## SECTION F **PROOF BY CONTRADICTION**

By the end of this section you will be able to
- understand the procedure for proof by contradiction
- negate a given proposition
- construct a proof by contradiction

In this section we prove two famous results from ancient Greek mathematics using proof by contradiction. They are '$\sqrt{2}$ is an irrational number' and 'there are an infinite number of primes'. Both these results belong to an area of mathematics called number theory. This is one of the most beautiful fields of mathematics and is the study of numbers and their properties.

### F1 **Procedure for Proof by Contradiction**

*What is meant by the term "contradiction" in everyday language?*
Normally it means opposite to a statement. In an earlier section we defined contradiction. *Do you remember what contradiction means in mathematical logic?*
A proposition which is **always false** is called a contradiction. *Can you think of any examples of contradiction?*
Let $P$ be a proposition then

$$P \text{ and } (\text{not } P) \text{ is a contradiction}$$

For example

$$x^2 - 1 = 0 \ [\text{Zero}] \quad \text{and} \quad x^2 - 1 \neq 0 \ [\text{Not Equal to Zero}]$$

is a contradiction. Another example, let $n$ be an integer then

'$n$ is even' and '$n$ is odd' is a contradiction

Suppose we want to prove a proposition $P$ then the procedure for proof by contradiction is as follows:

1. We assume the opposite that is $(\text{not } P)$ is true.
2. We follow our logical deductions in the proof and this will lead to a contradiction.
3. Since our assumption in part 1 of $(\text{not } P)$ is true leads to a contradiction therefore $(\text{not } P)$ is false.
4. Since $(\text{not } P)$ is false therefore our given proposition $P$ must be true.

This method is called **proof by contradiction**. The tradition name of this proof is "reductio ad absurdum" which means reduction to absurdity.
The challenge in these proofs is stating the negation of the given proposition $P$ that is writing down $(\text{not } P)$ and deducing a contradiction. Before we construct proofs by contradiction we investigate the negation of a proposition.

### F2 **Negation of a Proposition**

Consider the negation of the following propositions.
Let $P$ be the proposition 'there are an **infinite** number of primes'.
*What is $(not\ P)$ equal to?*

The proposition $(\text{not } P)$ is

'there are a **finite** number of primes'

Let $P$ be the proposition 'there are **some** integers which are odd'.
*What is the negation of P, that is* $(not\ P)$*, equal to in this case?*

The proposition $(\text{not } P)$ is

'there are **no** integers which are odd'

Let $R$ be the proposition 'if $n^2$ is even then $n$ is even'.
*What is* $(not\ R)$ *equal to?*

The proposition $(\text{not } R)$ is more difficult to write down because we have a $P \Rightarrow Q$ proposition where

$$\text{if } \underbrace{n^2 \text{ is even}}_{=P} \text{ then } \underbrace{n \text{ is even}}_{=Q}$$

*Why is 'if* $n^2$ *is even then* $n$ *is even' a* $P \Rightarrow Q$ *proposition?*
Because it has an 'if and then' in the statement. Thus proposition $R$ is $P \Rightarrow Q$.
*Therefore* $(not\ R)$ *is not* $(P \Rightarrow Q)$ *but what is not* $(P \Rightarrow Q)$ *equal to?*
By a truth table we can show that

$$\left[\text{not } (P \Rightarrow Q)\right] \equiv \left[P \wedge (\text{not } Q)\right] \qquad [\text{Equivalent}]$$

[You are asked to prove this result in Exercise 1(f)].
'$P \wedge (\text{not } Q)$' is '$P$ and $(\text{not } Q)$' which means that $(\text{not } R)$ equals '$P$ and $(\text{not } Q)$'. Hence $(\text{not } R)$ is

$$\text{'} \underbrace{n^2 \text{ is even}}_{P} \text{ and } \underbrace{n \text{ is odd}}_{\text{not } Q} \text{'}$$

Consider another proposition $Q$ given by 'it is **impossible** to find three non-zero integers $a$, $b$ and $c$ such that

$$a^n + b^n = c^n \text{ where } n \geq 3\text{'}$$

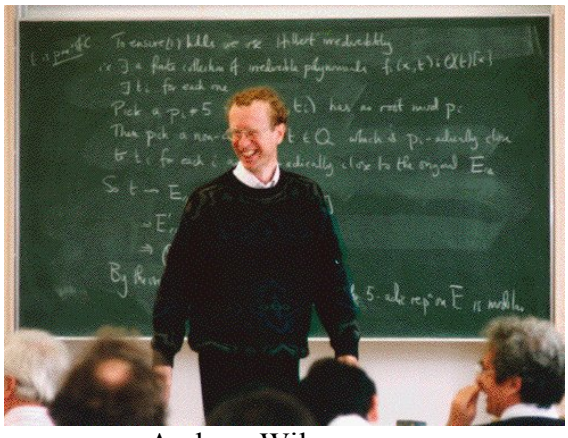
The negation of this, or $(\text{not } Q)$, is
'it is **possible** to find three non-zero integers $a$, $b$ and $c$ such that

$$a^n + b^n = c^n \text{ where } n \geq 3\text{'}$$

This proposition $Q$ is the famous Fermat's Last Theorem. Fermat was a French Lawyer and did mathematics in his spare time. The reason why Fermat's last theorem is popular is because Fermat stated this theorem around 1630 and added that "I have discovered a proof but the margin is too small to write the proof".

Fig 2


Pierre de Fermat


Andrew Wiles

However for over 350 years no one could find a proof for this theorem. Eventually in 1993 Andrew Wiles a British mathematician working in Princeton USA provided a proof at Cambridge. Initially this proof had a flaw but that was resolved in 1994.

Fermat's last theorem states that the equation

$$a^n + b^n = c^n \qquad \text{for} \quad n \geq 3$$

has **no** integer solutions. *What does this mean?*

We know there are integer solutions for $n = 2$ because it often crops up in Pythagoras's theorem:

$$3^2 + 4^2 = 5^2, \quad 5^2 + 12^2 = 13^2, \quad 8^2 + 15^2 = 17^2, \ldots$$

However when $n \geq 3$ we **cannot** find integer solutions to the above equation. This means there are no integers $a$, $b$ and $c$ such that

$$a^3 + b^3 = c^3, \quad a^4 + b^4 = c^4, \quad a^5 + b^5 = c^5, \ldots$$

Let *P* be another proposition '**every** non-zero real number has a unique reciprocal'. Then $(\text{not } P)$ is

'**there is** a non-zero real number whose reciprocal is **not** unique'.

*What does this mean?*

There is a number (not zero) which has **more than** one reciprocal. We will do an example involving reciprocals in the next subsection.

In general we use the negation of a given proposition, $(\text{not } P)$, to lead to a contradiction in the proof of the proposition.

## F3 **Proof by Contradiction**

In this subsection we look at examples of proof by contradiction. The proof is carried out by using the procedure outlined in subsection F1.

We need to define the term reciprocal mentioned above for the next example.

Definition (1.10). Let $x$ be a non-zero real number. The reciprocal of this real number, $x$, is a real number $y$ which has the property

$$xy = 1$$

For example the reciprocal of 3 is $\frac{1}{3}$, reciprocal of $-2$ is $-\frac{1}{2}$, reciprocal of $\pi$ is $\frac{1}{\pi}$ reciprocal of $-\frac{2}{3}$ is $-\frac{3}{2}$ etc.

### Example 38

Prove the following:

Proposition (1.11). Every non-zero real number has a unique reciprocal.

Comment. *What does the word 'unique reciprocal' mean?*

There is **only** one reciprocal.

We can use proof by contradiction to prove this proposition. *To use this approach, what do we need to do first?*

Need to state the negation of the proposition. *What is the negation of the given proposition?*

There is a non-zero real number whose reciprocal is **not** unique. *What does this statement mean?*

There is a non-zero real number such that it has more than one reciprocal.

*Proof*. Suppose there is a non-zero real number call it *x* whose reciprocal is **not** unique. Consider it has two different reciprocals call them *y* and *z*.
Then *y* does **not** equal *z*, that is $y \neq z$ . *Why not?*
Because if $y = z$ then *x* has the same (one) reciprocal and so that means it is unique and there is nothing left to prove.
Since *y* and *z* are the reciprocals of *x* therefore by definition (1.10) we have

$$xy = 1 \text{ and } xz = 1$$

Because they are both equal to 1 so we can equate them

$$xy = xz$$

Since *x* is non-zero we can divide through by *x* which gives

$$y = z$$

But above we had $y \neq z$ . We cannot have $y = z$ and $y \neq z$ . Hence this contradicts the first line of the proof, that there is a non-zero real number whose reciprocal is **not** unique. Thus the given proposition must be true.

■

*What exactly is the meaning of the negation of the original proposition in the above proof?*
If it is **not** unique means there must be more than one so we considered 2 reciprocals (of course we could have considered 3 or even more but it just makes the proof untidy and unreadable).
Next we applied logical mathematical deductions assuming 2 reciprocals in the above proof and this resulted in a contradiction. Since we had a contradiction this means that our assumption of 2 reciprocals must have been false. Hence the given proposition 'every non-zero real number has a unique reciprocal' must be true.
Proposition (1.11) is an important result in the mathematics of real numbers. The reciprocal is also called the **multiplicative inverse**. In general if $x$ is a non-zero real number then the **unique** reciprocal (or unique multiplicative inverse) of $x$ is $\frac{1}{x}$.

Example 39

Prove the following:
Lemma (1.12). If $n^2$ is even then $n$ is even.

Note. *What is the negation of this lemma?*
$n^2$ is even and $n$ is odd. (Remember we stated this in subsection F2).
*Why have we called this result a lemma rather than a proposition?*
Lemma is a proposition (or a theorem) which is used to prove another proposition or theorem. We use this lemma to prove $\sqrt{2}$ is irrational in the next example.
*Proof*. (By contradiction).
Suppose $n^2$ is even and $n$ is odd. [Negation of the given lemma].
Since *n* is odd we can write *n* as

$$n = 2m + 1 \text{ where } m \text{ is an integer}$$

Squaring both sides gives:

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 \qquad [\text{Expanding}]$$

$$= 2(2m^2 + 2m) + 1 \qquad [\text{Rewriting } 4 = 2(2)]$$

We have $n^2 = 2(\text{Integer}) + 1$ which means it is odd. Hence $n^2$ is odd and it is even

because in the first line of the proof we said '$n^2$ is even'. This is a contradiction. Our supposition $n^2$ is even and $n$ is odd is false therefore our given proposition is true.

■

In the above proof the **negation** of the given proposition leads to the contradiction, $n^2$ is even and $n^2$ is odd, therefore the proposition itself must be true.

In the next example we prove that $\sqrt{2}$ is **not** a rational number. *What is a rational number?*

Definition (1.13). A rational (ratio) number is an integer or is written as a fraction of 2 integers, $p$ and $q$, denoted by $\frac{p}{q}$.

For example $\frac{2}{3}$, $-\frac{1}{3}$, $3=\frac{3}{1}$, $-\frac{10\,000}{6}$ and $9=\frac{18}{2}$ are all rational numbers.

We can write each rational number $\frac{p}{q}$ in its simplest form. For example

$$\frac{4}{6}=\frac{2}{3},\quad \frac{2}{4}=\frac{1}{2},\quad \frac{9}{6}=\frac{3}{2},\quad \frac{15}{9}=\frac{5}{3}\ \text{etc}$$

A rational number in its simplest form is when it is written with **no** factors in common apart from 1. *What does the term **factor** mean?*

A factor is a number that divides another (or the same) number. For example $2 \mid 4$ [2 divides 4] and we say 2 is a factor of 4. Clearly 1 is always a factor of every number.

However we want to prove $\sqrt{2}$ is **not** a rational number. *Can you think of where $\sqrt{2}$ crops up?*

In a right-angled triangle with smaller sides of unit length as shown in Fig 3.

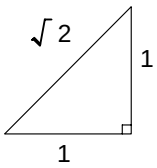



Fig 3

Example 40

Prove the following:

Theorem (1.14). $\sqrt{2}$ is **not** a rational number.

*Proof*. (By contradiction).

Suppose $\sqrt{2}$ is a rational number. By definition (1.13) we can write $\sqrt{2}$ as

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

where *p* and *q* are integers with **no** factors in common other than 1. We say $\frac{p}{q}$ is in its simplest form. If they do have factors in common then cancel them down to its simplest form. Multiplying both sides by $q$ gives

$$p=\sqrt{2}q$$

$$p^2=2q^2 \qquad \text{[Squaring Both Sides]}$$

Since $p^2$ is a multiple of 2 therefore it is even. By lemma (1.12) we have

$$p^2 \text{ is even} \Rightarrow p \text{ is even}$$

Since $p$ is even we can write this as

$$p = 2m \text{ where } m \text{ is an integer}$$

Hence $p^2 = (2m)^2 = 4m^2$

Substituting this, $p^2 = 4m^2$, into the above, $2q^2 = p^2$, gives

$$2q^2 = 4m^2$$

$$q^2 = 2m^2 \quad [\text{Dividing by } 2]$$

Since $q^2$ is a multiple of 2 therefore $q^2$ is even. Again by lemma (1.12) we have

$$q^2 \text{ is even} \Rightarrow q \text{ is even}$$

Hence we have **both** $p$ and $q$ are even. This means that both $p$ and $q$ have a common factor of 2. This is a contradiction. *Why?*
Because at the start of the proof we said that $p$ and $q$ have **no** factors in common (apart from 1) and now we have shown that $p$ and $q$ have a common factor of 2. Our supposition '$\sqrt{2}$ is a rational number' must be false. Hence $\sqrt{2}$ is **not** a rational number.

■

A number which is **not** a rational number is called an **irrational** number. We say $\sqrt{2}$ is an irrational number. $\sqrt{2}$ was the first known irrational number and again it was the Greeks who produced the first proof of the irrationality of $\sqrt{2}$.
Other examples of irrational numbers are

$$\sqrt{2},\quad \sqrt{3},\quad \sqrt{5},\quad \pi \text{ and } e$$

In fact square root of a non-square number is irrational therefore

$$\sqrt{6},\quad \sqrt{7},\quad \sqrt{8} \text{ and } \sqrt{10} \text{ are } \textbf{all} \text{ irrational numbers}$$

$\sqrt{9}$ is not irrational because 9 is a square number. A square number is an integer of the form $n^2$ where $n$ is an integer. More about irrational and other types of numbers in the next chapter.
Next we prove there are an infinite number of primes. Euclid proved that there are an infinite number of primes by applying a proof by contradiction. This is the first known application of proof by contradiction.

Euclid 320BC to 260BC

Fig 4

Lemma (1.12) $n^2$ is even $\Rightarrow$ $n$ is even

Euclid is known to be born around 320BC and died 260BC and taught at Alexandria in Egypt. He has become to be known as the author of the great work called 'Elements'. Euclid's Elements has become the second most published work after the bible.
Up until the 1970's school mathematics in Britain consisted of proving geometric concepts from Euclid's Elements. Actually there is a subject called "Euclidean Geometry" which is based on the work set out in Euclid's Elements.

*What is a prime number?*

Definition (1.15). A prime number, or just prime, is an integer greater than 1 whose only positive divisors are 1 and itself.

For example 2, 3, 5, 17, 19, 43 and 163 are **all** primes.
The primes have very important properties and one these is the following:

Example 41

Prove the following:
Lemma (1.16). Every integer greater than 1 is divisible by a prime.
*Proof*. See Exercise 1(f).

We will use this lemma to prove an important theorem about the number of primes.

Example 42

Prove the following:
Theorem (1.17). There are an infinite number of primes.
*Proof*. (By contradiction).
Suppose there are a finite number of primes and these are

$$2, 3, 5, 7, 11,\ldots, Q$$

where $Q$ is the largest prime. Consider the number

$$n=\left(2\times3\times5\times7\times11\times...\times Q\right)+1 \qquad (*)$$

Clearly $n$ is greater than 1 so by the above lemma (1.16) it is divisible by a prime say $p$. That is $p \mid n$. This prime, $p$, must be amongst the list

$$2, 3, 5, 7, 11,\ldots, Q$$

because these are the **only** primes we have. Since $p$ is in the list therefore $p$ divides

$$2\times3\times5\times7\times11\times...\times p\times...Q$$

That is $p \mid \left(2\times3\times5\times...\times Q\right)$. We already had $p \mid n$. By proposition (1.7) we have

$$p \mid \left[n-\left(2\times3\times5\times7\times11\times...\times Q\right)\right]$$

*What is* $n-\left(2\times3\times5\times7\times11\times...\times Q\right)$ *equal to?*

From (*)

$$n-\left(2\times3\times5\times7\times11\times...\times Q\right)=1$$

Hence the prime $p$ divides 1 or in symbolic form $p \mid 1$. This is impossible because by the abovedefinition (1.15) a prime is an integer greater than 1 so $p$ **cannot** be a prime. This is a contradiction. *Why?*
Because earlier we stated that $p$ was a prime and now we are claiming that $p$ is not a prime. Our supposition 'there are a **finite** number of primes' must be **false**.
Hence there are an **infinite** number of primes. ■

Proposition (1.7). If $a \mid b$ and $a \mid c$ then $a \mid \left(bm+cn\right)$ for any $m$ and $n$

Primes have been studied for the past $3\,000$ years. In this time mathematicians have discovered many fascinating results concerning primes. However research into primes continues today with many questions still unresolved. For example Goldbach's conjecture, which says:
'Every even number greater than 2 is the sum of two primes'. Examples are

$$6 = 3 + 3$$
$$8 = 5 + 3$$
$$100 = 97 + 3$$
$$102 = 97 + 5$$
$$....$$

This result has **not** been proven that is why it is still a conjecture. *What does the word conjecture mean?*
A statement which may be true but a prove has **not** been discovered yet. Even if today's computers show that Goldbach's conjecture is true for the first trillion numbers does **not** mean the conjecture is correct. Moreover this evaluation on a computer is not a proof.

SUMMARY
The procedure for proof by contradiction of a proposition $P$ is:
Write down the negation $(\text{not } P)$ in the first line of the proof. Using this deduce a contradiction. Since we have a contradiction therefore $(\text{not } P)$ is false which means that the given proposition $P$ is true.
The challenge in these proofs is writing down the negation of the given proposition and deducing a contradiction.
We can use this method to prove important mathematical results such as '$\sqrt{2}$ is irrational' and 'there are an infinite number of primes'.
Lemma is a proposition which is used to prove another proposition.