Slides

for Part IA CST 2021/22

Discrete Mathematics

<www.cl.cam.ac.uk/teaching/2122/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

What are we up to?

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

What is it that we do ?

In general:

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

In particular:

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

Lecture plan

I. Proofs.

II. Numbers.

III. Sets.

IV. Regular languages and finite automata.

Proofs

Objectives

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

Proofs in practice

We are interested in examining the following statement:

The product of two odd integers is odd.

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

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

More precisely put, we may write:

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

which further presupposes that you know:

- what variables are;
- what

  if . . . then . . .

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

Even more precisely, we should write

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

which now additionally presupposes that you know:

- what

  for all . . .

  statements are, and how one goes about proving them.

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

Some mathematical jargon

Statement

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

Example 1

$$\text{‘}e^{i\pi} + 1 = 0\text{’}$$

Non-example

‘This statement is false’

Predicate

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

Example 2

1. '$e^{ix} = \cos x + i \sin x$'

2. *'the function f is differentiable'*

Theorem

A very important true statement.

Proposition

A less important but nonetheless interesting true statement.

Lemma

A true statement used in proving other true statements.

Corollary

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

Example 3

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

Conjecture

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

Example 4

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

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.

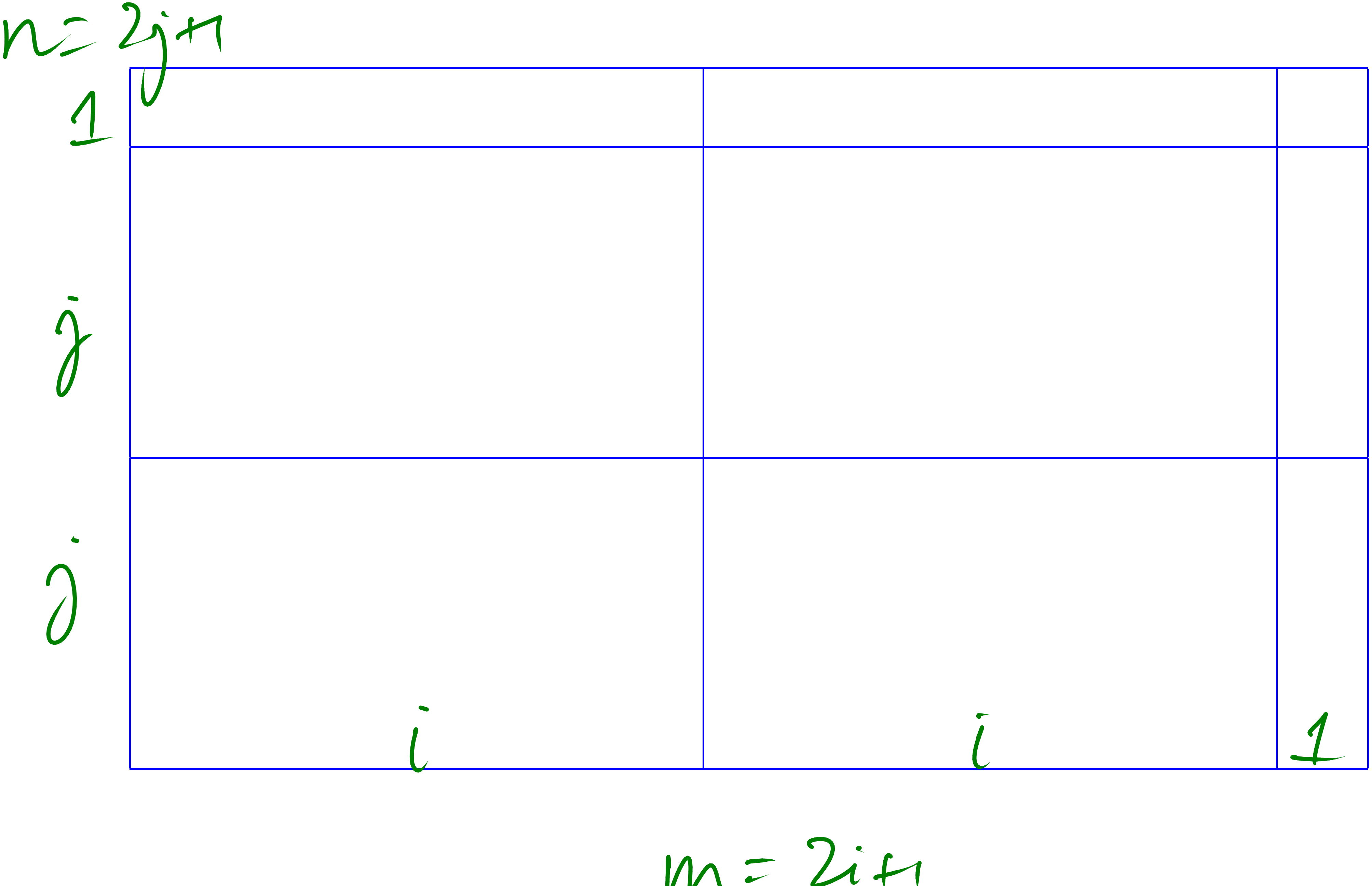
Definition, theorem, intuition, proof in practice

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* $m \cdot n$.

$$m \cdot n = (2i+1)(2j+1) = \ldots\ldots = 2(\ldots)+1$$

Intuition:



PROOF OF Proposition 8:

Let m and n be odd integers.

That is, $m = 2i+1$ for some int. i; and

$n = 2j+1$ for some int. j.

Consider

$$m \cdot n = (2i+1)\cdot(2j+1)$$

$$= 4ij + 2i + 2j + 1$$

$$= 2(2ij + i + j) + 1$$

Hence $m \cdot n$ is of the form $2k+1$ for k the

the integer $2ij+i+j$ is odd and so odd. $\boxtimes$

Simple and composite statements

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

Examples:

‘2 is a prime number’

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

Implication

Theorems can usually be written in the form

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

or, in other words,

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

or, in symbols,

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

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

The main proof strategy for implication:

To prove a goal of the form

$$P \implies Q$$

assume that P is true and prove Q.

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

Proof pattern:

In order to prove that

$$P \implies Q$$

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

Scratch work:

Before using the strategy

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

After using the strategy

Assumptions	Goal
	Q
$\vdots$	
P	

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

PROOF:

Assume m and n are odd integers

RTP: m·n is an integer.

So m = 2i+1 for int. i

n = 2j+1 for int. j

An alternative proof strategy for implication:

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

Definition:

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

Proof pattern:

In order to prove that

$$P \implies Q$$

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

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$
⋮	

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* $\sqrt{x}$*.*

PROOF:

Assume x is irrational

RTP: $\sqrt{x}$ is irrational

x is not of the form m/n for int. m and n.

By the contrapositive, we need show

$\sqrt{x}$ rational $\Rightarrow$ x rational

Assume $\sqrt{x}$ rational, that is, of the form p/q for integers p and q.

RTP: x rational, that is, of the form m/n for int. m and n.

Since $\sqrt{x} = p/q$

Then $x = p^2/q^2$ and we are done. $\boxtimes$

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* $P_1 \implies P_3$.

PROOF:

Assume (1) $P_1 \Rightarrow P_2$ and (2) $P_2 \Rightarrow P_3$

RTP: $P_1 \Rightarrow P_3$.

Assume: (3) P_1

RTP: P_3

From (1) and (3), by MP, we have (4) P_2

From (2) and (4), by MP, we have P_3 as required ☒

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

P iff Q

or, in symbols,

$$P \iff Q$$

Proof pattern:

In order to prove that

$$P \iff Q$$

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

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

PROOF: Let n be an integer.

($\Rightarrow$) RTP: n even $\Rightarrow$ n^2 even

Assume n even; that is, of the form 2i for an integer i.

RTP: n^2 even

We have $n^2 = (2i)^2 = 2(2i^2)$

and so n^2 is even.

($\Leftarrow$) n^2 even $\Rightarrow$ n even

Equivalently, by the contrapositive, we show

n odd $\Rightarrow$ n^2 odd.

This is so as a corollary of the establish fact that

i, j odd $\Rightarrow$ $i \cdot j$ odd

$\boxtimes$

Divisibility

a predicate, not an operation.

a divides b and write $a|b$

iff def $b = a \cdot k$ for some int. k