Today: Proofs!!!
Today: Proofs!!!

1. By Example (or Counterexample).
Today: Proofs!!!

1. By Example (or Counterexample).
2. Direct. (Prove $P \implies Q$.)
Today: Proofs!!

1. By Example (or Counterexample).
2. Direct. (Prove $P \implies Q$. )
3. by Contraposition (Prove $P \implies Q$ by proving $\neg Q \implies \neg P$)
Today: Proofs!!!

1. By Example (or Counterexample).
2. Direct. (Prove $P \implies Q$.)
3. by Contraposition (Prove $P \implies Q$ by proving $\neg Q \implies \neg P$)
4. by Contradiction (Prove $P$ by assuming $\neg P$ and reaching a contradiction.)
CS70: Lecture 2. Outline.

Today: Proofs!!!

1. By Example (or Counterexample).
2. Direct. (Prove $P \implies Q$.)
3. by Contraposition (Prove $P \implies Q$ by proving $\neg Q \implies \neg P$)
4. by Contradiction (Prove $P$ by assuming $\neg P$ and reaching a contradiction.)
5. by Cases (enumerate an exhaustive set of cases)
Quick Background and Notation.

Integers closed under addition.

$a, b \in \mathbb{Z} \Rightarrow a + b \in \mathbb{Z}$

$a | b$ means "$a$ divides $b$".

2 | 4? Yes!

7 | 23? No!

4 | 2? No!

Formally:

$a | b \iff \exists q \in \mathbb{Z}$ where $b = aq$.

3 | 15 since for $q = 5$, $15 = 3(5)$.

A natural number $p > 1$ is prime if it is divisible only by 1 and itself.
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

2 | 4? Yes!

7 | 23? No!

4 | 2? No!

Formally:

\[ a \mid b \iff \exists q \in \mathbb{Z} \text{ where } b = aq \]

3 | 15 since for \( q = 5 \), 15 = 3(5).

A natural number \( p > 1 \), is prime if it is divisible only by 1 and itself.
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a \mid b \) means “a divides b.”
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a \parallel b \) means “a divides b”.

2\parallel 4?

3\parallel 15 since for \( q = 5 \), 15 = 3(5).
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a | b \) means “a divides b”.

2|4? Yes!
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a | b \) means “a divides b”.

2 | 4? Yes!

7 | 23?
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a \mid b \) means “a divides b”.

2\mid4? Yes!

7\mid23? No!
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a | b \) means “a divides b”.

2|4? Yes!

7|23? No!

4|2?
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a \mid b \) means “a divides b”.

2\|4? Yes!

7\|23? No!

4\|2? No!
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a | b \) means “a divides b”.

2|4? Yes!

7|23? No!

4|2? No!

Formally: \( a | b \iff \exists q \in \mathbb{Z} \text{ where } b = aq \).
Quick Background and Notation.

Integers closed under addition.
\[ a, b \in Z \implies a + b \in Z \]

\( a \mid b \) means “\( a \) divides \( b \)”. 

\( 2 \mid 4 \)？ Yes!

\( 7 \mid 23 \)？ No!

\( 4 \mid 2 \)？ No!

Formally: \( a \mid b \iff \exists q \in Z \) where \( b = aq \).

\( 3 \mid 15 \)
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a|b \) means “\( a \) divides \( b \)”.\

2|4? Yes!\
7|23? No!\
4|2? No!\

Formally: \( a|b \iff \exists q \in \mathbb{Z} \text{ where } b = aq \).\

3|15 since for \( q = 5 \),
Quick Background and Notation.

Integers closed under addition.

\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]

\( a \mid b \) means “a divides b”.

2\( \mid \)4? Yes!

7\( \mid \)23? No!

4\( \mid \)2? No!

Formally: \( a \mid b \iff \exists q \in \mathbb{Z} \text{ where } b = aq \).

3\( \mid \)15 since for \( q = 5 \), \( 15 = 3(5) \).
Quick Background and Notation.

Integers closed under addition.
\[ a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z} \]
a\,|\,\,b \text{ means “a divides b”.}

2\,|\,\,4? Yes!
7\,|\,\,23? No!
4\,|\,\,2? No!

Formally: \[ a\,|\,\,b \iff \exists q \in \mathbb{Z} \text{ where } b = aq. \]

3\,|\,\,15 since for \,q = 5, \,15 = 3(5).

A natural number \,p > 1, is **prime** if it is divisible only by 1 and itself.
Direct Proof (Forward Reasoning).

**Theorem:** For any \( a, b, c \in \mathbb{Z} \), if \( a \mid b \) and \( a \mid c \) then \( a \mid b - c \).

**Proof:** Assume \( a \mid b \) and \( a \mid c \)
Theorem: For any $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then $a|b - c$.

Proof: Assume $a|b$ and $a|c$

\[ b = aq \]
Theorem: For any $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then $a|b - c$.

Proof: Assume $a|b$ and $a|c$

\[ b = aq \quad \text{and} \quad c = aq' \]
Direct Proof (Forward Reasoning).

**Theorem:** For any $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then $a|b - c$.

**Proof:** Assume $a|b$ and $a|c$

$b = aq$ and $c = aq'$ where $q, q' \in \mathbb{Z}$
Direct Proof (Forward Reasoning).

**Theorem:** For any $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then $a|b - c$.

**Proof:** Assume $a|b$ and $a|c$

\[ b = aq \text{ and } c = aq' \text{ where } q, q' \in \mathbb{Z} \]

\[ b - c = aq - aq' \]
Direct Proof (Forward Reasoning).

**Theorem:** For any \(a, b, c \in \mathbb{Z}\), if \(a|b\) and \(a|c\) then \(a|b - c\).

**Proof:** Assume \(a|b\) and \(a|c\)

\[
b = aq \quad \text{and} \quad c = aq' \quad \text{where} \quad q, q' \in \mathbb{Z}
\]

\[
b - c = aq - aq' = a(q - q')
\]

Done?
Direct Proof (Forward Reasoning).

**Theorem:** For any $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then $a|b - c$.

**Proof:** Assume $a|b$ and $a|c$

$$b = aq \text{ and } c = aq' \text{ where } q, q' \in \mathbb{Z}$$

$$b - c = aq - aq' = a(q - q')$$

Done?
Theorem: For any $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then $a|b - c$.

Proof: Assume $a|b$ and $a|c$

$b = aq$ and $c = aq'$ where $q, q' \in \mathbb{Z}$

$b - c = aq - aq' = a(q - q')$ Done?

$(b - c) = a(q - q')$
Theorem: For any $a, b, c \in \mathbb{Z}$, if $a | b$ and $a | c$ then $a | b - c$.

Proof: Assume $a | b$ and $a | c$

$b = aq$ and $c = aq'$ where $q, q' \in \mathbb{Z}$

$b - c = aq - aq' = a(q - q')$ Done?

$(b - c) = a(q - q')$ and $(q - q')$ is an integer so
**Theorem:** For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$ then $a \mid b - c$.

**Proof:** Assume $a \mid b$ and $a \mid c$

$b = aq$ and $c = aq'$ where $q, q' \in \mathbb{Z}$

$b - c = aq - aq' = a(q - q')$ Done?

$(b - c) = a(q - q')$ and $(q - q')$ is an integer so

$a \mid (b - c)$
Theorem: For any $a, b, c \in \mathbb{Z}$, if $a | b$ and $a | c$ then $a | b - c$.

Proof: Assume $a | b$ and $a | c$

$b = aq$ and $c = aq'$ where $q, q' \in \mathbb{Z}$

$b - c = aq - aq' = a(q - q')$ Done?

$(b - c) = a(q - q')$ and $(q - q')$ is an integer so

$a | (b - c)$
Theorem: For any $a, b, c \in \mathbb{Z}$, if $a|b$ and $a|c$ then $a|b - c$.

Proof: Assume $a|b$ and $a|c$

$b = aq$ and $c = aq'$ where $q, q' \in \mathbb{Z}$

$b - c = aq - aq' = a(q - q')$ Done?

$(b - c) = a(q - q')$ and $(q - q')$ is an integer so

$a|(b - c)$

Works for $\forall a, b, c$?
Direct Proof (Forward Reasoning).

**Theorem:** For any \( a, b, c \in \mathbb{Z} \), if \( a|b \) and \( a|c \) then \( a|b - c \).

**Proof:** Assume \( a|b \) and \( a|c \)

\[ b = aq \text{ and } c = aq' \text{ where } q, q' \in \mathbb{Z} \]

\[ b - c = aq - aq' = a(q - q') \text{ Done?} \]

\( (b - c) = a(q - q') \) and \( (q - q') \) is an integer so

\[ a|(b - c) \]

Works for \( \forall a, b, c \)?

Argument applies to every \( a, b, c \in \mathbb{Z} \).
**Direct Proof (Forward Reasoning).**

**Theorem:** For any \( a, b, c \in \mathbb{Z} \), if \( a|b \) and \( a|c \) then \( a|b − c \).

**Proof:** Assume \( a|b \) and \( a|c \)

\[
b = aq \quad \text{and} \quad c = aq' \quad \text{where} \quad q, q' \in \mathbb{Z}
\]

\[
b − c = aq − aq' = a(q − q') \quad \text{Done?}
\]

\[
(b − c) = a(q − q') \quad \text{and} \quad (q − q') \text{ is an integer so}
\]

\[
a| (b − c)
\]

Works for \( \forall a, b, c \)?

Argument applies to every \( a, b, c \in \mathbb{Z} \).

Direct Proof Form:
Direct Proof (Forward Reasoning).

**Theorem:** For any \(a, b, c \in \mathbb{Z}\), if \(a|b\) and \(a|c\) then \(a|b - c\).

**Proof:** Assume \(a|b\) and \(a|c\)

\[
b = aq \quad \text{and} \quad c = aq' \quad \text{where} \quad q, q' \in \mathbb{Z}
\]

\[
b - c = aq - aq' = a(q - q') \quad \text{Done?}
\]

\((b - c) = a(q - q')\) and \((q - q')\) is an integer so

\[a|(b - c)\]

Works for \(\forall a, b, c\)?

Argument applies to every \(a, b, c \in \mathbb{Z}\).

Direct Proof Form:

**Goal:** \(P \implies Q\)
Direct Proof (Forward Reasoning).

**Theorem:** For any \( a, b, c \in \mathbb{Z} \), if \( a \mid b \) and \( a \mid c \) then \( a \mid b - c \).

**Proof:** Assume \( a \mid b \) and \( a \mid c \)

\[
b = aq \quad \text{and} \quad c = aq'
\] where \( q, q' \in \mathbb{Z} \)

\[
b - c = aq - aq' = a(q - q')
\]

Done?

\[(b - c) = a(q - q') \] and \( (q - q') \) is an integer so

\[ a \mid (b - c) \]

Works for \( \forall a, b, c \)?

Argument applies to every \( a, b, c \in \mathbb{Z} \).

Direct Proof Form:

**Goal:** \( P \implies Q \)

Assume \( P \).
Theorem: For any \( a, b, c \in \mathbb{Z} \), if \( a | b \) and \( a | c \) then \( a | b - c \).

Proof: Assume \( a | b \) and \( a | c \)
    \( b = aq \) and \( c = aq' \) where \( q, q' \in \mathbb{Z} \)
\( b - c = aq - aq' = a(q - q') \) Done?
\( (b - c) = a(q - q') \) and \( (q - q') \) is an integer so \( a | (b - c) \)

Works for \( \forall a, b, c \)?
   Argument applies to every \( a, b, c \in \mathbb{Z} \).

Direct Proof Form:
   Goal: \( P \implies Q \)
   Assume \( P \).
   ...


Theorem: For any $a, b, c \in \mathbb{Z}$, if $a | b$ and $a | c$ then $a | b - c$.

Proof: Assume $a | b$ and $a | c$

\[ b = aq \text{ and } c = aq' \text{ where } q, q' \in \mathbb{Z} \]

\[ b - c = aq - aq' = a(q - q') \]

Done?

$(b - c) = a(q - q')$ and $(q - q')$ is an integer so $a | (b - c)$

Works for $\forall a, b, c$?

Argument applies to every $a, b, c \in \mathbb{Z}$.

Direct Proof Form:

Goal: $P \implies Q$

Assume $P$.

\[ \ldots \]

Therefore $Q$. 

\[ \square \]
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11 | n$. 

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alternating sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

$100a + 10b + c = 11k + 99a + 11b$

Left hand side is $n$, $k + 9a + b$ is integer.

$\Rightarrow 11 | n$. 

Direct proof of $P \Rightarrow Q$: Assumed $P$: $11 | a - b + c$.

Proved $Q$: $11 | n$. 

Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

- $n = 121$, Alt Sum: $1 - 2 + 1 = 0$, Divis. by 11.
- $n = 605$, Alt Sum: $6 - 0 + 5 = 11$, Divis. by 11.

Proof:

For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

$100a + 10b + c = 11k + 99a + 11b$

Left hand side is $n$, $k + 9a + b$ is integer.

$\implies 11|n$. 

Direct proof of $P \implies Q$: Assumed $P$: $11|a - b + c$.

Proved $Q$: $11|n$. 

Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

\[ \forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n \]

Examples:
\[ n = 121 \]
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11|n$.

\[ \forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n \]

Examples:
\[ n = 121 \quad \text{Alt Sum: } 1 - 2 + 1 = 0. \]
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11 \mid n$.

$$\forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n$$

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11 \mid n$.

\[
\forall n \in D_3, \ (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n
\]

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:
- $n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
- $n = 605$  Alt Sum: $6 - 0 + 5 = 11$
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11 \mid n$.

$$\forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n$$

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is 605
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11 | n$.

$\forall n \in D_3, (11 | \text{alt. sum of digits of } n) \implies 11 | n$

Examples:

- $n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
- $n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

$n = 121$ Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$ Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$,
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:
$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$. 
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum:
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

\[ \forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n \]

Examples:
- $n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
- $n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c$
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:
$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.
Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$. 
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11 | n$.

$$\forall n \in D_3, (11 | \text{alt. sum of digits of } n) \implies 11 | n$$

Examples:
- $n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
- $n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.
Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.
Add $99a + 11b$ to both sides.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:
- $n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
- $n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

$$100a + 10b + c = 11k + 99a + 11b$$
Another direct proof.

Let \( D_3 \) be the 3 digit natural numbers.

Theorem: For \( n \in D_3 \), if the alternating sum of digits of \( n \) is divisible by 11, than \( 11 | n \).

\[ \forall n \in D_3, (11 | \text{alt. sum of digits of } n) \implies 11 | n \]

Examples:
\[ n = 121 \quad \text{Alt Sum: } 1 - 2 + 1 = 0. \text{ Divis. by 11. As is 121.} \]
\[ n = 605 \quad \text{Alt Sum: } 6 - 0 + 5 = 11 \text{ Divis. by 11. As is } 605 = 11(55) \]

Proof: For \( n \in D_3 \), \( n = 100a + 10b + c \), for some \( a, b, c \).

Assume: Alt. sum: \( a - b + c = 11k \) for some integer \( k \).

Add \( 99a + 11b \) to both sides.

\[ 100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b) \]
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11 \mid n$.

\[ \forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n \]

Examples:

$n = 121$  \quad \text{Alt Sum: } 1 - 2 + 1 = 0. \text{ Divis. by 11. As is 121.}$

$n = 605$  \quad \text{Alt Sum: } 6 - 0 + 5 = 11 \text{ Divis. by 11. As is } 605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

\[ 100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b) \]

Left hand side is $n$,
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

\[
\forall n \in D_3, (11 | \text{alt. sum of digits of } n) \implies 11|n
\]

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

\[100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)\]

Left hand side is $n$, $k + 9a + b$ is integer.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11 \mid n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

$$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$$

Left hand side is $n$, $k + 9a + b$ is integer.  $\implies 11|n$. 
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$

Examples:

$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.

$n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

$$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$$

Left hand side is $n$, $k + 9a + b$ is integer.  $\implies 11|n$.  $\blacksquare$
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, then $11|n$.

$$\forall n \in D_3, (11|\text{alternating sum of digits of } n) \implies 11|n$$

Examples:
- $n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divisible by 11. As is 121.
- $n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divisible by 11. As is $605 = 11(55)$

**Proof:** For $n \in D_3$, $n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alternating sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$

Left hand side is $n$, $k + 9a + b$ is integer.  $\implies 11|n$.

$\square$ Direct proof of $P \implies Q$: Assumed $P$: $11|a - b + c$.
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.

Theorem: For $n \in D_3$, if the alternating sum of digits of $n$ is divisible by 11, than $11|n$.

\[ \forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n \]

Examples:
- $n = 121$  Alt Sum: $1 - 2 + 1 = 0$. Divis. by 11. As is 121.
- $n = 605$  Alt Sum: $6 - 0 + 5 = 11$ Divis. by 11. As is $605 = 11(55)$

Proof: For $n \in D_3, n = 100a + 10b + c$, for some $a, b, c$.

Assume: Alt. sum: $a - b + c = 11k$ for some integer $k$.

Add $99a + 11b$ to both sides.

\[ 100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b) \]

Left hand side is $n$, $k + 9a + b$ is integer.  \(\implies 11|n\).

\[ \square \] Direct proof of $P \implies Q$: Assumed $P$: $11|a - b + c$. Proved $Q$: $11|n$.  

The Converse

Thm: \( \forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n \)
The Converse

Thm: \( \forall n \in D_3, (11 | \text{alt. sum of digits of } n) \implies 11 | n \)

Is converse a theorem?

\( \forall n \in D_3, (11 | n) \implies (11 | \text{alt. sum of digits of } n) \)
The Converse

Thm: $\forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n$

Is converse a theorem?
$\forall n \in D_3, (11 \mid n) \implies (11 \mid \text{alt. sum of digits of } n)$

Example: $n = 264$. 
The Converse

Thm: $\forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n$

Is converse a theorem?

$\forall n \in D_3, (11 \mid n) \implies (11 \mid \text{alt. sum of digits of } n)$

Example: $n = 264$. $11 \mid n$?
The Converse

Thm: \( \forall n \in D_3, (11 \mid \text{alt. sum of digits of } n) \implies 11 \mid n \)

Is converse a theorem?
\( \forall n \in D_3, (11 \mid n) \implies (11 \mid \text{alt. sum of digits of } n) \)

Example: \( n = 264 \). Is \( 11 \mid n \)? Is \( 11 \mid 2 - 6 + 4 \)?
Another Direct Proof.

Theorem: $\forall n \in D_3, (11|n) \iff (11|\text{alt. sum of digits of } n)$
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \iff (11|\text{alt. sum of digits of } n) \)

Proof:

Assume \( 11|n \). \( n = 100a + 10b + c = 11k \) \( \implies 99a + 11b + (a - b + c) = 11k \) \( \implies a - b + c = 11\ell \) where \( \ell = (k - 9a - b) \in \mathbb{Z} \)

That is \( 11|\text{alternating sum of digits}. \)

Note: Similar proof to other. In this case every \( = \implies \iff \) Often works with arithmetic properties except when multiplying by 0.

We have.
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \iff (11|\text{alt. sum of digits of } n) \)

Proof: Assume \( 11|n \).
Another Direct Proof.

Theorem: $\forall n \in D_3, (11 \mid n) \iff (11 \mid \text{alt. sum of digits of } n)$

Proof: Assume $11 \mid n$.

$n = 100a + 10b + c = 11k$
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \iff (11|\text{alt. sum of digits of } n) \)

Proof: Assume 11|\(n\).

\[
n = 100a + 10b + c = 11k \implies 99a + 11b + (a - b + c) = 11k
\]
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \iff (11|\text{alt. sum of digits of } n) \)

Proof: Assume \(11|n\).

\[
\begin{align*}
n &= 100a + 10b + c = 11k 
\quad \implies \\
99a + 11b + (a - b + c) &= 11k 
\quad \implies \\
\quad a - b + c &= 11k - 99a - 11b
\end{align*}
\]
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n) \)

**Proof:** Assume \(11|n\).

\[
n = 100a + 10b + c = 11k \implies 99a + 11b + (a - b + c) = 11k \implies a - b + c = 11k - 99a - 11b \implies a - b + c = 11(k - 9a - b)
\]
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n) \)

Proof: Assume 11|n.

\[
n = 100a + 10b + c = 11k \implies 99a + 11b + (a - b + c) = 11k \implies a - b + c = 11k - 99a - 11b \implies a - b + c = 11(k - 9a - b) \implies a - b + c = 11\ell
\]
Another Direct Proof.

Theorem: $\forall n \in D_3, (11|n) \iff (11|\text{alt. sum of digits of } n)$

Proof: Assume $11|n$.

$n = 100a + 10b + c = 11k \implies$

$99a + 11b + (a - b + c) = 11k \implies$

$a - b + c = 11k - 99a - 11b \implies$

$a - b + c = 11(k - 9a - b) \implies$

$a - b + c = 11\ell \text{ where } \ell = (k - 9a - b) \in \mathbb{Z}$
Another Direct Proof.

Theorem: $\forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n)$

Proof: Assume $11|n$.

$n = 100a + 10b + c = 11k \implies$  
$99a + 11b + (a - b + c) = 11k \implies$  
$a - b + c = 11k - 99a - 11b \implies$  
$a - b + c = 11(k - 9a - b) \implies$  
$a - b + c = 11\ell$ where $\ell = (k - 9a - b) \in \mathbb{Z}$

That is $11|\text{alternating sum of digits.}$
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n) \)

**Proof:** Assume \( 11|n \).

\[
n = 100a + 10b + c = 11k \implies \\
99a + 11b + (a - b + c) = 11k \implies \\
a - b + c = 11k - 99a - 11b \implies \\
a - b + c = 11(k - 9a - b) \implies \\
a - b + c = 11\ell \text{ where } \ell = (k - 9a - b) \in \mathbb{Z}
\]

That is \( 11|\text{alternating sum of digits}. \)

Note: similar proof to other. In this case every \( \implies \) is \( \iff \).
Another Direct Proof.

Theorem: \( \forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n) \)

Proof: Assume \( 11|n \).

\[
\begin{align*}
n &= 100a + 10b + c = 11k \\ 99a + 11b + (a - b + c) &= 11k \\ a - b + c &= 11k - 99a - 11b \\ a - b + c &= 11(k - 9a - b) \\ a - b + c &= 11\ell \text{ where } \ell = (k - 9a - b) \in \mathbb{Z}
\end{align*}
\]

That is \( 11|\text{alternating sum of digits} \).

Note: similar proof to other. In this case every \( \implies \) is \( \iff \).

Often works with arithmetic properties except when multiplying by 0.
Theorem: \( \forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n) \)

Proof: Assume \( 11|n \).

\[
\begin{align*}
n = 100a + 10b + c &= 11k \\
99a + 11b + (a - b + c) &= 11k \\
a - b + c &= 11k - 99a - 11b \\
a - b + c &= 11(k - 9a - b) \\
a - b + c &= 11 \ell \text{ where } \ell = (k - 9a - b) \in \mathbb{Z}
\end{align*}
\]

That is \( 11|\text{alternating sum of digits.} \)

Note: similar proof to other. In this case every \( \implies \) is \( \iff \)

Often works with arithmetic properties except when multiplying by 0.

We have.
Another Direct Proof.

Theorem: $\forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n)$

Proof: Assume $11|n$.

$n = 100a + 10b + c = 11k$ \implies
$99a + 11b + (a - b + c) = 11k$ \implies
$a - b + c = 11k - 99a - 11b$ \implies
$a - b + c = 11(k - 9a - b)$ \implies
$a - b + c = 11\ell$ where $\ell = (k - 9a - b) \in \mathbb{Z}$

That is $11|\text{alternating sum of digits}$. 

Note: similar proof to other. In this case every $\implies$ is $\iff$

Often works with arithmetic properties except when multiplying by 0.

We have.

Theorem: $\forall n \in D_3, (11|\text{alt. sum of digits of } n) \iff (11|n)$
Another Proof?

Theorem: \( \forall n \in D_3, (11|n) \iff (11|\text{alt. sum of digits of } n) \)
Another Proof?

Theorem: \( \forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n) \)

"Proof":

Another Proof?

Theorem: $\forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n)$

“Proof”:
Let $n = abc$, where $a$, $b$, and $c$ are the hundreds, tens, and units digits of $n$, respectively.

If $11$ divides $n$, then there exists an integer $k$ such that: $n = 11k$

Now, let’s calculate the alternating sum of digits:
Alternating sum $= a - b + c$

Since $n = 11k$, we have: $a - b + c = 11k$

This shows that the alternating sum of digits is equal to $11$ times some integer $k$, and therefore, it is divisible by $11$. 
Proof by Contraposition

Thm: For \( n \in \mathbb{Z}^+ \) and \( d \mid n \). If \( n \) is odd then \( d \) is odd.

\( n = 2k + 1 \)

what do we know about \( d \)?

What to do?

Goal: Prove \( P \Rightarrow Q \).

Assume \( \neg Q \) ... and prove \( \neg P \).

Conclusion: \( \neg Q \Rightarrow \neg P \) equivalent to \( P \Rightarrow Q \).

Proof: Assume \( \neg Q \): \( d \) is even. \( d = 2k \).

\( d \mid n \) so we have

\( n = qd = q(2k) = 2(kq) \)

\( n \) is even. \( \neg P \)
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.
Thm: For $n \in Z^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$
Thm: For $n \in Z^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?
Thm: For \( n \in Z^+ \) and \( d | n \). If \( n \) is odd then \( d \) is odd.

\[
n = 2k + 1 \text{ what do we know about } d?\]

What to do?
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$. 
Proof by Contraposition

Thm: For $n \in Z^+$ and $d | n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$. 
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$
...and prove $\neg P$. 

Conclusion: $\neg Q = \implies \neg P$ equivalent to $P \implies Q$. 

Proof: Assume $\neg Q$:

$d$ is even.

$d = 2k$.

$d|n$ so we have $n = qd = q(2k) = 2(kq)$

$n$ is even.

$\neg P$
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$ equivalent to $P \implies Q$. 
Proof by Contraposition

Thm: For $n \in Z^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$ equivalent to $P \implies Q$.

Proof: Assume $\neg Q$: $d$ is even.
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$ equivalent to $P \implies Q$.

Proof: Assume $\neg Q$: $d$ is even. $d = 2k$. 
Thm: For \( n \in \mathbb{Z}^+ \) and \( d|n \). If \( n \) is odd then \( d \) is odd.

\[ n = 2k + 1 \] what do we know about \( d \)?

What to do?

Goal: Prove \( P \implies Q \).

Assume \( \neg Q \)

...and prove \( \neg P \).

Conclusion: \( \neg Q \implies \neg P \) equivalent to \( P \implies Q \).

Proof: Assume \( \neg Q \): \( d \) is even. \( d = 2k \).

\( d|n \) so we have
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$ equivalent to $P \implies Q$.

Proof: Assume $\neg Q$: $d$ is even. $d = 2k$.

d|n so we have

$n = qd$
Proof by Contraposition

Thm: For \( n \in \mathbb{Z}^+ \) and \( d|n \). If \( n \) is odd then \( d \) is odd.

\[ n = 2k + 1 \] what do we know about \( d \)?

What to do?

Goal: Prove \( P \implies Q \).

Assume \( \neg Q \)

...and prove \( \neg P \).

Conclusion: \( \neg Q \implies \neg P \) equivalent to \( P \implies Q \).

Proof: Assume \( \neg Q \): \( d \) is even. \( d = 2k \).

\( d|n \) so we have

\[ n = qd = q(2k) \]
Proof by Contraposition

Thm: For \( n \in \mathbb{Z}^+ \) and \( d|n \). If \( n \) is odd then \( d \) is odd.

\[ n = 2k + 1 \] what do we know about \( d \)?

What to do?

Goal: Prove \( P \implies Q \).

Assume \( \neg Q \)

...and prove \( \neg P \).

Conclusion: \( \neg Q \implies \neg P \) equivalent to \( P \implies Q \).

**Proof:** Assume \( \neg Q \): \( d \) is even. \( d = 2k \).

\( d|n \) so we have

\[ n = qd = q(2k) = 2(kq) \]
Proof by Contraposition

Thm: For $n \in \mathbb{Z}^+$ and $d|n$. If $n$ is odd then $d$ is odd.

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.
Assume $\neg Q$
...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$ equivalent to $P \implies Q$.

Proof: Assume $\neg Q$: $d$ is even. $d = 2k$.

$d|n$ so we have

$n = qd = q(2k) = 2(kq)$

$n$ is even.
Thm: For $n \in Z^+$ and $d|n$. If $n$ is odd then $d$ is odd. 

$n = 2k + 1$ what do we know about $d$?

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

...and prove $\neg P$.

Conclusion: $\neg Q \implies \neg P$ equivalent to $P \implies Q$.

Proof: Assume $\neg Q$: $d$ is even. $d = 2k$.

$d|n$ so we have

$n = qd = q(2k) = 2(kq)$

$n$ is even. $\neg P$
Lemma:
For every $n$ in $\mathbb{N}$, $n^2$ is even $\Rightarrow n$ is even. ($P \Rightarrow Q$)

Proof by contraposition: ($P \Rightarrow Q$) $\equiv$ ($\neg Q = \Rightarrow \neg P$)

$P$ = 'If $n^2$ is even, then $n$ is even.'

$\neg P$ = 'If $n^2$ is odd, then $n$ is even.'

$Q$ = 'If $n$ is odd, then $n^2$ is odd.'

Prove $\neg Q = \Rightarrow \neg P$:

$n$ is odd $\Rightarrow n^2$ is odd.

$n = 2k + 1$ where $k$ is a natural number.

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

$n^2 = 2l + 1$ where $l$ is a natural number.

And $n^2$ is odd!
Another Contrapostion...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

Proof by contraposition: ($P \implies Q$) $\equiv$ ($\neg Q = \implies \neg P$)

$P = \text{'}n^2$ is even.'

$\neg P = \text{'}n^2$ is odd.'

$Q = \text{'}n$ is even.'

$\neg Q = \text{'}n$ is odd.'

Prove $\neg Q = \implies \neg P$:

$n$ is odd $\implies n^2$ is odd.

$n = 2k + 1$

$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

$n^2 = 2l + 1$ where $l$ is a natural number.

...and $n^2$ is odd!

$\neg Q = \implies \neg P$ so $P = \implies Q$ and ...
Another Contraposition...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\iff n$ is even. ($P \iff Q$)

$n^2$ is even, $n^2 = 2k$, ...
Another Contrapostion...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

$n^2$ is even, $n^2 = 2k$, ... $\sqrt{2k}$ even?
Another Contraposition...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

Proof by contraposition: ($P \implies Q) \equiv (\neg Q \implies \neg P$)
Another Contraposition...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies$ $n$ is even. ($P \implies Q$)

**Proof by contraposition:** ($P \implies Q$) $\equiv$ ($\neg Q \implies \neg P$)

$P = \text{'}n^2 \text{ is even.}' \quad \text{............}$

$\neg P = \text{'}n^2 \text{ is odd.'} \quad \text{............}$

$\neg Q = \text{'}n \text{ is odd.'} \quad \text{............}$
Another Contrapostion...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

**Proof by contraposition:** ($P \implies Q) \equiv (\neg Q \implies \neg P$)

$P = 'n^2$ is even.' ............ $\neg P = 'n^2$ is odd'
Lemma: For every \( n \) in \( \mathbb{N} \), \( n^2 \) is even \( \implies \) \( n \) is even. \((P \implies Q)\)

Proof by contraposition: \((P \implies Q) \equiv (\neg Q \implies \neg P)\)

\( P = \) ’\( n^2 \) is even.’ ........... \( \neg P = \) ’\( n^2 \) is odd’

\( Q = \) ’\( n \) is even’ ............
Another Contrapostion...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

**Proof by contraposition:** $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P = 'n^2$ is even.' ........... $\neg P = 'n^2$ is odd'

$Q = 'n$ is even' ........... $\neg Q = 'n$ is odd'
Another Contraposition...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies$ $n$ is even. ($P \implies Q$)

**Proof by contraposition:** $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P = 'n^2$ is even.' ........... $\neg P = 'n^2$ is odd'

$Q = 'n$ is even' ........... $\neg Q = 'n$ is odd'

Prove $\neg Q \implies \neg P$: $n$ is odd $\implies n^2$ is odd.
Another Contrapostion...

**Lemma:** For every \( n \) in \( N \), \( n^2 \) is even \( \implies n \) is even. \((P \implies Q)\)

**Proof by contraposition:** \((P \implies Q) \equiv (\neg Q \implies \neg P)\)

\( P = 'n^2 \text{ is even}' \) \ .......... \( \neg P = 'n^2 \text{ is odd}' \)

\( Q = 'n \text{ is even}' \) \ .......... \( \neg Q = 'n \text{ is odd}' \)

Prove \( \neg Q \implies \neg P \): \( n \text{ is odd} \implies n^2 \text{ is odd}.\)

\( n = 2k + 1 \)
Another Contrapostion...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\iff n$ is even. $(P \implies Q)$

**Proof by contraposition:** $(P \implies Q) \equiv (\neg Q \implies \neg P)$

$P = 'n^2$ is even.’ ............ $\neg P = 'n^2$ is odd’

$Q = 'n$ is even’ ............ $\neg Q = 'n$ is odd’

Prove $\neg Q \implies \neg P$: $n$ is odd $\implies n^2$ is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. 
Another Contraposition...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

**Proof by contraposition:** ($P \implies Q$) $\equiv$ ($\neg Q \implies \neg P$)

$P = \text{'}n^2$ is even.' ............ $\neg P = \text{'}n^2$ is odd'

$Q = \text{'}n$ is even' ............ $\neg Q = \text{'}n$ is odd'

Prove $\neg Q \implies \neg P$: $n$ is odd $\implies n^2$ is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

$n^2 = 2l + 1$ where $l$ is a natural number..
Another Contrapostion...

**Lemma:** For every \( n \) in \( N \), \( n^2 \) is even \( \iff \) \( n \) is even. \((P \iff Q)\)

**Proof by contraposition:** \((P \iff Q) \equiv (\neg Q \iff \neg P)\)

\( P = 'n^2 \) is even.’ ............ \( \neg P = 'n^2 \) is odd’

\( Q = 'n \) is even’ ............ \( \neg Q = 'n \) is odd’

Prove \( \neg Q \iff \neg P\): \( n \) is odd \( \iff \) \( n^2 \) is odd.

\( n = 2k + 1 \)

\( n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1. \)

\( n^2 = 2l + 1 \) where \( l \) is a natural number..

... and \( n^2 \) is odd!
Lemma: For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

Proof by contraposition: ($P \implies Q$) $\equiv$ ($\neg Q \implies \neg P$)

$P = 'n^2$ is even.' ........... $\neg P = 'n^2$ is odd'

$Q = 'n$ is even' ........... $\neg Q = 'n$ is odd'

Prove $\neg Q \implies \neg P$: $n$ is odd $\implies n^2$ is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. 

$n^2 = 2l + 1$ where $l$ is a natural number..

... and $n^2$ is odd!

$\neg Q \implies \neg P$
Lemma: For every \( n \) in \( N \), \( n^2 \) is even \( \implies \) \( n \) is even. \((P \implies Q)\)

Proof by contraposition: \((P \implies Q) \equiv (\neg Q \implies \neg P)\)

\( P = 'n^2 \) is even.' .............. \( \neg P = 'n^2 \) is odd'

\( Q = 'n \) is even' .............. \( \neg Q = 'n \) is odd'

Prove \( \neg Q \implies \neg P: \) \( n \) is odd \( \implies \) \( n^2 \) is odd.

\( n = 2k + 1 \)

\( n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1. \)

\( n^2 = 2l + 1 \) where \( l \) is a natural number..

... and \( n^2 \) is odd!

\( \neg Q \implies \neg P \) so \( P \implies Q \) and ...
Another Contrapostion...

**Lemma:** For every $n$ in $N$, $n^2$ is even $\implies n$ is even. ($P \implies Q$)

**Proof by contraposition:** ($P \implies Q) \equiv (\neg Q \implies \neg P$)

$P = 'n^2$ is even.' ............ $\neg P = 'n^2$ is odd'

$Q = 'n$ is even' ............ $\neg Q = 'n$ is odd'

Prove $\neg Q \implies \neg P$: $n$ is odd $\implies n^2$ is odd.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

$n^2 = 2l + 1$ where $l$ is a natural number..

... and $n^2$ is odd!

$\neg Q \implies \neg P$ so $P \implies Q$ and ...
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

Must show:
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$,
Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.
Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$. 
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

Must show: For every \( a, b \in \mathbb{Z} \), \( \left( \frac{a}{b} \right)^2 \neq 2 \).

A simple property (equality) should always “not” hold.
Theorem: $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$. 
**Theorem:** $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P$
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $\left(\frac{a}{b}\right)^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P \implies P_1$
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

Must show: For every \( a, b \in Z \), \( \left( \frac{a}{b} \right)^2 \neq 2 \).

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** \( P \).

\[ \neg P \implies P_1 \ldots \]
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

Must show: For every \( a, b \in \mathbb{Z} \), \( \left( \frac{a}{b} \right)^2 \neq 2 \).

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** \( P \).

\( \neg P \implies P_1 \cdots \implies R \)
Theorem: $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $\left(\frac{a}{b}\right)^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P \implies P_1 \cdots \implies R \implies \neg P$
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P \implies P_1 \implies R$

$\neg P \implies P_1$
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

**Must show:** For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots$
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

Must show: For every \( a, b \in \mathbb{Z} \), \( \left( \frac{a}{b} \right)^2 \neq 2 \).

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** \( P \).

\[ \neg P \implies P_1 \cdots \implies R \]

\[ \neg P \implies P_1 \cdots \implies \neg R \]
Proof by Contradiction

**Theorem:** \( \sqrt{2} \) is irrational.

Must show: For every \( a, b \in \mathbb{Z} \), \( \left( \frac{a}{b} \right)^2 \neq 2 \).

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** \( P \).

\[ \neg P \implies P_1 \cdots \implies R \]

\[ \neg P \implies P_1 \cdots \implies \neg R \]

\[ \neg P \implies \text{False} \]
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P \implies \text{False}$

Contrapositive: True $\implies P$. 
Proof by Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Must show: For every $a, b \in Z$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

**Theorem:** $P$.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P \implies \text{False}$

Contrapositive: True $\implies P$. Theorem $P$ is proven.
Theorem: $\sqrt{2}$ is irrational.

Must show: For every $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

A simple property (equality) should always “not” hold.

Proof by contradiction:

Theorem: $P$.

$\neg P \implies P_1 \cdots \implies R$

$\neg P \implies P_1 \cdots \implies \neg R$

$\neg P \implies \text{False}$

Contrapositive: True $\implies P$. Theorem $P$ is proven.
Contradiction

Theorem: \( \sqrt{2} \) is irrational.
Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Assume $\neg P$:

Reduced form: $a$ and $b$ have no common factors.

$\sqrt{2}b = \frac{a}{b^2} = \frac{a^2}{b^2} = 4k^2$

$a^2$ is even $\Rightarrow a$ is even.

$a = 2k$ for some integer $k$.

$b^2 = 2k^2$

$b^2$ is even $\Rightarrow b$ is even.

$a$ and $b$ have a common factor. Contradiction.
Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$. 

Reduced form: $a$ and $b$ have no common factors.

$$\sqrt{2} \cdot b = a^2 = 2k^2$$

$a^2$ is even $\Rightarrow a$ is even.

$$a = 2k$$

For some integer $k$.

$$b^2 = 2k^2$$

$b^2$ is even $\Rightarrow b$ is even.

$a$ and $b$ have a common factor. Contradiction.
Theorem: $\sqrt{2}$ is irrational.
Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.
Reduced form: $a$ and $b$ have no common factors.
Theorem: $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

\[ \sqrt{2}b = a \]
**Theorem:** $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

$$\sqrt{2}b = a$$

$$2b^2 = a^2$$
**Theorem:** $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

\[ \sqrt{2}b = a \]

\[ 2b^2 = a^2 \]

$a^2$ is even $\implies a$ is even.
Theorem: $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

$$\sqrt{2}b = a$$

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

$a^2$ is even $\implies$ $a$ is even.

$a = 2k$ for some integer $k$.
Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

$$\sqrt{2}b = a$$

$$2b^2 = a^2 = 4k^2$$

$a^2$ is even $\implies$ $a$ is even.

$a = 2k$ for some integer $k$
Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

\[
\sqrt{2}b = a
\]

\[
2b^2 = a^2 = 4k^2
\]

$a^2$ is even $\implies$ $a$ is even.

$a = 2k$ for some integer $k$

\[
b^2 = 2k^2
\]
Contradiction

**Theorem:** $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

\[
\sqrt{2}b = a
\]

\[
2b^2 = a^2 = 4k^2
\]

$a^2$ is even $\implies$ $a$ is even.

$a = 2k$ for some integer $k$

\[
b^2 = 2k^2
\]

$b^2$ is even $\implies$ $b$ is even.
Contradiction

**Theorem**: $\sqrt{2}$ is irrational.

Assume $\neg P$: $\sqrt{2} = a/b$ for $a, b \in \mathbb{Z}$.

Reduced form: $a$ and $b$ have no common factors.

\[
\sqrt{2}b = a
\]

\[
2b^2 = a^2 = 4k^2
\]

$a^2$ is even $\implies$ $a$ is even.

$a = 2k$ for some integer $k$

\[
b^2 = 2k^2
\]

$b^2$ is even $\implies$ $b$ is even.

$a$ and $b$ have a common factor. Contradiction.
Theorem: \( \sqrt{2} \) is irrational.

Assume \( \neg P: \sqrt{2} = a/b \) for \( a, b \in \mathbb{Z} \).

Reduced form: \( a \) and \( b \) have no common factors.

\[
\sqrt{2}b = a
\]

\[
2b^2 = a^2 = 4k^2
\]

\( a^2 \) is even \( \Rightarrow \) \( a \) is even.

\( a = 2k \) for some integer \( k \)

\[
b^2 = 2k^2
\]

\( b^2 \) is even \( \Rightarrow \) \( b \) is even.

\( a \) and \( b \) have a common factor. Contradiction.
Proof by contradiction: example

**Theorem:** There are infinitely many primes.
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

Assume finitely many primes: $p_1, \ldots, p_k$.

Consider $q = p_1 \times p_2 \times \cdots \times p_k + 1$.

$q$ cannot be one of the primes as it is larger than any $p_i$.

$q$ has prime divisor $p$, which is one of $p_i$.

$p$ divides both $x = p_1 \times p_2 \times \cdots \times p_k$ and $q$, and divides $q - x$.

$p | q - x = q - 1$.

$p \leq q - 1$.

So $p \leq 1$.

(Contradicts the original assumption.)

The original assumption that "the theorem is false" is false, thus the theorem is proven.
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**
- Assume finitely many primes: $p_1, \ldots, p_k$. 

Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider
  \[ q = p_1 \times p_2 \times \cdots p_k + 1. \]
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**
- Assume finitely many primes: \( p_1, \ldots, p_k \).
- Consider
  \[
  q = p_1 \times p_2 \times \cdots p_k + 1.
  \]
- \( q \) cannot be one of the primes as it is larger than any \( p_i \).

\( q \) is a number larger than all primes, yet not a prime itself, leading to a contradiction. The original assumption is thus false, proving the theorem.
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: \( p_1, \ldots, p_k \).
- Consider \( q = p_1 \times p_2 \times \cdots p_k + 1 \).

- \( q \) cannot be one of the primes as it is larger than any \( p_i \).
- \( q \) has prime divisor \( p \) ("\( p > 1 \) = R") which is one of \( p_i \).
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider $q = p_1 \times p_2 \times \cdots p_k + 1$.

- $q$ cannot be one of the primes as it is larger than any $p_i$.
- $q$ has prime divisor $p$ ("$p > 1$" = R) which is one of $p_i$.
- $p$ divides both $x = p_1 \cdot p_2 \cdots p_k$ and $q$.

Thus, the original assumption that "the theorem is false" is false, thus the theorem is proven.
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: \( p_1, \ldots, p_k. \)
- Consider \( q = p_1 \times p_2 \times \cdots p_k + 1. \)
- \( q \) cannot be one of the primes as it is larger than any \( p_i. \)
- \( q \) has prime divisor \( p \) ("\( p > 1 \) = R") which is one of \( p_i. \)
- \( p \) divides both \( x = p_1 \cdot p_2 \cdots p_k \) and \( q, \) and divides \( q - x, \)
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: \( p_1, \ldots, p_k \).
- Consider \( q = p_1 \times p_2 \times \cdots \times p_k + 1 \).

- \( q \) cannot be one of the primes as it is larger than any \( p_i \).
- \( q \) has prime divisor \( p \) (”\( p > 1 \)” = R) which is one of \( p_i \).
- \( p \) divides both \( x = p_1 \cdot p_2 \cdot \cdots p_k \) and \( q \), and divides \( q - x \),

\[ \implies p \mid q - x \]
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider
  
  $$q = p_1 \times p_2 \times \cdots p_k + 1.$$

- $q$ cannot be one of the primes as it is larger than any $p_i$.
- $q$ has prime divisor $p$ ("$p > 1$" $= R$) which is one of $p_i$.
- $p$ divides both $x = p_1 \cdot p_2 \cdots p_k$ and $q$, and divides $q - x$, 
  
  $\implies p | q - x \implies p \leq q - x$.

The original assumption that "the theorem is false" is false, thus the theorem is proven.
Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: \( p_1, \ldots, p_k \).
- Consider \( q = p_1 \times p_2 \times \cdots p_k + 1 \).

- \( q \) cannot be one of the primes as it is larger than any \( p_i \).
- \( q \) has prime divisor \( p \) ("\( p > 1 \)" = R) which is one of \( p_i \).
- \( p \) divides both \( x = p_1 \cdot p_2 \cdots p_k \) and \( q \), and divides \( q - x \),
  \[ p \mid q - x \implies p \leq q - x = 1. \]
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider
  \[ q = p_1 \times p_2 \times \cdots p_k + 1. \]

- $q$ cannot be one of the primes as it is larger than any $p_i$.
- $q$ has prime divisor $p$ ("$p > 1$" = R) which is one of $p_i$.
- $p$ divides both $x = p_1 \cdot p_2 \cdots p_k$ and $q$, and divides $q - x$,
  \[ \implies p | q - x \implies p \leq q - x = 1. \]
- so $p \leq 1$. 

The original assumption that "the theorem is false" is false, thus the theorem is proven.
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider
  
  \[ q = p_1 \times p_2 \times \cdots p_k + 1. \]

- $q$ cannot be one of the primes as it is larger than any $p_i$.
- $q$ has prime divisor $p$ (”$p > 1$” = R ) which is one of $p_i$.
- $p$ divides both $x = p_1 \cdot p_2 \cdots p_k$ and $q$, and divides $q - x$,
  
  \[ \Rightarrow p \mid q - x \Rightarrow p \leq q - x = 1. \]
- so $p \leq 1$. (Contradicts $R$.)

The original assumption that “the theorem is false” is false, thus the theorem is proven.
Theorem: There are infinitely many primes.

Proof:

- Assume finitely many primes: $p_1, \ldots, p_k$.
- Consider $q = p_1 \times p_2 \times \cdots p_k + 1$.

- $q$ cannot be one of the primes as it is larger than any $p_i$.
- $q$ has prime divisor $p$ ("$p > 1$" = R) which is one of $p_i$.
- $p$ divides both $x = p_1 \cdot p_2 \cdots p_k$ and $q$, and divides $q - x$.
- $p|q - x \implies p \leq q - x = 1$.
- so $p \leq 1$. (Contradicts R.)

The original assumption that “the theorem is false” is false, thus the theorem is proven.
Proof by contradiction: example

**Theorem:** There are infinitely many primes.

**Proof:**

- Assume finitely many primes: \( p_1, \ldots, p_k \).
- Consider \( q = p_1 \times p_2 \times \cdots p_k + 1 \).

- \( q \) cannot be one of the primes as it is larger than any \( p_i \).
- \( q \) has prime divisor \( p \) ("\( p > 1 \)" = R) which is one of \( p_i \).
- \( p \) divides both \( x = p_1 \cdot p_2 \cdot \cdots p_k \) and \( q \), and divides \( q - x \),

\[ \implies p \mid q - x \implies p \leq q - x = 1. \]

- so \( p \leq 1 \). (Contradicts R.)

The original assumption that “the theorem is false” is false, thus the theorem is proven.
Did we prove?

- “The product of the first $k$ primes plus 1 is prime.”
Product of first $k$ primes.

Did we prove?
- “The product of the first $k$ primes plus 1 is prime.”
- No.

Consider example.

$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$

There is a prime in between 13 and $q = 30031$ that divides $q$.

Proof assumed no primes in between.
Did we prove?

- “The product of the first $k$ primes plus 1 is prime.”
- No.
- The chain of reasoning started with a false statement.
Product of first $k$ primes..

Did we prove?

- “The product of the first $k$ primes plus 1 is prime.”
- No.
- The chain of reasoning started with a false statement.

Consider example..
Product of first $k$ primes..

Did we prove?
- “The product of the first $k$ primes plus 1 is prime.”
- No.
- The chain of reasoning started with a false statement.

Consider example..
- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$
Did we prove?

- “The product of the first \( k \) primes plus 1 is prime.”
- No.
- The chain of reasoning started with a false statement.

Consider example..

- \( 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509 \)
- There is a prime \textit{in between} 13 and \( q = 30031 \) that divides \( q \).
Did we prove?

- “The product of the first $k$ primes plus 1 is prime.”
- No.
- The chain of reasoning started with a false statement.

Consider example..

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$
- There is a prime *in between* 13 and $q = 30031$ that divides $q$.
- Proof assumed no primes *in between*.
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** $x^5 - x + 1 = 0$ has no solution in the rationals.
Proof by cases. ("divide-and-conquer" strategy)

Theorem: $x^5 - x + 1 = 0$ has no solution in the rationals.

Proof: First a lemma...

Lemma: If $x$ is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, then both $a$ and $b$ are even.
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** $x^5 - x + 1 = 0$ has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If $x$ is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, then both $a$ and $b$ are even.

Reduced form $\frac{a}{b}$: $a$ and $b$ can’t both be even!
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** $x^5 - x + 1 = 0$ has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If $x$ is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, then both $a$ and $b$ are even.

Reduced form $\frac{a}{b}$: $a$ and $b$ can’t both be even! + Lemma
Proof by cases. (“divide-and-conquer” strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma

\[ \implies \text{ no rational solution.} \]
Proof by cases. (“divide-and-conquer” strategy)

**Theorem:** $x^5 - x + 1 = 0$ has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If $x$ is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, *then both $a$ and $b$ are even.*

Reduced form $\frac{a}{b}$: $a$ and $b$ can’t both be even! + Lemma $\implies$ no rational solution.

**Proof of lemma:** Assume a solution of the form $a/b$. 
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** \(x^5 - x + 1 = 0\) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \(x\) is a solution to \(x^5 - x + 1 = 0\) and \(x = a/b\) for \(a, b \in \mathbb{Z}\), then both \(a\) and \(b\) are even.

Reduced form \(\frac{a}{b}\): \(a\) and \(b\) can’t both be even! + Lemma \(\implies\) no rational solution.

**Proof of lemma:** Assume a solution of the form \(a/b\).

\[
\left(\frac{a}{b}\right)^5 - \frac{a}{b} + 1 = 0
\]
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = \frac{a}{b} \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( \frac{a}{b} \).

\[
\left( \frac{a}{b} \right)^5 - \frac{a}{b} + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[
\left( \frac{a}{b} \right)^5 - a/b + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]

**Case 1:** \( a \) odd, \( b \) odd: odd - odd + odd = even.
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[
\left( \frac{a}{b} \right)^5 - a/b + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]

**Case 1:** \( a \) odd, \( b \) odd: odd - odd + odd = even. Not possible.
Proof by cases. (“divide-and-conquer” strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[
\left( \frac{a}{b} \right)^5 - \frac{a}{b} + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]

Case 1: \( a \) odd, \( b \) odd: odd - odd + odd = even. Not possible.

Case 2: \( a \) even, \( b \) odd: even - even + odd = even.
Proof by cases. (“divide-and-conquer” strategy)

**Theorem:** \(x^5 - x + 1 = 0\) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \(x\) is a solution to \(x^5 - x + 1 = 0\) and \(x = a/b\) for \(a, b \in \mathbb{Z}\), then both \(a\) and \(b\) are even.

Reduced form \(\frac{a}{b}\): \(a\) and \(b\) can’t both be even! + Lemma \(\implies\) no rational solution.

**Proof of lemma:** Assume a solution of the form \(a/b\).

\[\left(\frac{a}{b}\right)^5 - \frac{a}{b} + 1 = 0\]

multiply by \(b^5\),

\[a^5 - ab^4 + b^5 = 0\]

**Case 1:** \(a\) odd, \(b\) odd: odd - odd + odd = even. Not possible.
**Case 2:** \(a\) even, \(b\) odd: even - even + odd = even. Not possible.
Proof by cases. (“divide-and-conquer” strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \iff \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[
\left( \frac{a}{b} \right)^5 - \frac{a}{b} + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]

Case 1: \( a \) odd, \( b \) odd: odd - odd + odd = even. Not possible.

Case 2: \( a \) even, \( b \) odd: even - even + odd = even. Not possible.

Case 3: \( a \) odd, \( b \) even: odd - even + even = even.
Proof by cases. (“divide-and-conquer” strategy)

**Theorem:** $x^5 - x + 1 = 0$ has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If $x$ is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, then both $a$ and $b$ are even.

Reduced form $\frac{a}{b}$: $a$ and $b$ can’t both be even! + Lemma $\implies$ no rational solution.

**Proof of lemma:** Assume a solution of the form $a/b$.

\[
\left( \frac{a}{b} \right)^5 - a/b + 1 = 0
\]

multiply by $b^5$,

\[
a^5 - ab^4 + b^5 = 0
\]

Case 1: $a$ odd, $b$ odd: odd - odd + odd = even. Not possible.

Case 2: $a$ even, $b$ odd: even - even + odd = even. Not possible.

Case 3: $a$ odd, $b$ even: odd - even + even = even. Not possible.
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[
\left( \frac{a}{b} \right)^5 - a/b + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]

**Case 1:** \( a \) odd, \( b \) odd: odd - odd +odd = even. Not possible.
**Case 2:** \( a \) even, \( b \) odd: even - even +odd = even. Not possible.
**Case 3:** \( a \) odd, \( b \) even: odd - even +even = even. Not possible.
**Case 4:** \( a \) even, \( b \) even: even - even +even = even.
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can't both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[
\left( \frac{a}{b} \right)^5 - \frac{a}{b} + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]

Case 1: \( a \) odd, \( b \) odd: odd - odd + odd = even. Not possible.
Case 2: \( a \) even, \( b \) odd: even - even + odd = even. Not possible.
Case 3: \( a \) odd, \( b \) even: odd - even + even = even. Not possible.
Case 4: \( a \) even, \( b \) even: even - even + even = even. Possible.
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** \( x^5 - x + 1 = 0 \) has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If \( x \) is a solution to \( x^5 - x + 1 = 0 \) and \( x = a/b \) for \( a, b \in \mathbb{Z} \), then both \( a \) and \( b \) are even.

Reduced form \( \frac{a}{b} \): \( a \) and \( b \) can’t both be even! + Lemma \( \implies \) no rational solution.

**Proof of lemma:** Assume a solution of the form \( a/b \).

\[
\left( \frac{a}{b} \right)^5 - \frac{a}{b} + 1 = 0
\]

multiply by \( b^5 \),

\[
a^5 - ab^4 + b^5 = 0
\]

Case 1: \( a \) odd, \( b \) odd: odd - odd +odd = even. Not possible.
Case 2: \( a \) even, \( b \) odd: even - even +odd = even. Not possible.
Case 3: \( a \) odd, \( b \) even: odd - even +even = even. Not possible.
Case 4: \( a \) even, \( b \) even: even - even +even = even. Possible.

The fourth case is the only one possible,
Proof by cases. ("divide-and-conquer" strategy)

**Theorem:** $x^5 - x + 1 = 0$ has no solution in the rationals.

**Proof:** First a lemma...

**Lemma:** If $x$ is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in \mathbb{Z}$, then both $a$ and $b$ are even.

Reduced form $\frac{a}{b}$: $a$ and $b$ can't both be even! + Lemma $\implies$ no rational solution.

**Proof of lemma:** Assume a solution of the form $a/b$.

$$
\left(\frac{a}{b}\right)^5 - a/b + 1 = 0
$$

multiply by $b^5$,

$$
a^5 - ab^4 + b^5 = 0
$$

Case 1: $a$ odd, $b$ odd: odd - odd +odd = even. Not possible.

Case 2: $a$ even, $b$ odd: even - even +odd = even. Not possible.

Case 3: $a$ odd, $b$ even: odd - even +even = even. Not possible.

Case 4: $a$ even, $b$ even: even - even +even = even. Possible.

The fourth case is the only one possible, so the lemma follows.
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational. Let $x = y = \sqrt{2}$.
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^\sqrt{2}$ is rational.
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!
Proof by cases.

**Theorem:** There exist irrational \( x \) and \( y \) such that \( x^y \) is rational.

Let \( x = y = \sqrt{2} \).

Case 1: \( x^y = \sqrt{2} \sqrt{2} \) is rational. Done!

Case 2: \( \sqrt{2} \sqrt{2} \) is irrational.
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.  
Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$. 

Thus, in this case, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., $2$).

One of the cases is true so theorem holds.

Question: Which case holds? 
Don't know!!
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^2$ is rational. Done!

Case 2: $\sqrt{2}^2$ is irrational.

  - New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

  $x^y =$
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$$
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^\sqrt{2}$ is rational. Done!

Case 2: $\sqrt{2}^\sqrt{2}$ is irrational.

- New values: $x = \sqrt{2}^\sqrt{2}$, $y = \sqrt{2}$.

\[
x^y = \left(\sqrt{2}^\sqrt{2}\right)^{\sqrt{2}} = \sqrt{2}^\sqrt{2*\sqrt{2}}
\]
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^\sqrt{2}$ is rational. Done!

Case 2: $\sqrt{2}^\sqrt{2}$ is irrational.

▶ New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

▶

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \times \sqrt{2}} = \sqrt{2}^2 = 2.$$
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.
Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^\sqrt{2}$ is rational. Done!

Case 2: $\sqrt{2}^\sqrt{2}$ is irrational.

▶ New values: $x = \sqrt{2}^\sqrt{2}$, $y = \sqrt{2}$.

$$x^y = \left(\sqrt{2}^\sqrt{2}\right)^\sqrt{2} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2.$$ 

Thus, in this case, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$.

Thus, in this case, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).

One of the cases is true so theorem holds.
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational. 

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

$$
x^y = \left( \sqrt{2}^{\sqrt{2}} \right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2.
$$

Thus, in this case, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).

One of the cases is true so theorem holds. $\square$
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

Thus, in this case, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).

One of the cases is true so theorem holds.

Question: Which case holds?
Proof by cases.

**Theorem:** There exist irrational $x$ and $y$ such that $x^y$ is rational.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

▶ New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

▶

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2.$$ 

Thus, in this case, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).

One of the cases is true so theorem holds.

Question: Which case holds? Don’t know!!!
Be careful.

**Theorem:** $3 = 4$
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. 

Don't assume what you want to prove!
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. 

Dividing one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds.

Don't assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

$$x^2 - xy = x^2 - y^2$$

$$x(x - y) = (x + y)(x - y)$$

$x = (x + y)$

$x = 2$

Dividing by zero is no good.

Also: Multiplying inequalities by a negative. $P \Rightarrow Q$ does not mean $Q \Rightarrow P$. 
Be careful.

**Theorem:** \( 3 = 4 \)

**Proof:** Assume \( 3 = 4 \). Start with \( 12 = 12 \). Divide one side by 3 and the other by 4 to get \( 4 = 3 \).
Be careful.

**Theorem:** \(3 = 4\)

**Proof:** Assume \(3 = 4\). Start with \(12 = 12\). Divide one side by 3 and the other by 4 to get \(4 = 3\). By commutativity
Theorem: 3 = 4

Theorem: $3 = 4$

Theorem: $3 = 4$


Don’t assume what you want to prove!
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:**
Be careful.

**Theorem:** \(3 = 4\)

**Proof:** Assume \(3 = 4\). Start with \(12 = 12\). Divide one side by 3 and the other by 4 to get \(4 = 3\). By commutativity theorem holds. 

Don’t assume what you want to prove!

**Theorem:** \(1 = 2\)

**Proof:** For \(x = y\), we have
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds.

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

$$(x^2 - xy) = x^2 - y^2$$
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

- $(x^2 - xy) = x^2 - y^2$
- $x(x - y) = (x + y)(x - y)$
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

\[
(x^2 - xy) = x^2 - y^2
\]

\[
x(x - y) = (x + y)(x - y)
\]

\[
x = (x + y)
\]
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

$(x^2 - xy) = x^2 - y^2$

$x(x - y) = (x + y)(x - y)$

$x = (x + y)$

$x = 2x$
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds.

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

\begin{align*}
(x^2 - xy) &= x^2 - y^2 \\
x(x - y) &= (x + y)(x - y) \\
x &= (x + y) \\
x &= 2x \\
1 &= 2
\end{align*}
Be careful.

**Theorem:** \(3 = 4\)

**Proof:** Assume \(3 = 4\). Start with \(12 = 12\). Divide one side by 3 and the other by 4 to get \(4 = 3\). By commutativity theorem holds. \(\square\)

Don’t assume what you want to prove!

**Theorem:** \(1 = 2\)

**Proof:** For \(x = y\), we have

\[
\begin{align*}
(x^2 - xy) &= x^2 - y^2 \\
x(x - y) &= (x + y)(x - y) \\
x &= (x + y) \\
x &= 2x \\
1 &= 2
\end{align*}
\]

\(\square\)
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. 

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

\[(x^2 - xy) = x^2 - y^2\]
\[x(x - y) = (x + y)(x - y)\]
\[x = (x + y)\]
\[x = 2x\]

\[1 = 2\]

Dividing by zero is no good.
Be careful.

**Theorem:** \(3 = 4\)

**Proof:** Assume \(3 = 4\). Start with \(12 = 12\). Divide one side by 3 and the other by 4 to get \(4 = 3\). By commutativity theorem holds. \(\square\)

Don’t assume what you want to prove!

**Theorem:** \(1 = 2\)

**Proof:** For \(x = y\), we have

\[
(x^2 - xy) = x^2 - y^2 \\
x(x - y) = (x + y)(x - y) \\
x = (x + y) \\
x = 2x \\
1 = 2
\]

Dividing by zero is no good.

Also: Multiplying inequalities by a negative.
Be careful.

**Theorem:** $3 = 4$

**Proof:** Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. \[\square\]

Don’t assume what you want to prove!

**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have

\[
\begin{align*}
(x^2 - xy) &= x^2 - y^2 \\
x(x - y) &= (x + y)(x - y) \\
x &= (x + y) \\
x &= 2x
\end{align*}
\]

\[x = 2x\]

\[1 = 2\] \[\square\]

Dividing by zero is no good.

Also: Multiplying inequalities by a negative.

$P \implies Q$ does not mean $Q \implies P$. 
Summary

Direct Proof:
To Prove: $P \implies Q$. Assume $P$. reason forward, Prove $Q$. 

By Contraposition:
To Prove: $P \implies Q$. Assume $\neg Q$. Prove $\neg P$.

By Contradiction:

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
Either $\sqrt{2}$ and $\sqrt{2}$ worked.
or $\sqrt{2}$ and $\sqrt{2}$ worked.

Careful when proving!
Don't assume the theorem. Divide by zero. Watch converse. ...
Summary

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). reason forward, Prove \( Q \).

By Contraposition:
To Prove: \( P \implies Q \) Assume \( \neg Q \). Prove \( \neg P \).

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.

Either \( \sqrt{2} \) and \( \sqrt{2} \) worked.
or \( \sqrt{2} \) and \( \sqrt{2} \). 

Careful when proving!
Don't assume the theorem. Divide by zero. Watch converse. ...
Summary

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). reason forward, Prove \( Q \).

By Contraposition:
To Prove: \( P \implies Q \)\, Assume \( \neg Q \). Prove \( \neg P \).

By Contradiction:
To Prove: \( P \)\, Assume \( \neg P \). Prove \text{False} .
Direct Proof:
To Prove: $P \implies Q$. Assume $P$. reason forward, Prove $Q$.

By Contraposition:
To Prove: $P \implies Q$. Assume $\neg Q$. Prove $\neg P$.

By Contradiction:
To Prove: $P$. Assume $\neg P$. Prove $\text{False}$.

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
Either $\sqrt{2}$ and $\sqrt{2}$ worked.
  or $\sqrt{2}$ and $\sqrt{2\sqrt{2}}$ worked.
Summary

Direct Proof:
To Prove: $P \implies Q$. Assume $P$. reason forward, Prove $Q$.

By Contraposition:
To Prove: $P \implies Q$ Assume $\neg Q$. Prove $\neg P$.

By Contradiction:
To Prove: $P$ Assume $\neg P$. Prove False.

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
  Either $\sqrt{2}$ and $\sqrt{2}$ worked.
    or $\sqrt{2}$ and $\sqrt{2} \sqrt{2}$ worked.

Careful when proving!
Don’t assume the theorem. Divide by zero. Watch converse. ...