



National University
of computer and emerging sciences

DISCRETE STRUCTURES

COURSE INSTRUCTOR: MUHAMMAD SAIF UL ISLAM

Course Outline

- **Logic and Proofs** (Chapter 1)
- **Sets and Functions** (Chapter 2)
- **Relations** (Chapter 9)
- **Number Theory** (Chapter 4)
- **Combinatorics** (Chapter 6)
- **Graphs** (Chapter 10)
- **Trees** (Chapter 11)
- Discrete Probability

Lecture Outline

➤ Terminologies

➤ Proving conditional Statements

- Direct Proofs
- Indirect Proofs
 - Proof by Contraposition
 - Proofs by Contradiction

➤ Proving Non-conditional Statements

- Indirect Proofs
- If-And-Only-If Proof
- Disproofs (Counterexample, Contradiction, Existence Statement)

➤ Mathematical Induction

Proofs

A proof is a valid argument that establishes the truth of a mathematical statement.

Ingredients:

- hypotheses of the theorem
- axioms assumed to be true
- previously proven theorems
- rules of inference

Axioms: A statement or proposition which is regarded as being established, accepted, or self-evidently true

You get:
truth of the
statement
being proved

Proofs

Formal proofs

- all steps were supplied
- rules for each step in the argument were given
- **Usefulness:** Automated Reasoning Systems.

Informal Proofs

- more than 1 rule of inference may be used per step
- where steps may be skipped,
- where the axioms being assumed
- rules of inference used are not explicitly stated
- **Usefulness:** Designed For Human Consumption.

Terminology

Axioms are assumed to be true. ('true without needing a proof')

- Axioms may be stated using primitive terms that **do not require definition**, but all other terms used in theorems and their proofs **must be defined**.

Theorem A statement that has been proven by logical arguments based on axioms, is a theorem. We generate a theorem by the way of analysis and proof.

Less important theorems sometimes are called **propositions, facts or results**.

A **conjecture** is a statement that is being proposed to be a true statement.

- If it can be proved, it's a theorem.
- Not a theorem, if it cannot be proved.

Terminology

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

A **lemma** is a small or minor proof needed to support the proof of a **theorem**. (plural *lemmas* or *lemmata*).

A **corollary** is a result or a theorem that is an immediate consequence/result of a theorem or proposition.

A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word or phrase.

e.g: \mathbb{N} , \mathbb{W} , \mathbb{R} , \mathbb{Q} , Φ , ∞ etc.

Definitions

An integer n is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

An integer n is **odd** if $n = 2a+1$ for some integer $a \in \mathbb{Z}$.

Is 5 or 10 even or odd ?

Two integers have the **same parity** if they are both even or they are both odd. Otherwise they have **opposite parity**.

Is 5 and -17 has same parity and what about 3 and 4?

Definitions

Suppose a and b are integers. We say that a **divides** b , written $a|b$, if $b=ac$ for some $c \in \mathbb{Z}$.

a is a **divisor** of b , and that b is a **multiple** of a .

$5|15$, $3|15$, $15|3$, $-6|6$ etc.

The expression $a|b$ is a *statement*, while a/b is a fraction.

For example, $8|16$ is true and $8|20$ is false.

By contrast, $8/16 = 0.5$ and $8/20 = 0.4$ are numbers, not statements.

Definitions

An integer n is **composite** if it factors as $n = ab$ where $a, b > 1$.

The **greatest common divisor** of integers a and b , denoted $\gcd(a, b)$, is the largest integer that divides both a and b and anyone of them must be non-zero.

- $\gcd(18, 24)$, $\gcd(5, 5)$, $\gcd(32, -8)$, $\gcd(50, 18)$
- $\gcd(50, 9) = 1$, $\gcd(0, 6) = 6$, $\gcd(0, 0) = \infty$ why?? , which condition of gcd solves this problem.

The **least common multiple** of non-zero integers a and b , denoted $\text{lcm}(a, b)$, is smallest positive integer that is a multiple of both a and b .

- $\text{lcm}(4, 6) = 12$, and $\text{lcm}(7, 7) = 7$

FACTS

Some statements are accepted without justification.

Fact 4.1 Suppose a and b are integers. Then:

- $a + b \in \mathbb{Z}$
- $a - b \in \mathbb{Z}$
- $ab \in \mathbb{Z}$

These three statements can be combined. For example, we see that if a, b and c are integers, then $a^2b - ca + b$ is also an integer.

Note that we will always MENTION the axioms found in Appendix 1 of Rosen. When you construct your own proofs, be careful NOT to use anything but these axioms, definitions, and previously proved results (BY YOU) as facts!

Types of Proofs

Proving conditional Statements

- Direct Proofs
- Indirect Proofs
 - **Proof by Contraposition**
 - **Proofs by Contradiction**

Proving Non-conditional Statements

- Indirect Proofs
- If-And-Only-If Proof
- Constructive Versus Non-constructive Proofs
- Existence Proofs; Existence and Uniqueness Proofs
- Disproofs (Counterexample, Contradiction, Existence Statement)

Mathematical Induction

Direct Proofs

Definition: The integer n is *even* if there exists an integer k such that $n = 2k$, and n is *odd* if there exists an integer k such that $n = 2k + 1$. (Note that every integer is either even or odd, and no integer is both even and odd.)

Prove that: “If n is an odd integer, then n^2 is odd.”

$P(n)$ is “ n is an odd integer”

$Q(n)$ is “ n^2 is odd.”

$\forall n (P(n) \rightarrow Q(n)) : n \text{ belongs to set of integers}$

We will prove $P(c) \rightarrow Q(c)$ for any arbitrary c

Direct Proofs

We assume that the hypothesis of this conditional statement is true, namely, we assume that *n is odd*.

By the definition of an odd integer, it follows that $n = 2k + 1$, where *k is some integer*.

Square both sides $n^2 = (2k + 1)^2$

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

Consequently, we have proved that if *n is an odd integer*, then n^2 is an odd integer

Prove that: “If x is an even integer, then $x^2 - 6x + 5$ is odd.”

$$\text{So } x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1.$$

Direct Proofs

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

- We assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares.
- By the definition of a perfect square, It follows that there are integers s and t such that $m = s^2$ and $n = t^2$.
- Multiplying both m and n to get s^2t^2 .
- Hence, $mn = s^2t^2 = (ss)(tt) = (st)(st) = (st)^2$, using commutativity and associativity of multiplication.
- By the definition of perfect square, it follows that mn is also a perfect square, because it is the square of st , which is an integer.
- We have proved that if m and n are both perfect squares, then mn is also a perfect square.

If n is an integer and $3n + 2$ is even, then n is even.

If $3n+2$ is even then there is $k \in \mathbb{Z}$ such that $3n+2=2k$

$$n = 2k - 2 - 2n = 2(\underbrace{k - 1 - n}_{\in \mathbb{Z}})$$

Direct Proofs

Proposition Let x and y be positive numbers. If $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$.

Proof. Suppose $x \leq y$. Subtracting y from both sides gives $x - y \leq 0$.

This can be written as $\sqrt{x}^2 - \sqrt{y}^2 \leq 0$.

Factor this to get $(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \leq 0$.

Dividing both sides by the positive number $\sqrt{x} + \sqrt{y}$ produces $\sqrt{x} - \sqrt{y} \leq 0$.

Adding \sqrt{y} to both sides gives $\sqrt{x} \leq \sqrt{y}$. ■

Direct VS Indirect Proofs

Direct proof begin with the premises, continue with a sequence of deductions, and end with the conclusion.

Attempts at direct proofs often reach dead ends

Proofs that **do not** start with the premises and end with the conclusion, are called **indirect proofs**

Indirect Proofs: Proof by Contraposition

$p \rightarrow q$ is equivalent to $\neg q \rightarrow \neg p$

Take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow.

Outline for Contrapositive Proof

Proposition If P , then Q .

Proof. Suppose $\sim Q$.

\vdots

Therefore $\sim P$. ■

Indirect Proofs: Proof by Contraposition

Prove by Contraposition that if n is an integer and $3n + 2$ is odd, then n is odd.

$$p \rightarrow q$$

$$\neg q \rightarrow \neg p$$

Assume that the conclusion of the conditional statement is false; namely, assume that n is even.

By the definition of an even integer, $n = 2k$ for some integer k .

Substituting $2k$ for n , we find that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. This tells us that $3n + 2$ is even (because it is a multiple of 2), and therefore **not odd**.

This is the negation of the premise of the theorem.

Hence Proved.

Indirect Proofs: Proof by Contraposition

Q. Prove by Contraposition that If $x^2 - 6x + 5$ is even, then x is odd.

Proof:

Suppose that x is even. Then we want to show that $x^2 - 6x + 5$ is odd.

Write $x = 2a$ for some $a \in \mathbb{Z}$, and plug in:

$$\begin{aligned}x^2 - 6x + 5 &= (2a)^2 - 6(2a) + 5 \\&= 4a^2 - 12a + 5 \\&= 2(2a^2 - 6a + 2) + 1.\end{aligned}$$

Indirect Proofs: Proof by Contradiction

- Suppose we want to prove that a statement p is true.
- Furthermore, suppose that we can find a **contradiction** c such that $\neg p \rightarrow c$ is true.
- Since c is false, but $\neg p \rightarrow c$ is true, we can conclude that $\neg p$ is false, which means that p is true.
- Any statement that leads to a contradictory statement cannot be true.

Write a tautology & contradiction, using one propositional variable

$p \vee \neg p$ is always true, it is a tautology.

$p \wedge \neg p$ is always false, it is a contradiction.

Outline for Proof by Contradiction

Proposition P .

Proof. Suppose $\sim P$.

\vdots

Therefore $C \wedge \sim C$. ■

Indirect Proofs: Proof by Contradiction

$$a^2 - 4b \neq 2: a, b \in \mathbb{Z}$$

Suppose FOR SAKE OF CONTRADICTION this proposition is *false*.

So there exist Integers a, b : $a^2 - 4b = 2$.

$$a^2 = 2 + 4b = 2(2b + 1) \text{ so } a^2 \text{ is even.}$$

Even * Even = Even. So a is even $a = 2c$.

$$(2c)^2 - 4b = 2, \text{ so } 2c^2 - 2b = 1$$

Or $1 = 2(c^2 - b)$, so 1 is even.

$p: (1 \text{ is odd}) \wedge (1 \text{ is even})$. p is a **contradiction**.

Indirect Proofs: Proof by Contradiction

Definition 6.1 A real number x is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$.
Also, x is **irrational** if it is not rational, that is if $x \neq \frac{a}{b}$ for every $a, b \in \mathbb{Z}$.

Theorem: $\sqrt{2}$ is not rational

Proof:

Assume for the sake of contradiction that it is rational

- $\sqrt{2} = n/m$
- n and m have no common factors
- We will show that this is impossible

$$\sqrt{2} = n/m \longrightarrow 2m^2 = n^2$$

$$\text{Therefore, } n^2 \text{ is even} \longrightarrow \begin{array}{l} n \text{ is even} \\ n = 2k \end{array}$$

$$2m^2 = 4k^2 \longrightarrow m^2 = 2k^2 \longrightarrow m = 2k$$

Thus, m and n are even and have common factor 2

Contradiction!

Indirect Proofs: Proof by Contradiction

Prove by contradiction that if you pick 22 days from the calendar, at least 4 must fall on the same day of the week.

Let p = “you pick 22 days from the calendar” and q = “at least 4 days must fall on the same day of the week”,

now assume $\neg q$ = “no more than 3 days fall on the same day of the week”.

Now use p to derive a contradiction: p implies 3 weeks and 1 day, which implies that one day will be repeated 4 times.

This is a contradiction to our assumption $\neg q$, therefore q . (QED)

Proof by Contradiction (Conditional Statements)

- Proof by contradiction begins with the assumption that $\neg(p \rightarrow q)$ is true,
- OR that $p \rightarrow q$ is false.
- We know that $p \rightarrow q$ is false, means that it is possible that P can be true while Q is false.
- Thus the first step in the proof is to assume P and $\neg Q$.

Outline for Proving a Conditional Statement with Contradiction

Proposition If P , then Q .

Proof. Suppose P and $\sim Q$.

\vdots

Therefore $C \wedge \sim C$. ■

Proof: If a^2 is even, then a is even.

For the sake of contradiction, suppose:

- a^2 is even and a is not even.

So a^2 is even, and a is odd.

Since a is odd, there is an integer c : $a = 2c + 1$.

Then $a^2 = (2c + 1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1$

- So a^2 is odd

Thus a^2 is even and a^2 is not even

- Contradiction.

Exercise: Prove by Contradiction that if n is an integer and $3n + 2$ is odd, then n is odd.

Proof by Contradiction VS Proof by Contraposition

Method of **Contradiction**: Assume P and $\neg Q$ and prove some sort of contradiction.

Method of **Contrapositive**: Assume $\neg Q$ and prove $\neg P$.

- The method of Contrapositive has the advantage that your goal is clear: Prove $\neg P$.
- In the method of Contradiction, your goal is to prove a contradiction, but it is not always clear what the contradiction is going to be at the start

When to use what?

Despite the power of proof by contradiction, it's best to use it only when the direct and contrapositive approaches do not seem to work. The reason for this is that a proof by contradiction can often have hidden in it a simpler contrapositive proof, and if this is the case it's better to go with the simpler approach. Consider the following example.

Proposition Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof. To the contrary, suppose $a^2 - 2a + 7$ is even and a is not odd.

That is, suppose $a^2 - 2a + 7$ is even and a is even.

Since a is even, there is an integer c for which $a = 2c$.

Then $a^2 - 2a + 7 = (2c)^2 - 2(2c) + 7 = 2(2c^2 - 2c + 3) + 1$, so $a^2 - 2a + 7$ is odd.

Thus $a^2 - 2a + 7$ is both even and odd, a contradiction. ■

Though there is nothing really wrong with this proof, notice that part of it assumes a is not odd and deduces that $a^2 - 2a + 7$ is not even. That is the contrapositive approach! Thus it would be more efficient to proceed as follows, using contrapositive proof.

Proposition Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof. (Contrapositive) Suppose a is not odd.

Then a is even, so there is an integer c for which $a = 2c$.

Then $a^2 - 2a + 7 = (2c)^2 - 2(2c) + 7 = 2(2c^2 - 2c + 3) + 1$, so $a^2 - 2a + 7$ is odd.


Thus $a^2 - 2a + 7$ is not even. ■

Mistakes in Proofs

What is wrong with this famous supposed “proof” that $1 = 2$?

“Proof:” We use these steps, where a and b are two equal positive integers.

Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

Solution: Every step is valid except for one, step 5 where we divided both sides by $a - b$. The error is that $a - b$ equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero. 

Mathematical Induction

Conjecture: The sum of the first n odd natural numbers equals n^2 .

n	sum of the first n odd natural numbers	n^2
1	$1 = \dots\dots\dots$	1
2	$1 + 3 = \dots\dots\dots$	4
3	$1 + 3 + 5 = \dots\dots\dots$	9
4	$1 + 3 + 5 + 7 = \dots\dots\dots$	16
5	$1 + 3 + 5 + 7 + 9 = \dots\dots\dots$	25
\vdots	\vdots	\vdots
n	$1 + 3 + 5 + 7 + 9 + 11 + \dots + (2n - 1) = \dots\dots\dots$	n^2
\vdots	\vdots	\vdots

An infinite ladder

Suppose that we have an infinite ladder, and we want to know whether we can reach every step on this ladder.

We know two things:

1. We can reach the first rung of the ladder.
2. If we can reach a particular rung of the ladder, then we can reach the next rung.

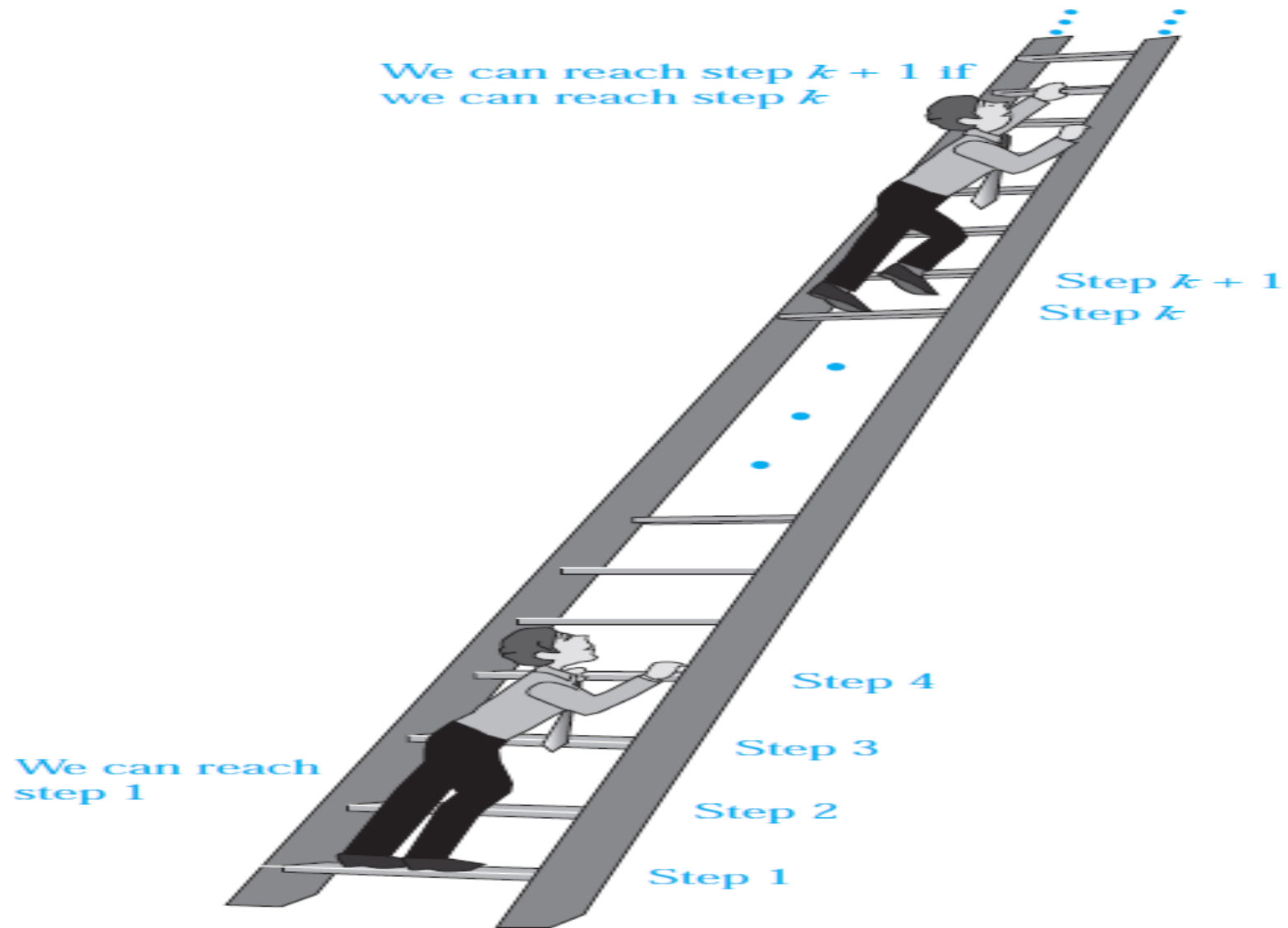


FIGURE 1 Climbing an Infinite Ladder.

PRINCIPLE OF MATHEMATICAL INDUCTION To prove that $P(n)$ is true for all positive integers n , where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that $P(1)$ is true. Exhaustive Proof?

INDUCTIVE STEP: We show that the conditional statement $P(k) \rightarrow P(k + 1)$ is true for all positive integers k . Direct Proof?

Outline for Proof by Induction

Proposition The statements $S_1, S_2, S_3, S_4, \dots$ are all true.

Proof. (Induction)

(1) Prove that the first statement S_1 is true.

(2) Given any integer $k \geq 1$, prove that the statement $S_k \Rightarrow S_{k+1}$ is true.

It follows by mathematical induction that every S_n is true. ■

Example

Prove that the sum of the n first odd positive integers is n^2

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Let $S(n)$ = the sum of the first n odd numbers greater than 0.

Show that $S(n) = 1 + 3 + \dots + (2n - 1) = n^2$.

Base Case ($n = 1$): $S(1) = 1 = 1^2$. So the result holds for $n = 1$.

Induction Hypothesis: Assume that $S(k) = k^2$.

Show that $S(k + 1) = (k + 1)^2$.

$$\begin{aligned} S(k + 1) &= 1 + 3 + \dots + (2k - 1) + (2(k + 1) - 1) \\ &= S(k) + 2(k + 1) - 1 && \text{(by definition of } S(n)) \\ &= k^2 + 2(k + 1) - 1 && \text{(by the induction hypothesis)} \\ &= k^2 + 2k + 1 \\ &= (k + 1)(k + 1) && \text{(factoring)} \\ &= (k + 1)^2 \end{aligned}$$

Hence proved!

Exercises

Show that, $1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$

Proof. First, we will *assume* that the formula is true for $n = k$; that is, we will assume:

$$1 + 2 + 3 + \dots + k = \frac{k(k+1)}{2} \quad (1)$$

This is the induction assumption. Assuming this, we must prove that the formula is true for its successor, $n = k + 1$. That is, we must show:

To do that, we will simply add the *next term* $(k + 1)$ to both sides of the induction assumption, [line \(1\)](#):

$$1 + 2 + 3 + \dots + (k + 1) = \frac{(k + 1)(k + 2)}{2} \quad (2)$$

$$1 + 2 + 3 + \dots + k + (k + 1) = \frac{k(k + 1)}{2} + (k + 1)$$

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

on adding those fractions,

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

on taking $(k + 1)$ as a common factor.

Hence proved!

Exercises

Prove that this rule of exponents is true for every natural number n :

$$(ab)^n = a^n b^n.$$

Prove this remarkable fact of arithmetic:

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left[\frac{n(n+1)}{2} \right]^2$$

Prove by mathematical induction

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

Use mathematical induction to prove that

$$1^3 + 2^3 + 3^3 + \dots + n^3 = n^2 (n+1)^2 / 4$$

Prove that

$$1^2 + 2^2 + 3^2 + \dots + n^2 = n(n+1)(2n+1)/6$$