CS0001

Discrete Structures 1

Module 4: Formal Proof Techniques

OBJECTIVE:

By the end of this module, you will be able to:

- **Distinguish** between different types of mathematical statements, such as theorems, axioms, and conjectures.
- **Construct** valid arguments using direct proof techniques.
- **Construct** valid arguments using indirect proof techniques, including proof by contradiction and proof by contraposition.
- **Apply** the principle of mathematical induction to prove statements about sequences and summations.

CS0001

Discrete Structures 1

Subtopic 1: Terminologies in Proving

RECAP OF TERMINOLOGIES

Proposition:

is a declarative statement that is either true or false but cannot be both.

In an implication:

$\mathbf{p \rightarrow q}$

p is referred to as **antecedent** or **hypothesis**

q is referred to as **consequent** or **conclusion**

RECAP OF TERMINOLOGIES

Hypothesis/Antecedent:

is the first part of a conditional statement, typically following the word "if." It represents the condition or assumption that leads to the conclusion.

Conclusion/Consequent:

is the second part of a conditional statement, typically following the word "then." It represents the outcome or result that follows from the hypothesis being true. In logical terms, it's the "effect" or consequence of the initial condition.

RECAP OF TERMINOLOGIES

1. $(-A \vee -B) \rightarrow (C \wedge D)$
2. $C \rightarrow E$
3. $-E$

These are **premises**.

$\therefore A$

This is the **conclusion**.

This is called an **argument**.

RECAP OF TERMINOLOGIES

Premise:
These are the statements or propositions that offer reasons or evidence. They are the foundation upon which the argument is built.

Conclusion:
This is the statement or proposition that the premises are intended to support or prove.

Argument:
in logic and philosophy is a set of statements or propositions, where some of the statements (called **premises**) are intended to provide support or reasons for accepting another statement (called the **conclusion**).

TERMINOLOGIES IN PROVING

What are the differences?

- Theorem
- Axioms / Postulates
- Conjecture
- Lemma
- Corollary

TERMINOLOGIES IN PROVING

Theorem

is a statement that can be shown to be true.

A **theorem** may be the **universal quantification of a conditional statement** with one or more premises and a conclusion.

A **proof** is a valid argument that establishes the truth of the theorem.

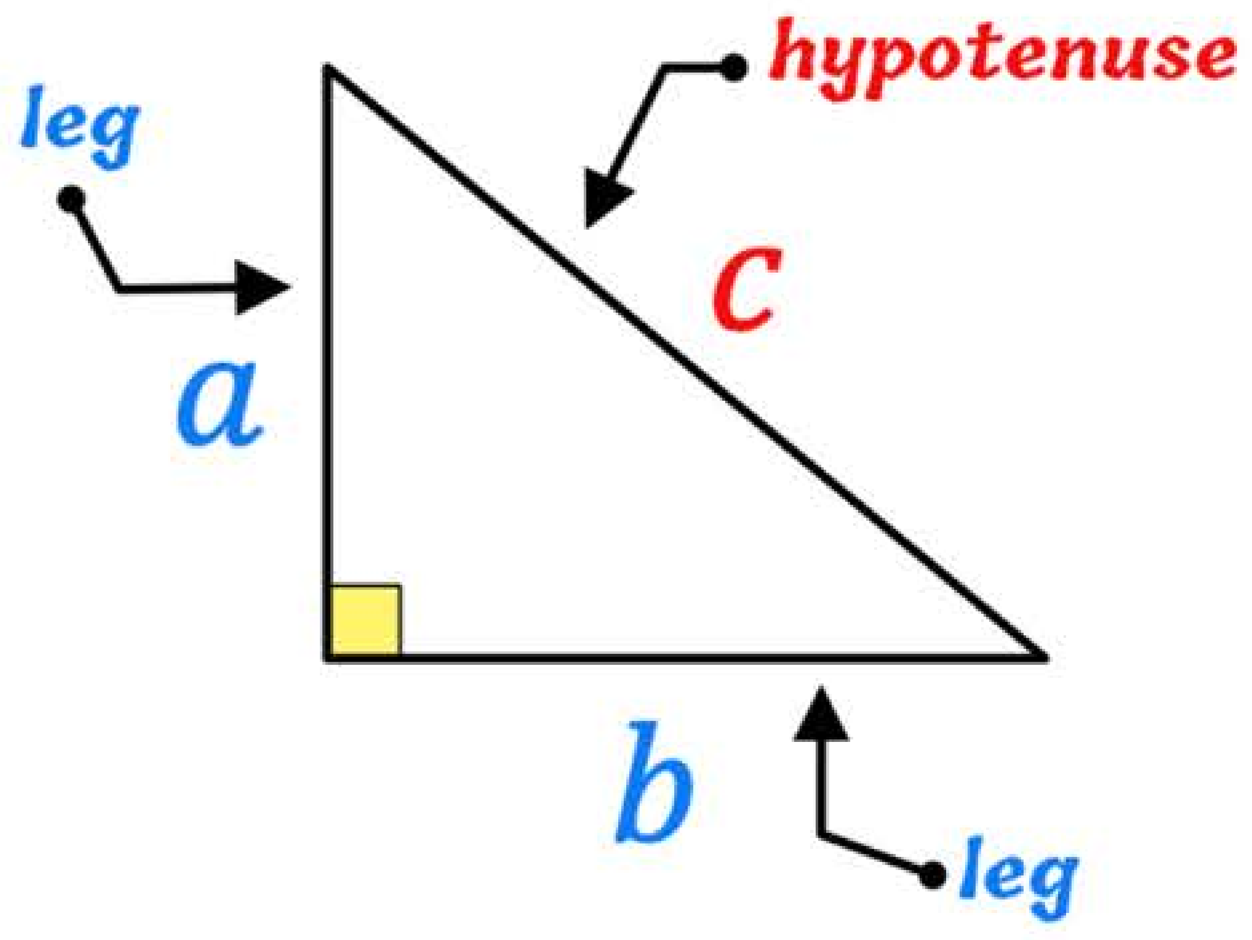
TERMINOLOGIES IN PROVING

Pythagorean Theorem

states that in a right triangle, the square of the length of the hypotenuse is equal to the sum of the squares of the lengths of the other two sides.

This theorem can be demonstrated through geometric proofs or algebraic methods.

PYTHAGOREAN THEOREM



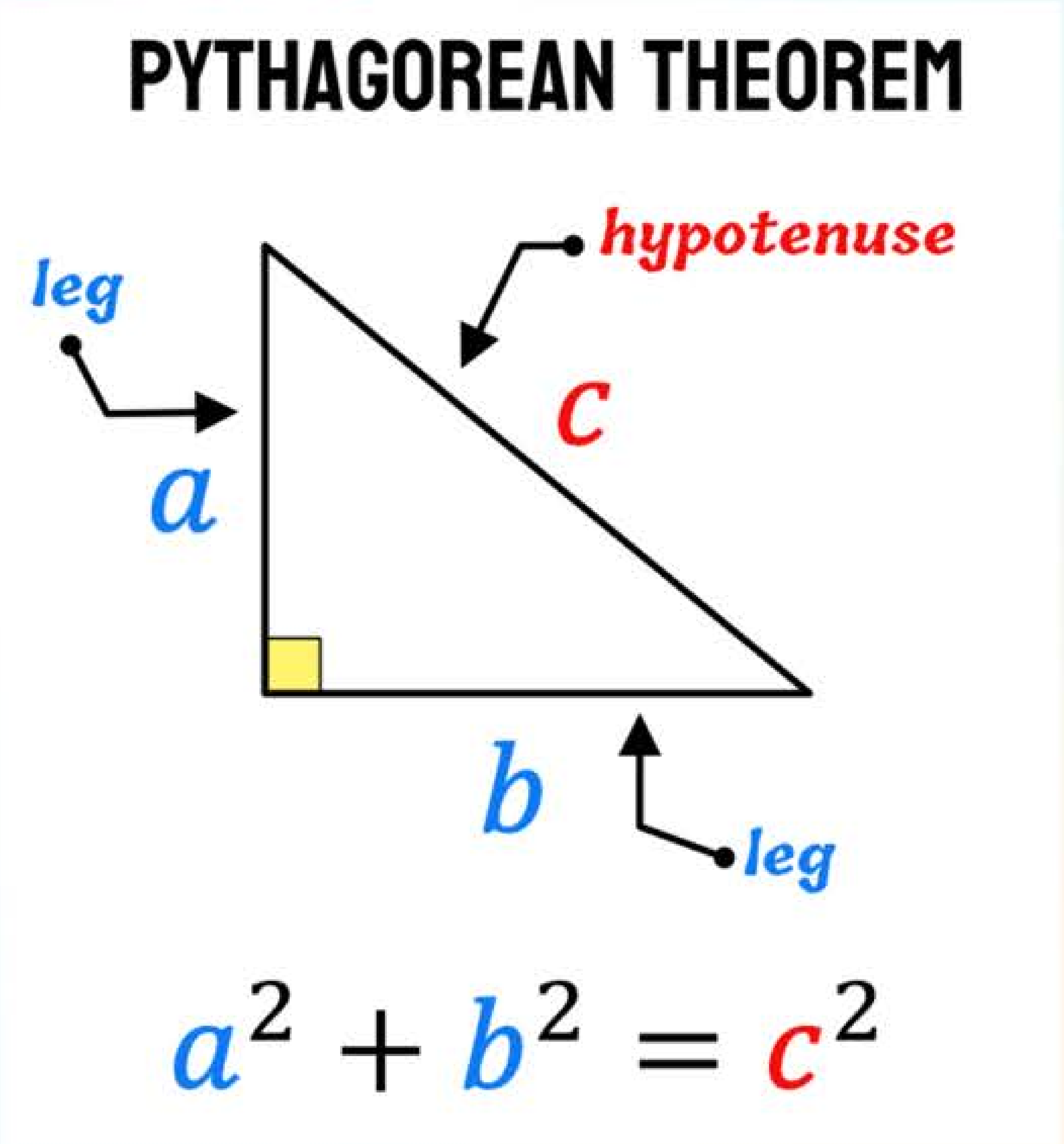
$$a^2 + b^2 = c^2$$

TERMINOLOGIES IN PROVING

Pythagorean Theorem

$\forall$a,b,c((a,b,c are lengths of a right triangle)$\rightarrow$($a^2+b^2=c^2$))

$\forall$ triangles T (if T is a right triangle, then (a,b,c) such that $a^2+ b^2= c^2$)



TERMINOLOGIES IN PROVING

Arguments:

1. (-A ∨ -B) -> (C ∧ D)
2. C -> E
3. -E

$\boxed{\therefore\ A}$

Solution:

(4) -C (2, 3, MT)
(5) -C V -D (4, A)
(6) -(C ∧ D) (5, DML)
(7) - (-A ∨ -B) (1,6, MT)
(8) (A ∧ B) (7, DML)
$\boxed{\text{(9) A (8, S)}}$

Rules of inference is used to draw conclusions from other assertions, trying together the steps of a proof.

The final step of a proof, is the conclusion of the theorem.

TERMINOLOGIES IN PROVING

Some forms of theorem are:

Lemma

A less important theorem that is helpful in the proof of other results. Can be defined as a theorem to prove other theorems. Sometimes called, “mini theorem”.

Corollary

A theorem that trivially follows another theorem. It is also defined as a proposition that can be proved as a consequence of a theorem that has just been proved.

TERMINOLOGIES IN PROVING

Axioms/Postulates

is a statement or proposition that is accepted as true without proof.

Axioms serve as foundational building blocks for a particular mathematical system or theory. They are self-evident truths or assumptions that do not require justification.

Example: Axiom of Identity: For any proposition P, it is true that P is equivalent to itself. $P \equiv P$

TERMINOLOGIES IN PROVING

Conjecture

is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

If the proof of a conjecture is found, **then it becomes a theorem**.

TERMINOLOGIES IN PROVING

Conjecture

Goldbach's Conjecture:
Every every **even natural number** greater than 2 can be expressed as the **sum of two prime numbers**.

Example:

- 8 can be expressed as 3 + 5 (both are prime nos.)
- 12 = 5 + 7
- 24 = 11 + 13

CS0001

Discrete Structures 1

Subtopic 2: Direct vs. Indirect Proof

PROVING THEOREMS

In the realm of mathematical proofs, there are: **direct proof** and **indirect proof (proof by contradiction)**.

A type of indirect proof is Proof by Contraposition (Contrapositive).

There exists, other proof methods:

- Proof of Equivalence
- Proof by Cases (Exhaustion/Case Analysis)
- Proof by Induction (Principle of Mathematical Induction)

DIRECT PROOF

A **direct proof** involves starting with given facts and using logical steps to straightforwardly establish the truth of a statement.

In direct proof, it shows that the conditional statement **$p \rightarrow q$ is true**, by showing that if p is true, then q must also be true.

DIRECT PROOF

If there exists an integer k such that **n = 2k,** then n is even an **even number**.

n is **odd** if there exists an integer k such that **n = 2k + 1**.

Even numbers can be written as **n = 2k**, where k is an integer. These are numbers divisible by 2 without any remainder.

Odd numbers can be written as **n = 2k + 1**, where k is an integer. These are numbers that leave a remainder of 1 when divided by 2.

DIRECT PROOF

Give a direct proof to the theorem, "**If n is an odd integer, then n^2 is odd.**"

This states that $\forall$ **nP((n) → Q(n))**, where P(n) is **"n is an odd integer"**, and Q(n) is **"n^2 is also an odd integer"**.

Example:
$n = 3$, 3 is an odd integer.
$n^2 = 9$, 9 is also an odd integer.

DIRECT PROOF

Earlier, we defined odd as **n is odd if there exists an integer k such that n = 2k + 1**.

Therefore, using **direct proof**:

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

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

$4k^2 + 2k + 1$ can also be expressed as $\mathbf{2(2k^2 + k) + 1}$.

We can say assume that $m = (2k^2 + k)$.
So **2m + 1** is also an **odd number**.

DIRECT PROOF

Theorem: If a and b are even integers, then a + b is also an even integer. Prove this using Direct Proof.

Direct Proof:

Let $a = 2k$ and $b = 2m$, where k and m are integers. These equations define a and b as even integers.

Now, consider the sum a + b:
$a + b = 2k + 2m$
Which can be written as $\mathbf{2(k + m)}$.

Let $n = k + m$, so $2(k + m)$ can be expressed as $\mathbf{2n}$.

Hence, **a + b is also an even integer** if a and b are even integers

DIRECT PROOF

Theorem: If x is an odd integer, then $y = x^2 + 3$ is even. Prove this using Direct Proof.

We can express x as **2k + 1** to indicate that it is an odd integer.

Thus, $y = x^2 + 3$ can be written as:

$$\mathbf{y = (2k + 1)^2 + 3}$$
$$= (4k^2 + 4k + 1) + 3$$
$$= 4k^2 + 4k + 4$$
$$= 4(k^2 + k + 1)$$
$$= 4(m)$$

4m is even.

Let $m = k^2 + k + 1$

Hence, $x^2 + 3$ is even.

TABLE GUIDE

Sample Mathematical Expression	Equivalent
$y = 2k$	**y is an even number**
$y = 2k + 1$ $y = k + k + 1$	**y is an odd number**
$y = (2k+1)^2$	**y is the square of an odd number** **y is an odd number**
$y = 4k$	**y is divisible by 4** **y is an even number**

*** this non-exhaustive list**

TABLE GUIDE

Sample Mathematical Expression	Equivalent
$y = 2k$	y is an even number
$y = 2k + 1$ $y = k + k + 1$	y is an odd number y is the square of an odd number
$y = (2k+1)^2$	y is an odd number y is divisible by 4
$y = 4k$	y is an even number

Given the table guide, analyze if they are odd or even:

- $4k + 2$
- $2k + 3$
- $(2k+1)^3$
- $6k + 6$
- $(2k+1)^4 + 3$
- $2k - 3$

TABLE GUIDE

Sample Mathematical Expression	Equivalent
$y = 2k$	**y is an even number**
$y = 2k + 1$ $y = k + k + 1$	**y is an odd number** **y is the square of an odd number**
$y = (2k+1)^2$	**y is an odd number** **y is divisible by 4**
$y = 4k$	**y is an even number**

Given the table guide, analyze if they are odd or even:

- $4k + 2$ **EVEN**
- $2k + 3$ **ODD**
- $(2k+1)^3$ **ODD**
- $6k + 6$ **EVEN**
- $(2k+1)^4 + 3$ **EVEN**
- $2k - 3$ **ODD**

CHALLENGE

Prove the following using direct proof:

1. If a is an even integer, then $b = 2a + 1$ is odd.
2. If m is even and n is odd, then the product mn is even.
3. If x is an even integer, then x^3 is even

INDIRECT PROOF

Conversely, in an **indirect proof**, one assumes the negation of what they aim to prove and demonstrates that this assumption leads to a contradiction, hence affirming the original statement's truth.

It is also called as **Proof by Contradiction**.

Example:

Theorem: If p is even, then 7p - 3 is odd.
Prove using **indirect proof**.

In indirect proof, we can use **T → F = F** (true implies false is false).

INDIRECT PROOF

Theorem: If p is even, then 7p - 3 is odd.

Assumption: Assume p is even and 7p - 3 is even

If our assumption leads to a logical contradiction, then our original theorem must be true.

Proof:

1. Assume the theorem is false. This means we assume the hypothesis is true AND the conclusion is false.
2. Assumption: Assume p is an even integer AND 7p - 3 is an even integer.
3. By definition of even integers, we can write **p = 2k** and **7p - 3 = 2m** for some integers k and m.
4. Now, we substitute 2k for p into the second equation:

$$\mathbf{7(2k) - 3 = 2m}$$

INDIRECT PROOF

Proof (cont.):

Using algebra, we try to find a contradiction:

$$\underline{14k - 3 = 2m}$$
$$\underline{14k - 2m = 3}$$
$$\underline{2(7k - m) = 3}$$

Let **j = 7k - m.** Since k and m are integers, j is also an integer.
The equation becomes **2j = 3**.

Contradiction: This statement, 2j = 3, asserts that 3 is an even number, which is a logical contradiction.

Conclusion: Because our **assumption led to a contradiction**, the assumption must be false.

Therefore, the original theorem, "If p is even, then 7p - 3 is odd," must be true.

CHALLENGE

Prove the following using indirect proof:

1. For any integers a and b, if the product ab is even, then a is even or b is even.

PROOF BY CONTRAPOSITION

Proof by contraposition is also a useful type of indirect proof.

We will make use of the fact that **($p \rightarrow q$) will always be logically equivalent to its contrapositive ($\neg q \rightarrow \neg p$)**.

A proof by contraposition for $p \rightarrow q$ is actually a direct proof for $\neg q \rightarrow \neg p$.

It starts by assuming $\neg q$, and finishes by establishing $\neg p$.

PROOF BY CONTRAPOSITION

Example: Prove that if $3n + 2$ is odd, then n is odd using **contraposition**.

By contraposition, it will be:

If n is even, then 3n + 2 is even

$3n + 2$

$= 3(2k) + 2$

$= 6k + 2$

$= 2(3k + 1)$

$\mathbf{= 2m}$

We can represent n as 2k (even).

Let $m = 3k + 1$

Hence, 3n + 2 is even

PROOF BY CONTRAPOSITION

Example: Prove that if x is an odd integer, then $y = x^2 + 3$ is even using **contraposition**.

By contraposition, it will be:

If $y = x^2 + 3$ is odd, then x is an even integer.

$y = x^2 + 3, x = 2k$
$= (2k)^2 + 3$
$= 4k^2 + 3$

Hence, $4k^2 + 3$ is odd.

CS0001

Discrete Structures 1

Subtopic 3: Principle of Mathematical Induction

PROOF BY INDUCTION

Mathematical induction is a technique often used to prove statements about **sequences** or **patterns**, where one first demonstrates the statement holds for a **base case** and then shows that if it holds for any given value, it also holds for the next, thereby proving its validity for all values.

PROOF BY INDUCTION

The primary purpose of mathematical induction is to prove that a statement holds for all natural numbers (or some subset of natural numbers). This is typically done by following two main steps:

Base Case: The first step is to prove that the statement holds true for the smallest value in the domain (usually $n = 0$ or $n = 1$ depending on the context). This is often referred to as the base case.

Inductive Step: The second step is to prove that assuming the statement holds for some arbitrary natural number k (this is called the induction hypothesis), then the statement also holds for the next natural number, $k+1$.

PROOF BY INDUCTION

Claim: $1 + 3 + 5 + \ldots + (2n-1) = n^2$

We start with the base case. This is usually 0 or 1 if not specified. Start with some examples below to make sure you believe the claim.

PROOF BY INDUCTION

Claim: $1 + 3 + 5 + \ldots + (2n-1) = n^2$

Step 1: Result is true for n = 1

That is $2(1)-1 = (1)^2$

$1 = 1$ (True)

Step 2: Assume that result is true for n = k

$1 + 3 + 5 + \ldots + (2k-1) = k^2$

Step 3: Check for n = k + 1

$1 + 3 + 5 + \ldots + (2\mathbf{(k+1)}-1) = \mathbf{(k+1)}^2$

WHY? Assume the equality

i.e. $1 + 3 + 5 + \ldots + (2k-1) = k^2$

assuming this

is equal to this

Step 4: Simplify the equation

$\mathbf{k^2} + (2(k+1)-1) = (k+1)^2$

Step 5: Perform the operation

$k^2 + 2k + 2 - 1 = (k+1)^2$

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

$\mathbf{(k+1)^2 = (k+1)^2}$

PROOF BY INDUCTION

Prove that $2+4+6+.... + 2n = n(n + 1)$

Step 1: Result is true for n = 1

$2n = n(n + 1)$

$2(1) = (1)(1 + 1)$

$2 = 2$

Step 2: Assume that result is true for n = k

$2+4+6+.... + 2k = k(k + 1)$

Step 3: Check for n = k + 1

$2+4+6+.... + 2(k+1) = (k + 1)((k + 1) + 1)$

Step 4: Simplify the equation

$(k(k + 1)) + 2(k+1) = (k+1)(k+2)$

Step 5: Perform the operation

$(k(k + 1)) + 2(k+1) = (k+1)(k+2)$

$k^2 + k + 2k + 2 = k^2 + k + 2k + 2$

$k^2 + 3k + 2 = k^2 + 3k + 2$

KEY TAKEAWAYS

- A proof is a valid argument that rigorously establishes the truth of a theorem.
- Direct Proofs assume the hypothesis is true and work forward to the conclusion.
- Indirect Proofs (Contradiction and Contraposition) assume the conclusion is false and show that this leads to an impossible result.
- Mathematical Induction is a powerful technique for proving that a statement is true for all positive integers.

Ready for the Summative Test 2?

CS0001

Discrete Structures 1

END OF MODULE

REFERENCES

Chartrand, G., Zhang, P., & Polimeni, A. (2013). Mathematical Proofs: A Transition to Advanced Mathematics (3rd ed.). Pearson.

Goodman, F. M. (1982). Mathematical Induction and Analysis (2nd ed.). Springer.

Grimaldi, R. P. (2003). Discrete and Combinatorial Mathematics: An Applied Introduction (5th ed.). Pearson Education.

Rosen, K. H. (2011). Discrete Mathematics and Its Applications (7th ed.). McGraw-Hill Education.

Stewart, I. (2019). Taming the Infinite: The Story of Mathematics from the First Numbers to Chaos Theory . Quercus Publishing Plc.

Velleman, D. J. (2018). How to Prove It: A Structured Approach (3rd ed.). Cambridge University Press.