Discrete Mathematics

Lecture 9: Proof Technique (Case Study)

Instructor: Sourav Chakraborty

Proof Techniques

To prove statement $A \implies B$.

There are different proof techniques:

- Constructive Proofs
- Proof by Contradiction
- Proof by Contrapositive
- Induction
- Counter example
- Existential Proof

Which approach to apply

Which approach to apply

- It depends on the problem.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.
- Whether to split a problem or how to split a problem or how to look at a problem is an ART that has to be developed.

Which approach to apply

- It depends on the problem.
- Sometimes the problem can be split into smaller problems that can be easier to tackle individually.
- Sometimes viewing the problem is a different way can also help in tackling the problem easily.
- Whether to split a problem or how to split a problem or how to look at a problem is an ART that has to be developed.
- There are some thumb rules but at the end it is a skill you develop using a lot of practice.

Splitting into smaller problem

- If the problem is to prove $A \implies B$ and B can be written as $B = C \wedge D$ then note that

$$(A \implies B) \equiv (A \implies C \wedge D) \equiv (A \implies C) \wedge (A \implies D).$$

Splitting into smaller problem

- If the problem is to prove $A \implies B$ and B can be written as $B = C \wedge D$ then note that

$$(A \implies B) \equiv (A \implies C \wedge D) \equiv (A \implies C) \wedge (A \implies D).$$

- For example:

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 (mod\ 4)$.

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 (mod\ 4)$.

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 (mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

If b is an odd prime then $b^2 \equiv 1 (mod\ 4)$.

Problem (Second Part)

If b is an odd prime then $2b^2 \geq (b+1)^2$.

Redundant Assumptions

Redundant Assumptions

- There can be assumption that are not necessary.

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.
- If $A \implies B$ then $A \wedge C$ also implies B.

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.
- If $A \implies B$ then $A \wedge C$ also implies B.

$$(A \implies B) \implies (A \wedge C \implies B) = True$$

Redundant Assumptions

- There can be assumption that are not necessary.
- We can throw them.
- If $A \implies B$ then $A \wedge C$ also implies B.

$$(A \implies B) \implies (A \wedge C \implies B) = True$$

- Which assumption are not needed is something to guess using your intelligence.

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 (mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

If b is an odd prime then $b^2 \equiv 1 (mod\ 4)$.

Problem (Second Part)

If b is an odd prime then $2b^2 \geq (b+1)^2$.

Splitting of Problems in Smaller Problems

Problem

If b is an odd prime then $2b^2 \geq (b+1)^2$ and $b^2 \equiv 1 (mod\ 4)$.

The above problem is same as proving the following two problems:

Problem (First Part)

If b is an odd integer then $b^2 \equiv 1 (mod\ 4)$.

Problem (Second Part)

If b is a real number ≥ 3 then $2b^2 \geq (b+1)^2$.

Constructive Proof

To prove $A \implies B$.

There are two techniques:

Constructive Proof

To prove $A \implies B$.

There are two techniques:

- Direct Proof: You directly proof $A \implies B$.

Constructive Proof

To prove $A \implies B$.

There are two techniques:

- Direct Proof: You directly proof $A \implies B$.
- Case Studies: You split the problem into smaller problems.

Direct Proof: Example 1

Problem

If n is an odd integer then $n^2 \equiv 1 (mod\ 4)$.

Direct Proof: Example 1

Problem

If n is an odd integer then $n^2 \equiv 1 (mod\ 4)$.

Since n is odd. So $N = 2k + 1$ for some integer k.

Direct Proof: Example 1

Problem

If n is an odd integer then $n^2 \equiv 1 (mod\ 4)$.

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.

Direct Proof: Example 1

Problem

If n is an odd integer then $n^2 \equiv 1 (mod\ 4)$.

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So $(n^2 - 1) = 4(k^2 + k)$.

Direct Proof: Example 1

Problem

If n is an odd integer then $n^2 \equiv 1 (mod\ 4)$.

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So $(n^2 - 1) = 4(k^2 + k)$.
Since k is an integer so $k^2 + k$ is also an integer and hence $4 \mid n^2 - 1$.

Direct Proof: Example 1

Problem

If n is an odd integer then $n^2 \equiv 1 (mod\ 4)$.

Since n is odd. So $N = 2k + 1$ for some integer k.
So $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$.
So $(n^2 - 1) = 4(k^2 + k)$.
Since k is an integer so $k^2 + k$ is also an integer and hence $4 \mid n^2 - 1$.
Hence $n^2 \equiv 1 (\text{mod } 4)$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:
Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.
So $b^2 - 2b + 1 > 2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:

Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.
So $b^2 - 2b + 1 > 2$.
Hence $b^2 > 2b + 1$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

First Proof:
Since $b \geq 3$ so $(b-1) \geq 2$ and hence $(b-1)^2 \geq 4$.
Thus $(b-1)^2 > 2$.
So $b^2 - 2b + 1 > 2$.
Hence $b^2 > 2b + 1$.
Adding b^2 to both sides we get $2b^2 > b^2 + 2b + 1 = (b+1)^2$.

A simple approach to obtain a proof

- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.

A simple approach to obtain a proof

- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a back ward proof.

A simple approach to obtain a proof

- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a back ward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.

A simple approach to obtain a proof

- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a back ward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.
- And if $C \iff B$ then $(A \implies B) \equiv (A \implies C)$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

$\iff (b-1)^2 - 2 > 0$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

$\iff (b-1)^2 - 2 > 0$ for $b \geq 3$

$\iff (b-1)^2 > 2$ for $b \geq 3$

Direct Proof: Example 2

Problem

If b is any real number ≥ 3 then $2b^2 > (b+1)^2$.

Second Proof (Backward Proof):

To prove: $2b^2 > (b+1)^2$ for $b \geq 3$

$\iff 2b^2 > b^2 + 2b + 1$ for $b \geq 3$

$\iff b^2 - 2b - 1 > 0$ for $b \geq 3$

$\iff (b-1)^2 - 2 > 0$ for $b \geq 3$

$\iff (b-1)^2 > 2$ for $b \geq 3$

And this is true because $b \geq 3 \implies (b-1) \geq 2$
$\implies (b-1)^2 \geq 4 > 2$.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a backward proof.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a backward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.

Direct proof

- For proving $A \implies B$ we can start with the assumption A and step-by-step prove that B is true.
- Sometimes a direct proof (as in the previous example) can be magical and hard to understand how to obtain.
- A simpler technique is to have a backward proof.
- If we have to prove $(A \implies B)$ then the idea is to simplify B.
- And if $C \iff B$ then $(A \implies B) \equiv (A \implies C)$.

Sometimes proving something stronger is easier

If we have to prove $A \implies B$

Sometimes proving something stronger is easier

If we have to prove $A \implies B$

- If $C \implies B$ then

$$(A \implies C) \implies (A \implies B).$$

Sometimes proving something stronger is easier

If we have to prove $A \implies B$

- If $C \implies B$ then
$$(A \implies C) \implies (A \implies B).$$
- For example:

Problem

If b is a real number and $b \geq 2$ then $2b^3 > 3b + 2$

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Sometimes proving something stronger is easier

Problem

If b *is a real number and* $b \geq 2$ *then* $2b^3 \geq 3b + 2$

Proof:

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

$\Leftarrow b^2 \geq 2b + 2$ (for $b \geq 2$) [Since $(b^2 - b) \geq 0$]

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

$\Leftarrow b^2 \geq 2b + 2$ (for $b \geq 2$) [Since $(b^2 - b) \geq 0$]

$\Leftrightarrow (b-1)^2 \geq 1$ (for $b \geq 2$)

Sometimes proving something stronger is easier

Problem

If b is a real number and $b \geq 2$ then $2b^3 \geq 3b + 2$

Proof:

Since $b \geq 2$ so $b^3 \geq b^2$.So,

$2b^3 \geq 3b + 2$ (for $b \geq 2$)

$\Leftarrow 2b^2 \geq 3b + 2$ (for $b \geq 2$)

$\Leftrightarrow b^2 + (b^2 - b) \geq 2b + 2$ (for $b \geq 2$)

$\Leftarrow b^2 \geq 2b + 2$ (for $b \geq 2$) [Since $(b^2 - b) \geq 0$]

$\Leftrightarrow (b-1)^2 \geq 1$ (for $b \geq 2$)

And this is true as $(b \geq 2) \implies (b-1) \geq 1$ and hence $(b-1)^2 > 1$.

Techniques so far

To prove $A \implies B$

Techniques so far

To prove $A \implies B$

- If $B = C \wedge D$ then $A \implies B$ is same as $(A \implies C) \wedge (A \implies D)$.

Techniques so far

To prove $A \implies B$

- If $B = C \wedge D$ then $A \implies B$ is same as $(A \implies C) \wedge (A \implies D)$.
- If $B \equiv C$ then $A \implies B$ is same as $A \implies C$

Techniques so far

To prove $A \implies B$

- If $B = C \wedge D$ then $A \implies B$ is same as $(A \implies C) \wedge (A \implies D)$.
- If $B \equiv C$ then $A \implies B$ is same as $A \implies C$
- If $C \implies B$ then to show $A \implies B$ it is enough to show $A \implies C$.

Splitting the assumption into cases

Splitting the assumption into cases

- Sometimes the assumption or the premise can be split into different cases. In that case we can split the problem according to cases.

Splitting the assumption into cases

- Sometimes the assumption or the premise can be split into different cases. In that case we can split the problem according to cases.
- If $A = C \vee D$ then

$$(A \implies B) \equiv (C \implies B) \wedge (D \implies B).$$

Problem of last class

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Problem of last class

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Thus we have to prove that for any positive integer a

$$a^2 \not\equiv 2 \pmod 4$$

Proof Technique: Case Analysis

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

Proof Technique: Case Analysis

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

Proof Technique: Case Analysis

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

We will solve in in case by case basis.

Proof Technique: Case Analysis

If a and b are two positive integers then prove that $a^2 - 4b$ cannot be equal to 2.

If a positive integer a is divided by 4 then the possible remainders are $0, 1, 2$ and 3.

We will solve in in case by case basis.

We split the problem into 4 case depending on the remainder when a is divided by 4 and show that for every case $a^2 - 4b$ cannot be equal to 2.

Prime Numbers

A positive number p is a prime is for all $1 < x < p$, x does not divide p.

Prime Numbers

A positive number p is a prime is for all $1 < x < p$, x does not divide p.

A number that is not a prime is divisible by a prime.

Prime Numbers

A positive number p is a prime is for all $1 < x < p$, x does not divide p.

A number that is not a prime is divisible by a prime.

If a, b are two integers such that p divides a but does not divide b then p does not dive $(a + b)$.

Problem

Prove that the square of a prime number is always $1 (mod\ 6)$, when the prime number if ≥ 5.

Or in other words, if p is a prime number, such that $p \geq 5$, then $p^2 - 1$ is divisible by 6.

Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

We will prove it case by case.

Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

We will prove it case by case.

Consider the remainders when divided by 6

Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 1 The remainder when p is divided by 6 is 0

Case 2 The remainder when p is divided by 6 is 1

Case 3 The remainder when p is divided by 6 is 2

Case 4 The remainder when p is divided by 6 is 3

Case 5 The remainder when p is divided by 6 is 4

Case 6 The remainder when p is divided by 6 is 5

Proof: Case 1

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 1 The remainder when p is divided by 6 is 0

Proof: Case 1

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 1 The remainder when p is divided by 6 is 0

Can a PRIME when divided by 6 have remainder 0?

Proof: Case 1

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 1 The remainder when p is divided by 6 is 0

Can a PRIME when divided by 6 have remainder 0?
That is can a prime p be $= 6k$ for some integer $k \geq 1$?

Proof: Case 1

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 1 The remainder when p is divided by 6 is 0

Can a PRIME when divided by 6 have remainder 0?
That is can a prime p be $= 6k$ for some integer $k \geq 1$?

No. because $6k$ is divisible by 2.

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 3 The remainder when p is divided by 6 is 2

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 3 The remainder when p is divided by 6 is 2

Can a PRIME when divided by 6 have remainder 2?

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 3 The remainder when p is divided by 6 is 2

Can a PRIME when divided by 6 have remainder 2?
That is can a prime p be $= 6k + 2$ for some integer $k \geq 1$?

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 3 The remainder when p is divided by 6 is 2

Can a PRIME when divided by 6 have remainder 2?
That is can a prime p be $= 6k + 2$ for some integer $k \geq 1$?

No. because $6k + 2 = 2(3k + 1)$ and so is divisible by 2.

Proof

If p ($p \geq 6$) is a prime then only 1 and 5 are the possible remainders possible when divided by 6.

Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 2 The remainder when p is divided by 6 is 1

Case 6 The remainder when p is divided by 6 is 5

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 2 The remainder when p is divided by 6 is 1

$$p = 6k + 1.$$

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 2 The remainder when p is divided by 6 is 1

$p = 6k + 1$.
So $p^2 = (6k+1)^2 = 36k^2 + 12k + 1 = 6(6k^2 + 2k) + 1$

Proof: Case 2

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 2 The remainder when p is divided by 6 is 1

$p = 6k + 1$.
So $p^2 = (6k + 1)^2 = 36k^2 + 12k + 1 = 6(6k^2 + 2k) + 1$

So $p^2 - 1$ is divisible by 6.

Proof: Case 6

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 6 The remainder when p is divided by 6 is 5

$$p = 6k + 5.$$

Proof: Case 6

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 6 The remainder when p is divided by 6 is 5

$p = 6k + 5$.
So $p^2 = (6k+5)^2 = 36k^2 + 60k + 25 = 6(6k^2 + 10k + 4) + 1$

Proof: Case 6

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Case 6 The remainder when p is divided by 6 is 5

$p = 6k + 5$.
So $p^2 = (6k+5)^2 = 36k^2 + 60k + 25 = 6(6k^2 + 10k + 4) + 1$

So $p^2 - 1$ is divisible by 6.

Complete Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

Complete Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

We did a case by case analysis by considering the different remainders possible when we divide a number p by 6.

Complete Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

We did a case by case analysis by considering the different remainders possible when we divide a number p by 6.

Some of the cases cannot happen because p is a prime.

Complete Proof

If p is a prime number, such that $p \geq 6$, then $p^2 - 1$ is divisible by 6.

We did a case by case analysis by considering the different remainders possible when we divide a number p by 6.

Some of the cases cannot happen because p is a prime.

For the other cases we did a case by case analysis.

Thus so far ...

To prove $A \implies B$

Thus so far ...

To prove $A \implies B$

- Split the problem if $B = C \land D$

Thus so far ...

To prove $A \implies B$

- Split the problem if $B = C \wedge D$
- Remove redundant assumptions.

Thus so far ...

To prove $A \implies B$

- Split the problem if $B = C \wedge D$
- Remove redundant assumptions.
- Sometimes its easier to proof a stronger statement

Thus so far ...

To prove $A \implies B$

- Split the problem if $B = C \wedge D$
- Remove redundant assumptions.
- Sometimes its easier to proof a stronger statement
- Direct Proof

Thus so far ...

To prove $A \implies B$

- Split the problem if $B = C \wedge D$
- Remove redundant assumptions.
- Sometimes its easier to proof a stronger statement
- Direct Proof
- Backward proof.

Thus so far ...

To prove $A \implies B$

- Split the problem if $B = C \wedge D$
- Remove redundant assumptions.
- Sometimes its easier to proof a stronger statement
- Direct Proof
- Backward proof.
- Is $A = C \vee D$ then split into cases.

Infiniteness of Primes

Prove that primes are infinite.

Infiniteness of Primes

Prove that primes are infinite.

That is, $\forall n \in \mathbb{Z}^+ \; \exists x > n \; x$ is a prime.

Proof by Contradiction

- Note that

$$(A \implies B) \equiv (\neg B \wedge A = \quad \text{False})$$

- To proof $A \implies B$

  sometimes its easier to prove that

$$\neg B \wedge A = \quad \text{False}.$$

Proof by Contradiction

Proof by Contradiction

Example: **Prove that earth is not flat.**

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1:

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2:

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2: Lets assume the earth is flat. Then when a ship came from the horizon the whole ship would appear at the same time.

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2: Lets assume the earth is flat. Then when a ship came from the horizon the whole ship would appear at the same time.
But that does not happen - first the mast is seen then the whole ship. So a contradiction.

Proof by Contradiction

Example: **Prove that earth is not flat.**

Attempt 1: If a ship is coming from the horizon we first see the mast (top) of the ship and slowly the complete ship. So the earth must be round hence not flat.

Attempt 2: Lets assume the earth is flat. Then when a ship came from the horizon the whole ship would appear at the same time.
But that does not happen - first the mast is seen then the whole ship. So a contradiction.
Hence initial assumption that earth is flat does not hold.

Next week...

We will learn the following proof techniques:

- Proof using contradiction
- Proof using contraposetive.
- Counter Example