1. Direct proof
2. by Contraposition
3. by Contradiction
4. by Cases
Quick Background and Notation.

Integers closed under addition.
Quick Background and Notation.

Integers closed under addition.

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

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

\[ a \mid b \text{ means “a divides b”}. \]
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”.

\( 2 \mid 4 \)?
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!
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?
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!
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\( \mid 2 \)?
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!
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: \( a \mid b \iff \exists q \in \mathbb{Z} \) where \( b = aq \).
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!

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

3|15
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 \( q = 5 \),
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 \( q = 5 \), \( 15 = 3(5) \).
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!

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

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

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

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

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

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

\[ b - c = aq - aq' \]
**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 $q, q' \in \mathbb{Z}$

$b - c = aq - aq' = a(q - q')$
**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 $q, q' \in \mathbb{Z}$

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

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

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

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

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

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

\[ a|(b - c) \]

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

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

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

$b - c = aq - aq' = a(q - q')$  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 $a, b, c \in \mathbb{Z}$. 

\[ \square \]
**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:
**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: $P \implies Q$
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

$a \mid (b - c)$

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

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

Direct Proof Form:

Goal: $P \implies Q$

Assume $P$. 

$\blacksquare$
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 $a|c$

$b = aq$ 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 $P$.

... 

Therefore $Q$. 

\[ \square \]
Another direct proof.

Let $D_3$ be the 3 digit natural numbers.
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 $11|n$. 

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.

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

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

$\Rightarrow 11 | n$.

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, then $11|n$. 

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, than $11|n$.

$$\forall n \in D_3, (11|\text{alt. sum of digits of } n) \implies 11|n$$
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, 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:
$n = 121$  Alt Sum: $1 - 2 + 1 = 0$. 

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.

$\implies 11|n$.

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, 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.
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.
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.

$n = 605$
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 $11|n$.

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

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
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 $605 = 11(55)$
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 $605 = 11(55)$
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 $n \in D_3$,
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 $k$.  


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.
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:

$n = 121$  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.

$100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b)$
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 $n$,
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.
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.  $\implies 11 | n$.  $\square$
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.
\[ 100a + 10b + c = 11k + 99a + 11b = 11(k + 9a + b) \]

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:
\begin{align*}
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) \\
\end{align*}

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. $\implies 11|n$. \qed

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

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

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

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

Yes?
The Converse

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

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

Yes? No?
Another Direct Proof.

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

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

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

Proof: Assume 11|n.

\[ n = 100a + 10b + c = 11k \]
Theorem: \( \forall n \in D_3, (11|n) \implies (11|\text{alt. sum of digits of } n) \)

**Proof:** Assume 11|n.

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

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

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

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

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

Proof: Assume \( 11 \mid n \).

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

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

Proof: Assume \( 11 \mid n \).

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

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

Proof: Assume $11|n$.

\[ n = 100a + 10b + c = 11k \implies \]
\[ 99a + 11b + (a - b + c) = 11k \implies \]
\[ a - b + c = 11k - 99a - 11b \implies \]
\[ a - b + c = 11(k - 9a - b) \implies \]
\[ a - b + c = 11\ell \text{ where } \ell = (k - 9a - b) \in Z \]
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|alternating sum of digits.
Another Direct Proof.

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

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

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

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

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

Often works with arithmetic properties ...
Another Direct Proof.

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

Proof: Assume \( 11|n \).

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

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

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

Often works with arithmetic properties ...

...not when multiplying by 0.
Another Direct Proof.

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

Proof: Assume 11|n.

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

That is 11|alternating sum of digits.

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

Often works with arithmetic properties ...

...not 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 \( 11|n \).

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

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

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

Often works with arithmetic properties ...

...not when multiplying by 0.

We have.

Theorem: \( \forall n \in N', (11|\text{alt. sum of digits of } n) \iff (11|n) \)
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 \( P \implies Q \).

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 \mid n \text{ so we have } n = qd = q(2k) = 2(kq) \]

\( n \) is even.\[ \text{\( \neg P \) } \]
Proof by Contraposition

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

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

$n = 2k + 1$
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 $d$?
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?
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 $P \implies Q$. 

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 $P \implies Q$. 
Thm: For $n \in Z^+$ 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 $P \implies Q$.

Assume $\neg Q$
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 \( P \implies Q \).

Assume \( \neg Q \)

...and prove \( \neg P \).
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 $P \iff Q$.
Assume $\neg Q$
...and prove $\neg P$.
Conclusion: $\neg Q \iff \neg P$
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 $P \implies Q$. 
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.
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. \( d = 2k \).
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. $d = 2k$.

d|n so we have
Proof by Contraposition

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

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

What to do?

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

Assume \( \neg Q \)

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

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

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

\( d \mid n \) 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

$n = qd = q(2k) = 2(kq)$
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.
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. $\neg P$
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' ...........
$\neg Q = 'n$ 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 ...
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.

$n = 2k + 1$

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

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

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

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

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

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

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

$n$ is odd

$n = 2k + 1$

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

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

$\neg Q = \implies \neg P$ so $P = \implies Q$ and ...
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.' ............
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'
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' ............
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'
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.
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.

$n = 2k + 1$
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.

$n = 2k + 1$

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + k) + 1.$
Lemma: For every \( n \) in \( \mathbb{N} \), \( n^2 \) 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.

\( n = 2k + 1 \)

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

\( n^2 = 2l + 1 \) where \( l \) is a natural number..
Lemma: For every $n$ in $N$, $n^2$ is even $\Rightarrow$ $n$ is even. ($P \Rightarrow Q$)

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

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

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

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

$n = 2k + 1$

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

$n^2 = 2l + 1$ 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.' $\quad \neg P = 'n^2$ is odd' $\quad Q = 'n$ is even.' $\quad \neg Q = 'n$ is odd'

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

$n = 2k + 1$

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

$n^2 = 2l + 1$ 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 $\Rightarrow$ $n$ is even. ($P \Rightarrow Q$)

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

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

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

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

$n = 2k + 1$

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

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

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

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

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

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

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

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

\( n = 2k + 1 \)

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

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

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

\( \neg Q \implies \neg P \) so \( P \implies Q \) and ...
Theorem: $\sqrt{2}$ is irrational.
Theorem: $\sqrt{2}$ is irrational.

Must show:
Proof by contradiction: form

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

Must show: For every $a, b \in \mathbb{Z}$,
**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.
Proof by contradiction: \textbf{form}

\textbf{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: form

**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**: $P$. 

Proof by contradiction: form

**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:** $P$.

$\neg P$
Proof by contradiction: form

**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**: $P$.

$\neg P \implies P_1$
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: $P$.

$\neg P \implies P_1 \ldots$
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 $a, b \in \mathbb{Z}$, $(\frac{a}{b})^2 \neq 2$.

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

Proof by contradiction:

Theorem: $P$.

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

$\neg P$
Proof by contradiction: form

**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:** \( P \).

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

\[ \neg P \implies Q_1 \]
**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:** \( P \).

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

\[ \neg P \implies Q_1 \cdots \]
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: $P$.

$\neg P \implies P_1 \ldots \implies R$

$\neg P \implies Q_1 \ldots \implies \neg R$
**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:** $P$. 

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

$$\neg P \implies Q_1 \cdots \implies \neg R$$

$$\neg P \implies R \land \neg R$$
**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**: $P$.

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

$\neg P \implies Q_1 \cdots \implies \neg R$

$\neg P \implies R \land \neg R \equiv \text{False}$
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: $P$.

$\neg P \implies P_1 \ldots \implies R$

$\neg P \implies Q_1 \ldots \implies \neg R$

$\neg P \implies R \land \neg R \equiv \text{False}$

Contrapositive: $\text{True} \implies P$. 
**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:** $P$.

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

\[ \neg P \implies Q_1 \cdots \implies \neg R \]

\[ \neg P \implies R \land \neg R \equiv \text{False} \]

Contrapositive: True $\implies P$. Theorem $P$ is proven.
Proof by contradiction: form

**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:** $P$.

$\neg P \implies P_1 \ldots \implies R$

$\neg P \implies Q_1 \ldots \implies \neg R$

$\neg P \implies R \land \neg R \equiv \text{False}$

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

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

Assume $\neg P$:

\[ \sqrt{2} = \frac{a}{b} \text{ for } a, b \in \mathbb{Z}. \]

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

\[ \sqrt{2}b = a^2 b^2 = 4k^2 \]

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

Let $a = 2k$ 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 $a, b \in \mathbb{Z}$.
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 \( k \)
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 $k$
**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 $k$

$$b^2 = 2k^2$$
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.
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.
Theorem: \( \sqrt{2} \) is irrational.

Assume \( \neg P: \sqrt{2} = \frac{a}{b} \) 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 \( \implies \) \( a \) 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.
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 \( x = p_1 \cdot p_2 \cdot \cdots \cdot p_k \) and \( q \), and divides \( q - x \), \( \Rightarrow \) \( p \) \( | q - x \) \( \Rightarrow \) \( p \leq q - x = 1 \).
• 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 $q = (p_1 \times p_2 \times \cdots \times p_k) + 1$.
- $q$ cannot be one of the primes as it is larger than any $p_i$.
- $q$ has prime divisor $p (\text{"> 1" = R})$ which is one of $p_i$.
- $p$ divides both $x = p_1 \cdot p_2 \cdots p_k$ and $q$, and divides $q - x \Rightarrow p | q - x \Rightarrow p \leq q - x = 1$.
- 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: \( p_1, \ldots, p_k \).
**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 \( p_i \).

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 \( p \) ("\( p > 1 \) = \( \mathbb{R} \)") which is one of \( p_i \).
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 $q$,
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 $x = p_1 \cdot p_2 \cdots p_k$ 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
  \[ q = (p_1 \times p_2 \times \cdots p_k) + 1. \]

• \( q \) 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 \( q - x \),
• \( \implies p | q - x \)
**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 $q - x$.
- $\implies p | q - x \implies p \leq q - x = 1$. 

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 \( q - x \),
  - \( \implies p \mid q - x \implies p \leq q - x = 1. \)
  - so \( p \leq 1. \)
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 $q - x$,
  $$p | q - x \implies p \leq q - x = 1.$$
- so $p \leq 1$. (**Contradicts R.**)
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 $q - x$,
  - $p | q - x \implies p \leq q - x = 1$.
  - so $p \leq 1$. (Contradicts $R$.)

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

- “The product of the first $k$ primes plus 1 is prime.”
- No.
- The chain of reasoning started with a false statement.
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..
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 $in between$ 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 \textit{in between} 13 and $q = 30031$ that divides $q$.
- Proof assumed no primes \textit{in between} $p_k$ and $q$. 
Proof by cases.

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

**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 $x = a \div b$ for $a$, $b \in \mathbb{Z}$, then both $a$ and $b$ are even.

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

**Proof of lemma:** Assume a solution of the form $a \div b$. 

\[
(a \div b)^5 - a \div b + 1 = 0 \quad \text{(Multiply by $b^5$)}
\]

**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.
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.
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!
**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.

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. \( \square \)
Proof by cases.

**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 $a/b$. 

\[ \square \]
Proof by cases.

**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. $\square$

**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.

**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.

**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.
**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 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.
Proof by cases.

**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.
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 \(b^5\),

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

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.

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. \( \square \)

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 \( b^5 \),

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

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.
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 $\frac{a}{b}$.

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

Multiply by $b^5$,

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

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.

**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

\[ \implies \text{no rational solution.} \]

**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 \( b^5 \),

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

**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.

**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.

**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. \[\square\]

**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.

**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 \( \frac{a}{b} \).

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

Multiply by \( b^5 \),

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

**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.

Let $x = y = \sqrt{2}$.

Case 1: $x^y = \sqrt{2} \cdot \sqrt{2}$ is rational. Done!

Case 2: $\sqrt{2} \cdot \sqrt{2}$ is irrational.

- New values: $x = \sqrt{2} \cdot \sqrt{2}, y = \sqrt{2}$.
- $x^y = (\sqrt{2} \cdot \sqrt{2}) \cdot \sqrt{2} = \sqrt{2} \cdot 2 \cdot \sqrt{2} = 2 \cdot 2 = 4$.

Thus, 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 $x = y = \sqrt{2}$.
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.
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!
**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.
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: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$. 
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 = $
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: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
- $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$

Thus, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).

One of the cases is true so the 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: $x^y = \sqrt{2}^{\sqrt{2}}$ is rational. Done!

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

- New values: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}}$$
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: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.
  •

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2$$

Thus, 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: \( x^y = \sqrt{2}^{\sqrt{2}} \) 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, we have irrational \( x \) and \( y \) with a rational \( x^y \) (i.e., 2).

One of the cases is true so the 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: $x^y = \sqrt{2}^{\sqrt{2}}$ 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, 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, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).

One of the cases is true so theorem holds.
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, we have irrational $x$ and $y$ with a rational $x^y$ (i.e., 2).

One of the cases is true so theorem holds. \qed
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, 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?
**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: $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$.

  \[
  x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \times \sqrt{2}} = \sqrt{2}^2 = 2.
  \]

Thus, 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:** $3 = 4$

*Proof:* Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity, the theorem holds. Don't assume what you want to prove!
Theorem: 3 = 4

Proof: Assume 3 = 4.
Be careful.

Theorem: \(3 = 4\)

Proof: Assume \(3 = 4\).

Start with \(12 = 12\).
Theorem: $3 = 4$

Proof: Assume $3 = 4$.

Start with $12 = 12$.

Divide one side by 3 and the other by 4 to get $4 = 3$. 
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

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.
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.
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!
Be really careful!

**Theorem:** $1 = 2$

**Proof:**
**Theorem:** $1 = 2$

**Proof:** For $x = y$, we have
Theorem: $1 = 2$
Proof: For $x = y$, we have

$$(x^2 - xy) = x^2 - y^2$$
Theorem: $1 = 2$
Proof: For $x = y$, we have
\[
(x^2 - xy) = x^2 - y^2
\]
\[
x(x - y) = (x + y)(x - y)
\]
Theorem: $1 = 2$

Proof: For $x = y$, we have

\[(x^2 - xy) = x^2 - y^2\]
\[x(x - y) = (x + y)(x - y)\]
\[x = (x + y)\]
Theorem: $1 = 2$
Proof: For $x = y$, we have

\[(x^2 - xy) = x^2 - y^2\]
\[x(x - y) = (x + y)(x - y)\]
\[x = (x + y)\]
\[x = 2x\]

Dividing by zero is no good.
Also: Multiplying inequalities by a negative.
$P \Rightarrow Q$ does not mean $Q \Rightarrow P$. 
Theorem: $1 = 2$

Proof: For $x = y$, we have

\[
(x^2 - xy) = x^2 - y^2
\]
\[
x(x - y) = (x + y)(x - y)
\]
\[
x = (x + y)
\]
\[
x = 2x
\]
\[
1 = 2
\]
Theorem: $1 = 2$

Proof: For $x = y$, we have

\[
(x^2 - xy) = x^2 - y^2
\]
\[
x(x - y) = (x + y)(x - y)
\]
\[
x = (x + y)
\]
\[
x = 2x
\]

$1 = 2$
Be really careful!

**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 really careful!

**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.
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.

$P \implies Q$ does not mean $Q \implies P$. 
Summary: Note 2.

Direct Proof:

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

Assume \( P \).

Prove \( Q \).

By Contraposition:

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

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 \( \sqrt{2} \) worked.

Careful when proving!

Don't assume the theorem.

Divide by zero.

Watch converse.

...
Direct Proof:
To Prove: $P \Rightarrow Q$. 
Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \).
Direct Proof:
To Prove: $P \implies Q$. Assume $P$. 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: Note 2.

Direct Proof:
To Prove: $P \implies Q$. Assume $P$. Prove $Q$.

By Contraposition:

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: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). Prove \( Q \).

By Contraposition:
To Prove: \( P \implies Q \)

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 \( \sqrt{2} \) worked.

Careful when proving!
Don't assume the theorem.
Divide by zero.
Watch converse.

...
Summary: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). Prove \( Q \).

By Contraposition:
To Prove: \( P \implies Q \). Assume \( \neg Q \).

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 \( \sqrt{2} \).}

Careful when proving!
Don't assume the theorem.
Divide by zero.
Watch converse.
...
Summary: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). 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 \( \sqrt{2} \) worked.

Careful when proving!
Don't assume the theorem.
Divide by zero.
Watch converse.
...
Direct Proof:
   To Prove: $P \implies Q$. Assume $P$. Prove $Q$.

By Contraposition:
   To Prove: $P \implies Q$ Assume $\neg Q$. Prove $\neg P$.

By Contradiction:
Summary: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). Prove \( Q \).

By Contraposition:
To Prove: \( P \implies Q \). Assume \( \neg Q \). Prove \( \neg P \).

By Contradiction:
To Prove: \( P \)

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: Note 2.

Direct Proof:
To Prove: $P \implies Q$. Assume $P$. Prove $Q$.

By Contraposition:
To Prove: $P \implies Q$ Assume $\neg Q$. Prove $\neg P$.

By Contradiction:
To Prove: $P$ Assume $\neg P$. 

17
Direct Proof:
To Prove: $P \implies Q$. Assume $P$. 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.
Summary: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). 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.

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.
Direct Proof:
   To Prove: $P \implies Q$. Assume $P$. 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.
Direct Proof:
To Prove: $P \implies Q$. Assume $P$. 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.
Summary: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). Prove \( Q \).

By Contraposition:
To Prove: \( P \implies Q \) Assume \( \neg Q \). Prove \( \neg P \).

By Contradiction:
To Prove: \( P \) Assume \( \neg P \). Prove \textbf{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.

Careful when proving!
Don't assume the theorem.
Divide by zero.
Watch converse.
...
Summary: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). 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.
Summary: Note 2.

Direct Proof:
To Prove: \( P \implies Q \). Assume \( P \). 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.
Direct Proof:
To Prove: $P \implies Q$. Assume $P$. 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!
Direct Proof:
To Prove: $ P \implies Q $. Assume $ P $. 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.
Summary: Note 2.

Direct Proof:
To Prove: $P \implies Q$. Assume $P$. 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 $\sqrt{2^2}$ worked.

Careful when proving!
Don’t assume the theorem. Divide by zero.
Direct Proof:
To Prove: $P \implies Q$. Assume $P$. 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.
Summary: Note 2.

Direct Proof:
To Prove: $P \implies Q$. Assume $P$. 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 $\sqrt{2}^2$ worked.

Careful when proving!
Don’t assume the theorem. Divide by zero. Watch converse. ...
1. The natural numbers.
2. 5 year old Gauss.
3. ..and Induction.
4. Simple Proof.
The naturals.
The naturals.
The naturals.
The naturals.
The naturals.

0, 1, 2, ...

0, 1, 2, 3,
The naturals.

0, 1, 2, 3,
The naturals.

0, 1, 2, 3, ...

\[0, 1, 2, 3, \ldots\]
The naturals.

0, 1, 2, 3, ..., n,
The naturals.

0, 1, 2, 3, ..., n, n+1,
The naturals.

\[ 0, 1, 2, 3, \ldots, n, n+1, n+2, n+3, \]
The naturals.

0, 1, 2, 3, …, n, n+1, n+2, n+3, …
A formula.

Teacher: Hello class.

Teacher: Please add the numbers from 1 to 100.

Gauss: It's \( \left( \frac{100}{2} \right) \times 101 \) or 5050!
Teacher: Hello class.
Teacher: Hello class.
Teacher:

A formula.

Please add the numbers from 1 to 100.

Gauss: \((100)(101)\) or 5050!
Teacher: Hello class.
Teacher: Please add the numbers from 1 to 100.
Teacher: Hello class.
Teacher: Please add the numbers from 1 to 100.

Gauss: It’s
Teacher: Hello class.
Teacher: Please add the numbers from 1 to 100.

Gauss: It’s \( \frac{(100)(101)}{2} \)
Teacher: Hello class.
Teacher: Please add the numbers from 1 to 100.

Gauss: It’s \( \frac{(100)(101)}{2} \) or 5050!
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\)
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\).

\(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k+1\)?

\(\sum_{k+1}^{k+1} i = \frac{k(k+1)}{2} + k+1 = \frac{(k+1)(k+2)}{2}\).

How about \(k+2\).

Same argument starting at \(k+1\) works!

Induction Step. \(P(k) = \Rightarrow P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{0}^{0} i = 0 = \frac{(0)(0+1)}{2}\) Base Case.

Statement is true for \(n = 0\) \(P(0)\) is true plus inductive step = \(\Rightarrow\) true for \(n = 1\) \((P(0) \land (P(0) = \Rightarrow P(1))) = \Rightarrow P(1)\) plus inductive step = \(\Rightarrow\) true for \(n = 2\) \((P(1) \land (P(1) = \Rightarrow P(2))) = \Rightarrow P(2)\)...

...true for \(n = k\) = \(\Rightarrow\) true for \(n = k+1\) \((P(k) \land (P(k) = \Rightarrow P(k+1))) = \Rightarrow P(k+1)\)...

Predicate, \(P(n)\), True for all natural numbers! Proof by Induction.
Child Gauss: \((\forall n \in \mathbb{N}) (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\).
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i\]
Child Gauss: $(\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$ Proof?

Idea: assume predicate $P(n)$ for $n = k$. $P(k)$ is $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$.

Is predicate, $P(n)$ true for $n = k + 1$?

$$\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1)$$
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1
\]
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\begin{align*}
\sum_{i=1}^{k+1} i &= (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\end{align*}
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i)+ (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\).
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!
Child Gauss: \( (\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2}) \) Proof?

Idea: assume predicate \( P(n) \) for \( n = k \). \( P(k) \) is \( \sum_{i=1}^{k} i = \frac{k(k+1)}{2} \).

Is predicate, \( P(n) \) true for \( n = k + 1 \)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \( k + 2 \). Same argument starting at \( k + 1 \) works!

**Induction Step.**
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof?
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere.
Child Gauss: \((\forall n \in \mathbb{N}) \left( \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \right)\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\)
Gauss and Induction

Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) Base Case.
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) Base Case.

Statement is true for \(n = 0\)
Child Gauss: \((\forall n \in \mathbb{N}) (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\)  

*Base Case.*

Statement is true for \(n = 0\) \(P(0)\) is true.
Gauss and Induction

Child Gauss: \((\forall n \in \mathbb{N}) (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true

plus inductive step
Child Gauss: \( (\forall n \in \mathbb{N}) (\sum_{i=1}^{n} i = \frac{n(n+1)}{2}) \) Proof?

Idea: assume predicate \( P(n) \) for \( n = k \). \( P(k) \) is \( \sum_{i=1}^{k} i = \frac{k(k+1)}{2} \).

Is predicate, \( P(n) \) true for \( n = k + 1 \)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \( k + 2 \). Same argument starting at \( k + 1 \) works!

**Induction Step.** \( P(k) \implies P(k + 1) \).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \( P(0) \) is \( \sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2} \) **Base Case.**

Statement is true for \( n = 0 \) \( P(0) \) is true

plus inductive step \( \implies \) true for \( n = 1 \)
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true

plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \wedge (P(0) \implies P(1))) \implies P(1)\)
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true

\begin{align*}
\text{plus inductive step} & \implies \text{true for } n = 1 \ (P(0) \land (P(0) \implies P(1))) \implies P(1) \\
\text{plus inductive step} & \implies \text{true for } n = 2 \\
\text{...} & \implies \text{true for } n = k \\
& \implies \text{true for } n = k + 1
\end{align*}
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = \left(\sum_{i=1}^{k} i\right) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true
  plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)
  plus inductive step \(\implies\) true for \(n = 2\)
Child Gauss: \( \forall n \in \mathbb{N} (\sum_{i=1}^{n} i = \frac{n(n+1)}{2}) \) Proof?

Idea: assume predicate \( P(n) \) for \( n = k \). \( P(k) \) is \( \sum_{i=1}^{k} i = \frac{k(k+1)}{2} \).

Is predicate, \( P(n) \) true for \( n = k + 1 \)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \( k + 2 \). Same argument starting at \( k + 1 \) works!

**Induction Step.** \( P(k) \implies P(k+1) \).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \( P(0) \) is \( \sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2} \) **Base Case.**

Statement is true for \( n = 0 \) \( P(0) \) is true

plus inductive step \( \implies \) true for \( n = 1 \) \( (P(0) \land (P(0) \implies P(1))) \implies P(1) \)

plus inductive step \( \implies \) true for \( n = 2 \) \( (P(1) \land (P(1) \implies P(2))) \implies P(2) \)
Gauss and Induction

Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true

plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)

plus inductive step \(\implies\) true for \(n = 2\) \((P(1) \land (P(1) \implies P(2))) \implies P(2)\)

...
Child Gauss: $\forall n \in \mathbb{N} (\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$ Proof?

Idea: assume predicate $P(n)$ for $n = k$. $P(k)$ is $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$.

Is predicate, $P(n)$ true for $n = k + 1$?

$$\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.$$  

How about $k + 2$. Same argument starting at $k + 1$ works!

**Induction Step.** $P(k) \implies P(k + 1)$.

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. $P(0)$ is $\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}$ **Base Case.**

Statement is true for $n = 0$ $P(0)$ is true
  plus inductive step $\implies$ true for $n = 1$ $(P(0) \land (P(0) \implies P(1))) \implies P(1)$  
  plus inductive step $\implies$ true for $n = 2$ $(P(1) \land (P(1) \implies P(2))) \implies P(2)$  
  ...  
  true for $n = k$
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true  
plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)  
plus inductive step \(\implies\) true for \(n = 2\) \((P(1) \land (P(1) \implies P(2))) \implies P(2)\)  
\[\ldots\]  
true for \(n = k\) \(\implies\) true for \(n = k + 1\)
Child Gauss: $(\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})$ Proof?

Idea: assume predicate $P(n)$ for $n = k$. $P(k)$ is $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$.

Is predicate, $P(n)$ true for $n = k + 1$?

$$\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.$$  

How about $k + 2$. Same argument starting at $k + 1$ works!  

**Induction Step.** $P(k) \implies P(k + 1)$.

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. $P(0)$ is $\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}$  

**Base Case.**

Statement is true for $n = 0$ $P(0)$ is true  
plus inductive step $\implies$ true for $n = 1$ $(P(0) \land (P(0) \implies P(1))) \implies P(1)$  
plus inductive step $\implies$ true for $n = 2$ $(P(1) \land (P(1) \implies P(2))) \implies P(2)$  

...  

true for $n = k$ $\implies$ true for $n = k + 1$ $(P(k) \land (P(k) \implies P(k + 1))) \implies P(k + 1)$
Gauss and Induction

Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) Base Case.

Statement is true for \(n = 0\) \(P(0)\) is true

plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)

plus inductive step \(\implies\) true for \(n = 2\) \((P(1) \land (P(1) \implies P(2))) \implies P(2)\)

\[
\vdots
\]

true for \(n = k\) \(\implies\) true for \(n = k + 1\) \((P(k) \land (P(k) \implies P(k + 1))) \implies P(k + 1)\)

\[
\vdots
\]
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k+1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true

plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)

plus inductive step \(\implies\) true for \(n = 2\) \((P(1) \land (P(1) \implies P(2))) \implies P(2)\)

\[
\vdots
\]

true for \(n = k \implies\) true for \(n = k + 1\) \((P(k) \land (P(k) \implies P(k+1))) \implies P(k+1)\)

\[
\vdots
\]
Gauss and Induction

Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true
    plus inductive step \(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)
        plus inductive step \(\implies\) true for \(n = 2\) \((P(1) \land (P(1) \implies P(2))) \implies P(2)\)
            \ldots
                true for \(n = k\) \(\implies\) true for \(n = k + 1\) \((P(k) \land (P(k) \implies P(k + 1))) \implies P(k + 1)\)
            \ldots

Predicate, \(P(n)\), True for all natural numbers!
Child Gauss: \((\forall n \in \mathbb{N})(\sum_{i=1}^{n} i = \frac{n(n+1)}{2})\) Proof?

Idea: assume predicate \(P(n)\) for \(n = k\). \(P(k)\) is \(\sum_{i=1}^{k} i = \frac{k(k+1)}{2}\).

Is predicate, \(P(n)\) true for \(n = k + 1\)?

\[
\sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k + 1) = \frac{k(k+1)}{2} + k + 1 = \frac{(k+1)(k+2)}{2}.
\]

How about \(k + 2\). Same argument starting at \(k + 1\) works!

**Induction Step.** \(P(k) \implies P(k + 1)\).

Is this a proof? It shows that we can always move to the next step.

Need to start somewhere. \(P(0)\) is \(\sum_{i=0}^{0} i = 1 = \frac{(0)(0+1)}{2}\) **Base Case.**

Statement is true for \(n = 0\) \(P(0)\) is true

\(\implies\) true for \(n = 1\) \((P(0) \land (P(0) \implies P(1))) \implies P(1)\)

\(\implies\) true for \(n = 2\) \((P(1) \land (P(1) \implies P(2))) \implies P(2)\)

\[\ldots\]

\(\implies\) true for \(n = k\) \((P(k) \land (P(k) \implies P(k + 1))) \implies P(k + 1)\)

\[\ldots\]

Predicate, \(P(n)\), **True** for all natural numbers! **Proof by Induction.**