CSE 20

Lecture 15: Proof Techniques
Midterm Review

- Representation of integers in base $b$
- Logic
- Proof systems:
  - Direct Proof
  - Proof by contradiction
  - Contrapositive
- Sets Theory
- Functions
Midterm Review

- Representation of integers in base $b$
- Logic
- Proof systems:
  - Direct Proof
  - Proof by contradiction
  - Contrapositive
- Sets Theory
- Functions

NO CALCULATOR, NO CHEAT SHEET
Proof Techniques

To prove statement $B$ from $A$:

Direct Proof:

$$A = \Rightarrow B$$

If $A = X \lor Y \lor Z$,

$$[(X = \Rightarrow B) \land (Y = \Rightarrow B) \land (Z = \Rightarrow B)] = \Rightarrow (A = \Rightarrow B)$$

Proof by contradiction:

$$(\neg B \land A)$$ gives a contradiction

Proof by Contrapositive:

$A = \Rightarrow B$ is same as proving $\neg B = \Rightarrow \neg A$.
Proof Techniques

To prove statement $B$ from $A$:

- Direct Proof:
  
  $$ A \implies B $$

  If $A = X \lor Y \lor Z$

  $$ [(X \implies B) \land (Y \implies B) \land (Z \implies B)] \implies (A \implies B) $$
Proof Techniques

To prove statement $B$ from $A$:

- Direct Proof:
  \[ A \implies B \]
  If $A = X \lor Y \lor Z$
  \[ [(X \implies B) \land (Y \implies B) \land (Z \implies B))] \implies (A \implies B) \]

- Proof by contradiction:
  \[ (\neg B \land A) \text{ gives a contradiction} \]
Proof Techniques

To prove statement $B$ from $A$:

- **Direct Proof:**
  \[ A \implies B \]

  If $A = X \lor Y \lor Z$

  \[ [(X \implies B) \land (Y \implies B) \land (Z \implies B))] \implies (A \implies B) \]

- **Proof by contradiction:**
  \((\neg B \land A)\text{ gives a contradiction}\)

- **Proof by Contrapositive:** $A \implies B$ is same as proving $\neg B \implies \neg A$. 
Is $\sqrt{2}$ a rational?

Earlier in class we used proof by contradiction to prove that $\sqrt{2}$ is not rational.
A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

$1/\text{Rational}$ is rational.

$1/(\text{not rational})$ is not rational.

$1/\sqrt{2}$ is not rational.

$\text{Not Rational} \times \text{Not Rational} = ?$

Eg: \[ \sqrt{2} \times (1/\sqrt{2}) \text{ is rational.} \]
Rational Numbers

A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational $\times$ Rational = Rational

- Rational $\times$ Not Rational = Not Rational

- So $(-\sqrt{2})$ is not rational.

- $1/\text{Rational}$ is rational.

- $1/(\text{not rational})$ is not rational.

- $1/\sqrt{2}$ is not rational.

- Not Rational $\times$ Not Rational = ?

Eg:

$\sqrt{2} \times (1/\sqrt{2})$ is rational.
A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational $\times$ Rational $= \text{Rational}$
- Rational $\times$ Not Rational $= \text{Not Rational}$.
A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational $\times$ Rational = Rational
- Rational $\times$ Not Rational = Not Rational.

So $(-\sqrt{2})$ is not rational.
Rational Numbers

A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational $\times$ Rational = Rational
- Rational $\times$ Not Rational = Not Rational. So $(-\sqrt{2})$ is not rational.
- $1/Rational$ is rational.
A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational $\times$ Rational = Rational
- Rational $\times$ Not Rational = Not Rational.
  
So $(-\sqrt{2})$ is not rational.

- $1/Rational$ is rational.
- $1/(not\ rational)$ is not rational.
Rational Numbers

A number \( x \) is rational if it can be written as \( p/q \) where \( p \) and \( q \) are integers.

- Rational \( \times \) Rational = Rational
- Rational \( \times \) Not Rational = Not Rational.
  So \( (-\sqrt{2}) \) is not rational.
- \( 1/Rational \) is rational.
- \( 1/(not\ rational) \) is not rational. \( 1/\sqrt{2} \) is not rational.
Rational Numbers

A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational $\times$ Rational = Rational
- Rational $\times$ Not Rational = Not Rational.  
  So $(-\sqrt{2})$ is not rational.
- $1/Rational$ is rational.
- $1/(not\ rational)$ is not rational.  $1/\sqrt{2}$ is not rational.
- Not Rational $\times$ Not Rational = ?
Rational Numbers

A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational $\times$ Rational = Rational
- Rational $\times$ Not Rational = Not Rational.
  So $(-\sqrt{2})$ is not rational.
- $1/Rational$ is rational.
- $1/(not\ rational)$ is not rational. $1/\sqrt{2}$ is not rational.
- Not Rational $\times$ Not Rational = ?

Eg: $\sqrt{2} \times (1/\sqrt{2})$ is rational.
Is $\sqrt{6}$ rational?

Prove that $\sqrt{6}$ is not rational.
A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.
A number \( x \) is rational if it can be written as \( p/q \) where \( p \) and \( q \) are integers.

- Rational + Rational = Rational

\((2 - \sqrt{2})\) is not rational.

Not Rational + Not Rational = ?

Eg:
\[ \sqrt{2} + (2 - \sqrt{2}) \text{ is rational.} \]
A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational + Rational = Rational
- Rational + Not Rational = Not Rational.
A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational + Rational = Rational
- Rational + Not Rational = Not Rational.
  $(2 - \sqrt{2})$ is not rational.
- Not Rational + Not Rational = ?
Rational Numbers

A number $x$ is rational if it can be written as $p/q$ where $p$ and $q$ are integers.

- Rational + Rational = Rational
- Rational + Not Rational = Not Rational. 
  $(2 - \sqrt{2})$ is not rational.
- Not Rational + Not Rational = ?

Eg: $\sqrt{2} + (2 - \sqrt{2})$ is rational.
Is \( \sqrt{2} + \sqrt{3} \) a rational?

Prove that \( \sqrt{2} + \sqrt{3} \) is not rational.

To prove this by contradiction, what should be assumed?

\begin{enumerate}
\item A \( \sqrt{2} + \sqrt{3} \) is not a rational number.
\item B \( \sqrt{2} + \sqrt{3} \) is a rational number.
\item C Either \( \sqrt{2} \) or \( \sqrt{3} \) is a rational number.
\item D Both \( \sqrt{2} \) and \( \sqrt{3} \) are rational numbers.
\end{enumerate}
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.
To proof this by contradiction what should be assume.

A $\sqrt{2} + \sqrt{3}$ is not a rational number.
B $\sqrt{2} + \sqrt{3}$ is a rational number.
C Either $\sqrt{2}$ or $\sqrt{3}$ is a rational number.
D Both $\sqrt{2}$ and $\sqrt{3}$ are a rational number.
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.
To prove by contradiction what do have to prove:
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

To prove by contradiction what do have to prove:

- Let $\sqrt{2} + \sqrt{3}$ be a rational number
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.
To prove by contradiction what do have to prove:

- Let $\sqrt{2} + \sqrt{3}$ be a rational number
- $\sqrt{2} + \sqrt{3}$ can be written as $\frac{p}{q}$ for any positive integer $p$ and $q$. 
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.
To prove by contradiction what do have to prove:
- Let $\sqrt{2} + \sqrt{3}$ be a rational number
- $\sqrt{2} + \sqrt{3}$ can be written as $\frac{p}{q}$ for any positive integer $p$ and $q$.
- If $\sqrt{2} + \sqrt{3} = \frac{p}{q}$ for some positive integers $p$ and $q$ then there is some problem
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

- Let $\sqrt{2} + \sqrt{3} = \frac{p}{q}$
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

- Let $\sqrt{2} + \sqrt{3} = p/q$
- $\iff \sqrt{3} = p/q - \sqrt{2}$
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

- Let $\sqrt{2} + \sqrt{3} = p/q$
- $\iff \sqrt{3} = p/q - \sqrt{2}$
- $\iff 3 = (p^2/q^2) - 2\sqrt{2}p/q + 2$

So $\sqrt{2}$ is a rational since $(p^2 - q^2)$ and $2pq$ are integers.
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

- Let $\sqrt{2} + \sqrt{3} = \frac{p}{q}$
- $\iff \sqrt{3} = \frac{p}{q} - \sqrt{2}$
- $\iff 3 = \left(\frac{p^2}{q^2}\right) - 2\sqrt{2}\frac{p}{q} + 2$
- $\iff 2\sqrt{2}\frac{p}{q} = \left(\frac{p^2}{q^2}\right) - 1 = \left(\frac{p^2 - q^2}{q^2}\right)$
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

- Let $\sqrt{2} + \sqrt{3} = p/q$
- $\iff \sqrt{3} = p/q - \sqrt{2}$
- $\iff 3 = (p^2/q^2) - 2\sqrt{2}p/q + 2$
- $\iff 2\sqrt{2}p/q = (p^2/q^2) - 1 = (p^2 - q^2)/q^2$
- $\iff \sqrt{2} = (p^2 - q^2)/(2pq) = p'/q'$

So $\sqrt{2}$ is a rational since $(p^2 - q^2)$ and $2pq$ are integers.
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

- Let $\sqrt{2} + \sqrt{3} = p/q$
- $\iff \sqrt{3} = p/q - \sqrt{2}$
- $\iff 3 = (p^2/q^2) - 2\sqrt{2}p/q + 2$
- $\iff 2\sqrt{2}p/q = (p^2/q^2) - 1 = (p^2 - q^2)/q^2$

$\iff \sqrt{2} = \frac{(p^2 - q^2)}{2pq} = \frac{p'}{q'}$

So $\sqrt{2}$ is a rational since $(p^2 - q^2)$ and $2pq$ are integers.
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

So if $\sqrt{2} + \sqrt{3}$ is rational then $\sqrt{2}$ is rational which is a contradiction.
Is $\sqrt{2} + \sqrt{3}$ a rational?

Prove that $\sqrt{2} + \sqrt{3}$ is not rational.

So If $\sqrt{2} + \sqrt{3}$ is rational then $\sqrt{2}$ is rational which is a contradiction.

Thus our initial assumption was wrong. Thus $\sqrt{2} + \sqrt{3}$ is not a rational number.
Is $\sqrt{3}$ rational?

Prove that $\sqrt{3}$ is not rational.

To proof this by contradiction what should be assume.

A $\sqrt{3}$ is not rational. So $\sqrt{3} = \text{non-integer}/\text{non-integer}$.
B $\sqrt{3}$ is a rational number. So $\sqrt{3} = \text{integer}/\text{integer}$.
C $\sqrt{3}$ is a not rational. So $\sqrt{3} = \text{non-integer}/\text{integer}$.
D $\sqrt{3}$ is a not rational. So $\sqrt{3} = \text{integer}/\text{non-integer}$. 
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

Let $\sqrt{3} = \frac{p}{q}$

We can assume both $p$ and $q$ cannot be divisible by 3.

Now $\sqrt{3} = \frac{p}{q} \iff 3 = \frac{p^2}{q^2} \iff 3q^2 = p^2$

We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = \frac{p}{q}$
- We can assume $p$ and $q$ has no common factors else we can factor it out.
- In other words we can assume both $p$ and $q$ cannot be divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We can assume $p$ and $q$ has no common factors else we can factor it out.
- In other words we can assume both $p$ and $q$ cannot be divisible by 3.
- Now $\sqrt{3} = p/q \iff 3 = p^2/q^2 \iff 3q^2 = p^2$
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = \frac{p}{q}$
- We can assume $p$ and $q$ has no common factors else we can factor it out.
- In other words we can assume both $p$ and $q$ cannot be divisible by 3.
- Now $\sqrt{3} = \frac{p}{q} \iff 3 = \frac{p^2}{q^2} \iff 3q^2 = p^2$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
Prove \( \sqrt{3} \) is not rational

We prove by contradiction.

- Let \( \sqrt{3} = p/q \)
- We prove by case by case analysis that if \( p \) and \( q \) are integers, not both divisible by 3 then \( 3q^2 \) cannot be equal to \( p^2 \) and hence we get a contradiction.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 1: Both $p$ and $q$ are not divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 1: Both $p$ and $q$ are not divisible by 3.
- Case 2: $p$ is not-divisible by 3 and $q$ is divisible by 3.
- Case 3: $p$ is divisible by 3 and $q$ is not divisible by 3.

If for all the above cases we prove that $3q^2 = p^2$ is not a possibility then we are done.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 1: Both $p$ and $q$ are not divisible by 3.
- Case 2: $p$ is not-divisible by 3 and $q$ is divisible by 3.
- Case 3: $p$ is divisible by 3 and $q$ is not divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.

  - Case 1: Both $p$ and $q$ are not divisible by 3.
  - Case 2: $p$ is not-divisible by 3 and $q$ is divisible by 3.
  - Case 3: $p$ is divisible by 3 and $q$ is not divisible by 3.

If for all the above cases we prove that $3q^2 = p^2$ is not a possibility then we are done.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 1: Both $p$ and $q$ are not divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 1: Both $p$ and $q$ are not divisible by 3.

$3q^2$ is divisible by 3.
We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 1: Both $p$ and $q$ are not divisible by 3.

\[
3q^2 \text{ is divisible by 3.} \\
p^2 \text{ is not divisible by 3.}
\]
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 1: Both $p$ and $q$ are not divisible by 3.

$3q^2$ is divisible by 3.
$p^2$ is not divisible by 3.
So $3q^2$ cannot be equal to $p^2$. 
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 2: $p$ is not-divisible by 3 and $q$ is divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = \frac{p}{q}$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 2: $p$ is not-divisible by 3 and $q$ is divisible by 3.

$3q^2$ is divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 2: $p$ is not-divisible by 3 and $q$ is divisible by 3.

$3q^2$ is divisible by 3.
$p^2$ is not divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 2: $p$ is not-divisible by 3 and $q$ is divisible by 3.

$3q^2$ is divisible by 3.
$p^2$ is not divisible by 3.
So $3q^2$ cannot be equal to $p^2$. 
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 3: $p$ is divisible by 3 and $q$ is not-divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 3: $p$ is divisible by 3 and $q$ is not-divisible by 3.

Let $p = 3k$. 
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

1. Let $\sqrt{3} = p/q$
2. We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
3. Case 3: $p$ is divisible by 3 and $q$ is not-divisible by 3.

Let $p = 3k$. So

$3q^2 = p^2 \iff 3q^2 = 9k^2 \iff q^2 = 3k^2$ $3k^2$ is divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 3: $p$ is divisible by 3 and $q$ is not-divisible by 3.

Let $p = 3k$. So

$3q^2 = p^2 \iff 3q^2 = 9k^2 \iff q^2 = 3k^2$ 3k^2 is divisible by 3.

$q^2$ is not divisible by 3.
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 3: $p$ is divisible by 3 and $q$ is not-divisible by 3.

Let $p = 3k$. So

$$3q^2 = p^2 \iff 3q^2 = 9k^2 \iff q^2 = 3k^2$$

3$k^2$ is divisible by 3.
$q^2$ is not divisible by 3.
So $3k^2$ cannot be equal to $q^2$. 
Prove $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
- Case 3: $p$ is divisible by 3 and $q$ is not-divisible by 3.

Let $p = 3k$. So

$3q^2 = p^2 \iff 3q^2 = 9k^2 \iff q^2 = 3k^2$ $3k^2$ is divisible by 3.

$q^2$ is not divisible by 3.
So $3k^2$ cannot be equal to $q^2$.
So $3q^2$ cannot be equal to $p^2$. 
Overview of the proof that \( \sqrt{3} \) is not rational

We prove by contradiction.

Let \( \sqrt{3} = \frac{p}{q} \). We can assume \( p \) and \( q \) has no common factors else we can factor it out. In other words we can assume both \( p \) and \( q \) cannot be divisible by 3.

Now \( \sqrt{3} = \frac{p}{q} \iff 3 = \frac{p^2}{q^2} \iff 3q^2 = p^2 \).

We prove by case by case analysis that if \( p \) and \( q \) are integers, not both divisible by 3 then \( 3q^2 \) cannot be equal to \( p^2 \) and hence we get a contradiction.
Overview of the proof that $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$

We can assume $p$ and $q$ has no common factors else we can factor it out. In other words we can assume both $p$ and $q$ cannot be divisible by 3.

$\sqrt{3} = p/q \iff 3 = p^2/q^2 \iff 3q^2 = p^2$.

We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
Overview of the proof that $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We can assume $p$ and $q$ has no common factors else we can factor it out.
- In other words we can assume both $p$ and $q$ cannot be divisible by 3.
Overview of the proof that $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We can assume $p$ and $q$ has no common factors else we can factor it out.
- In other words we can assume both $p$ and $q$ cannot be divisible by 3.
- Now $\sqrt{3} = p/q \iff 3 = p^2/q^2 \iff 3q^2 = p^2$
Overview of the proof that $\sqrt{3}$ is not rational

We prove by contradiction.

- Let $\sqrt{3} = p/q$
- We can assume $p$ and $q$ has no common factors else we can factor it out.
- In other words we can assume both $p$ and $q$ cannot be divisible by 3.
- Now $\sqrt{3} = p/q \iff 3 = p^2/q^2 \iff 3q^2 = p^2$
- We prove by case by case analysis that if $p$ and $q$ are integers, not both divisible by 3 then $3q^2$ cannot be equal to $p^2$ and hence we get a contradiction.
Problems for practice

- Prove that $\sqrt{6}$ is not rational.
- Prove that $\sqrt{5}$ is not rational.
Challenge Problem for Assignment 2

Prove that there are infinitely many primes of form $5 \pmod{6}$. 
Challenge Problem for Assignment 2

Prove that there are infinitely many primes of form \(5(\text{mod } 6)\).

We have proved that primes are either 2 or 3 or \(1(\text{mod } 6)\) or \(5(\text{mod } 6)\).
Challenge Problem for Assignment 2

Prove that there are infinitely many primes of form $5 \pmod{6}$.

We have proved that primes are either $2$ or $3$ or $1 \pmod{6}$ or $5 \pmod{6}$.

We have seen that there are infinitely many primes.
Prime distribution

- 2
- 3
- 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, ...
- 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, ....
Proof of Infiniteness of primes

Let there be finitely many primes: let them be

\[ p_1, p_2, \ldots, p_t \]

With \( p_t \) being the largest prime

Then we prove that in that case: \( (p_1 \times p_2 \times \cdots \times p_t) + 1 \) is a prime.
Proof of Infiniteness of primes

Let there be finitely many primes: let them be

\[ p_1, p_2, \ldots, p_t \]

With \( p_t \) being the largest prime

Then we prove that in that case: \((p_1 \times p_2 \times \cdots \times p_t) + 1\) is a prime.

Hence we have an even larger prime and hence that contradicts that \( p_t \) was the largest prime. And so by contradiction we are done.