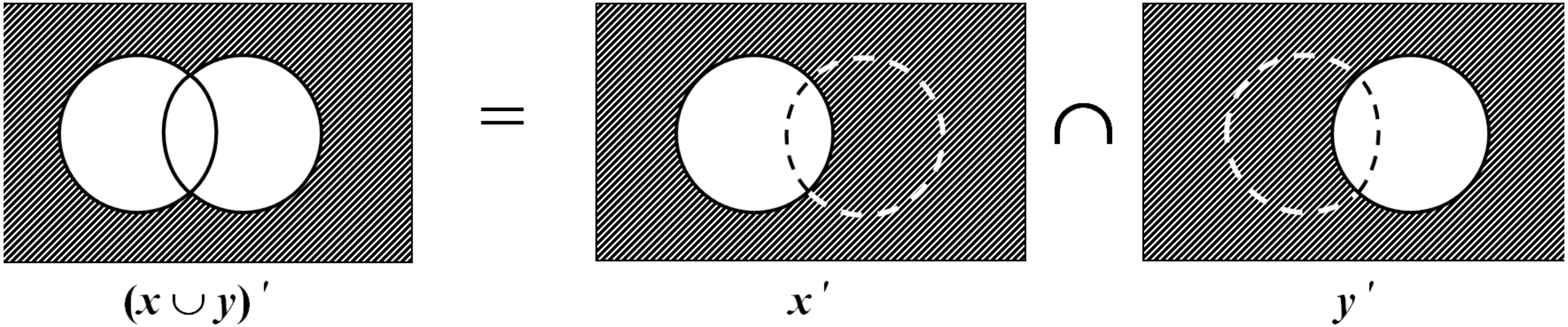
$$\neg(\neg P) \iff P$$

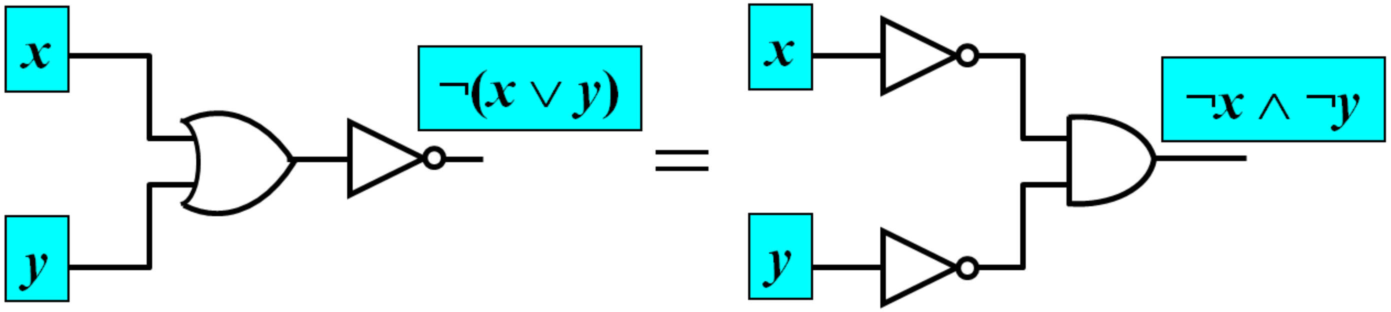
$$\neg P \iff (P \Rightarrow \mathbf{false})$$

THEOREM OF THE DAY

De Morgan's Laws *If B, a set containing at least two elements, and equipped with the operations $+$, $\times$ and $'$ (complement), is a Boolean algebra, then, for any x and y in B,*

$$(x+y)' = x' \times y', \text{ and } (x \times y)' = x' + y'.$$





Truth table verification:

x	y	$\neg$	$(x \vee y)$	$\neg x$	$\wedge$	$\neg y$
0	0	1	0	1	1	1
0	1	0	1	1	0	0
1	0	0	1	0	0	1
1	1	0	1	0	0	0

and $\neg(x \wedge y) = \neg x \vee \neg x$ similarly.

De Morgan's laws are readily derived from the axioms of Boolean algebra and indeed are themselves sometimes treated as axiomatic. They merit special status because of their role in translating between $+$ and $\times$, which means, for example, that Boolean algebra can be defined entirely in terms of one or the other. This property, entirely absent in the arithmetic of numbers, would seem to mark Boolean algebras as highly specialised creatures, but they are found everywhere from computer circuitry to the sigma-algebras of probability theory. The illustration here shows De Morgan's laws in their set-theoretic, logic circuit guises, and truth table guises.

These laws are named after Augustus De Morgan (1806–1871) as is the building in which resides the London Mathematical Society, whose first president he was.

Web link: www.mathcs.org/analysis/reals/logic/notation.html

Further reading: *Boolean Algebra and Its Applications* by J. Eldon Whitesitt, Dover Publications Inc., 1995.

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

$$(P \implies Q) \implies (\neg Q \implies \neg P) \quad .$$

YOUR PROOF:

MY PROOF: Assume

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

Assume

$$\neg Q \quad ;$$

that is,

$$(\mathrm{ii})\ \ Q \implies \mathbf{false} \quad .$$

From (i) and (ii), by Theorem 11 (on page 54), we have that

$$P \implies \mathbf{false} \quad ;$$

that is,

$$\neg P$$

as required.

Theorem 38 *The real number $\sqrt{2}$ is irrational.*

YOUR PROOF:

MY PROOF: To prove:

$$\neg(\sqrt{2}\ \text{is rational})$$

we prove the equivalent statement:

$$(\sqrt{2}\ \text{is rational}) \implies \mathbf{false}$$

by showing that the assumption

$$(i) \quad \sqrt{2}\ \text{is rational}$$

leads to contradiction.

Assume (i); that is, that there exist integers m and n such that $\sqrt{2} = m/n$. Equivalently, by simplification (see also Lemma 43 on page 149 below), assume that there exist integers p and q *both of which are not even* such that $\sqrt{2} = p/q$. Under this assumption, let p_0 and q_0 be such integers; that is, integers such that

$$(ii) \quad p_0 \text{ and } q_0 \text{ are not both even}$$

and

$$(iii) \quad \sqrt{2} = p_0/q_0 \quad .$$

From (iii), one calculates that ${p_0}^2 = 2 \cdot {q_0}^2$ and, by Proposition 42 (on page 147), concludes that p_0 is even; that is, of the form $2 \cdot k$ for an integer k. With this, and again from (iii), one deduces that ${q_0}^2 = 2 \cdot k^2$ and hence, again by Proposition 42 (on page 147), that also q_0 is even; thereby contradicting assumption (ii). Hence, $\sqrt{2}$ is not rational.

Proof by contradiction

Amongst the equivalences for negation, we have postulated the somewhat controversial:

$$\neg\neg P \iff P$$

which is *classically* accepted.

In this light,

to prove P

one may equivalently

prove $\neg P \implies \mathbf{false}$;

that is,

assuming $\neg P$ leads to contradiction .

This technique is known as *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 39 *For all statements* P *and* Q,

$$(\neg Q \implies \neg P) \implies (P \implies Q) \quad .$$

YOUR PROOF:

MY PROOF: Assume

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

Assume

$$(\mathrm{ii})\ P \quad .$$

We need show Q.

Assume, by way of contradiction, that

$$(\mathrm{iii})\ \neg Q$$

holds.

From (i) and (iii), by Theorem 11 (on page 54), we have

$$(\mathrm{i}\nu) \quad \neg P$$

and now, from (ii) and $(\mathrm{i}\nu)$, we obtain a contradiction. Thus, $\neg Q$ cannot be the case; hence

$$Q$$

as required.

Proof by contrapositive

Corollary 40 *For all statements P and Q,*

$$(P \implies Q) \iff (\neg Q \implies \neg P) \quad .$$

Btw Using the above equivalence to prove an implication is known as *proof by contrapositive*.

Corollary 41 *For every positive irrational number x, the real number $\sqrt{x}$ is irrational.*

Proposition 42 *Suppose that* n *is an integer. Then,* n *is even iff* n^2 *is even.*

YOUR PROOF:

MY PROOF:

$(\Longrightarrow)$ This implication is a corollary of the fact that the product of two integers is even whenever one of them is.

$(\Longleftarrow)$ We prove the contrapositive; that is, that n odd implies n^2 odd. This is a corollary of Proposition 8.

Lemma 43 *A positive real number x is rational iff*

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

YOUR PROOF:

MY PROOF:

$(\Longleftarrow)$ Holds trivially.

$(\Longrightarrow)$ Assume that

$$(i) \quad \exists \text{ positive integers } a, b : \; x = a/b \; .$$

We show $(\dagger)$ by contradiction. So, suppose $(\dagger)$ is false; that is[a], assume that

$$(ii) \quad \forall \text{ positive integers } m, n :$$
$$x = m/n \implies \exists \text{ prime } p : \; p \mid m \wedge p \mid n \; .$$

From (i), let a_0 and b_0 be positive integers such that

[a] Here we use three of the logical equivalences of page 133 (btw, which ones?) and the logical equivalence $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

$$(iii) \quad x = a_0/b_0 \quad .$$

It follows from (ii) and (iii) that there exists a prime p_0 that divides both a_0 and b_0. That is, $a_0 = p_0 \cdot a_1$ and $b_0 = p_0 \cdot b_1$ for positive integers a_1 and b_1. Since

$$(iv) \quad x = a_1/b_1 \quad ,$$

it follows from (ii) and (iv) that there exists a prime p_1 that divides both a_1 and b_1. Hence, $a_0 = p_0 \cdot p_1 \cdot a_2$ and $b_0 = p_0 \cdot p_1 \cdot b_2$ for positive integers a_2 and b_2. Iterating this argument l number of times, we have that $a_0 = p_0 \cdot \ldots \cdot p_l \cdot a_{l+1}$ and $b_0 = p_0 \cdot \ldots \cdot p_l \cdot b_{l+1}$ for primes $p_0, \ldots, p_l$ and positive integers a_{l+1} and b_{l+1}. In particular, for $l = \lfloor \log a_0 \rfloor$ we have

$$a_0 \;=\; p_0 \cdot \ldots \cdot p_l \cdot a_{l+1} \;\geq\; 2^{l+1} \;>\; a_0 \quad .$$

This is a contradiction. Therefore, $(\dagger)$ must be true.

Problem Like many proofs by contradiction, the previous proof is unsatisfactory in that it does not gives us as much information as we would like [a]. In this particular case, for instance, given a pair of numerator and denominator representing a rational number we would like a method, construction, or algorithm providing us with its representation in lowest terms (or reduced form). We will see later on (see page 227) that there is in fact an efficient algorithm for doing so, but for that a bit of mathematical theory needs to be developed.

[a] In the logical jargon this is referred to as not being *constructive*.

Numbers

Topics

Natural numbers. The laws of addition and multiplication. Integers and rational numbers: additive and multiplicative inverses. The division theorem and algorithm: quotients and remainders. Modular arithmetic. Euclid's Algorithm for computing the gcd (greatest common divisor)[a]. Euclid's Theorem. The Extended Euclid's Algorithm for computing the gcd as a linear combination. Multiplicative inverses in modular arithmetic. Diffie-Hellman cryptographic method. Mathematical induction: principles of induction and strong induction. Binomial Theorem and Pascal's

[a]aka hcf (highest common factor).

Triangle. Fermat's Little Theorem. Fundamental Theorem of Arithmetic. Infinity of primes.

Complementary reading:

On numbers

- ♦ Chapters 27 to 29 of *How to Think Like a Mathematician* by K. Houston.
- ★ Chapter 8 of *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.
- ★ Chapters I and VIII of *The Higher Arithmetic* by H. Davenport.

On induction

- Chapters 24 and 25 of *How to Think Like a Mathematician* by K. Houston.
- Chapter 4 of *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.
- Chapter 6 of *How to Prove it* by D. J. Velleman.

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
```

Remark This viewpoint will be looked at later in the course.

The basic operations of this number system are:

- Addition

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

- Multiplication

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

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*.

Commutative monoid laws

- Neutral element laws

$$\overbrace{}^{0}\overbrace{*\cdots\cdots*}^{n} = \overbrace{*\cdots\cdots*}^{n} = \overbrace{*\cdots\cdots*}^{n}\overbrace{}^{0}$$

- Associativity law

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

- Commutativity law

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

Monoids

Definition 44 *A monoid is an algebraic structure with*

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

satisfying

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

A monoid is commutative if:

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

is satisfied.

Btw: Most probably, though without knowing it, you have already encountered several monoids elsewhere.

For instance:

1. The booleans with **false** and disjunction.
2. The booleans with **true** and conjunction.
3. Lists with nil and concatenation.

While the first two above are commutative this is not generally the case for the latter. However, `unit 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

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

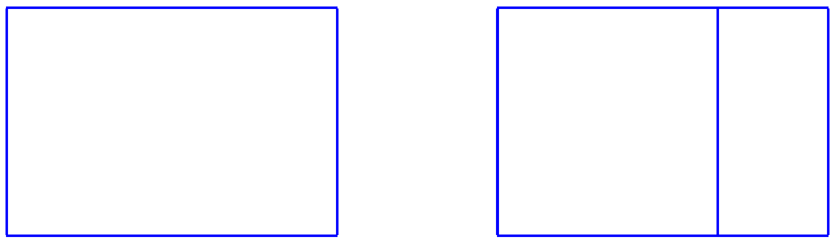
- Commutativity law

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

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

- Distributive laws

$$\begin{aligned} l \cdot 0 &= 0 \\ l \cdot (m + n) &= l \cdot m + l \cdot n \end{aligned}$$



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

Semirings

Definition 45 *A semiring (or rig) is an algebraic structure with*

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

satifying the distributivity 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 $k \cdot m = k \cdot n \implies m = n \quad .$

Definition 46 *A binary operation $\bullet$ allows* cancellation *by an element* c

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

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

Inverses

Definition 47 *For a monoid with a neutral element e and a binary operation $\bullet$, and element x is said to admit an*

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

Proposition 48 *For a monoid $(e, \bullet)$ if an element admits an inverse then its left and right inverses are equal.*

YOUR PROOF:

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

$$r = e \bullet r = (\ell \bullet x) \bullet r = \ell \bullet (x \bullet r) = \ell \bullet e = \ell \ .$$

Proposition 49 *For a monoid $(e, \bullet)$, if an element has an inverse then it is cancellable.*

YOUR PROOF:

MY PROOF: Let c be an element with inverse $\overline{c}$. We need prove:

$$(i)\ \forall x, y.\, c \bullet x = c \bullet y \implies x = y$$

and

$$(ii)\ \forall x, y.\, x \bullet c = y \bullet c \implies x = y$$

For (i), assume x and y arbitrary such that $c \bullet x = c \bullet y$. Then, $x = e \bullet x = (\overline{c} \bullet c) \bullet x = \overline{c} \bullet (c \bullet x) = \overline{c} \bullet (c \bullet y) = (\overline{c} \bullet c) \bullet y = e \bullet y = y$.

One shows (ii) analogously.

Groups

Definition 50 *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 51

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 $x \cdot y = 1$.*

Remark In the presence of inverses, we have cancellation; though the converse is not necessarily the case. For instance, in the system of natural numbers, only 0 has an additive inverse (namely itself), while only 1 has a multiplicative inverse (namely itself).

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

Definition 52 *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

Definition 53 *A* field *is a commutative ring in which every element besides* 0 *has a reciprocal (that is, and inverse with respect to* $\otimes$*).*

The division theorem and algorithm

Theorem 54 (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 55 *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* $\mathrm{rem}(m, n)$*.*

Btw Definitions determined by existence and uniqueness properties such as the above are very common in mathematics.

YOUR PROOF OF Theorem 54:

MY PROOF OF Theorem 54: Uniqueness follows from Lemma 56 and existence from Theorem 57.

Lemma 56 *Let* q *be an integer,* n *be a positive natural number, and* r *be a natural number. If* $q \cdot n + r = 0$ *and* $0 \leq r < n$ *then* $q = 0$ *and, consequently,* $r = 0$*.*

PROOF: Let q be an integer, n be a positive natural number, and r be a natural number. Assume that $q \cdot n + r = 0$ and that $0 \leq r < n$.

As $q \cdot n = -r$ we have that (i) $q \cdot n \leq 0$ and that (ii) $q \cdot n > -n$. Since $n > 0$, it follows from (i) that $q \leq 0$ and from (ii) that $q > -1$. Hence, $q = 0$.

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 57 *For every natural number m and positive natural number n, the evaluation of $\mathtt{divalg}(m, n)$ terminates, outputing a pair of natural numbers (q_0, r_0) such that $r_0 < n$ and $m = q_0 \cdot n + r_0$.*

YOUR PROOF:

MY PROOF SKETCH: Let m and n be natural numbers with n positive.

The evaluation of $\texttt{divalg}(m,n)$ diverges iff so does the evaluation of $\texttt{diviter}(0,m)$ within this call; and this is in turn the case iff $m - i \cdot n \geq n$ for all natural numbers i. Since this latter statement is absurd, the evaluation of $\texttt{divalg}(m,n)$ terminates. In fact, it does so with worst time complexity $O(m)$.

For all calls of $\texttt{diviter}$ with (q,r) originating from the evaluation of $\texttt{divalg}(m,n)$ one has that

$$0 \leq q \ \wedge \ 0 \leq r \ \wedge \ m = q \cdot n + r$$

because

1. for the first call with $(0, m)$ one has

   $$0 \leq 0 \ \wedge\ 0 \leq m \ \wedge\ m = 0 \cdot n + m \ ,$$

   and

2. all subsequent calls with $(q+1, r-n)$ are done with

   $$0 \leq q \ \wedge\ n \leq r \ \wedge\ m = q \cdot n + r$$

   so that

   $$0 \leq q+1 \ \wedge\ 0 \leq r-n \ \wedge\ m = (q+1) \cdot n + (r-n)$$

   follows.

Finally, since in the last call the output pair (q_0, r_0) further satisfies that $r_0 < n$, we have that

$$0 \leq q_0 \ \wedge\ 0 \leq r_0 < n \ \wedge\ m = q_0 \cdot n + r_0$$

as required.

Proposition 58 *Let* m *be a positive integer. For all natural numbers* k *and* l,

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

YOUR PROOF:

MY PROOF: Let m be a positive integer, and let k, l be natural numbers.

$(\Longrightarrow)$ Assume $k \equiv l \pmod{m}$. Then,

$$\max\big(\, \mathrm{rem}(k, m)\,,\ \mathrm{rem}(l, m)\,\big) - \min\big(\, \mathrm{rem}(k, m)\,,\ \mathrm{rem}(l, m)\,\big)$$

is a non-negative multiple of m below it. Hence, it is necessarily 0 and we are done.

$(\Longleftarrow)$ Assume that $\mathrm{rem}(k, m) = \mathrm{rem}(l, m)$. Then,

$$k - l = \big(\mathrm{quo}(k, m) - \mathrm{quo}(l, m)\big) \cdot m$$

and we are done.

Corollary 59 *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*

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

YOUR PROOF:

MY PROOF: Let m be a positive integer.

(1) Holds because, for every natural number n, we have that $n - \mathrm{rem}(n, m) = \mathrm{quo}(n, m) \cdot m$.

(2) Let k be an integer. Noticing that $k + |k| \cdot m$ is a natural number congruent to k modulo m, define $[k]_m$ as

$$\mathrm{rem}\Big(\, k + |k| \cdot m \,,\; m \,\Big) \quad .$$

This establishes the existence property. As for the uniqueness property, we will prove the following statement:

> For all integers l such that $0 \leq l < m$ and $k \equiv l \pmod{m}$ it is necessarily the case that $l = [k]_m$.

To this end, let l be an integer such that $0 \leq l < m$ and $k \equiv l \pmod{m}$. Then,

$$\begin{aligned} l &= \mathrm{rem}(l, m) \\ &= \mathrm{rem}(k, m) && \text{, by Proposition 58 (on page 182)} \\ &= \mathrm{rem}\big([k]_m, m\big) && \text{, by Proposition 58 (on page 182)} \\ &= [k]_m \end{aligned}$$

Modular arithmetic

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

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

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

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

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

For k and l in $\mathbb{Z}_m$,

$$k +_m l \quad \text{and} \quad k \cdot_m l$$

are the unique modular integers in $\mathbb{Z}_m$ such that

$$k +_m l \equiv k + l \pmod{m}$$

$$k \cdot_m l \equiv k \cdot l \pmod{m}$$

Example 60 *The modular-arithmetic structure* $(\mathbb{Z}_2, 0, +_2, 1, \cdot_2)$ *is that of booleans with logical XOR as addition and logical AND as multiplication.*

Example 61 *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 62 *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 63 *For all natural numbers* $m > 1$, *the modular-arithmetic structure*

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

is a commutative ring.

Remark The most interesting case of the omitted proof consists in establishing the associativity laws of addition and multiplication.

NB Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses (see page 257) .

Proposition 64 *Let* m *be a positive integer. A modular integer* k *in* $\mathbb{Z}_m$ *has a reciprocal if, and only if, there exist integers* i *and* j *such that* $k \cdot i + m \cdot j = 1$*.*

YOUR PROOF:

MY PROOF: Let m be a positive integer and let k be a modular integer in $\mathbb{Z}_m$.

$(\Longrightarrow)$ Assume that there exists i in $\mathbb{Z}_m$ such that $k \cdot_m i \equiv 1 \pmod{m}$. As $k \cdot i \equiv k \cdot_m i \pmod{m}$ we have that $k \cdot i - 1 = m \cdot j$ for some integer j.

$(\Longleftarrow)$ Assume integers i and j such that $k \cdot i + m \cdot j = 1$. Then, k has reciprocal $[i]_m$ modulo m. Indeed,

$$k \cdot_m [i]_m = [k \cdot i]_m \equiv k \cdot i = 1 - m \cdot j \equiv 1 \pmod{m} \ .$$

Integer linear combinations

Definition 65 *An integer* r *is said to be a* linear combination *of a pair of integers* m *and* n *whenever there are integers* s *and* t *such that* $s \cdot m + t \cdot n = r$.

Proposition 66 *Let* m *be a positive integer. A modular integer* k *in* $\mathbb{Z}_m$ *has a reciprocal if, and only if,* 1 *is an integer linear combination of* m *and* k.

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.

Though only implicitly, we have already encountered many sets so far, e.g. the sets of natural numbers $\mathbb{N}$, integers $\mathbb{Z}$, positive integers, even integers, odd integers, primes, rationals $\mathbb{Q}$, reals $\mathbb{R}$, booleans, and finite initial segments of natural numbers $\mathbb{Z}_m$.

It is now due time to be explicit. The *theory of sets* plays important roles in mathematics, logic, and computer science, and we will be looking at some of its very basics later on in the course (see page 308). For the moment, we will just introduce some of its surrounding notation.

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. Thus, for instance, $\pi \in \mathbb{R}$ is a true statement, while $\sqrt{-1} \in \mathbb{R}$ is not. The negation of the set membership predicate is written by means of the symbol '$\notin$'; so that $\sqrt{-1} \notin \mathbb{R}$ is a true statement, while $\pi \notin \mathbb{R}$ is not.

Remark The notations

$$\forall x \in A.\, P(x) \qquad , \qquad \exists x \in A.\, P(x)$$

are shorthand for

$$\forall x.\, \big(x \in A \implies P(x)\big) \qquad , \qquad \exists x.\, x \in A \;\wedge\; P(x) \qquad .$$

Defining sets

The conventional way to write down a finite set (i.e. a set with a finite number of elements) is to list its elements in between curly brackets. For instance,

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

Defining huge finite sets (such as $\mathbb{Z}_{\text{googolplex}}$) and infinite sets (such as the set of primes) in the above style is impossible and requires a technique known as *set comprehension*[a] (or *set-builder notation*), which we will look at next.

---

[a] Btw, many programming languages provide a *list comprehension* construct modelled upon set comprehension.

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.

Here, given an already constructed set A and a statement $P(x)$ for the variable x ranging over the set A, we will be using either of the following set-comprehension notations

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

for defining the set consisting of all those elements a of the set A such that the statement $P(a)$ holds. In other words, the following statement is true

$$\forall a.\, \Big(a \in \{\, x \in A \mid P(x) \,\} \iff \big(a \in A \,\wedge\, P(a) \big) \Big) \qquad (\dagger)$$

by definition.

Example 67

1. $\mathbb{N} = \{ n \in \mathbb{Z} \mid n \geq 0 \}$

2. $\mathbb{N}^{+} = \{ n \in \mathbb{N} \mid n \geq 1 \}$

3. $\mathbb{Q} = \{ x \in \mathbb{R} \mid \exists\, p \in \mathbb{Z}.\, \exists\, q \in \mathbb{N}^{+}.\, x = p/q \}$

4. $\mathbb{Z}_{\mathrm{googolplex}} = \{ n \in \mathbb{N} \mid n < \mathrm{googolplex} \}$

Set equality

Two sets are equal precisely when they have the same elements

Examples:

- $\{ x \in \mathbb{N} \ : \ 2 \mid x \ \wedge \ x \text{ is prime} \} = \{ 2 \}$
- For a positive integer m,
$$\{ x \in \mathbb{Z} \ : \ m \mid x \} = \{ x \in \mathbb{Z} \ : \ x \equiv 0 \pmod{m} \}$$
- $\{ d \in \mathbb{N} \ : \ d \mid 0 \} = \mathbb{N}$

Equivalent predicates specify equal sets:

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

iff

$$\forall x.\ P(x) \iff Q(x)$$

Example: For a positive integer m,

$$\{ x \in \mathbb{Z}_m \mid x \text{ has a reciprocal in } \mathbb{Z}_m \}$$

$$=$$

$$\{ x \in \mathbb{Z}_m \mid 1 \text{ is an integer linear combination of } m \text{ and } x \}$$

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 68

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 69

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

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*?

Proposition 70 *For all natural numbers l, m, and n,*

1. $\mathrm{CD}(m, n) = \mathrm{CD}(n, m)$*, and*

2. $\mathrm{CD}(l \cdot n, n) = \mathrm{D}(n)$*.*

Corollary 71 *For a natural number ℓ,*

1. $\mathrm{CD}(\ell, \ell) = \mathrm{CD}(\ell, 0) = \mathrm{D}(\ell)$

2. $\mathrm{CD}(1, \ell) = \{ 1 \}$

Lemma 72 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $m \equiv m' \pmod{n}$*. Then,*

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

YOUR PROOF:

MY PROOF: Let m and m' be natural numbers, and let n be a positive integer such that

$$(\mathrm{i})\ m \equiv m' \pmod{n} \ .$$

We will prove that for all positive integers d,

$$d \mid m \ \wedge \ d \mid n \iff d \mid m' \ \wedge \ d \mid n \ .$$

$(\Longrightarrow)$ Let d be a positive integer that divides both m and n. Then,

$$d \mid (k \cdot n + m) \text{ for all integers } k$$

and since, by (i), $m' = k_0 \cdot n + m$ for some integer k_0, it follows that $d \mid m'$. As $d \mid n$ by assumption, we have that d divides both m' and n.

$(\Longleftarrow)$ Analogous to the previous implication.

Corollary 73

1. *For all natural numbers* m *and positive integers* n,

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

2. *For all natural numbers* m *and* n,

$$\mathrm{CD}(m,n) = \mathrm{CD}\big(q-p,p\,\big)$$

where $p = \min(m,n)$ *and* $q = \max(m,n)$.

YOUR PROOF:

MY PROOF: The claim follows from the Key Lemma 72 (on page 209). Item (1) by Corollary 59 (on page 184), and item (2) because $l \equiv l - k \pmod{k}$ for all integers k and l.

Putting previous knowledge together we have:

Lemma 74 *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 (*with* divalg)

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

gcd (*with* div)

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

Example 75 ($\mathrm{gcd}(13,34) = 1$)

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

NB If $\mathtt{gcd}$ terminates on input (m,n) with output $\mathtt{gcd}(m,n)$ then $\mathrm{CD}(m,n) = \mathrm{D}\big(\mathtt{gcd}(m,n)\big)$.

Proposition 76 *For all natural numbers* m, n *and* a, b, *if* $\mathrm{CD}(m, n) = \mathrm{D}(a)$ *and* $\mathrm{CD}(m, n) = \mathrm{D}(b)$ *then* $a = b$.

Proposition 77 *For all natural numbers* m, n *and* k, *the following statements are equivalent:*

1. $\mathrm{CD}(m, n) = \mathrm{D}(k)$.
2. - $k \mid m \ \wedge \ k \mid n$, *and*
   - *for all natural numbers* d, $d \mid m \ \wedge \ d \mid n \implies d \mid k$.

Definition 78 *For natural numbers* m, n *the unique natural number* k *such that*

- $k \mid m \ \wedge \ k \mid n$, *and*
- *for all natural numbers* d, $d \mid m \ \wedge \ d \mid n \implies d \mid k$.

is called the greatest common divisor *of* m *and* n, *and denoted* $\gcd(m, n)$.

Theorem 79 *Euclid's Algorithm* $\mathtt{gcd}$ *terminates on all pairs of positive integers and, for such* m *and* n*, the positive integer* $\mathtt{gcd}(m, n)$ *is the greatest common divisor of* m *and* n *in the sense that the following two properties hold:*

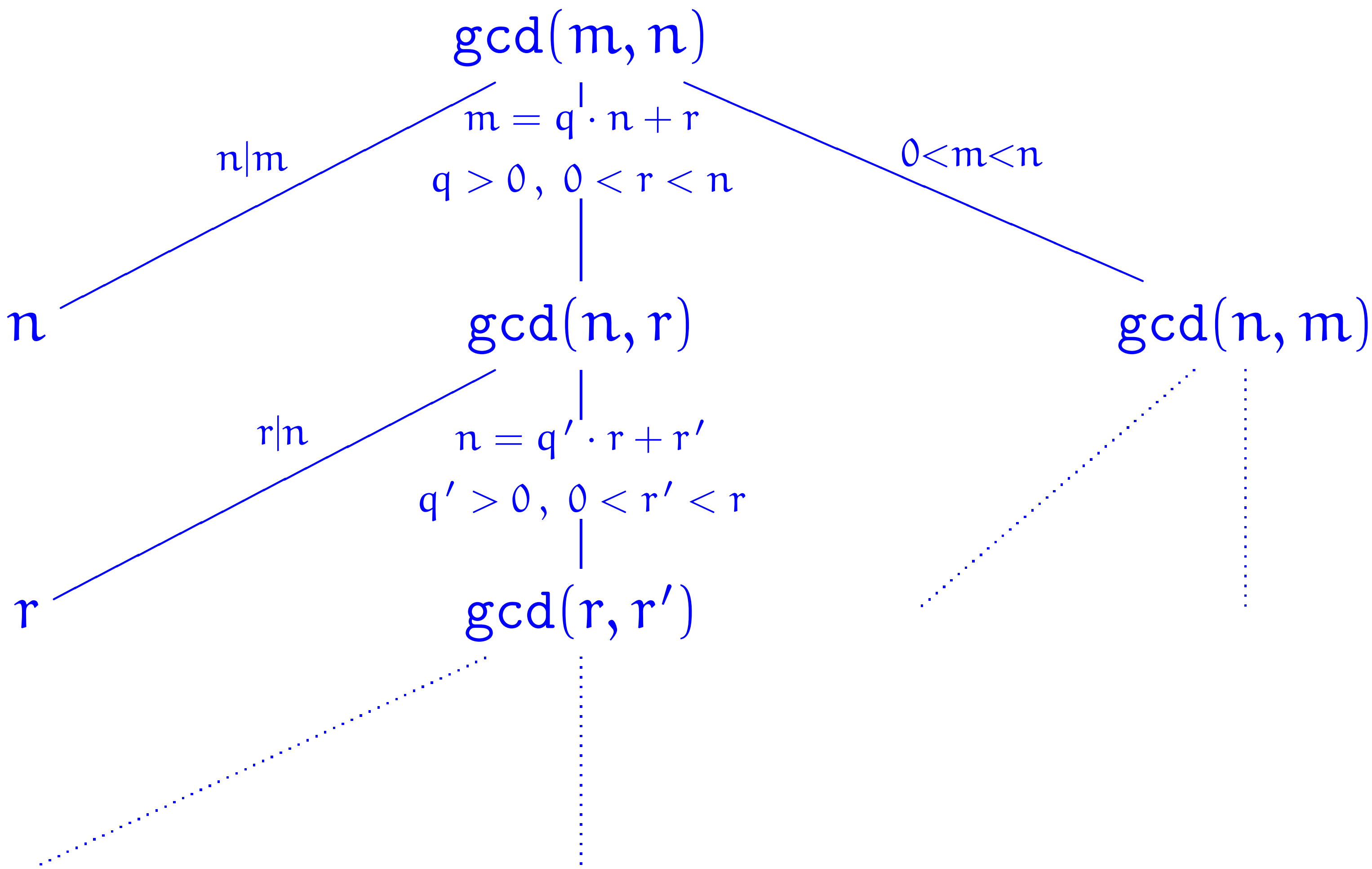
(i) *both* $\mathtt{gcd}(m, n) \mid m$ *and* $\mathtt{gcd}(m, n) \mid n$*, and*

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

YOUR PROOF:

MY PROOF: To establish the termination of $\mathtt{gcd}$ on a pair of positive integers (m, n) we consider and analyse the computations arising from the call $\mathtt{gcd}(m, n)$. For intuition, these can be visualised as on page 221.

As a start, note that, if $m < n$, the computation of $\mathtt{gcd}(m, n)$ reduces in one step to that of $\mathtt{gcd}(n, m)$; so that it will be enough to establish the termination of $\mathtt{gcd}$ on pairs where the first component is greater than or equal to the second component.


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′)

Consider then $\mathrm{gcd}(m, n)$ where $m \geq n$. We have that $\mathrm{gcd}(m, n)$ either terminates in one step, whenever $n \mid m$; or that, whenever $m = q \cdot n + r$ with $q > 0$ and $0 < r < n$, it reduces in one step to a computation of $\mathrm{gcd}(n, r)$.

In this latter case, the passage of computing $\mathrm{gcd}(m, n)$ by means of computing $\mathrm{gcd}(n, r)$ maintains the invariant of having the first component greater than or equal to the second one, but also strictly decreases the second component of the two pairs. As this process cannot go on for ever while maintaining the second components of the recurring pairs positive, the recursive calls must eventually stop and the overall computation terminate (in a number of steps less than or equal the minimum input of the pair).

The previous analysis can be refined further to get a nice upper bound on the computation of gcds. For fun, we look into this next.

Note that, for $m \geq n$, a call of $\mathtt{gcd}$ on (m, n) terminates in at most 2 steps, or in 2 steps reduces to a computation of $\mathtt{gcd}(r, r')$ for a pair of positive integers (r, r') such that:

$$m = q \cdot n + r \text{ for } q > 0 \text{ and } 0 < r < n$$

and

$$n = q' \cdot r + r' \text{ for } q' > 0 \text{ and } 0 < r' < r \quad .$$

(Btw, for $n > m$, the same occurs but with an extra computation step.) As before, this process cannot go on for ever and the $\mathtt{gcd}$ algorithm necessarily terminates.

I claim that $r' < n/2$. Indeed, this is because:

$$2 \cdot r' < r + r' \leq q' \cdot r + r' = n \ .$$

Thus, after 2 steps in the computation of $\mathtt{gcd}$ on inputs (m, n) with $m \geq n$ the second (and smallest) component n of the pair being computed is reduced to more than $1/2$ its size. Since this pattern recurs until termination, the total number of steps in the computation of $\mathtt{gcd}$ on a pair (m, n) is bounded by

$$1 + 2 \cdot \log\big(\min(m, n)\big) \ .$$

Hence, the time complexity of the $\mathtt{gcd}$ is at most of logarithmic order.[a]

[a]Let me note for the record that a more precise complexity analysis involving *Fibonacci numbers* is also available.

As for the characterisation of $\mathrm{gcd}(m, n)$, for positive integers m and n, by means of the properties (i) and (ii) stated in the theorem, we note first that it follows from Lemma 74 (on page 213) that

$$\mathrm{CD}(m, n) = \mathrm{D}\big(\mathrm{gcd}(m, n)\big) \quad ;$$

that is, in other words,

for all positive integers d,

$$d \mid m \wedge d \mid n \iff d \mid \mathrm{gcd}(m, n)$$

which is a single statement equivalent to the statements (i) and (ii) together.

NB Euclid's Algorithm (on page 213) and Theorem 79 (on page 219) provide two views of the gcd: an algorithmic one and a mathematical one. Both views are complementary, neither being more important than the other, and a proper understanding of gcds should involve both. As a case in point, we will see that some properties of gcds are better approached from the algorithmic side (e.g. linearity) while others from the mathematical side (e.g. commutativity and associativity).

This situation arises as a general pattern in interactions between computer science and mathematics.

Fractions in lowest terms

Here's our solution to the problem raised on page 152.

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

Some fundamental properties of gcds

Corollary 80 *Let m and n be positive integers.*

1. *For all integers k and l,*

$$\gcd(m, n) \mid (k \cdot m + l \cdot n) \quad .$$

2. *If there exist integers k and l, such that $k \cdot m + l \cdot n = 1$ then $\gcd(m, n) = 1$.*

YOUR PROOF:

MY PROOF:

(1) Follows from the fact that $\gcd(m, n) \mid m$ and $\gcd(m, n) \mid n$, for all positive intergers m and n, and from general elementary properties of divisibility.

(2) Because, by the previous item, one would have that the $\gcd$ divides 1.

Lemma 81 *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] $\gcd(l \cdot m, l \cdot n) = l \cdot \gcd(m, n)$.

YOUR PROOF:

[a] Aka (Distributivity).

MY PROOF: Let l, m, and n be positive integers.

(1) In a nutshell, the result follows because $\mathrm{CD}(m, n) = \mathrm{CD}(n, m)$.

Let me however give you a detailed argument to explain a basic, and very powerful, argument for proving properties of gcds (and in fact of any mathematical structure similarly defined by what in the mathematical jargon is known as a *universal property*).

Theorem 79 (on page 219) tells us that $\gcd(m, n)$ is the positive integer precisely characterised by the following *universal property*:

$$\forall \text{ positive integers } d.\ d \mid m \wedge d \mid n \iff d \mid \gcd(m, n) \quad . \qquad (\dagger)$$

Now, $\gcd(n, m) \mid m$ and $\gcd(n, m) \mid n$; hence by $(\dagger)$ above $\gcd(n, m) \mid \gcd(m, n)$. An analogous argument (with m and n interchanged everywhere) shows that $\gcd(m, n) \mid \gcd(n, m)$.

Since $\mathrm{gcd}(m,n)$ and $\mathrm{gcd}(n,m)$ are positive integers that divide each other, then they must be equal.

(2) In a nutshell, the result follows because both $\mathrm{gcd}\big(l,\mathrm{gcd}(m,n)\big)$ and $\mathrm{gcd}(\mathrm{gcd}(l,m),n)$ are the greatest common divisor of the triple of numbers (l,m,n). But again I'll give a detailed proof by means of the universal property of gcds, from which we have that for all positive integers d,

$$\begin{aligned} & d \mid \mathrm{gcd}\big(l,\mathrm{gcd}(m,n)\big) \\ & \quad\iff\quad d \mid l \;\wedge\; d \mid \mathrm{gcd}(m,n) \\ & \quad\iff\quad d \mid l \;\wedge\; d \mid m \;\wedge\; d \mid n \\ & \quad\iff\quad d \mid \mathrm{gcd}(l,m) \;\wedge\; d \mid n \\ & \quad\iff\quad d \mid \mathrm{gcd}(\mathrm{gcd}(l,m),n) \end{aligned}$$

It follows that both $\gcd\big(l, \gcd(m, n)\big)$ and $\gcd(\gcd(l, m), n)$ are positive integers dividing each other, and hence equal.[a]

(3) One way to prove the result is to note that the following Remainder-Linearity Property of the Division Algorithm:

$$\text{for all positive integers } k, m, n,$$
$$\mathtt{divalg}(k \cdot m, k \cdot n) = \big(\mathrm{quo}(m, n), k \cdot \mathrm{rem}(m, n)\big)$$

transfers to Euclid's $\mathtt{gcd}$ Algorithm.

This is because

- every computation step

  $\mathtt{gcd}(m, n) = n$,

  which happens when $\mathrm{rem}(m, n) = 0$

[a] Btw, though I have not, one may try to give a proof using Euclid's Algorithm. If you try and succeed, please let me know.

corresponds to a computation step

$\mathrm{gcd}(l \cdot m, l \cdot n) = l \cdot n$,

which happens when $l \cdot \mathrm{rem}(m, n) = \mathrm{rem}(l \cdot m, l \cdot n) = 0$

i.e. when $\mathrm{rem}(m, n) = 0$

while

- every computation step

  $\mathrm{gcd}(m, n) = \mathrm{gcd}\left(n, \mathrm{rem}(m, n)\right)$,

  which happens when $\mathrm{rem}(m, n) \neq 0$

  corresponds to a computation step

$$\begin{aligned} \mathrm{gcd}(l \cdot m, l \cdot n) &= \mathrm{gcd}(l \cdot n, \mathrm{rem}(l \cdot m, l \cdot n)) \\ &= \mathrm{gcd}\big(l \cdot n, l \cdot \mathrm{rem}(m, n)\big) \end{aligned},$$

which happens when $l \cdot \mathrm{rem}(m, n) = \mathrm{rem}(l \cdot m, l \cdot n) \neq 0$,

i.e. when $\mathrm{rem}(m, n) \neq 0$

Thus, the computation of $\texttt{gcd}(m, n)$ leads to a sequence of calls to $\texttt{gcd}$ with

inputs $(m, n)\,,\,\big(n, \mathrm{rem}(m, n)\big)\,,\ldots\,,(r, r')\,,\ldots$
and output $\mathrm{gcd}(m, n)$

if, and only if, the computation of $\texttt{gcd}(l \cdot m, l \cdot n)$ leads to a sequence of calls to $\texttt{gcd}$ with

inputs $(l \cdot m, l \cdot n)\,,\,\big(l \cdot n, l \cdot \mathrm{rem}(m, n)\big)\,,\ldots\,,(l \cdot r, l \cdot r')\,,\ldots$
and output $l \cdot \mathrm{gcd}(m, n)$.

Finally, and for completeness, let me also give a non-algorithmic proof of the result. We show the following in turn:

(i) $l \cdot \mathrm{gcd}(m, n) \;\mid\; \mathrm{gcd}(l \cdot m, l \cdot n)$.

(ii) $\mathrm{gcd}(l \cdot m, l \cdot n) \;\mid\; l \cdot \mathrm{gcd}(m, n)$.

For (i), since $\gcd(m, n) \mid m \;\;\wedge\;\; \gcd(m, n) \mid n$ we have that $l \cdot \gcd(m, n) \mid l \cdot m \;\;\wedge\;\; l \cdot \gcd(m, n) \mid l \cdot n$ and hence that $l \cdot \gcd(m, n) \;\mid\; \gcd(l \cdot m, l \cdot n)$.

As for (ii): we note first that since $l \mid l \cdot m$ and $l \mid l \cdot n$ we have that $l \mid \gcd(l \cdot m, l \cdot n)$ and so that there exists a positive integer, say k_0, such that $\gcd(l \cdot m, l \cdot n) = l \cdot k_0$. But then, since $l \cdot k_0 = \gcd(l \cdot m, l \cdot n) \mid l \cdot m \;\;\wedge\;\; l \cdot k_0 = \gcd(l \cdot m, l \cdot n) \mid l \cdot n$ we have that $k_0 \mid m \;\;\wedge\;\; k_0 \mid n$, and so that $k_0 \mid \gcd(m, n)$. Finally, then, $\gcd(l \cdot m, l \cdot n) = l \cdot k_0 \mid l \cdot \gcd(m, n)$.

Coprimality

Definition 82 *Two natural numbers are said to be* coprime *whenever their greatest common divisor is* 1*.*

Euclid's Theorem

Theorem 83 *For positive integers* k*,* m*, and* n*, if* $k \mid (m \cdot n)$ *and* $\gcd(k, m) = 1$ *then* $k \mid n$*.*

YOUR PROOF:

MY PROOF: Let k, m, and n be positive integers, and assume that

$$(i)\ \ k \mid (m \cdot n) \quad \text{and} \quad (ii)\ \ \gcd(k, m) = 1 \ .$$

Using (i), let l be an integer such that

$$(iii)\ \ k \cdot l = m \cdot n \ .$$

In addition, using (ii) and the linearity of $\gcd$ (Lemma 81.3 on page 230), we have that

$$\begin{aligned} n &= \gcd(k, m) \cdot n && \text{, by } (ii) \\ &= \gcd(k \cdot n, m \cdot n) && \text{, by linearity} \\ &= \gcd(k \cdot n, k \cdot l) && \text{, by } (iii) \\ &= k \cdot \gcd(n, l) && \text{, by linearity} \end{aligned}$$

and we are done.

Corollary 84 (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 (on page 128) follows as a corollary of the first part and Euclid's Theorem.

YOUR PROOF OF Theorem 36.2 (on page 128):

MY PROOF OF Theorem 36.2 (on page 128): Let p be a prime and i a natural number that is not a multiple of p. By the first part of Fermat's Little Theorem, we know that $p \mid i \cdot (i^{p-1} - 1)$. It thus follows by Euclid's Theorem (Corollary 84 on the previous page) that $p \mid (i^{p-1} - 1)$.

Corollary 85 *For all primes* p *and integers* m *such that* $0 < m < p$*,*

$$p \mid \binom{p}{m} \quad \textit{and} \quad (p-m) \mid \binom{p-1}{m} \ .$$

YOUR PROOF:

MY PROOF: Let p be a prime and m be an integer such that $0 < m < p$. As

$$\gcd(p, p-m) = 1 \quad \text{and} \quad p \cdot \binom{p-1}{m} = (p-m) \cdot \binom{p}{m}$$

the result follows from Theorem 83 (on page 237).

Fields of modular arithmetic

Corollary 86 *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.*

We can however say a bit more, because an extension of Euclid's `gcd` Algorithm gives both a test for checking the existence of and an efficient method for finding multiplicative inverses in modular arithmetic.

Extended Euclid's Algorithm

Example 87 $\left[\mathtt{egcd}(34,13) = \big((5,-13),1\big)\right]$

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

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

Integer linear combinations

Definition 65[a] 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
>
> $$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r \ ;$$
>
> that is
>
> $$s \cdot m + t \cdot n = r \ .$$

[a]See page 196.

Remark Note that the ways in which an integer can be expressed as a linear combination is infinite; as, for all integers m, n and r, s, t, we have that

$$\begin{bmatrix} s & t \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r$$

iff

for all integers k, $\begin{bmatrix} (s+k\cdot n) & (t-k\cdot m) \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = r$.

Theorem 88 *For all positive integers* m *and* n*,*

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

$$\left[\begin{array}{cc} \mathrm{lc}_1(m,n) & \mathrm{lc}_2(m,n) \end{array}\right] \cdot \left[\begin{array}{c} m \\ n \end{array}\right] = \mathrm{gcd}(m,n) \quad ,$$

   can be efficiently computed.

The proof of Theorem 88, which is left as an exercise for the interested reader, is by means of the Extended Euclid's Algorithm `egcd` on page 251 relying on the following elementary properties of linear combinations.

Proposition 89 *For all integers m and n,*

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

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

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

   implies

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

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

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

We extend Euclid's Algorithm $\mathrm{gcd}(m, n)$ from computing on pairs of positive integers to computing on pairs of triples $((s, t), r)$ with s, t integers and r a positive integer satisfying the invariant that s, t are coefficientes expressing r as an integer linear combination of m and n.

egcd (*with* divalg)

```
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
```

egcd (*with* div)

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val q = r1 div r2 ; val 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
```

Example 90 ($\mathtt{egcd}(13, 34) = ((-13, 5), 1)$)

$$
\begin{aligned}
\mathtt{egcd}(13, 34) &= \mathtt{egcditer}\big(\, ((1, 0), 13)\ ,\ ((0, 1), 34)\ \big) \\
&= \mathtt{egcditer}\big(\, ((0, 1), 34)\ ,\ ((1, 0), 13)\ \big) \\
&= \mathtt{egcditer}\big(\, ((1, 0), 13)\ ,\ ((-2, 1), 8)\ \big) \\
&= \mathtt{egcditer}\big(\, ((-2, 1), 8)\ ,\ ((3, -1), 5)\ \big) \\
&= \mathtt{egcditer}\big(\, ((3, -1), 5)\ ,\ ((-5, 2), 3)\ \big) \\
&= \mathtt{egcditer}\big(\, ((-5, 2), 3)\ ,\ ((8, -3), 2)\ \big) \\
&= \mathtt{egcditer}\big(\, ((8, -3), 2)\ ,\ ((-13, 5), 1)\ \big) \\
&= \big(\, (-13, 5)\ ,\ 1\ \big)
\end{aligned}
$$

```
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 ) ) )
```

Proposition 91 *For all distinct positive integers* m *and* n*,*

$$\mathrm{lc}_1(m, n) = \mathrm{lc}_2(n, m) \quad .$$

Another characterisation of gcds

Theorem 92 *For all positive integers* m *and* n, $\gcd(m, n)$ *is the least positive linear combination of* m *and* n.

YOUR PROOF:

MY PROOF: Let m and n be arbitrary positive integers. By Theorem 88.1 (on page 248), $\gcd(m, n)$ is a linear combination of m and n. Furthermore, since it is positive, by Corollary 80.1 (on page 228), it is the least such.

Multiplicative inverses in modular arithmetic

Corollary 93 *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* $\mathbb{Z}_m$ *.*

Remark For every pair of positive integers m and n, we have that $[n]_m$ has a multiplicative inverse in $\mathbb{Z}_m$ iff $\gcd(m,n) = 1$.

Diffie-Hellman cryptographic method

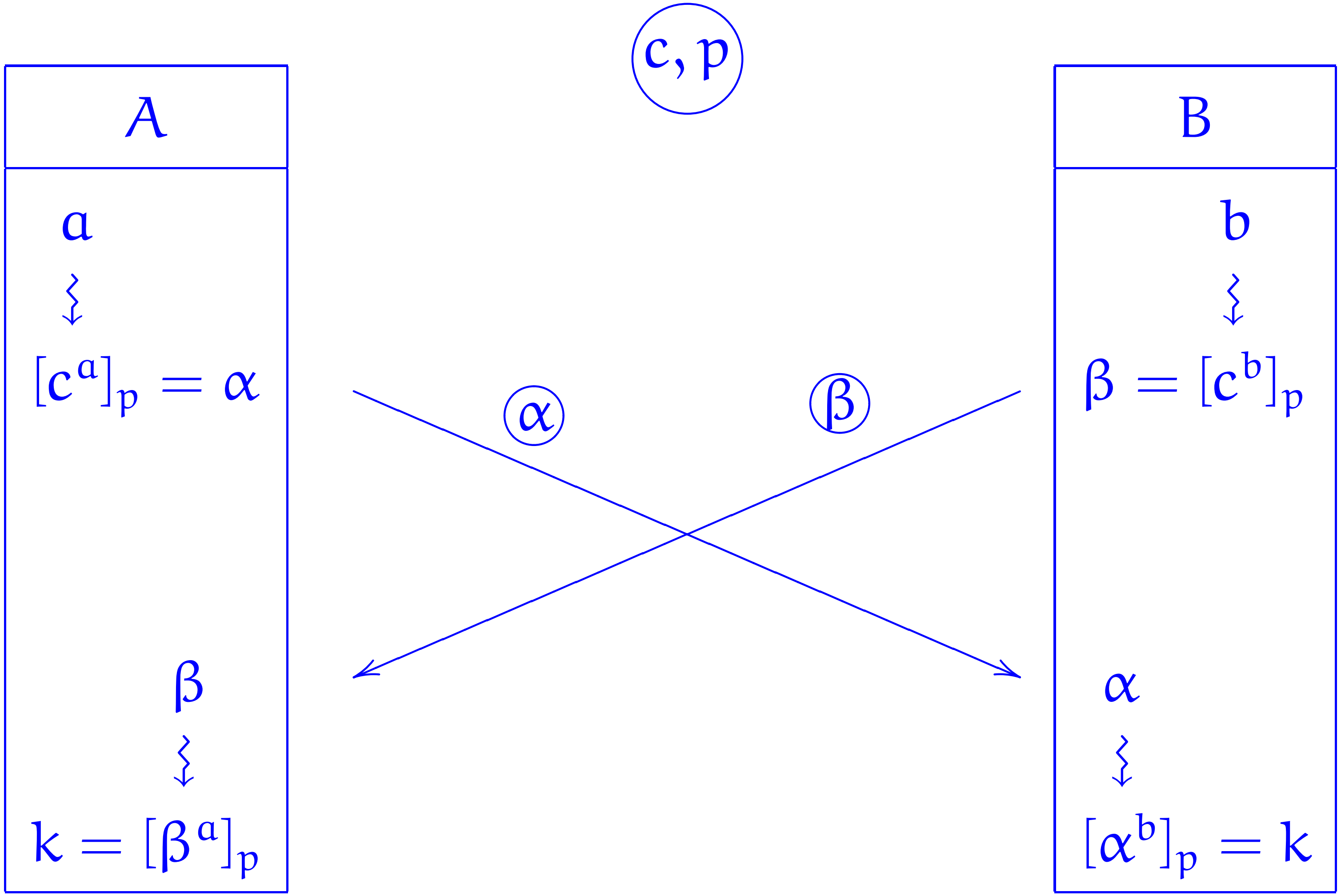
Shared secret key

c, p

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

Diffie-Hellman cryptographic method

Shared secret key



Key exchange

Mathematical modelling:

- Encrypt and decrypt by means of modular exponentiation:

$$[k^e]_p \qquad\qquad [\ell^d]_p$$

- Encrypting-decrypting have no effect:

By Fermat's Little Theorem,

$$k^{1+c\cdot(p-1)} \equiv k \pmod{p}$$

for every natural number c, integer k, and prime p.

- Consider d, e, p such that $e \cdot d = 1 + c \cdot (p-1)$; equivalently,

$$d \cdot e \equiv 1 \pmod{p} \quad .$$

Lemma 94 *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*,*

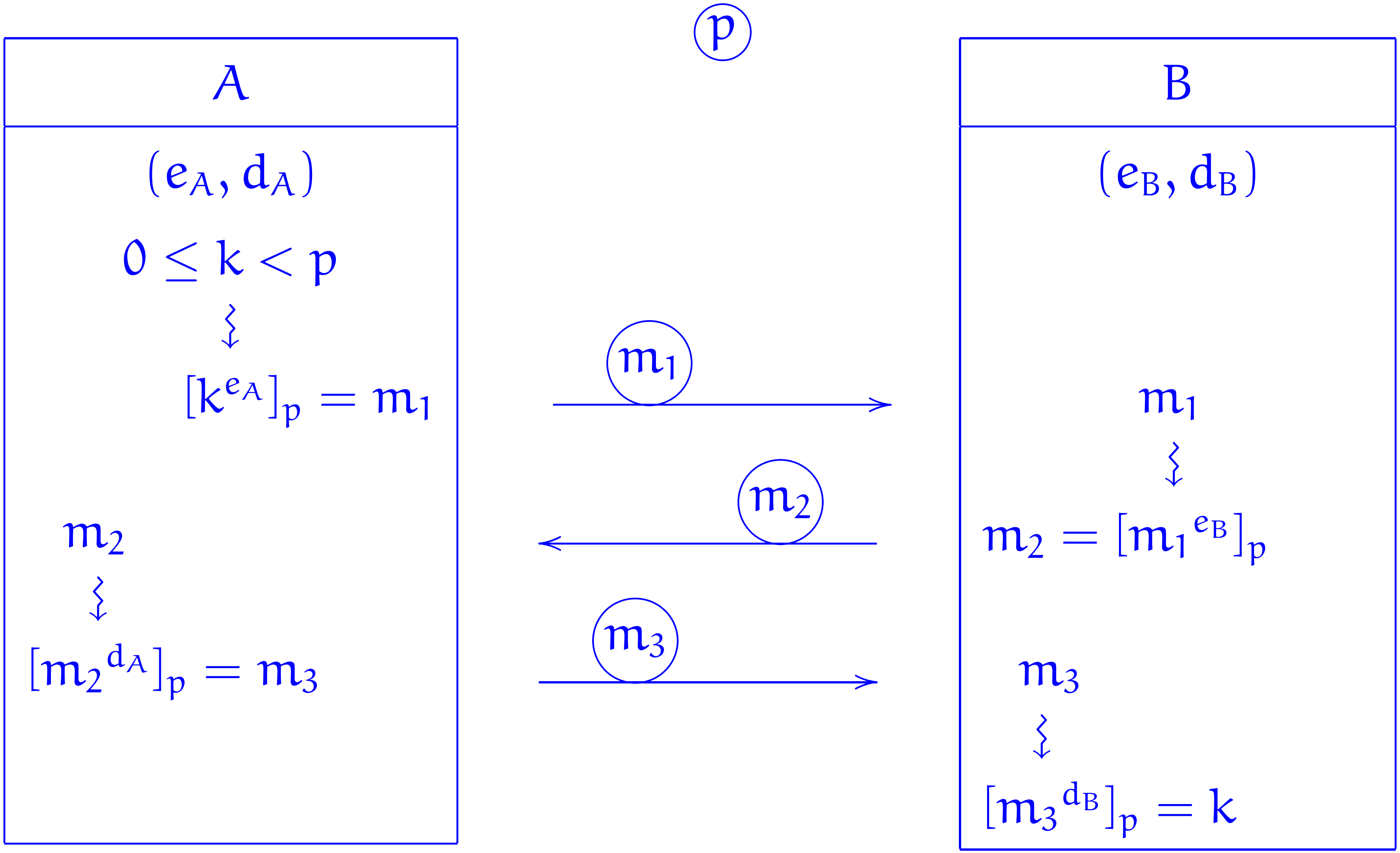
$$(k^e)^d \equiv k \pmod{p} \quad .$$

YOUR PROOF:

MY PROOF: Let p, e, and d be as stated in the lemma. Then, $e \cdot d = 1 + c \cdot (p - 1)$ for some natural number c and hence, by Fermat's Little Theorem (Theorem 36 on page 36),

$$k^{e \cdot d} = k \cdot k^{c \cdot (p-1)} \equiv k \pmod{p}$$

for all integers k not multiple of p. For integers k multiples of p the result is trivial.



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

Encryption/Decryption in RSA

Lemma 95 *Let* p, q *be distinct primes and* d, e *be positive integers such that* $e \cdot d \equiv 1 \pmod{(p-1)\cdot(q-1)}$*. Then, for all integers* k*,* $(k^e)^d \equiv k \pmod{p \cdot q}$*.*

Natural Numbers and mathematical induction

We have mentioned in passing on page 157 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.

NB When thinking about mathematical induction it is most convenient and advisable to have in mind their definition in ML:

```
datatype
  N = zero | succ of N
```

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.

NB By the Principle of Induction, thus, to establish the statement

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

it is enough to prove the following two statements:

1. $P(0)$, and
2. $\forall n \in \mathbb{N}.\ \big(P(n) \implies P(n+1) \big)$.

The induction proof strategy:

To prove a goal of the form

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

First prove

$P(0)$,

and then prove

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

Proof pattern:

In order to prove that

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

1. Write: Base case: and give a proof of $P(0)$.
2. Write: Inductive step: and give a proof that

   for all natural numbers n, $P(n)$ implies $P(n+1)$.
3. Write: By the Principle of Induction, we conclude that $P(m)$ holds for all natural numbers m.

A template for induction proofs:

1. State that the proof uses induction.
2. Define an appropriate property $P(m)$ for m ranging over the set of natural numbers. This is called the *induction hypothesis*.
3. Prove that $P(0)$ is true. This is called the *base case*.
4. Prove that $P(n) \implies P(n+1)$ for every natural number n. This is called the *inductive step*.
5. Invoke the principle of mathematical induction to conclude that $P(m)$ is true for all natural numbers m.

NB Always be sure to explicitly label the *induction hypothesis*, the *base case*, and the *inductive step*.

Binomial Theorem

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

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

YOUR PROOF:

MY PROOF SKETCH: We prove

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

for

$$P(m) \text{ the statement } (x+y)^m = \sum_{k=0}^{m} \binom{m}{k} \cdot x^{m-k} \cdot y^k$$

by the Principle of Induction.

Base case: $P(0)$ holds because

$$(x+y)^0 = 1 = \binom{0}{0} \cdot x^0 \cdot y^0 = \sum_{k=0}^{0} \binom{0}{k} \cdot x^{0-k} \cdot y^k \quad .$$

Inductive step: We need prove that, for all natural numbers n, $P(n)$ implies $P(n+1)$. To this end, let n be a natural number and assume $P(n)$; that is, assume that the following Induction Hypothesis

$$\text{(IH)} \qquad (x+y)^n \; = \; \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k$$

holds.

We will now proceed to show that

$$(x+y)^{n+1} \; = \; \sum_{k=0}^{n+1} \binom{n+1}{k} \cdot x^{(n+1)-k} \cdot y^k \qquad (\dagger)$$

follows.

We first try unfolding the left-hand side of $(\dagger)$ on the previous page:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)^n \cdot (x+y) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \right) \cdot (x+y) \\
&\qquad \text{, by the Induction Hypothesis } (\mathrm{IH}) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k+1} \cdot y^k \right) + \left(\sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^{k+1} \right)
\end{aligned}$$

Unfortunately, we seem to be kind of stuck here. So, we next try unfolding the right-hand side of $(\dagger)$:

$$\sum_{k=0}^{n+1} \binom{n+1}{k} \cdot x^{(n+1)-k} \cdot y^k$$

in the hope that this will help us bridge the gap. But, how can we make any progress? The clue seems to be in relating the coefficients $\binom{n}{k}$ and $\binom{n+1}{k}$ that appear in the above expressions.

At this point you may know about *Pascal's triangle* (see, for example, page 278), and get unstuck. Otherwise, you can reconstruct Pascal's rule by counting! Let's see how.

The natural number $\binom{n+1}{k}$ counts the number of ways in which k objects can be chosen amongst $n+1$ objects, say $o_1, \ldots, o_n, o_{n+1}$. One can count these by looking at two cases: (i) when the object o_{n+1} is not chosen, plus (ii) when the object o_{n+1} is chosen. Under case (i), we have $\binom{n}{k}$ possible ways to choose the k objects amongst $o_1, \ldots, o_n$; while, under case (ii) we have $\binom{n}{k-1}$ possible ways to choose the remaining $k-1$ objects amongst $o_1, \ldots, o_n$. Hence, we conjecture that

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \quad . \tag{‡}$$

We have a choice now: either we prove the conjecture and then check whether it is of any help for our problem at hand; or we assume it for the time being, push on, and, if it is what we need, prove it to leave no gaps in our reasoning. For reasons that will become apparent, I will here take the second route, and calculate:

$$\sum_{k=0}^{n+1} \binom{n+1}{k} \cdot x^{(n+1)-k} \cdot y^k$$

$$= \quad x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} \cdot x^{n-k+1} \cdot y^k + y^{n+1}$$

$$= \quad x^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) \cdot x^{n-k+1} \cdot y^k + y^{n+1}$$

, provided the conjecture $(\ddagger)$ is true!

$$= \quad x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} \cdot x^{n-k+1} \cdot y^k + \sum_{k=1}^{n} \binom{n}{k-1} \cdot x^{n-k+1} \cdot y^k + y^{n+1}$$

$$= \quad \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k+1} \cdot y^k + \sum_{j=0}^{n} \binom{n}{j} \cdot x^{n-j} \cdot y^{j+1}$$

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

$$= \quad \left(\sum_{i=0}^{n} \binom{n}{i} \cdot x^{n-i} \cdot y^i \right) \cdot (x + y)$$

$$= \quad (x + y)^n \cdot (x + y)$$, by the Induction Hypothesis (IH)

$$= \quad (x + y)^{n+1}$$

We have now established the inductive step, provided that we can prove the conjecture; and *you* should move onto this next:

Homework

1. Prove that, for all positive integers m and k such that $1 \leq k \leq m$,
$$\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1} \quad .$$
2. Turn the above scratch work into a proof.

Btw Note that our proof works in any commutative semiring.

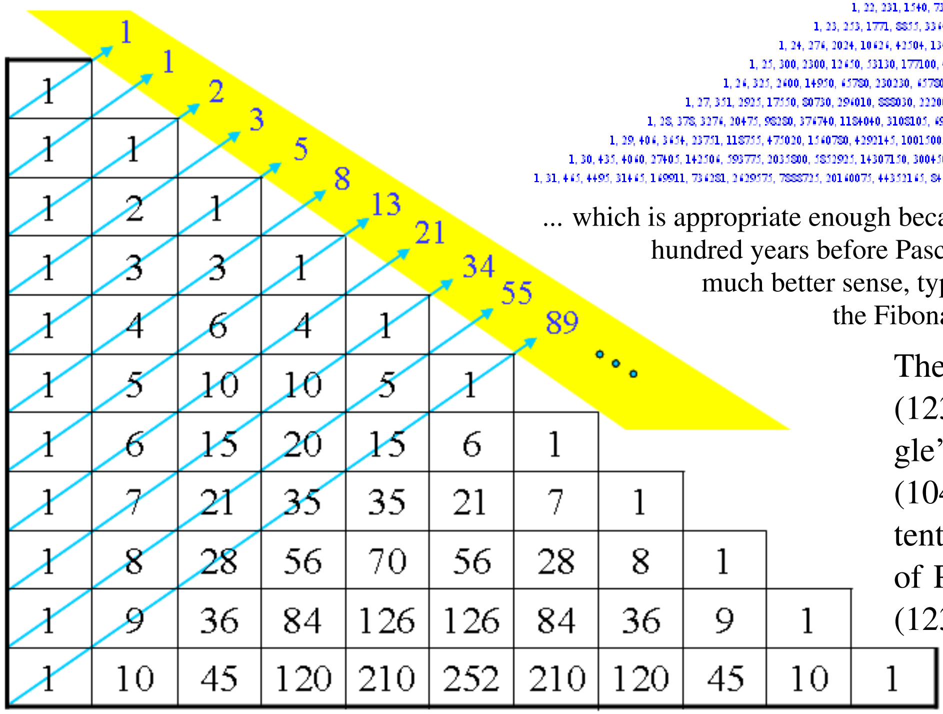
Pascal's Rule *For any positive integers n and k,*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

1
1, 1
1, 2, 1
1, 3, 3, 1
1, 4, 6, 4, 1
1, 5, 10, 10, 5, 1
1, 6, 15, 20, 15, 6, 1
1, 7, 21, 35, 35, 21, 7, 1
1, 8, 28, 56, 70, 56, 28, 8, 1
1, 9, 36, 84, 126, 126, 84, 36, 9, 1
1, 10, 45, 120, 210, 252, 210, 120, 45, 10, 1
1, 11, 55, 165, 330, 462, 462, 330, 165, 55, 11, 1
1, 12, 66, 220, 495, 792, 924, 792, 495, 220, 66, 12, 1
1, 13, 78, 286, 715, 1287, 1716, 1716, 1287, 715, 286, 78, 13, 1
1, 14, 91, 364, 1001, 2002, 3003, 3432, 3003, 2002, 1001, 364, 91, 14, 1
1, 15, 105, 455, 1365, 3003, 5005, 6435, 6435, 5005, 3003, 1365, 455, 105, 15, 1
1, 16, 120, 560, 1820, 4368, 8008, 11440, 12870, 11440, 8008, 4368, 1820, 560, 120, 16, 1
1, 17, 136, 680, 2380, 6188, 12376, 19448, 24310, 24310, 19448, 12376, 6188, 2380, 680, 136, 17, 1
1, 18, 153, 816, 3060, 8568, 18564, 31824, 43758, 48620, 43758, 31824, 18564, 8568, 3060, 816, 153, 18, 1
1, 19, 171, 969, 3876, 11628, 27132, 50388, 75582, 92378, 92378, 75582, 50388, 27132, 11628, 3876, 969, 171, 19, 1
1, 20, 190, 1140, 4845, 15504, 38760, 77520, 125970, 167960, 184756, 167960, 125970, 77520, 38760, 15504, 4845, 1140, 190, 20, 1
1, 21, 210, 1330, 5985, 20349, 54264, 116280, 203490, 293930, 352716, 352716, 293930, 203490, 116280, 54264, 20349, 5985, 1330, 210, 21, 1
1, 22, 231, 1540, 7315, 26334, 74613, 170544, 319770, 497420, 646646, 705432, 646646, 497420, 319770, 170544, 74613, 26334, 7315, 1540, 231, 22, 1
1, 23, 253, 1771, 8855, 33649, 100947, 245157, 490314, 817190, 1144066, 1352078, 1352078, 1144066, 817190, 490314, 245157, 100947, 33649, 8855, 1771, 253, 23, 1
1, 24, 276, 2024, 10626, 42504, 134596, 346104, 735471, 1307504, 1961256, 2496144, 2704156, 2496144, 1961256, 1307504, 735471, 346104, 134596, 42504, 10626, 2024, 276, 24, 1
1, 25, 300, 2300, 12650, 53130, 177100, 480700, 1081575, 2042975, 3268760, 4457400, 5200300, 5200300, 4457400, 3268760, 2042975, 1081575, 480700, 177100, 53130, 12650, 2300, 300, 25, 1
1, 26, 325, 2600, 14950, 65780, 230230, 657800, 1562275, 3124550, 5311735, 7726160, 9657700, 10400600, 9657700, 7726160, 5311735, 3124550, 1562275, 657800, 230230, 65780, 14950, 2600, 325, 26, 1
1, 27, 351, 2925, 17550, 80730, 296010, 888030, 2220075, 4686825, 8436285, 13037895, 17383860, 20058300, 20058300, 17383860, 13037895, 8436285, 4686825, 2220075, 888030, 296010, 80730, 17550, 2925, 351, 27, 1
1, 28, 378, 3276, 20475, 98280, 376740, 1184040, 3108105, 6906900, 13123110, 21474180, 30421755, 37442160, 40116600, 37442160, 30421755, 21474180, 13123110, 6906900, 3108105, 1184040, 376740, 98280, 20475, 3276, 378, 28, 1
1, 29, 406, 3654, 23751, 118755, 475020, 1560780, 4292145, 10015005, 20030010, 34597290, 51895935, 67863915, 77558760, 77558760, 67863915, 51895935, 34597290, 20030010, 10015005, 4292145, 1560780, 475020, 118755, 23751, 3654, 406, 29, 1
1, 30, 435, 4060, 27405, 142506, 593775, 2035800, 5852925, 14307150, 30045015, 54627300, 86493225, 119759850, 145422675, 155117520, 145422675, 119759850, 86493225, 54627300, 30045015, 14307150, 5852925, 2035800, 593775, 142506, 27405, 4060, 435, 30, 1
1, 31, 465, 4495, 31465, 169911, 736281, 2629575, 7888725, 20160075, 44352165, 84672315, 141120525, 206253075, 265182525, 300540195, 300540195, 265182525, 206253075, 141120525, 84672315, 44352165, 20160075, 7888725, 2629575, 736281, 169911, 31465, 4495, 465, 31, 1

Rows are numbered from zero; cells in each row are likewise numbered from zero. Row zero consists of $\binom{0}{0} = 1$; the n-th row starts with $\binom{n}{0} = 1$.

In words, this is read as "$n+1$ choose k = n choose k + n choose $k-1$", i.e. the number of choices if you must select k objects from $n+1$ is the same as the number of choices if you are selecting from n objects and have an initial choice of whether to take k or $k-1$. The rule defines what is usually called Pascal's triangle, presented as shown on the right. However, this is a misnomer for two reasons. Firstly, it isn't a triangle at all, unless font size decreases exponentially with increasing row number; it is more like a Chinese hat!



... which is appropriate enough because, secondly, this triangle and rule were known to the Chinese scholar Jia Xian, six hundred years before Pascal. Aligning the rows of the triangle on the left (as shown on the left) seems to make much better sense, typographically, computationally and combinatorially. A well-known relationship with the Fibonacci series, for instance, becomes immediately apparent as a series of diagonal sums.

The work of Jia Xian has passed to us through the commentary of Yang Hui (1238-1298) and Pascal's triangle is known in China as 'Yang Hui's triangle'. In Iran, it is known as the 'Khayyám triangle' after Omar Khayyám (1048-1131), although it was known to Persian, and Indian, scholars in the tenth century. Peter Cameron cites Robin Wilson as dating Western study of Pascal's triangle as far back as the Majorcan theologian Ramon Llull (1232–1316).

Web link: ptri1.tripod.com. See the wikipedia entry on nomenclature.
Further reading: Pascal's Arithmetical Triangle by A.W.F. Edwards, Johns Hopkins University Press, 2002. The Cameron citation appears in *Combinatorics: Topics, Techniques, Algorithms,* by Peter J. Cameron, CUP, 1994, section 3.3.

Fermat's Little Theorem

The argument given for the Many Dropout Lemma (Proposition 35 on page 126) that we used to prove the first part of Fermat's Little Theorem (Theorem 36.1 on page 128) contains an “iteration”. Such arguments are, typically, induction proofs in disguise. Here, to illustrate the point, I'll give a proof of the result by the Principle of Induction.

Theorem 36.1 *For all natural numbers* i *and primes* p*,*

$$i^p \equiv i \pmod{p} \quad .$$

YOUR PROOF:

MY PROOF: Let p be a prime. We prove

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

for

$P(i)$ the statement $i^p \equiv i \pmod{p}$

by the Principle of Induction.

Base case: $P(0)$ holds because

$$0^p = 0 \equiv 0 \pmod{p} \quad .$$

Inductive step: We need prove that, for all natural numbers i, $P(i)$ implies $P(i+1)$. To this end, let i be a natural number and assume $P(i)$; that is, assume that the following Induction Hypothesis

$$\text{(IH)} \qquad i^p \equiv i \pmod p$$

holds.

Then,

$$\begin{aligned}
(i+1)^p &= i^p + p \cdot \textstyle\sum_{k=1}^{p-1} \frac{(p-1)!}{(p-k)! \cdot k!} \cdot i^k + 1 \\
&\equiv i^p + 1 \pmod p && \text{, as } \tfrac{(p-1)!}{(p-k)! \cdot k!} \in \mathbb{N} \\
&\equiv i + 1 \pmod p && \text{, by Induction Hypothesis (IH)}
\end{aligned}$$

and we are done.

Two further induction techniques

Technique 1. Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

Let us consider the derived statement

$$P_\ell(m) = P(\ell + m)$$

for m ranging over the natural numbers.

We are now interested in analysing and stating the Principle of Induction associated to the derived Induction Hypothesis $P_\ell(n)$ solely in terms of the original statements $P(n)$.

To do this, we notice the following logical equivalences:

- $P_\ell(0) \iff P(\ell)$

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

  $\iff \forall\, n \geq \ell \text{ in } \mathbb{N}. \big(P(n) \implies P(n+1) \big)$

- $\forall m \in \mathbb{N}. P_\ell(m) \iff \forall m \geq \ell \text{ in } \mathbb{N}. P(m)$

Replacing the left-hand sides by their equivalent right-hand sides in the Principle of Induction with Induction Hypothesis $P_\ell(m)$ yields what is known as the

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.

Proof pattern:

In order to prove that

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

1. Write: Base case: and give a proof of $P(\ell)$.
2. Write: Inductive step: and give a proof that for all natural numbers n greater than or equal ℓ, $P(n)$ implies $P(n+1)$.
3. Write: By the Principle of Induction from basis ℓ, we conclude that $P(m)$ holds for all natural numbers m greater than or equal ℓ.

Technique 2. Let $P(m)$ be a statement for m ranging over the natural numbers greater than or equal a fixed natural number ℓ.

Let us consider the derived statement

$$P^{\#}(m) = \ \forall\, k \in [\ell..m].\, P(k)$$

again for m ranging over the natural numbers greater than or equal ℓ.

We are now interested in analysing and stating the Principle of Induction from basis ℓ associated to the derived Induction Hypothesis $P^{\#}(n)$ solely in terms of the original statements $P(n)$.

To do this, we proceed as before, noticing the following logical equivalences:

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

Replacing the left-hand sides by their equivalent right-hand sides in the Principle of Induction from basis ℓ with Induction Hypothesis $P^{\#}(m)$ yields what is known as the

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.

Proof pattern:

In order to prove that

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

1. Write: Base case: and give a proof of $P(\ell)$.
2. Write: Inductive step: and give a proof that for all natural numbers $n \geq \ell$, if $P(k)$ holds for all $\ell \leq k \leq n$ then so does $P(n+1)$.
3. Write: By the Principle of Strong Induction, we conclude that $P(m)$ holds for all natural numbers m greater than or equal ℓ.

Fundamental Theorem of Arithmetic

Every positive integer is expressible as the product of a unique finite sequence of ordered primes.

Proposition 96 *Every positive integer greater than or equal* 2 *is a prime or a product of primes.*

YOUR PROOF:

MY PROOF: Let $P(m)$ be the statement:

Either m is a prime or a product of primes .

We prove

$$\forall\, m \geq 2 \text{ in } \mathbb{N}.\, P(m)$$

by the Principle of Strong Induction (from basis 2).

Base case: $P(2)$ holds because 2 is a prime.

Inductive step: We need prove that for all natural numbers $n \geq 2$,

$$\text{If } P(k) \text{ for all natural numbers } 2 \leq k \leq n, \text{ then } P(n+1) \quad .$$

To this end, let $n \geq 2$ be an arbitrary natural number, and assume the following Strong Induction Hypothesis

$$(\mathrm{SIH}) \qquad \begin{array}{c} \text{for all natural numbers } 2 \leq k \leq n, \\ \text{either } k \text{ is prime or a product of primes} \quad . \end{array}$$

We will now prove that

$$\text{either } n+1 \text{ is a prime or a product of primes} \qquad (\dagger)$$

by cases (see page 111).

If $n+1$ is a prime, then of course $(\dagger)$ holds. Now suppose that $n+1$ is composite. Hence, it is the product of natural numbers p and q in the integer interval $[2..n]$. Since, by the Strong Induction Hypothesis (SIH), both p and q are either primes or a product of primes, so is $n+1 = p \cdot q$; and $(\dagger)$ holds.

By the Principle of Strong Induction (from basis 2), we conclude that every natural number greater than or equal 2 is either a prime or a product of primes.

Theorem 97 (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*

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

NB For $\ell = 0$, the sequence is empty and $\prod(\,) = 1$; for $\ell = 1$, $\prod(p_1) = p_1$; and, for $\ell \geq 2$, $\prod(p_1, \ldots, p_\ell) = p_1 \cdot \ldots \cdot p_\ell$.

YOUR PROOF:

MY PROOF: Since, by the previous proposition, every number greater than or equal 2 is a prime or a product of primes, it can either be expressed as $\prod(p)$ for a prime p or as $\prod(p_1, \ldots, p_\ell)$ with $\ell \geq 2$ for a finite ordered sequence of primes $p_1, \ldots, p_\ell$. As for the number 1, it can uniquely be expressed in this form as the product $\prod(\,)$ of the empty sequence $(\,)$.

We are thus left with the task of showing that for $n \geq 2$ in $\mathbb{N}$, such representations are *unique*.

To this end, we will establish that

> for all $\ell, k \geq 1$ in $\mathbb{N}$, and for all finite ordered sequences of primes $(p_1 \leq \cdots \leq p_\ell)$ and $(q_1 \leq \cdots \leq q_k)$, if $\prod(p_1, \ldots, p_\ell) = \prod(q_1, \ldots, q_k)$ then $(p_1, \ldots, p_\ell) = (q_1, \ldots, q_k)$; that is, $\ell = k$ and $p_i = q_i$ for all $i \in [1..\ell]$. $(\dagger)$

Let $(p_1 \leq \cdots \leq p_\ell)$ and $(q_1 \leq \cdots \leq q_k)$ with $\ell, k \geq 1$ in $\mathbb{N}$, be two arbitrary finite ordered sequences of primes, and assume that $\prod(p_1, \ldots, p_\ell) = \prod(q_1, \ldots, q_k)$.

By Euclid's Theorem (Corollary 84 on page 239), since p_1 divides $\prod(p_1, \ldots, p_\ell) = \prod(q_1, \ldots, q_k)$ it follows that it divides, and hence equals, some q_i for $i \in [1..k]$; so that $q_1 \leq p_1$. Analogously, one argues that $p_1 \leq q_1$; so that $p_1 = q_1$.

It follows by cancellation that $\prod(p_2, \dots, p_\ell) = \prod(q_2, \dots, q_k)$, and by iteration of this argument that $p_i = q_i$ for all $1 \le i \le \min(\ell, k)$. But, ℓ cannot be greater than k because otherwise one would have $\prod(p_{k+1}, \dots, p_\ell) = 1$, which is absurd. Analogously, k cannot be greater than ℓ; and we are done.

Btw, my argument above requires an "iteration", and I have already mentioned that, typically, these are induction proofs in disguise. To reinforce this, I will now give an inductive proof of uniqueness.[a]

[a]However, do have in mind that later on in the course, you will encounter more *Structural Principles of Induction* for finite sequences and other such data types.

Indeed, we consider $(\dagger)$ on page 296 in the form

$$\forall\, \ell \geq 1 \text{ in } \mathbb{N}.\, P(\ell) \qquad (\ddagger)$$

for $P(\ell)$ the statement

(IH) For all $k \geq 1$ in $\mathbb{N}$, and for all finite ordered sequences of primes $(p_1 \leq \cdots \leq p_\ell)$ and $(q_1 \leq \cdots \leq q_k)$, if $\prod(p_1, \ldots, p_\ell) = \prod(q_1, \ldots, q_k)$ then $(p_1, \ldots, p_\ell) = (q_1, \ldots, q_k)$; that is, $\ell = k$ and $p_i = q_i$ for all $i \in [1..\ell]$.

and prove $(\ddagger)$ by the Principle of Induction (from basis 1).

Base case: Establishing $P(1)$ is equivalent to showing that for all finite ordered sequences $(q_1 \leq \cdots \leq q_k)$ with $k \geq 1$ in $\mathbb{N}$, if $\prod(q_1, \ldots, q_k)$ is prime then $k = 1$; which is the case by definition of prime number.

Inductive step: Let $\ell \geq 1$ in $\mathbb{N}$ and assume the Induction Hypothesis $P(\ell)$.

To prove $P(\ell + 1)$, let $k \geq 1$ be an arbitrary natural number, and let $(p_1 \leq \cdots \leq p_{\ell+1})$ and $(q_1 \leq \cdots \leq q_k)$ be arbitrary finite ordered sequences of primes. In addition, assume that

$$\prod (p_1, \ldots, p_{\ell+1}) = \prod (q_1, \ldots, q_k) \quad .$$

By arguments as above, it follows that

$$p_1 = q_1$$

and hence that

$$\prod (p_2, \ldots, p_{\ell+1}) = \prod (q_2, \ldots, q_k) \quad .$$

Furthermore, note that $k > 1$; because otherwise the product of the 2 or more primes $p_1, \ldots, p_{\ell+1}$ would be a prime, which is absurd.

We have now the finite ordered sequence of primes $(p_2, \ldots, p_{\ell+1})$ of length ℓ and the finite ordered sequence of primes $(q_2, \ldots, q_k)$ of length $(k-1) \geq 1$ such that $\prod (p_2, \ldots, p_{\ell+1}) = \prod (q_2, \ldots, q_k)$ to which we may apply the Induction Hypothesis (IH). Doing so, it follows that $\ell = k - 1$ and that $p_i = q_i$ for all $i \in [2..\ell + 1]$.

Thus, $\ell + 1 = k$ and $p_i = q_i$ for all $i \in [1..\ell + 1]$. Hence, $P(\ell + 1)$ holds.

Homework

1. Argue that the uniqueness of prime factorisation is also a consequence of the statement

$$\forall \ell \geq 1 \text{ in } \mathbb{N}.\, P'(\ell) \qquad (*)$$

for $P'(\ell)$ the statement[a]

   For all $k \geq \ell$ in $\mathbb{N}$ and for all finite ordered sequences of primes $(p_1 \leq \cdots \leq p_\ell)$ and $(q_1 \leq \cdots \leq q_k)$, if $\prod(p_1, \ldots, p_\ell) = \prod(q_1, \ldots, q_k)$ then $(p_1, \ldots, p_\ell) = (q_1, \ldots, q_k)$; that is, $\ell = k$ and $p_i = q_i$ for all $i \in [1..\ell]$.

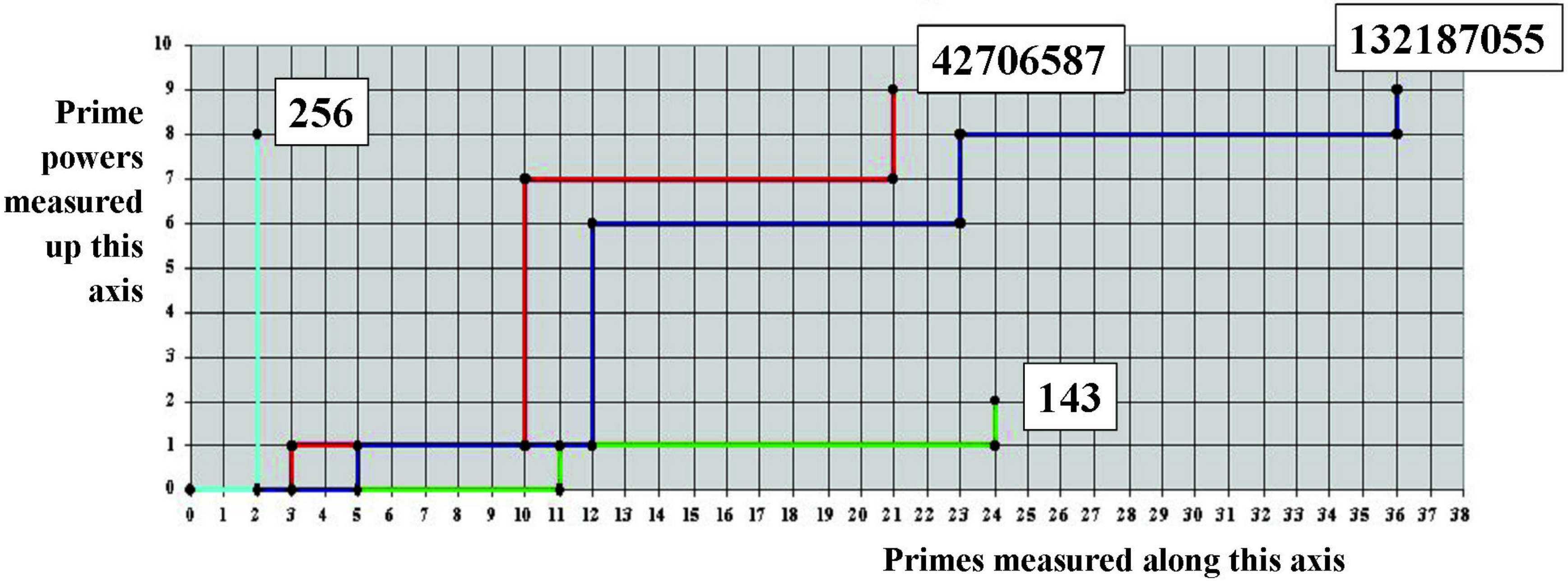
2. Prove $(*)$ above by the Principle of Induction (from basis 1), and compare your proof with mine for $(\ddagger)$.

[a]Note that the difference with the previously considered Induction Hypothesis is in the range of k, which here is $\geq \ell$ and previously was ≥ 1.

THEOREM OF THE DAY

The Fundamental Theorem of Arithmetic *Every integer greater than one can be expressed uniquely (up to order) as a product of powers of primes.*

Some Fundamental Paths



Every number corresponds to a unique path (which we may call a *fundamental path*) plotted on the xy-plane. Starting at $(0, 0)$ we progress horizontally along the x axis for each prime factor, taking the primes in ascending order. After each prime, we ascend the y axis to represent its power. Thus:

$256 = 2^8$ $\qquad 143 = 11 \times 13\ (= 11^1.13^1)$ $\qquad 42706587 = 3.7^6.11^2$ $\qquad 132187055 = 5.7^5.11^2.13.$

The end-points of fundamental paths may be called *fundamental points*. Some well-known conjectures about primes can be expressed in terms of questions about fundamental points: Goldbach's conjecture that every even integer greater than 2 is the sum of two primes could be solved if we knew which points on the line $y = 2$ were fundamental (the line for 143 shows that 24=11+13, for instance.) The 'twin primes conjecture', that there are infinitely many primes separated by 2 is a question about fundamental points on the line $y = 1$ (for example, $(3, 1)$ and $(5, 1)$ are fundamental points.)

Euclid, **Book 7, Proposition 30** of the *Elements*, proves that if a prime divides the product of two numbers then it must divide one or both of these numbers. This provided a key ingredient of the Fundamental Theorem which then had to wait more than two thousand years before it was finally established as the bedrock of modern number theory by Gauss, in 1798, in his *Disquisitiones Arithmeticae*.

Web link: www.dpmms.cam.ac.uk/~wtg10/FTA.html

Further reading: *Elementary Number Theory* by Gareth Jones and Mary Jones, Springer, Berlin, 1998.

gcd and min

It is sometimes customary, and very convenient, to restate the Fundamental Theorem of Arithmetic in the following terms:

Every positive integer n *is expressible as*

$$\prod_p p^{n_p}$$

where the product is taken over all primes but where the powers are natural numbers with $n_p \neq 0$ *for only finitely many primes* p*.*

Example 98

- $1224 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \cdot 17^1 \cdot 19^0 \cdot \ldots$
- $660 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot \ldots$

In these terms, gcds are given by taking mins of powers. Precisely,

$$\gcd\left(\prod_p p^{m_p}, \prod_p p^{n_p}\right) = \prod_p p^{\min(m_p,n_p)} . \qquad (\star)$$

Example 99

$$\begin{aligned}
&\gcd(1224, 660) \\
&= \quad 2^{\min(2,2)} \cdot 3^{\min(2,1)} \cdot 5^{\min(0,1)} \cdot 7^{\min(0,0)} \cdot 11^{\min(0,1)} \cdot 13^{\min(0,0)} \\
&\qquad \cdot 17^{\min(1,0)} \cdot 19^{\min(0,0)} \cdot \ldots \\
&= \quad 2^2 \cdot 3 \\
&= \quad 12
\end{aligned}$$

Euclid's infinitude of primes

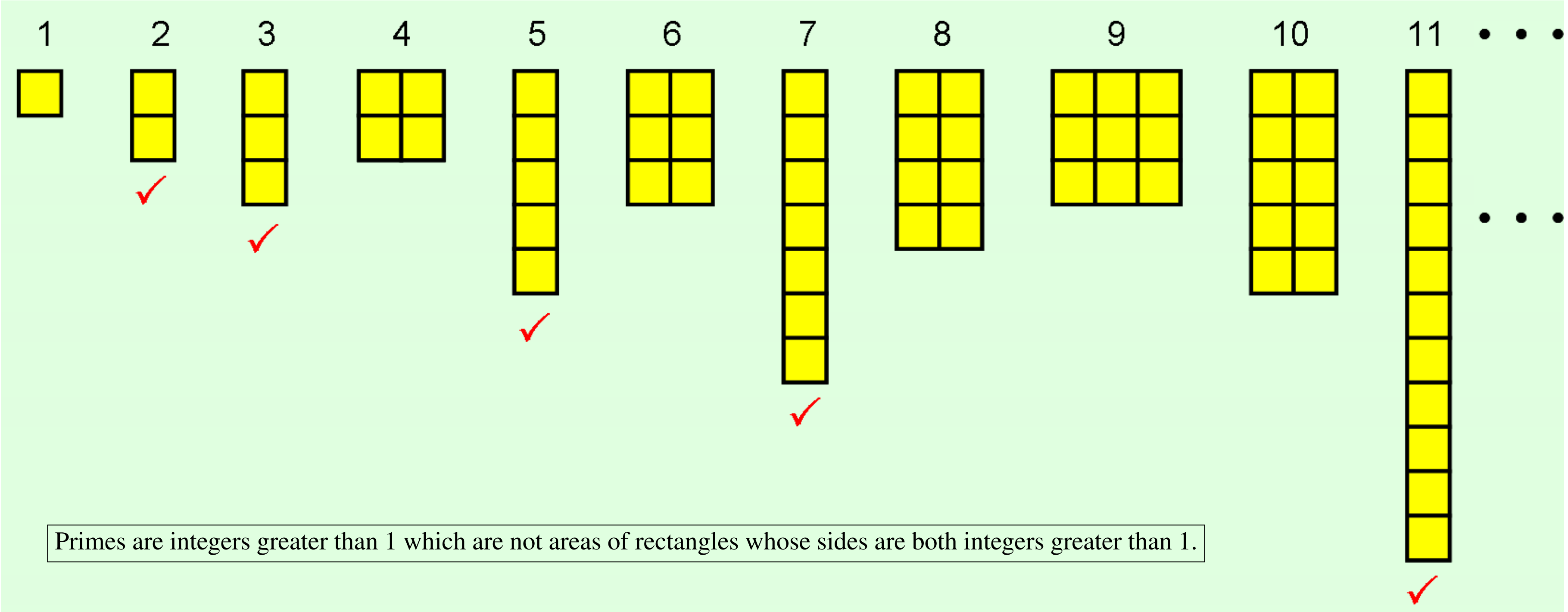
Theorem 100 *The set of primes is infinite.*

YOUR PROOF:

MY PROOF: We use proof by contradiction. So, suppose that the set of primes is finite, and let $p_1, \ldots, p_\ell$ with $\ell \in \mathbb{N}$ be the collection of them all. Consider the natural number $p = p_1 \cdot \ldots \cdot p_\ell + 1$. As p is not in the list of primes, by the Fundamental Theorem of Arithmetic (see Proposition 96), it is a product of primes. Thus, there exists a p_i for $i \in [1..\ell]$ such that $p_i \mid p$; and, since $p_i \mid (p_1 \cdot \cdots \cdot p_\ell)$, we have that p_i divides $p-(p_1 \cdot \ldots \cdot p_\ell) = 1$. This is a contradiction. Therefore, the set of primes is infinite.

THEOREM OF THE DAY

Euclid's Infinity of Primes *There are infinitely many prime numbers.*



A prime number is an integer greater than one which cannot be divided exactly by any other integer greater than one. Euclid's proof, well over two thousand years old, that such numbers form an infinity, is often cited by mathematicians today as the prototype of a beautiful mathematical argument. Thus, suppose there are just N primes, where N is a positive integer. Then we can list the primes: $p_1, p_2, \ldots, p_N$. Calculate $q = 1 + p_1 \times p_2 \times \ldots \times p_N$. Now q cannot be prime since it is larger than any prime in our list. But dividing q by any prime in our list leaves remainder 1, so q cannot be divided exactly by any prime in our list. So it cannot be divided by any integer greater than 1 other than q and is therefore prime by definition. This contradiction refutes the assertion that there were only N primes. So no such assertion can be made.

Remarks: (1) Euclid's proof uses the fact that non-divisibility by a prime implies non-divisibility by a non-prime (a composite). This is the content of **Book 7, Proposition 32** of his *Elements*.
(2) It would be a mistake to think that we always get a new prime directly from q since, for example, $2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$ and $1 + 30030$ is not prime, being the product of the two prime numbers 59 and 509.

Scant record exists of any such person as Euclid of Alexandria (325–265 BC) having existed. However, the *Elements* certainly date from third century BC Alexandria and although Greek mathematics, rooted in geometry, did not recognise the concept of infinity, this theorem with what is effectively this proof appears as *Proposition 20* in *Book IX*.

Web link: aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html. Is 1 prime? Find out here: arxiv.org/abs/1209.2007.
Further reading: *Ancient Mathematics (Sciences of Antiquity)*, by Serafina Cuomo, Routledge, 2001.

Created by Robin Whitty for www.theoremoftheda

Sets

Topics

Abstract sets. Extensionality. Subsets and supersets. Separation and comprehension. Russell's paradox. Empty set. Powerset. Hasse and Venn diagrams. The powerset Boolean algebra. Unordered and ordered pairing. Singletons. Products. Big unions. Big intersections. Disjoint unions. Relations. Matrices. Directed graphs. Reachability. Preorders. Reflexive-transitive closure. Partial functions. Functions (or maps). Bijections. Equivalence relations and set partitions. Calculus of bijections. Characteristic (or indicator) functions. Finite and infinite sets. Surjections. Stirling numbers of the second kind. Enumerability and countability. Choice. Injections. Cantor-Bernstein-Schroeder Theorem. Direct and inverse images. Replacement. Set-indexed constructions.

Unbounded cardinality: Cantor's diagonalisation argument and Lawvere's fixed-point argument. Foundation.

Complementary reading:

- Chapters 1, 30, and 31 of *How to Think Like a Mathematician* by K. Houston.
- Chapters 4.1 and 7 of *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.
- Chapters 1.3, 1.4, 4, 5, and 7 of *How to Prove it* by D. J. Velleman.

Objectives

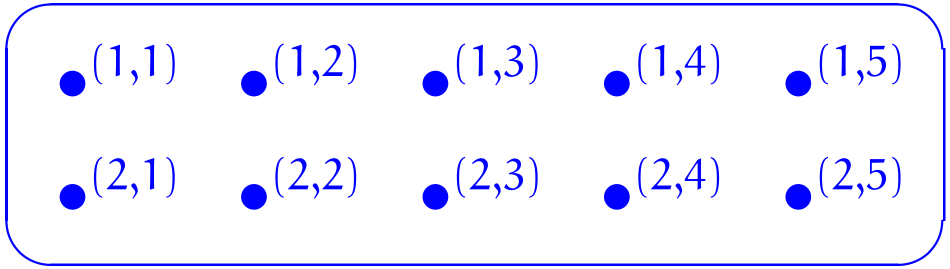
To introduce the basics of the theory of sets and some of its uses.

Abstract sets

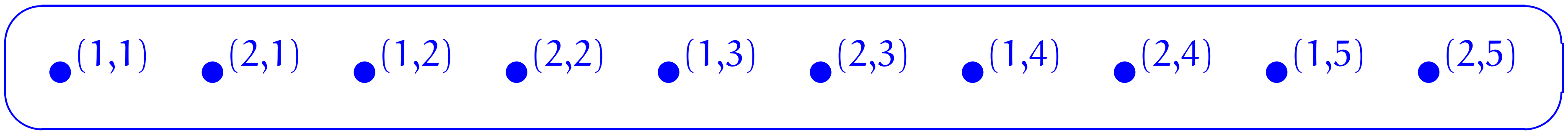
adapted from Section 1.1 of *Sets for Mathematics*
by F.W. Lawvere and R. Rosebrugh

An *abstract set* is supposed to have elements, each of which has no structure, and is itself supposed to have no internal structure (except that the elements can be distinguished as equal or unequal) and to have no external structure except for the number of elements. There are sets of all possible sizes, including finite and infinite sizes.

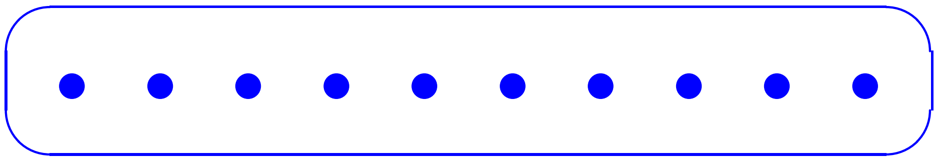
It has been said that a set is like a mental “bag of dots”, except of course that the bag has no shape; thus,



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.

Set Theory

Set Theory[a] is the branch of mathematical logic that studies axiom systems for the notion of abstract set as based on a membership predicate (recall page 199). As we will see (on page 324), care must be taken in such endeavour.

Set Theory aims at providing foundations for mathematics. There are however other approaches, as *Category Theory* and *Type Theory*, that also play an important role in Computer Science.

[a](for which you may consult the book *Naive Set Theory* by P. Halmos)

A widely used set theory is ZFC: Zermelo-Fraenkel Set Theory with Choice. It embodies postulates of: extensionality (page 315); separation [aka restricted comprehension, subset, or specification] (page 321); powerset (page 328); pairing (page 344); union (page 370); infinity (page 440); choice (page 453) replacement (page 464); foundation [aka regularity] (page 480).

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.

Set membership

We write $\in$ for the *membership predicate*; so that

$$x \in A \text{ stands for } x \text{ is an element of } A \quad .$$

We further write

$$x \notin A \text{ for } \neg(x \in A) \quad .$$

Example: $0 \in \{0, 1\}$ and $1 \notin \{0\}$ are true statements.

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:

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

Proposition 101 *For* $b, c \in \mathbb{R}$, *let*

$$\begin{aligned} A &= \{\, x \in \mathbb{C} \mid x^2 - 2bc + c = 0 \,\} \\ B &= \{\, b + \sqrt{b^2 - c}\,,\; b - \sqrt{b^2 - c} \,\} \\ C &= \{\, b \,\} \end{aligned}$$

Then,

1. $A = B$, *and*
2. $B = C \iff b^2 = c$.

Subsets and supersets

Definition 102 *For sets A and B, A is said to be a* subset *of B, written $A \subseteq B$, and B is said to be a* superset *of A, written $B \supseteq A$, whenever the statement*

$$\forall x.\, x \in A \implies x \in B$$

holds.

Example:

$$\{0\} \subseteq \{0,1\} \supseteq \{1\}$$

Notation 103 *The* proper subset *notation $A \subset B$ stands for $(A \subseteq B \ \wedge \ A \neq B)$. Analogously, the* proper superset *notation $B \supset A$ stands for $(B \supseteq A \ \wedge \ B \neq A)$.*

Lemma 104

1. *Reflexivity.*

   For all sets A, $A \subseteq A$.

2. *Transitivity.*

   For all sets A, B, C, $(A \subseteq B \ \wedge \ B \subseteq C) \implies A \subseteq C$.

3. *Antisymmetry.*

   For all sets A, B, $(A \subseteq B \ \wedge \ B \subseteq A) \implies A = B$.

Proper subsets

We let

$$A \subset B$$

stand for

$$A \subseteq B \ \wedge \ A \neq B \ .$$

Hence,

$$A \subset B \ \text{ iff } \ (\forall x. x \in A \implies x \in B) \ \wedge \ (\exists y. y \notin A \ \wedge \ y \in B) \ .$$

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.

Set comprehension

The set whose existence is postulated by the separation principle for a set A and a property P is typically denoted

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

(Recall the discussion on set comprehension on page 202.)

Thus, the statement $(\dagger)$ on page 202 follows.

NB

$$\{\, x \in A \mid P(x) \,\} \;\subseteq\; \{\, y \in B \mid Q(y) \,\}$$

is equivalent to

$$\forall z.\, \big[\, z \in A \;\wedge\; P(z) \,\big] \;\Longrightarrow\; \big[\, z \in B \;\wedge\; Q(z) \,\big]$$

Russell's paradox

The separation principle does not allow us to consider the class of those R such that $R \notin R$ as a set (and, btw, the same goes for the class of all sets). This is not a bug, but a feature!

Empty set

Set theory has an

empty set ,

typically denoted

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

with no elements.

Its defining statement is

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

or, equivalently,

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

NB: $\emptyset = \{\, x \in A \mid \mathbf{false} \,\}$.

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:

$$\#\emptyset = 0$$

Finite sets

The *finite sets* are those with cardinality a natural number.

Example: For $n \in \mathbb{N}$,

$$[n] = \{ x \in \mathbb{N} \mid x < n \}$$

is finite of cardinality n.

Powerset axiom

$\boxed{\text{For any set, there is a set consisting of all its subsets.}}$

The set of all subsets of a set U whose existence is postulated by the powerset axiom is typically denoted

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

Thus,

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

NB: The powerset construction can be iterated. In particular,

$$\mathcal{F} \in \mathcal{P}\big(\mathcal{P}(U)\big) \iff \mathcal{F} \subseteq \mathcal{P}(U) \quad ;$$

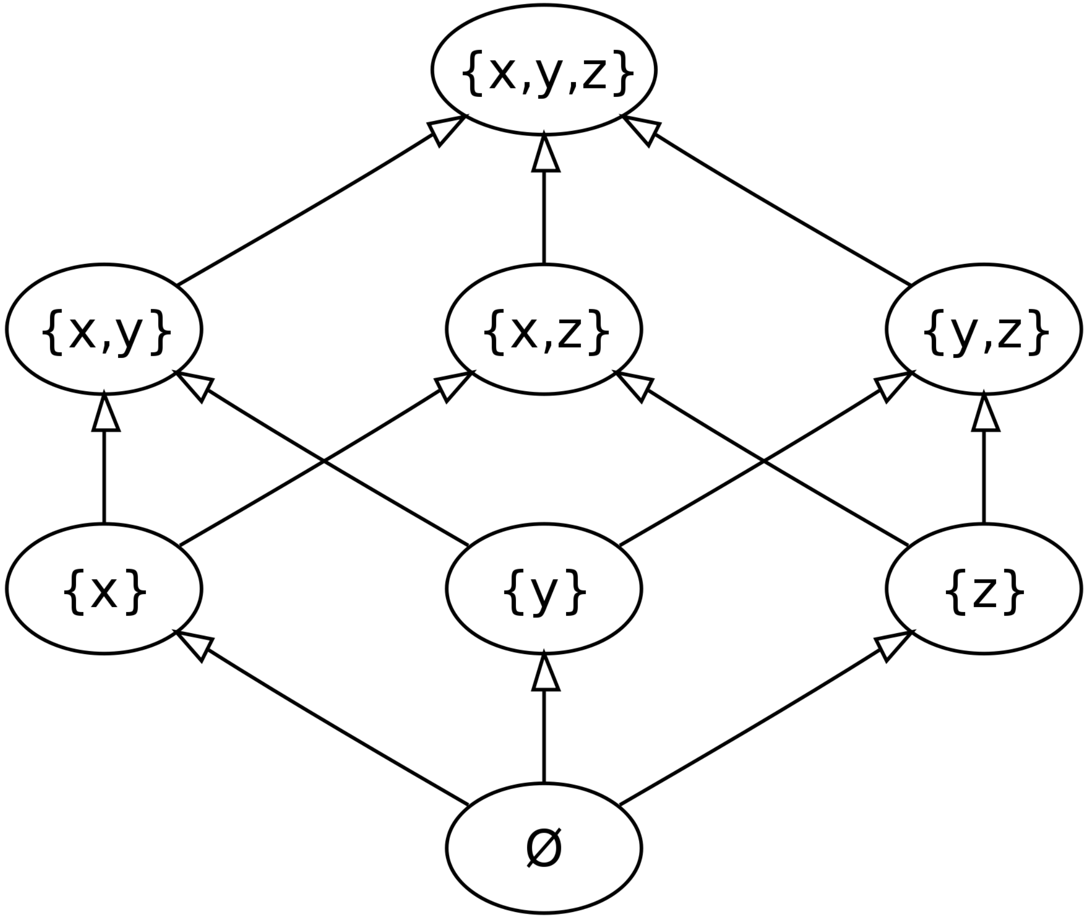
that is, $\mathcal{F}$ is a set of subsets of U, sometimes referred to as a *family*.

Example: The family $\mathcal{E} \subseteq \mathcal{P}\big([5]\big)$ consisting of the non-empty subsets of $[5] = \{0, 1, 2, 3, 4\}$ whose elements are even is

$$\mathcal{E} = \big\{ \{0\}, \{2\}, \{4\}, \{0, 2\}, \{0, 4\}, \{2, 4\}, \{0, 2, 4\} \big\} \ .$$

Hasse diagrams[a]

Example: $\mathcal{P}(\{x, y, z\})$



[a]From http://en.wikipedia.org/wiki/Powerset; see also http://en.wikipedia.org/wiki/Hasse_diagram.

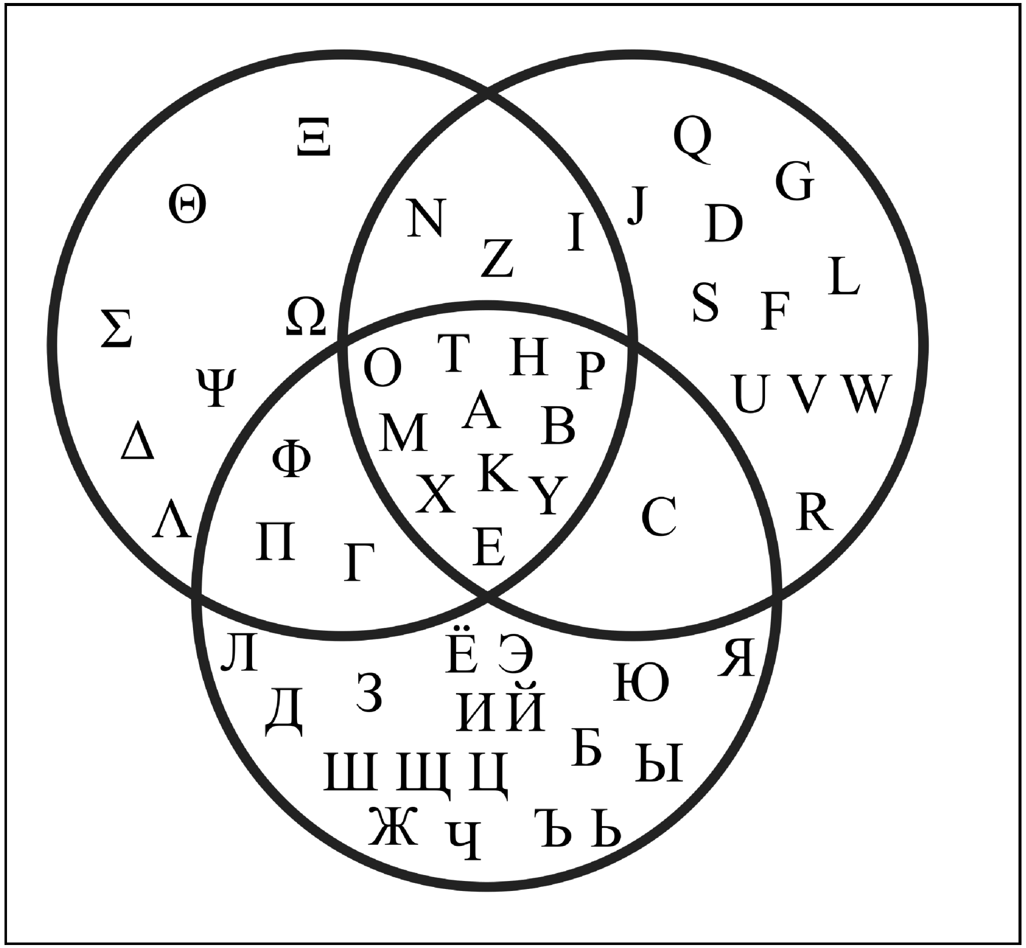
Proposition 105 *For all finite sets* U,

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

PROOF IDEA [a] :

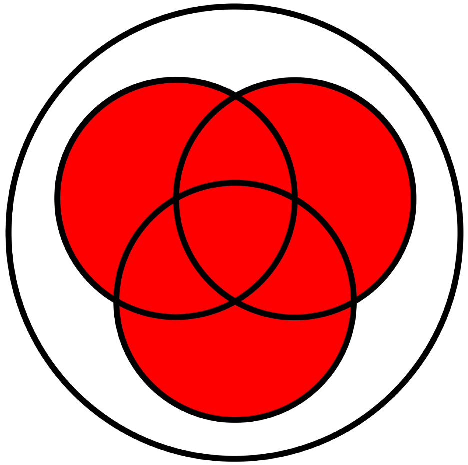
[a]See Theorem 162.1 on page 439.

Venn diagrams[a]

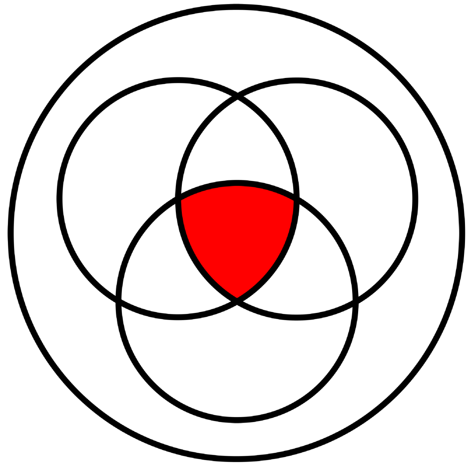


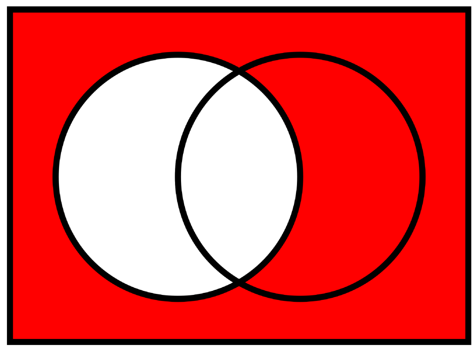
[a]From http://en.wikipedia.org/wiki/Union_(set_theory) and http://en.wikipedia.org/wiki/Intersection_(set_theory); see also http://en.wikipedia.org/wiki/Venn_diagram.

Union



Intersection





Complement

Homework Explicitly describe the family

$$\mathcal{S} = \{ S \subseteq [5] \mid \text{the sum of the elements of } S \text{ is } 6 \}$$

and depict its Hasse and Venn diagrams.

The powerset Boolean algebra

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

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

$$\begin{aligned}
A \cup B &= \{x \in U \mid x \in A \vee x \in B\} && \in \mathcal{P}(U) \\
A \cap B &= \{x \in U \mid x \in A \wedge x \in B\} && \in \mathcal{P}(U) \\
A^c &= \{x \in U \mid \neg(x \in A)\} && \in \mathcal{P}(U)
\end{aligned}$$

- 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* $\mathbb{U}$ is a neutral element for $\cap$.

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

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

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

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

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

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

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

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

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

Proposition 106 *Let* U *be a set and let* $A, B \in \mathcal{P}(U)$*.*

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

YOUR PROOF:

MY PROOF:

1. Let $X \in \mathcal{P}(U)$.

   $(\Longrightarrow)$ Assume $A \cup B \subseteq X$. Then, since $A \subseteq A \cup B$ and $B \subseteq A \cup B$, we have by transitivity of $\subseteq$ (Lemma 104(2) on page 319) both that $A \subseteq X$ and $B \subseteq X$ as required.

   $(\Longleftarrow)$ Assume that (i) $A \subseteq X$ and (ii) $B \subseteq X$. We need show that, for all $u \in U$,

   $$\big(u \in A \ \vee \ u \in B \big) \implies u \in X \quad .$$

   So, let $u \in U$ and assume (iii) $u \in A \ \vee \ u \in B$. Then, if $u \in A$ we have $u \in X$, by assumption (i); and, if $u \in B$ we also have $u \in X$, by assumption (ii). Thus, assumption (iii) yields $u \in X$ as required.

2. Let $X \in \mathcal{P}(U)$.

$(\Longrightarrow)$ Assume $X \subseteq A \cap B$. Then, since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, we have by transitivity of $\subseteq$ (Lemma 104(2) on page 319) both that $X \subseteq A$ and $X \subseteq B$ as required.

$(\Longleftarrow)$ Assume that (i) $X \subseteq A$ and (ii) $X \subseteq B$. We need show that, for all $u \in U$,

$$u \in X \implies \big(u \in A \wedge u \in B \big) \quad .$$

So, let $u \in U$ and assume $u \in X$. Then, by (i), $x \in A$ and, by (ii), $x \in B$ as required.

Corollary 107 *Let* U *be a set and let* $A, B, C \in \mathcal{P}(U)$.

1. $C = A \cup B$

iff

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

$$\land$$

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

2. $C = A \cap B$

iff

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

$$\land$$

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

Sets and logic

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

Pairing axiom

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

The set whose existence is postulated by the pairing axiom for a and b is typically denoted by

$$\{ a , b \} \quad .$$

Thus, the statement

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

holds, and we have that:

$$\#\{a, b\} = 1 \iff a = b \quad \text{and} \quad \#\{a, b\} = 2 \iff a \neq b \quad .$$

Singletons

For every a, the pairing axiom provides the set $\{a, a\}$ which is abbreviated as

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

and referred to as a *singleton*.

NB

$$\#\{\, a \,\} \ = \ 1$$

Examples:

$$\emptyset \subset \{\emptyset\} \subset \{\emptyset, \{\emptyset\}\} \supset \{\{\emptyset\}\} \supset \emptyset$$

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

NB

$$\{\emptyset\} \in \{\{\emptyset\}\} \quad , \quad \{\emptyset\} \not\subseteq \{\{\emptyset\}\} \quad , \quad \{\{\emptyset\}\} \not\subseteq \{\emptyset\}$$

Proposition 108 *For all* a, b, c, x, y,

1. $\{ a \} = \{ x, y \} \implies x = y = a$
2. $\{ c, x \} = \{ c, y \} \implies x = y$

YOUR PROOF:

MY PROOF: Let a, b, c, x, y be arbitrary.

1. Assume $\{a\} = \{x, y\}$.

   Then, $x \in \{a\}$ and therefore $x = a$. Analogously, $y = a$.

2. Assume $\{c, x\} = \{c, y\}$.

   Then, $(x = c \lor x = y) \land (y = c \lor y = x)$.
   Therefore, $(x = y = c) \lor (x = y)$. In either case, $x = y$.

Ordered pairing

Notation:

$$(a, b) \quad \text{or} \quad \langle a, b \rangle$$

Fundamental property:

$$(a, b) = (x, y) \implies a = x \wedge b = y$$

A construction:

For every pair a and b, three applications of the pairing axiom provide the set

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}$$

which defines an *ordered pairing* of a and b.

Proposition 109 (Fundamental property of ordered pairing)
For all a, b, x, y,

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

YOUR PROOF:

MY PROOF: *Let* a, b, x, y *be arbitrary.*

$(\Longleftarrow)$ *Vacuous.*

$(\Longrightarrow)$ *Assume* $\{\{a\},\{a,b\}\} = \{\{x\},\{x,y\}\}$.

Then, $\{a\} = \{x\} \vee \{a\} = \{x,y\}$*; and, in either case,* $a = x$. *Hence,* $\{\{a\},\{a,b\}\} = \{\{a\},\{a,y\}\}$ *and, by Proposition 108.2 (on page 347),* $\{a,b\} = \{a,y\}$ *which, again by Proposition 108.2, implies* $b = y$.

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

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

Thus,

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

More generally, for a fixed natural number n and sets $A_1, \ldots, A_n$, we have

$$\begin{aligned} \prod_{i=1}^{n} A_i &= A_1 \times \cdots \times A_n \\ &= \{ x \mid \exists\, a_1 \in A_1, \ldots, a_n \in A_n.\ x = (a_1, \ldots, a_n) \} \end{aligned}$$

where

$$\begin{aligned} &\forall\, a_1, a_1' \in A_1, \ldots, a_n, a_n' \in A_n. \\ &\quad (a_1, \ldots, a_n) = (a_1', \ldots, a_n') \iff (a_1 = a_1' \ \wedge \ \cdots \ \wedge \ a_n = a_n') \end{aligned} \quad .$$

NB Cunningly enough, the definition is such that $\prod_{i=1}^{0} A_i = \{ () \}$.

Notation 110 *For a natural number* n *and a set* A*, one typically writes* A^n *for* $\prod_{i=1}^{n} A$*.*

Pattern-matching notation

Example: The subset of ordered pairs from a set A with equal components is formally

$$\{ x \in A \times A \mid \exists\, a_1 \in A.\, \exists\, a_2 \in A.\, x = (a_1, a_2) \ \wedge\ a_1 = a_2 \}$$

but often abbreviated using *pattern-matching notation* as

$$\{ (a_1, a_2) \in A \times A \mid a_1 = a_2 \} \ .$$

Notation: For a property $P(a, b)$ with a ranging over a set A and b ranging over a set B,

$$\{ (a, b) \in A \times B \mid P(a, b) \}$$

abbreviates

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

Proposition 111 *For all finite sets A and B,*

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

PROOF IDEA [a] :

[a] See Theorem 162.2 on page 439.

Sets and logic

$\mathcal{P}(\mathbb{U})$	$\{\,\mathbf{false}\,,\ \mathbf{true}\,\}$
$\emptyset$	**false**
$\mathbb{U}$	**true**
$\cup$	$\vee$
$\cap$	$\wedge$
$(\cdot)^{\mathrm{c}}$	$\neg(\cdot)$
$\bigcup$	$\exists$
$\bigcap$	$\forall$

Big unions

Example:

- Consider the family of sets

$$\mathcal{T} = \left\{ T \subseteq [5] \;\middle|\; \begin{array}{l} \text{the sum of the elements of} \\ T \text{ is less than or equal } 2 \end{array} \right\}$$

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

- The *big union* of the family $\mathcal{T}$ is the set $\bigcup \mathcal{T}$ given by the union of the sets in $\mathcal{T}$:

$$n \in \bigcup \mathcal{T} \iff \exists T \in \mathcal{T}.\, n \in T \quad .$$

Hence, $\bigcup \mathcal{T} = \{\, 0, 1, 2 \,\}$.

Definition 112 *Let U be a set. For a collection of sets $\mathcal{F} \in \mathcal{P}(\mathcal{P}(U))$, we let the* big union *(relative to U) be defined as*

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

Btw To get some intuition behind this definition, it might be useful to compare the construction with the ML function

```
flatten :  'a list list -> 'a list
```

associated with the ML `list` datatype constructor.

Examples:

1. For $A, A_1, A_2 \in \mathcal{P}(\mathcal{U})$,

$$\bigcup \emptyset = \emptyset$$

$$\bigcup \{A\} = A$$

$$\bigcup \{A_1, A_2\} = A_1 \cup A_2$$

$$\bigcup \{A, A_1, A_2\} = A \cup A_1 \cup A_2$$

2. For $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(U)))$, let us introduce the notation

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

for the set

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

noticing that this is justified by the fact that, for all $x \in U$,

$$\begin{aligned} x \in \bigcup \{ X \in \mathcal{P}(U) \mid \exists \mathcal{A} \in \mathcal{F}.\, X = \bigcup \mathcal{A} \} \\ \iff \exists X \in \mathcal{P}(U).\, \exists \mathcal{A} \in \mathcal{F}.\, X = \bigcup \mathcal{A} \wedge x \in X \\ \iff \exists \mathcal{A} \in \mathcal{F}.\, x \in \bigcup \mathcal{A} \end{aligned}$$

We then have the following *associativity law*:

Proposition 113 *For all* $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(U)))$,

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

Btw In trying to understand this statement, ponder about the following analogous identity for the ML `list` datatype constructor: for all `F : 'a list list list`,

```
flatten ( flatten F )
  = flatten ( map flatten F ) : 'a list
```

The above two identities are the *associativity law* of a mathematical structure known as a *monad*, which has become a fundamental tool in functional programming.

YOUR PROOF:

MY PROOF: For $\mathcal{F} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{U})))$ and $x \in \mathcal{U}$, one calculates that:

$$
\begin{aligned}
& x \in \bigcup \left(\bigcup \mathcal{F} \right) \\
& \quad \iff \exists X \in \bigcup \mathcal{F}.\ x \in X \\
& \quad \iff \exists \mathcal{A} \in \mathcal{F}.\ \exists X \in \mathcal{A}.\ x \in X \\
& \quad \iff \exists \mathcal{A} \in \mathcal{F}.\ x \in \bigcup \mathcal{A} \\
& \quad \iff x \in \bigcup \left\{ \bigcup \mathcal{A} \in \mathcal{P}(\mathcal{U}) \mid \mathcal{A} \in \mathcal{F} \right\}
\end{aligned}
$$

Big intersections

Example:

- Consider the family of sets

$$\mathcal{S} = \left\{ S \subseteq [5] \;\middle|\; \text{the sum of the elements of } S \text{ is } 6 \right\}$$

$$= \{\{2,4\},\{0,2,4\},\{1,2,3\}\}$$

- The *big intersection* of the family $\mathcal{S}$ is the set $\bigcap \mathcal{S}$ given by the intersection of the sets in $\mathcal{S}$:

$$n \in \bigcap \mathcal{S} \iff \forall S \in \mathcal{S}.\, n \in S \quad .$$

Hence, $\bigcap \mathcal{S} = \{2\}$.

Definition 114 *Let $\mathcal{U}$ be a set. For a collection of sets $\mathcal{F} \subseteq \mathcal{P}(\mathcal{U})$, we let the* big intersection *(relative to $\mathcal{U}$) be defined as*

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

Examples: For $A, A_1, A_2 \in \mathcal{P}(\mathcal{U})$,

$$\bigcap \emptyset = \mathcal{U}$$

$$\bigcap \{A\} = A$$

$$\bigcap \{A_1, A_2\} = A_1 \cap A_2$$

$$\bigcap \{A, A_1, A_2\} = A \cap A_1 \cap A_2$$

Theorem 115 *Let*

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

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

NB This result is typically interpreted as stating that:

> $\mathbb{N}$ is the least set of numbers containing 0 and closed under successors.

PROOF:

Proposition 116 *Let U be a set and let $\mathcal{F} \subseteq \mathcal{P}(U)$ be a family of subsets of U.*

1. *For all* $S \in \mathcal{P}(U)$,
$$S = \bigcup \mathcal{F}$$
iff
$$\big[\forall A \in \mathcal{F}.\, A \subseteq S\big] \wedge \big[\forall X \in \mathcal{P}(U).\, (\forall A \in \mathcal{F}.\, A \subseteq X) \Rightarrow S \subseteq X\big]$$

2. *For all* $T \in \mathcal{P}(U)$,
$$T = \bigcap \mathcal{F}$$
iff
$$\big[\forall A \in \mathcal{F}.\, T \subseteq A\big] \wedge \big[\forall Y \in \mathcal{P}(U).\, (\forall A \in \mathcal{F}.\, Y \subseteq A) \Rightarrow Y \subseteq T\big]$$

Union axiom

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

The set whose existence is postulated by the union axiom for a collection $\mathcal{F}$ is typically denoted

$$\bigcup \mathcal{F}$$

and, in the case $\mathcal{F} = \{A, B\}$, abbreviated to

$$A \cup B \quad .$$

Thus,

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

and hence

$$x \in (A \cup B) \iff (x \in A) \vee (x \in B) \quad .$$

Using the separation and union axioms, for every collection $\mathcal{F}$, consider the set

$$\{\, x \in \bigcup \mathcal{F} \mid \forall X \in \mathcal{F}.\, x \in X \,\} \quad .$$

For *non-empty* $\mathcal{F}$ this set is denoted

$$\bigcap \mathcal{F}$$

because, in this case,

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

In particular, for $\mathcal{F} = \{A, B\}$, this is abbreviated to

$$A \cap B$$

with defining property

$$\forall x.\; x \in (A \cap B) \iff (x \in A) \wedge (x \in B) \quad .$$

Tagging

The construction

$$\{\,\ell\,\} \times A = \big\{\,(\ell, a) \mid a \in A\,\big\}$$

provides copies of A, as tagged by labels ℓ.

Indeed, note that

$$\forall\, y \in \big(\{\,\ell\,\} \times A\big).\, \exists!\, x \in A.\ y = (\ell, x) \quad ,$$

and that $\{\,\ell_1\,\} \times A_1 = \{\,\ell_2\,\} \times A_2 \iff (\ell_1 = \ell_2) \wedge (A_1 = A_2)$ so that

$$\{\,\ell_1\,\} \times A = \{\,\ell_2\,\} \times A \iff \ell_1 = \ell_2 \quad .$$

Disjoint unions

Definition 117 *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,

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

More generally, for a fixed natural number n and sets $A_1, \ldots, A_n$, we have

$$\begin{aligned} \biguplus_{i=1}^{n} A_i &= A_1 \uplus \cdots \uplus A_n \\ &= \big(\{1\} \times A_1\big) \cup \cdots \cup \big(\{n\} \times A_n\big) \end{aligned}$$

NB Cunningly enough, the definition is such that $\biguplus_{i=1}^{0} A_i = \emptyset$.

Notation 118 *For a natural number n and a set A, one typically writes $n \cdot A$ for $\biguplus_{i=1}^{n} A$.*

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

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

PROOF IDEA:

Corollary 120[a] *For all finite sets* A *and* B,

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

[a] See Theorem 162.3 on page 439.

Corollary 121 *Let* m, n *be a positive integers and* k *a natural number. For finite sets* $A_1, \ldots, A_n$, *if* $\#A_i \leq k$ *for all* $1 \leq i \leq n$ *and* $\#\left(\biguplus_{i=1}^{n} A_i\right) = m$ *then* $m \leq n \cdot k$.

NB The contrapositive gives:

The Generalised Pigeonhole Principle

Let m, n be positive integers and k a natural number. If m objects are distributed into n boxes and $m > n \cdot k$, then at least one box contains at least $k + 1$ objects.

Relations

Definition 122 *A* <u>(binary) relation</u> R *from a set* A *to a set* B *, denoted*

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

is a subset of the product set $A \times B$*; that is,*

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

Notation 123 *One typically writes* $a\,R\,b$ *for* $(a, b) \in R$*.*

NB Binary relations come with a *source* and a *target*.

One may also consider more general n*-ary relations*, for any natural number n. These are defined as subsets of n-ary products; that is, elements of

$$\mathcal{P}(A_1 \times \cdots \times A_n)$$

for sets $A_1, \cdots, A_n$.

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:

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

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

Relational extensionality

$$R = S : A \leftrightarrow B$$

iff

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

Relational composition

Definition 124 *The* composition *of two relations* $R : A \rightarrow\!\!\!\!\!+\, B$ *and* $S : B \rightarrow\!\!\!\!\!+\, C$ *is the relation*

$$S \circ R : A \rightarrow\!\!\!\!\!+\, C$$

defined by setting

$$a\ (S \circ R)\ c \iff \exists\, b \in B.\ a\ R\ b \ \wedge\ b\ S\ c$$

for all $a \in A$ *and* $c \in C$.

Theorem 125 *Relational composition is associative and has the identity relation as neutral element. That is,*

- *Associativity.*

  For all $R : A \rightarrow\!\!\!\!+\!\!\!\!\rightarrow B$, $S : B \rightarrow\!\!\!\!+\!\!\!\!\rightarrow C$, *and* $T : C \rightarrow\!\!\!\!+\!\!\!\!\rightarrow D$,

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

- *Neutral element.*

  For all $R : A \rightarrow\!\!\!\!+\!\!\!\!\rightarrow B$,

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

Relations and matrices

Definition 126

1. *For positive integers* m *and* n*, an* $(m \times n)$*-*<u>*matrix*</u> 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* $0 \leq j < n$*.*

   Btw *Rows and columns are enumerated from* 0*, and not* 1*. This is non-standard, but convenient for what follows.*

2. *The* identity $(n \times n)$*-matrix* I_n *has entries*

$$(I_n)_{i,j} = \begin{cases} 1 & \text{, if } i = j \\ 0 & \text{, if } i \neq j \end{cases}$$

3. *The* multiplication *of an* $(\ell \times m)$*-matrix* L *with an* $(m \times n)$*-matrix* M *is the* $(\ell \times n)$*-matrix* $M \cdot L$ *with entries*

$$\begin{aligned} (M \cdot L)_{i,j} &= (M_{0,j} \odot L_{i,0}) \oplus \cdots \oplus (M_{m-1,j} \odot L_{i,m-1}) \\ &= \bigoplus_{k=0}^{m-1} M_{k,j} \odot L_{i,k} \end{aligned}$$

Theorem 127 *Matrix multiplication is associative and has the identity matrix as neutral element.*

Definition 128

1. *The* <u>null</u> $(m \times n)$*-matrix* $Z_{m,n}$ *has entries*

$$(Z_{m,n})_{i,j} = 0 \quad .$$

2. *The* <u>addition</u> *of two* $(m \times n)$*-matrices* M *and* L *is the* $(m \times n)$*-matrix* $M + L$ *with entries*

$$(M + L)_{i,j} = M_{i,j} \oplus L_{i,j} \quad .$$

Theorem 129

1. *Matrix addition is associative, commutative, and has the null matrix as neutral element.*

2. *For every* $(\ell \times m)$*-matrices* L, L' *and* $(m \times n)$*-matrices* M, M', *the distributive laws*

$$M \cdot Z_{\ell,m} = Z_{\ell,n} \quad , \quad Z_{m,n} \cdot L = Z_{\ell,n}$$

and

$$\begin{aligned} M \cdot (L + L') &= (M \cdot L) + (M \cdot L') \\ (M + M') \cdot L &= (M \cdot L) + (M' \cdot L) \end{aligned}$$

hold.

Definition 130 *For every natural number* n*, let*

$$[n] = \{0, \ldots, n-1\} \quad .$$

NB Cunningly enough, $[0] = \emptyset$; so that $\#\,[n] = n$.

A relation $R : [m] \longrightarrow\!\!\!\!\!\!\!+\;\; [n]$ can be seen as the $(m \times n)$-matrix $\mathrm{mat}(R)$ over the commutative semiring of Booleans

$$\big(\{\mathbf{false}, \mathbf{true}\}, \mathbf{false}\,, \mathbf{true}\,, \;\vee\;, \;\wedge\;\big)$$

given by

$$\mathrm{mat}(R)_{i,j} \;=\; \big[\,(i,j) \in R\,\big] \quad .$$

Conversely, every $(m \times n)$-matrix M can be seen as the relation $\mathrm{rel}(M) : [m] \longrightarrow\!\!\!\!\!\!\!+\;\; [n]$ given by

$$(i,j) \in \mathrm{rel}(M) \iff M_{i,j} \quad .$$

In fact,

$$\mathrm{rel}\big(\mathrm{mat}(R)\big) = R \quad \text{and} \quad \mathrm{mat}\big(\mathrm{rel}(M)\big) = M \quad .$$

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

More interestingly, this carries over to identities :

$$\mathrm{mat}(\mathrm{id}_{[n]}) = I_n \quad \text{and} \quad \mathrm{rel}(I_n) = \mathrm{id}_{[n]} \quad ,$$

and to composition/multiplication :

$$\mathrm{mat}(S \circ R) = \mathrm{mat}(S) \cdot \mathrm{mat}(R) \quad \text{and} \quad \mathrm{rel}(M \cdot L) = \mathrm{rel}(M) \circ \mathrm{rel}(L) \quad .$$

Indeed,

$$
\begin{aligned}
(i,j) \in \mathrm{rel}\big(\,\mathrm{mat}(S)\cdot \mathrm{mat}(R)\,\big) \\
&\iff \quad \big(\,\mathrm{mat}(S)\cdot \mathrm{mat}(R)\,\big)_{i,j} \\
&\iff \quad \bigvee_{k=0}^{m-1}\ \mathrm{mat}(S)_{k,j}\ \wedge\ \mathrm{mat}(R)_{i,k} \\
&\iff \quad \exists\, k \in [m].\ \ (k,j) \in S\ \wedge\ (i,k) \in R \\
&\iff \quad (i,j) \in \big(S \circ R\big)
\end{aligned}
$$

Thus, the composition of relations between finite sets can be implemented by means of matrix multiplication:

$$
S \circ R = \mathrm{rel}\big(\,\mathrm{mat}(S)\cdot \mathrm{mat}(R)\,\big) \quad .
$$

Directed graphs

Definition 131 *A* directed graph (A, R) *consists of a set* A *and a relation* R *on* A *(i.e. a relation from* A *to* A*).*

Notation 132 *We write* $\mathrm{Rel}(A)$ *for the set of relations on a set* A*; that is,* $\mathrm{Rel}(A) = \mathcal{P}(A \times A)$*.*

Corollary 133 *For every set A, the structure*

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

is a monoid.

Definition 134 *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

Definition 135 *Let* (A, R) *be a directed graph. For* $s, t \in A$, *a* path *of length* $n \in \mathbb{N}$ *in* R, *with* source s *and* target t, *is a tuple* $(a_0, \ldots, a_n) \in A^{n+1}$ *such that* $a_0 = s$, $a_n = t$, *and* $a_i \ R \ a_{i+1}$ *for all* $0 \le i < n$.

NB Cunningly enough, the unary tuple (a_0) is a path of length 0 with source s and target t iff $s = a_0 = t$.

Proposition 136 *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 137 *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 138 *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 $\big([n], R\big)$ for n a positive integer is called its *adjacency matrix*.

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

$$\left\{ \begin{array}{rcl} M_0 & = & I_n \\ M_{k+1} & = & I_n + \big(M \cdot M_k\big) \end{array} \right.$$

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

NB The same algorithm but over other semirings (rather than over the Boolean semiring) can be used to compute other information on paths; like the weight of shortest paths[a], or the set of paths.

[a](for which you may see Chapter 25.1 of *Introduction to Algorithms (Second Edition)* by T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein)

Preorders

Definition 139 *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.*

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

Definition 140 *A* partial order*, or* poset[a]*, is a preorder* $(P , \sqsubseteq)$ *that further satisfies*

- *Antisymmetry.*

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

[a](standing for *partially ordered set*)

Examples:

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

Theorem 141 *For* $R \subseteq A \times A$, *let*

$$\mathcal{F}_R = \{ Q \subseteq A \times A \mid R \subseteq Q \land Q \textit{ is a preorder} \} \quad .$$

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

NB This result is typically interpreted in various forms as stating that:

- $R^{\circ *}$ is the reflexive-transitive closure of R.
- $R^{\circ *}$ is the least preorder containing R.
- $R^{\circ *}$ is the preorder freely generated by R.

PROOF:

Partial functions

Definition 142 *A relation* $R : A \rightarrow\!\!\!\!\!+\!\!\!\rightarrow B$ *is said to be* functional, *and called a* partial function, *whenever it is such that*

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

NB $R : A \rightarrow\!\!\!\!\!+\!\!\!\rightarrow B$ is *not* functional if there are a in A and $b_1 \neq b_2$ in B such that both (a, b_1) and (a, b_2) are in R.

Example: The relation

$$\{\,(x,y) \mid y = x^2\,\} : \mathbb{Z} \longrightarrow\!\!\!\!\!\!\!+\;\; \mathbb{N}$$

is functional, while the relation

$$\{\,(m,n) \mid m = n^2\,\} : \mathbb{N} \longrightarrow\!\!\!\!\!\!\!+\;\; \mathbb{Z}$$

is not because, for instance, both $(1,1)$ and $(1,-1)$ are in it.

Notation 143 *We write* $f : A \rightharpoonup B$ *to indicate that* f *is a partial function from* A *to* B, *and let*

$$\mathrm{PFun}(A, B) = (A \rightleftharpoons B) \ \subseteq \mathrm{Rel}(A, B)$$

denote the set of partial functions from A *to* B.

Every partial function $f : A \rightharpoonup B$ satisfies that

> for each element a of A there is at most one element b of B such that b is a value of f at a.

The expression

$$f(a)$$

is taken to denote "the value" of f at a whenever this exists and considered *undefined* otherwise.

To see this in action, let $f : A \rightharpoonup B$ and $g : B \rightharpoonup C$ and consider the expression

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

This is defined iff $f(a)$ is defined (and hence an element of B) and also $g\big(f(a)\big)$ is defined (and hence an element of C), in which case it denotes the value of $(g \circ f)$ at a.

One typically writes $f(a)\downarrow$ (respectively $f(a)\uparrow$) to indicate that the partial function f is defined (respectively undefined) at a.

Thus, in symbols,

$$\big[\ f(a)\downarrow \wedge\, g\big(f(a)\big)\downarrow\ \big] \implies \big[\ \big(g \circ f\big)(a)\downarrow\ \wedge \big(g \circ f\big)(a) = g\big(f(a)\big)\ \big] \ .$$

Theorem 144 *The identity relation is a partial function, and the composition of partial functions yields a partial function.*

NB

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

iff

$$\forall a \in A. \big(\, f(a){\downarrow} \iff g(a){\downarrow} \,\big) \;\wedge\; f(a) = g(a)$$

In practice, a partial function $f : A \rightharpoonup B$ is typically defined by specifying:

- a *domain of definition* $D_f \subseteq A$, and
- a *mapping*

$$f : a \mapsto b_a$$

  given by a *rule* that to each element a in the domain of definition D_f assigns a unique element b_a in the target B (so that $f(a) = b_a$).

Warning: When proceeding as above, it is important to note that you need make sure that:

1. D_f is a subset of A,

2. for every a in D_f, the b_a as described by your mapping (i.e. rule) is unique and is in B (so that it is a well-defined value for f at a).

Example: The following are examples of partial functions.

- rational division $\div : \mathbb{Q} \times \mathbb{Q} \rightharpoonup \mathbb{Q}$, with domain of definition $\{(r, s) \in \mathbb{Q} \times \mathbb{Q} \mid s \neq 0\}$;
- integer square root $\sqrt{\_} : \mathbb{Z} \rightharpoonup \mathbb{Z}$, with domain of definition $\{m \in \mathbb{Z} \mid \exists n \in \mathbb{Z}.\, m = n^2\}$;
- real square root $\sqrt{\_} : \mathbb{R} \rightharpoonup \mathbb{R}$, whose domain of definition is $\{x \in \mathbb{R} \mid x \geq 0\}$.

Btw There are alternative notations for mappings

$$f : a \mapsto b_a$$

that, although with different syntax, you have already encountered; namely, the notations

$$f(a) = b_a \qquad \text{and} \qquad f = \lambda\, a.\, b_a$$

from which the ML declaration styles

$$\mathtt{fun}\ f(a)\ \mathtt{=}\ b_a \qquad \text{and} \qquad \mathtt{val}\ f\ \mathtt{=}\ \mathtt{fn}\ a\ \mathtt{=>}\ b_a$$

come from.

Proposition 145 *For all finite sets* A *and* B,

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

PROOF IDEA [a] :

[a] See Theorem 162.4 on page 439.

Functions (or maps)

Definition 146 *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.*

The notation $f : A \longrightarrow B$ is used to indicate that f is a function from A to B, and we write

$$\mathrm{Fun}(A, B) \;=\; (A \Rightarrow B)$$

for the set of functions from A to B.

Thus,

$$(A \Rightarrow B) \subseteq (A \rightharpoonup B) \subseteq \mathrm{Rel}(A, B)$$

and we have the following fact:

Theorem 147 *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 148 *For all finite sets A and B,*

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

PROOF IDEA [a] :

[a] See Theorem 162.5 on page 439.

Our discussion on how to define partial functions also applies to functions; but, because of their total nature, simplifies as follows.

In practice, a function $f : A \longrightarrow B$ is defined by specifying a mapping

$$f : a \mapsto b_a$$

given by a *rule* that to each $a \in A$ assigns a unique element $b_a \in B$ (which is the value of f at a denoted $f(a)$).

Warning: When proceeding as above, it is important to note that your mapping should be defined for every a in A and that the described b_a should be a uniquely determined element of B.

Theorem 149 *The identity partial function is a function, and the composition of functions yields a function.*

NB

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

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

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

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

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

Inductive definitions

Examples:

- $\mathrm{add} : \mathbb{N}^2 \longrightarrow \mathbb{N}$

$$\begin{cases} \mathrm{add}(m, 0) &= m \\ \mathrm{add}(m, n+1) &= \mathrm{add}(m, n) + 1 \end{cases}$$

- $S : \mathbb{N} \longrightarrow \mathbb{N}$

$$\begin{cases} S(0) &= 0 \\ S(n+1) &= \mathrm{add}(n, S(n)) \end{cases}$$

The function

$$\rho_{a,f} : \mathbb{N} \to A$$

inductively defined from

$$\begin{cases} a \in A \\ f : \mathbb{N} \times A \to A \end{cases}$$

is the unique such that

$$\begin{cases} \rho_{a,f}(0) &=& a \\ \rho_{a,f}(n+1) &=& f\big(n, \rho_{a,f}(n)\big) \end{cases}$$

Examples:

- $\mathrm{add} : \mathbb{N}^2 \to \mathbb{N}$

  $\mathrm{add}(m, n) = \boldsymbol{\rho}_{m,f}(n)$ for $f(x, y) = y + 1$

- $S : \mathbb{N} \to \mathbb{N}$

  $S = \boldsymbol{\rho}_{0,\mathrm{add}}$

For a set A, consider $a \in A$ and a function $f : \mathbb{N} \times A \to A$.

Definition 150 *Define* $R \subseteq \mathbb{N} \times A$ *to be* (a, f)-closed *whenever*

- $0 \, R \, a$, *and*
- $\forall \, n \in \mathbb{N}. \, \forall \, x \in A. \, n \, R \, x \implies (n+1) \, R \, f(n, x)$.

Theorem 151 *Let* $\rho_{a,f} = \bigcap \{ R \subseteq \mathbb{N} \times A \mid R$ *is* (a, f)*-closed* $\}$.

1. *The relation* $\rho_{a,f} : \mathbb{N} \rightarrowtail A$ *is functional and total.*
2. *The function* $\rho_{a,f} : \mathbb{N} \to A$ *is the unique such that* $\rho_{a,f}(0) = a$ *and* $\rho_{a,f}(n+1) = f\big(n, \rho_{a,f}(n)\big)$ *for all* $n \in \mathbb{N}$.

Bijections, I

Definition 152 *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:*

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

Notation 153 *The inverse of a function f is necessarily unique and typically denoted f^{-1}.*

Example: The mapping mat associating an $(m \times n)$-matrix to a relation from $[m]$ to $[n]$ is a bijection, with inverse the mapping rel; see page 391 for definitions.

The set of bijections from A to B is denoted

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

and we thus have

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

Proposition 154 *For all finite sets* A *and* B,

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

PROOF IDEA [a] :

[a] See Theorem 162.6 on page 439.

Theorem 155 *The identity function is a bijection, and the composition of bijections yields a bijection.*

Definition 156 *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.

  Definition 157 *A relation* E *on a set* A *is said to be an* equivalence relation *whenever it is:*

  1. *reflexive*

     $$\forall x \in A.\, x \mathrel{E} x$$

  2. *symmetric*

     $$\forall x, y \in A.\, x \mathrel{E} y \implies y \mathrel{E} x$$

  3. *transitive*

     $$\forall x, y, z \in A.\, (x \mathrel{E} y \wedge y \mathrel{E} z) \implies x \mathrel{E} z$$

  The set of all equivalence relations on A *is denoted* $\mathrm{EqRel}(A)$.

- Set partitions.

Definition 158 *A* partition P *of a set* A *is a set of non-empty subsets of* A *(that is,* $P \subseteq \mathcal{P}(A)$ *and* $\emptyset \notin P$*), whose elements are typically referred to as* blocks*, such that*

1. *the union of all blocks yields* A*:*

$$\bigcup P = A \quad ,$$

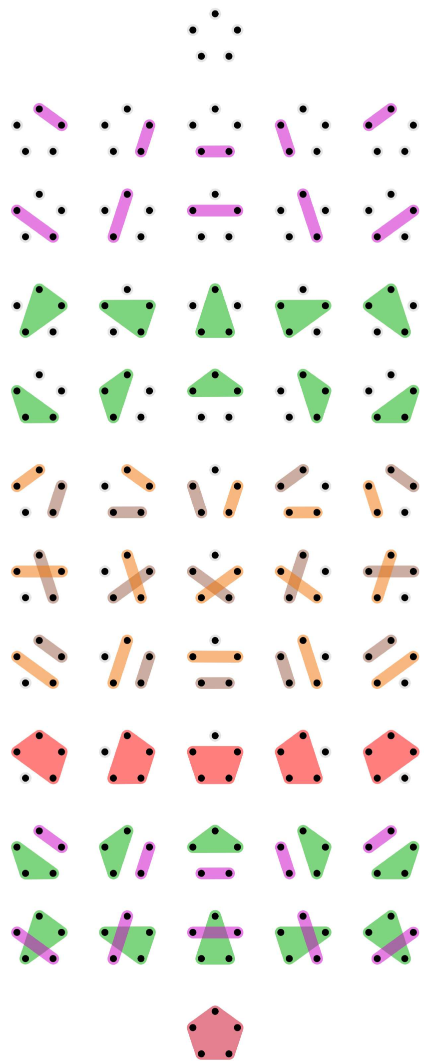
   and

2. *all blocks are pairwise disjoint:*

$$\text{for all } b_1, b_2 \in P,\ b_1 \neq b_2 \implies b_1 \cap b_2 = \emptyset \quad .$$

The set of all partitions of A *is denoted* $\mathrm{Part}(A)$*.*

The partitions of a 5-element set[a]



[a] From http://en.wikipedia.org/wiki/Partition_of_a_set.

Theorem 159 *For every set A,*

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

PROOF OUTLINE:

1. Prove that the mapping

$$E \quad \mapsto \quad A_{/E} = \{\, b \subseteq A \mid \exists\, a \in A.\, b = [a]_E \,\}$$

where $[a]_E = \{\, x \in A \mid x\, E\, a \,\}$

yields a function $\mathrm{EqRel}(A) \to \mathrm{Part}(A)$.

2. Prove that the mapping

$$P \quad \mapsto \quad \equiv_P$$

where $x \equiv_R y \iff \exists\, b \in P.\ x \in b \wedge y \in b$

yields a function $\mathrm{Part}(A) \to \mathrm{EqRel}(A)$.

3. Prove that the above two functions are inverses of each other.

Proposition 160 *For all finite sets* A*,*

$$\#\mathrm{EqRel}(A) = \#\mathrm{Part}(A) = \mathrm{B}_{\#A}$$

where, for $n \in \mathbb{N}$*, the so-called* Bell numbers *are defined by*

$$\mathrm{B}_n = \begin{cases} 1 & \text{, for } n = 0 \\ \sum_{i=0}^{m} \binom{m}{i} \mathrm{B}_i & \text{, for } n = m+1 \end{cases}$$

PROOF IDEA [a] :

[a]See Theorem 162.7-8 on page 439.

Calculus of bijections, I

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

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

Example: The key combinatorial argument in proving Pascal's rule (see pages 274 and 278) resides in the bijection

$$\mathcal{P}\big(X \uplus [1]\big) \cong \mathcal{P}(X) \uplus \mathcal{P}(X)$$

deducible as

$$\begin{aligned}
\mathcal{P}\big(X \uplus [1]\big) &\cong \big((X \uplus [1]) \Rightarrow [2]\big) \\
&\cong \big(X \Rightarrow [2]\big) \times \big([1] \Rightarrow [2]\big) \\
&\cong \mathcal{P}(X) \times [2] \\
&\cong \mathcal{P}(X) \times \big([1] \uplus [1]\big) \\
&\cong \big(\mathcal{P}(X) \times [1]\big) \uplus \big(\mathcal{P}(X) \times [1]\big) \\
&\cong \mathcal{P}(X) \uplus \mathcal{P}(X)
\end{aligned}$$

Finite cardinality

Definition 161 *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 162 *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. $\mathrm{Bij}\big([n], [n]\big) \cong [n!]$
7. $\mathrm{Part}\big([0]\big) \cong [1]$
8. $\mathrm{Part}\big([n + 1]\big) \cong \biguplus_{S \subseteq [n]} \mathrm{Part}(S^c)$

Infinity axiom

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

Bijections, II

Proposition 163 *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. $$\begin{array}{l} \quad \big(\forall\, b \in B.\, \exists\, a \in A.\, f(a) = b\big) \\ \wedge \\ \quad \big(\forall\, a_1, a_2 \in A.\, f(a_1) = f(a_2) \implies a_1 = a_2\big) \end{array}$$

Surjections

Definition 164 *A function* $f : A \to B$ *is said to be* surjective*, or a* surjection*, and indicated* $f : A \twoheadrightarrow B$ *whenever*

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

Examples:

1. Every bijection is a surjection.

2. The unique function $A \to [1]$ is surjective iff $A \neq \emptyset$.

3. The quotient function $A \to A_{/E} : a \mapsto [a]_E = \{\, x \in A \mid x\, E\, a \,\}$ associated to an equivalence relation E on a set A is surjective.

4. The projection function $A \times B \to A : (a, b) \mapsto a$ is surjective iff $B \neq \emptyset$ or $A = \emptyset$.

5. For natural numbers m and n with $m < n$, there is no surjection from $[m]$ to $[n]$.

Theorem 165 *The identity function is a surjection, and the composition of surjections yields a surjection.*

The set of surjections from A to B is denoted

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

and we thus have

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

Proposition 166

1. *For all finite sets* A *and natural numbers* n, *the cardinality of the set* $\mathrm{Part}_n(A)$ *of partitions of* A *in* n *blocks has cardinality* $S\big(\#A, n\big)$, *where the* Stirling numbers of the second kind $S(m, n)$ *are defined by*
   - $S(0, 0) = 1$;
   - $S(k, 0) = S(0, k) = 0$, *for* $k \geq 1$;
   - $S(m + 1, n + 1) \ = \ S(m, n) + (n + 1) \cdot S(m, n + 1)$, *for* $m, n \geq 0$.

2. *For all finite sets* A *and* B,

$$\#\mathrm{Sur}(A, B) \ = \ S\big(\#A, \#B\big) \cdot (\#B)! \quad .$$

PROOF IDEA:

Enumerability

Definition 167

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.*

Btw For an enumeration $e : \mathbb{N} \twoheadrightarrow A$, if

$$e(n) = a \qquad (n \in \mathbb{N}, a \in A)$$

we think of the natural number n as a *code* for the element a of A. Codes need not be unique, but since

$$\{\, e(n) \in A \mid n \in \mathbb{N} \,\} = A$$

every element of A is guaranteed to have a code. These will be unique whenever the enumeration is a bijection.

Examples:

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

$\cdots$	-3	-2	-1	0	1	2	3	$\cdots$
$\cdots$	5	3	1	0	2	4	6	$\cdots$

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

	0	1	2	3	4	5	$\cdots$
0	0	2	3	9	10	$\cdots$	
1	1	4	8	11			
2	5	7	12				
3	6	13		$\ddots$			
4	14						
$\vdots$	$\vdots$						

Proposition 168 *Every non-empty subset of an enumerable set is enumerable.*

YOUR PROOF:

MY PROOF: Let $\emptyset \neq S \subseteq A$ and let $e : \mathbb{N} \twoheadrightarrow A$ be surjective.

Note that $\{ n \in \mathbb{N} \mid e(n) \in S \} \neq \emptyset$ and let

$$\mu(0) = \min\{ n \in \mathbb{N} \mid e(n) \in S \} \quad .$$

Furthermore, define by induction

$$\mu(k+1) = \min\{ n \in \mathbb{N} \mid n > \mu(k) \wedge e(n) \in S \} \qquad (k \in \mathbb{N})$$

where, by convention, $\min \emptyset = \mu(0)$.[a]

Finally, one checks[b] that the mapping

$$k \mapsto e\big(\mu(k)\big) \qquad (k \in \mathbb{N})$$

defines a function $\mathbb{N} \twoheadrightarrow S$ that is surjective.

---

[a] Btw, the operation of *minimisation* is at the heart of recursion theory.

[b] Please do it!

Countability

Proposition 169

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.*

Btw Corollary 180 (on page 469) provides more examples.

Axiom of choice

$\boxed{\text{Every surjection has a section.}}$

Injections

Definition 170 *A function* $f : A \to B$ *is said to be* injective*, or an* injection*, and indicated* $f : A \rightarrowtail B$ *whenever*

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

Examples:

- Every section is an injection; so that, in particular, bijections are injections.
- All functions including a set into another one are injections.
- For all natural numbers k, the function $\mathbb{N} \to \mathbb{N} : n \mapsto n + k$ is an injection.
- For all natural numbers k, the function $\mathbb{N} \to \mathbb{N} : n \mapsto n \cdot k$ is an injection iff $k \geq 1$.
- For all natural numbers k, the function $\mathbb{N} \to \mathbb{N} : n \mapsto k^n$ is an injection iff $k \geq 2$.

Theorem 171 *The identity function is an injection, and the composition of injections yields an injection.*

The set of injections from A to B is denoted

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

and we thus have

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

with

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

Proposition 172 *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:

Cantor-Bernstein-Schroeder Theorem

Definition 173 *A set* A *is of* <u>less than or equal cardinality</u> *to a set* B *whenever there is an injection* $A \rightarrowtail B$*, in which case we write*

$$A \lesssim B \quad \textit{or} \quad \#A \leq \#B \quad .$$

NB It follows from the axiom of choice that the existence of a surjection $B \twoheadrightarrow A$ implies $\#A \leq \#B$.

Theorem 174 (Cantor-Schroeder-Bernstein theorem) *For all sets* A *and* B,

$$\big(A \lesssim B \ \wedge \ B \lesssim A\big) \implies A \cong B \quad .$$

Relational images

Definition 175 *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*

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

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

Functional images

Proposition 176 *Let* $f : A \to B$ *be a function.*

For all $X \subseteq A$*,*

$$\overrightarrow{f}(X) = \{\, b \in B \mid \exists\, a \in X.\ f(a) = b \,\} \quad .$$

Remark More intuitively, this set is commonly denoted by

$$\{\, f(a) \in B \mid a \in X \,\}$$

conveying the idea that the direct-image function is to the powerset construction as the map function is to the list type constructor.

Proposition 177 *Let* $f : A \to B$ *be a function.*

For all $Y \subseteq B$,

$$\overleftarrow{f}(Y) = \{ a \in A \mid f(a) \in Y \} \quad .$$

Remark Hence,

$$a \in \overleftarrow{f}(Y) \iff f(a) \in Y \quad .$$

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

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

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 178 *An enumerable indexed disjoint union of enumerable sets is enumerable.*

YOUR PROOF:

MY PROOF: Let $\{ A_i \}_{i \in I}$ be a family of sets indexed by a set I. Furthermore, let $e : \mathbb{N} \twoheadrightarrow I$ be a surjection and, for all $i \in I$, let $e_i : \mathbb{N} \twoheadrightarrow A_i$ be surjections.

The function $\varepsilon : \mathbb{N} \times \mathbb{N} \to \biguplus_{i \in I} A_i$ defined, for all $(m, n) \in \mathbb{N} \times \mathbb{N}$, by

$$\varepsilon(m, n) = \big(i, e_i(n)\big) \quad , \quad \text{where } i = e(m)$$

is a surjection, which pre-composed with any surjection $\mathbb{N} \twoheadrightarrow \mathbb{N} \times \mathbb{N}$ yields a surjection $\mathbb{N} \twoheadrightarrow \biguplus_{i \in I} A_i$ as required.

Corollary 179 *A countable indexed disjoint union of countable sets is countable.*

Corollary 180 *If* X *and* A *are countable sets then so are* A^**,* $\mathcal{P}_{\mathrm{fin}}(A)$*, and* $(X \rightharpoonup_{\mathrm{fin}} A)$*.*

Calculus of bijections, II

- $\biguplus_{i\in[n]} A_i \cong ((\cdots(A_0 \uplus A_1)\cdots) \uplus A_{n-1})$
- $\prod_{i\in[n]} A_i \cong ((\cdots(A_0 \times A_1)\cdots) \times A_{n-1})$
- $(\biguplus_{i\in I} A_i) \times B \cong \biguplus_{i\in I}(A_i \times B)$
- $(A \Rightarrow \prod_{i\in I} B_i) \cong \prod_{i\in I}(A \Rightarrow B_i)$
- $((\biguplus_{i\in I} A_i) \Rightarrow B) \cong \prod_{i\in I}(A_i \Rightarrow B)$
- $A \cong \biguplus_{a\in A}[1]$
- $(A \Rightarrow B) \cong \prod_{a\in A} B$

Combinatorial examples:

1. . The combinatorial content of the Binomial Theorem (Theorem 265 and page 270) comes from a bijection

$$\big(U \Rightarrow (X \uplus Y)\big) \;\cong\; \biguplus_{S\in\mathcal{P}(U)} (S \Rightarrow X) \times (S^c \Rightarrow Y)$$

available for any triple of sets U, X, Y.

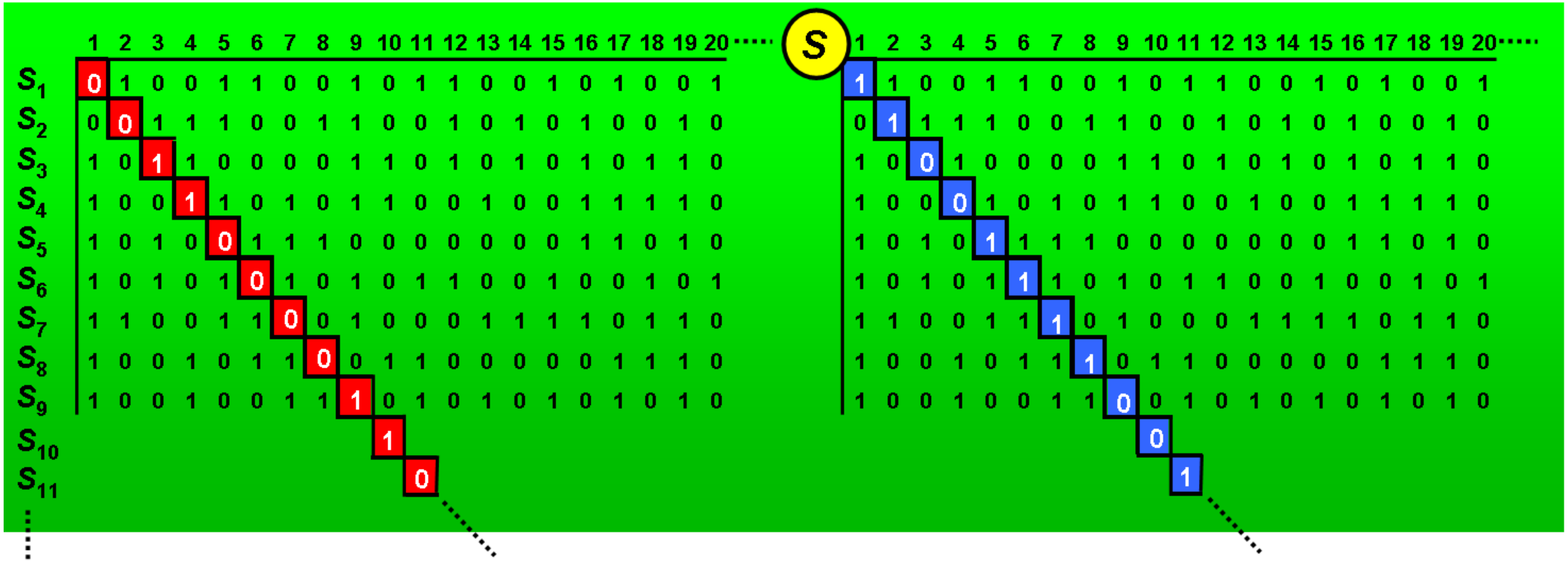
2. The combinatorial content underlying the Bell numbers comes from a bijection

$$\mathrm{Part}\big(A \uplus [1]\big) \;\cong\; \biguplus_{S\subseteq A} \mathrm{Part}(S^c) \quad .$$

available for all sets 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 181 (Cantor's diagonalisation argument) *For every set* A*, no surjection from* A *to* $\mathcal{P}(A)$ *exists.*

YOUR PROOF:

Btw The *diagonalisation technique* is very important in both logic and computation.

MY PROOF: Assume, by way of contradiction, a surjection $e : A \twoheadrightarrow \mathcal{P}(A)$, and let $a \in A$ be such that

$$e(a) \; = \; \{ \, x \in A \mid x \notin e(x) \, \} \quad .$$

Then,

$$\forall \, x \in A. \, x \in e(a) \iff x \notin e(x)$$

and hence

$$a \in e(a) \iff a \notin e(a) \quad ;$$

that is, a contradiction. Therefore, there is no surjection from A to $\mathcal{P}(A)$.

Definition 182 *A* fixed-point *of a function* $f : X \to X$ *is an element* $x \in X$ *such that* $f(x) = x$*.*

Btw Solutions to many problems in computer science are computations of fixed-points.

Theorem 183 (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.*

YOUR PROOF:

MY PROOF: Assume a surjection $e : A \twoheadrightarrow (A \Rightarrow X)$. Then, for an arbitrary function $f : X \longrightarrow X$ let $a \in A$ be such that

$$e(a) = \lambda x \in A.\, f\big(e(x)(x)\big) \in (A \Rightarrow X) \quad .$$

Then,

$$e(a)(a) = f\big(e(a)(a)\big) \quad ,$$

and we are done.

Corollary 184 *The sets*

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

are not enumerable.

Corollary 185 *There are* non-computable *infinite sequences of bits; that is, there are infinite sequences of bits* σ *with the property that for all programs* p *that forever print bits there is a natural number index* i_p *for which the* i_p *bit of* σ *disagrees with the* i_p *bit output by* p*.*

Corollary 186 *For a set* D*, there exists a surjection* $\mathrm{D} \twoheadrightarrow (\mathrm{D} \Rightarrow \mathrm{D})$ *iff* D *is a singleton.*

Note however that in ML we have the

```
datatype
  D = afun of D -> D
```

coming with functions

```
afun                                : (D->D) -> D

fn x => case x of afun f => f       : D -> (D->D)
```

that is highly non-trivial!

And indeed is inhabited by an enumerable infinitude of elements; for instance,

```
afun( fn x => x )                                  : D

afun( fn x => case x of afun f => f x )            : D

afun( fn x => case x of afun f => f f x )          : D

afun( fn x => case x of
        afun f => case f x of
          afun g => g x )                          : D
```

Foundation axiom

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

Thereby, providing a

Principle of $\in$*-Induction* .

Well-founded relations

Definition 187 *Let* $\prec \subseteq A \times A$ *be a relation on a set* A*.*

1. *An element* $m \in S \subseteq A$ *is a* minimal element of S *whenever* $\neg\big(\exists\, x \in S.\, x \prec m\big)$ *(equivalently,* $\forall\, x \in A.\, x \prec m \implies x \notin S$*).*
2. *The binary relation* $\prec$ *on* A *is* well-founded *whenever every non-empty subset of* A *has a minimal element.*

Example: The strictly less than relation on natural numbers is well-founded.

Proposition 188 *A relation* $\prec \subseteq A \times A$ *on a set* A *is well-founded if, and only if, there are no infinite sequences*

$$a_0\,,\ a_1\,,\ \ldots\,,\ a_i\,,\ \ldots$$

that are descending in the sense that

$$a_0 \succ a_1 \succ \cdots \succ a_i \succ \cdots$$

Principle of Well-founded induction

Let $\prec \subseteq A \times A$ be a well-founded relation and let $P(a)$ be a statement for $a \in A$.

To prove

$$\forall\, a \in A.\, P(a)$$

show that, for $x \in A$, the induction hypothesis

$$\text{(IH)} \quad \forall\, y \in A.\, y \prec x \implies P(y)$$

implies

$$P(x) \quad .$$

In symbols,

$$\begin{aligned} &\big(\forall\, x \in A.\, \big[\forall\, y \in A.\, y \prec x \implies P(y)\big] \implies P(x)\big) \\ &\qquad \implies \forall\, a \in A.\, P(a) \end{aligned}$$

Homework

1. Show that

$$
\begin{array}{l}
\quad \big(\forall x \in \mathbb{N}.\, \big[\forall y \in \mathbb{N}.\, y < x \implies P(y)\big] \implies P(x)\big) \\
\iff \\
\quad \big(P(0) \wedge \big[\forall n \in \mathbb{N}.\, (\forall y \in \mathbb{N}.\, y \leq n \implies P(y)) \implies P(n+1)\big]\big)
\end{array}
$$

2. Spellout the principle of well-founded induction for $\mathbb{N} \times \mathbb{N}$ ordered by each of the following two well-founded relations:

   (a) $(i, j) < (k, l) \iff (i < k) \wedge (j < l)$

   (b) $(i, j) < (k, l) \iff (i < k) \vee \big[(i = k) \wedge (j < l)\big]$