P2 Chapter 1: Algebra Techniques

Proof by Contradiction

Proof By Contradiction

✏ To prove a statement is true by contradiction:

- **Assume** that the statement is in fact **false**.
- Prove that this would **lead to a contradiction**.
- Therefore we were wrong in assuming the statement was false, and therefore it must be true.

Prove that there is no greatest odd integer.

Assume that there is a greatest odd integer, n.

Then $n + 2$ is an odd integer which is larger than n.
This contradicts the assumption that n is the greatest odd integer.

Therefore, there is no greatest odd integer.

How to structure/word proof:

1. "Assume that *[negation of statement]*."
2. [*Reasoning followed by…*] "*This contradicts the assumption that…*" or "*This is a contradiction*".
3. "Therefore [*restate original statement*]."

Negating the original statement

The first part of a proof by contradiction requires you to negate the original statement. What is the negation of each of these statements? ***(Click to choose)***

"There are infinitely many prime numbers."

"All Popes are Catholic."

"If it is raining, my garden is wet."

"There are infinitely many non-prime (i.e. composite) numbers."

"There are finitely many prime numbers."

"There are finitely many non-composite numbers."

"There exists a Pope who is not Catholic."

"No Popes are Catholic."

"Harry Potter is the Pope."

"It is not raining and my garden is dry."

"It is not raining and my garden is wet."

"It is raining and my garden is not wet."

Comments: The negation of "all are" isn't "none are". So the negation of "everyone likes green" <u>wouldn't</u> be "no one likes green", but: "not everyone likes green". Do not confuse a 'negation' with the 'opposite'.

Comments: If you have a <u>conditional</u> statement like "*If A then B*", then the negation is "*A and not B*", i.e. the condition is true, but the conclusion is false/negated.

More Examples

Prove by contradiction that if n^2 is even, then n must be even.

? Assumption

? Show contradiction

? Conclusion

Remember the negation of “if A then B” is “A and not B”.

More Examples

Prove by contradiction that if n^2 is even, then n must be even.

Assume there exists a number n such that n^2 is even, but n is not even.

Remember the negation of "if A then B" is "A and not B".

n is odd therefore $n = 2k + 1$ for some integer k.

$$\begin{aligned} n^2 &= (2k+1)^2 = 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

which is odd.

This contradicts the assumption that n^2 is even.

Therefore if n^2 is even then n must be even.

More Examples

Prove by contradiction that $\sqrt{2}$ is an irrational number.

? Assumption

? Show contradiction

? Conclusion

A **rational number** is one that can be expressed in the form $\frac{a}{b}$ where a, b are integers.

An **irrational** number cannot be expressed in this form, e.g. $\pi, e, \sqrt{3}$.

The set of all rational numbers is $\mathbb{Q}$ (real numbers: $\mathbb{R}$, natural numbers: $\mathbb{N}$, integers: $\mathbb{Z}$).

This is the standard (and well known) proof for the irrationality of $\sqrt{2}$. Here's Dr Frost's non-standard but quicker proof:

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

If a number is square then the powers in the prime factorisation are even. The power of 2 on the RHS is therefore even, but odd on the LHS (due to the extra 2). This is a contradiction.

More Examples

Prove by contradiction that $\sqrt{2}$ is an irrational number.

Assume that $\sqrt{2}$ is a rational number.
Then $\sqrt{2} = \frac{a}{b}$, where a and b are integers and $\frac{a}{b}$ is a fraction in its simplest form.

$$\therefore 2 = \frac{a^2}{b^2} \quad \Rightarrow \quad 2b^2 = a^2$$

Since LHS is even, a^2 is even, and therefore a is even.
Therefore let $a = 2k$ where k is an integer.

$$2b^2 = (2k)^2 = 4k^2$$
$$b^2 = 2k^2$$

Since RHS is even, b^2 is even, and therefore b is even.
But then a and b are both even, contradicting that $\frac{a}{b}$ is a fraction in its simplest form.

Therefore $\sqrt{2}$ is irrational.

A **rational number** is one that can be expressed in the form $\frac{a}{b}$ where a, b are integers.

An **irrational** number cannot be expressed in this form, e.g. $\pi, e, \sqrt{3}$.

The set of all rational numbers is $\mathbb{Q}$ (real numbers: $\mathbb{R}$, natural numbers: $\mathbb{N}$, integers: $\mathbb{Z}$).

This is the standard (and well known) proof for the irrationality of $\sqrt{2}$. Here's Dr Frost's non-standard but quicker proof:

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

If a number is square then the powers in the prime factorisation are even. The power of 2 on the RHS is therefore even, but odd on the LHS (due to the extra 2). This is a contradiction.

More Examples

Prove by contradiction that there are infinitely many prime numbers.

? Assumption

? Show contradiction

? Conclusion

This proof is courtesy of Euclid, and is one of the earliest known proofs.

More Examples

Prove by contradiction that there are infinitely many prime numbers.

This proof is courtesy of Euclid, and is one of the earliest known proofs.

Assume that there is a finite number of prime numbers.
Therefore we can list all the prime numbers:

$$p_1, p_2, p_3, \dots, p_n$$

Consider the number:

$$N = (p_1 \times p_2 \times \cdots \times p_n) + 1$$

When you divide N by any of $p_1, p_2, \dots, p_n$, the remainder will always be 1.
Therefore N is not divisible by any of these primes.

Therefore N must itself be prime, or its prime factorisation contains only primes not in our original list.
This contradicts the assumption that $p_1, p_2, \dots, p_n$ contained the list of all prime numbers.

Therefore, there are an infinite number of primes.

Exercise 1.1

Pearson Pure Mathematics Year 2/AS
Page 1

Extension

[STEP I 2008 Q1] What does it mean to say that a number x is rational?
Prove by contradiction statements A and B below, where p and q are real numbers.

A: If pq is irrational, then at least one of p and q is irrational.
B: If $p + q$ is irrational, then at least one of p and q is irrational.

Disprove by means of a counterexample statement C below, where p and q are real numbers.

C: If p and q are irrational, then $p + q$ is irrational.

Note: $\boldsymbol{e}$ is Euler's Number and you will encounter it later at A Level. But for the moment, you only need to know it is an irrational number, like π.

If the numbers e, π, π^2, e^2 and $e\pi$ are irrational, prove that at most one of the numbers $\pi + e, \pi - e, \pi^2 - e^2, \pi^2 + e^2$ is rational.

<u>**Solutions on next slide.**</u>

Solution to Extension Problem

What does it mean to say that a number x is irrational?

It means that we cannot write $x = m/n$ where m and n are integers with $n \neq 0$.

Prove by contradiction statements A and B below, where p and q are real numbers.

A: *If pq is irrational, then at least one of p and q is irrational.*

B: *If $p + q$ is irrational, then at least one of p and q is irrational.*

We first prove statement A.

Assume that pq is irrational, but neither p nor q is irrational, so that both p and q are rational. But then pq is the product of two rational numbers, so is rational. This contradicts that assumption that pq is irrational. So statement A is true.

Now for statement B we argue similarly.

Assume that $p + q$ is irrational, but neither p nor q is irrational, so that both p and q are rational. But then $p + q$ is the sum of two rational numbers, so is rational. This contradicts the assumption that $p + q$ is irrational. So statement B is true.

Disprove by means of a counterexample statement C below, where p and q are real numbers.

C: *If p and q are irrational, then $p + q$ is irrational.*

One example is $p = \sqrt{2}$, $q = -\sqrt{2}$.

Solution to Extension Problem

If the numbers e, π, π^2, e^2 and $e\pi$ are irrational, prove that at most one of the numbers $\pi + e$, $\pi - e$, $\pi^2 - e^2$, $\pi^2 + e^2$ is rational.

We assume that the five given numbers are, indeed, irrational.

We have $(\pi + e) + (\pi - e) = 2\pi$, which is irrational (if p is irrational, then so is $2p$). So by statement B, at least one of $\pi + e$ and $\pi - e$ is irrational.

Similarly, $(\pi^2 + e^2) + (\pi^2 - e^2) = 2\pi^2$, which is irrational. So by statement B again, at least one of $\pi^2 + e^2$ and $\pi^2 - e^2$ is irrational.

Assume that both $\pi + e$ and $\pi^2 - e^2$ are rational. Then

$$\pi - e = \frac{\pi^2 - e^2}{\pi + e}$$

would also be rational. But we know that at least one of $\pi + e$ and $\pi - e$ is irrational, so $\pi + e$ and $\pi^2 - e^2$ cannot both be rational. Similarly, we can't have both $\pi - e$ and $\pi^2 - e^2$ rational.

Thus if two of the four numbers are rational, they must be $\pi^2 + e^2$ and one of $\pi \pm e$.

Assume that $\pi^2 + e^2$ and $\pi + e$ are rational. Then $(\pi + e)^2 = (\pi^2 + e^2) + 2e\pi$ is the square of a rational number, so is rational. But then $2e\pi = (\pi + e)^2 - (\pi^2 + e^2)$ would be rational, contradicting the irrationality of $e\pi$. Thus we cannot have both $\pi^2 + e^2$ and $\pi + e$ rational.

Similarly, if $\pi^2 + e^2$ and $\pi - e$ are both rational, we would have $2e\pi = (\pi^2 + e^2) - (\pi - e)^2$ being rational, again a contradiction.

Thus at most one of these four numbers is rational.

Fun Fact: No mathematician has yet managed to prove that $\pi + e$ or $\pi - e$ is irrational.

Homework Exercise

1 Select the statement that is the negation of 'All multiples of three are even'.

A All multiples of three are odd.

B At least one multiple of three is odd.

C No multiples of three are even.

2 Write down the negation of each statement.

a All rich people are happy.

b There are no prime numbers between 10 million and 11 million.

c If p and q are prime numbers then $(pq + 1)$ is a prime number.

d All numbers of the form $2^n - 1$ are either prime numbers or multiples of 3.

e At least one of the above four statements is true.

3 Statement: If n^2 is odd then n is odd.

a Write down the negation of this statement.

b Prove the original statement by contradiction.

4 Prove the following statements by contradiction.

a There is no greatest even integer.

b If n^3 is even then n is even.

c If pq is even then at least one of p and q is even.

d If $p + q$ is odd then at least one of p and q is odd.

Homework Exercise

5 **a** Prove that if ab is an irrational number then at least one of a and b is an irrational number. **(3 marks)**

b Prove that if $a + b$ is an irrational number then at least one of a and b is an irrational number. **(3 marks)**

c A student makes the following statement:

If $a + b$ is a rational number then at least one of a and b is a rational number.

Show by means of a counterexample that this statement is not true. **(1 mark)**

6 Use proof by contradiction to show that there exist no integers a and b for which $21a + 14b = 1$.

Hint Assume the opposite is true, and then divide both sides by the highest common factor of 21 and 14.

7 **a** Prove by contradiction that if n^2 is a multiple of 3, n is a multiple of 3. **(3 marks)**

b Hence prove by contradiction that $\sqrt{3}$ is an irrational number. **(3 marks)**

Hint Consider numbers in the form $3k + 1$ and $3k + 2$.

Homework Exercise

8 Use proof by contradiction to prove the statement:
'There are no integer solutions to the equation
$x^2 - y^2 = 2$'

Hint You can assume that x and y are positive, since $(-x)^2 = x^2$.

9 Prove by contradiction that $\sqrt[3]{2}$ is irrational. **(5 marks)**

10 This student has attempted to use proof by contradiction to show that there is no least positive rational number:

> **Assumption:** There is a least positive rational number.
> Let this least positive rational number be n.
>
> As n is rational, $n = \frac{a}{b}$ where a and b are integers.
>
> $n - 1 = \frac{a}{b} - 1 = \frac{a - b}{b}$
>
> Since a and b are integers, $\frac{a - b}{b}$ is a rational number that is less than n.
>
> This contradicts the statement that n is the least positive rational number.
> Therefore, there is no least positive rational number.

Problem-solving You might have to analyse student working like this in your exam. The question says, 'the error', so there should only be one error in the proof.

a Identify the error in the student's proof. **(1 mark)**

b Prove by contradiction that there is no least positive rational number. **(5 marks)**

Homework Answers

1 B At least one multiple of three is odd.

2 a At least one rich person is not happy.

b There is at least one prime number between 10 million and 11 million.

c If p and q are prime numbers there exists a number of the form $(pq + 1)$ that is not prime.

d There is a number of the form $2^n - 1$ that is neither a prime nor a multiple of 3.

e None of the above statements are true.

3 a There exists a number n such that n^2 is odd but n is even.

b n is even so write $n = 2k$

$n^2 = (2k)^2 = 4k^2 = 2(2k^2) \Rightarrow n^2$ is even.

This contradicts the assumption that n^2 is odd.

Therefore if n^2 is odd then n must be odd.

4 a Assumption: there is a greatest even integer $2n$.

$2(n + 1)$ is also an integer and $2(n + 1) > 2n$

$2n + 2 =$ even + even = even

So there exists an even integer greater that $2n$.

This contradicts the assumption.

Therefore there is no greatest even integer.

4 b Assumption: there exists a number n such that n^3 is even but n is odd.

n is odd so write $n = 2k + 1$

$n^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1$

$= 2(4k^3 + 6k^2 + 3k) + 1 \Rightarrow n^3$ is odd.

This contradicts the assumption that n^3 is even.

Therefore, if n^3 is even then n must be even.

c Assumption: if pq is even then neither p nor q is even.

p is odd, $p = 2k + 1$

q is odd, $q = 2m + 1$

$pq = (2k + 1)(2m + 1) = 4km + 2k + 2m + 1$

$= 2(2km + k + m) + 1 \Rightarrow pq$ is odd.

This contradicts the assumption that pq is even.

Therefore, if pq is even then at least one of p and q is even.

d Assumption: if $p + q$ is odd then neither p nor q is odd

p is even, $p = 2k$

q is even, $q = 2m$

$p + q = 2k + 2m = 2(k + m) \Rightarrow p + q$ is even

This contradicts the assumption then $p + q$ is odd.

Therefore, if $p + q$ is odd then at least one of p and q is odd.

Homework Answers

5 **a** Assumption: if ab is an irrational number then neither a nor b is irrational.

a is rational, $a = \frac{c}{d}$ where c and d are integers.

b is rational, $b = \frac{e}{f}$ where e and f are integers.

$ab = \frac{ce}{df}$, ce is an integer, df is an integer.

Therefore ab is a rational number.
This contradicts assumption then ab is irrational.
Therefore if ab is an irrational number then at least one of a and b is an irrational number.

b Assumption: neither a nor b is irrational.

a is rational, $a = \frac{c}{d}$ where c and d are integers.

b is rational, $b = \frac{e}{f}$ where e and f are integers.

$$a + b = \frac{cf + de}{df}$$

cf, de and df are integers.
So $a + b$ is rational. This contradicts the assumption that $a + b$ is irrational.
Therefore if $a + b$ is irrational then at least one of a and b is irrational.

c Many possible answers e.g. $a = 2 - \sqrt{2}$, $b = \sqrt{2}$.

6 Assumption: there exists integers a and b such that $21a + 14b = 1$.
Since 21 and 14 are multiples of 7, divide both sides by 7.
So now $3a + 2b = \frac{1}{7}$
$3a$ is also an integer. $2b$ is also an integer.
The sum of two integers will always be an integer, so $3a + 2b$ = 'an integer'.
This contradicts the statement that $3a + 2b = \frac{1}{7}$.
Therefore there exists no integers a and b for which $21a + 14b = 1$.

7 **a** Assumption: There exists a number n such that n^2 is a multiple of 3, but n is not a multiple of 3.
We know that all multiples of 3 can be written in the form $n = 3k$, therefore $3k + 1$ and $3k + 2$ are not multiples of 3.
Let $n = 3k + 1$
$n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$
In this case n^2 is *not* a multiple of 3.
Let $m = 3k + 2$
$m^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$
In this case m^2 is also not a multiple of 3.
This contradicts the assumption that n^2 is a multiple of 3.
Therefore if n^2 is a multiple of 3, n is a multiple of 3.

b Assumption: $\sqrt{3}$ is a rational number.

Then $\sqrt{3} = \frac{a}{b}$ for some integers a and b.

Further assume that this fraction is in its simplest terms: there are no common factors between a and b.

So $3 = \frac{a^2}{b^2}$ or $a^2 = 3b^2$.

Therefore a^2 must be a multiple of 3.
We know from part **a** that this means a must also be a multiple of 3.
Write $a = 3c$, which means $a^2 = (3c)^2 = 9c^2$.
Now $9c^2 = 3b^2$, or $3c^2 = b^2$.
Therefore b^2 must be a multiple of 3, which implies b is also a multiple of 3.
If a and b are both multiples of 3, this contradicts the statement that there are no common factors between a and b.
Therefore, $\sqrt{3}$ is an irrational number.

Homework Answers

8 Assumption: there is an integer solution to the equation $x^2 - y^2 = 2$.
Remember that $x^2 - y^2 = (x - y)(x + y) = 2$
To make a product of 2 using integers, the possible pairs are: (2, 1), (1, 2), (−2, −1) and (−1, −2).
Consider each possibility in turn.
$x - y = 2$ and $x + y = 1 \Rightarrow x = \frac{3}{2}, y = -\frac{1}{2}$.
$x - y = 1$ and $x + y = 2 \Rightarrow x = \frac{3}{2}, y = \frac{1}{2}$.
$x - y = -2$ and $x + y = -1 \Rightarrow x = -\frac{3}{2}, y = \frac{1}{2}$.
$x - y = -1$ and $x + y = -2 \Rightarrow x = -\frac{3}{2}, y = -\frac{1}{2}$.
This contradicts the statement that there is an integer solution to the equation $x^2 - y^2 = 2$.
Therefore the original statement must be true: There are no integer solutions to the equation $x^2 - y^2 = 2$.

9 Assumption: $\sqrt[3]{2}$ is rational and can be written in the form $\sqrt[3]{2} = \frac{a}{b}$ and there are no common factors between a and b.
$2 = \frac{a^3}{b^3}$ or $a^3 = 2b^3$
This means that a^3 is even, so a must also be even.
If a is even, $a = 2n$.
So $a^3 = 2b^3$ becomes $(2n)^3 = 2b^3$ which means $8n^3 = 2b^3$ or $4n^3 = b^3$ or $2(2n^3) = b^3$.
This means that b^3 must be even, so b is also even.
If a and b are both even, they will have a common factor of 2.
This contradicts the statement that a and b have no common factors.
We can conclude the original statement is true: $\sqrt[3]{2}$ is an irrational number.

10 a $n - 1$ could be non-positive, e.g. if $n = \frac{1}{2}$

b Assumption: There is a least positive rational number, n.
$n = \frac{a}{b}$ where a and b are integers.
Let $m = \frac{a}{2b}$. Since a and b are integers, m is rational and $m < n$.
This contradicts the statement that n is the least positive rational number.
Therefore, there is no least positive rational number.