Proofs

Proofs

In maths, we need to prove our results with absolute certainty.

Proofs

In maths, we need to prove our results with absolute certainty.

A proof is a logical explanation of why a result is true.

Proofs

In maths, we need to prove our results with absolute certainty.

A proof is a logical explanation of why a result is true.

Proofs are hard!

Proofs

In maths, we need to prove our results with absolute certainty.

A proof is a logical explanation of why a result is true.

Proofs are hard!

But we'll look at proof structure and some standard techniques.

Structure of a proof

Structure of a proof

Theorem: Let n be an integer. If n is even, then n^2 is even.

Structure of a proof

Theorem: Let n be an integer. If n is even, then n^2 is even.

hypotheses

conclusion

Structure of a proof

Theorem: Let n be an integer. If n is even, then n^2 is even.

hypotheses conclusion

Structure of the proof.
Let n be an integer, and suppose n is even. Then

⋮
(some argument)
⋮

so n^2 is even. □

Structure of a proof

Theorem: Let n be an integer. If n is even, then n^2 is even.

hypotheses conclusion

Structure of the proof.
Let n be an integer, and suppose n is even. Then

⋮
(some argument)
⋮

so n^2 is even. □

Important: Start with the hypotheses, end with the conclusion.

Quantifiers

Quantifiers

It’s important to recognise when a statement contains a quantifier.

Quantifiers

It’s important to recognise when a statement contains a quantifier.

- For a “for all” statement, we need to give a general argument that works for every value of the variable.

Quantifiers

It's important to recognise when a statement contains a quantifier.

- For a "for all" statement, we need to give a general argument that works for every value of the variable.

  ("For all" statements can also be phrased with "if . . . then" or "Let . . . ".)

Quantifiers

It's important to recognise when a statement contains a quantifier.

- For a "for all" statement, we need to give a general argument that works for every value of the variable.

  ("For all" statements can also be phrased with "if . . . then" or "Let . . . ".)

- For a "there exists" statement, we need to give an example of the thing that's supposed to exist, and say why it works.

Proofs with several parts

Proofs with several parts

Some proofs may have several parts. Set the proof out clearly, and explain the parts.

Proofs with several parts

Some proofs may have several parts. Set the proof out clearly, and explain the parts.

- “If and only if” proofs:

Proofs with several parts

Some proofs may have several parts. Set the proof out clearly, and explain the parts.

- "If and only if" proofs: to prove $P \Leftrightarrow Q$, we might write:

Proofs with several parts

Some proofs may have several parts. Set the proof out clearly, and explain the parts.

- "If and only if" proofs: to prove $P \Leftrightarrow Q$, we might write:

  "Suppose P is true. Then . . . , so Q is true.
  Conversely, suppose Q is true . Then . . . , so P is true. $\square$"

Proofs with several parts

Some proofs may have several parts. Set the proof out clearly, and explain the parts.

- "If and only if" proofs: to prove $P \Leftrightarrow Q$, we might write:

  "Suppose P is true. Then ..., so Q is true.
  Conversely, suppose Q is true . Then ..., so P is true. $\square$*"*

- Proofs with cases: sometimes we need different arguments to cover different situations.

Proofs with several parts

Some proofs may have several parts. Set the proof out clearly, and explain the parts.

- "If and only if" proofs: to prove $P \Leftrightarrow Q$, we might write:

  "Suppose P is true. Then . . . , so Q is true.
  Conversely, suppose Q is true . Then . . . , so P is true. $\square$*"*

- Proofs with cases: sometimes we need different arguments to cover different situations. We might write:

Proofs with several parts

Some proofs may have several parts. Set the proof out clearly, and explain the parts.

- "If and only if" proofs: to prove $P \Leftrightarrow Q$, we might write:

  "Suppose P is true. Then . . . , so Q is true.
  Conversely, suppose Q is true . Then . . . , so P is true. $\square$"

- Proofs with cases: sometimes we need different arguments to cover different situations. We might write:

  "We consider two cases.
  First suppose . . . . Then . . . , so the theorem is true in this case.
  Now suppose instead that . . . . Then . . . , so the theorem is true in this case too. $\square$"

Disproving a statement

Disproving a statement

Disproving a statement means proving that it isn't true, i.e. proving its negation.

Disproving a statement

Disproving a statement means proving that it isn't true, i.e. proving its negation.

To disprove a "for all" statement, you just need to give one example where the statement doesn't hold.

Disproving a statement

Disproving a statement means proving that it isn't true, i.e. proving its negation.

To disprove a "for all" statement, you just need to give one example where the statement doesn't hold. This is called a counterexample.

Disproving a statement

Disproving a statement means proving that it isn't true, i.e. proving its negation.

To disprove a "for all" statement, you just need to give one example where the statement doesn't hold. This is called a counterexample.

Non-Theorem 3.4: If n is a prime number, then $2^n - 1$ is prime.

Disproving a statement

Disproving a statement means proving that it isn't true, i.e. proving its negation.

To disprove a "for all" statement, you just need to give one example where the statement doesn't hold. This is called a counterexample.

Non-Theorem 3.4: If n is a prime number, then $2^n - 1$ is prime.

To find a counterexample, we need to find a prime number n such that $2^n - 1$ isn't prime.

Disproving a statement

Disproving a statement means proving that it isn't true, i.e. proving its negation.

To disprove a "for all" statement, you just need to give one example where the statement doesn't hold. This is called a counterexample.

Non-Theorem 3.4: If n is a prime number, then $2^n - 1$ is prime.

To find a counterexample, we need to find a prime number n such that $2^n - 1$ isn't prime.

$n = 2, 3, 5, 7$ don't work . . .