Proof Techniques

K. Subramani[1]

[1]Lane Department of Computer Science and Electrical Engineering
West Virginia University

4, 9, 11 February 2016

Outline

Outline

Outline

Outline

Some well-known theorems

Some well-known theorems

Theorems in Number Theory

Some well-known theorems

Theorems in Number Theory

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd,

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$,

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$,

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square,

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$,

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.
5. If a and b are two rational numbers,

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.
5. If a and b are two rational numbers, then so is $a \cdot b$.

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.
5. If a and b are two rational numbers, then so is $a \cdot b$.
6. For every n, $(n^2 + n)$ is even.

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.
5. If a and b are two rational numbers, then so is $a \cdot b$.
6. For every n, $(n^2 + n)$ is even.

Observation

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.
5. If a and b are two rational numbers, then so is $a \cdot b$.
6. For every n, $(n^2 + n)$ is even.

Observation

Theorems generally have the form

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.
5. If a and b are two rational numbers, then so is $a \cdot b$.
6. For every n, $(n^2 + n)$ is even.

Observation

Theorems generally have the form $P \rightarrow Q$

Some well-known theorems

Theorems in Number Theory

1. If x and y are two natural numbers and $x \cdot y$ is odd, then x and y are both odd.
2. If a and b are two integers, such that $a \mid b$ and $b \mid a$, then $a = b$.
3. If $n = 25$ or $n = 100$, then n is a perfect square, and n is a sum of two perfect squares.
4. If $x^2 + 2 \cdot x - 3 = 0$, then $x \neq 2$.
5. If a and b are two rational numbers, then so is $a \cdot b$.
6. For every n, $(n^2 + n)$ is even.

Observation

Theorems generally have the form $P \rightarrow Q$ *or* $(\forall x)[P(x) \rightarrow Q(x)]$.

Theorems and conjectures

Theorems and conjectures

Domain dependence

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

In other words, we are interested in **relative truth** and not **absolute truth.**

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

In other words, we are interested in **relative truth** and not **absolute truth.**

For instance, Pythagoras' theorem applies to the domain of right-angle triangles,

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

In other words, we are interested in **relative truth** and not **absolute truth.**

For instance, Pythagoras' theorem applies to the domain of right-angle triangles, Fermat's theorem applies to number triplets,

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

In other words, we are interested in **relative truth** and not **absolute truth.**

For instance, Pythagoras' theorem applies to the domain of right-angle triangles, Fermat's theorem applies to number triplets, and so on.

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

In other words, we are interested in **relative truth** and not **absolute truth.**

For instance, Pythagoras' theorem applies to the domain of right-angle triangles, Fermat's theorem applies to number triplets, and so on.

Definition

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

In other words, we are interested in **relative truth** and not **absolute truth.**

For instance, Pythagoras' theorem applies to the domain of right-angle triangles, Fermat's theorem applies to number triplets, and so on.

Definition

Arguments which are contextually true (as opposed to being universally true) are called **theorems**.

Theorems and conjectures

Domain dependence

Arguments (like theorems) are statements having the form $P \rightarrow Q$ or more generally $(\forall x)[P(x) \rightarrow Q(x)]$.

Therefore, the techniques for proving validity of arguments can be used to prove theorems.

Note that in Mathematics, we are interested in establishing **truth** in a specific interpretation and not all interpretations.

In other words, we are interested in **relative truth** and not **absolute truth.**

For instance, Pythagoras' theorem applies to the domain of right-angle triangles, Fermat's theorem applies to number triplets, and so on.

Definition

Arguments which are contextually true (as opposed to being universally true) are called **theorems**.

If an argument (contextual or universal) is not yet proven, it is called a **conjecture**.

Proof Techniques

Proof Techniques

Note

Proof Techniques

Note

How to prove theorems?

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.

(ii) Direct proof.

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.

(ii) Direct proof.

(iii) Proof by contraposition.

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.
(ii) Direct proof.
(iii) Proof by contraposition.
(iv) Proof by contradiction.

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.
(ii) Direct proof.
(iii) Proof by contraposition.
(iv) Proof by contradiction.
(v) Serendipity.

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.
(ii) Direct proof.
(iii) Proof by contraposition.
(iv) Proof by contradiction.
(v) Serendipity.

Applicable to Structured Domains

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.
(ii) Direct proof.
(iii) Proof by contraposition.
(iv) Proof by contradiction.
(v) Serendipity.

Applicable to Structured Domains

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.
(ii) Direct proof.
(iii) Proof by contraposition.
(iv) Proof by contradiction.
(v) Serendipity.

Applicable to Structured Domains

(i) Mathematical Induction.

Proof Techniques

Note

How to prove theorems? Simply add additional facts as hypotheses.

Then use rules of predicate logic (or propositional logic)!

Applicable to unstructured domains

(i) Exhaustive proof.
(ii) Direct proof.
(iii) Proof by contraposition.
(iv) Proof by contradiction.
(v) Serendipity.

Applicable to Structured Domains

(i) Mathematical Induction.
(ii) Diagonalization.

Axiomatic Number Theory

Axiomatic Number Theory

Motivating points

Axiomatic Number Theory

Motivating points

Arithmetic involving addition and multiplication over the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots, \}$ has been studied for centuries.

Axiomatic Number Theory

Motivating points

Arithmetic involving addition and multiplication over the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots, \}$ has been studied for centuries.

We focus on **Peano arithmetic** that permits addition and multiplication

Peano Arithmetic (PA)

Peano Arithmetic (PA)

Main Issues

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

($\mathcal{A}1.$) $(\forall x)\ [(x + 1) = 0]'$.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

($\mathcal{A}1.$) $(\forall x)\ [(x + 1) = 0]'$.

($\mathcal{A}2.$) $(\forall x)(\forall y)\ [(x + 1) = (y + 1)] \rightarrow (x = y)$.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

($\mathcal{A}1.$) $(\forall x)\ [(x+1) = 0]'$.

($\mathcal{A}2.$) $(\forall x)(\forall y)\ [(x+1) = (y+1)] \rightarrow (x = y)$.

($\mathcal{A}3.$) $(F[0] \wedge (\forall x)\ (F[x] \rightarrow F[x+1])) \rightarrow (\forall x)\ F[x]$.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

($\mathcal{A}1.$) $(\forall x)\ [(x + 1) = 0]'$.

($\mathcal{A}2.$) $(\forall x)(\forall y)\ [(x + 1) = (y + 1)] \rightarrow (x = y)$.

($\mathcal{A}3.$) $(F[0] \wedge (\forall x)\ (F[x] \rightarrow F[x + 1])) \rightarrow (\forall x)\ F[x]$.

($\mathcal{A}4.$) $(\forall x)\ (x + 0 = x)$.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

($\mathcal{A}1.$) $(\forall x)\ [(x+1) = 0]'$.

($\mathcal{A}2.$) $(\forall x)(\forall y)\ [(x+1) = (y+1)] \rightarrow (x = y)$.

($\mathcal{A}3.$) $(F[0] \wedge (\forall x)\ (F[x] \rightarrow F[x+1])) \rightarrow (\forall x)\ F[x]$.

($\mathcal{A}4.$) $(\forall x)\ (x + 0 = x)$.

($\mathcal{A}5.$) $(\forall x)(\forall y)\ x + (y+1) = (x+y) + 1$.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

($\mathcal{A}1.$) $(\forall x)\ [(x+1) = 0]'$.

($\mathcal{A}2.$) $(\forall x)(\forall y)\ [(x+1) = (y+1)] \rightarrow (x = y)$.

($\mathcal{A}3.$) $(F[0] \wedge (\forall x)\ (F[x] \rightarrow F[x+1])) \rightarrow (\forall x)\ F[x]$.

($\mathcal{A}4.$) $(\forall x)\ (x + 0 = x)$.

($\mathcal{A}5.$) $(\forall x)(\forall y)\ x + (y+1) = (x+y) + 1$.

($\mathcal{A}6.$) $(\forall x)\ x \cdot 0 = 0$.

Peano Arithmetic (PA)

Main Issues

The theory of Peano Arithmetic (T_{PA}) or **first-order arithmetic** has the signature:

$$\Sigma_{PA} \ : \ \{0, 1, +, \cdot, =\}$$

where,

(i) 0 and 1 are constants.

(ii) $+$ and $\cdot$ are binary functions.

(iii) $=$ is a binary predicate.

Its axiom set is the following:

($\mathcal{A}1.$) $(\forall x)\ [(x+1) = 0]'$.

($\mathcal{A}2.$) $(\forall x)(\forall y)\ [(x+1) = (y+1)] \rightarrow (x = y)$.

($\mathcal{A}3.$) $(F[0] \wedge (\forall x)\ (F[x] \rightarrow F[x+1])) \rightarrow (\forall x)\ F[x]$.

($\mathcal{A}4.$) $(\forall x)\ (x + 0 = x)$.

($\mathcal{A}5.$) $(\forall x)(\forall y)\ x + (y+1) = (x+y) + 1$.

($\mathcal{A}6.$) $(\forall x)\ x \cdot 0 = 0$.

($\mathcal{A}7.$) $(\forall x)(\forall y)\ x \cdot (y+1) = x \cdot y + x$.

Auxiliary Definitions

Auxiliary Definitions

Common Predicates

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1 + 1$, the symbol 3 for $1 + 1 + 1$ and so on.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1 + 1$, the symbol 3 for $1 + 1 + 1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1 + 1$, the symbol 3 for $1 + 1 + 1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow$

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1 + 1$, the symbol 3 for $1 + 1 + 1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1 + 1$, the symbol 3 for $1 + 1 + 1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow$

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1 + 1$, the symbol 3 for $1 + 1 + 1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow \textbf{even}(x)']$.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1 + 1$, the symbol 3 for $1 + 1 + 1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow \textbf{even}(x)']$.
- $(\forall x)(\forall y)[x < y \rightarrow$

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1+1$, the symbol 3 for $1+1+1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow \textbf{even}(x)']$.
- $(\forall x)(\forall y)[x < y \rightarrow ((\exists w)\ (w = 0)' \wedge (y = x + w))]$.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1+1$, the symbol 3 for $1+1+1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow \textbf{even}(x)']$.
- $(\forall x)(\forall y)[x < y \rightarrow ((\exists w)\ (w = 0)' \wedge (y = x + w))]$.
- $(\forall x)(\forall y)[x \mid y \rightarrow$

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1+1$, the symbol 3 for $1+1+1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow \textbf{even}(x)']$.
- $(\forall x)(\forall y)[x < y \rightarrow ((\exists w)\ (w = 0)' \wedge (y = x + w))]$.
- $(\forall x)(\forall y)[x \mid y \rightarrow ((\exists z)\ y = x \cdot z)]$.

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1+1$, the symbol 3 for $1+1+1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow \textbf{even}(x)']$.
- $(\forall x)(\forall y)[x < y \rightarrow ((\exists w)\ (w = 0)' \wedge (y = x + w))]$.
- $(\forall x)(\forall y)[x \mid y \rightarrow ((\exists z)\ y = x \cdot z)]$.
- $(\forall x)[\textbf{prime}(x) \rightarrow$

Auxiliary Definitions

Common Predicates

The "rudimentary" theory discussed above is sufficient for number theory.

However, in order to make mathematics readable, we need additional predicates, such as **even**(x), **odd**(x), and so on.

Here are some first order definitions, which we will assume have been added to the list of axioms:

- We use the symbol 2 for $1+1$, the symbol 3 for $1+1+1$ and so on.
- We use $a \cdot x$ to represent the addition of x with itself a times.
- $(\forall x)[\textbf{even}(x) \rightarrow ((\exists z)\ x = 2 \cdot z)]$.
- $(\forall x)[\textbf{odd}(x) \rightarrow \textbf{even}(x)']$.
- $(\forall x)(\forall y)[x < y \rightarrow ((\exists w)\ (w = 0)' \wedge (y = x + w))]$.
- $(\forall x)(\forall y)[x \mid y \rightarrow ((\exists z)\ y = x \cdot z)]$.
- $(\forall x)[\textbf{prime}(x) \rightarrow ((1 < x) \wedge (\forall z)\ z \mid x \rightarrow ((z = 1) \vee (z = x)))]$.

Exhaustive Proof

Exhaustive Proof

Technique

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Let $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Let $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Conjecture: *If $x \in D$ and x is divisible by 4, then x is divisible by 2.*

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Let $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Conjecture: *If $x \in D$ and x is divisible by 4, then x is divisible by 2.*

Let $P(x) \equiv x$ is divisible by 4, and $Q(x) \equiv x$ is divisible by 2.

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Let $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Conjecture: *If $x \in D$ and x is divisible by 4, then x is divisible by 2.*

Let $P(x) \equiv x$ is divisible by 4, and $Q(x) \equiv x$ is divisible by 2.

The conjecture is $(\forall x \in D)[P(x) \rightarrow Q(x)]$.

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Let $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Conjecture: *If $x \in D$ and x is divisible by 4, then x is divisible by 2.*

Let $P(x) \equiv x$ is divisible by 4, and $Q(x) \equiv x$ is divisible by 2.

The conjecture is $(\forall x \in D)[P(x) \rightarrow Q(x)]$.

Check for $x = 1$, $x = 2$, ...

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Let $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Conjecture: *If $x \in D$ and x is divisible by 4, then x is divisible by 2.*

Let $P(x) \equiv x$ is divisible by 4, and $Q(x) \equiv x$ is divisible by 2.

The conjecture is $(\forall x \in D)[P(x) \rightarrow Q(x)]$.

Check for $x = 1$, $x = 2$, ...

Note

Exhaustive Proof

Technique

Simply enumerate all elements of the domain and check if the argument holds for each element.

If it does, then the conjecture is a theorem.

Example

Let $D = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

Conjecture: *If $x \in D$ and x is divisible by 4, then x is divisible by 2.*

Let $P(x) \equiv x$ is divisible by 4, and $Q(x) \equiv x$ is divisible by 2.

The conjecture is $(\forall x \in D)[P(x) \rightarrow Q(x)]$.

Check for $x = 1$, $x = 2$, ...

Note

Only works when the domain is finite.

Another example for Exhaustive Proof

Another example for Exhaustive Proof

Example

Another example for Exhaustive Proof

Example

Let $D = \{0, 1, 2, 3, 4, 5\}$.

Another example for Exhaustive Proof

Example

Let $D = \{0, 1, 2, 3, 4, 5\}$.

Consider the following conjecture:

Another example for Exhaustive Proof

Example

Let $D = \{0, 1, 2, 3, 4, 5\}$.

Consider the following conjecture: For all $x \in D$, $x^2 \leq 10 + 5 \cdot x$.

Another example for Exhaustive Proof

Example

Let $D = \{0, 1, 2, 3, 4, 5\}$.

Consider the following conjecture: For all $x \in D$, $x^2 \leq 10 + 5 \cdot x$.

Is the conjecture a theorem?

Direct Proof

Direct Proof

Technique

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Example

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Example

Show that the product of two even integers is even.

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Example

Show that the product of two even integers is even.

Let us first symbolize the argument:

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Example

Show that the product of two even integers is even.

Let us first symbolize the argument:

$(\forall x)(\forall y)\ (x$ **even** $\wedge\ y$ **even**$) \rightarrow x \cdot y$ **even**

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Example

Show that the product of two even integers is even.

Let us first symbolize the argument:

$(\forall x)(\forall y)\ (x$ **even** $\wedge\ y$ **even**$) \rightarrow x \cdot y$ **even**

Is the above symbolization complete?

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Example

Show that the product of two even integers is even.

Let us first symbolize the argument:

$(\forall x)(\forall y)\ (x$ **even** $\wedge\ y$ **even**$) \rightarrow x \cdot y$ **even**

Is the above symbolization complete?

Formal Proof:

Direct Proof

Technique

Given the conjecture $P \rightarrow Q$, assume that P is true and show that Q must be true.

This is exactly what we did in Formal Logic!

Example

Show that the product of two even integers is even.

Let us first symbolize the argument:

$(\forall x)(\forall y)$ (x **even** $\wedge$ y **even**) $\rightarrow$ $x \cdot y$ **even**

Is the above symbolization complete?

Formal Proof: On dot-cam.

Proof of Example

Proof of Example

Proof.

Proof of Example

Proof.

We now give an informal but rigorous proof.

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Therefore,

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Therefore, $x \cdot y =$

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Therefore, $x \cdot y = (2 \cdot k) \cdot (2 \cdot r) =$

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Therefore, $x \cdot y = (2 \cdot k) \cdot (2 \cdot r) = 2 \cdot (2 \cdot k \cdot r) =$

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Therefore, $x \cdot y = (2 \cdot k) \cdot (2 \cdot r) = 2 \cdot (2 \cdot k \cdot r) = 2 \cdot p$, for some integer p.

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Therefore, $x \cdot y = (2 \cdot k) \cdot (2 \cdot r) = 2 \cdot (2 \cdot k \cdot r) = 2 \cdot p$, for some integer p.

It follows that $x \cdot y$ is even. □

Proof of Example

Proof.

We now give an informal but rigorous proof.

Since x is even, $x = 2 \cdot k$, for some integer k.

Since y is even, $y = 2 \cdot r$, for some integer r.

Therefore, $x \cdot y = (2 \cdot k) \cdot (2 \cdot r) = 2 \cdot (2 \cdot k \cdot r) = 2 \cdot p$, for some integer p.

It follows that $x \cdot y$ is even. □

Example

Show that if an integer is divisible by 4, then it is divisible by 2.

Proof by Contraposition

Proof by Contraposition

Technique

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally,

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally, $(\forall x)(x^2 \text{ odd}) \rightarrow (x \text{ odd})$.

Proof by Contraposition

Technique

Given the argument $P \to Q$, use the direct proof technique to show that $Q' \to P'$.

We know that $(P \to Q) \Leftrightarrow (Q' \to P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally, $(\forall x)(x^2 \text{ odd}) \to (x \text{ odd})$.

Proof.

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally, $(\forall x)(x^2 \text{ odd}) \rightarrow (x \text{ odd})$.

Proof.

We will instead show that if x is not odd, then x^2 is not odd.

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally, $(\forall x)(x^2 \text{ odd}) \rightarrow (x \text{ odd})$.

Proof.

We will instead show that if x is not odd, then x^2 is not odd.

However, if x is not odd, then it must be even.

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally, $(\forall x)(x^2 \text{ odd}) \rightarrow (x \text{ odd})$.

Proof.

We will instead show that if x is not odd, then x^2 is not odd.

However, if x is not odd, then it must be even. Likewise, with x^2.

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally, $(\forall x)(x^2 \text{ odd}) \rightarrow (x \text{ odd})$.

Proof.

We will instead show that if x is not odd, then x^2 is not odd.

However, if x is not odd, then it must be even. Likewise, with x^2.

We thus have to show that if x is even, then so is x^2.

Proof by Contraposition

Technique

Given the argument $P \rightarrow Q$, use the direct proof technique to show that $Q' \rightarrow P'$.

We know that $(P \rightarrow Q) \Leftrightarrow (Q' \rightarrow P')$!

Example

Show that if the square of an integer is odd, then x must be odd.

Formally, $(\forall x)(x^2 \text{ odd}) \rightarrow (x \text{ odd})$.

Proof.

We will instead show that if x is not odd, then x^2 is not odd.

However, if x is not odd, then it must be even. Likewise, with x^2.

We thus have to show that if x is even, then so is x^2.

But we have already shown that if two numbers are even so is their product! □

Contraposition (contd.)

Contraposition (contd.)

Example

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Note

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Note

Do not confuse contrapositive with converse.

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Note

Do not confuse contrapositive with converse.

The converse of $P \rightarrow Q$ is

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Note

Do not confuse contrapositive with converse.

The converse of $P \rightarrow Q$ is $Q \rightarrow P$.

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Note

Do not confuse contrapositive with converse.

The converse of $P \rightarrow Q$ is $Q \rightarrow P$.

The converse of a theorem may or may not be true.

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Note

Do not confuse contrapositive with converse.

The converse of $P \rightarrow Q$ is $Q \rightarrow P$.

The converse of a theorem may or may not be true.

For instance, the argument, "If $a > 5$, then $a > 2$" is a theorem.

Contraposition (contd.)

Example

Show that if 5 apples are given to 4 students, then at least one student will get ≥ 2 apples.

The apples must be given as wholes.

Note

Do not confuse contrapositive with converse.

The converse of $P \rightarrow Q$ is $Q \rightarrow P$.

The converse of a theorem may or may not be true.

For instance, the argument, "If $a > 5$, then $a > 2$" is a theorem.

What about the converse?

Proof by Contradiction

Proof by Contradiction

Main Idea

Proof by Contradiction

Main Idea

Observe that $[(P \wedge Q') \rightarrow \textbf{false}] \rightarrow (P \rightarrow Q)$ is a tautology.

Proof by Contradiction

Main Idea

Observe that $[(P \wedge Q') \rightarrow \textbf{false}] \rightarrow (P \rightarrow Q)$ is a tautology.

It follows that if we show that $(P \wedge Q')$ is unequivocally **false**, we have in fact, proven $P \rightarrow Q$.

Proof by Contradiction

Main Idea

Observe that $[(P \wedge Q') \rightarrow \textbf{false}] \rightarrow (P \rightarrow Q)$ is a tautology.

It follows that if we show that $(P \wedge Q')$ is unequivocally **false**, we have in fact, proven $P \rightarrow Q$.

Definition

Proof by Contradiction

Main Idea

Observe that $[(P \wedge Q') \rightarrow \textbf{false}] \rightarrow (P \rightarrow Q)$ is a tautology.

It follows that if we show that $(P \wedge Q')$ is unequivocally **false**, we have in fact, proven $P \rightarrow Q$.

Definition

A rational number is one that can be expressed in the form $\frac{p}{q}$, where p and q are integers, with no common divisor and $q \neq 0$.

Proof by Contradiction

Main Idea

Observe that $[(P \wedge Q') \rightarrow \textbf{false}] \rightarrow (P \rightarrow Q)$ is a tautology.

It follows that if we show that $(P \wedge Q')$ is unequivocally **false**, we have in fact, proven $P \rightarrow Q$.

Definition

A rational number is one that can be expressed in the form $\frac{p}{q}$, where p and q are integers, with no common divisor and $q \neq 0$.

The condition of having no common divisors is denoted by $gcd(p, q) = 1$.

Proof by Contradiction

Main Idea

Observe that $[(P \wedge Q') \rightarrow \textbf{false}] \rightarrow (P \rightarrow Q)$ is a tautology.

It follows that if we show that $(P \wedge Q')$ is unequivocally **false**, we have in fact, proven $P \rightarrow Q$.

Definition

A rational number is one that can be expressed in the form $\frac{p}{q}$, where p and q are integers, with no common divisor and $q \neq 0$.

The condition of having no common divisors is denoted by $gcd(p, q) = 1$.

Example

Proof by Contradiction

Main Idea

Observe that $[(P \wedge Q') \rightarrow \textbf{false}] \rightarrow (P \rightarrow Q)$ is a tautology.

It follows that if we show that $(P \wedge Q')$ is unequivocally **false**, we have in fact, proven $P \rightarrow Q$.

Definition

A rational number is one that can be expressed in the form $\frac{p}{q}$, where p and q are integers, with no common divisor and $q \neq 0$.

The condition of having no common divisors is denoted by $gcd(p, q) = 1$.

Example

Show that $\sqrt{2}$ is not rational.

Proof by Contradiction (contd.)

Proof by Contradiction (contd.)

Proof.

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational.

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1$, $q \neq 0$.

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1$, $q \neq 0$.

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1$, $q \neq 0$.

$$\sqrt{2} \cdot q \quad = \quad p$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1$, $q \neq 0$.

$$\begin{aligned} \sqrt{2} \cdot q &= p \\ \rightarrow 2 \cdot q^2 &= p^2 \end{aligned}$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$\begin{aligned} \sqrt{2} \cdot q &= p \\ \rightarrow 2 \cdot q^2 &= p^2 \\ \rightarrow 2 &\mid p^2 \end{aligned}$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$\begin{aligned} \sqrt{2} \cdot q &= p \\ \rightarrow 2 \cdot q^2 &= p^2 \\ \rightarrow 2 &\mid p^2 \\ \rightarrow 2 &\mid p \end{aligned}$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$\begin{aligned} \sqrt{2} \cdot q &= p \\ \rightarrow 2 \cdot q^2 &= p^2 \\ \rightarrow 2 &\mid p^2 \\ \rightarrow 2 &\mid p \\ \rightarrow p &= 2 \cdot k, \text{ for some k} \end{aligned}$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$\begin{aligned}
\sqrt{2} \cdot q &= p \\
\rightarrow 2 \cdot q^2 &= p^2 \\
\rightarrow 2 &\mid p^2 \\
\rightarrow 2 &\mid p \\
\rightarrow p &= 2 \cdot k, \text{ for some k} \\
\rightarrow p^2 &= 4 \cdot k^2
\end{aligned}$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$\begin{aligned}
\sqrt{2} \cdot q &= p \\
\rightarrow 2 \cdot q^2 &= p^2 \\
\rightarrow 2 &\mid p^2 \\
\rightarrow 2 &\mid p \\
\rightarrow p &= 2 \cdot k, \text{ for some k} \\
\rightarrow p^2 &= 4 \cdot k^2 \\
\rightarrow 2 \cdot q^2 &= 4 \cdot k^2
\end{aligned}$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$\begin{aligned}
\sqrt{2} \cdot q &= p \\
\rightarrow 2 \cdot q^2 &= p^2 \\
\rightarrow 2 &\mid p^2 \\
\rightarrow 2 &\mid p \\
\rightarrow p &= 2 \cdot k, \text{ for some k} \\
\rightarrow p^2 &= 4 \cdot k^2 \\
\rightarrow 2 \cdot q^2 &= 4 \cdot k^2 \\
\rightarrow q^2 &= 2 \cdot k^2
\end{aligned}$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$
\begin{aligned}
\sqrt{2} \cdot q &= p \\
\rightarrow 2 \cdot q^2 &= p^2 \\
\rightarrow 2 &\mid p^2 \\
\rightarrow 2 &\mid p \\
\rightarrow p &= 2 \cdot k, \text{ for some k} \\
\rightarrow p^2 &= 4 \cdot k^2 \\
\rightarrow 2 \cdot q^2 &= 4 \cdot k^2 \\
\rightarrow q^2 &= 2 \cdot k^2 \\
\rightarrow 2 &\mid q^2
\end{aligned}
$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$
\begin{aligned}
\sqrt{2} \cdot q &= p \\
\rightarrow 2 \cdot q^2 &= p^2 \\
\rightarrow 2 &\mid p^2 \\
\rightarrow 2 &\mid p \\
\rightarrow p &= 2 \cdot k, \text{ for some k} \\
\rightarrow p^2 &= 4 \cdot k^2 \\
\rightarrow 2 \cdot q^2 &= 4 \cdot k^2 \\
\rightarrow q^2 &= 2 \cdot k^2 \\
\rightarrow 2 &\mid q^2 \\
\rightarrow 2 &\mid q
\end{aligned}
$$

Proof by Contradiction (contd.)

Proof.

Let $\sqrt{2}$ be rational. Therefore, $\sqrt{2} = \frac{p}{q}$, $gcd(p, q) = 1,\ q \neq 0$.

$$
\begin{array}{rcl}
\sqrt{2} \cdot q & = & p \\
\rightarrow 2 \cdot q^2 & = & p^2 \\
\rightarrow 2 & | & p^2 \\
\rightarrow 2 & | & p \\
\rightarrow p & = & 2 \cdot k, \text{ for some k} \\
\rightarrow p^2 & = & 4 \cdot k^2 \\
\rightarrow 2 \cdot q^2 & = & 4 \cdot k^2 \\
\rightarrow q^2 & = & 2 \cdot k^2 \\
\rightarrow 2 & | & q^2 \\
\rightarrow 2 & | & q \\
\rightarrow & \textit{Bingo}! &
\end{array}
$$

□

Proof by Contradiction (contd.)

Proof by Contradiction (contd.)

Example

(i) Show that $\sqrt{3}$ is not rational.

(ii) Show that the product of two odd integers is odd.

Proof by Contradiction (contd.)

Example

(i) Show that $\sqrt{3}$ is not rational.

(ii) Show that the product of two odd integers is odd. (Can you do it by direct proof?)

Serendipity

Serendipity

Technique

Serendipity

Technique

Prayer!

Serendipity

Technique

Prayer! Good Luck.

Serendipity

Technique

Prayer! Good Luck. Coffee.

Serendipity

Technique

Prayer! Good Luck. Coffee.

Example

Serendipity

Technique

Prayer! Good Luck. Coffee.

Example

Number of games in a tennis tournament.

Induction

Induction

Motivation

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Every non-empty set of positive integers has a **least element**.

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Every non-empty set of positive integers has a **least element**.

Note

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Every non-empty set of positive integers has a **least element**.

Note

Induction can only be applied to a well-ordered domain, where the concept of "next" is unambiguous,

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Every non-empty set of positive integers has a **least element**.

Note

Induction can only be applied to a well-ordered domain, where the concept of "next" is unambiguous, e.g, non-negative integers.

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Every non-empty set of positive integers has a **least element**.

Note

Induction can only be applied to a well-ordered domain, where the concept of "next" is unambiguous, e.g, non-negative integers.

How about all integers?

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Every non-empty set of positive integers has a **least element**.

Note

Induction can only be applied to a well-ordered domain, where the concept of "next" is unambiguous, e.g, non-negative integers.

How about all integers?

How about non-negative reals?

Induction

Motivation

Reaching arbitrary rungs of a ladder.

Well-Ordering Principle

Every non-empty set of positive integers has a **least element**.

Note

Induction can only be applied to a well-ordered domain, where the concept of "next" is unambiguous, e.g, non-negative integers.

How about all integers?

How about non-negative reals?

How about non-negative rationals?

The first principle of Mathematical Induction

The first principle of Mathematical Induction

Principle

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.
2. $(\forall k)[P(k)$ is **true** $\rightarrow P(k+1)$ is **true**$]$

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.
2. $(\forall k)[P(k)$ is **true** $\rightarrow P(k+1)$ is **true**$]$

then,

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.
2. $(\forall k)[P(k)$ is **true** $\rightarrow P(k+1)$ is **true**$]$

then,

$P(n)$ is **true**, for all positive integers n.

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.
2. $(\forall k)[P(k)$ is **true** $\rightarrow P(k+1)$ is **true**$]$

then,

$P(n)$ is **true**, for all positive integers n.

Observations

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.
2. $(\forall k)[P(k)$ is **true** $\rightarrow P(k+1)$ is **true**$]$

then,

$P(n)$ is **true**, for all positive integers n.

Observations

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.
2. $(\forall k)[P(k)$ is **true** $\rightarrow P(k+1)$ is **true**$]$

then,

$P(n)$ is **true**, for all positive integers n.

Observations

(i) Showing that $P(1)$ is **true** is called the basis step.

The first principle of Mathematical Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture (argument) that we need to show holds, for every $n \geq 1$.

If

1. $P(1)$ is **true**.
2. $(\forall k)[P(k)$ is **true** $\rightarrow P(k+1)$ is **true**$]$

then,

$P(n)$ is **true**, for all positive integers n.

Observations

(i) Showing that $P(1)$ is **true** is called the basis step.

(ii) Assuming that $P(k)$ is **true**, in order to show that $P(k+1)$ is **true** is called the inductive hypothesis.

First Example

First Example

Example

First Example

Example

Show that the sum of the first n integers is $\frac{n \cdot (n+1)}{2}$.

First Example

Example

Show that the sum of the first n integers is $\frac{n\cdot(n+1)}{2}$.

Formally, $(\forall n)\ [\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}]$.

Formal Proof

Formal Proof

Proof.

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture:

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture: $(\forall n) P(n)$.

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture: $(\forall n) P(n)$.

Basis ($P(1)$):

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture: $(\forall n) P(n)$.

BASIS ($P(1)$):

$$LHS \quad =$$

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture: $(\forall n) P(n)$.

BASIS ($P(1)$):

$$LHS = \sum_{i=1}^{1} i$$

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture: $(\forall n) P(n)$.

BASIS ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i \\ &= 1 \end{aligned}$$

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture: $(\forall n) P(n)$.

BASIS ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i \\ &= 1 \\ RHS &= \frac{1 \cdot (1+1)}{2} \end{aligned}$$

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}$.

We are required to prove the conjecture: $(\forall n)P(n)$.

BASIS ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i \\ &= 1 \\ RHS &= \frac{1\cdot(1+1)}{2} = \frac{1\cdot(2)}{2} \end{aligned}$$

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$.

We are required to prove the conjecture: $(\forall n) P(n)$.

BASIS ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i \\ &= 1 \\ RHS &= \frac{1 \cdot (1+1)}{2} = \frac{1 \cdot (2)}{2} = \frac{2}{2} \end{aligned}$$

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}$.

We are required to prove the conjecture: $(\forall n)P(n)$.

BASIS ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i \\ &= 1 \\ RHS &= \frac{1\cdot(1+1)}{2} = \frac{1\cdot(2)}{2} = \frac{2}{2} = 1 \end{aligned}$$

Formal Proof

Proof.

Let $P(n)$ denote the predicate $\sum_{i=1}^{n} i = \frac{n\cdot(n+1)}{2}$.

We are required to prove the conjecture: $(\forall n)P(n)$.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i \\ &= 1 \\ RHS &= \frac{1\cdot(1+1)}{2} = \frac{1\cdot(2)}{2} = \frac{2}{2} = 1 \end{aligned}$$

Thus, $LHS = RHS$ and $P(1)$ is true. □

Example

Proof.

Example

Proof.

Let us assume that $P(k)$ is true, i.e.,

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i =$$

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

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

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

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

We need to show that $P(k+1)$ is true,

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

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

We need to show that $P(k+1)$ is true, i.e., we need to show that

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

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

We need to show that $P(k+1)$ is true, i.e., we need to show that

$$\sum_{i=1}^{k+1} i =$$

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

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

We need to show that $P(k+1)$ is true, i.e., we need to show that

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

Example

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

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

We need to show that $P(k+1)$ is true, i.e., we need to show that

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

Proof (contd.)

Proof (contd.)

Proof.

Observe that,

Proof (contd.)

Proof.

Observe that,

$$LHS \quad =$$

Proof (contd.)

Proof.

Observe that,

$$LHS = \sum_{i=1}^{k+1} i$$

Proof (contd.)

Proof.

Observe that,

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1} i \\ &= 1 + 2 + 3 + \ldots + k + (k+1) \end{aligned}$$

Proof (contd.)

Proof.

Observe that,

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1} i \\ &= 1 + 2 + 3 + \ldots + k + (k+1) \\ &= (1 + 2 + 3 + \ldots + k) + (k+1) \end{aligned}$$

Proof (contd.)

Proof.

Observe that,

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1} i \\ &= 1 + 2 + 3 + \ldots + k + (k+1) \\ &= (1 + 2 + 3 + \ldots + k) + (k+1) \\ &= \frac{k \cdot (k+1)}{2} + (k+1), \text{ using the inductive hypothesis} \end{aligned}$$

Proof (contd.)

Proof.

Observe that,

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1} i \\ &= 1+2+3+\ldots+k+(k+1) \\ &= (1+2+3+\ldots+k)+(k+1) \\ &= \frac{k\cdot(k+1)}{2}+(k+1), \text{ using the inductive hypothesis} \\ &= (k+1)\cdot(\frac{k}{2}+1) \end{aligned}$$

Proof (contd.)

Proof.

Observe that,

$$\begin{aligned}
LHS &= \sum_{i=1}^{k+1} i \\
&= 1 + 2 + 3 + \ldots + k + (k+1) \\
&= (1 + 2 + 3 + \ldots + k) + (k+1) \\
&= \frac{k \cdot (k+1)}{2} + (k+1), \text{ using the inductive hypothesis} \\
&= (k+1) \cdot (\frac{k}{2} + 1) \\
&= (k+1) \cdot (\frac{k+2}{2})
\end{aligned}$$

Proof (contd.)

Proof.

Observe that,

$$
\begin{aligned}
LHS &= \sum_{i=1}^{k+1} i \\
&= 1 + 2 + 3 + \ldots + k + (k+1) \\
&= (1 + 2 + 3 + \ldots + k) + (k+1) \\
&= \frac{k \cdot (k+1)}{2} + (k+1), \text{ using the inductive hypothesis} \\
&= (k+1) \cdot (\frac{k}{2} + 1) \\
&= (k+1) \cdot (\frac{k+2}{2}) \\
&= \frac{(k+1) \cdot (k+2)}{2}
\end{aligned}
$$

Proof (contd.)

Proof.

Observe that,

$$
\begin{aligned}
LHS &= \sum_{i=1}^{k+1} i \\
&= 1 + 2 + 3 + \ldots + k + (k+1) \\
&= (1 + 2 + 3 + \ldots + k) + (k+1) \\
&= \frac{k \cdot (k+1)}{2} + (k+1), \text{ using the inductive hypothesis} \\
&= (k+1) \cdot (\frac{k}{2} + 1) \\
&= (k+1) \cdot (\frac{k+2}{2}) \\
&= \frac{(k+1) \cdot (k+2)}{2} \\
&= RHS.
\end{aligned}
$$

Proof (contd.)

Proof.

Observe that,

$$\begin{aligned}
LHS &= \sum_{i=1}^{k+1} i \\
&= 1 + 2 + 3 + \ldots + k + (k+1) \\
&= (1 + 2 + 3 + \ldots + k) + (k+1) \\
&= \frac{k \cdot (k+1)}{2} + (k+1), \text{ using the inductive hypothesis} \\
&= (k+1) \cdot (\frac{k}{2} + 1) \\
&= (k+1) \cdot (\frac{k+2}{2}) \\
&= \frac{(k+1) \cdot (k+2)}{2} \\
&= RHS.
\end{aligned}$$

□

Completing the proof

Completing the proof

Final Steps

Completing the proof

Final Steps

Since, $LHS{=}RHS$, we have shown that $P(k) \rightarrow P(k+1)$.

Completing the proof

Final Steps

Since, $LHS{=}RHS$, we have shown that $P(k) \rightarrow P(k+1)$.

Applying the first principle of mathematical induction, we conclude that the conjecture is **true**, i.e., $(\forall n)P(n)$ holds.

Central Theme

Central Theme

Main Ideas

Central Theme

Main Ideas

(i) Mathematicize the conjecture.

Central Theme

Main Ideas

(i) Mathematicize the conjecture.

(ii) Prove the basis (usually $P(1)$ and usually easy.)

Central Theme

Main Ideas

(i) Mathematicize the conjecture.

(ii) Prove the basis (usually $P(1)$ and usually easy.)

(iii) Assume $P(k)$.

Central Theme

Main Ideas

(i) Mathematicize the conjecture.

(ii) Prove the basis (usually $P(1)$ and usually easy.)

(iii) Assume $P(k)$.

(iv) Show $P(k+1)$.

Central Theme

Main Ideas

(i) Mathematicize the conjecture.

(ii) Prove the basis (usually $P(1)$ and usually easy.)

(iii) Assume $P(k)$.

(iv) Show $P(k+1)$. (The hard part.

Central Theme

Main Ideas

(i) Mathematicize the conjecture.

(ii) Prove the basis (usually $P(1)$ and usually easy.)

(iii) Assume $P(k)$.

(iv) Show $P(k+1)$. (The hard part. Use mathematical manipulation.)

Central Theme

Main Ideas

(i) Mathematicize the conjecture.

(ii) Prove the basis (usually $P(1)$ and usually easy.)

(iii) Assume $P(k)$.

(iv) Show $P(k+1)$. (The hard part. Use mathematical manipulation.)

(v) To show $P(k) \rightarrow P(k+1)$, you may use any of the proof techniques discussed, including exhaustive proof, direct proof, contraposition, contradiction, serendipity and induction!

Another Induction Example

Another Induction Example

Example

Another Induction Example

Example

Show that the sum of the squares of the first n integers is $\frac{n \cdot (n+1) \cdot (2 \cdot n+1)}{6}$,

Another Induction Example

Example

Show that the sum of the squares of the first n integers is $\frac{n\cdot(n+1)\cdot(2\cdot n+1)}{6}$, i.e., show that $\sum_{i=1}^{n} i^2 = \frac{n\cdot(n+1)\cdot(2\cdot n+1)}{6}$.

Proving the Basis

Proving the Basis

Proof.

Proving the Basis

Proof.

Basis ($P(1)$):

Proving the Basis

Proof.

Basis ($P(1)$):

$$LHS \quad =$$

Proving the Basis

Proof.

Basis ($P(1)$):

$$LHS = \sum_{i=1}^{1} i^2$$

Proving the Basis

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i^2 \\ &= 1 \end{aligned}$$

Proving the Basis

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i^2 \\ &= 1 \\ RHS &= \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} \end{aligned}$$

Proving the Basis

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i^2 \\ &= 1 \\ RHS &= \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} \\ &= \frac{1 \cdot (2) \cdot (3)}{6} \end{aligned}$$

Proving the Basis

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i^2 \\ &= 1 \\ RHS &= \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} \\ &= \frac{1 \cdot (2) \cdot (3)}{6} \\ &= \frac{6}{6} \end{aligned}$$

Proving the Basis

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i^2 \\ &= 1 \\ RHS &= \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} \\ &= \frac{1 \cdot (2) \cdot (3)}{6} \\ &= \frac{6}{6} \\ &= 1 \end{aligned}$$

Proving the Basis

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1} i^2 \\ &= 1 \\ RHS &= \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6} \\ &= \frac{1 \cdot (2) \cdot (3)}{6} \\ &= \frac{6}{6} \\ &= 1 \end{aligned}$$

Thus, $LHS = RHS$ and $P(1)$ is true. □

Induction example (contd.)

Induction example (contd.)

Proof.

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 =$$

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true,

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 =$

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$.

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$.

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$.

$$LHS \quad =$$

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$.

$$LHS = \sum_{i=1}^{k+1} i^2$$

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$.

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1} i^2 \\ &= 1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 \end{aligned}$$

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$.

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1} i^2 \\ &= 1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 \\ &= (1^2 + 2^2 + 3^2 + \ldots + k^2) + (k+1)^2 \end{aligned}$$

Induction example (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k} i^2 = \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6}.$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1} i^2 = \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$.

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1} i^2 \\ &= 1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 \\ &= (1^2 + 2^2 + 3^2 + \ldots + k^2) + (k+1)^2 \end{aligned}$$

□

Induction proof (contd.)

Induction proof (contd.)

Proof.

Induction proof (contd.)

Proof.

$$= \frac{k \cdot (k+1) \cdot (2 \cdot k+1)}{6} + (k+1)^2, \text{ using the inductive hypothesis}$$

Induction proof (contd.)

Proof.

$$= \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6} + (k+1)^2, \text{ using the inductive hypothesis}$$

$$= \frac{k+1}{6}(k \cdot (2 \cdot k + 1) + 6 \cdot (k+1))$$

Induction proof (contd.)

Proof.

$$
\begin{aligned}
&= \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6} + (k+1)^2, \text{ using the inductive hypothesis} \\
&= \frac{k+1}{6}(k \cdot (2 \cdot k + 1) + 6 \cdot (k+1)) \\
&= \frac{k+1}{6}(2 \cdot k^2 + k + 6 \cdot k + 6)
\end{aligned}
$$

Induction proof (contd.)

Proof.

$$
\begin{aligned}
&= \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6} + (k+1)^2, \text{ using the inductive hypothesis} \\
&= \frac{k+1}{6}(k \cdot (2 \cdot k + 1) + 6 \cdot (k+1)) \\
&= \frac{k+1}{6}(2 \cdot k^2 + k + 6 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 7 \cdot k + 6)
\end{aligned}
$$

Induction proof (contd.)

Proof.

$$
\begin{aligned}
&= \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6} + (k+1)^2, \text{ using the inductive hypothesis} \\
&= \frac{k+1}{6}(k \cdot (2 \cdot k + 1) + 6 \cdot (k+1)) \\
&= \frac{k+1}{6}(2 \cdot k^2 + k + 6 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 7 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 4 \cdot k + 3 \cdot k + 6)
\end{aligned}
$$

Induction proof (contd.)

Proof.

$$
\begin{aligned}
&= \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6} + (k+1)^2, \text{ using the inductive hypothesis} \\
&= \frac{k+1}{6}(k \cdot (2 \cdot k + 1) + 6 \cdot (k+1)) \\
&= \frac{k+1}{6}(2 \cdot k^2 + k + 6 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 7 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 4 \cdot k + 3 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k \cdot (k+2) + 3 \cdot (k+2))
\end{aligned}
$$

Induction proof (contd.)

Proof.

$$
\begin{aligned}
&= \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6} + (k+1)^2, \text{ using the inductive hypothesis} \\
&= \frac{k+1}{6}(k \cdot (2 \cdot k + 1) + 6 \cdot (k+1)) \\
&= \frac{k+1}{6}(2 \cdot k^2 + k + 6 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 7 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 4 \cdot k + 3 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k \cdot (k+2) + 3 \cdot (k+2)) \\
&= \frac{k+1}{6}(2 \cdot k + 3) \cdot (k+2))
\end{aligned}
$$

Induction proof (contd.)

Proof.

$$
\begin{aligned}
&= \frac{k \cdot (k+1) \cdot (2 \cdot k + 1)}{6} + (k+1)^2, \text{ using the inductive hypothesis} \\
&= \frac{k+1}{6}(k \cdot (2 \cdot k + 1) + 6 \cdot (k+1)) \\
&= \frac{k+1}{6}(2 \cdot k^2 + k + 6 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 7 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k^2 + 4 \cdot k + 3 \cdot k + 6) \\
&= \frac{k+1}{6}(2 \cdot k \cdot (k+2) + 3 \cdot (k+2)) \\
&= \frac{k+1}{6}(2 \cdot k + 3) \cdot (k+2))
\end{aligned}
$$

□

Induction Proof (contd.)

Induction Proof (contd.)

Proof.

Induction Proof (contd.)

Proof.

$$= \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$$

Induction Proof (contd.)

Proof.

$$= \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6}$$

$$= RHS.$$

Induction Proof (contd.)

Proof.

$$\begin{aligned} &= \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6} \\ &= RHS. \end{aligned}$$

Since, $LHS{=}RHS$, we have shown that $P(k) \rightarrow P(k+1)$.

Induction Proof (contd.)

Proof.

$$\begin{aligned} &= \frac{(k+1)\cdot(k+2)\cdot(2\cdot(k+1)+1)}{6} \\ &= RHS. \end{aligned}$$

Since, $LHS{=}RHS$, we have shown that $P(k) \rightarrow P(k+1)$.
Applying the first principle of mathematical induction, we conclude that the conjecture is true. □

Induction Example

Induction Example

Example

Induction Example

Example

Show that the sum of the first n odd integers is n^2,

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$LHS \quad =$$

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$LHS = \sum_{i=1}^{1}(2 \cdot i - 1)$$

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1}(2 \cdot i - 1) \\ &= 2 \cdot 1 - 1 \end{aligned}$$

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1}(2 \cdot i - 1) \\ &= 2 \cdot 1 - 1 \\ &= 1 \end{aligned}$$

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1}(2 \cdot i - 1) \\ &= 2 \cdot 1 - 1 \\ &= 1 \\ RHS &= 1^2 \end{aligned}$$

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1}(2 \cdot i - 1) \\ &= 2 \cdot 1 - 1 \\ &= 1 \\ RHS &= 1^2 \\ &= 1 \end{aligned}$$

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1}(2 \cdot i - 1) \\ &= 2 \cdot 1 - 1 \\ &= 1 \\ RHS &= 1^2 \\ &= 1 \end{aligned}$$

Induction Example

Example

Show that the sum of the first n odd integers is n^2, i.e., show that $\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$.

Proof.

Basis ($P(1)$):

$$\begin{aligned} LHS &= \sum_{i=1}^{1}(2 \cdot i - 1) \\ &= 2 \cdot 1 - 1 \\ &= 1 \\ RHS &= 1^2 \\ &= 1 \end{aligned}$$

Thus, $LHS = RHS$ and $P(1)$ is true. □

Proof (contd.)

Proof (contd.)

Proof.

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k}(2 \cdot i - 1) =$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k}(2 \cdot i - 1) = k^2$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k}(2 \cdot i - 1) = k^2$$

We need to show that $P(k+1)$ is true,

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k}(2 \cdot i - 1) = k^2$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1}(2 \cdot i - 1) = (k+1)^2$.

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that

$$\sum_{i=1}^{k}(2 \cdot i - 1) = k^2$$

We need to show that $P(k+1)$ is true, i.e., we need to show that $\sum_{i=1}^{k+1}(2 \cdot i - 1) = (k+1)^2$.

□

Completing the proof

Completing the proof

Proof.

Completing the proof

Proof.

Completing the proof

Proof.

$$LHS \quad =$$

Completing the proof

Proof.

$$LHS = \sum_{i=1}^{k+1} (2 \cdot i - 1)$$

Completing the proof

Proof.

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\ &= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \end{aligned}$$

Completing the proof

Proof.

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\ &= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \\ &= (1 + 3 + 5 + \ldots (2 \cdot k - 1)) + (2 \cdot k + 1) \end{aligned}$$

Completing the proof

Proof.

$$
\begin{aligned}
LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\
&= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \\
&= (1 + 3 + 5 + \ldots (2 \cdot k - 1)) + (2 \cdot k + 1) \\
&= k^2 + (2 \cdot k + 1), \text{ using the inductive hypothesis}
\end{aligned}
$$

Completing the proof

Proof.

$$
\begin{aligned}
LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\
&= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \\
&= (1 + 3 + 5 + \ldots (2 \cdot k - 1)) + (2 \cdot k + 1) \\
&= k^2 + (2 \cdot k + 1), \text{ using the inductive hypothesis} \\
&= (k+1)^2
\end{aligned}
$$

Completing the proof

Proof.

$$
\begin{aligned}
LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\
&= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \\
&= (1 + 3 + 5 + \ldots (2 \cdot k - 1)) + (2 \cdot k + 1) \\
&= k^2 + (2 \cdot k + 1), \text{ using the inductive hypothesis} \\
&= (k+1)^2 \\
&= RHS
\end{aligned}
$$

Completing the proof

Proof.

$$
\begin{aligned}
LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\
&= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \\
&= (1 + 3 + 5 + \ldots (2 \cdot k - 1)) + (2 \cdot k + 1) \\
&= k^2 + (2 \cdot k + 1), \text{ using the inductive hypothesis} \\
&= (k+1)^2 \\
&= RHS
\end{aligned}
$$

Completing the proof

Proof.

$$
\begin{aligned}
LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\
&= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \\
&= (1 + 3 + 5 + \ldots (2 \cdot k - 1)) + (2 \cdot k + 1) \\
&= k^2 + (2 \cdot k + 1), \text{ using the inductive hypothesis} \\
&= (k+1)^2 \\
&= RHS
\end{aligned}
$$

Since $LHS = RHS$, we have shown that $P(k) \rightarrow P(k+1)$.

Completing the proof

Proof.

$$\begin{aligned} LHS &= \sum_{i=1}^{k+1}(2 \cdot i - 1) \\ &= 1 + 3 + 5 + \ldots (2 \cdot k - 1) + (2 \cdot (k+1) - 1) \\ &= (1 + 3 + 5 + \ldots (2 \cdot k - 1)) + (2 \cdot k + 1) \\ &= k^2 + (2 \cdot k + 1), \text{ using the inductive hypothesis} \\ &= (k+1)^2 \\ &= RHS \end{aligned}$$

Since $LHS = RHS$, we have shown that $P(k) \rightarrow P(k+1)$. Applying the first principle of mathematical induction, we conclude that the conjecture is true. □

One Final Example

One Final Example

Example

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$,

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

Basis ($P(0)$):

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

Basis ($P(0)$):

$$LHS \quad =$$

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

Basis ($P(0)$):

$$LHS \quad = \quad 7^0 - 5^0$$

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

Basis ($P(0)$):

$$\begin{aligned} LHS &= 7^0 - 5^0 \\ &= 1 - 1 \end{aligned}$$

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

Basis ($P(0)$):

$$\begin{aligned} LHS &= 7^0 - 5^0 \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

Basis ($P(0)$):

$$\begin{aligned} LHS &= 7^0 - 5^0 \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

One Final Example

Example

Show that $7^n - 5^n$ is always an even number for $n \geq 0$, i.e., show that $2 \mid (7^n - 5^n)$, $\forall n \geq 0$.

Proof.

Basis ($P(0)$):

$$\begin{aligned} LHS &= 7^0 - 5^0 \\ &= 1 - 1 \\ &= 0 \end{aligned}$$

Since the LHS is even, we have proven the basis $P(0)$.

□

Proof (contd.)

Proof (contd.)

Proof.

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e.,

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k. It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true,

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$7^{k+1} - 5^{k+1} \quad =$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$7^{k+1} - 5^{k+1} \quad = \quad 7 \cdot 7^k - 5 \cdot 5^k$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned} 7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\ &= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \end{aligned}$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned} 7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\ &= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \\ &= 14 \cdot m + 7 \cdot 5^k - 5 \cdot 5^k \end{aligned}$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned} 7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\ &= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \\ &= 14 \cdot m + 7 \cdot 5^k - 5 \cdot 5^k \\ &= 14 \cdot m + 5^k \cdot (7 - 5) \end{aligned}$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned} 7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\ &= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \\ &= 14 \cdot m + 7 \cdot 5^k - 5 \cdot 5^k \\ &= 14 \cdot m + 5^k \cdot (7 - 5) \\ &= 14 \cdot m + 2 \cdot 5^k \end{aligned}$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned} 7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\ &= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \\ &= 14 \cdot m + 7 \cdot 5^k - 5 \cdot 5^k \\ &= 14 \cdot m + 5^k \cdot (7 - 5) \\ &= 14 \cdot m + 2 \cdot 5^k \\ &= 2 \cdot (7 \cdot m + 5^k) \end{aligned}$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned}
7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\
&= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \\
&= 14 \cdot m + 7 \cdot 5^k - 5 \cdot 5^k \\
&= 14 \cdot m + 5^k \cdot (7 - 5) \\
&= 14 \cdot m + 2 \cdot 5^k \\
&= 2 \cdot (7 \cdot m + 5^k) \\
&= \text{some even number!}
\end{aligned}$$

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned}
7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\
&= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \\
&= 14 \cdot m + 7 \cdot 5^k - 5 \cdot 5^k \\
&= 14 \cdot m + 5^k \cdot (7 - 5) \\
&= 14 \cdot m + 2 \cdot 5^k \\
&= 2 \cdot (7 \cdot m + 5^k) \\
&= \text{some even number!}
\end{aligned}$$

We have thus shown that $P(k) \rightarrow P(k+1)$.

Proof (contd.)

Proof.

Let us assume that $P(k)$ is true, i.e., assume that $(7^k - 5^k)$ is divisible by 2 for some k.

It follows that $(7^k - 5^k) = 2 \cdot m$, for some integer m.

We need to show that $P(k+1)$ is true, i.e., $(7^{k+1} - 5^{k+1})$ is divisible by 2.

Observe that,

$$\begin{aligned}
7^{k+1} - 5^{k+1} &= 7 \cdot 7^k - 5 \cdot 5^k \\
&= 7 \cdot (2 \cdot m + 5^k) - 5 \cdot 5^k, \text{ using the inductive hypothesis} \\
&= 14 \cdot m + 7 \cdot 5^k - 5 \cdot 5^k \\
&= 14 \cdot m + 5^k \cdot (7 - 5) \\
&= 14 \cdot m + 2 \cdot 5^k \\
&= 2 \cdot (7 \cdot m + 5^k) \\
&= \text{some even number!}
\end{aligned}$$

We have thus shown that $P(k) \rightarrow P(k+1)$. Applying the first principle of mathematical induction, we conclude that the conjecture is true.

□

Second Principle of Induction

Second Principle of Induction

Principle

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

(i) $P(1)$ is **true**, and

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

(i) $P(1)$ is **true**, and

(ii) $(\forall r)(1 \leq r \leq k)[P(r) \text{ is } \textbf{true}] \rightarrow P(k+1) \text{ is } \textbf{true}]$

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

(i) $P(1)$ is **true**, and

(ii) $(\forall r)(1 \leq r \leq k)[P(r) \text{ is } \textbf{true}] \rightarrow P(k+1) \text{ is } \textbf{true}]$

then,

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

(i) $P(1)$ is **true**, and

(ii) $(\forall r)(1 \leq r \leq k)[P(r) \text{ is } \textbf{true}] \rightarrow P(k+1) \text{ is } \textbf{true}]$

then,

$P(n)$ is **true** for all n.

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

(i) $P(1)$ is **true**, and

(ii) $(\forall r)(1 \leq r \leq k)[P(r) \text{ is } \textbf{true}] \rightarrow P(k+1) \text{ is } \textbf{true}]$

then,

$P(n)$ is **true** for all n.

Note

Second Principle of Induction

Principle

Assume that the domain is the set of positive integers.

Let $P(n)$ denote a conjecture which we want to prove holds for every $n \geq 1$.

If

(i) $P(1)$ is **true**, and

(ii) $(\forall r)(1 \leq r \leq k)[P(r) \text{ is } \textbf{true}] \rightarrow P(k+1) \text{ is } \textbf{true}]$

then,

$P(n)$ is **true** for all n.

Note

Also called Strong Induction. Is necessary, when the first principle does not help us.

Example of Strong Induction

Example of Strong Induction

Example

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k + 1)$.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k + 1)$.

(iv) Without loss of generality, we assume that $(k + 1) \geq 11$.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k+1)$.

(iv) Without loss of generality, we assume that $(k+1) \geq 11$.

(v) Observe that $(k+1) - 3 = (k-2)$ is at least 8 and less than k.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k+1)$.

(iv) Without loss of generality, we assume that $(k+1) \geq 11$.

(v) Observe that $(k+1) - 3 = (k-2)$ is at least 8 and less than k.

(vi) As per the inductive hypothesis, $(k-2)$ can be expressed in the form $3 \cdot a + 5 \cdot b$, for suitably chosen a and b.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k+1)$.

(iv) Without loss of generality, we assume that $(k+1) \geq 11$.

(v) Observe that $(k+1) - 3 = (k-2)$ is at least 8 and less than k.

(vi) As per the inductive hypothesis, $(k-2)$ can be expressed in the form $3 \cdot a + 5 \cdot b$, for suitably chosen a and b.

(vii) It follows that $(k+1) =$

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k+1)$.

(iv) Without loss of generality, we assume that $(k+1) \geq 11$.

(v) Observe that $(k+1) - 3 = (k-2)$ is at least 8 and less than k.

(vi) As per the inductive hypothesis, $(k-2)$ can be expressed in the form $3 \cdot a + 5 \cdot b$, for suitably chosen a and b.

(vii) It follows that $(k+1) = (k-2) + 3 =$

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k+1)$.

(iv) Without loss of generality, we assume that $(k+1) \geq 11$.

(v) Observe that $(k+1) - 3 = (k-2)$ is at least 8 and less than k.

(vi) As per the inductive hypothesis, $(k-2)$ can be expressed in the form $3 \cdot a + 5 \cdot b$, for suitably chosen a and b.

(vii) It follows that $(k+1) = (k-2) + 3 = 3 \cdot a + 5 \cdot b + 3 =$

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k+1)$.

(iv) Without loss of generality, we assume that $(k+1) \geq 11$.

(v) Observe that $(k+1) - 3 = (k-2)$ is at least 8 and less than k.

(vi) As per the inductive hypothesis, $(k-2)$ can be expressed in the form $3 \cdot a + 5 \cdot b$, for suitably chosen a and b.

(vii) It follows that $(k+1) = (k-2) + 3 = 3 \cdot a + 5 \cdot b + 3 = 3 \cdot (a+1) + 5 \cdot b$ can also be so expressed.

Example of Strong Induction

Example

Show that every number greater than or equal to 8 can be expressed in the form $5 \cdot a + 3 \cdot b$, for suitably chosen a and b.

Proof.

(i) The conjecture is clearly true for 8, 9 and 10.

(ii) Assume that the conjecture holds for all r, $8 \leq r \leq k$.

(iii) Consider the integer $(k+1)$.

(iv) Without loss of generality, we assume that $(k+1) \geq 11$.

(v) Observe that $(k+1) - 3 = (k-2)$ is at least 8 and less than k.

(vi) As per the inductive hypothesis, $(k-2)$ can be expressed in the form $3 \cdot a + 5 \cdot b$, for suitably chosen a and b.

(vii) It follows that $(k+1) = (k-2) + 3 = 3 \cdot a + 5 \cdot b + 3 = 3 \cdot (a+1) + 5 \cdot b$ can also be so expressed.

(viii) Applying the second principle of mathematical induction, we conclude that the conjecture is true, for all $n \geq 8$.

□

Another Example

Another Example

Example

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.
3. Now consider the number $(k + 1)$.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.
3. Now consider the number $(k + 1)$. If $(k + 1)$ is a prime, then

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.
3. Now consider the number $(k + 1)$. If $(k + 1)$ is a prime, then we are done.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.
3. Now consider the number $(k + 1)$. If $(k + 1)$ is a prime, then we are done.
4. If $(k + 1)$ is composite, then $(k + 1) = a \cdot b$, where $a, b < (k + 1)$.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.
3. Now consider the number $(k + 1)$. If $(k + 1)$ is a prime, then we are done.
4. If $(k + 1)$ is composite, then $(k + 1) = a \cdot b$, where $a, b < (k + 1)$.
5. As per the inductive hypothesis, both a and b are either primes themselves or can be expressed as products of primes.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.
3. Now consider the number $(k + 1)$. If $(k + 1)$ is a prime, then we are done.
4. If $(k + 1)$ is composite, then $(k + 1) = a \cdot b$, where $a, b < (k + 1)$.
5. As per the inductive hypothesis, both a and b are either primes themselves or can be expressed as products of primes.
6. In either case, it follows that $(k + 1)$ can be expressed as a product of primes.

Another Example

Example

Show that every element in the set $S = \{2, 3, \ldots, \}$ is either a prime number or a product of primes.

Proof.

1. For the basis, observe that 2 is a prime.
2. Assume that the conjecture holds for all r, $2 \leq r \leq k$.

   In other words, assume that every number in the set $S_k = \{2, 3, \ldots, k\}$ is either a prime or can be expressed as a product of primes.
3. Now consider the number $(k + 1)$. If $(k + 1)$ is a prime, then we are done.
4. If $(k + 1)$ is composite, then $(k + 1) = a \cdot b$, where $a, b < (k + 1)$.
5. As per the inductive hypothesis, both a and b are either primes themselves or can be expressed as products of primes.
6. In either case, it follows that $(k + 1)$ can be expressed as a product of primes.
7. Applying the second principle of mathematical induction, we conclude that the conjecture is true for all elements in the domain.

□