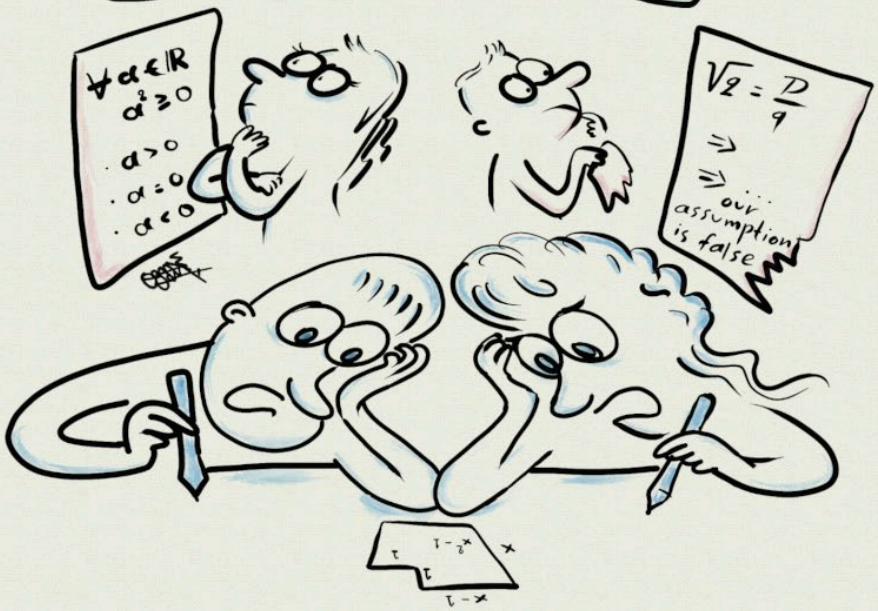
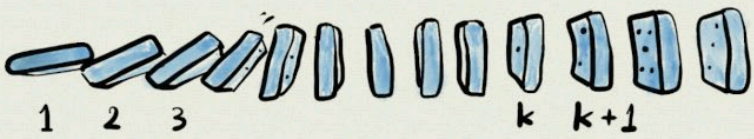
THINKING ABOUT PROOF





The cover image was created by Thomas Thoma. It includes four types of proof - the student on the left-hand side is engaging with a proof by exhaustion, the one in the right-hand side is engaging with a proof by contradiction. The two students at the front are working on a part of a direct proof and the dominos at the front show how proof by induction works.

Table of contents

1. Introduction

In Spring 2022 we conducted the 'Mathematics in Transit' project. In this project a team of teachers and researchers from post-16 schools, the Southampton Education School and the School of Mathematics, explored curriculum materials to find the topic that would be most helped with a supporting booklet. The most useful topic was 'proof'. This booklet is aimed at students interested in learning more about proof and different types of proof. In this booklet, we go through what is a proof, how to construct a proof, and different types/methods of proof.

The booklet has made use of the extensive SMP archives at the University of Southampton and is accompanied by a website with the solutions to the exercises provided here: http://blog.soton.ac.uk/mshe/solutions-mit-proof-booklet/

Christian Bokhove – Southampton Education School, University of Southampton
Athina Thoma – Southampton Education School, University of Southampton
David Gammack – School of Mathematics, University of Southampton
Lu Heng Sunny Yu – School of Mathematics, University of Southampton
Sarah Roberts – Barton Peveril College, Eastleigh
Frances Downey – St Edward's School, Poole

1st edition. July 2022.

2. What is a Proof?

Proof is at the heart of all mathematics. A proof uses previously known truths and logical arguments to show that a statement is true and, once the statement has been proved this way, we can say with certainty that it will always be true. Many of the facts that you use in day-to-day mathematics and take for granted were at some point an idea or a **conjecture,** that needed to be proved. Once a conjecture is proved, it is then known as a **proposition** or **theorem**.

Let's consider the following proposition:

$x^2 - 1 = (x - 1)(x + 1)$ for all real values of x

We can satisfy ourselves that this is true by substituting in the equality values of x. For example:

When $x = 1$, $\quad x^2 - 1 = 1^2 - 1 = 0$

and $\quad (x + 1)(x - 1) = (1 + 1)(1 - 1) = 2 \times 0 = 0$

Since both sides equal the same value then we can say that they are equal when $x = 1$. But can we repeat this process for **all** values of x? If we could then we would be using a type of Proof called **Proof by Exhaustion**. We will look more at this type of proof later in section 5.

However, in this case we cannot try every single possible value of x, so this does not provide us with absolute certainty that the proposition is true for **all** values of x. When we are proving a statement, it is not sufficient for it to only be true in some cases.

You may have looked at the proposition and thought that this is obviously true because of your existing knowledge of how algebraic multiplication works –

you can multiply out the right-hand side and that will give you the left-hand side. $(x+1)(x-1) = (x \times x) + (1 \times x) + (-1 \times x) + \big(1 \times (-1)\big)$

$$= x^2 - x + x - 1 = x^2 - 1$$

This is an example of **Direct Proof** – it starts with what is known and proceeds, by a sequence of logical steps, to the conclusion. This is the most common type of proof that you will have come across at A-level. In section 6 we go through this type of proof in more detail. A direct proof is not necessarily algebraic in nature. Geometry or reasoning may be involved, provided one step logically leads to the next. Figure 2.1 shows another way we could directly prove the proposition:

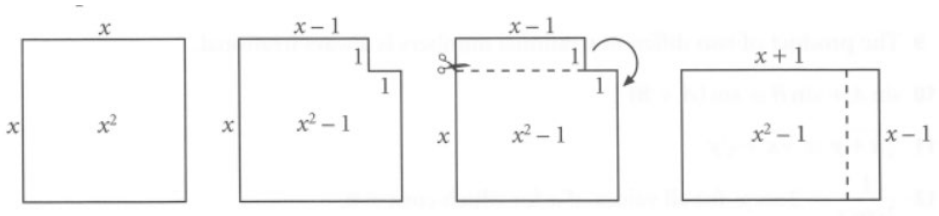


Figure 2.1: A visual direct proof of the proposition (SMP AS/A2 Core 3 for AQA chapter 10).

A further type of direct proof that you may not have come across is **Proof by Induction**. This is studied in Further Maths A-level and is used considerably within degree-level mathematics. We will look at this type of proof in more detail in section 7. There are times when we cannot use a direct method of proof. You will come across one type of **Indirect Proof** at A-level, known as **Proof by Contradiction**. This involves assuming the opposite of your conjecture and then proving that this cannot be true. You will see more information about this type of proof in section 9. However, before we look at the different types of proof, we will look at how we can disprove a statement (or a conjecture).

3. Disproof - Counterexample

Whenever we are given a conjecture our first step is to try some values and see whether we think it is true. It may be that the conjecture is false and we can therefore disprove it. Disproof only requires one **Counterexample** – because that one example demonstrates that the conjecture is not true in all cases.

Example 3.1

By finding a suitable counterexample, prove that the following conjecture is false: $a^3 + b^3 = (a + b)^3$

Solution 3.1

When $a = 4$ and $b = 1$, then $a^3 + b^3 = 4^3 + 1^3 = 64 + 1 = 65$

and $(a + b)^3 = (4 + 1)^3 = 5^3 = 125$

Since $65 \neq 125$, this counterexample shows that the conjecture is false.

3. Exercises

Prove that each of these conjectures is false by finding a suitable counterexample. The solutions to these exercises are in the website accompanying this booklet[1].

1. The product of two odd numbers is always a multiple of 3.
2. $\cos(-\theta) = -\cos\ \theta$
3. $\sin(2\theta) = 2\sin\theta$
4. For all real values of $x, x^2 \geq x$
5. The product of two different irrational numbers is always irrational
6. $e^{2x} = e^x + e^2$
7. For all positive values of a and b, $\ln(ab) = \ln a \ln b$
8. For all real values of x and $y, x^2 > y^2 \Rightarrow\ x > y$

[1] http://blog.soton.ac.uk/mshe/solutions-mit-proof-booklet/

4. What is the structure of a proof?

From studying at A-level, you will now appreciate that mathematics is not simply about getting the correct answer to a question. The process of *how you reach that answer* is the important part. This is particularly true in proof, since we already have an idea of the answer and we have to demonstrate precisely how we get to it.

Students often find producing a mathematical proof extremely difficult. It can be hard to know where to start or how to proceed if you get stuck in the middle of the proof. Sometimes you may be able to follow a proof that someone else has produced, but feel that you could never have constructed it for yourself.

The truth is that many published proofs are the polished result of a messy process that has involved many dead-ends. The final proof may look effortless and elegant but does not reveal the work involved in constructing it. Most people only feel confident about proof after a lot of experience of proving things in a variety of mathematical contexts.

We do use certain notation within a proof – in particular we use the implication sign ⇒ to show that one step implies the next step:

For example, $P \Rightarrow Q$ can be read as "P implies Q" and it means that **if** statement P is true **then** statement Q is true.

For example, if we have the following statements:

P: $ABCD$ is a square

Q: $ABCD$ is a quadrilateral

then $P \Rightarrow Q$. However, you cannot say that $Q \Rightarrow P$ as that is not true in all cases.

Now consider, the following statements:

P: $AB^2 + BC^2 = AC^2$

Q: Triangle ABC is a right-angled triangle

In this case $P \Rightarrow Q$, but also the converse is true, $Q \Rightarrow P$. We can therefore say that statement P is true **if and only if** Q is true and can write this as $P \Leftrightarrow Q$ or "P iff Q".

Key Symbols

In the table below you have some key symbols which are going to be useful when reading or writing a proof.

Table 1. Key mathematical symbols

Symbol	Meaning
$\Leftrightarrow$	if and only if (iff)
$\Rightarrow$	implies
$\in$	element of
$\therefore$	therefore
Q.E.D[2] , ■, □	end of the proof

Constructing a Proof

Let's now look at how you might construct a proof. Consider this conjecture.

[2] Q.E.D stands for the Latin phrase *Quod Erat Demonstrandum* which means "Which was shown"

Example 4.1

For all odd numbers n, show that $n^2 - 1$ is divisible by 8.

A good place to start is to try some values. This may disprove the conjecture, in which case you're done. But if it doesn't then you are going to need to prove it and this step may help you spot any useful patterns and reasons for them:

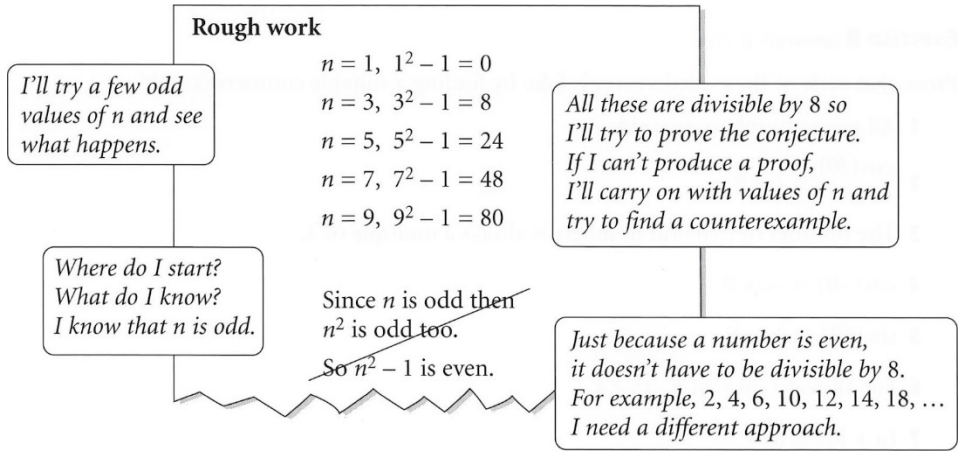


Figure 4.1: An example proof (SMP AS/A2 Core 3 for AQA chapter 10).

At this point it can be really useful to think about whether we could use direct proof and describe what is happening using algebra:

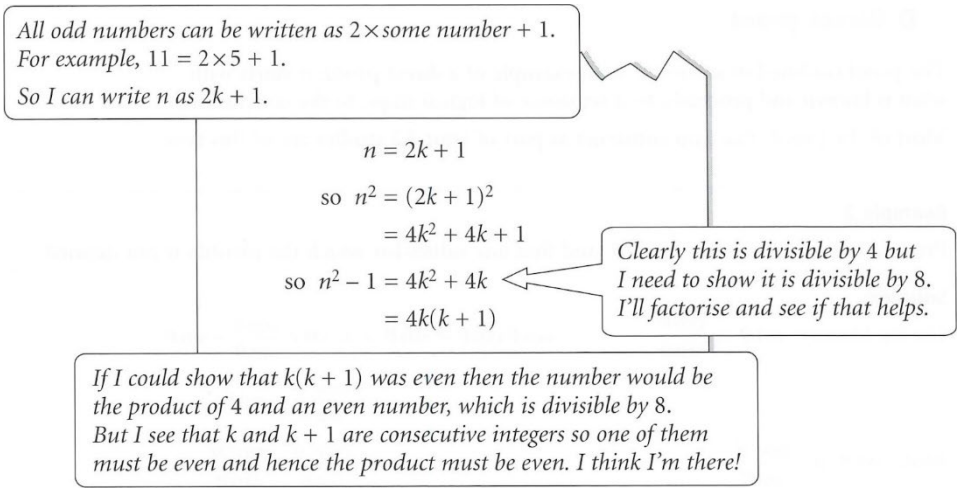


Figure 4.2: Another example proof (SMP AS/A2 Core 3 for AQA chapter 10).

It may be that your final algebraic step is not sufficient to clearly prove the conjecture. You always need to finish a proof by explaining the reasoning and drawing a conclusion:

Solution 4.2

As n is odd there is some integer k such that $n = 2k + 1$

So, $$n^2 - 1 = (2k + 1)^2 - 1$$

$$= 4k^2 + 4k + 1 - 1$$

$$= 4k^2 + 4k$$

$$= 4k(k + 1)$$

Since k and $k + 1$ are consecutive integers, one of them must be even, so the product $k(k + 1)$ is even too. So $4k(k + 1)$ is the product of 4 and an even number. Hence $4k(k + 1)$ is divisible by 8. So for all odd $n, n^2 - 1$ is divisible by 8. □

As you can see, a proof is a combination of writing and mathematics and should be laid out so that the sequence of logical steps leads to the conclusion and you are convinced by the reasoning in each step.

5. Proof by Exhaustion

The basic idea of the proof by exhaustion is the following:

Split the statement into a couple of distinct *cases*. Then for each of the cases, check that the statement you'd like to prove is true.

You can think of proof by exhaustion as a *two-step process*:

Step 1: Split the statement into finite number of exhaustive cases, then

Step 2: Show the statement is true in each case.

Before we look at examples, let us mention a few "fine prints" regarding the two steps. While they may sound abstract at this stage, these points will become clear once we see a few examples.

The "fine prints" are regarding:

1. The cases in **Step 1**:
   a. The number of cases must be *finite*. Otherwise, you are then tasked with checking infinite number of cases, which is impossible (at least within a finite period of time!).

Example 5.1

Prove the following statement:

The square of any real number is never negative.

In principle, you can "split" all possible real numbers into a case of just themselves, and check if the square of every possible real number from $-\infty$ to

∞ is not negative taking one-by-one all the numbers. But this will take forever, and hence impossible.

But if we split all real numbers into three cases: (i) numbers less than zero, (ii) numbers larger than zero, (iii) zero, it will be more feasible to check these three cases.

b. The cases must be *exhaustive*. This means while the number of cases are finite, it must also cover all possibilities of the statement.

2. When you get to **Step 2** which is "checking each case", this is basically saying "prove each individual case". Having said that, for a lot of proofs using this method, it simply amounts to a direct "check" if this case is true.

Therefore, in some sense, rather than being a full and standalone "method for proof" itself, proof by exhaustion can be thought of as a potential "first step" towards a complete proof of the initial statement.

Why is this method useful?

The purpose of employing this method is to take the initial statement and break it down to smaller cases, such that each of the subsequent cases are easy (or easier) to prove.

Once you've split into cases, each case should be proved independently. For a lot of questions, after you have split into cases, the cases will be simple enough to prove by simply substituting in the numbers and check. Occasionally, you may then need to use other types of proof so that you can provide a proof for each of the cases.

Before we look at some examples, we shall list a few common finite exhaustive cases.

Tips: Common types of finite, exhaustive cases

1. <u>"Trichotomy of real numbers"</u>

Every real number is either (i) positive, (ii) negative, or (iii) zero.

i.e.,

$$a \in \mathbb{R} \Rightarrow \begin{cases} a > 0, \text{ or} \\ a < 0, \text{ or} \\ a = 0. \end{cases}$$

*All real numbers satisfy this property.

Note: Trichotomy is a Greek word and means "divide in three sections".

2. <u>Even and odd (integers)</u>

All integers are either (i) even or (ii) odd.

i.e.,

$$n \in \mathbb{Z} \Rightarrow \begin{cases} n = 2k, \text{ or} \\ n = 2k + 1, \end{cases} \text{ where } k \in \mathbb{Z}.$$

Note: Recall the formal definitions of *even* and *odd* numbers:

Definition of *even*:

n is *even* if it can be written in the form $n = 2k$, where k is any integer.

Definition of *odd*:

n is *odd* if it can be written as $n = 2k+1$, where k is any integer.

*All integers satisfy this property.

3. <u>Divisibility of integers</u>

An integer n is either:

- A multiple of some other integer m,
- 1 more than a multiple of m,
- 2 more than a multiple of m,
- …, or
- $k-1$ more than a multiple of m.

Note: This is also an extension to the "odd and even" type. Basically, "odd and even" type is splitting numbers into cases that can be divided by 2 precisely, and numbers that can be divided by 2 with remainder 1. (i.e. $n = 2k$ or $n = 2k+1$, where k is an integer.)

*All integers satisfy this property.

4. <u>Explicit testing of each case</u>

Finally, if the statement to be proved only refers to a finite number of explicit cases, you just need to test the cases explicitly one by one.

E.g. If you are asked: Prove that $2^{\frac{n}{5}} \leq 1 + \frac{n}{5}$ if $n = 0, 1, 2, 3, 4, 5$ then you can simply run through each case of n explicitly to check if the statement holds.

Note: Of course this type of proof should only be used, in examinations or during your studies, if there is a manageable number of cases (for example under 10). Beyond that, it will be not be an efficient or realistic way to complete the proof within a reasonable time. Nevertheless, outside of secondary school or undergraduate studies, explicitly running through a large number of finite case to prove certain statements is sometimes used in real research (often with the help of a computer). The famous "four-colour theorem" in mathematics is an early example of this, where the infinite cases

are first reduced down to 1,834 cases (later reduced to 1,482), and the researchers had a computer run through each case explicitly[3].

Example 5.1 (Using trichotomy)

Prove that the square of any real number is never negative.

Solution 5.1

Let a be any real number.	It is always useful to first define the variable you are working with and consider the domain they belong to e.g., naturals, reals etc.
To prove: $$a \in \mathbb{R} \Rightarrow a^2 \geq 0$$	If possible, always try to first translate the "worded statement" into a "mathematical statement".
By *trichotomy of real numbers*, a satisfies either $a > 0$, $a < 0$, or $a = 0$.	
Case 1: $a > 0$	
Then $a^2 > 0$	Multiply both sides by a
Case 2: $a < 0$	Multiply both sides by a
Then $a^2 > 0$	Here you use the property that when you have an inequality and you multiply it with a negative

[3] Appel, K. I., & Haken, W. (1989). *Every planar map is four colorable* (Vol. 98). American Mathematical Soc..

	number that process flips the sign of inequality.
Case 3: $a = 0$	
Then $a^2 = 0$	Multiply both sides by a
∴ Proved $\forall\, a \in \mathbb{R}, a^2 \geq 0$. $\square$	

Example 5.1 (Using divisibility)

Prove the following statement:

If *m* is an integer that is not a multiple of 3, show that $m^2 - 1$ will be a multiple of 3.

Solution 5.2

From the divisibility of integers, any integers are one of the following:

(i) multiple of 3

(ii) 1 more than a multiple of 3

(iii) 2 more than a multiple of 3

Since case (i) is ruled out in the question, we just need to check the two latter cases:

Case (ii): m is 1 more than a multiple of 3. You can write $m = 3k + 1$, where k is some integer.

Then, $$m^2 - 1 = (3k + 1)^2 - 1$$

$$= (3k + 1 - 1)(3k + 1 + 1)$$

$= 3k(3k + 2)$ which is a multiple of 3.

Case (iii): m is 2 more than a multiple of 3. You can write $m = 3k + 2$, where k is some integer.

Then, $m^2 - 1 = (3k + 2)^2 - 1$

$= (3k + 2 - 1)(3k + 2 + 1)$

$= (3k + 1)(3k + 3)$

$= 3(3k + 1)(k + 1)$ which is a multiple of 3.

Since all cases are verified, the initial statement is proved. □

Example 5.2 (Testing all cases explicitly)

Prove that $(n + 1)^3 \geq 3^n$ for all $n \in \mathbb{N}, n \leq 4$.

Solution 5.3

For all $n \in \mathbb{N}, n \leq 4$, n can only be four numbers[4]: $n \in \{1, 2, 3, 4\}$

Case (i): $n = 1$. Then you have

$(n + 1)^3 = (1 + 1)^3 = 8$

$3^n = 3^1 = 3$

$\because 8 > 3$. The statement is true if $n = 1$.

Case (ii): $n = 2$

$(n + 1)^3 = (2 + 1)^3 = 27$

$3^n = 3^2 = 9$

$\because 27 > 9$. The statement is true if $n = 2$.

[4] Note: Some authors may consider $0 \in \mathbb{N}$. The statement will still be true. This additional case will be left as an exercise for you to check.

Case (iii): $n = 3$

$$(n+1)^3 = (3+1)^3 = 64$$

$$3^n = 3^3 = 27$$

$\because 64 > 27$. The statement is true if $n = 3$.

Case (iv): $n = 4$

$$(n+1)^3 = (4+1)^3 = 125$$

$$3^n = 3^4 = 81$$

$\because 125 > 81$. The statement is true if $n = 4$.

$\therefore$ Initial statement is proved. □

Potential mistakes

- Checking one or two values does not mean the result is true for *all* values!
  - When a statement makes a claim about certain sets of numbers, *all* values within that set the statement has claimed to be about will need to be tested!

    E.g. If *n* is an integer between $10 \leq n \leq 20$, then $2^{\frac{n}{10}}$ is always larger than $\left(\frac{n}{10}\right)^2$.

    If you had checked only say $n = 10,11,12, \ldots, 19$, you may be convinced the statement is true. But upon more careful inspection, you will find $n = 20$ fails. Therefore we must be careful to check all possible values that the statement claims it holds true for before the proper proof is complete. And if the statement claims to hold for an infinite set of numbers, then other methods must be used, since it is impossible prove by exhaustion for *infinite* number of cases!

- Make sure cases are exhaustive.
    - Make sure the cases you split do cover all possible scenarios that the statement claims to apply to.

      E.g. If a statement refers to all real numbers and you would like to use the trichotomy of real numbers, don't forget to check the statement is also true for the case $a = 0$.

When is this method useful?

This method is useful when the statement you are given can be easily split into a handful of simpler or more limiting cases.

Of course, it takes a bit of experience to know if the subsequent cases are really "easier" to prove or not, or would it be easier to just directly prove the original statement (via some of the other methods).
And in some cases, it is just a matter of trial and error. Like most things in mathematics (and life), experience is just a result of sufficient trial and errors!

5. Exercises[5]

1. Prove that $2^{\frac{n}{5}} \leq 1 + \frac{n}{5}$, if $n = 0, 1, 2, 3, 4, 5$.
2. Show that $n^2 + 2$ is not a multiple of 4, if n is an integer, $2 \leq n \leq 7$.
3. If p is a prime number such that $3 < p < 25$, then prove by exhaustion that $(p-1)(p+1)$ is a multiple of 12.
4. If x is a positive integer less than 5, prove that the last digit of x^5 is x.
5. Prove that $a^2 + 1$ is not divisible by 3, where $6 \leq a \leq 10$.
6. Prove that the difference between $n^3 + 7$ and a multiple of 7 is always 1, for all integers in the interval $1 \leq n \leq 4$.
7. Let n be an integer. Prove by exhaustion that $n^2 - 5n + 4$ is positive for $6 \leq n \leq 8$.
8. Prove by exhaustion that if n is not divisible by 3, then $n^2 = 3k + 1$ for some integer k.
9. If a is not a multiple of 3, use exhaustion to prove that $a^2 - 1$ is a multiple of 3.
10. If n is a positive integer, then $n^7 - n$ is divisible by 7.
11. Prove that $\forall\, x \in \mathbb{R}, x^2 = |x|^2$

Hint: Recall the definition of $|x|$:

$$|x| \coloneqq \begin{cases} x & \text{, if } x \geq 0\,; \\ -x & \text{, if } x < 0\,. \end{cases}$$

[5] The solutions are here
http://blog.soton.ac.uk/mshe/solutions-mit-proof-booklet/

6. Direct proof

The proof we saw in Section 4, Example 4.1 is often known as **Proof by Deduction** and is the type of Direct Proof that we will now consider in more detail. It will, most likely, be the type of proof that you are most familiar with from A-level.

In the first instance it is often easiest to look for a way to describe what is happening algebraically and then use your algebraic knowledge to prove the conjecture.

We tend to use

- n to represent any integer. Use n and m to represent any two integers.
- n, $n+1$ and $n+2$ to represent 3 consecutive integers. You might also consider $n-1$, n and $n+1$
- n^2 and m^2 to represent any two square numbers.
- n^2 and $(n+1)^2$ represent any two consecutive square numbers.

If n represents any integer, then $2k$ represents any even integer and $2k+1$ represents any odd integer.

It follows that $2k$ and $2k+2$ represent any two consecutive even numbers and $2k+1$ and $2k+3$ represent any two consecutive odd numbers.

There is also certain knowledge that is considered known and can simply be stated within a proof.

For example,

- even number $\times$ even number $=$ even number,
- even number $\times$ odd number $=$ even number,
- even number $+$ even number $=$ even number etc.

Example 6.1

Prove that the sum of any two consecutive odd numbers is a multiple of 4

Solution 6.1

Let two consecutive odd numbers be $2k+1$ and $2k+3$	*Make sure that you define what symbols you will use*
Then their sum can be expressed as $2k+1+2k+3=4k+4$	*Carry out what the conjecture suggests, i.e. find their sum*
$4k+4=4(k+1)$, which is a multiple of 4	*Factorise to show that you can take out a factor of* 4
Hence the sum of any two consecutive odd numbers is a multiple of 4 $\square$	*Write the conclusion to reflect the wording of the conjecture*

This type of example requires less reasoning as the algebra does the work for you, but it is not always possible to use algebra.

Example 6.2

Prove that the product of any three consecutive positive integers is a multiple of 6.

Solution 6.2

Let three consecutive integers be $n, n+1, n+2$	*Make sure that you define what symbols you will use*
Then their product is	

$n(n+1)(n+2)$ $= n(n^2+3n+2)$ $= n^3+3n^2+2n$	*Realise that you're not sure how that helps as you cannot take out a factor of 6*

Start again

In three consecutive integers, you will have either one or two even numbers – so the product must be a multiple of 2. Since every third number is divisible by three, in three consecutive integers, one of the integers will be divisible by 3. Hence their product must be a multiple of 3. Thus if the product of three consecutive numbers is a multiple of 2 and a multiple of 3 then it must be a multiple of 6.	*Think about what it means if you have three consecutive numbers and their relationship to odd and even numbers* *Bringing it together*

As you can see, there is a certain amount of trialling and dismissing ideas within proof.

6. Exercises[6]

Prove each of these statements:

1. The cube of any even number is divisible by 8
2. The sum of the first n odd numbers is n^2
3. $\cos\theta \cot\theta + \sin\theta \equiv \operatorname{cosec}\theta$ and find any values for which the identity is not defined
4. For any four consecutive integers, the difference between the product of the last two and the product of the first two of these numbers is equal to their sum.
5. The graphs of $y = |\sin x \cos x + 1|$ and $y = \sin x \cos x + 1$ are identical
6. The product of four consecutive integers is always 1 less than a perfect square.
7. $9^n - 1$ is a multiple of 8 for any positive integer n
8. If p is a prime number such that $p > 3$, then $p^2 - 1$ is a multiple of 24.

[6] The solutions are here
http://blog.soton.ac.uk/mshe/solutions-mit-proof-booklet/

7. Proof by induction

Proof by induction is a type of proof that you can find in many areas of Mathematics (e.g., Algebra, Geometry, Trigonometry, Analysis, Combinatorics and Graph Theory etc.). Let's take a look at a few examples.

Example 7.1

Prove the following statement: $1 + 3 + 5 + \ldots + (2n - 1) = n^2$ is true for n positive integer.

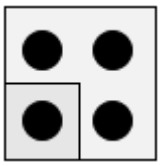
Solution 7.1 -A

First let's have a look at this virtually[7], starting from 1 and then slowly adding the next terms of the summation.

If we have 1 on the left-hand side of the equality then $1 = 1^2$.

If we have $1 + 3$ on the left-hand side of the equality then

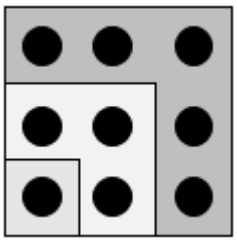
$1 + 3 = 4$ and the right-hand side of the equality is $2^2 = 4$



Virtually we can see now that if we add 3 more circles then that gives us a square with side 2 and area 4.

---

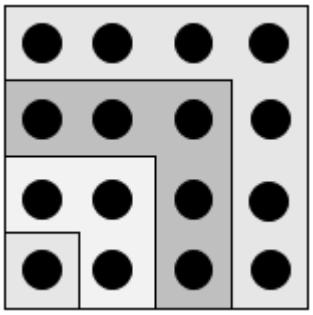
[7] The idea of this virtual proof is presented in Brown, J. R. (1997). Proofs and pictures. The British Journal for the Philosophy of Science, 48(2), 161-180.



If we have $1 + 3 + 5$ on the left-hand side of the equality then

$1 + 3 + 5 = 9$ and the right-hand side of the equality is $3^2 = 9$

Virtually we can see now that if we add 5 more circles then that gives us a square with side 3 and area 9.



If we have $1 + 3 + 5 + 7$ on the left-hand side of the equality then $1 + 3 + 5 + 7 = 16$ and the right-hand side of the equality is $4^2 = 16$

Virtually we can see now that if we add 7 more circles then that gives us a square with side 4 and area 16.

And this can continue with the addition of the next odd numbers.

Let's now think about the same proof but we will now think of the first step, a random k step and the step that comes after that, step k+1.

Solution 7.1- B

Step 1 – *Base Case* – Check that the statement you have holds for $n = 1$

When $n = 1$ the left-hand side of the equation is 1 and the right hand side is $1^2 = 1$. So, the statement holds for $n = 1$.

Step 2 – *Induction hypothesis* – Assume that the statement holds for $n = k$

You assume that the statement holds for k. This means that the left-hand side of the equality for $n = k$ is equal to k^2. In other words that $1 + 3 + 5 + \ldots + (2k - 1) = k^2$

Step 3 – *Induction step* – Prove that if the statement holds for $n = k$ then it holds for $n = k + 1$

You will now show that the statement holds for $n = k + 1$. You will aim to show that $1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) = (k + 1)^2$.

You will start from the left-hand side. You have:

$1 + 3 + 5 + \ldots + (2k - 1) + (2(k + 1) - 1)$	*The first part of the summation you have to prove is the same as the summation you have in your induction hypothesis (left-hand side).*
$= k^2 + (2(k + 1) - 1)$	*You can replace it with the right-hand side of the induction hypothesis.*
$= k^2 + 2k + 2 - 1$	*Now you will manipulate the expression aiming to simplify it.*
$= k^2 + 2k + 1$	*You now need to factorise it*
$= (k + 1)^2$	

In this step you proved that if the statement holds for $n = k$ then it holds for $n = k + 1$, which concluded the *induction* step.

Step 4 – Summarise and conclude

Hence, the statement $1 + 3 + 5 + \ldots + (2n - 1) = n^2$ is correct for all positive integers n.

Example 7.2

Prove that $n! > 2^n$ for $n \geq 4$

Solutions 7. 2

You will follow exactly the same steps as before.

Step 1 – *Base Case* – Check that the statement you have holds for $n = 4$

Note that the base step is now different (the base step is the smallest value n can take but not necessarily 1).

When $n = 4$ the left-hand side of the equation is $4! = 1 \times 2 \times 3 \times 4 = 24$

and the right hand side is $2^4 = 16$. And $24 > 16$ so, the statement holds for $n = 4$.

Step 2 – *Induction hypothesis* – Assume that the statement holds for $n = k$

You assume that the statement holds for k. This means that the left-hand side of the equality for $n = k$ is more than 2^k. In other words that $k! > 2^k$

Step 3 – *Induction step* – Prove that if the statement holds for $n = k$ then it holds for $n = k + 1$

You will now show that the statement holds for $n = k + 1$. In other words you need to show that $(k + 1)! > 2^{k+1}$

You will start from the left-hand side. You have:

$(k+1)! = (k+1)k!$	*You expand the factorial but you keep the* $k!$ *as that appears in your induction hypothesis.*
$= kk! + k!$	*You expand the brackets and you have two appearances of* $k!$ *and you can use your induction hypothesis* $k! > 2^k$
$> \ k2^k + 2^k$	
$= 2^k(k+1)$	*Now you will manipulate the expression aiming to simplify it.*
$\geq 2^k(4+1) > 2^k(1+1) = 2^k 2$ $= 2^{k+1}$	*Also you have that the smallest value k can take is* $k \geq 4$

In this step you proved that if the statement holds for $n = k$ then it holds for $n = k + 1$, which concluded the *induction* step.

Step 4 – Summarise and conclude

Hence, the statement $n! > 2^n$ is true for all $n \geq 4$.

Example 7.3

Prove the for n positive integer $f(n) = 4^n + 15n - 1$ is divisible by 9.

Solution 7.3

Step 1 – *Base Case* – Check that the statement you have holds for $n = 1$

When $n = 1$ then $f(1) = 4^1 + 15 \times 1 - 1 = 4 + 15 - 1 = 18$. And 18 is divisible by 9 so, the statement holds for $n = 1$.

Step 2 – *Induction hypothesis* – Assume that the statement holds for $n = k$

You assume that the statement holds for k. This means that $f(k) = 4^k + 15k - 1$ is a multiple of 9. You can rewrite this as $4^k + 15k - 1 = 9m$ where m a positive integer.

Step 3 – *Induction step* – Prove that if the statement holds for $n = k$ then it holds for $n = k + 1$

You will now show that the statement holds for $n = k + 1$. In other words you need to show that $4^{k+1} + 15(k + 1) - 1 = 9l$ where l a positive integer.

You will start from the left-hand side. You have:

$4^{k+1} + 15(k+1) - 1$ $= 4^k 4 + 15k + 15 - 1$ $= 4^k(3+1) + 15k + 15 - 1$	*You expand your expression by breaking up the* 4^{k+1} *and the* $15(k+1)$*. You do this as* $4^k + 15k - 1$ *appears in your induction hypothesis.*
$= 4^k(3+1) + 15k + 15 - 1$ $= 4^k + 3 \times 4^k + 15k + 15 - 1$	*Now you have* $4^k + 15k - 1$ *and you can use your induction hypothesis that* $4^k + 15k - 1 = 9m$
$= [4^k + 15k - 1] + 3 \times 4^k + 15$ $= 9m + 3 \times 4^k + 15$	*Now you need to show that* $3 \times 4^k + 15$ *is a multiple of 9. To do this you need to prove by induction (this is a*

	proof by induction within a proof by induction)

You need to show that *that* $3 \times 4^k + 15$ *is a multiple of 9.*

Step 1 – ***Base Case*** $-$ Check that the statement you have holds for $k = 1$

When $k = 1$ then $3 \times 4^1 + 15 = 12 + 15 = 27$. And 27 is divisible by 9 so, the statement holds for $k = 1$.

Step 2 – ***Induction hypothesis*** $-$ Assume that the statement holds for $k = t$

You assume that the statement holds for t. This means that $3 \times 4^t + 15$ is a multiple of 9. You can rewrite this as $3 \times 4^t + 15 = 9s$ where s a positive integer.

Step 3 – ***Induction step*** $-$ Prove that if the statement holds for $k = t$ then it holds for $k = t + 1$

You will now show that the statement holds for $k = t + 1$. In other words you need to show that $3 \times 4^{t+1} + 15 = 9v$ where v a positive integer.

You will start from the left-hand side. You have:

$3 \times 4^{t+1} + 15$	*You expand your expression by breaking up the* 4^{t+1} *. You do this as* $3 \times 4^t + 15$ *appears in your induction hypothesis.*
$= 3 \times 4^t \times 4 + 15$	
$= 3 \times 4^t \times 4 + 15$	
$= 3 \times 4^t \times 4 + 60 - 45$	*You now need to write 15 as a difference of two numbers.*

	However, these cannot be any numbers. One of them needs to be a multiple of 9 and the other one a multiple of 4 and 15 so that you can create your induction hypothesis.
$= 4(3 \times 4^t + 15) - 45$ $= 4(9s) - 45$ $= 4(9s) - 9 \times 5$ $= 9\,(4s - 5) = 9v$	*Now you have* $3 \times 4^t + 15$ *and you can use your induction hypothesis that* $3 \times 4^t + 15 = 9s$

In this step you proved that if the statement holds for $k = t$ then it holds for $k = t + 1$, which concluded the *induction* step.

Step 4 – Summarise and conclude

Hence, the statement $3 \times 4^k + 15$ is a multiple of 9.

You can now return to the step of the previous proof we had left unanswered.

$4^{k+1} + 15(k+1) - 1$ $= 4^k 4 + 15k + 15 - 1$ $= 4^k(3+1) + 15k + 15 - 1$	*You expand your expression by breaking up the* 4^{k+1} *and the* $15(k+1)$*. You do this as* $4^k + 15k - 1$ *appears in your induction hypothesis.*
$= 4^k(3+1) + 15k + 15 - 1$	

$= 4^k + 3 \times 4^k + 15k + 15 - 1$	*Now you have* $4^k + 15k - 1$ *and you can use your induction hypothesis that* $4^k + 15k - 1 = 9m$
$= [4^k + 15k - 1] + 3 \times 4^k + 15$ $= 9m + 3 \times 4^k + 15$ $= 9m + 9s = 9(m + s) = 9l$	*Now you need to show that* $3 \times 4^k + 15$ *is a multiple of 9. Using the previous proof by induction you have that* $3 \times 4^t + 15 = 9s$ *where s is a positive integer.*

Step 4 – Summarise and conclude

Hence, $f(n) = 4^n + 15n - 1$ is divisible by 9 for n positive integer.

7. Exercises[8]

1. Prove that $1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ is true for $n \geq 1$
2. Prove that $n! > n^n$ for $n \geq 2$
3. Prove that $2^n > n^2$ for $n \geq 5$
4. Prove that $2n^3 + 3n^2 + n$ is divisible by 6 for $n \geq 1$
5. Prove that $x^n - y^n$ is divisible by $x - y$ for n positive integer.

[8] The solutions are here
http://blog.soton.ac.uk/mshe/solutions-mit-proof-booklet/

8. Proof by contradiction

This type of proof, assumes that what you want to prove is in fact false and tries to derive a logical contradiction, a so-called *proof by contradiction*.

A famous example concerns proving that the number $\sqrt{2}$ is irrational.

Recall that an irrational number is a number that cannot be expressed as the ratio of two integers.

We will start with this famous example.

Example 8.1

Proof by contradiction that $\sqrt{2}$ is irrational

Solution 8.1

Assume that $\sqrt{2}$ is rational.

Then there must exist integers p and q such that $\sqrt{2} = \frac{p}{q}$ in its simplest form.

$$\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2}$$

$$\Rightarrow p^2 = 2q^2$$

So p^2 is even and therefore p is even too.

If p is even then there exists an integer k such that $p = 2k$ and so $p^2 = (2k)^2 = 4k^2$.

But as $p^2 = 2q^2$ and $p^2 = 4k^2$ it follows that $2q^2 = 4k^2$ which gives $q^2 = 2k^2$.

In other words, q^2 is even and therefore q is even too.

But if both p and q are even, then $\frac{p}{q}$ is not in its simplest form and our original assumption was false.

We conclude that $\sqrt{2}$ is irrational. □

Example 8.2 – infinitely many primes

Although some argue that this is not strictly a proof by contradiction because it also provides a 'recipe' for creating new prime numbers, many would call this one of the first known proofs by contradiction. It is Euclid's proof that there are infinitely many prime numbers. It is considered to be one of the most elegant proofs in mathematics.

Solution 8.2

Assume that there are a finite number of primes.

Let $p_1 = 2, p_2 = 3, p_3 = 5,\ p_4 = 7$ … be the primes in ascending order and let p_n be the largest. Now consider N, which is one more than the product of all the primes:

$$N = p_1 p_2 p_3 p_4 \cdots p_n + 1$$

This number is not divisible by any of the primes p_1, p_2, p_3, p_4, … p_n as division by each leaves a remainder of 1. Hence N is divisible by a prime larger than p_n or is itself prime.

This contradicts the assumption that p_n is the largest prime.

Hence our original assumption is false and there must be infinitely many primes. □

Example 8.3 – divided by 1001

Prove that the product of two positive integers whose sum is 1001 cannot be divided by 1001.

Solution 8.3

Let the two positive integers be n and m.

We want to prove that nm is not divisible by 1001.

Suppose nm is divisible by 1001, in other words $nm = 1001k$ with k a positive integer

$$nm = 1001k = 7 \times 11 \times 13k$$

So, n (or m or both) has a factor of 7.

But $n + m = 1001$ was given.

So, $n + m = 7 \times 11 \times 13$

So, $n + m$ also has a factor of 7.

Hence both n and m have a factor of 7.

The argument can be repeated with 11 and 13.

So *n* and *m* have factors of 7, 11 and 13.

That can only mean that both n and m are greater than or equal to 1001.

Since $n \geq 1001$ and $m \geq 1001$ we have $n + m \geq 2002$,

So, if nm is divisible by 1001, then $n + m$ must be greater than 1001.

But $n + m = 1001$ (given) and so the product *nm* cannot be divisible by 1001 if $n + m = 1001$. □

Example 8.4 – no integer solutions

Prove that the equation $x^3 = 99x + 1$ has no integer solutions.

Solution 8.4

Assume that the equation $x^3 = 99x + 1$ does have at least one integer solution and call it k. Hence $k^3 = 99x + 1$.

Now k is either even or odd.

- If k is even then k^3 is even and $99k + 1$ is odd which is not possible.
- If k is odd then k^3 is odd and $99k + 1$ is even which is not possible either.

In both cases we have a contradiction.

Hence our original assumption is false and the equation $x^3 = 99x + 1$ has no integer solutions. □

Example 8.5

Prove the following proposition: Suppose *a* is an integer: If a^2 is even, then *a* is even.

Solution 8.5

Suppose a^2 is even and a is not even.

Then a^2 is even, and a is odd.

Since a is odd, there is an integer c for which $a = 2c + 1$.

Then $a^2 = (2c + 1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1$, so a^2 is odd.

Thus a^2 is even and a^2 is not even, a contradiction. Our proposition is true.

□

Example 8.6

Prove the following proposition:

If a and b are integers, then $a^2 - 4b \neq 2$.

Solution 8.6

Suppose this proposition is false.

In other words, there exist numbers a and b for which a and b are integers but $a^2 - 4b \neq 2$ is false. Or again worded differently: there exist integers a and b for which $a^2 - 4b = 2$.

From the equation it follows that $a^2 = 4b + 2 = 2(2b + 1)$, so a^2 is even.

Since a^2 is even, it follows that a is even, so $a = 2c$ for some integer *c*.

If we now plug in $a = 2c$ in $a^2 - 4b = 2$, we get $(2c)^2 - 4b = 2$ and so $4c^2 - 4b = 2$.

Dividing by 2 gives $2c^2 - 2b = 1$.

Therefore $1 - 2(c^2 - b)$, and since $c^2 - b$ is an integer, it follows that 1 is even. This is a contradiction. Our assumption that our proposition was false….is false.

This means that the proposition is true. □

Example 8.7

Prove the following proposition:

For every real number $x \in \left[0, \frac{\pi}{2}\right]$, we have $\sin x + \cos x \geq 1$.

Solution 8.7

Suppose the statement is not true.

Then there exists an $x \in \left[0, \frac{\pi}{2}\right]$ for which $\sin x + \cos x < 1$.

But recalling the graphs of $\sin x$ and $\cos x$, both are positive for $x \in \left[0, \frac{\pi}{2}\right]$, so $0 \leq \sin x + \cos x < 1$. Thus $0^2 \leq (\sin x + \cos x)^2 < 1^2$, which gives $0^2 \leq \sin^2 x + 2 \sin x \cos x + \cos^2 x < 1^2$. As $\sin^2 x + \cos^2 x = 1$, this becomes $0 \leq 1 + 2\sin x \cos x < 1$, so $1 + 2\sin x \cos x < 1$. Subtracting 1 from both sides gives $2\sin x \cos x < 0$.

But this contradicts the fact that neither $\sin x$ nor $\cos x$ is negative. □

Example 8.8

Up until now examples have been algebraic. Proof by contradiction, however, is more a concept, an idea, which could be used for any mathematical sub-discipline. Let's look at a famous historical problem, and how contradiction can be used to prove it.

The Königsberg bridge problem has been made famous by Leonard Euler. Based on communications with others, people wondered whether it was possible to make a roundtrip in the town of Königsberg, crossing each of the seven bridges $a, b, \ldots, g$ only once, as can be seen in Figure 8.1.

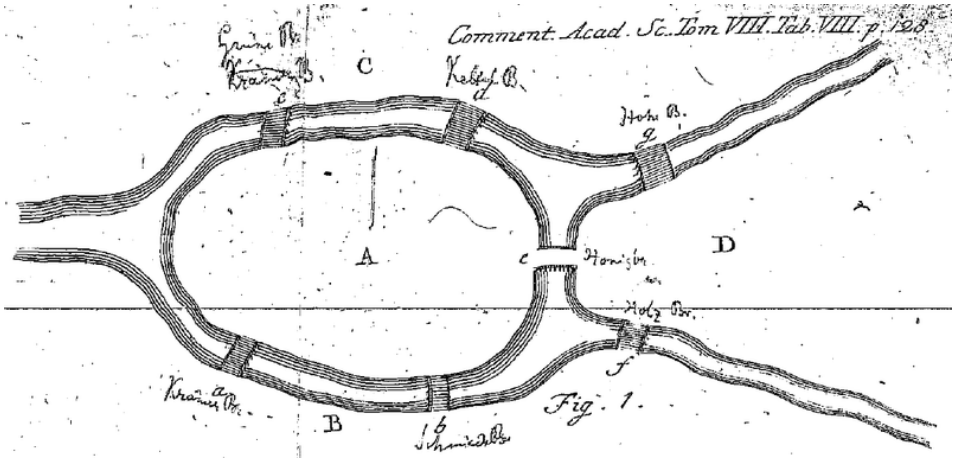


Figure 8.1: Diagram by Leonard Euler from Solutio problematis ad geometriam situs pertinentis . Created 2014 by Ushakaron. Wikimedia commons.

Figure 8.1 shows a stylised version of Königsberg and its seven bridges. Euler first translates the problem to finding a route across the seven bridges as one that would require travelling across at most eight areas. He denoted these with capital letters, and hence crossing seven bridges would be a series of eight capital letters. Then Euler analysed the situation further by looking at simpler examples of landmasses and bridges, for example in Figure 8.2.

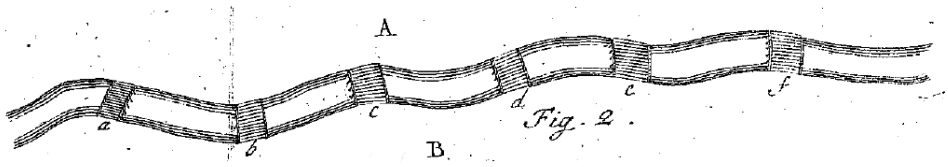


Figure 8.2: Diagram by Leonard Euler from Solutio problematis ad geometriam situs pertinentis . Created 2014 by Ushakaron. Wikimedia commons.

Looking at Figure 8.2 he concluded that "In general, if the number of bridges is any odd number, and if it is increased by one, then the number of occurrences of A is half of the result."[9]

[9] For more extensive information on the problem see https://www.maa.org/press/periodicals/convergence/leonard-eulers-solution-to-the-konigsberg-bridge-problem-the-fate-of-konigsberg

In other words, we could look at the number of bridges leading to an area, and then we can find the number of times that area has to occur -crossing a bridge only once- by adding one and dividing by 2. For area A in Figure 1 that means for five bridges that A must occur three times. Area B, C and D must occur twice because three bridges lead to them. In total, that is 3 (for A) + 2 (for B) + 2 (for C) +2 (for D)=9. But we knew that there only must be eight occurrences for the seven bridges. This is a contradiction. It therefore is impossible to travel the bridges in the city of Königsberg once and only once. Euler then set out to generalise the statement as well. □

8. Exercises[10]

Prove each of the following by contradiction.

1) $\sqrt[3]{2}$ is irrational.

2) $x^4 = 45x + 1$ has no integer solutions.

3) There are no pairs of positive integers x and y such that $x^2 - y^2 = 10$.

4) For all integers n, if $3n + 2$ is odd then n is odd.

5) For all integers n, if $n^3 + 5$ is odd then n is even.

6) There exist no integers a and b for which $21a + 30b = 1$.

7) The sum of a rational number and an irrational number is irrational.

8) If *a* and *b* are positive real numbers, then $a + b \leq 2\sqrt{ab}$

9) There are infinitely many primes *p* such that $p + 2$ is **not** prime.

10) Suppose a and b and c are positive real numbers. If $ab = c$ then $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.

[10] The solutions are here
http://blog.soton.ac.uk/mshe/solutions-mit-proof-booklet/

9. How do I know which proof type I need to use?

In the previous sections of this booklet, we have discussed different types of proof: by exhaustion, direct, by induction, by contradiction.

The next question is:

How do I know which one to use when I have been given only a statement?

This is a bit tricky and requires practice to recognise standard ways to prove a statement. Sometimes you might find that the question provides you with some hints as to which type of proof you should follow. Other times you need to trial different types prior to deciding which one is appropriate. This is what Mathematicians do as well, when it is not obvious which type of proof is the best they try a few different methods and then they decide which one is the correct one.

To prove that the statement is true (or false) we have to construct a mathematical argument using correct reasoning and ensure that our arguments follow properly from each other.

A very useful question to ask yourself when you are deciding which type of proof to use is the following:

> Is your statement of the type "If A, then B"? In that case, your proof would either be Direct proof or Proof by Contradiction.

Let's briefly remember what we do in each type.

In the direct proof, you have to prove a conditional statement: "If A is true, then B is true".

You start from A and using axioms (assumptions) you demonstrate that you can get to B.

In the proof by contradiction, you have to prove a conditional statement "If A is true, then B is true". You start by assuming that A is true and try to show that B is false. This leads you to find something false (a contradiction). Which means that B is true.

Let's have a look at some examples:

Prove the following statements:

1. If m and n are odd integers then $m + n$ is an even integer.
2. If n is an odd integer then $n^3 + 1$ is an even integer.

Let's first try them both with direct proof. So, we start with the A being true and we want to show that B is true.

1. If m and n are odd integers then $m + n$ is an even integer.

   It is really important to initially translate the words into the appropriate symbols.

   "If m and n are odd integers" means that $m = 2k + 1$ and $n = 2l + 1$ where k, l are integers. *Notice that we are very careful with our use of symbols. You need to make sure that you do not use the same symbol for different things.*

   Now that you have translated the phrase "If m and n are odd integers" in symbols, you need to try to get from "If m and n are odd integers" to "then $m + n$ is an even integer" which means that you have to show that $m + n = 2t$ where t is an integer.

   So, your proof should have the following structure:
   $m = 2k + 1, n = 2l + 1$

…and then some steps

Then $m + n = 2t$

Let's try to fill in the missing steps now.

You have that $m = 2k + 1, n = 2l + 1$ and you want to find a statement about their summation. So you need to sum the two statements you have about m and n.

$m + n = 2k + 1 + 2l + 1$	Now you can notice that you can start collecting like terms
$= 2k + 2l + 2$	You can see that all the terms have a common factor of 2
$= 2(k + l + 1)$	Now you can name the sum in the brackets *t* as that sum is an integer.
$= 2t$, where $t = k + l + 1$	

So, you have shown that If m and n are odd integers then $m + n$ is an even integer.

Let's try the other statement now.

2. If n is an odd integer then $n^3 + 1$ is an even integer.

Does this seem reasonable? One way to convince yourself if to try with a selection of values. For $n = 1$, $(1)^3 + 1 = 1 + 1 = 2$

For $n = 2$, $(2)^3 + 1 = 8 + 1 = 9$

And we have found a value of n for which the statement is false.

Can we do this in general?

Let's assume that $n^3 + 1$ is an even integer, ie. $n^3 + 1 = 2k$ where k is an integer.

If n is odd, $n = 2p + 1$, then $n^3 + 1 = (2p + 1)^3 + 1 = (2p)^3 + (1)^3 + 3(2p)(1)(2p + 1) + 1$.

This looks messy, but let's examine this term by term:

The first term is even: $(2p)$^3 $= 2(4p^3)$

The second term is odd (1)^3 $= 1$

The third term is even $6p(2p + 1)$

The final term, 1, is odd

Therefore, when n is odd, $n^3 + 1 = 2k$, is even.

The next parts were going to be…

Exhaustion:

Proving that each case is true

Does the statement say it is only valid for a set number of cases?

Induction:

If the statement is meant to be true for many different values

Does the statement say A is true for all n?

Examples:

Show that the difference between two consecutive square numbers is always odd.	Show that the difference between two consecutive square numbers between 9 and 81 is odd.	Show that the sum of the first n square numbers is given by $\frac{n(n+1)(n+2)}{6}$.	Show that if the square of a number is positive, the number is positive.
If we have A (two consecutive square numbers), then B (the difference is odd). Looks like a direct proof!	The square numbers between 9 and 81 are: 16, 25, 36, 49, 64 These can be checked individually.	This statement has to be true for all n. Looks like proof by induction.	But $(-3)^2 = 9$ Looks like proof by contradiction

	Looks like a proof by exhaustion.		

A quest for prime number formulas

Let's do a more extensive exploration of a statement and its proof. It will demonstrate how finding a proof can sometimes be a real quest. The quest ends with a proof by contradiction.

Many quadratic formulas generate long strings of prime numbers. The formula $n^2 - n + 41$ is a much-quoted example.

First conjecture

$n^2 - n + 41$ is always prime.

Let's first test the conjecture with values of n up to 10.

$\boldsymbol{n}$	1	2	3	4	5	6	7	8	9	10
$\boldsymbol{n^2 - n + 41}$	41	43	47	53	61	71	83	97	113	131

Yes, these are all prime numbers[11].

The conjecture is true for all values of n up to and including 40.

However, when $n = 41$, $n^2 - n + 41 = 41^2$, when $n = 42$, $n^2 - n + 41 = 41 \times 43$.

And there are more values of n for which $n^2 - n + 41$ is divisible by 41.

[11] You can check manually, but there also are websites that can check this for you, for example http://www.math.com/students/calculators/source/prime-number.htm

So, we formulate a second conjecture.

Second conjecture

No quadratic expression in n is prime for all integral (*another word for integer*) values of n.

Let's start by looking at a few quadratic expressions in n, for example:

$$n^2 + 7n + 5$$

$$n^2 - 1$$

$$3n^2 + 2$$

You can fairly quickly find values of n for which the expression is not prime, for example for the first one $n = 3$ gives 35, the second one $n = 3$ gives 8, and the last one $n = 4$ gives 50. It is likely that the more quadratic expressions you try, the more you will become convinced of the truth of the second conjecture. But, as you know, it is not sufficient simply to try lots of examples – you may miss the one example which turns out to be a counter-example.

This process is an exciting phase of mathematical problem solving where all sorts of ideas must be tried out as you search for either a convincing proof or a counter-example. Let's try to prove the conjecture now.

First attempted proof

The general quadratic is of the form $an^2 + bn + c$.

Putting $n = c$ gives $ac^2 + bc + c = c(ac + b + 1)$, which is not prime because it is divisible by both $ac + b + 1$ and c. Therefore no quadratic expression in *n* can be prime for all integral values of n.

However, this proof doesn't work. Which particular cases spoil the 'proof' (think of the definition of a prime number)?

Second attempted proof (by contradiction)

Suppose $an^2 + bn + c$ is prime for all integers n.

In particular, for $n = 1$, $a + b + c$ must be prime.

Let $a + b + c = p$,

For $n = 1 + p$,

$$an^2 + bn + c = a(p + 1)^2 + b(p + 1) + c$$

$$= ap^2 + 2ap + bp + a + b + c$$

$$= ap^2 + 2ap + bp + p$$

$an^2 + bn + c$ is therefore $(ap + 2a + b + 1)p$.

Similarly, we can find a similar expression for $an^2 + bn + c$ when $n = 1 + 2p$.

So, $an^2 + bn + c$ is divisible by p when $n = 1$, $n = 1 + p$ and $n = 1 + 2p$.

If it is prime for each of these values then $an^2 + bn + c$ must equal *p* itself and we would have three points on a horizontal line.

This is not possible for a quadratic.

So $an^2 + bn + c$ is *not* prime for at least one of these three values.

Combining techniques

The following proof combines proof types. The overall approach is direct, but inside the direct proof is a separate proof by contradiction.

Example 8.9

Prove the following proposition:

Every nonzero rational number can be expressed as a product of two irrational numbers.

Solution 8.9

The proposition first can be reworded: If r is a nonzero rational number, then r is the product of two irrational numbers.

Suppose r is a nonzero rational number. Then $r = \frac{a}{b}$ for integers a and b. r can also be written as a product of two numbers:

$$r = \sqrt{2} \cdot \frac{r}{\sqrt{2}}$$

We know $\sqrt{2}$ is irrational (see example 8.1), so to complete the proof we should show that $\frac{r}{\sqrt{2}}$ also is irrational. We now use proof by contradiction.

Suppose $\frac{r}{\sqrt{2}}$ is rational. This means that $\frac{r}{\sqrt{2}} = \frac{c}{d}$ for integers c and d, so $\sqrt{2} = r\frac{d}{c}$.

But we know that $r = \frac{a}{b}$ and combining both equations gives:

$$\sqrt{2} = r\frac{d}{c} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc}$$

This means $\sqrt{2}$ is rational, a contradiction. Therefore $\frac{r}{\sqrt{2}}$ is irrational.

As a consequence, $r = \sqrt{2} \cdot \frac{r}{\sqrt{2}}$ is a product of two irrational numbers. □

10. Are the following proofs correct?

Sometimes a proof can look convincing, but may not actually be valid. It is a good practice to always go through the steps of the proof in detail and check whether you agree with the correctness of each one.

Example 10.1

Suppose that $a = b$

Hence $a^2 = ab$

$a^2 - b^2 = ab - b^2$

$(a - b)(a + b) = b(a - b)$

$a + b = b$

$b + b = b$

$2b = b$

$2 = 1$

We seem to have proved using algebra that $2 = 1$, which we know is not true. This is known as a Mathematical fallacy – we have used what may appear to be logical steps but the issue is between line 4 and 5. We cannot divide by $a - b$, because it equals 0 since $a = b$. Division by zero is undefined which makes the proof invalid.

It can be very difficult to identify why a proof is invalid. For example,

Example 10.2

Prove that $\sqrt{9}$ is irrational

Assume $\sqrt{9} = \frac{a}{b}$ where $a, b \in \backslash Z$ and a, b are co-prime (have no common factor other than 1)

$$9 = \frac{a^2}{b^2}$$

$$9b^2 = a^2$$

Therefore a^2 is a multiple of 9 so a is a multiple of 9 and we can let $a = 9k$.

$$\text{Then } 9b^2 = (9k)^2$$

$$9b^2 = 81k^2$$

$$b^2 = 9k^2$$

Therefore $b^2$is a multiple of 9 so b is a multiple of 9. a, b are both multiples of 9 so cannot be co-prime. By contradiction, $\sqrt{9}$ is irrational.

Here they have used incorrect reasoning to conclude that a is a multiple of 9 because a^2 is. Sometimes when you are trying to unpick algebraic reasoning you can try some values and look for a counter-example to help identify where the error is.

10. Exercises[12]

Can you identify what is wrong with the following proof?

Exercise 10.1

The following statement is true but the proof by induction is wrong. Can you find the error and write the correct proof?

Prove that for an odd positive integer $n, f(n) = 7^n + 1$ is divisible by 8.

Step 1 – *Base Case*

When $n = 1$ then $f(1) = 7^1 + 1 = 7 + 1 = 8$. And 8 is divisible by 8 so, the statement holds for $n = 1$.

Step 2 – *Induction hypothesis*

You assume that the statement holds for k. This means that $f(k) = 7^k + 1$ is a multiple of 8. You can rewrite this as $7^k + 1 = 8m$ where m a positive integer.

Step 3 – *Induction step*

You need to show that the statement holds for $n = k + 1$. In other words you need to show that $7^{k+1} + 1 = 8l$ where l a positive integer.

You will start from the left-hand side. You have:

$$\begin{aligned} 7^{k+1} + 1 &= 7^k 7 + 1 \\ &= 7^k 7 + 7 - 6 \\ &= 7(7^k + 1) - 6 \\ &= 7 \times 8m - 6 \end{aligned}$$

[12] The solutions are here
http://blog.soton.ac.uk/mshe/solutions-mit-proof-booklet/

$= 8(7m) - 6$, which is not a multiple of 8

Can you identify what is wrong with the following proof?

Exercise 10.2

$$\cos^2\theta + \sin^2\theta \equiv 1$$

Hence

$$\cos^2\theta \equiv 1 - \sin^2\theta$$

$$cos\theta \equiv \sqrt{1 - \sin^2\theta}$$

$$1 + cos\theta \equiv 1 + \sqrt{1 - \sin^2\theta}$$

Now this is true for all values of θ, so substitute $\theta = \pi$ to obtain

$$1 + cos\pi = 1 + \sqrt{1 - \sin^2\pi}$$

$$1 + -1 = 1 + \sqrt{1 - 0^2}$$

$$0 = 2$$

11. Conclusion

This booklet aimed to give an overview of the challenging topic of ‘proof’. We explained what proofs were and gave several types/methods of proof. It is not always easy to see which types of proof you need in what circumstances. Only after a lot of practice and immersing yourself in the world of mathematics, you will become more proficient in recognising which approaches to proof you might use when. However, when you do, you will more and more appreciate the beauty of proofs as well. Proofs are the building blocks of mathematics; after all, if we do not ‘prove’ our claims and statements, it could be conceived as little more than speculation.

https://doi.org/10.5258/SOTON/P1082

University of Southampton

One of the important building blocks of mathematics is proof. In this booklet we explain what constitutes a good proof, and present several types/methods of proof. The booklet gives numerous examples and exercises.