Notes
for Part IA CST 2013/14

Discrete Mathematics For Computer Science

<cl.cam.ac.uk/teaching/1314/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

Lecture plan

1. Preliminaries (pages 4–10) and introduction (pages 11–37).
2. On implication (pages 38–56) and bi-implication (pages 57–67).
3. On universal quantification (pages 68–75) and conjunction (pages 76–83).
4. On existential quantification (pages 84–97).
5. On disjunction (pages 98–109) and a little arithmetic (pages 110–125).

6. On negation (pages 126–145).
7. On number systems (pages 146–157).
8. On the division theorem and algorithm (pages 158–168) and modular arithmetic (pages 169–175).
9. On sets (pages 176–181), the greatest common divisor (pages 182–189), and Euclid's algorithm (pages 190–211) and theorem (pages 212–217).
10. On the Extended Euclid's Algorithm (pages 218–231) and the Diffie-Hellman cryptographic method (pages 232–236).

11. On mathematical induction: the Principle of Induction (pages 237–258), the Principle of Induction from a basis (pages 259–263), and the Principle of Strong Induction from a basis (pages 263–285).

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 work with, mathematical arguments.
- Doing some basic discrete mathematics.
- Getting a taste of computer science applications.

What is it that we do?

In general:

Mathematical models and 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

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

Mathematical argument

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:

The product of two odd integers is odd.

This seems innocuously 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:

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

which further presupposes that you know:

- what variables are;
- what

  if . . . then . . .

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

Even more precisely, we should write

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

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 of false — but not both.

Example 1

'$e^{i\pi} + 1 = 0$'

Non-example

'This statement is false'

THEOREM OF THE DAY

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

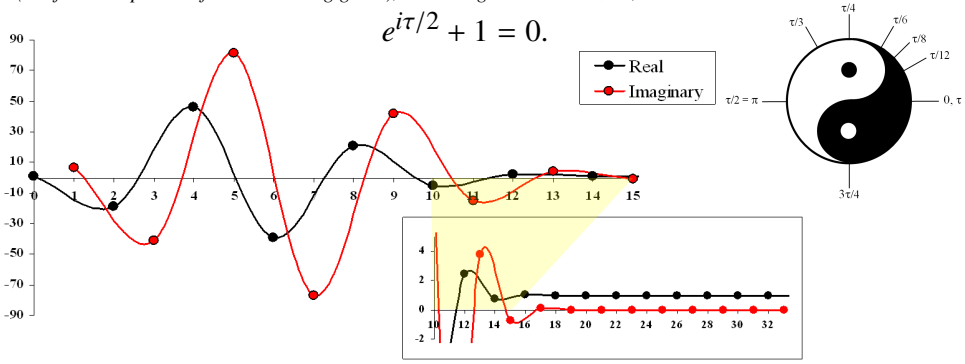
$\tau = 2\pi = 6.2831853071\ 7958647692\ 5286766559\ 0057683943\ 3879875021\ 1641949889\ 1846156328\ 1257241799\ 7256069650\ 6842341359\ldots$

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

From www.theoremoftheday.org by Robin Whitty. This file hosted by London South Bank University

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*

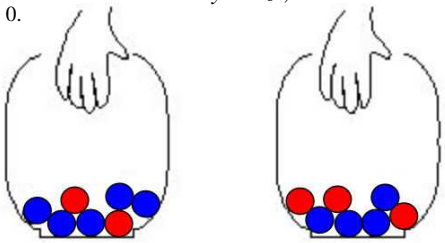
2. *The Pumping Lemma*

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.

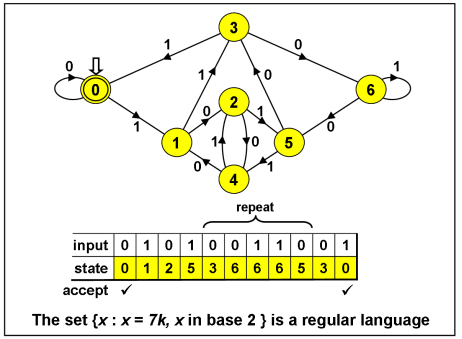
Fermat's innocent statement was famously left unproved when he died in 1665 and was the last of his unproved 'theorems' to be settled true or false, hence the name. The non-modularity of the Frey curve was established in the 1980s by the successive efforts of Gerhard Frey, Jean-Pierre Serre and Ken Ribet. 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.

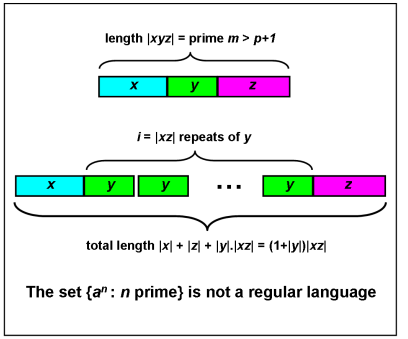
Web link: math.stanford.edu/~lekheng/flt/kleiner.pdf

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 $\mathcal{L}$.*





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*
3. *Schanuel's Conjecture*

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.

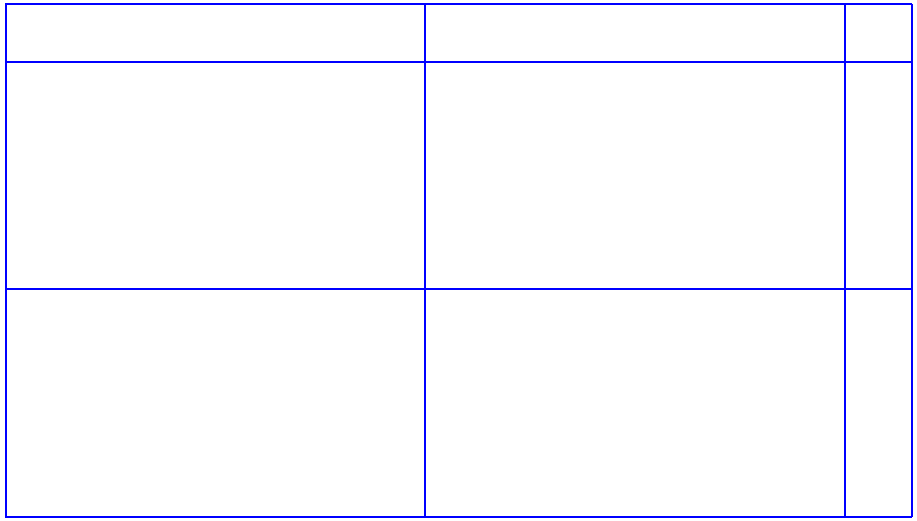
Warning: It is vitally important that you can recall definitions precisely. A common problem is not to be able to advance in some problem because the definition of a word is unknown.

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 28):

MY PROOF OF Proposition 8 (on page 28): 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 indeed odd.

Warning: Though the scratch work

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

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.

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* **imply** some *conclusion*

or, in symbols,

a collection of *hypotheses* $\Longrightarrow$ some *conclusion*

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

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'

The main proof strategy for implication:

To prove a goal of the form

$$P \Longrightarrow Q$$

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
	$P \implies Q$
⋮	

After using the strategy

Assumptions	Goal
	Q
⋮	
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, $m \cdot n = (2 \cdot i + 1) \cdot (2 \cdot j + 1) = \cdots$
...

Go to Workout 1
on page 287

An alternative proof strategy for implication:

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

Since

the *contrapositive* of 'P implies Q' is 'not Q implies not P'

we obtain the following:

[a] See Corollary 40 (on page 140).

Proof pattern:
In order to prove that

$$P \implies Q$$

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

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$
⋮	

After using the strategy

Assumptions	Goal
	not P
⋮	
not Q	

Definition 9 *A real number is:*

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

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

YOUR PROOF:

MY PROOF: Assume that x is a positive real number. We prove the contrapositive; that is, if $\sqrt{x}$ is rational then so is x. Assume that $\sqrt{x}$ is a rational number. That is, by definition, assume that $\sqrt{x} = m/n$ 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.

Go to Workout 2
on page 288

Logical Deduction
— Modus Ponens —

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

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

or, in other words,

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

or, in symbols,

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

The use of implications:

> To use an assumption of the form $P \implies Q$,
> 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) P_2 holds

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

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

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

Proof pattern:
In order to prove that

$$P \iff Q$$

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

Bi-implication

Some theorems can be written in the form

P is equivalent to Q

or, in other words,

P implies Q, and vice versa

or

Q implies P, and vice versa

or

P if, and only if, Q $\qquad$ P iff Q

or, in symbols,

$$P \iff Q$$

Proposition 12 *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 Workout 1.1 (on page 287).

($\Longleftarrow$) We prove the contrapositive; that is, that n odd implies n^2 odd. Assume that n is odd; that is, by definition, that $n = 2 \cdot k + 1$ for some integer k. Then, $n^2 = \cdots$ ...

Homework Provide details of the argument for ($\Longrightarrow$) and finish the proof of ($\Longleftarrow$).

Go to Workout 3 on page 289

Divisibility

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

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

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

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

Example 16

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

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

Proposition 17 *For every integer* n*,*

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

Homework Prove the above proposition.

Go to Workout 4
on page 291

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 $Q \implies P$.

Go to Workout 5
on page 293

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,

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

Example 18

1. *Proposition 8 (on page 28).*
2. *(Proposition 10 on page 49) For every positive real number x, if x is irrrational then so is $\sqrt{x}$.*
3. *(Proposition 12 on page 59) For every integer n, we have that n is even iff so is n^2.*
4. *Proposition 17 (on page 64).*

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 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
	$\forall x.\, P(x)$
⋮	

After using the strategy

Assumptions	Goal
	$P(x)$ (for a fresh x)
⋮	

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

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 $m \mid (n \cdot a - n \cdot b)$, 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 $a \equiv b \pmod{m}$.

Go to Workout 6
on page 295

Conjunction

Conjunctive statements are of the form

P **and** Q

or, in other words,

both P and also Q hold

or, in symbols,

P & Q or P ∧ Q

The proof strategy for conjunction:

To prove a goal of the form

P & Q

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

Proof pattern:
In order to prove

P & 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 & Q
⋮	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	P		Q
⋮		⋮	

The use of conjunctions:

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

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

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:

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

Go to Workout 7
on page 297

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,

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

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

Intuition:

The main proof strategy for existential statements:

To prove a goal of the form

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

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

Proof pattern:
In order to prove

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

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

Scratch work:

Before using the strategy

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

After using the strategy

Assumptions	Goals
	$P(w)$
$\vdots$	
$w = \ldots$ (the witness you decided on)	

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

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 22:

MY PROOF OF Proposition 22: 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 23 *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 24 *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

$(\dagger)$ $\exists$ integer i. $m = i \cdot l$

and that

$(\ddagger)$ $\exists$ integer j. $n = j \cdot m$.

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 $l \mid m$; 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 $k \cdot l = j_0 \cdot i_0 \cdot l = j_0 \cdot m = n$.

Go to Workout 8
on page 299

Disjunction

Disjunctive statements are of the form

P or Q

or, in other words,

either P, Q, or both hold

or, in symbols,

$P \vee Q$

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

Go to Workout 9
on page 301

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
	$P \vee Q$
⋮	

After using the strategy

Assumptions	Goal
	Q
⋮	
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
⋮	
$P_1 \vee P_2$	

After using the strategy

Assumptions	Goal	Assumptions	Goal
	Q		Q
⋮		⋮	
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 natural numbers* p *and* m*, if* $m = 0$ *or* $m = p$ *then* $\binom{p}{m} \equiv 1 \pmod{p}$.

YOUR PROOF:

MY PROOF: Let p and m be arbitrary natural numbers.

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 greater than 0 and less than p.

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:

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

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 110), we have that $\binom{p}{m} \equiv 1 \pmod{p}$; in the second case (ii), by Lemma 28 (on page 112), we have that $\binom{p}{m} \equiv 0 \pmod{p}$; and, in the third case (iii), by Lemma 27 (on page 110), we have that $\binom{p}{m} \equiv 1 \pmod{p}$.

Binomial theorem

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

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

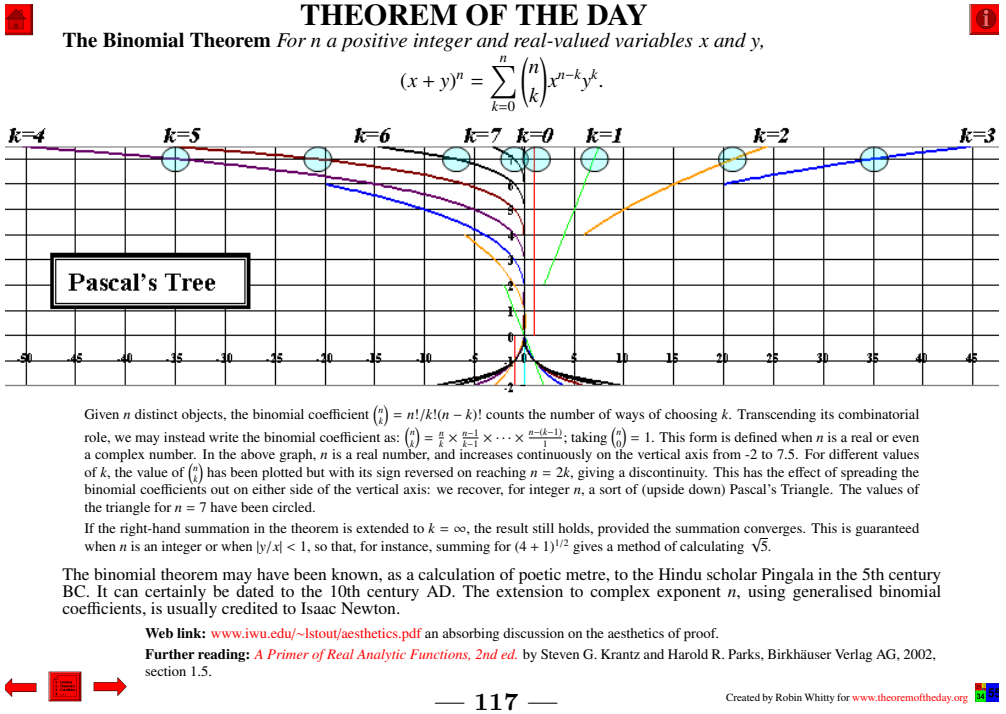
Corollary 31

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 246.



A little more arithmetic

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

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

YOUR PROOF: [a]

[a] Hint: Use Proposition 29 (on page 114) and the Binomial Theorem (Theorem 30 on page 116).

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 116),

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

   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 116) and Proposition 29 (on page 114),

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

   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:

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

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

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

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

The fact that the first part of Fermat's Little Theorem implies the second one will be proved later on (see page 214) .

Btw

1. The answer to the puzzle on page 14 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.

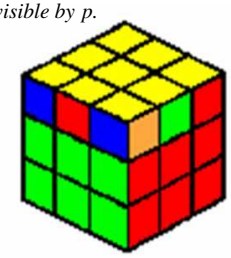
[a] For instance, to establish that a positive integer m is not prime one may proceed to find an integer i such that $i^m \not\equiv i \pmod{m}$.

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.

Go to Workout 10
on page 303

Negation

Negations are statements of the form

not P

or, in other words,

P is not the case

or

P is absurd

or

P leads to contradiction

or, in symbols,

$\neg P$

A first proof strategy for negated goals and assumptions:

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

Logical equivalences

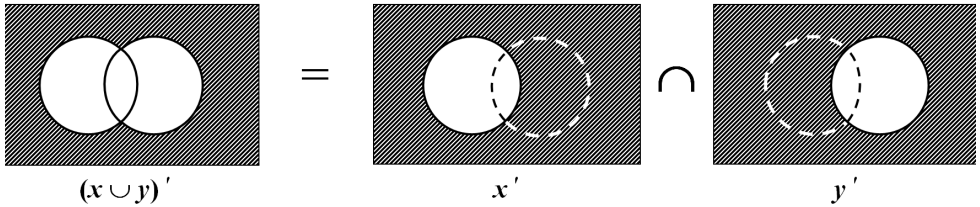
$$\begin{aligned}
\neg(P \Longrightarrow Q) &\iff P \;\&\; \neg Q \\
\neg(P \iff Q) &\iff \neg P \iff \neg Q \\
\neg(\forall x.\, P(x)) &\iff \exists x.\, \neg P(x) \\
\neg(P \;\&\; Q) &\iff (\neg P) \vee (\neg Q) \\
\neg(\exists x.\, P(x)) &\iff \forall x.\, \neg P(x) \\
\neg(P \vee Q) &\iff (\neg P) \;\&\; (\neg Q) \\
\neg(\neg P) &\iff P \\
\neg P &\iff (P \Rightarrow \mathbf{false})
\end{aligned}$$

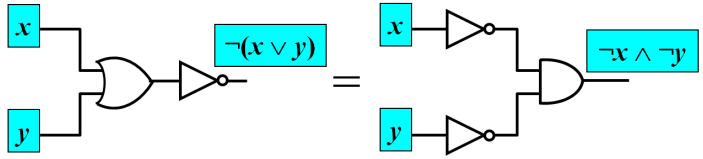
Go to Workout 11
on page 304

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	¬	$(x \vee y)$	$\neg x$	∧	$\neg y$
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 ×, 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.

Created by Robin Whitty for www.theoremoftheday.org

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

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

YOUR PROOF:

MY PROOF: Assume

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

Assume

$$\neg Q \quad ;$$

that is,

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

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: We prove the equivalent statement:

it is not the case that $\sqrt{2}$ is rational

by showing that the assumption

(i) $\sqrt{2}$ 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 41 on page 142 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) p_0 and q_0 are not both even

and

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

From (iii), one calculates that ${p_0}^2 = 2 \cdot {q_0}^2$ and, by Proposition 12 (on page 59), 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 12 (on page 59), that also q_0 is even; thereby contradicting assumption (ii). Hence, $\sqrt{2}$ is not rational.

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

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

Assume

(ii) P .

We need show Q.

Assume, by way of contradiction, that

(iii) $\neg Q$

holds.

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

(iv) $\neg P$

and now, from (ii) and (iv), we obtain a contradiction. Thus, $\neg Q$ cannot be the case; hence

Q

as required.

Corollary 40 *For all statements* P *and* Q*,*

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

Lemma 41 *A positive real number* x *is rational iff*

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

YOUR PROOF:

Go to Workout 12
on page 306

MY PROOF:

$(\Longleftarrow)$ Holds trivially.

$(\Longrightarrow)$ Assume that

(i) $\exists$ positive integers $a, b : \ x = a/b$.

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

(ii) $\forall$ positive integers $m, n :$

$$x = m/n \implies \exists \text{ prime } p : \ p \mid m \ \ \& \ \ p \mid n \ .$$

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

[a] Here we use three of the logical equivalences of page 127 (btw, which ones?) and the logical equivalence $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

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

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

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

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 201) 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*.

Number systems

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.

[a] aka hcf (highest common factor).

Complementary reading:

- ▶ 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.

Objectives

- Get an appreciation for the abstract notion of number system, considering four examples: natural numbers, integers, rationals, and modular integers.
- Prove the correctness of three basic algorithms in the theory of numbers: the division algorithm, Euclid's algorithm, and the Extended Euclid's algorithm.
- Exemplify the use of the mathematical theory surrounding Euclid's Theorem and Fermat's Little Theorem in the context of public-key cryptography.

Natural numbers

In the beginning there were the *natural numbers*

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

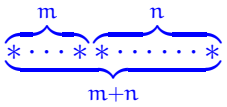
generated from *zero* by successive increment; that is, put in ML:

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

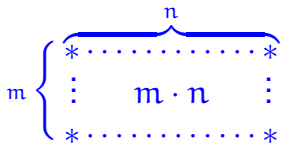
Remark This viewpoint will be looked at later in the course.

The basic operations of this number system are:

- Addition



- Multiplication



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

- Monoid laws

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

- Commutativity law

$$m + n = n + m$$

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

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

- Monoid laws

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

- Commutativity law

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

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

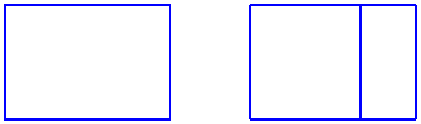
1. The booleans with $\mathbf{false}$ and disjunction.
2. The booleans with $\mathbf{true}$ and conjunction.
3. Lists with nil and concatenation.

While the first two above are commutative this is not generally the case for the latter.

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

- Distributive law

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



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

Cancellation

The additive and multiplicative structures of natural numbers further satisfy the following laws.

- Additive cancellation

  For all natural numbers k, m, n,

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

- Multiplicative cancellation

  For all natural numbers k, m, n,

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

Inverses

Definition 42

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

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

(i) the *integers*

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

which then form what in the mathematical jargon is referred to as a *commutative ring*, and

(ii) the *rationals* $\mathbb{Q}$ which then form what in the mathematical jargon is referred to as a *field*.

The division theorem and algorithm

Theorem 43 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$, $0 \leq r < n$, *and* $m = q \cdot n + r$.

Definition 44 *The natural numbers* q *and* r *associated to a given pair of a natural number* m *and a positive integer* n *determined by the Division Theorem are respectively denoted* $\mathrm{quo}(m, n)$ *and* $\mathrm{rem}(m, n)$.

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

The Division Algorithm in ML:

```
fun divalg( m , n )
  = let
      fun diviter( q , r )
        = if r < n then ( q , r )
          else diviter( q+1 , r-n )
    in
      diviter( 0 , m )
    end

fun quo( m , n ) = #1( divalg( m , n ) )

fun rem( m , n ) = #2( divalg( m , n ) )
```

Theorem 45 *For every natural number m and positive natural number n, the evaluation of $\texttt{divalg}(m, n)$ terminates, outputing a pair of natural numbers (q_0, r_0) such that $r_0 < n$ and $m = q_0 \cdot n + r_0$.*

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 worse 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

$$0 \leq q \;\&\; 0 \leq r \;\&\; m = q \cdot n + r$$

because

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

   $$0 \leq 0 \;\&\; 0 \leq m \;\&\; m = 0 \cdot n + m \;\;,$$

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

   $$0 \leq q \;\&\; n \leq r \;\&\; m = q \cdot n + r$$

   so that

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

   follows.

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

$$0 \leq q_0 \;\&\; 0 \leq r_0 \leq n \;\&\; m = q_0 \cdot n + r_0$$

as required.

Proposition 46 *Let m be a positive integer. For all integers k and l,*

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

YOUR PROOF:

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

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

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

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

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

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

and we are done.

Corollary 47 *Let m be a positive integer.*

1. *For every natural number n,*
$$n \equiv \operatorname{rem}(n,m) \pmod{m} \quad .$$
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 $n - \operatorname{rem}(n,m) = \operatorname{quo}(n,m) \cdot m$.

(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

$$\operatorname{rem}\big(k + |k| \cdot m\,,\,m\big) \quad .$$

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,

$$\begin{aligned} l &= \operatorname{rem}(l,m) \\ &= \operatorname{rem}(k,m) && \text{, by Proposition 46 (on page 163)} \\ &= \operatorname{rem}([k]_m,m) && \text{, by Proposition 46 (on page 163)} \\ &= [k]_m \end{aligned}$$

Go to Workout 13
on page 307

Modular arithmetic

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

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

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

$$k +_m l = [k+l]_m \quad , \quad k \cdot_m l = [k \cdot l]_m$$

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

Example 48 *The modular-arithmetic structure $(\mathbb{Z}_2, 0, +_2, 1, \cdot_2)$ is that of booleans with logical OR as addition and logical AND as multiplication.*

Example 49 *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 50 *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 51 *For all natural numbers $\mathfrak{m} > 1$, the modular-arithmetic structure*

$$(\mathbb{Z}_\mathfrak{m}, 0, +_\mathfrak{m}, 1, \cdot_\mathfrak{m})$$

is a commutative ring.

Remark The most interesting case of the omitted proof consists in establishing the associativity laws of addition and multiplication, for which see Workout 14.2 on page 309.

NB Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses (see page 230) .

Go to Workout 14
on page 309

Important mathematical jargon : Sets

Very roughly, sets are the mathematicians' datatypes. 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 $\mathbb{Z}_m$.

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 notation	$\forall x \in A.\, P(x)$ $\exists x \in A.\, P(x)$	is shorthand for	$\forall x.\, (x \in A \implies P(x))$ $\exists x.\, x \in A \;\&\; P(x)$

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. For the moment, we will just introduce some of its surrounding notation.

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

Definining 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

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

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

$$\forall a. \Big(a \in \{x \in A \mid P(x)\} \iff \big(a \in A \ \&\ P(a)\big) \Big)$$

by definition.

Example 52

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

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 53

1. $D(0) = \mathbb{N}$
2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 54, \\ 68, 72, 102, 153, 204, 306, 612, 918, 1224 \end{array} \right\}$

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

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

Example 54

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

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

Proposition 55 *For all natural numbers* l, m, *and* n,

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

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

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

We will prove that for all positive integers d,

$$\mathrm{d} \mid \mathrm{m} \ \&\ \mathrm{d} \mid \mathrm{n} \iff \mathrm{d} \mid \mathrm{m}' \ \&\ \mathrm{d} \mid \mathrm{n} \ .$$

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

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

and since, by (i), $\mathrm{m}' = \mathrm{k}_0 \cdot \mathrm{n} + \mathrm{m}$ for some integer k_0, it follows that $\mathrm{d} \mid \mathrm{m}'$. As $\mathrm{d} \mid \mathrm{n}$ by assumption, we have that d divides both m' and n.

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

Lemma 56 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $\mathrm{m} \equiv \mathrm{m}' \pmod{\mathrm{n}}$. *Then,*

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

YOUR PROOF:

Corollary 57

1. *For all natural numbers* m *and positive integers* n,
$$\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{CD}\big(\mathrm{rem}(\mathrm{m}, \mathrm{n}), \mathrm{n}\big) \ .$$
2. *For all natural numbers* m *and* n,
$$\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{CD}\big(\mathrm{q} - \mathrm{p}, \mathrm{p}\big)$$
where $\mathrm{p} = \min(\mathrm{m}, \mathrm{n})$ *and* $\mathrm{q} = \max(\mathrm{m}, \mathrm{n})$.

YOUR PROOF:

MY PROOF: The claim follows from the Key Lemma 56 (on page 185). Item (1) by Corollary 47 (on page 165), and item (2) because $l \equiv l - k \pmod{k}$ for all integers k and l.

Putting previous knowledge together we have:

Lemma 58 *For all positive integers m and n,*

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

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 59 ($\gcd(13,34)=1$)

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

Theorem 60 *Euclid's Algorithm* $\gcd$ *terminates on all pairs of positive integers and, for such* m *and* n, $\gcd(m,n)$ *is the greatest common divisor of* m *and* n *in the sense that the following two properties hold:*

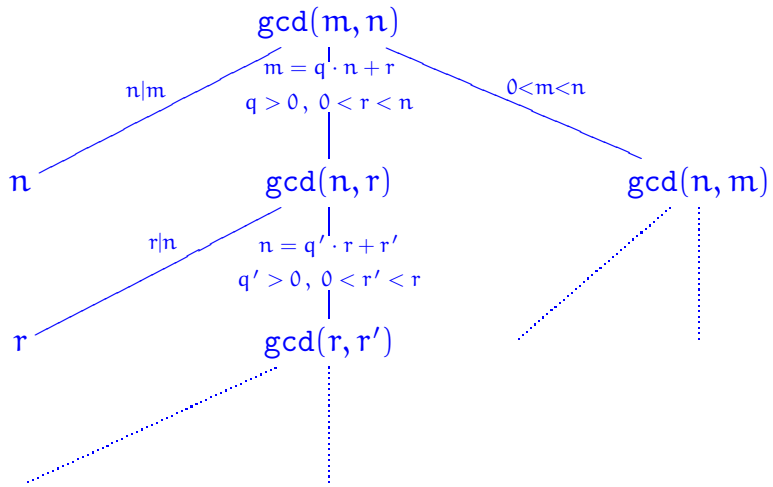
(i) *both* $\gcd(m,n) \mid m$ *and* $\gcd(m,n) \mid n$, *and*

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

YOUR PROOF:

MY PROOF: To establish the termination of $\gcd$ on a pair of positive integers (m,n) we consider and analyse the computations arising from the call $\gcd(m,n)$. For intuition, these can be visualised as on page 195.

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



Consider then $\gcd(m,n)$ where $m \geq n$. We have that $\gcd(m,n)$ 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 $\gcd(n,r)$.

In this latter case, the passage of computing $\gcd(m,n)$ by means of computing $\gcd(n,r)$ 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 $\gcd$s. For fun, we look into this next.

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

$$\max(m,n) > r = \max(r,r') > 0 \ .$$

For $n > m$, the same occurs with an extra computation step. As before, this process cannot go on for ever and the $\gcd$ algorithm necessarily terminates.

In the case that

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

one has that

$$m = q \cdot n + r < 2 \cdot q \cdot n = 2 \cdot (m - r)$$

and hence that

$$r < m/2 \ .$$

Thus, after 2 steps in the computation of $\gcd$ on inputs (m,n) satisfying $(\dagger)$, the first (and biggest) component m 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 $\gcd$ on a pair (m,n) is bounded by

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

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

As for the characterisation of $\gcd(m,n)$, 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 58 (on page 189) that

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

that is, in other words,

for all positive integers d,

$$d \mid m \ \&\ d \mid n \iff d \mid \gcd(m,n)$$

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

[a] Let me note for the record that a more precise complexity analysis involving *Fibonacci numbers* is also available. (See Workout 19.3a on page 320.)

NB Euclid's Algorithm (on page 189) and Theorem 60 (on page 193) 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 $\gcd$s should involve both. As a case in point, we will see that some properties of $\gcd$s 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.

Some fundamental properties of gcds

Corollary 61 *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:

Fractions in lowest terms

Here's our solution to the problem raised on page 145.

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

Homework Do Workout 15.7 on page 313.

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, for which see Workout 7.4 (on page 298).

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

Lemma 62 *For all positive integers* $\mathtt{l}$, $\mathtt{m}$, *and* $\mathtt{n}$,

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

YOUR PROOF:

[a] Aka (Distributivity).

MY PROOF: Let $\mathtt{l}$, $\mathtt{m}$, and $\mathtt{n}$ be positive integers.

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

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 60 (on page 193) tells us that $\gcd(\mathtt{m},\mathtt{n})$ is the positive integer precisely characterised by the following *universal property*:

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

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

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

(2) In a nutshell, the result follows because both $\gcd\big(\mathtt{l},\gcd(\mathtt{m},\mathtt{n})\big)$ and $\gcd(\gcd(\mathtt{l},\mathtt{m}),\mathtt{n})$ are the greatest common divisor of the triple of numbers $(\mathtt{l},\mathtt{m},\mathtt{n})$. 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 $\mathtt{d}$,

$$\begin{aligned}
&\mathtt{d} \mid \gcd\big(\mathtt{l},\gcd(\mathtt{m},\mathtt{n})\big)\\
&\iff \mathtt{d} \mid \mathtt{l}\ \&\ \mathtt{d} \mid \gcd(\mathtt{m},\mathtt{n})\\
&\iff \mathtt{d} \mid \mathtt{l}\ \&\ \mathtt{d} \mid \mathtt{m}\ \&\ \mathtt{d} \mid \mathtt{n}\\
&\iff \mathtt{d} \mid \gcd(\mathtt{l},\mathtt{m})\ \&\ \mathtt{d} \mid \mathtt{n}\\
&\iff \mathtt{d} \mid \gcd(\gcd(\mathtt{l},\mathtt{m}),\mathtt{n})
\end{aligned}$$

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

(3) One way to prove the result is to note that the linearity of `divalg`, for which see Workout 13.4 (on page 307), transfers to Euclid's `gcd` Algorithm. This is because

- every computation step

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

  corresponds to a computation step

  $\mathtt{gcd}(\mathtt{l}\cdot\mathtt{m},\mathtt{l}\cdot\mathtt{n}) = \mathtt{l}\cdot\mathtt{n}$,
  which happens when $\mathtt{l}\cdot\mathrm{rem}(\mathtt{m},\mathtt{n}) = \mathrm{rem}(\mathtt{l}\cdot\mathtt{m},\mathtt{l}\cdot\mathtt{n}) = 0$
  i.e. when $\mathrm{rem}(\mathtt{m},\mathtt{n}) = 0$

[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.

while

- every computation step

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

  corresponds to a computation step

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

  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 $\gcd(m,n)$ leads to a sequence of calls to $\gcd$ with

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

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

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

(i) $l\cdot\gcd(m,n) \mid \gcd(l\cdot m, l\cdot n)$.

(ii) $\gcd(l\cdot m, l\cdot n) \mid l\cdot\gcd(m,n)$.

For (i), since $\gcd(m,n) \mid m$ & $\gcd(m,n) \mid n$ we have that $l\cdot\gcd(m,n) \mid l\cdot m$ & $l\cdot\gcd(m,n) \mid l\cdot n$ 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 $l\cdot k_0 = \gcd(l\cdot m, l\cdot n) \mid l\cdot m$ & $l\cdot k_0 = \gcd(l\cdot m, l\cdot n) \mid l\cdot n$ we have that $k_0 \mid m$ & $k_0 \mid n$, and so that $k_0 \mid \gcd(m,n)$. Finally, then, $\gcd(l\cdot m, l\cdot n) = l\cdot k_0 \mid l\cdot\gcd(m,n)$.

Go to Workout 15
on page 311

Euclid's Theorem

Theorem 63 *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 62.3 on page 204), 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 64 (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 122) follows as a corollary of the first part and Euclid's Theorem.

YOUR PROOF OF Theorem 36.2 (on page 122):

MY PROOF OF Theorem 36.2 (on page 122): 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 64 on the previous page) that $p \mid (i^{p-1} - 1)$.

Fields of modular arithmetic

Corollary 65 *For prime p, every non-zero element i of $\mathbb{Z}_p$ has i^{p-2} 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.

Go to Workout 16
on page 315

Extended Euclid's Algorithm

Example 66 ($\mathrm{egcd}(34,13) = ((5,-13),1)$)

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

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

Linear combinations

Definition 67 *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

$$s \cdot m + t \cdot n = r \ .$$

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 68 *For all positive integers* m *and* n*,*

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

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

can be efficiently computed.

The proof of Theorem 68, which is left as an exercise for the interested reader, is by means of the Extended Euclid's Algorithm egcd on page 224 relying on the following elementary properties of linear combinations.

Proposition 69 *For all integers* m *and* n*,*

1. $\begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = m \ \ \& \ \ \begin{bmatrix} 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} m \\ n \end{bmatrix} = n$;
2. *for all integers* s_1, t_1, r_1 *and* s_2, t_2, r_2,

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

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,

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

egcd (*with* divalg)

```
fun egcd( m , n )
= let
    fun egcditer( ((s1,t1),r1) , lc as ((s2,t2),r2) )
    = let
        val (r,q) = 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 70 ($\mathtt{egcd}(13,34) = ((-13,5),1)$**)**

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


```
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 71 *For all distinct positive integers* m *and* n*,*

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

Another characterisation of gcds

Theorem 72 *For all positive integers* m *and* n, $\gcd(\mathrm{m},\mathrm{n})$ *is the least positive linear combination of* m *and* n.

YOUR PROOF:

MY PROOF: Let m and n be arbitrary positive integers. By Theorem 68.1 (on page 222), $\gcd(\mathrm{m},\mathrm{n})$ is a linear combination of m and n. Furthermore, since it is positive, by Corollary 61.1 (on page 202), it is the least such.

Multiplicative inverses in modular arithmetic

Corollary 73 *For all positive integers* m *and* n,

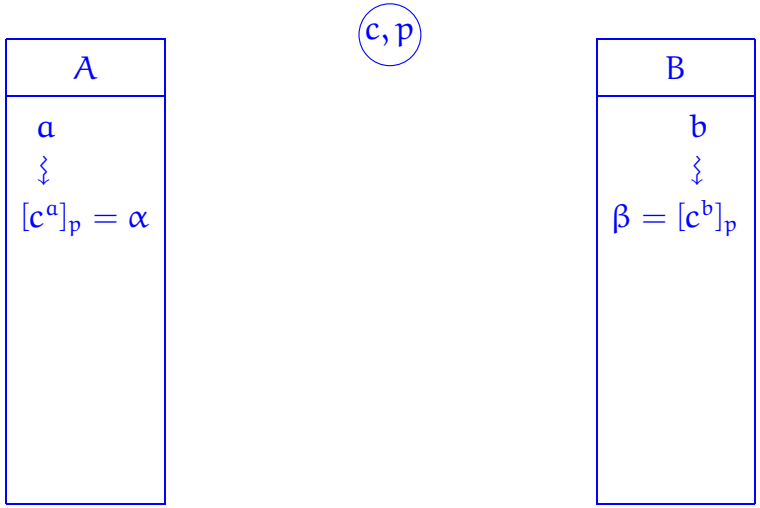
1. $\mathrm{n}\cdot \mathrm{lc}_2(\mathrm{m},\mathrm{n}) \equiv \gcd(\mathrm{m},\mathrm{n}) \pmod{\mathrm{m}}$, *and*
2. *whenever* $\gcd(\mathrm{m},\mathrm{n}) = 1$,

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

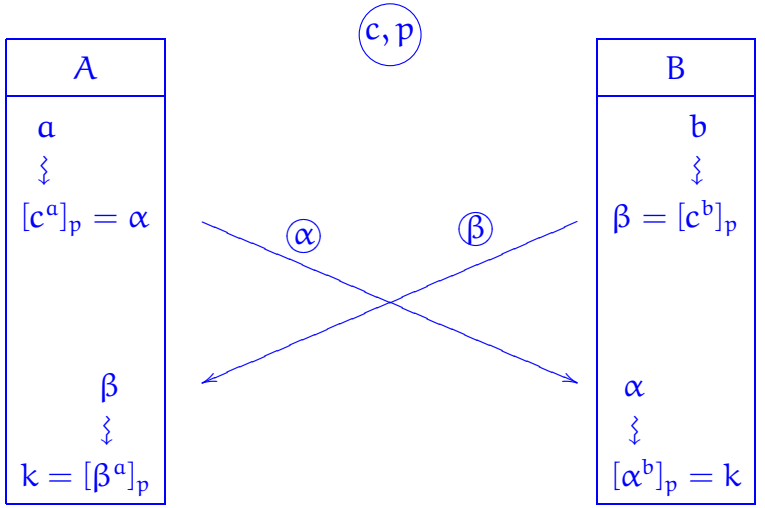
Remark For every pair of positive integers m and n, we have that $[\mathrm{n}]_{\mathrm{m}}$ has a multiplicative inverse in $\mathbb{Z}_{\mathrm{m}}$ iff $\gcd(\mathrm{m},\mathrm{n}) = 1$.

Go to Workout 17
on page 316

Shared secret key



Shared secret key



Key exchange

Lemma 74 *Let p be a prime and e a positive integer with $\gcd(p-1, e) = 1$. Define*

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

Then, for all integers k,

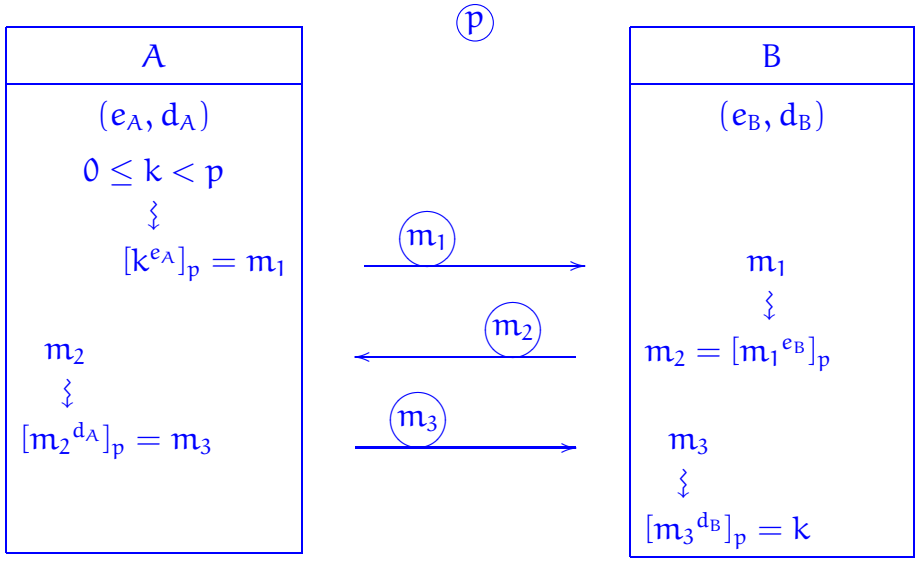
$$(k^e)^d \equiv k \pmod{p} .$$

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.



Go to Workout 18
on page 318

Mathematical structure

Topics

Mathematical induction: Principles of Induction and Strong Induction. Binomial Theorem and Pascal's Triangle. Fermat's Little Theorem. Fundamental Theorem of Arithmetic. Infinity of primes.

Complementary reading:

- Chapters 1, 24, 25, 30, and 31 of *How to Think Like a Mathematician* by K. Houston.
- Chapters 4 to 7 of *Mathematics for Computer Science* by E. Lehman, F. T. Leighton, and A. R. Meyer.
- Chapters 4 to 7 of *How to Prove it* by D. J. Velleman.

Objectives

- To understand and be able to proficiently use the Principle of Mathematical Induction in its various forms.

Mathematical induction

We have mentioned in passing on page 149 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

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

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:

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

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 254), 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

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \quad . \qquad (\ddagger)$$

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:

$$
\begin{aligned}
&\textstyle\sum_{k=0}^{n+1} \binom{n+1}{k} \cdot x^{(n+1)-k} \cdot y^k \\
&= x^{n+1} + \textstyle\sum_{k=1}^{n} \binom{n+1}{k} \cdot x^{n-k+1} \cdot y^k + y^{n+1} \\
&= x^{n+1} + \textstyle\sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) \cdot x^{n-k+1} \cdot y^k + y^{n+1} \\
&\qquad \text{, provided the conjecture } (\ddagger) \text{ is true!} \\
&= x^{n+1} + \textstyle\sum_{k=1}^{n} \binom{n}{k} \cdot x^{n-k+1} \cdot y^k + \sum_{k=1}^{n} \binom{n}{k-1} \cdot x^{n-k+1} \cdot y^k + y^{n+1} \\
&= \textstyle\sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k+1} \cdot y^k + \sum_{j=0}^{n} \binom{n}{j} \cdot x^{n-j} \cdot y^{j+1} \\
&= \left(\textstyle\sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k \right) \cdot x + \left(\sum_{j=0}^{n} \binom{n}{j} \cdot x^{n-j} \cdot y^j \right) \cdot y \\
&= \left(\textstyle\sum_{i=0}^{n} \binom{n}{i} \cdot x^{n-i} \cdot y^i \right) \cdot (x+y) \\
&= (x+y)^n \cdot (x+y) \quad \text{, by the Induction Hypothesis } (\mathrm{IH}) \\
&= (x+y)^{n+1}
\end{aligned}
$$

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.

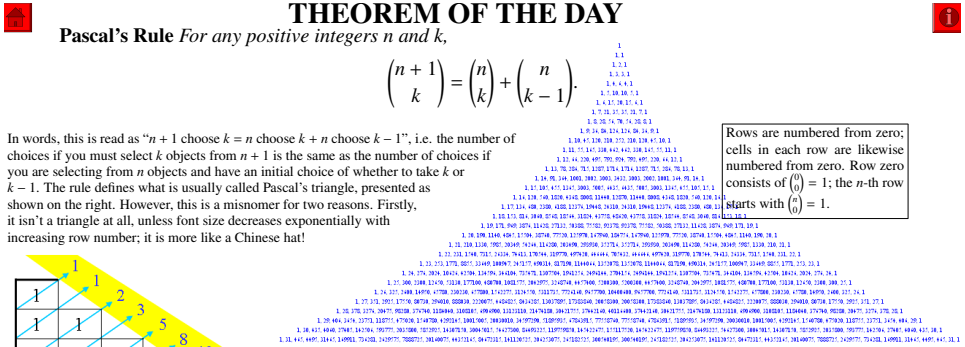
Btw Note that our proof works in any commutative semiring!

THEOREM OF THE DAY

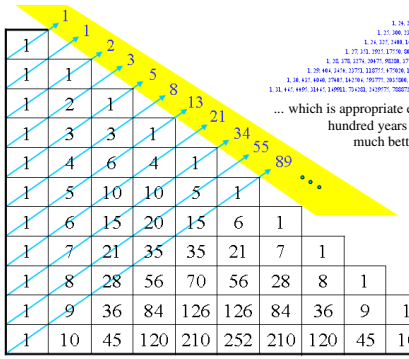
Pascal's Rule *For any positive integers n and k,*

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

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!



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 $\binom{n}{0} = 1$.



... 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 120) that we used to prove the first part of Fermat's Little Theorem (Theorem 36.1 on page 122) 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

(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.

Go to Workout 19
on page 319

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

then

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

hold, then

- $\forall m \geq \ell \text{ in } \mathbb{N}.\, P(m)$ 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 75 *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 $n \geq 2$,

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

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

(SIH) for all natural numbers $2 \leq k \leq n$,
either k is prime or a product of primes .

We will now prove that

either $n+1$ is a prime or a product of primes . $(\dagger)$

by cases (see page 105).

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 76 (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*

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

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 $i \in [1..\ell]$. $\quad (\dagger)$

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 64 on page 214), 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 $\prod(p_2, \ldots, p_\ell) = \prod(q_2, \ldots, q_k)$, and by iteration of this argument that $p_i = q_i$ for all $1 \leq i \leq \min(\ell, k)$. But, ℓ cannot be greater than k because otherwise one would have $\prod(p_{k+1}, \ldots, p_\ell) = 1$, 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 273 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

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

By arguments as above, it follows that

$$p_1 = q_1$$

and hence that

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

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 $i \in [1..\ell]$.

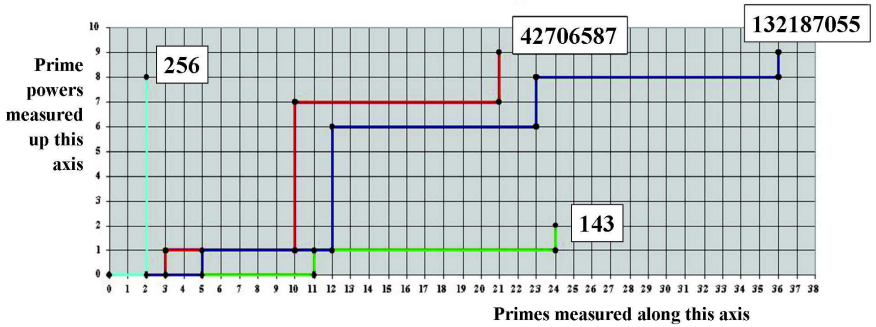
2. Prove $(*)$ above by the Principle of Induction (from basis 1), and compare your proof with mine for $(\ddagger)$.

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

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.

Created by Robin Whitty for www.theoremoftheday.org

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 77

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

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

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

Example 78

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

Go to Workout 20
on page 321

Euclid's infinitude of primes

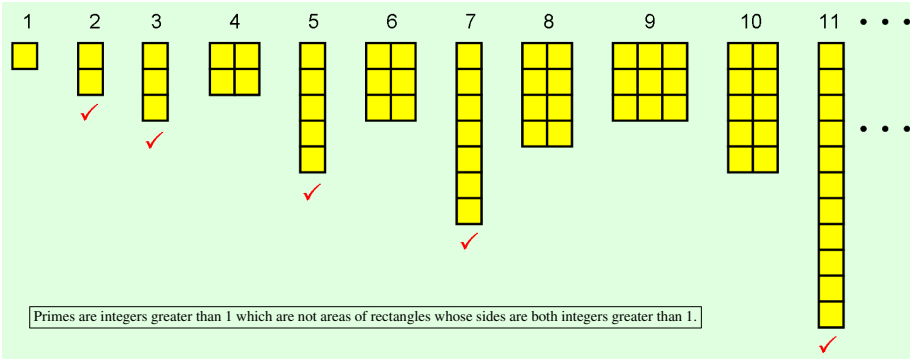
Theorem 79 *The set of primes is infinite.*

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 75), 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 $p_i \mid (p_1 \cdot \ldots \cdot p_\ell)$, 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

Workouts
for Part IA CST 2013/14

Discrete Mathematics For Computer Science

<cl.cam.ac.uk/teaching/1314/DiscMath>

Prof Marcelo Fiore
Marcelo.Fiore@cl.cam.ac.uk

Workout 1
from page 44

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

Prove or disprove the following statements.

1. The product of two even natural numbers is even.
2. The product of an even and an odd natural number is odd.
3. If $x > 3$ and $y < 2$ then $x^2 - 2 \cdot y > 5$.

Workout 2
from page 51

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

Prove or disprove the following statements.

1. Suppose n is a natural number larger than 2, and n is not a prime number. Then $2 \cdot n + 13$ is not a prime number.
2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Workout 3
from page 62

1. Characterise those integers d and n such that:
   (a) $0 \mid n$,
   (b) $d \mid 0$.
2. Write an ML function

   ```
   divides:  int * int -> bool
   ```

   such that, for all integers m and n, `divides(m,n) = true` iff $m \mid n$ holds.

   Note that the function

   ```
   fn (m,n) => ( n div m ) = 0
   ```

   will not do.
3. Let n be a natural number. Show that $n \mid n$.

Workout 4
from page 65

1. Let i, j be integers and let m be a positive integer. Show that:
   (a) $i \equiv i \pmod{m}$
   (b) $i \equiv j \pmod{m} \implies j \equiv i \pmod{m}$
   (c) $i \equiv j \pmod{m} \implies i^2 \equiv j^2 \pmod{m}$
2. Find integers i, j, natural numbers k, l, and a positive integer m for which both $i \equiv j \pmod{m}$ and $k \equiv l \pmod{m}$ hold while $i^k \equiv j^l \pmod{m}$ does not.

3. Find an integer i, natural numbers k, l, and a positive integer m for which $k \equiv l \pmod{m}$ holds while $i^k \equiv i^l \pmod{m}$ does not.
4. Formalise and prove the following statement: A natural number is a multiple of 3 iff so is the number obtained by summing its digits. What about multiples of 9? And multiples of 11?

Workout 5
from page 67

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

1. Prove or disprove that, for an integer n, n^2 is even if and only if n is even.

2. Show that for all integers d and n the following statements are equivalent:
   (a) $d \mid n$.
   (b) $-d \mid n$.
   (c) $d \mid -n$.
   (d) $-d \mid -n$.
3. Let k, m, n be integers with k positive. Show that:
   $$(k \cdot m) \mid (k \cdot n) \iff m \mid n \quad .$$

Workout 6
from page 75

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

1. Prove or disprove the following statements.
   (a) For real numbers a and b, if $0 < a < b$ then $a^2 < b^2$.
   (b) For real numbers a, b, and c with $a > b$, if $a \cdot c \leq b \cdot c$ then $c \geq 0$.
2. Prove or disprove that for all natural numbers n, $2 \mid 2^n$.

Workout 7
from page 83

1. Taking inspiration from the proof of Theorem 20 (on page 81), or otherwise, prove that for all integers n,

$$30 \mid n \iff \big(2 \mid n \;\&\; 3 \mid n \;\&\; 5 \mid n\big) \quad .$$

   Can you spot a pattern here? Can you formalise it, test it, and prove it?
2. Find a counterexample to the statement: For all positive integers k, m, n, if $m \mid k$ & $n \mid k$ then $(m \cdot n) \mid k$.

3. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the derived statement

$$P^{\#}(m) \;=\; \forall \text{ integer } k.\ 0 \leq k \leq m \implies P(k)$$

   again for m ranging over the natural numbers.
   Prove the following equivalences:

$$\begin{aligned} P^{\#}(0) &\iff P(0) \\ \big(P^{\#}(n) \implies P^{\#}(n+1)\big) &\iff \big(P^{\#}(n) \implies P(n+1)\big) \\ \big(\forall m \in \mathbb{N}.\, P^{\#}(m)\big) &\iff \big(\forall m \in \mathbb{N}.\, P(m)\big) \end{aligned}$$

3. Show that for all integers l, m, n,

$$l \mid m \;\&\; m \mid n \implies l \mid n \quad .$$

4. Prove that for all integers d, k, l, m, n,
   (a) $d \mid m \;\&\; d \mid n \implies d \mid (m+n)$,
   (b) $d \mid m \implies d \mid k \cdot m$,
   (c) $d \mid m \;\&\; d \mid n \implies d \mid (k \cdot m + l \cdot n)$.
5. Prove that for all integers i, j, k, l, m, n with m positive and n nonnegative,
   (a) $i \equiv j \pmod m \;\&\; j \equiv k \pmod m \implies i \equiv k \pmod m$
   (b) $i \equiv j \pmod m \;\&\; k \equiv l \pmod m \implies i + k \equiv j + l \pmod m$
   (c) $i \equiv j \pmod m \;\&\; k \equiv l \pmod m \implies i \cdot k \equiv j \cdot l \pmod m$
   (d) $i \equiv j \pmod m \implies i^n \equiv j^n \pmod m$

Workout 8
from page 97

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

Prove or disprove the following statements.

1. For every real number x, if $x > 0$ then there is a real number y such that $y(y+1) = x$.
2. For all real numbers x and y there is a real number z such that $x + z = y - z$.

3. For all integers x and y there is an integer z such that $x + z = y - z$.
4. For every real number x, if $x \neq 2$ then there is a unique real number y such that $2y/(y+1) = x$.
5. The addition of two rational numbers is a rational number.
6. Prove that for all natural numbers p, p_1, p_2,
   (a) $\min(p, p_1 + p_2) = \min\big(p, \min(p, p_1) + \min(p, p_2)\big)$, and
   (b) $\min(p, p_1 + p_2) = \min(p, p_1) + \min\big(p - \min(p, p_1), p_2\big)$.

Workout 9
from page 104

NB The main aim here is for you to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements), and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

1. Prove or disprove that for integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

2. If every pair of people in a group has met, then we will call the group a *club*. If every pair of people in a group has not met, then we will call it a group of *strangers*.
   Prove that every collection of 6 people includes a club of 3 people or a group of 3 strangers.
3. Show that for all integers m and n,
   $$m \mid n \;\&\; n \mid m \implies m = n \vee m = -n \ .$$
4. Prove or disprove that for all positive integers k, m, n,
   if $k \mid (m \cdot n)$ then $k \mid m$ or $k \mid n$.
5. Prove that for all integers n, there exist natural numbers i and j such that $n = i^2 - j^2$ iff either $n \equiv 0 \pmod 4$, or $n \equiv 1 \pmod 4$, or $n \equiv 3 \pmod 4$. [Hint: Recall Proposition 22 (on page 89).]

Workout 10
from page 125

1. Search for “Fermat’s Little Theorem” in YouTube and watch a video or two about it.
2. Let i and n be positive integers and let p be a prime. Show that if $n \equiv 1 \pmod{p-1}$ then $i^n \equiv i \pmod{p}$ for all i not multiple of p.

$$(P_1 \implies (P_2 \implies Q)) \iff ((P_1 \;\&\; P_2) \implies Q)$$
$$(P \iff Q) \iff ((P \implies Q) \;\&\; (Q \implies P))$$

by means of truth tables, where the truth tables for the boolean statements are:

P	Q	$P \implies Q$	$P \iff Q$	$P \;\&\; Q$	$P \vee Q$	$\neg P$
true	**true**	**true**	**true**	**true**	**true**	**false**
false	**true**	**true**	**false**	**false**	**true**	**true**
true	**false**	**false**	**false**	**false**	**true**	
false	**false**	**true**	**true**	**false**	**false**	

Workout 11
from page 128

Justify the boolean equivalences:

$$\begin{aligned}
\neg(P \implies Q) &\iff P \;\&\; \neg Q \\
\neg(P \iff Q) &\iff \neg P \iff \neg Q \\
\neg(P \;\&\; Q) &\iff (\neg P) \vee (\neg Q) \\
\neg(P \vee Q) &\iff (\neg P) \;\&\; (\neg Q) \\
\neg(\neg P) &\iff P \\
\neg P &\iff (P \implies \mathbf{false}) \\
(P \implies Q) &\iff (\neg Q \implies \neg P) \\
(\mathbf{false} \implies P) &\iff \mathbf{true}
\end{aligned}$$

Workout 12
from page 141

Give three justifications for the following scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$

$\vdots$

After using the strategy

Assumptions	Goal
	contradiction

$\vdots$

$P \;,\; \neg Q$

Workout 13
from page 168

1. Show that for every integer n, the remainder when n^2 is divided by 4 is either 0 or 1.
2. Write the division algorithm in imperative code.
3. Prove that for all natural numbers k, l, and positive integer m,
   (a) $\text{rem}(k + l, m) = \text{rem}\big(k + \text{rem}(l, m), m\big)$, and
   (b) $\text{rem}(k \cdot l, m) = \text{rem}\big(k \cdot \text{rem}(l, m), m\big)$.
4. Prove the following Linearity Property of the Division Algorithm: for all positive integers k, m, n,
   $\texttt{divalg}(k \cdot m, k \cdot n) = \big(k \cdot \text{quo}(m, n), k \cdot \text{rem}(m, n)\big)$.

5. Prove the General Division Theorem for integers:
   For every integer m and non-zero integer n, there exists a unique pair of integers q and r such that $0 \leq r < |n|$, and $m = q \cdot n + r$.
6. Prove that for all positive integers m and n,
   (a) $n < m \implies \text{quo}(n, m) = 0$ & $\text{rem}(n, m) = n$, and
   (b) $n \leq m \implies \text{rem}(m, n) < m/2$.

Workout 14
from page 175

1. Calculate that $2^{153} \equiv 53 \pmod{153}$.
   Btw, at first sight this seems to contradict Fermat's Little Theorem, why isn't this the case though?
2. Let m be a positive integer.
   (a) Prove the associativity of the addition and multiplication operations in $\mathbb{Z}_m$; that is, that for all i, j, k in $\mathbb{Z}_m$,
   $(i +_m j) +_m k = i +_m (j +_m k)$, and
   $(i \cdot_m j) \cdot_m k = i \cdot_m (j \cdot_m k)$.
   [Hint: Use Workout 13.3 on page 307.]

   (b) Prove that the additive inverse of k in $\mathbb{Z}_m$ is $[-k]_m$.
3. Calculate the addition and multiplication tables, and the additive and multiplicative inverses tables for $\mathbb{Z}_3$, $\mathbb{Z}_6$, and $\mathbb{Z}_7$. Can you spot any patterns?

Workout 15
from page 211

1. Write Euclid's Algorithm in imperative code.
2. Calculate the set $\mathrm{CD}(666, 330)$ of common divisors of 666 and 330.
3. Show that for all integers k, the conjuction of the two statements
   - $k \mid m \;\&\; k \mid n$, and
   - for all positive integers d, $d \mid m \;\&\; d \mid n \implies d \mid k$

   is equivalent to the single statement

   for all positive integers d, $d \mid m \;\&\; d \mid n \iff d \mid k$.

4. Prove that for all positive integers m and n,

$$\gcd(m, n) = m \iff m \mid n \ .$$

5. Prove that, for all positive integers m and n, and integers k and l,

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

6. Prove that, for all positive integers m and n, there exist integers k and l such that $k \cdot m + l \cdot n = 1$ iff $\gcd(m, n) = 1$.

7. For all positive integers m and n, define

$$m' = \frac{m}{\gcd(m,n)} \quad \text{and} \quad n' = \frac{n}{\gcd(m,n)} \ .$$

   Prove that

   (a) m' and n' are positive integers, and that

   (b) $\gcd(m', n') = 1$.

   Conclude that the representation in lowest terms of the fraction m/n is m'/n'.

8. Use the Key Lemma 56 (on page 185) to show the correctness of the following algorithm

```
fun gcd0( m , n )
  = if m = n then m
    else
      let
        val p = min(m,n) ; val q = max(m,n)
      in
        gcd0( p , q - p )
      end
```

   for computing the $\gcd$ of two positive integers. Give an analysis of the time complexity.

Workout 16
from page 217

1. Revisit Theorem 20 (on page 81) and Workout 7.1 (on page 297) using Euclid's Theorem (Corollary 64 on page 64) to give new proofs for them. Can you now state and prove a general result from which these follow?

4. Prove that for all positive integers l, m, and n, if $\gcd(l, m \cdot n) = 1$ then $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$.

5. Prove that for all integers n and primes p, if $n^2 \equiv 1 \pmod{p}$ then either $n \equiv 1 \pmod{p}$ or $n \equiv -1 \pmod{p}$.

6. (a) Show that the $\gcd$ of two linear combinations of positive integers m and n is itself a linear combination of m and n.

   (b) Argue that the output $((s, t), r)$ of calling `egcditer` with input

   $$\Big(\big((s_1, t_1),\, s_1 \cdot m + t_1 \cdot n\big),\ \big((s_2, t_2),\, s_2 \cdot m + t_2 \cdot n\big) \Big)$$

   is such that

   $$\gcd\big(s_1 \cdot m + t_1 \cdot n,\, s_2 \cdot m + t_2 \cdot n\big) = r = s \cdot m + t \cdot n \quad .$$

Workout 17
from page 231

1. Write the Extended Euclid's Algorithm in imperative code.

2. Prove Theorem 68 (on page 222).

3. Let m and n be positive integers with $\gcd(m, n) = 1$. Prove that for every natural number k,

   $$m \mid k \ \&\ n \mid k \implies (m \cdot n) \mid k \quad .$$

Workout 18
from page 236

1. Search for "Diffie-Hellman Key Exchange" in YouTube and watch a video or two about it.

Workout 19
from page 258

1. State the Principle of Induction for the ML

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

2. Establish the following:
   (a) For all positive integers m and n,
   $$(2^n - 1) \cdot \sum_{i=0}^{m-1} 2^{i \cdot n} = 2^{m \cdot n} - 1 \quad .$$
   (b) Suppose k is a positive integer that is not prime. Then $2^k - 1$ is not prime.

3. Recall that the Fibonacci numbers F_n for n ranging over the natural numbers are defined by $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.
   (a) Prove that $\gcd(F_{n+1}, F_n)$ terminates in $n + 1$ steps for all natural numbers n.
   (b) Prove that for all natural numbers n,
   $$F_n \cdot F_{n+2} = {F_{n+1}}^2 + (-1)^n \quad .$$

Workout 20
from page 282

1. Equation $(\star)$ on page 281 gives a *Transfer Principle* of additive properties of $\min$ as multiplicative properties of $\gcd$. To see this, prove that for all positive integers m, m_1, m_2,
   (a) $\gcd(m, m_1 \cdot m_2) = \gcd\big(m, \gcd(m, m_1) \cdot \gcd(m, m_2)\big)$, and
   (b) $\gcd(m, m_1 \cdot m_2) = \gcd(m, m_1) \cdot \gcd\left(\frac{m}{\gcd(m, m_1)}, m_2\right)$.
   [Hint: Use Workout 8.6 on page 300.]

2. Give two proofs of the following proposition

   For all positive integers m, n, p, q such that $\gcd(m, n) = \gcd(p, q) = 1$, if $m \cdot q = p \cdot n$ then $m = p$ and $n = q$.

   respectively using Theorem 63 and Equation $(\star)$ on page 281.