Proofs

Objectives

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

Proofs in practice

We are interested in examining the following statement:

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

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

Proofs in practice

We are interested in examining the following statement:

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

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

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

More precisely put, we may write:

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

More precisely put, we may write:

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

which further presupposes that you know:

- what variables are;
- what

  if . . . then . . .

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

Even more precisely, we should write

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

which now additionally presupposes that you know:

- what

  for all . . .

  statements are, and how one goes about proving them.

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

Some mathematical jargon

Statement

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

Example 1

$$\text{‘}e^{i\pi} + 1 = 0\text{’}$$

Non-example

‘This statement is false’

Predicate

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

Example 2

1. ‘$e^{ix} = \cos x + i \sin x$’

2. *‘the function f is differentiable’*

Theorem

A very important true statement.

Proposition

A less important but nonetheless interesting true statement.

Lemma

A true statement used in proving other true statements.

Corollary

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

Example 3

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

Proof

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

Proof

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

Logic

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

Example 5

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

Axiom

A basic assumption about a mathematical situation.

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

Example 6

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

Definition

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

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

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

Definition, theorem, intuition, proof in practice

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

Definition, theorem, intuition, proof in practice

Definition 7 *An integer is said to be 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* $m \cdot n$*.*

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.

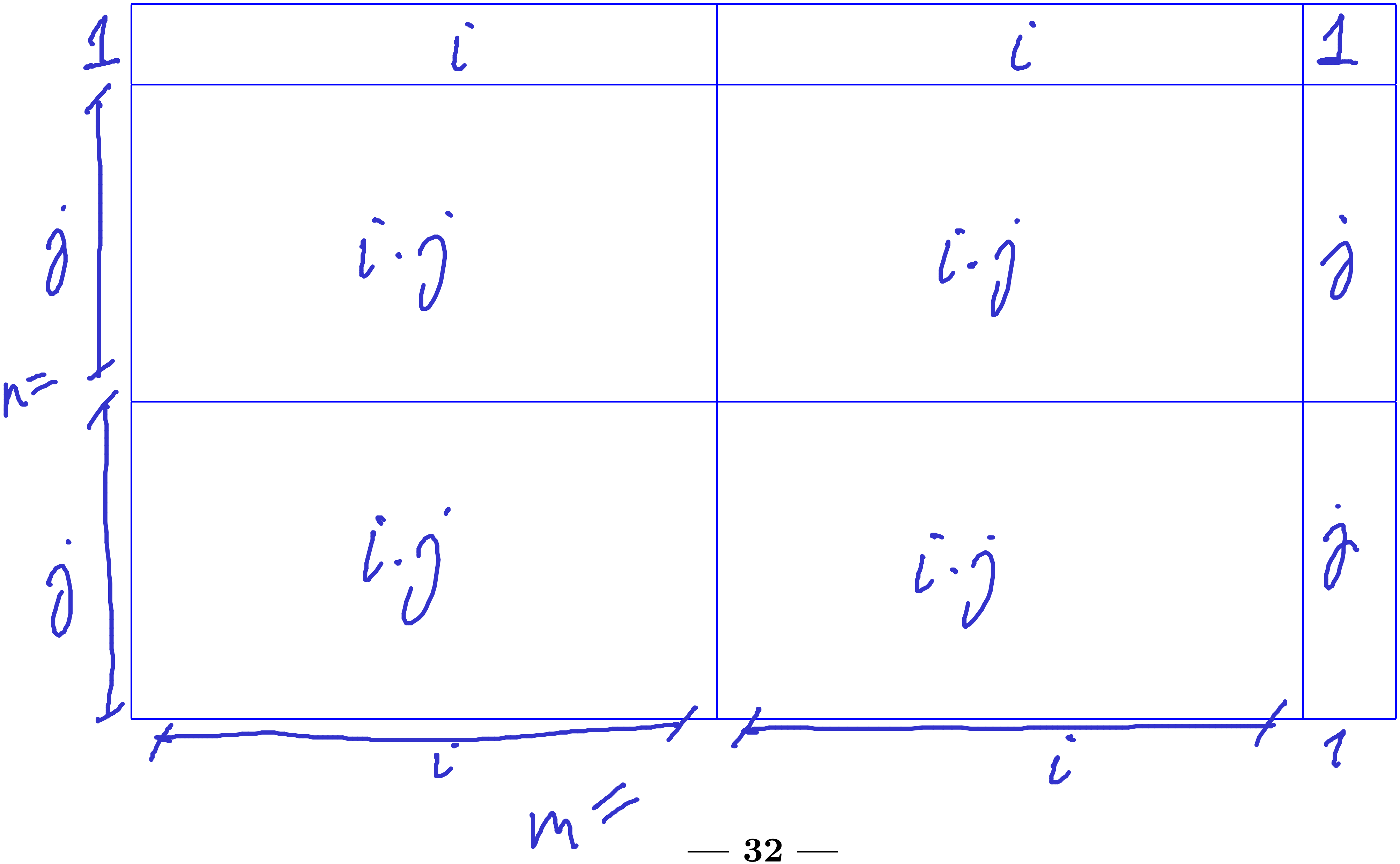
  Examine the solution obtained.

Intuition:

$m = 2i+1$

$n = 2j+1$

$m \cdot n = 4ij + 2i + 2j + 1$



SCRATCH WORK

$m = 2i + 1 \qquad n = 2j + 1$

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

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

$$= 2(2ij + i + j) + 1 \quad \text{odd.}$$

PROOF OF Proposition 8: Let m and n be odd integers. That is, $m = 2i+1$ for some integer i and $n = 2j+1$ for an integer j.

Then, $m \cdot n = 2(2ij+i+j)+1$ and therefore of the form $2k+1$ (for $k = 2ij+i+j$). Hence an odd integer. $\boxtimes$

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'

PROOF STRUCTURE

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