CS70: Lecture 2. Outline.

Today: Proofs!!!

1. By Example (or Counterexample).
2. Direct. (Prove $P \implies Q$.)
3. by Contraposition (Prove $P \implies Q$)
4. by Contradiction (Prove P.)
5. by Cases

Quick Background and Notation.

Integers closed under addition.

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

$a|b$ means “a divides b”.

Quick Background and Notation.

Integers closed under addition.

$$a, b \in Z \implies a + b \in Z$$

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

$2|4$?

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

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

$2|4$? Yes!

Quick Background and Notation.

Integers closed under addition.

$$a, b \in Z \implies a + b \in Z$$

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

$2|4$? Yes!

$7|23$?

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

$a|b$ means “a divides b”.

$2|4$? Yes!

$7|23$? No!

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

$a|b$ means “a divides b”.

$2|4$? Yes!

$7|23$? No!

$4|2$?

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

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

$2|4$? Yes!

$7|23$? No!

$4|2$? No!

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

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

$2|4$? Yes!

$7|23$? No!

$4|2$? No!

Formally: $a|b \iff \exists q \in Z$ where $b = aq$.

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

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

$2|4$? Yes!

$7|23$? No!

$4|2$? No!

Formally: $a|b \iff \exists q \in Z$ where $b = aq$.

$3|15$

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

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

$2|4$? Yes!

$7|23$? No!

$4|2$? No!

Formally: $a|b \iff \exists q \in Z$ where $b = aq$.

$3|15$ since for $q = 5$,

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

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

2|4? Yes!

7|23? No!

4|2? No!

Formally: $a|b \iff \exists q \in Z$ where $b = aq$.

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

Quick Background and Notation.

Integers closed under addition.

$a, b \in Z \implies a + b \in Z$

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

$2|4$? Yes!

$7|23$? No!

$4|2$? No!

Formally: $a|b \iff \exists q \in Z$ 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.

Direct Proof (Forward Reasoning).

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

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

Direct Proof (Forward Reasoning).

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

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

$b = aq$

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

Direct Proof (Forward Reasoning).

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

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

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

$b - c = aq - aq'$

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

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

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

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

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

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

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

Direct Proof (Forward Reasoning).

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

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

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

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

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

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

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

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

$a|(b - c)$

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

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

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

$a|(b - c)$ □

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q,q' \in Z$

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

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

$a|(b - c)$ $\square$

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

Direct Proof (Forward Reasoning).

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

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

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

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

Direct Proof (Forward Reasoning).

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

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

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

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

Direct Proof Form:

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

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

Direct Proof Form:
Goal: $P \implies Q$

Direct Proof (Forward Reasoning).

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

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

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

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

Direct Proof Form:

Goal: $P \implies Q$

Assume P.

Direct Proof (Forward Reasoning).

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

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

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

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

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

$a|(b-c)$ $\square$

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

Argument applies to *every* $a, b, c \in Z$.

Direct Proof Form:

Goal: $P \implies Q$

Assume P.

$\ldots$

Direct Proof (Forward Reasoning).

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

Proof: Assume $a|b$ and $a|c$
$b = aq$ and $c = aq'$ where $q, q' \in Z$

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

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

$a|(b - c)$ $\square$

Works for $\forall a, b, c$?
Argument applies to *every* $a, b, c \in Z$.

Direct Proof Form:
Goal: $P \implies Q$
Assume P.
...
Therefore Q.

Another direct proof.

Let D_3 be the 3 digit natural numbers.

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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, than $11|n$.

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

Examples:
$n = 121$ Alt Sum: $1 - 2 + 1 = 0$.

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.

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.

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.

$n = 605$

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: $6 - 0 + 5 = 11$

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, than $11|n$.

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

Examples:

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

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

Proof: For $n \in D_3$,

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

Assume: Alt. sum:

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

Assume: Alt. sum: $a - b + c$

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

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

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

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:
$n = 121$ 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,

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

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

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

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

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

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

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

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

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

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

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

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

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

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

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

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

□

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

Examples:

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

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

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

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

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

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

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

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

Another direct proof.

Let D_3 be the 3 digit natural numbers.

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

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

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

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

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

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

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

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

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

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

The Converse

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

The Converse

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

Is converse a theorem?

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

The Converse

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

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

Example: $n = 264$.

The Converse

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

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

Example: $n = 264$. $11|n$?

The Converse

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

Is converse a theorem?

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

Example: $n = 264$. $11 | n$? $11 | 2 - 6 + 4$?

Another Direct Proof.

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

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

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

Another Direct Proof.

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

$n = 100a + 10b + c = 11k \implies$
$99a + 11b + (a - b + c) = 11k$

Another Direct Proof.

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

Proof: Assume $11|n$.

$$
\begin{aligned}
n = 100a + 10b + c = 11k &\implies \\
99a + 11b + (a - b + c) = 11k &\implies \\
a - b + c = 11k - 99a - 11b &
\end{aligned}
$$

Another Direct Proof.

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

Proof: Assume $11|n$.

$$n = 100a + 10b + c = 11k \implies$$
$$99a + 11b + (a - b + c) = 11k \implies$$
$$a - b + c = 11k - 99a - 11b \implies$$
$$a - b + c = 11(k - 9a - b)$$

Another Direct Proof.

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

$$n = 100a + 10b + c = 11k \implies$$
$$99a + 11b + (a - b + c) = 11k \implies$$
$$a - b + c = 11k - 99a - 11b \implies$$
$$a - b + c = 11(k - 9a - b) \implies$$
$$a - b + c = 11\ell$$

Another Direct Proof.

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

Proof: Assume $11|n$.

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

Another Direct Proof.

Theorem: $\forall n \in D_3, (11|n) \implies$ (11|alt. sum of digits of n)
Proof: Assume $11|n$.

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

That is 11|alternating sum of digits. □

Another Direct Proof.

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

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

That is $11|$alternating sum of digits. □

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

Another Direct Proof.

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

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

That is 11|alternating sum of digits. □

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

Often works with arithmetic properties except when multiplying by 0.

Another Direct Proof.

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

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

That is $11|$alternating sum of digits. □

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

Often works with arithmetic properties except when multiplying by 0.

We have.

Another Direct Proof.

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

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

That is $11|$alternating sum of digits. □

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

Often works with arithmetic properties except 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

Proof by Contraposition

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

Proof by Contraposition

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

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

What to do?

Proof by Contraposition

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

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

What to do?

Goal: Prove $P \implies Q$.

Proof by Contraposition

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

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

What to do?

Goal: Prove $P \implies Q$.

Proof by Contraposition

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

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

What to do?

Goal: Prove $P \implies Q$.

Assume $\neg Q$

Proof by Contraposition

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

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

What to do?

Goal: Prove $P \implies Q$.

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

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: $\neg Q \implies \neg P$

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 by Contraposition

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

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

What to do?

Goal: Prove $P \implies Q$.

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

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

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

Proof by Contraposition

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

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

What to do?

Goal: Prove $P \implies Q$.

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

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

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

$d|n$ so we have

$n = qd$

Proof by Contraposition

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

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

What to do?

Goal: Prove $P \implies Q$.

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

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

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

$d|n$ so we have

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

Proof by Contraposition

Thm: For $n \in Z^+$ 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.

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

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

n is even. $\neg P$ $\square$

Another Contrapostion...

Another Contrapostion...

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

Another Contrapostion...

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

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

Another Contrapostion...

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

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

Another Contrapostion...

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

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

Another Contrapostion...

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

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

$P =$ 'n^2 is even.' ....

Another Contrapostion...

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

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

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

Another Contrapostion...

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

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

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

$Q =$ 'n is even' ....

Another Contrapostion...

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

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

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

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

Another Contrapostion...

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

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

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

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

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

Another Contrapostion...

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

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

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

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

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

$n = 2k + 1$

Another Contrapostion...

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

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

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

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

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

$n = 2k + 1$

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

Another Contrapostion...

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

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

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

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

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

$n = 2k + 1$

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

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

Another Contrapostion...

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

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

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

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

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

$n = 2k + 1$

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

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

... and n^2 is odd!

Another Contrapostion...

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

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

$P =$ '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.

$n = 2k + 1$

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

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

... and n^2 is odd!

$\neg Q \implies \neg P$

Another Contrapostion...

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

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

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

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

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

$n = 2k + 1$

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

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

... and n^2 is odd!

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

Another Contrapostion...

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

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

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

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

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

$n = 2k + 1$

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

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

... and n^2 is odd!

$\neg Q \implies \neg P$ so $P \implies Q$ and ... $\square$

Proof by Contradiction

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

Proof by Contradiction

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

Must show:

Proof by Contradiction

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

Must show: For every $a, b \in Z$,

Proof by Contradiction

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

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

Proof by Contradiction

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

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

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

Proof by Contradiction

Theorem: $\sqrt{2}$ 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:

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

Proof by Contradiction

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

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

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

Proof by contradiction:

Theorem: P.

$\neg P$

Proof by Contradiction

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

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

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

Proof by contradiction:

Theorem: P.

$\neg P \implies P_1$

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

$\neg P \implies P_1 \cdots$

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

$\neg P$

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

$\neg P \implies P_1$

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

$\neg P \implies P_1 \cdots$

Proof by Contradiction

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

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

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

Proof by contradiction:

Theorem: P.

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

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

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

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

$\neg P \implies$ False

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

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

$\neg P \implies$ False

Contrapositive: True $\implies P$.

Proof by Contradiction

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

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

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

Proof by contradiction:

Theorem: P.

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

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

$\neg P \implies$ False

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

Proof by Contradiction

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

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

A simple property (equality) should always "not" hold.

Proof by contradiction:

Theorem: P.

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

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

$\neg P \implies$ False

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

Contradiction

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

Contradiction

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

Assume $\neg P$:

Contradiction

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

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

Contradiction

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

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

Reduced form: a and b have no common factors.

Contradiction

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

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

Reduced form: a and b have no common factors.

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

Contradiction

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

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

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

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

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

Contradiction

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

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

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.

Contradiction

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

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

Reduced form: a and b have no common factors.

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

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

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

$a = 2k$ for some integer k

Contradiction

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

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

Reduced form: a and b have no common factors.

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

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

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

$a = 2k$ for some integer k

Contradiction

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

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

Reduced form: a and b have no common factors.

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

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

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

$a = 2k$ for some integer k

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

Contradiction

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

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

Reduced form: a and b have no common factors.

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

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

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

$a = 2k$ for some integer k

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

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

Contradiction

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

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

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.

Contradiction

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

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

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 by contradiction: example

Theorem: There are infinitely many primes.

Proof:

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

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

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

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

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

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

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

The original assumption that "the theorem is false" is false, thus the theorem is proven.

Proof by contradiction: example

Theorem: There are infinitely many primes.

Proof:

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

The original assumption that "the theorem is false" is false, thus the theorem is proven. □

Product of first k primes..

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.

Product of first k primes..

Did we prove?

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

Product of first k primes..

Did we prove?

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

Consider example..

Product of first k primes..

Did we prove?

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

Consider example..

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

Product of first k primes..

Did we prove?

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

Consider example..

- $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$
- There is a prime *in between* 13 and $q = 30031$ that divides q.

Product of first k primes..

Did we prove?

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

Consider example..

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

Proof by cases. (“divide-and-conquer” strategy)

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

Proof by cases. ("divide-and-conquer" strategy)

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

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

Proof by cases. (“divide-and-conquer” strategy)

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

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

Reduced form $\frac{a}{b}$: a and b can't both be even!

Proof by cases. (“divide-and-conquer” strategy)

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

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

Reduced form $\frac{a}{b}$: a and b can't both be even! + Lemma

Proof by cases. ("divide-and-conquer" strategy)

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

Proof: First a lemma...
Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, *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 by cases. ("divide-and-conquer" strategy)

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

Proof: First a lemma...
Lemma: If x is a solution to $x^5 - x + 1 = 0$ and $x = a/b$ for $a, b \in Z$, *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.

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd: odd - odd +odd = even.

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

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

Proof by cases. (“divide-and-conquer” strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd: odd - odd +odd = even. Not possible.
Case 2: a even, b odd: even - even +odd = even.

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd: odd - odd +odd = even. Not possible.
Case 2: a even, b odd: even - even +odd = even. Not possible.

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: *a* odd, *b* odd: odd - odd +odd = even. Not possible.
Case 2: *a* even, *b* odd: even - even +odd = even. Not possible.
Case 3: *a* odd, *b* even: odd - even +even = even.

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd: odd - odd +odd = even. Not possible.
Case 2: a even, b odd: even - even +odd = even. Not possible.
Case 3: a odd, b even: odd - even +even = even. Not possible.

Proof by cases. (“divide-and-conquer” strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: *a* odd, *b* odd: odd - odd +odd = even. Not possible.
Case 2: *a* even, *b* odd: even - even +odd = even. Not possible.
Case 3: *a* odd, *b* even: odd - even +even = even. Not possible.
Case 4: *a* even, *b* even: even - even +even = even.

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd: odd - odd +odd = even. Not possible.
Case 2: a even, b odd: even - even +odd = even. Not possible.
Case 3: a odd, b even: odd - even +even = even. Not possible.
Case 4: a even, b even: even - even +even = even. Possible.

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: a odd, b odd: odd - odd +odd = even. Not possible.
Case 2: a even, b odd: even - even +odd = even. Not possible.
Case 3: a odd, b even: odd - even +even = even. Not possible.
Case 4: a even, b even: even - even +even = even. Possible.

The fourth case is the only one possible,

Proof by cases. ("divide-and-conquer" strategy)

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

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

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

Proof of lemma: Assume a solution of the form a/b.

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

multiply by b^5,

$$a^5 - ab^4 + b^5 = 0$$

Case 1: *a* odd, *b* odd: odd - odd +odd = even. Not possible.
Case 2: *a* even, *b* odd: even - even +odd = even. Not possible.
Case 3: *a* odd, *b* even: odd - even +even = even. Not possible.
Case 4: *a* even, *b* even: even - even +even = even. Possible.

The fourth case is the only one possible, so the lemma follows. □

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ 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!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

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

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

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

One of the cases is true so theorem holds.

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

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

One of the cases is true so theorem holds. □

Proof by cases.

Theorem: There exist irrational x and y such that x^y is rational.

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

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

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

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

One of the cases is true so theorem holds. □

Question: Which case holds?

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!

Case2: $\sqrt{2}^{\sqrt{2}}$ is irrational.

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

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

One of the cases is true so theorem holds. □

Question: Which case holds? Don't know!!!

Be careful.

Theorem: $3 = 4$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. $\square$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don't assume what you want to prove!

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. $\square$

Don't assume what you want to prove!

Theorem: $1 = 2$
Proof:

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. $\square$

Don't assume what you want to prove!

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

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. $\square$

Don't assume what you want to prove!

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

$$(x^2 - xy) = x^2 - y^2$$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don't assume what you want to prove!

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

$$(x^2 - xy) = x^2 - y^2$$
$$x(x - y) = (x + y)(x - y)$$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. $\square$

Don't assume what you want to prove!

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

$$\begin{aligned} (x^2 - xy) &= x^2 - y^2 \\ x(x-y) &= (x+y)(x-y) \\ x &= (x+y) \end{aligned}$$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. $\square$

Don't assume what you want to prove!

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

$$\begin{aligned} (x^2 - xy) &= x^2 - y^2 \\ x(x-y) &= (x+y)(x-y) \\ x &= (x+y) \\ x &= 2x \end{aligned}$$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don't assume what you want to prove!

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

$$\begin{aligned}(x^2 - xy) &= x^2 - y^2 \\ x(x-y) &= (x+y)(x-y) \\ x &= (x+y) \\ x &= 2x \\ 1 &= 2\end{aligned}$$

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don't assume what you want to prove!

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

$$
\begin{aligned}
(x^2 - xy) &= x^2 - y^2 \\
x(x - y) &= (x + y)(x - y) \\
x &= (x + y) \\
x &= 2x \\
1 &= 2
\end{aligned}
$$

□

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don't assume what you want to prove!

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

$$\begin{aligned} (x^2 - xy) &= x^2 - y^2 \\ x(x-y) &= (x+y)(x-y) \\ x &= (x+y) \\ x &= 2x \\ 1 &= 2 \end{aligned}$$

□

Dividing by zero is no good.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. □

Don't assume what you want to prove!

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

$$\begin{aligned} (x^2 - xy) &= x^2 - y^2 \\ x(x-y) &= (x+y)(x-y) \\ x &= (x+y) \\ x &= 2x \\ 1 &= 2 \end{aligned}$$

□

Dividing by zero is no good.

Also: Multiplying inequalities by a negative.

Be careful.

Theorem: $3 = 4$

Proof: Assume $3 = 4$. Start with $12 = 12$. Divide one side by 3 and the other by 4 to get $4 = 3$. By commutativity theorem holds. $\square$

Don't assume what you want to prove!

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

$$\begin{aligned} (x^2 - xy) &= x^2 - y^2 \\ x(x-y) &= (x+y)(x-y) \\ x &= (x+y) \\ x &= 2x \\ 1 &= 2 \end{aligned} \quad \square$$

Dividing by zero is no good.

Also: Multiplying inequalities by a negative.

$P \implies Q$ does not mean $Q \implies P$.

Summary

Direct Proof:

To Prove: $P \implies Q$. Assume P. reason forward, Prove Q.

Summary

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

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

Summary

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

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

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

Summary

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

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

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

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
Either $\sqrt{2}$ and $\sqrt{2}$ worked.
or $\sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}$ worked.

Summary

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

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

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

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
Either $\sqrt{2}$ and $\sqrt{2}$ worked.
or $\sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}$ worked.

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