MATHEMATICAL REASONING

BY PANKAJ KAMTHAN

1. INTRODUCTION

Thinking like a computer scientist means more than being able to program a computer. It requires **thinking at multiple levels of abstraction**.
— Jeannette M. Wing

Some people say, "How can you live without knowing?" I do not know what they mean. I always live without knowing. That is easy. How you get to know is what I want to know.
— Richard P. Feynman

A mathematician's work is mostly a tangle of guesswork, analogy, wishful thinking and frustration, and proof, far from being the core of discovery, is more often than not a way of making sure that our minds are not playing tricks.
— Gian-Carlo Rota

The ability to apply logic for establishing or verifying facts is **mathematical reasoning** [Rossi, 2006; Bramanti, Travaglini, 2018]. There are three different kinds of reasoning [Wikipedia]: **deductive, inductive, and abductive**. In mathematics, deductive and inductive reasoning is usually presented in the form of a **mathematical proof** [Taylor, Garnier, 2014, Section 1.3].

This document explores the different avenues of deductive and inductive reasoning, especially the notion of 'proof'.

2. THE SIGNIFICANCE OF MATHEMATICAL REASONING TO COMPUTER SCIENCE AND SOFTWARE ENGINEERING

It is useless to attempt to reason a man out of a thing he was never reasoned into.
— Jonathan Swift

Perhaps software practitioners who say, I don't use mathematics, really mean, I don't use mathematics explicitly or formally. Many practicing engineers ... do implicitly use mathematical reasoning all the time. Similarly, software engineers should learn to use foundational discrete mathematics concepts and logical reasoning at all times.

— Peter B. Henderson

The notion of mathematical reasoning is central to many areas in computer science and software engineering:

- For **instilling mathematical thinking** [Mclnerny, 2004; Bramanti, Travaglini, 2018] **and computational thinking** [Wing, 2006].

- For **developing problem-solving ability** [Bruce, Drysdale, Kelemen, Tucker, 2007; Baldwin, Walker, Henderson, 2013].

- For **increasing mathematical aptitude**.

- For **advancing mathematical maturity** [Henderson, 2003; Sedgewick, Wayne, 2015].

- For **appreciating the necessity and power of abstraction** [Henderson, 2003; [Ording, 2019].

- For **improving algorithmic skills**.

- For **improving technical writing skills**.

- For **providing a convincing argument** for the **correctness** of an algorithm or a program [Houston, 2009, Chapter 17; Roberts, 2010, Appendix A].

  "When algorithms and protocols only 'mostly work' due to reliance on hand-waving arguments, the results can range from **problematic to catastrophic**." [Lehman, Leighton, Meyer, 2012].

- For **discovering connections between proofs and algorithms** [Dowek, 2011].

- For **artificial intelligence**.

PROOFS, PROOFS EVERYWHERE

The significance of proofs is exemplified by **ProofWiki**[1], which is "a compendium of mathematical proofs" and its goal is "the collection, collaboration and classification of mathematical proofs", and by **Proofs from The Book**[2], which "celebrates the beauty and elegance of mathematical theorems discussed in school mathematics and their proofs".

2.1. THE ROLE OF PROOFS IN MATHEMATICS, COMPUTER SCIENCE, AND SOFTWARE ENGINEERING

To really think like a mathematician you must embrace proof.
— Kevin Houston

The notion of proof has its **origins in mathematics** [Franklin, Daoud, 1988; Chemla, 2012; O'Regan, 2016, Chapter 4].

Indeed, proofs are central to **mathematical knowledge** [Detlefsen, 1992; Velleman, 2006, Preface; Hammack, 2009; Houston, 2009; Nickerson, 2010; Bloch, 2011; Cunningham, 2012; Gerstein, 2012; Chartrand, Polimeni, Zhang, 2013; Cupillari, 2013; Hammack, 2013; Stewart, Tall, 2015; Kane, 2016], and there are many **renowned mathematical proofs** [Aigner, Ziegler, 2014].

There are **applications of mathematics** to a number of seemingly **unorthodox areas** [Herrmann, 2012; Khare, Lachowska, 2015]. The **educational and 'recreational'** value of these applications also rests on the fact that they are supported by proofs.

The notion of proof is also **essential** to many areas of computer science and software engineering, given that mathematics is among the foundations for both computer science and software engineering [Dowek, 2011; Gallier, 2011, Chapter 1; Rosen, 2012, Chapter 2; Reba, Shier, 2015, Chapter 9; Dougherty, 2017].

[1] URL: https://proofwiki.org/ .
[2] URL: http://proofsfromthebook.com/ .

It is important for a prospective or professional computer scientist or a software engineer to learn how to **read, understand, and write** a proof [Cunningham, 2012; Solow, 2014; Taylor, Garnier, 2014].

2.2. THE RELATIONSHIP BETWEEN MATHEMATICAL REASONING/ MATHEMATICAL PROOFS AND SOFTWARE ENGINEERING

SWEBOK®

The **Guide to the Software Engineering Body of Knowledge (SWEBOK)** "describes the sum of knowledge within the profession of software engineering" [IEEE, 2014]. In SWEBOK, there are a number of Knowledge Areas (KAs). The study of proof techniques is part of **Mathematical Foundations KA** of the SWEBOK3, as shown in Figure 1.

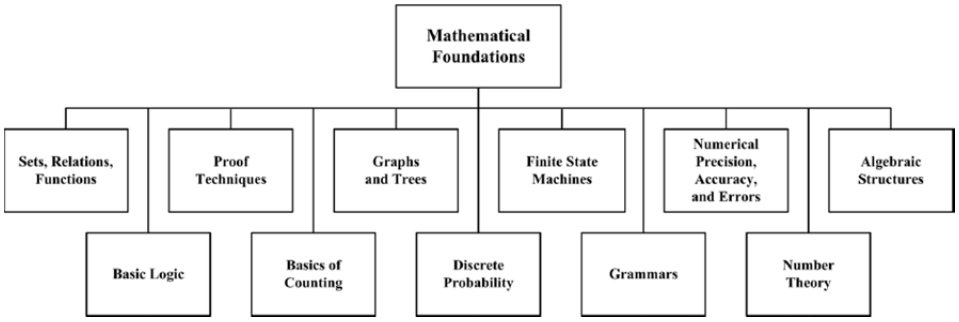


Figure 1. Mathematical Foundations is a Knowledge Area in the Guide to the Software Engineering Body of Knowledge (SWEBOK). (Source: SWEBOK [IEEE, 2014].)

2.3. THE RELATIONSHIP BETWEEN MATHEMATICAL REASONING/ MATHEMATICAL PROOFS AND COMPUTER PROGRAMMING

There is interest is looking at process of writing mathematical proofs and that of writing computer programs [Calude, Calude, Marcus, 2007; Lehman, Leighton, Meyer, 2012, Section 3.2].

There are many views of software engineering, in general, and programming, in particular, one of which is that it is a **knowledge acquisition** process. In [Hartwig, 2011], it has been shown using the model of knowledge management called SECI that **proof writing is a knowledge acquisition process**.

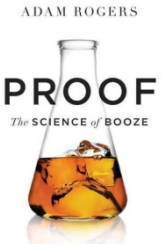
The **similarities** between writing mathematical proofs and writing computer programs include the following:

- Understanding Input and Output
- Correctness
- Clarity

The **differences** between writing mathematical proofs and writing computer programs include the following:

- Type of Universe
- Type of Readership

REMARKS



The notion of proof goes beyond mathematics (and exists in other disciplines, such as **publishing** and **photography**). This document is, however, concerned with 'mathematical' proofs only.

3. MATHEMATICAL ARGUMENTS

In logic, an **argument** is a sequence of statements that end with a conclusion. An argument is used to **persuade someone of something** or to **present reasons for accepting a conclusion** [Wikipedia].

3.1 QUALITY OF MATHEMATICAL ARGUMENTS

A **rational argument** always presents reasons (premise) for its claim (conclusion) [Reba, Shier, 2015, Chapter 7]. An argument based on **emotional appeal, eloquent persuasion, indoctrination, or coercion** is not rational, and therefore not acceptable in technical disciplines, including computer science and software engineering.

An **argument is valid** if whenever all hypotheses are (assumed to be) true, the conclusion is also true.

The following is the general strategy for proving an argument is valid (or showing that the conclusion follows logically from the hypotheses):

1. It is **assumed** that the **hypotheses are true**.

2. The **rules of inference** and **logical equivalences** are used to determine that the **conclusion is true**.

4. RULES OF INFERENCE

An **inference** is a **process** of **deriving logical conclusions** from premises known or assumed to be true. This derivation is based on **evidence and reasoning**.

A **rule of inference** is a logical rule allowing the deduction of conclusions from premises. It has two main parts: (1) H_1, H_2 , …, H_n are the **hypotheses**, and (2) C is the **conclusion**. (1) and (2) are separated by a '∴'.

NOTATION

U+2234

The symbol ∴ means 'Therefore' or 'It follows that'.

REMARKS

It is **not** unusual for the same symbol to be used differently in different contexts. For example, in **meteorology**, the ∴ symbol is sometimes used as a substitute for an **asterism**, a symbol used to indicate **moderate snow**:

4.1. RULES OF INFERENCE FOR PROPOSITIONS

In Table 1, several **common rules of inference for propositions** are defined: Modus Ponens, Modus Tollens, Hypothetical Syllogism, Disjunctive Syllogism, Addition Simplification, Conjunction, and Resolution.

Rule of Inference	Tautology	Name
$p \longrightarrow q$ p _____ $\therefore q$	$[(p \longrightarrow q) \wedge p] \longrightarrow q$	Modus Ponens
$\neg q$ $p \longrightarrow q$ _____ $\therefore \neg p$	$[(p \longrightarrow q) \wedge \neg q] \longrightarrow \neg p$	Modus Tollens
$p \longrightarrow q$ $q \longrightarrow r$ _____ $\therefore p \longrightarrow r$	$[(p \longrightarrow q) \wedge (q \longrightarrow r)] \longrightarrow (p \longrightarrow r)$	Hypothetical Syllogism
$p \vee q$ $\neg p$ _____ $\therefore q$	$[(p \vee q) \wedge \neg p] \longrightarrow q$	Disjunctive Syllogism
p _____ $\therefore p \vee q$	$p \longrightarrow p \vee q$	Addition
$p \wedge q$ _____ $\therefore p$	$(p \wedge q) \longrightarrow p$	Simplification
p q _____ $\therefore p \wedge q$	$[(p) \wedge (q)] \longrightarrow (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ _____ $\therefore q \vee r$	$[(p \vee q) \wedge (\neg p \vee r)] \longrightarrow (q \vee r)$	Resolution

Table 1. A collection of most prominent rules of inferences for propositions.

REMARKS

- It could be noted that the **rules of inference** are **tautologies**. This is because a rule must (within the context of logic) always be true.

- The names of some of the rules of inference are derived from **Latin**. The purpose of naming is to create a **mnemonic** for **communication**.

4.2. RULES OF INFERENCE FOR QUANTIFIED STATEMENTS

In Table 2, several **common rules of inference for quantified statements** are defined: Universal Instantiation, Universal Generalization, Existential Instantiation, and Existential Generalization.

Rule of Inference	Name
$\forall x\, P(x)$ $\_\_\_\_\_$ $\therefore P(c)$	Universal Instantiation
$P(c)$ for an arbitrary c $\_\_\_\_\_$ $\therefore \forall x\, P(x)$	Universal Generalization
$\exists x\, P(x)$ $\_\_\_\_\_$ $\therefore P(c)$ for some element c	Existential Instantiation
$P(c)$ for some element c $\_\_\_\_\_$ $\therefore \exists x\, P(x)$	Existential Generalization

Table 2. A collection of most prominent rules of inferences for quantified statements.

EXAMPLE

Express the following in form of rules of inference.

> Everyone in the discrete mathematics (DM) class has taken a computer science (CS) course.
>
> Mona is a student in the DM class.
>
> Therefore, Mona has taken a CS course.

Solution.

First, **"mathematize"** to create an **abstraction**:

$D(x)$: x is in the DM class.
$C(x)$: x has taken a CS course.

Second, **use the rules of inference**:

Step	Reason
(1) $\forall x\,(D(x) \longrightarrow C(x))$	Premise
(2) D(Mona) $\longrightarrow C$(Mona)	Universal Instantiation using (1)
(3) D(Mona)	Premise
(4) C(Mona)	Modus Ponens using (3) and (2)

EXAMPLE

For the following argument, provide the rules of inference that are used in each step. "Mary, a student in this class, owns a red sports car. Everyone who owns a red sports car has gotten at least one speeding ticket. Therefore, someone in this class has gotten a speeding ticket."

Solution.

Premise: Mary, a student in this class, owns a red sports car. Everyone who owns a red sports car has gotten at least one speeding ticket.
Conclusion: Therefore, someone in this class has gotten a speeding ticket.

First, **"mathematize"** to create an **abstraction**:

$C(x)$: x is in this class.
$R(x)$: x owns a red sports car.
$T(x)$: x has gotten a speeding ticket.

Second, **"mathematize"** to state the **premise**:

C(Mary).
R(Mary).
$\forall x\,[R(x) \longrightarrow T(x)]$.

Third, **"mathematize"** to state the **conclusion**:

$\exists x\,[C(x) \wedge T(x)]$.

Fourth, **use the rules of inference**:

Step	Reason
(1) $\forall x\,(R(x) \longrightarrow T(x))$	Hypothesis
(2) $R(\text{Mary}) \longrightarrow T(\text{Mary})$	Universal Instantiation using (1)
(3) $R(\text{Mary})$	Hypothesis
(4) $T(\text{Mary})$	Modus Ponens using (3) and (2)
(5) $C(\text{Mary})$	Hypothesis
(6) $C(\text{Mary}) \wedge T(\text{Mary})$	Conjunction using (4) and (5)
(7) $\exists x\,[C(x) \wedge T(x)]$	Existential Generalization using (6)

EXAMPLE

Use rules of inference to show that if $\forall x\,[P(x) \vee Q(x)]$ and $\forall x\,[(\neg P(x) \wedge (Q(x)) \longrightarrow R(x))]$ are true, then $\forall x\,[\neg R(x) \longrightarrow P(x)]$ is also true, given that all the quantifiers have the same domain.

Solution.

Premise: (1) $\forall x\,(P(x) \vee Q(x))$, and (2) $\forall x\,[(\neg P(x) \wedge (Q(x)) \longrightarrow R(x))]$.
Conclusion: $\forall x\,[\neg R(x) \longrightarrow P(x)]$.

The purpose is to show that $\neg R(c) \longrightarrow P(c)$ is true for all c in the domain. Then, the desired conclusion follows from Universal Generalization.

Thus, the aim is to show that if $\neg R(c)$ is true for a particular c, then $P(c)$ is also true.

For such a c, applying Universal Instantiation to (1) gives $P(c) \vee Q(c)$.

For such a c, applying Universal Modus Tollens to (2) gives $\neg(\neg P(c)) \wedge Q(c))$ that, in turn, is equal to $P(c) \vee \neg Q(c)$, from the rules of propositional logic. (The previous argument can be explained as follows. If $\neg R(c)$ is true c, then $R(c)$ is false. Now, (2) is a conditional statement, which means that its LHS must be false for it to be true, which means $\neg P(c)) \wedge Q(c)$ must be false, or that $\neg(\neg P(c)) \wedge Q(c))$ must be true.)

Now, by Resolution it can be concluded that $P(c) \vee P(c)$, which is logically equivalent to $P(c)$, as desired.

EXAMPLE

Show that the argument form with premises $(p \wedge t) \longrightarrow (r \vee s)$, $q \longrightarrow (u \wedge t)$, $u \longrightarrow p$, and $\neg s$ and conclusion $q \longrightarrow r$ is valid.

Solution.

The argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion $q \longrightarrow r$ is valid if the argument form with premises $p_1, p_2, \ldots, p_n, q$, and conclusion r is valid. (This is from Exercise 11 of Section 1.6 of [Rosen, 2012]. There is a straightforward reason why this works: q itself is a premise for r, so q is simply being "added" to the other n premises, resulting in n + 1 premises.)

Premise: $(p \wedge t) \longrightarrow (r \vee s)$, $q \longrightarrow (u \wedge t)$, $u \longrightarrow p$, $\neg s$, and q.
Conclusion: r.

Then, use an **"input-output chain" and the rules of inference**:

Input	Output	Reason
q and $q \longrightarrow (u \wedge t)$	$u \wedge t$	Premise and Modus Ponens
$u \wedge t$	u and t	Simplification (and Commutative Law)
u and $u \longrightarrow p$	p	Premise and Modus Ponens
p and t	$p \wedge t$	Conjunction
$(p \wedge t) \longrightarrow (r \vee s)$	$r \vee s$	Premise and Modus Ponens
$r \vee s$ and $\neg s$	r	Premise and Disjunctive Syllogism

5. MATHEMATICAL ASSERTIONS

An **assertion** is a statement of fact or declaration.

5.1. A CLASSIFICATION OF MATHEMATICAL ASSERTIONS

The axiomatic structure of mathematics suggests that there can be different kinds of mathematical assertions that require a proof [Rossi, 2006]:

- **Conjecture.** A **conjecture** is a statement for which there is some evidence supporting the belief that the statement is true, but for which there is **no proof** [Cunningham, 2012, Page 61]. For example, the Goldbach Conjecture.

- **Theorem.** A **theorem** is an important result that is usually considered to be one of the highlights of the area. A theorem typically requires an **elaborate**, **non-trivial** proof. In some cases, an established theorem is given a **name** [Scheinerman, 2013, Chapter 1]. For example, the Pythagorean Theorem.

- **Proposition.** A **proposition** is an important result, but not as important as a theorem. (The notion of 'proposition' is not the same as in propositional logic.)

- **Lemma.** A **lemma** is a result that is needed to prove other results, such as a theorem. In this sense, a lemma is a kind of **'pre-theorem'**. It is often singled out because it is useful and interesting in its own right. For example, the Zorn's Lemma.

- **Corollary.** A **corollary** is a result that is a direct consequence of a theorem. In this sense, a corollary is a kind of **'post-theorem'**.

An aspect **common** to these mathematical structures is the presence of a **premise (hypotheses)** and a **conclusion**.

5.2. PROVING A MATHEMATICAL ASSERTION

A mathematical proof is a **logically structured argument** which **demonstrates** that a certain **mathematical assertion** is true.

A mathematical assertion can be proven using one or more of the following means:

- **Definition.**
- **Axiom.**
- **Rule of Inference.**
- **Other Theorems/Propositions/Lemmas/Corollaries.**

NOTATION FOR END OF PROOF

It is customary to denote the **end of proof** by a symbol, so as to clearly separate the proof from the text that follows the proof.

There are (at least) two commonly-used symbols:

□

■

There are alternatives, such as **Q.E.D. (Quod Erat Demonstrandum)**, shown in a cartoon in Figure 2.

Figure 2. Q.E.D. (Source: Wikipedia.)

6. LOGICAL FALLACIES REVISITED

A fallacy is an **irrational argument** [Reba, Shier, 2015, Chapter 7]. It **resembles** a rule of inference, but is based on **contingency** rather than tautology.

A fallacy is an **incorrect inference** [Bunch, 1982].

Therefore, it is important that fallacies be **avoided** in mathematical proofs [Mclnerny, 2004; Vivaldi, 2014].

A proof involving a fallacy leads to **bogus proofs** [Lehman, Leighton, Meyer, 2012, Section 1.9; Bourchtein, Bourchtein, 2015].

There are three **common types of fallacies** in mathematical arguments:

1. Affirming the Consequent
2. Denying the Antecedent
3. Circular Reasoning

6.1. FALLACY OF AFFIRMING THE CONSEQUENT

$$\begin{array}{l} p \longrightarrow q \\ \underline{q\qquad} \\ \therefore p \end{array}$$

$[(p \longrightarrow q) \wedge q] \longrightarrow p$ is **not** a tautology, and therefore **not** a rule of inference.

EXAMPLE

Let S be a student.

If S does every problem in this book, then S will learn the subject.

S learned the subject.

Therefore, S did every problem in this book.

This is a fallacy because it is possible that S **learned the subject by other means**.

EXAMPLE

If I have the flu, then I have a sore throat.

I have a sore throat.

Therefore, I have the flu.

This is a fallacy because there are **many causes of sore throat**. Therefore, a given **effect** should **not** automatically be mapped to a single **cause [**Kleinberg, 2016**]**.

6.2. FALLACY OF DENYING THE ANTECEDENT

$$\begin{array}{l} p \longrightarrow q \\ \underline{\neg p\quad\quad} \\ \therefore \neg q \end{array}$$

$[(p \longrightarrow q) \wedge \neg p] \longrightarrow \neg q$ is **not** a tautology, and therefore **not** a rule of inference.

EXAMPLE

If you do every problem in this book, then you will learn the subject.

You did not do every problem in this book.

Therefore, you did not learn the subject.

6.3. FALLACY OF CIRCULAR REASONING

In this case, one or more steps of the proof are **based upon** the truth of the statement being proven.

In other words, p is true because q is true, and q is true because p is true.

EXAMPLE

The proof of the following problem is **wrong**. (It is wrong because it **assumes** that n is odd and then concludes the same.)

Show that if n^2 is odd, then n is odd.

Solution.

If n^2 is odd, then $n^2 = 2k + 1$, for some integer k. Now, let $n = 2p + 1$, for some integer p. Therefore, n is odd.

EXAMPLE

Determine whether the following arguments are valid:

(a) If x is a positive real number, then x^2 is a positive real number. Therefore, if a^2 is a positive real number, where a is a real number, then a is a positive real number.

(b) If $x^2 \neq 0$, where x is a real number, then $x \neq 0$. Therefore, if a be a real number with $a^2 \neq 0$, then, $a \neq 0$.

Solution.

(a) This is invalid. It is the **Fallacy of Affirming the Consequent**. $a = -2$ provides a counterexample.

(b) This is valid. It is **Modus Ponens**.

7. METHODS OF PROOF

A good proof is like telling a story —there is a beginning, middle, and end, and the writer needs to hold the reader's interest through all three parts.
— Michael Hvidsten

There are several ways of **classifying** mathematical proofs[3]. There are several methods of proof [Rossi, 2006, Chapter 3; Cunningham, 2012; Scheinerman, 2013, Chapter 1; Solow, 2014; Vivaldi, 2014; Joshi, 2015; Bramanti, Travaglini, 2018, Chapter 5; Grieser, 2018, Chapter 3, Chapter 7; Sundstrom, 2018, Chapter 3; Ording, 2019].

- Direct Proof
- Indirect Proof (Proof by Contraposition)
- Vacuous Proof
- Trivial Proof
- Proof by Contradiction (Reductio Ad Absurdum)
- Proof by Cases
- Existence Proof
- Geometric Proof

[3] URL: https://proofwiki.org/wiki/Category:Proofs .

REMARKS

In an attempt to show the beauty of mathematical proofs, in [Ording, 2019], 99 styles of writing a mathematical proof have been illustrated, and the rationale of each is given:

8. GUIDELINES FOR WRITING PROOFS

Obvious is the most dangerous word in mathematics.
— E. T. Bell

Patience and perseverance have a magical effect before which difficulties disappear and obstacles vanish.
— John Quincy Adams

Minimalism isn't always the right choice, but it's rarely the wrong choice.
— Jeff Atwood

8.1. UNDERSTANDING THE PROBLEM

It is important to **understand the problem** before attempting a solution. (This goes beyond the problems requiring proofs.) In particular, it is important that the **hypotheses** be understood.

A proof will be based upon the conditions stated in the hypotheses, and more. (This is yet another reason why the **hypotheses should be understood** before attempting a proof of an assertion.)

The goal is to establish the truth of $p \longrightarrow q$. To do that, it is sufficient to show that q is true if p is true. $p \longrightarrow q$ is a **conjecture** until a proof is produced.

8.2. SKILLS IN WRITING A PROOF

A **proof** (like a computer program) is **read more often than written**, and should therefore be **readable**.

The ability to write proof properly is a **skill** that requires a combination of **art, science, and engineering** [Velleman, 2006; Houston, 2009, Chapter 17; Beck, Geoghegan, 2010; Roberts, 2010, Appendix A; Bloch, 2011, Section 2.6; Cunningham, 2012; Solow, 2014; Ording, 2019]. There is **no general 'recipe'** for proving a mathematical statement [Houston, 2009, Chapter 17]. In the real-world, the proof of a statement usually does **not** come equipped with the method of proof to be used. The **selection and use** of a method **depends** on the **type** of problem.

8.3. NUMBER OF PROOFS

For certain mathematical assertions, there can be **more than one proof**. Indeed, the quest for alternative proofs is not uncommon in mathematics [Dawson, 2015].

However, not all proofs are 'equal'. Indeed, **some proofs may be simpler** (have less number of steps, or are easier to understand, or both) than others.

8.4. LENGTH OF PROOF

A proof could be **short or long**. As of 2011, the **longest mathematical proof**, measured by number of published journal pages, is the classification of finite simple groups with well over **10,000 pages** [Wikipedia].

A proof could be **simple or complex**. The aim should be to achieve a **simpler proof**. A simple proof is **not only correct**, but also **clear and concise**. To do that, for example, a simple proof may have fewer steps, may reuse other results, may have a smooth and easier to understand transition across steps, and use an **appropriate combination of natural language and mathematical notation**. Thus, proof writing is an **iterative process**.

A proof could be **incorrect** [Velleman, 2006]. For example, a proof based on a **fallacy** is incorrect. The aim therefore should be to **avoid fallacies in a proof**. This can be done, for example, by being **aware** of the types of fallacies and by **reviewing** the "proof".

9. DIRECT PROOF

- The hypotheses are assumed to be true.

- The rules of inference and logical equivalences are used to establish the truth of the conclusion.

To prove that a proposition of the form "$\forall$k P(k) $\longrightarrow$ Q(k)" is true, derive that "Q(k) is true" for any k which satisfies "P(k) is true".

EXAMPLE

Using a **direct proof** verify that Modus Ponens, $[(p \longrightarrow q) \wedge p] \longrightarrow q$, is a tautology.

Solution.

Suppose the LHS is true. Then, both $p \longrightarrow q$ and p have value true.

Since $p \longrightarrow q$ and p are true, it follows that q is true.

Therefore, the RHS is true.

EXAMPLE

Using a **direct proof** verify that Modus Tollens, $[(p \longrightarrow q) \wedge \neg q] \longrightarrow \neg p$, is a tautology.

Solution. Improvise.

EXAMPLE

Use a **direct proof** to show that the sum of two even integers is even.

Solution.

Let x and y be two even integers. Then, by the definition of an even integer, there exist integers j and k such that $x = 2j$ and $y = 2k$.

Now,

$$x + y = 2j + 2k = 2(j + k).$$

Therefore, $x + y$ is an even integer.

EXAMPLE

Use a **direct proof** to show that, for an integer n, if n is odd, then n^2 is odd.

Solution.

If n is odd, then, by the definition of an odd integer, there exists an integer k such that $n = 2k + 1$.

Now,

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

where $m = 2k^2 + 2k$ is an integer. Therefore, n^2 is odd.

REMARKS

The converse is true as well, that is, if n^2 is odd, then n is odd. (This can be shown by an **indirect proof** or by **proof by contradiction**.)

EXAMPLE

Use a **direct proof** to show that, for an integer n, if n is even, then n^2 is even.

Solution. Improvise. (Use the definition of an even integer.)

EXAMPLE

Use a **direct proof** to show that the product of two odd integers is odd.

Solution.

Let x and y be two odd integers. Then, by the definition of an odd integer, there exist integers j and k such that $x = 2j + 1$ and $y = 2k + 1$.

Now,

$$xy = (2j + 1)(2k + 1) = 4jk + 2j + 2k + 1 = 2(2jk + j + k) + 1.$$

Therefore, xy is an odd integer.

EXAMPLE

Use a **direct proof** to show that the product of two rational numbers is a rational number.

Solution.

(The set of rational numbers can be defined or characterized as $\mathbf{Q} = \{p/q \mid p, q$ are integers that are co-prime, with $q \neq 0\}$.)

Let x and y be two rational numbers. Then, by the definition of a rational number, there exist integers p and q, $q \neq 0$, such that $x = p/q$, and there exist integers r and s, $s \neq 0$, such that $y = r/s$.

Now,

$$xy = (p/q)(r/s) = pr/qs, \text{ where pr and qs are integers, and } qs \neq 0.$$

Therefore, xy is a rational number.

EXAMPLE

Prove that if x is a rational number and $x \neq 0$, then $1/x$ is a rational number.

Solution. Improvise. (Use the definition of a rational number, which, in this case, would be a quotient of two **nonzero** integers.)

EXAMPLE

Prove that if n is a perfect square, then n + 2 is not a perfect square.

Solution.

Let $n = m^2$. If m = 0, then n + 2 = 2, which is not a perfect square. If m = 1, then n + 2 = 3, which is not a perfect square. Therefore, assume that m > 1.

The **smallest perfect square greater than n** is $(m + 1)^2$, and

$$(m + 1)^2 = m^2 + 2m + 1 = n + 2m + 1 > n + 2 \cdot 1 + 1 > n + 2.$$

Therefore, n + 2 is in between n and $(m + 1)^2$, and so it cannot be a perfect square.

EXAMPLE

If n is an odd positive integer, then

$$8 \mid (n - 1)(n + 1).$$

Solution.

If n is an odd positive integer, then for some integer $k \geq 0$,

$$n = 2k + 1.$$

Now,

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

and

$$8 = 4 \cdot 2.$$

Finally, 4 | 4, and 2 | k(k + 1), because either k is **even** or k + 1 is **even**.

Therefore, 8 | (n – 1)(n + 1).

EXAMPLE

For a real number x, $x \neq 0$ or 1, and an integer $n \geq 0$, prove that

$$1 + x + x^2 + \cdots + x^n = (1 - x^{n+1}) / (1 - x).$$

Solution.

Let

$$S_n = 1 + x + x^2 + \cdots + x^n.$$

Then,

$$xS_n = x + x^2 + x^3 + \cdots + x^{n+1}.$$

It follows that,

$$S_n - xS_n = (1 - x)S_n = 1 - x^{n+1}.$$

Therefore,

$$1 + x + x^2 + \cdots + x^n = (1 - x^{n+1}) / (1 - x).$$

REMARKS

S_n is called the **partial sum** of a **geometric series**.

EXAMPLE

For a natural number $n \geq 2$, prove that

$$\text{if } 4^n > 4n + 1, \text{ then } 4^{n+1} > 4(n + 1) + 1.$$

Solution.

(The proof uses **two conditions** given in the hypotheses: (1) the inequality $4^n > 4n + 1$, and (2) the fact that $n \geq 2$ means $12n \geq 12 \cdot 2 > 1$.)

$$4^{n+1} = 4 \cdot 4^n > 4(4n + 1) = 16n + 4 = 4n + 4 + 12n = 4(n + 1) + 12n > 4(n + 1) + 1.$$

EXAMPLE

For an integer n, prove that if $n \geq 3$, then

$$2^{n-1} + 2^{n-2} + 2^{n-3} < 2^n.$$

Solution. Improvise. (Transform the problem into an **equivalent, simpler, problem**. Multiply both sides by 2^3 and proceed.)

EXAMPLE

For a real number n, prove that if $n \geq 3$, then $n^2 > 2n + 1$.

Solution. Improvise. ($n^2 > 2n + 1 = n^2 - 2n - 1 = (n^2 - 2n + 1) - 2 = (n - 1)^2 - 2 \geq (4 - 1)^2 - 2 > 0$.)

EXAMPLE

The sum of the squares of any two rational numbers is a rational number.

Solution.

Let x and y be two rational numbers. Then, by definition of a rational number, it is possible to express

$$x = p_1/q_1 \text{ and } y = p_2/q_2,$$

where p_1, q_1, p_2, and q_2 are integers.

Now,

$$x^2 + y^2 = [\ (p_1)^2 \cdot (q_2)^2\ + (p_2)^2 \cdot (q_1)^2\ ] / [\ (q_1)^2 \cdot (q_2)^2\ ],$$

which is a rational number.

EXAMPLE

Prove that $m^2 = n^2$ if and only if $m = n$ or $m = -n$.

Solution. There are **two parts** of this proof.

(1) If $m^2 = n^2$, then m = n or m = –n.

If $m^2 = n^2$, then $(m^2 – n^2) = (m + n)(m – n) = 0$. Therefore, m = n or m = –n.

(2) If m = n or m = –n, then $m^2 = n^2$.

Improvise.

EXAMPLE

For propositions p, q, r, and s show that

$$[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)] \longrightarrow (r \vee s)$$

is a tautology.

Solution.

Let LHS be $[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)]$ and RHS be $(r \vee s)$.

Let LHS be true. Then, it is to be shown that RHS is also true.

$[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)]$ is true, means $(p \vee q)$ is true and $p \longrightarrow r$ is true and $q \longrightarrow s$ is true.

This, in turn, means that

(a) p is F and q is F

and

(b) p is T and r is F

and

(c) q is T and s is F

is **not** possible.

Case 1: If p is T, then by (b), r is T **and** by (c) either q is F or s is T.

Case 2: If p is F, then by (a), q is T **and** by (c) either q is F or s is T. This means that if p is F, then by (a), q is T **and** by (c) s is T.

Thus, from the previous cases, either r is T or s is T, which means RHS is true.

10. INDIRECT PROOF (PROOF BY CONTRAPOSITION)

This is a direct proof of the **contrapositive**. Hence, it is known as **proof by contraposition**.

This style of proof uses the following contrapositive logical equivalence:

$$p \longrightarrow q \Leftrightarrow \neg q \longrightarrow \neg p.$$

For proving $\forall k\, P(\mathrm{k}) \longrightarrow Q(\mathrm{k})$, for any k, assume $\neg Q(\mathrm{k})$ and derive $\neg P(\mathrm{k})$.

It is assumed that $\neg q$ is true, that is, q is false. Then the rules of inference and logical equivalences are used to show that $\neg p$ is true, that is, p is false.

EXAMPLE

Using **indirect proof**, prove that

if 3n + 2 is odd, then n is odd.

Solution.

The contrapositive is:

if n is even, then 3n + 2 is even.

If n is even, then, by definition, it is possible to write n = 2k, for some integer k.

Now,

$$3n + 2 = 3(2k) + 2 = 2(3k + 1)$$

is a multiple of 2, and is therefore also even.

EXAMPLE

Using **indirect proof**, for an integer n, show that if n is even, then n^2 is even.

Solution.

The contrapositive is:

$$\text{if } n^2 \text{ is not even, then n is not even.}$$

Then, n^2 is odd. This

$\Longrightarrow \exists k$ such that $n^2 = 2k + 1$
$\Longrightarrow \exists k$ such that $n^2 - 1 = 2n$
$\Longrightarrow \exists k$ such that $(n - 1)(n + 1) = 2n$
$\Longrightarrow 2 \mid (n - 1)(n + 1)$
$\Longrightarrow 2 \mid (n - 1) \vee 2 \mid (n + 1)$, since 2 is a prime number,
$\Longrightarrow \exists a$ such that $n - 1 = 2a \vee \exists b$ such that $n + 1 = 2b$
$\Longrightarrow \exists a$ such that $n = 2a + 1 \vee \exists b$ such that $n = 2b - 1$.

In both cases, n is odd. Therefore, n is not even.

EXAMPLE

Let n be a positive integer. Using **indirect proof**, prove that

$$\text{if } n^3 + 2n + 1 \text{ is odd, then n is even.}$$

Solution.

The contrapositive is: if n is odd, then $n^3 + 2n + 1$ is even.

If n is odd, then, by definition, it is possible to write $n = 2k + 1$, for some integer k.

Now,

$$n^3 + 2n + 1 = (2k + 1)^3 + 2(2k + 1) + 1 = 2(4k^3 + 6k^2 + 5k + 2)$$

is also even.

EXAMPLE

Prove that if n^3 is an irrational number, then n is an irrational number.

Solution.

This could be proven by considering the **contrapositive** of the given statement: if n is not an irrational number, then n^3 is also not an irrational number.

If n is a rational number, then it is possible to write $n = p/q$, such that p and q are integers with $q \neq 0$. Then, $n^3 = p^3/q^3$.

In other words, n^3 has been expressed as a quotient of two integers, the second one being nonzero. Therefore, n^3 is a rational number.

EXAMPLE

Prove that if m and n are integers and mn is even, then either m is even or n is even.

Solution.

This could be proven by considering the **contrapositive** of the given statement: if it is not true than m is even or n is even, then m and n are both odd.

Then, it is possible to write $m = 2j + 1$, for some integer j, and $n = 2k + 1$, for some integer k. Thus,

$$mn = (2j + 1)(2k + 1) = 4jk + 2j + 2k + 1 = 2(2jk + j + k) + 1,$$

which is also odd.

EXAMPLE

Prove that if n is a positive integer, then n is even if and only if $7n + 4$ is even.

Solution. There are **two parts** of this proof.

(1) If n is even, then 7n + 4 is even.

This is a **direct proof**.

Since n is even, it can be written as 2k, for some integer k. Then, 7n + 4 = 14k + 4 = 2(7k + 2), which is even.

(2) If 7n + 4 is even, then n is even.

This is an **indirect proof**.

Suppose that n is not even, that is, n is odd. Then, n can be written as 2k + 1, for some integer k. Thus, 7n + 4 = 14k + 11 = 2(7k +5) + 1, which is odd.

REMARKS

This example shows that sometimes **multiple proof methods** can be used to solve the same problem.

EXAMPLE

Using **indirect proof**, prove that for all positive real numbers x, if x is an irrational number, then $\sqrt{x}$ is an irrational number.

Solution.

The contrapositive is:

if $\sqrt{x}$ is a rational number, then x is a rational number.

So, suppose $\sqrt{x}$ is a rational number. Then, there exist positive integers p and q such that

$$\sqrt{x} = p/q.$$

Then,

$$x = p^2/q^2,$$

which is a rational number.

EXAMPLE

For propositions p, q, r, and s show that

$$[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)] \longrightarrow (r \vee s)$$

is a tautology.

Solution.

Let LHS be $[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)]$ and RHS be $(r \vee s)$.

This is an implication, which can be false only if the RHS is false. Now, RHS can be false only if both r and s are false.

If r and s are both false, then LHS is

$$(p \vee q) \wedge (p \longrightarrow \mathrm{F}) \wedge (q \longrightarrow \mathrm{F}).$$

Now, p can be either true or false.

Case 1: If p is true, then $(\mathrm{T} \longrightarrow \mathrm{F})$ is false and because of the conjunction, the entire LHS is false. Therefore, one has

$$\mathrm{F} \longrightarrow \mathrm{F},$$

which is true. In this case, $[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)] \longrightarrow (r \vee s)$ is a tautology.

Case 2: If p is false, then LHS is

$$(\mathrm{F} \vee q) \wedge (\mathrm{F} \longrightarrow \mathrm{F}) \wedge (q \longrightarrow \mathrm{F}),$$

or

$$q \wedge \mathrm{T} \wedge (q \longrightarrow \mathrm{F}),$$

or

$$q \wedge (q \longrightarrow \mathrm{F}).$$

Case 2(a): If q is true, then $q \wedge (q \longrightarrow \mathrm{F})$ is $\mathrm{T} \wedge (\mathrm{T} \longrightarrow \mathrm{F})$, which is false. Therefore, one has

$$\mathrm{F} \longrightarrow \mathrm{F},$$

which is true. In this case, $[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)] \longrightarrow (r \vee s)$ is a tautology.

Case 2(b): If q is false, then $q \wedge (q \longrightarrow \mathrm{F})$ is $\mathrm{F} \wedge (\mathrm{F} \longrightarrow \mathrm{F})$, which is false. Therefore, one has

$$\mathrm{F} \longrightarrow \mathrm{F},$$

which is true. In this case, $[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)] \longrightarrow (r \vee s)$ is a tautology.

If either r or s is not false, then RHS must be true. In that case, regardless of the truth value of the LHS, $[(p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow s)] \longrightarrow (r \vee s)$ is true. This completes the proof.

11. VACUOUS PROOF

If it is known **one** of the hypotheses in p is false, then $p \longrightarrow q$ is **vacuously** true. This is because $\mathbf{F} \longrightarrow \mathbf{T}$ and $\mathbf{F} \longrightarrow \mathbf{F}$ are both true.

EXAMPLE

If I am both rich and poor, then a Bugatti Divo moves like a turtle.

Solution.

The hypotheses ($p \wedge \neg p$) form a contradiction. Therefore, q follows from the hypotheses vacuously.

12. TRIVIAL PROOF

If it is known that the conclusion q is true, then $p \longrightarrow q$ is true. This is because $\mathbf{F} \longrightarrow \mathbf{T}$ and $\mathbf{T} \longrightarrow \mathbf{T}$ are both true.

EXAMPLE

If it is February 30th today, then the empty set is a subset of every set.

Solution.

The assertion is **trivially** true, independent of the truth value of the hypotheses p.

13. PROOF BY CONTRADICTION

The unique and peculiar character of mathematical reasoning is best exhibited in proofs of impossibility.
— Mark Kac and Stanislaw Ulam

For any k, assume $P(\mathrm{k}) \wedge \neg Q(\mathrm{k})$ and derive $\neg P(\mathrm{k}) \vee Q(\mathrm{k})$.

It is assumed that the claim is false. Therefore, p is true **and** q is false.

It is then shown that the assumption leads to a contradiction. In other words, p is false **or** q is true. Therefore, the claim is true.

The proof by contradiction uses the logical equivalence:

$$
\begin{aligned}
& p \longrightarrow q \\
\Leftrightarrow\ & \neg p \vee q \\
\Leftrightarrow\ & \neg p \vee q \vee \neg p \vee q \\
\Leftrightarrow\ & (\neg p \vee q) \vee (\neg p \vee q) \\
\Leftrightarrow\ & \neg(p \wedge \neg q) \vee (\neg p \vee q) \\
\Leftrightarrow\ & (p \wedge \neg q) \longrightarrow (\neg p \vee q)
\end{aligned}
$$

EXAMPLE

Using **proof by contradiction** verify that Modus Ponens, $[(p \longrightarrow q) \wedge p] \longrightarrow q$, is a tautology.

Solution.

Let $[(p \longrightarrow q) \wedge p] \longrightarrow q$ not be a tautology. Then, there must be an instance when it is false.

In such a case, (since $[(p \longrightarrow q) \wedge p] \longrightarrow q$ is a conditional) the LHS must be true and the RHS must be false.

This means that $p \longrightarrow q$ is true, p is true, and q is false. However, this is a contradiction, as when p is true and q is false, then $p \longrightarrow q$ is false.

Therefore, the assumption is incorrect, and $[(p \longrightarrow q) \wedge p] \longrightarrow q$, is a tautology.

EXAMPLE

Using **proof by contradiction** verify that Modus Tollens, $[(p \longrightarrow q) \wedge \neg q] \longrightarrow \neg p$, is a tautology.

Solution.

Let $[(p \longrightarrow q) \wedge \neg q] \longrightarrow \neg p$ not be a tautology. Then, there must be an instance when it is false.

In such a case, the LHS must be true and the RHS must be false. Then, $p \longrightarrow q$ and $\neg q$ are true, but $\neg p$ is false. This implies that $p \longrightarrow q$ is true, q is false, and p is true.

Now, since $p \longrightarrow q$ is true and q is false, it follows that p is false.

However, this contradicts the assumption that p is true.

Therefore, the assumption is incorrect, and $[(p \longrightarrow q) \wedge \neg q] \longrightarrow \neg p$, is a tautology.

EXAMPLE

Using **proof by contradiction** verify that

$$[(p \longrightarrow q) \wedge (q \longrightarrow r)] \longrightarrow (p \longrightarrow r)$$

is a tautology.

Solution.

Let $[(p \longrightarrow q) \wedge (q \longrightarrow r)] \longrightarrow (p \longrightarrow r)$ not be a tautology. Then, there must be a time when it is false.

In such a case, the LHS must be true and the RHS must be false.

Now, since RHS is false, p is true and r is false. Furthermore, since LHS is true, both $p \longrightarrow q$ and $q \longrightarrow r$ are true.

Since p is true and $p \longrightarrow q$ is true, q is true.

Since q is true and $q \longrightarrow r$ is true, r is true.

However, this contradicts the fact that r is false.

Therefore, the assumption is incorrect, and $[(p \longrightarrow q) \wedge (q \longrightarrow r)] \longrightarrow (p \longrightarrow r)$, is a tautology.

EXAMPLE

If 5n + 2 is odd, then n is odd.

Solution. This is a proof by contradiction.

Assume the contrary. That is, say n is even.

Then, by definition, it is possible to write n = 2k, for some integer k. However, then 5n + 2 = 5(2k) + 2 = 2(5k + 1) would also be even.

This is a contradiction to the fact that 5n + 2 is odd. Therefore, the assumption is incorrect, and n is odd.

EXAMPLE

For propositions p, q, and r, show that

$$[(p \longrightarrow q) \wedge (\neg p \longrightarrow r) \wedge (q \longrightarrow r)] \longrightarrow r$$

is a tautology.

Solution. This is a proof by contradiction.

Let $P(p, q, r) := [(p \longrightarrow q) \wedge (\neg p \longrightarrow r) \wedge (q \longrightarrow r)]$.

Then, $P(p, q, r) \longrightarrow r$ would be a tautology if it could be shown that it is **not possible** that $P(p, q, r)$ is true and r is false.

Assume the contrary. In other words, assume that $P(p, q, r)$ is true and r is false.

Then:

(a) $p \longrightarrow q$ and (b) $\neg p \longrightarrow r$ and (c) $q \longrightarrow r$ must all be true.

However,

(c) can only be true if q is false.
(b) can only be true if $\neg p$ is false, that is, p is true.
(a) must be false from (b) and (c).

This is a contradiction.

EXAMPLE

Use **proof by contradiction** to show the following:

If the integers 1, 2, 3, …, 7, are placed around a circle, in any order, without repetition, then there exist two adjacent integers that have a sum greater than or equal to 9.

Solution.

Assume the contrary. Then, every pair of adjacent integers placed around a circle has a sum less than or equal to 8.

Now, excluding 1 that must be placed somewhere, there remain exactly three groups of adjacent integers.

The total sum is then (no greater than) 1 + 8 + 8 + 8 = 25.

However, the sum of 1, 2, 3, 4, 5, 6, and 7, should be 28.

This is a contradiction.

EXAMPLE

Prove that the sum of an irrational number and a rational number is an irrational number.

Solution. This is a proof by contradiction.

Suppose that the claim is false.

Therefore, for x rational and y irrational, $x + y$ is rational.

Now, the difference of rational numbers is rational, since

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}.$$

Therefore, $y = (x + y) - x$, and so y must be rational.

This contradicts the hypotheses. Thus, the assumption that the claim was false is incorrect, and the claim must be true.

EXAMPLE

Show that $\sqrt{2}$ is an irrational number.

Solution. This is a proof by contradiction.

Assume the contrary. That is, $\sqrt{2}$ is a rational number r.

Then, using the definition of a rational number, it is possible to write r = p/q, such that p and q are positive integers with $q \neq 0$.

Now, $r^2 = p^2/q^2$, or $p^2 = 2q^2$. Thus, p^2 is an even integer that, in turn, implies that p is an even integer. Let p = 2n, for some integer n.

Thus, $p^2 = (2n)^2 = 2q^2$, or $q^2 = 2n^2$. Thus, q^2 is an even integer that, in turn, implies that q is an even integer.

From this, it can be concluded that the numerator and denominator of r **cannot be co-prime**. This violates the assumption of rationality of r. Therefore, $\sqrt{2}$ is an irrational number.

REMARKS

There are several ways of proving that $\sqrt{2}$ is an irrational number [Laczkovich, 2001]. The **irrationality of $\sqrt{2}$** has been voted to be among the **most beautiful theorems in mathematics**:

Rank	Theorem	Average
(1)	$e^{i\pi} = -1$	7.7
(2)	Euler's formula for a polyhedron: $V + F = E + 2$	7.5
(3)	The number of primes is infinite.	7.5
(4)	There are 5 regular polyhedra.	7.0
(5)	$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots = \pi^2/6.$	7.0
(6)	A continuous mapping of the closed unit disk into itself has a fixed point.	6.8
(7)	There is no rational number whose square is 2.	6.7
(8)	π is transcendental.	6.5
(9)	Every plane map can be coloured with 4 colours.	6.2
(10)	Every prime number of the form $4n + 1$ is the sum of two integral squares in exactly one way.	6.0

REMARKS

- There can be other criteria of a 'good' proof besides 'beauty'. For example, a good' proof could be **interesting** [Kugel, 1976; Thomas, 2016]

- The approach for proving that $\sqrt{2}$ is an irrational number can be **generalized** to some, but not all, cases. For example, it can be used to prove that $\sqrt{2} + 1$ and $\sqrt{8}$ are both irrational numbers.

EXAMPLE

Show that $\sqrt{3}$ is an irrational number.

Solution. Improvise. (Use the fact that if $3 \mid p^2$ then $3 \mid p$.)

EXAMPLE

Prove or disprove that the product of a nonzero rational number and an irrational number is an irrational number.

Solution. This is a proof by contradiction.

Let p/q be a nonzero rational number and x be an irrational number. The goal is to prove that the product xp/q is also an irrational number.

Suppose that xp/q were a rational number. Since p/q $\neq 0$, it can be concluded that p $\neq 0$, and so q/p is also a rational number.

The product of two rational numbers is a rational number. However, the product

$$(x\text{p/q}) \cdot (\text{q/p}) = x$$

is, by assumption, an irrational number. This is a contradiction, and so xp/q is an irrational number.

EXAMPLE

For n a positive integer that is not a perfect square, prove that $\sqrt{2} + \sqrt{3}$ is irrational.

(Use the following result: for n a positive integer that is not a perfect square, $\sqrt{n}$ is irrational.)

Solution. This is a proof by contradiction.

If $\sqrt{2} + \sqrt{3}$ were a rational number, then so would be $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$. Then, subtracting 5 and dividing by 2 shows that $\sqrt{6}$ is a rational number. However, this is a contradiction to the result to be used.

EXAMPLE

Prove that if n is an integer and 3n + 2 is even, then n is even, using

(a) a proof by contraposition, and
(b) a proof by contradiction.

Solution.

(a) Suppose that n is odd. Then, it is possible to write n = 2k + 1, for some integer k. Then 3n + 2 = 3(2k + 1) + 2 = 6k + 5 = 2(3k + 2) + 1. Thus, 3n + 2 is odd.

(b) Suppose that 3n + 2 is even and that n is odd. Since 3n + 2 is even, so is 3n. If an odd integer is subtracted from an even integer, the result is an odd integer, so 3n – n = 2n is odd. However, this is obviously not true. Therefore, the assumption is wrong, and n is even.

14. PROOF BY CASES

Break the premise of $p \longrightarrow q$ into an **equivalent disjunction** of the form $p_1 \vee p_2 \vee \ldots \vee p_n$.

Then, use the tautology

$$[\,(p_1 \longrightarrow q) \wedge (p_2 \longrightarrow q) \wedge \cdots \wedge (p_n \longrightarrow q)\,]$$
$$\longleftrightarrow$$
$$[\,(p_1 \vee p_2 \vee \cdots \vee p_n) \longrightarrow q\,]$$

Each of the implications $p_i \longrightarrow q$ is a **case**.

There is a need to ensure that:

- The cases are inclusive, that is, they **exhaust** all possibilities.
- All implications are established.

EXAMPLE

Show that $|\,x\,|^2 \geq 0$ for any real number x.

Solution. There are three cases:

(1) $x < 0$.
(2) $x = 0$.
(3) $x > 0$.

The rest is straightforward, by the definition of **absolute value function**.

EXAMPLE

Let $n \in \mathbf{Z}^+$. Then,

$$6 \mid n(n + 1)(n + 2) .$$

The relevant divisors of 6 are 2 and 3.

It is **always** that $2 \mid n$ or $2 \mid (n + 1)$, since either n is even or n is odd.

There remain **three cases** to be considered.

For some $k \in \mathbf{Z}^+$, $k \geq 0$:

1. $n = 3k$. In this case, $3 \mid n$,
2. $n = 3k + 1$. In this case, $3 \mid (n + 2)$,
3. $n = 3k + 2$. In this case, $3 \mid (n + 1)$.

In proving certain assertions, it is **not** necessary to consider **all** possible cases, as the arguments behind some cases are, essentially, the same as or similar to other cases. This notion is known as **Without Lost Of Generality (WLOG)**.

EXAMPLE

Prove that $5x + 5y$ is an odd integer when x and y are integers of opposite parity.

(The term **"parity"** means that if one is even, then the other is odd, and conversely.)

Solution.

It is given that x and y are of opposite parities. Therefore, it can be assumed, without loss of generality, that x is even and y is odd. (The proof of x is odd and y is even is the same.)

This implies that $x = 2m$, for some integer m, and $y = 2n + 1$, for some integer n. Then,

$$5x + 5y = 5(2m) + 5(2n + 1) = 10(m + n) + 5 = 5 \cdot [2(m + n) + 1],$$

which means that $5x + 5y$ is an odd number.

15. PROVING AN EQUIVALENCE

To prove that $p \Leftrightarrow q$, there is a need to show that $p \leftrightarrow q$ is a tautology.

This can be done by showing that $p \longrightarrow q$ and $q \longrightarrow p$ are both true since,

$$p \leftrightarrow q \Leftrightarrow [(p \longrightarrow q) \wedge (q \longrightarrow p)]$$

This can be **generalized** to arbitrary (but finite) number of propositions.

To prove that $p_1 \Leftrightarrow p_2 \Leftrightarrow p_3 \Leftrightarrow \ldots \Leftrightarrow p_n$, there is a need to show that $p_1 \leftrightarrow p_2 \leftrightarrow p_3 \cdots \leftrightarrow p_n$ is a tautology.

This can be done by showing that $p_1 \longrightarrow p_2, p_2 \longrightarrow p_3, \ldots, p_n \longrightarrow p_1$, are all true since,

$$[p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n]$$
$$\Leftrightarrow$$
$$[(p_1 \longrightarrow p_2) \wedge (p_2 \longrightarrow p_3) \wedge \cdots \wedge (p_n \longrightarrow p_1)]$$

EXAMPLE

The integer n is odd if and only if n^2 is odd.

Solution. Improvise. (The "only if" part has been done; so the "if" part needs to be done.)

16. EXISTENCE PROOF

The proof of $\exists x\, P(x)$ is called an existence proof.

There are two types of existence proofs: **constructive and non-constructive**.

1. **Constructive Existence Proof.** Find an element c in the universe of discourse such that $P(c)$ is true.

2. **Non-Constructive Existence Proof.** Assume no c exists that makes $P(c)$ true. Derive a contradiction.

EXAMPLE

(a) Show that there exist positive integers x, y, and z such that

$$x^2 + y^2 = z^2.$$

(b) Show that there exist positive integers x, y, and z such that

$$x^3 + y^3 = z^2.$$

Solution. Improvise.

EXAMPLE

Show that there exist irrational numbers a and b such that a^b is a rational number.

Solution 1.

Let $a = \sqrt{2}$ and $b = \log_2(9)$. Then, $a^b = 3$.

- This is a **constructive existence proof**. That is because examples of a and b are shown **explicitly**.

- The assertion can also be proven using a **non-constructive existence proof**.

Solution 2.

Perhaps a thing is simple if you can describe it fully in several different ways without immediately knowing that you are describing the same thing.
— Richard P. Feynman

Let $a = \sqrt{2}$ and $b = \sqrt{2}$.

Then, $c = (\sqrt{2})^{\sqrt{2}}$ is either a rational number or an irrational number.

If c is a rational number, then the assertion is proven. If c is an irrational number, then the assertion is proven with $a = (\sqrt{2})^{\sqrt{2}}$ and $b = \sqrt{2}$ since

$$((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = 2.$$

REMARKS

The use of **"if"** in the solution 2 of the previous example is important. It does **not** say that "c is an irrational number" explicitly. This is the reason why the proof is non-constructive.

The above example can be generalized:

Gelfond-Schneider Theorem. If a and b are algebraic numbers with $a \neq 0$ or 1, and b is an irrational number, then any value of a^b is a transcendental number.

REMARKS

- The **Gelfond-Schneider Theorem** establishes the **transcendence** of a large class of numbers [Laczkovich, 2001].

- The **Gelfond-Schneider Theorem** is a response to **Hilbert's Seventh Problem**.

EXAMPLE

There exists an irrational number between any two rational numbers.

Solution. Improvise. (The solution is in the scope of **Real Analysis**.)

17. PROOF BY DISREFUTATION

Disproving claims can sometimes be much easier than proving them.

Claims are usually of the form $\forall k\ P(k)$. Thus, to disprove, it is enough to find **one** k that makes $P(k)$ false. This one k is called a **counterexample**.

This process is known as **disrefutation by counterexample**.

EXAMPLE

Prove or disprove that the product of irrational numbers is an irrational number.

Solution.

Let $x = \sqrt{2}$ and $y = 1/\sqrt{2}$.

Now, both x and y are irrational numbers.

However, their product

$$xy = \sqrt{2} \cdot 1/\sqrt{2} = 1,$$

is a rational number.

EXAMPLE

Prove or disprove that if a and b are rational numbers, then a^b is also a rational number.

Solution.

Let $a = 2$ and $b = 1/2$. Then $a^b = 2^{1/2} = \sqrt{2}$, which is not a rational number.

EXAMPLE

Show that if a, b, and c are real numbers and $a \neq 0$, then there is a unique solution of the equation $ax + b = c$.

Solution.

The equation $ax + b = c$ is equivalent to the equation $x = (c - b)/a$.

EXAMPLE

Use **forward reasoning** to show that if x is a nonzero real number, then

$$x^2 + \frac{1}{x^2} \geq 2.$$

Solution.

The square of every real number is nonnegative, and so

$$\left(x - \frac{1}{x}\right)^2 \geq 0.$$

This simplifies to

$$x^2 - 2 + 1/x^2 \geq 0,$$

and so

$$x^2 + \frac{1}{x^2} \geq 2,$$

as desired.

18. MATHEMATICAL INDUCTION

Induction makes you feel guilty for getting something out of nothing, and it is artificial, but it is one of the greatest ideas of civilization.
— Herbert S. Wilf

The term ‘mathematical induction’ was introduced in the 19th century [Gunderson, 2010, Section 1.8], although the ideas behind induction go back several centuries earlier [Roberts, 2010, Chapter 6].

The purpose of mathematical induction is to prove propositions of the form ∀n P(n), where the universe of discourse usually is the set of positive integers.

It can be noted that mathematical induction can be used only to prove results obtained in some other way. It is **not** an avenue for discovering theorems.

There are a variety of **applications of mathematical induction in computer science** [O’Donnell, Hall, Page, 2006, Chapter 4]:

- **Proving Properties of Recursion Schemes.** Mathematical induction is a natural tool for proving properties of recursively defined objects.

- **Confirming Validity of Conjectures/Theorems.** Mathematical induction can be used to show the validity of summation formulas, inequalities, divisibility results, and so on.

- **Checking Algorithm (Program) Correctness.** Mathematical induction can be used to show that algorithms (programs) using iterative loops are correct.

18.1. PRINCIPLE OF MATHEMATICAL INDUCTION

Statement:

If:

[**Basis**]
$P(0)$ (or the smallest case)
[**Induction**]
$\forall n\ P(n) \longrightarrow P(n + 1)$

Then:

$\forall n\ P(n)$

Proof.

In [Gunderson, 2010, Section 2.4], a proof of correctness of mathematical induction has been given.

18.2. WELL-ORDERED SETS

An **axiom** is a statement that is taken to be true, to serve as a premise or starting point for further reasoning and arguments [Wikipedia].

The **validity of mathematical induction** follows from the following fundamental axiom about the set of integers.

Axiom [The Well Ordering Property]. Every non-empty subset of nonnegative integers has a smallest element.

EXAMPLE

Find, if possible, the smallest element of the set $\{\lfloor 5.99 + 1/n \rfloor \mid n \in \mathbf{Z}^+\}$.

Solution. The smallest element of $\{\lfloor 5.99 + 1/n \rfloor \mid n \in \mathbf{Z}^+\}$ is 5. (For example, setting n = 1 gives 6, but setting n = 1000 gives 5.)

REMARKS

The well ordering property does **not** necessarily apply to number systems **other than nonnegative integers**. For example, the well-ordering property does **not** apply to **infinite subsets of negative integers** or to **subsets of R**.

EXAMPLE

Find, if possible, the smallest element of the set $\{5.99 + 1/n \mid n \in \mathbf{R}\}$.

Solution. The set $\{5.99 + 1/n \mid n \in \mathbf{R}\}$ does **not** have a smallest element. (It does have limit-point 5.99, though.)

18.3. THE PROCESS OF MATHEMATICAL INDUCTION

A proof by mathematical induction consists of two steps:

1. Basis Step.
2. Inductive Step.

It is **important** to realize that **both** the basis step and the inductive step are needed for the proof. If the proof does not use both the steps, then it is **incorrect**.

Basis Step.

Show that the proposition holds for n = 0 (**or** whatever the smallest case is).

Usually, the **difficulties** about the base case lie in **understanding** what is meant when n = 0 (or the smallest case) or **finding** the smallest case.

Inductive Step.

Show that if the proposition holds for n, then statement holds for n + 1.

For formulas, this amounts to experimenting with formula for n and algebraically deriving the formula for n + 1.

Expressed as a rule of inference, mathematical induction proof approach can be stated as

$$[P(0) \wedge \forall n\,(P(n) \longrightarrow P(n+1))] \longrightarrow \forall n\,P(n).$$

REMARKS

In a proof by mathematical induction, it is **not** assumed that $P(n)$ is true for all positive integers. It is only shown that **if** it is assumed that $P(n)$ is true, then $P(n + 1)$ is also true. (This should be evident from the implication $P(n) \longrightarrow P(n + 1)$.) Thus, a proof by mathematical induction is **not** a case of **circular reasoning**.

EXAMPLE

Use mathematical induction to prove that for all positive integers n

$$(n^3 - n) \textbf{ mod } 3 = 0.$$

Solution.

Basis Step. n = 1.

$$(1^3 - 1) \textbf{ mod } 3 = (0) \textbf{ mod } 3 = 0.$$

Inductive Hypothesis. It is **assumed** that $(n^3 - n)$ **mod** 3 = 0, for all positive integers n.

Inductive Step. n > 1.

There is a need to show that

$$[(n + 1)^3 - (n + 1)] \textbf{ mod } 3 = 0.$$

It can be seen that,

$[(n + 1)^3 – (n + 1)]$ **mod** 3
$= (n^3 + 3n^2 + 3n – n)$ **mod** 3
$= [3(n^2 + n) + n^3 – n]$ **mod** 3
$= [(3(n^2 + n))$ **mod** $3 + (n^3 – n)$ **mod** $3]$ **mod** 3
$= [0 + (n^3 – n)$ **mod** $3]$ **mod** 3
$= (n^3 – n)$ **mod** 3
= 0, by the inductive hypothesis.

Therefore, by the Principle of Mathematical Induction, $(n^3 – n)$ **mod** 3 = 0, all positive integers n.

EXAMPLE

Use mathematical induction to prove that for all positive integers n

$$1 + 2 + 3 + \cdots + n = n(n + 1)/2.$$

Solution. Improvise. Use the following in the inductive step:

$$n(n + 1)/2 + (n + 1) = (n + 1)(n + 2)/2.$$

EXAMPLE

Use mathematical induction to prove that

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

Solution. Improvise. Use the following in the inductive step:

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

EXAMPLE

Use mathematical induction to prove that for all positive integers n

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} – 1.$$

Solution. Improvise. **(**Show that $2^{n+1} – 1 + 2^{n+1} = 2^{n+2} – 1$.)

EXAMPLE

Use mathematical induction to prove that for all positive integers n

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

Solution. Improvise. Use the following in the inductive step:

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

EXAMPLE

Prove that

$$1^3 + 2^3 + \cdots + n^3 = (n(n + 1)/2)^2,$$

for the positive integer n.

Solution. Improvise. Use the following in the inductive step:

$$\left(\frac{n(n + 1)}{2}\right)^2 + (n + 1)^3 = (n + 1)^2 \left(\frac{n^2}{4} + n + 1\right) = (n + 1)^2 \left(\frac{n^2 + 4n + 1}{4}\right) = \left(\frac{(n + 1)(n + 2)}{2}\right)^2.$$

EXAMPLE

Use mathematical induction to prove that

$$n! \geq 2^n,$$

for all integers $n > 3$.

Solution.

(It can be checked that the inequality does **not** hold for $n \leq 3$.)

Basis Step. $n = 4$.

$$4! = 24 \geq 2^4 = 16.$$

Inductive Hypothesis. It is **assumed** that $n! \geq 2^n$, for all integers $n > 3$.

Inductive Step. $n > 4$.

There is a need to show that

$$(n + 1)! \geq 2^{(n + 1)}.$$

It can be seen that,

$(n + 1)!$
$= (n + 1) \cdot n!$
$\geq (n + 1) \cdot 2^n$, by the inductive hypothesis
$= n2^n + 2^n$
$\geq 2^n + 2^n$, since $n > 4$
$= 2^{(n + 1)}$.

Therefore, by the Principle of Mathematical Induction, $n! \geq 2^n$, for all integers $n > 3$.

EXAMPLE

Prove that

$$n! < n^n,$$

where n is an integer greater than 1.

Solution. Improvise. Use the following in the inductive step:

$$(k + 1)! = (k + 1)k! < (k + 1)k^k < (k + 1)(k + 1)^k = (k + 1)^{k+1}.$$

EXAMPLE

Prove that

$$1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n + 1)! - 1,$$

whenever n is a positive integer.

Solution. Improvise. Use the following in the inductive step:

$$(k + 1)! - 1 + (k + 1) \cdot (k + 1)! = (k + 1)!(1 + k + 1) - 1.$$

EXAMPLE

Prove that

$$(n^2 + n) < 2^n,$$

whenever n is an integer greater than 4.

Solution. Improvise. Use the following in the inductive step:

$$[(k + 1)^2 + (k + 1)] = [k^2 + 3k + 2] < k^2 + 4k < k^2 + k^2 = 2k^2 < 2(k^2 + k) < 2 \cdot 2^k = 2^{k+1}.$$

EXAMPLE

Prove that for every positive integer n,

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n + 1)(n + 2) = n(n + 1)(n + 2)(n + 3)/4.$$

Solution. Improvise. Use the following in the inductive step:

$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + k(k + 1)(k + 2) + (k + 1)(k + 2)(k + 3)$

$= [\ k(k + 1)(k + 2)(k + 3)/4\ ] + (k + 1)(k + 2)(k + 3)$

$= (k + 1)(k + 2)(k + 3)\ [\ k/4 + 1]$

$= (k + 1)(k + 2)(k + 3)(k + 4)/4.$

EXAMPLE

Prove that

$$3 \mid (n^3 + 2n),$$

whenever n is a positive integer.

Solution. Improvise. Use the following in the inductive step:

$$(k + 1)^3 + 2(k + 1) = k^3 + 3k^2 + 3k + 1 + 2k + 2 = (k^3 + 2k) + 3(k^2 + k + 1).$$

EXAMPLE

Prove that

$$2 - 2 \cdot 7 + 2 \cdot 7^2 - \cdots + 2(-7)^n = (1 - (-7)^{n+1})/4,$$

whenever n is a nonnegative integer.

Solution. Improvise. Use the following in the inductive step:

$$\begin{aligned}
&\left[2 - 2\cdot 7 + 2\cdot 7^2 - \cdots + 2\cdot(-7)^n\right] + 2\cdot(-7)^{n+1} \\
&= \frac{1 - (-7)^{n+1}}{4} + 2\cdot(-7)^{n+1} \\
&= \frac{1 - (-7)^{n+1} + 8\cdot(-7)^{n+1}}{4} \\
&= \frac{1 + 7\cdot(-7)^{n+1}}{4} \\
&= \frac{1 - (-7)\cdot(-7)^{n+1}}{4} \\
&= \frac{1 - (-7)^{(n+1)+1}}{4}.
\end{aligned}$$

EXAMPLE

Determine the nonnegative integers n for which

$$n^2 \le n!.$$

Prove your claim using mathematical induction.

Solution. Improvise. This requires **trial-and-error** (a **combination of mental and manual labor**).

It can be checked that the inequality holds for n = 0 and n = 1, but does **not** hold for n = 2 or n = 3.

It can be noted that **factorial increases far more rapidly than the square** as the number increases. (This can be checked by graphing the two together.)

The basis step in fact is n = 4.

Use the following in the inductive step:

$(n + 1)^2 = n^2 + 2n + 1$
$\leq n! + 2n + 1$
$\leq n! + 2n + n = n! + 3n$
$\leq n! + n \cdot n$
$\leq n! + n \cdot n! = (n + 1)n! = (n + 1)!.$

EXAMPLE

Prove that for every positive integer n,

$$\sum_{k=1}^{n} k \cdot 2^k = (n - 1)2^{n+1} + 2.$$

Solution. Improvise. Use the following in the inductive step:

$$\sum_{k=1}^{n+1} k \cdot 2^k = \left(\sum_{k=1}^{n} k \cdot 2^k \right) + (n + 1)2^{n+1} = (n - 1)2^{n+1} + 2 + (n + 1)2^{n+1} = 2n \cdot 2^{n+1} + 2 = 2n \cdot 2^{n+2} + 2.$$

EXAMPLE

Determine the positive integers n for which

$$2^n \geq n^2.$$

Prove your claim using mathematical induction.

Solution. Improvise. (It can be checked that the inequality holds for n = 1 and n = 2, but does **not** hold for n = 3. It can be noted that **exponential increases far more rapidly than the square** as the power increases.)

EXAMPLE

Use mathematical induction to prove that for all integers $n > 6$

$$3^n < n!.$$

Solution.

(It can be checked that the inequality does **not** hold for $n \leq 6$.)

Basis Step. $n = 7$.

$$3^7 = 2187 < 5040 = 7!$$

Inductive Step. $n > 7$.

There is a need to show that

$$3^{(n+1)} < (n+1)!.$$

It can be seen that,

$$3^{(n+1)} = 3 \cdot 3^n < 3 \cdot n! < (n+1) \cdot n! = (n+1)!.$$

Therefore, by the Principle of Mathematical Induction, $3^n < n!$, for $n \geq 7$.

EXAMPLE

Use mathematical induction to prove that for all positive integers n

$$n < 2^n.$$

Solution. Improvise. **(**Use the fact that $1 < 2^n$, for all positive integers n.)

EXAMPLE

Use mathematical induction to prove that for a real numbers a and r, $r \neq 0$ or 1, and for all nonnegative integers n

$$a + ar + ar^2 + \cdots + ar^n = (ar^{n+1} - a) / (r - 1).$$

(The LHS is the **geometric series** and the RHS is the **partial sum** of the **geometric series**.)

Solution. Improvise. (Show that $(ar^{n+1} - a) / (r - 1) + ar^{n+1} = (ar^{n+2} - a) / (r - 1)$.)

EXAMPLE

Use mathematical induction to show that

$$6 \mid (n^3 - n),$$

when n is a non-negative integer.

Solution.

Basis Step. $n = 0$.

$$6 \mid (0^3 - 0) = 0.$$

Inductive Step. $n > 0$.

There is a need to show that

$$6 \mid [(n + 1)^3 - (n + 1)].$$

It can be seen that,

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

Now, by the inductive hypothesis, $6 \mid (n^3 - n)$. Also, since $n(n + 1)$ is even, $6 \mid 3n(n + 1)$.

Therefore, by the Principle of Mathematical Induction, $6 \mid (n^3 - n)$, when n is a non-negative integer.

EXAMPLE

Use mathematical induction to show that,

$$21 \mid (4^{n+1} + 5^{2n-1}),$$

whenever n is a positive integer.

Solution.

Basis Step. n = 1.

$$21 \mid (4^{n+1} + 5^{2n-1}) = (4^{1+1} + 5^{2-1}) = 21.$$

Inductive Step. n > 1.

$(4^{n+2} + 5^{2n+1})$
$= 4(4^{n+1} + 5^{2n-1}) - 4 \cdot 5^{2n-1} + 5^{2n+1}$
$= 4(4^{n+1} + 5^{2n-1}) - 4 \cdot 5^{2n-1} + 25 \cdot 5^{2n-1}$
$= 4(4^{n+1} + 5^{2n-1}) + 21 \cdot 5^{2n-1}.$

The first term is divisible by 21 due to the inductive hypothesis and the second term is obviously divisible by 21.

Therefore, by the Principle of Mathematical Induction, $21 \mid (4^{n+1} + 5^{2n-1})$, whenever n is a positive integer.

EXAMPLE

Use mathematical induction to prove that the sum of the first n odd positive integers is n^2. In other words,

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

Solution.

Basis Step. n = 1.

$$\text{LHS} = 1 = 1^2 = \text{RHS}.$$

Inductive Step. $n > 1$.

LHS
$= 1 + 3 + 5 + \cdots + (2(n + 1) - 1)$
$= 1 + 3 + 5 + \cdots + (2n - 1) + [2(n + 1) - 1]$
$= n^2 + [2n + 1]$
$= (n + 1)^2$
= RHS.

Therefore, by the Principle of Mathematical Induction, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

EXAMPLE

Prove that $n^2 - 7n + 12$ is nonnegative whenever n is an integer with $n \geq 3$.

Solution. Improvise. Use the following in the inductive step:

$$(n + 1)^2 + 7(n + 1) + 12 = n^2 + 2n + 1 - 7n - 7 + 12 = (n^2 - 7n + 12) + (2n - 6).$$

EXAMPLE

Let a and b be real numbers with $0 < b < a$. Prove that if n is a positive integer, then

$$a^n - b^n \leq na^{n-1}(a - b).$$

Solution. Improvise.

It is easier to think about the given statement as $na^{n-1}(a - b) \geq a^n - b^n$. Use the following in the inductive step:

$$(k + 1)a^k(a - b) \geq a(a^k - b^k) + a^k(a - b).$$

EXAMPLE

Prove the following by mathematical induction:

$$1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} > 1 - \frac{1}{2^n},$$

for $n \geq 0$.

Solution. Improvise. Use the following in the inductive step:

$$\left(1 - \frac{1}{2^n}\right) + \frac{1}{2^{n+1}} = \left(1 - \frac{1}{2^{n+1}}\right).$$

18.4. FIBONACCI NUMBERS

A000045

The **Fibonacci Sequence of numbers** is defined **recursively** by

$$f_0 = 0,$$

$$f_1 = 1,$$

and

$$f_n = f_{n-1} + f_{n-2},$$

for $n > 1$.

Thus:

$$\{f_n\} = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \text{and so on.}$$

REMARKS

- The first two numbers in the Fibonacci Sequence are either **0 and 1**, or **1 and 1**, depending on the chosen starting point of the sequence, and each **subsequent number** is the **sum of the previous two**.

- It could be noted that **every third** Fibonacci Number is **even**. Using mathematical induction, it is possible to prove that this is true in general.

- The Fibonacci Sequence has several applications, including the use of it to **create beautiful art and geometries** [Maor, Jost, 2014, Chapter 20].

EXAMPLE

For all natural numbers n,

$$2 \mid f_{3n}.$$

Proof.

Basis Step. n = 0.

$$f_{3\cdot 0} = f_0 = 0, \text{ which is divisible by 2.}$$

Inductive Step. n > 0.

It can be seen that,

$$f_{3n} = f_{3n-1} + f_{3n-2} = (f_{3n-2} + f_{3n-3}) + f_{3n-2} = 2f_{3n-2} + f_{3n-3} = 2f_{3n-2} + f_{3(n-1)}.$$

Now, by the inductive hypothesis, $2 \mid f_{3(n-1)}$. Thus, $2 \mid (2f_{3n-2} + f_{3(n-1)})$.

Therefore, by the Principle of Mathematical Induction, $2 \mid f_{3n}$, all natural numbers n.

EXAMPLE

Use mathematical induction to show that, when n is a positive integer, the terms of the Fibonacci Sequence satisfy the following:

$$(f_1)^2 + (f_2)^2 + \cdots + (f_n)^2 = f_n \cdot f_{n+1}.$$

Solution. Improvise.

Basis Step. n = 1.

$$(f_1)^2 = 1 = f_1 \cdot f_2.$$

Inductive Step. n > 1.

$$(f_1)^2 + (f_2)^2 + \cdots + (f_n)^2 + (f_{n+1})^2 = (f_n \cdot f_{n+1}) + (f_{n+1})^2 = f_{n+1} \cdot (f_n + f_{n+1}) = f_{n+1} \cdot f_{n+2}.$$

EXAMPLE

Use mathematical induction to show that, when n is a positive integer, the terms of the Fibonacci Sequence satisfy the following:

$$f_0 - f_1 + f_2 - \cdots - f_{2n-1} + f_{2n} = f_{2n-1} - 1.$$

Solution. Improvise.

(For the inductive step (n + 1), find and organize the terms on the LHS. Then, use the inductive hypothesis and the definition of Fibonacci Numbers to derive the following:

$(f_0 - f_1 + f_2 - \cdots - f_{2n-1} + f_{2n}) - f_{2n+1} + f_{2n+2}$
$= (f_{2n-1} - 1) - f_{2n+1} + f_{2n+2}$
$= f_{2n-1} - 1 + f_{2n}$
$= f_{2n+1} - 1.$)

EXAMPLE

Use mathematical induction to show that, for every n ≥ 2, the terms of the Fibonacci Sequence satisfy the following:

$$f_{n-1} \cdot f_{n+1} - (f_n)^2 = (-1)^n.$$

(This is known as the **Cassini's Identity** [Erickson, 2010, Page 28].)

Solution.

$\{f_n\}$ = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, and so on.

Basis Step. n = 2.

$$f_1 \cdot f_3 - (f_2)^2 = 2 - 1 = 1 = (-1)^2.$$

Inductive Step. n > 2.

To show that,

$$f_n \cdot f_{n+2} - (f_{n+1})^2 = (-1)^{n+1},$$

or

$$f_n \cdot f_{n+2} - (f_{n+1})^2 = -(-1)^n,$$

or

$$f_n \cdot f_{n+2} - (f_{n+1})^2 = -[\, f_{n-1} \cdot f_{n+1} - (f_n)^2],$$

or

$$[\, f_n \cdot f_{n+2} - (f_{n+1})^2 \,] + [\, f_{n-1} \cdot f_{n+1} - (f_n)^2] = 0.$$

Now, LHS, after a rearrangement, is

$$f_n \cdot [\, f_{n+2} - f_n \,] - f_{n+1} \cdot [\, f_{n+1} - f_{n-1} \,] = f_n \cdot f_{n+1} - f_{n+1} \cdot f_n = 0.$$

18.5. THE GOLDEN RATIO

A001622

In mathematics, two quantities are in the Golden Ratio if their ratio is the same as the ratio of their sum to the larger of the two quantities. In other words, say a and b are two quantities, with $a > b > 0$.

Then, the **Golden Ratio**, φ, is given by

$$(a + b) / a = a / b = \varphi.$$

It is possible to express the **meaning** of the Golden Ratio **geometrically**, as shown in Figure 3.

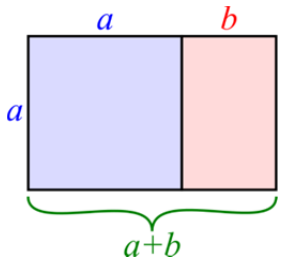


Figure 3. A geometrical interpretation of the Golden Ratio. (Source: Wikipedia.)

A **golden rectangle** with longer side *a* and shorter side b, when placed adjacent to a square with sides of length a, will produce a **similar golden rectangle** with longer side *a* + *b* and shorter side *a*. This illustrates the relationship (*a* + *b*) / *a* = *a* / *b* = φ. (Source: Wikipedia.)

PROPERTIES OF THE GOLDEN RATIO

The Golden Ratio has many **interesting properties** [Khare, Lachowska, 2015, Chapter 4].

The Golden Ratio is an **irrational number**:

$$\frac{1 + \sqrt{5}}{2}.$$

The **limit of the ratios of successive terms** of the Fibonacci Sequence is the **Golden Ratio**.

The **Fibonacci Spiral** is an **approximation of the golden spiral** created by drawing circular arcs connecting the opposite corners of squares in the Fibonacci Tiling, as shown in Figure 4. (This one uses squares of sizes 1, 1, 2, 3, 5, 8, 13, 21, and 34.)

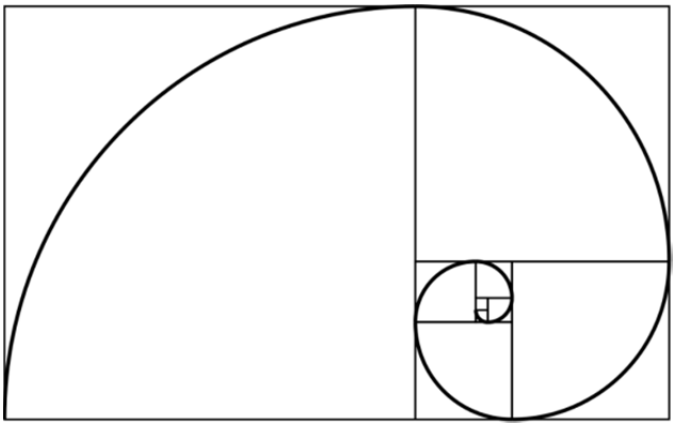


Figure 4. Fibonacci Spiral. (Source: Wikipedia.)

18.6. BINOMIAL COEFFICIENTS AND IDENTITIES

FACTORIAL

The **factorial** of a nonnegative integer n is denoted by n! and is defined by

$$n! = \begin{cases} 1, & \text{if } n = 0 \\ 1 \cdot 2 \cdot 3 \cdots n, & \text{if } n > 0. \end{cases}$$

For example,

$$1! = 1 \text{ and } 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$$

The factorials grow rather quickly.

For example,

$$10! = 3628800 \text{ and } 100! = 9.332621544 \times 10^{157}.$$

REMARKS

The conventional notion of factorial does **not** apply to fractions. This is one of the motivations for the extension of the Factorial Function to **Gamma Function**.

BINOMIAL COEFFICIENTS

Let n and k be nonnegative integers such that $k \leq n$. Then,

$$C(n, k) = n!/k!(n - k)!$$

(C(n, k) is called the **Binomial Coefficient**.)

For example,

$$C(1, 1) = 1, C(n, 0) = 1, \text{ and } C(n, n) = 1.$$

Let n and k be nonnegative integers such that $k \leq n$.

Then,

$$C(n, k) = C(n, n - k).$$

For example,

$$C(n, 0) = C(n, n) = 1.$$

Let n and k be positive integers such that $k \leq n$.

Then,

$$C(n + 1, k) = C(n, k - 1) + C(n, k).$$

(This is the **Pascal's Identity** [Erickson, 2010, Page 6].)

For example,

$$C(n + 1, 1) = C(n, 0) + C(n, 1) = C(n, 1) + C(1, 1).$$

REMARKS

The **Pascal's Triangle** is a triangular array of the **Binomial Coefficients** [Neto, 2017, Chapter 4], as shown in Figure 5.

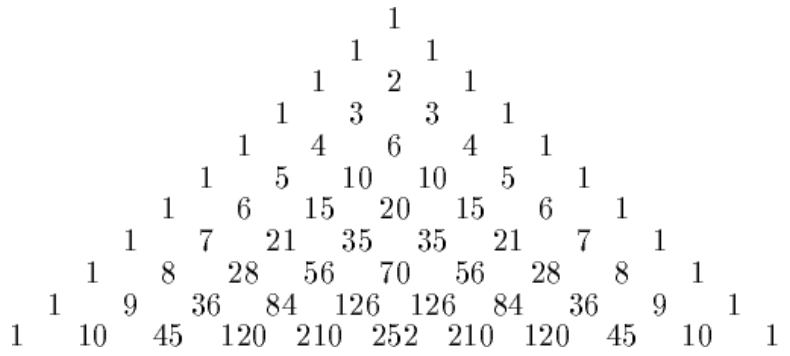


Figure 5. Pascal's Triangle: View 1. (Source: Google Images.)

If the **rows** of the **Pascal's Triangle** are **left-justified**, the **diagonal colored bands** add up to successive **Fibonacci Numbers**, as shown in Figure 6.

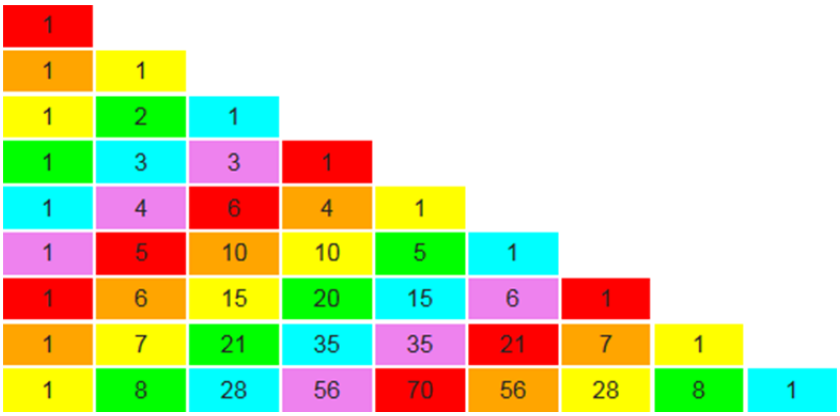


Figure 6. Pascal's Triangle: View 2. (Source: Wikipedia.)

EXAMPLE

Use mathematical induction to show that for a nonnegative integer n, and nonzero a and b,

$$(a + b)^n = a^n + C(n, 1)\cdot a^{(n-1)}b + C(n, 2)\cdot a^{(n-2)}b^2 + \cdots + C(n, n-1)\cdot ab^{(n-1)} + b^n.$$

(This is the **Binomial Theorem**.)

Solution.

Basis Step. n = 0.

$$LHS = (a + b)^0 = 1 = RHS.$$

Inductive Step. $n > 0$.

It can be seen that,

LHS

$= (a + b)^{(n + 1)}$
$= (a + b)(a + b)^n$
$= (a + b)(a^n + C(n, 1)\cdot a^{(n-1)}b + C(n, 2)\cdot a^{(n-2)}b^2 + \cdots + C(n, n - 1)\cdot ab^{(n-1)} + b^n)$

$=$

$a^{(n + 1)}$

$+$

$C(n, 1)\cdot a^n b + C(n, 2)\cdot a^{(n-1)}b^2 + \cdots + C(n, n - 1)\cdot a^2 b^{(n-1)} + ab^n$

$+$

$a^n b + C(n, 1)\cdot a^{(n-1)}b^2 + C(n, 2)\cdot a^{(n-2)}b^3 + \cdots + C(n, n - 1)\cdot ab^n$

$+$

$b^{(n + 1)}$

$=$

$a^{(n + 1)}$

$+$

$[C(n, 1) + C(1, 1)]\cdot a^n b + [C(n, 2) + C(n, 1)]\cdot a^{(n-1)}b^2 + \cdots + [C(n, n - 1) + C(1, 1)]\cdot ab^n$

$+$

$b^{(n + 1)}$

$= a^{(n+1)} + C(n + 1, 1)\cdot a^n b + C(n + 1, 2)\cdot a^{(n-1)}b^2 + \cdots + C(n + 1, n)\cdot ab^n + b^{(n+1)}$

= RHS.

Therefore, by the Principle of Mathematical Induction, $(a + b)^n = a^n + C(n, 1)\cdot a^{(n-1)}b + C(n, 2)\cdot a^{(n-2)}b^2 + \cdots + C(n, n-1)\cdot ab^{(n-1)} + b^n$, for a nonnegative integer n, and nonzero a and b.

EXAMPLE

Use mathematical induction to show that for n = 1, 2, 3, …, and $a > -1$,

$$(1 + a)^n \geq 1 + na.$$

(This is the **Bernoulli's Inequality** [Kurgalin, Borzunov, 2018, Chapter 1].)

Solution.

Basis Step. n = 1.

$$\text{LHS} = (1 + a) = \text{RHS}.$$

Inductive Step. n > 1.

It can be seen that,

LHS

$= (1 + a)^{(n+1)}$
$= (1 + a)^n \cdot (a + b)$
$\geq (1 + na) \cdot (a + b)$
$= 1 + (n + 1)a + na^2$
$\geq 1 + (n + 1)a$, since $na^2 \geq 0$

= RHS.

Therefore, by the Principle of Mathematical Induction, $(1 + a)^n \geq 1 + na$, for for n = 1, 2, 3, …, and $a > -1$.

18.7. STRONG INDUCTION

In some cases, a **stronger version** of induction is needed that allows **going back** to **values smaller** than just the previous value of n.

A **comparison** between the Fibonacci Sequence and the sequence 2^n is of interest.

$\{f_n\}$ = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, and so on.

$\{2^n\}$ = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, and so on.

EXAMPLE [INCOMPLETE]

For all n, the terms of the Fibonacci Sequence satisfy the following:

$$f_n < 2^n.$$

Proof.

Basis Step. n = 0.

$$f_0 = 0 < 1 = 2^0.$$

Inductive Step. n > 0.

$$f_n = f_{n-1} + f_{n-2} < 2^{n-1} + f_{n-2},$$

by applying the inductive hypothesis to n – 1.

It is of interest to apply the same to n – 2; however, that is **not** possible with the **conventional** form of mathematical induction.

This **motivates** an **extension** of the conventional form of mathematical induction.

18.8. SECOND PRINCIPLE OF MATHEMATICAL INDUCTION (STRONG INDUCTION)

If:

[**Basis**]
$P(0)$ (at times, more base cases may be needed)
[**Strong Induction**]
$\forall n\,[P(0) \wedge P(1) \wedge \cdots \wedge P(n)] \longrightarrow P(n+1)$

Then:

$\forall n\, P(n)$

EXAMPLE

For all n, the terms of the Fibonacci Sequence satisfy the following:

$$f_n < 2^n.$$

Solution.

Basis Step. n = 0 and n = 1.

There is a need for **both** base cases, n = 0 and n = 1. This is because the inductive step **cannot** be applied on f_1 since f_{-1} is **undefined**.

n = 0:
$f_0 = 0 < 1 = 2^0$.

n = 1:
$f_1 = 1 < 2 = 2^1$.

Inductive Step. n > 1.

$$f_n = f_{n-1} + f_{n-2} < 2^{n-1} + 2^{n-2}.$$

This is a result of applying **both** $P(n-1)$ and $P(n-2)$, which can be assumed to be true by strong inductive hypothesis.

Now,

$$2^{n-1} + 2^{n-2} = 2 \cdot 2^{n-2} + 2^{n-2} = (2+1) \cdot 2^{n-2} < 2^2 \cdot 2^{n-2} = 2^n.$$

Therefore, $f_n < 2^n$.

Therefore, by the Second Principle of Mathematical Induction, $f_n < 2^n$.

EXAMPLE

Use strong induction to show that every positive integer n can be written as a sum of distinct powers of 2.

Solution.

Basis Step.

$$1 = 2^0,$$
$$2 = 2^1,$$
$$3 = 2^1 + 2^0,$$
$$4 = 2^2,$$
$$5 = 2^2 + 2^0,$$

and so on. Indeed, this is the **representation of a number in binary form** (that is, base two).

Inductive Step.

The strong inductive hypothesis suggests that every positive integer up to k can be written as a sum of distinct powers of 2.

The goal is to show that k + 1 can be written as a sum of distinct powers of 2.

Case 1: k + 1 is odd.

Then, k is even, and so 2^0 is not part of the sum for k. Therefore, the sum for k + 1 is the same as the sum for k with the extra term 2^0 added.

Case 2: k + 1 is even.

Then, (k + 1)/2 is a positive integer, and so by the inductive hypothesis (k + 1)/2 can be written as a sum of distinct powers of 2. Now, increasing each exponent by 1 doubles the value and yields the desired sum for k + 1.

19. GEOMETRIC PROOFS: "THE PROOF IS IN THE PICTURE"

There can be **proofs without words** [Nelsen, 1983; Nelsen, 2000; Alsina, Nelsen, 2006; Brown, 2008; Nelsen, 2015], as shown in Figures 7 to 9.

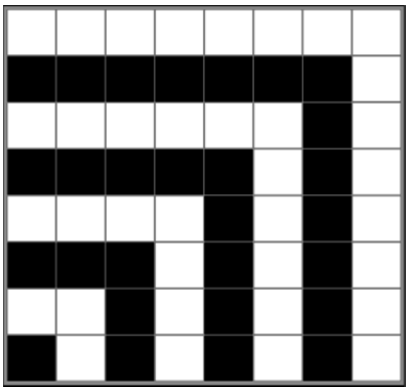


Figure 7. $1 + 3 + \cdots + (2n - 1) = n^2$. (Source: Wikipedia.)

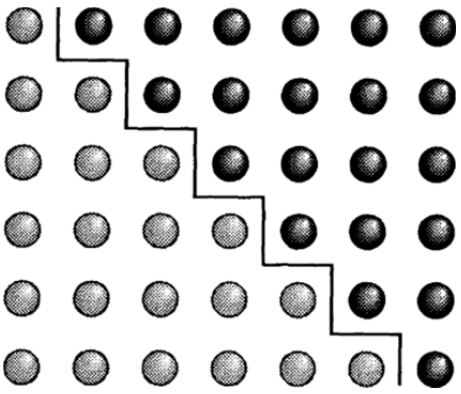


Figure 8. $1 + 2 + \cdots + n = n(n + 1)/2$. (Source: [Nelsen, 1983].)

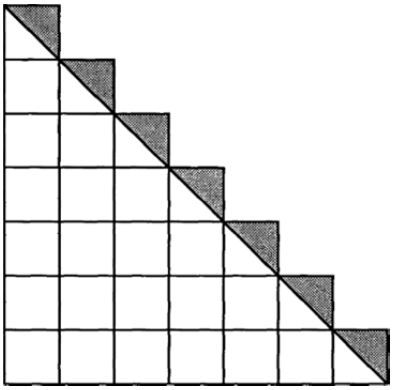


Figure 9. $1 + 2 + \cdots + n = (n^2/2) + n/2$. (Source: [Nelsen, 1983].)

The geometric proofs do have their **limitations**. For example, a diagram, by its very nature, must be **specific rather than generic**. For another example, a diagram, by its very nature, must be **constrained by space**. This prevents the use of a diagram to represent a large number of elements. Therefore, geometric proofs are usually used as an addition to, rather than a substitution of, algebraic proofs.

20. RECURSION

To iterate is human, to recurse, divine.
— Peter Deutsch

Recursion is the root of computation since it trades description for time.
— Alan Perlis

There are many applications of recursion in computer programming [Rohl, 1984].

EXAMPLE

The following is a **simple recursive definition of a tree** (that is, the tree is defined in terms of itself):

1. A tree is a trunk with two shorter branches emanating of the top of it at a right angle to each other.
2. A branch is a tree.

This definition can be used to construct a tree, as shown in Figure 10.

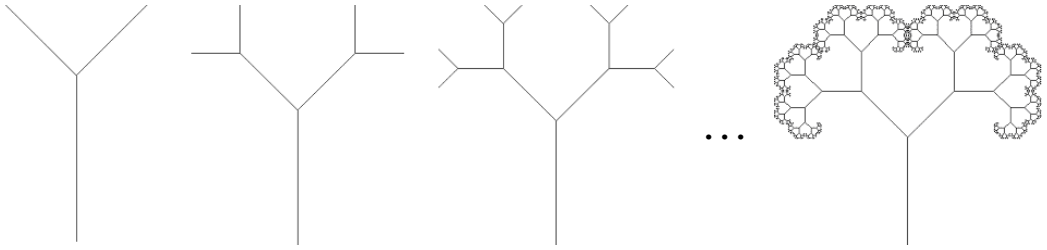


Figure 10. The process of constructing a tree recursively. (Source: Google Images.)

It could be noted that first, a tree is a trunk with two branches; second, each branch is a tree, third, each of those branches is a tree; and so on, leading to a structure that approximates an actual tree.

20.1. RECURSION FOR SETS

A **recursive definition of a set** is used to define the elements in a set S in terms of other elements in S.

EXAMPLE

The set **N** of natural numbers can be defined recursively:

(1) 0 is in **N**.
(2) If an element n is in **N**, then n + 1 is in **N**.
(3) **N** is the smallest set satisfying (1) and (2).

(1) is called the **base case**. (2) and (3) are called the **recursive case**.

20.2. RECURSION FOR FUNCTIONS

A **recursive definition of a function** defines values of the functions for some inputs in terms of the values of the same function for other inputs.

EXAMPLE

The **Factorial Function** can be defined recursively by:

(1) $0! = 1$.
(2) $(n + 1)! = (n + 1)\cdot n!$.

(1) is called the **base case**. (2) is called the **recursive case**.

For example, $6! = 6 \cdot 5! = 6 \cdot 5 \cdot 4! = \cdots = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

EXAMPLE

Let f(n) be defined recursively by f(0) = 3 and for n = 0, 1, 2, …

$$f(n + 1) = 3^{f(n)/3}.$$

Find f(100).

Solution.

It can be noted that

$$f(1) = 3^{f(0)/3} = 3^{3/3} = 3 = f(0).$$

Therefore,

$$f(100) = f(99) = \cdots = f(0) = 3.$$

EXAMPLE

Let f be defined recursively by f(0) = f(1) = 1 and for n = 1, 2, 3, …

$$f(n + 1) = f(n) / f(n - 1).$$

Find f(100).

Solution.

It can be noted that

$$f(2) = f(1) / f(0) = 1.$$

Therefore,

$$f(100) = f(99) = \cdots = f(0) = 1.$$

EXAMPLE

Give a recursive definition of the sequence $\{a_n\}$, n = 1, 2, 3, … if

(a) $a_n = 4n - 2$.
(b) $a_n = 1 + (-1)^n$.

Solution.

(a)

It can be noted that

$$a_1 = 2, a_2 = 6, a_3 = 10, a_4 = 14, \ldots$$

In other words, the terms of the sequence have a **pattern**, namely each term is 4 more than the term before it.

Therefore, it is possible to have a recursive definition of the sequence $\{a_n\}$ as

$$a_1 = 2 \text{ and } a_{n+1} = a_n + 4 \text{ for } n \geq 1.$$

(b)

It can be noted that

$$a_1 = 0, a_2 = 2, a_3 = 0, a_4 = 2, \ldots$$

In other words, the terms of the sequence **alternate**.

Therefore, it is possible to have a recursive definition of the sequence $\{a_n\}$ as

$$a_1 = 0, a_2 = 2, \text{ and } a_n = a_{n-2} \text{ for } n \geq 3.$$

EXAMPLE

In each of the following cases, determine whether the proposed definition is a valid recursive definition of a function f from the set of nonnegative integers to the set of integers. If f is well-defined, find a formula for f(n) when n is a nonnegative integer and prove that the formula is valid.

(a) $f(0) = 1$ and $f(n) = -f(n - 1)$, for $n \geq 1$.
(b) $f(0) = 0$, $f(1) = 1$, and $f(n) = 2f(n + 1)$, for $n \geq 2$.

Solution.

(a)

This is **valid** because the value of f at $n = 0$ has been provided, and each subsequent value can be determined by the previous one.

It can be noted that all that changes from one value to the next is the **sign**. Therefore, it could be **conjectured** that

$$f(n) = (-1)^n.$$

Basis Step. $n = 0$.

$$(-1)^0 = 1.$$

Inductive Step. $n \geq 1$.

$$f(k + 1) = -f(k + 1 - 1) = -f(k) = -(-1)^k = (-1)^{k+1}.$$

Therefore, by the Principle of Strong Mathematical Induction, $f(n) = (-1)^n$, for $n \geq 0$.

(b)

This is **invalid** because the formula says that f(2) is defined in terms of f(3), but f(3) has **not** been defined.

20.3. RECURSION FOR TREES

Definition [Rooted Tree]. A tree in which **one vertex** has been designated as the root and every edge is **directed away** from the root.

Definition [Rooted Binary Tree]. A rooted binary tree in which every vertex has at most two children.

Definition [Full Binary Tree]. A tree in which every vertex has either 0 or 2 children.

A full binary tree can also be defined **recursively**:

1. **Basis Step.** A single vertex.

2. **Recursive Step.** A graph formed by taking two (full) binary trees, adding a vertex, and adding an edge directed from the new vertex to the root of each binary tree.

EXAMPLE

Figure 11 shows how a rooted tree is constructed recursively.

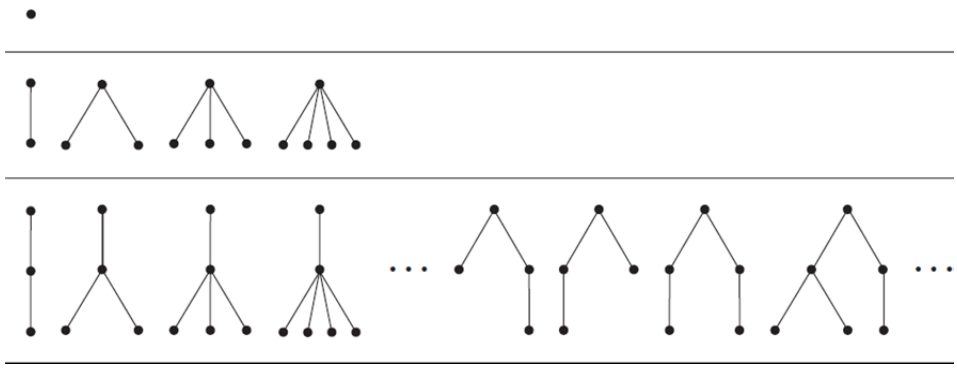


Figure 11. The process of constructing rooted trees recursively. (Source: [Rosen, 2012].)

EXAMPLE

Figure 12 shows how a full binary tree is constructed recursively.

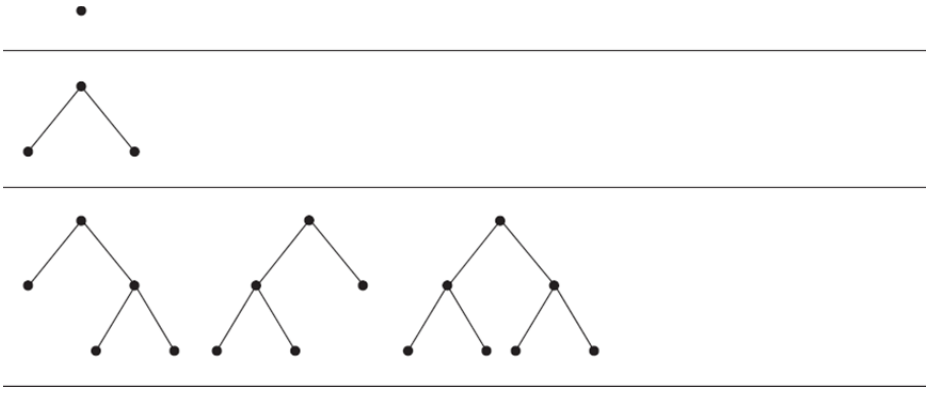


Figure 12. The process of constructing full binary trees recursively. (Source: [Rosen, 2012].)

Definition [Height of Full Binary Tree]. The height, h(T), of a full binary tree, T, can be defined **recursively**:

1. **Basis Step.** The height of T consisting of only a single vertex is h(T) = 0.

2. **Recursive Step.** If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 \cdot T_2$ has height $h(T) = 1 + \max(h(T_1), h(T_2))$.

Definition [Number of Vertices in Full Binary Tree]. The number of vertices, n(T), of a full binary tree, T, can be defined **recursively**:

1. **Basis Step.** The number of vertices in T consisting of only a single vertex is n(T) = 1.

2. **Recursive Step.** If T_1 and T_2 are full binary trees, then the number of vertices of the full binary tree $T = T_1 \cdot T_2$ is $n(T) = 1 + n(T_1) + n(T_2)$.

The next theorem shows that **h(T) and n(T) are related**. In fact, it sets the **lower and upper bounds** on n(T) in terms of h(T).

Theorem. If T is a full binary tree T, then

$$2h(T) + 1 \leq n(T) \leq 2^{h(T)+1} - 1.$$

Proof. This is a proof by **structural induction**. There are two parts, one for each inequality.

(1)

Basis Step. h(T) = 0.

LHS = $2 \cdot 0 + 1 = 1$.

RHS = n(T) = 1.

Thus, LHS ≤ RHS, and the inequality is satisfied.

Recursive Step. $h(T) > 0$.

It is assumed that for full binary trees T_1 and T_2,

$$2h(T_1) + 1 \leq n(T_1)$$

and

$$2h(T_2) + 1 \leq n(T_2).$$

Furthermore, from the recursive definitions of n(T) and h(T),

$$n(T) = 1 + n(T_1) + n(T_2)$$

and

$$h(T) = 1 + \max(h(T_1), h(T_2)).$$

Now,

$n(T)$

$= 1 + n(T_1) + n(T_2)$

$\geq 1 + 2h(T_1) + 1 + 2h(T_2) + 1$, by inductive hypothesis

$\geq 1 + 2 \cdot \max(h(T_1), h(T_2)) + 2$

$= 1 + 2 \cdot (\max(h(T_1), h(T_2)) + 1)$

$= 1 + 2h(T)$.

Thus, LHS $\leq$ RHS, and the inequality is satisfied.

(2)

Basis Step. $h(T) = 0$.

LHS = $n(T) = 1$.

RHS = $2^{0+1} - 1 = 1$.

Thus, LHS ≤ RHS, and the inequality is satisfied.

Recursive Step. h(T) > 0.

It is assumed that for full binary trees T_1 and T_2,

$$n(T_1) \leq 2^{h(T_1)+1} - 1$$

and

$$n(T_2) \leq 2^{h(T_2)+1} - 1.$$

Furthermore, from the recursive definitions of n(T) and h(T),

$$n(T) = 1 + n(T_1) + n(T_2)$$

and

$$h(T) = 1 + \max(h(T_1), h(T_2)).$$

Now,

n(T)

$= 1 + n(T_1) + n(T_2)$

$\leq 1 + (2^{h(T_1)+1} - 1) + (2^{h(T_2)+1} - 1)$, by inductive hypothesis

$\leq 2 \cdot \max(2^{h(T_1)+1}, 2^{h(T_2)+1}) - 1$

$= 2 \cdot (2^{\max(h(T_1), h(T_2))+1}) - 1$, since $\max(2^x, 2^y) = 2^{\max(x, y)}$

$= 2 \cdot 2^{h(T)} - 1$

$= 2^{h(T)+1} - 1$.

Thus, LHS ≤ RHS, and the inequality is satisfied.

■

EXAMPLE [FOR INQUISITIVENESS AND NOT FOR FAINT OF HEART ONLY]

There is a close relationship between recursion and fractals [Gulick, Scott, 2010].

For example, the **Koch Curve** can be constructed recursively[4], as shown in Figure 13.

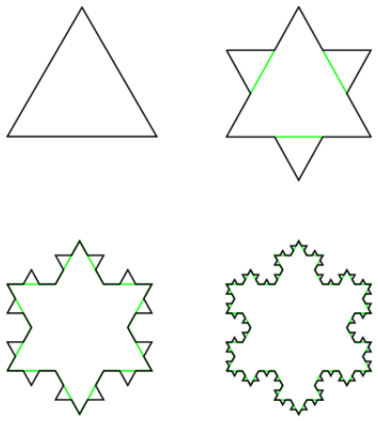


Figure 13. A recursively-generated Koch Curve. (Source: Wikipedia.)

21. CONCLUSION

The **ability to reason mathematically** is important in several technically-oriented disciplines, including computer science and engineering.

In particular, such reasoning is considered significant in discrete mathematics in order to establish or to verify results [Rosen, 2012]. Indeed, many such results are an outcome of mathematical reasoning and rely intimately on the notion of proof [Sundstrom, 2014].

ACKNOWLEDGEMENT

This document has benefited from the Lecture Notes on Discrete Mathematics by Eusebius Doedel, especially from the examples therein. The Tree Trunk example is due to Christopher Jennings. The inclusion of images from external sources is only for non-commercial educational purposes, and their use is hereby acknowledged. In particular, the author is grateful to Richard J. Kinch for the use of the 'dangerous bend' symbol.

[4] This is done by starting with an equilateral triangle, and then recursively altering each line segment as follows: (1) divide the line segment into three segments of equal length, (2) draw an equilateral triangle that has the middle segment from (1) as its base and points outward, and (3) remove the line segment that is the base of the triangle from (2).

REFERENCES

[Aigner, Ziegler, 2014] Proofs from THE BOOK. By M. Aigner, G. M. Ziegler. Fifth Edition. Springer-Verlag. 2014.

[Alsina, Nelsen, 2006] Math Made Visual: Creating Images for Understanding Mathematics. By C. Alsina, R. Nelsen. Mathematical Association of America. 2006.

[Beck, Geoghegan, 2010] The Art of Proof: Basic Training for Deeper Mathematics. By M. Beck, R. Geoghegan. Springer. 2010.

[Bloch, 2011] Proofs and Fundamentals: A First Course in Abstract Mathematics. By E. D. Bloch. Second Edition. Springer Science+Business Media. 2011.

[Bourchtein, Bourchtein, 2015] CounterExamples: From Elementary Calculus to the Beginnings of Analysis. By A. Bourchtein, L. Bourchtein. CRC Press. 2015.

[Bramanti, Travaglini, 2018] Studying Mathematics: The Beauty, the Toil and the Method. By M. Bramanti, G. Travaglini. Springer International Publishing. 2018.

[Brown, 2008] Philosophy of Mathematics: A Contemporary Introduction to the World of Proofs and Pictures. By J. R. Brown. Second Edition. Routledge. 2008.

[Bruce, Drysdale, Kelemen, Tucker, 2007] Why Math? By K. B. Bruce, R. L. S. Drysdale, C. Kelemen, A. Tucker. Communications of the ACM. Volume 46. Issue 9. 2003. Pages 41-44.

[Bunch, 1982] Mathematical Fallacies and Paradoxes. By B. Bunch. Dover Publications. 1982.

[Calude, Calude, Marcus, 2007] Proving and Programming. By C. S. Calude, E. Calude, S. Marcus. CDMTCS Research Reports CDMTCS-309. Department of Computer Science. The University of Auckland. Auckland, New Zealand. 2007.

[Calude, Marcus, 2004] Mathematical Proofs at a Crossroad? By C. S. Calude, S. Marcus. CDMTCS Research Reports CDMTCS-236. Department of Computer Science. The University of Auckland. Auckland, New Zealand. 2004.

[Chartrand, Polimeni, Zhang, 2013] Mathematical Proofs: A Transition to Advanced Mathematics. By G. Chartrand, A. D. Polimeni, P. Zhang. Third Edition. Pearson Education. 2013.

[Chemla, 2012] The History of Mathematical Proof in Ancient Traditions. By K. Chemla. Cambridge University Press. 2012.

[Cunningham, 2012] A Logical Introduction to Proof. By D. W. Cunningham. Springer Science+Business Media. 2012.

[Cupillari, 2013] The Nuts and Bolts of Proofs: An Introduction to Mathematical Proofs. By A. Cupillari. Fourth Edition. Academic Press. 2013.

[Dawson, 2015] Why Prove it Again? Alternative Proofs in Mathematical Practice. By J. W. Dawson, Jr. Springer International Publishing. 2015.

[Detlefsen, 1992] Proof and Knowledge in Mathematics. By M. Detlefsen (Editor). Routledge. 1992.

[Dougherty, 2017] Where Mathematics Meets Software Engineering. By J. P. Dougherty. ACM Inroads. Volume 8. Number 3. 2017. Pages 13-15.

[Dowek, 2011] Proofs and Algorithms: An Introduction to Logic and Computability. By G. Dowek. Springer-Verlag. 2011.

[Erickson, 2010] Pearls of Discrete Mathematics. By M. Erickson. CRC Press. 2010.

[Franklin, Daoud, 1988] Introduction to Proofs in Mathematics. By J. Franklin, A. Daoud. Prentice-Hall. 1988.

[Gallier, 2011] Discrete Mathematics. By J. Gallier. Springer Science+Business Media. 2011.

[Gerstein, 2012] Introduction to Mathematical Structures and Proofs. By L. J. Gerstein. Springer Science+Business Media. 2012.

[Grieser, 2018] Exploring Mathematics: Problem-Solving and Proof. By D. Grieser. Springer International Publishing. 2018.

[Gulick, Scott, 2010] The Beauty of Fractals: Six Different Views. By D. Gulick, J. Scott (Editors). The Mathematical Association of America. 2010.

[Gunderson, 2010] Handbook of Mathematical Induction: Theory and Applications. By D. S. Gunderson. CRC Press. 2010.

[Hammack, 2009] Book of Proof. By R. Hammack. Virginia Commonwealth University. Richmond, U.S.A. 2009.

[Hammack, 2013] Book of Proof. By R. Hammack. Second Edition. Virginia Commonwealth University. Richmond, U.S.A. 2013.

[Hartwig, 2011] On the Relationship between Proof Writing and Programming: Some Conclusions for Teaching Future Software Developers. By M. Hartwig. The Second International Conference on Software Engineering and Computer Systems (ICSECS 2011). Kuantan, Malaysia. June 27-29, 2011.

[Henderson, 2003] Mathematical Reasoning in Software Engineering Education. By P. B. Henderson. Communications of the ACM. Volume 46. Issue 9. 2003. Pages 45-50.

[Herrmann, 2012] The Beauty of Everyday Mathematics. By N. Herrmann. Springer-Verlag. 2012.

[Houston, 2009] How to Think Like a Mathematician: A Companion to Undergraduate Mathematics. By K. Houston. Cambridge University Press. 2009.

[IEEE, 2014] Guide to the Software Engineering Body of Knowledge (SWEBOK) Version 3.0. The Institute of Electrical and Electronics Engineers (IEEE) Computer Society. 2014.

[Joshi, 2015] Proof Patterns. By M. Joshi. Springer International Publishing. 2015.

[Kane, 2016] Writing Proofs in Analysis. By J. M. Kane. Springer International Publishing. 2016.

[Khare, Lachowska, 2015] Beautiful, Simple, Exact, Crazy: Mathematics in the Real World. By A. Khare, A. Lachowska. Yale University Press. 2015.

[Kleinberg, 2016] Why: A Guide to Finding and Using Causes. By S. Kleinberg. O'Reilly Media. 2016.

[Kugel, 1976] On Uninteresting Theorems. By P. Kugel. ACM SIGACT News. Volume 8. Issue 1. 1976. Pages 27-29.

[Kurgalin, Borzunov, 2018] The Discrete Math Workbook: A Companion Manual for Practical Study. By S. Kurgalin, S. Borzunov. Springer International Publishing. 2018.

[Laczkovich, 2001] Conjecture and Proof. By M. Laczkovich. The Mathematical Association of America. 2001.

[Lehman, Leighton, Meyer, 2012] Mathematics for Computer Science. By E. Lehman, F. T. Leighton, A. R. Meyer. January 4, 2012.

[Maor, Jost, 2014] Beautiful Geometry. By E. Maor, E. Jost. Princeton University Press. 2014.

[Mclnerny, 2004] Being Logical: A Guide to Good Thinking. By D. Q. Mclnerny. Random House. 2004.

[Nelsen, 1983] Proofs Without Words: Further Exercises in Visual Thinking. By R. B. Nelsen. The Mathematical Association of America. 1983.

[Nelsen, 2000] Proofs Without Words II: Further Exercises in Visual Thinking. By R. B. Nelsen. The Mathematical Association of America. 2000.

[Nelsen, 2015] Proofs Without Words III: Further Exercises in Visual Thinking. By R. B. Nelsen. The Mathematical Association of America. 2015.

[Neto, 2017] An Excursion through Elementary Mathematics, Volume I: Real Numbers and Functions. By A. C. M. Neto. Springer International Publishing. 2017.

[Nickerson, 2010] Mathematical Reasoning: Patterns, Problems, Conjectures, and Proofs. By R. S. Nickerson. Psychology Press. 2010.

[O'Donnell, Hall, Page, 2006] Discrete Mathematics Using a Computer. By J. O'Donnell, C. Hall, R. Page. Second Edition. Springer-Verlag. 2006.

[Ording, 2019] 99 Variations on a Proof. By P. Ording. Princeton University Press. 2019.

[O'Regan, 2016] Guide to Discrete Mathematics: An Accessible Introduction to the History, Theory, Logic and Applications. By G. O'Regan. Springer International Publishing. 2016.

[Reba, Shier, 2015] Puzzles, Paradoxes, and Problem Solving: An Introduction to Mathematical Thinking. By M. A. Reba, D. R. Shier. CRC Press. 2015.

[Roberts, 2010] Introduction to Mathematical Proofs: A Transition. By C. E. Roberts, Jr. CRC Press. 2010.

[Rohl, 1984] Recursion via Pascal. By J. S. Rohl. Cambridge University Press. 1984.

[Rosen, 2012] Discrete Mathematics and Its Applications. By K. H. Rosen. Seventh Edition. McGraw-Hill. 2012.

[Rossi, 2006] Theorems, Corollaries, Lemmas, and Methods of Proof. By R. J. Rossi. John Wiley and Sons. 2006.

[Scheinerman, 2013] Mathematics: A Discrete Introduction. By E. R. Scheinerman. Third Edition. Brooks/Cole. 2013.

[Sedgewick, Wayne, 2015] Introduction to Programming in Python: An Interdisciplinary Approach. By R. Sedgewick, K. Wayne. Addison-Wesley. 2015.

[Solow, 2014] How to Read and Do Proofs: An Introduction to Mathematical Thought Processes. By D. Solow. Sixth Edition. John Wiley and Sons. 2014.

[Stewart, Tall, 2015] The Foundations of Mathematics. By I. Stewart, D. Tall. Second Edition. Oxford University Press. 2015.

[Sundstrom, 2014] Mathematical Reasoning: Writing and Proof. By T. Sundstrom. Version 1.1. Grand Valley State University. Allendale, U.S.A. February 16, 2014.

[Sundstrom, 2018] Mathematical Reasoning: Writing and Proof. By T. Sundstrom. Version 2.1. Grand Valley State University. Allendale, U.S.A. October 16, 2018.

[Taylor, Garnier, 2014] Understanding Mathematical Proof. By J. Taylor, R. Garnier. CRC Press. 2014.

[Thomas, 2016] Beauty Is Not All There Is To Aesthetics in Mathematics. By R. S. D. Thomas. Philosophia Mathematica. Volume 25. Number 1. 2016. Pages 116-127.

[Velleman, 2006] How To Prove It: A Structured Approach. By D. J. Velleman. Second Edition. Cambridge University Press. 2006.

[Vivaldi, 2014] Mathematical Writing. By F. Vivaldi. Springer-Verlag. 2014.

[Wing, 2006] Computational Thinking. By J. M. Wing. Communications of the ACM. Volume 49. Number 3. 2006. Pages 33-35.

APPENDIX A. QUESTIONING THE NATURE OF PROOF: WHAT IS A PROOF, REALLY?

The notion of proof has changed over time, especially with the advent of machines (computers). It was believed for centuries that proof must be written, read, and verified by a human. However, in the past few decades, with using computers, people have been able to prove statements that were considered impossible previously by humans. In some of these cases, such proofs are also impossible to verify by humans [Calude, Marcus, 2004].